



## **Fireware XTM**

# **WatchGuard System Manager 11.4 User Guide**

---

WatchGuard XTM Devices

---

## About this User Guide

The *Fireware XTM WatchGuard System Manager User Guide* is updated with each major product release. For minor product releases, only the *Fireware XTM WatchGuard System Manager Help* system is updated. The Help system also includes specific, task-based implementation examples that are not available in the *User Guide*.

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Guide revised: 1/26/2011

## Copyright, Trademark, and Patent Information

Copyright © 1998-2011 WatchGuard Technologies, Inc. All rights reserved. All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

**Note** *This product is for indoor use only.*

---

## About WatchGuard

WatchGuard offers affordable, all-in-one network and content security solutions that provide defense-in-depth and help meet regulatory compliance requirements. The WatchGuard XTM line combines firewall, VPN, GAV, IPS, spam blocking and URL filtering to protect your network from spam, viruses, malware, and intrusions. The new XCS line offers email and web content security combined with data loss prevention. WatchGuard extensible solutions scale to offer right-sized security ranging from small businesses to enterprises with 10,000+ employees. WatchGuard builds simple, reliable, and robust security appliances featuring fast implementation and comprehensive management and reporting tools. Enterprises throughout the world rely on our signature red boxes to maximize security without sacrificing efficiency and productivity.



# Table of Contents

---

<b>Introduction to Network Security</b> .....	<b>1</b>
About Networks and Network Security.....	1
About Internet Connections.....	1
About Protocols.....	2
About IP Addresses.....	3
Private Addresses and Gateways.....	3
About Subnet Masks.....	3
About Slash Notation.....	3
About Entering IP Addresses.....	4
Static and Dynamic IP Addresses.....	4
About DNS (Domain Name System).....	5
About Firewalls.....	6
About Services and Policies.....	7
About Ports.....	8
<b>Introduction to Fireware XTM</b> .....	<b>9</b>
About Fireware XTM.....	9
Fireware XTM Components.....	10
WatchGuard System Manager.....	10
WatchGuard Server Center.....	11
Fireware XTM Web UI and Command Line Interface.....	12
Fireware XTM with a Pro Upgrade.....	13
<b>Service and Support</b> .....	<b>15</b>
About WatchGuard Support.....	15
LiveSecurity Service.....	15
LiveSecurity Service Gold.....	16
Service Expiration.....	16
<b>Getting Started</b> .....	<b>17</b>
Before You Begin.....	17
Verify Basic Components.....	17
Get an XTM Device Feature Key.....	18

---

Gather Network Addresses.....	18
Select a Firewall Configuration Mode.....	19
Decide Where to Install Server Software.....	20
Install WatchGuard System Manager Software.....	20
Back up Your Previous Configuration.....	20
Download WatchGuard System Manager.....	21
About Software Encryption Levels.....	22
About the Quick Setup Wizard.....	22
Run the Web Setup Wizard.....	23
Run the WSM Quick Setup Wizard.....	26
Complete Your Installation.....	28
Customize Your Security Policy.....	28
About LiveSecurity Service.....	28
Start WatchGuard System Manager.....	29
Connect to an XTM Device.....	29
Start WSM Applications.....	30
Additional Installation Topics.....	32
Install WSM and Keep an Older Version.....	32
Install WatchGuard Servers on Computers with Desktop Firewalls.....	32
Dynamic IP Support on the External Interface.....	33
About Connecting the XTM Device Cables.....	33
Connect to an XTM Device with Firefox v3.....	34
Disable the HTTP Proxy in the Browser.....	35
Find Your TCP/IP Properties.....	36
<b>Configuration and Management Basics.....</b>	<b>39</b>
About Basic Configuration and Management Tasks.....	39
About Configuration Files.....	39
Open a Configuration File.....	39
Make a New Configuration File.....	41
Save the Configuration File.....	42
Make a Backup of the XTM Device Image.....	43
Restore an XTM Device Backup Image.....	44

---

Use a USB Drive for System Backup and Restore.....	44
About the USB Drive.....	44
Save a Backup Image to a Connected USB Drive.....	45
Restore a Backup Image from a Connected USB Drive.....	45
Automatically Restore a Backup Image from a USB Drive.....	46
USB Drive Directory Structure.....	48
Save a Backup Image to a USB Drive Connected to Your Management Computer.....	49
Use a USB Drive to Save a Support Snapshot.....	49
Use an Existing Configuration for a New XTM Device Model.....	50
Upgrade a Non-e-Series Configuration File For Use With an e-Series or XTM Device.....	52
Configure a Replacement XTM Device.....	54
Save the Configuration from the Original XTM Device to a File.....	54
Get the Feature Key for the Replacement XTM Device.....	54
Use the Quick Setup Wizard to Configure Basic Settings.....	54
Update the Feature Key in the Original Configuration File and Save to the New Device.....	54
Reset an XTM Device to a Previous or New Configuration.....	55
Start an XTM Device in Safe Mode.....	55
Reset an XTM 2 Series Device to Factory-Default Settings.....	55
Run the Quick Setup Wizard.....	56
About Factory-Default Settings.....	56
About Feature Keys.....	58
When You Purchase a New Feature.....	58
See Features Available with the Current Feature Key.....	58
Verify Feature Key Compliance.....	59
Get a Feature Key from LiveSecurity.....	59
Add a Feature Key to Your XTM Device.....	62
See the Details of a Feature Key.....	64
Download a Feature Key.....	64
Enable NTP and Add NTP Servers.....	65
Set the Time Zone and Basic Device Properties.....	66
About SNMP.....	67
SNMP Polls and Traps.....	67

---

Enable SNMP Polling .....	68
Enable SNMP Management Stations and Traps .....	69
About Management Information Bases (MIBs) .....	71
About WatchGuard Passphrases, Encryption Keys, and Shared Keys .....	72
Create a Secure Passphrase, Encryption Key, or Shared Key .....	72
XTM Device Passphrases .....	73
User Passphrases .....	73
Server Passphrases .....	73
Encryption Keys and Shared Keys .....	74
Change XTM Device Passphrases .....	75
Define XTM Device Global Settings .....	76
Define ICMP Error Handling Global Settings .....	77
Configure TCP Settings .....	78
Enable or Disable Traffic Management and QoS .....	78
Change the Web UI Port .....	78
Automatic Reboot .....	79
Manage an XTM device from a Remote Location .....	79
Upgrade to a New Version of Fireware XTM .....	81
Install the Upgrade on Your Management Computer .....	81
Upgrade the XTM Device .....	82
Use Multiple Versions of Policy Manager .....	83
About Upgrade Options .....	83
Subscription Services Upgrades .....	83
Appliance and Software Upgrades .....	84
How to Apply an Upgrade .....	84
Renew Security Subscriptions .....	84
Renew Subscriptions from Firebox System Manager .....	85
<b>Network Setup and Configuration .....</b>	<b>87</b>
About Network Interface Setup .....	87
Network Modes .....	88
Interface Types .....	89
About Network Interfaces on the Edge e-Series .....	89

---

Mixed Routing Mode.....	90
Configure an External Interface.....	90
Configure DHCP in Mixed Routing Mode.....	94
About the Dynamic DNS Service.....	96
Use Dynamic DNS.....	96
Drop-In Mode.....	98
Use Drop-In Mode for Network Interface Configuration.....	98
Configure Related Hosts.....	99
Configure DHCP in Drop-In Mode.....	100
Bridge Mode.....	103
Common Interface Settings.....	105
Disable an Interface.....	108
Configure DHCP Relay.....	110
Restrict Network Traffic by MAC Address.....	110
Add WINS and DNS Server Addresses.....	111
Configure a Secondary Network.....	112
About Advanced Interface Settings.....	114
Network Interface Card (NIC) Settings.....	114
Set Outgoing Interface Bandwidth.....	116
Set DF Bit for IPSec.....	117
PMTU Setting for IPSec.....	117
Use Static MAC Address Binding.....	118
Find the MAC Address of a Computer.....	118
About LAN Bridges.....	119
Create a Network Bridge Configuration.....	119
Assign a Network Interface to a Bridge.....	121
About Routing.....	123
Add a Static Route.....	123
About Virtual Local Area Networks (VLANs).....	124
VLAN Requirements and Restrictions.....	124
About Tagging.....	125
About VLAN ID Numbers.....	125

---

Define a New VLAN.....	125
Assign Interfaces to a VLAN.....	129
Network Setup Examples.....	130
Configure Two VLANs on the Same Interface.....	130
Configure One VLAN Bridged Across Two Interfaces.....	133
Use Your XTM Device with the 3G Extend Wireless Bridge.....	138
<b>Multi-WAN.....</b>	<b>141</b>
About Using Multiple External Interfaces.....	141
Multi-WAN Requirements and Conditions.....	141
Multi-WAN and DNS.....	142
Multi-WAN and FireCluster.....	142
About Multi-WAN Options.....	142
Round-Robin Order.....	142
Failover.....	143
Interface Overflow.....	143
Routing Table.....	143
Serial Modem (XTM 2 Series only).....	144
Configure Round-Robin.....	145
Before You Begin.....	145
Configure the Interfaces.....	145
Find How to Assign Weights to Interfaces.....	147
Configure Failover.....	147
Before You Begin.....	147
Configure the Interfaces.....	147
Configure Interface Overflow.....	149
Before You Begin.....	149
Configure the Interfaces.....	149
Configure Routing Table.....	150
Before You Begin.....	150
Routing Table mode and load balancing.....	150
Configure the Interfaces.....	150
About the XTM Device Route Table.....	151

---

When to Use Multi-WAN Methods and Routing .....	152
Serial Modem Failover.....	153
Enable Serial Modem Failover.....	153
Account Settings.....	154
DNS Settings.....	154
Dial-up Settings.....	155
Advanced Settings.....	155
Link Monitor Settings.....	155
Advanced Multi-WAN Settings.....	157
About Sticky Connections.....	157
Set a Global Sticky Connection Duration.....	157
Set the Failback Action.....	158
About WAN Interface Status.....	159
Time Needed for the XTM Device to Update its Route Table.....	159
Define a Link Monitor Host .....	159
<b>Network Address Translation (NAT).....</b>	<b>161</b>
About Network Address Translation.....	161
Types of NAT.....	162
About Dynamic NAT.....	162
Add Firewall Dynamic NAT Entries.....	163
Configure Policy-Based Dynamic NAT.....	165
About 1-to-1 NAT.....	168
About 1-to-1 NAT and VPNs.....	169
Configure Firewall 1-to-1 NAT.....	169
Configure Policy-Based 1-to-1 NAT.....	172
Configure NAT Loopback with Static NAT.....	173
Add a Policy for NAT Loopback to the Server.....	174
NAT Loopback and 1-to-1 NAT.....	175
Configure Static NAT.....	179
Add a Static NAT Action.....	179
Add a Static NAT Action to a Policy.....	180
Edit or Remove a Static NAT Action.....	181

---

Configure Server Load Balancing .....	182
Add a Server Load Balancing SNAT Action .....	183
Add a Server Load Balancing SNAT Action to a Policy .....	185
Edit or Remove a Server Load Balancing SNAT Action .....	186
NAT Examples .....	187
1-to-1 NAT Example .....	187
<b>Wireless Setup .....</b>	<b>189</b>
About Wireless Configuration .....	189
About Wireless Access Point Configuration .....	190
Before You Begin .....	191
About Wireless Configuration Settings .....	192
Enable/Disable SSID Broadcasts .....	193
Change the SSID .....	193
Log Authentication Events .....	193
Change the Fragmentation Threshold .....	193
Change the RTS Threshold .....	195
About Wireless Security Settings .....	196
Set the Wireless Authentication Method .....	196
Use a RADIUS Server for Wireless Authentication .....	197
Use the XTM Device as an Authentication Server for Wireless Authentication .....	198
Set the Encryption Level .....	200
Enable Wireless Connections to the Trusted or Optional Network .....	201
Enable a Wireless Guest Network .....	204
Enable a Wireless Hotspot .....	207
Configure User Timeout Settings .....	208
Customize the Hotspot Splash Screen .....	208
Connect to a Wireless Hotspot .....	209
See Wireless Hotspot Connections .....	210
Configure Your External Interface as a Wireless Interface .....	211
Configure the Primary External Interface as a Wireless Interface .....	212
Configure a BOVPN tunnel for additional security .....	214
About Wireless Radio Settings .....	215



---

Country is Set Automatically.....	216
Select the Band and Wireless Mode.....	217
Select the Channel.....	217
Configure the Wireless Card on Your Computer.....	218
Rogue Access Point Detection.....	218
Enable Rogue Access Point Detection.....	218
Add an XTM Wireless Device as a Trusted Access Point.....	222
Find the Wireless MAC Address of a Trusted Access Point.....	225
Rogue Access Point Scan Results.....	226
<b>Dynamic Routing.....</b>	<b>227</b>
About Dynamic Routing.....	227
About Routing Daemon Configuration Files.....	227
About Routing Information Protocol (RIP).....	228
Routing Information Protocol (RIP) Commands.....	228
Configure the XTM Device to Use RIP v1.....	230
Configure the XTM Device to Use RIP v2.....	232
Sample RIP Routing Configuration File.....	234
About Open Shortest Path First (OSPF) Protocol.....	235
OSPF Commands.....	236
OSPF Interface Cost Table.....	239
Configure the XTM Device to Use OSPF.....	239
Sample OSPF Routing Configuration File.....	241
About Border Gateway Protocol (BGP).....	244
BGP Commands.....	245
Configure the XTM Device to Use BGP.....	247
Sample BGP Routing Configuration File.....	249
<b>FireCluster.....</b>	<b>251</b>
About WatchGuard FireCluster.....	251
FireCluster Status.....	253
About FireCluster Failover.....	253
Events that Trigger a Failover.....	253
What Happens When a Failover Occurs.....	254

---

FireCluster Failover and Server Load Balancing.....	254
Monitor the Cluster During a Failover.....	255
Features not Supported With FireCluster.....	255
FireCluster Network Configuration Limitations.....	255
FireCluster Management Limitations.....	255
About the Interface for Management IP Address.....	255
Configure the Interface for Management IP Address.....	255
Use the Management IP Address to Restore a Backup Image.....	256
Use the Management IP Address to Upgrade from an External Location.....	256
The Management IP Address and the WatchGuard Policy.....	257
Configure FireCluster.....	257
FireCluster Requirements and Restrictions.....	258
Cluster Synchronization and Status Monitoring.....	258
FireCluster Device Roles.....	259
FireCluster Configuration Steps.....	259
Before You Begin.....	260
Connect the FireCluster Hardware.....	262
Switch and Router Requirements for an Active/Active FireCluster.....	263
Use the FireCluster Setup Wizard.....	269
Configure FireCluster Manually.....	274
Find the Multicast MAC Addresses for an Active/Active Cluster.....	280
Active/Passive Cluster ID and the Virtual MAC Address.....	281
Monitor and Control FireCluster Members.....	282
Monitor Status of FireCluster Members.....	283
Monitor and Control Cluster Members.....	284
Discover a Cluster Member.....	284
Force a Failover of the Cluster Master.....	285
Reboot a Cluster Member.....	286
Shut Down a Cluster Member.....	286
Connect to a Cluster Member.....	287
Make a Member Leave a Cluster.....	288
Make a Member Join a Cluster.....	289

---

Remove or Add a Cluster Member.....	290
Remove a Device from a FireCluster.....	290
Add a New Device to a FireCluster.....	291
Update the FireCluster Configuration.....	291
Configure FireCluster Logging and Notification.....	292
About Feature Keys and FireCluster.....	292
See the Feature Keys and Cluster Features for a Cluster.....	293
See or Update the Feature Key for a Cluster Member.....	294
See the FireCluster Feature Key in Firebox System Manager.....	296
Create a FireCluster Backup Image.....	297
Restore a FireCluster Backup Image.....	298
Make the Backup Master Leave the Cluster.....	298
Restore the Backup Image to the Backup Master.....	298
Restore the Backup Image to the Cluster Master.....	298
Make the Backup Master Rejoin the Cluster.....	299
Upgrade Fireware XTM for FireCluster Members.....	299
Disable FireCluster.....	301
<b>Authentication.....</b>	<b>303</b>
About User Authentication.....	303
User Authentication Steps.....	304
Manage Authenticated Users.....	305
Use Authentication to Restrict Incoming Traffic.....	306
Use Authentication Through a Gateway Firebox.....	307
About the WatchGuard Authentication (WG-Auth) Policy.....	308
Set Global Firewall Authentication Values.....	308
Set Global Authentication Timeouts.....	309
Allow Multiple Concurrent Logins.....	310
Limit Login Sessions.....	310
Automatically Redirect Users to the Authentication Portal.....	311
Use a Custom Default Start Page.....	312
Set Management Session Timeouts.....	312
About Single Sign-On (SSO).....	312

---

Before You Begin.....	314
Set Up SSO.....	314
Install the WatchGuard Single Sign-On (SSO) Agent.....	314
Configure the SSO Agent.....	315
Install the WatchGuard Single Sign-On (SSO) Client.....	319
Enable Single Sign-On (SSO).....	320
Install and Configure the Terminal Services Agent.....	324
Install the Terminal Services Agent.....	325
Configure the Terminal Services Agent.....	325
Configure Terminal Services Settings.....	326
Authentication Server Types.....	328
About Third-Party Authentication Servers.....	328
Use a Backup Authentication Server.....	328
Configure Your XTM Device as an Authentication Server.....	329
Types of Firebox Authentication.....	329
Define a New User for Firebox Authentication.....	332
Define a New Group for Firebox Authentication.....	334
Configure RADIUS Server Authentication.....	335
Authentication Key.....	335
RADIUS Authentication Methods.....	335
Before You Begin.....	335
Use RADIUS Server Authentication with Your XTM Device.....	335
How RADIUS Server Authentication Works.....	337
WPA and WPA2 Enterprise Authentication.....	340
Configure VASCO Server Authentication.....	340
Configure SecurID Authentication.....	343
Configure LDAP Authentication.....	345
About LDAP Optional Settings.....	347
Configure Active Directory Authentication.....	348
Add an Active Directory Authentication Domain and Server.....	348
About Active Directory Optional Settings.....	352
Edit an Existing Active Directory Domain.....	352

---

Delete an Active Directory Domain.....	354
Find Your Active Directory Search Base.....	354
Change the Default Port for the Active Directory Server.....	355
Use Active Directory or LDAP Optional Settings.....	356
Before You Begin.....	356
Specify Active Directory or LDAP Optional Settings.....	357
Use a Local User Account for Authentication.....	360
Use Authorized Users and Groups in Policies.....	360
Define Users and Groups for Firebox Authentication.....	360
Define Users and Groups for Third-Party Authentication.....	360
Add Users and Groups to Policy Definitions.....	361
<b>Policies.....</b>	<b>363</b>
About Policies.....	363
Packet Filter and Proxy Policies.....	363
Add Policies to Your XTM device.....	364
About Policy Manager.....	364
Open Policy Manager.....	366
About Policy Manager Views.....	367
Change Colors Used for Policy Manager Text.....	369
Find a Policy by Address, Port, or Protocol.....	371
Add Policies to Your Configuration.....	372
See the List of Policy Templates.....	372
Add a Policy from the List of Templates.....	374
Add More than One Policy of the Same Type.....	376
See Template Details and Modify Policy Templates.....	376
Disable or Delete a Policy.....	377
About Aliases.....	378
Alias Members.....	378
Create an Alias.....	379
About Policy Precedence.....	383
Automatic Policy Order.....	383
Policy Specificity and Protocols.....	384

---

Traffic Rules.....	384
Firewall Actions.....	385
Schedules.....	385
Policy Types and Names.....	385
Set Precedence Manually.....	385
Create Schedules for XTM Device Actions.....	386
Set an Operating Schedule.....	387
About Custom Policies.....	388
Create or Edit a Custom Policy Template.....	388
Import and Export Custom Policy Templates.....	390
About Policy Properties.....	391
Policy Tab.....	391
Properties Tab.....	391
Advanced Tab.....	392
Proxy Settings.....	392
Set Access Rules for a Policy.....	392
Configure Policy-Based Routing.....	395
Set a Custom Idle Timeout.....	399
Set ICMP Error Handling.....	399
Apply NAT Rules.....	399
Set the Sticky Connection Duration for a Policy.....	400
<b>Proxy Settings.....</b>	<b>401</b>
About Proxy Policies and ALGs.....	401
Proxy Configuration.....	402
Proxy and AV Alarms.....	402
About Proxy Actions.....	403
About Rules and Rulesets.....	408
Use Predefined Content Types.....	417
Add a Proxy Policy to Your Configuration.....	417
About the DNS-Proxy.....	419
Policy Tab.....	419
Properties Tab.....	419

---

Advanced Tab.....	420
Configure the Proxy Action.....	420
DNS-Proxy: General Settings.....	420
DNS-Proxy: OPcodes.....	422
DNS-Proxy: Query Types.....	423
DNS-Proxy: Query Names.....	425
About MX (Mail eXchange) Records.....	426
About the FTP-Proxy.....	428
Policy Tab.....	428
Properties Tab.....	428
Advanced Tab.....	429
Configure the Proxy Action.....	429
FTP-Proxy: General Settings.....	430
FTP-Proxy: Commands.....	431
FTP-Proxy: Content.....	432
FTP-Proxy: AntiVirus.....	433
About the H.323-ALG.....	434
VoIP Components.....	434
ALG Functions.....	434
Policy Tab.....	435
Properties Tab.....	435
Advanced Tab.....	435
Configure the Proxy Action.....	435
H.323-ALG: General Settings.....	436
H.323-ALG: Access Control.....	437
H.323 ALG: Denied Codecs.....	439
About the HTTP-Proxy.....	440
Policy Tab.....	441
Properties Tab.....	441
Advanced Tab.....	441
Configure the Proxy Action.....	441
HTTP Request: General Settings.....	442

---

HTTP Request: Request Methods .....	444
HTTP Request: URL Paths .....	445
HTTP Request: Header Fields.....	445
HTTP Request: Authorization.....	446
HTTP Response: General Settings.....	447
HTTP Response: Header Fields.....	448
HTTP Response: Content Types .....	449
HTTP Response: Cookies.....	451
HTTP Response: Body Content Types.....	452
HTTP-Proxy: Exceptions.....	452
HTTP-Proxy: WebBlocker.....	453
HTTP-Proxy: AntiVirus.....	454
HTTP-Proxy: Reputation Enabled Defense.....	454
HTTP-Proxy: Deny Message.....	455
Enable Windows Updates Through the HTTP-Proxy.....	457
Use a Caching Proxy Server.....	457
About the HTTPS-Proxy.....	459
Policy Tab.....	459
Properties Tab.....	460
Advanced Tab.....	460
Configure the Proxy Action.....	460
HTTPS-Proxy: General Settings.....	461
HTTPS-Proxy: Content Inspection.....	463
HTTPS-Proxy: Certificate Names.....	465
HTTPS-Proxy: WebBlocker.....	466
About the POP3-Proxy.....	467
Policy Tab.....	467
Properties Tab.....	468
Advanced Tab.....	468
Configure the Proxy Action.....	468
POP3-Proxy: General Settings.....	469
POP3-Proxy: Authentication.....	471



---

POP3-Proxy: Content Types.....	472
POP3-Proxy: File Names.....	474
POP3-Proxy: Headers.....	475
POP3-Proxy: AntiVirus.....	476
POP3-Proxy: Deny Message.....	477
POP3-Proxy: spamBlocker.....	479
About the SIP-ALG.....	480
VoIP Components.....	480
Instant Messaging Support.....	480
ALG Functions.....	481
Policy Tab.....	481
Properties Tab.....	481
Advanced Tab.....	482
Configure the Proxy Action.....	482
SIP-ALG: General Settings.....	483
SIP-ALG: Access Control.....	485
SIP-ALG: Denied Codecs.....	486
About the SMTP-Proxy.....	488
Policy Tab.....	488
Properties Tab.....	488
Advanced Tab.....	489
Configure the Proxy Action.....	489
SMTP-Proxy: General Settings.....	490
SMTP Proxy: Greeting Rules.....	493
SMTP-Proxy: ESMTP Settings.....	494
SMTP-Proxy: Authentication.....	495
SMTP-Proxy: Content Types.....	497
SMTP-Proxy: File Names.....	498
SMTP-Proxy: Mail From/Rcpt To.....	499
SMTP-Proxy: Headers.....	501
SMTP-Proxy: AntiVirus.....	501
SMTP-Proxy: Deny Message.....	502

---

SMTP-Proxy: spamBlocker.....	504
Configure the SMTP-Proxy to Quarantine Email.....	504
Protect Your SMTP Server from Email Relaying.....	504
About the TCP-UDP-Proxy.....	506
Policy Tab.....	506
Properties Tab.....	506
Advanced Tab.....	507
Configure the Proxy Action.....	507
TCP-UDP-Proxy: General Settings.....	507
<b>Traffic Management and QoS.....</b>	<b>509</b>
About Traffic Management and QoS.....	509
Enable Traffic Management and QoS.....	509
Guarantee Bandwidth.....	510
Restrict Bandwidth.....	511
QoS Marking.....	511
Traffic priority.....	511
Set Connection Rate Limits.....	512
About QoS Marking.....	512
Before you begin.....	512
QoS marking for interfaces and policies.....	513
QoS marking and IPSec traffic.....	513
Marking Types and Values.....	514
Enable QoS Marking for an Interface.....	515
Enable QoS Marking or Prioritization Settings for a Policy.....	516
Enable QoS Marking for a Managed BOVPN Tunnel.....	518
Traffic Control and Policy Definitions.....	520
Define a Traffic Management Action.....	520
Add a Traffic Management Action to a Policy.....	521
Add a Traffic Management Action to a BOVPN Firewall Policy.....	522
<b>Default Threat Protection.....</b>	<b>525</b>
About Default Threat Protection.....	525
About Default Packet Handling Options.....	526

---

Set Logging and Notification Options.....	527
About Spoofing Attacks.....	527
About IP Source Route Attacks.....	528
About Port Space and Address Space Probes.....	529
About Flood Attacks.....	531
About Unhandled Packets.....	532
About Distributed Denial-of-Service Attacks.....	533
About Blocked Sites.....	535
Permanently Blocked Sites.....	535
Auto-Blocked Sites/Temporary Blocked Sites List.....	535
Blocked Site Exceptions.....	535
Block a Site Permanently.....	536
Create Blocked Site Exceptions.....	537
Import a List of Blocked Sites or Blocked Sites Exceptions.....	538
Block Sites Temporarily with Policy Settings.....	538
Change the Duration that Sites are Auto-Blocked.....	539
About Blocked Ports.....	539
Default Blocked Ports.....	540
Block a Port.....	541
<b>WatchGuard Server Setup.....</b>	<b>543</b>
About WatchGuard Servers.....	543
Set Up WatchGuard Servers.....	545
Before You Begin.....	545
Start the Wizard.....	545
General Settings.....	545
Management Server Settings.....	546
Log Server and Report Server Settings.....	546
Quarantine Server Settings.....	547
WebBlocker Server Settings.....	547
Review and Finish.....	547
About the Gateway Firebox.....	548
Find Your Management Server License Key.....	548

---

Monitor the Status of WatchGuard Servers.....	549
Configure Your WatchGuard Servers.....	550
Open WatchGuard Server Center.....	551
Stop and Start Your WatchGuard Servers.....	552
Install or Configure WatchGuard Servers from WatchGuard Server Center.....	553
Exit or Open WatchGuard Server Center.....	555
<b>Management Server Setup and Administration.....</b>	<b>557</b>
About the WatchGuard Management Server.....	557
Install the Management Server.....	557
Set up and Configure the Management Server.....	558
Configure Settings for the Management Server.....	558
Configure the Certificate Authority on the Management Server.....	560
Configure License Key, Device Monitoring, and Notification Settings.....	562
Enable and Configure Active Directory Authentication.....	564
Configure Logging Settings for the Management Server.....	567
Define Configuration History Settings.....	568
Update the Management Server with a New Gateway Address.....	569
Change the IP Address of a Management Server.....	571
If Your Management Server is Configured with a Private IP Address.....	572
If Your Management Server is Configured with a Public IP Address.....	573
Update the Certificate Revocation List (CRL) Distribution IP Address.....	573
Update Managed XTM Devices.....	574
Change the Administrator Passphrase.....	574
Back Up or Restore the Management Server Configuration.....	576
Back up Your Configuration.....	576
Restore Your Configuration.....	576
Move the Management Server to a New Computer.....	577
Back up, Move, and Restore Your Management Server.....	577
Configure Other Installed WatchGuard Servers.....	577
Use WSM to Connect to your Management Server.....	578
Disconnect from the Management Server.....	579
Import or Export a Management Server Configuration.....	579

---

Export a Configuration.....	579
Import a Configuration.....	579
<b>Centralized Management.....</b>	<b>581</b>
About WatchGuard System Manager.....	581
Device Status.....	581
Device Management.....	582
About the Device Management Page.....	584
Review Information for Managed Devices.....	584
Verify the Connection Status of a Device.....	585
About Centralized Management Modes.....	586
Change the Centralized Management Mode.....	587
Add Managed Devices to the Management Server.....	590
If You Know the Current IP Address of the Device.....	591
If You Do Not Know the IP Address of the Device.....	592
Set Device Management Properties.....	593
Connection Settings.....	593
IPSec Tunnel Preferences.....	595
Contact Information.....	596
Schedule Tasks for Managed Devices.....	597
Schedule OS Update.....	598
Schedule Feature Key Synchronization.....	601
Schedule Reboot.....	602
Review, Cancel, or Delete Scheduled Tasks.....	606
Update the Configuration For a Fully Managed Device.....	608
About Filtered View.....	609
Manage Server Licenses.....	611
Review Current License Key Information.....	611
Add or Remove a License Key.....	611
Save or Discard Your Changes.....	612
Manage Customer Contact Information.....	612
Add a Contact to the Management Server.....	612
Edit a Contact in the Contact List.....	612

---

Review and Manage the Monitored Report Servers List .....	613
Add a Report Server to the List .....	614
Edit Information for a Report Server.....	614
Remove a Report Server from the List .....	615
Add and Manage VPN Tunnels and Resources .....	615
See VPN Tunnels.....	615
Add a VPN Tunnel.....	615
Edit a VPN Tunnel.....	616
Remove a VPN Tunnel.....	617
Add a VPN Resource.....	617
Configure an XTM Device as a Managed Device.....	618
Edit the WatchGuard Policy.....	618
Set Up the Managed Device.....	619
Configure a Firebox III or Firebox X Core Running WFS as a Managed Device.....	620
About Edge (v10.x and Older) and SOHO Devices as Managed Devices.....	622
Prepare a Firebox X Edge (v10.x and Older) for Management .....	623
Configure a Firebox SOHO 6 as a Managed Device.....	626
Start WatchGuard System Manager Tools.....	628
Expire the Lease for a Managed Device.....	628
Configure Network Settings (Edge Devices v10.x and Older Only).....	630
About the Configuration Template Section.....	631
Update or Reboot a Device, or Remove a Device from Management .....	631
Update a Device.....	631
Reboot a Device.....	632
Remove a Device from Management .....	632
Create Device Configuration Templates.....	633
Create a New Device Configuration Template.....	634
Configure a Template for a Managed Edge Device.....	635
Configure a Template for an XTM Device.....	637
Review XTM Template Settings.....	641
Apply an XTM Template to an XTM Device.....	642
Change an XTM Configuration Template.....	642

---

Add a Predefined Policy to an Edge Device Configuration Template.....	643
Add a Custom Policy to an Edge Device Configuration Template.....	644
Change the Name of a Device Configuration Template.....	646
Clone a Device Configuration Template.....	647
Configure an SNAT Action.....	647
Apply Device Configuration Templates to Managed Devices.....	652
Drag-and-Drop to Apply a Template.....	652
Use the Apply Template Wizard for an XTM Device.....	652
About Configuration History and Template Application History.....	654
Review Configuration History and Application History Details.....	655
Revert to an Earlier Configuration.....	657
Manage Aliases for Firebox X Edge Devices.....	657
Change the Name of an Alias.....	659
Define Aliases on a Firebox X Edge Device.....	660
Remove a Device from Fully Managed Mode.....	663
<b>Role-Based Administration.....</b>	<b>665</b>
About Role-Based Administration.....	665
Roles and Role Policies.....	665
Audit Trail.....	666
About Predefined Roles.....	666
Use Role-Based Administration with an External Management Server.....	670
Define or Remove Users or Groups.....	671
Use WatchGuard System Manager to Configure Users or Groups.....	671
Use WatchGuard Server Center to Configure Users or Groups.....	673
Remove a User or Group.....	674
Define Roles and Role Properties.....	675
Define Roles in WatchGuard Server Center.....	675
Define Roles in WatchGuard System Manager.....	676
Configure Roles and Role Properties.....	677
Remove a Role.....	677
Assign Roles to a User or Group.....	678
Assign Roles in WatchGuard System Manager.....	678

---

Assign Roles in the WatchGuard Server Center.....	679
<b>Logging and Notification.....</b>	<b>683</b>
About Logging and Log Files.....	683
Log Servers.....	683
LogViewer.....	684
Logging and Notification in Applications and Servers.....	684
About Log Messages.....	684
Log Files.....	685
Databases.....	685
Performance and Disk Space.....	685
Types of Log Messages.....	686
Log Message Levels.....	687
About Notification.....	688
Quick Start — Set Up Logging for Your Network.....	688
Set Up a Log Server.....	691
Install the Log Server.....	691
Before You Begin.....	691
Configure System Settings.....	692
Configure the Log Server.....	692
Configure Database, Encryption Key, and Diagnostic Log Settings.....	693
Configure Database Settings.....	694
Configure Notification Settings.....	699
Configure Logging Settings for the Log Server.....	702
Move the Log Data Directory.....	704
Start and Stop the Log Server.....	707
Configure Logging Settings for Your WatchGuard Servers.....	708
Configure Logging to a WatchGuard Log Server.....	709
Configure Logging to Windows Event Viewer.....	709
Save Log Messages in a Log File.....	710
Define Where the XTM Device Sends Log Messages.....	711
Add a Log Server.....	712
Set Log Server Priority.....	715



---

Configure Syslog .....	716
Set Up Performance Statistic Logging .....	718
Set the Diagnostic Log Level .....	720
Configure Logging and Notification for a Policy .....	722
Set Logging and Notification Preferences .....	723
Use Scripts, Utilities, and Third-Party Software with the Log Server .....	725
Back Up and Restore the Log Server Database .....	725
Use Crystal Reports with the Log Server .....	726
Use LogViewer to See Log Files .....	727
Open LogViewer .....	727
Connect to a Device .....	728
Open Logs for the Primary Log Server .....	729
Set LogViewer User Preferences .....	730
Log Message Details .....	733
Use Search Manager .....	735
Search Parameter Settings .....	737
Filter Log Messages by Type and Time, or Run a String Search .....	738
Use Log Excerpt to Filter Search Results .....	740
Run Local Diagnostic Tasks .....	742
Import and Export Data to LogViewer .....	743
Email, Print, or Save Log Messages .....	743
<b>Monitor Your Device .....</b>	<b>745</b>
About Firebox System Manager (FSM) .....	745
Start Firebox System Manager .....	746
Disconnect from and Reconnect to a XTM device .....	746
Set the Refresh Interval and Pause Display .....	747
Basic XTM Device and Network Status (Front Panel) .....	748
Warnings and Notifications .....	748
Expand and Close Tree Views .....	749
Visual Display of Traffic Between Interfaces .....	749
Traffic Volume, Processor Load, and Basic Status .....	751
XTM Device Status .....	752

---

Device Log Messages (Traffic Monitor).....	754
Sort and Filter Traffic Monitor Log Messages.....	755
Change Traffic Monitor Settings.....	755
Copy Messages to Another Application.....	758
Learn More About Traffic Log Messages.....	758
Enable Notification for Specific Messages.....	761
Visual Display of Bandwidth Usage (Bandwidth Meter).....	762
Change Bandwidth Meter Settings.....	762
Change the Scale.....	763
Add and Remove Lines.....	763
Change Colors.....	764
Change Interface Appearance.....	764
Visual Display of Policy Usage (Service Watch).....	764
Change Service Watch Settings.....	765
Change the Scale.....	766
Display Bandwidth Used by a Policy.....	766
Add and Remove Lines.....	766
Change Colors.....	766
Change How Policy Names Appear.....	767
Traffic and Performance Statistics (Status Report).....	767
Change the Refresh Interval.....	769
Review Packet Trace Information for Troubleshooting.....	769
Save the Status Report.....	770
Authenticated Users (Authentication List).....	770
Wireless Hotspot Connections.....	771
Manage the Blocked Sites List (Blocked Sites).....	772
Change the Block Sites List.....	773
Blocked Sites and Traffic Monitor.....	774
Subscription Services Statistics (Subscription Services).....	776
Gateway AntiVirus Statistics.....	777
Application Control and Intrusion Prevention Service Statistics.....	778
spamBlocker Statistics.....	779

---

Reputation Enabled Defense Statistics.....	780
Subscription Services Status and Manual Signatures Updates.....	780
About HostWatch.....	782
DNS Resolution and HostWatch.....	783
Start HostWatch.....	783
Pause and start the HostWatch display.....	783
Select Connections and Interfaces to Monitor.....	784
Filter Content of the HostWatch Window.....	786
Change HostWatch Visual Properties.....	787
Visit or Block a Site from HostWatch.....	788
About the Performance Console.....	789
Start the Performance Console.....	789
Make Graphs with the Performance Console.....	790
Types of Counters.....	790
Stop Monitoring or Close the Window.....	790
Define Performance Counters.....	791
Add Charts or Change Polling Intervals.....	794
About Certificates and FSM.....	795
Communication Log.....	797
Use Firebox System Manager (FSM).....	798
Synchronize the System Time.....	798
Reboot or Shut Down Your XTM Device.....	798
Clear the ARP Cache.....	799
See and Synchronize Feature Keys.....	799
Calculate the Fireware XTM Checksum.....	802
Clear Alarms.....	802
Rekey BOVPN Tunnels.....	803
Control FireCluster.....	804
Update the Wireless Region for an XTM 2 Series Device.....	804
Change Passphrases.....	804
<b>Reporting.....</b>	<b>805</b>
About the Report Server.....	805

---

Set Up the Report Server.....	806
Start or Stop the Report Server.....	829
About WatchGuard Report Manager.....	830
Open Report Manager.....	831
Set Report Options.....	832
Predefined Reports List.....	835
Select Report Parameters.....	838
Select Reports to Generate.....	841
View a Report.....	843
View Client Web Usage Reports.....	844
Filter Report Data.....	846
Select the Report Format.....	850
Email, Print, or Save a Report.....	851
Use the Web Services API to Retrieve Log and Report Data.....	852
Installation and Documentation.....	852
<b>Certificates and the Certificate Authority.....</b>	<b>853</b>
About Certificates.....	853
Use Multiple Certificates to Establish Trust.....	854
How the XTM device Uses Certificates.....	854
Certificate Lifetimes and CRLs.....	856
Certificate Authorities and Signing Requests.....	856
Certificate Authorities Trusted by the XTM Device.....	857
Manage XTM Device Certificates.....	862
Manage Management Server Certificates.....	866
Create a Certificate with FSM or the Management Server.....	869
Create a Certificate with FSM.....	869
Create a Self-Signed Certificate with CA Manager.....	872
Create a CSR with OpenSSL.....	873
Use OpenSSL to Generate a CSR.....	873
Sign a Certificate with Microsoft CA.....	873
Issue the Certificate.....	874
Download the Certificate.....	874

---

Use Certificates for Authentication.....	875
Certificates for Mobile VPN with IPSec Tunnel Authentication.....	875
Certificates for Branch Office VPN (BOVPN) Tunnel Authentication.....	876
Configure the Web Server Certificate for Firebox Authentication.....	878
Use Certificates for the HTTPS-Proxy.....	880
Protect a Private HTTPS Server.....	880
Examine Content from External HTTPS Servers.....	881
Export the HTTPS Content Inspection Certificate.....	882
Import the Certificates on Client Devices.....	882
Troubleshoot Problems with HTTPS Content Inspection.....	882
Import a Certificate on a Client Device.....	883
Import a PEM Format Certificate with Windows XP.....	883
Import a PEM format certificate with Windows Vista.....	883
Import a PEM Format Certificate with Mozilla Firefox 3.x.....	884
Import a PEM Format Certificate with Mac OS X 10.5.....	885
<b>Virtual Private Networks (VPNs).....</b>	<b>887</b>
Introduction to VPNs.....	887
Branch Office VPN.....	887
Mobile VPN.....	888
About IPSec VPNs.....	888
About IPSec Algorithms and Protocols.....	888
About IPSec VPN Negotiations.....	890
Configure Phase 1 and Phase 2 Settings.....	893
About Mobile VPNs.....	894
Select a Mobile VPN.....	894
Internet Access Options for Mobile VPN Users.....	896
Mobile VPN Setup Overview.....	897
<b>Managed Branch Office VPN Tunnels.....</b>	<b>899</b>
About Managed Branch Office VPN Tunnels.....	899
How to Create a Managed BOVPN Tunnel.....	899
Tunnel Options.....	900
VPN Failover.....	900

---

Global VPN Settings.....	900
BOVPN tunnel Status.....	900
Rekey BOVPN Tunnels.....	901
Add VPN Resources.....	901
Get the Current Resources from a Device.....	901
Create a New VPN Resource.....	902
Add a Host or Network.....	902
Add VPN Firewall Policy Templates.....	903
Set a Schedule for the Policy Template.....	904
Use QoS Marking in a Policy Template.....	905
Configure Traffic Management in a Policy Template.....	905
Add Security Templates.....	905
Make Managed Tunnels Between Devices.....	908
Edit a Tunnel Definition.....	908
Remove Tunnels and Devices.....	909
Remove a Tunnel.....	909
Remove a Device.....	909
VPN Tunnel Status and Subscription Services.....	910
Mobile VPN Tunnel Status.....	911
Subscription Services Status.....	911
<b>Manual Branch Office VPN Tunnels.....</b>	<b>913</b>
What You Need to Create a Manual BOVPN.....	913
About Manual Branch Office VPN Tunnels.....	914
What You Need to Create a VPN.....	914
How to Create a Manual BOVPN Tunnel.....	915
Custom Tunnel Policies.....	915
One-Way Tunnels.....	915
VPN Failover.....	915
Global VPN Settings.....	915
BOVPN Tunnel Status.....	916
Rekey BOVPN Tunnels.....	916
Sample VPN Address Information Table.....	917

---

Configure Gateways.....	918
Define Gateway Endpoints.....	920
Configure Mode and Transforms (Phase 1 Settings).....	922
Edit and Delete Gateways.....	926
Disable Automatic Tunnel Startup.....	926
If Your XTM Device is Behind a Device That Does NAT.....	926
Make Tunnels Between Gateway Endpoints.....	928
Define a Tunnel.....	928
Add Routes for a Tunnel.....	930
Configure Phase 2 Settings.....	931
Add a Phase 2 Proposal.....	932
Change Order of Tunnels.....	934
About Global VPN Settings.....	935
Enable IPSec Pass-Through.....	935
Enable TOS for IPSec.....	935
Enable the Use of Non-Default (Static or Dynamic) Routes to Determine if IPSec is Used.....	936
Enable LDAP Server for Certificate Verification.....	937
BOVPN Notification.....	937
Define a Custom Tunnel Policy.....	938
Choose a Name for the Policies.....	938
Select the Policy Type.....	938
Select the BOVPN Tunnels.....	938
Create an Alias for the Tunnels.....	938
The BOVPN Policy Wizard has Completed Successfully.....	938
Set Up Outgoing Dynamic NAT Through a Branch Office VPN Tunnel.....	939
Configure the Endpoint Where All Traffic Must Appear to Come from a Single Address (Site A).....	939
Configure the Endpoint that Expects All Traffic to Come from a Single IP Address (Site B).....	941
Use 1-to-1 NAT Through a Branch Office VPN Tunnel.....	944
1-to-1 NAT and VPNs.....	944
Other Reasons to Use 1-to-1 NAT Through a VPN.....	944
Alternative to Using NAT.....	944

---

How to Set Up the VPN.....	945
Example.....	945
Configure the Local Tunnel.....	946
Configure the Remote Tunnel.....	948
Define a Route for All Internet-Bound Traffic.....	949
Configure the BOVPN Tunnel on the Remote XTM Device.....	949
Configure the BOVPN Tunnel on the Central XTM Device.....	950
Add a Dynamic NAT Entry on the Central XTM Device.....	951
Enable Multicast Routing Through a Branch Office VPN Tunnel.....	952
Enable an XTM Device to Send Multicast Traffic Through a Tunnel.....	953
Enable the Other XTM Device to Receive Multicast Traffic Through a Tunnel.....	955
Enable Broadcast Routing Through a Branch Office VPN Tunnel.....	955
Enable Broadcast Routing for the Local XTM device.....	956
Configure Broadcast Routing for the XTM Device at the Other End of the Tunnel.....	958
Branch Office VPN Tunnel Switching.....	958
Configure VPN Failover.....	959
Define Multiple Gateway Pairs.....	960
Force a Branch Office VPN Tunnel Rekey.....	961
To Rekey One BOVPN Tunnel.....	962
To Rekey all BOVPN Tunnels.....	962
Related Questions About Branch Office VPN Set Up.....	962
Why do I Need a Static External Address?.....	962
How do I Get a Static External IP Address?.....	962
How do I Troubleshoot the Connection?.....	963
Why is Ping not Working?.....	963
Improve Branch Office VPN Tunnel Availability.....	964
<b>Mobile VPN with PPTP.....</b>	<b>969</b>
About Mobile VPN with PPTP.....	969
Mobile VPN with PPTP Requirements.....	969
Encryption Levels.....	970
Configure Mobile VPN with PPTP.....	971
Authentication.....	972



---

Set Encryption for PPTP Tunnels.....	972
MTU and MRU.....	972
Define Timeout Settings for PPTP Tunnels.....	972
Add to the IP Address Pool.....	973
Save Your Changes.....	974
Configure WINS and DNS Servers.....	974
Add New Users to the PPTP-Users Group.....	974
Options for Internet Access Through a Mobile VPN with PPTP Tunnel.....	976
Default-Route VPN.....	977
Split Tunnel VPN.....	977
Default-Route VPN Setup for Mobile VPN with PPTP.....	977
Split Tunnel VPN Setup for Mobile VPN with PPTP.....	977
Configure Policies to Control Mobile VPN with PPTP Client Access.....	978
Allow PPTP Users to Access a Trusted Network.....	978
Use Other Groups or Users in a PPTP Policy.....	981
Prepare Client Computers for PPTP.....	982
Prepare a Windows NT or 2000 Client Computer: Install MSDUN and Service Packs.....	982
Create and Connect a PPTP Mobile VPN for Windows Vista.....	983
Create and Connect a PPTP Mobile VPN for Windows XP.....	984
Create and Connect a PPTP Mobile VPN for Windows 2000.....	984
Make Outbound PPTP Connections from Behind an XTM Device.....	985
<b>Mobile VPN with IPSec.....</b>	<b>987</b>
About Mobile VPN with IPSec.....	987
Configure a Mobile VPN with IPSec Connection.....	987
System Requirements.....	988
Options for Internet Access Through a Mobile VPN with IPSec Tunnel.....	988
About Mobile VPN Client Configuration Files.....	989
Configure the XTM Device for Mobile VPN with IPSec.....	990
Add Users to a Firebox Mobile VPN Group.....	996
Modify an Existing Mobile VPN with IPSec Group Profile.....	998
Configure WINS and DNS Servers.....	1010
Lock Down an End User Profile.....	1011

---

Save the Profile to a XTM Device.....	1011
Mobile VPN with IPsec Configuration Files.....	1011
Configure Policies to Filter Mobile VPN Traffic.....	1012
Distribute the Software and Profiles.....	1013
Additional Mobile VPN Topics.....	1014
Configure Mobile VPN with IPsec to a Dynamic IP Address.....	1016
About the Mobile VPN with IPsec Client.....	1017
Client Requirements.....	1018
Install the Mobile VPN with IPsec Client Software.....	1018
Connect and Disconnect the Mobile VPN Client.....	1020
See Mobile VPN Log Messages.....	1024
Secure Your Computer with the Mobile VPN Firewall.....	1024
End-User Instructions for WatchGuard Mobile VPN with IPsec Client Installation.....	1031
Mobile VPN for Windows Mobile Setup.....	1036
Mobile VPN WM Configurator and Windows Mobile IPsec Client Requirements.....	1036
Install the Mobile VPN WM Configurator Software.....	1037
Select a Certificate and Enter the PIN.....	1037
Import an End-User Profile.....	1038
Install the Windows Mobile Client Software on the Windows Mobile Device.....	1038
Upload the End-User Profile to the Windows Mobile Device.....	1040
Connect and Disconnect the Mobile VPN for Windows Mobile Client.....	1042
Secure Your Windows Mobile Device with the Mobile VPN Firewall.....	1043
Stop the WatchGuard Mobile VPN Service.....	1044
Uninstall the Configurator, Service, and Monitor.....	1044
<b>Mobile VPN with SSL.....</b>	<b>1047</b>
About Mobile VPN with SSL.....	1047
Configure the XTM Device for Mobile VPN with SSL.....	1047
Configure Authentication and Connection Settings.....	1048
Configure the Networking and IP Address Pool Settings.....	1049
Configure Advanced Settings for Mobile VPN with SSL.....	1051
Configure User Authentication for Mobile VPN with SSL.....	1053
Configure Policies to Control Mobile VPN with SSL Client Access.....	1053

---

Options for Internet Access Through a Mobile VPN with SSL Tunnel.....	1054
Name Resolution for Mobile VPN with SSL.....	1055
Install and Connect the Mobile VPN with SSL Client.....	1058
Client Computer Requirements.....	1058
Download the Client Software.....	1058
Install the Client Software.....	1059
Connect to Your Private Network.....	1060
Mobile VPN with SSL Client Controls.....	1060
Manually Distribute and Install the Mobile VPN with SSL Client Software and Configuration File.....	1061
Uninstall the Mobile VPN with SSL Client.....	1062
<b>WebBlocker.....</b>	<b>1065</b>
About WebBlocker.....	1065
Set Up the WebBlocker Server.....	1066
Install the WebBlocker Server software.....	1066
Manage the WebBlocker Server.....	1066
Download the WebBlocker Database.....	1067
Keep the WebBlocker Database Updated.....	1068
Change the WebBlocker Server Port.....	1070
Copy the WebBlocker Database from One WebBlocker Server to Another.....	1071
Get Started with WebBlocker.....	1073
Before You Begin.....	1073
Activate WebBlocker.....	1073
Set Policies for WebBlocker.....	1073
Identify the WebBlocker Servers.....	1074
Select Categories to Block.....	1076
Use Exception Rules to Restrict Web Site Access.....	1076
Configure WebBlocker.....	1077
Configure WebBlocker Settings for a Policy.....	1077
Copy WebBlocker Settings from One Policy to Another.....	1078
Add New WebBlocker Servers or Change Their Order.....	1078
About WebBlocker Categories.....	1080

---

Change Categories to Block .....	1080
See Whether a Site is Categorized .....	1081
Add, Remove, or Change a Category .....	1082
Define Advanced WebBlocker Options .....	1084
Define WebBlocker Alarms .....	1086
About WebBlocker Exceptions .....	1086
Define the Action for Sites that do not Match Exceptions .....	1087
Components of Exception Rules .....	1087
Exceptions with Part of a URL .....	1087
Add WebBlocker Exceptions .....	1088
Change the Order of Exception Rules .....	1090
Import or Export WebBlocker Exception Rules .....	1090
Restrict Users to a Specific Set of Web Sites .....	1092
Use WebBlocker Actions in Proxy Definitions .....	1097
Define Additional WebBlocker Actions .....	1097
Add WebBlocker Actions to a Policy .....	1097
Schedule WebBlocker Actions .....	1098
About WebBlocker Subscription Services Expiration .....	1099
Examples .....	1099
Use WebBlocker Local Override .....	1099
Use a WebBlocker Server Protected by Another XTM Device .....	1100
Configure WebBlocker Policies for Groups with Active Directory Authentication .....	1107
Configure WebBlocker Policies for Groups with Firebox Authentication .....	1123
<b>spamBlocker .....</b>	<b>1141</b>
About spamBlocker .....	1141
spamBlocker Requirements .....	1142
spamBlocker Actions, Tags, and Categories .....	1142
Activate spamBlocker .....	1144
Apply spamBlocker Settings to Your Policies .....	1145
Create New Proxy Policies .....	1145
Configure spamBlocker .....	1146
About spamBlocker Exceptions .....	1148

---

Configure Virus Outbreak Detection Actions for a Policy.....	1151
Configure spamBlocker to Quarantine Email.....	1153
About Using spamBlocker with Multiple Proxies.....	1153
Set Global spamBlocker Parameters.....	1153
Use an HTTP Proxy Server for spamBlocker.....	1155
Add Trusted Email Forwarders to Improve Spam Score Accuracy.....	1155
Enable and Set Parameters for Virus Outbreak Detection (VOD).....	1156
About spamBlocker and VOD Scan Limits.....	1157
Create Rules for Your Email Reader.....	1157
Send Spam or Bulk Email to Special Folders in Outlook.....	1158
Send a Report about False Positives or False Negatives.....	1158
Use RefID Record Instead of Message Text.....	1159
Find the Category a Message is Assigned To.....	1160
<b>Reputation Enabled Defense.....</b>	<b>1161</b>
About Reputation Enabled Defense.....	1161
Reputation Thresholds.....	1161
Reputation Scores.....	1162
Reputation Lookups.....	1162
Reputation Enabled Defense Feedback.....	1163
Configure Reputation Enabled Defense.....	1163
Before You Begin.....	1163
Enable Reputation Enabled Defense.....	1163
Configure the Reputation Thresholds.....	1164
Configure Alarm Notification for RED Actions.....	1165
Send Gateway AV Scan Results to WatchGuard.....	1165
<b>Gateway AntiVirus.....</b>	<b>1167</b>
About Gateway AntiVirus.....	1167
Install and Upgrade Gateway AV.....	1167
About Gateway AntiVirus and Proxy Policies.....	1168
Activate Gateway AntiVirus.....	1168
Activate Gateway AntiVirus with a Wizard from Policy Manager.....	1168
Activate Gateway AntiVirus from Proxy Definitions.....	1171

---

Configure Gateway AntiVirus Actions .....	1172
Configure Gateway AntiVirus actions for a Proxy Policy.....	1174
Configure Gateway AntiVirus Actions in Policy Rulesets.....	1176
Configure Alarm Notification for Antivirus Actions.....	1179
Unlock a File Locked by Gateway AntiVirus.....	1179
Configure Gateway AntiVirus to Quarantine Email.....	1181
About Gateway AntiVirus Scan Limits.....	1181
Update Gateway AntiVirus Settings.....	1182
If you Use a Third-Party Antivirus Client.....	1182
Configure Gateway AV Decompression Settings.....	1182
Configure the Gateway AV Update Server.....	1183
<b>Intrusion Prevention Service.....</b>	<b>1187</b>
About Intrusion Prevention Service.....	1187
IPS Threat Levels.....	1187
Add the IPS Upgrade.....	1187
Keep IPS Signatures Updated.....	1188
See IPS Status.....	1188
Configure Intrusion Prevention.....	1188
Enable IPS and Configure IPS Actions.....	1188
Configure other IPS Settings.....	1189
Configure the IPS Update Server.....	1190
Configure Automatic Signature Updates.....	1190
Connect to the Update Server Through an HTTP Proxy Server.....	1191
Block Access from the Trusted Network to the Update Server.....	1191
Update Signatures Manually.....	1191
Configure IPS Exceptions.....	1191
Find the IPS Signature ID.....	1191
Add an IPS Signature Exception.....	1192
Show IPS Signature Information.....	1193
Find IPS Signature Information in Firebox System Manager.....	1193
Disable or Enable IPS for a Policy.....	1194
<b>Application Control.....</b>	<b>1197</b>

---

---

About Application Control.....	1197
Add the Application Control Upgrade.....	1197
Keep Application Control Signatures Updated.....	1198
How Application Control Identifies Applications.....	1198
Application Control — Begin with Monitoring.....	1198
Monitor Application Use.....	1198
Application Control Reports.....	1199
Policy Guidelines for Application Control.....	1201
Global Application Control Action.....	1202
Configure Application Control Actions.....	1202
Connect to the XTM Device To Get The Latest Signatures.....	1203
Add or Edit Application Control Actions.....	1203
Remove Configured Applications From an Application Control Action.....	1206
Apply an Application Control Action to a Policy.....	1207
Clone an Application Control Action.....	1207
Remove Application Control Actions.....	1208
Use Categories.....	1209
Configure Application Control for Policies.....	1210
Enable Application Control in a Policy.....	1211
Edit or Clone Application Control Actions.....	1211
Get Information About Applications.....	1212
Configure the Application Control Update Server.....	1212
Configure Signature Updates.....	1212
Connect to the Update Server Through an HTTP Proxy Server.....	1213
Block Access from the Trusted Network to the Update Server.....	1213
Update Signatures Manually.....	1213
Application Control and Proxies.....	1213
Application Control and WebBlocker.....	1214
Manage SSL Applications.....	1215
Manage Evasive Applications.....	1215
Block User Logins to Skype.....	1215
Manage Applications that Use Multiple Protocols.....	1216

---

Example: Block FlashGet .....	1216
File Transfer Applications and Protocols .....	1217
Monitor Downloads and File Transfers .....	1219
Manage Facebook Applications .....	1219
Application Control Policy Examples .....	1221
Allow an Application For a Group of Users .....	1221
Block Applications During Business Hours .....	1222
Application Control and Policy Precedence .....	1223
<b>Quarantine Server .....</b>	<b>1225</b>
About the Quarantine Server .....	1225
Set Up the Quarantine Server .....	1226
Install the Quarantine Server Software .....	1226
Run the WatchGuard Server Center Setup Wizard .....	1226
Configure the Quarantine Server Settings .....	1227
Configure the XTM Device to Quarantine Email .....	1227
Configure the Quarantine Server .....	1228
Configure Database and SMTP Server Settings .....	1229
Configure Deletion Settings and Accepted Domains .....	1231
Configure User Notification Settings .....	1232
Configure Logging Settings for the Quarantine Server .....	1234
Configure Quarantine Server Rules .....	1235
Define the Quarantine Server Location on the XTM Device .....	1237
About the Quarantine Server Client .....	1238
Manage Quarantined Messages .....	1240
Manage Quarantine Server Users .....	1242
Get Statistics on Quarantine Server Activity .....	1245
Configure User Notification with Microsoft Exchange Server 2003 or 2007 .....	1247
Configure User Notification if Your Microsoft Exchange Server Does Not Require Authentication .....	1247
Configure User Notification if Your Microsoft Exchange Server Requires Authentication .....	1248



# 1 Introduction to Network Security

---

## About Networks and Network Security

A *network* is a group of computers and other devices that are connected to each other. It can be two computers in the same room, dozens of computers in an organization, or many computers around the world connected through the Internet. Computers on the same network can work together and share data.

Although networks like the Internet give you access to a large quantity of information and business opportunities, they can also open your network to attackers. Many people think that their computers hold no important information, or that a hacker is not interested in their computers. This is not correct. A hacker can use your computer as a platform to attack other computers or networks. Information from your organization, including personal information about users, employees, or customers, is also valuable to hackers.

Your XTM device and LiveSecurity subscription can help you prevent these attacks. A good network security policy, or a set of access rules for users and resources, can also help you find and prevent attacks to your computer or network. We recommend that you configure your XTM device to match your security policy, and think about threats from both inside and outside your organization.

## About Internet Connections

ISPs (Internet service providers) are companies that give access to the Internet through network connections. The rate at which a network connection can send data is known as *bandwidth*: for example, 3 megabits per second (Mbps).

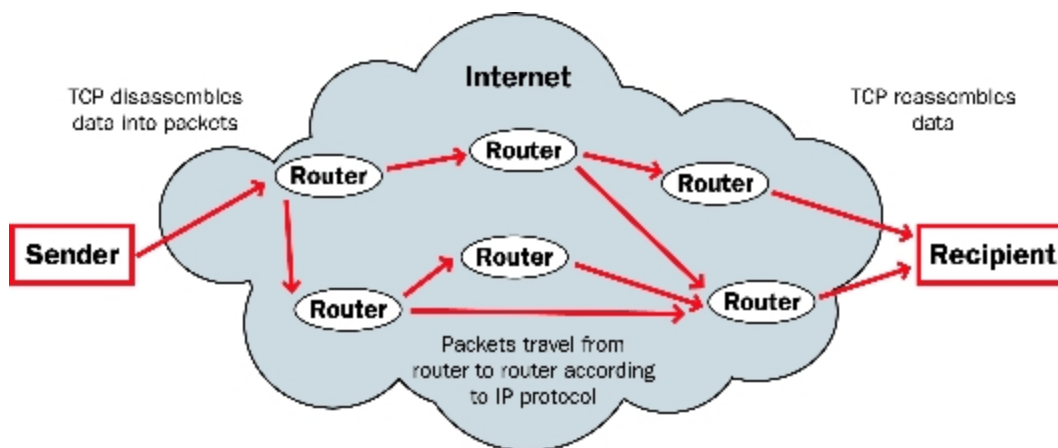
A high-speed Internet connection, such as a cable modem or a DSL (Digital Subscriber Line), is known as a *broadband connection*. Broadband connections are much faster than dial-up connections. The bandwidth of a dial-up connection is less than .1 Mbps, while a cable modem can be 5 Mbps or more.

Typical speeds for cable modems are usually lower than the maximum speeds, because each computer in a neighborhood is a member of a LAN. Each computer in that LAN uses some of the bandwidth. Because of this *shared-medium* system, cable modem connections can become slow when more users are on the network.

DSL connections supply constant bandwidth, but they are usually slower than cable modem connections. Also, the bandwidth is only constant between your home or office and the DSL central office. The DSL central office cannot guarantee a good connection to a web site or network.

## How Information Travels on the Internet

The data that you send through the Internet is cut into units, or packets. Each packet includes the Internet address of the destination. The packets that make up a connection can use different routes through the Internet. When they all get to their destination, they are assembled back into the original order. To make sure that the packets get to the destination, address information is added to the packets.



## About Protocols

A *protocol* is a group of rules that allow computers to connect across a network. Protocols are the *grammar* of the language that computers use when they speak to each other across a network. The standard protocol when you connect to the Internet is the IP (Internet Protocol). This protocol is the usual language of computers on the Internet.

A protocol also tells how data is sent through a network. The most frequently used protocols are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). TCP/IP is the basic protocol used by computers that connect to the Internet.

You must know some of the TCP/IP settings when you set up your XTM device. For more information on TCP/IP, see *Find Your TCP/IP Properties* on page 36.

## About IP Addresses

To send ordinary mail to a person, you must know his or her street address. For one computer on the Internet to send data to a different computer, it must know the address of that computer. A computer address is known as an *Internet Protocol (IP) address*. All devices on the Internet have unique IP addresses, which enable other devices on the Internet to find and interact with them.

An IP address consists of four octets (8-bit binary number sequences) expressed in decimal format and separated by periods. Each number between the periods must be within the range of 0 and 255. Some examples of IP addresses are:

- 206.253.208.100
- 4.2.2.2
- 10.0.4.1

## Private Addresses and Gateways

Many companies create private networks that have their own address space. The addresses 10.x.x.x and 192.168.x.x are reserved for private IP addresses. Computers on the Internet cannot use these addresses. If your computer is on a private network, you connect to the Internet through a *gateway* device that has a public IP address.

Usually, the *default gateway* is the router that is between your network and the Internet. After you install the XTM device on your network, it becomes the default gateway for all computers connected to its trusted or optional interfaces.

## About Subnet Masks

Because of security and performance considerations, networks are often divided into smaller portions called subnets. All devices in a subnet have similar IP addresses. For example, all devices that have IP addresses whose first three octets are 50.50.50 would belong to the same subnet.

A network IP address's subnet mask, or netmask, is a series of bits that *mask* sections of the IP address that identify which parts of the IP address are for the network and which parts are for the host. A subnet mask can be written in the same way as an IP address, or in slash or CIDR notation.

## About Slash Notation

Your XTM device uses *slash notation* for many purposes, including policy configuration. Slash notation, also known as CIDR (Classless Inter-Domain Routing) notation, is a compact way to show or write a subnet mask. When you use slash notation, you write the IP address, a forward slash (/), and the subnet mask number.

To find the subnet mask number:

1. Convert the decimal representation of the subnet mask to a binary representation.
2. Count each "1" in the subnet mask. The total is the subnet mask number.

For example, to write the IP address 192.168.42.23 with a subnet mask of 255.255.255.0 in slash notation:

1. Convert the subnet mask to binary.  
*In this example, the binary representation of 255.255.255.0 is:  
11111111.11111111.11111111.00000000.*
2. Count each 1 in the subnet mask.  
*In this example, there are twenty-four (24).*
3. Write the original IP address, a forward slash (/), and then the number from Step 2.  
*The result is 192.168.42.23/24.*

This table shows common network masks and their equivalents in slash notation.

Network mask	Slash equivalent
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30

## About Entering IP Addresses

When you type IP addresses in the Quick Setup Wizard or dialog boxes, type the digits and decimals in the correct sequence. Do not use the TAB key, arrow keys, spacebar, or mouse to put your cursor after the decimals.

For example, if you type the IP address 172.16.1.10, do not type a space after you type 16. Do not try to put your cursor after the subsequent decimal to type 1. Type a decimal directly after 16, and then type 1.10. Press the slash (/) key to move to the netmask.

## Static and Dynamic IP Addresses

ISPs (Internet service providers) assign an IP address to each device on their network. The IP address can be *static* or *dynamic*.

## Static IP Addresses

A static IP address is an IP address that always stays the same. If you have a web server, FTP server, or other Internet resource that must have an address that cannot change, you can get a static IP address from your ISP. A static IP address is usually more expensive than a dynamic IP address, and some ISPs do not supply static IP addresses. You must configure a static IP address manually.

## Dynamic IP Addresses

A dynamic IP address is an IP address that an ISP lets you use temporarily. If a dynamic address is not in use, it can be automatically assigned to a different device. Dynamic IP addresses are assigned using either DHCP or PPPoE.

## About DHCP

Dynamic Host Configuration Protocol (DHCP) is an Internet protocol that computers on a network use to get IP addresses and other information such as the default gateway. When you connect to the Internet, a computer configured as a DHCP server at the ISP automatically assigns you an IP address. It could be the same IP address you had before, or it could be a new one. When you close an Internet connection that uses a dynamic IP address, the ISP can assign that IP address to a different customer.

You can configure your XTM device as a DHCP server for networks behind the device. You assign a range of addresses for the DHCP server to use.

## About PPPoE

Some ISPs assign IP addresses through Point-to-Point Protocol over Ethernet (PPPoE). PPPoE adds some of the features of Ethernet and PPP to a standard dial-up connection. This network protocol allows the ISP to use the billing, authentication, and security systems of their dial-up infrastructure with DSL modem and cable modem products.

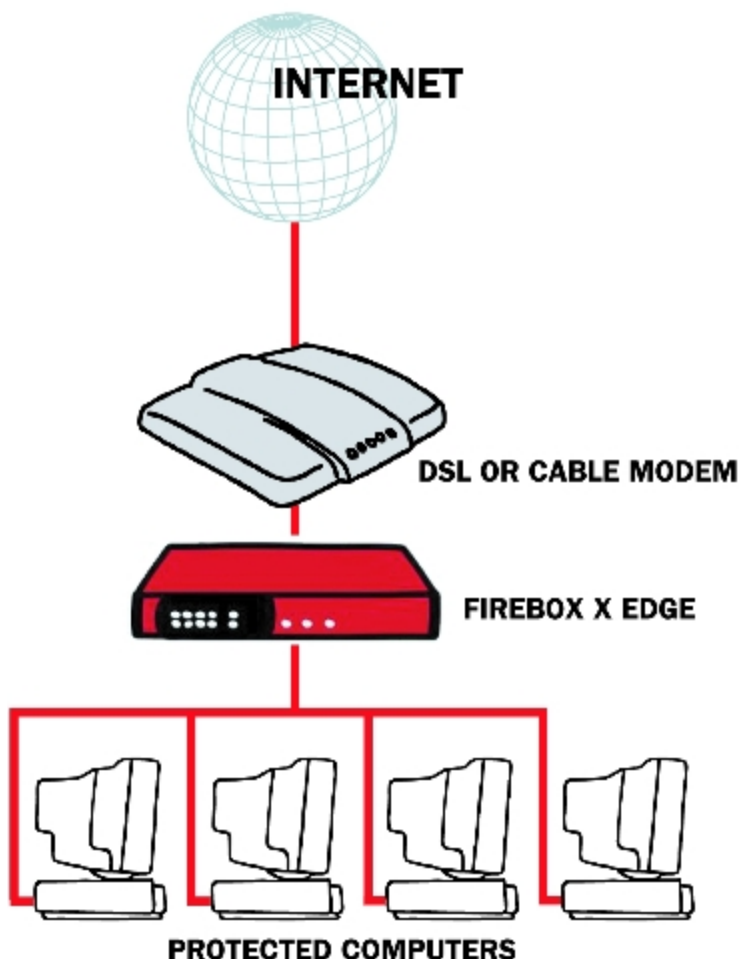
## About DNS (Domain Name System)

You can frequently find the address of a person you do not know in the telephone directory. On the Internet, the equivalent to a telephone directory is the *DNS* (Domain Name System). DNS is a network of servers that translate numeric IP addresses into readable Internet addresses, and vice versa. DNS takes the *friendly* domain name you type when you want to see a particular web site, such as `www.example.com`, and finds the equivalent IP address, such as `50.50.50.1`. Network devices need the actual IP address to find the web site, but domain names are much easier for users to type and remember than IP addresses.

A *DNS server* is a server that performs this translation. Many organizations have a private DNS server in their network that responds to DNS requests. You can also use a DNS server on your external network, such as a DNS server provided by your ISP (Internet Service Provider.)

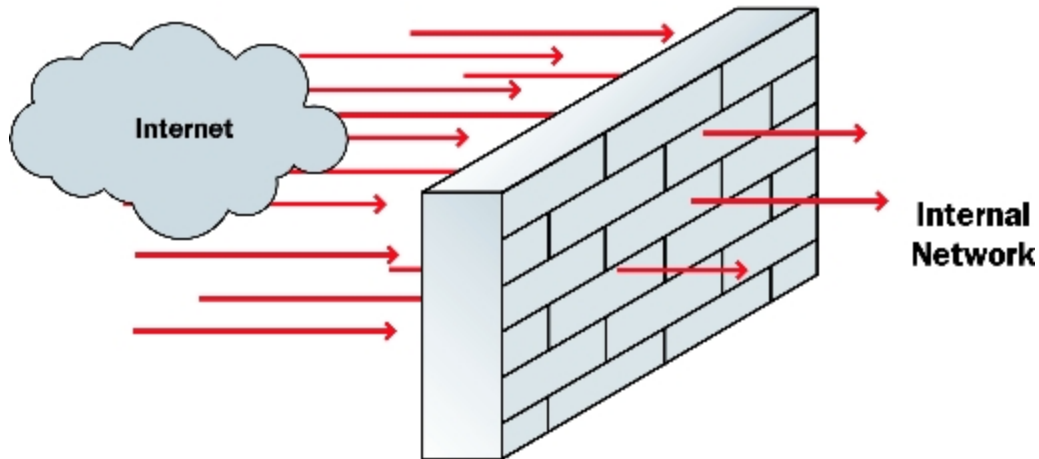
## About Firewalls

A network security device, such as a firewall, separates your internal networks from external network connections to decrease the risk of an external attack. The figure below shows how a firewall protects the computers on a trusted network from the Internet.



Firewalls use access policies to identify and filter different types of information. They can also control which policies or ports the protected computers can use on the Internet (outbound access). For example, many firewalls have sample security policies that allow only specified traffic types. Users can select the policy that is best for them. Other firewalls, such as XTM devices, allow the user to customize these policies.

For more information, see *About Services and Policies* on page 7 and *About Ports* on page 8



Firewalls can be in the form of hardware or software. A firewall protects private networks from unauthorized users on the Internet. Traffic that enters or leaves the protected networks is examined by the firewall. The firewall denies network traffic that does not match the security criteria or policies.

In some closed, or *default-deny* firewalls, all network connections are denied unless there is a specific rule to allow the connection. To deploy this type of firewall, you must have detailed information about the network applications required to meet needs of your organization. Other firewalls allow all network connections that have not been explicitly denied. This type of open firewall is easier to deploy, but it is not as secure.

## About Services and Policies

You use a *service* to send different types of data (such as email, files, or commands) from one computer to another across a network or to a different network. These services use protocols. Frequently used Internet services are:

- World Wide Web access uses Hypertext Transfer Protocol (HTTP)
- Email uses Simple Mail Transfer Protocol (SMTP) or Post Office Protocol (POP3)
- File transfer uses File Transfer Protocol (FTP)
- Resolve a domain name to an Internet address uses Domain Name Service (DNS)
- Remote terminal access uses Telnet or SSH (Secure Shell)

When you allow or deny a service, you must add a *policy* to your XTM device configuration. Each policy you add can also add a security risk. To send and receive data, you must *open a door* in your computer, which puts your network at risk. We recommend that you add only the policies that are necessary for your business.

As an example of how you can use a policy, suppose the network administrator of a company wants to activate a Windows terminal services connection to the company's public web server on the optional interface of the XTM device. He or she routinely administers the web server with a Remote Desktop

connection. At the same time, he or she wants to make sure that no other network users can use the Remote Desktop Protocol terminal services through the XTM device. The network administrator would add a policy that allows RDP connections only from the IP address of his or her own desktop computer to the IP address of the public web server.

When you configure your XTM device with the Quick Setup Wizard, the wizard adds only limited outgoing connectivity. If you have more software applications and network traffic for your XTM device to examine, you must:

- Configure the policies on your XTM device to pass through necessary traffic
- Set the approved hosts and properties for each policy
- Balance the requirement to protect your network against the requirements of your users to get access to external resources

## About Ports

Although computers have hardware ports you use as connection points, ports are also numbers used to map traffic to a particular process on a computer. These ports, also called *TCP and UDP ports*, are where programs transmit data. If an IP address is like a street address, a port number is like an apartment unit number or building number within that street address. When a computer sends traffic over the Internet to a server or another computer, it uses an IP address to identify the server or remote computer, and a port number to identify the process on the server or computer that receives the data.

For example, suppose you want to see a particular web page. Your web browser attempts to create a connection on port 80 (the port used for HTTP traffic) for each element of the web page. When your browser receives the data it requests from the HTTP server, such as an image, it closes the connection.

Many ports are used for only one type of traffic, such as port 25 for SMTP (Simple Mail Transfer Protocol). Some protocols, such as SMTP, have ports with assigned numbers. Other programs are assigned port numbers dynamically for each connection. The IANA (Internet Assigned Numbers Authority) keeps a list of well-known ports. You can see this list at:

<http://www.iana.org/assignments/port-numbers>

Most policies you add to your XTM device configuration have a port number between 0 and 1024, but possible port numbers can be from 0 to 65535.

Ports are either open or closed. If a port is open, your computer accepts information and uses the protocol identified with that port to create connections to other computers. However, an open port is a security risk. To protect against risks created by open ports, you can block ports used by hackers to attack your network. For more information, see *About Blocked Ports* on page 539.

You can also block port space probes: TCP or UDP traffic that is sent by a host to a range of ports to find information about networks and their hosts. For more information, see *About Port Space and Address Space Probes* on page 529.



# 2 Introduction to Fireware XTM

---

## About Fireware XTM

Fireware XTM gives you an easy and efficient way to view, manage, and monitor each XTM device in your network. The Fireware XTM solution includes four software applications:

- WatchGuard System Manager (WSM)
- Fireware XTM Web UI
- Fireware XTM Command Line Interface (CLI)
- WatchGuard Server Center

You can use one or more of the Fireware XTM applications to configure your network for your organization. For example, if you have only one XTM 2 Series device, you can perform most configuration tasks with Fireware XTM Web UI or Fireware XTM Command Line Interface. However, for more advanced logging and reporting features, you must use WatchGuard Server Center. If you manage more than one XTM device, or if you have purchased Fireware XTM with a Pro upgrade, we recommend that you use WatchGuard System Manager (WSM). If you choose to manage and monitor your configuration with Fireware XTM Web UI, there are some features that you cannot configure.

For more information about these limitations, see the *Fireware XTM Web UI Help* at:

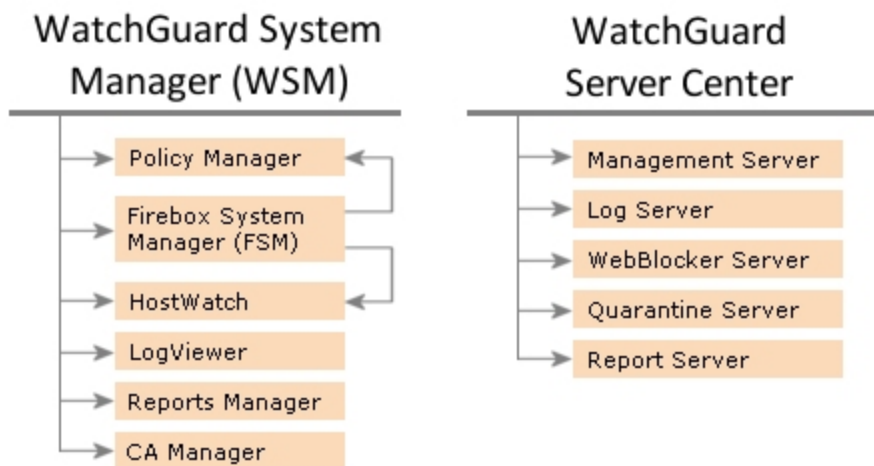
<http://www.watchguard.com/help/docs/webui/11/en-US/index.html>.

For more information on how to connect to your XTM device with Fireware XTM Web UI or Fireware XTM Command Line Interface, see the *Help* or *User Guide* for those products. You can view and download the most current documentation for these products on the Fireware XTM Product Documentation page:

<http://www.watchguard.com/help/documentation/xtm.asp>

## Fireware XTM Components

To start WatchGuard System Manager or WatchGuard Server Center from your Windows desktop, select the shortcut from the Start Menu. You can also start WatchGuard Server Center from an icon in the System Tray. From these applications, you can launch other tools that help you manage your network. For example, from WatchGuard System Manager (WSM), you can launch Policy Manager or HostWatch.



## WatchGuard System Manager

WatchGuard System Manager (WSM) is the primary application for network management with your XTM device. You can use WSM to manage many different XTM devices, even those that use different software versions. WSM includes a comprehensive suite of tools to help you monitor and control network traffic.

### *Policy Manager*

You can use Policy Manager to configure your firewall. Policy Manager includes a full set of pre-configured packet filters, proxy policies, and application layer gateways (ALGs). You can also make a custom packet filter, proxy policy, or ALG in which you set the ports, protocols, and other options. Other features of Policy Manager help you to stop network intrusion attempts, such as SYN Flood attacks, spoofing attacks, and port or address space probes.

For more information, see *About Policy Manager*.

### *Firebox System Manager (FSM)*

Firebox System Manager gives you one interface to monitor all components of your XTM device. From FSM, you can see the real-time status of your XTM device and its configuration.

For more information, see *About Firebox System Manager (FSM)*.

### *HostWatch*

HostWatch is a real-time connection monitor that shows network traffic between different XTM device interfaces. HostWatch also shows information about users, connections, ports, and services.

For more information, see *About HostWatch*.

### *LogViewer*

LogViewer is the WatchGuard System Manager tool you use to see log file data. It can show the log data page by page, or search and display by key words or specified log fields.

For more information, see *About Logging and Log Files*.

### *Report Manager*

You can use Report Manager to generate reports of the data collected from your Log Servers for all your XTM devices. From Report Manager, you can see the available WatchGuard Reports for you XTM devices.

For more information, see *About WatchGuard Report Manager*.

### *CA Manager*

The Certificate Authority (CA) Manager shows a complete list of security certificates installed on your management computer with Fireware XTM. You can use this application to import, configure, and generate certificates for use with VPN tunnels and other authentication purposes.

## **WatchGuard Server Center**

WatchGuard Server Center is the application where you configure and monitor all your WatchGuard servers.

For more information about WatchGuard Server Center, see *Set Up WatchGuard Servers*.

### *Management Server*

The Management Server operates on a Windows computer. With this server, you can manage all firewall devices and create virtual private network (VPN) tunnels using a simple drag-and-drop function. The basic functions of the Management Server are:

- Certificate authority to distribute certificates for Internet Protocol Security (IPSec) tunnels
- VPN tunnel configuration management
- Management for multiple XTM devices

For more information on the Management Server, see *About the WatchGuard Management Server*.

### *Log Server*

The Log Server collects log messages from each XTM device. These log messages are encrypted when they are sent to the Log Server. The log message format is XML (plain text). The information collected from firewall devices includes these log messages: traffic, event, alarm, debug (diagnostic), and statistic.

For more information, see *Set Up a Log Server*.

#### *WebBlocker Server*

The WebBlocker Server operates with the XTM device HTTP proxy to deny user access to specified categories of web sites. When you configure your XTM device, you specify the categories of web sites to allow or block.

For more information on WebBlocker and the WebBlocker Server, see *About WebBlocker*.

#### *Quarantine Server*

The Quarantine Server collects and isolates email messages that spamBlocker suspects to be email spam, or emails that are suspected to have a virus.

For more information, see *About the Quarantine Server*.

#### *Report Server*

The Report Server periodically consolidates data collected by your Log Servers from your XTM devices, and then periodically generates reports. Once the data is on the Report Server, you can use Report Manager to generate and see reports.

For more information about reports and the Report Server, see *About the Report Server*.

## **Fireware XTM Web UI and Command Line Interface**

Fireware XTM Web UI and Command Line Interface are alternative management solutions that can perform most of the same tasks as WatchGuard System Manager and Policy Manager. Some advanced configuration options and features, such as FireCluster settings, are not available in Fireware XTM Web UI or Command Line Interface.

## Fireware XTM with a Pro Upgrade

The Pro upgrade to Fireware XTM provides several advanced features for experienced customers, such as server load balancing and additional SSL VPN tunnels. The features available with a Pro upgrade depend on the type and model of your XTM device:

Feature	XTM 5 Series	XTM 5 Series, 8 Series, and 1050 (Pro)	XTM 2 Series	XTM 2 Series (Pro)
FireCluster		X		
VLANs	75 max.	75 max. (Core/5 Series) 200 max. (Peak/XTM 8 Series and 1050)	20 max.	50 max.
Dynamic Routing (OSPF and BGP)		X		X
Policy-Based Routing		X		X
Server Load Balancing		X		
Maximum SSL VPN Tunnels		X		X
Multi-WAN Failover	X	X		X
Multi-WAN Load Balancing		X		X

To purchase Fireware XTM with a Pro upgrade, contact your local reseller.



# 3 Service and Support

---

## About WatchGuard Support

WatchGuard® knows just how important support is when you must secure your network with limited resources. Our customers require greater knowledge and assistance in a world where security is critical. LiveSecurity® Service gives you the backup you need, with a subscription that supports you as soon as you register your XTM device.

### LiveSecurity Service

Your XTM device includes a subscription to our ground-breaking LiveSecurity Service, which you activate online when you register your product. As soon as you activate, your LiveSecurity Service subscription gives you access to a support and maintenance program unmatched in the industry.

LiveSecurity Service comes with the following benefits:

#### *Hardware Warranty with Advance Hardware Replacement*

An active LiveSecurity subscription extends the one-year hardware warranty that is included with each XTM device. Your subscription also provides advance hardware replacement to minimize downtime in case of a hardware failure. If you have a hardware failure, WatchGuard will ship a replacement unit to you before you have to send back the original hardware.

#### *Software Updates*

Your LiveSecurity Service subscription gives you access to updates to current software and functional enhancements for your WatchGuard products.

#### *Technical Support*

When you need assistance, our expert teams are ready to help:

- Representatives available 12 hours a day, 5 days a week in your local time zone\*
- Four-hour targeted maximum initial response time
- Access to online user forums moderated by senior support engineers

### Support Resources and Alerts

Your LiveSecurity Service subscription gives you access to a variety of professionally produced instructional videos, interactive online training courses, and online tools specifically designed to answer questions you may have about network security in general or the technical aspects of installation, configuration, and maintenance of your WatchGuard products.

Our Rapid Response Team, a dedicated group of network security experts, monitors the Internet to identify emerging threats. They then deliver LiveSecurity Broadcasts to tell you specifically what you can do to address each new menace. You can customize your alert preferences to fine-tune the kind of advice and alerts the LiveSecurity Service sends you.

## LiveSecurity Service Gold

LiveSecurity Service Gold is available for companies that require 24-hour availability. This premium support service gives expanded hours of coverage and faster response times for around-the-clock remote support assistance. LiveSecurity Service Gold is required on each unit in your organization for full coverage.

Service Features	LiveSecurity Service	LiveSecurity Service Gold
Technical Support hours	6AM–6PM, Monday–Friday*	24/7
Number of support incidents (online or by phone)	5 per year	Unlimited
Targeted initial response time	4 hours	1 hour
Interactive support forum	Yes	Yes
Software updates	Yes	Yes
Online self-help and training tools	Yes	Yes
LiveSecurity broadcasts	Yes	Yes
Installation Assistance	Optional	Optional
Three-incident support package	Optional	N/A
One-hour, single incident priority response upgrade	Optional	N/A
Single incident after-hours upgrade	Optional	N/A

\* In the Asia Pacific region, standard support hours are 9AM–9PM, Monday–Friday (GMT +8).

## Service Expiration

To secure your organization, we recommend that you keep your LiveSecurity subscription active. When your subscription expires, you lose up-to-the-minute security warnings and regular software updates. This loss can put your network at risk. Damage to your network is much more expensive than a LiveSecurity Service subscription renewal. If you renew within 30 days, there is no reinstatement fee.



# 4 Getting Started

---

## Before You Begin

Before you begin the installation process, make sure you complete the tasks described in the subsequent sections.

**Note** *In these installation instructions, we assume your XTM device has one trusted, one external, and one optional interface configured. To configure additional interfaces on your device, use the configuration tools and procedures described in the Network Setup and Configuration topics.*

## Verify Basic Components

Make sure that you have these items:

- A computer with a 10/100BaseT Ethernet network interface card and a web browser installed
- A WatchGuard XTM device
- A serial cable (blue)
- One crossover Ethernet cable (red)
- One straight Ethernet cable (green)
- Power cable or AC power adapter

## Get an XTM Device Feature Key

To enable all of the features on your XTM device, you must register the device on the WatchGuard LiveSecurity web site and get your feature key. The XTM device has only one user license (seat license) until you apply your feature key.

If you register your XTM device before you use the Quick Setup Wizard, you can paste a copy of your feature key in the wizard. The wizard then applies it to your device. If you do not paste your feature key into the wizard, you can still finish the wizard. Until you add your feature key, only one connection is allowed to the Internet.

You also get a new feature key for any optional products or services when you purchase them. After you register your XTM device or any new feature, you can synchronize your XTM device feature key with the feature keys kept in your registration profile on the WatchGuard LiveSecurity site. You can use WatchGuard System Manager (WSM) at any time to get your feature key.

To learn how to register your XTM device and get a feature key, see *Get a Feature Key from LiveSecurity* on page 59.

## Gather Network Addresses

We recommend that you record your network information before and after you configure your XTM device. Use the first table below for your network IP addresses before you put the device into operation.

WatchGuard uses slash notation to show the subnet mask. For more information, see *About Slash Notation* on page 3. For more information on IP addresses, see *About IP Addresses* on page 3.

Table 1: Network IP addresses without the XTM device	
Wide Area Network	____.____.____.____ / ____
Default Gateway	____.____.____.____
Local Area Network	____.____.____.____ / ____
Secondary Network (if applicable)	____.____.____.____ / ____
Public Server(s) (if applicable)	____.____.____.____
	____.____.____.____
	____.____.____.____

Use the second table for your network IP addresses after you put the XTM device into operation.

### *External interface*

Connects to the external network (typically the Internet) that is not trusted.

### *Trusted interface*

Connects to the private LAN (local area network) or internal network that you want to protect.

*Optional interface(s)*

Usually connects to a mixed trust area of your network, such as servers in a DMZ (demilitarized zone). You can use optional interfaces to create zones in the network with different levels of access.

**Table 2: Network IP addresses with the XTM device**

Default Gateway	____.____.____.____
External Interface	____.____.____.____ / ____
Trusted Interface	____.____.____.____ / ____
Optional Interface	____.____.____.____ / ____
Secondary Network (if applicable)	____.____.____.____ / ____

## Select a Firewall Configuration Mode

You must decide how you want to connect the XTM device to your network before you run the Quick Setup Wizard. The way you connect the device controls the interface configuration. When you connect the device, you select the configuration mode—routed or drop-in—that is best suited to your current network.

Many networks operate best with mixed routing configuration, but we recommend the drop-in mode if:

- You have already assigned a large number of static IP addresses and do not want to change your network configuration.
- You cannot configure the computers on your trusted and optional networks that have public IP addresses with private IP addresses.

This table and the descriptions below the table show three conditions that can help you to select a firewall configuration mode.

Mixed Routing Mode	Drop-in Mode
All of the XTM device interfaces are on different networks.	All of the XTM device interfaces are on the same network and have the same IP address.
Trusted and optional interfaces must be on different networks. Each interface has an IP address on its network.	The computers on the trusted or optional interfaces can have a public IP address.
Use static NAT (network address translation) to map public addresses to private addresses behind the trusted or optional interfaces.	NAT is not necessary because the computers that have public access have public IP addresses.

For more information about drop-in mode, see *Drop-In Mode* on page 98.

For more information about mixed routing mode, see *Mixed Routing Mode* on page 90.

The XTM device also supports a third configuration mode called bridge mode. This mode is less commonly used. For more information about bridge mode, see *Bridge Mode* on page 103.

**Note** You can use the Web Setup Wizard or the WSM Quick Setup Wizard to create your initial configuration. When you run the Web Setup Wizard, the firewall configuration is automatically set to mixed routing mode. When you run the WSM Quick Setup Wizard, you can configure the device in mixed routing mode or drop-in mode.

## Decide Where to Install Server Software

When you run the WatchGuard System Manager Installer, you can install WatchGuard System Manager and the WatchGuard servers on the same computer. You can also use the same installation procedure to install the WatchGuard servers on different computers. This helps to distribute the server load and supply redundancy. To ensure the Management Server operates correctly, you must install it on a computer also has WSM installed. To decide where to install server software, you must examine the capacity of your management computer and select the installation method that matches your environment.

If you install server software on a computer with an active desktop firewall other than Windows Firewall, you must open the ports necessary for the servers to connect through the firewall. Windows Firewall users do not have to change their desktop firewall configuration because the installation program opens the necessary ports through Windows Firewall automatically.

For more information, see *Install WatchGuard Servers on Computers with Desktop Firewalls* on page 32 .

To start the installation process, *Install WatchGuard System Manager Software*.

## Install WatchGuard System Manager Software

You install WatchGuard System Manager (WSM) software on a computer that you designate as the *management computer*. You can use tools on the management computer to get access to information on the XTM device, such as connection and tunnel status, statistics on traffic, and log messages.

Select one Windows-based computer on your network as the management computer and install the management software. To install the WatchGuard System Manager software, you must have administrative privileges on the management computer. After installation, you can operate with Windows XP or Windows 2003 Power User privileges.

You can install more than one version of WatchGuard System Manager on the same management computer. However, you can install only one version of server software on a computer at a time. For example, you cannot have two Management Servers on the same computer.

## Back up Your Previous Configuration

If you have a previous version of WatchGuard System Manager, make a backup of your security policy configuration before you install a new version. For instructions to make a backup of your configuration, see *Make a Backup of the XTM Device Image* on page 43.

## Download WatchGuard System Manager

You can download the most current WatchGuard System Manager software at any time from <https://www.watchguard.com/archive/softwarecenter.asp>. You must log in with your LiveSecurity user credentials. If you are a new user, before you can download the WSM software, you must create a user profile and activate your product at <http://www.watchguard.com/activate>.

The management computer software is available in two encryption levels. Make sure you select the correct encryption level. For more information, see *About Software Encryption Levels* on page 22.

**Note** *If you install one of the WSM servers on a computer with a personal firewall other than the Microsoft Windows firewall, you must open the ports for the servers to connect through the firewall. To allow connections to the WebBlocker Server, open UDP port 5003. It is not necessary to change your configuration if you use the Microsoft Windows firewall. For more information, see the *Install WatchGuard Servers on Computers with Desktop Firewalls* on page 32.*

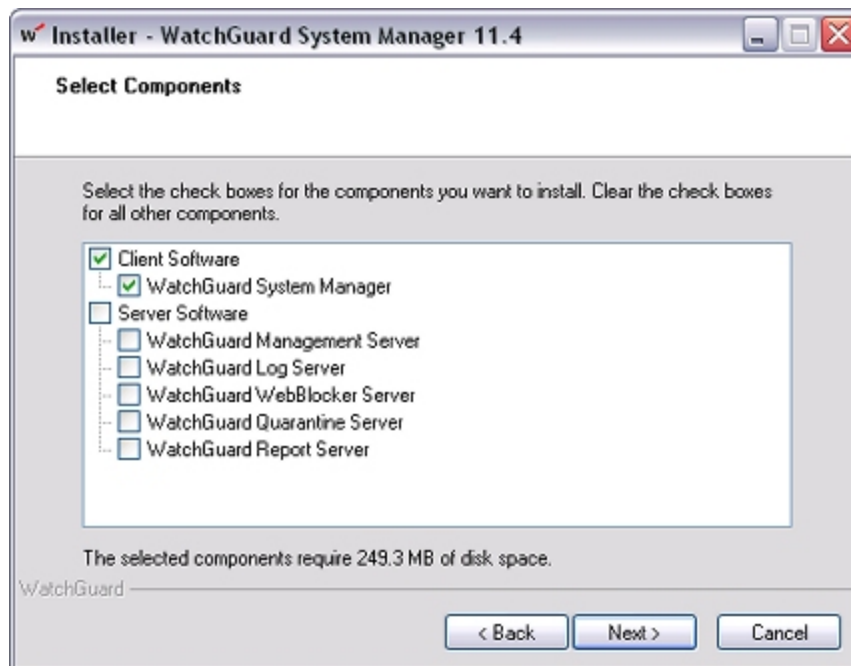
To install the Management Server:

1. On the management computer, download the latest WatchGuard System Manager (WSM) software.
2. On the same computer, download the latest Fireware XTM OS.
3. Run the Installer and follow the instructions to complete the installation.

The Installer includes a **Select Components** page, where you select the software components or upgrades to install.

Make sure you select the check boxes for only the components you want to install.

Some software components require a different license.



4. Run the Quick Setup Wizard. You can run this wizard from the web or as a Windows application.
  - For instructions to run the wizard from the web, see *Run the Web Setup Wizard* on page 23.
  - For instructions to run the wizard as a Windows application, see *Run the WSM Quick Setup Wizard* on page 26.

## About Software Encryption Levels

WatchGuard management computer software is available in these two encryption levels:

### *Base*

Supports 40-bit encryption for Mobile VPN with PPTP tunnels. You cannot create an IPSec VPN tunnel with this level of encryption.

### *Strong*

Supports 40-bit and 128-bit encryption for Mobile VPN with PPTP. Also supports 56-bit and 168-bit DES, and 128-bit, 192-bit, and 256-bit AES.

To use virtual private networking with IPSec, you must download the strong encryption software. Strong export limits apply to the strong encryption software. It is possible that it is not available for download in your location.

## About the Quick Setup Wizard

You can use the Quick Setup Wizard to create a basic configuration for your XTM device. The device uses this basic configuration file when it starts for the first time. This enables it to operate as a basic firewall. You can use this same procedure at any time to reset the device to a new basic configuration. This is helpful for system recovery.

When you configure your XTM device with the Quick Setup Wizard, you set only the basic policies (TCP and UDP outgoing, FTP packet filter, ping, and WatchGuard) and interface IP addresses. If you have more software applications and network traffic for the device to examine, you must:

- Configure the policies on the XTM device to let the necessary traffic through
- Set the approved hosts and properties for each policy
- Balance the requirement to protect your network against the requirements of your users to connect to external resources

You can run the Quick Setup Wizard from a web browser or as a Windows application.

For instructions to run the wizard from a web browser, see *Run the Web Setup Wizard* on page 23.

For instructions to run the wizard as a Windows application, see *Run the WSM Quick Setup Wizard* on page 26.

## Run the Web Setup Wizard

You can use the Web Setup Wizard to set up a basic configuration on any WatchGuard XTM device. The Web Setup Wizard automatically configures the XTM device for mixed routing mode.

To use the Web Setup Wizard, you must make a direct network connection to the XTM device and use a web browser to start the wizard. When you configure your XTM device, it uses DHCP to send a new IP address to your management computer.

Before you start the Web Setup Wizard, make sure you:

- Register your XTM device with LiveSecurity Service
- Store a copy of your XTM device feature key in a text file on your management computer

## Start the Web Setup Wizard

1. Use the red crossover Ethernet cable that ships with your XTM device to connect the management computer to interface number 1 of your XTM device. This is the trusted interface.
2. Connect the power cord to the XTM device power input and to a power source.
3. Start the XTM device in factory default mode. This is also known as safe mode.

For more information, see *Reset an XTM Device to a Previous or New Configuration* on page 55.

4. Make sure your management computer is configured to accept a DHCP-assigned IP address.

If your management computer uses Windows XP:

- In the Windows **Start** menu, select **All Programs > Control Panel > Network Connections > Local Area Connections**.
  - Click **Properties**.
  - Select **Internet Protocol (TCP/IP)** and click **Properties**.
  - Make sure **Obtain an IP Address Automatically** is selected.
5. If your browser uses an HTTP proxy server, you must temporarily disable the HTTP proxy setting in your browser.

For more information, see *Disable the HTTP Proxy in the Browser* on page 35.

6. Open a web browser and type the factory default IP address of the trusted interface (interface 1), `https://10.0.1.1:8080`.

If you use Internet Explorer, make sure you type `https://` at the start of the IP address. This opens a secure HTTP connection between your management computer and the XTM device.

*The Web Setup Wizard starts automatically.*

7. Log in with the default administrator account credentials:

**Username:** admin

**Passphrase:** readwrite

8. Complete the subsequent screens of the wizard.

The Web Setup Wizard includes this set of dialog boxes. Some dialog boxes appear only if you select certain configuration methods:

*Login*

Log in with the default administrator account credentials. For **Username**, select admin. For **Passphrase**, use the passphrase: readwrite.

*Welcome*

The first screen tells you about the wizard.

*Select a configuration type*

Select whether to create a new configuration or restore a configuration from a saved backup image.

*License agreement*

You must accept the license agreement to continue with the wizard.

*Retrieve Feature Key, Apply Feature Key, Feature key options*

If your XTM device does not already have a feature key the wizard provides options for you to download or import a feature key. The wizard can only download a feature key if it has a connection to the Internet. If you have downloaded a local copy of the feature key to your computer, you can paste that into the setup wizard.

If the XTM device does not have an Internet connection while you run the wizard, and you did not register the device and download the feature key to your computer before you started the wizard, you can choose to not apply a feature key.

**Note** *If you do not apply a feature key in the Web Setup Wizard you must register the device and apply the feature key in the Fireware XTM Web UI. Functionality of the device is limited until you apply a feature key.*

*Configure the External Interface of your Firebox*

Select the method your ISP uses to assign your IP address. The choices are DHCP, PPPoE or Static.

*Configure the External Interface for DHCP*

Type your DHCP identification as supplied by your ISP.

*Configure the External Interface for PPPoE*

Type your PPPoE information as supplied by your ISP.

*Configure the External Interface with a static IP address*

Type your static IP address information as supplied by your ISP.

*Configure the DNS and WINS Servers*

Type the Domain DNS and WINS server addresses you want the XTM device to use.



### *Configure the Trusted Interface of the Firebox*

Type the IP address of the trusted interface. Optionally, you can enable the DHCP server for the trusted interface.

### *Create passphrases for your device*

Type a passphrase for the status (read only) and admin (read/write) management accounts on the XTM device.

### *Enable remote management*

Enable remote management if you want to manage this device from the external interface.

### *Add contact information for your device*

You can type a device name, location, and contact information to save management information for this device. By default, the device name is set to the model number of your XTM device. We recommend that you choose a unique name that you can use to easily identify this device, especially if you use remote management.

### *Set the Time Zone*

Select the time zone where the XTM device is located.

### *The Quick Setup Wizard is complete*

After you complete the wizard, the XTM device restarts.

If you leave the Web Setup Wizard idle for 15 minutes or more, you must go back to Step 3 and start again.

**Note** *If you change the IP address of the trusted interface, you must change your network settings to make sure your IP address matches the subnet of the trusted network before you connect to the XTM device. If you use DHCP, restart your computer.*

## **After the Wizard Finishes**

After you complete all screens in the wizard, the XTM device is configured with a basic configuration that includes four policies (TCP outgoing, FTP packet filter, ping, and WatchGuard) and the interface IP addresses you specified. You can use Policy Manager to expand or change the configuration for your XTM device.

- For information about how to complete the installation of your XTM device after the Web Setup Wizard is finished, see *Complete Your Installation* on page 28.
- For information about how to start WatchGuard System Manager, see *Start WatchGuard System Manager* on page 29.

## If You Have Problems with the Wizard

If the Web Setup Wizard is unable to install the Fireware XTM OS on the XTM device, the wizard times out. If you have problems with the wizard, check these things:

- The Fireware XTM OS file you downloaded from the LiveSecurity web site could be corrupted. For an XTM 5 Series, 8 Series, or 1050 device, if the software image is corrupted, this message can appear on the LCD interface: *File Truncate Error*.

If this message appears, download the software again and try the wizard once more.

- If you use Internet Explorer 6, clear the file cache in your web browser and try again.

To clear the cache, in Internet Explorer select **Tools > Internet Options > Delete Files**.

## Run the WSM Quick Setup Wizard

The Quick Setup Wizard runs as a Windows application to help you make a basic configuration file. This basic configuration file allows your device to operate as a basic firewall when you start it for the first time. After you run the Quick Setup Wizard, you can use Policy Manager to expand or change the configuration.

The Quick Setup Wizard uses a device discovery procedure to find the XTM device model you want to configure. This procedure uses UDP multicast. Software firewalls (for example, the firewall in Microsoft Windows XP SP2) can cause problems with device discovery.

## Before You Begin

Before you start the Quick Setup Wizard, make sure you:

- Register your XTM device with LiveSecurity Service.
- Store a copy of your feature key in a text file on your management computer.
- Download WSM and Fireware XTM installation files from the LiveSecurity Service web site to your management computer.
- Install the WSM and Fireware XTM software on your management computer.
- Configure the management computer with a static IP address on the same network as the trusted interface of your device. Or, configure the management computer to accept an IP address assigned with DHCP.

## Start the Quick Setup Wizard

1. Use the red, crossover Ethernet cable that ships with your XTM device to connect the management computer to the trusted interface (interface number 1) of your XTM device.
2. From the Windows Start Menu, select **All Programs > WatchGuard System Manager 11.x > Quick Setup Wizard**.

Or, from WatchGuard System Manager, select **Tools > Quick Setup Wizard**.

*The Quick Setup Wizard starts.*

3. Complete the wizard to set up your XTM device with a basic configuration. The steps include:

*Identify and discover your device*

Follow the instructions for device discovery. You might need to select your XTM device model or reconnect the crossover Ethernet cable. After the wizard discovers the XTM device, you give it a name that identifies this device in WatchGuard System Manager, log files, and reports.

*Select a setup procedure*

Select whether you want to install the Fireware XTM OS and create a new configuration, or if you want to only create a new configuration for your XTM device.

*Add a feature key*

Follow the instructions to download the feature key from the LiveSecurity Service web site, or browse to the location of the feature key file you previously downloaded.

*Configure the external interface*

You can configure the external interface with a static IP address, or you can configure it to use an IP address assigned with DHCP or PPPoE. You must also add an IP address for the default gateway of the XTM device. This is the IP address of your gateway router.

*Configure the internal interfaces*

Select the IP addresses to use for the trusted and optional interfaces. If you want to configure the XTM device in drop-in mode, you can also use the external interface IP address for these interfaces.

For more information about drop-in mode, see *Drop-In Mode* on page 98.

*Set passphrases*

You must create two passphrases for connections to the XTM device: a status passphrase for read-only connections and a configuration passphrase for read-write connections. Both passphrases must be at least 8 characters long, and they must be different from each other.

4. Click **Finish** to close the wizard.

*The wizard saves the basic configuration to the XTM device and to a local configuration file.*

## After the Wizard Finishes

After you complete the wizard, the XTM device restarts. If you changed the IP address of your management computer to run the Quick Setup Wizard, you might need to change the IP address back again after you complete the wizard.

After the XTM device restarts, it uses a basic configuration that includes five policies (TCP and UDP outgoing, FTP packet filter, ping, WatchGuard, and WatchGuard Web UI) and the interface IP addresses you specified. You can use Policy Manager to change this basic configuration.

- For information about how to complete the installation of your XTM device after the Quick Setup Wizard is finished, see *Complete Your Installation* on page 28.
- For information about how to start WatchGuard System Manager, see *Start WatchGuard System Manager* on page 29.

## Complete Your Installation

After you are finished with either the Web Setup Wizard or the WSM Quick Setup Wizard, you must complete the installation of your XTM device on your network.

1. Put the XTM device in its permanent physical location.
2. Make sure the gateway of management computer and the rest of the trusted network is the IP address of the trusted interface of your XTM device.
3. To connect the management computer to your XTM device, open WatchGuard System Manager and select **File > Connect To Device**.

**Note** You must use the status (read-only) passphrase to connect to the XTM device.

4. If you use a routed configuration, make sure you change the default gateway on all the computers that connect to your XTM device to match the IP address of the XTM device trusted interface.
5. Customize your configuration as necessary for the security purposes of your business.

For more information, see the subsequent *Customize your security policy* section.

6. If you installed one or more WatchGuard servers, *Set Up WatchGuard Servers*.

**Note** If you installed WatchGuard server software on a computer with an active desktop firewall other than Windows Firewall, you must open the ports necessary for the servers to connect through the firewall. Windows Firewall users do not have to change their configuration. For more information, see *Install WatchGuard Servers on Computers with Desktop Firewalls* on page 32.

## Customize Your Security Policy

Your security policy controls who can get into and out of your network, and where they can go in your network. The configuration file of your XTM device manages the security policies.

When you completed the Quick Setup Wizard, the configuration file that you made was only a basic configuration. You can modify this configuration to align your security policy with the business and security requirements of your company. You can add packet filter and proxy policies to set what you let in and out of your network. Each policy can have an effect on your network. The policies that increase your network security can decrease access to your network. And the policies that increase access to your network can put the security of your network at risk. For more information on policies, see *About Policies* on page 363.

For a new installation, we recommend that you use only packet filter policies until all your systems operate correctly. As necessary, you can add proxy policies.

## About LiveSecurity Service

Your XTM device includes a subscription to LiveSecurity Service. Your subscription:

- Makes sure that you get the newest network protection with the newest software upgrades
- Gives solutions to your problems with full technical support resources
- Prevents service interruptions with messages and configuration help for the newest security problems

- Helps you to find out more about network security through training resources
- Extends your network security with software and other features
- Extends your hardware warranty with advanced replacement

For more information about LiveSecurity Service, see *About WatchGuard Support* on page 15.

## Start WatchGuard System Manager

On the computer where you installed WatchGuard System Manager (WSM):


Select **Start > All Programs > WatchGuard System Manager 11.x > WatchGuard System Manager 11.x**.

*Replace 11.x in the program path with the current version of WSM you have installed.*

*WatchGuard System Manager appears.*

For information on how to use WatchGuard System Manager (WSM), see *About WatchGuard System Manager* on page 581.

## Connect to an XTM Device

1. Start WatchGuard System Manager.
2. Click .

Or, select **File > Connect to Device**.

Or, right-click anywhere on the WSM **Device Status** tab and select **Connect To > Device**.


*The Connect to Firebox dialog box appears.*



3. In the **Name / IP Address** drop-down list, type the name or IP address of your XTM device. On subsequent connections, you can select the XTM device name or IP address in the **Name / IP Address** drop-down list.
4. In the **Passphrase** text box, type the XTM device status (read-only) passphrase. You use the status passphrase to monitor traffic and XTM device conditions. You must type the configuration passphrase when you save a new configuration to the device.

5. (Optional) Change the value in the **Timeout** field. This value sets the time (in seconds) that the management computer listens for data from the XTM device before it sends a message that shows that it cannot get data from the device.  
If you have a slow network or Internet connection to the device, you can increase the timeout value. Decreasing the value decreases the time you must wait for a timeout message if you try to connect to a XTM device that is not available.
6. Click **Login**.  
*The XTM device appears in WatchGuard System Manager.*

## Disconnect from an XTM Device

1. Select the **Device Status** tab.
2. Select the device.
3. Click .  
Or, select **File > Disconnect**.  
Or, right-click and select **Disconnect**.

## Disconnect from all XTM Devices

If you are connected to more than one XTM device, you can disconnect from them all at the same time.

1. Select the **Device Status** tab.
2. Select **File > Disconnect All**.  
Or, right-click and select **Disconnect All**.

## Start WSM Applications

You can start these tools from WatchGuard System Manager.

### Policy Manager

You can use Policy Manager to install, configure, and customize network security policies for your XTM device.

For more information on Policy Manager, see *About Policy Manager* on page 364.

To start Policy Manager:

- Click .  
Or, select **Tools > Policy Manager**.

---

## Firebox System Manager

With Firebox System Manager, you can start many different security tools in one easy-to-use interface. You can also use Firebox System Manager to monitor real-time traffic through the firewall.

For more information on Firebox System Manager, see *About Firebox System Manager (FSM)* on page 745.

To start Firebox System Manager:

Click .

Or, select **Tools > Firebox System Manager**.

## HostWatch

HostWatch shows the connections through a XTM device from the trusted network to the external network, or from and to other interfaces or VLANs you choose. It shows the current connections, or it can show historical connections from a log file.

For more information on HostWatch, see *About HostWatch* on page 782.

To start HostWatch:

Click .

Or, select **Tools > HostWatch**.

## LogViewer

LogViewer shows a static view of a log file. You can use LogViewer to:

- Apply a filter by data type
- Search for words and fields
- Print and save to a file

For more information on LogViewer, see *Use LogViewer to See Log Files* on page 727.

To start LogViewer:

Click .

Or, select **Tools > Logs > LogViewer**.

## Report Manager

WatchGuard Reports are summaries of the data that you have selected to collect from the XTM device log files. You can use Report Manager to see the information in your WatchGuard Reports.

For more information on Report Manager, see *About WatchGuard Report Manager* on page 830.

To start Report Manager:

Click .

Or, select **Tools > Logs > Report Manager**.

## Quick Setup Wizard

You can use the Quick Setup Wizard to create a basic configuration for your XTM device. The XTM device uses this basic configuration file when it starts for the first time. This enables the device to operate as a basic firewall. You can use this same procedure any time you want to reset the XTM device to a new basic configuration for recovery or other reasons.

For more information on the Quick Setup Wizard, see *About the Quick Setup Wizard* on page 22.

To start the Quick Setup Wizard:

Click .

Or, select **Tools > Quick Setup Wizard**.

## CA Manager

In WatchGuard System Manager, the workstation that is configured as the Management Server also operates as a certificate authority (CA). The CA gives certificates to managed XTM device clients when they contact the Management Server to receive configuration updates.

Before you can use the Management Server as a CA, you must *Configure the Certificate Authority on the Management Server*.

To set up or change the parameters of the certificate authority:

Click .

Or, select **Tools > CA Manager**.

## Additional Installation Topics

### Install WSM and Keep an Older Version

You can install the current version of WSM (WatchGuard System Manager) and keep the old version as long as you do not install two versions of the WatchGuard server software (Management Server, Log Server, Report Server, Quarantine Server, and WebBlocker Server). Because you can have only one version of the servers installed, you must either remove the server software from the older version of WSM or install the new version of WSM without the server software. We recommend you remove the previous version of the server software before you install the current WSM version together with the current server software.

### Install WatchGuard Servers on Computers with Desktop Firewalls

Desktop firewalls can block the ports necessary for WatchGuard server components to operate. Before you install the Management Server, Log Server, Report Server, Quarantine Server, or WebBlocker Server on a computer with an active desktop firewall, you might need to open the necessary ports on the desktop firewall. Windows Firewall users do not need to change their configuration because the installation program opens the necessary ports in Windows Firewall automatically.

This table shows you the ports you must open on a desktop firewall.



Server Type/Appliance Software	Protocol/Port
Management Server	TCP 4109, TCP 4110, TCP 4112, TCP 4113
Log Server with Fireware appliance software	TCP 4115
Log Server with WFS appliance software	TCP 4107
WebBlocker Server	TCP 5003, UDP 5003
Quarantine Server	TCP 4119, TCP 4120
Report Server	TCP 4122
Log Server	TCP 4121

## Dynamic IP Support on the External Interface

If you use dynamic IP addresses, you must configure your XTM device in routed mode when you use the Quick Setup Wizard.

If you select DHCP, your XTM device connects to the DHCP server controlled by your Internet service provider (ISP) to get its IP address, gateway, and netmask. This server can also give DNS server information for your XTM device. If it does not give you that information, you must add it manually to your configuration. If necessary, you can change the IP addresses that your ISP gives you.

You also can use PPPoE. As with DHCP, the XTM device makes a PPPoE protocol connection to the PPPoE server of your ISP. This connection automatically configures your IP address, gateway, and netmask.

If you use PPPoE on the external interface, you must have the PPP user name and password when you configure your network. If your ISP gives you a domain name to use, type your user name in the format *user@domain* when you use the Quick Setup Wizard.

A static IP address is necessary for the XTM device to use some functions. When you configure the XTM device to receive dynamic IP addresses, the device cannot use these functions:

- FireCluster
- Drop-in mode
- 1-to-1 NAT on an external interface
- Mobile VPN with PPTP

**Note** *If your ISP uses a PPPoE connection to give a static IP address, the XTM device allows you to enable Mobile VPN with PPTP because the IP address is static.*

## About Connecting the XTM Device Cables

Use these guidelines when you connect cables to your XTM device.

- Connect the power cable to the XTM device power input and to a power source.
- Use a straight Ethernet cable (green) to connect your management computer to a hub or switch.
- Use a different straight Ethernet cable to connect your XTM device to the same hub or switch.

- Use a red crossover cable to connect the XTM device trusted interface to the management computer Ethernet port.

For XTM 5 Series devices, Interface 0 does not support Auto-MDIX, which automatically senses the cable polarity. Use these guidelines to decide which type of Ethernet cable to use with Interface 0:

- To connect Interface 0 to an interface on a switch or router that supports Auto-MDIX, you can use either Ethernet cable.
- To connect Interface 0 to an interface on an older switch or router that does not support Auto-MDIX, use the green Ethernet cable. Your switch or router might be set to a different polarity. If the green Ethernet cable does not work, try the red cross-over Ethernet cable.
- To connect Interface 0 to a PC, use the red cross-over Ethernet cable.

## Connect to an XTM Device with Firefox v3

Web browsers use certificates to ensure that the device on the other side of an HTTPS connection is the device you expect. Users see a warning when a certificate is self-signed, or when there is a mismatch between the requested IP address or host name and the IP address or host name in the certificate. By default, your XTM device uses a self-signed certificate that you can use to set up your network quickly. However, when users connect to the XTM device with a web browser, a *Secure Connection Failed* warning message appears.

To avoid this warning message, we recommend that you add a valid certificate signed by a CA (Certificate Authority) to your configuration. This CA certificate can also be used to improve the security of VPN authentication. For more information on the use of certificates with XTM devices, see *About Certificates* on page 853.

If you continue to use the default self-signed certificate, you can add an exception for the XTM device on each client computer. Current versions of most Web browsers provide a link in the warning message that the user can click to allow the connection. If your organization uses Mozilla Firefox v3, your users must add a permanent certificate exception before they can connect to the XTM device.

Actions that require an exception include:

- *About User Authentication*
- *Install and Connect the Mobile VPN with SSL Client*
- *Run the Web Setup Wizard*
- *About Edge (v10.x and Older) and SOHO Devices as Managed Devices*

Common URLs that require an exception include:

```
https://IP address or host name of an XTM device interface:8080
https://IP address or host name of an XTM device interface:4100
https://IP address or host name of an XTM device:4100/sslvpn.html
```

## Add a Certificate Exception to Mozilla Firefox v3

If you add an exception in Firefox v3 for the XTM device certificate, the warning message does not appear on subsequent connections. You must add a separate exception for each IP address, host name, and port used to connect to the XTM device. For example, an exception that uses a host name does not operate properly if you connect with an IP address. Similarly, an exception that specifies port 4100 does not apply to a connection where no port is specified.

**Note** *A certificate exception does not make your computer less secure. All network traffic between your computer and the XTM device remains securely encrypted with SSL.*

There are two methods to add an exception. You must be able to send traffic to the XTM device to add an exception.

- Click the link in the **Secure Connection Failed** warning message.
- Use the Firefox v3 Certificate Manager to add exceptions.

In the *Secure Connection Failed* warning message:

1. Click **Or you can add an exception**.
2. Click **Add Exception**.  
*The Add Security Exception dialog box appears.*
3. Click **Get Certificate**.
4. Select the **Permanently store this exception** check box.
5. Click **Confirm Security Exception**.

To add multiple exceptions:

1. In Firefox, select **Tools > Options**.  
*The Options dialog box appears.*
2. Select **Advanced**.
3. Click the **Encryption** tab, then click **View Certificates**.  
*The Certificate Manager dialog box opens.*
4. Click the **Servers** tab, then click **Add Exception**.
5. In the **Location** text box, type the URL to connect to the XTM device. The most common URLs are listed above.
6. When the certificate information appears in the **Certificate Status** area, click **Confirm Security Exception**.
7. Click **OK**.
8. To add more exceptions, repeat Steps 4–6.

## Disable the HTTP Proxy in the Browser

Many web browsers are configured to use an HTTP proxy server to increase the download speed of web pages. To manage or configure the XTM device with the Web UI, your browser must connect directly to the device. If you use an HTTP proxy server, you must temporarily disable the HTTP proxy setting in your browser. You can enable the HTTP proxy server setting in your browser again after you set up the XTM device.

Use these instructions to disable the HTTP proxy in Firefox, Safari, or Internet Explorer. For other browsers, use the browser Help system to find the necessary information. Many browsers automatically disable the HTTP proxy feature.

## Disable the HTTP proxy in Internet Explorer 6.x, 7.x, or 8.x

1. Open Internet Explorer.
2. Select **Tools > Internet Options**.  
*The Internet Options dialog box appears.*
3. Select the **Connections** tab.
4. Click **LAN Settings**.  
*The Local Area Network (LAN) Settings dialog box appears.*
5. Clear the **Use a proxy server for your LAN** check box.
6. Click **OK** to close the **Local Area Network (LAN) Settings** dialog box.
7. Click **OK** to close the **Internet Options** dialog box.

## Disable the HTTP proxy in Firefox 2.x or 3.x

1. Open Firefox.
2. Select **Tools > Options**.  
*The Options dialog box appears.*
3. Click **Advanced**.
4. Select the **Network** tab.
5. Click **Settings**.
6. Click **Connection Settings**.  
*The Connection Settings dialog box appears.*
7. For Firefox 2.x, make sure the **Direct Connection to the Internet** option is selected.  
For Firefox 3.x, make sure the **No proxy** option is selected.
8. Click **OK** to close the **Connection Settings** dialog box.
9. Click **OK** to close the **Options** dialog box.

## Disable the HTTP proxy in Safari 2.0

1. Open Safari.
2. Select **Preferences**.  
*The Safari preferences dialog box appears.*
3. Click **Advanced**.
4. Click **Change Settings**.  
*The System Preference dialog box appears.*
5. Clear the **Web Proxy (HTTP)** check box.
6. Click **Apply Now**.

## Find Your TCP/IP Properties

To learn about the properties of your network, look at the TCP/IP properties of your computer or any other computer on the network. You must have this information to install your XTM device:

- IP address
- Subnet mask

- Default gateway
- Whether your computer has a static or dynamic IP address

**Note** *If your ISP assigns your computer an IP address that starts with 10, 192.168, or 172.16 to 172.31, then your ISP uses NAT (Network Address Translation) and your IP address is private. We recommend that you get a public IP address for your XTM device external IP address. If you use a private IP address, you can have problems with some features, such as virtual private networking.*

To find the TCP/IP properties for your computer operating system, use the instructions in the subsequent sections .

## Find Your TCP/IP Properties on Microsoft Windows Vista

1. Select **Start > Programs > Accessories > Command Prompt**.  
*The Command Prompt dialog box appears.*
2. At the command prompt, type `ipconfig /all` and press **Enter**.
3. Write down the values that you see for the primary network adapter.

## Find Your TCP/IP Properties on Microsoft Windows 2000, Windows 2003, and Windows XP

1. Select **Start > All Programs > Accessories > Command Prompt**.  
*The Command Prompt dialog box appears.*
2. At the command prompt, type `ipconfig /all` and press **Enter**.
3. Write down the values that you see for the primary network adapter.

## Find Your TCP/IP Properties on Microsoft Windows NT

1. Select **Start > Programs > Command Prompt**.  
*The Command Prompt dialog box appears.*
2. At the command prompt, type `ipconfig /all` and press **Enter**.
3. Write down the values that you see for the primary network adapter.

## Find Your TCP/IP Properties on Macintosh OS 9

1. Select the **Apple menu > Control Panels > TCP/IP**.  
*The TCP/IP dialog box appears.*
2. Write down the values that you see for the primary network adapter.

## Find Your TCP/IP Properties on Macintosh OS X 10.5

1. Select the **Apple menu > System Preferences**, or select the icon from the Dock.  
*The System Preferences dialog box appears.*
2. Click the **Network** icon.  
*The Network preference pane appears.*
3. Select the network adapter you use to connect to the Internet.
4. Write down the values that you see for the network adapter.

## Find Your TCP/IP Properties on Other Operating Systems (Unix, Linux)

1. Read your operating system guide to find the TCP/IP settings.
2. Write down the values that you see for the primary network adapter.

# 5 Configuration and Management Basics

---

## About Basic Configuration and Management Tasks

After your XTM device is installed on your network and is set up with a basic configuration file, you can start to add custom configuration settings. The topics in this section help you complete these basic management and maintenance tasks.

## About Configuration Files

A *configuration file* includes all configuration data, options, IP addresses, and other information that makes up the security policy for your XTM device. Configuration files have the extension .xml.

Policy Manager is a WatchGuard software tool that lets you make, change, and save configuration files. You can use Policy Manager to easily examine and change your configuration file.



When you use Policy Manager, you can:

- *Open a Configuration File* , either open the configuration file currently in use on the XTM device, or a local configuration file (a configuration file saved on your hard drive)
- *Make a New Configuration File*
- *Save the Configuration File*
- Make changes to existing configuration files

## Open a Configuration File

Network administrators often need to make changes to their network security policies. Perhaps, for example, your company purchased a new software application, and you must open a port and protocol to a server at a vendor location. Your company might have also purchased a new feature for your XTM device or hired a new employee who needs access to network resources. For all of these tasks, and many more, you must open your configuration file, use Policy Manager to modify it, and then save the configuration file.

## Open the Configuration File with WatchGuard System Manager


1. On your Windows desktop, select **Start > All Programs > WatchGuard System Manager 11.x > WatchGuard System Manager 11.x**.  
*WatchGuard System Manager 11.x is the default name of the folder for the Start menu icons. You cannot change this folder name when you run the installer, but you can change it through the Windows user interface.*
2. Click .  
Or, select **File > Connect To Device**.  
*The Connect to Firebox dialog box appears.*
3. From the **Name / IP Address** drop-down list, type or select the IP address for the trusted interface of your XTM device.
4. Type the status (read-only) passphrase. Click **OK**.  
*The device appears in the WatchGuard System Manager Device Status tab.*
5. On the **Device Status** tab, select the XTM device. Click .  
Or, select **Tools > Policy Manager**.  
Policy Manager opens with the configuration file that is in use on the selected device. The changes you make to the configuration do not take effect until you save the configuration to the XTM device.



## Open a Local Configuration File

You can open configuration files that are saved on any local drive or any network drive to which your management computer can connect.

If you want to use an existing configuration file for a XTM device in a factory-default state, we recommend that you first run the Quick Setup Wizard to create a basic configuration and then open the existing configuration file.

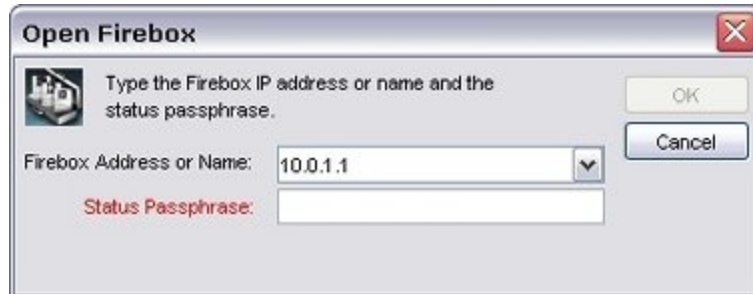
1. In WatchGuard System Manager, click .  
Or, select **Tools > Policy Manager**.  
*The Policy Manager dialog box appears.*
2. Select **Open configuration file** and click **Browse**.
3. Select the configuration file.
4. Click **Open**.  
*The configuration file appears in Policy Manager.*



## Open a Configuration File with Policy Manager

1. Select **File > Open > Firebox**.

The *Open Firebox* dialog box appears.



2. From the **Firebox Address or Name** drop-down list, select an XTM device.  
You can also type the IP address or host name.
3. In the **Status Passphrase** text box, type the status (read-only) passphrase.  
You must use the configuration passphrase to save the configuration to the XTM device.
4. Click **OK**.


The *configuration file appears in Policy Manager*.

If you cannot connect to the XTM device, try these steps:

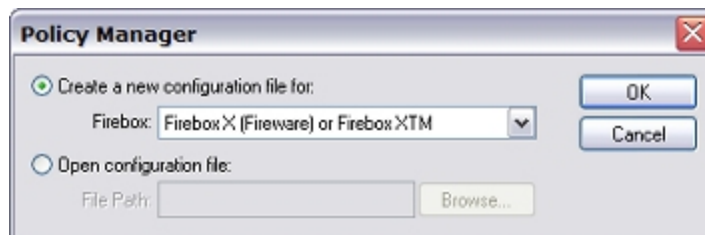
- If the **Connect to Firebox** or **Open Firebox** dialog box immediately appears after you type the passphrase, make sure that Caps Lock is off and that you typed the passphrase correctly. The passphrase is case-sensitive.
- If the **Connect to Firebox** or **Open Firebox** dialog box times out, make sure that you have a link on the trusted interface and on your computer. Make sure that you typed the correct IP address for the trusted interface of the XTM device. Also make sure that your computer IP address is in the same network as the trusted interface of the XTM device.

## Make a New Configuration File

The Quick Setup Wizard makes a basic configuration file for your XTM device. We recommend that you use this as the base for each of your configuration files. You can also use Policy Manager to make a new configuration file with only the default configuration properties.

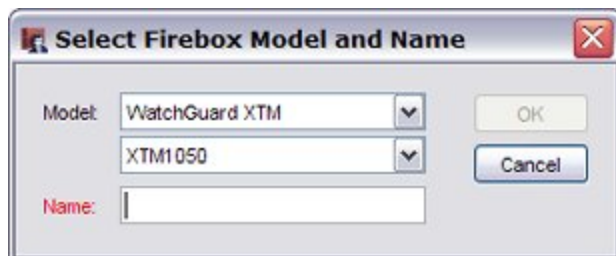
1. In WatchGuard System Manager, before you connect to a device, click .  
Or, select **Tools > Policy Manager**.

The *Policy Manager* dialog box appears.



2. Select **Create a new configuration file for**.
3. From the **Firebox** drop-down list, select the type of XTM device for which you want to make a new configuration file.
4. Click **OK**.

*The Select Firebox Model and Name dialog box appears.*



5. In the **Model** drop-down lists, select your XTM device model. Because some groups of features are unique to specific models, select the same model as your hardware device.
6. In the **Name** text box, type the name for the device configuration file. This name is also used to identify the device if it is managed by a WatchGuard Management Server, and for logging and reporting.
7. Click **OK**.

Policy Manager makes a new configuration with the file name <name>.xml, where <name> is the name you gave the device.

## Save the Configuration File

If you make a new configuration file or change the current configuration file and want your changes to take effect on the XTM device, you must save the configuration file directly to the XTM device.

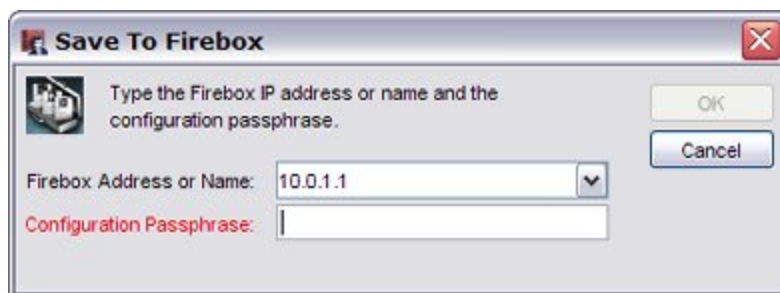
You can also save the current configuration file to any local drive or any network drive to which your management computer can connect. If you plan to make one or more major changes to your configuration file, we recommend that you save a copy of the old configuration file first. If you have problems with your new configuration, you can restore the old version.

## Save a Configuration Directly to the Device

You can use Policy Manager to save your configuration file directly to the XTM device.

1. Select **File > Save > To Firebox**.

*The Save to Firebox dialog box appears.*



2. In the **Firebox Address or Name** drop-down list, select or type an IP address or name. If you use a name, the name must resolve through DNS.  
When you type an IP address, type all the numbers and the periods. Do not use the TAB key or arrow key.
3. Type the **Configuration Passphrase**. You must use the configuration passphrase to save the configuration to the XTM device.
4. Click **OK**.

## Save a Configuration to a Local or Network Drive

You can use Policy Manager to save your configuration file to a local or network drive.

1. Select **File > Save > As File**.  
*You can also use CTRL-S. A standard Windows save file dialog box appears.*
2. Type the name of the file.

The default location is the My Documents\My WatchGuard\configs directory. You can also save the file in any folder you can connect to from the management computer. For better security, we recommend that you save the files in a safe folder that no other users can get access to.

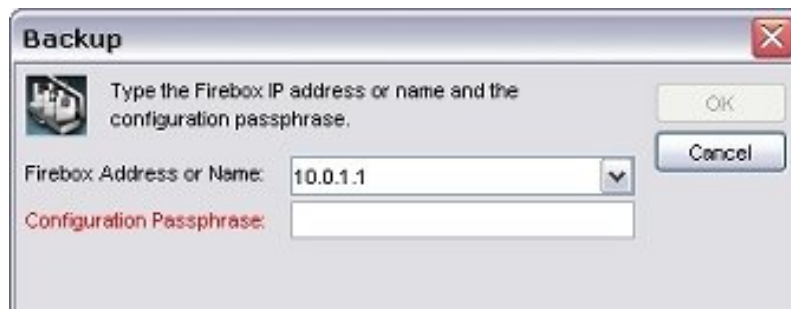
3. Click **Save**.  
*The configuration file is saved to the directory you specify.*

## Make a Backup of the XTM Device Image

An XTM device backup image is an encrypted and saved copy of the flash disk image from the XTM device flash disk. It includes the XTM device OS, configuration file, licenses, and certificates. You can save a backup image to your management computer or to a directory on your network.

We recommend that you regularly make backup files of the XTM device image. We also recommend that you create a backup image of the XTM device before you make significant changes to your configuration file, or before you upgrade your XTM device or its OS. You can use Policy Manager to make a backup of your device image.

1. Select **File > Backup**.  
*The Backup dialog box appears.*



2. Type the **Configuration Passphrase** for your XTM device.  
*The second part of the Backup dialog box appears.*

3. Type and confirm an encryption key. This key is used to encrypt the backup file. If you lose or forget this encryption key, you cannot restore the backup file.
4. Click **Browse** to select the directory in which to save the backup file.

The default location for a backup file with an “.fxi” extension is:

```
C:\Documents and Settings\All Users\Shared WatchGuard\backups\  
<XTM device IP address>-<date>.<wsm_version>.fxi
```

5. Click **OK**.

## Restore an XTM Device Backup Image

You can use Policy Manager to restore a previously created backup image to your XTM device. If your device is centrally managed, you must open Policy Manager for your device from your Management Server to restore a backup image to your device.

For more information about how to update the configuration of a Fully Managed device, see *Update the Configuration For a Fully Managed Device* on page 608.

1. Select **File > Restore**.  
*The Restore dialog box appears.*
2. Type the configuration passphrase for your XTM device. Click **OK**.
3. Type the encryption key you used when you created the backup image.  
*The XTM device restores the backup image. It restarts and uses the backup image.*

Make sure you wait two minutes before you connect to the XTM device again.

The default location for a backup file with an “.fxi” extension is:

```
C:\Documents and Settings\All Users\Shared WatchGuard\backups\  
<XTM device IP address>-<date>.<wsm_version>.fxi
```

If you cannot successfully restore your XTM device image, you can reset the XTM device. Depending on the XTM device model you have, you can reset a XTM device to its factory-default settings or rerun the Quick Setup Wizard to create a new configuration.

For more information, see *Reset an XTM Device to a Previous or New Configuration* on page 55.

## Use a USB Drive for System Backup and Restore

A WatchGuard XTM device backup image is a copy of the flash disk image from the XTM device that is encrypted and saved. The backup image file includes the XTM device OS, configuration file, feature key, and certificates.

For XTM 2 Series, 5 Series, 8 Series, or XTM 1050 devices, you can attach a USB drive or storage device to the USB port on the XTM device for system backup and restore procedures. When you save a system backup image to a connected USB drive, you can restore your XTM device to a known state more quickly.

### About the USB Drive

The USB drive must be formatted with the FAT or FAT32 file system. If the USB drive has more than one partition, Fireware XTM only uses the first partition. Each system backup image can be as large as 30 MB. We recommend you use a USB drive large enough to store several backup images.

## Save a Backup Image to a Connected USB Drive

For this procedure, a USB drive must be connected to your XTM device.

1. Start *Firebox System Manager*.
2. Select **Tools > USB Drive**.

The *Backup/Restore to USB drive dialog box* appears.

New backup image

Filename: 2010-04-27.v11.3.fxi

Encryption key:

Confirm encryption key:

Save to USB Drive

3. In the **New backup image** section, type a **Filename** for the backup image. Or you use the default filename provided.
4. Type and confirm an **Encryption key**. This key is used to encrypt the backup file. If you lose or forget this encryption key, you cannot restore the backup file.
5. Click **Save to USB Drive**.

The saved image appears on the list of **Available device backup images** after the save is complete.

## Restore a Backup Image from a Connected USB Drive

For this procedure, a USB drive must be connected to your XTM device.

1. Start *Firebox System Manager*.
2. Select **Tools > USB Drive**.

The *Backup/Restore to USB drive dialog box* appears.

USB Drive: USB DRIVE (596,432K of 1,007,328K available) Refresh

Available backup images

Image	Saved
2010-04-27.v11.3.fxi	4/27/10 6:06 PM

Restore Selected Image Use Selected Image for Auto-Restore

3. From the **Available backup images** list, select a backup image file to restore.
4. Click **Restore Selected Image**.
5. Type the **Encryption key** you used when you created the backup image.
6. Type the configuration passphrase for your XTM device. Click **OK**.
7. Click **Restore**.

*The XTM device restores the backup image. It restarts and uses the backup image.*

## Automatically Restore a Backup Image from a USB Drive

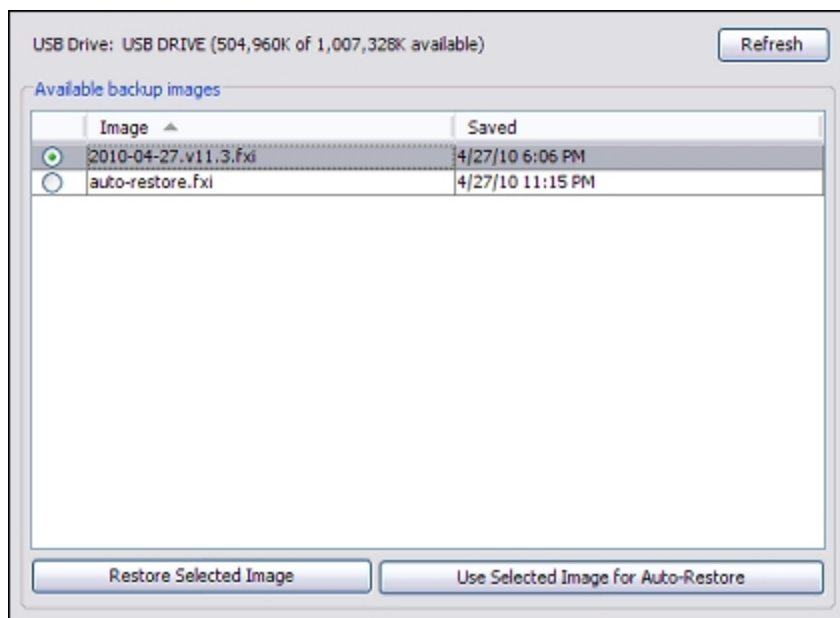
If a USB drive (storage device) is connected to a WatchGuard XTM device in recovery mode, the device can automatically restore the previously backed up image from the USB drive. To use the auto-restore feature, you must first select a backup image on the USB drive as the one you want to use for the restore process. You must use Fireware XTM Web UI, Firebox System Manager, or Fireware XTM command line interface to select this backup image.

You can use the same backup image for more than one device in the same WatchGuard XTM model family. For example, you can use a backup image saved from an XTM 530 as the backup image for any other XTM 5 Series device.

## Select the Backup Image to Auto-restore

1. Start *Firebox System Manager*.
2. Select **Tools > USB Drive**.

*The Backup/Restore to USB Drive dialog box appears.*



3. From the **Available backup images** list, select a backup image file.
4. Click **Use Selected Image for Auto-Restore**.
5. Type the **Encryption Key** used to create the backup image. Click **OK**.

6. Type the configuration passphrase for your XTM device. Click **OK**.

*The XTM device saves a copy of the selected backup image as the auto-restore image **auto-restore.fxi**. This image is saved in the auto-restore directory on the USB drive, and is encrypted with a random encryption key that can only be used by the automatic restore process.*

If you had a previous auto-restore image saved, the auto-restore.fxi file is replaced with a copy of the backup image you selected.

**Warning** *If your XTM device has used a version of the Fireware XTM OS before v11.3, you must update the recovery mode software image on the device to v11.3 for the auto-restore feature to operate. See the Fireware XTM 11.3 Release Notes for upgrade instructions.*

## Restore the Backup Image for an XTM 5 Series, 8 Series, or XTM 1050 Device

1. Connect the USB drive with the auto-restore image to a USB port on the XTM device.
2. Power off the XTM device.
3. Press the up arrow on the device front panel while you power on the device.
4. Keep the button depressed until Recovery Mode starting appears on the LCD display.  
*The device restores the backup image from the USB drive, and automatically uses the restored image after it reboots.*

If the USB drive does not contain a valid auto-restore image for this XTM device model family, the device does not reboot and is instead started in recovery mode. If you restart the device again, it uses your current configuration. When the device is in recovery mode, you can use the WSM Quick Setup Wizard to create a new basic configuration.

For information about the WSM Quick Setup Wizard, see *Run the WSM Quick Setup Wizard* on page 26.

## Restore the Backup Image for an XTM 2 Series Device

1. Attach the USB drive with the auto-restore image to a USB port on the XTM 2 Series device.
2. Disconnect the power supply.
3. Press and hold the **Reset** button on the back of the device.
4. Connect the power supply while you continue to hold down the **Reset** button.
5. After 10 seconds, release the **Reset** button.  
*The device restores the backup image from the USB drive, and automatically uses the restored image after it reboots.*

If the USB drive does not contain a valid 2 Series auto-restore image, the auto-restore fails and the device does not reboot. If the auto-restore process is not successful, you must disconnect and reconnect the power supply to start the 2 Series device with factory-default settings.

For information about factory default settings, see *About Factory-Default Settings*.

## USB Drive Directory Structure

The USB drive contains directories for backup images, configuration files, feature key, certificates and diagnostics information for your XTM device.

When you save a backup image to a USB drive, the file is saved in a directory on the USB drive with the same name as the serial number of your XTM device. This means that you can store backup images for more than one XTM device on the same USB drive. When you restore a backup image, the software automatically retrieves the list of backup images stored in the directory associated with that device.

For each device, the directory structure on the USB device is as follows, where `sn` is replaced by the serial number of the XTM device:

```
\sn\flash-images\  
\sn\configs\  
\sn\feature-keys\  
\sn\certs\  

```

The backup images for a device is saved in the `\sn\flash-images` directory. The backup image file saved in the flash-images directory contains the Fireware XTM OS, the device configuration, feature keys, and certificates. The `\configs`, `\feature-keys` and `\certs` subdirectories are not used for any USB drive backup and restore operations. You can use these to store additional feature keys, configuration files, and certificates for each device.

There is also one directory at the root level of the directory structure which is used to store the designated auto-restore backup image.

```
\auto-restore\  

```

When you designate a backup image to use for automatic restore, a copy of the selected backup image file is encrypted and stored in the `\auto-restore` directory with the file name `auto-restore.fx1`. You can have only one auto-restore image saved on each USB drive. You can use the same auto-restore backup image for more than one device, if both devices are the same WatchGuard XTM model family. For example, you can use an auto-restore image saved from an XTM 530 as the auto-restore image for any other XTM 5 Series device.

You must use the Firebox System Manager **Tools > USB Drive** command to create an auto-restore image. If you manually copy and rename a backup image and store it in this directory, the automatic restore process does not operate correctly.

There is also another directory at the root level of the directory structure which is used to store the support snapshot that can be used by WatchGuard technical support to help diagnose issues with your XTM device.

```
\wgdiag\  

```

For more information about the support snapshot, see *Use a USB Drive to Save a Support Snapshot*.



## Save a Backup Image to a USB Drive Connected to Your Management Computer

You can use Policy Manager to save a backup image to a USB drive or storage device connected to your management computer. If you save the configuration files for multiple devices to the same USB drive, you can attach the USB drive to any of those XTM devices for recovery.

If you use the Firebox System Manager **Tools > USB Drive** command to do this, the files are automatically saved in the proper directory on the USB drive. If you use the Policy Manager **File > Backup** command, or if you use Windows or another operating system to manually copy configuration files to the USB device, you must manually create the correct serial number and flash-image directories for each device (if they do not already exist).

### Before You Begin

Before you begin, it is important that you understand the *USB Drive Directory Structure* used by the USB backup and restore feature. If you do not save the backup image in the correct location, the device cannot find it when you attach the USB drive to the device.

### Save the Backup Image

To save a backup image to a USB drive connected to your management computer, follow the steps in *Make a Backup of the XTM Device Image*. When you select the location to save the file, select the drive letter of the USB drive attached to your computer. If you want the backup image you save to be recognized by the XTM device when you attach the USB drive, make sure to save the backup in the `\flash-images` folder, in the directory that is named with the serial number of your XTM device.

For example, if your XTM device serial number is 70A10003C0A3D, save the backup image file to this location on the USB drive:

```
\70A10003C0A3D\flash-images\
```

### Designate a Backup Image for Auto-restore

To designate a backup image for use with the auto-restore feature, you must connect the USB drive to the device and designate the backup image to use for auto-restore, as described in *Use a USB Drive for System Backup and Restore*. If you manually save a backup image to the auto-restore directory, the automatic restore process does not operate correctly.

### Use a USB Drive to Save a Support Snapshot

A support snapshot is a file that contains a snapshot of your device configuration and other information that can help WatchGuard technical support troubleshoot issues with your device. If a USB drive is connected to one of the USB interfaces, the XTM device automatically generates a new support snapshot and saves the snapshot to the USB drive as an encrypted file, with the read-only passphrase for the device as the encryption key. This happens automatically when the device is powered on and a USB drive is connected to the device. Any time you connect a USB drive, the XTM device automatically saves a current support snapshot in the `\wgdiag` directory on the USB drive.

When the XTM device detects a connected USB drive, it automatically completes these actions:

- If the `\wgdiag` directory does not exist on the USB drive, the XTM device creates it.
- If the `\wgdiag` directory already exists on the USB drive, the XTM device deletes and recreates it.
- The XTM device saves the new support snapshot in the `\wgdiag` directory with the filename `support1.tgz`.

Each time you connect the USB drive or restart the XTM device, any files in the `\wgdiag` directory are removed and a new support snapshot is saved.

**Note** *If you want to keep a support snapshot, either rename the `\wgdiag` directory on the USB drive or copy the `support1.tgz` file from the USB drive to your computer before you reconnect the USB drive to the XTM device.*

Status messages about USB diagnostics file generation appear as *Info* level messages in the log file. These log messages contain the text *USB Diagnostic*. For XTM 5 Series, 8 Series, and XTM 1050 models, messages also appear on the LCD screen when the USB diagnostic file is being written, and when a USB drive is connected or removed.

By default, the XTM device saves only a single support snapshot per USB drive when the USB drive is first detected. You can use the `usb diagnostic` command in the command line interface to enable the XTM device to automatically save multiple support snapshots to the USB drive periodically while the device is in operation. If the XTM device is configured to save multiple support snapshots, the number at the end of the file name is incrementally increased each time a new snapshot is saved, so that you can see a sequence of support snapshots. The file names for the first two support snapshots would be `support1.tgz` and `support2.tgz`. If enabled, the USB diagnostics stores a maximum of 48 support snapshots on the USB drive. For more information about how to use the `usb diagnostic` command, see the *Fireware XTM Command Line Interface Reference*.

## Use an Existing Configuration for a New XTM Device Model

When you replace your Firebox or XTM device with a different XTM device model, you can continue to use the same configuration file. When you import a new feature key to your existing configuration file, Policy Manager automatically updates the existing configuration file so that it operates correctly with the new XTM device model specified in the feature key.

To move a configuration file from one Firebox X e-Series or XTM device to another device model, you must complete these steps in Policy Manager:

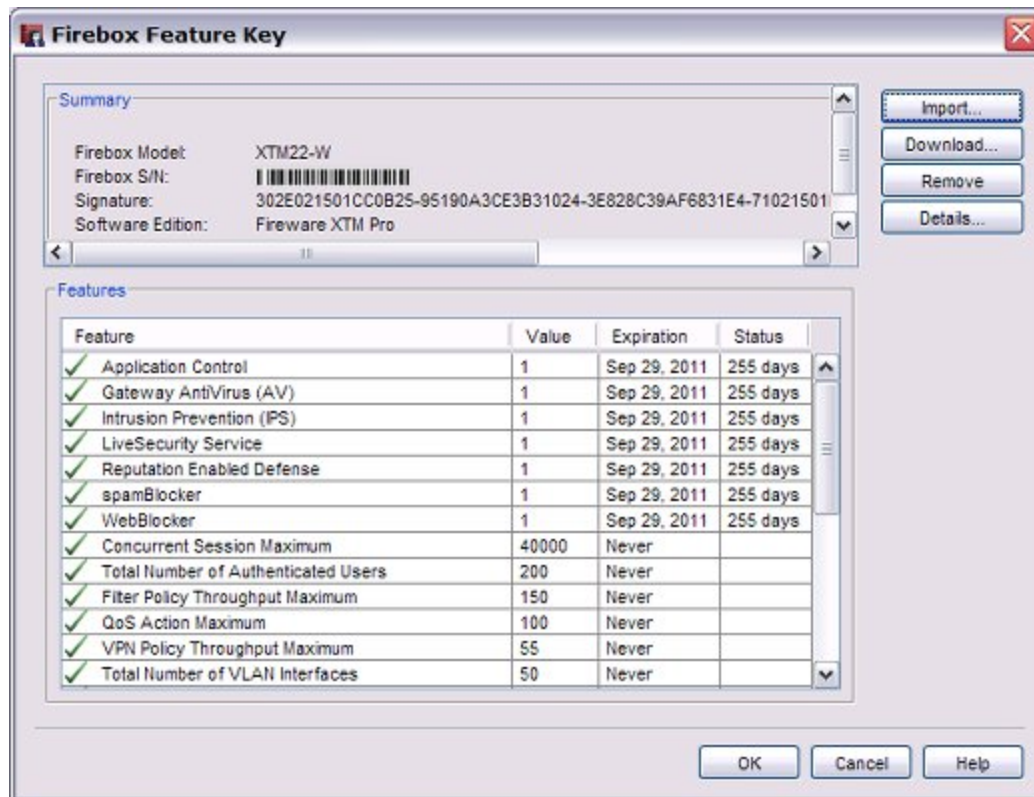
- Remove feature key for the old model from the configuration file.
- Add the feature key for the new model to the configuration file.
- Review the network interface configuration, and update it if necessary.
- Save the configuration to the new XTM device.

**Note** *If your old device is a Firebox X Core or Firebox X Peak device that is not an e-Series model, the upgrade steps are different. For more information, see *Upgrade a Non-e-Series Configuration File For Use With an e-Series or XTM Device*.*

To update your configuration file:

1. If you have not already done so, *Get a Feature Key from LiveSecurity* for your new XTM device.
2. For your existing Firebox or XTM device configuration, *Open Policy Manager*.
3. Select **Setup > Feature Keys**.

*The Firebox Feature Key dialog box appears.*



4. Click **Remove** to remove the current feature key.
5. Click **Import**.

*The Import Firebox Feature Key dialog box appears.*



6. When you got a feature key for your new XTM device, you copied the full feature key to a text file and saved it on your computer. Open this file and paste the contents of the feature key file for the new XTM device into the **Import Firebox Feature Key** dialog box.
7. Click **OK**.  
*The model information and features from the new feature key appears in the Firebox Feature Key dialog box.*
8. Click **OK**.

If your new XTM device model has a different number of interfaces than the old device model, Policy Manager displays a message that advises you to verify the configuration of the network interfaces.

9. Select **Network > Configuration** to review the network interface configuration.
10. Select **File > Save > To Firebox** to save the configuration to the new XTM device.

## Upgrade a Non-e-Series Configuration File For Use With an e-Series or XTM Device

You cannot use Fireware XTM v11.x with Firebox X Core and Firebox X Peak devices that are not e-Series models. WatchGuard System Manager v11.4 provides an upgrade path for you to move an existing configuration to a new e-Series or XTM device that is supported by Fireware XTM v11.x. This procedure applies only to these Firebox X Core or Firebox X Peak devices (not e-Series):

- Firebox X Core models — X500, X700, X1000, X2500
- Firebox X Peak models — X5000, X6000, X8000

**Note** *The procedure to move a configuration file from a Firebox X e-Series device to an XTM device model is different. For more information, see [Use an Existing Configuration for a New XTM Device Model](#).*

## Before You Begin

Before you can use an upgraded configuration file from a Firebox X Core or Peak device that is not an e-series device on your new XTM device, you must set up your new XTM device with a basic configuration file. You can then follow the subsequent procedure to convert your existing configuration file to v11.4 and save it to your new XTM device.

## Upgrade the Configuration File

To upgrade an existing v10.x configuration file from a device that is not an e-Series device for use with a new e-Series or XTM device:

1. Start Policy Manager v10.x for the v10.x device that is not an e-Series device.
2. Select **File > Save > As File**.
3. In WatchGuard System Manager v11.4, start Policy Manager, and select **Open configuration file**.
4. Open the v10.x configuration file you saved in Step 2.  
*The Upgrade Available dialog box appears. If your management computer has both v10.x and v11.x WatchGuard System Manager installed, you have a choice about whether to upgrade or to use the older version of Policy Manager.*

5. Select **Upgrade device to v11.x**. Click **OK**.

*A confirmation dialog box appears.*

6. Click **OK** to confirm that you want to update the configuration file.

*The Import Firebox Feature Key dialog box appears.*

7. If you have the feature key file for the new XTM device, select **Feature key**.  
Click **Browse** to find the feature key file.  
Or, copy the text of the feature key file and click **Paste** to insert it in the text box.

If you do not have the feature key for the new XTM device, select **Device model**.

From the **Model** drop-down lists, select the model name and number of the new XTM device.

8. Click **Upgrade Configuration File**.

*A message appears when the configuration file has been updated.*

9. Click **OK** to dismiss the success message.

*The converted configuration appears in Policy Manager.*

If your new XTM device model has a different number of interfaces than the old device model, you must review the configuration of the network interfaces after the configuration upgrade.

10. To review the network interface configuration, select **Network > Configuration**.
11. If you did not add the feature key during the upgrade, select **Setup > Feature Keys** to add the feature key for the new device.  
For more information, see *Add a Feature Key to Your XTM Device*.
12. To save the upgraded configuration file to the new XTM device, select **File > Save > To Firebox**.

If the new XTM device use Fireware XTM OS v11.4, Policy Manager must complete one more step to upgrade the configuration to v11.4. An upgrade message appears.

13. To complete the upgrade of the configuration file to v11.4, click **Yes**.

## Configure a Replacement XTM Device

If your XTM device hardware fails during the warranty period, WatchGuard may replace it with an RMA ([Return Merchandise Agreement](#)) unit of the same model. When you exchange an XTM device for an RMA replacement, WatchGuard Customer Care transfers the licenses from the original XTM device serial number to the new XTM device serial number. All the features that were licensed to the original XTM device are transferred to the replacement XTM device.

To set up your new XTM device to use the configuration from your original XTM device, follow the steps in the subsequent sections.

### Save the Configuration from the Original XTM Device to a File

For this procedure, you must have a saved configuration file from your original XTM device. The configuration file is saved by default to the My Documents\My WatchGuard\configs directory.

For instructions to save the configuration to a local file, see *Save the Configuration File* on page 42.

### Get the Feature Key for the Replacement XTM Device

Because your replacement XTM device has a different serial number, you must get a new feature key for it from the Support section of the WatchGuard web site. The replacement XTM device is listed in your activated products list with the same Product Name as the original XTM device, but with the serial number of the replacement XTM device. For instructions to get the feature key, see *Get a Feature Key from LiveSecurity* on page 59.

### Use the Quick Setup Wizard to Configure Basic Settings

Just as with any new XTM device, you must use the Quick Setup Wizard to create a basic configuration for the replacement XTM device. The Quick Setup Wizard runs either from the web or as a Windows application.

For information about how to run the wizard from the web, see *Run the Web Setup Wizard* on page 23.

For information about how to run the wizard as a Windows application, see *Run the WSM Quick Setup Wizard* on page 26.

### Update the Feature Key in the Original Configuration File and Save to the New Device

1. In WatchGuard System Manager, select **Tools > Policy Manager**.
2. Select **Open configuration file**.
3. Click **Browse** and select the saved configuration file from the original XTM device.
4. Click **Open**. Click **OK**.
5. Open Policy Manager for the new device.
6. Select **Setup > Feature Keys**.
7. Click **Remove** and remove the original feature key.
8. Click **Import** and import the new feature key.

9. Click **Browse** and select the replacement feature key file you downloaded from the LiveSecurity site.  
Or, click **Paste** and paste the contents of the feature key for the replacement unit.
10. Click **OK** twice to close the **Firebox Feature Key** dialog boxes.
11. Select **File > Save > To Firebox** and save the configuration to the replacement XTM device.

Configuration of the replacement XTM device is now complete. The replacement XTM device now uses all the policies and configuration settings from the original XTM device.

## Reset an XTM Device to a Previous or New Configuration

If your XTM device has a severe configuration problem, you can reset the device to its factory-default settings. For example, if you do not know the configuration passphrase or if a power interruption causes damage to the Fireware XTM OS, you can use the Quick Setup Wizard to build your configuration again or restore a saved configuration.

For a description of the factory-default settings, see *About Factory-Default Settings* on page 56.

**Note** You can also use safe mode to automatically restore a system backup image from a USB storage device. For more information, see *Automatically Restore a Backup Image from a USB Drive*.

### Start an XTM Device in Safe Mode

To restore the factory-default settings for a WatchGuard XTM 5 Series, 8 Series, or 10 Series device, you must start the XTM device in safe mode.

1. Power off the XTM device.
2. Press the down arrow on the device front panel while you power on the XTM device.
3. Keep the down arrow button depressed until the message **Safe Mode Starting** appears on the LCD display:

When the device is started in safe mode, the display shows the model number followed by the word "safe".

When you start a device in safe mode:

- The device temporarily uses the factory-default network and security settings.
- The current feature key is not removed. If you run the Quick Setup Wizard to create a new configuration, the wizard uses the feature key you previously imported.
- Your current configuration is deleted only when you save a new configuration. If you restart the XTM device before you save a new configuration, the device uses your current configuration again.

### Reset an XTM 2 Series Device to Factory-Default Settings

When you reset an XTM 2 Series device, the original configuration settings are replaced by the factory-default settings. To reset the device to factory-default settings:

1. Disconnect the power supply.
2. Press and hold the **Reset** button on the back of the device.
3. While you continue to hold down the **Reset** button, connect the power supply.
4. Continue to hold down the **Reset** button until the yellow **Attn** indicator stays lit. This shows that the device successfully restored the factory-default settings.

*For a 2 Series device, this process can take 75 seconds or more.*

5. Release the **Reset** button.

**Note** *You must start the device again before you can connect to it. If you do not restart, when you try to connect to the device, a web page appears with this message: Your device is running from a backup copy of firmware. You can also see this message if the **Reset** button is stuck in the depressed position. If you continue to see this message, check the **Reset** button and restart the device.*

6. Disconnect the power supply.
7. Connect the power supply again.

*The Power Indicator lights and your device is reset.*

## Run the Quick Setup Wizard

After you restore the factory-default settings, you can use the Quick Setup Wizard to create a basic configuration or restore a saved backup image.

For more information, see *About the Quick Setup Wizard* on page 22.

## About Factory-Default Settings

The term *factory-default settings* refers to the configuration on the XTM device when you first receive it before you make any changes. You can also reset the XTM device to factory-default settings as described in *Reset an XTM Device to a Previous or New Configuration* on page 55.

The default network and configuration properties for the XTM device are:

### *Trusted network*

The default IP address for the trusted network is 10.0.1.1. The subnet mask for the trusted network is 255.255.255.0.

The default IP address and port for the Firewall XTM Web UI is `https://10.0.1.1:8080`.

The XTM device is configured to give IP addresses to computers on the trusted network through DHCP. By default, these IP addresses can be from 10.0.1.2 to 10.0.1.254.

### *External network*

The XTM device is configured to get an IP address with DHCP.

### *Optional network*

The optional network is disabled.



#### *Administrator (read/write) account credentials*

Username: admin

Passphrase: readwrite

#### *Status (read-only) account credentials*

Username: status

Passphrase: readonly

#### *Firewall settings*

All incoming traffic is denied. The outgoing policy allows all outgoing traffic. Ping requests received from the external network are denied.

#### *System Security*

The XTM device has the built-in administrator accounts *admin* (read-write access) and *status* (read-only access). When you first configure the device with the Quick Setup Wizard, you set the status and configuration passphrases. After you complete the Quick Setup Wizard, you can log in to Fireware XTM Web UI with either the admin or status administrator accounts. For full administrator access, log in with the *admin* user name and type the configuration passphrase. For read-only access, log in with the *status* user name and type the read-only passphrase.

By default, the XTM device is set up for local management from the trusted network only. Additional configuration changes must be made to allow administration from the external network.

#### *Upgrade Options*

To enable upgrade options such as WebBlocker, spamBlocker, and Gateway AV/IPS, you must paste or import the feature key that enables these features into the configuration page or use the **Get Feature Key** command to activate upgrade options. If you start the XTM device in safe mode, you do not need to import the feature key again.

## About Feature Keys

A feature key is a license that enables you to use a set of features on your XTM device. You increase the functionality of your device when you purchase an option or upgrade and get a new feature key.

## When You Purchase a New Feature

When you purchase a new feature for your XTM device, you must:

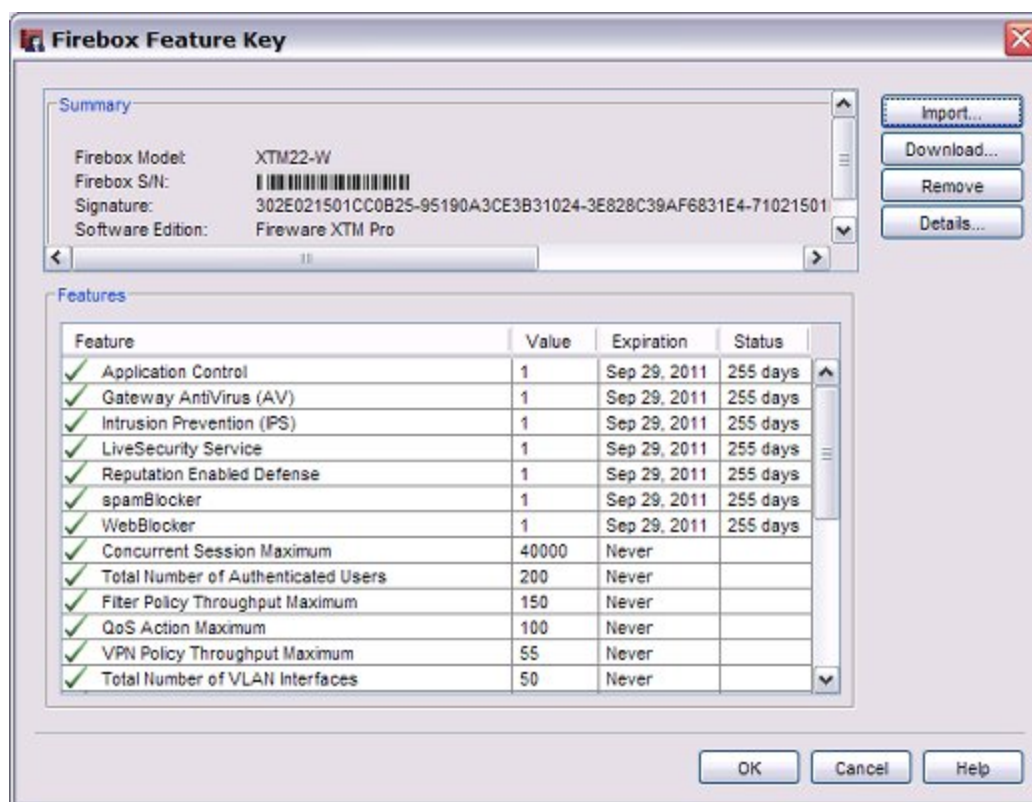
- Get a Feature Key from LiveSecurity
- Add a Feature Key to Your XTM Device

## See Features Available with the Current Feature Key

Your XTM device always has one currently active feature key. To see the features available with this feature key:

1. Open Policy Manager.
2. Select **Setup > Feature Keys**.

The Firebox Feature Key dialog box appears.



The **Firebox Feature Key** dialog box includes:

- A list of available features
- Whether the feature is enabled or disabled
- Value assigned to the feature such as the number of VLAN interfaces allowed
- Expiration date of the feature

- Current status on expiration, such as how many days remain before the feature expires
- Version of software to which the feature key applies

## Verify Feature Key Compliance

To make sure all features on your XTM device are correctly enabled on your feature key:

1. *Open Policy Manager.*
2. Click .

*The Feature Key Compliance dialog box appears.*

*The Description field includes a note to indicate if a feature is in compliance with the feature key, or if it has expired.*

To get a new feature key:

1. In the **Feature Key Compliance** dialog box, click **Add Feature Key**.  
*The Firebox Feature Key dialog box appears.*
2. Either *Add a Feature Key to Your XTM Device* or *Download a Feature Key*.

## Get a Feature Key from LiveSecurity

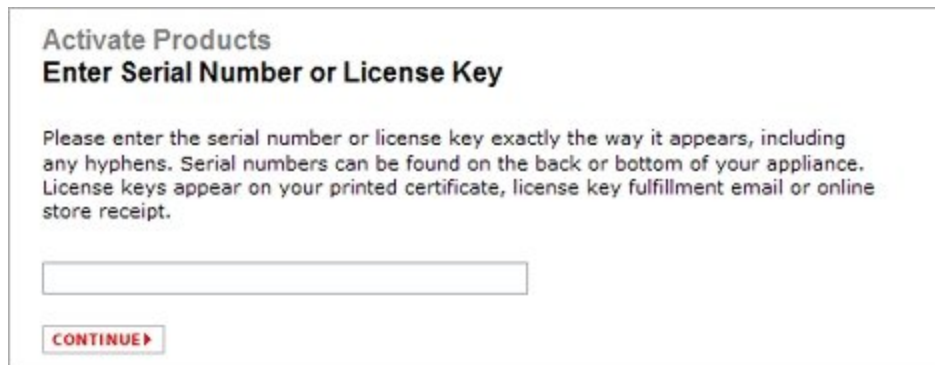
Before you activate a new feature, or renew a subscription service, you must have a license key certificate from WatchGuard that is not already registered on the LiveSecurity web site. When you activate the license key, you can get the feature key that enables the activated feature on the XTM device. You can also retrieve an existing feature key at a later time.

## Activate the License Key for a Feature

To activate a license key and get the feature key for the activated feature:

1. Open a web browser and go to <https://www.watchguard.com/activate>.  
*If you have not already logged in to LiveSecurity, the LiveSecurity Log In page appears.*
2. Type your LiveSecurity user name and password.  
*The Activate Products page appears.*
3. Type the serial number or license key for the product as it appears on your printed certificate. Make sure to include any hyphens.

Use the serial number to register a new XTM device, and the license key to register add-on features.



4. Click **Continue**.  
*The Choose Product to Upgrade page appears.*

5. In the drop-down list, select the device to upgrade or renew.  
If you added a device name when you registered your XTM device, that name appears in the list.
6. Click **Activate**.  
*The Retrieve Feature Key page appears.*
7. Copy the full feature key to a text file and save it on your computer.
8. Click **Finish**.

## Get a Current Feature Key

You can log in to the LiveSecurity web site to get a current feature key, or you can use Firebox System Manager to retrieve the current feature key and add it directly to your XTM device.

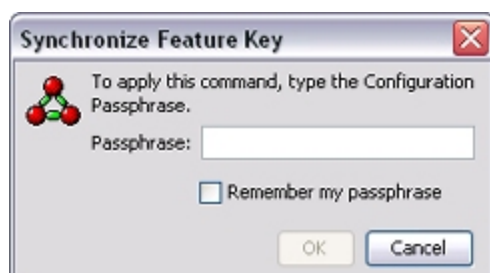
When you go to the LiveSecurity web site to retrieve your feature key, you can choose to download one or more feature keys in a compressed file. If you select multiple devices, the compressed file contains one feature key file for each device.

To retrieve a current feature key from the LiveSecurity web site:

1. Open a web browser and go to <https://www.watchguard.com/archive/manageproducts.asp>.  
*If you have not already logged in to LiveSecurity, the LiveSecurity Log In page appears.*
2. Type your LiveSecurity user name and password.  
*The Manage Products page appears.*
3. Select **Feature Keys**.  
*The Retrieve Feature Key page appears, with a drop-down list to select a product.*
4. In the drop-down list, select your XTM device.
5. Click **Get Key**.  
*A list of all your registered devices appears. A check mark appears next to the device you selected.*
6. Select **Show feature keys on screen**.
7. Click **Get Key**.  
*The Retrieve Feature Key page appears.*
8. Copy the feature key to a text file and save it on your computer.

To use Firebox System Manager (FSM) to retrieve the current feature key:

1. *Start Firebox System Manager.*
2. Select **Tools > Synchronize Feature Key**.  
*The Synchronize Feature Key dialog box appears. If you are connected to your device with only the Status passphrase, you must provide the Configuration passphrase for your device. If you are connected to your device through your Management Server, you do not have to provide the Configuration passphrase.*





3. If you are connected to your device with the Status passphrase, in the **Passphrase** text box, type the Configuration Passphrase and click OK.

If you are connected to your Management Server, click **Yes** to synchronize your feature key.

*The XTM device gets the feature key from the LiveSecurity web site and updates it on the XTM device.*

## Add a Feature Key to Your XTM Device

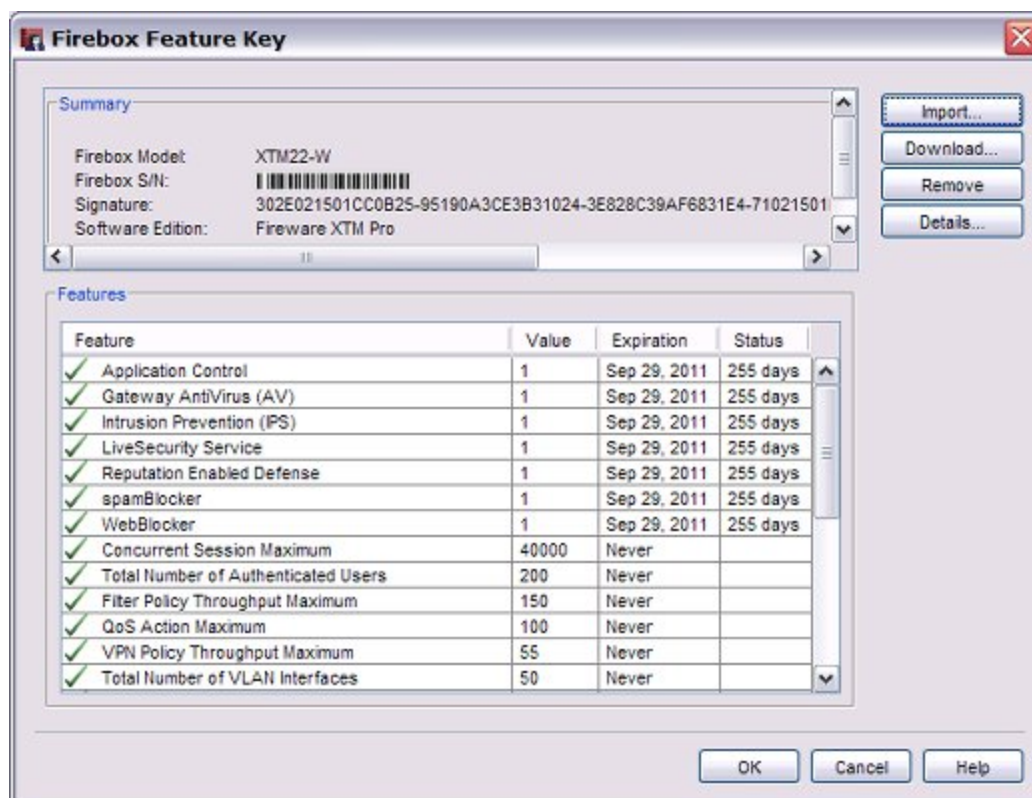
If you purchase a new option or upgrade your XTM device, you can use Policy Manager to add a new feature key to enable the new features. Before you install the new feature key, you must completely remove the old feature key.

1. Select **Setup > Feature Keys**.

*The Firebox Feature Keys dialog box appears.*

The features that are available with this feature key appear in this dialog box. This dialog box also includes:

- Whether each feature is enabled or disabled
- A value assigned to the feature, such as the number of VLAN interfaces allowed
- The expiration date of the feature
- The amount of time that remains before the feature expires



2. To remove the current feature key, click **Remove**.  
*All feature key information is cleared from the dialog box.*
3. Click **Import**.  
*The Import Firebox Feature Key dialog box appears.*



4. Click **Browse** to find the feature key file.  
Or, copy the text of the feature key file and click **Paste** to insert it in the text box.
5. Click **OK**.  
*The Import a Firebox Feature Key dialog box closes and the new feature key information appears in the Firebox Feature Key dialog box.*
6. Click **OK**.  
*In some instances, new dialog boxes and menu commands to configure the feature appear in Policy Manager.*
7. **Save the Configuration File**.  
*The feature key does not operate on the XTM device until you save the configuration file to the device.*

## Remove a Feature Key

1. Select **Setup > Feature Keys**.  
*The Firebox Feature Keys dialog box appears.*
2. Click **Remove**.  
*All feature key information is cleared from the dialog box.*
3. Click **OK**.
4. **Save the Configuration File**.

## See the Details of a Feature Key

From Policy Manager, you can review the details of your current feature key.

The available details include:

- Serial number of the XTM device to which this feature key applies
- XTM device ID and name
- Device model and version number
- Available features

To review the details of your feature key:

1. Select **Setup > Feature Keys**.  
*The Firebox Feature Key dialog box appears.*
2. Click **Details**.  
*The Feature Key Details dialog box appears.*



3. Use the scroll bar to review the details of your feature key.

## Download a Feature Key

You can download a copy of your current feature key from the XTM device to your management computer.

1. Select **Setup > Feature Keys**.  
*The Feature Keys dialog box appears.*
2. Click **Download**.  
*The Get Firebox Feature keys dialog box appears.*
3. Type the status passphrase of the device.
4. Click **OK**.

If you have already created a LiveSecurity user account, you can also use Firebox System Manager to download a current feature key.



1. Start *Firebox System Manager*.
2. Select **Tools > Synchronize Feature Key**.  
*The XTM device contacts the LiveSecurity web site and downloads the current feature key to your device.*

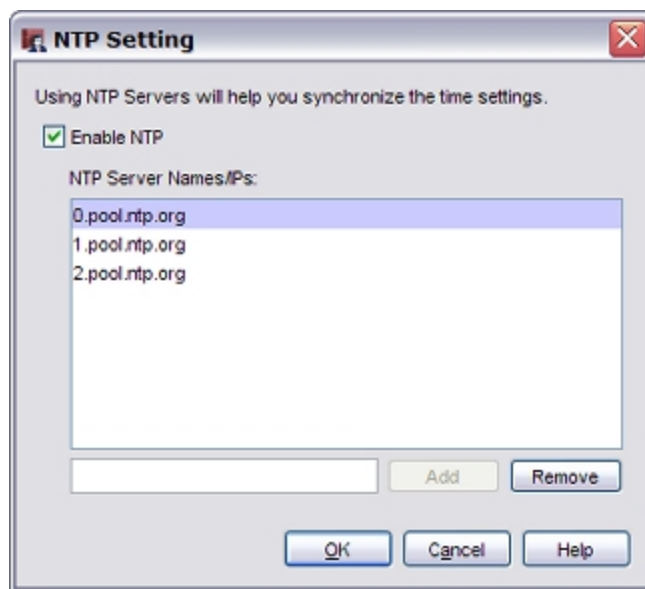
## Enable NTP and Add NTP Servers

Network Time Protocol (NTP) synchronizes computer clock times across a network. Your XTM device can use NTP to get the correct time automatically from NTP servers on the Internet. Because the XTM device uses the time from its system clock for each log message it generates, the time must be set correctly. You can change the NTP server that the XTM device uses. You can also add more NTP servers or delete existing ones, or you can set the time manually.

To use NTP, your XTM device configuration must allow DNS. DNS is allowed in the default configuration by the Outgoing policy. You must also configure DNS servers for the external interface before you configure NTP.

For more information about these addresses, see *Add WINS and DNS Server Addresses* on page 111.

1. Select **Setup > NTP**.  
*The NTP Setting dialog box appears.*



2. Select the **Enable NTP** check box.
3. To add an NTP server, type the IP address or host name of the NTP server you want to use in the text box and click **Add**.  
*You can configure up to three NTP servers.*
4. To delete a server, select the server entry in the **NTP Server Names/IPs** list and click **Remove**.
5. Click **OK**.

## Set the Time Zone and Basic Device Properties

When you run the Quick Setup Wizard, you set the time zone and other basic device properties.

To change the basic device properties:

1. Open Policy Manager.
2. Click **Setup > System**.

*The Device Configuration dialog box appears.*



3. Configure these options:

### *Firebox model*

The XTM device model and model number, as determined by Quick Setup Wizard. You normally do not need to change these settings. If you add a new feature key to the XTM device with a model upgrade, the XTM device model in the device configuration is automatically updated.

### *Name*

The friendly name of the XTM device. You can give the XTM device a friendly name that appears in your log files and reports. Otherwise, the log files and reports use the IP address of the XTM device external interface. Many customers use a Fully Qualified Domain Name as the friendly name if they register such a name with the DNS system. You must give the XTM device a friendly name if you use the Management Server to configure VPN tunnels and certificates.

### *Location, Contact*

Type any information that could be helpful to identify and maintain the XTM device. These fields are filled in by the Quick Setup Wizard if you entered this information there. This information appears on the **Front Panel** tab of Firebox System Manager.

### *Time zone*

Select the time zone for the physical location of the XTM device. The time zone setting controls the date and time that appear in the log file and on tools such as LogViewer, WatchGuard Reports, and WebBlocker.

4. Click **OK**.

## About SNMP

SNMP (Simple Network Management Protocol) is used to monitor devices on your network. SNMP uses management information bases (MIBs) to define what information and events are monitored. You must set up a separate software application, often called an event viewer or MIB browser, to collect and manage SNMP data.

There are two types of MIBs: standard and enterprise. Standard MIBs are definitions of network and hardware events used by many different devices. Enterprise MIBs are used to give information about events that are specific to a single manufacturer. Your XTM device supports eight standard MIBs: IP-MIB, IF-MIB, TCP-MIB, UDP-MIB, SNMPv2-MIB, SNMPv2-SMI, RFC1213-MIB, and RFC1155 SMI-MIB. It also supports two enterprise MIBs: WATCHGUARD-PRODUCTS-MIB and WATCHGUARD-SYSTEM-CONFIG-MIB.

## SNMP Polls and Traps

You can configure your XTM device to accept SNMP polls from an SNMP server. The XTM device reports information to the SNMP server such as the traffic count from each interface, device uptime, the number of TCP packets received and sent, and when each network interface on the XTM device was last modified.

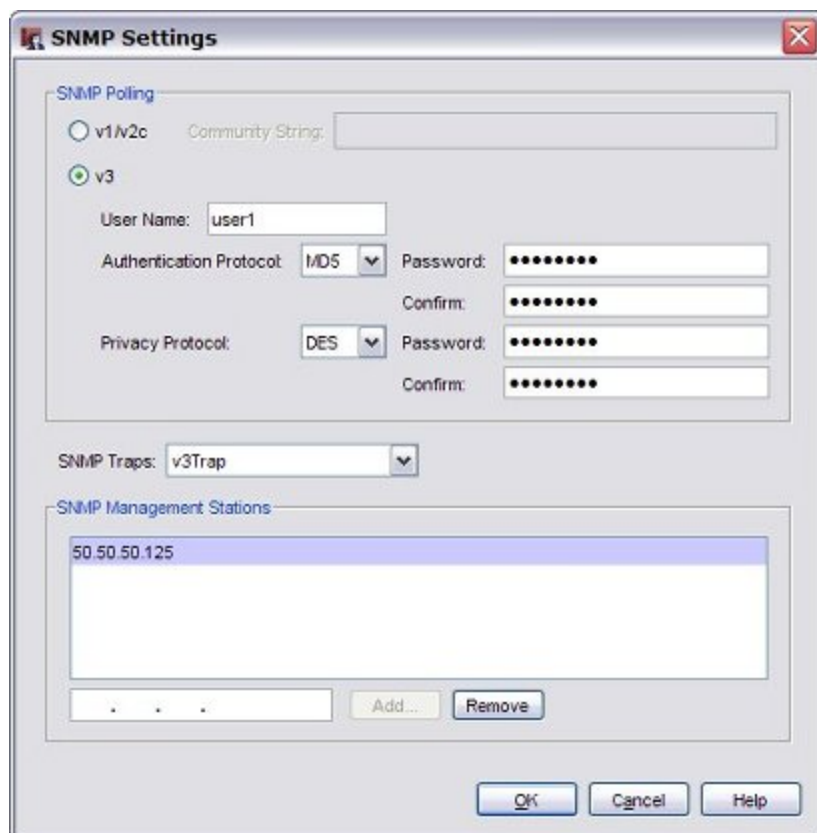
A SNMP trap is an event notification your XTM device sends to an SNMP management station. The trap identifies when a specific condition occurs, such as a value that is more than its predefined threshold. Your XTM device can send a trap for any policy in Policy Manager.

A SNMP inform request is similar to a trap, but the receiver sends a response. If your XTM device does not get a response, it sends the inform request again until the SNMP manager sends a response. A trap is sent only once, and the receiver does not send any acknowledgement when it gets the trap.

## Enable SNMP Polling

You can configure your XTM device to accept SNMP polls from an SNMP server. Your XTM device reports information to the SNMP server such as the traffic count from each interface, device uptime, the number of TCP packets received and sent, and when each network interface was last modified.

1. Select **Setup > SNMP**.



2. Select the version of SNMP you want to use: **v1/v2c** or **v3**.

If you chose **v1/v2c**, type the **Community String** your XTM device must use when it connects to the SNMP server.

If you chose **v3**:

- **User Name** — Type the user name for SNMPv3 authentication and privacy protection.
- **Authentication Protocol** — Select **MD5** (Message Digest 5) or **SHA** (Secure Hash Algorithm).
- **Authentication Password** — Type and confirm the authentication password.
- **Privacy Protocol** — Select **DES** (Data Encryption Standard) to encrypt traffic or **None** to not encrypt SNMP traffic.
- **Privacy Password** — Type and confirm a password to encrypt outgoing messages and decrypt incoming messages.

3. Click **OK**.

To make your XTM device able to receive SNMP polls, you must add a SNMP policy. Policy Manager prompts you to add a SNMP policy automatically.

In the **New Policy Properties** dialog box:

1. In the **From** section, click **Add**.  
*The Add Address dialog box appears.*
2. Click **Add Other**.  
*The Add Member dialog box appears.*
3. From the **Choose Type** drop-down list, select **Host IP**.
4. In the **Value** text box, type the IP address of your SNMP server computer.
5. Click **OK** to close the **Add Member** dialog box.
6. Click **OK** to close the **Add Address** dialog box.  
*The Policy tab of the new policy appears.*
7. In the **To** section, click **Add**.  
*The Add Address dialog box appears.*
8. From the **Available Members** list, select **Firebox**. Click **Add**.  
*XTM device appears in the Selected Members and Addresses list.*
9. Click **OK** to close the **Add Address** dialog box.
10. Click **OK** to close the **New Policy Properties** dialog box.
11. Click **Close**.

## Enable SNMP Management Stations and Traps

An SNMP trap is an event notification your XTM device sends to an SNMP management station. The trap identifies when a specific condition occurs, such as a value that is more than its predefined threshold. Your XTM device can send a trap for any policy.

An SNMP inform request is similar to a trap, but the receiver sends a response. If your XTM device does not get a response, it sends the inform request again until the SNMP manager sends a response. A trap is sent only once, and the receiver does not send any acknowledgement when it gets the trap.

An inform request is more reliable than a trap because your XTM device knows whether the inform request was received. However, inform requests consume more resources. They are held in memory until the sender gets a response. If an inform request must be sent more than once, the retries increase traffic. We recommend you consider whether the receipt every SNMP notification is worth the use of memory in the router and increase in network traffic.

To enable SNMP inform requests, you must use SNMPv2 or SNMPv3. SNMPv1 supports only traps, not inform requests.

## Configure SNMP Management Stations

1. Select **Setup > SNMP**.

*The SNMP Settings window appears.*

2. In the **SNMP Traps** drop-down list, select the version of trap or inform you want to use. SNMPv1 supports only traps, not inform requests.
3. In the SNMP Management Stations text box, type the IP address of your SNMP management station. Click **Add**.  
*Repeat steps 2–3 to add more SNMP management stations.*
4. Click **OK**.

## Add an SNMP Policy

To enable your XTM device to receive SNMP polls, you must also add an SNMP policy.

1. Click **+**.  
Or, select **Edit > Add Policy**.  
*The Add Policies dialog box appears.*
2. Expand the **Packet Filters** list and select **SNMP**. Click **Add**.  
*The New Policy Properties dialog box appears.*
3. In the **From** section, click **Add**.  
*The Add Address dialog box appears.*

4. Click **Add Other**.  
*The Add Member dialog box appears.*
5. From the **Choose Type** drop-down list, select **Host IP**.
6. In the **Value** text box, type the IP address of your SNMP server computer.
7. Click **OK** to close the **Add Member** dialog box.
8. Click **OK** to close the **Add Address** dialog box.  
*The Policy tab of the new policy appears.*
9. In the **To** section, click **Add**.  
*The Add Address dialog box appears.*
10. In the **Available Members** list, select **Firebox**. Click **Add**.
11. Click **OK** on each dialog box to close it. Click **Close**.
12. Save the configuration.

## Send an SNMP Trap for a Policy

Your XTM device can send an SNMP trap when traffic is filtered by a policy. You must have at least one SNMP management station configured to enable SNMP traps.

1. Double-click the SNMP policy.  
*In the Edit Policy Properties dialog box.*
2. Select the **Properties** tab.
3. Click **Logging**.  
*The Logging and Notification dialog box appears.*
4. Select the **Send SNMP Trap** check box.
5. Click **OK** to close the **Logging and Notification** dialog box.
6. Click **OK** to close the **Edit Policy Properties** dialog box.

## About Management Information Bases (MIBs)

Fireware XTM supports two types of Management Information Bases (MIBs).

### *Standard MIBs*

Standard MIBs are definitions of network and hardware events used by many different devices. Your XTM device supports these eight standard MIBs:

- IP-MIB
- IF-MIB
- TCP-MIB
- UDP-MIB
- SNMPv2-MIB
- SNMPv2-SMI
- RFC1213-MIB
- RFC1155 SMI-MIB

These MIBs include information about standard network information, such as IP addresses and network interface settings.

### *Enterprise MIBs*

Enterprise MIBs are used to give information about events that are specific to a single manufacturer. Your XTM device supports these enterprise MIBs:

- WATCHGUARD-PRODUCTS-MIB
- WATCHGUARD-SYSTEM-CONFIG-MIB
- UCD-SNMP-MIB

These MIBs include more specific information about device hardware.

When you install the Fireware XTM OS on your management computer, MIBs are installed in this location:

#### *Windows XP*

C:\Documents and Settings\All Users\Shared WatchGuard\SNMP

#### *Windows 7, Windows Server 2008, and Windows Vista*

C:\Users\Public\Shared WatchGuard\SNMP

If you want to install all MIBs, you must run the Fireware XTM OS installer for all XTM models you use. You can find the Fireware XTM OS installation on the Software Downloads section of the WatchGuard web site, <http://www.watchguard.com>.

## About WatchGuard Passphrases, Encryption Keys, and Shared Keys

As part of your network security solution, you use passphrases, encryption keys, and shared keys. This topic includes information about most of the passphrases, encryption keys, and shared keys you use for WatchGuard products. It does not include information about third-party passwords or passphrases. Information about restrictions for passphrases, encryption keys, and shared keys is also included in the related procedures.

### Create a Secure Passphrase, Encryption Key, or Shared Key

To create a secure passphrase, encryption key, or shared key, we recommend that you:

- Use a combination of uppercase and lowercase ASCII characters, numbers, and special characters (for example, Im4e@tiN9).
- Do not use a word from standard dictionaries, even if you use it in a different sequence or in a different language.
- Do not use a name. It is easy for an attacker to find a business name, familiar name, or the name of a famous person.

As an additional security measure, we recommend that you change your passphrases, encryption keys, and shared keys at regular intervals.



## XTM Device Passphrases

An XTM device uses two passphrases:

### *Status passphrase*

The read-only password or passphrase that allows access to the XTM device. When you log in with this passphrase, you can review your configuration, but you cannot save changes to the XTM device. The status passphrase is associated with the user name *status*.

### *Configuration passphrase*

The read-write password or passphrase that allows an administrator full access to the XTM device. You must use this passphrase to save configuration changes to the XTM device. This is also the passphrase you must use to change your XTM device passphrases. The configuration passphrase is associated with the user name *admin*.

Each of these XTM device passphrases must be at least 8 characters.

## User Passphrases

You can create user names and passphrases to use with Firebox authentication and role-based administration.

### *User Passphrases for Firebox authentication*

After you set this user passphrase, the characters are masked and it does not appear in simple text again. If the passphrase is lost, you must set a new passphrase. The allowed range for this passphrase is 8–32 characters.

### *User Passphrases for role-based administration*

After you set this user passphrase, it does not appear again in the **User and Group Properties** dialog box. If the passphrase is lost, you must set a new passphrase. This passphrase must be at least 8 characters.

## Server Passphrases

### *Administrator passphrase*

The Administrator passphrase is used to control access to the WatchGuard Server Center. You also use this passphrase when you connect to your Management Server from WatchGuard System Manager (WSM). This passphrase must be at least 8 characters. The Administrator passphrase is associated with the user name *admin*.

### *Authentication server shared secret*

The shared secret is the key the XTM device and the authentication server use to secure the authentication information that passes between them. The shared secret is case-sensitive and must be the same on the XTM device and the authentication server. RADIUS, SecurID, and VASCO authentication servers all use a shared key.

## Encryption Keys and Shared Keys

### *Log Server encryption key*

The encryption key is used to create a secure connection between the XTM device and the Log Servers, and to avoid man-in-the-middle attacks. The allowed range for the encryption key is 8–32 characters. You can use all characters except spaces and slashes (/ or \).

### *Backup/Restore encryption key*

This is the encryption key you create to encrypt a backup file of your XTM device configuration. When you restore a backup file, you must use the encryption key you selected when you created the configuration backup file. If you lose or forget this encryption key, you cannot restore the backup file. The encryption key must be at least 8 characters, and cannot be more than 15 characters.

### *VPN shared key*

The shared key is a passphrase used by two devices to encrypt and decrypt the data that goes through the tunnel. The two devices use the same passphrase. If the devices do not have the same passphrase, they cannot encrypt and decrypt the data correctly.

## Change XTM Device Passphrases

An XTM device uses two passphrases:

### *Status passphrase*

The read-only password or passphrase that allows access to the XTM device.

### *Configuration passphrase*

The read-write password or passphrase that allows an administrator full access to the XTM device.

For more information about passphrases, see *About WatchGuard Passphrases, Encryption Keys, and Shared Keys* on page 72.

To change the passphrases:

1. Open the XTM device configuration file.
2. Click **File > Change Passphrases**.

*The Change Passphrases dialog box appears.*

3. From the **Firebox Address or Name** drop-down list, type or select the IP address or name of the XTM device.
4. In the **Configuration Passphrase** text box, type the configuration (read/write) passphrase.
5. Type and confirm the new status (read-only) and configuration (read/write) passphrases. The status passphrase must be different from the configuration passphrase.
6. Click **OK**.

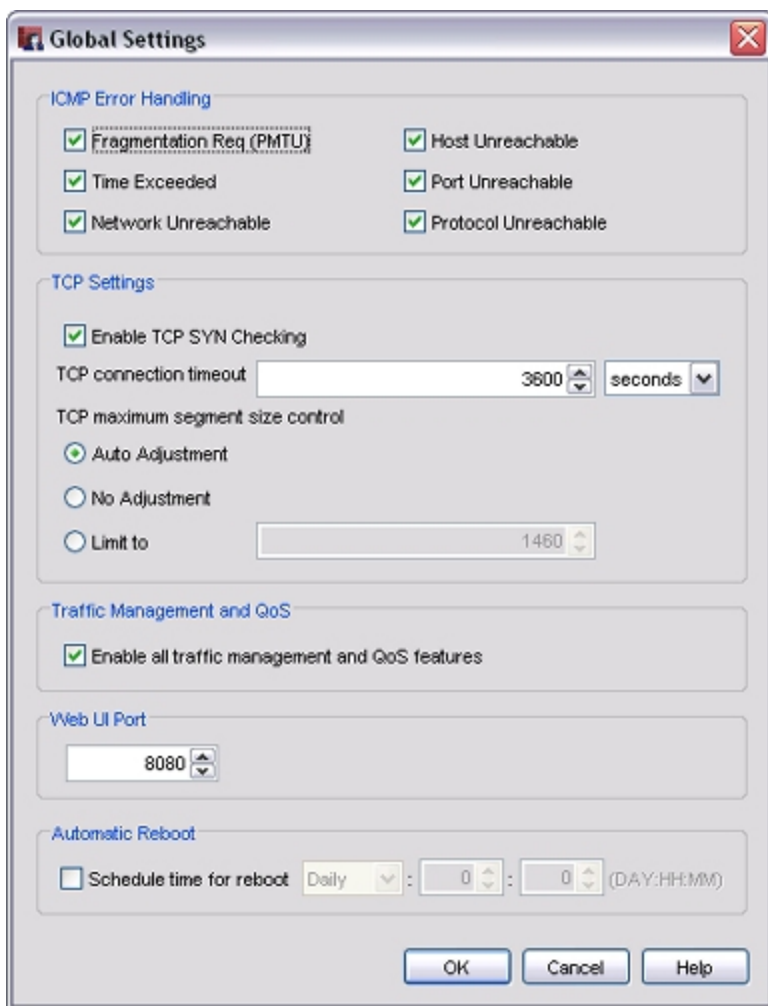
## Define XTM Device Global Settings

From Policy Manager, you can select settings that control the actions of many XTM device features. You can specify the basic parameters for:

- ICMP error handling
- TCP SYN checking
- TCP maximum size adjustment
- Traffic management and QoS
- Web UI port

To configure the global settings:

1. Select **Setup > Global Settings**.  
*The Global Settings dialog box appears.*



2. Configure the different categories of global settings as described in the subsequent sections.
3. Click **OK**.
4. Save the configuration file to your device.

## Define ICMP Error Handling Global Settings

Internet Control Message Protocol (ICMP) settings control errors in connections. It is used for two types of operations:

- To tell client hosts about error conditions
- To probe a network to find general characteristics about the network

The XTM device sends an ICMP error message each time an event occurs that matches one of the parameters you selected. These messages are good tools to use when you troubleshoot problems, but can also decrease security because they expose information about your network. If you deny these ICMP messages, you can increase security if you prevent network probes, but this can also cause timeout delays for incomplete connections, which can cause application problems.

Settings for global ICMP error handling are:

### *Fragmentation Req (PMTU)*

Select this check box to allow ICMP Fragmentation Req messages. The XTM device uses these messages to find the MTU path.

### *Time Exceeded*

Select this check box to allow ICMP Time Exceeded messages. A router usually sends these messages when a route loop occurs.

### *Network Unreachable*

Select this check box to allow ICMP Network Unreachable messages. A router usually sends these messages when a network link is broken.

### *Host Unreachable*

Select this check box to allow ICMP Host Unreachable messages. Your network usually sends these messages when it cannot use a host or service.

### *Port Unreachable*

Select this check box to allow ICMP Port Unreachable messages. A host or firewall usually sends these messages when a network service is not available or is not allowed.

### *Protocol Unreachable*

Select this check box to allow ICMP Protocol Unreachable messages.

To override these global ICMP settings for a specific policy, from Policy Manager:

1. On the **Firewall** tab, select the specific policy.
2. Double-click the policy to edit it.  
*The Edit Policy Properties dialog box appears.*
3. Select the **Advanced** tab.
4. From the **ICMP Error Handling** drop-down list, select **Specify setting**.
5. Click **ICMP Setting**.  
*The ICMP Error Handling Settings dialog box appears.*

6. Select only the check boxes for the settings you want to enable.
7. Click **OK**.

## Configure TCP Settings

### *Enable TCP SYN checking*

To enable TCP SYN checking to make sure that the TCP three-way handshake is completed before the XTM device allows a data connection, select this option.

### *TCP connection timeout*

Specify the connection timeout value in seconds, minutes, hours, or days. The default setting is 3600 seconds.

### *TCP maximum segment size control*

The TCP segment can be set to a specified size for a connection that must have more TCP/IP layer 3 overhead (for example, PPPoE, ESP, or AH). If this size is not correctly configured, users cannot get access to some web sites.

The global TCP maximum segment size adjustment settings are:

- **Auto Adjustment**— This option enables the XTM device to examine all maximum segment size (MSS) negotiations and changes the MSS value to the applicable one.
- **No Adjustment**— The XTM device does not change the MSS value.
- **Limit to**— Type or select a size adjustment limit.

## Enable or Disable Traffic Management and QoS

For performance testing or network debugging purposes, you can disable the Traffic Management and QoS features.

To enable these features:

Select the **Enable all traffic management and QoS features** check box.

To disable these features:

Clear the **Enable all traffic management and QoS features** check box.

## Change the Web UI Port

By default, Fireware XTM Web UI uses port 8080.

To change the default port:

1. In the **Web UI Port** text box, type or select a different port number.
2. Use the new port to connect to Fireware XTM Web UI and test the connection with the new port.

## Automatic Reboot

You can schedule your XTM device to automatically reboot at the day and time you specify.

To schedule an automatic reboot for your device:

1. Select the **Schedule time for reboot** check box.
2. In the adjacent drop-down list, select **Daily** to reboot at the same time every day, or select a day of the week for a weekly reboot.
3. In the adjacent text boxes, type or select the hour and minute of the day (in 24-hour time format) that you want the reboot to start.

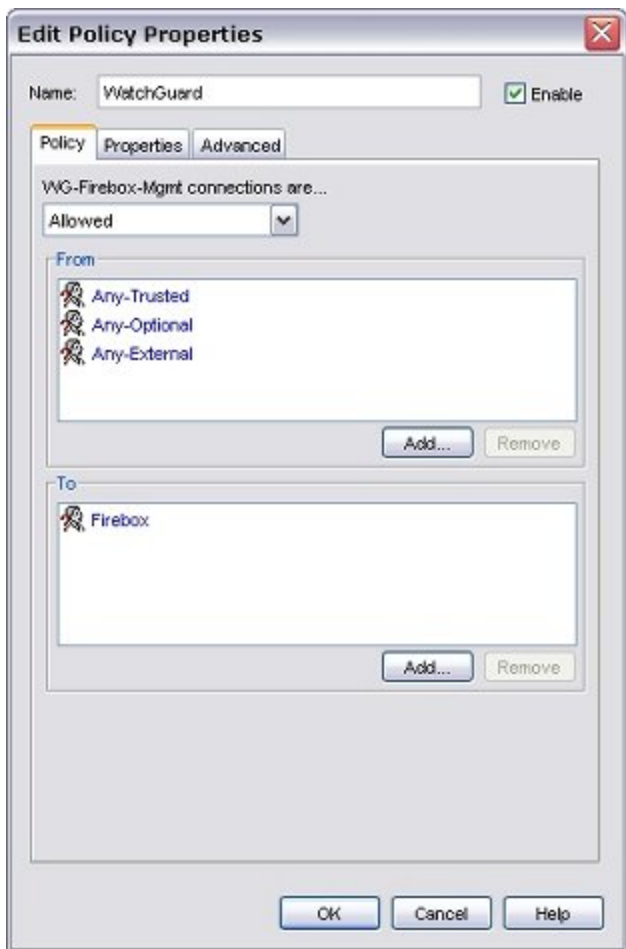
## Manage an XTM device from a Remote Location

When you configure an XTM device with the Quick Setup Wizard, the WatchGuard policy is created automatically. This policy allows you to connect to and administer the XTM device from any computer on the trusted or optional networks. If you want to manage the XTM device from a remote location (any location external to the XTM device), then you must modify the WatchGuard policy to allow administrative connections from the IP address of your remote location.

The WatchGuard policy controls access to the XTM device on these four TCP ports: 4103, 4105, 4117, 4118. When you allow connections in the WatchGuard policy, you allow connections to each of these four ports.

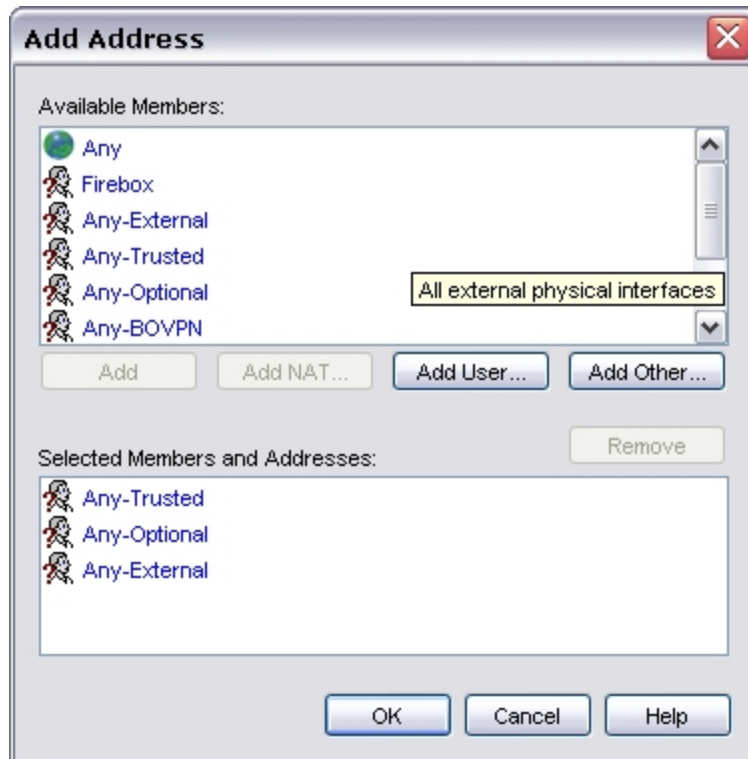
Before you modify the WatchGuard policy, we recommend that you consider connecting to the XTM device with a VPN. This greatly increases the security of the connection. If this is not possible, we recommend that you allow access from the external network to only certain authorized users and to the smallest number of computers possible. For example, your configuration is more secure if you allow connections from a single computer instead of from the alias *Any-External*.

1. Double-click the **WatchGuard** policy.  
Or, right-click the WatchGuard policy and select **Modify Policy**.  
*The Edit Policy Properties dialog box appears.*



2. In the **From** section, click **Add**.  
*The Add Address dialog box appears.*





3. To add the IP address of the external computer that connects to the XTM device, click **Add Other**, make sure **Host IP** is the selected type, and type the IP address.
4. To give access to an authorized user, in the **Add Address** dialog box, click **Add User**.  
*The Add Authorized Users or Groups dialog box appears.*  
 For information about how to create an alias, see *Create an Alias* on page 379.

## Upgrade to a New Version of Fireware XTM

Periodically, WatchGuard makes new versions of WatchGuard System Manager (WSM) and Fireware XTM appliance software available to XTM device users with active LiveSecurity subscriptions. To upgrade from one version of WSM with Fireware XTM to a new version of WSM with Fireware XTM, use the procedures in the subsequent sections.

### Install the Upgrade on Your Management Computer

1. Download the updated Fireware XTM and WatchGuard System Manager software from the Software Downloads section of the WatchGuard web site at <http://www.watchguard.com>.
2. Back up your current XTM device configuration file and Management Server configuration files.

For more information on how to create a backup image of your XTM device configuration, see *Make a Backup of the XTM Device Image* on page 43.

To back up the settings on your Management Server, see *Back Up or Restore the Management Server Configuration* on page 576.

3. Use Windows Add or Remove Programs to uninstall your existing WatchGuard System Manager and WatchGuard Fireware XTM installation. You can have more than one version of WatchGuard System

Manager client software installed on your management computer, but only one version of WatchGuard server software.

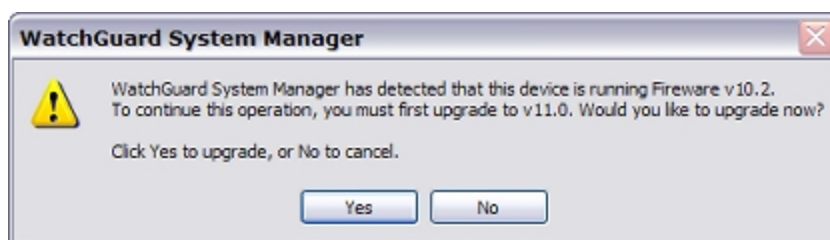
For more information, see *Install WSM and Keep an Older Version* on page 32.

4. Launch the file or files that you downloaded from the LiveSecurity web site.
5. Use the on-screen procedure to install the Fireware XTM upgrade file in the WatchGuard installation directory on your management computer.

## Upgrade the XTM Device

1. To save the upgrade to the XTM device, use Policy Manager to open your XTM device configuration file.

*WatchGuard System Manager detects that the configuration file is for an older version, and displays an upgrade dialog box.*



2. Click **Yes** to upgrade the configuration file. Use the on-screen instructions to convert the configuration file to the newer version.

**Note** *The upgrade dialog box looks different if you have multiple versions of WatchGuard System Manager installed on your management computer. For more information, see Use Multiple Versions of Policy Manager on page 83.*

If you do not see the upgrade dialog box when you open Policy Manager:

1. Select **File > Upgrade**.
2. Type the configuration passphrase.  
*The Upgrade — Enter the path to the upgrade image dialog box appears.*
3. The default path is automatically selected. If your installation path is different, click **Browse** to change the path to the upgrade image.



4. Click **OK**.

The upgrade procedure can take up to 15 minutes and automatically reboots the XTM device.

If your XTM device has been in operation for some time before you upgrade, you might have to restart the device before you start the upgrade to clear the temporary memory.

## Use Multiple Versions of Policy Manager

In WatchGuard System Manager v11.x, if you open a configuration file created by an older version of Policy Manager, and if the older version of WatchGuard System Manager is also installed on the management computer, the **Upgrade Available** dialog box appears. You can choose to launch the older version of Policy Manager or to upgrade the configuration file to the newer version.

If you do not want WatchGuard System Manager to display this dialog box when you open an older configuration file, select the **Do not show this message again** check box.

To enable the **Upgrade Available** dialog box if you disabled it:

1. In WatchGuard System Manager, select **Edit > Options**.  
*The Options dialog box appears.*
2. Select the **Show upgrade dialog when launching Policy Manager** check box.
3. Click **OK**.

## About Upgrade Options

You can add upgrades to your XTM device to enable additional subscription services, features, and capacity.

For a list of available upgrade options, see [www.watchguard.com/products/options.asp](http://www.watchguard.com/products/options.asp).

## Subscription Services Upgrades

### *WebBlocker*

The WebBlocker upgrade enables you to control access to web content.

For more information, see *About WebBlocker* on page 1065.

### *spamBlocker*

The spamBlocker upgrade allows you to filter spam and bulk email.

For more information, see *About spamBlocker* on page 1141.

### *Gateway AV/IPS*

The Gateway AV/IPS upgrade enables you to block viruses and prevent intrusion attempts by hackers.

For more information, see *About Gateway AntiVirus* on page 1167.

## Appliance and Software Upgrades

### *Pro*

The Pro upgrade to Fireware XTM provides several advanced features for experienced customers, such as server load balancing and additional SSL VPN tunnels. The features available with a Pro upgrade depend on the type and model of your XTM device.

For more information, see *Fireware XTM with a Pro Upgrade* on page 13.

### *Model upgrades*

For some XTM device models, you can purchase a license key to upgrade the device to a higher model in the same product family. A model upgrade gives your XTM device the same functions as a higher model.

To compare the features and capabilities of different XTM device models, go to <http://www.watchguard.com/products/compare.asp>.

## How to Apply an Upgrade

When you purchase an upgrade, you register the upgrade on the WatchGuard LiveSecurity web site. Then you download a feature key that enables the upgrade on your XTM device.

For information about feature keys, see *About Feature Keys* on page 58.

## Renew Security Subscriptions

Your WatchGuard subscription services (Gateway AntiVirus, Intrusion Prevention Service, Application Control, WebBlocker, and spamBlocker) must get regular updates to operate effectively.

Your XTM device gives you reminders to renew your subscriptions when you save changes to a configuration file. WatchGuard System Manager reminds you that your subscription is about to expire 60 days before, 30 days before, 15 days before, and the day before the expiration date.

When your subscriptions expire, you cannot save any changes to your configuration until you either renew or disable the expired subscription. You can use Policy Manager to update the feature key for your subscriptions.

1. Select **File > Save > To Firebox**.  
*You see a message that tells you to update your feature key.*
2. Click **OK**.  
*The Feature Key Compliance dialog box appears.*



3. Select the expired subscription.
4. If you already have the new feature key, click **Add Feature Key**. Paste your new feature key.

You cannot right-click to paste. You must use CTRL-V or click **Paste**.

If you do not already have your new feature key, you must click **Disable** even if you plan to renew later. You do not lose your settings if you disable the subscription. If you renew your subscription at a later time, you can reactivate the settings and save them to the XTM device.

3. Click **OK**.

## Renew Subscriptions from Firebox System Manager

If a subscription is to expire soon, a warning appears on the front panel of Firebox System Manager and **Renew Now** appears at the upper-right corner of the window. Click **Renew Now** to go to the LiveSecurity Service web site and renew the subscription.



# 6 Network Setup and Configuration

---

## About Network Interface Setup

A primary component of your XTM device setup is the configuration of network interface IP addresses. When you run the Quick Setup Wizard, the external and trusted interfaces are set up so traffic can flow from protected devices to an outside network. You can use the procedures in this section to change the configuration after you run the Quick Setup Wizard, or to add other components of your network to the configuration. For example, you can set up an optional interface for public servers such as a web server.

Your XTM device physically separates the networks on your Local Area Network (LAN) from those on a Wide Area Network (WAN) like the Internet. Your device uses *routing* to send packets from networks it protects to networks outside your organization. To do this, your device must know what networks are connected on each interface.

We recommend that you record basic information about your network and VPN configuration in the event that you need to contact technical support. This information can help your technician resolve your problem quickly.

## Network Modes

Your XTM device supports several network modes:

### *Mixed routing mode*

In mixed routing mode, you can configure your XTM device to send network traffic between a wide variety of physical and virtual network interfaces. This is the default network mode, and this mode offers the greatest amount of flexibility for different network configurations. However, you must configure each interface separately, and you may have to change network settings for each computer or client protected by your XTM device. The XTM device uses Network Address Translation (NAT) to send information between network interfaces.

For more information, see *About Network Address Translation* on page 161.

The requirements for a mixed routing mode are:

- All interfaces of the XTM device must be configured on different subnets. The minimum configuration includes the external and trusted interfaces. You also can configure one or more optional interfaces.
- All computers connected to the trusted and optional interfaces must have an IP address from that network.

### *Drop-in mode*

In a drop-in configuration, your XTM device is configured with the same IP address on all interfaces. You can put your XTM device between the router and the LAN and not have to change the configuration of any local computers. This configuration is known as *drop-in* because your XTM device is *dropped in* to an existing network. Some network features, such as bridges and VLANs (Virtual Local Area Networks), are not available in this mode.

For drop-in configuration, you must:

- Assign a static external IP address to the XTM device.
- Use one logical network for all interfaces.
- Not configure multi-WAN in Round-robin or Failover mode.

For more information, see *Drop-In Mode* on page 98.

### *Bridge mode*

Bridge mode is a feature that allows you to place your XTM device between an existing network and its gateway to filter or manage network traffic. When you enable this feature, your XTM device processes and forwards all incoming network traffic to the gateway IP address you specify. When the traffic arrives at the gateway, it appears to have been sent from the original device. In this configuration, your XTM device cannot perform several functions that require a public and unique IP address. For example, you cannot configure an XTM device in bridge mode to act as an endpoint for a VPN (Virtual Private Network).

For more information, see *Bridge Mode* on page 103.



## Interface Types

You use three interface types to configure your network in mixed routing or drop-in mode:

### *External Interfaces*

An external interface is used to connect your XTM device to a network outside your organization. Often, an external interface is the method by which you connect your XTM device to the Internet. You can configure a maximum of four (4) physical external interfaces.

When you configure an external interface, you must choose the method your Internet service provider (ISP) uses to give you an IP address for your XTM device. If you do not know the method, get this information from your ISP or network administrator.

### *Trusted Interfaces*

Trusted interfaces connect to the private LAN (local area network) or internal network of your organization. A trusted interface usually provides connections for employees and secure internal resources.

### *Optional Interfaces*

Optional interfaces are *mixed-trust* or *DMZ* environments that are separate from your trusted network. Examples of computers often found on an optional interface are public web servers, FTP servers, and mail servers.

For more information on interface types, see *Common Interface Settings* on page 105.

If you have an XTM 2 Series device, you can use Fireware XTM Web UI to configure failover with an external modem over the serial port.

For more information, see *Serial Modem Failover* on page 153.

When you configure the interfaces on your XTM device, you must use slash notation to denote the subnet mask. For example, you would enter the network range 192.168.0.0 subnet mask 255.255.255.0 as 192.168.0.0/24. A trusted interface with the IP address of 10.0.1.1/16 has a subnet mask of 255.255.0.0.

For more information on slash notation, see *About Slash Notation* on page 3.

## About Network Interfaces on the Edge e-Series

When you use WatchGuard System Manager to manage a Firebox X Edge e-Series device, the network interface numbers that appear in WatchGuard System Manager do not match the network interface labels printed below the physical interfaces on the device. Use the table below to understand how the interface numbers in WatchGuard System Manager map to the physical interfaces on the device.

Interface number in Fireware XTM	Interface label on the Firebox X Edge e-Series hardware
0	WAN 1
1	LAN 0, LAN 1, LAN 2
2	WAN 2
3	Opt

You can consider the interfaces labeled LAN 0, LAN 1, and LAN 2 as a three interface network hub that is connected to a single Firebox interface. In Fireware XTM, you configure these interfaces together as Interface 1.

## Mixed Routing Mode

In mixed routing mode, you can configure your XTM device to send network traffic between many different types of physical and virtual network interfaces. Mixed routing mode is the default network mode. While most network and security features are available in this mode, you must carefully check the configuration of each device connected to your XTM device to make sure that your network operates correctly.

A basic network configuration in mixed routing mode uses at least two interfaces. For example, you can connect an external interface to a cable modem or other Internet connection, and a trusted interface to an internal router that connects internal members of your organization. From that basic configuration, you can add an optional network that protects servers but allows greater access from external networks, configure VLANs, and other advanced features, or set additional options for security like MAC address restrictions. You can also define how network traffic is sent between interfaces.

To get started on interface configuration in mixed routing mode, see *Common Interface Settings* on page 105.

It is easy to forget IP addresses and connection points on your network in mixed routing mode, especially if you use VLANs (Virtual Local Area Networks), secondary networks, and other advanced features. We recommend that you record basic information about your network and VPN configuration in the event that you need to contact technical support. This information can help your technician resolve your problem quickly.

## Configure an External Interface

An external interface is used to connect your XTM device to a network outside your organization. Often, an external interface is the method by which you connect your device to the Internet. You can configure a maximum of four (4) physical external interfaces.

When you configure an external interface, you must choose the method your Internet service provider (ISP) uses to give you an IP address for your device. If you do not know the method, get this information from your ISP or network administrator.

For information about methods used to set and distribute IP addresses, see *Static and Dynamic IP Addresses* on page 4.

## Use a Static IP Address

1. Select **Network > Configuration**.  
*The Network Configuration dialog box appears.*
2. Select an external interface. Click **Configure**.  
*The Interface Settings dialog box appears.*
3. Select **Use Static IP**.
4. In the **IP address** text box, type or select the IP address of the interface.
5. In the **Default Gateway** text box, type or select the IP address of the default gateway.

Use Static IP

IP Address: 50.50.50.10/24

Default Gateway: 50.50.50.1

6. Click **OK**.

## Use PPPoE Authentication

If your ISP uses PPPoE, you must configure PPPoE authentication before your device can send traffic through the external interface.

1. Select **Network > Configuration**.  
*The Network Configuration dialog box appears.*
2. Select an external interface. Click **Configure**.
3. In the **Interface Settings** dialog box, select **Use PPPoE**.
4. Select an option:
  - **Obtain an IP address automatically**
  - **Use IP address** (supplied by your Internet Service Provider)
5. If you selected **Use IP Address**, in the adjacent text box, type or select the IP address.
6. Type the **User Name** and **Password**. Type the password again.  
*ISPs use the email address format for user names, such as user@example.com.*

Use PPPoE

Obtain an IP address automatically

Use IP address:

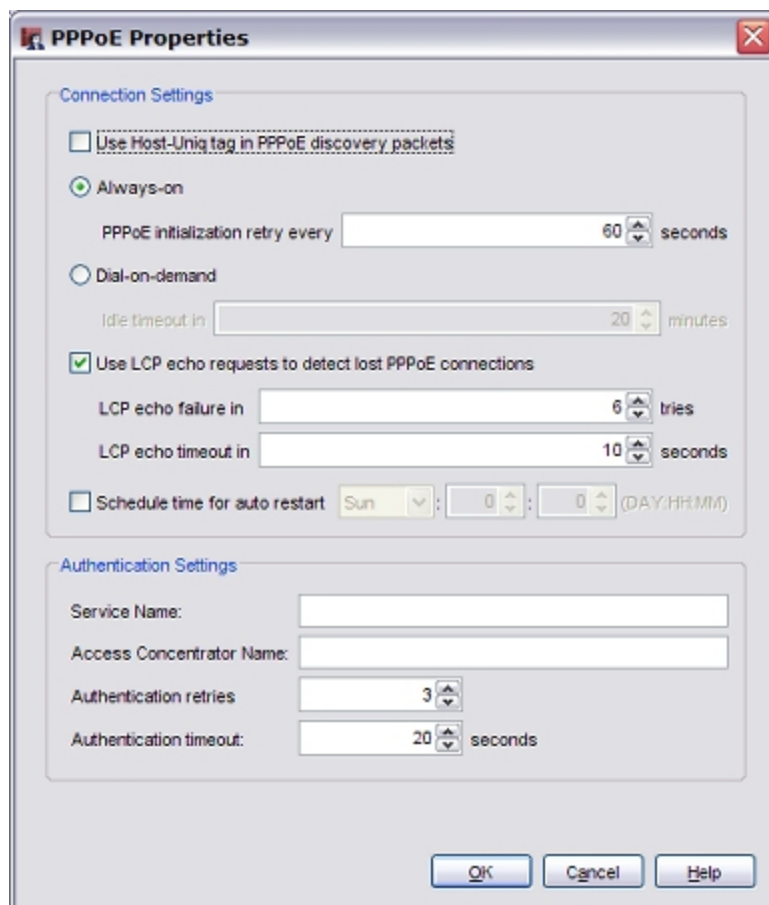
User Name:

Password:

Reenter Password:

Advanced Properties...

7. To configure PPPoE options, click **Advanced Properties**.  
*The PPPoE Properties dialog box appears. Your ISP can tell you if you must change the timeout or LCP values.*



8. If your ISP requires the Host-Uniq tag for PPPoE discovery packets, select the **Use Host-Uniq tag in PPPoE discovery packets** check box.
9. Select when the device connects to the PPPoE server:
  - **Always-on** — The XTM device keeps a constant PPPoE connection. It is not necessary for network traffic to go through the external interface.  
If you select this option, type or select a value in the **PPPoE initialization retry every** text box to set the number of seconds that PPPoE tries to initialize before it times out.
  - **Dial-on-Demand** — The XTM device connects to the PPPoE server only when it gets a request to send traffic to an IP address on the external interface. If your ISP regularly resets the connection, select this option.  
If you select this option, in the **Idle timeout in** text box, set the length of time a client can stay connected when no traffic is sent. If you do not select this option, you must manually restart the XTM device each time the connection resets.
10. In the **LCP echo failure in** text box, type or select the number of failed LCP echo requests allowed before the PPPoE connection is considered inactive and closed.
11. In the **LCP echo timeout in** text box, type or select the length of time, in seconds, that the response to each echo timeout must be received.
12. To configure the XTM device to automatically restart the PPPoE connection on a daily or weekly basis, select the **Schedule time for auto restart** check box.

13. In the **Schedule time for auto restart** drop-down list, select **Daily** to restart the connection at the same time each day, or select a day of the week to restart weekly. Select the hour and minute of the day (in 24 hour time format) to automatically restart the PPPoE connection.
14. In the **Service Name** text box, type a PPPoE service name.  
This is either an ISP name or a class of service that is configured on the PPPoE server. Usually, this option is not used. Select it only if there is more than one access concentrator, or you know that you must use a specified service name.
15. In the **Access Concentrator Name** text box, type the name of a PPPoE access concentrator, also known as a PPPoE server. Usually, this option is not used. Select it only if you know there is more than one access concentrator.
16. In the **Authentication retries** text box, type or select the number of times that the XTM device can try to make a connection.  
*The default value is three (3) connection attempts.*
17. In the **Authentication timeout** text box, type a value for the amount of time between retries.  
*The default value is 20 seconds between each connection attempt.*
18. Click **OK**.
19. Save your configuration.

## Use DHCP

1. In the **Interface Settings** dialog box, select **Use DHCP Client**.
2. If your ISP or external DHCP server requires a client identifier, such as a MAC address, in the **Client** text box, type this information.
3. To specify a host name for identification, in the **Host Name** text box, type the host name.

The screenshot shows a configuration window titled 'Use DHCP Client'. At the top, there is a radio button labeled 'Use DHCP Client' which is selected. Below this are two text input fields: 'Client' and 'Host Name'. Underneath these is a section titled 'Host IP' containing two radio buttons: 'Obtain an IP automatically' (which is selected) and 'Use IP address:' (which has a dropdown arrow next to it). At the bottom of the window, there is a checkbox labeled 'Leasing Time:' followed by a dropdown menu currently displaying '8 hours'.

4. To enable DHCP to assign an IP address to the XTM device, in the **Host IP** section, select **Obtain an IP automatically**.

To manually assign an IP address and use DHCP to give this assigned address to the XTM device, select **Use IP address** and type the IP address in the adjacent text box.

IP addresses assigned by a DHCP server have an eight hour lease by default, which means the address is valid for eight hours.

5. To change the lease time, select the **Leasing Time** check box and select the value in the adjacent drop-down list.

## Configure DHCP in Mixed Routing Mode

DHCP (Dynamic Host Configuration Protocol) is a method to assign IP addresses automatically to network clients. You can configure your XTM device as a DHCP server for the networks that it protects. If you have a DHCP server, we recommend that you continue to use that server for DHCP.

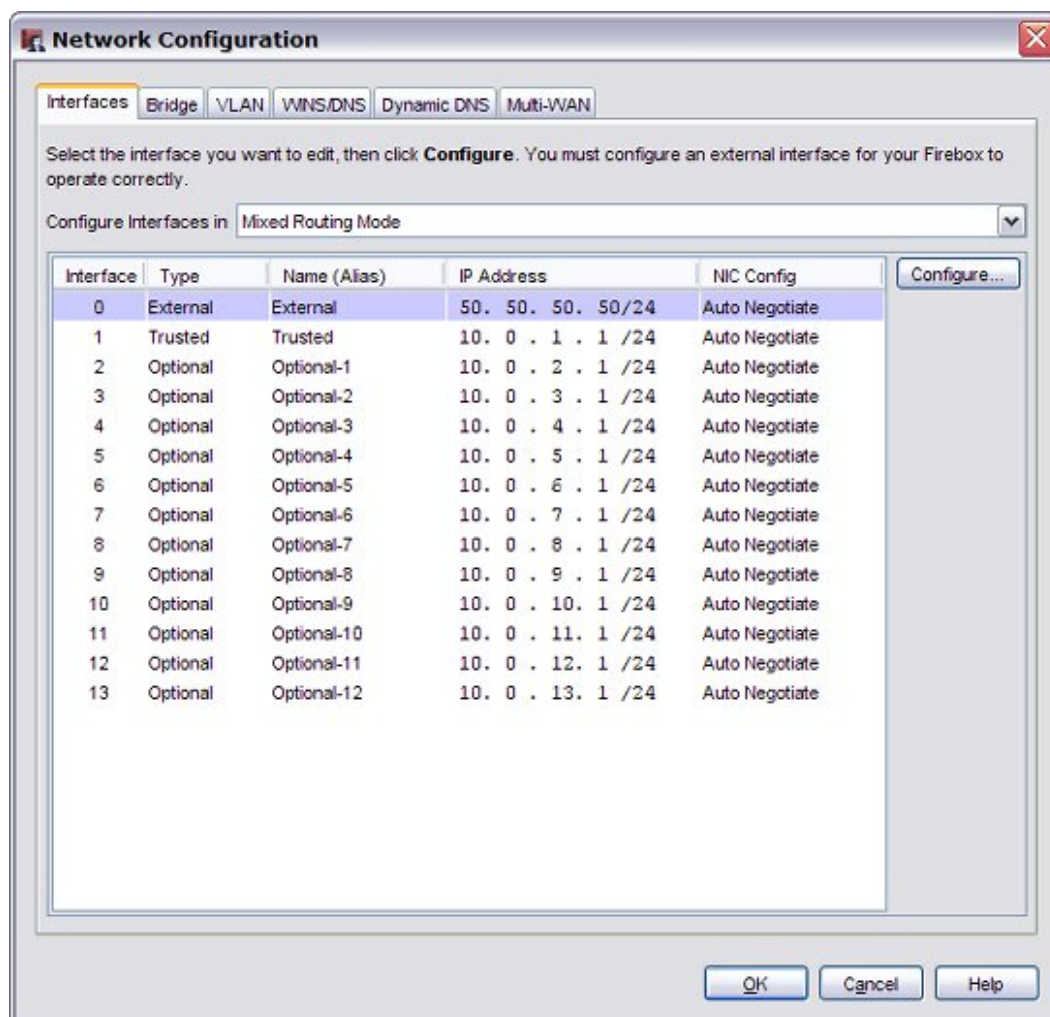
If your XTM device is configured in drop-in mode, see *Configure DHCP in Drop-In Mode* on page 100.

**Note** You cannot configure DHCP on any interface for which FireCluster is enabled.

### Configure DHCP

1. Select **Network > Configuration**.
2. Select a trusted or an optional interface. Click **Configure**.

To configure DHCP for a wireless guest network, select **Network > Wireless** and click **Configure** for the wireless guest network.



3. Select **Use DHCP Server**, or for the wireless guest network, select the **Enable DHCP Server on Wireless Guest Network** check box.

Use DHCP Server

You can configure a maximum of six address ranges.

**Address Pool**

Starting IP	Ending IP
10.0.1.2	10.0.1.254

Add  
Edit  
Delete

**Reserved Addresses:**

Reserved Name	Reservation IP	MAC Address
---------------	----------------	-------------

Add  
Edit  
Delete

Leasing Time: 8 hours

Configure DNS/WINS servers

4. To add a group of IP addresses to assign to users on this interface, in the **Address Pool** section, click **Add**. Specify starting and ending IP addresses on the same subnet, then click **OK**.  
The address pool must belong either to the interface's primary or secondary IP subnet.  
*You can configure a maximum of six address ranges. Address groups are used from first to last. Addresses in each group are assigned by number, from lowest to highest.*
5. To change the default lease time, select a different option in the **Leasing Time** drop-down list.  
*This is the time interval that a DHCP client can use an IP address that it receives from the DHCP server. When the lease time is about to expire, the client sends data to the DHCP server to get a new lease.*
6. By default, when it is configured as a DHCP server your XTM device gives out the DNS and WINS server information configured on the **Network Configuration > WINS/DNS** tab. To specify different information for your device to assign when it gives out IP addresses, click **Configure DNS/WINS servers**.
  - Type a **Domain Name** to change the default DNS domain.
  - To create a new DNS or WINS server entry, click **Add** adjacent to the server type you want, type an IP address, and click **OK**.
  - To change the IP address of the selected server, click **Edit**.
  - To remove the selected server from the adjacent list, click **Delete**.

## Configure DHCP Reservations

To reserve a specific IP address for a client:

1. Adjacent to the **Reserved Addresses** field, click **Add**.  
For a wireless guest network, click **DHCP Reservations** and then click **Add**.
2. Type a name for the reservation, the IP address you want to reserve, and the MAC address of the client's network card.
3. Click **OK**.

## About the Dynamic DNS Service

You can register the external IP address of your XTM device with the dynamic Domain Name System (DNS) service DynDNS.org. A dynamic DNS service makes sure that the IP address attached to your domain name changes when your ISP gives your device a new IP address. This feature is available in either mixed routing or drop-in network configuration mode.

If you use this feature, your XTM device gets the IP address of members.dyndns.org when it starts up. It makes sure the IP address is correct every time it restarts and at an interval of every twenty days. If you make any changes to your DynDNS configuration on your XTM device, or if you change the IP address of the default gateway, it updates DynDNS.com immediately.

For more information on the Dynamic DNS service or to create a DynDNS account, go to <http://www.dyndns.com>.

**Note** WatchGuard is not affiliated with DynDNS.com.

## Use Dynamic DNS

You can register the external IP address of your XTM device with the dynamic DNS (Domain Name System) service called Dynamic Network Services (DynDNS). This is a free service for a maximum of two host names. WatchGuard System Manager does not currently support other dynamic DNS providers.

A dynamic DNS service makes sure that the IP address attached to your domain name changes when your ISP gives your XTM device a new IP address. Your device checks the IP address of members.dyndns.org when it starts up. It makes sure the IP address is correct every time it restarts and at an interval of every twenty days. If you make any changes to your DynDNS configuration on your XTM device, or if you change the IP address of the default gateway configured for your device, your configuration at DynDNS.com is updated immediately.

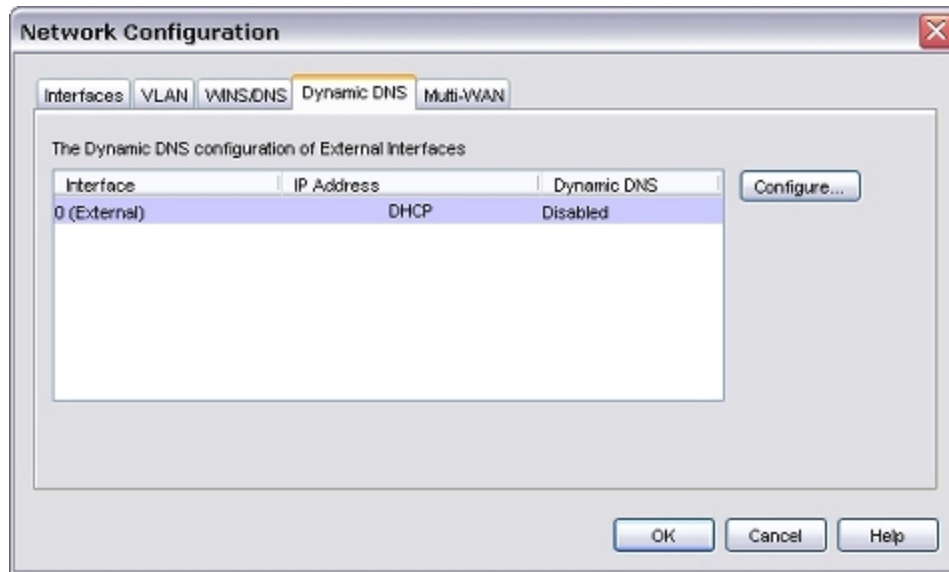
For more information on dynamic DNS, go to <http://www.dyndns.com>.

**Note** WatchGuard is not affiliated with DynDNS.com.

1. Set up a dynDNS account. Go to the DynDNS web site and follow the instructions on the site.
2. In Policy Manager, select **Network > Configuration**.
3. Select the **WIN/DNS** tab.



4. Make sure you have defined at least one DNS server. If you have not, use the procedure in *Add WINS and DNS Server Addresses* on page 111.
5. Select the **Dynamic DNS** tab.



6. Select the external interface for which you want to configure dynamic DNS and click **Configure**.  
*The Per Interface Dynamic DNS dialog box appears.*
7. To enable dynamic DNS, select the **Enable Dynamic DNS** check box.
8. Type the user name, password, and domain name you used to set up your dynamic DNS account.
9. From the **Service Type** drop-down list, select the system to use for this update:
  - **dyndns** — Sends updates for a Dynamic DNS host name. Use this option when you have no control over your IP address (for example, it is not static, and it changes on a regular basis).
  - **custom** — Sends updates for a custom DNS host name. This option is frequently used by businesses that pay to register their domain with dyndns.com.

For more information on each option, see <http://www.dyndns.com/services/>.

10. In the **Options** text box, you can type any of the subsequent options. You must type the “&” character before and after each option you add. If you add more than one option, you must separate the options with the “&” character.

For example:

```
&backmx=NO&wildcard=ON&
```

```
mx=mailexchanger
```

```
backmx=YES|NO
```

```
wildcard=ON|OFF|NOCHG
```

```
offline=YES|NO
```

For more information on options, see <http://www.dyndns.com/developers/specs/syntax.html>.

11. Use the arrows to set a time interval (in days) to force an update of the IP address.

## Drop-In Mode

In a drop-in configuration, your XTM device is configured with the same IP address on all interfaces. The drop-in configuration mode distributes the network's logical address range across all available network interfaces. You can put your XTM device between the router and the LAN and not have to change the configuration of any local computers. This configuration is known as drop-in mode because your XTM device is *dropped in* to a previously configured network.

In drop-in mode:

- You must assign the same primary IP address to all interfaces on your XTM device (external, trusted, and optional).
- You can assign secondary networks on any interface.
- You can keep the same IP addresses and default gateways for hosts on your trusted and optional networks, and add a secondary network address to the primary external interface so your XTM device can correctly send traffic to the hosts on these networks.
- The public servers behind your XTM device can continue to use public IP addresses. Network address translation (NAT) is not used to route traffic from outside your network to your public servers.

The properties of a drop-in configuration are:


- You must assign and use a static IP address on the external interface.
- You use one logical network for all interfaces.
- You cannot configure more than one external interface when your XTM device is configured in drop-in mode. Multi-WAN functionality is automatically disabled.

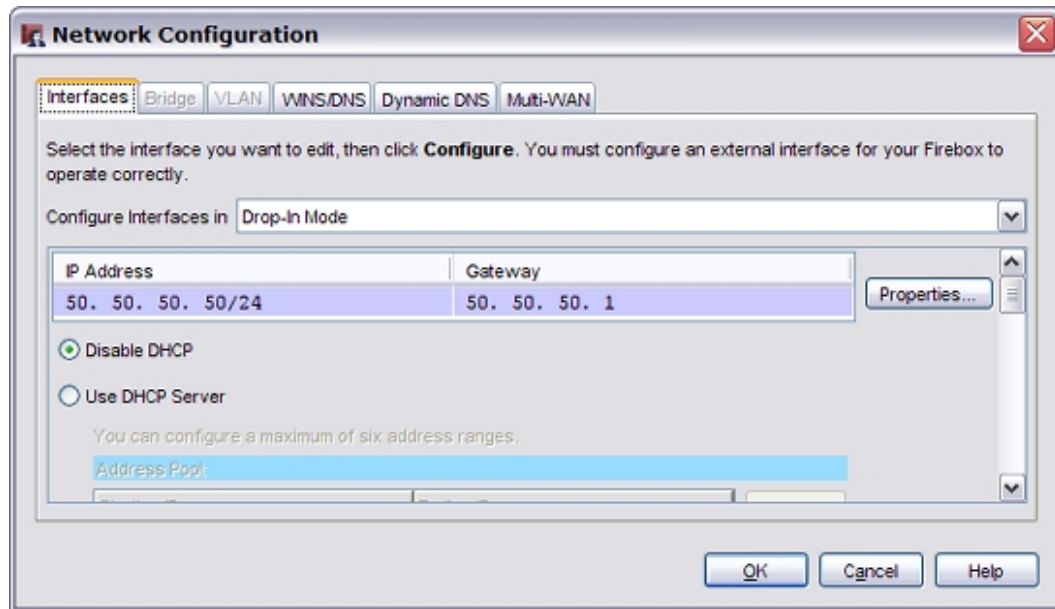
It is sometimes necessary to *Clear the ARP Cache* of each computer protected by the XTM device, but this is not common.

**Note** *If you move an IP address from a computer located behind one interface to a computer located behind a different interface, it can take several minutes before network traffic is sent to the new location. Your XTM device must update its internal routing table before this traffic can pass. Traffic types that are affected include logging, SNMP, and XTM device management connections.*

You can configure your network interfaces with drop-in mode when you run the Quick Setup Wizard. If you have already created a network configuration, you can use Policy Manager to switch to drop-in mode. For more information, see *Run the Web Setup Wizard* on page 23.

## Use Drop-In Mode for Network Interface Configuration


1. Click .  
Or, select **Network > Configuration**.  
*The Network Configuration dialog box appears.*
2. From the **Configure Interfaces in** drop-down list, select **Drop-In Mode**.
3. In the **IP Address** text box, type the IP address you want to use as the primary address for all interfaces on your XTM device.
4. In the **Gateway** text box, type the IP address of the gateway. This IP address is automatically added to the Related Hosts list.

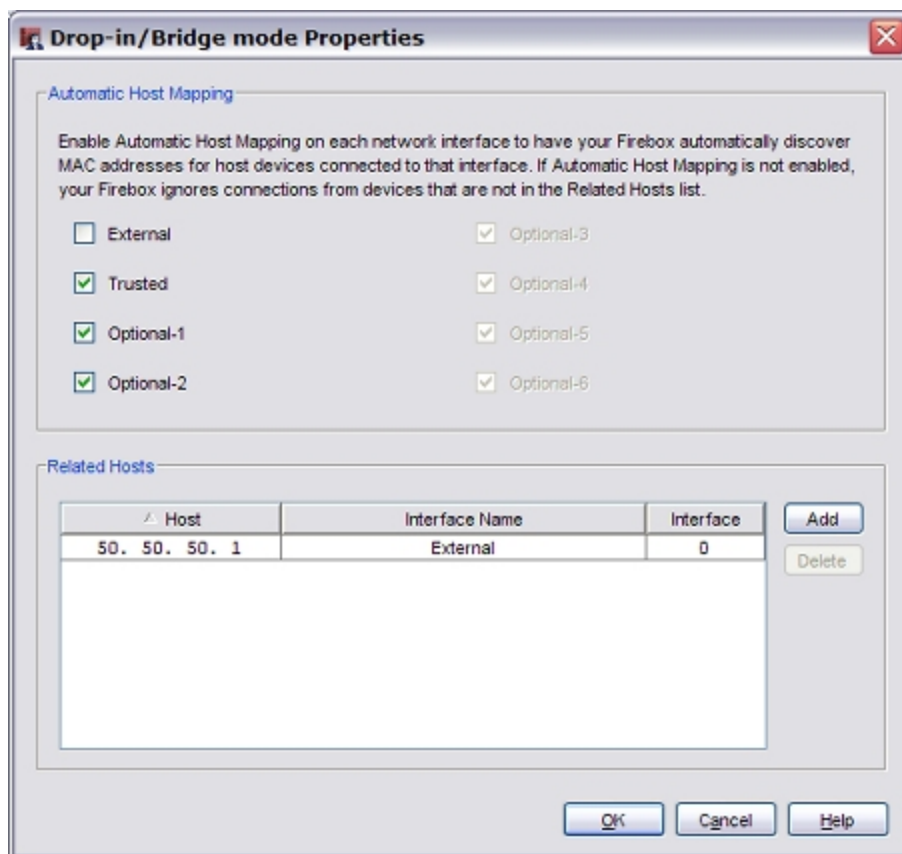


5. Click **OK**.
6. *Save the Configuration File.*

## Configure Related Hosts

In a drop-in or bridge configuration, the XTM device is configured with the same IP address on each interface. Your XTM device automatically discovers new devices that are connected to these interfaces and adds each new MAC address to its internal routing table. If you want to configure device connections manually, or if the Automatic Host Mapping feature does not operate correctly, you can add a related hosts entry. A related hosts entry creates a static route between the host IP address and one network interface. We recommend that you disable Automatic Host Mapping on interfaces for which you create a related hosts entry.

1. Click .  
Or, select **Network > Configuration**.  
*The Network Configuration dialog box appears.*
2. Configure network interfaces in drop-in or bridge mode, then click **Properties**.  
*The Drop-In Mode Properties dialog box appears.*
3. Clear the check box for any interface for which you want to add a related hosts entry.
4. Click **Add**. Type the IP address of the device for which you want to build a static route from the XTM device.
5. Click the **Interface Name** column area to select the interface for the related hosts entry.




6. Click **OK**.
7. *Save the Configuration File.*

## Configure DHCP in Drop-In Mode

When you use drop-in mode for network configuration, you can use Policy Manager to optionally configure the XTM device as a DHCP server for networks it protects, or make the XTM device a DHCP relay agent. If you have a configured DHCP server, we recommend that you continue to use that server for DHCP.

### Use DHCP

1. Click .
 

Or, select **Network > Configuration**.

*The Network Configuration dialog box appears.*
2. If your XTM device is not already configured in drop-in mode, from the **Configure Interfaces in** drop-down list select **Drop-In Mode**.

**Use DHCP Server**

You can configure a maximum of six address ranges.

**Address Pool**

Starting IP	Ending IP
50.50.50.100	50.50.50.200

**Reserved Addresses:**


Reserved Name	Reservation IP	MAC Address
---------------	----------------	-------------

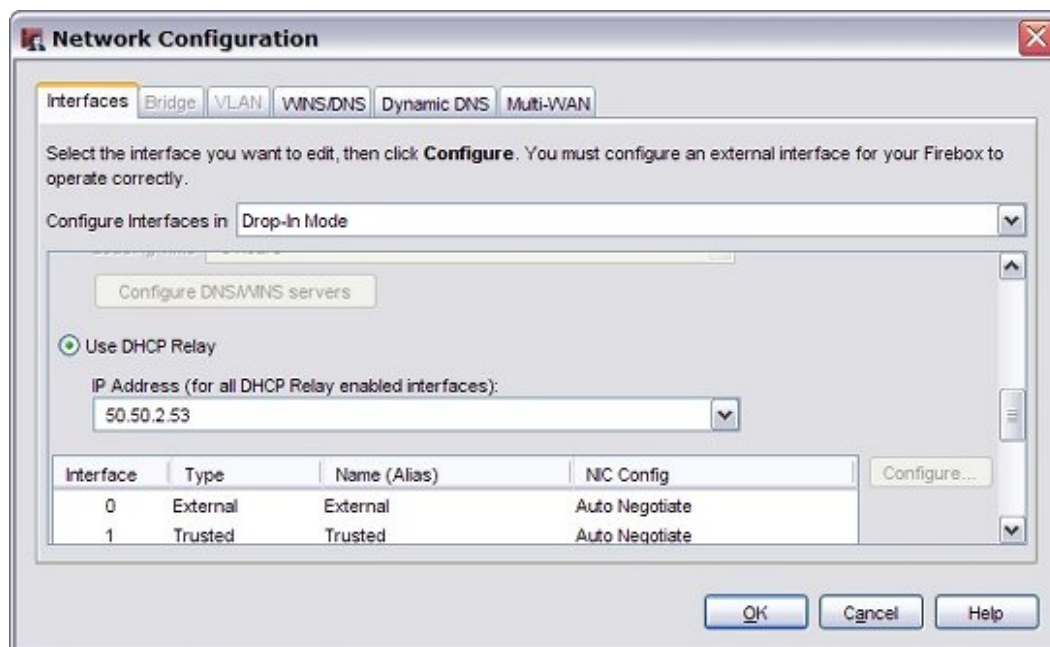
Leasing Time: 8 hours

Configure DNS/WINS servers

3. Select **Use DHCP Server**.
4. To add an address pool from which your XTM device can give out IP addresses, click **Add** next to the **Address Pool** box and specify starting and ending IP addresses that are on the same subnet as the drop-in IP address.  
Do not include the drop-in IP address in the address pool. Click **OK**.  
*You can configure a maximum of six address ranges.*
5. To reserve a specific IP address from an address pool for a device or client, adjacent to the **Reserved Addresses** field, click **Add**. Type a name to identify the reservation, the IP address you want to reserve, and the MAC address for the device. Click **OK**.
6. In the **Leasing Time** drop-down list, select the maximum amount of time that a DHCP client can use an IP address.
7. By default, your XTM device gives out the DNS/WINS server information configured on the **Network Configuration > WINS/DNS** tab when it is configured as a DHCP server. To send different DNS/WINS server information to DHCP clients, click the **Configure DNS/WINS servers** button.
8. Click **OK**.
9. *Save the Configuration File.*

## Use DHCP Relay

1. Click .  
Or, select **Network > Configuration**.  
*The Network Configuration dialog box appears.*
2. Select **Use DHCP Relay**.



3. Type the IP address of the DHCP server in the related field. Make sure to *Add a Static Route* to the DHCP server, if necessary.
4. Click **OK**.
5. *Save the Configuration File.*

### Specify DHCP Settings for a Single Interface

You can specify different DHCP settings for each trusted or optional interface in your configuration.

1. Click .
 

Or, select **Network > Configuration**.

*The Network Configuration dialog box appears.*
2. Scroll to the bottom of the **Network Configuration** dialog box and select an interface.
3. Click **Configure**.
4. Update the DHCP settings:
  - To use the same DHCP settings that you configured for drop-in mode, select **Use System DHCP Setting**.
  - To disable DHCP for clients on that network interface, select **Disable DHCP**.
  - To configure different DHCP options for clients on a secondary network, select **Use DHCP Server for Secondary Network**. Complete Steps 3–6 of the *Use DHCP relay* procedure to add IP address pools, set the default lease time, and manage DNS/WINS servers.
5. Click **OK**.

## Bridge Mode

Bridge mode is a feature that allows you to install your XTM device between an existing network and its gateway to filter or manage network traffic. When you enable this feature, your XTM device processes and forwards all network traffic to other gateway devices. When the traffic arrives at a gateway from the XTM device, it appears to have been sent from the original device.

To use bridge mode, you must specify an IP address that is used to manage your XTM device. The device also uses this IP address to get Gateway AV/IPS updates and to route to internal DNS, NTP, or WebBlocker servers as necessary. Because of this, make sure you assign an IP address that is routable on the Internet.

In bridge mode, L2 and L3 headers are not changed. If you want traffic on the same physical interface of a XTM device to pass through the device, you cannot use bridge mode. In this case, you must use drop-in or mixed routing mode, and set the default gateway of those computers to be the XTM device itself.


When you use bridge mode, your XTM device cannot complete some functions that require the device to operate as a gateway. These functions include:

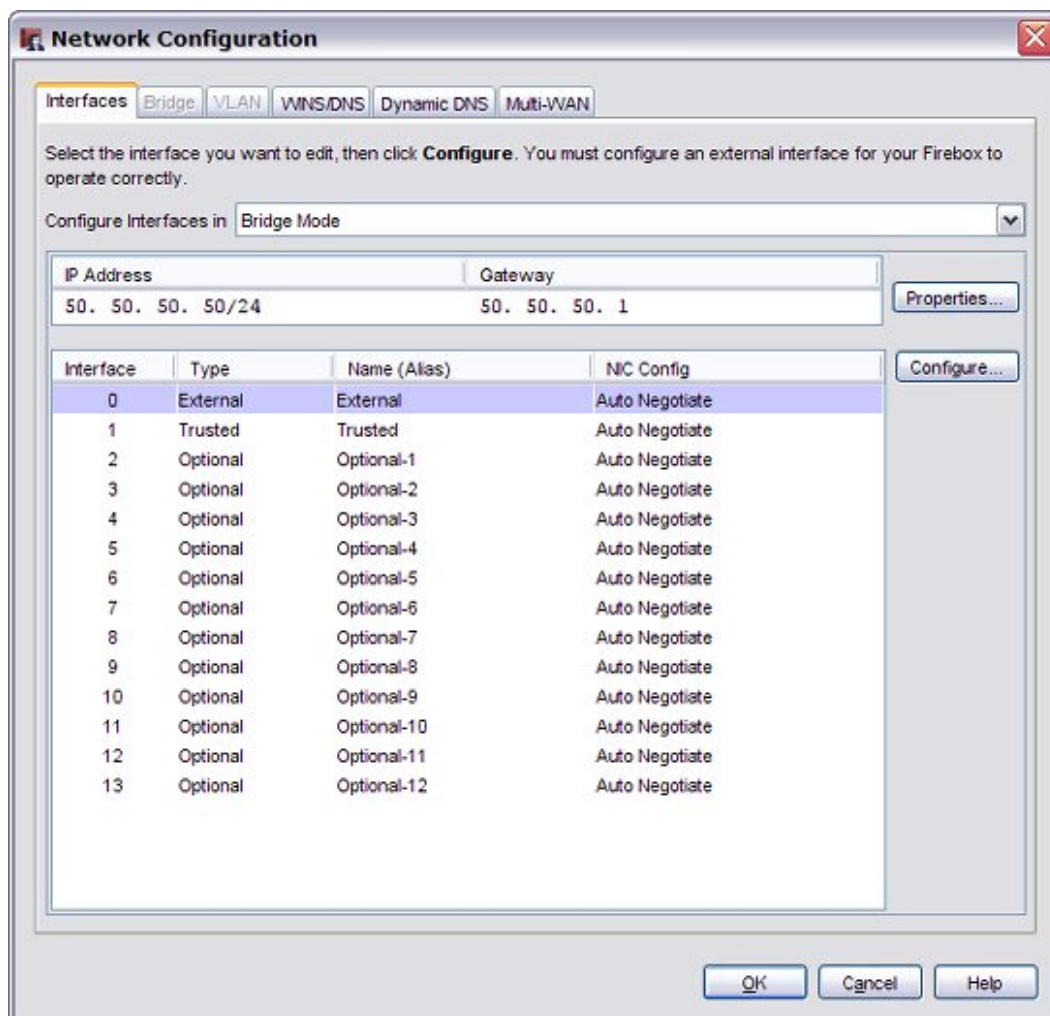
- Multi-WAN
- VLANs (Virtual Local Area Networks)
- Network bridges
- Static routes
- FireCluster
- Secondary networks
- DHCP server or DHCP relay
- Serial modem failover (XTM 2 Series only)
- 1-to-1, dynamic, or static NAT
- Dynamic routing (OSPF, BGP, or RIP)
- Any type of VPN for which the XTM device is an endpoint or gateway
- Some proxy functions, including HTTP Web Cache Server

If you have previously configured these features or services, they are disabled when you switch to bridge mode. To use these features or services again, you must use a different network mode. If you return to drop-in or mixed routing mode, you might have to configure some features again.

**Note** *When you enable bridge mode, any interfaces with a previously configured network bridge or VLAN are disabled. To use those interfaces, you must first change to either drop-in or mixed routing mode, and configure the interface as External, Optional, or Trusted, then return to bridge mode. Wireless features on XTM wireless devices operate correctly in bridge mode.*

To enable bridge mode:

1. Click .  
Or, select **Network > Configuration**.  
*The Network Configuration window appears.*
2. From the **Configure Interfaces In** drop-down list, select **Bridge Mode**.



3. If you are prompted to disable interfaces, click **Yes** to disable the interfaces, or **No** to return to your previous configuration.
4. Type the **IP Address** of your XTM device in slash notation.  
For more information on slash notation, see *About Slash Notation* on page 3.
5. Type the **Gateway** IP address that receives all network traffic from the device.
6. Click **OK**.
7. *Save the Configuration File.*

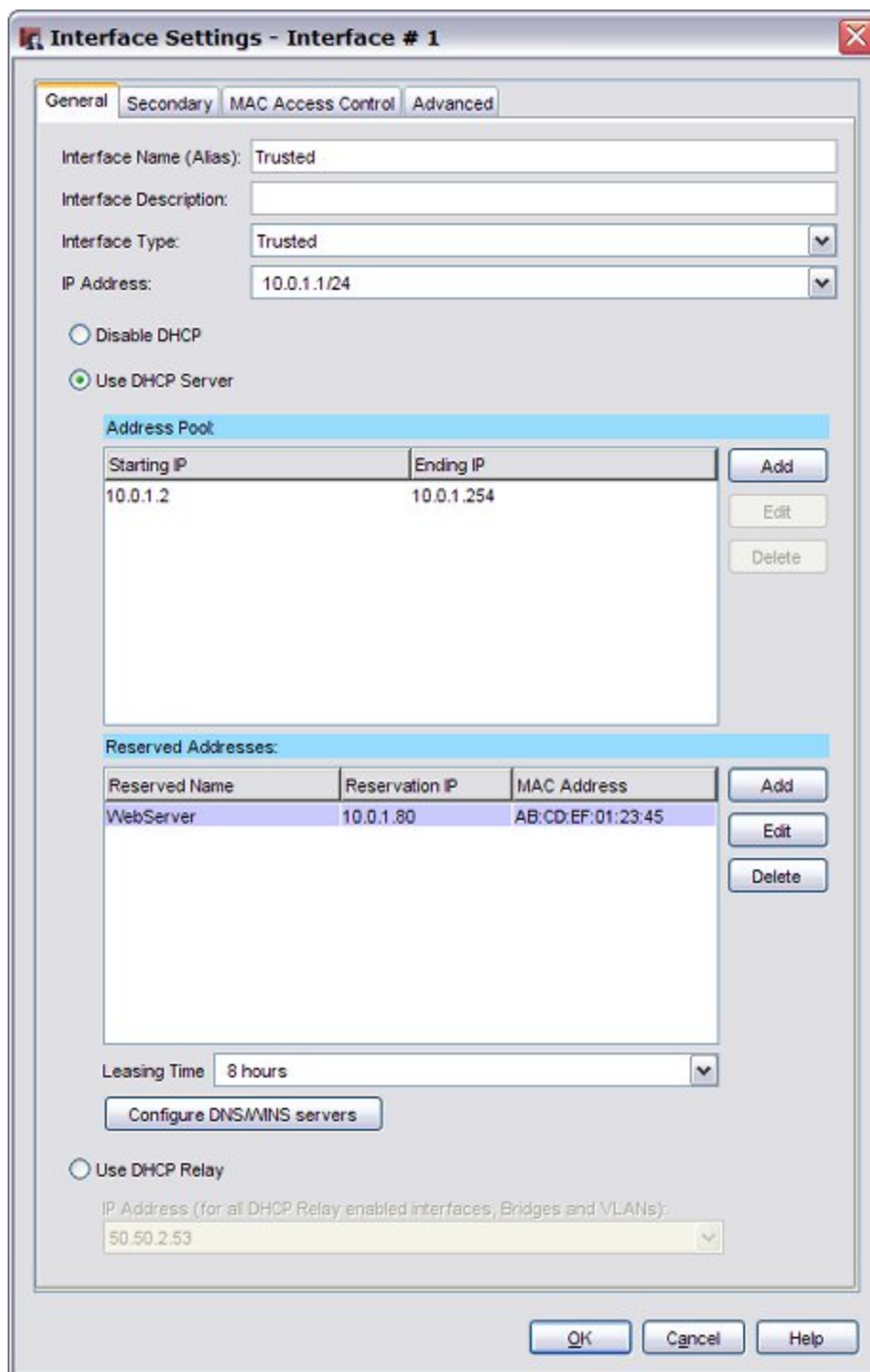


## Common Interface Settings

With mixed routing mode, you can configure your XTM device to send network traffic between a wide variety of physical and virtual network interfaces. This is the default network mode, and it offers the greatest amount of flexibility for different network configurations. However, you must configure each interface separately, and you may have to change network settings for each computer or client protected by your XTM device.

To configure your XTM device with mixed routing mode:

1. Select **Network > Configuration**.  
*The Network Configuration dialog box appears.*
2. Select the interface you want to configure, then click **Configure**. The options available depend on the type of interface you selected.  
*The Interface Settings dialog box appears.*

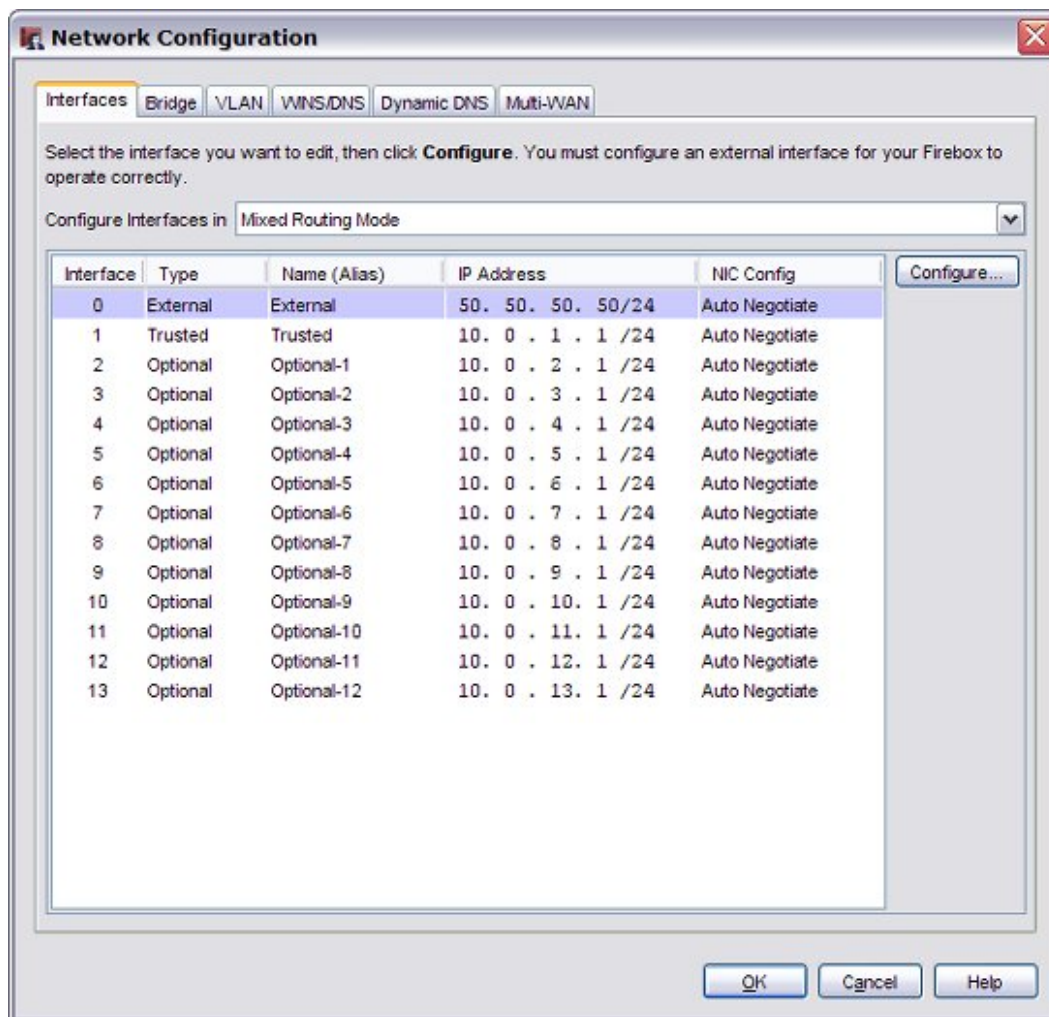


3. In the **Interface Name (Alias)** text box, you can retain the default name or change it to one that more closely reflects your own network and its own trust relationships. Make sure the name is unique among interface names as well as all MVPN group names and tunnel names. You can use this alias with other features, such as proxy policies, to manage network traffic for this interface.
4. (Optional) Enter a description of the interface in the **Interface Description** text box.

5. In the **Interface Type** drop-down list, you can change the interface type from its default value. You can select **External, Trusted, Optional, Bridge, Disabled, or VLAN**. Some interface types have additional settings.
  - For more information about how to assign an IP address to an external interface, see *Configure an External Interface* on page 90. To set the IP address of a trusted or optional interface, type the IP address in slash notation.
  - To assign IP addresses automatically to clients on a trusted or optional interface, see *Configure DHCP in Mixed Routing Mode* on page 94 or *Configure DHCP Relay* on page 110.
  - To use more than one IP address on a single physical network interface, see *Configure a Secondary Network* on page 112.
  - For more information about VLAN configurations, see *About Virtual Local Area Networks (VLANs)* on page 124.
  - To remove an interface from your configuration, see *Disable an Interface* on page 108.
6. Configure your interface as described in one of the above topics.
7. Click **OK**.

## Disable an Interface

1. Select **Network > Configuration**.  
*The Network Configuration dialog box appears.*



2. Select the interface you want to disable. Click **Configure**.  
*The Interface Settings dialog box appears.*



3. From the **Interface Type** drop-down list, select **Disabled**. Click **OK**.

## Configure DHCP Relay

One way to get IP addresses for the computers on the trusted or optional networks is to use a DHCP server on a different network. You can use DHCP relay to get IP addresses for the computers on the trusted or optional network. With this feature, the XTM device sends DHCP requests to a server on a different network.

If the DHCP server you want to use is not on a network protected by your XTM device, you must set up a VPN tunnel between your XTM device and the DHCP server for this feature to operate correctly.

**Note** *You cannot use DHCP relay on any interface on which FireCluster is enabled.*

To configure DHCP relay:

1. Select **Network > Configuration**.  
*The Network Configuration dialog box appears.*
2. Select a trusted or an optional interface and click **Configure**.
3. Select **Use DHCP Relay**.
4. Type the IP address of the DHCP server in the related field. Make sure to *Add a Static Route* to the DHCP server, if necessary.
5. Click **OK**.

## Restrict Network Traffic by MAC Address

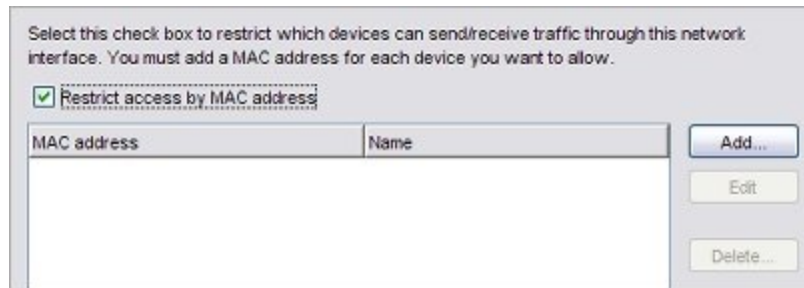
You can use a list of MAC addresses to manage which devices are allowed to send traffic on the network interface you specify. When you enable this feature, your XTM device checks the MAC address of each computer or device that connects to the specified interface. If the MAC address of that device is not on the MAC Access Control list for that interface, the device cannot send traffic.

This feature is especially helpful to prevent any unauthorized access to your network from a location within your office. However, you must update the MAC Address Control list for each interface when a new, authorized computer is added to the network.

**Note** *If you choose to restrict access by MAC address, you must include the MAC address for the computer you use to administer your XTM device.*

To enable MAC Access Control for a network interface:

1. Select **Network > Configuration**.  
*The Network Configuration window appears.*
2. Select the interface on which you want to enable MAC Access Control, then click **Configure**.  
*The Interface Settings window appears.*
3. Select the **MAC Access Control** tab.



4. Select the **Restrict access by MAC address** check box.
5. Click **Add**.

*The Add a MAC address window appears.*

6. Type the **MAC address** of the computer or device to give it access to the specified interface.
7. (Optional) Type a **Name** for the computer or device to identify it in the list.
8. Click **OK**.

*Repeat steps 5–8 to add more computers or devices to the MAC Access Control list.*

## Add WINS and DNS Server Addresses

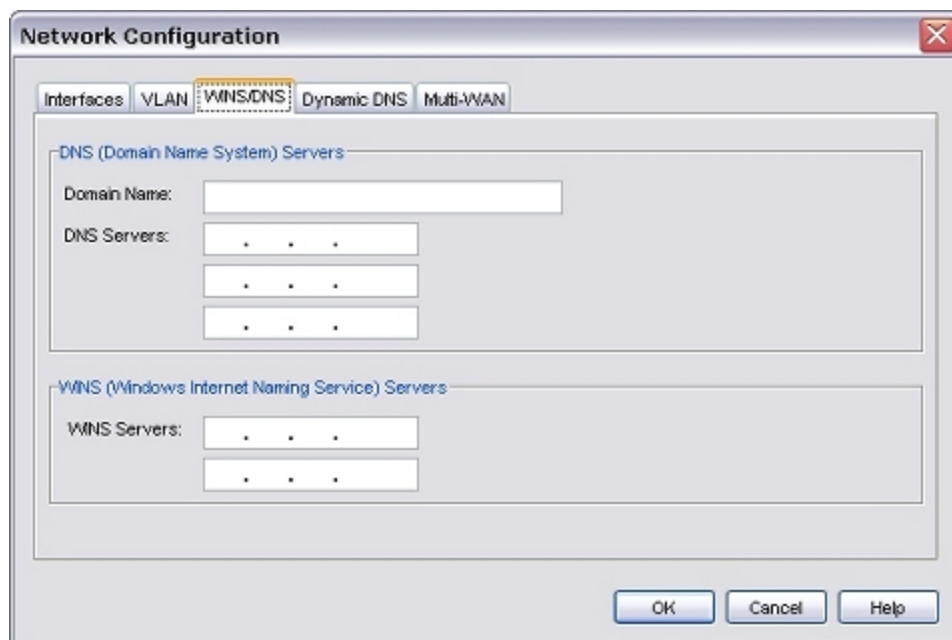
A number of the features of the XTM device have shared Windows Internet Name Server (WINS) and Domain Name System (DNS) server IP addresses. These features include DHCP and Mobile VPN. Access to these servers must be available from the trusted interface of the XTM device.

This information is used for two purposes:

- The XTM device uses the DNS server shown here to resolve names to IP addresses for IPSec VPNs and for the spamBlocker, Gateway AV, and IPS features to operate correctly.
- The WINS and DNS entries are used by DHCP clients on the trusted or optional networks, and by Mobile VPN users to resolve DNS queries.

Make sure that you use only an internal WINS and DNS server for DHCP and Mobile VPN. This helps to make sure that you do not create policies that have configuration properties that prevent users from connecting to the DNS server.

1. Select **Network > Configuration**.
- The Network Configuration dialog box appears.*
2. Select the **WINS/DNS** tab.
- The information on the WINS/DNS tab appears.*



3. Type the primary and secondary addresses for the WINS and DNS servers. You can specify up to three DNS servers. You can also type a domain suffix in the **Domain Name** text box for a DHCP client to use with unqualified names such as "watchguard\_mail".

## Configure a Secondary Network

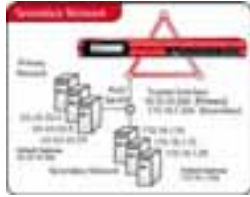
A secondary network is a network that shares one of the same physical networks as one of the XTM device interfaces. When you add a secondary network, you make (or add) an IP alias to the interface. This IP alias is the default gateway for all the computers on the secondary network. The secondary network tells the XTM device that there is one more network on the XTM device interface.

For example, if you configure an XTM device in drop-in mode, you give each XTM device interface the same IP address. However, you probably use a different set of IP addresses on your trusted network. You can add this private network as a secondary network to the trusted interface of your XTM device. When you add a secondary network, you create a route from an IP address on the secondary network to the IP address of the XTM device interface.

If your XTM device is configured with a static IP address on an external interface, you can also add an IP address on the same subnet as your primary external interface as a secondary network. You can then configure static NAT for more than one of the same type of server. For example, configure an external secondary network with a second public IP address if you have two public SMTP servers and you want to configure a static NAT rule for each.

You can add up to 2048 secondary networks per XTM device interface. You can use secondary networks with either a drop-in or a routed network configuration. You can also add a secondary network to an external interface of an XTM device if that external interface is configured to get its IP address through PPPoE or DHCP.



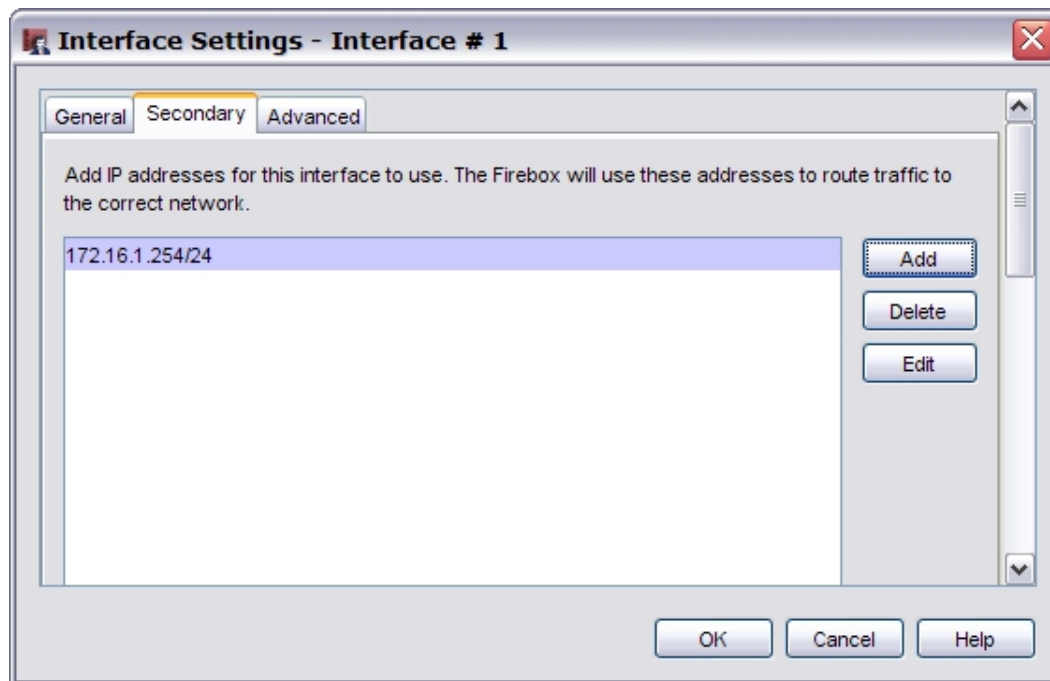


To define a secondary IP address, you must have:

- An unused IP address on the secondary network to assign to the XTM device interface
- An unused IP address on the same network as the XTM device external interface

To define a secondary IP address:

1. Select **Network > Configuration**.  
*The Network Configuration dialog box appears.*
2. Select the interface for the secondary network and click **Configure**.  
*The Interface Settings dialog box appears.*
3. Select the **Secondary** tab.
4. Click **Add**. Type an unassigned host IP address from the secondary network.
5. Click **OK**.
6. Click **OK** again.



**Note** Make sure to add secondary network addresses correctly. The XTM device does not tell you if the address is correct. We recommend that you do not create a subnet as a secondary network on one interface that is a component of a larger network on a different interface. If you do this, spoofing can occur and the network cannot operate correctly.

## About Advanced Interface Settings

You can use several advanced settings for XTM device interfaces:

### *Network Interface Card (NIC) Settings*

Configures the speed and duplex parameters for XTM device interfaces to automatic or manual configuration. We recommend you keep the link speed configured for automatic negotiation. If you use the manual configuration option, you must make sure the device the XTM device connects to is also manually set to the same speed and duplex parameters as the XTM device. Use the manual configuration option only when you must override the automatic XTM device interface parameters to operate with other devices on your network.

### *Set Outgoing Interface Bandwidth*

When you use Traffic Management settings to guarantee bandwidth to policies, this setting makes sure that you do not guarantee more bandwidth than actually exists for an interface. This setting also helps you make sure the sum of guaranteed bandwidth settings does not fill the link such that non-guaranteed traffic cannot pass.

### *Enable QoS Marking for an Interface*

Creates different classifications of service for different kinds of network traffic. You can set the default marking behavior as traffic goes out of an interface. These settings can be overridden by settings defined for a policy.

### *Set DF Bit for IPSec*

Determines the setting of the Don't Fragment (DF) bit for IPSec.

### *PMTU Setting for IPSec*

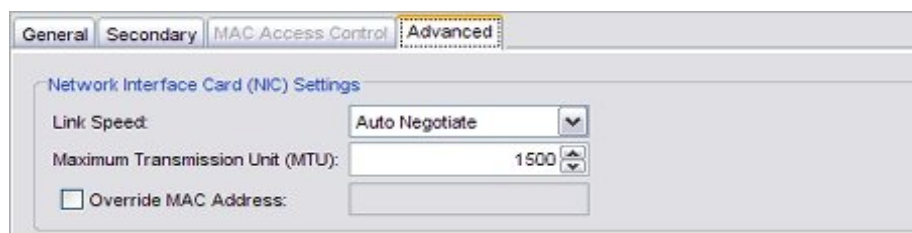
(External interfaces only) Controls the length of time that the XTM device lowers the MTU for an IPSec VPN tunnel when it gets an ICMP Request to Fragment packet from a router with a lower MTU setting on the Internet.

### *Use Static MAC Address Binding*

Uses computer hardware (MAC) addresses to control access to an XTM device interface.

## Network Interface Card (NIC) Settings

1. Select **Network > Configuration**.
2. Click the interface you want to configure, and then click **Configure**.
3. Select the **Advanced** tab.



4. In the **Link Speed** drop-down list, select **Auto Negotiate** if you want the XTM device to select the best network speed. You can also select one of the half-duplex or full-duplex speeds that you know is compatible with your other network equipment.

**Auto Negotiate** is the default setting. We strongly recommend that you do not change this setting unless instructed to do so by Technical Support. If you set the link speed manually and other devices on your network do not support the speed you select, this can cause a conflict that does not allow your XTM device interface to reconnect after failover.

5. In the **Maximum Transmission Unit (MTU)** text box, select the maximum packet size, in bytes, that can be sent through the interface. We recommend that you use the default, 1500 bytes, unless your network equipment requires a different packet size.

*You can set the MTU from a minimum of 68 to a maximum of 9000.*

6. To change the MAC address of the external interface, select the **Override MAC Address** check box and type the new MAC address.

For more information about MAC addresses, see the subsequent section.

7. Click **OK**.
8. *Save the Configuration File.*

## About MAC Addresses

Some ISPs use a MAC address to identify the computers on their network. Each MAC address gets one static IP address. If your ISP uses this method to identify your computer, then you must change the MAC address of the XTM device external interface. Use the MAC address of the cable modem, DSL modem, or router that connected directly to the ISP in your original configuration.

The MAC address must have these properties:

- The MAC address must use 12 hexadecimal characters. Hexadecimal characters have a value between 0 and 9 or between "a" and "f."
- The MAC address must operate with:
  - One or more addresses on the external network.
  - The MAC address of the trusted network for the device.
  - The MAC address of the optional network for the device.
- The MAC address must not be set to 000000000000 or ffffffff.

If the **Override MAC Address** check box is not selected when the XTM device is restarted, the device uses the default MAC address for the external network.

To decrease problems with MAC addresses, the XTM device makes sure that the MAC address you assign to the external interface is unique on your network. If the XTM device finds a device that uses the same MAC address, the XTM device changes back to the standard MAC address for the external interface and starts again.

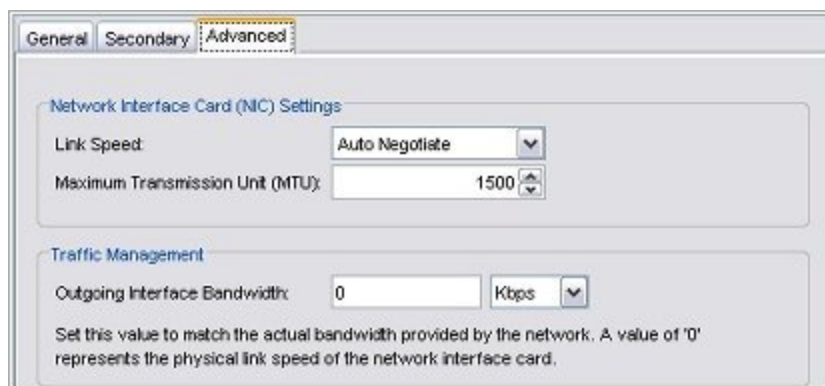
## Set Outgoing Interface Bandwidth

Some traffic management features require that you set a bandwidth limit for each network interface. For example, you must configure the **Outgoing Interface Bandwidth** setting to use QoS marking and prioritization.

After you set this limit, your XTM device completes basic prioritization tasks on network traffic to prevent problems with too much traffic on the specified interface. Also, a warning appears in Policy Manager if you allocate too much bandwidth as you create or adjust traffic management actions.

If you do not change the **Outgoing Interface Bandwidth** setting for any interface from the default value of 0, it is set to the auto-negotiated link speed for that interface.

1. Select **Network > Configuration**.  
*The Network Configuration dialog box appears.*
2. Select the interface for which you want to set bandwidth limits and click **Configure**.  
*The Interface Settings dialog box appears.*
3. Select the **Advanced** tab.



4. In the **Outgoing Interface Bandwidth** text box, type the amount of bandwidth provided by the network. Use your Internet connection upload speed (in Kbps rather than KBps) as the limit for external interfaces. Set your LAN interface bandwidth based on the minimum link speed supported by your LAN infrastructure.
5. Click **OK**.
6. Click **OK** again.
7. *Save the Configuration File.*

## Set DF Bit for IPSec

When you configure the external interface, select one of the three options to determine the setting for the **Don't Fragment (DF) bit for IPSec** section.

Don't Fragment (DF) Bit Setting for IPSec (Applicable to External only)

- Copy** - Original DF bit setting of the IPSec packet is copied to the encapsulating header
- Set** - Firebox cannot fragment IPSec packets regardless of the original bit setting
- Clear** - Firebox can fragment IPSec packets regardless of the original bit setting

### Copy

Select **Copy** to apply the DF bit setting of the original frame to the IPSec encrypted packet. If a frame does not have the DF bits set, Fireware XTM does not set the DF bits and fragments the packet if needed. If a frame is set to not be fragmented, Fireware XTM encapsulates the entire frame and sets the DF bits of the encrypted packet to match the original frame.

### Set

Select **Set** if you do not want your XTM device to fragment the frame regardless of the original bit setting. If a user must make IPSec connections to a XTM device from behind a different XTM device, you must clear this check box to enable the IPSec pass-through feature. For example, if mobile employees are at a customer location that has a XTM device, they can make IPSec connections to their network with IPSec. For your local XTM device to correctly allow the outgoing IPSec connection, you must also add an IPSec policy.

### Clear

Select **Clear** to break the frame into pieces that can fit in an IPSec packet with the ESP or AH header, regardless of the original bit setting.

## PMTU Setting for IPSec

This advanced interface setting applies to external interfaces only.

PMTU Setting for IPSec (Applicable to External only)

Minimum MTU  Bytes

Aging time of learned PMTU

The Path Maximum Transmission Unit (PMTU) setting controls the length of time that the XTM device lowers the MTU for an IPSec VPN tunnel when it gets an ICMP Request to Fragment packet from a router with a lower MTU setting on the Internet.

We recommend that you keep the default setting. This can protect you from a router on the Internet with a very low MTU setting.

## Use Static MAC Address Binding

You can control access to an interface on your XTM device by computer hardware (MAC) address. This feature can protect your network from ARP poisoning attacks, in which hackers try to change the MAC address of their computers to match a real device on your network. To use MAC address binding, you must associate an IP address on the specified interface with a MAC address. If this feature is enabled, computers with a specified MAC address can only send and receive information with the associated IP address.

You can also use this feature to restrict all network traffic to devices that match the MAC and IP addresses on this list. This is similar to the MAC access control feature.

For more information, see *Restrict Network Traffic by MAC Address* on page 110.

**Note** *If you choose to restrict network access by MAC address binding, make sure that you include the MAC address for the computer you use to administer your XTM device.*

To configure the static MAC address binding settings:

1. Select **Network > Configuration**. Select an interface, then click **Configure**.
2. Select the **Advanced** tab.
3. Adjacent to the **Static MAC/IP Address Binding** table, click **Add**.

4. Adjacent to the **IP Address** field, click **Add**.
5. Type an IP address and MAC address pair. Click **OK**. Repeat this step to add additional pairs.
6. If you want this interface to pass only traffic that matches an entry in the **Static MAC/IP Address Binding** list, select the **Only allow traffic sent from or to these MAC/IP addresses** check box.

If you do not want to block traffic that does not match an entry in the list, clear this check box.

## Find the MAC Address of a Computer

A MAC address is also known as a hardware address or an Ethernet address. It is a unique identifier specific to the network card in the computer. A MAC address is usually shown in this form: XX-XX-XX-XX-XX-XX, where each X is a digit or letter from A to F. To find the MAC address of a computer on your network:

1. From the command line of the computer whose MAC address you want to find, type `ipconfig /all` (Windows) or `ifconfig` (OS X or Linux).
2. Look for the entry for the computer's "physical address." This value is the MAC or hardware address for the computer.

## About LAN Bridges

A network bridge makes a connection between multiple physical network interfaces on your XTM device. A bridge can be used in the same ways as a normal physical network interface. For example, you can configure DHCP to give IP addresses to clients on a bridge, or use it as an alias in firewall policies.


To use a bridge, you must:

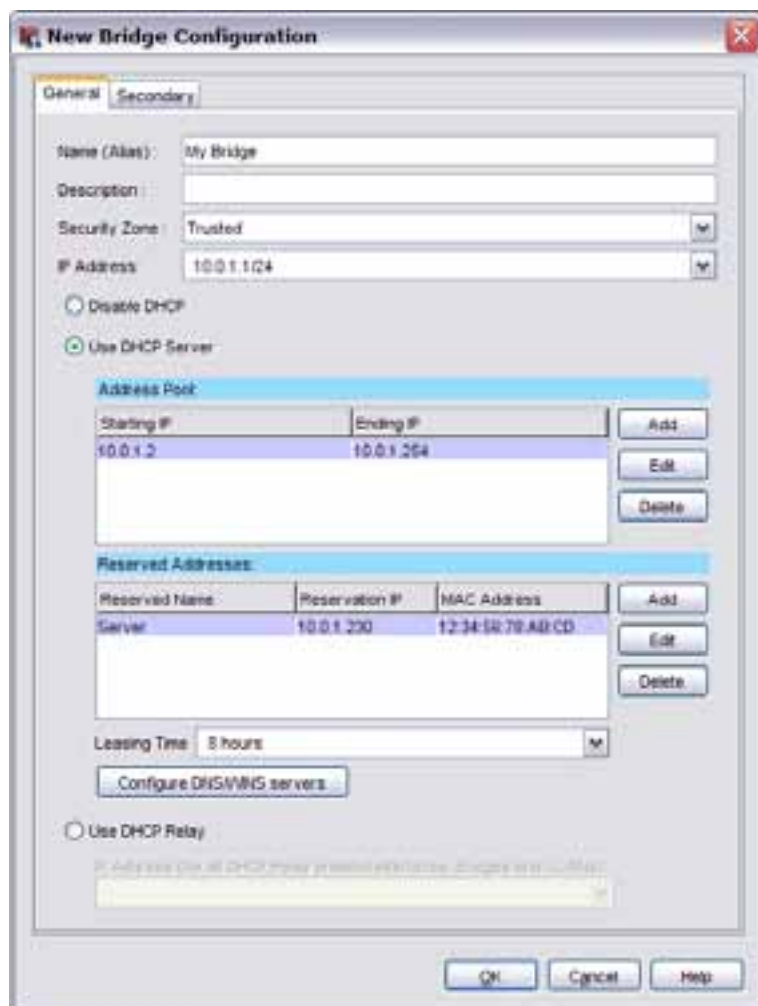
1. *Create a Network Bridge Configuration.*
2. *Assign a Network Interface to a Bridge.*

If you want to bridge all traffic between two interfaces, we recommend that you use bridge mode for your network configuration.

## Create a Network Bridge Configuration

To use a bridge, you must create a bridge configuration and assign one or more network interfaces to the bridge.

1. Click .  
Or, select **Network > Configuration**.  
*The Network Configuration dialog box appears.*
2. Select the **Bridge** tab.
3. Click **Add**.  
*The New Bridge Configuration dialog box appears.*



4. Type a **Name** or **Alias** for the new bridge. This name is used to identify the bridge in network interface configurations. You can also type a **Description** for more information.
5. From the **Security Zone** list, select **Trusted** or **Optional**. The bridge is added to the alias of the zone you specify.


For example, if you choose the Optional security zone, the bridge is added to the Any-Optional network alias.

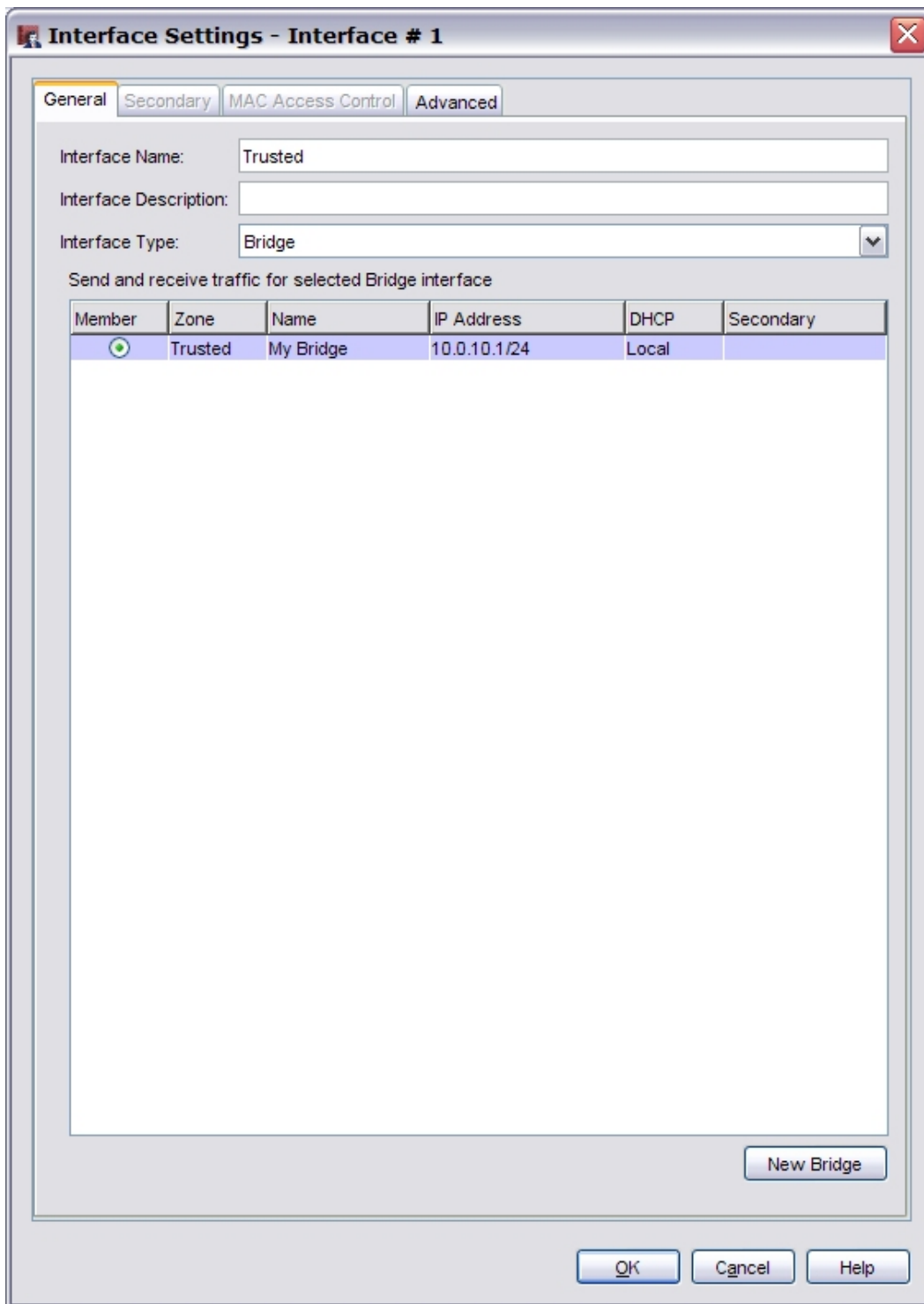
6. Type an **IP address** in slash notation for the bridge to use.  
For more information, see *About Slash Notation* on page 3.
7. Select **Disable DHCP**, **Use DHCP Server**, or **Use DHCP Relay** to set the method of IP address distribution for the bridge. If necessary, configure your DHCP server, DHCP relay, and DNS/WINS server settings.  
For more information on DHCP configuration, see *Configure DHCP in Mixed Routing Mode* on page 94 and *Configure DHCP Relay* on page 110.
8. Select the **Secondary** tab to create one or more secondary network IP addresses.  
For more information on secondary networks, see *Configure a Secondary Network* on page 112.
9. Click **OK**.



## Assign a Network Interface to a Bridge

To use a bridge, you must create a bridge configuration and assign it to one or more network interfaces. You can create the bridge configuration in the **Network Configuration** dialog box, or when you configure a network interface.

1. Click .  
Or, select **Network > Configuration**.  
*The Network Configuration window appears.*
2. Select the interface that you want to add to the bridge, then click **Configure**.  
*The Interface Configuration - Interface # window appears.*



3. In the **Interface Type** drop-down list, select **Bridge**.
4. Select the radio button adjacent to the network bridge configuration you created, or click **New Bridge** to create a new bridge configuration.
5. Click **OK**.

## About Routing

A *route* is the sequence of devices through which network traffic is sent. Each device in this sequence, usually called a *router*, stores information about the networks it is connected to inside a *route table*. This information is used to forward the network traffic to the next router in the route.

Your XTM device automatically updates its route table when you change network interface settings, when a physical network connection fails, or when it is restarted. To update the route table at other times, you must use *dynamic routing* or add a *static route*. Static routes can improve performance, but if there is a change in the network structure or if a connection fails, network traffic cannot get to its destination. Dynamic routing ensures that your network traffic can reach its destination, but it is more difficult to set up.

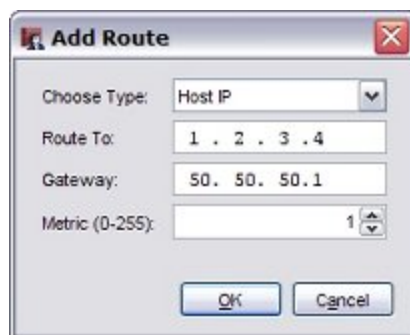
## Add a Static Route

A *route* is the sequence of devices through which network traffic must go to get from its source to its destination. A *router* is the device in a route that finds the subsequent network point through which to send the network traffic to its destination. Each router is connected to a minimum of two networks. A packet can go through a number of network points with routers before it gets to its destination.

You can create *static routes* to send traffic to specific hosts or networks. The router can then send the traffic to the correct destination from the specified route. Add a network route if you have a full network behind a router on your local network. If you do not add a route to a remote network, all traffic to that network is sent to the XTM device default gateway.

Before you start, you must understand the difference between a network route and a host route. A network route is a route to a full network behind a router located on your local network. Use a host route if there is only one host behind the router, or if you want traffic to go to only one host.

1. Select **Network > Routes**.  
*The Setup Routes dialog box appears.*
2. Click **Add**.  
*The Add Route dialog box appears.*



3. In the **Choose Type** drop-down list, select **Network IP** if you have a full network behind a router on your local network. Select **Host IP** if only one host is behind the router or you want traffic to go to only one host.
4. In the **Route To** field, type the network address or host address. If you type a network address, use slash notation.

For more information about slash notation, see *About Slash Notation* on page 3.

5. In the **Gateway** field, type the IP address of the router. Make sure that you type an IP address that is on one of the same networks as the XTM device.
6. Type a **Metric** for the route. Routes with lower metrics have higher priority.
7. Click **OK** to close the **Add Route** dialog box.

*The Setup Routes dialog box shows the configured network route.*

8. Click **OK** to close the **Setup Routes** dialog box.

## About Virtual Local Area Networks (VLANs)

An 802.1Q VLAN (virtual local area network) is a collection of computers on a LAN or LANs that are grouped together in a single broadcast domain independent of their physical location. This enables you to group devices according to traffic patterns, instead of physical proximity. Members of a VLAN can share resources as if they were connected to the same LAN. You can also use VLANs to split a switch into multiple segments. For example, suppose your company has full-time employees and contract workers on the same LAN. You want to restrict the contract employees to a subset of the resources used by the full-time employees. You also want to use a more restrictive security policy for the contract workers. In this case, you split the interface into two VLANs.

VLANs enable you to divide your network into groups with a logical, hierarchical structure or grouping instead of a physical one. This helps free IT staff from the restrictions of their existing network design and cable infrastructure. VLANs make it easier to design, implement, and manage your network. Because VLANs are software-based, you can quickly and easily adapt your network to additions, relocations, and reorganizations.

VLANs use bridges and switches, so broadcasts are more efficient because they go only to people in the VLAN, not everyone on the wire. Consequently, traffic across your routers is reduced, which means a reduction in router latency. You can configure your XTM device to act as a DHCP server for devices on the VLAN, or use DHCP relay with a separate DHCP server.

You assign a VLAN to the Trusted, Optional, or External security zone. VLAN security zones correspond to aliases for interface security zones. For example, VLANs of type Trusted are handled by policies that use the alias Any-Trusted as a source or destination. VLANs of type External appear in the list of external interfaces when you configure policy-based routing.

## VLAN Requirements and Restrictions

- The WatchGuard VLAN implementation does not support the spanning tree link management protocol.
- If your XTM device is configured to use drop-in network mode, you cannot use VLANs.
- A physical interface can be an untagged VLAN member of only one VLAN. For example, if External-1 is an untagged member of a VLAN named VLAN-1, it cannot be an untagged member of a different VLAN at the same time. Also, external interfaces can be a member of only one VLAN.
- Your multi-WAN configuration settings are applied to VLAN traffic. However, it can be easier to manage bandwidth when you use only physical interfaces in a multi-WAN configuration.
- Your device model and license controls the number of VLANs you can create.  
To see the number of VLANs you can add to your XTM device, *Open Policy Manager* and select **Setup > Feature Keys**.  
Find the row labeled **Total number of VLAN interfaces**.

- We recommend that you do not create more than 10 VLANs that operate on external interfaces. Too many VLANs on external interfaces affect performance.
- All network segments you want to add to a VLAN must have IP addresses on the VLAN network.

**Note** *If you define VLANs, you can ignore messages with the text “802.1d unknown version”. These occur because the WatchGuard VLAN implementation does not support spanning tree link management protocol.*

## About Tagging

To enable VLANs, you must deploy VLAN-capable switches in each site. The switch interfaces insert tags at layer 2 of the data frame that identify a network packet as part of a specified VLAN. These tags, which add an extra four bytes to the Ethernet header, identify the frame as belonging to a specific VLAN. Tagging is specified by the IEEE 802.1Q standard.

The VLAN definition includes disposition of tagged and untagged data frames. You must specify whether the VLAN receives tagged, untagged, or no data from each interface that is enabled. Your XTM device can insert tags for packets that are sent to a VLAN-capable switch. Your device can also remove tags from packets that are sent to a network segment that belongs to a VLAN that has no switch.

## About VLAN ID Numbers

By default, each interface on most new, unconfigured switches belongs to VLAN number 1. Because this VLAN exists on every interface of most switches by default, the possibility exists that this VLAN can accidentally span the entire network, or at least very large portions of it.

We recommend you use a VLAN ID number that is not 1 for any VLAN that passes traffic to the XTM device.

## Define a New VLAN

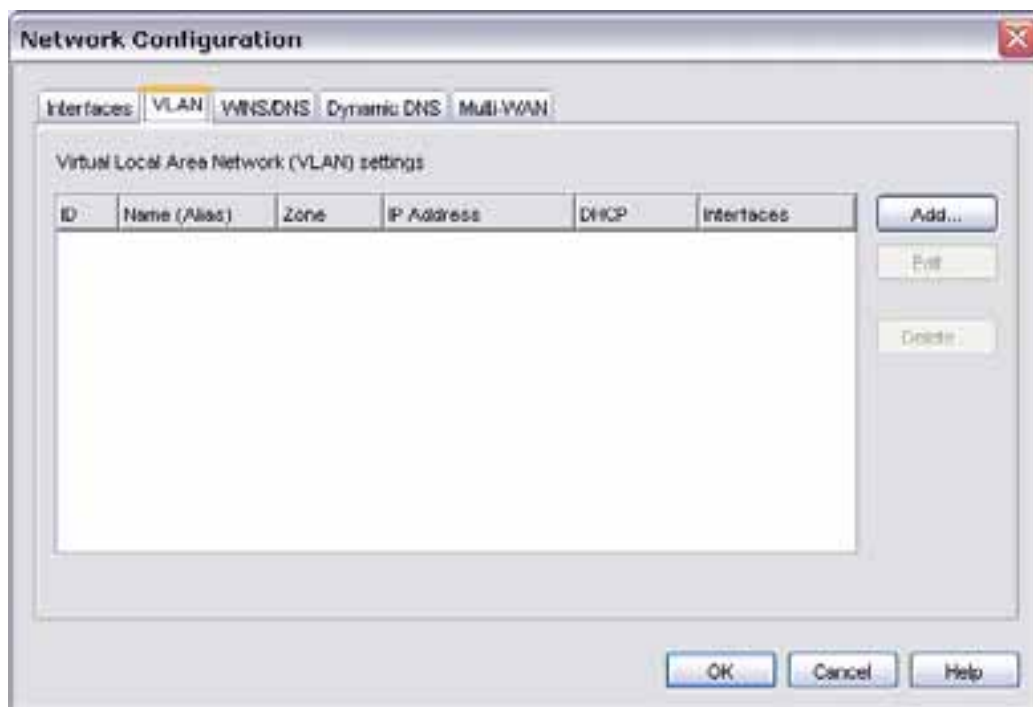
Before you create a new VLAN, make sure you understand the concepts about, and restrictions for VLANs, as described in *About Virtual Local Area Networks (VLANs)* on page 124.

When you define a new VLAN, you add an entry in the **VLAN Settings** table. You can change the view of this table:

- Click a column header to sort the table based on the values in that column.
- The table can be sorted in descending or ascending order.
- The values in the Interface column show the physical interfaces that are members of this VLAN.
- The interface number in bold is the interface that sends untagged data to that VLAN.

To create a new VLAN:

1. Select **Network > Configuration**.  
*The Network Configuration dialog box appears.*
2. Click the **VLAN** tab.  
*A table of existing user-defined VLANs and their settings appears.*



3. Click **Add**.  
*The New VLAN Configuration dialog box appears.*

4. In the **Name (Alias)** field, type a name for the VLAN. The name cannot contain spaces.
5. (Optional) In the **Description** field, type a description of the VLAN.
6. In the **VLAN ID** field, or type or select a value for the VLAN.
7. In the **Security Zone** field, select **Trusted**, **Optional**, or **External**.  
Security zones correspond to aliases for interface security zones. For example, VLANs of type *Trusted* are handled by policies that use the alias *Any-Trusted* as a source or destination.
8. In the **IP Address** field, type the address of the VLAN gateway.  
Note that any computer in this new VLAN must use this IP address as its default gateway.

### Use DHCP on a VLAN

You can configure the XTM device as a DHCP server for the computers on your VLAN network.

1. In the **New VLAN Configuration** dialog box, select the **Use DHCP Server** radio button to configure the XTM device as the DHCP server for your VLAN network. If necessary, type your domain name to supply it to the DHCP clients.
2. To add an IP address pool, click **Add** and type the first and last IP addresses assigned for distribution. Click **OK**.  
*You can configure a maximum of six address pools.*
3. To reserve a specific IP address for a client, click **Add** adjacent to the **Reserved Addresses** box. Type a **name** for the reservation, the **IP address** you want to reserve, and the **MAC address** of the client's network card. Click **OK**.
4. To change the default lease time, click the **Leasing Time** arrows.  
*This is the time interval that a DHCP client can use an IP address that it receives from the DHCP server. When the lease time is about to expire, the client sends a request to the DHCP server to get a new lease.*
5. To add DNS or WINS servers to your DHCP configuration, click the **DNS/WINS Servers** button.
6. If necessary, type a **Domain Name** for DNS information.
7. Click the **Add** button adjacent to each list to create an entry for each server you want to add.
8. Select a server from the list and click **Edit** to change the information for that server, or click **Delete** to remove the selected server.

### Use DHCP Relay on a VLAN

1. In the **New VLAN Configuration** dialog box, select **Use DHCP Relay**.
2. Type the IP address of the DHCP server. Make sure to add a route to the DHCP server, if necessary.

You can now take the next steps, and *Assign Interfaces to a VLAN*.



## Assign Interfaces to a VLAN

When you create a new VLAN, you specify the type of data it receives from XTM device interfaces. However, you can also make an interface a member of a VLAN that is currently defined, or remove an interface from a VLAN.

1. In the **Network Configuration** dialog box, select the **Interfaces** tab.
2. Select an interface and click **Configure**.  
*The Interface Settings dialog box appears.*
3. In the **Interface Type** drop-down list, select **VLAN**.  
*A table that shows all current VLANs appears. You may need to increase the size of this dialog box to see all of the options.*

General Secondary MAC Access Control Advanced

Interface Name: Trusted-2

Interface Description:

Interface Type: VLAN

Send and receive tagged traffic for selected VLANs

You can add one or more VLANs to this interface. New VLAN

Member	ID	Zone	Name	Network Configuration
<input checked="" type="checkbox"/>	10	Trusted	Example	10.0.3.1/24 (DHCP disabled)
<input type="checkbox"/>	20	Trusted	Example2	10.0.4.1/24 (DHCP disabled)

4. Select the **Send and receive tagged traffic for selected VLANs** check box to receive tagged data on this network interface.
5. Select the **Member** check box for each interface you want to include in this VLAN.

To remove an interface from this VLAN, clear the adjacent **Member** check box.  
*An interface can be a member of one external VLAN, or multiple trusted or optional VLANs.*

6. To configure the interface to receive untagged data, select the **Send and receive untagged traffic for selected VLAN** check box at the bottom of the dialog box.
7. Select a VLAN configuration from the adjacent drop-down list, or click **New VLAN** to create a new VLAN configuration.

Send and receive untagged traffic for selected VLAN

Example 2 (10.0.4.1/24) New VLAN

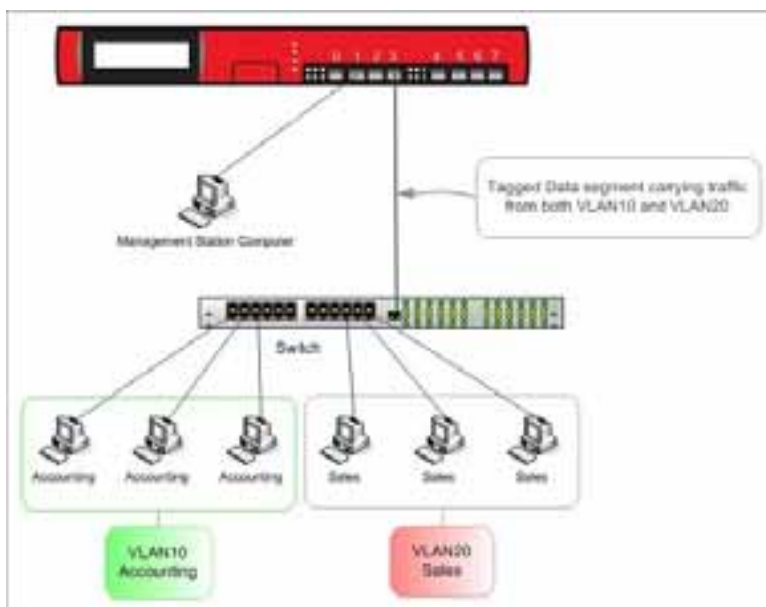
8. Click **OK**.

# Network Setup Examples

## Configure Two VLANs on the Same Interface

A network interface on a XTM device is a member of more than one VLAN when the switch that connects to that interface carries traffic from more than one VLAN. This example shows how to connect one switch that is configured for two different VLANs to a single interface on the XTM device.

The subsequent diagram shows the configuration for this example.



In this example, computers on both VLANs connect to the same 802.1Q switch, and the switch connects to interface 3 on the XTM device.

The subsequent instructions show you how to configure the VLAN settings in Policy Manager.

## Define the Two VLANs

1. From Policy Manager, select **Network > Configuration**.
2. Select the **VLAN** tab.
3. Click **Add**.  
*The New VLAN Configuration dialog box appears.*
4. In the **Name (Alias)** text box, type a name for the VLAN. For this example, type `VLAN10`.
5. In the **Description** text box, type a description. For this example, type `Accounting`.
6. In the **VLAN ID** text box, type the VLAN number configured for the VLAN on the switch. For this example, type `10`.
7. From the **Security Zone** drop-down list, select the security zone. For this example, select **Trusted**.
8. In the **IP Address** text box, type the IP address to use for the XTM device on this VLAN. For this example, type `192.168.10.1/24`.

9. (Optional) To configure the XTM device to act as a DHCP server for the computers on VLAN10:
  - Select **Use DHCP Server**.
  - To the right of the **Address Pool** list, click **Add**.
  - For this example, in the **Starting address** text box, type 192 . 168 . 10 . 10 and in the **Ending address** text box type 192 . 168 . 10 . 20.

The finished VLAN10 configuration for this example looks like:

The screenshot shows a configuration window for a VLAN. The fields are filled with the following information:

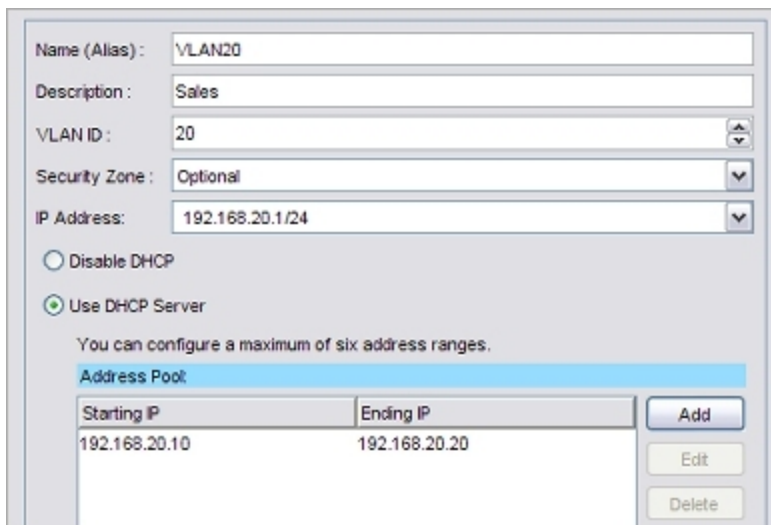
- Name (Alias): VLAN10
- Description: Accounting
- VLAN ID: 10
- Security Zone: Trusted
- IP Address: 192.168.10.1/24

Below these fields, there are two radio buttons: "Disable DHCP" (unselected) and "Use DHCP Server" (selected). A note below the radio buttons states: "You can configure a maximum of six address ranges." Below this note is a table for the "Address Pool":

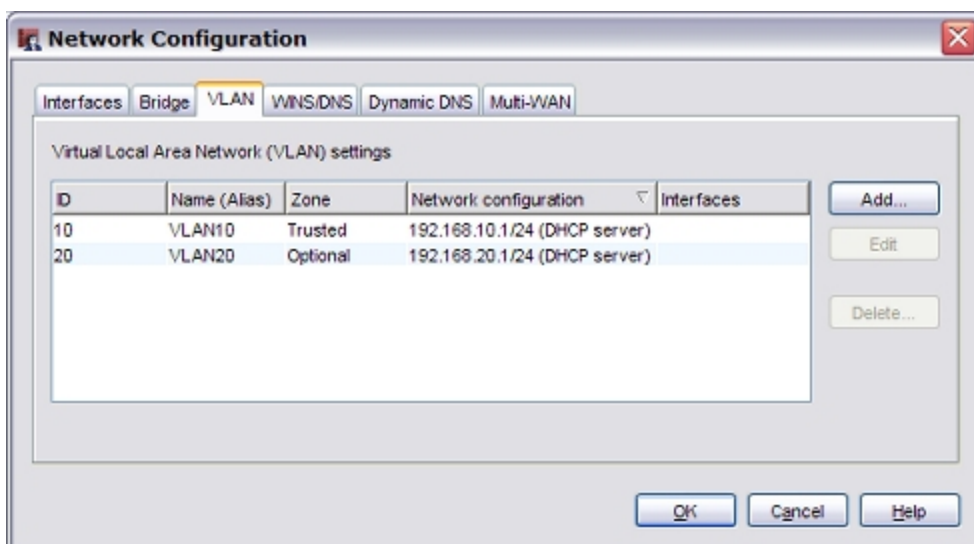
Starting IP	Ending IP
192.168.10.10	192.168.10.20

To the right of the table are three buttons: "Add", "Edit", and "Delete".

10. Click **OK** to add the new VLAN.
11. Click **Add** to add the second VLAN.
12. In the **Name (Alias)** text box, type VLAN20.
13. In the **Description** text box, type Sales.
14. In the **VLAN ID** text box, type 20.
15. From the **Security Zone** drop-down list, select **Optional**.
16. In the **IP Address** field, type the IP address to use for the XTM device on this VLAN. For this example, type 192 . 168 . 20 . 1 / 24.
17. (Optional) To configure the XTM device to act as a DHCP server for the computers on VLAN20:
  - Select **Use DHCP Server**.
  - To the right of the **Address Pool** list, click **Add**.
  - For this example, in the **Starting address** text box, type 192 . 168 . 20 . 10 and in the **Ending address** text box type 192 . 168 . 20 . 20.



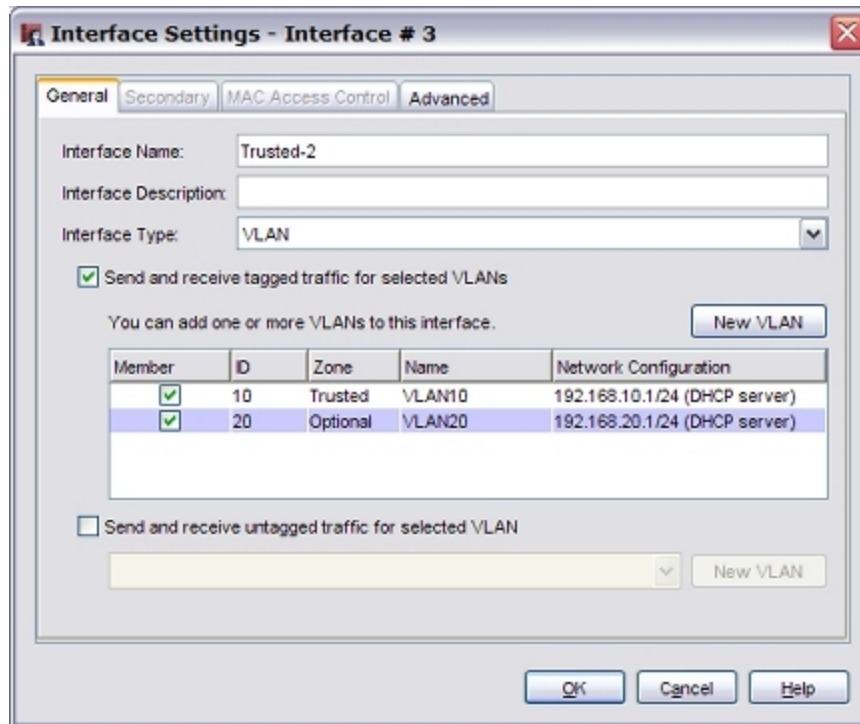
- Click **OK** to add the new VLAN.  
 Both VLANs now appear in the VLAN tab of the Network Configuration dialog box.



### Configure Interface 3 as a VLAN Interface

After you define the VLANs, you can configure Interface 3 to send and receive VLAN traffic.

- Click the **Interfaces** tab.
- Select Interface 3. Click **Configure**.



3. From the **Interface Type** drop-down list, select **VLAN**.
4. Select the **Send and receive tagged traffic for selected VLANs** check box.
5. Select the check boxes for **VLAN10** and **VLAN20**.
6. Click **OK**.

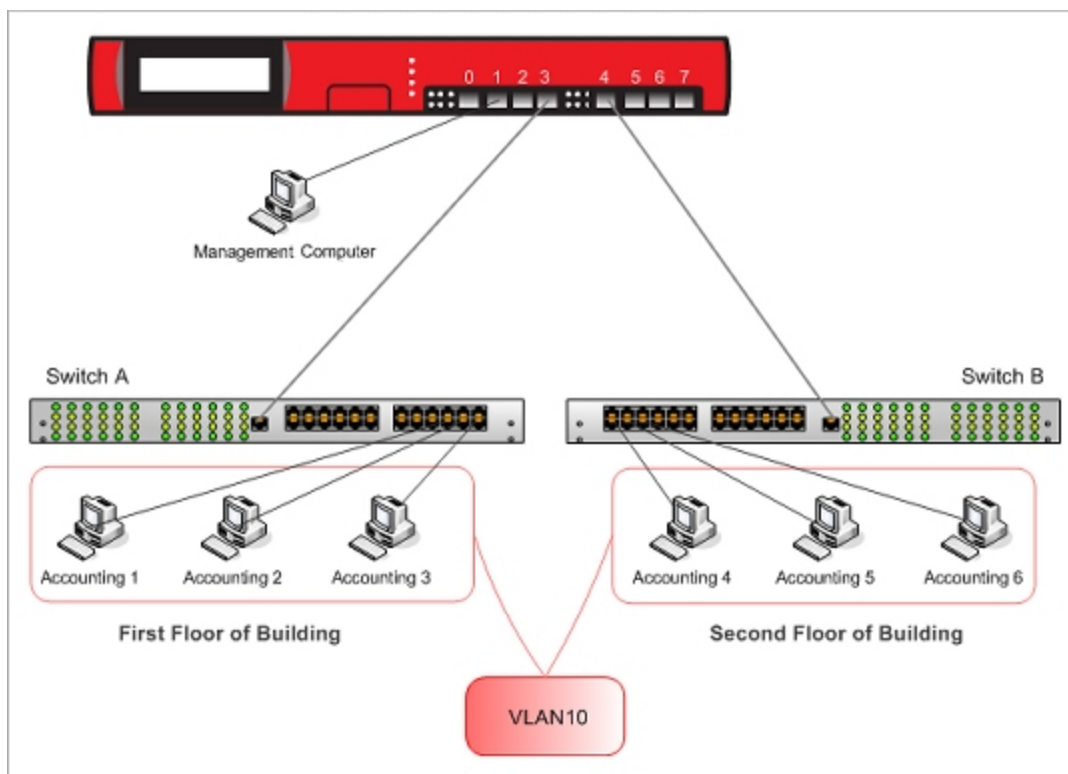
Each device on these two VLANs must set the IP address of the default gateway to be the IP address configured for the VLAN. In this example:

- Devices on VLAN10 must use 192.168.10.1 as their default gateway.
- Devices on VLAN20 must use 192.168.20.1 as their default gateway.

## Configure One VLAN Bridged Across Two Interfaces

You can configure a VLAN to bridge across two interfaces of the XTM device. You might want to bridge one VLAN across two interfaces if your organization is spread across multiple locations. For example, suppose your network is on the first and second floors in the same building. Some of the computers on the first floor are in the same functional group as some of the computers on the second floor. You want to group these computers into one broadcast domain so that they can easily share resources, such as a dedicated file server for their LAN, host-based shared files, printers, and other network accessories.

This example shows how to connect two 802.1Q switches so that both switches can send traffic from the same VLAN to two interfaces on the same XTM device.



In this example, two 802.1Q switches are connected to XTM device interfaces 3 and 4, and carry traffic from the same VLAN.

## Define the VLAN on the XTM Device

1. From Policy Manager, select **Network > Configuration**.
2. Select the **VLAN** tab.
3. Click **Add**.  
*The New VLAN Configuration dialog box appears.*
4. In the **Name (Alias)** text box, type a name for the VLAN. For this example, type `VLAN10`.
5. In the **Description** text box, type a description. For this example, type `Accounting`.
6. In the **VLAN ID** text box, type the VLAN number configured for the VLAN on the switch. For this example, type `10`.
7. From the **Security Zone** drop-down list, select the security zone. For this example, select **Trusted**.
8. In the **IP Address** text box, type the IP address to use for the XTM device on this VLAN. For this example, type `192.168.10.1/24`.

**Note** Any computer in this new VLAN must use this IP address as its default gateway.

9. (Optional) To configure the XTM device to act as a DHCP server for the computers on VLAN10:
  - Select **Use DHCP Server**.
  - To the right of the **Address Pool** list, click **Add**.
  - For this example, in the **Starting address** text box, type `192.168.10.10` and in the **Ending address** text box type `192.168.10.20`.

The finished VLAN10 configuration for this example looks like this:

Name (Alias): VLAN10

Description: Accounting

VLAN ID: 10

Security Zone: Trusted

IP Address: 192.168.10.1/24

Disable DHCP

Use DHCP Server

You can configure a maximum of six address ranges.

Address Pool:

Starting IP	Ending IP	
192.168.10.10	192.168.10.20	Add
		Edit
		Delete

10. Click **OK** to add the new VLAN.
11. To make XTM device interfaces 3 and 4 members of the new VLAN, select the **Interfaces** tab.
12. Select **Interface 3**. Click **Configure**.

*The Interface Settings dialog box appears.*

Interface Settings - Interface # 3

General Secondary MAC Access Control Advanced

Interface Name: vlanfloor1

Interface Description:

Interface Type: VLAN

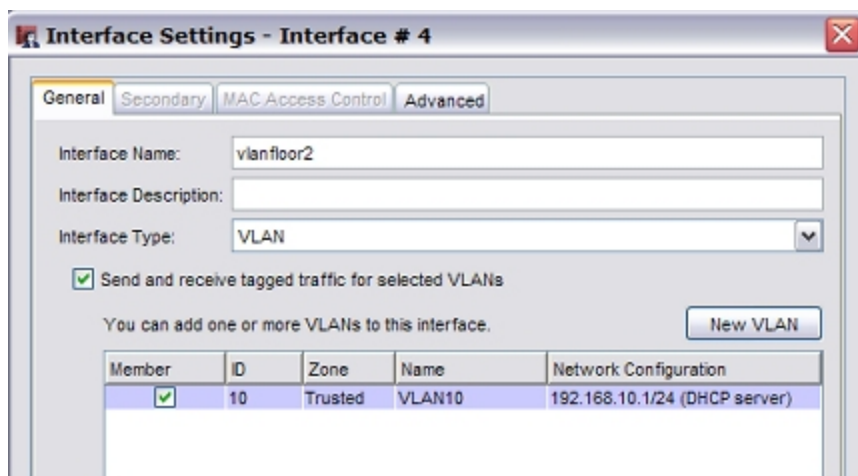
Send and receive tagged traffic for selected VLANs

You can add one or more VLANs to this interface. New VLAN

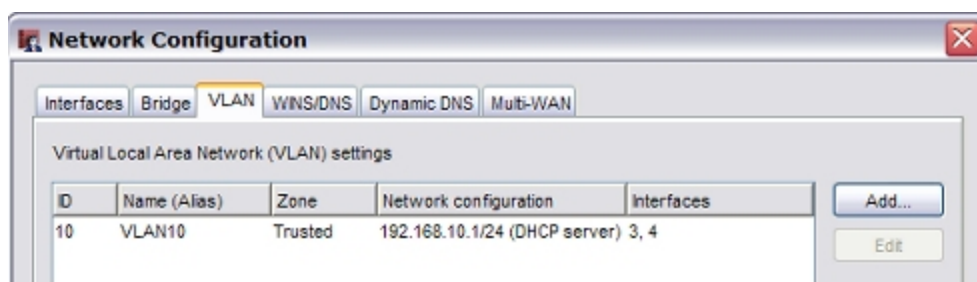
Member	ID	Zone	Name	Network Configuration
<input checked="" type="checkbox"/>	10	Trusted	VLAN10	192.168.10.1/24 (DHCP server)

13. From the **Interface Type** drop-down list, select **VLAN**.
14. Select the **Send and receive tagged traffic for selected VLANs** check box.
15. In the **Member** column, select the check box for VLAN10. Click **OK**.
16. Select **Interface 4**. Click **Configure**.

*The Interface Settings dialog box appears.*



17. From the **Interface Type** drop-down list, select **VLAN**.
18. Select the **Send and receive tagged traffic for selected VLANs** check box.
19. In the **Member** column, select the check box for VLAN10. Click **OK**.
20. Select the **VLAN** tab.



21. Verify that **Interfaces** column for VLAN10 shows interfaces 3 and 4.
22. Save the configuration to the device.

## Configure the Switches

Configure each of the switches that connect to interfaces 3 and 4 of the XTM device. Refer to the instructions from your switch manufacturer for details about how to configure your switches.

### Configure the Switch Interfaces Connected to the XTM Device

The physical segment between the switch interface and the XTM device interface is a tagged data segment. Traffic that flows over this segment must use 802.1Q VLAN tagging.

**Note** Some switch manufacturers refer to an interface configured in this way as a trunk port or a trunk interface.

On each switch, for the switch interface that connects to the XTM device:

- Disable Spanning Tree Protocol.
- Configure the interface to be a member of VLAN10.



- Configure the interface to send traffic with the VLAN10 tag.
- If necessary for your switch, set the switch mode to trunk.
- If necessary for your switch, set the encapsulation mode to 802.1Q.

## Configure the Other Switch Interfaces

The physical segments between each of the other switch interfaces and the computers (or other networked devices) that connect to them are untagged data segments. Traffic that flows over these segments does not have VLAN tags.

On each switch, for the switch interfaces that connect computers to the switch:

- Configure these switch interfaces to be members of VLAN10.
- Configure these switch interfaces to send untagged traffic for VLAN10.

## Physically Connect All Devices

1. Use an Ethernet cable to connect XTM device interface 3 to the Switch A interface that you configured to tag for VLAN10 (the VLAN trunk interface of Switch A).
2. Use an Ethernet cable to connect the XTM device interface 4 to the Switch B interface that you configured to tag for VLAN10 (the VLAN trunk interface of Switch B).
3. Connect a computer to the interface on Switch A that you configured to send untagged traffic for VLAN10.
4. Configure the network settings on the connected computer. The settings depend on whether you configured the XTM device to act as a DHCP server for the computers on VLAN10 in Step 9 of **Define the VLAN on the XTM Device**.
  - If you configured the XTM device to act as a DHCP server for the computers on VLAN10, configure the computer to use DHCP to get an IP address automatically. See Step 9 in the procedure **Define the VLAN**, above.
  - If you did not configure the XTM device to act as a DHCP server for the computers on VLAN10, configure the computer with an IP address in the VLAN subnet 192.168.10.x. Use subnet mask 255.255.255.0 and set the default gateway on the computer to the XTM device VLAN IP address 192.168.10.1
5. Repeat the previous two steps to connect a computer to Switch B.

## Test the Connection

After you complete these steps, the computers connected to Switch A and Switch B can communicate as if they were connected to the same physical local area network. To test this connection you can:

- Ping from a computer connected to Switch A to a computer connected to Switch B.
- Ping from a computer connected to Switch B to a computer connected to Switch A.

## Use Your XTM Device with the 3G Extend Wireless Bridge

The WatchGuard 3G Extend wireless bridge adds 3G cellular connectivity to your WatchGuard XTM 2 Series device. When you connect the external interface of your XTM device to the 3G Extend wireless bridge, computers on your network can connect wirelessly to the Internet via the 3G cellular network.

The 3G Extend has two models based on technology from Top Global and Cradlepoint.

To connect your XTM device to the 3G cellular network you need:

- An XTM 2 Series device
- A 3G Extend wireless bridge
- A 3G wireless broadband data card

## Use the 3G Extend/Top Global MB5000K Device

Follow these steps to use the 3G Extend wireless bridge with your XTM 2 Series device.

1. Configure the external interface on your XTM device to get its address with PPPoE. Make sure to set the PPPoE user name / password to public/public. To learn more about how to configure your external interface for PPPoE, see *Configure an External Interface* on page 90.
2. Activate your broadband data card. See the instructions included with your broadband data card for more information.
3. Prepare your 3G Extend wireless bridge:
  - Insert the broadband data card into the slot on the 3G Extend wireless bridge
  - Plug in the power to the 3G Extend wireless bridge
  - Verify the LED lights are active
4. Use an Ethernet cable to connect the 3G Extend wireless bridge to the external interface of your XTM device.

It is not necessary to change any settings on the 3G Extend device before you connect it to your XTM device. There are some times when it is necessary to connect to the web management interface of the 3G Extend device. To connect to the 3G Extend web interface, connect your computer directly to the MB5000K with an Ethernet cable and make sure your computer is configured to get its IP address with DHCP. Open your web browser and type `http://172.16.0.1`. Connect with a user name/password of public/public.

- To operate correctly with your XTM device, the 3G Extend wireless bridge must be configured to run in "Auto Connect" mode. All 3G Extend/MB5000K devices are pre-configured to run in this mode by default. To verify if your 3G Extend device is configured in Auto Connect mode, connect directly to the device and select **Interfaces > Internet access**. Select the **WAN#0** interface. In the **Networking** section, make sure the **Connect** mode drop-down list is set to **Auto**.
- If your 3G wireless card runs on the GPRS cellular network, it may be necessary to add a network login and password to our 3G Extend device configuration. To add a network login and password, connect to the 3G Extend wireless bridge and select **Services > Manageable Bridge**.
- To reset the MB5000K to its factory default settings, connect to the 3G Extend wireless bridge and select **System > Factory defaults**. Click **Yes**.

For security, we recommend that you change the default PPPoE user name/password from public/public after your network is up and running. You must change the user name and password on both your XTM device and your 3G Extend Wireless Bridge.

- To change the PPPoE user name and password on your XTM device, see *Configure an External Interface* on page 90.
- To change the PPPoE user name and password on the 3G Extend device, connect to the device and go to **Services > Manageable Bridge**.

The 3G Extend device supports more than 50 modem cards and ISP plan options. For detailed information about the Top Global product, including the MB5000 User Guide, go to [http://www.topglobaluse.com/support\\_mb5000.htm](http://www.topglobaluse.com/support_mb5000.htm).

## Use the 3G Extend/Cradlepoint CBA250 Device

Follow these steps to use the 3G Extend Cradlepoint cellular broadband adapter with your WatchGuard XTM 2 Series device.

1. Follow the instructions in the [Cradlepoint CBA250 Quick Start Guide](#) to set up the Cradlepoint device and update the device firmware. If you have a newer modem that is not supported by the firmware version that ships on the device, you must use different steps to upgrade your firmware to the latest version:
  - Download the latest firmware for the CBA250 to your computer from the Cradlepoint support site at <http://www.cradlepoint.com/support/cba250>.
  - Use these instructions to update your firmware: [Updating the Firmware on your Cradlepoint Router](#).
2. Configure the external interface on your XTM device to get its address with DHCP. To learn how to configure your external interface for PPPoE, see *Configure an External Interface* on page 90.
3. Use an Ethernet cable to connect the Cradlepoint device to the external interface of the XTM device.
4. Start (or restart) the XTM device.

*When the XTM device starts, it gets a DHCP address from the Cradlepoint device. After an IP address is assigned, the XTM device can connect to the Internet via the cellular broadband network.*

The Cradlepoint supports a large number of USB or ExpressCard broadband wireless devices. For a list of supported devices, see <http://www.cradlepoint.com/support./cba250>.



# 7 Multi-WAN

---

## About Using Multiple External Interfaces

You can use your XTM device to create redundant support for the external interface. This is a helpful option if you must have a constant Internet connection.

With the multi-WAN feature, you can configure up to four external interfaces, each on a different subnet. This allows you to connect your XTM device to more than one Internet Service Provider (ISP). When you configure a second interface, the multi-WAN feature is automatically enabled.

## Multi-WAN Requirements and Conditions

You must have a second Internet connection and more than one external interface to use most multi-WAN configuration options.

Conditions and requirements for multi-WAN use include:

- If you have a policy configured with an individual external interface alias in its configuration, you must change the configuration to use the alias *Any-External*, or another alias you configure for external interfaces. If you do not do this, some traffic could be denied by your firewall policies.
- Multi-WAN settings do not apply to incoming traffic. When you configure a policy for inbound traffic, you can ignore all multi-WAN settings.
- To override the multi-WAN configuration in any individual policy, enable policy-based routing for that policy. For more information on policy-based routing, see *Configure Policy-Based Routing* on page 395.
- Map your company's Fully Qualified Domain Name to the external interface IP address of the lowest order. If you add a multi-WAN XTM device to your Management Server configuration, you must use the lowest-ordered external interface to identify it when you add the device.
- To use multi-WAN, you must use mixed routing mode for your network configuration. This feature does not operate in drop-in or bridge mode network configurations.
- To use the Interface Overflow method, you must have Fireware XTM with a Pro upgrade. You must also have a Fireware XTM Pro license if you use the Round-robin method and configure different weights for the XTM device external interfaces.

You can use one of four multi-WAN configuration options to manage your network traffic.

For configuration details and setup procedures, see the section for each option.

## Multi-WAN and DNS

Make sure that your DNS server can be reached through every WAN. Otherwise, you must modify your DNS policies such that:

- The **From** list includes **Firebox**.
- The **Use policy-based routing** check box is selected.  
If only one WAN can reach the DNS server, select that interface in the adjacent drop-down list.  
If more than one WAN can reach the DNS server, select any one of them, select **Failover**, select **Configure**, and select all the interfaces that can reach the DNS server. The order does not matter.

***Note** You must have Fireware XTM with a Pro upgrade to use policy-based routing.*

## Multi-WAN and FireCluster

You can use multi-WAN failover with the FireCluster feature, but they are configured separately. Multi-WAN failover caused by a failed connection to a link monitor host does not trigger FireCluster failover. FireCluster failover occurs only when the physical interface is down or does not respond. FireCluster failover takes precedence over multi-WAN failover.

## About Multi-WAN Options

When you configure multiple external interfaces, you have several options to control which interface an outgoing packet uses. Some of these features require that you have Fireware XTM with a Pro upgrade.

### Round-Robin Order

When you configure multi-WAN with the Round-robin method, the XTM device looks at its internal routing table to check for specific static or dynamic routing information for each connection. If no specified route is found, the XTM device distributes the traffic load among its external interfaces. The XTM device uses the average of sent (TX) and received (RX) traffic to balance the traffic load across all external interfaces you specify in your round-robin configuration.

If you have Fireware XTM with a Pro upgrade, you can assign a weight to each interface used in your round-robin configuration. By default and for all Fireware XTM users, each interface has a weight of 1. The weight refers to the proportion of load that the XTM device sends through an interface. If you have Fireware XTM Pro and you assign a weight of 2 to an interface, you double the portion of traffic that will go through that interface compared to an interface with a weight of 1.

As an example, if you have three external interfaces with 6M, 1.5M, and .075M bandwidth and want to balance traffic across all three interfaces, you would use 8, 2, and 1 as the weights for the three interfaces. Fireware will try to distribute connections so that 8/11, 2/11, and 1/11 of the total traffic flows through each of the three interfaces.

For more information, see *Configure Round-Robin* on page 145.

## Failover

When you use the failover method to route traffic through the XTM device external interfaces, you select one external interface to be the primary external interface. Other external interfaces are backup interfaces, and you set the order for the XTM device to use the backup interfaces. The XTM device monitors the primary external interface. If it goes down, the XTM device sends all traffic to the next external interface in its configuration. While the XTM device sends all traffic to the backup interface, it continues to monitor the primary external interface. When the primary interface is active again, the XTM device immediately starts to send all new connections through the primary external interface again.

You control the action for the XTM device to take for existing connections; these connections can failback immediately, or continue to use the backup interface until the connection is complete. Multi-WAN failover and FireCluster are configured separately. Multi-WAN failover caused by a failed connection to a link monitor host does not trigger FireCluster failover. FireCluster failover occurs only when the physical interface is down or does not respond. FireCluster failover takes precedence over multi-WAN failover.

For more information, see *Configure Failover* on page 147.

## Interface Overflow

When you use the Interface Overflow multi-WAN configuration method, you select the order you want the XTM device to send traffic through external interfaces and configure each interface with a bandwidth threshold value. The XTM device starts to send traffic through the first external interface in its Interface Overflow configuration list. When the traffic through that interface reaches the bandwidth threshold you have set for that interface, the XTM device starts to send traffic to the next external interface you have configured in your Interface Overflow configuration list.

This multi-WAN configuration method allows the amount of traffic sent over each WAN interface to be restricted to a specified bandwidth limit. To determine bandwidth, the XTM device examines the amount of sent (TX) and received (RX) packets and uses the higher number. When you configure the interface bandwidth threshold for each interface, you must consider the needs of your network for this interface and set the threshold value based on these needs. For example, if your ISP is asymmetrical and you set your bandwidth threshold based on a large TX rate, interface overflow will not be triggered by a high RX rate.

If all WAN interfaces have reached their bandwidth limit, the XTM device uses the ECMP (Equal Cost MultiPath Protocol) routing algorithm to find the best path.

**Note** You must have Fireware XTM with a Pro upgrade to use this multi-WAN routing method.

For more information, see *Configure Interface Overflow* on page 149.

## Routing Table

When you select the Routing Table option for your multi-WAN configuration, the XTM device uses the routes in its internal route table or routes it gets from dynamic routing processes to send packets through the correct external interface. To see whether a specific route exists for a packet's destination, the XTM device examines its route table from the top to the bottom of the list of routes. You can see the list of routes in the route table on the **Status** tab of Firebox System Manager. The Routing Table option is the default multi-WAN option.

If the XTM device does not find a specified route, it selects the route to use based on source and destination IP hash values of the packet, using the ECMP (Equal Cost Multipath Protocol) algorithm specified in:

<http://www.ietf.org/rfc/rfc2992.txt>

With ECMP, the XTM device uses an algorithm to decide which next-hop (path) to use to send each packet. This algorithm does not consider current traffic load.

For more information, see *When to Use Multi-WAN Methods and Routing* on page 152.

## **Serial Modem (XTM 2 Series only)**

If your organization has a dial-up account with an ISP, you can connect an external modem to the USB port on your XTM 2 Series and use that connection for failover when all other external interfaces are inactive.

For more information, see *Serial Modem Failover* on page 153.



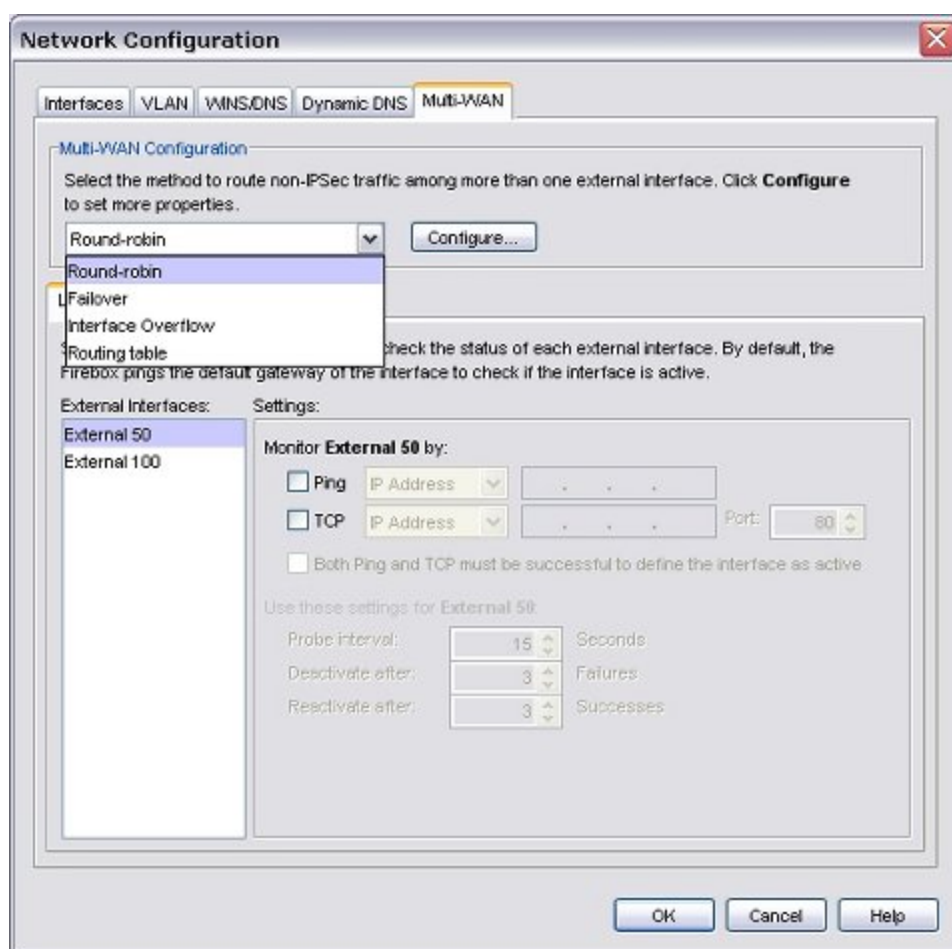
# Configure Round-Robin

## Before You Begin

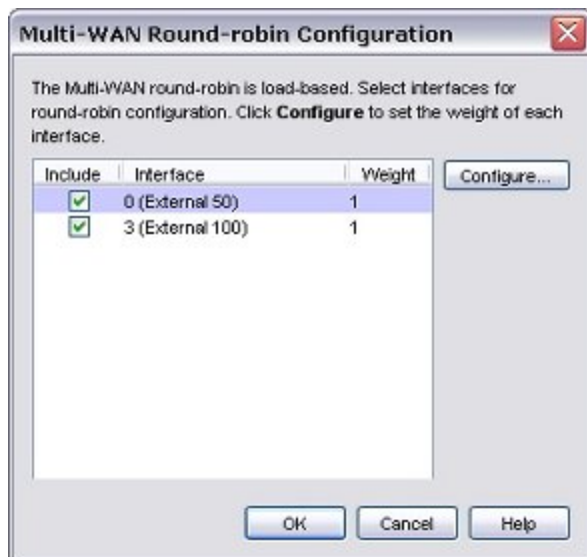
- To use the multi-WAN feature, you must have more than one external interface configured. If necessary, use the procedure described in *Configure an External Interface* on page 90.
- Make sure you understand the concepts and requirements for multi-WAN and the method you choose, as described in *About Using Multiple External Interfaces* on page 141 and *About Multi-WAN Options* on page 142.

## Configure the Interfaces

1. Select **Network > Configuration**.
2. Click the **Multi-WAN** tab.
3. In the **Multi-WAN Configuration** section drop-down list, select **Round-robin**.



4. Click **Configure**.
5. In the **Include** column, select the check box for each interface you want to use in the round-robin configuration. It is not necessary to include all external interfaces in your round-robin configuration.



For example, you may have one interface that you want to use for policy-based routing that you do not want to include in your round-robin configuration.

6. If you have Fireware XTM with a Pro upgrade and you want to change the weights assigned to one or more interfaces, click **Configure**.
7. Click the value control to set an interface weight. The weight of an interface sets the percentage of load through the XTM device that will use that interface.

**Note** You can change the weight from its default of 1 only if you have Fireware XTM with a Pro upgrade. Otherwise, you see an error when you try to close the **Network Configuration** dialog box.

8. Click **OK**.



For information on changing the weight, see *Find How to Assign Weights to Interfaces* on page 147.

9. To complete your configuration, you must add link monitor information as described in *About WAN Interface Status* on page 159.

For information on advanced multi-WAN configuration options, see *Advanced Multi-WAN Settings* on page 157.

10. Click **OK**.

## Find How to Assign Weights to Interfaces

If you use Fireware XTM with a Pro upgrade, you can assign a weight to each interface used in your round-robin multi-WAN configuration. By default, each interface has a weight of 1. The weight refers to the proportion of load that the XTM device sends through an interface.

You can use only whole numbers for the interface weights; no fractions or decimals are allowed. For optimal load balancing, you might have to do a calculation to know the whole-number weight to assign for each interface. Use a common multiplier so that the relative proportion of the bandwidth given by each external connection is resolved to whole numbers.

For example, suppose you have three Internet connections. One ISP gives you 6 Mbps, another ISP gives you 1.5 Mbps, and a third gives you 768 Kbps. Convert the proportion to whole numbers:

- First convert the 768 Kbps to approximately .75 Mbps so that you use the same unit of measurement for all three lines. Your three lines are rated at 6, 1.5, and .75 Mbps.
- Multiply each value by 100 to remove the decimals. Proportionally, these are equivalent: [6 : 1.5 : .75] is the same ratio as [600 : 150 : 75]
- Find the greatest common divisor of the three numbers. In this case, 75 is the largest number that evenly divides all three numbers 600, 150, and 75.
- Divide each of the numbers by the greatest common divisor.

The results are 8, 2, and 1. You could use these numbers as weights in a round-robin multi-WAN configuration.

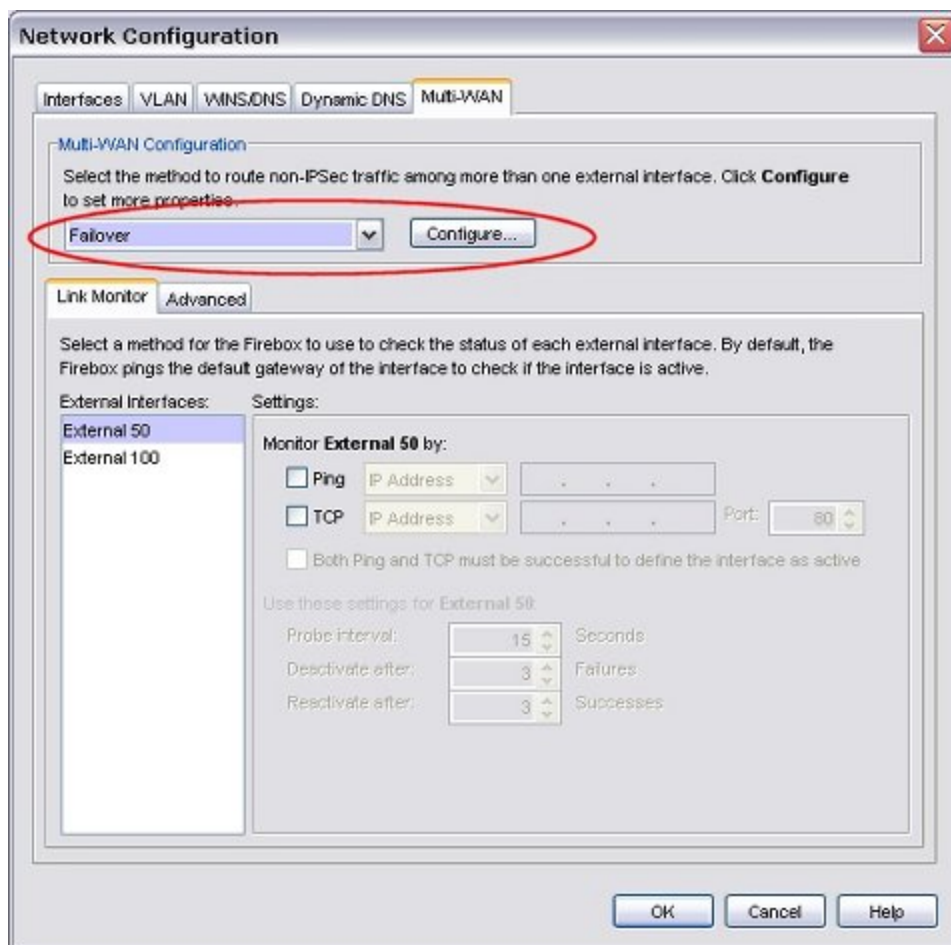
## Configure Failover

### Before You Begin

- To use the multi-WAN feature, you must have more than one external interface configured. If necessary, use the procedure described in *Configure an External Interface* on page 90.
- Make sure you understand the concepts and requirements for multi-WAN and the method you choose, as described in *About Using Multiple External Interfaces* on page 141 and *About Multi-WAN Options* on page 142.

### Configure the Interfaces

1. Select **Network > Configuration**.
2. Click the **Multi-WAN** tab.
3. In the Multi-WAN Configuration section drop-down list, select **Failover**.



4. Click **Configure** to specify a primary external interface and select backup external interfaces for your configuration. In the **Include** column, select the check box for each interface you want to use in the failover configuration.
5. Click **Move Up** or **Move Down** to set the order for failover. The first interface in the list is the primary interface.
6. To complete your configuration, you must add link monitor information as described in *About WAN Interface Status* on page 159.

For information on advanced multi-WAN configuration options, see *Advanced Multi-WAN Settings* on page 157.

7. Click **OK**.

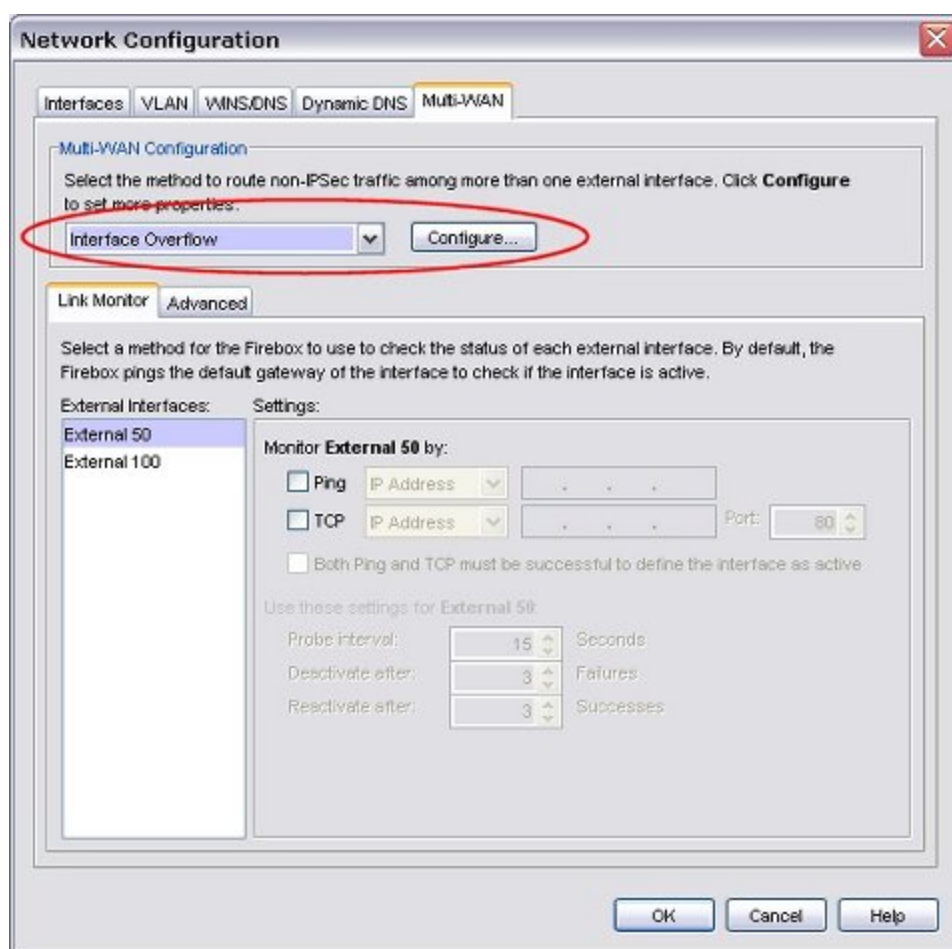
# Configure Interface Overflow

## Before You Begin

- To use the multiple WAN feature, you must have more than one external interface configured. If necessary, use the procedure described in *Configure an External Interface* on page 90.
- Make sure you understand the concepts and requirements for multi-WAN and the method you choose, as described in *About Using Multiple External Interfaces* on page 141 and *About Multi-WAN Options* on page 142.

## Configure the Interfaces

1. Select **Network > Configuration**.
2. Click the **Multi-WAN** tab.
3. In the **Multi-WAN Configuration** section drop-down list, select **Interface Overflow**.



4. Click **Configure**.
5. In the **Include** column, select the check box for each interface you want to include in your configuration.

6. To configure a bandwidth threshold for an external interface, select the interface from the list and click **Configure**.  
The Interface Overflow Threshold dialog box appears.
7. In the drop-down list, select **Mbps** or **Kbps** as the unit of measurement for your bandwidth setting and type the threshold value for the interface.  
The XTM device calculates bandwidth based on the higher value of sent or received packets.



8. Click **OK**.
9. To complete your configuration, you must add information as described in *About WAN Interface Status* on page 159.

For information on advanced multi-WAN configuration options, see *Advanced Multi-WAN Settings* on page 157.

## Configure Routing Table

### Before You Begin

- To use the multi-WAN feature, you must have more than one external interface configured. If necessary, use the procedure described in *Configure an External Interface* on page 90.
- You must decide whether the Routing Table method is the correct multi-WAN method for your needs. For more information, see *When to Use Multi-WAN Methods and Routing* on page 152
- Make sure you understand the concepts and requirements for multi-WAN and the method you choose, as described in *About Using Multiple External Interfaces* on page 141 and *About Multi-WAN Options* on page 142.

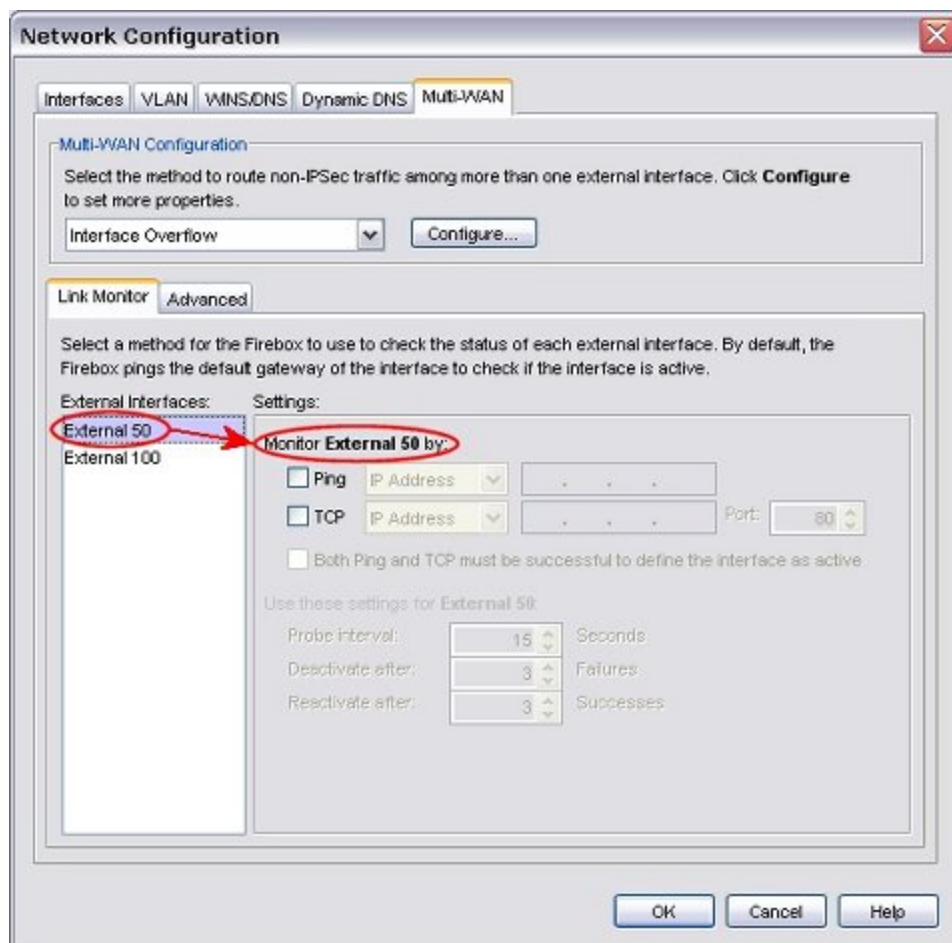
### Routing Table mode and load balancing

It is important to note that the Routing Table option does not do load balancing on connections to the Internet. The XTM device reads its internal route table from top to bottom. Static and dynamic routes that specify a destination appear at the top of the route table and take precedence over default routes. (A default route is a route with destination 0.0.0.0/0.) If there is no specific dynamic or static entry in the route table for a destination, the traffic to that destination is routed among the external interfaces of the XTM device through the use of ECMP algorithms. This may or may not result in even distribution of packets among multiple external interfaces.

### Configure the Interfaces

1. Select **Network > Configuration**.  
*The Network Configuration dialog box appears.*
2. Click the **Multi-WAN** tab.

- In the **Multi-WAN Configuration** section drop-down list, select **Routing table**.  
By default, all external interface IP addresses are included in the configuration.



- To remove external interfaces from the multi-WAN configuration, click **Configure** and clear the check box adjacent to the external interface you want to exclude from the multi-WAN configuration.  
You can have as few as one external interface included in your configuration. This is useful if you want to use policy-based routing for specific traffic and keep only one WAN for default traffic.
- To complete your configuration, you must add link monitor information as described in *About WAN Interface Status* on page 159.

For information on advanced multi-WAN configuration options, see *Advanced Multi-WAN Settings* on page 157.

## About the XTM Device Route Table

When you select the Routing Table configuration option, it is a good idea to know how to look at the routing table that is on your XTM device.

From WatchGuard System Manager:

- Start **Firebox System Manager**.
- Select the **Status Report** tab.

3. Scroll down until you see **Kernel IP routing table**.

This shows the internal route table on your XTM device. The ECMP group information appears below the routing table.

Routes in the internal route table on the XTM device include:

- The routes the XTM device learns from dynamic routing processes running on the device (RIP, OSPF, and BGP) if you enable dynamic routing.
- The permanent network routes or host routes you add.
- The routes the XTM device automatically makes when it reads the network configuration information.

If your XTM device detects that an external interface is down, it removes any static or dynamic routes that use that interface. This is true if the hosts specified in the Link Monitor become unresponsive and if the physical Ethernet link is down.

For more information on interface status and route table updates, see *About WAN Interface Status* on page 159.

## When to Use Multi-WAN Methods and Routing

If you use dynamic routing, you can use either the Routing Table or Round-Robin multi-WAN configuration method. Routes that use a gateway on an internal (optional or trusted) network are not affected by the multi-WAN method you select.

### When to Use the Routing Table Method

The Routing Table method is a good choice if:

- You enable dynamic routing (RIP, OSPF, or BGP) and the routers on the external network advertise routes to the XTM device so that the device can learn the best routes to external locations.
- You must get access to an external site or external network through a specific route on an external network. Examples include:
  - You have a private circuit that uses a frame relay router on the external network.
  - You want all traffic to an external location to always go through a specific XTM device external interface.

The Routing Table method is the fastest way to load balance more than one route to the Internet. After you enable this option, the ECMP algorithm manages all connection decisions. No additional configuration is necessary on the XTM device.

### When to Use the Round-Robin Method

Load balancing traffic to the Internet using ECMP is based on connections, not bandwidth. Routes configured statically or learned from dynamic routing are used before the ECMP algorithm. If you have Fireware XTM with a Pro upgrade, the weighted round-robin option gives you options to send more traffic through one external interface than another. At the same time, the round-robin algorithm distributes traffic to each external interface based on bandwidth, not connections. This gives you more control over how many bytes of data are sent through each ISP.



## Serial Modem Failover

*(This topic applies only to XTM 2 Series devices.)*

You can configure your XTM 2 Series device to send traffic through a serial modem when it cannot send traffic with any external interface. You must have a dial-up account with an ISP (Internet Service Provider) and an external modem connected on the USB port (2 Series) to use this option.

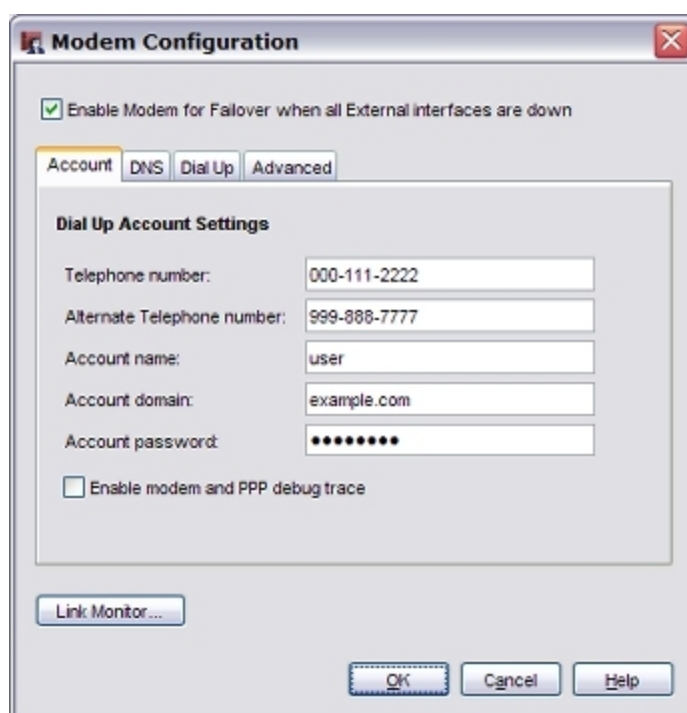
The XTM 2 Series has been tested with these modems:

- Zoom FaxModem 56K model 2949
- MultiTech 56K Data/Fax Modem International
- OMRON ME5614D2 Fax/Data Modem
- Hayes 56K V.90 serial fax modem

For a serial modem, use a USB to serial adapter to connect the modem to the XTM 2 Series device.

### Enable Serial Modem Failover

1. Select **Network > Modem**.  
*The Modem Configuration dialog box appears.*
2. Select the **Enable Modem for Failover when all external interfaces are down** check box.



3. Complete the **Account**, **DNS**, **Dial-Up**, and **Link Monitor** settings, as described in the subsequent sections.
4. Click **OK**.
5. Save your configuration.

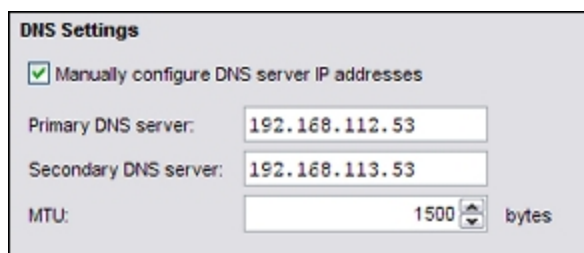
## Account Settings

1. Select the **Account** tab.
2. In the **Telephone number** text box, type the telephone number of your ISP.
3. If you have another number for your ISP, the **Alternate Telephone number** text box, type that number.
4. In the **Account name** text box, type your dial-up account name.
5. If you log in to your account with a domain name, in the **Account domain** text box, type the domain name.  
*An example of a domain name is msn.com.*
6. In the **Account password** text box, type the password you use to connect to your dial-up account.
7. If you have problems with your connection, select the **Enable modem and PPP debug trace** check box. When this option is selected, the XTM device sends detailed logs for the serial modem failover feature to the event log file.

## DNS Settings

If your dial-up ISP does not give DNS server information, or if you must use a different DNS server, you can manually add the IP addresses for a DNS server to use after failover occurs.

1. Select the **DNS** tab.  
*The DNS Settings page appears.*



**DNS Settings**

Manually configure DNS server IP addresses

Primary DNS server: 192.168.112.53

Secondary DNS server: 192.168.113.53

MTU: 1500 bytes

2. Select the **Manually configure DNS server IP addresses** check box.
3. In the **Primary DNS Server** text box, type the IP address of the primary DNS server.
4. If you have a secondary DNS server, in the **Secondary DNS server** text box, type the IP address for the secondary server.
5. In the **MTU** text box, for compatibility purposes, you can set the Maximum Transmission Unit (MTU) to a different value. Most users can keep the default setting.

## Dial-up Settings

1. Select the **Dial Up** tab.

*The Dialing Options page appears.*



**Dialing Options**

Dial up timeout:  minutes

Redial attempts:

Inactivity timeout:  minutes

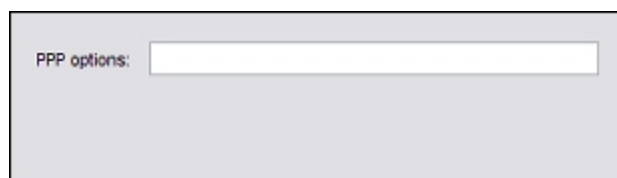
Speaker volume:

2. In the **Dial up timeout** text box, type or select the number of seconds before a timeout occurs if your modem does not connect. The default value is two (2) minutes.
3. In the **Redial attempts** text box, type or select the number of times the XTM device tries to redial if your modem does not connect. The default is to wait for three (3) connection attempts.
4. In the **Inactivity Timeout** text box, type or select the number of minutes to wait if no traffic goes through the modem before a timeout occurs. The default value is no timeout.
5. From the **Speaker volume** drop-down list, select your modem speaker volume.

## Advanced Settings

Some ISPs require that you specify one or more ppp options in order to connect. In China, for example, some ISPs require that you use the ppp option *receive-all*. The receive-all option causes ppp to accept all control characters from the peer.

1. Select the **Advanced** tab.



PPP options:

2. In the **PPP options** text box, type the required ppp options. To specify more than one ppp option, separate each option with a comma.

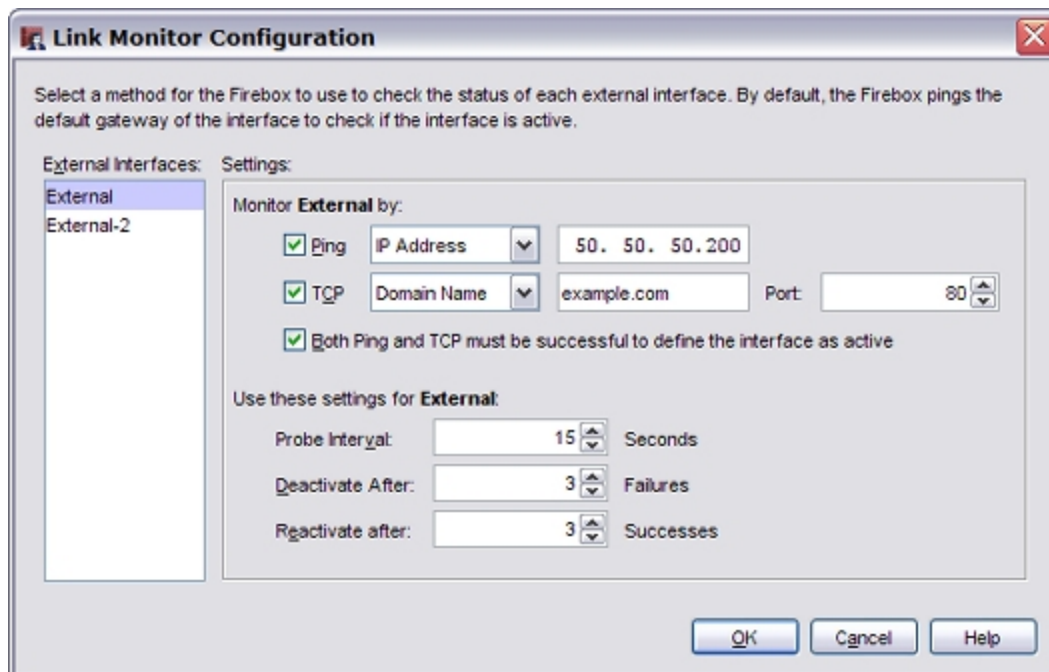
## Link Monitor Settings

You can set options to test one or more external interfaces for an active connection. When an external interface becomes active again, the XTM device no longer sends traffic over the serial modem and uses the external interface or interfaces instead. You can configure the Link Monitor to ping a site or device on the external interface, create a TCP connection with a site and port number you specify, or both. You can also set the time interval between each connection test, and configure the number of times a test must fail or succeed before an interface is activated or deactivated.

To configure the link monitor settings for an interface:

1. Click **Link Monitor**.

*The Link Monitor Configuration dialog box appears.*



2. To modify settings for an external interface, select it in the **External Interfaces** list. You must configure each interface separately. Set the link monitor configuration for each interface.
3. To ping a location or device on the external network, select the **Ping** check box and type an IP address or host name in the adjacent text box.
4. To create a TCP connection to a location or device on the external network, select the **TCP** check box and type an IP address or host name in the adjacent text box. You can also type or select a **Port** number.  
*The default port number is 80 (HTTP).*
5. To require successful ping and TCP connections before an interface is marked as active, select the **Both Ping and TCP must be successful** check box.
6. To change the time interval between connection attempts, in the **Probe interval** text box, type or select a different number.  
*The default setting is 15 seconds.*
7. To change the number of failures that mark an interface as inactive, in the **Deactivate after** text box, type or select a different number .  
*The default value is three (3) connection attempts.*
8. To change the number of successful connections that mark an interface as active, in the **Reactivate after** text box, type or select a different number.  
*The default value is three (3) connection attempts.*
9. Click **OK**.

## Advanced Multi-WAN Settings

In your multi-WAN configuration, you can set preferences for sticky connections, failback, and notification of multi-WAN events. Not all configuration options are available for all multi-WAN configuration options. If a setting does not apply to the multi-WAN configuration option you selected, those fields are not active.

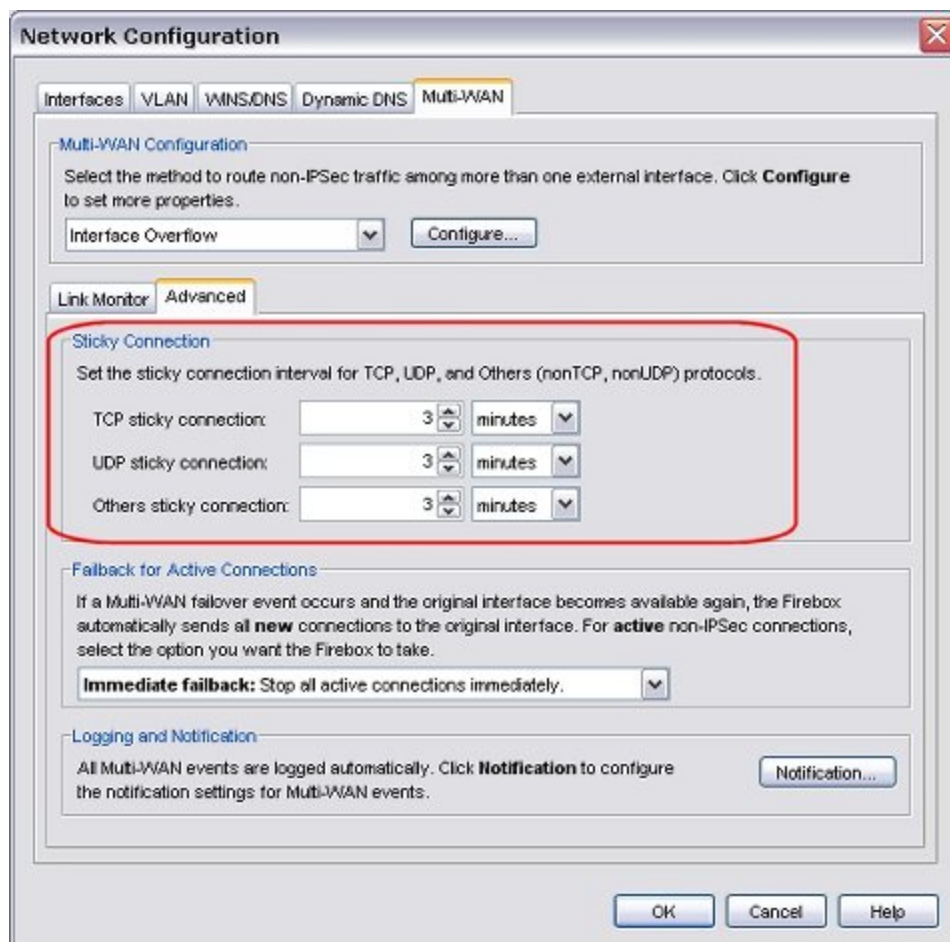
### About Sticky Connections

A sticky connection is a connection that continues to use the same WAN interface for a defined period of time. You can set sticky connection parameters if you use the Round-robin or Interface Overflow options for multi-WAN. Sticky connections make sure that, if a packet goes out through an external interface, any future packets between the source and destination address pair use the same external interface for a specified period of time. By default, sticky connections use the same interface for 3 minutes.

If a policy definition contains a sticky connection setting, this setting can override any global sticky connection duration.

### Set a Global Sticky Connection Duration

Use the **Advanced** tab to configure a global sticky connection duration for TCP connections, UDP connections, and connections that use other protocols.



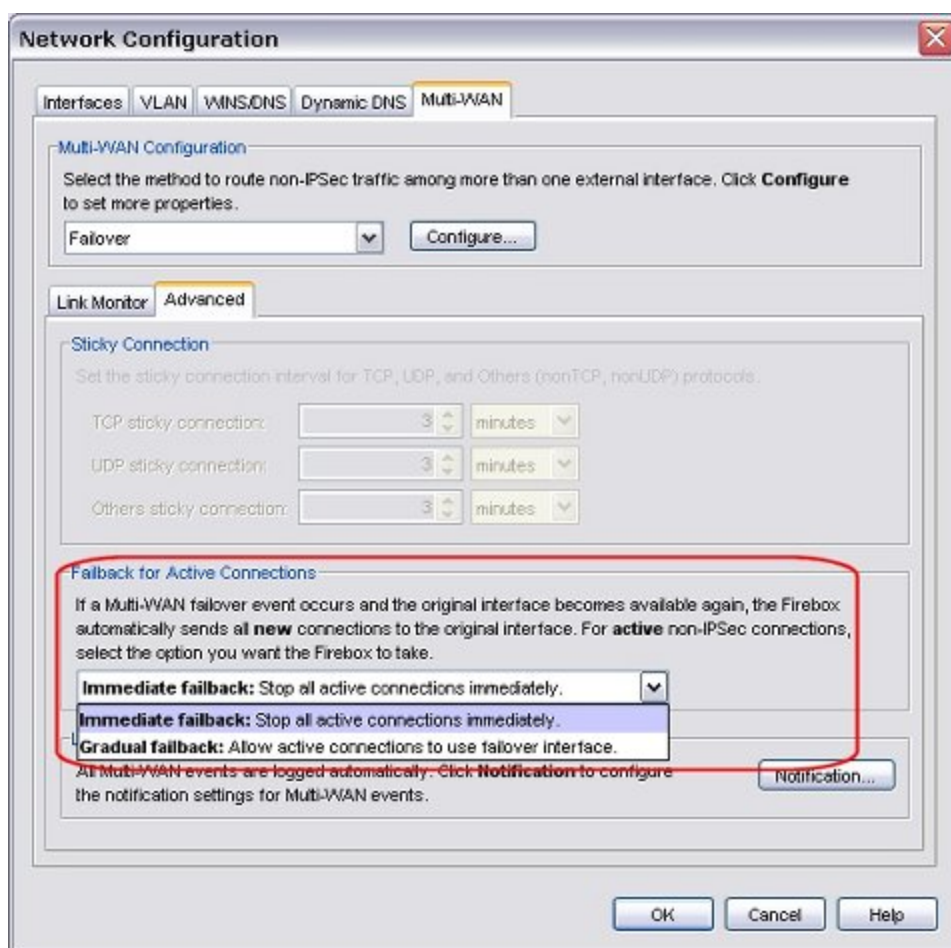
If you set a sticky connection duration in a policy, you can override the global sticky connection duration.

For more information, see *Set the Sticky Connection Duration for a Policy* on page 400.

## Set the Failback Action

You can set the action you want the XTM device to take when a failover event has occurred and then the primary external interface becomes active again. When this occurs, all new connections immediately fail back to the primary external interface. However, you can select the method you want to use for connections that are in process at the time of failback. This failback setting also applies to any policy-based routing configuration you set to use failover external interfaces.

1. In the **Network Configuration** dialog box, select the Multi-WAN tab.
2. Click the **Advanced** tab.



3. In the **Failback for Active Connections** section drop-down list select an option:
  - **Immediate failback** — The XTM device immediately stops all existing connections.
  - **Gradual failback** — The XTM device continues to use the failover interface for existing connections until each connection is complete.
4. Click **OK**.

## About WAN Interface Status

You can choose the method and frequency you want the XTM device to use to check the status of each WAN interface. If you do not configure a specified method for the XTM device to use, it pings the interface default gateway to check interface status.

### Time Needed for the XTM Device to Update its Route Table

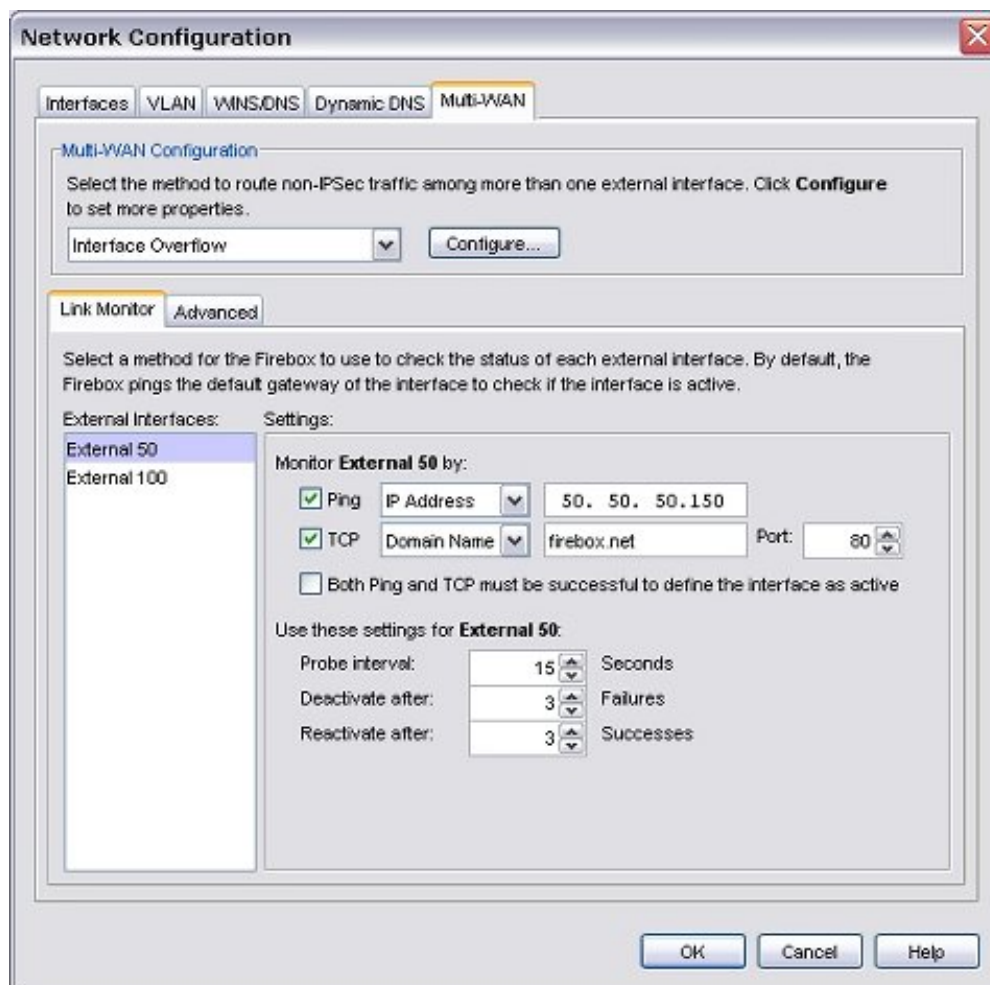
If a link monitor host does not respond, it can take from 40–60 seconds for the XTM device to update its route table. When the same Link Monitor host starts to respond again, it can take from 1–60 seconds for your XTM device to update its route table.

The update process is much faster when your XTM device detects a physical disconnect of the Ethernet port. When this happens, the XTM device updates its route table immediately. When your XTM device detects the Ethernet connection is back up, it updates its route table within 20 seconds.

### Define a Link Monitor Host

1. In the **Network Configuration** dialog box, select the **Multi-WAN** tab, and click the **Link Monitor** tab.
2. Highlight the interface in the **External Interface** column. The **Settings** information changes dynamically to show the settings for that interface.
3. Select the check boxes for each link monitor method you want the XTM device to use to check status of each external interface:
  - **Ping** — Add an IP address or domain name for the XTM device to ping to check for interface status.
  - **TCP** — Add the IP address or domain name of a computer that the XTM device can negotiate a TCP handshake with to check the status of the WAN interface.
  - **Both ping and TCP must be successful to define the interface as active** — The interface is considered inactive unless both a ping and TCP connection complete successfully.

If an external interface is a member of a FireCluster configuration, a multi-WAN failover caused by a failed connection to a link monitor host does not trigger FireCluster failover. FireCluster failover occurs only when the physical interface is down or does not respond. If you add a domain name for the XTM device to ping and any one of the external interfaces has a static IP address, you must configure a DNS server, as described in *Add WINS and DNS Server Addresses* on page 111.



4. To configure the frequency you want the XTM device to use to check the status of the interface, type or select a **Probe Interval** setting.  
*The default setting is 15 seconds.*
5. To change the number of consecutive probe failures that must occur before failover, type or select a **Deactivate after** setting.  
*The default setting is three (3). After the selected number of failures, the XTM device starts to send traffic through the next specified interface in the multi-WAN failover list.*
6. To change the number of consecutive successful probes through an interface before an interface that was inactive becomes active again, type or select a **Reactivate after** setting.
7. Repeat these steps for each external interface.
8. Click **OK**.
9. *Save the Configuration File.*



# 8 Network Address Translation (NAT)

---

## About Network Address Translation

Network Address Translation (NAT) is a term used to describe any of several forms of IP address and port translation. At its most basic level, NAT changes the IP address of a packet from one value to a different value.

The primary purposes of NAT are to increase the number of computers that can operate off a single publicly routable IP address, and to hide the private IP addresses of hosts on your LAN. When you use NAT, the source IP address is changed on all the packets you send.

You can apply NAT as a general firewall setting, or as a setting in a policy. Firewall NAT settings do not apply to BOVPN policies.

If you have Fireware XTM with a Pro upgrade, you can configure server load balancing as part of an SNAT rule. The server load balancing feature is designed to help you increase the scalability and performance of a high-traffic network with multiple public servers protected by your XTM device. With server load balancing, you can have the XTM device control the number of sessions initiated to multiple servers for each firewall policy you configure. The XTM device controls the load based on the number of sessions in use on each server. The XTM device does not measure or compare the bandwidth that is used by each server.

For more information on server load balancing, see *Configure Server Load Balancing* on page 182.

## Types of NAT

The XTM device supports three different types of NAT. Your configuration can use more than one type of NAT at the same time. You apply some types of NAT to all firewall traffic, and other types as a setting in a policy.

### *Dynamic NAT*

Dynamic NAT is also known as IP masquerading. The XTM device can apply its public IP address to the outgoing packets for all connections or for specified services. This hides the real IP address of the computer that is the source of the packet from the external network. Dynamic NAT is generally used to hide the IP addresses of internal hosts when they get access to public services.

For more information, see *About Dynamic NAT* on page 162.

### *Static NAT*

Also known as port forwarding, you configure static NAT in an SNAT action and then use that action when you configure policies. Static NAT is a port-to-host NAT. A host sends a packet from the external network to a port on an external interface. Static NAT changes this IP address to an IP address and port behind the firewall.

For more information, see *Configure Static NAT* on page 179.

### *1-to-1 NAT*

1-to-1 NAT creates a mapping between IP addresses on one network and IP addresses on a different network. This type of NAT is often used to give external computers access to your public, internal servers.

For more information, see *About 1-to-1 NAT* on page 168.

## About Dynamic NAT

Dynamic NAT is the most frequently used type of NAT. It changes the source IP address of an outgoing connection to the public IP address of the XTM device. Outside the XTM device, you see only the external interface IP address of the XTM device on outgoing packets.

Many computers can connect to the Internet from one public IP address. Dynamic NAT gives more security for internal hosts that use the Internet, because it hides the IP addresses of hosts on your network. With dynamic NAT, all connections must start from behind the XTM device. Malicious hosts cannot start connections to the computers behind the XTM device when the XTM device is configured for dynamic NAT.

In most networks, the recommended security policy is to apply NAT to all outgoing packets. With Fireware, dynamic NAT is enabled by default in the **Network > NAT** dialog box. It is also enabled by default in each policy you create. You can override the firewall setting for dynamic NAT in your individual policies, as described in *Apply NAT Rules* on page 399.

## Add Firewall Dynamic NAT Entries

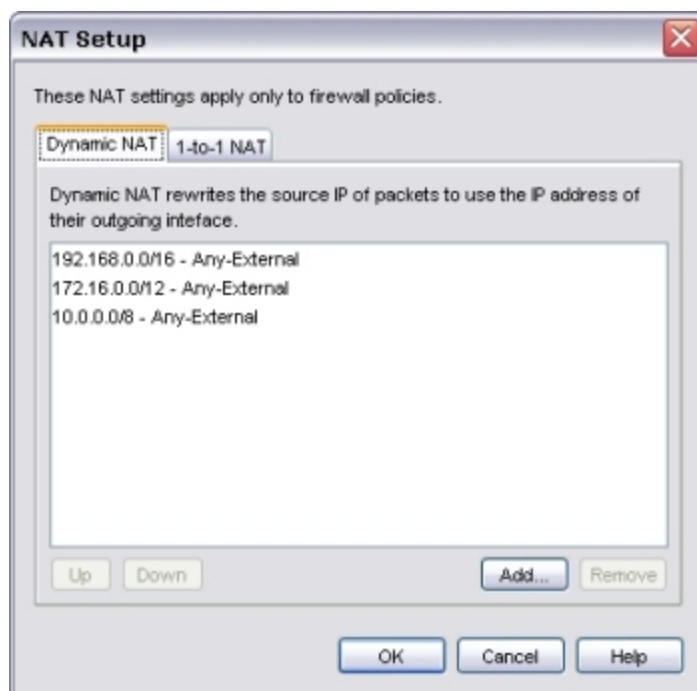
The default configuration of dynamic NAT enables dynamic NAT from all private IP addresses to the external network. The default entries are:

- 192.168.0.0/16 – Any-External
- 172.16.0.0/12 – Any-External
- 10.0.0.0/8 – Any-External

These three network addresses are the private networks reserved by the Internet Engineering Task Force (IETF) and usually are used for the IP addresses on LANs. To enable dynamic NAT for private IP addresses other than these, you must add an entry for them. The XTM device applies the dynamic NAT rules in the sequence that they appear in the Dynamic NAT Entries list. We recommend that you put the rules in a sequence that matches the volume of traffic the rules apply to.

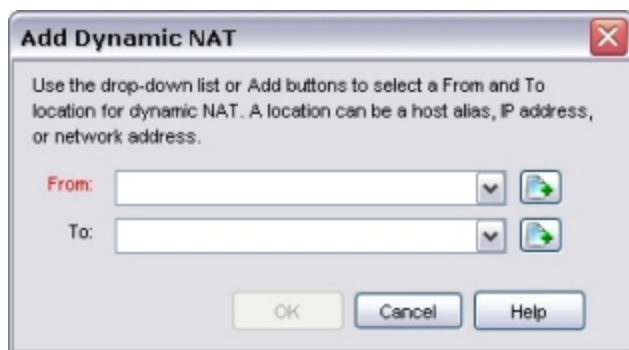
1. Select **Network > NAT**.


*The NAT Setup dialog box appears.*

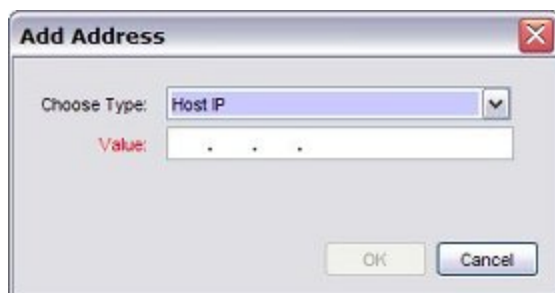


2. On the **Dynamic NAT** tab, click **Add**.

*The Add Dynamic NAT dialog box appears.*



3. In the **From** drop-down list, select the source of the outgoing packets.  
For example, use the trusted host alias to enable NAT from all of the trusted network.  
For more information on built-in XTM device aliases, see *About Aliases* on page 378.
4. In the **To** drop-down list, select the destination of the outgoing packets.
5. To add a host or a network IP address, click .  
*The Add Address dialog box appears.*



6. In the **Choose Type** drop-down list, select the address type.
7. In the **Value** text box, type the IP address or range.  
You must type a network address in slash notation.  
When you type an IP address, type all the numbers and the periods. Do not use the TAB or arrow keys.
8. Click **OK**.  
*The new entry appears in the Dynamic NAT Entries list.*

## Delete a Dynamic NAT Entry

You cannot change an existing dynamic NAT entry. If you want to change an existing entry, you must delete the entry and add a new one.

To delete a dynamic NAT entry:

1. Select the entry to delete.
2. Click **Remove**.  
*A warning message appears.*
3. Click **Yes**.

## Reorder Dynamic NAT Entries

To change the sequence of the dynamic NAT entries:

1. Select the entry to change.
2. Click **Up** or **Down** to move it in the list.

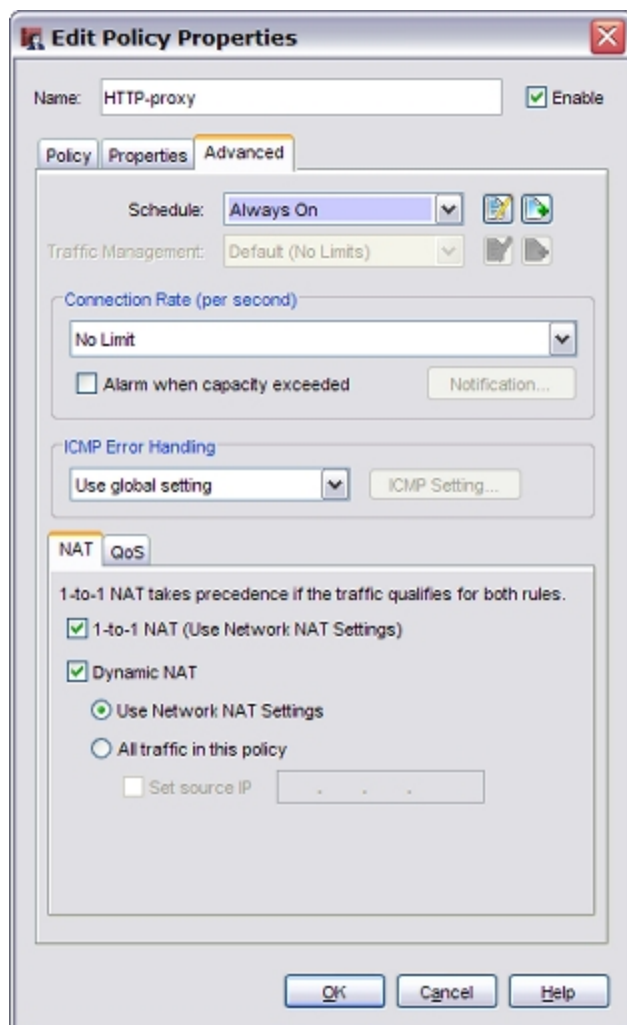
## Configure Policy-Based Dynamic NAT

In policy-based dynamic NAT, the XTM device maps private IP addresses to public IP addresses. Dynamic NAT is enabled in the default configuration of each policy. You do not have to enable it unless you previously disabled it.

For policy-based dynamic NAT to work correctly, use the **Policy** tab of the **Edit Policy Properties** dialog box to make sure the policy is configured to allow traffic out through only one XTM device interface.

1-to-1 NAT rules have higher precedence than dynamic NAT rules.

1. Right-click a policy and select **Modify Policy**.  
*The Edit Policy Properties dialog box appears.*
2. Click the **Advanced** tab.



3. If you want to use the dynamic NAT rules set for the XTM device, select **Use Network NAT Settings**. If you want to apply NAT to all traffic in this policy, select **All traffic in this policy**.
4. If you selected **All traffic in this policy**, you can set a dynamic NAT source IP address for any policy that uses dynamic NAT. Select the **Set source IP** check box.

When you select a source IP address, any traffic that uses this policy shows a specified address from your public or external IP address range as the source. This is most often used to force outgoing SMTP traffic to show the MX record address for your domain when the IP address on the XTM device external interface is not the same as your MX record IP address. This source address must be on the same subnet as the interface you specified for outgoing traffic.

We recommend that you do not use the **Set source IP** option if you have more than one external interface configured on your XTM device.

If you do not select the **Set source IP** check box, the XTM device changes the source IP address for each packet to the IP address of the interface from which the packet is sent.

5. Click **OK**.
6. *Save the Configuration File.*

## Disable Policy-Based Dynamic NAT

Dynamic NAT is enabled in the default configuration of each policy. To disable dynamic NAT for a policy:

1. Right-click a policy and select **Modify Policy**.  
*The Edit Policy Properties dialog box appears.*
2. Click the **Advanced** tab.
3. To disable NAT for the traffic controlled by this policy, clear the **Dynamic NAT** check box.
4. Click **OK**.
5. *Save the Configuration File.*

## About 1-to-1 NAT

When you enable 1-to-1 NAT, your XTM device changes the routes for all incoming and outgoing packets sent from one range of addresses to a different range of addresses. A 1-to-1 NAT rule always has precedence over dynamic NAT.

1-to-1 NAT is frequently used when you have a group of internal servers with private IP addresses that must be made public. You can use 1-to-1 NAT to map public IP addresses to the internal servers. You do not have to change the IP address of your internal servers. When you have a group of similar servers (for example, a group of email servers), 1-to-1 NAT is easier to configure than static NAT for the same group of servers.

To understand how to configure 1-to-1 NAT, we give this example:

Company ABC has a group of five privately addressed email servers behind the trusted interface of their XTM device. These addresses are:

10.1.1.1  
10.1.1.2  
10.1.1.3  
10.1.1.4  
10.1.1.5

Company ABC selects five public IP addresses from the same network address as the external interface of their XTM device, and creates DNS records for the email servers to resolve to.

These addresses are:

50.1.1.1  
50.1.1.2  
50.1.1.3  
50.1.1.4  
50.1.1.5

Company ABC configures a 1-to-1 NAT rule for their email servers. The 1-to-1 NAT rule builds a static, bi-directional relationship between the corresponding pairs of IP addresses. The relationship looks like this:

10.1.1.1 <--> 50.1.1.1  
10.1.1.2 <--> 50.1.1.2  
10.1.1.3 <--> 50.1.1.3  
10.1.1.4 <--> 50.1.1.4  
10.1.1.5 <--> 50.1.1.5

When the 1-to-1 NAT rule is applied, your XTM device creates the bi-directional routing and NAT relationship between the pool of private IP addresses and the pool of public addresses. 1-to-1 NAT also operates on traffic sent from networks that your XTM device protects.



## About 1-to-1 NAT and VPNs

When you create a VPN tunnel, the networks at each end of the VPN tunnel must have different network address ranges. You can use 1-to-1 NAT when you must create a VPN tunnel between two networks that use the same private network address. If the network range on the remote network is the same as on the local network, you can configure both gateways to use 1-to-1 NAT.

1-to-1 NAT for a VPN tunnel is configured when you configure the VPN tunnel and not in the **Network > NAT** dialog box.

1. Select a range of IP addresses that your computers show as the source IP addresses when traffic comes from your network and goes to the remote network through the BOVPN tunnel.

Consult the network administrator for the other network to select a range of IP addresses that are not in use. Do not use any of the IP addresses from:

- The trusted, optional, or external network connected to your XTM device
  - A secondary network connected to a trusted, optional, or external interface of your XTM device
  - A routed network configured in Policy Manager (**Network > Routes**)
  - Networks to which you already have a BOVPN tunnel
  - Mobile VPN virtual IP address pools
  - Networks that the remote IPsec device can reach through its interfaces, network routes, or VPN routes
2. *Configure Gateways* for the local and remote XTM devices.
  3. *Make Tunnels Between Gateway Endpoints*.

In the **Tunnel Route Settings** dialog box for each XTM device, select the **1:1 NAT** check box and type the masqueraded IP address range for that XTM device in the adjacent text box.

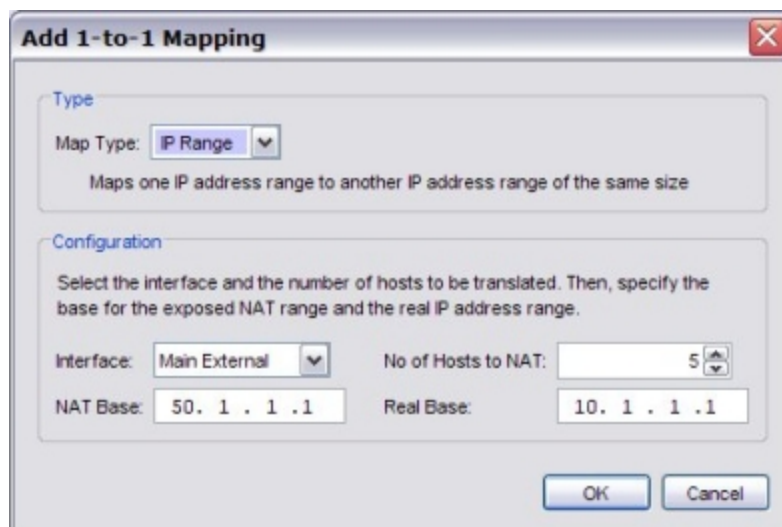
The number of IP addresses in this text box must be exactly the same as the number of IP addresses in the **Local** text box at the top of the dialog box. For example, if you use slash notation to indicate a subnet, the value after the slash must be the same in both text boxes.

For more information, see *About Slash Notation* on page 3.

For more detailed information, and an example, see *Use 1-to-1 NAT Through a Branch Office VPN Tunnel* on page 944.

## Configure Firewall 1-to-1 NAT

1. Select **Network > NAT**.  
*The NAT Setup dialog box appears.*
2. Click the **1-to-1 NAT** tab.
3. Click **Add**.  
*The Add 1-to-1 Mapping dialog box appears.*



4. In the **Map Type** drop-down list, select **Single IP** (to map one host), **IP range** (to map a range of hosts), or **IP subnet** (to map a subnet).

If you select **IP range** or **IP subnet**, do not include more than 256 IP addresses in that range or subnet. If you have more than 256 IP addresses that you want to apply 1-to-1 NAT to, you must create more than one rule.

5. Complete all the fields in the **Configuration** section of the dialog box.

For more information on how to use these fields, see the subsequent *Define a 1-to-1 NAT rule* section.

6. Click **OK**.
7. Add the NAT IP addresses to the appropriate policies.
  - For a policy that manages outgoing traffic, add the **Real Base** IP addresses to the **From** section of the policy configuration.
  - For a policy that manages incoming traffic, add the **NAT Base** IP addresses to the **To** section of the policy configuration.

In the previous example, where we used 1-to-1 NAT to give access to a group of email servers described in *About 1-to-1 NAT* on page 168, we must configure the SMTP policy to allow SMTP traffic. To complete this configuration, you must change the policy settings to allow traffic from the external network to the IP address range 10.1.1.1–10.1.1.5.

1. Add a new policy, or modify an existing policy.
2. Adjacent to the **From** list, click **Add**.
3. Select the alias **Any-External** and click **OK**.
4. Adjacent to the **To** list, click **Add**. Click **Add Other**.
5. To add one IP address at a time, select **Host IP** from the drop-down list and type the IP address in the adjacent text box. Click **OK** twice.
6. Repeat Steps 3–4 for each IP address in the NAT address range.
 

To add several IP addresses at once, select **Host Range** in the drop-down list. Type the first and last IP addresses from the NAT Base range and click **OK** twice.

**Note** To connect to a computer located on a different interface that uses 1-to-1 NAT, you must use that computer's public (NAT base) IP address. If this is a problem, you can disable 1-to-1 NAT and use static NAT.

## Define a 1-to-1 NAT Rule

In each 1-to-1 NAT rule, you can configure a host, a range of hosts, or a subnet. You must also configure:

### *Interface*

The name of the Ethernet interface on which 1-to-1 NAT is applied. Your XTM device applies 1-to-1 NAT for packets sent in to, and out of, the interface. In our example above, the rule is applied to the external interface.

### *NAT base*

When you configure a 1-to-1 NAT rule, you configure the rule with a *from* and a *to* range of IP addresses. The NAT base is the first available IP address in the *to* range of addresses. The NAT base IP address is the address that the real base IP address changes to when the 1-to-1 NAT is applied. You cannot use the IP address of an existing Ethernet interface as your NAT base. In our example above, the NAT base is 50.50.50.1.

### *Real base*

When you configure a 1-to-1 NAT rule, you configure the rule with a *from* and a *to* range of IP addresses. The Real base is the first available IP address in the *from* range of addresses. It is the IP address assigned to the physical Ethernet interface of the computer to which you will apply the 1-to-1 NAT policy. When packets from a computer with a real base address go through the specified interface, the 1-to-1 action is applied. In the example above, the Real base is 10.0.1.50.

### *Number of hosts to NAT (for ranges only)*

The number of IP addresses in a range to which the 1-to-1 NAT rule applies. The first real base IP address is translated to the first NAT Base IP address when 1-to-1 NAT is applied. The second real base IP address in the range is translated to the second NAT base IP address when 1-to-1 NAT is applied. This is repeated until the *Number of hosts to NAT* is reached. In the example above, the number of hosts to apply NAT to is 5.

You can also use 1-to-1 NAT when you must create a VPN tunnel between two networks that use the same private network address. When you create a VPN tunnel, the networks at each end of the VPN tunnel must have different network address ranges. If the network range on the remote network is the same as on the local network, you can configure both gateways to use 1-to-1 NAT. Then, you can create the VPN tunnel and not change the IP addresses of one side of the tunnel. You configure 1-to-1 NAT for a VPN tunnel when you configure the VPN tunnel and not in the **Network > NAT** dialog box.

For an example of how to use 1-to-1 NAT, see *1-to-1 NAT Example*.

## Configure Policy-Based 1-to-1 NAT

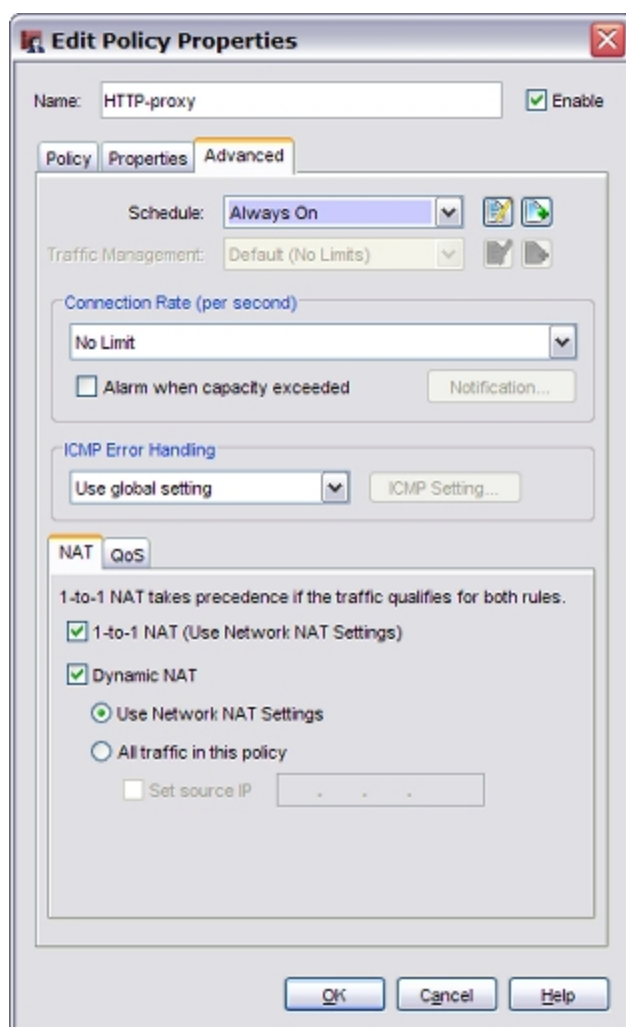
In policy-based 1-to-1 NAT, your XTM device uses the private and public IP ranges that you set when you configured global 1-to-1 NAT, but the rules are applied to an individual policy. 1-to-1 NAT is enabled in the default configuration of each policy. If traffic matches both 1-to-1 NAT and dynamic NAT policies, 1-to-1 NAT takes precedence.

### Enable Policy-Based 1-to-1 NAT

Because policy-based 1-to-1 NAT is enabled by default, you do not need to do anything else to enable it. If you have previously disabled policy-based 1-to-1 NAT, select the check box in Step 3 of the subsequent procedure to enable it again.

### Disable Policy-Based 1-to-1 NAT

1. Right-click a policy and select **Modify Policy**.  
*The Edit Policy Properties dialog box appears.*
2. Click the **Advanced** tab.



3. Clear the **1-to-1 NAT** check box to disable NAT for the traffic controlled by this policy.
4. Click **OK**.
5. *Save the Configuration File.*

## Configure NAT Loopback with Static NAT

Fireware XTM includes support for NAT loopback. NAT loopback allows a user on the trusted or optional networks to get access to a public server that is on the same physical XTM device interface by its public IP address or domain name. For NAT loopback connections, the XTM device changes the source IP address of the connect to be the IP address of the internal XTM device interface (the primary IP address for the interface where the client and server both connect to the XTM device).

To understand how to configure NAT loopback when you use static NAT, we give this example:

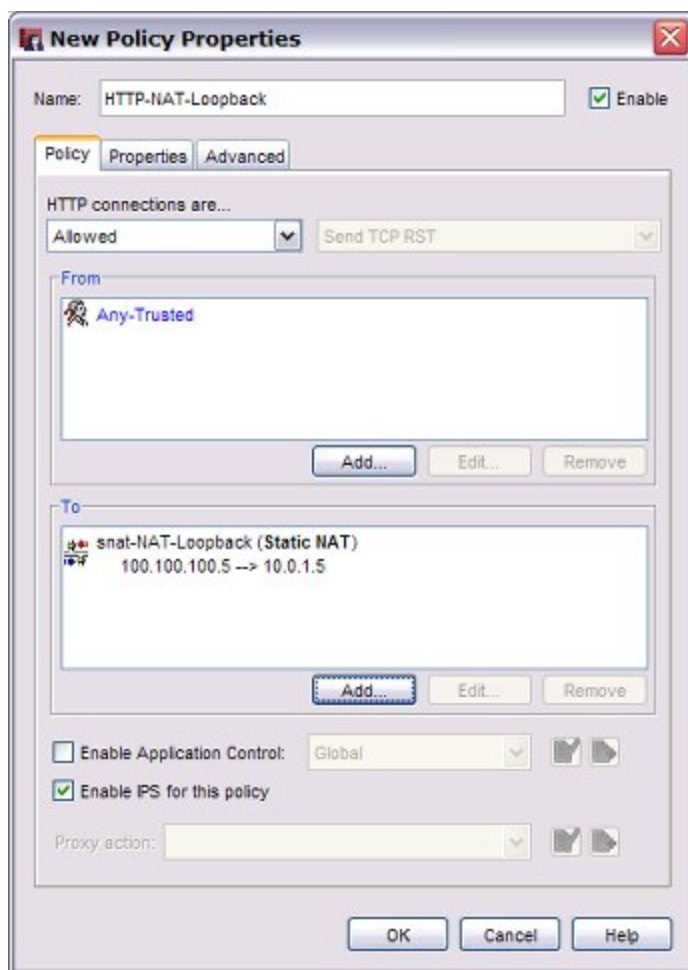
Company ABC has an HTTP server on the XTM device trusted interface. The company uses static NAT to map the public IP address to the internal server. The company wants to allow users on the trusted network to use the public IP address or domain name to get access to this public server.

For this example, we assume:

- The trusted interface is configured with an IP address on the 10.0.1.0/24 network
- The trusted interface is also configured with a secondary IP address on the 192.168.2.0/24 network
- The HTTP server is physically connected to the 10.0.1.0/24 network. The Real Base address of the HTTP server is on the trusted network.

## Add a Policy for NAT Loopback to the Server

In this example, to allow users on your trusted and optional networks to use the public IP address or domain name to access a public server that is on the trusted network, you must create an SNAT action and add it to an HTTP policy. The policy addresses could look like this:



The **To** section of the policy contains an SNAT action that defines a static NAT route from the public IP address of the HTTP server to the real IP address of that server.

For more information about static NAT, see *Configure Static NAT* on page 179.

If you use 1-to-1 NAT to route traffic to servers inside your network, see *NAT Loopback and 1-to-1 NAT* on page 175.

## NAT Loopback and 1-to-1 NAT

NAT loopback allows a user on the trusted or optional networks to connect to a public server with its public IP address or domain name if the server is on the same physical XTM device interface. If you use 1-to-1 NAT to route traffic to servers on the internal network, use these instructions to configure NAT loopback from internal users to those servers. If you do not use 1-to-1 NAT, see *Configure NAT Loopback with Static NAT* on page 173.

To understand how to configure NAT loopback when you use 1-to-1 NAT, we give this example:

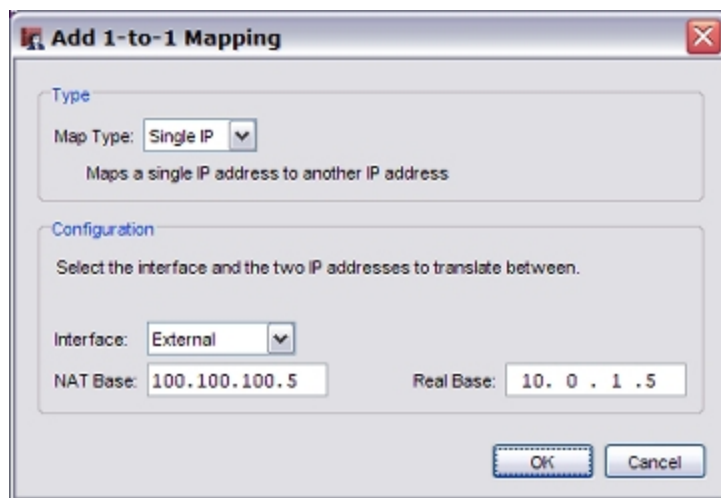
Company ABC has an HTTP server on the XTM device trusted interface. The company uses a 1-to-1 NAT rule to map the public IP address to the internal server. The company wants to allow users on the trusted interface to use the public IP address or domain name to access this public server.

For this example, we assume:

- A server with public IP address 100.100.100.5 is mapped with a 1-to-1 NAT rule to a host on the internal network.

*In the 1-to-1 NAT tab of the NAT Setup dialog box, select these options:*

Interface — **External**, NAT Base — **100.100.100.5**, Real Base — **10.0.1.5**

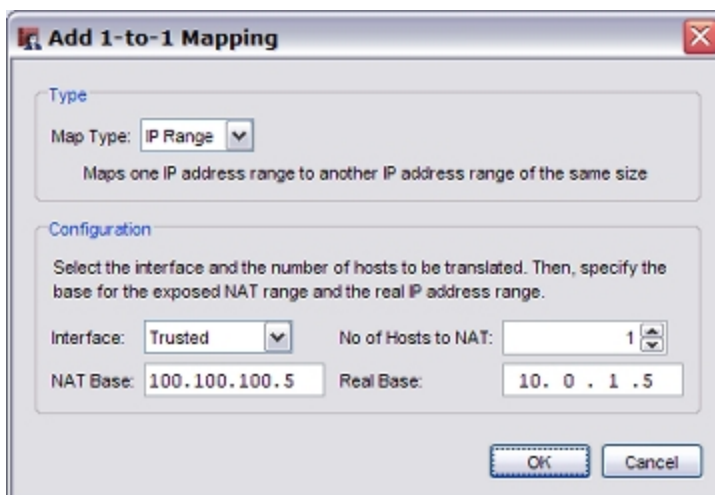


- The trusted interface is configured with a primary network, 10.0.1.0/24
- The HTTP server is physically connected to the network on the trusted interface. The **Real Base** address of that host is on the trusted interface.
- The trusted interface is also configured with a secondary network, 192.168.2.0/24.

For this example, to enable NAT loopback for all users connected to the trusted interface, you must:

1. Make sure that there is a 1-to-1 NAT entry for each interface that traffic uses when internal computers get access to the public IP address 100.100.100.5 with a NAT loopback connection.

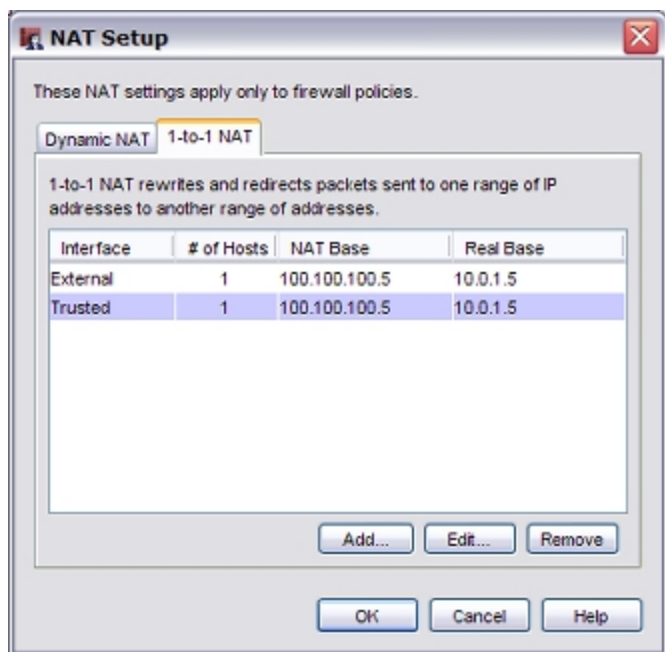
You must add one more 1-to-1 NAT mapping to apply to traffic that starts from the trusted interface. The new 1-to-1 mapping is the same as the previous one, except that the **Interface** is set to **Trusted** instead of **External**.



After you add the second 1-to-1 NAT entry, the **1-to-1 NAT** tab on the **NAT Setup** dialog box shows two 1-to-1 NAT mappings: one for External and one for Trusted.

*In the 1-to-1 NAT tab of the NAT Setup dialog box, add these two entries:*

- Interface — **External**, NAT Base — **100.100.100.5**, Real Base — **10.0.1.5**
- Interface — **Trusted**, NAT Base — **100.100.100.5**, Real Base — **10.0.1.5**



2. Add a Dynamic NAT entry for every network on the interface that the server is connected to.

The **From** field for the Dynamic NAT entry is the network IP address of the network from which computers get access to the 1-to-1 NAT IP address with NAT loopback.

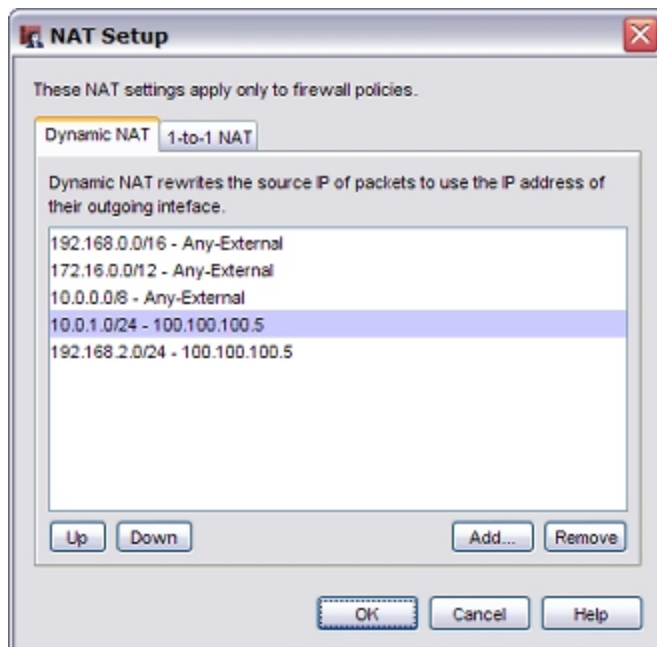
The **To** field for the Dynamic NAT entry is the NAT base address in the 1-to-1 NAT mapping.



For this example, the trusted interface has two networks defined, and we want to allow users on both networks to get access to the HTTP server with the public IP address or host name of the server. We must add two Dynamic NAT entries.

*In the Dynamic NAT tab of the NAT Setup, add:*

10.0.1.0/24 - 100.100.100.5  
192.168.2.0/24 - 100.100.100.5



3. Add a policy to allow users on your trusted network to use the public IP address or domain name to get access to the public server on the trusted network. For this example:

*From*

Any-Trusted

*To*

100.100.100.5



The public IP address that users want to connect to is 100.100.100.5. This IP address is configured as a secondary IP address on the external interface.

In the **To** section of the policy, add 100.100.100.5 .

For more information about configuring static NAT, see *Configure Static NAT* on page 179.

For more information about how to configure 1-to-1 NAT, see *Configure Firewall 1-to-1 NAT* on page 169.

## Configure Static NAT

Static NAT, also known as port forwarding, is a port-to-host NAT. A host sends a packet from the external network to a port on an external interface. Static NAT changes the destination IP address to an IP address and port behind the firewall. If a software application uses more than one port and the ports are selected dynamically, you must either use 1-to-1 NAT, or check whether a proxy on your XTM device manages this kind of traffic. Static NAT also operates on traffic sent from networks that your XTM device protects.

When you use static NAT, you use an external IP address from your XTM device instead of the IP address from a public server. You could do this because you choose to, or because your public server does not have a public IP address. For example, you can put your SMTP email server behind your XTM device with a private IP address and configure static NAT in your SMTP policy. Your XTM device receives connections on port 25 and makes sure that any SMTP traffic is sent to the real SMTP server behind the XTM device.

## Add a Static NAT Action

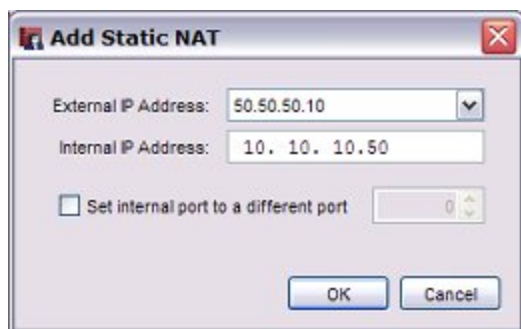
You can create a static NAT action and then add it to a policy, or you can create the static NAT action from within the policy configuration. In either case, after you add the SNAT action, you can use it in multiple policies.

To add a static NAT action before you add it to a policy:

1. In Policy Manager, select **Setup > Actions > SNAT**.  
*The SNAT dialog box appears.*
2. Click **Add**.  
*The Add SNAT dialog box appears.*



3. In the **SNAT Name** text box, type a name for this SNAT action. Optionally, type a **Description**.
4. Select the **Static NAT** radio button to specify a static NAT action.  
*This is the default selection.*
5. Click **Add**.  
*The Add Static NAT dialog box appears.*



6. In the **External IP address** drop-down list, select the external IP address or alias you want to use in this action.

For example, you can use static NAT for packets received on only one external IP address. Or, you can use static NAT for packets received on any external IP address if you select the Any-External alias.

7. Type the **Internal IP Address**. This is the destination on the trusted or optional network.
8. If necessary, select the **Set internal port to a different port** check box. This enables port address translation (PAT).

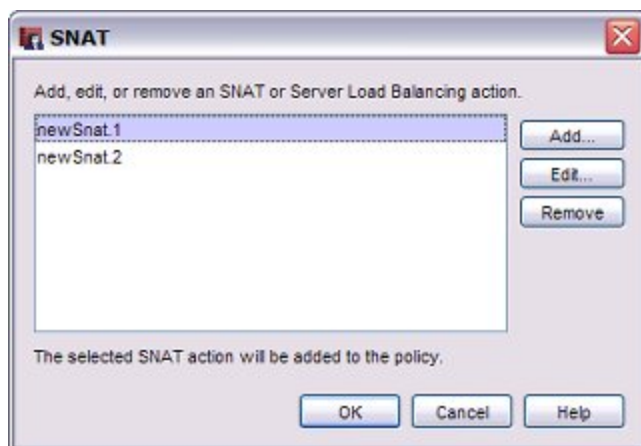
This feature enables you to change the packet destination not only to a specified internal host but also to a different port. If you select this check box, type the port number or click the up or down arrow to select the port you want to use.

**Note** If you use static NAT in a policy that allows traffic that does not have ports (traffic other than TCP or UDP), the internal port setting is not used for that traffic.

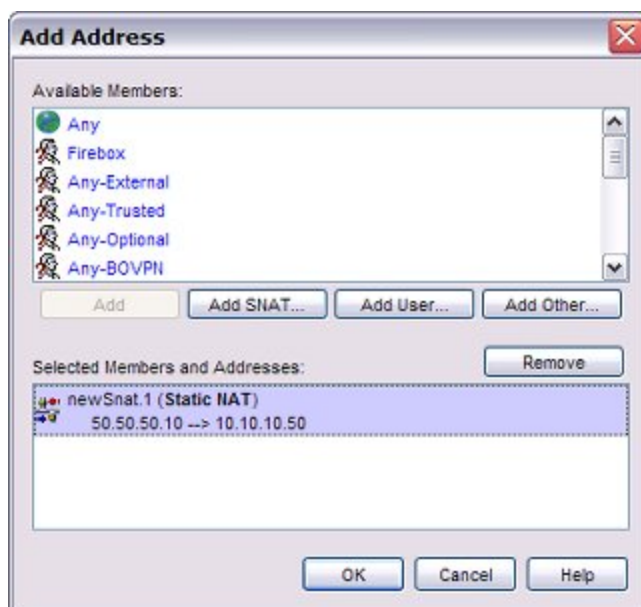
9. Click **OK**.  
*The static NAT route appears in the SNAT Members list.*
10. Click **OK**.  
*The new SNAT action appears in the SNAT dialog box.*

## Add a Static NAT Action to a Policy

1. In Policy Manager, double-click a policy to edit it.
2. From the **Connections are** drop-down list, select **Allowed**.  
To use static NAT, the policy must let incoming traffic through.
3. Below the **To** list, click **Add**.  
*The Add Address dialog box appears.*
4. Click **Add SNAT**.  
*The SNAT dialog box appears. It shows a list of the configured static NAT and Server Load Balancing actions.*



5. Select a configured SNAT action to add. Click **OK**.  
Or, click **Add** to define a new static NAT action. Use the steps in the previous procedure to configure the static NAT action.
6. Click **OK** to close the **SNAT** dialog box.  
*The static NAT route appears in the Members and Addresses list.*



7. Click **OK** to close the **Add Address** dialog box.
8. Click **OK** to close the **Policy Properties** dialog box.

## Edit or Remove a Static NAT Action

To edit an SNAT action:

1. In Policy Manager, select **Setup > Actions > SNAT**.  
*The SNAT dialog box appears.*
2. Click an SNAT action to select it.
3. Click **Edit** to edit the SNAT action.

4. Make any changes you want to the SNAT action.  
*When you edit an SNAT action, any changes you make apply to all policies that use that SNAT action.*
5. Click **OK**.

To remove an SNAT action:

1. In Policy Manager, select **Setup > Actions > SNAT**.  
*The SNAT dialog box appears.*
2. Click an SNAT action to select it.
3. Click **Remove** to remove the SNAT action.  
*You cannot remove an SNAT action that is used by a policy.*
4. Click **Yes** to confirm that you want to remove the action.
5. Click **OK**.

## Configure Server Load Balancing

**Note** To use the server load balancing feature your XTM device must have an XTM 5 Series, 8 Series, or XTM 1050 device and Fireware XTM with a Pro upgrade.

The server load balancing feature in Fireware XTM is designed to help you increase the scalability and performance of a high-traffic network with multiple public servers. With server load balancing, you can enable the XTM device to control the number of sessions initiated to as many as 10 servers for each firewall policy you configure. The XTM device controls the load based on the number of sessions in use on each server. The XTM device does not measure or compare the bandwidth that is used by each server.

You configure server load balancing as an SNAT action. The XTM device can balance connections among your servers with two different algorithms. When you configure server load balancing, you must choose the algorithm you want the XTM device to apply.

### *Round-robin*

If you select this option, the XTM device distributes incoming sessions among the servers you specify in the policy in round-robin order. The first connection is sent to the first server specified in your policy. The next connection is sent to the next server in your policy, and so on.

### *Least Connection*

If you select this option, the XTM device sends each new session to the server in the list that currently has the lowest number of open connections to the device. The XTM device cannot tell how many connections the server has open on other interfaces.

You can add any number of servers to a server load balancing action. You can also add a weight to each server to make sure that your most powerful servers are given the heaviest load. By default, each server has a weight of 1. The weight refers to the proportion of load that the XTM device sends to a server. If you assign a weight of 2 to a server, you double the number of sessions that the XTM device sends to that server, compared to a server with a weight of 1.

When you configure server load balancing, it is important to know:

- You can configure server load balancing for any policy to which you can apply static NAT.
- If you apply server load balancing to a policy, you cannot set policy-based routing or other NAT rules in the same policy.

- The XTM device does not modify the *sender*, or source IP address, of traffic sent to these devices. While the traffic is sent directly from the XTM device, each device that is part of your server load balancing configuration sees the original source IP address of the network traffic.
- If you use server load balancing in an active/passive FireCluster configuration, real-time synchronization does not occur between the cluster members when a failover event occurs. When the passive backup master becomes the active cluster master, it sends connections to all servers in the server load balancing list to see which servers are available. It then applies the server load balancing algorithm to all available servers.
- If you use server load balancing for connections to a group of RDP servers, you must configure the firewall on each RDP server to allow ICMP requests from the XTM device.

## Add a Server Load Balancing SNAT Action

You can create a server load balancing SNAT action and then add it to a policy, or you can create the server load balancing SNAT action from within the policy configuration. In either case, after you add the SNAT action, you can use it in multiple policies.

To add a server load balancing SNAT action before you add it to a policy:

1. In Policy Manager, select **Setup > Actions > SNAT**.  
*The SNAT dialog box appears.*
2. Click **Add**.  
*The Add SNAT dialog box appears.*
3. In the **SNAT Name** text box, type a name for this action. Optionally, type a **Description**.
4. Select the **Server Load Balancing** radio button to configure a Server Load Balancing SNAT action.
5. Click **Add**.  
*The Add Server Load Balancing NAT dialog box appears.*



6. From the **External IP address** drop-down list, select the external IP address or alias you want to use in this server load balancing action.

For example, you can have the XTM device apply server load balancing for this action to packets received on only one external IP address. Or, you can have the XTM device apply server load balancing for packets received on any external IP address if you select the Any-External alias.

7. From the **Method** drop-down list, select the algorithm you want the XTM device to use for server load balancing: **Round-robin** or **Least Connection**.
8. Click **Add** to add the IP address of an internal server to this action.  
*The Add Server dialog box appears.*

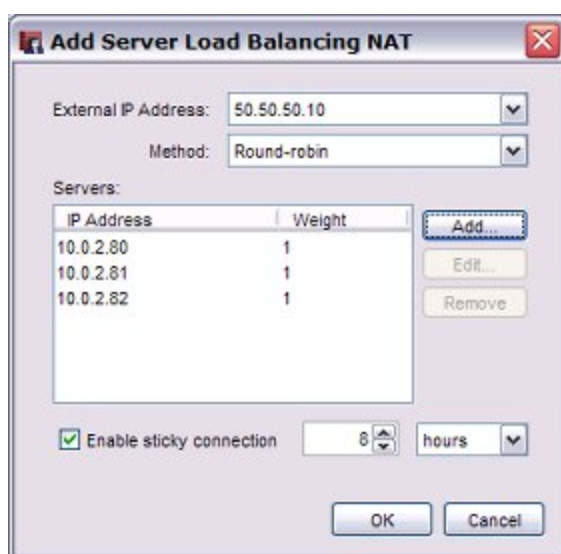


9. In the **IP Address** text box, type the IP address of the server to add.
10. In the **Weight** text box, select the weight for this server for load balancing.
11. If necessary, select the **Set internal port to a different port** check box. This enables port address translation (PAT).

This feature enables you to change the packet destination not only to a specified internal host but also to a different port. If you select this check box, type the port number or click the up or down arrow to select the port you want to use.

**Note** If you use static NAT in a policy that allows traffic that does not have ports (traffic other than TCP or UDP), the internal port setting is not used for that traffic.

12. Click **OK**.  
*The server is added to the Servers list for this action.*





13. Click **Add** to add another server to this action.
14. To set sticky connections for your internal servers, select the **Enable sticky connection** check box and set the time period in the **Enable sticky connection** text box and drop-down list.

A sticky connection is a connection that continues to use the same server for a defined period of time. Stickiness makes sure that all packets between a source and destination address pair are sent to the same server for the time period you specify.

15. Click **OK**.

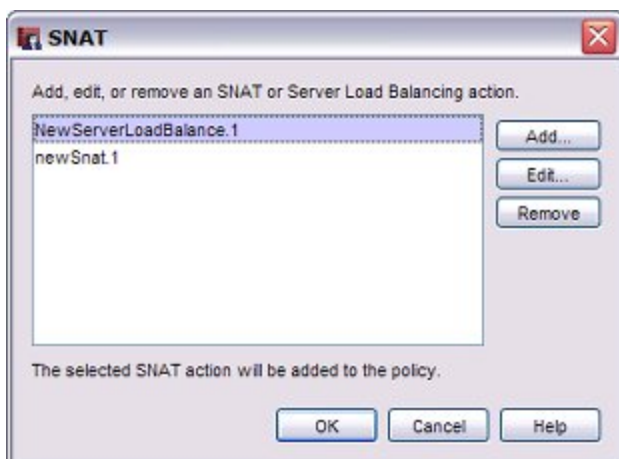
*The servers are added to the SNAT Members list for this action.*



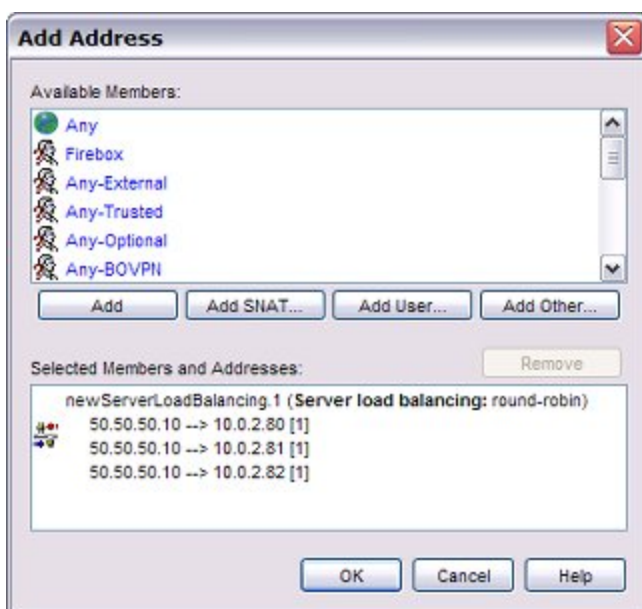
16. Click **OK**.  
The SNAT action is added.
17. Click **OK**.

## Add a Server Load Balancing SNAT Action to a Policy

1. Double-click the policy to which you want to apply server load balancing.  
Or, highlight the policy and select **Edit > Modify Policy**.  
To create a new policy and enable server load balancing in that policy, select **Edit > Add Policy**.
2. In the **To** section, click **Add**.  
*The Add Address dialog box appears.*
3. Click **Add SNAT**.  
*The SNAT dialog box appears. This list shows all configured Static NAT and Server Load Balancing actions.*



4. Select a configured Server Load Balancing Action to add. Click **OK**.  
Or, click **Add** to define a new Server Load Balancing action. Use the steps in the previous procedure to configure the server load balancing SNAT action.  
*The selected server load balancing action appears in the Add Address dialog box.*



5. Click **OK** to close the **Add Address** dialog box.
6. Click **OK** to close the **Policy Properties** dialog box.

## Edit or Remove a Server Load Balancing SNAT Action

To edit an SNAT action:

1. In Policy Manager, select **Setup > Actions > SNAT**.  
*The SNAT dialog box appears.*
2. Click an SNAT action to select it.
3. Click **Edit** to edit the SNAT action.

4. Make any changes you want to the SNAT action.  
*When you edit an SNAT action, any changes you make apply to all policies that use that SNAT action.*
5. Click **OK**.

To remove an SNAT action:

1. In Policy Manager, select **Setup > Actions > SNAT**.  
*The SNAT dialog box appears.*
2. Click an SNAT action to select it.
3. Click **Remove** to remove the SNAT action.  
*You cannot remove an SNAT action that is used by a policy.*
4. Click **Yes** to confirm that you want to remove the action.
5. Click **OK**.

## NAT Examples

### 1-to-1 NAT Example

When you enable 1-to-1 NAT, the XTM device changes and routes all incoming and outgoing packets sent from one range of addresses to a different range of addresses.

Consider a situation in which you have a group of internal servers with private IP addresses that must each show a different public IP address to the outside world. You can use 1-to-1 NAT to map public IP addresses to the internal servers, and you do not have to change the IP addresses of your internal servers. To understand how to configure 1-to-1 NAT, consider this example:

A company has a group of three privately addressed servers behind an optional interface of their XTM device. The addresses of these servers are:

10.0.2.11  
10.0.2.12  
10.0.2.13

The administrator selects three public IP addresses from the same network address as the external interface of their XTM device, and creates DNS records for the servers to resolve to. These addresses are:

50.50.50.11  
50.50.50.12  
50.50.50.13

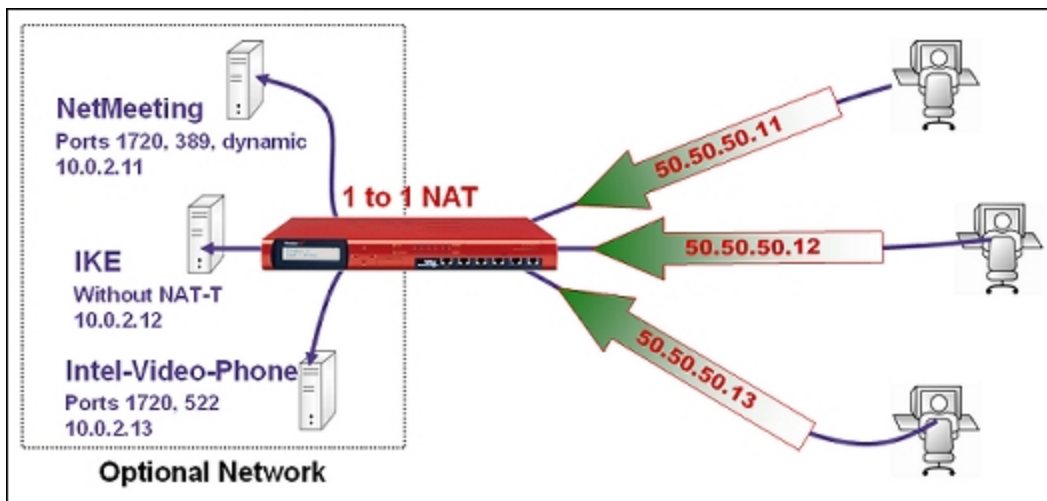
Now the administrator configures a 1-to-1 NAT rule for the servers. The 1-to-1 NAT rule builds a static, bidirectional relationship between the corresponding pairs of IP addresses. The relationship looks like this:

10.0.2.11 <--> 50.50.50.11

10.0.2.12 <--> 50.50.50.12

10.0.2.13 <--> 50.50.50.13

When the 1-to-1 NAT rule is applied, the XTM device creates the bidirectional routing and NAT relationship between the pool of private IP addresses and the pool of public addresses.



For the instructions to define a 1-to-1 NAT rule, see *Configure Firewall 1-to-1 NAT*.

# 9 Wireless Setup

---

## About Wireless Configuration

When you enable the wireless feature of the XTM wireless device, you can configure the external interface to use wireless, or you can configure the XTM device as a wireless access point for users on the trusted, optional, or guest networks.

Before you set up wireless network access, see *Before You Begin* on page 191.

**Note** Before you can enable wireless, you must get the feature key for your device.  
For more information, see *About Feature Keys* on page 58.

To enable the wireless feature on your XTM device:

1. Select **Network > Wireless**.

*The Wireless Configuration dialog box appears.*

<input checked="" type="checkbox"/> Enable wireless		
<input type="radio"/> Enable wireless client as external interface		Configure...
<input checked="" type="radio"/> Enable wireless access points		
Access point 1	Enabled	Configure...
Access point 2	Disabled	Configure...
Wireless guest	Disabled	Configure...

2. Select the **Enable wireless** check box.
3. In the **Wireless Configuration** dialog box, select a wireless configuration option:

*Enable wireless client as external interface*

This setting allows you to configure the external interface of the XTM wireless device to connect to a wireless network. This is useful in areas with limited or no existing network infrastructure.

For information about how to configure the external interface as wireless, see *Configure Your External Interface as a Wireless Interface* on page 211.

#### *Enable wireless access points*

This setting allows you to configure the XTM wireless device as an access point for users on the trusted, optional or guest networks.

For more information, see *About Wireless Access Point Configuration* on page 190.

4. In the **Radio Settings** section, select your wireless radio settings.

For more information, see *About Wireless Radio Settings* on page 215.

5. Select the **Enable rogue access point detection** check box to enable the device to scan for untrusted wireless access points.

For more information, see *Enable Rogue Access Point Detection* on page 218.

6. Click **OK**.

## About Wireless Access Point Configuration

Any XTM wireless device can be configured as a wireless access point with three different security zones. You can enable other wireless devices to connect to the XTM wireless device as part of the trusted network or part of the optional network. You can also enable a wireless guest services network for XTM device users. Computers that connect to the guest network connect through the XTM wireless device, but do not have access to computers on the trusted or optional networks.

Before you enable the XTM wireless device as a wireless access point, you must look carefully at the wireless users who connect to the device and determine the level of access you want for each type of user. There are three types of wireless access you can allow:

#### *Allow Wireless Connections to a Trusted Interface*

When you allow wireless connections through a trusted interface, wireless devices have full access to all computers on the trusted and optional networks, and full Internet access based on the rules you configure for outgoing access on your XTM device. If you enable wireless access through a trusted interface, we strongly recommend that you enable and use the MAC restriction feature to allow access through the XTM device only for devices you add to the Allowed MAC Address list.

For more information about restricting access by MAC addresses, see *Use Static MAC Address Binding* on page 118.

#### *Allow Wireless Connections to an Optional Interface*

When you allow wireless connections through an optional interface, those wireless devices have full access to all computers on the optional network, and full Internet access based on the rules you configure for outgoing access on your XTM wireless device.

### *Allow Wireless Guest Connections Through the External Interface*

Computers that connect to the wireless guest network connect through the XTM wireless device to the Internet based on the rules you configure for outgoing access on your XTM device.

These wirelessly connected computers do not have access to computers on the trusted or optional network.

For more information about how to configure a wireless guest network, see *Enable a Wireless Guest Network* on page 204.

Before you set up wireless network access, see *Before You Begin* on page 191.

To allow wireless connections to your trusted or optional network, see *Enable Wireless Connections to the Trusted or Optional Network* on page 201.

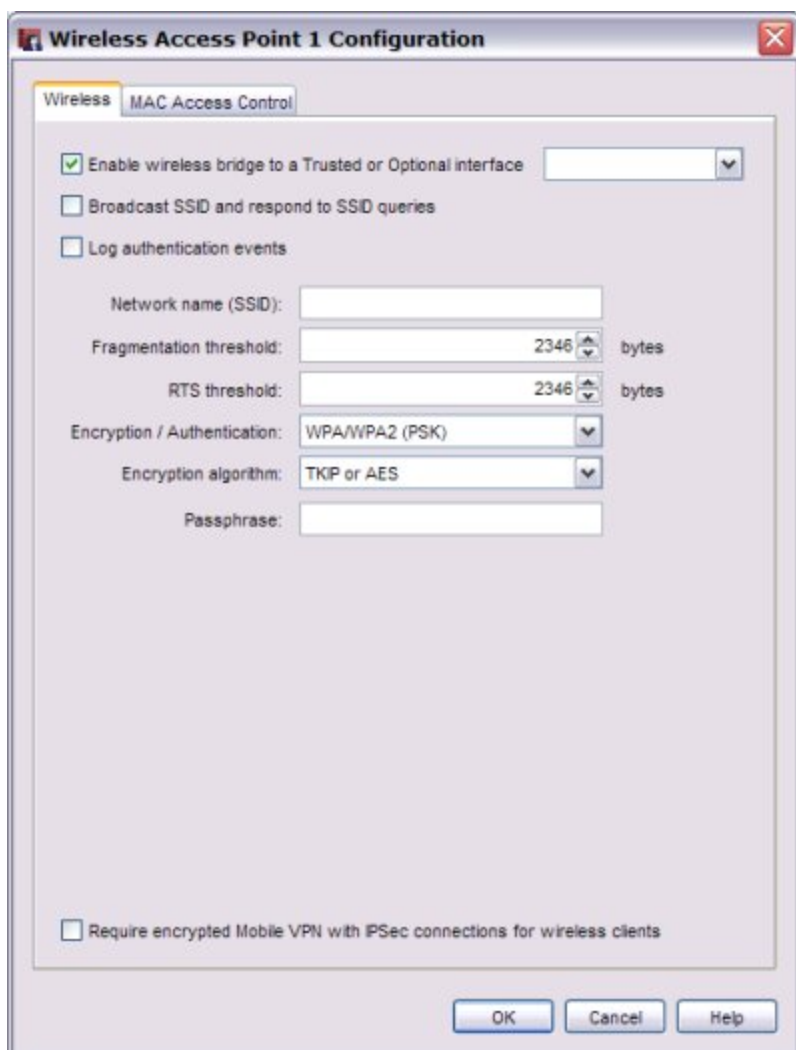
## Before You Begin

WatchGuard XTM wireless devices adhere to 802.11n, 802.11b and 802.11g guidelines set by the Institute of Electrical and Electronics Engineers (IEEE). When you install an XTM wireless device:

- Make sure that the wireless device is installed in a location more than 20 centimeters from all persons. This is an FCC requirement for low power transmitters.
- It is a good idea to install the wireless device away from other antennas or transmitters to decrease interference
- The default wireless authentication algorithm configured for each wireless security zone is not the most secure authentication algorithm. If you the wireless devices that connect to your XTM wireless device can operate correctly with WPA2, we recommend that you increase the authentication level to WPA2.
- A wireless client that connects to the XTM wireless device from the trusted or optional network can be a part of any branch office VPN tunnels in which the local network component of the Phase 2 settings includes optional or trusted network IP addresses. To control access to the VPN tunnel, you can force XTM device users to authenticate.

## About Wireless Configuration Settings

When you enable wireless access to the trusted, optional, or wireless guest network, some configuration settings are defined the same way for each of the three security zones. These can be set to different values for each zone.



For information about the **Broadcast SSID and respond to SSID queries** setting, see *Enable/Disable SSID Broadcasts* on page 193.

For information about setting the **Network Name (SSID)**, see *Change the SSID* on page 193.

For information about the **Log Authentication Events** setting, see *Log Authentication Events* on page 193.

For information about the **Fragmentation Threshold**, see *Change the Fragmentation Threshold* on page 193.

For information about the **RTS Threshold**, see *Change the RTS Threshold* on page 195.

For information about the **Encryption (Authentication)** setting, see *Set the Wireless Authentication Method* on page 196.

For information about the **Encryption algorithm** setting, see *Set the Encryption Level* on page 200.



## Enable/Disable SSID Broadcasts

Computers with wireless network cards send requests to see whether there are wireless access points to which they can connect.

To configure an XTM device wireless interface to send and answer these requests, select the **Broadcast SSID and respond to SSID queries** check box. For security, enable this option only while you configure computers on your network to connect to the XTM wireless device. Disable this option after all your clients are configured. If you use the wireless guest services feature, it can be necessary to allow SSID broadcasts in standard operation.

## Change the SSID

The SSID (Service Set Identifier) is the unique name of your wireless network. To use the wireless network from a client computer, the wireless network card in the computer must have the same SSID as the WatchGuard wireless network to which the computer connects.

The Fireware XTM OS automatically assigns an SSID to each wireless network. This SSID uses a format that contains the interface name and the 5th-9th digits from the XTM wireless device serial number. To change the SSID, type a new name in the SSID field to uniquely identify your wireless network.

## Log Authentication Events

An authentication event occurs when a wireless computer tries to connect to the wireless interface of a WatchGuard XTM wireless device. To include these events in the log file, select the **Log Authentication Events** check box.

## Change the Fragmentation Threshold

Fireware XTM allows you to set the maximum frame size the XTM wireless device can send and not fragment the frame. This is called the fragmentation threshold. This setting is rarely changed. The default setting is the maximum frame size of 2346, which means that it will never fragment any frames that it sends to wireless clients. This is best for most environments.

## When to Change the Default FragmentationThreshold

A collision happens when two devices that use the same medium transmit packets at exactly the same time. The two packets can corrupt each other, and the result is a group of unreadable pieces of data. If a packet results in a collision, the packet is discarded and it must be transmitted again. This adds to the overhead on the network and can reduce the throughput or speed of the network.

Larger frames are more likely to collide with each other than smaller frames. To make the wireless packets smaller, you lower the fragmentation threshold on the XTM wireless device. If you lower the maximum frame size, it can reduce the number of repeat transmissions caused by collisions, and lower the overhead caused by repeat transmissions.

Smaller frames introduce more overhead on the network. This is especially true on a wireless network, because every fragmented frame sent from one wireless device to another requires the receiving device to acknowledge the frame. When packet error rates are high (more than five or ten percent collisions or errors), you can help improve the performance of the wireless network if you lower the fragmentation threshold. The time that is saved when you reduce repeat transmissions can be enough to offset the extra overhead added with smaller packets. This can result in higher throughput.

If the rate of packet error is low and you lower the fragmentation threshold, wireless network performance decreases. This occurs because when you lower the threshold, protocol overhead is added and protocol efficiency is reduced.

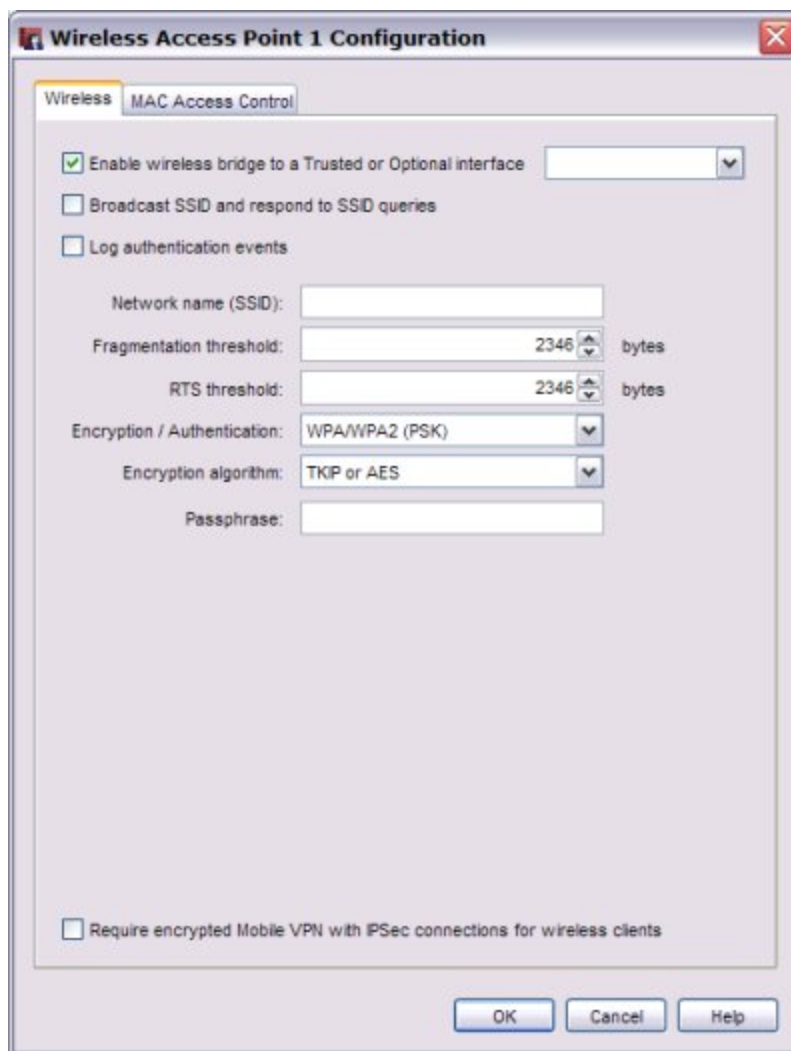
If you want to experiment, start with the default maximum 2346, and lower the threshold a small amount at a time. To get the most benefit, you must monitor the network for packet errors at different times of the day. Compare the effect that a lower threshold has on network performance when errors are very high with the effect on performance when errors are moderately high.

In general, we recommend that you leave this setting at its default of 2346.

## Change the Fragmentation Threshold

1. Select **Network > Wireless**.
2. Select the wireless network to configure. Adjacent to **Access point 1** or **Access point 2** or **Wireless Guest**, click **Configure**.

*The wireless configuration settings for that wireless network appear.*



3. To change the fragmentation threshold, in the **Fragmentation Threshold** text box, type or select a value between 256 and 2346.
4. Click **OK**.
5. Save the configuration.

## Change the RTS Threshold

RTS/CTS (Request To Send / Clear To Send) helps prevent problems when wireless clients can receive signals from more than one wireless access point on the same channel. The problem is sometimes known as *hidden node*.

We do not recommend that you change the default RTS threshold. When the **RTS Threshold** is set to the default of 2346, RTS/CTS is disabled.

If you must change the RTS threshold, adjust it incrementally. Lower it a small amount at a time. After each change, allow enough time to decide whether the change in network performance is positive before you change it again. If you lower this value too much, you can introduce more latency into the network, as *Requests to Send* are increased so much that the shared medium is reserved more often than necessary.

## About Wireless Security Settings

WatchGuard XTM wireless devices use three security protocol standards to protect your wireless network: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), and WPA2. Each protocol standard can encrypt the transmissions on the wireless LAN between the computers and the access points. They also can prevent unauthorized access to the wireless access point.

To protect privacy, you can use these features together with other LAN security mechanisms such as password protection, VPN tunnels, and user authentication.

## Set the Wireless Authentication Method

From the **Encryption (Authentication)** drop-down list in the wireless access point configuration, select the level of authentication method for your wireless connections. The eight available authentication methods, from least secure to most secure, are listed below. Select the most secure authentication method that is supported by your wireless network clients.

### Open System and Shared Key

The Open System and Shared Key authentication methods use WEP encryption. WEP is not as secure as WPA2 and WPA (Wi-Fi Protected Access). We recommend you do not use these less secure methods unless your wireless clients do not support WPA or WPA2.

- **Open System** — Open System authentication allows any user to authenticate to the access point. This method can be used with no encryption or with WEP encryption.
- **Shared Key** — In Shared Key authentication, only those wireless clients that have the shared key can connect. Shared Key authentication can be used only with WEP encryption.

### WPA and WPA2 with Pre-Shared Keys

WPA (PSK) and WPA2 (PSK) Wi-Fi Protected Access methods use pre-shared keys for authentication. WPA (PSK) and WPA2 (PSK) are more secure than WEP shared key authentication. When you choose one of these methods, you configure a pre-shared key that all wireless devices must use to authenticate to the wireless access point.

The XTM wireless device supports three wireless authentication settings that use pre-shared keys:

- **WPA ONLY (PSK)** — The XTM wireless device accepts connections from wireless devices configured to use WPA with pre-shared keys.
- **WPA/WPA2 (PSK)** — The XTM wireless device accepts connections from wireless devices configured to use WPA or WPA2 with pre-shared keys.
- **WPA2 ONLY (PSK)** — The XTM wireless device accepts connections from wireless devices configured to use WPA2 with pre-shared keys authentication. WPA2 implements the full 802.11i standard; it does not work with some older wireless network cards.

## WPA and WPA2 with Enterprise Authentication

The WPA Enterprise and WPA2 Enterprise authentication methods use the IEEE 802.1X standard for network authentication. These authentication methods use the EAP (Extensible Authentication Protocol) framework to enable user authentication to an external RADIUS authentication server or to the XTM device (Firebox-DB). The WPA Enterprise and WPA2 Enterprise authentication methods are more secure than WPA/WPA2 (PSK) because users authenticate with their own credentials instead of a shared key.

The XTM wireless device supports three WPA and WPA2 Enterprise wireless authentication methods:

- **WPA Enterprise** — The XTM wireless device accepts connections from wireless devices configured to use WPA Enterprise authentication.
- **WPA/WPA2 Enterprise** — The XTM wireless device accepts connections from wireless devices configured to use WPA Enterprise or WPA2 Enterprise authentication.
- **WPA2 Enterprise** — The XTM wireless device accepts connections from wireless devices configured to use WPA2 Enterprise authentication. WPA2 implements the full 802.11i standard; it does not work with some older wireless network cards.

For more information about these authentication methods, see *WPA and WPA2 Enterprise Authentication*.

To use the Enterprise authentication methods, you must configure an external RADIUS authentication server or configure the XTM device as an authentication server.

For more information about how to configure the settings for these authentication methods, see

- *Use a RADIUS Server for Wireless Authentication*
- *Use the XTM Device as an Authentication Server for Wireless Authentication*

## Use a RADIUS Server for Wireless Authentication

If you select the **WPA Enterprise**, **WPA2 Enterprise**, or **WPA/WPA2 Enterprise** authentication methods in your wireless configuration, you can use a RADIUS server for wireless authentication.

To configure your wireless access point to use RADIUS authentication:

1. Select **Network > Wireless**.
2. Click **Configure** adjacent to the **Access point 1**, **Access point 2**, or **Wireless Guest** configuration.
3. Select the **Wireless** tab.
4. From the **Encryption (Authentication)** drop-down list, select **WPA Enterprise**, **WPA2 Enterprise**, or **WPA/WPA2 Enterprise**.

*The Encryption, Authentication server, and EAP authentication timeout settings appear.*

The screenshot shows a configuration window with four tabs: Network, Wireless (selected), MAC Access Control, and Hotspot. Under the Wireless tab, there are three checkboxes: 'Broadcast SSID and respond to SSID queries' (checked), 'Log authentication events' (checked), and 'Prohibit client to client wireless network traffic' (unchecked). Below these are several input fields and dropdown menus: 'Network name (SSID):' with the value 'network-1'; 'Fragmentation threshold:' and 'RTS threshold:' both set to '2346' bytes; 'Encryption (Authentication):' set to 'WPA/WPA2 Enterprise'; 'Encryption algorithm:' set to 'TKIP or AES'; 'Authentication server:' set to 'RADIUS'; and 'EAP authentication timeout:' set to '3600' seconds.

5. From the **Encryption algorithm** drop-down list, select the encryption method. For more information, see *Set the Encryption Level*.
6. From the **Authentication server** drop-down list, select **RADIUS**.  
*The authentication and protocol configuration settings are disabled. You must configure these settings on your RADIUS server.*
7. In the **EAP authentication timeout** text box, you can change the timeout value for authentication. The default is 3600 seconds.
8. Click **OK**.

If you have not previously configured a RADIUS server, you are prompted to do this when you click **OK**. For more information, see *Configure RADIUS Server Authentication*.

## Use the XTM Device as an Authentication Server for Wireless Authentication

If you select the **WPA Enterprise**, **WPA2 Enterprise**, or **WPA/WPA2 Enterprise** authentication methods in your wireless configuration, you can use the XTM device as the authentication server for wireless authentication.

1. Select **Network > Wireless**.
2. Click **Configure** adjacent to the **Access point 1**, **Access point 2**, or **Wireless Guest** configuration.
3. Select the **Wireless** tab.
4. From the **Encryption (Authentication)** drop-down list, select **WPA Enterprise**, **WPA2 Enterprise** or **WPA/WPA2 Enterprise**.

**Wireless Guest Configuration**

The Wireless Guest network allows access only to the External network. Access to the Trusted and Optional networks is not permitted.

Network Wireless MAC Access Control Hotspot

Broadcast SSID and respond to SSID queries

Log authentication events

Prohibit client to client wireless network traffic

Network name (SSID): network-1

Fragmentation threshold: 2346 bytes

RTS threshold: 2346 bytes

Encryption (Authentication): WPA/WPA2 Enterprise

Encryption algorithm: TKIP or AES

Authentication server: Firebox-DB

EAP authentication timeout: 3600 seconds

EAP protocol: EAP-PEAP

EAP tunnel protocol: MSCHAPv2

Select certificate:  Default certificate signed by Firebox  
 Third party certificates

Validate client certificate

Certificate: [dropdown]

CA Certificate: [dropdown]

OK Cancel Help

5. From the **Encryption algorithm** drop-down list, select the encryption method to use. For more information, see *Set the Encryption Level*.
6. From the **Authentication server** drop-down list, select **Firebox-DB**.
7. In the **EAP authentication timeout** text box, you can change the timeout value for authentication. The default is 3600 seconds.
8. From the **EAP protocol** drop-down list, select the EAP protocol wireless clients must use to connect to the access point.
  - **EAP-PEAP** — EAP Protected Extensible Authentication Protocol
  - **EAP-TTLS** — EAP Tunneled Transport Layer Security
  - **EAP-TLS** — EAP Transport Layer Security
9. From the **EAP tunnel protocol** drop-down list, select the EAP tunnel protocol to use. The available tunnel protocols depend on the selected EAP protocol.
10. Select the certificate type to use for authentication.
  - **Default certificate signed by Firebox** — This is the default.
  - **Third party certificates** — Select from a list of installed third party certificates.

11. If you selected **Third party certificates**, select a certificate from the **Certificate** drop-down list.
12. If you want to use a certificate authority (CA) to validate the client certificate, select the **Validate client certificate** check box and select a CA certificate from the **CA Certificate** drop-down list.

For more information about certificates, see *About Certificates*.

13. Click **OK**.

To use this authentication method, you must configure your XTM device as an authentication server. For more information, see *Configure Your XTM Device as an Authentication Server*.

## Set the Encryption Level

From the **Encryption algorithm** drop-down list in the wireless access point configuration, select the level of encryption for your wireless connections. The available selections change when you use different authentication mechanisms. The Fireware XTM OS automatically creates a random encryption key for you when a key is required. You can use this key or change it to a different key. Each wireless client must use this same key when they connect to the XTM wireless device.

## Encryption for Open System and Shared Key Authentication

Encryption options for Open System and Shared Key authentication are WEP 64-bit hexadecimal, WEP 40-bit ASCII, WEP 128-bit hexadecimal, and WEP 128-bit ASCII. If you select Open System authentication, you can also select **No encryption**.

1. If you use WEP encryption, in the **Key** text boxes, type hexadecimal or ASCII characters. Not all wireless adapter drivers support ASCII characters. You can have a maximum of four keys.
  - A WEP 64-bit hexadecimal key must have 10 hexadecimal (0-f) characters.
  - A WEP 40-bit ASCII key must have 5 characters.
  - A WEP 128-bit hexadecimal key must have 26 hexadecimal (0-f) characters.
  - A WEP 128-bit ASCII key must have 13 characters.
2. If you typed more than one key, from the **Key Index** drop-down list, select the key to use as the default key.

The XTM wireless device can use only one wireless encryption key at a time. If you select a key other than the first key in the list, you also must set your wireless client to use the same key.

## Encryption for WPA and WPA2 Authentication

The encryption options for Wi-Fi Protected Access (WPA and WPA2) authentication methods are:

- **TKIP** — Use only TKIP (Temporal Key Integrity Protocol) for encryption. This option is not available for wireless modes that support 802.11n.
- **AES** — Use only AES (Advanced Encryption Standard) for encryption.
- **TKIP or AES** — Use either TKIP or AES.

We recommend that you select **TKIP or AES**. This allows the XTM wireless device to accept connections from wireless clients configured to use TKIP or AES encryption. For 802.11n wireless clients, we recommend you configure the wireless client to use AES encryption.



## Enable Wireless Connections to the Trusted or Optional Network

To allow wireless connections to your trusted or optional network:

1. Select **Network > Wireless**.

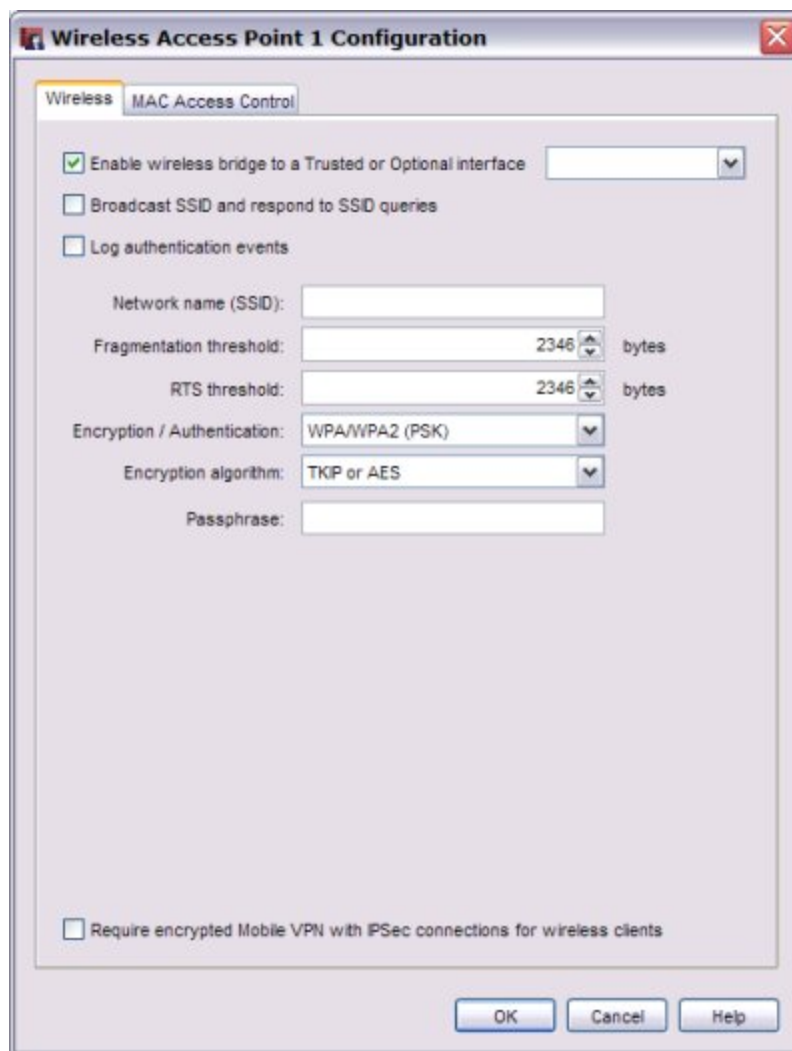
*The Wireless Configuration dialog box appears.*



<input checked="" type="checkbox"/> Enable wireless		
<input type="radio"/> Enable wireless client as external interface		Configure...
<input checked="" type="radio"/> Enable wireless access points		
Access point 1	Enabled	Configure...
Access point 2	Disabled	Configure...
Wireless guest	Disabled	Configure...

2. Select the **Enable wireless** check box.
3. Select **Enable wireless access points**.
4. Adjacent to **Access point 1** or **Access point 2**, click **Configure**.

*The Wireless Access Point configuration dialog box appears.*



5. Select the **Enable wireless bridge to a Trusted or Optional interface** check box.
6. In the drop-down list adjacent to **Enable wireless bridge to a Trusted or Optional interface**, select a trusted or optional interface.

#### *Trusted*

Any wireless clients on the trusted network have full access to computers on the trusted and optional networks, and access to the Internet as defined in the outgoing firewall rules on your XTM device.

*If the wireless client sets the IP address on its wireless network card with DHCP, the DHCP server on the optional network of the XTM device must be active and configured.*

#### *Optional*

Any wireless clients on the optional network have full access to computers on the optional network, and access to the Internet as defined in the outgoing firewall rules on your XTM device.

*If the wireless client sets the IP address on its wireless network card with DHCP, the DHCP server on the optional network of the XTM device must be active and configured.*

7. To configure the wireless interface to send and answer SSID requests, select the **Broadcast SSID and respond to SSID queries** check box.

For information about this setting, see *Enable/Disable SSID Broadcasts* on page 193.

8. Select the **Log Authentication Events** check box if you want the XTM device to send a log message to the log file each time a wireless computer tries to connect to the interface.

For more information about logging, see *Log Authentication Events* on page 193.

9. To require wireless users to use the Mobile VPN with IPsec client, select the **Require encrypted Mobile VPN with IPsec connections for wireless clients** check box.

When you select this check box, the only packets the XTM device allows over the wireless network are DHCP, ICMP, IKE (UDP port 500), ARP and IPsec (IP protocol 50). If you require wireless users to use the Mobile VPN with IPsec client, it can increase the security for wireless clients if you do not select WPA or WPA2 as the wireless authentication method.

10. In the **Network name (SSID)** text box, type a unique name for your wireless optional network or use the default name.

For information about changing the SSID, see *Change the SSID* on page 193.

11. To change the fragmentation threshold, in the **Fragmentation Threshold** text box, type a value: 256–2346. We do not recommend you change this setting.

For more information about this setting, see *Change the Fragmentation Threshold* on page 193.

12. In the **Encryption (Authentication)** drop-down list, select the encryption and authentication to enable for wireless connections to the optional interface. We recommend that you use WPA2 if the wireless devices in your network can support WPA2.

For more information about this setting, see *Set the Wireless Authentication Method*.

13. In the **Encryption algorithm** drop-down list, select the type of encryption to use for the wireless connection and add the keys or passwords required for the type of encryption you select. If you select an encryption option with pre-shared keys, a random pre-shared key is generated for you. You can use this key or type your own.

For more information, see *Set the Encryption Level* on page 200.

14. Save the configuration.

**Note** *If you enable wireless connections to the trusted interface, we recommend that you restrict access by MAC address. This prevents users from connecting to the XTM wireless device from unauthorized computers that could contain viruses or spyware. Click the **MAC Access Control** tab to enable MAC access control. You use this tab the same way as when you restrict network traffic on an interface as described in *Restrict Network Traffic by MAC Address* on page 110.*

To configure a wireless guest network with no access to the computers on your trusted or optional networks, see *Enable a Wireless Guest Network* on page 204.

## Enable a Wireless Guest Network

You can enable a wireless guest network to give a guest user wireless access to the Internet without access to computers on your trusted and optional networks.

To set up a wireless guest network:

1. Select **Network > Wireless**.

*The Wireless Configuration dialog box appears.*



2. Select the **Enable wireless** check box.
3. Select **Enable wireless access points**.
4. Adjacent to **Wireless guest**, click **Configure**.

*The Wireless Guest Configuration dialog box appears.*

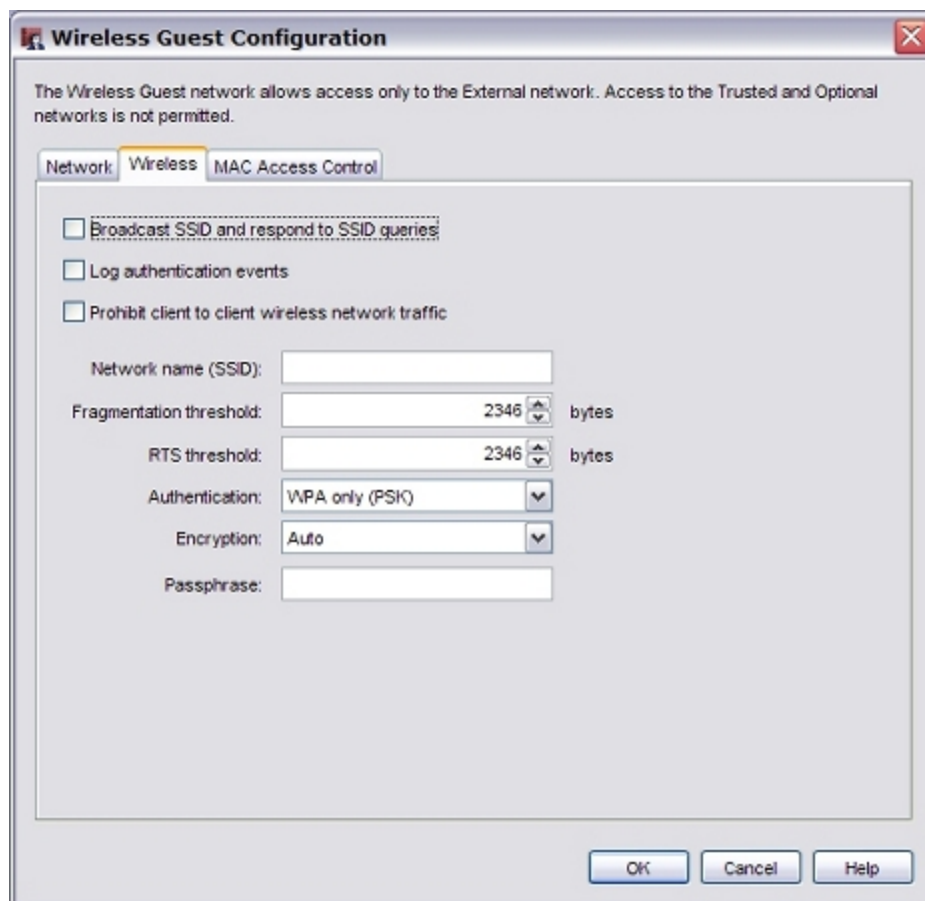
5. Select the **Enable Wireless Guest Network** check box.

Wireless connections are allowed through the XTM device to the Internet based on the rules you have configured for outgoing access on your device. These computers have no access to computers on the trusted or optional network.

6. In the **IP Address** text box, type the private IP Address to use for the wireless guest network. The IP address you type must not already be in use on one of your network interfaces.
7. In the **Subnet Mask** text box, type the subnet mask. The correct value is usually 255.255.255.0.
8. To configure the XTM device as a DHCP server when a wireless device tries to make a connection, select the **Enable DHCP Server on Wireless Guest Network** check box.

For more information about how to configure the settings for the DHCP Server, see *Configure DHCP in Mixed Routing Mode* on page 94.

9. Click the **Wireless** tab to see the security settings for the wireless guest network.  
*The Wireless settings appear.*



10. Select the **Broadcast SSID and respond to SSID queries** check box to make your wireless guest network name visible to guest users.

For information about this setting, see *Enable/Disable SSID Broadcasts* on page 193.

11. To send a log message to the log file each time a wireless computer tries to connect to the guest wireless network, select the **Log Authentication Events** check box.

For more information about logging, see *Log Authentication Events* on page 193.

12. To allow wireless guest users to send traffic to each other, clear the **Prohibit client to client wireless network traffic** check box.
13. In the **Network name (SSID)** text box, type a unique name for your wireless guest network or use the default name.

For information about changing the SSID, see *Change the SSID* on page 193.

14. To change the fragmentation threshold, in the **Fragmentation Threshold** text box, type a value: 256–2346. We do not recommend you change this setting.

For more information about this setting, see *Change the Fragmentation Threshold* on page 193.

15. In the **Authentication** drop-down list, select the type of authentication to enable for connections to the wireless guest network. The setting you choose depends on the type of guest access you want to provide, and whether you want to require your guests to enter a passphrase to use the network.

For more information about this setting, see *Set the Wireless Authentication Method* on page 196.

- In the **Encryption / Authentication** drop-down list, select the type of encryption to use for the wireless connection and add the keys or passwords required for the type of encryption you select. If you select an authentication option that uses pre-shared keys, a random pre-shared key is generated for you. You can use this key or type your own.

For more information, see *Set the Encryption Level* on page 200.

- Click **OK**.
- Save the configuration.

Optionally, you can configure your wireless guest network as a wireless hotspot. Click the **Hotspot** tab to enable a wireless hotspot. For more information, see *Enable a Wireless Hotspot*.

You can also restrict access to the Guest network by MAC address. Click the **MAC Access Control** tab to enable MAC access control. You use this tab the same way as when you restrict network traffic on an interface as described in *Restrict Network Traffic by MAC Address* on page 110.

## Enable a Wireless Hotspot

You can configure your WatchGuard XTM wireless guest network as a wireless hotspot to give wireless Internet connectivity to your visitors or customers. When you enable the hotspot feature, you have more control over connections to your wireless guest network.

When you configure your device as a wireless hotspot you can customize:

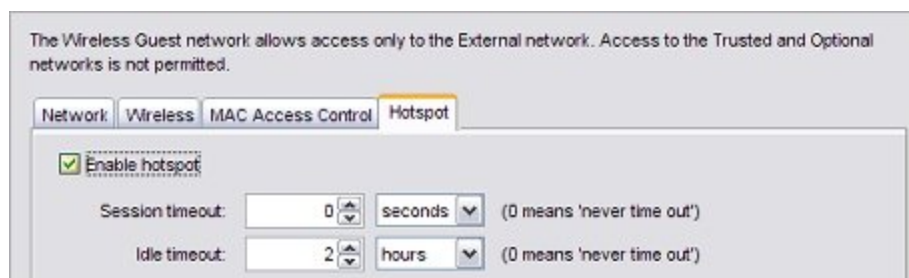
- A splash screen that users see when they connect
- Terms and conditions that users must accept before they can browse to a web site
- Maximum length of time a user can be continuously connected

When you enable the wireless hotspot feature, the **Allow Hotspot-Users** policy is automatically created. This policy allows connections from the wireless guest interface to your external interfaces. This gives wireless hotspot users wireless access to the Internet without access to computers on your trusted and optional networks.

Before you set up a wireless hotspot, you must configure the settings for your wireless guest network as described in *Enable a Wireless Guest Network*.

To set up the wireless hotspot:

- Select **Network > Wireless**.
- Adjacent to **Wireless guest**, click **Configure**.
- In the **Wireless Guest Configuration** dialog box, select the **Hotspot** tab.
- Select the **Enable hotspot** check box.



## Configure User Timeout Settings

You can configure timeout settings to limit the amount of time that users can continuously use your hotspot. When the timeout period expires, the user is disconnected. When a user is disconnected, the user loses all Internet connectivity but is still connected to the wireless network. The hotspot splash screen reappears, and the user must accept the Terms and Conditions again before they can continue to use the wireless hotspot.

1. In the **Session timeout** text box, specify the maximum amount of time a user can remain continuously connected to your hotspot. You can specify the unit of time with the adjacent drop-down list. If the Session timeout is set to 0 (the default value), wireless guest users are not disconnected after a specified time interval.
2. In the **Idle timeout** text box, specify the amount of time that a user must be idle for the connection to time out. You can specify the unit of time with the adjacent drop-down list. If the Idle timeout is set to 0, users are not disconnected if they do not send or receive traffic.

## Customize the Hotspot Splash Screen

When users connect to your hotspot, they see a *splash screen*, or a web site they must visit before they can browse to other web sites. You can configure the text that appears on this page, and the appearance of the page. You can also redirect the user to a specified web page after they accept the terms and conditions.

At a minimum, you must specify the **Page title** and the **Terms and Conditions** to enable this feature.

1. In the **Page title** text box, type the title text you want to appear on the hotspot splash screen.

The screenshot shows a configuration window for the hotspot splash screen. It contains the following fields and options:

- Page title:** A text input field.
- Welcome message:** A checkbox with a corresponding text area below it.
- Use a custom logo if available (.jpg, .gif or .png, 90x50):** A checkbox with an **Upload...** button.
- Terms and Conditions:** A large text area.
- Redirect URL:** A text input field.
- Note:** This will re-route guest users from any requested URL.
- Font:** A dropdown menu.
- Size:** A dropdown menu with "medium" selected.
- Text color:** A color picker showing "#000000" with a black swatch.
- Background color:** A color picker showing "#FFFFFF" with a white swatch.
- Preview Splash Screen...** button at the bottom.

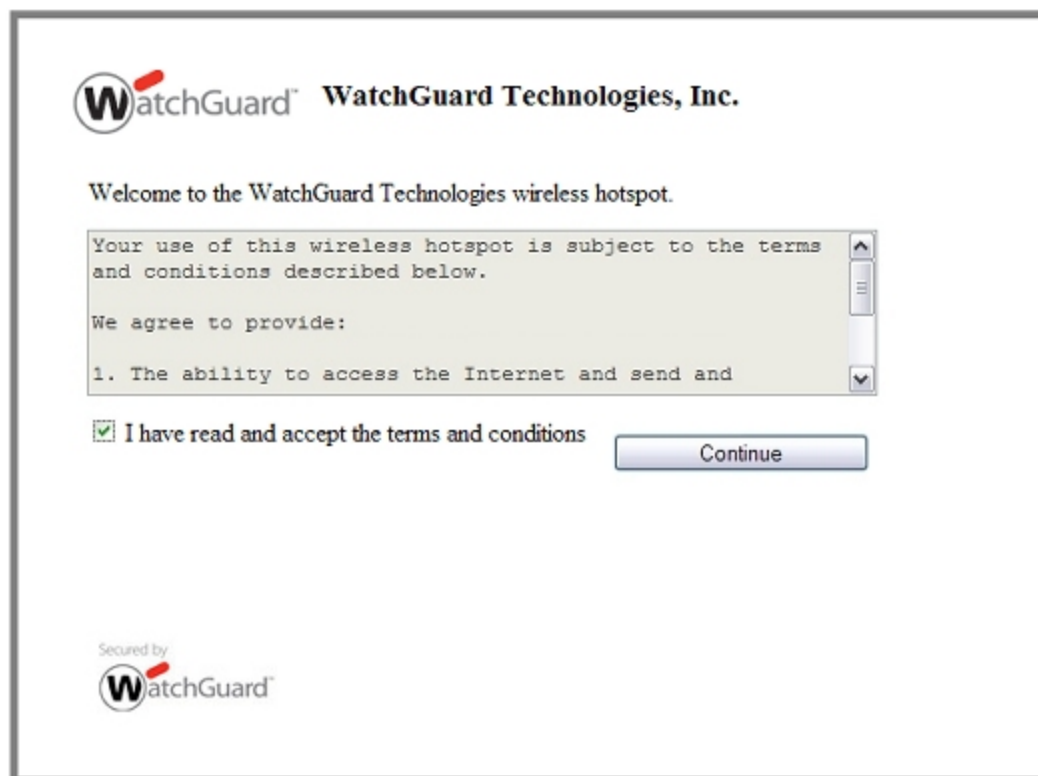


2. To include a welcome message:
    - Select the **Welcome Message** check box.
    - In the **Welcome Message** text box, type the message your users see when they connect to the hotspot.
  3. (Optional) To use a custom logo in the splash screen:
    - Select the **Use a custom logo** check box.
    - Click **Upload** to upload your custom logo file.  
The file must be in .jpg, .gif or .png format. We recommend that the image be no larger than 90 x 50 (width x height) pixels, or 50 kB.
  4. In the **Terms and Conditions** text box, type or paste the text you want your users to agree to before they can use the hotspot. The maximum length is 20,000 characters.
  5. To automatically redirect users to a web site after they accept the Terms and Conditions, in the **Redirect URL** text box, type the URL of the web site.
  6. You can customize the fonts and colors for your Welcome page:
    - **Font** — Select the font from the **Font** drop-down list. If you do not specify a font, the Welcome page uses the browser default font for each user.
    - **Size** — Select the text size from the **Size** drop-down list. The default text size is Medium.
    - **Text Color** — This is the color for the text on the hotspot splash screen. The default color is #000000 (black). The configured color appears in a square adjacent to the Text Color text box. Click the colored square to select a different color from a color palette. Or, type the HTML color code in the **Text Color** text box.
    - **Background Color** — This is the color to use for the background of the hotspot splash screen. The default color is #FFFFFF (white). The configured color appears in a square adjacent to the Background Color text box. Click the colored square to select a different color from a color palette. Or, type the HTML color code in the **Background Color** text box.
  7. Click **Preview Splash Screen**.  
*The Preview Splash Screen dialog box appears. This dialog box shows the page title, welcome message, and terms and conditions you configured.*
- Note** In Policy Manager, the **Preview Splash Screen** dialog box does not show the selected text font and size. To see the selected fonts on the splash screen, you must save the configuration and connect to the hotspot, or use Firewall XTM Web UI to preview it in the wireless guest hotspot configuration page.
8. Click **OK** to close the preview dialog box.
  9. Click **OK** to save the settings.

## Connect to a Wireless Hotspot

After you configure your wireless hotspot, you can connect to it to see the hotspot splash screen.

1. Use a wireless client to connect to your wireless guest network. Use the SSID and other settings that you configured for the wireless guest network.
2. Open a web browser. Browse to any web site.  
*The wireless hotspot splash screen appears in the browser.*



3. Select the **I have read and accept the terms and conditions** check box.
4. Click **Continue**.

*The browser displays the original URL you requested. Or, if the hotspot is configured to automatically redirect the browser to a URL, the browser goes to the web site.*

The content and appearance of the hotspot splash screen can be configured with the hotspot settings for your wireless guest network.

The URL of the wireless hotspot splash screen is:

https://<IP address of the wireless guest network>:4100/hotspot.

## See Wireless Hotspot Connections

When you enable the wireless hotspot feature, you can see information about the number of wireless clients that are connected. You can also disconnect wireless clients.

To see the list of connected wireless hotspot clients:

1. Start *Firebox System Manager* and connect to your wireless device.
2. Select the **Authentication List** tab.
3. Click **Hotspot Clients**.

*For each connected wireless client, the IP address and MAC address appear.*



To disconnect a wireless hotspot client, from the **Wireless Hotspot Clients** dialog box:

1. Select one or more connected wireless hotspot clients.
2. Click **Disconnect**.
3. Type the configuration passphrase.

## Configure Your External Interface as a Wireless Interface

In areas with limited or no existing network infrastructure, you can use your XTM wireless device to provide secure network access. You must physically connect your network devices to the XTM device. Then you configure your external interface to connect to a wireless access point that connects to a larger network.

**Note** When the external interface is configured with a wireless connection, the XTM wireless device can no longer be used as a wireless access point. To provide wireless access for users, connect a wireless access point device to the XTM wireless device.

## Configure the Primary External Interface as a Wireless Interface

1. Select **Network > Wireless**.

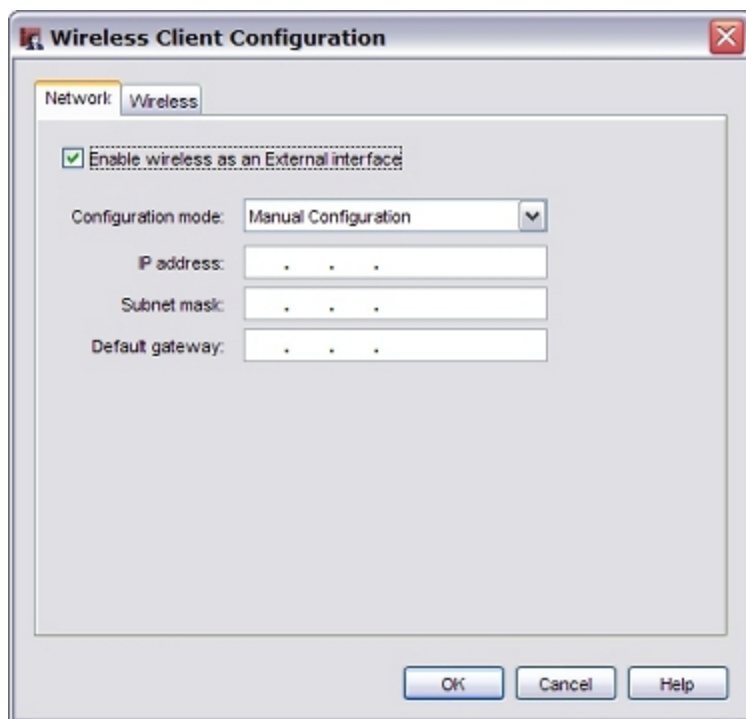
*The Wireless Configuration dialog box appears.*



2. Select the **Enable wireless** check box.
3. Select **Enable wireless client as external interface**.
4. Click **Configure**.
5. In the **Configuration Mode** drop-down list, select an option:

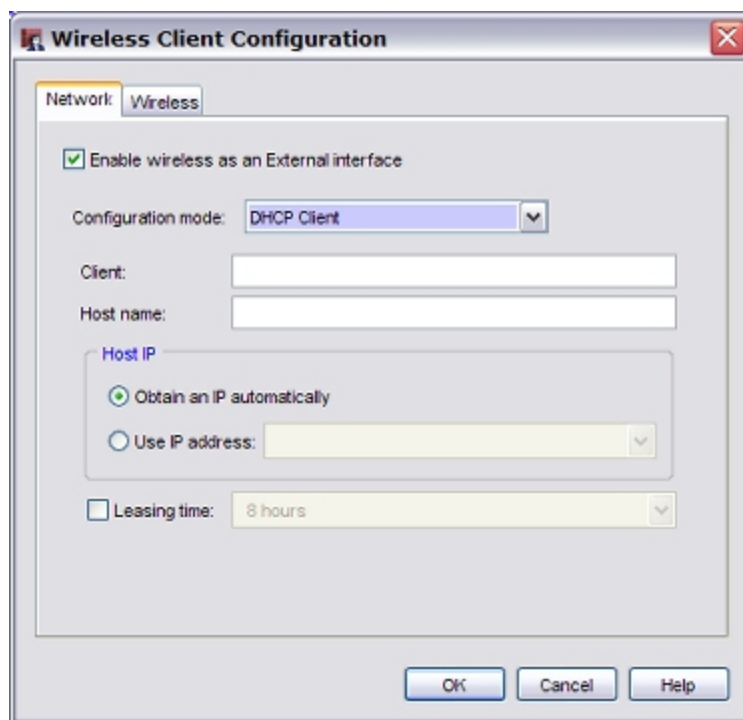
*Manual Configuration*

To use a static IP address, select this option. Type the **IP Address**, **Subnet Mask**, and **Default Gateway**.



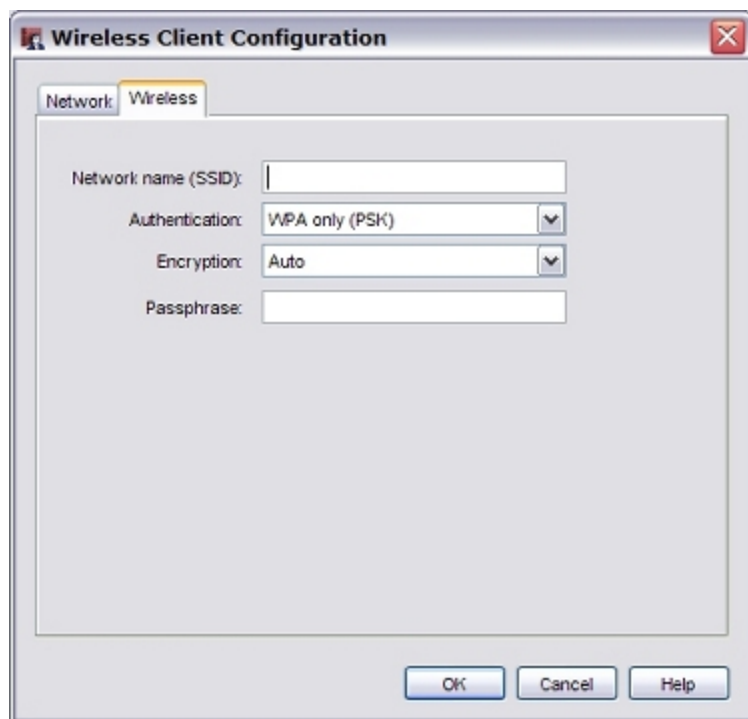
### DHCP Client

To configure the external interface as a DHCP client, select this option. Type the DHCP configuration settings.



For more information about how to configure the external interface to use a static IP address or DHCP, see *Configure an External Interface* on page 90.

6. Click the **Wireless** tab.  
*The wireless client configuration settings appear.*



7. In the **Network name (SSID)** text box, type a unique name for your wireless external network.
8. In the **Authentication** drop-down list, select the type of authentication to enable for wireless connections. We recommend that you use WPA2 if the wireless devices in your network can support WPA2.

For more information about wireless authentication methods, see *About Wireless Security Settings* on page 196.

9. In the **Encryption** drop-down list, select the type of encryption to use for the wireless connection and add the keys or passwords required for the type of encryption you select. If you select an encryption option with pre-shared keys, a random pre-shared key is generated for you. You can use this key or type your own.
10. Click **OK**.

## Configure a BOVPN tunnel for additional security

To create a wireless bridge and provide additional security, add a BOVPN tunnel between your XTM device and the external gateway. You must set the mode to **Aggressive Mode** in the Phase 1 settings of your BOVPN configuration on both devices.

For information about how to set up a BOVPN tunnel, see *About Manual Branch Office VPN Tunnels* on page 914.

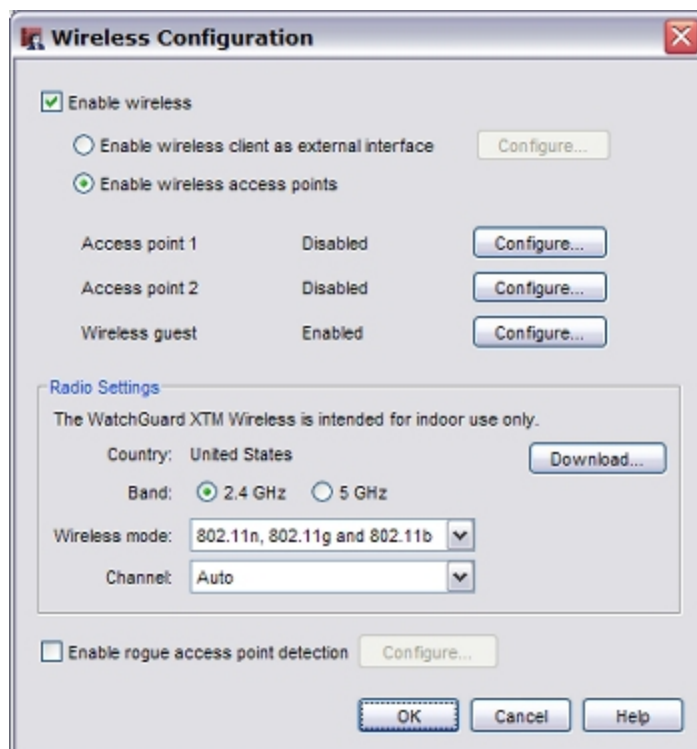
## About Wireless Radio Settings

WatchGuard XTM wireless devices use radio frequency signals to send and receive traffic from computers with wireless Ethernet cards.

To view or change the radio settings:

1. Open Policy Manager.
2. Select **Network > Wireless**.

*The Wireless Configuration dialog box appears.*



The **Radio Settings** appear at the bottom of this dialog box.

## Country is Set Automatically

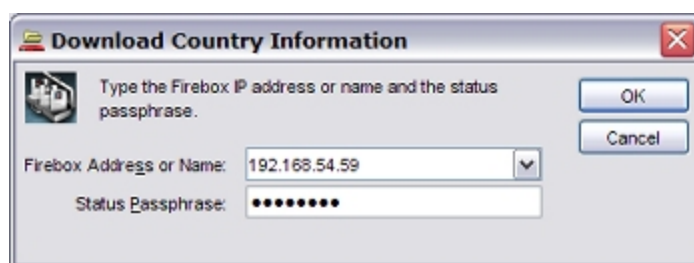
Due to regulatory requirements in different parts of the world, you cannot use all wireless radio settings in every country. Each time you power on the XTM wireless device, the device contacts a WatchGuard server to determine the country and the allowed wireless radio settings for that country. To do this, the device must have an Internet connection. Once the country is determined, you can configure all supported wireless radio settings that can be used in that country.

When you configure an XTM wireless device for the first time, the Wireless Configuration page in Policy Manager might not show the country. After the XTM wireless device connects to the Internet for the first time, Policy Manager must connect to the XTM device to get the country setting, if it has been determined.

To update the Policy Manager configuration with the country setting from the XTM wireless device:

1. Click **Download**.

*The Download Country Information dialog box appears.*



2. Type the XTM device status (readonly) passphrase.

*The Country is updated to show the country on the XTM 2 Series device*

In the Wireless Configuration dialog box, the **Country** setting shows which country the device detects it is in. You cannot change the **Country** setting. The available options for the other radio settings are based on the regulatory requirements of the country the device detects it is located in.

**Note** *If Policy Manager has not yet connected with the XTM wireless device, or if the XTM wireless device cannot connect to the WatchGuard server, the country is unknown. In this case, you can only select from the limited set of wireless radio settings that are allowed in all countries. The XTM wireless device periodically continues to retry to connect to the WatchGuard server to determine the country and allowed wireless radio settings.*

If the XTM wireless device does not have a region set yet, or if the region is not up to date, you can force the device to update the wireless radio region.

To update the Wireless Radio Region:

1. [Start Firebox System Manager](#)
2. Select **Tools > Update Wireless Radio Region**.

*The 2 Series device contacts a WatchGuard server to determine the current operating region.*



## Select the Band and Wireless Mode

The WatchGuard XTM wireless device supports two different wireless bands, 2.4 GHz and 5 GHz. The the band you select and the country determine the wireless modes available. Select the **Band** that supports the wireless mode you want to use. Then select the mode from the **Wireless mode** drop-down list.

The 2.4 GHz band supports these wireless modes:

### *802.11n, 802.11g and 802.11b*

This is the default mode in the 2.4 GHz band, and is the recommended setting. This mode allows the XTM wireless device to connect with devices that use 802.11n, 802.11g, or 802.11b.

### *802.11g and 802.11b*

This mode allows the XTM wireless device to connect to devices that use 802.11g or 802.11b.

### *802.11b ONLY*

This mode allows the XTM wireless device to connect only to devices that use 802.11b.

The 5 GHz band supports these wireless modes:

### *802.11a and 802.11n*

This is the default mode in 5 GHz band. This mode allows the XTM wireless device to connect to devices that use 802.11a or 802.11n.

### *802.11a ONLY*

This mode allows the XTM wireless device to connect only to devices that use 802.11a.

**Note** *If you choose a wireless mode that supports multiple 802.11 standards, the overall performance can drop considerably. This is partly because of the need for backward compatibility when devices that use slower modes are connected. The slower devices tend to dominate the throughput because it can take much longer to send or receive the same amount of data to devices that use a slower mode.*

The 5 GHz band provides greater performance than the 2.4 GHz band, but may not be compatible with all wireless devices. Select the band and mode based on the wireless cards in the devices that will connect to the XTM wireless device.

## Select the Channel

The available channels depend on the country and the wireless mode you select. By default, the **Channel** is set to **Auto**. When the channel is set to Auto, the XTM wireless device automatically selects a quiet channel from the available list in the band you have selected. Or you can select a specific channel from the **Channel** drop-down list.

## Configure the Wireless Card on Your Computer

These instructions are for the Windows XP with Service Pack 2 operating system. For installation instructions for other operating systems, see your operating system documentation or help files.

1. Select **Start > Settings > Control Panel > Network Connections**.  
*The Network Connections dialog box appears.*
2. Right-click **Wireless Network Connection** and select **Properties**.  
*The Wireless Network Connection dialog box appears.*
3. Select the **Wireless Networks** tab.
4. Below **Preferred Networks**, click **Add**.  
*The Wireless Network Properties dialog box appears.*
5. Type the SSID in the **Network Name (SSID)** text box.
6. Select the network authentication and data encryption methods in the drop-down lists. If necessary, clear **The key is provided for me automatically** check box and type the network key two times.
7. Click **OK** to close the **Wireless Network Properties** dialog box.
8. Click **View Wireless Networks**.  
*All available wireless connections appear in the Available Networks text box.*
9. Select the SSID of the wireless network and click **Connect**.

If the network uses encryption, type the network key twice in the Wireless Network Connection dialog box and click **Connect** again.

10. Configure the wireless computer to use DHCP.

## Rogue Access Point Detection

You can configure your XTM wireless device to detect (unknown) wireless access points that operate in the same area. A rogue access point is any wireless access point within range of your network that is not recognized as an authorized access point. When you enable rogue access point detection on your XTM wireless device, the wireless radio in the device scans wireless channels to identify unknown wireless access points. You can configure the scan to run continuously, or to run at a scheduled interval and time of day.

When a rogue access point scan begins, the XTM wireless device scans the airwaves within range for other radio broadcasts. The device scans for wireless access points in 802.11a, 802.11b, 802.11g, and 802.11n wireless modes on all available wireless channels for the country where the device is located. The scan is not limited to the wireless mode and channel settings configured in the radio settings of your device.

When the XTM wireless device detects the signal of another wireless access point, it compares the characteristics of the access point to a list of trusted access points that you configure. If the discovered access point does not match any trusted access point, the XTM device reports the device as a potential rogue access point. You can configure the device to send an alarm when a rogue access point is detected. If you enable logging, you can run a report of all scans and scan results.

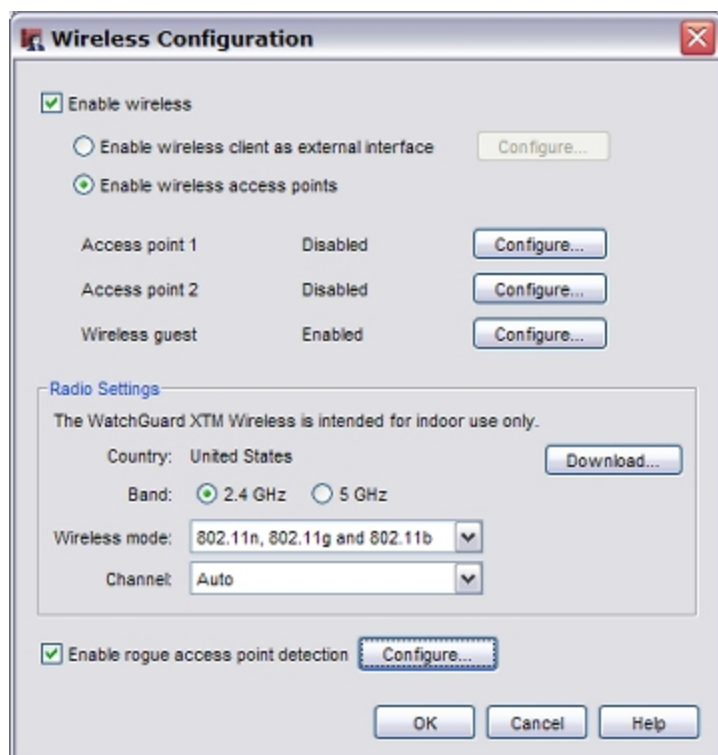
## Enable Rogue Access Point Detection

To configure rogue access point detection on your XTM wireless device, you need to know the configuration of the other wireless access points on your network; this enables you to identify them as trusted in your configuration. You can then set up a schedule for rogue access point detection scans.

## Configure Rogue Access Point Detection

1. Select **Network > Wireless**.

The *Wireless Configuration dialog box* appears.



2. Select the **Enable rogue access point detection** check box.
3. Adjacent to the **Enable rogue access point detection** check box, click **Configure**.

The *Trusted Access Point Configuration dialog box* appears.

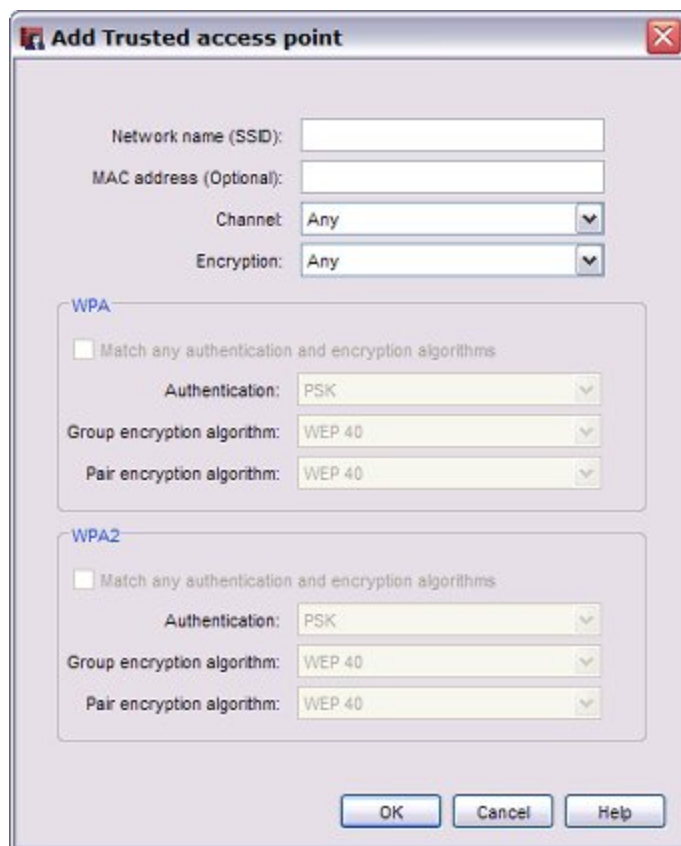


On the **Access Points** tab you can add information about all other trusted wireless access points on your network so the rogue access point scan does not identify them as potential rogue access points.

## Add a Trusted Access Point

1. To add a trusted access point to the list, click **Add**.

*The Add Trusted access point dialog box appears.*



In the **Add Trusted access point** dialog box, provide as much information as you can to identify your trusted access point. The more information you provide, the more likely it is that a rogue access point detection scan can correctly identify a trusted access point.

2. In the **Network name (SSID)** text box, type the SSID of the trusted access point.
3. In the **MAC address (Optional)** text box, type the wireless MAC address of the trusted access point. If your trusted access point is an XTM wireless device, see *Find the Wireless MAC Address of a Trusted Access Point*.
4. From the **Channel** drop-down list, select the channel used by the trusted access point. If the trusted access point is a WatchGuard device and the **Channel** in the radio settings of that trusted wireless device is set to **Auto**, select **Any**.
5. From the **Encryption** drop-down list, select the encryption method used by the trusted access point. *The WPA or WPA2 authentication and encryption settings that apply to the encryption method you select are enabled.*

6. If you select **WPA** or **WPA/WPA2** as the encryption method, configure the WPA settings to match the configuration of your trusted access point.  
Or, if you do not know these settings, select the **Match any authentication and encryption algorithms** check box.
7. If you selected **WPA2** or **WPA/WPA2** as the encryption method, configure the WPA settings to match the configuration of your trusted access point.  
Or, if you do not know these settings, select the **Match any authentication and encryption algorithms** check box.
8. Click **OK**.  
*The trusted access point is added to the list of trusted access points.*

For information about how to add an XTM 2 Series device as a trusted access point, see *Add an XTM Wireless Device as a Trusted Access Point*.

### Edit or Remove a Trusted Access Point

To edit a trusted access point:

1. Select the access point in the list.
2. Click **Edit**.
3. Edit the information used to identify the trusted access point as described in the previous section.

To remove a trusted access point, select the access point in the list and click **Remove**.

### Configure Logging and Notification

You must enable logging to see information about rogue access point scans in a report. When you enable logging, the log records the start and stop time, and the results of each scan. To enable logging, select the **Enable logging for reports** check box.

You can also configure the device to notify you when a rogue access point is detected. To configure notification:

1. Click **Notification**.
2. Select a notification method: SNMP trap, email message, or pop-up window.

For more information about notification settings, see *Set Logging and Notification Preferences* on page 723.

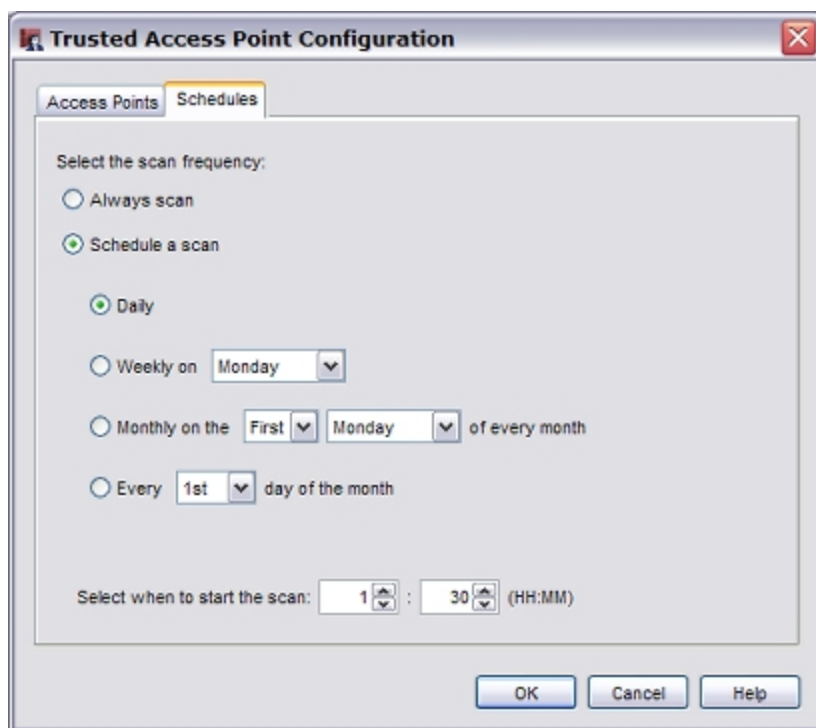
### Set the Scan Frequency

If you enable rogue access point detection on an XTM wireless device that is also configured as a wireless access point, the device alternates between the two functions. When a rogue access point scan is not in progress, the device operates as wireless access point. When a rogue access point scan begins, the XTM device access point functionality is temporarily disabled, and wireless clients cannot connect to the XTM wireless device until the scan completes. You cannot set the scan frequency to **Always scan** if your device is also configured as a wireless access point.

If your XTM wireless device is configured to operate as a wireless client, the rogue access point scan does not interrupt the wireless connection, but it does decrease the throughput of the wireless connection while the scan is in progress.

To set the scan frequency:

1. In the **Trusted Access Point Configuration** dialog box, select the **Schedules** tab.



2. Select the scan frequency.
  - Select **Always scan** to automatically scan for rogue access points every 15 minutes.
  - Select **Schedule a scan** to scan on a periodic schedule.
3. If you selected **Schedule a scan**, select how often the scan should run (daily, weekly, or monthly) and select the time of day to start the scan.
4. Click **OK**.

If you have added information about some trusted access points but still need to collect information about other trusted access points, you might not be ready to enable the rogue access point scan. To disable rogue access point detection scans, in the Wireless Configuration dialog box, clear the **Enable rogue access point detection** check box. When you disable rogue access point detection, your trusted access point information is saved, but the device does not scan for rogue access points.

## Add an XTM Wireless Device as a Trusted Access Point

If you have multiple wireless access points, you must add their information to the rogue access point detection configuration's trusted access points list. The wireless settings you can select to identify a trusted wireless access point are similar to the settings you use to configure an XTM wireless device as a wireless access point. Use these steps to find the settings for your XTM wireless device so you can add it to the trusted access point list.

## Find the Settings for Your XTM Trusted Access Points

To find the required settings to identify a trusted access point:

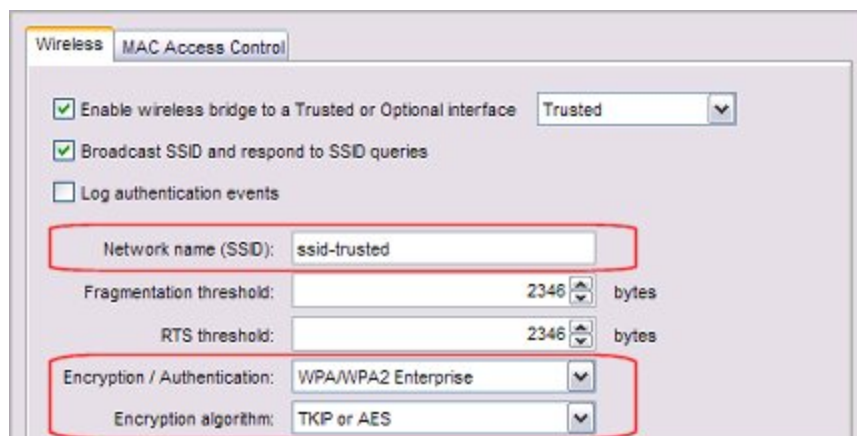
1. Select **Network > Wireless**.

*The Wireless Configuration dialog box appears.*



2. In the **Radio Settings** section, make a note of the **Channel**.
3. Click **Configure** adjacent to the enabled wireless access point name.

*The Wireless settings for this access point appear.*



4. Make a note of these settings:
  - Network name (SSID)
  - Encryption / Authentication
  - Encryption algorithm
5. Find the wireless MAC address. For an XTM 2 Series wireless device, the wireless MAC address is six higher than the MAC address of the Eth0 interface.  
For more information, see *Find the Wireless MAC Address of a Trusted Access Point*.

An XTM wireless device can have up to three enabled wireless access points with different settings. If the XTM wireless device has multiple enabled access points, repeat these steps to get the information about each enabled access point. Repeat these steps for any other trusted access points on your network.

## Add the Trusted Access Points to the Trusted Access Point List

On the wireless device that performs the rogue access point scan:

1. Select **Network > Wireless**.
2. Adjacent to **Enable rogue access point detection**, click **Configure**.  
*The list of trusted access points appears.*
3. Click **Add**.  
*The Add Trusted access point page appears.*

The screenshot shows a dialog box titled "Add Trusted access point". It contains the following fields and options:

- Network name (SSID): ssid-trusted
- MAC address (Optional): 00:90:7F:80:1A:67
- Channel: Any
- Encryption: WPA / WPA2
- WPA section:
  - Match any authentication and encryption algorithms
  - Authentication: Enterprise
  - Group encryption algorithm: TKIP+CCMP(AES)
  - Pair encryption algorithm: TKIP+CCMP(AES)
- WPA2 section:
  - Match any authentication and encryption algorithms
  - Authentication: Enterprise
  - Group encryption algorithm: TKIP+CCMP(AES)
  - Pair encryption algorithm: TKIP+CCMP(AES)

Buttons at the bottom: OK, Cancel, Help.

4. Type or select the information to match the configuration of your trusted access point.  
For more information about these settings, see *Enable Rogue Access Point Detection*.



**Note** The **Encryption / Authentication** setting in the wireless network configuration corresponds to two settings (**Encryption** and **Authentication**) in the Trusted Access Point configuration.

5. Click **OK** to add the trusted access point.

Repeat these steps to add other trusted wireless access points.

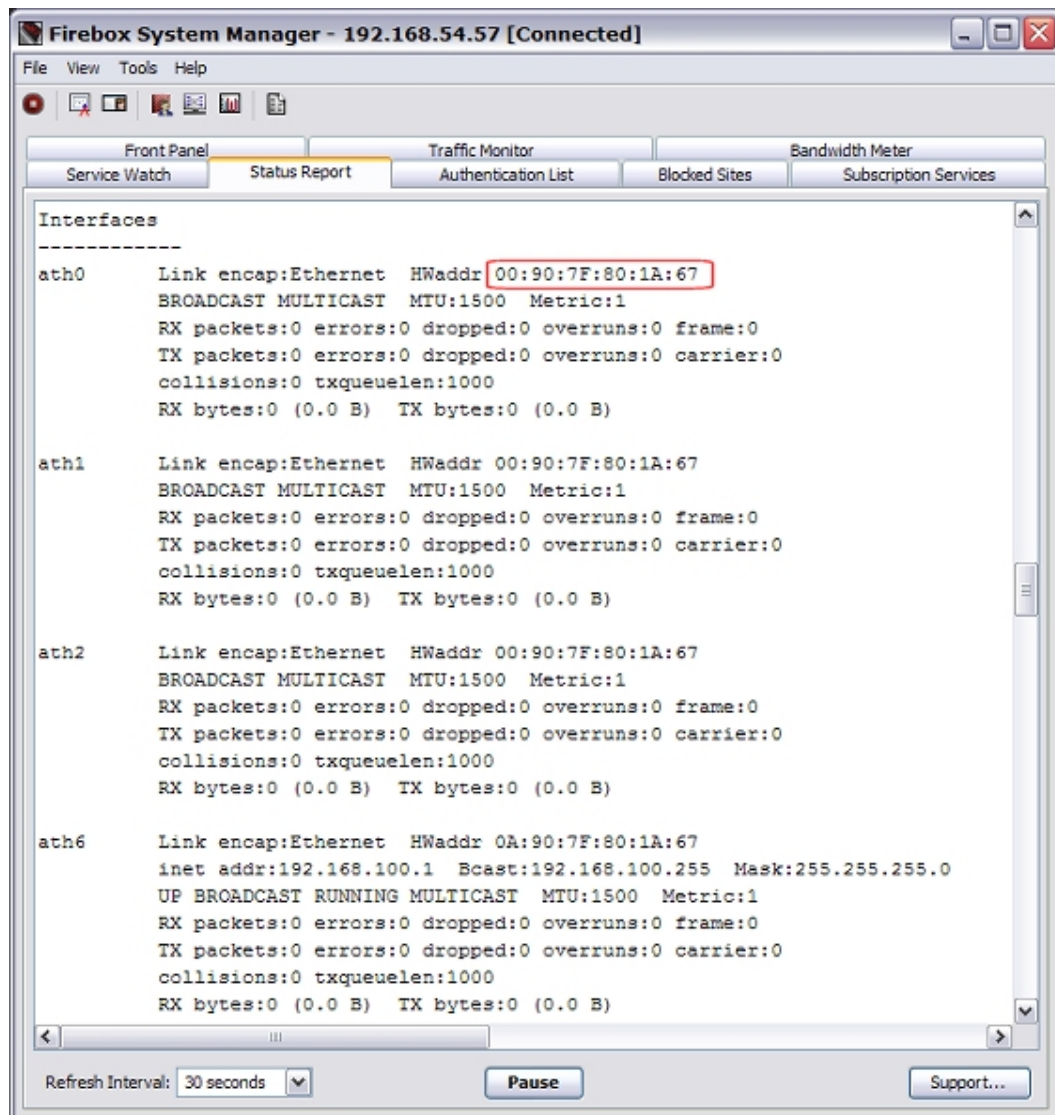
## Find the Wireless MAC Address of a Trusted Access Point

When you enable rogue access point detection, you can specify the wireless MAC address of your other trusted wireless access points so they can be identified as trusted.

To see the wireless MAC address of a trusted access point:

1. Start *Firebox System Manager* for the trusted access point you want to add.
2. Select the **Status Report** tab.
3. Scroll down to the **Interfaces** section.

The wireless MAC address appears on the first line of information for the ath interfaces.



For a wireless device, the first four interfaces listed are the wireless interfaces. These correspond to the four wireless configuration options:

- ath0 — Wireless client as external interface
- ath1 — Access point 1
- ath2 — Access point 2
- ath6 — Wireless guest

All of these wireless interfaces have the same MAC address. For an XTM 2 Series wireless device, the wireless MAC address is always six higher than the MAC address of the Eth0 interface.

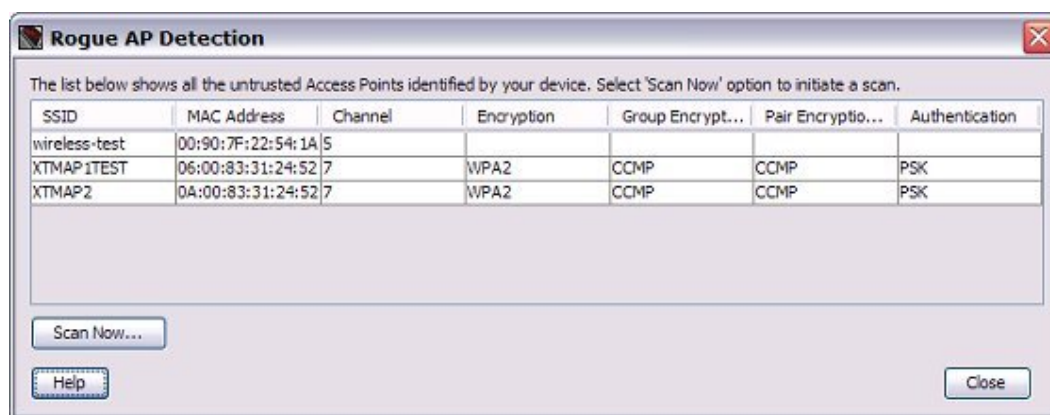
## Rogue Access Point Scan Results

You can see the results of a wireless rogue access detection point scan in the **Rogue Access Point Detection** (Wireless Intrusion Detection System) dialog box. This page displays a list of untrusted wireless access points found by the most recent rogue access point detection scan. This list does not include access points that match the trusted access points defined in your wireless rogue access point detection configuration.

To see and update the list:

1. In Firebox System Manager, select **Tools > Rogue AP Detection**.

*The Rogue AP Detection dialog box appears.*



2. To start an immediate scan for rogue access points, click **Scan now**.

*The wireless access point starts a rogue access point detection scan and updates the list of untrusted access points.*

If a trusted access point appears on this list, it is because you have not yet added it as a trusted access point. For information about how to add an access point to the trusted access point list, see *Enable Rogue Access Point Detection*.

# 10 Dynamic Routing

---

## About Dynamic Routing

A routing protocol is the language a router speaks with other routers to share information about the status of network routing tables. With static routing, routing tables are set and do not change. If a router on the remote path fails, a packet cannot get to its destination. Dynamic routing makes automatic updates to route tables as the configuration of a network changes.

**Note** Support for some dynamic routing protocols is available only on Fireware XTM with a Pro upgrade.

Fireware XTM supports the RIP v1 and RIP v2 protocols. Fireware XTM with a Pro upgrade supports the RIP v1, RIP v2, OSPF, and BGP v4 protocols.

## About Routing Daemon Configuration Files

To use any of the dynamic routing protocols with Fireware XTM, you must import or type a dynamic routing configuration file for the routing daemon you choose. This configuration file includes information such as a password and log file name. To see sample configuration files for each of the routing protocols, see these topics:

- *Sample RIP Routing Configuration File*
- *Sample OSPF Routing Configuration File*
- *Sample BGP Routing Configuration File*

Notes about configuration files:

- The "!" and "#" characters are placed before comments, which are lines of text in configuration files that explain the function of subsequent commands. If the first character of a line is a comment character, then the rest of the line is interpreted as a comment.
- You can use the word "no" at the beginning of the line to disable a command. For example: "no network 10.0.0.0/24 area 0.0.0.0" disables the backbone area on the specified network.

## About Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is used to manage router information in a self-contained network, such as a corporate LAN or a private WAN. With RIP, a gateway host sends its routing table to the closest router each 30 seconds. This router, then sends the contents of its routing tables to neighboring routers.

RIP is best for small networks. This is because the transmission of the full routing table each 30 seconds can put a large traffic load on the network, and because RIP tables are limited to 15 hops. OSPF is a better alternative for larger networks.

There are two versions of RIP. RIP v1 uses a UDP broadcast over port 520 to send updates to routing tables. RIP v2 uses multicast to send routing table updates.

## Routing Information Protocol (RIP) Commands

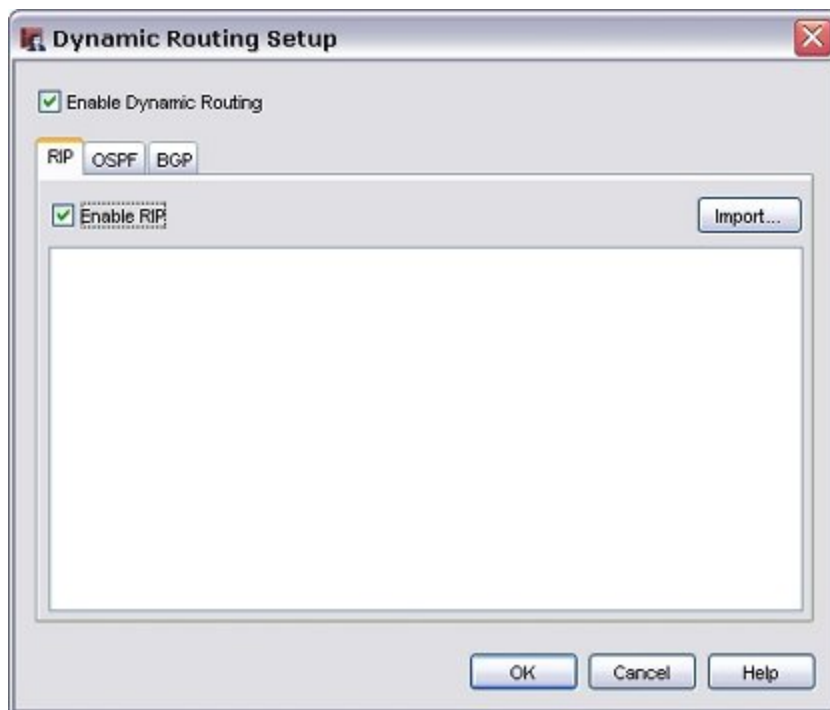
The subsequent table is a catalog of supported routing commands for RIP v1 and RIP v2 that you can use to create or modify a routing configuration file. If you use RIP v2, you must include the subnet mask with any command that uses a network IP address or RIP v2 will not operate. The sections must appear in the configuration file in the same order they appear in this table.

Section	Command	Description
<b>Set simple password or MD5 authentication on an interface</b>		
	interface eth [N]	Begin section to set
		Authentication type for interface
	ip rip authentication string [PASSWORD]	Set RIP authentication password
	key chain [KEY-CHAIN]	Set MD5 key chain name
	key [INTEGER]	Set MD5 key number
	key-string [AUTH-KEY]	Set MD5 authentication key
	ip rip authentication mode md5	Use MD5 authentication
	ip rip authentication mode key-chain [KEY-CHAIN]	Set MD5 authentication key-chain
<b>Configure RIP routing daemon</b>		
	router rip	Enable RIP daemon
	version [1/2]	Set RIP version to 1 or 2 (default version 2)
	ip rip send version [1/2]	Set RIP to send version 1 or 2
	ip rip receive version [1/2]	Set RIP to receive version 1 or 2
	no ip split-horizon	Disable split-horizon; enabled by default

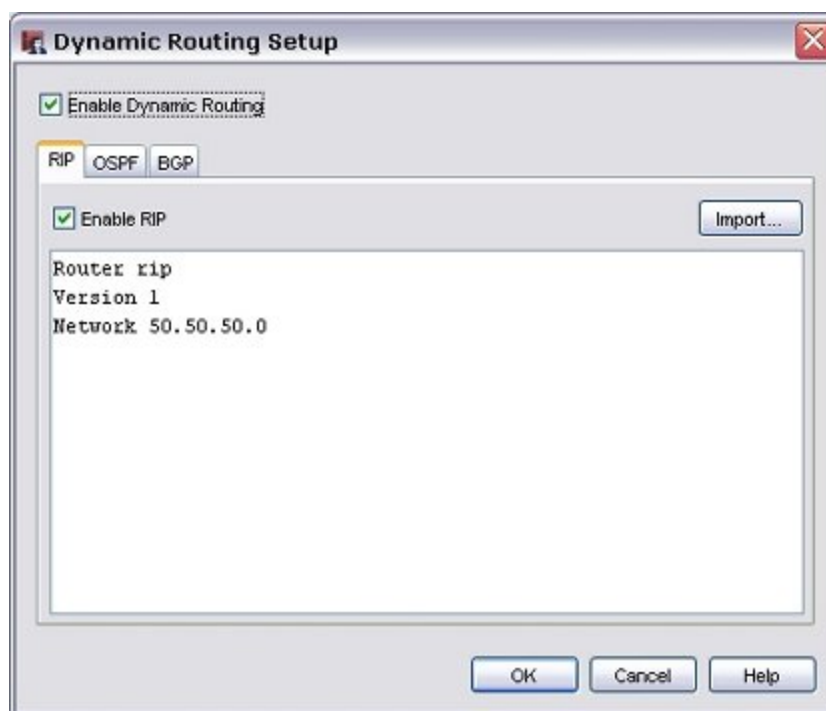
Section	Command	Description
<b>Configure interfaces and networks</b>		
	no network eth[N]	
	passive-interface eth[N]	
	passive-interface default	
	network [A.B.C.D/M]	
	neighbor [A.B.C.D/M]	
<b>Distribute routes to RIP peers and inject OSPF or BGP routes to RIP routing table</b>		
	default-information originate	Share route of last resort (default route) with RIP peers
	redistribute kernel	Redistribute firewall static routes to RIP peers
	redistribute connected	Redistribute routes from all interfaces to RIP peers
	redistribute connected route-map [MAPNAME]	Redistribute routes from all interfaces to RIP peers, with a route map filter (mapname)
	redistribute ospf	Redistribute routes from OSPF to RIP
	redistribute ospf route-map [MAPNAME]	Redistribute routes from OSPF to RIP, with a route map filter (mapname)
	redistribute bgp	Redistribute routes from BGP to RIP
	redistribute bgp route-map [MAPNAME]	Redistribute routes from BGP to RIP, with a route map filter (mapname)
<b>Configure route redistribution filters with route maps and access lists</b>		
	access-list [PERMIT DENY] [LISTNAME] [A,B,C,D/M   ANY]	Create an access list to allow or deny redistribution of only one IP address or for all IP addresses
	route-map [MAPNAME] permit [N]	Create a route map with a name and allow with a priority of N
	match ip address [LISTNAME]	

## Configure the XTM Device to Use RIP v1

1. Select **Network > Dynamic Routing**.  
*The Dynamic Routing Setup dialog box appears.*
2. Select the **Enable Dynamic Routing** check box.
3. Click the **RIP** tab.



4. Select the **Enable RIP** check box.
5. To import a routing daemon configuration file, click **Import** and select the file.  
Or, copy and paste the text of your configuration file in the text box.



6. Click **OK**.

For more information, see *About Routing Daemon Configuration Files* on page 227.

## Allow RIP v1 Traffic Through the XTM Device

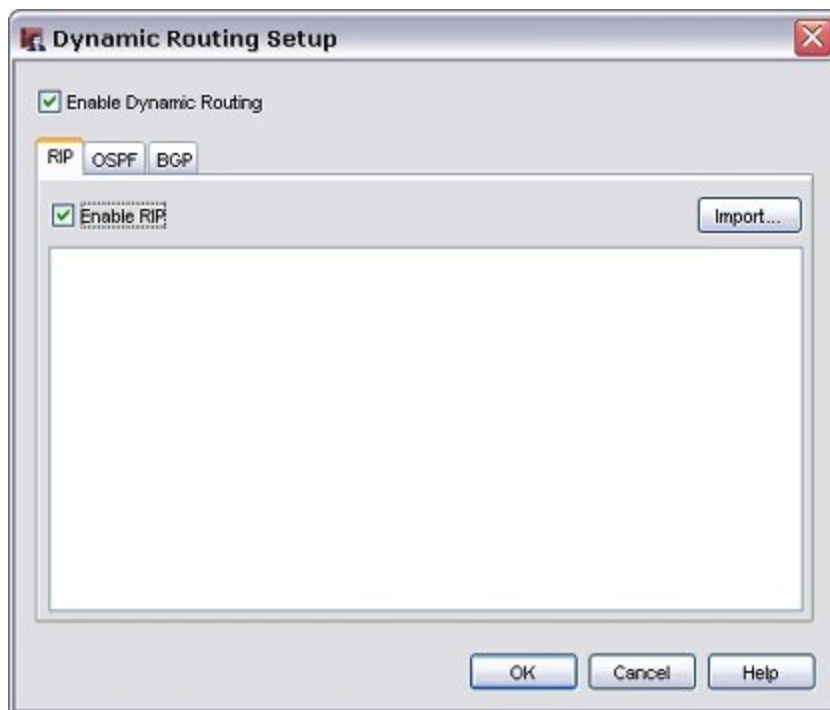
You must add and configure a policy to allow RIP broadcasts from the router to the network broadcast IP address. You must also add the IP address of the XTM device interface to the **To** section.

1. Click **+**  
Or, select **Edit > Add Policies**.
2. From the list of packet filters, select **RIP**. Click **Add**.
3. In the **New Policy Properties** dialog box, configure the policy to allow traffic from the IP or network address of the router that uses RIP to the XTM device interface to which it connects. You must also add the network broadcast IP address.
4. Click **OK**.
5. Set up the router you selected in Step 3.
6. After you configure the router, open the *Traffic and Performance Statistics (Status Report)* and look at the dynamic routing section to verify that the XTM device and the router are sending updates to each other.

You can then add authentication and restrict the RIP policy to listen only on the correct interfaces.

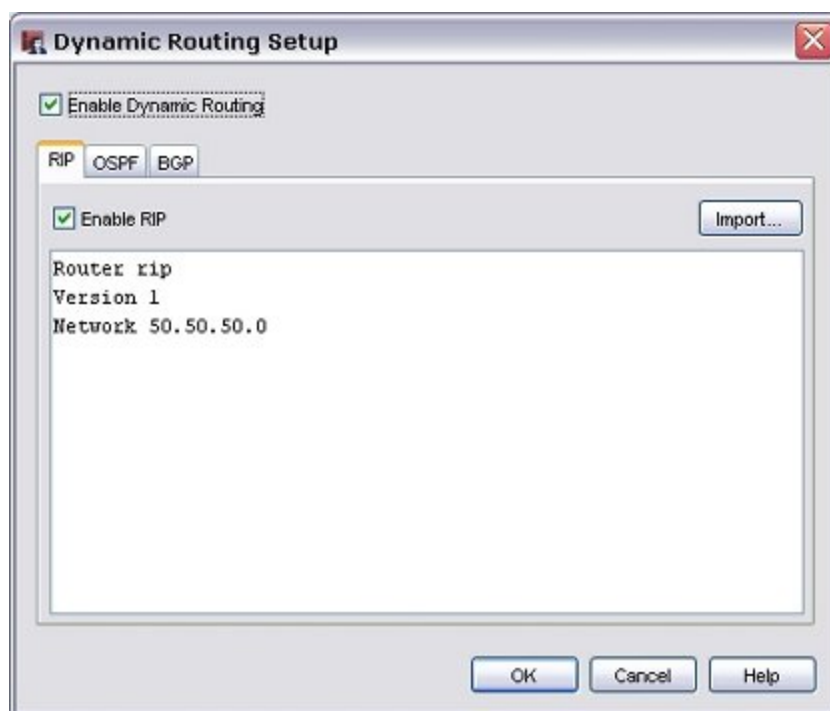
## Configure the XTM Device to Use RIP v2

1. Select **Network > Dynamic Routing**.  
*The Dynamic Routing Setup dialog box appears.*
2. Select the **Enable Dynamic Routing** check box.
3. Select the **RIP** tab.



4. Select the **Enable RIP** check box.
5. To import a routing daemon configuration file, click **Import** and select the file.  
Or, copy and paste the text of your configuration file in the text box.





6. Click **OK**.

For more information, see *About Routing Daemon Configuration Files* on page 227.

## Allow RIP v2 Traffic Through the XTM Device

You must add and configure a policy to allow RIP v2 multicasts from the routers that have RIP v2 enabled to the reserved multicast IP address for RIP v2.

1. Click **+**  
Or, select **Edit > Add Policies**.
2. From the list of packet filters, select **RIP**. Click **Add**.
3. In the **New Policy Properties** dialog box, configure the policy to allow traffic from the IP or network address of the router that uses RIP to the multicast address 224.0.0.9.
4. Click **OK**.
5. Set up the router you selected in Step 3.
6. After you configure the router, open the *Traffic and Performance Statistics (Status Report)* and look at the dynamic routing section to verify that the XTM device and the router are sending updates to each other.

You can then add authentication and restrict the RIP policy to listen only on the correct interfaces.

## Sample RIP Routing Configuration File

To use any of the dynamic routing protocols with Fireware XTM, you must import or copy and paste a configuration file for the dynamic routing daemon. This topic includes a sample configuration file for the RIP routing daemon. If you want to use this configuration file as a base for your own configuration file, copy the text into an application such as Notepad or Wordpad and save it with a new name. You can then edit the parameters to meet the requirements of your organization.

Optional commands are commented with the "!" character. To enable a command, delete the "!" and modify variables as necessary.

```
!! SECTION 1: Configure MD5 authentication keychains.
! Set MD5 authentication key chain name (KEYCHAIN), key number (1),
! and authentication key string (AUTHKEY).
! key chain KEYCHAIN
! key 1 ! key-string AUTHKEY
!! SECTION 2: Configure interface properties.
! Set authentication for interface (eth1).
! interface eth1
!
! Set RIP simple authentication password (SHAREDKEY).
! ip rip authentication string SHAREDKEY
!
! Set RIP MD5 authentication and MD5 keychain (KEYCHAIN).
! ip rip authentication mode md5
! ip rip authentication key-chain KEYCHAIN
!
!! SECTION 3: Configure global RIP daemon properties.
! Enable RIP daemon. Must be enabled for all RIP configurations. router rip
!
! Set RIP version to 1; default is version 2.
! version 1
!
! Set RIP to send or received to version 1; default is version 2.
! ip rip send version 1
! ip rip receive version 1
!
! Disable split-horizon to prevent routing loop. Default is enabled.
! no ip split-horizon
!! SECTION 4: Configure interfaces and networks.
! Disable RIP send and receive on interface (eth0).
! no network eth0
!
! Set RIP to receive-only on interface (eth2).
! passive-interface eth2
!
! Set RIP to receive-only on all interfaces.
! passive-interface default
!
! Enable RIP broadcast (version 1) or multicast (version 2) on
! network (192.168.253.0/24). !network 192.168.253.0/24
!
```

```

! Set unicast routing table updates to neighbor (192.168.253.254).
! neighbor 192.168.253.254
!! SECTION 5: Redistribute RIP routes to peers and inject OSPF or BGP
!! routes to RIP routing table.
! Share route of last resort (default route) from kernel routing table
! with RIP peers.
! default-information originate
!
! Redistribute firewall static routes to RIP peers.
! redistribute kernel
!
! Set route maps (MAPNAME) to restrict route redistribution in Section 6.
! Redistribute routes from all interfaces to RIP peers or with a route map
! filter (MAPNAME).
! redistribute connected
! redistribute connected route-map MAPNAME
!
! Redistribute routes from OSPF to RIP or with a route map filter (MAPNAME).
! redistribute ospf !redistribute ospf route-map MAPNAME
!
! Redistribute routes from BGP to RIP or with a route map filter (MAPNAME).
! redistribute bgp !redistribute bgp route-map MAPNAME
!! SECTION 6: Configure route redistribution filters with route maps and
!! access lists.
! Create an access list to only allow redistribution of 172.16.30.0/24.
! access-list LISTNAME permit 172.16.30.0/24
! access-list LISTNAME deny any
!
! Create a route map with name MAPNAME and allow with a priority of 10.
! route-map MAPNAME permit 10
! match ip address LISTNAME

```

## About Open Shortest Path First (OSPF) Protocol

**Note** Support for this protocol is available only on Fireware XTM with a Pro upgrade.

OSPF (Open Shortest Path First) is an interior router protocol used in larger networks. With OSPF, a router that sees a change to its routing table or that detects a change in the network immediately sends a multicast update to all other routers in the network. OSPF is different from RIP because:

- OSPF sends only the part of the routing table that has changed in its transmission. RIP sends the full routing table each time.
- OSPF sends a multicast only when its information has changed. RIP sends the routing table every 30 seconds.

Also, note the following about OSPF:

- If you have more than one OSPF area, one area must be area 0.0.0.0 (the backbone area).
- All areas must be adjacent to the backbone area. If they are not, you must configure a virtual link to the backbone area.

## OSPF Commands

To create or modify a routing configuration file, you must use the correct routing commands. The subsequent table is a catalog of supported routing commands for OSPF. The sections must appear in the configuration file in the same order they appear in this table. You can also use the sample text found in the *Sample OSPF Routing Configuration File* on page 241.

Section	Command	Description
<b>Configure Interface</b>		
	ip ospf authentication-key [PASSWORD]	Set OSPF authentication password
	interface eth[N]	Begin section to set properties for interface
	ip ospf message-digest-key [KEY-ID] md5 [KEY]	Set MD5 authentication key ID and key
	ip ospf cost [1-65535]	Set link cost for the interface (see OSP Interface Cost table below)
	ip ospf hello-interval [1-65535]	Set interval to send hello packets; default is 10 seconds
	ip ospf dead-interval [1-65535]	Set interval after last hello from a neighbor before declaring it down; default is 40 seconds
	ip ospf retransmit-interval [1-65535]	Set interval between link-state advertisements (LSA) retransmissions; default is 5 seconds
	ip ospf transmit-delay [1-3600]	Set time required to send LSA update; default is 1 second
	ip ospf priority [0-255]	Set route priority; high value increases eligibility to become the designated router (DR)
<b>Configure OSPF Routing Daemon</b>		
	router ospf	Enable OSPF daemon
	ospf router-id [A.B.C.D]	set router ID for OSPF manually; router determines its own ID if not set
	ospf rfc 1583compatibility	Enable RFC 1583 compatibility (can lead to route loops)

Section	Command	Description
	ospf abr-type [cisco   ibm   shortcut   standard]	More information about this command can be found in draft-ietf-abr-o5.txt
	passive-interface eth[N]	Disable OSPF announcement on interface eth[N]
	auto-cost reference bandwidth[0-429495]	Set global cost (see OSPF cost table below); do not use with "ip ospf [COST]" command
	timers spf [0-4294967295][0-4294967295]	Set OSPF schedule delay and hold time
<b>Enable OSPF on a Network</b>		
*The "area" variable can be typed in two formats: [W.X.Y.Z]; or as an integer [Z].		
	network [A.B.C.D/M] area [Z]	Announce OSPF on network A.B.C.D/M for area 0.0.0.Z
<b>Configure Properties for Backbone area or Other Areas</b>		
The "area" variable can be typed in two formats: [W.X.Y.Z]; or as an integer [Z].		
	area [Z] range [A.B.C.D/M]	Create area 0.0.0.Z and set a classful network for the area (range and interface network and mask setting should match)
	area [Z] virtual-link [W.X.Y.Z]	Set virtual link neighbor for area 0.0.0.Z
	area [Z] stub	Set area 0.0.0.Z as a stub
	area [Z] stub no-summary	
	area [Z] authentication	Enable simple password authentication for area 0.0.0.Z
	area [Z] authentication message-digest	Enable MD5 authentication for area 0.0.0.Z
<b>Redistribute OSPF Routes</b>		
	default-information originate	Share route of last resort (default route) with OSPF

Section	Command	Description
	default-information originate metric [0-16777214]	Share route of last resort (default route) with OSPF, and add a metric used to generate the default route
	default-information originate always	Always share the route of last resort (default route)
	default-information originate always metric [0-16777214]	Always share the route of last resort (default route), and add a metric used to generate the default route
	redistribute connected	Redistribute routes from all interfaces to OSPF
	redistribute connected metrics	Redistribute routes from all interfaces to OSPF, and a metric used for the action
<b>Configure Route Redistribution with Access Lists and Route Maps</b>		
	access-list [LISTNAME] permit [A.B.C.D/M]	Create an access list to allow distribution of A.B.C.D/M
	access-lists [LISTNAME] deny any	Restrict distribution of any route map not specified above
	route-map [MAPNAME] permit [N]	Create a route map with name [MAPNAME] and allow with a priority of [N]
	match ip address [LISTNAME]	

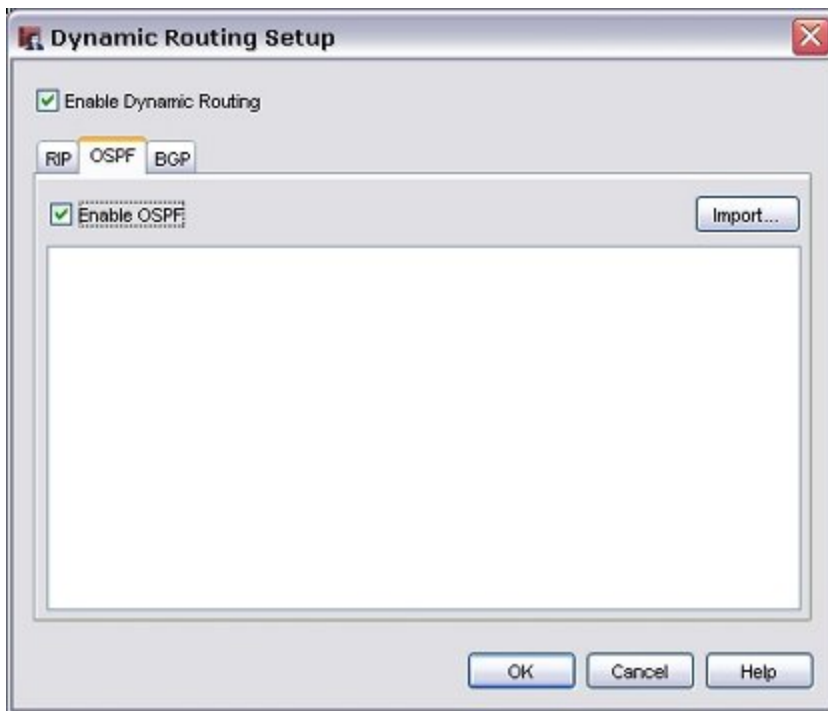
## OSPF Interface Cost Table

The OSPF protocol finds the most efficient route between two points. To do this, it looks at factors such as interface link speed, the number of hops between points, and other metrics. By default, OSPF uses the actual link speed of a device to calculate the total cost of a route. You can set the interface cost manually to help maximize efficiency if, for example, your gigabyte-based firewall is connected to a 100M router. Use the numbers in this table to manually set the interface cost to a value different than the actual interface cost.

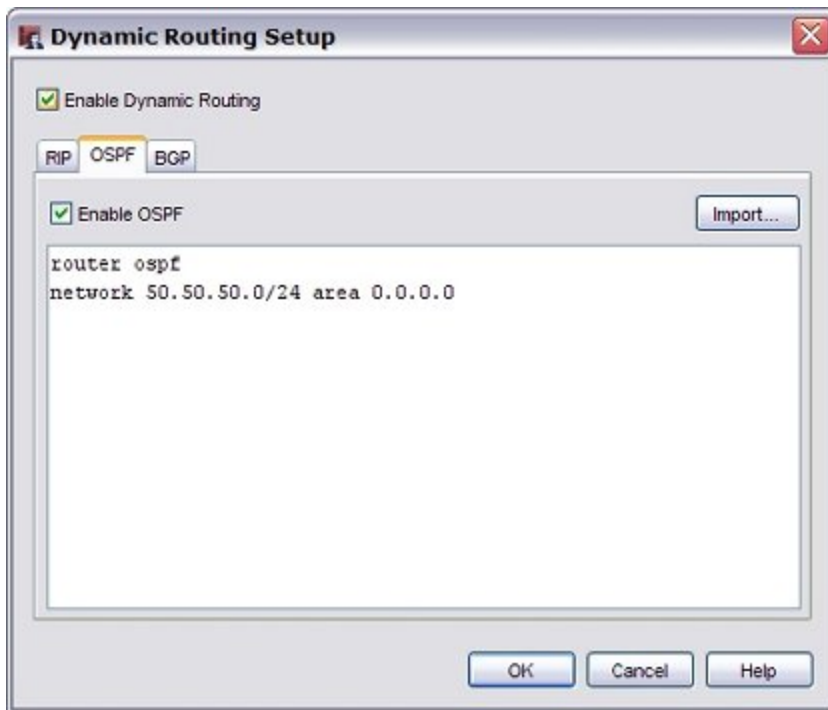
Interface Type	Bandwidth in bits/second	Bandwidth in bytes/second	OSPF Interface Cost
Ethernet	1G	128M	1
Ethernet	100M	12.5M	10
Ethernet	10M	1.25M	100
Modem	2M	256K	500
Modem	1M	128K	1000
Modem	500K	62.5K	2000
Modem	250K	31.25K	4000
Modem	125K	15625	8000
Modem	62500	7812	16000
Serial	115200	14400	10850
Serial	57600	7200	21700
Serial	38400	4800	32550
Serial	19200	2400	61120
Serial	9600	1200	65535

## Configure the XTM Device to Use OSPF

1. Select **Network > Dynamic Routing**.  
*The Dynamic Routing Setup dialog box appears.*
2. Select the **Enable Dynamic Routing** check box.
3. Click the **OSPF** tab.



4. Select the **Enable OSPF** check box.
5. Click **Import** to import a routing daemon configuration file, or copy and paste your configuration file in the text box.



For more information, see *About Routing Daemon Configuration Files* on page 227.



To get started, you need only two commands in your OSPF configuration file. These two commands, in this order, start the OSPF process:

```
router ospf
network <network IP address of the interface you want the process to listen on and distribute
through the protocol> area <area ID in x.x.x.x format, such as 0.0.0.0>
```

6. Click **OK**.

## Allow OSPF Traffic Through the XTM Device

You must add and configure a policy to allow OSPF multicasts from the routers that have OSPF enabled, to the reserved multicast addresses for OSPF.

1. Click **+**  
Or, select **Edit > Add Policies**.
2. From the list of packet filters, select **OSPF**. Click **Add**.
3. In the **New Policy Properties** dialog box, configure the policy to allow traffic from the IP or network address of the router using OSPF to the IP addresses 224.0.0.5 and 224.0.0.6.

For information on how to set the source and destination addresses for a policy, see *Set Access Rules for a Policy* on page 392.

4. Click **OK**.
5. Set up the router you selected in Step 3.
6. After you configure the router, open the *Traffic and Performance Statistics (Status Report)* and look at the dynamic routing section to verify that the XTM device and the router are sending updates to each other.

You can then add authentication and restrict the OSPF policy to listen only on the correct interfaces.

## Sample OSPF Routing Configuration File

To use any of the dynamic routing protocols with Firewall XTM, you must import or copy and paste a configuration file for the dynamic routing daemon. This topic includes a sample configuration file for the OSPF routing daemon. To use this configuration file as a base for your own configuration file, copy the text into a new text file and save it with a new name. You can then edit the parameters to meet the requirements of your organization.

Optional commands are commented with the "!" character. To enable a command, delete the "!" and modify variables as necessary.

```
!! SECTION 1: Configure interface properties.
! Set properties for interface eth1.
! interface eth1
!
! Set simple authentication password (SHAREDKEY).
! ip ospf authentication-key SHAREDKEY
!
! Set MD5 authentication key ID (10) and MD5 authentication key (AUTHKEY).
! ip ospf message-digest-key 10 md5 AUTHKEY
!
! Set link cost to 1000 (1-65535) on interface eth1.
! for OSPF link cost table. !ip ospf cost 1000
```

```
!  
! Set hello interval to 5 seconds (1-65535); default is 10 seconds.  
! ip ospf hello-interval 5  
!  
! Set dead-interval to 15 seconds (1-65535); default is 40 seconds.  
! ip ospf dead-interval 15  
!  
! Set interval between link-state advertisements (LSA) retransmissions  
! to 10 seconds (1-65535); default is 5 seconds.  
! ip ospf retransmit-interval 10  
!  
! Set LSA update interval to 3 seconds (1-3600); default is 1 second.  
! ip ospf transmit-delay 3  
!  
! Set high priority (0-255) to increase eligibility to become the  
! designated router (DR).  
! ip ospf priority 255  
!! SECTION 2: Start OSPF and set daemon properties.  
! Enable OSPF daemon. Must be enabled for all OSPF configurations.  
! router ospf  
!  
! Set the router ID manually to 100.100.100.20. If not set, the firewall will  
! set its own ID based on an interface IP address.  
! ospf router-id 100.100.100.20  
!  
! Enable RFC 1583 compatibility (increases probability of routing loops).  
! ospf rfc1583compatibility  
!  
! Set area border router (ABR) type to cisco, ibm, shortcut, or standard.  
! More information about ABR types is in draft-ietf-ospf-abr-alt-05.txt.  
! ospf abr-type cisco  
!  
! Disable OSPF announcement on interface eth0.  
! passive interface eth0  
!  
! Set global cost to 1000 (0-429495).  
! auto-cost reference bandwidth 1000  
!  
! Set SPF schedule delay to 25 (0-4294967295) seconds and hold time to  
! 20 (0-4294967295) seconds; default is 5 and 10 seconds. !timers spf 25 20  
!! SECTION 3: Set network and area properties. Set areas with W.X.Y.Z  
!! or Z notation.  
! Announce OSPF on network 192.168.253.0/24 network for area 0.0.0.0.  
! network 192.168.253.0/24 area 0.0.0.0  
!  
! Create area 0.0.0.1 and set a classful network range (172.16.254.0/24)  
! for the area (range and interface network settings must match).  
! area 0.0.0.1 range 172.16.254.0/24  
!  
! Set virtual link neighbor (172.16.254.1) for area 0.0.0.1.  
! area 0.0.0.1 virtual-link 172.16.254.1  
!  
! Set area 0.0.0.1 as a stub on all routers in area 0.0.0.1.  
! area 0.0.0.1 stub
```

```
!  
! area 0.0.0.2 stub no-summary  
!  
! Enable simple password authentication for area 0.0.0.0.  
! area 0.0.0.0 authentication  
!  
! Enable MD5 authentication for area 0.0.0.1.  
! area 0.0.0.1 authentication message-digest  
!! SECTION 4: Redistribute OSPF routes  
! Share route of last resort (default route) from kernel routing table  
! with OSPF peers.  
! default-information originate  
!  
! Redistribute static routes to OSPF.  
! redistribute kernel  
!  
! Redistribute routes from all interfaces to OSPF.  
! redistribute connected  
! redistribute connected route-map  
!! Redistribute routes from RIP and BGP to OSPF.  
! redistribute rip !redistribute bgp  
!! SECTION 5: Configure route redistribution filters with access lists  
!! and route maps.  
! Create an access list to only allow redistribution of 10.0.2.0/24.  
! access-list LISTNAME permit 10.0.2.0/24  
! access-list LISTNAME deny any  
!  
! Create a route map with name MAPNAME and allow with a  
priority of 10 (1-199).  
! route-map MAPNAME permit 10  
! match ip address LISTNAME
```

## About Border Gateway Protocol (BGP)

**Note** Support for this protocol is available only in Fireware XTM with a Pro upgrade.

Border Gateway Protocol (BGP) is a scalable dynamic routing protocol used on the Internet by groups of routers to share routing information. BGP uses route parameters or *attributes* to define routing policies and create a stable routing environment. This protocol allows you to advertise more than one path to and from the Internet to your network and resources, which gives you redundant paths and can increase your uptime.

Hosts that use BGP use TCP to send updated routing table information when one host finds a change. The host sends only the part of the routing table that has the change. BGP uses classless interdomain routing (CIDR) to reduce the size of the Internet routing tables. The size of the BGP routing table in Fireware XTM is set at 32K.

The size of the typical WatchGuard customer wide area network (WAN) is best suited for OSPF dynamic routing. A WAN can also use external border gateway protocol (EBGP) when more than one gateway to the Internet is available. EBGP allows you to take full advantage of the redundancy possible with a multi-homed network.

To participate in BGP with an ISP you must have an autonomous system number (ASN). You must get an ASN from one of the regional registries in the table below. After you are assigned your own ASN, you must contact each ISP to get their ASNs and other necessary information.

Region	Registry Name	Web Site
North America	RIN	<a href="http://www.arin.net">www.arin.net</a>
Europe	RIPE NCC	<a href="http://www.ripe.net">www.ripe.net</a>
Asia Pacific	APNIC	<a href="http://www.apnic.net">www.apnic.net</a>
Latin America	LACNIC	<a href="http://www.lacnic.net">www.lacnic.net</a>
Africa	AfriNIC	<a href="http://www.afrinic.net">www.afrinic.net</a>

## BGP Commands

To create or modify a routing configuration file, you must use the correct routing commands. The subsequent table is a catalog of supported BGP routing commands. The sections must appear in the configuration file in the same order they appear in this table.

Do not use BGP configuration parameters that you do not get from your ISP.

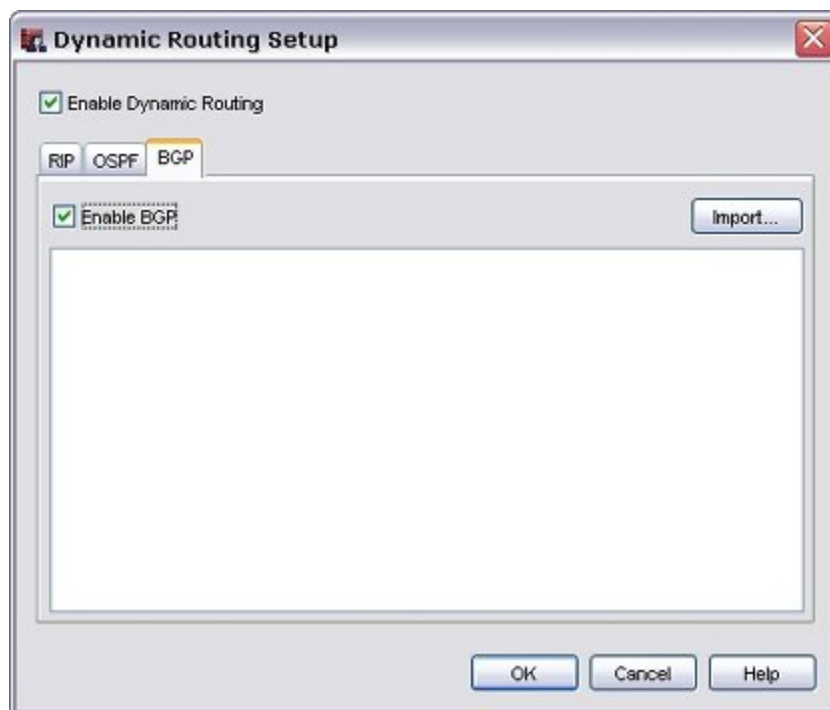
Section	Command	Description
<b>Configure BGP Routing Daemon</b>		
	router bgp [ASN]	Enable BGP daemon and set autonomous system number (ASN); this is supplied by your ISP
	network [A.B.C.D/M]	Announce BGP on network A.B.C.D/M
	no network [A.B.C.D/M]	Disable BGP announcements on network A.B.C.D/M
<b>Set Neighbor Properties</b>		
	neighbor [A.B.C.D] remote-as [ASN]	Set neighbor as a member of remote ASN
	neighbor [A.B.C.D] ebgp-multihop	Set neighbor on another network using EBGp multi-hop
	neighbor [A.B.C.D] version 4+	Set BGP version (4, 4+,4-) for communication with neighbor; default is 4
	neighbor [A.B.C.D] update-source [WORD]	Set the BGP session to use a specific interface for TCP connections
	neighbor [A.B.C.D] default-originate	Announce default route to BGP neighbor [A,B,C,D]
	neighbor [A.B.C.D] port 189	Set custom TCP port to communicate with BGP neighbor [A,B,C,D]
	neighbor [A.B.C.D] send-community	Set peer send-community
	neighbor [A.B.C.D] weight 1000	Set a default weight for neighbor's [A.B.C.D] routes
	neighbor [A.B.C.D] maximum-prefix [NUMBER]	Set maximum number of prefixes allowed from this neighbor
<b>Community Lists</b>		
	ip community-list [<1-99> <100-199>] permit AA:NN	Specify community to accept autonomous system number and network number separated by a colon

Section	Command	Description
<b>Peer Filtering</b>		
	neighbor [A.B.C.D] distribute-list [LISTNAME] [IN   OUT]	Set distribute list and direction for peer
	neighbor [A.B.C.D] prefix-list [LISTNAME] [IN   OUT]	To apply a prefix list to be matched to incoming advertisements or outgoing advertisements to that neighbor
	neighbor [A.B.C.D] filter-list [LISTNAME] [IN   OUT]	To match an autonomous system path access list to incoming routes or outgoing routes
	neighbor [A.B.C.D] route-map [MAPNAME] [IN   OUT]	To apply a route map to incoming or outgoing routes
<b>Redistribute Routes to BGP</b>		
	redistribute kernel	Redistribute static routes to BGP
	redistribute rip	Redistribute RIP routes to BGP
	redistribute ospf	Redistribute OSPF routes to BGP
<b>Route Reflection</b>		
	bgp cluster-id A.B.C.D	To configure the cluster ID if the BGP cluster has more than one route reflector
	neighbor [W.X.Y.Z] route-reflector-client	To configure the router as a BGP route reflector and configure the specified neighbor as its client
<b>Access Lists and IP Prefix Lists</b>		
	ip prefix-lists PRELIST permit A.B.C.D/E	Set prefix list
	access-list NAME [deny allow] A.B.C.D/E	Set access list
	route-map [MAPNAME] permit [N]	In conjunction with the "match" and "set" commands, this defines the conditions and actions for redistributing routes
	match ip address prefix-list [LISTNAME]	Matches the specified access-list
	set community [A:B]	Set the BGP community attribute
	match community [N]	Matches the specified community_list
	set local-preference [N]	Set the preference value for the autonomous system path

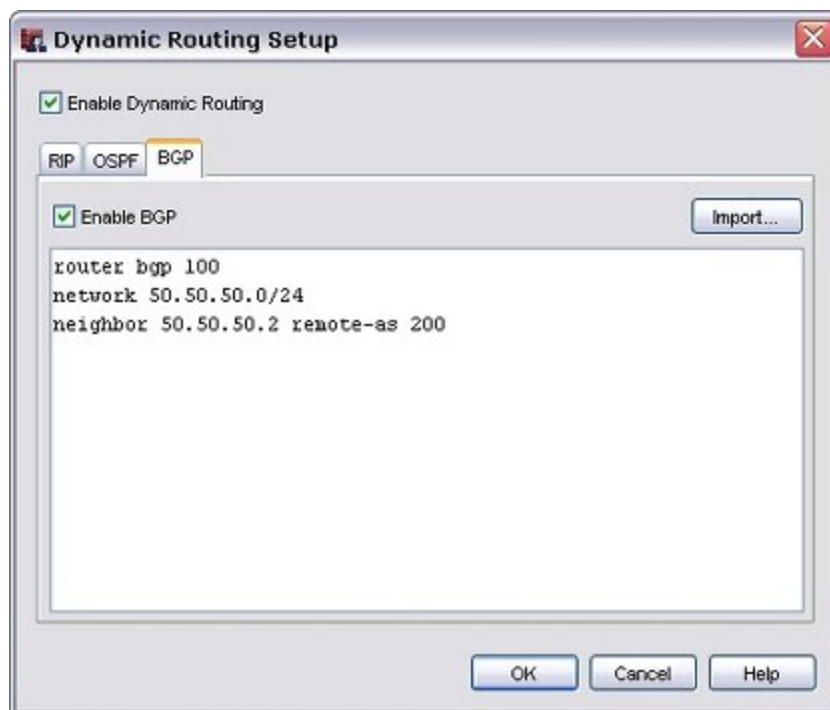
## Configure the XTM Device to Use BGP

To participate in BGP with an ISP you must have an autonomous system number (ASN). For more information, see *About Border Gateway Protocol (BGP)* on page 244.

1. Select **Network > Dynamic Routing**.  
*The Dynamic Routing Setup dialog box appears.*
2. Select the **Enable Dynamic Routing** check box.
3. Click the **BGP** tab.



4. Select the **Enable BGP** check box.
5. Click **Import** to import a routing daemon configuration file, or copy and paste your configuration file in the text box.



For more information, see *About Routing Daemon Configuration Files* on page 227.

To get started, you need only three commands in your BGP configuration file. These three commands, start the BGP process, set up a peer relationship with the ISP, and create a route for a network to the Internet. You must use the commands in this order.

```
router BGP: BGP autonomous system number supplied by your ISP
network: network IP address that you want to advertise a route to from the Internet
neighbor: <IP address of neighboring BGP router> remote-as <BGP autonomous number>
```

6. Click **OK**.

## Allow BGP Traffic Through the XTM Device

You must add and configure a policy to allow BGP traffic to the XTM device from the approved networks. These networks must be the same networks you defined in your BGP configuration file.

1. Click **+**  
Or, select **Edit > Add Policies**.
2. From the list of packet filters, select **BGP**. Click **Add**.
3. In the **New Policy Properties** dialog box, configure the policy to allow traffic from the IP or network address of the router that uses BGP to the XTM device interface it connects to. You must also add the network broadcast IP address.
4. Click **OK**.
5. Set up the router you selected in Step 3.
6. After you configure the router, open the *Traffic and Performance Statistics (Status Report)* and look at the dynamic routing section to verify that the XTM device and the router are sending updates to each other.

You can then add authentication and restrict the BGP policy to listen only on the correct interfaces.



## Sample BGP Routing Configuration File

To use any of the dynamic routing protocols with Fireware XTM, you must import or type a configuration file for the dynamic routing daemon. This topic includes a sample configuration file for the BGP routing daemon. If you want to use this configuration file as a base for your own configuration file, copy the text into an application such as Notepad or Wordpad and save it with a new name. You can then edit the parameters to meet your own business requirements.

Optional commands are commented with the "!" character. To enable a command, delete the "!" and modify variables as necessary.

```
!! SECTION 1: Start BGP daemon and announce network blocks to BGP neighbors
! Enable BGP and set local ASN to 100 router bgp 100
! Announce local network 64.74.30.0/24 to all neighbors defined in section 2
! network 64.74.30.0/24
!! SECTION 2: Neighbor properties
! Set neighbor (64.74.30.1) as member of remote ASN (200)
! neighbor 64.74.30.1 remote-as 200
! Set neighbor (208.146.43.1) on another network using EBGP multi-hop
! neighbor 208.146.43.1 remote-as 300
! neighbor 208.146.43.1 ebgp-multihop
! Set BGP version (4, 4+, 4-) for communication with a neighbor; default is 4
! neighbor 64.74.30.1 version 4+
! Announce default route to BGP neighbor (64.74.30.1)
! neighbor 64.74.30.1 default-originate
! Set custom TCP port 189 to communicate with BGP neighbor (64.74.30.1). Default
  port is TCP 179
! neighbor 64.74.30.1 port 189
! Set peer send-community
! neighbor 64.74.30.1 send-community
! Set a default weight for neighbor's (64.74.30.1) routes
! neighbor 64.74.30.1 weight 1000
! Set maximum number of prefixes allowed from this neighbor
! neighbor 64.74.30.1 maximum-prefix NUMBER

!! SECTION 3: Set community lists
  ! ip community-list 70 permit 7000:80

!! SECTION 4: Announcement filtering
! Set distribute list and direction for peer
! neighbor 64.74.30.1 distribute-list LISTNAME [in|out]
  ! To apply a prefix list to be matched to incoming or outgoing advertisements
  to that neighbor
! neighbor 64.74.30.1 prefix-list LISTNAME [in|out]
! To match an autonomous system path access list to incoming or outgoing routes
! neighbor 64.74.30.1 filter-list LISTNAME [in|out]
! To apply a route map to incoming or outgoing routes
! neighbor 64.74.30.1 route-map MAPNAME [in|out]

!! SECTION 5: Redistribute routes to BGP
! Redistribute static routes to BGP
! Redistribute kernel
```

```
! Redistribute rip routes to BGP
! Redistribute rip
! Redistribute ospf routes to BGP

! Redistribute ospf

!! SECTION 6: Route reflection
! Set cluster ID and firewall as a client of route reflector server 51.210.0.254
! bgp cluster-id A.B.C.D
! neighbor 51.210.0.254 route-reflector-client

!! SECTION 7: Access lists and IP prefix lists
! Set prefix list
! ip prefix-list PRELIST permit 10.0.0.0/8
! Set access list!access-list NAME deny 64.74.30.128/25
! access-list NAME permit 64.74.30.0/25
! Create a route map with name MAPNAME and allow with a priority of 10
! route-map MAPNAME permit 10
! match ip address prefix-list LISTNAME
! set community 7000:80
```

# 11 FireCluster

---

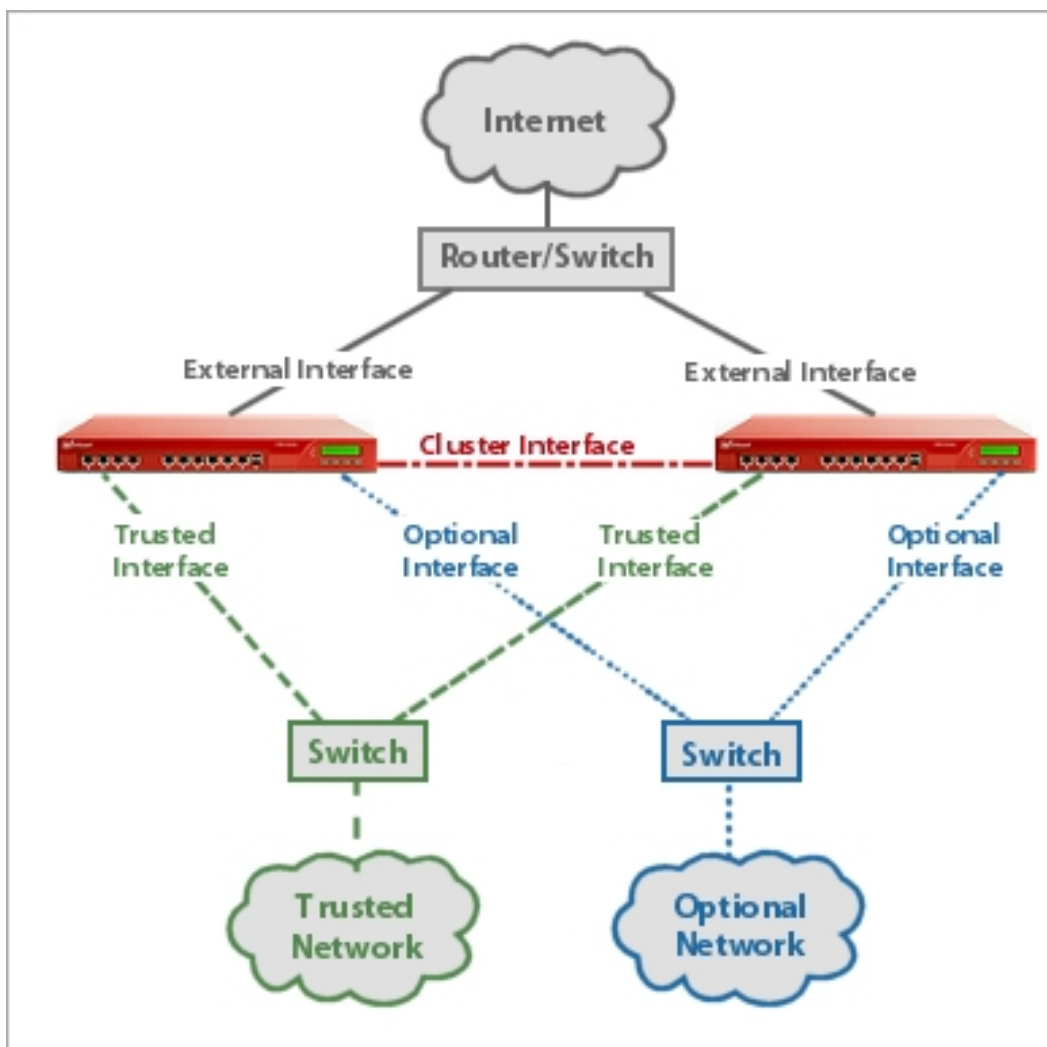
## About WatchGuard FireCluster

You can use WatchGuard FireCluster to configure two XTM devices as a cluster to increase network performance and scalability.

**Note** *FireCluster is not supported on XTM 2 Series devices.*

There are two configuration options available when you configure FireCluster: active/passive and active/active. To add redundancy, choose an active/passive cluster. To add both redundancy and load sharing to your network, select an active/active cluster.

When you enable FireCluster, you manage and monitor the two devices in the cluster as a single virtual device.



To configure an active/passive cluster, your network interfaces must be configured in mixed routing or drop-in mode. To configure an active/active cluster, your network interfaces must be configured in mixed routing mode. FireCluster does not support bridge network mode. For more information about network modes, see *About Network Interface Setup*.

When FireCluster is enabled, your XTM devices continue to support:

- Secondary networks on external, trusted, or optional interfaces
- Multi-WAN connections  
(Limitation: a multi-WAN failover caused by a failed connection to a link monitor host does not trigger FireCluster failover. FireCluster failover occurs only when the physical interface is down or does not respond.)
- VLANs

When a cluster member fails, the cluster seamlessly fails over and maintains:

- Packet filter connections
- BOVPN tunnels
- User sessions

These connections may be disconnected when a failover event occurs:

- Proxy connections
- Mobile VPN with PPTP
- Mobile VPN with IPsec
- Mobile VPN with SSL

Mobile VPN users may need to manually restart the VPN connection after a failover.

For more information about FireCluster failover, see *About FireCluster Failover* on page 253.

## FireCluster Status

To see the status of FireCluster in Firebox System Manager:

1. *Start Firebox System Manager.*
2. Find the FireCluster information, as described in *XTM Device Status*.

**Note** *You cannot use Fireware XTM Web UI to manage or monitor a device that is configured as a FireCluster member.*

## About FireCluster Failover

The FireCluster failover process is the same for an active/active cluster or an active/passive cluster. With both types of clusters, each cluster member maintains state and session information at all times. When failover occurs, the packet filter connections, BOVPN tunnels, and user sessions from the failed device fail over automatically to the other device in the cluster.

In a FireCluster, one device is the cluster master and the other device is the backup master. The backup master uses the primary cluster interface to synchronize connection and session information with the cluster master. If the primary cluster interface fails or is disconnected, the backup master uses the backup cluster interface to communicate with the cluster master. We recommend that you always configure both a primary cluster interface and a backup cluster interface. This helps to make sure that if a failover occurs on the cluster master, the backup master has all the necessary information to become the new cluster master, and can transfer connections and sessions appropriately.

## Events that Trigger a Failover

There are three types of events that can trigger a failover.

### *Monitored interface link down on the cluster master*

A failover starts if a monitored interface on the cluster master is unable to send or receive traffic. You can see the list of monitored interfaces in the FireCluster configuration in Policy Manager.

### *Cluster master device not fully functional*

A failover starts if a software malfunction or hardware failure is detected on the cluster master, or if a critical process fails on the cluster master.

*Cluster receives the Failover Master command from Firebox System Manager*

In Firebox System Manager, when you select **Tools > Cluster > Failover Master**, you force a failover from the cluster master to the backup master.

For more information about this command, see *Force a Failover of the Cluster Master* on page 285.

## What Happens When a Failover Occurs

When a failover of the cluster master occurs, the backup master becomes the cluster master. Then the original cluster master reboots and rejoins the cluster as the backup master. The cluster fails over and maintains all packet filter connections, BOVPN tunnels and user sessions. This behavior is the same for an active/active or an active/passive FireCluster.

In an active/active cluster, if the backup master fails, the cluster fails over and maintains all packet filter connections, BOVPN tunnels, and user sessions. Proxy connections and Mobile VPN connections can be interrupted, as described in the subsequent table. In an active/passive cluster, if the backup master fails, there is no interruption of connections or sessions because nothing is assigned to the backup master.

Connection/Session type	Impact of a failover event
Packet filter connections	Connections fail over to the other cluster member.
BOVPN tunnels	Tunnels fail over to the other cluster member.
User sessions	Sessions fail over to the other cluster member.
Proxy connections	Connections assigned to the failed device (master or backup master) must be restarted. Connections assigned to the other device are not interrupted.
Mobile VPN with IPSec	If the cluster master fails over, all sessions must be restarted. If the backup master fails, only the sessions assigned to the backup master must be restarted. Sessions assigned to the cluster master are not interrupted.
Mobile VPN with SSL	If either device fails over, all sessions must be restarted.
Mobile VPN with PPTP	All PPTP sessions are assigned to the cluster master, even for an active/active cluster. If the cluster master fails over, all sessions must be restarted. If the backup master fails, PPTP sessions are not interrupted.

## FireCluster Failover and Server Load Balancing

If you use server load balancing to balance connections between your internal servers, when a FireCluster failover event occurs, real-time synchronization does not occur. After a failover, the new cluster master sends connections to all servers in the server load balancing list to discover which servers are available. It then applies the server load balancing algorithm to all available servers.

For information about server load balancing, see *Configure Server Load Balancing* on page 182.

## Monitor the Cluster During a Failover

The role of each device in the cluster appears after the member name on the Firebox System Manager **Front Panel** tab. If you look at the Front Panel tab during a failover of the cluster master, you can see the cluster master role move from one device to another. During a failover, you see:

- The role of the old backup master changes from "backup master" to "master".
- The role of the old cluster master changes to "inactive" and then to "idle" while the device restarts.
- The role of the old cluster master changes to "backup master" after the device restarts.

For more information, see *Monitor and Control FireCluster Members* on page 282.

## Features not Supported With FireCluster

There are some Fireware XTM configuration and management features that you cannot use with FireCluster.

### FireCluster Network Configuration Limitations

- For an active/active cluster, you cannot configure the network interfaces in bridge mode or drop-in mode.
- For an active/passive cluster, you cannot configure the network interfaces in bridge mode.
- You cannot configure the external interface to use PPPoE or DHCP.
- You cannot use dynamic routing protocols (RIP, OSPF and BGP).

### FireCluster Management Limitations

- You cannot use the Web UI to manage any device that is a member of a FireCluster.
- You cannot use WSM with a Management Server to schedule an OS update for any device that is a member of a FireCluster.

## About the Interface for Management IP Address

In a FireCluster configuration, all devices in the cluster share the same IP addresses for each enabled interface. When you connect to the cluster in WatchGuard System Manager, you are automatically connected to the cluster master, and see the status for all cluster members. You can use Firebox System Manager to monitor the cluster and individual cluster members as described in *Monitor and Control FireCluster Members* on page 282. You can also use Policy Manager to update the configuration of the cluster, as described in *Update the FireCluster Configuration* on page 291.

### Configure the Interface for Management IP Address

In addition to the shared IP addresses for each interface, each cluster member also has its own unique IP address for management. You can use this IP address to connect directly to an individual cluster member to monitor or manage that member.

This interface you choose for individual FireCluster device management is known as the *Interface for management IP address*. When you configure a FireCluster, you select the *Interface for management IP address* to be used by all cluster members. This interface is not dedicated to management. You can use any available interface, except a VLAN interface.

For each member, you then specify the unique *Management* IP address to use on the selected *Interface for management IP address*.

For the FireCluster Management IP address, select an unused IP address on the same subnet as the address assigned to the interface configured as the *Interface for management IP address*. You must specify a different management IP address for each cluster member. For example, if you select the trusted interface as the *Interface for management IP address*, then choose two unused IP addresses from your trusted subnet to use as the FireCluster management IP addresses. If you choose the External interface as the *Interface for management IP address*, specify two unused external IP addresses that you can dedicate to FireCluster management functions.

For most daily FireCluster management tasks, you do not use the FireCluster Management IP address.

**Note** If you use the FireCluster Management IP address to connect to the backup master, you cannot save configuration changes in Policy Manager.

## Use the Management IP Address to Restore a Backup Image

When you restore a FireCluster backup image, you must use the *Management* IP address to connect directly to a cluster member. When you use this IP address to connect to a cluster member, there are two additional commands available in Firebox System Manager on the **Tools** menu: **Cluster > Leave** and **Cluster > Join**. You use these commands when you restore a backup image to the cluster.

For more information, see *Restore a FireCluster Backup Image* on page 298.

## Use the Management IP Address to Upgrade from an External Location

The WatchGuard System Manager software uses the Management IP address when you upgrade the OS for the members of a cluster. If you want to update the OS from a remote location, make sure that:

- The *Interface for management IP address* is set to an external interface
- The *Management* IP address for each cluster member is a public IP address and is routable

For more information, see *Upgrade Fireware XTM for FireCluster Members* on page 299.



## The Management IP Address and the WatchGuard Policy

The **WatchGuard** policy (policy type WG-Firebox-Mgmt) controls administrative connections to the device. By default, the WatchGuard policy allows management connections from the **Any-Trusted** or **Any-Optional** aliases. If you set the FireCluster Management Interface to a Trusted or Optional interface, the Management Interface IP addresses are automatically included in the Any-Trusted alias or the Any-Optional alias, and you do not need to modify the WatchGuard policy for FireCluster management connections to operate correctly.

There are two situations for which you must edit the WatchGuard policy to add the FireCluster Management IP addresses:

- **If you restrict management access to specific IP addresses**  
To restrict management access to specific IP addresses, you could edit the WatchGuard policy to remove the Any-Trusted or Any-Optional aliases from the From section, and add only the IP addresses or aliases that you want to manage the device. If you do this, it is important that you also add the FireCluster Management IP addresses to the From section of the WatchGuard policy.
- **If you set the FireCluster Management Interface to an External interface**  
If you select an External interface as the FireCluster Management Interface, you must either add the FireCluster Management IP addresses or add the Any-External alias to the From section of the WatchGuard policy. Your configuration is more secure if you add the specific Management IP addresses than it is if you add the Any-External alias.

For more information about the WatchGuard policy, see *Manage an XTM device from a Remote Location*.

## Configure FireCluster

FireCluster supports two types of cluster configurations.

### *Active/Passive cluster*

In an active/passive cluster, one device is active, and the other is passive. The active device handles all network traffic unless a failover event occurs. The passive device actively monitors the status of the active device. If the active device fails, the passive device takes over the connections assigned to the failed device. After a failover event, all traffic for existing connections is automatically routed to the active device.

### *Active/Active cluster*

In an active/active cluster, the cluster members share the traffic that passes through the cluster. To distribute connections between the active devices in the cluster, configure FireCluster to use a *round-robin* or *least connections* algorithm. If one device in a cluster fails, the other cluster member takes over the connections assigned to the failed device. After a failover event, all traffic for existing connections is automatically routed to the remaining active device.

## FireCluster Requirements and Restrictions

Make sure you understand these requirements and restrictions before you begin:

- WatchGuard XTM devices in a cluster must be the same model. Supported models are XTM 5 Series, 8 Series and 10 Series. FireCluster is not supported on XTM 2 Series models.
- Each device in a cluster must use the same version of Fireware XTM with a Pro upgrade.
- Each device in a cluster must have an active LiveSecurity Service subscription.
- For an active/passive cluster, your network interfaces must be configured in mixed routing mode or drop-in mode.
- For an active/active cluster, your network interfaces must be configured in mixed routing mode.
- FireCluster does not support bridge network mode.
- For an active/active cluster, we recommend all devices have active licenses for the same optional subscription services such as WebBlocker or Gateway AntiVirus.

For more information, see *About Feature Keys and FireCluster* on page 292.

- The external interface must be configured with a static IP address. You cannot enable FireCluster if the external interface is configured to use DHCP or PPPoE.
- You must have a network switch for each active traffic interface.
- For an active/active cluster, all switches and routers in the broadcast domain must be configured to support multicast traffic.

For more information, see *Switch and Router Requirements for an Active/Active FireCluster* on page 263.

- For an active/active cluster, you must know the IP address and MAC address of each layer 3 switch or router connected to the cluster. Then you can add static ARP entries for these network devices to the FireCluster configuration.

For more information, see *Add Static ARP Entries for an Active/Active FireCluster* on page 265.

- FireCluster does not support the use of dynamic routing protocols.

## Cluster Synchronization and Status Monitoring

When you enable FireCluster, you must dedicate at least one interface to communication between the cluster members. This is called a *cluster interface*. When you set up the cluster hardware, you connect the primary cluster interfaces of each device to each other. For redundancy, we recommend you configure a backup cluster interface. The cluster members use the cluster interfaces to continually synchronize all information needed for load sharing and transparent failover.

---

## FireCluster Device Roles

When you configure devices in a cluster, it is important to understand the roles each device can play in the cluster.

### *Cluster master*

This cluster member assigns network traffic flows to cluster members, and responds to all requests from external systems such as WatchGuard System Manager, SNMP, DHCP, ARP, routing protocols, and IKE. When you configure or modify the cluster configuration, you save the cluster configuration to the cluster master. The cluster master can be either device. The first device in a cluster to power on becomes the cluster master.

### *Backup cluster master*

This cluster member synchronizes all necessary information with the cluster master, so that it can become the cluster master if the master fails. The Backup cluster master can be active or passive.

### *Active member*

This can be any cluster member that actively handles traffic flow. In an active/active cluster, both devices are active. In an active/passive cluster, the cluster master is the only active device

### *Passive member*

A device in an active/passive cluster that does not handle network traffic flows unless an active device fails over. In an active/passive cluster the passive member is the backup cluster master.

## FireCluster Configuration Steps

To configure XTM devices as a FireCluster, you must:

1. Plan your FireCluster configuration, as described in *Before You Begin* on page 260.
2. Connect the FireCluster devices to the network, as described in *Connect the FireCluster Hardware* on page 262.
3. Configure FireCluster in Policy Manager. You can use one of these methods:
  - *Use the FireCluster Setup Wizard*
  - *Configure FireCluster Manually*

For an active/active cluster, you must also complete these steps:

1. Make any necessary configuration changes to your layer 3 network routers and switches to support the multicast MAC addresses used by the FireCluster.

For more information, see *Switch and Router Requirements for an Active/Active FireCluster* on page 263.

2. Add static ARP entries for each of the layer 3 network routers and switches that connect to the FireCluster.

For more information, see *Add Static ARP Entries for an Active/Active FireCluster* on page 265.

## Before You Begin

Before you configure FireCluster, you must complete the tasks described in the subsequent sections.

### Verify Basic Components

Make sure that you have these items:

- Two WatchGuard XTM 5 Series, 8 Series or XTM 1050 devices of the same model
- The same version of Fireware XTM with a Pro upgrade installed on each device
- One crossover cable (red) for each cluster interface (If you configure a backup cluster interface, you must use two crossover cables.)
- One network switch for each active traffic interface
- Ethernet cables to connect the devices to the network switches
- The serial numbers for each device
- Feature keys for each device

For information about feature key requirements for FireCluster, see *About Feature Keys and FireCluster* on page 292

### Configure the External Interface with a Static IP Address

To use FireCluster, you must configure each external interface with a static IP Address. You cannot enable FireCluster if any external interface is configured to use DHCP or PPPoE.

### Configure Network Routers and Switches

In an active/active FireCluster configuration, the network interfaces for the cluster use multicast MAC addresses. Before you enable an active/active FireCluster, make sure your network routers and other devices are configured to properly route traffic to and from the multicast MAC addresses.

For more information, see *Switch and Router Requirements for an Active/Active FireCluster* on page 263.

This step is not necessary for an active/passive cluster because an active/passive cluster does not use multicast MAC addresses.

## Select IP Addresses for Cluster Interfaces

We recommend you make a table with the network addresses you plan to use for the cluster interfaces and interface for management IP address. The FireCluster setup wizard asks you to configure these individually for each cluster member. If you plan the interfaces and IP addresses in advance, it is easier to configure these interfaces with the wizard. For example, your table could look something like this:

Interface # and IP addresses for cluster interfaces			
	Interface #	IP address for Member 1	IP address for Member 2
Primary cluster interface	5	10.10.5.1/24	10.10.5.2/24
Backup cluster interface	6	10.10.6.1/24	10.10.6.2/24
Interface for management IP address	1	10.10.1.1/24	10.10.1.2/24

### *Primary cluster interface*

This is the interface on the XTM device that you dedicate to communication between the cluster members. This interface is not used for regular network traffic. If you have an interface configured as a dedicated VLAN interface, do not choose that interface as a dedicated cluster interface.

The primary interface IP addresses for both cluster members must be on the same subnet.

### *Backup cluster interface (optional, but recommended)*

This is a second interface on the XTM device that you dedicate to communication between the cluster members. The cluster members use the backup cluster interface to communicate if the primary cluster interface is not available. For redundancy, we recommend you use two cluster interfaces.

The backup interface IP addresses for both cluster members must be on the same subnet.

**Note** Each XTM device has a set of default IP addresses assigned to the device interfaces in the range 10.0.0.1 - 10.0.11.1. Do not set the Primary or Backup cluster interface to an IP address that is the same as one of the default IP addresses for the device.

### *Interface for management IP address*

This is an interface on the XTM device that you use to make a direct connection to a cluster device from any WatchGuard management application.

The management IP addresses for each cluster member must be an unused IP address on the same subnet as the address assigned to the interface configured as the *Interface for management IP address*.

For more information, see *About the Interface for Management IP Address* on page 255.

## Connect the FireCluster Hardware

**Note** *Each device in a cluster must be the same model, and must use the same version of Fireware XTM with a Pro upgrade.*

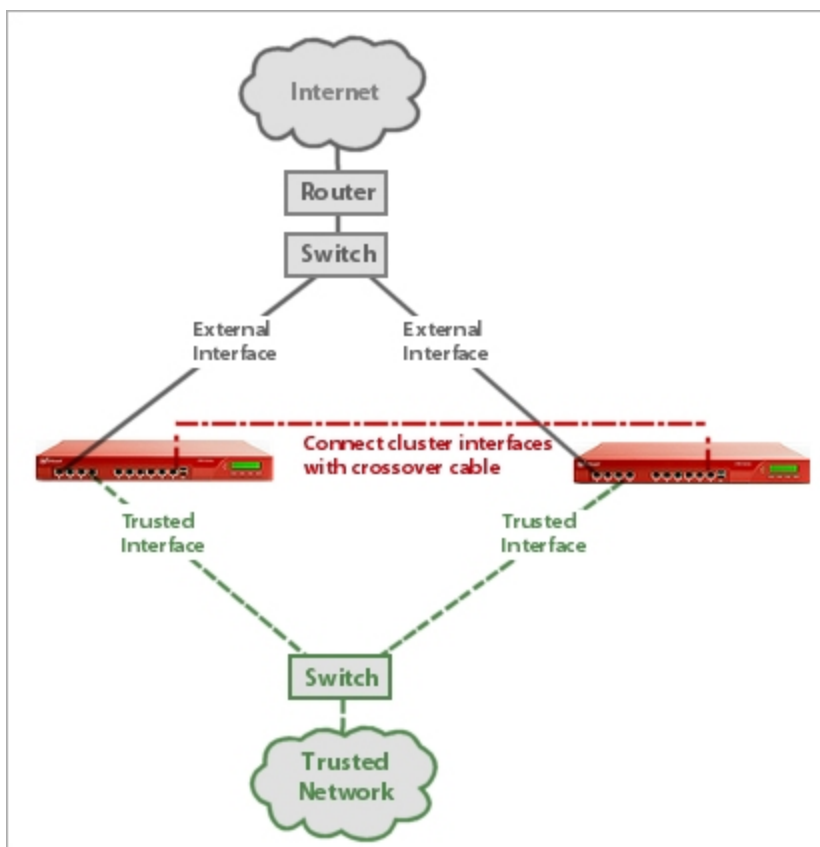
To connect two XTM devices in a FireCluster configuration:

1. Use a crossover Ethernet cable (red) to connect the primary cluster interface on one XTM device to the primary cluster interface on the other device.
2. If you want to enable a backup cluster interface, use a second crossover Ethernet cable to connect the backup cluster interfaces. If you have a network interface available, we recommend that you connect and configure a backup cluster interface for redundancy.
3. Connect the external interface of each device to a network switch. If you use Multi-WAN, connect the second external interface of each device to another network switch.
4. Connect the trusted interface of each device to an internal network switch.
5. For each device, connect the other trusted or optional network interfaces to the internal network switch for that device.

For information about network switch requirements, see *Switch and Router Requirements for an Active/Active FireCluster* on page 263.

**Note** *You must connect each pair of network interfaces to its own dedicated switch or hub. Do not connect more than one pair of interfaces to the same switch.*

The diagram below shows connections for a simple FireCluster configuration.



In this example, the FireCluster has one external and one trusted interface connected to network switches. The primary cluster interfaces are connected by a crossover cable.

After you connect the FireCluster devices, you are ready to configure the FireCluster in Policy Manager. You can do this two ways:

- Use the FireCluster Setup Wizard
- Configure FireCluster Manually

## Switch and Router Requirements for an Active/Active FireCluster

**Note** When you configure FireCluster in an active/active configuration, the cluster uses multicast MAC addresses for all interfaces that send network traffic. Before you enable FireCluster, make sure your network switches, routers, and other devices are configured to route network traffic with multicast MAC addresses.

A layer 2 *broadcast domain* is a logical part of a computer network in which all network nodes can communicate with each other without the use of a layer 3 routing device, such as a router or managed switch.

An active/active FireCluster uses a single multicast MAC address. Most network routers and managed switches ignore traffic from multicast MAC addresses by default. Before you enable an active/active FireCluster, make sure that all the network switches and routers in the layer 2 broadcast domain meet the requirements.

## Requirements for Switches and Routers

All switches and routers in an active/active FireCluster broadcast domain must meet these requirements.

1. All switches and routers in the broadcast domain must not block ARP requests if the response contains a multicast MAC address.
  - This requirement must be met for all switches and routers in the broadcast domain, even if the switch or router is not connected directly to the FireCluster devices.
  - For unmanaged layer 2 switches, this is the default behavior, and a configuration change is not required.
  - For routers and most managed switches, the default behavior is to block ARP responses that contain a multicast MAC address. Check the documentation for your managed switch or router to see if there is a configuration option to allow ARP responses that contain a multicast MAC address. In some network routers you can add the multicast MAC address as a static ARP entry. If your router supports this, add a static ARP entry to map the cluster IP address to its multicast MAC address.
  - The router must not be configured to support the multicast ARP requirement in RFC 1812, section 3.3.2.
2. The switches that you directly attach to the cluster external and internal interfaces must be configured to forward traffic to all ports when the destination MAC address is a multicast MAC address.
  - For unmanaged layer 2 switches, this is the default behavior and a configuration change is not required.
  - For routers and most managed switches, you must make a configuration change to meet this requirement. You might need to insert a static mac-address-table entry to specify the port destinations for the traffic destined for the cluster multicast MAC address.

One multicast MAC address is shared between the pair. The MAC address starts with 01:00:5E. You can find the multicast MAC addresses for a cluster in the Firebox System Manager **Status Report** tab, or in the FireCluster configuration dialog box in Policy Manager.

For more information, see *Find the Multicast MAC Addresses for an Active/Active Cluster* on page 280.

For an active/active FireCluster, you must also add static ARP entries for your layer 3 routers to the FireCluster configuration in Policy Manager.

For more information, see *Add Static ARP Entries for an Active/Active FireCluster* on page 265.

For an example of how to configure two switches for an active/active FireCluster, see *Example Switch and Static ARP Configuration for an Active/Active FireCluster* on page 265.




## Add Static ARP Entries for an Active/Active FireCluster

An active/active FireCluster uses a multicast MAC address for each active interface connected to your network. The active/active FireCluster sends this multicast MAC address across the network.

For some switches, you might need to add static ARP entries for each layer 3 network switch connected to the FireCluster traffic interface. Otherwise, network communication might not work properly. You can use Policy Manager to add the static ARP entries to the FireCluster.

To add static ARP entries to your XTM device configuration:

1. In WatchGuard System Manager, use the configured cluster interface IP address to connect to the FireCluster. Do not use the Management IP address.
2. Click .  
Or, select **Tools > Policy Manager**.  
*Policy Manager appears.*
3. Select **Network > ARP Entries**.  
*The Static ARP Entries dialog box appears.*
4. Click **Add**.  
*The Add ARP Entry dialog box appears.*
5. In the **Interface** drop-down list, select the interface for the layer 3 switch.
6. In the **IP Address** text box, type the IP address of the network switch.
7. In the **MAC Address** text box, type the MAC address of the switch. Click **OK**.  
*The static ARP entry is added to the Static ARP Entries list.*
8. Repeat Steps 4–7 to add static ARP entries for each switch that is directly connected to each interface of the FireCluster.
9. Click **OK**.
10. Select **File > Save > to Firebox** to save the static ARP entries to the FireCluster.

You must also configure the network switches to work with the active/active FireCluster. For more information, see *Switch and Router Requirements for an Active/Active FireCluster* on page 263.

For an example of how to configure two switches for an active/active FireCluster, see *Example Switch and Static ARP Configuration for an Active/Active FireCluster* on page 265.

## Example Switch and Static ARP Configuration for an Active/Active FireCluster

Layer 3 switches that operate in default mode do not have issues with multicast traffic, so the FireCluster works without configuration changes. A layer 3 switch that has all ports configured in one VLAN also works without issues. If the layer 3 switch has ports configured for different VLANs you must change the configuration to enable the switch to operate correctly with a FireCluster.

Layer 3 switches that perform VLAN, and/or IP address routing, discard multicast traffic from the FireCluster members. The switch discards traffic to and through the router unless you configure static MAC and ARP entries for the FireCluster multicast MAC on the switch that receives the multicast traffic.

When you configure an active/active FireCluster, you might need to make some configuration changes on the FireCluster and on your network switches so that the FireCluster multicast MAC addresses work properly. For general information, see:

- *Switch and Router Requirements for an Active/Active FireCluster*
- *Add Static ARP Entries for an Active/Active FireCluster*

This topic includes an example of how to configure the switches and the FireCluster static ARP settings for an active/active FireCluster. This example does not include all the other steps to configure a FireCluster. For instructions to configure a FireCluster, see *Configure FireCluster* on page 257.

Before you begin, make sure you have:

- The IP address and multicast MAC address of the FireCluster interface to which the switch is connected.  
For more information, see *Find the Multicast MAC Addresses for an Active/Active Cluster* on page 280.
- The IP address and MAC address of each switch or router connected to the FireCluster interfaces.

**Note** *WatchGuard provides interoperability instructions to help our customers configure WatchGuard products to work with products created by other organizations. If you need more information or technical support about how to configure a non-WatchGuard product, see the documentation and support resources for that product.*

## Example Configuration

In this example, the FireCluster configuration has one external and one internal interface. The external interface of each cluster member is connected to a Cisco 3750 switch. The internal interface of each cluster member is connected to an Extreme Summit 15040 switch. For the equivalent commands to make these configuration changes on your switch, see the documentation for your switch. The commands for two different switches are included in this example.

IP addresses in this example:

- **FireCluster interface 0 (External) interface**  
IP address: 50.50.50.50/24  
Multicast MAC address: 01:00:5e:32:32:32
- **FireCluster interface 1 (Trusted) interface**  
IP address: 10.0.1.1/24  
Multicast MAC address: 01:00:5e:00:01:01
- **Cisco 3750 switch connected to the FireCluster external interface**  
IP address: 50.50.50.100  
VLAN interface MAC address: 00:10:20:3f:48:10  
VLAN ID: 1  
Interface: gi1/0/11

- **Extreme Summit 48i switch connected to the FireCluster internal interface**

IP address: 10.0.1.100

MAC address: 00:01:30:f3:f1:40

VLAN ID: Border-100

Interface: 9

## Configure the Cisco Switch

In this example, the Cisco switch is connected to the FireCluster interface 0 (external). You must use the Cisco command line to add static MAC and ARP entries for the multicast MAC address of the external FireCluster interface.

1. Start the Cisco 3750 command line interface.
2. Add a static ARP entry for the multicast MAC address of the FireCluster interface.  
Type this command:  
`arp <FireCluster interface IP address> <FireCluster MAC address> arpa`  
For this example, type:  
`arp 50.50.50.50 0100.5e32.3232 arpa`
3. Add an entry to the MAC address table.  
Type this command:  
`mac-address-table static <FireCluster interface MAC address> vlan <ID>  
interface <#>`  
For this example, type:  
`mac-address-table static 0100.5e32.3232 vlan 1 interface gi1/0/11`


## Configure the Extreme Switch

In this example, the Extreme Summit switch is connected to the FireCluster interface 1 (trusted). You must use the Extreme Summit command line to add static MAC and ARP entries for the multicast MAC address of the trusted FireCluster interface.

1. Start the Extreme Summit 48i command line.
2. Add a static ARP entry for the multicast MAC address of the FireCluster interface.  
Type this command:  
`configured iparp add <ip address> <MAC Address>`  
For this example, type:  
`configured iparp add 10.0.1.1/24 01:00:5e:00:01:01`
3. Add an entry to the MAC address table.  
Type this command:  
`create fdbentry <MAC> VLAN <ID> port <#>`  
For this example, type:  
`create fdbentry 01:00:5e:00:01:01 VLAN Border-100 port 9`

## Add Static ARP Entries to the FireCluster Configuration for Each Switch

For an explanation of why this is required, see *Add Static ARP Entries for an Active/Active FireCluster* on page 265.

1. In WatchGuard System Manager, use the cluster trusted interface IP address to connect to the FireCluster. Do not use the management IP address.
2. Click .  
Or, select **Tools > Policy Manager**.  
*Policy Manager appears.*
3. Select **Network > ARP Entries**.  
*The Static ARP Entries dialog box appears.*
4. Click **Add**.  
*The Add ARP Entry dialog box appears.*
5. In the **Interface** drop-down list, select **External**.
6. In the **IP Address** text box, type the IP address of the switch interface that is connected to the external interface.  
For this example, type: 50.50.50.100
7. In the **MAC Address** text box, type the MAC address of the VLAN interface on the Cisco switch that is connected to the external interface.  
For this example, type: 00:10:20:3f:48:10
8. Click **OK**.  
*The static ARP entry is added to the Static ARP Entries list.*
9. Click **Add**.  
*The Add ARP Entry dialog box appears.*
10. In the **Interface** drop-down list, select **Trusted**.
11. In the **IP Address** text box, type the IP address of the switch interface that is connected to the trusted interface.  
For this example, type: 10.0.1.100
12. In the **MAC Address** text box, type the MAC address of the switch interface that is connected to the trusted interface.  
For this example, type: 00:01:30:f3:f1:40
13. Click **OK**.  
*The static ARP entry is added to the Static ARP Entries list.*
14. Click **OK** to close the **Static ARP Entries** dialog box.
15. Select **File > Save > to Firebox** to save the static ARP entries to the FireCluster.

## Use the FireCluster Setup Wizard

To configure FireCluster, you can either run the FireCluster Setup Wizard or you can configure FireCluster manually.


For more information about how to configure FireCluster manually, see *Configure FireCluster Manually* on page 274 .

Before you enable FireCluster:

- Make sure you have everything necessary to configure your FireCluster, and have planned your configuration settings.  
For information, see *Before You Begin* on page 260.
- Connect the FireCluster devices to each other and to the network as described in *Connect the FireCluster Hardware* on page 262.

**Note** *In an active/active FireCluster configuration, the network interfaces for the cluster use multicast MAC addresses. Before you enable an active/active FireCluster, make sure your network routers and other devices are configured to support multicast network traffic. For more information, see *Switch and Router Requirements for an Active/Active FireCluster* on page 263.*

## Configure FireCluster

1. In WatchGuard System Manager, connect to the XTM device that has the configuration you want to use for the cluster. After you enable FireCluster, this device becomes the cluster master the first time you save the configuration.
2. Click .  
Or, select **Tools > Policy Manager**.  
*Policy Manager opens the configuration file for the selected device.*
3. Select **FireCluster > Setup**.  
*The FireCluster Setup Wizard starts.*



4. Click **Next**.
5. Select the type of cluster you want to enable:

#### *Active/Passive cluster*

Enables the cluster for high availability, but not load sharing. If you select this option, the cluster has an active device that handles all the connections, and a passive device that handles connections only if a failover of the first device occurs.

#### *Active/Active cluster*

Enables the cluster for high availability and load sharing. If you select this option, the cluster balances incoming connection requests across both devices in the cluster.

You cannot configure an active/active cluster if:

- The external interface of your XTM device is configured for DHCP or PPPoE
- The XTM device is configured to use dynamic routing
- The XTM device is configured in drop-in network mode

6. Select the **Cluster ID**.

The cluster ID uniquely identifies this cluster if you set up more than one cluster on the same layer 2 broadcast domain. If you only have one cluster, you can keep the default value of 1.

7. If you selected **Active/Active cluster**, select the **Load-balance method**.

The load-balance method is the method used to balance connections among active cluster members. There are two options:

#### *Least connection*

If you select this option, each new connection is assigned to the active cluster member with the lowest number of open connections. This is the default setting.

### *Round-robin*

If you select this option, new connections are distributed among the active cluster members in round-robin order. The first connection goes to one cluster member. The next connection goes to the other cluster member, and so on.

8. Select the **Primary** and **Backup** cluster interfaces. The cluster interfaces are dedicated to communication between cluster members and are not used for other network traffic. You must configure the **Primary** interface. For redundancy, we recommend you also configure the **Backup** interface.

### *Primary*

The XTM device interface that you dedicate to primary communication between the cluster members. Select the interface number that you used to connect the FireCluster devices to each other.

### *Backup*

The XTM device interface that you dedicate to communication between the cluster members if the primary interface fails. Select the second interface number that you used to connect the FireCluster devices to each other, if any.

**Note** *If you have an interface configured as a dedicated VLAN interface, do not choose that interface as a dedicated cluster interface.*

9. Select the **Interface for Management IP address**. You use this interface to connect directly to FireCluster member devices for maintenance operations. This is not a dedicated interface. It also is used for other network traffic. You cannot select a VLAN interface as the Interface for Management IP address.  
For more information, see *About the Interface for Management IP Address* on page 255.
10. When prompted by the configuration wizard, add these FireCluster member properties for each device:

### *Feature Key*

For each device, import or download the feature key to enable all features for the device. If you previously imported the feature key in Policy Manager, the wizard automatically uses that feature key for the first device in the cluster.

### *Member Name*

The name that identifies each device in the FireCluster configuration.

### *Serial Number*

The serial number of the device. The serial number is used as the Member ID in the **FireCluster Configuration** dialog box. The wizard sets this automatically when you import or download the feature key for the device.

### Primary cluster interface IP address

The IP address the cluster members use to communicate with each other over the primary cluster interface. The primary FireCluster IP address for each cluster member must be on the same subnet.

If both devices start at the same time, the cluster member with the highest IP address assigned to the primary cluster interface becomes the master.

### Backup cluster interface IP address

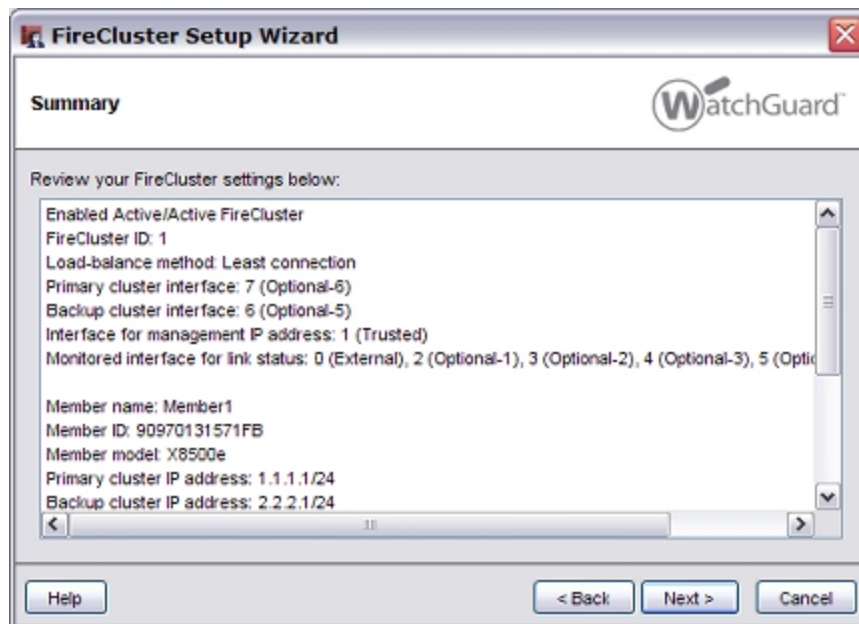
The IP address the cluster members use to communicate with each other over the backup cluster interface. The backup FireCluster IP address for each cluster member must be on the same subnet.

**Note** Do not set the Primary or Backup cluster IP address to the default IP address of any interface on the device. The default interface IP addresses are in the range 10.0.0.1–10.0.13.1.

### Management IP address

A unique IP address that you can use to connect to an individual XTM device while it is configured as part of a cluster. You must specify a different management IP address for each cluster member. The management IP address must be an unused IP address on the same subnet as the address assigned to the interface you selected as the *Interface for management IP address*.

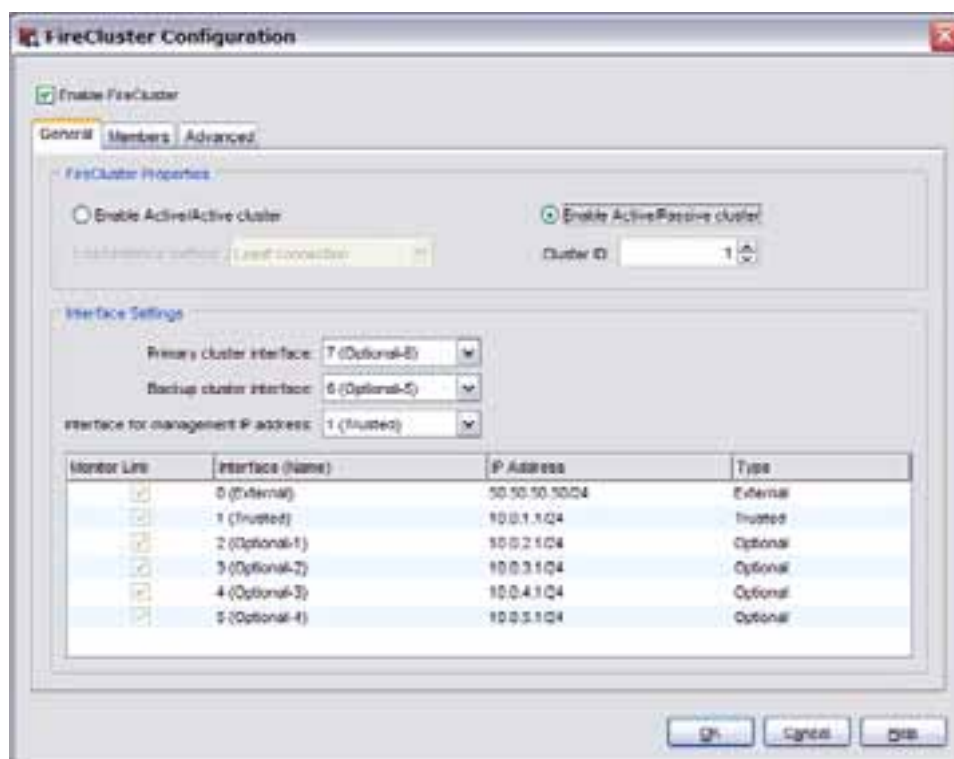
11. Review the configuration summary on the final screen of the FireCluster Setup Wizard. The configuration summary includes the options you selected and which interfaces are monitored for link status.





12. Click **Finish**.

The *FireCluster Configuration* dialog box appears.



13. In the **Interface Settings** section, review the list of monitored interfaces.

The list of monitored interfaces does not include the interfaces you configured as the Primary and Backup cluster interfaces. FireCluster monitors the link status for all enabled interfaces. If the cluster master detects loss of link on a monitored interface, the cluster master starts failover for that device.

You must disable any interfaces that are not connected to your network before you save the FireCluster configuration to the XTM device. To disable an interface:

- In Policy Manager, select **Network > Configuration**.
- Double-click the interface that you want to disable, and set the **Interface Type** to **Disabled**.

**Note** Do not save the configuration file until you start the second device in safe mode.

14. Start the second XTM device in safe mode.

To start in safe mode, press and hold the down arrow on the device front panel while you power on the device.

Hold down the arrow button until WatchGuard Technologies appears on the LCD display. When the device is in safe mode, the model number followed by the word safe appears on the LCD display.

15. Save the configuration to the cluster master.

The cluster is activated, and the cluster master automatically discovers the other configured cluster member.

After the cluster is active, you can monitor the status of the cluster members on the Firebox System Manager **Front Panel** tab.

For more information, see *Monitor and Control FireCluster Members* on page 282.

If the second device is not automatically discovered, you can manually trigger device discovery as described in *Discover a Cluster Member* on page 284.

## Configure FireCluster Manually


You can enable FireCluster manually or use the FireCluster Setup Wizard. For more information, see *Use the FireCluster Setup Wizard* on page 269 .

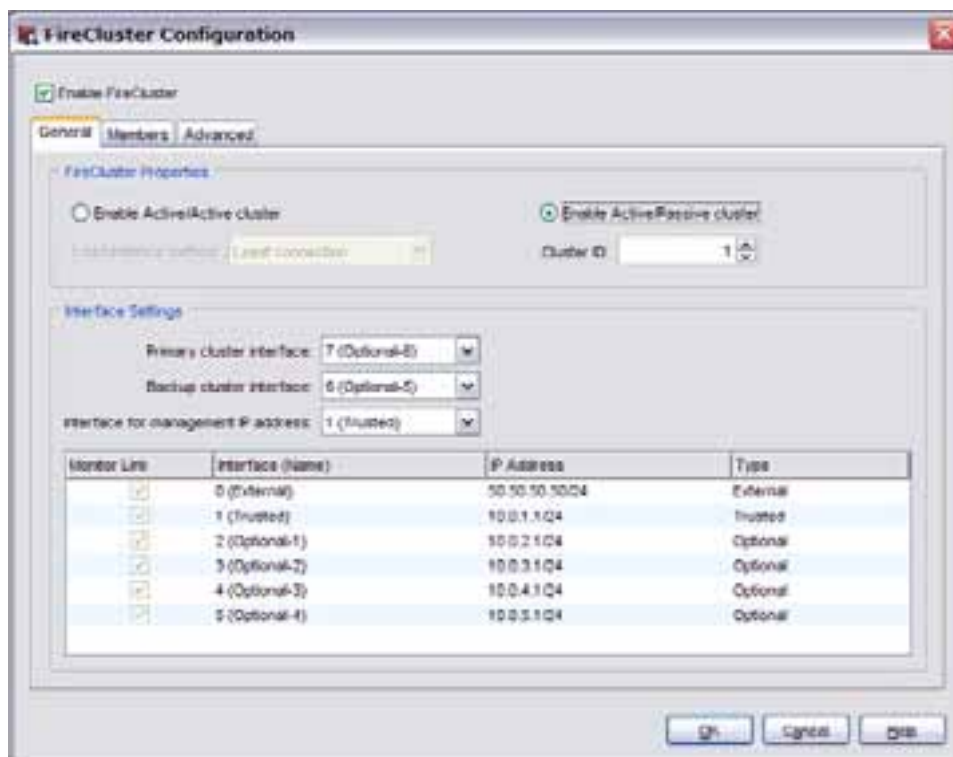
Before you enable FireCluster:

- Make sure you have everything necessary to configure your FireCluster, and have planned your configuration settings.  
For more information, see *Before You Begin* on page 260.
- Connect the FireCluster devices to each other and to the network as described in *Connect the FireCluster Hardware* on page 262.

**Warning** *In an active/active FireCluster configuration, the network interfaces for the cluster use multicast MAC addresses. Before you enable an active/active FireCluster, make sure your network routers and other devices are configured to support multicast network traffic. For more information, see *Switch and Router Requirements for an Active/Active FireCluster* on page 263.*

## Enable FireCluster

1. In WatchGuard System Manager, connect to the XTM device that has the configuration you want to use for the cluster. This device becomes the cluster master the first time you save the configuration with FireCluster enabled.
2. Click .  
Or, select **Tools > Policy Manager**.  
*Policy Manager appears.*
3. Select **FireCluster > Configure**.  
*The FireCluster Cluster Configuration dialog box appears.*



4. Select the **Enable FireCluster** check box.
5. Select which type of cluster you want to enable.

#### *Enable Active/Passive cluster*

Enables the cluster for high availability, but not load sharing. If you select this option, the cluster has an active device that handles all the network traffic, and a passive device that handles traffic only if a failover of the first device occurs.

#### *Enable Active/Active cluster*

Enables the cluster for high availability and load sharing. If you select this option, the cluster balances traffic load across both devices in the cluster.

You cannot configure an active/active cluster if:

- The external interface of your XTM device is configured for DHCP or PPPoE
- The XTM device is configured to use dynamic routing
- The XTM device is configured in drop-in network mode

6. If you selected **Enable Active/Active cluster**, in the **Load-balance method** drop-down list, select the method to use to balance the traffic load between active cluster members.

#### *Least connection*

If you select this option, each new connection is assigned to the active cluster member that has the lowest number of open connections.

#### *Round-robin*

If you select this option, connections are distributed among the active cluster members in round-robin order. The first connection goes to one cluster member. The next connection goes to the other cluster member, and so on.

7. In the **Cluster ID** drop-down list, select a number to identify this FireCluster.

The cluster ID uniquely identifies this FireCluster if there is more than one FireCluster active on the same network segment. If you only have one FireCluster, you can keep the default value of 1.

## Configure Interface Settings

The FireCluster interface is the dedicated interface the cluster members use to communicate with each other about system status. You can configure either one or two FireCluster interfaces. For redundancy, if you have the interfaces available, we recommend you configure two FireCluster interfaces. If you have an interface configured as a dedicated VLAN interface, do not choose that interface as a dedicated FireCluster interface. You must disable any interfaces that are not connected to your network before you save the FireCluster configuration to the XTM device.

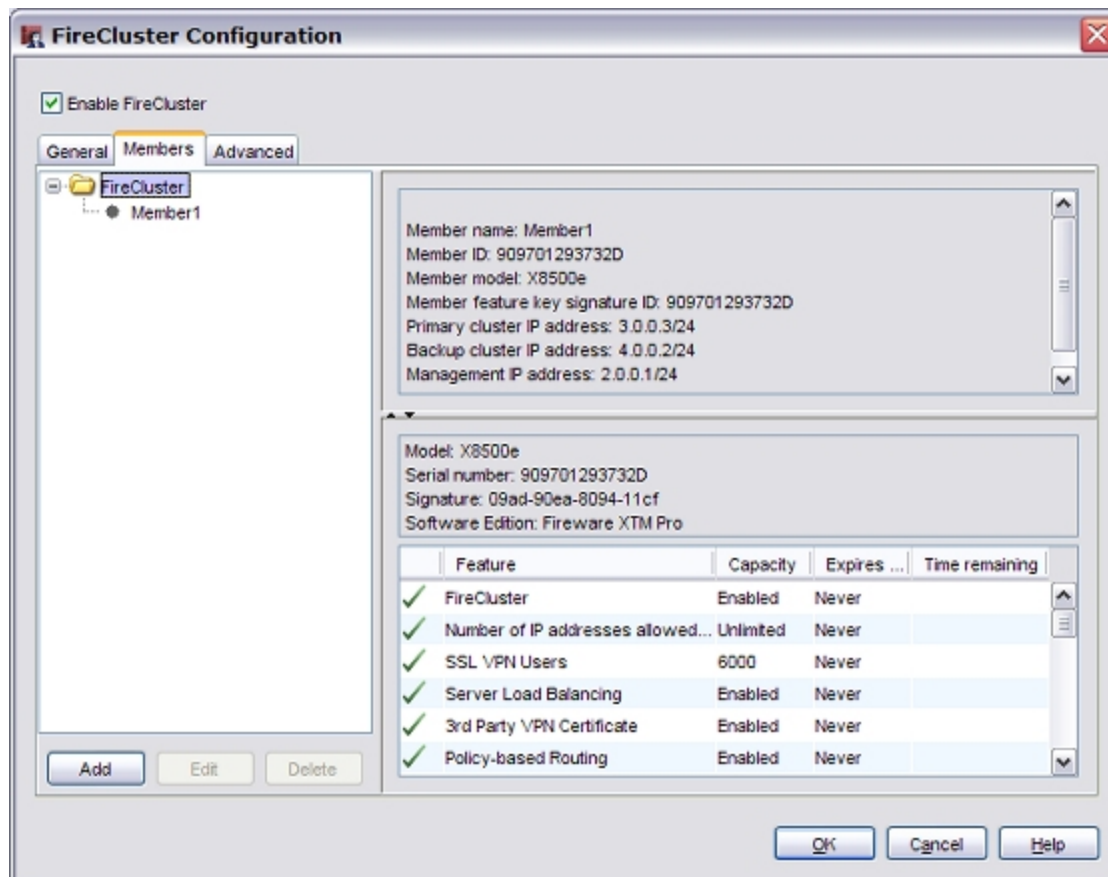
1. In the **Primary cluster interface** drop-down list, select an interface to use as the primary interface.
2. To use a second cluster interface, in the **Backup cluster interface** drop-down list, select an interface to use as the backup interface.
3. Select an **Interface for management IP address**. This is the XTM device network interface you use to make a direct connection to a cluster device with any WatchGuard management application. You cannot select a VLAN interface as the Interface for Management IP address.  
For more information, see *About the Interface for Management IP Address* on page 255.
4. Review the list of monitored interfaces. The list of monitored interfaces does not include the interfaces you configured as the Primary and Backup FireCluster interfaces. FireCluster monitors the link status for all enabled interfaces. If the cluster master detects a loss of link on a monitored interface, the cluster master starts failover for that device.
5. To disable an interface, in Policy Manager, select **Network > Configuration**.
6. Double-click the interface that you want to disable.
7. Set the **Interface Type** to **Disabled**.

**Note** *FireCluster monitors the status of all enabled network interfaces. Make sure that all interfaces in the list of monitored interfaces are connected to a network switch.*

## Define the FireCluster Members

1. Select the **Members** tab.

*The FireCluster members configuration settings appear.*

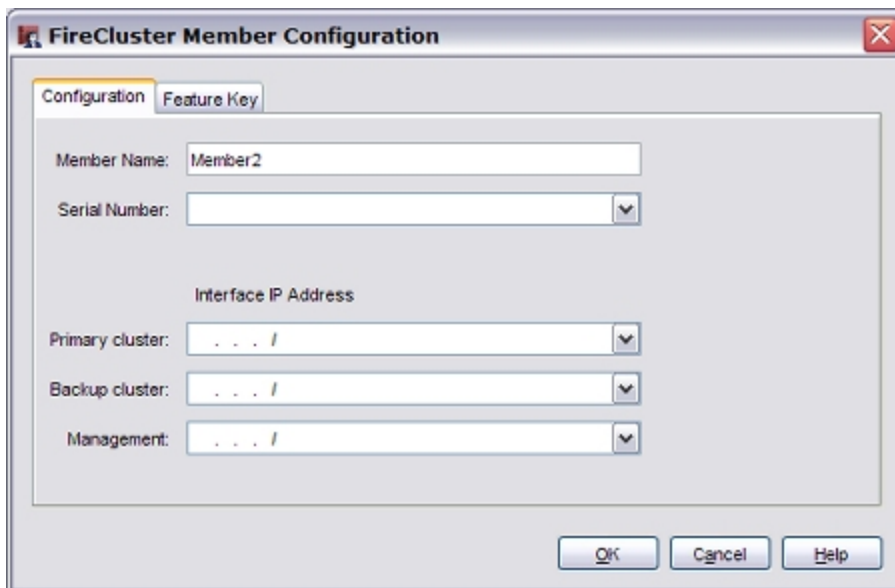


If you previously imported a feature key in this configuration file, that device is automatically configured as Member 1.

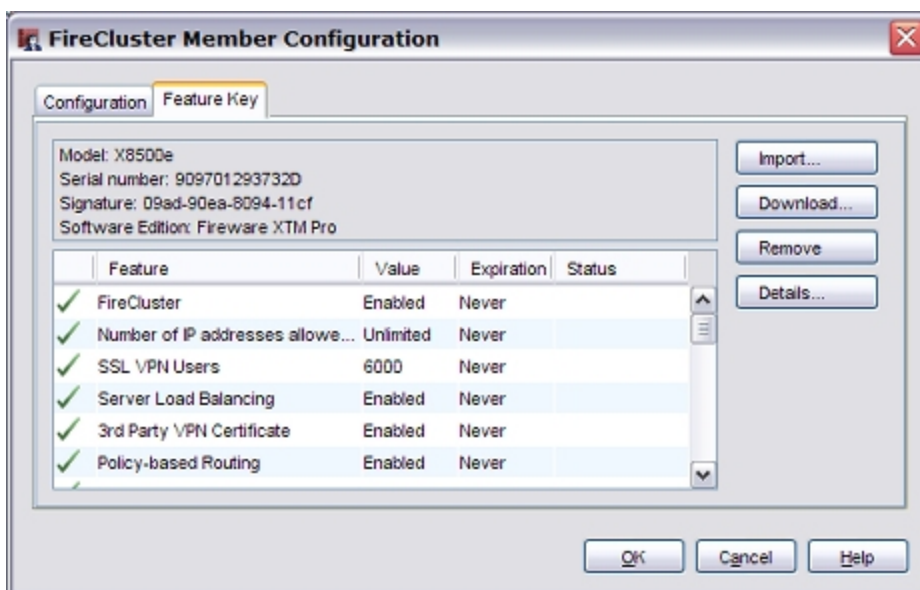
If you do not have a feature key in this configuration file, a FireCluster member does not appear in the list. In this case, you must add each device as a member, and import the configuration file for each device as described in the subsequent steps.

2. To add a member, click **Add**.

*The Add member dialog appears.*



3. In the **Member Name** text box, type a name. This name identifies this device in the members list.
4. Select the **Feature Key** tab.



5. Click **Import**.  
*The Import Firebox Feature Key dialog box appears.*
6. To find the feature key file, click **Browse**.  
Or, copy the text of the feature key file and click **Paste** to insert it in the dialog box.
7. Click **OK**.
8. Select the **Configuration** tab.  
*The Serial Number field is automatically filled with the serial number from the feature key.*

9. In the **Interface IP Address** section, type the addresses to use for each cluster interface and the interface for management IP address.
  - In the **Primary cluster** text box, type the IP address to use for the primary cluster interface. The IP address for the primary cluster interface must be on the same subnet for each cluster member. The cluster member that has the highest IP address assigned to the primary cluster interface becomes the master if both devices start at the same time.
  - In the **Backup cluster** text box, type the IP address to use for the backup cluster interface. This option only appears if you configured a backup cluster interface. The IP address for the backup cluster interface must be on the same subnet for each cluster member.
  - In the **Management** text box, type the IP address to use to connect to an individual cluster member for maintenance operations. The interface for management is not a dedicated interface. It also is used for other network traffic. You must specify a different management IP address for each cluster member. The management IP address must be an unused IP address on the same subnet as the address assigned to the interface.  
For more information, see *About the Interface for Management IP Address* on page 255.

**Note** Do not set the Primary or Backup cluster IP address to the default IP address of any interface on the device. The default interface IP addresses are in the range 10.0.0.1 - 10.0.13.1.

10. Click **OK**.  
*The device you added appears on the Members tab as a cluster member.*
11. Repeat the previous steps to add the second XTM device to the cluster configuration.

**Note** Do not save the configuration to the XTM device until you start the second device in safe mode.

12. Start the second XTM device in safe mode.

To start in safe mode, press and hold the down arrow on the device front panel while you power on the device. Hold down the down arrow until *Safe Mode Starting...* appears on the LCD display. When the device is in safe mode, the model number followed by the word *safe* appears on the LCD display.

13. Save the configuration file to the XTM device.  
*The cluster is activated. The cluster master automatically discovers the other configured cluster member and synchronizes the configuration.*

After the cluster is active, you can monitor the status of the cluster members on the Firebox System Manager **Front Panel** tab.

For more information, see *Monitor and Control FireCluster Members* on page 282.

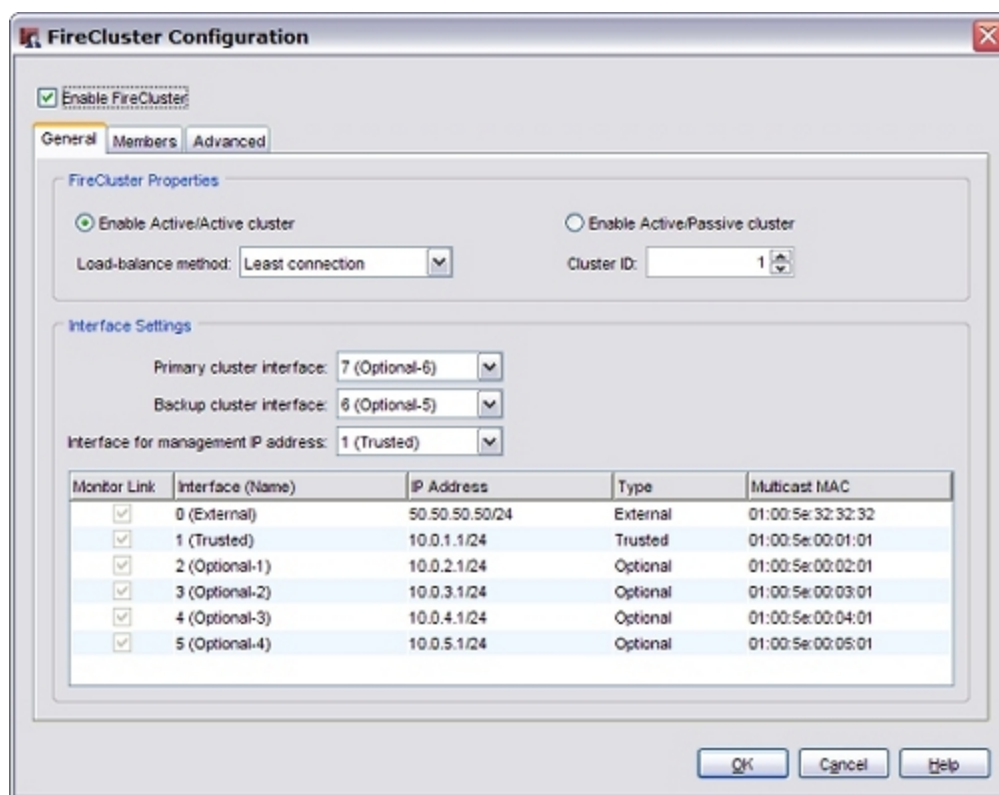
If the second device is not automatically discovered, you can manually trigger device discovery as described in *Discover a Cluster Member* on page 284.

## Find the Multicast MAC Addresses for an Active/Active Cluster

To configure your switch to support the FireCluster multicast MAC addresses, you might need to know the multicast MAC addresses the cluster uses for each interface. There are two ways to find the MAC addresses assigned to the interfaces.

### Find the MAC Addresses in Policy Manager

1. Open Policy Manager for the active/active FireCluster.
2. Select **FireCluster > Configure**.  
*The FireCluster Configuration dialog box appears.*
3. In the **Interface Settings** section, find the multicast MAC address for each interface.



To copy a multicast MAC address from the FireCluster configuration to your switch or router configuration:

1. In the **Multicast MAC** column, double-click the MAC address.  
*The MAC address appears highlighted.*
  2. Click and drag to highlight the MAC address.
  3. Press **Ctrl+C** on your keyboard to copy it to the clipboard
  4. Paste the MAC address in your switch or router configuration.
- For more information, see *Switch and Router Requirements for an Active/Active FireCluster* on page 263.

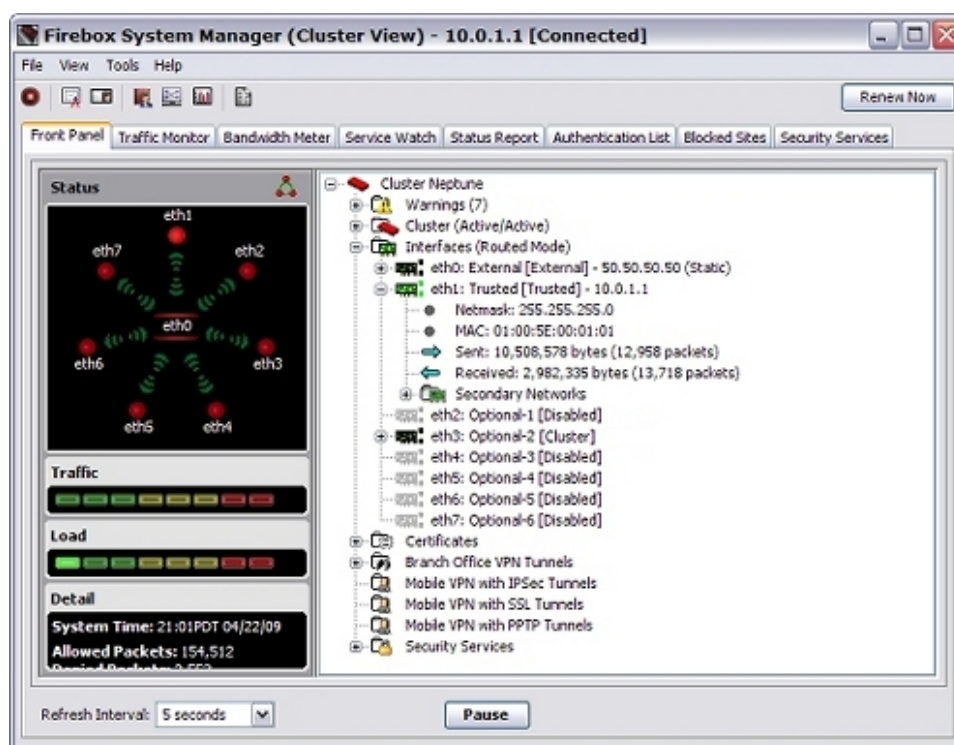


## Find the MAC Address in Firebox System Manager

You can also find the multicast MAC addresses in Firebox System Manager.

1. Open Firebox System Manager.
2. Select the **Front Panel** tab.
3. Expand **Interfaces**.

*The multicast MAC address is included with each interface in the cluster.*



## Active/Passive Cluster ID and the Virtual MAC Address

An active/passive FireCluster uses a virtual MAC address, calculated based on the Cluster ID and the interface numbers. If you configure more than one active/passive FireCluster on the same subnet, it is important to know how to set the Cluster ID to avoid a possible virtual MAC address conflict.

### How the Virtual MAC Address is Calculated

The virtual MAC addresses for interfaces on an active/passive FireCluster start with 00:00:5E:00:01. The sixth octet of the MAC address is set to a value that is equal to the interface number plus the Cluster ID.

For example, for a FireCluster with the Cluster ID set to 1, the virtual MAC addresses are:

Interface 0: 00:00:5E:00:01:01

Interface 1: 00:00:5E:00:01:02

Interface 2: 00:00:5E:00:01:03

If you add a second FireCluster to the same subnet, you must make sure to set the Cluster ID to a number that is different enough from the Cluster ID of the first FireCluster to avoid a virtual MAC address conflict. For example, if the first FireCluster has 5 interfaces, you must set the Cluster ID of the second FireCluster at least 5 higher than the Cluster ID for the first FireCluster.

For example, if the second FireCluster has the Cluster ID set to 6, the virtual MAC addresses are:

Interface 0: 00:00:5E:00:01:06


Interface 1: 00:00:5E:00:01:07

Interface 2: 00:00:5E:00:01:08

## Monitor and Control FireCluster Members

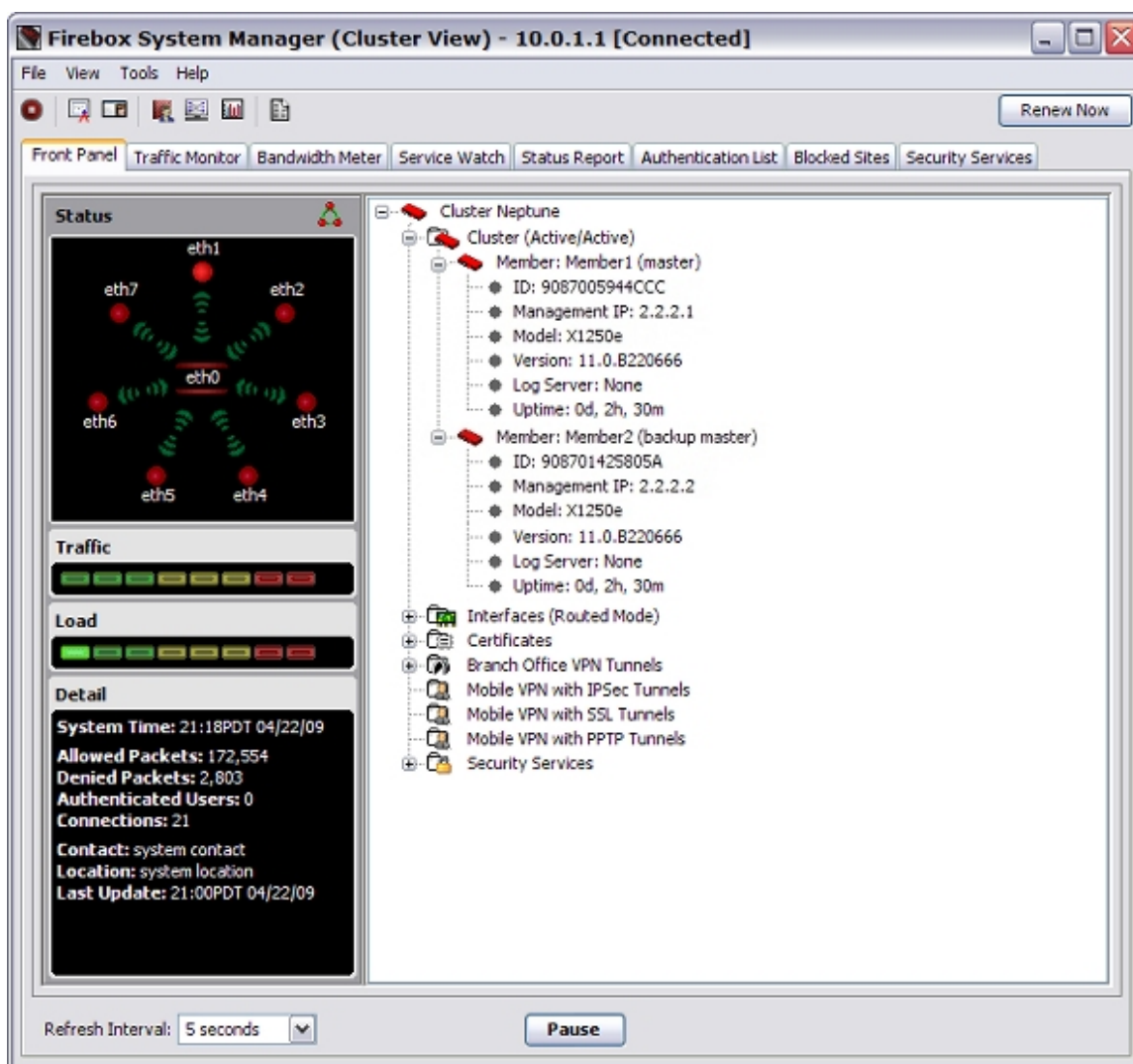
Use the IP address of the trusted interface to monitor and manage the cluster. When you monitor the cluster in Firebox System Manager, you see an aggregated view of the devices in the cluster. In FSM, you view the status of the cluster members as if the cluster were one device.

To monitor a cluster:

1. In Policy Manager, connect to the trusted IP address of the cluster.
2. Click .

*Firebox System Manager appears.*

When you connect to the trusted IP address of the cluster in Firebox System Manager, the clustered devices appear on the **Front Panel** tab. The other tabs include information that is combined for all devices in the cluster.



## Monitor Status of FireCluster Members

When you monitor a FireCluster, the Firebox System Manager tabs include information about all devices in the cluster. On the **Front Panel** tab, you can expand the cluster to view the status of each member. This shows which device is the master, and the status of each device in the cluster. The other tabs include information that is combined for all devices in the cluster.

**Note** You can also use the interface for management IP address to connect to and monitor an individual cluster member. When you monitor only one cluster member, you do not see all the information about the cluster. For more information, see *About the Interface for Management IP Address* on page 255.

## Monitor and Control Cluster Members

You can also use Firebox System Manager to monitor and control individual cluster members. Although FireCluster operations usually occur automatically, you can manually complete some of the functions in Firebox System Manager.

To control cluster members:

1. Select **Tools > Cluster**.
2. Select an option:
  - *Discover a Cluster Member*
  - *Force a Failover of the Cluster Master*
  - *Reboot a Cluster Member*
  - *Shut Down a Cluster Member*
  - *Connect to a Cluster Member*
  - *Make a Member Leave a Cluster*
  - *Make a Member Join a Cluster*

## Discover a Cluster Member

When you add a device to a FireCluster, the cluster master automatically discovers the device. You can also use the *Discover member* command to trigger the cluster master to discover a device. This can be a new device or an existing cluster member.

Before you begin, make sure that the device is:

- Connected to the network correctly, as described in *Connect the FireCluster Hardware* on page 262
- Configured as a cluster member in the cluster configuration. Use one of these methods:
  - *Use the FireCluster Setup Wizard*
  - *Configure FireCluster Manually*

To trigger the cluster master to discover a device:

1. If this is a new device for this cluster, start the new device in safe mode.  
For more information, see the subsequent section.
2. In WatchGuard System Manager, connect to the cluster master.
3. *Start Firebox System Manager.*
4. Select **Tools > Cluster > Discover member**.  
*The Discover member dialog box appears.*



5. Type the configuration passphrase for the cluster.  
*A message appears to tell you the discovery process has started.*

6. Click **OK**.

*The cluster master tries to discover new devices connected to the cluster.*

When the cluster master discovers a connected device, it checks the serial number of the device. If the serial number matches the serial number of a cluster member in the FireCluster configuration, the cluster master loads the cluster configuration on the second device. That device then becomes active in the cluster. The second device synchronizes all cluster status with the cluster master.

After discovery and the initial synchronization is complete, the device appears on the Firebox System Manager **Front Panel** tab as a member of the cluster.

## Start Your Device in Safe Mode

1. Press and hold the down arrow on the device front panel while you power on the device.
2. Hold down the down arrow until **Safe Mode Starting...** appears on the LCD display.
3. Release the down arrow.

*When the device is in safe mode, the model number followed by the word **safe** appears on the LCD display.*

## Force a Failover of the Cluster Master

You can use the Firebox System Manager **Failover Master** command to force the cluster master to fail over. The backup master becomes the cluster master, and the original master device becomes the backup master.

1. Select **Tools > Cluster > Failover master**.

*The Failover Master dialog box appears.*



2. Type the configuration passphrase.
3. Click **OK**.

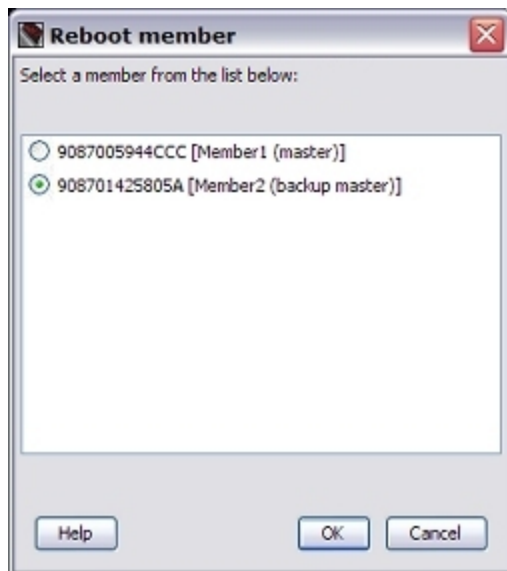
*The cluster master fails over to the backup master, and the backup master becomes the master.*

## Reboot a Cluster Member

You can use the **Reboot member** command in Firebox System Manager to reboot a cluster member. This is equivalent to the **File > Reboot** command that you use to reboot a non-clustered device.

1. Select **Tools > Cluster > Reboot member**.

*The Reboot member dialog box appears.*



2. Select the cluster member you want to reboot.
3. Type the configuration passphrase.
4. Click **OK**.

*The cluster member reboots, and then rejoins the cluster.*

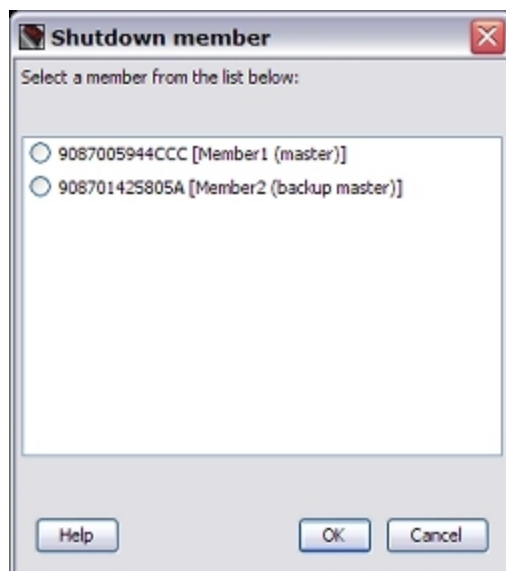
If you reboot the cluster master, this triggers failover. The backup master becomes the master. After the reboot is complete, the original master rejoins the cluster as the backup master.

## Shut Down a Cluster Member

You can use the **Shutdown member** command in Firebox System Manager to shut down a member of a cluster. This is equivalent to the **File > Shutdown** command that you use to shut down a non-clustered device.

1. Select **Tools > Cluster > Shutdown member**.

*The Shutdown member dialog box appears.*



2. Select the cluster member you want to shut down.
3. Type the configuration passphrase.
4. Click **OK**.

*The cluster member shuts down. Any traffic handled by that cluster member shifts to the other cluster member.*

When you shut down a cluster member, the LCD, the serial port, and all interfaces of the device are shut down. The power indicator changes to orange, and the fans continue to run, but you cannot communicate with the device. To restart the device after a shut down, you must press the power button to power off the device. Then press the power button again to power on the device and restart it.

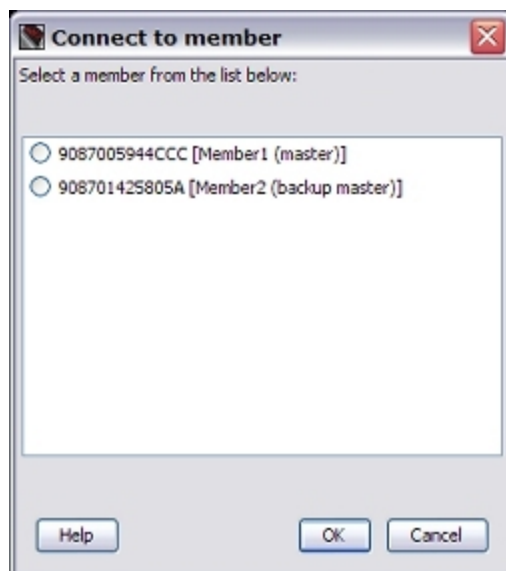
## Connect to a Cluster Member

When you connect to a FireCluster with WatchGuard System Manager, the available information is combined for all members of the cluster. To monitor an individual cluster member, you can connect to the cluster member with Firebox System Manager (FSM). FSM has two available methods to connect to a cluster member: the FSM main menu or the right-click menu.

To use the main menu:

1. Select **Tools > Cluster > Connect to member**.

*The Connect to member dialog appears.*



2. Select the cluster member to which you want to connect.
3. Click **OK**.

*Another Firebox System Manager window opens for the selected cluster member.*

To use the right-click menu:

1. On the **Front Panel** tab, select a cluster member.
2. Right-click the device and select **Connect to Member**.

## Make a Member Leave a Cluster

If you use the FireCluster management IP address to connect to the cluster member, the **Leave** command is available in Firebox System Manager. The **Leave** command is part of the procedure to restore a FireCluster backup image.

When a member leaves the cluster, it is still part of the cluster configuration, but does not participate in the cluster. The other cluster member handles all traffic in the cluster after the second member has left.

To make a member leave the cluster:

1. In WatchGuard System Manager, use the FireCluster Management IP address to connect to the backup master.
2. Start Firebox System Manager for the backup master.
3. Select **Tools > Cluster > Leave**.

*The backup master leaves the cluster and reboots.*

For information about the Management IP address, see *About the Interface for Management IP Address* on page 255.

For information about how to restore a backup image to members of a cluster, see *Restore a FireCluster Backup Image* on page 298.



## Make a Member Join a Cluster

The **Join** command is only available in Firebox System Manager if you connect to a cluster member with the interface for management IP address, and if you previously used the **Leave** command to make the member leave the cluster. The **Leave** and **Join** commands are part of the procedure to restore a FireCluster backup image.

1. In WatchGuard System Manager, use the FireCluster management IP address to connect to the backup master.  
If the backup image you restored has a different Management IP address for this cluster member or a different passphrase, use the Management IP and passphrase from the backup image to reconnect to the device in WSM.
2. Start Firebox System Manager for the backup master.
3. Select **Tools > Cluster > Join**.  
*The backup master reboots and rejoins the cluster.*

For information about the Management IP address, see *About the Interface for Management IP Address* on page 255.


For information about how to restore a backup image to members of a cluster, see *Restore a FireCluster Backup Image* on page 298.

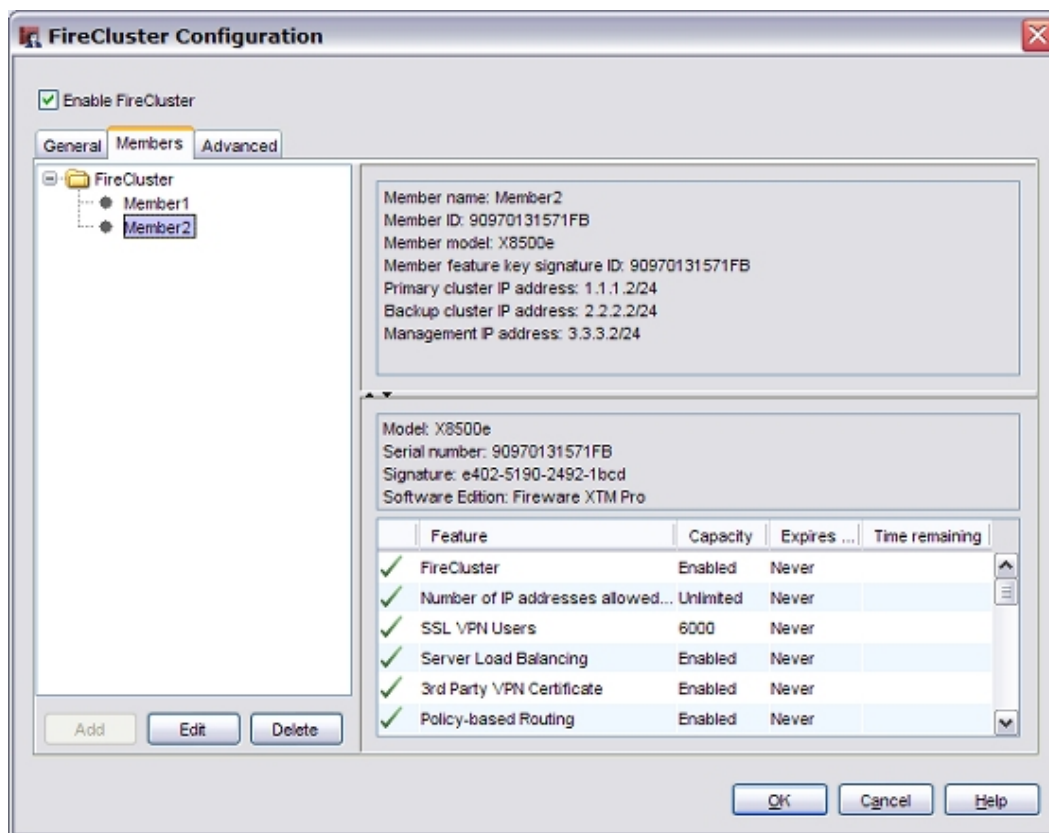
## Remove or Add a Cluster Member

You can use Policy Manager to remove and add devices to the FireCluster.

### Remove a Device from a FireCluster

To remove a device from a FireCluster:

1. In WatchGuard System Manager, open the configuration for the cluster master.
2. Click .  
Or, select **Tools > Policy Manager**.  
*Policy Manager appears.*
3. Select **FireCluster > Configure**.  
*The FireCluster Cluster Configuration dialog box appears.*
4. Click the **Members** tab.  
*A list of cluster members appears.*



5. Select the name of the cluster member you want to delete.
6. Click **Delete**.  
*The device is removed from the member list.*
7. Click **OK**.
8. Save the configuration file to the cluster.  
*The device is removed from the cluster.*

**Note** When you save the configuration tile to the cluster, Policy Manager checks to see if the current cluster master is in the cluster configuration. If the device you removed from the configuration is the current cluster master, Policy Manager attempts to force a failover, so the backup master becomes the new cluster master. If the failover succeeds, the configuration change is saved. If the failover does not succeed, Policy Manager does not allow you to save the configuration to the cluster.

After you remove an XTM device from a cluster, when you save the configuration to the cluster the device you removed reboots and all settings on the device are reset to factory defaults. The other member becomes the cluster master.

For information about how to see which device is the cluster master, or to manually force failover from the cluster master to another member, see *Monitor and Control FireCluster Members* on page 282.

## Add a New Device to a FireCluster

You can add a new cluster member on the **FireCluster Configuration** dialog box **Members** tab.

To add a new device to the cluster:


1. Click **Add**.
2. Configure the settings for the new cluster member as described in *Configure FireCluster Manually* on page 274.

When FireCluster is enabled, you must have at least one device in the cluster.


3. To remove both devices from the cluster, you must *Disable FireCluster*.

## Update the FireCluster Configuration

You update the configuration of a FireCluster in much the same way that you update the configuration for an individual XTM device. You can only save an updated configuration to the cluster master.

1. In WatchGuard System Manager, click .  
Or, select **File > Connect To Device**.  
*The Connect to Firebox dialog box appears.*
2. Select or type the trusted IP address for the cluster. Type the status (read-only) passphrase. Click **OK**.

*The cluster appears as a device in the WatchGuard System Manager Device Status tab.*

3. On the **Device Status** tab, select the cluster device.
4. Click .
- Or, select **Tools > Policy Manager**.  
*Policy Manager appears with the current configuration file for the cluster.*
5. Make any configuration changes to the cluster.
6. Save the configuration file to the trusted IP address of the cluster.

When you save the configuration to a cluster, the cluster master automatically sends the updated configuration to the other cluster member.

## Configure FireCluster Logging and Notification

The **Advanced** tab in the **FireCluster Configuration** dialog box includes settings for logging and notification.

Log messages are always created for FireCluster events.

To configure notification settings for FireCluster failover and failback events:

1. Click **Notification**.
2. Select a notification method: SNMP trap, email message, or pop-up window.

For more information about notification settings, see *Set Logging and Notification Preferences* on page 723.

To set the diagnostic log level for FireCluster events in Policy Manager:

1. Select **Setup > Logging**.
2. Click **Diagnostic Log Level**.

For more information about diagnostic logging, see *Set the Diagnostic Log Level* on page 720.

## About Feature Keys and FireCluster

Each device in a cluster has its own feature key. When you configure a FireCluster, you import feature keys for each cluster member. The FireCluster has a set of Cluster Features, which apply to the whole cluster. The Cluster Features are based on the feature keys for all devices in the cluster.

For more information about how to get a feature key for a device, see *Get a Feature Key from LiveSecurity* on page 59.

When you enable a FireCluster, the subscription services and upgrades activated for cluster members operate as follows:

### *LiveSecurity Service subscription*

A LiveSecurity Service subscription applies to a single device, even when that device is configured as a member of a cluster. You must have an active LiveSecurity Service subscription for each device in the cluster. If the LiveSecurity subscription expires for a cluster member, you cannot upgrade the Fireware XTM OS on that device.

### *BOVPN and Mobile VPN upgrades*

Branch Office VPN (BOVPN) and Mobile VPN licenses operate differently for an active/active cluster and an active/passive cluster.

**Active/Active** — Licenses for Branch Office VPN and Mobile VPN are aggregated for devices configured as a FireCluster. If you purchase additional BOVPN or Mobile VPN licenses for each device in a cluster, that additional capacity is shared between the devices in the cluster. For example, if you have two devices in a cluster and each device feature key has a capacity for 2000 Mobile VPN users, the effective license for the FireCluster is 4000 Mobile VPN users.

**Active/Passive** — Licenses for Branch Office and Mobile VPN are not aggregated for devices configured as a FireCluster. The active device uses the highest capacity Branch Office and Mobile VPN activated for either device. If you purchase additional BOVPN or Mobile VPN licenses for either device in a cluster, the additional capacity is used by the active device.

### Subscription Services

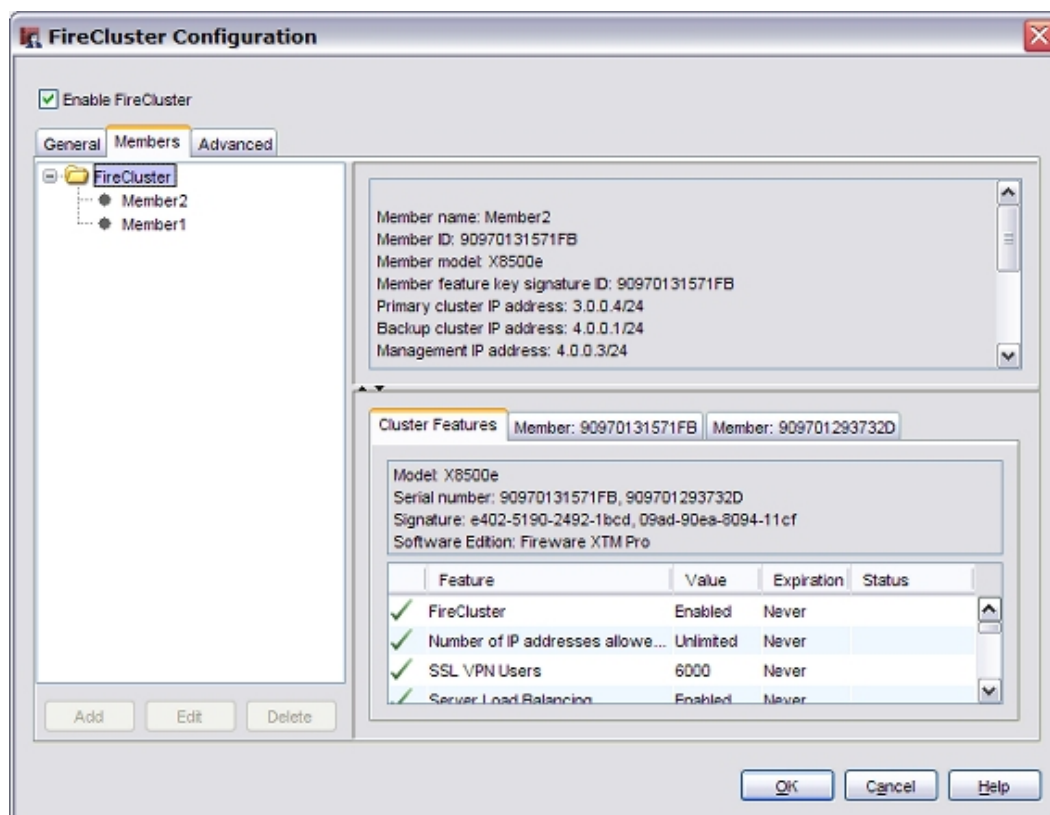
Subscription Services such as WebBlocker, spamBlocker, and Gateway AV operate differently for an active/active cluster and an active/passive cluster.

- Active/Active — You must have the same subscription services enabled in the feature keys for both devices. Each cluster member applies the services from its own feature key.
- Active/Passive — You must enable the subscription services in the feature key for only one cluster member. The active cluster member uses the subscription services that are active in the feature key of either cluster member.

**Note** In an active/active cluster, it is very important to renew subscription services for both cluster members. If a subscription service expires on one member of an active/active cluster, the service does not function for that member. The member with the expired license continues to pass traffic, but does not apply the service to that traffic.

## See the Feature Keys and Cluster Features for a Cluster

1. Open Policy Manager for the cluster master.
2. Select **FireCluster > Configure**.
3. Select the **Members** tab.



4. Select the **FireCluster** folder.  
*Tabs with the cluster features, and features for each cluster member, appear at the bottom of the dialog box.*

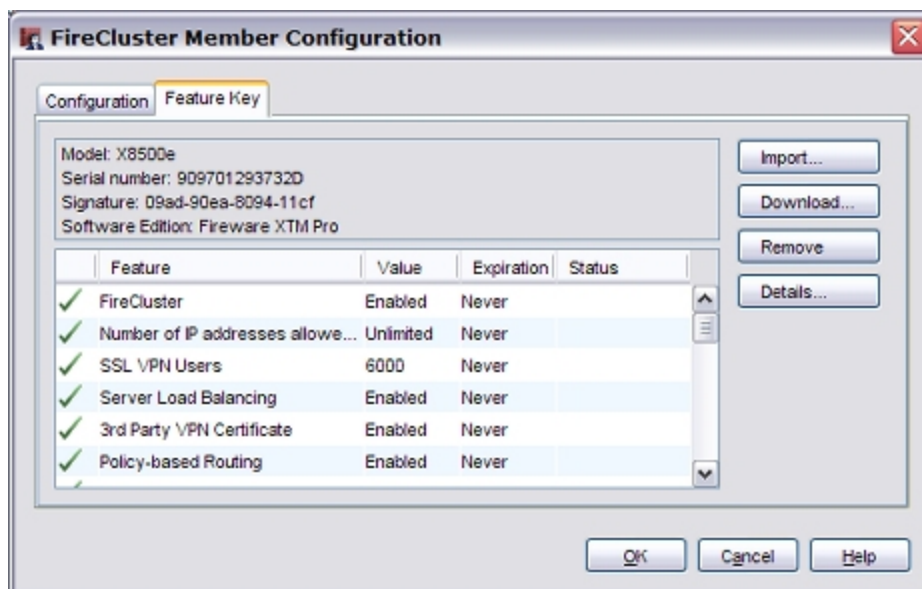
5. To see the licensed features for the cluster, select the **Cluster Features** tab.
  - The **Expiration** and **Status** columns show the latest expiration date and days remaining for that service among the cluster members.
  - The **Value** column shows the status or capacity of the feature for the cluster as a whole.
6. Select the **Member** tabs to see the individual licenses for each cluster member.  
Make sure to check the expiration date on any services for each cluster member.

## See or Update the Feature Key for a Cluster Member

You can use Policy Manager to see or update the feature key for each cluster member.

1. Select **FireCluster > Configure**.
2. Select the **Members** tab.
3. In the **FireCluster** tree, select the member name. Click **Edit**.

*The FireCluster Member Configuration dialog box appears.*



4. Select the **Feature Key** tab.  
*The features that are available from this feature key appear.*  
This tab also includes:
  - Whether each feature is enabled or disabled
  - A value assigned to the feature, such as the number of allowed VLAN interfaces
  - The expiration date of the feature
  - The amount of time that remains before the feature expires
5. Click **Import**.  
*The Import Firebox Feature Key dialog box appears.*



6. To find the feature key file, click **Browse**.  
Or, copy the text of the feature key file and click **Paste** to insert it in the dialog box. Click **OK**.
7. *Save the Configuration File.*  
*The feature key is not copied to the device until you save the configuration file to the cluster master.*

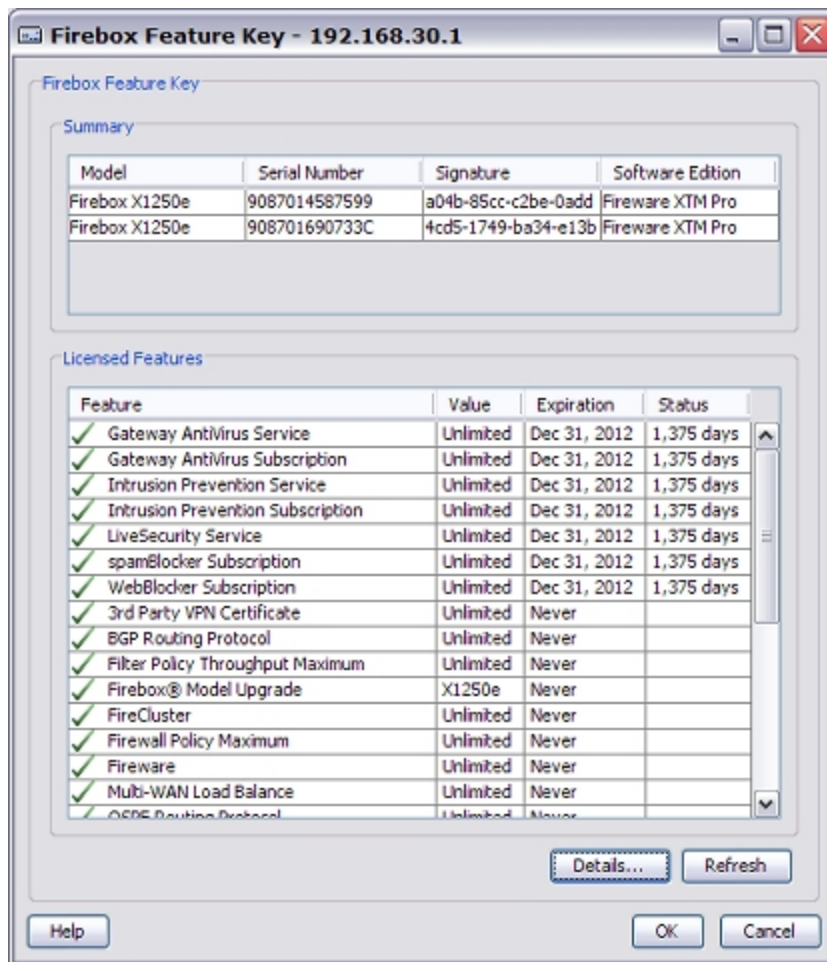
In Policy Manager, you can also select **Setup > Feature Keys** to see the feature key information for the cluster.

## See the FireCluster Feature Key in Firebox System Manager

You can also see the feature key from Firebox System Manager:

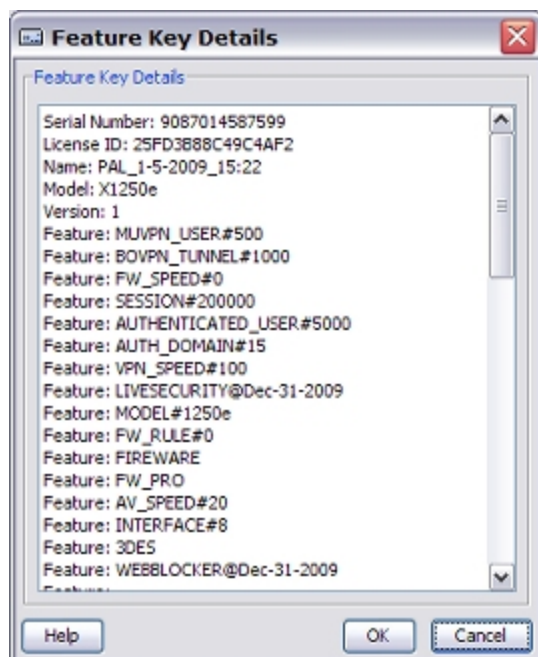
1. Select **View > Feature Keys**.

*The Firebox Feature Key dialog appears with a summary of all devices in the cluster. The Licensed Features section includes the features licensed for the entire cluster.*



2. Click **Details** to see the details about the feature key for each device in the cluster.





3. Scroll down to see the feature key for the second device.

## Create a FireCluster Backup Image

Because the cluster master synchronizes the configuration with the cluster members, you only have to back up the image of the cluster master.

To create a backup of the flash image (.fxi) of the cluster master:

1. In WatchGuard System Manager, use the cluster trusted interface IP address to connect to the cluster master.
2. Open Policy Manager for the cluster master.
3. *Make a Backup of the XTM Device Image.*

To create a backup image of an individual cluster member:

1. In WatchGuard System Manager, use the cluster trusted interface IP address to connect to the cluster master.
2. Open Policy Manager for the cluster member.
3. *Make a Backup of the XTM Device Image.*

**Note** *Make sure to keep a record of the management IP addresses and passphrases in the backup image. If you restore a FireCluster from this image, you must have this information to connect to the cluster members.*

## Restore a FireCluster Backup Image

To restore a FireCluster backup image to a cluster, you must restore the image to each cluster member one at a time. The backup master must leave the cluster before you restore the backup image to each cluster member. After you restore the configuration to both cluster members, the backup master must rejoin the cluster.

When you restore a backup image, you must use the cluster Management IP address to connect to the device. All other interfaces on the device are inactive until the final step when the backup master rejoins the cluster.

For more information about the cluster Management IP address, see *About the Interface for Management IP Address*.

### Make the Backup Master Leave the Cluster

1. In WatchGuard System Manager, use the FireCluster Management IP address to connect to the backup master.
2. Start Firebox System Manager for the backup master.
3. Select **Tools > Cluster > Leave**.

*The backup master leaves the cluster and reboots.*

**Note** Do not make configuration changes to the cluster master after the backup master has left the cluster.

### Restore the Backup Image to the Backup Master

1. In WatchGuard System Manager, use the FireCluster Management IP address to connect to the backup master.
2. Start Policy Manager for the backup master.
3. Select **File > Restore** to restore the backup image.

*The device restarts with the restored configuration.*

For more information about the Restore command, see *Restore an XTM Device Backup Image* on page 44.

**Note** After you restore the backup image to a cluster member, the device appears to be a member of a cluster in WatchGuard System Manager and Firebox System Manager. The cluster does not function until after the last step when the backup master rejoins the cluster.

### Restore the Backup Image to the Cluster Master

1. In WatchGuard System Manager, use the interface for management IP address to connect to the cluster master.
2. Start Policy Manager for the cluster master.
3. Select **File > Restore** to restore the backup image.

*The device restarts with the restored configuration.*

For more information about the Restore command, see *Restore an XTM Device Backup Image* on page 44.

4. In WatchGuard System Manager, use the interface for management IP address to connect to the cluster master.

If the backup image you restored has a different interface for management IP address for this cluster member or a different passphrase, use the interface for management IP and passphrase from the backup image to reconnect to the device.

## Make the Backup Master Rejoin the Cluster

1. In WatchGuard System Manager, use the management IP address to connect to the backup master.

If the backup image you restored has a different interface for management IP address for this cluster member or a different passphrase, use the interface for management IP and passphrase from the backup image to reconnect to the device.

2. Start Fireware System Manager for the backup master.
3. Select **Tools > Cluster > Join**.

*The backup master reboots and rejoins the cluster.*

## Upgrade Fireware XTM for FireCluster Members

To upgrade the Fireware XTM software for devices in a FireCluster configuration, you use Policy Manager.

When you upgrade the software on a member of a cluster, the device reboots. When the upgrade is in progress, network traffic is handled by the other device in the cluster. When the reboot completes, the device you upgraded automatically rejoins the cluster. Because the cluster cannot do load balancing at the time of the reboot, if you have an active/active cluster, we recommend you schedule the upgrade at a time when the network traffic is lightest.

**Note** *For some Fireware XTM software upgrades, such as an upgrade from Fireware XTM v11.3.x to Fireware XTM v11.4, the cluster becomes unavailable and passes no traffic until the upgrade is complete and the devices in the cluster reboot. If an upgrade will cause a service interruption, Policy Manager displays a warning and requires you to confirm that you want to continue.*

To upgrade Fireware XTM for a device in a cluster:

1. Open the cluster configuration file in Policy Manager
2. Select **File > Upgrade**.
3. Type the configuration passphrase.
4. Type or select the location of the upgrade file.
5. To create a backup image, select **Yes**.

*A list of the cluster members appears.*

6. Select the check box for each device you want to upgrade.

*A message appears when the upgrade for each device is complete.*

When the upgrade is complete, each cluster member reboots and rejoins the cluster. If you upgrade both devices in the cluster at the same time, the devices are upgraded one at a time. This is to make sure there is not an interruption in network access at the time of the upgrade.

Policy Manager upgrades the backup master first. When the upgrade of the first member is complete, that device becomes the new cluster master. Then Policy Manager upgrades the second device.

**Note** *We recommend you use the same software version on both devices. A cluster functions best if all devices in the cluster run the same software version.*


If you want to upgrade the firmware from a remote location, make sure the interface for management IP address is configured on the external interface, and the IP address is public and routable.

For more information, see *About the Interface for Management IP Address* on page 255.

## Disable FireCluster

When you disable FireCluster, both cluster members reboot at the same time. We recommend that you plan this for a time when you can have a brief network interruption.

To disable FireCluster:

1. In WatchGuard System Manager, open the configuration for the cluster master.
2. Click .  
Or, select **Tools > Policy Manager**.
3. Select **FireCluster > Configure**.  
*The FireCluster Cluster Configuration dialog box appears.*
4. Clear the **Enable FireCluster** check box.
5. Click **OK**.
6. Save the configuration to the XTM device.  
*The configuration is saved and both devices in the cluster reboot.*
  - The cluster master starts with the same IP addresses that were assigned to the cluster.
  - The cluster backup master starts with the default IP addresses and configuration.

You can remove one member from the cluster and not disable the FireCluster feature. This results in a cluster with only one member, but does not disable FireCluster or cause a network interruption.

For more information, see *Remove or Add a Cluster Member* on page 290.



# 12 Authentication

---

## About User Authentication

User authentication is a process that finds whether a user is who he or she is declared to be and verifies the privileges assigned to that user. On the XTM device, a user account has two parts: a user name and a passphrase. Each user account is associated with an IP address. This combination of user name, passphrase, and IP address helps the device administrator to monitor connections through the device. With authentication, users can log in to the network from any computer, but access only the network ports and protocols for which they are authorized. The XTM device can then map the connections that start from a particular IP address and also transmit the session name while the user is authenticated.

You can create firewall polices to give users and groups access to specified network resources. This is useful in network environments where different users share a single computer or IP address.

You can configure your XTM device as a local authentication server, or use your existing Active Directory or LDAP authentication server, or an existing RADIUS authentication server. When you use Firebox authentication over port 4100, account privileges can be based on user name. When you use third-party authentication, account privileges for users that authenticate to the third-party authentication servers are based on group membership.

The WatchGuard user authentication feature allows a user name to be associated with a specific IP address to help you authenticate and track user connections through the device. With the device, the fundamental question that is asked and answered with each connection is, *"Should I allow traffic from source X to go to destination Y?"* For the WatchGuard authentication feature to work correctly, the IP address of the user's computer must not change while the user is authenticated to the device.

In most environments, the relationship between an IP address and the user computer is stable enough to use for authentication. Environments in which the association between the user and an IP address is not consistent, such as kiosks or networks where applications are run from a terminal server, are usually not good candidates for the successful use of the user authentication feature.

WatchGuard supports Authentication, Accounting, and Access control (AAA) in the firewall products, based on a stable association between IP address and person.

The WatchGuard user authentication feature also supports authentication to an Active Directory domain with Single Sign-On (SSO), as well as other common authentication servers. In addition, it supports inactivity settings and session time limits. These controls restrict the amount of time an IP address is allowed to pass traffic through the XTM device before users must supply their passwords again (reauthenticate).

If you control SSO access with a white list and manage inactivity timeouts, session timeouts, and who is allowed to authenticate, you can improve your control of authentication, accounting, and access control.

To prevent a user from authenticating, you must disable the account for that user on the authentication server.

## User Authentication Steps

After you configure your XTM device as a local authentication server, the HTTPS server on the XTM device accepts authentication requests. To authenticate, a user must connect to the authentication portal web page on the XTM device.

1. Go to either:

`https://[device interface IP address]:4100/`

or

`https://[device hostname]:4100`

*An authentication web page appears.*

2. Type a user name and password.
3. Select the authentication server from the drop-down list, if more than one type of authentication is configured.

*The XTM device sends the name and password to the authentication server using PAP (Password Authentication Protocol).*

When authenticated, the user is allowed to use the approved network resources.

**Note** *Because Fireware XTM uses a self-signed certificate by default for HTTPS, you see a security warning from your web browser when you authenticate. You can safely ignore this security warning. If you want to remove this warning, you can use a third-party certificate or create a custom certificate that matches the IP address or domain name used for authentication.*

*For more information, see [Configure the Web Server Certificate for Firebox Authentication](#) on page 878.*



## Manually Close an Authenticated Session

Users do not have to wait for the session timeout to close their authenticated sessions. They can manually close their sessions before the timeout occurs. The Authentication web page must be open for a user to close a session. If it is closed, the user must authenticate again to log out.

To close an authenticated session:

1. Go to the Authentication portal web page:

`https://[device interface IP address]:4100/`

or

`https://[device host name]:4100`

2. Click **Logout**.

**Note** *If the Authentication portal web page is configured to automatically redirect to another web page, the portal is redirected just a few seconds after you open it. Make sure you logout before the page redirects.*

## Manage Authenticated Users

You can use Firebox System Manager to see a list of all the users authenticated to your XTM device and close sessions for those users.

### See Authenticated Users

To see the users authenticated to your XTM device:

1. Start *Firebox System Manager*.
2. Select the **Authentication List** tab.  
*A list of all users authenticated to the Firebox appears.*

### Close a User Session

From Firebox System Manager:

1. Select the **Authentication List** tab.  
*A list of all users authenticated to the Firebox appears.*
2. Select one or more user names from the list.
3. Right-click the user name(s) and select **Log Off User**.

For more information, see *Authenticated Users (Authentication List)* on page 770.

## Use Authentication to Restrict Incoming Traffic

One function of the authentication tool is to restrict outgoing traffic. You can also use it to restrict incoming network traffic. When you have an account on the XTM device and the device has a public external IP address, you can authenticate to the device from a computer external to the device.

For example, you can type this address in your web browser: `https://<IP address of XTM device external interface>:4100/`.

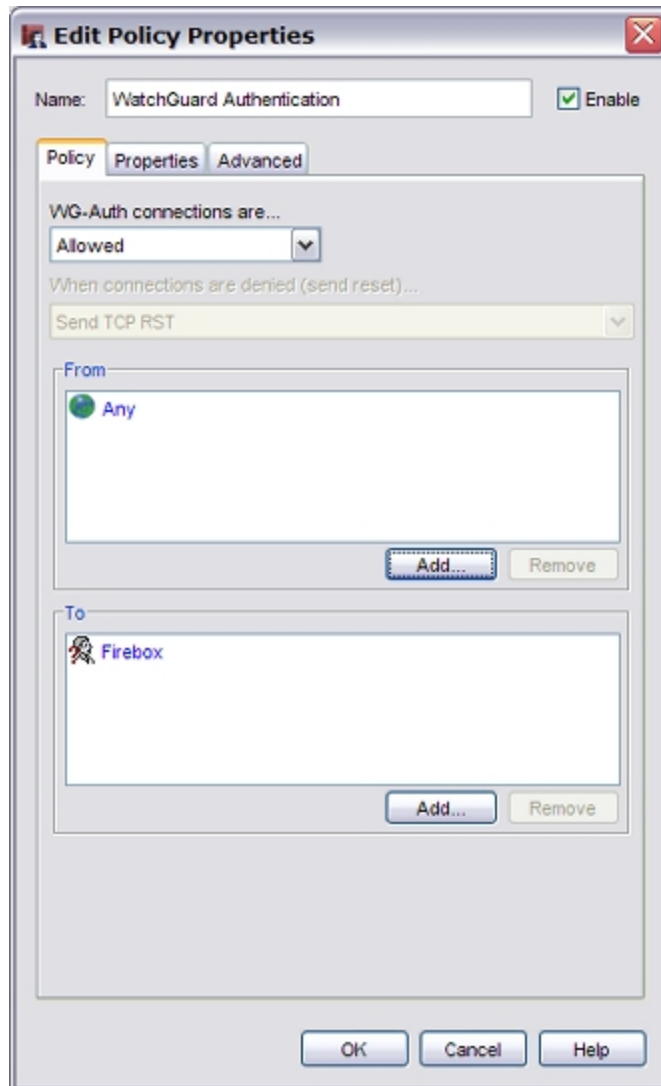
After you authenticate, you can use the policies that are configured for you on the device.

To enable a remote user to authenticate from the external network:

1. *Open Policy Manager* for your device.
2. Double-click the **WatchGuard Authentication** policy. This policy appears after you add a user or group to a policy configuration.  
*The Edit Policy Properties dialog box appears.*
3. From the **WG-Auth connections are** drop-down list, make sure **Allowed** is selected.
4. In the **From** section, click **Add**.  
*The Add Address dialog box appears.*
5. From the **Available Members** list, select **Any** and click **Add**.
6. Click **OK**.  
*Any appears in the From list.*
7. In the **To** section, click **Add**.
8. From the **Available Members** list, select **Firebox** and click **Add**.

9. Click **OK**.

*Firebox appears in the To list.*



10. Click **OK** to close the **Edit Policy Properties** dialog box.

## Use Authentication Through a Gateway Firebox

The gateway Firebox is the XTM device that you place in your network to protect your Management Server from the Internet.

For more information, see *About the Gateway Firebox* on page 548.

To send an authentication request through a gateway Firebox to a different device, you must have a policy that allows the authentication traffic on the gateway device. If authentication traffic is denied on the gateway device, use Policy Manager to add the WG-Auth policy. This policy controls traffic on TCP port 4100. You must configure the policy to allow traffic to the IP address of the destination device.

## About the WatchGuard Authentication (WG-Auth) Policy

The WatchGuard Authentication (WG-Auth) policy is automatically added to your XTM device configuration when you add the first policy that has a user or group name in the **From** list on the **Policy** tab of the policy definition. The WG-Auth policy controls access to port 4100 on your XTM device. Your users send authentication requests to the device through this port. For example, to authenticate to an XTM device with an IP address of 10.10.10.10, your users type `https://10.10.10.10:4100` in the web browser address bar.

If you want to send an authentication request through a gateway device to a different device, you might have to add the WG-Auth policy manually. If authentication traffic is denied on the gateway device, you must use Policy Manager to add the WG-Auth policy. Modify this policy to allow traffic to the IP address of the destination device.

For more information on when to modify the WatchGuard Authentication policy, see *Use Authentication to Restrict Incoming Traffic* on page 306.

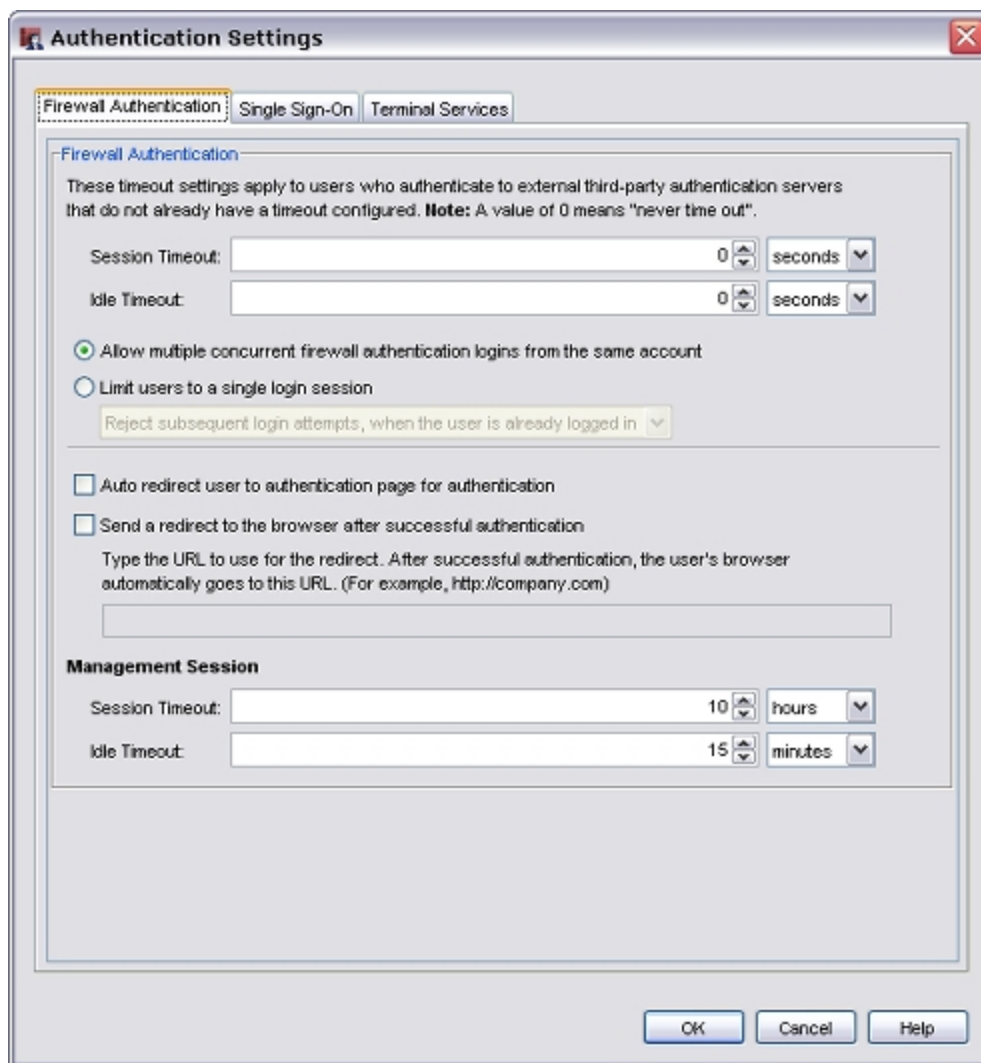
## Set Global Firewall Authentication Values

When you configure your global authentication settings, you can configure the global values for firewall authentication, such as timeout values, user login session limits, and authentication page redirect settings. You can also enable Single Sign-On (SSO), and configure settings for Terminal Services. For more information, see the topics *Enable Single Sign-On (SSO)* and *Configure Terminal Services Settings*.

To configure Firewall Authentication settings:

1. *Open Policy Manager.*
2. Select **Setup > Authentication > Authentication Settings**.

*The Authentication Settings dialog box appears with the Firewall Authentication tab selected by default.*



3. Configure authentication settings as described in the subsequent sections.
4. Click **OK**.

## Set Global Authentication Timeouts

You can set the time period that users remain authenticated after they close their last authenticated connection. This timeout is set either in the **Authentication Settings** dialog box, or in the **Setup Firebox User** dialog box.

For more information about user authentication settings and the **Setup Firebox User** dialog box, see *Define a New User for Firebox Authentication* on page 332.

For users authenticated by third-party servers, the timeouts set on those servers also override the global authentication timeouts.

Authentication timeout values do not apply to Mobile VPN with PPTP users.

### *Session Timeout*

The maximum length of time the user can send traffic to the external network. If you set this field to zero (0) seconds, minutes, hours, or days, the session does not expire and the user can stay connected for any length of time.

### *Idle Timeout*

The maximum length of time the user can stay authenticated when idle (not passing any traffic to the external network). If you set this field to zero (0) seconds, minutes, hours, or days, the session does not timeout when idle and the user can stay idle for any length of time.

## Allow Multiple Concurrent Logins

You can allow more than one user to authenticate with the same user credentials at the same time, to one authentication server. This is useful for guest accounts or in laboratory environments. When the second user logs in with the same credentials, the first user authenticated with the credentials is automatically logged out. If you do not allow this feature, a user cannot authenticate to the authentication server more than once at the same time.

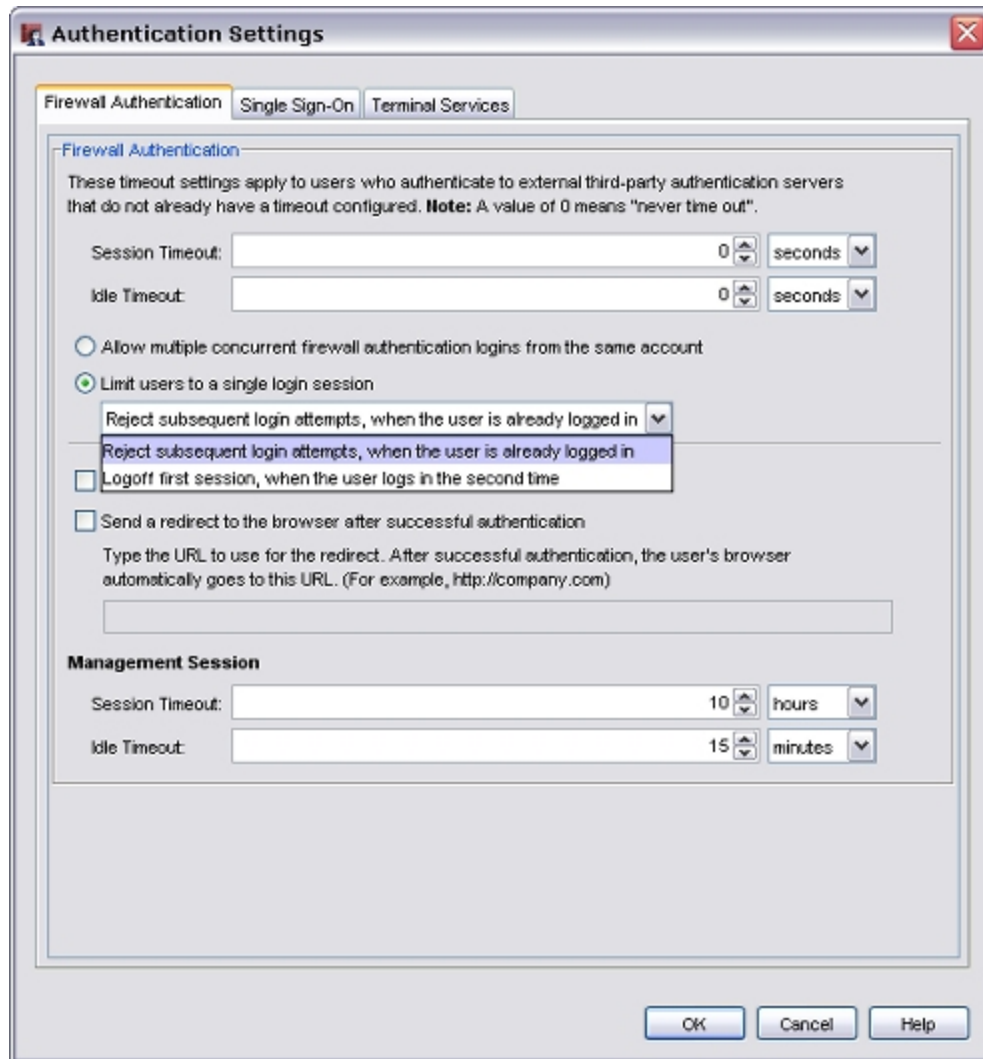
1. Go to the **Authentication Settings** dialog box.
2. Select the **Allow multiple concurrent firewall authentication logins from the same account** option.

For Mobile VPN with IPSec and Mobile VPN with SSL users, concurrent logins from the same account are always supported regardless of whether this option is selected. These users must log in from different IP addresses for concurrent logins, which means that they cannot use the same account to log in if they are behind an XTM device that uses NAT. Mobile VPN with PPTP users do not have this restriction.

## Limit Login Sessions

From the **Authentication Settings** dialog box, you can limit your users to a single authenticated session. If you select this option, your users cannot login to one authentication server from different IP addresses with the same credentials. When a user is authenticated, and tries to authenticate again, you can select whether the first user session is terminated when the subsequent session is authenticated, or if the subsequent session is rejected.

1. Select **Limit users to a single login session**.
2. From the drop-down list, select an option:
  - **Reject subsequent login attempts, when the user is already logged in**
  - **Logoff first session, when user logs in the second time.**



## Automatically Redirect Users to the Authentication Portal

If you require your users to authenticate before they can get access to the Internet, you can choose to automatically send users who are not already authenticated to the authentication portal, or have them manually navigate to the portal. This applies only to HTTP and HTTPS connections.

### *Auto redirect users to authentication page for authentication*

When you select this check box, all users who have not yet authenticated are automatically redirected to the authentication portal when they try to get access to the Internet. If you do not select this checkbox, unauthenticated users must manually navigate to the authentication portal to log in.

For more information about user authentication, see *User Authentication Steps* on page 304.

If you have users who must manually authenticate to the authentication portal, and you use SSO, you can add an SSO exception for those users to reduce the amount of time it takes for them to authenticate. For more information about SSO exceptions, see *Enable Single Sign-On (SSO)*.

## Use a Custom Default Start Page

When you select the **Auto redirect users to authentication page for authentication** check box to require your users to authenticate before they can get access to the Internet, the Authentication portal appears when a user opens a web browser. If you want the browser to go to a different page after your users successfully log in, you can define a redirect.

From the **Authentication Settings** dialog box:

1. Select the **Send a redirect to the browser after successful authentication** check box.
2. In the text box, type the URL of the web site to which users are redirected.

## Set Management Session Timeouts

Use these fields to set the time period that a user logged in with read/write privileges remains authenticated before the XTM device terminates the session.

### *Session Timeout*

The maximum length of time the user can send traffic to the external network. If you set this field to zero (0) seconds, minutes, hours, or days, the session does not expire and the user can stay connected for any length of time.

### *Idle Timeout*

The maximum length of time the user can stay authenticated when idle (not passing any traffic to the external network). If you set this field to zero (0) seconds, minutes, hours, or days, the session does not expire when the user is idle, and the user can stay idle for any length of time.

## About Single Sign-On (SSO)

When users log on to computers on your network, they must give a user name and password. If you use Active Directory authentication on your XTM device to restrict outgoing network traffic to specified users or groups, they must also log on again when they manually authenticate to the device to access network resources such as the Internet. You can use Single Sign-On (SSO) to enable users on the trusted or optional networks to automatically authenticate to the XTM device when they log on to their computers.

WatchGuard SSO is a two-part solution that includes the SSO agent and SSO client services. For SSO to work, you must install the SSO agent software on a computer in your domain. The SSO client software is optional and is installed on each user's client computer. If you configure multiple Active Directory domains, your users must install the SSO client. For more information, see *Configure Active Directory Authentication* on page 348 and *Install the WatchGuard Single Sign-On (SSO) Client* on page 319.

The SSO agent software makes a call to the client computer over port 4116 to verify who is currently logged in. If there is no response, the SSO agent reverts to the previous protocol from versions prior to WSM 10.2.4, and makes a *NetWkstaUserEnum* call to the client computer. It then uses the information it gets to authenticate a user for Single Sign-On.



If the SSO client is not installed, the SSO agent can get more than one answer from the computer it queries. This can occur if more than one user logs on to the same computer or because of service or batch logons that occur on the computer. The SSO agent uses only the first answer it gets from the computer and reports that user to the XTM device as the user that is logged on. The device can then check the user information against all the defined policies for that user and/or user group at one time. The SSO agent caches this data for about 10 minutes by default so that a query does not have to be generated for every connection.

When the SSO client software is installed, it receives the call from the SSO agent and returns accurate information about the user who is currently logged in to the workstation. The SSO agent does not contact the Active Directory server for user credentials from the SSO client, because it receives the correct information about who is currently logged in to the computer and to which Active Directory groups the user belongs. If you configure multiple Active Directory domains, your users must install the SSO client.

If you work in an environment where more than one person uses a computer, we recommend that you install the SSO client software. If you do not use the SSO client, there are access control limitations you must be aware of. For example, for services installed on a client computer (such as a centrally administered antivirus client) that have been deployed so that they log on with domain account credentials, the XTM device gives all users access rights as defined by the first user that is logged on (and the groups of which that user is a member), and not the credentials of the individual users that log on interactively. Also, all log messages generated from the user's activity show the user name of the service account, and not the individual user.

**Note** *If you do not install the SSO client, we recommend you do not use SSO for environments where users log on to computers with service or batch logons. When more than one user is associated with an IP address, network permissions may not operate correctly. This can be a security risk.*

If you enable Single Sign-On, you can also use Firewall authentication to log in to Firewall authentication page and authenticate with different user credentials. For more information, see *Firewall Authentication* on page 330.

## Before You Begin

- You must have an Active Directory server configured on a trusted or optional network.
- Your XTM device must be configured to use Active Directory authentication.
- Each user must have an account set up on the Active Directory server.
- Each user must log on to a domain account for Single Sign-On (SSO) to operate correctly. If users log on to an account that exists only on their local computers, their credentials are not checked and the XTM device does not recognize that they are logged in.
- If you use third-party firewall software on your network computers, make sure that TCP port 445 (Samba/ Windows Networking) is open on each client.
- Make sure that printing and file sharing is enabled on every computer from which users authenticate with SSO.
- Make sure that NetBIOS and SMB ports are not blocked on every computer from which users authenticate with SSO. NetBIOS uses TCP/UDP ports 137, 138, and 139. SMB uses TCP port 445.
- Make sure that port 4116 is open on the client computers.
- Make sure that all computers from which users authenticate with SSO are members of the domain with unbroken trust relationships.

## Set Up SSO

To use SSO, you must install the SSO agent software. We recommend that you also install the SSO client on your users' computers. Though you can use SSO with only the SSO agent, you increase your security and access control when you also use the SSO client.

To set up SSO, follow these steps:

1. *Install the WatchGuard Single Sign-On (SSO) Agent.*
2. *Install the WatchGuard Single Sign-On (SSO) Client (optional, but recommended).*
3. *Enable Single Sign-On (SSO).*

## Install the WatchGuard Single Sign-On (SSO) Agent

To use Single Sign-On (SSO), you must install the WatchGuard SSO agent. The SSO agent is a service that receives requests for Firebox authentication and checks user status with the Active Directory server. The service runs with the name *WatchGuard Authentication Gateway* on the computer on which you install the SSO agent software. This computer must have the Microsoft .NET Framework 2.0 or later installed.

## Download the SSO Agent Software

1. Open a web browser and go to <http://www.watchguard.com/>.
2. Log in with your LiveSecurity Service user name and password.
3. Click the **Software Downloads** link.
4. Select your device type and model number.
5. Download the WatchGuard Authentication Gateway software and save the file to a convenient location.

## Before You Install

The SSO agent service must run as a user account, not an administrator account. We recommend that you create a new user account for this purpose. For the SSO agent service to operate correctly, make sure you configure the user account with a password that never expires.

## Install the SSO Agent Service

1. Double-click **WG-Authentication-Gateway.exe** to start the Authentication Gateway Setup Wizard. On some operating systems, you might need to type a local administrator password to run the installer.
2. To install the software, use the instructions on each page and complete the wizard.

For the domain user name, you must type the user name in the form: domain\username. Do not include the .com or .net part of the domain name.

For example, if your domain is *mywatchguard.com* and you use the domain account *ssoagent*, type *mywatchguard\ssoagent*.

You can also use the UPN form of the user name: *username@mywatchguard.com*. If you use the UPN form of the user name then you must include the .com or .net part of the domain name.

3. Click **Finish** to close the wizard.

When the wizard completes, the WatchGuard Authentication Gateway service starts automatically. Each time the computer starts, the service starts automatically.

After you have completed the SSO Agent installation, you must configure the domain settings for the SSO Agent. For more information, see *Configure the SSO Agent* on page 315.

## Configure the SSO Agent

If you use multiple Active Directory domains, you must specify the domains to use for SSO. After you have installed the SSO Agent on your computer, you can specify the domains to use for authentication and synchronize the domain configuration with the SSO Agent. To configure the SSO Agent settings, you must have administrator privileges on your computer.

When you first launch the SSO Agent, it generates the *Users.xml* and *AdInfos.xml* configuration files. These configurations files are encrypted and store the domain configuration details you specify when you configure the SSO Agent.

The SSO Agent has two default accounts, *administrator* and *status*. To log in to the SSO Agent, use these accounts. To make changes to the configuration, you must log in with the administrator credentials. The default credentials (username/password) for these accounts are:

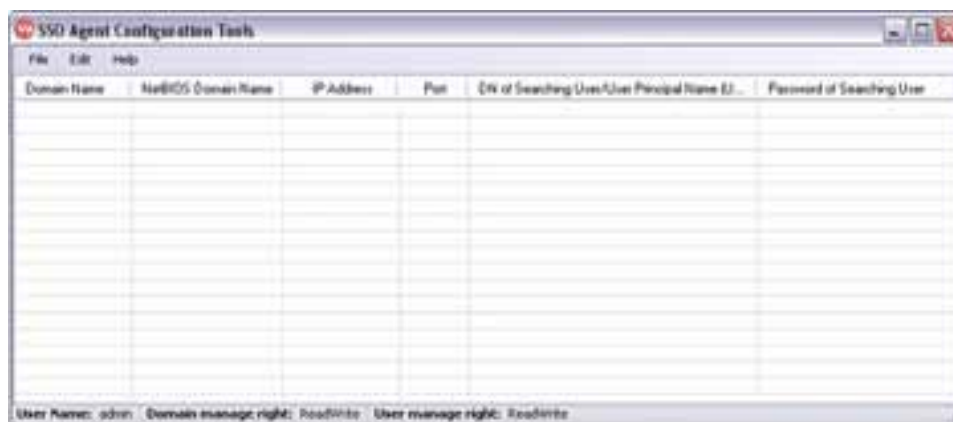
- administrator — admin/readwrite
- status — status/readonly

After you log in for the first time, we recommend you change the passwords for the default accounts.

For more information about Active Directory, see *Configure Active Directory Authentication*.

## Log In to the SSO Agent Configuration Tool

1. Select **Start > WatchGuard SSO Agent Configuration Tool**.  
*The SSO Agent Configuration Tool appears.*
2. In the **User Name** text box, type the administrator user name: `admin`.
3. In the **Password** text box, type the administrator password: `readwrite`.  
*The SSO Agent Configuration Tools appears.*



4. Configure your SSO Agent as described in the subsequent sections.
5. To save your changes, select **File > Save**.

## Manage User Accounts and Passwords

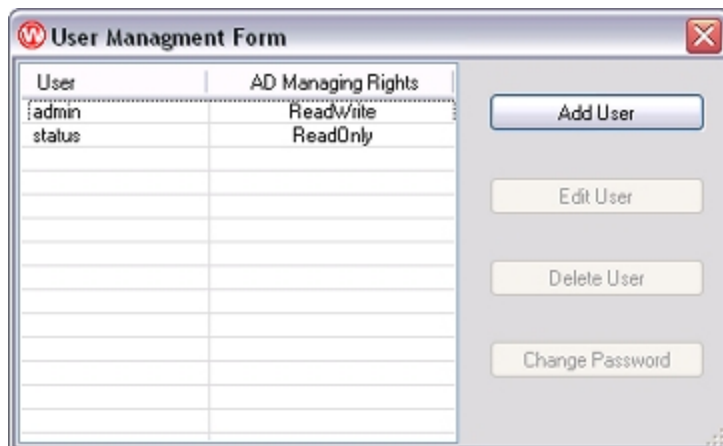
After you log in for the first time, you can change the password for the default accounts. Because you must log in with the administrator credentials to change the SSO Agent settings, make sure you remember the password specified for the administrator account. You can also add new user accounts and change the settings for existing user accounts.

### Change a User Account Password

For the `admin` and `status` accounts, you can only change the password for the account; you cannot change the user name.

From **SSO Agent Configuration Tools**:

1. Select **Edit > User Management**.  
*The User Management Form dialog box appears.*



2. Select the account to change.  
For example, select **admin**.
3. Click **Change Password**.  
*The Change Password dialog box appears.*
4. In the **Password** and **Confirm Password** text boxes, type the new password for this user account.
5. Click **OK**.

### Add a New User Account

From **SSO Agent Configuration Tools**:

1. Select **Edit > User Management**.  
*The User Management Form appears.*
2. Click **Add User**.  
*The Add User dialog box appears.*
3. In the **User Name** text box, type the name for this user account.
4. In the **Password** and **Confirm Password** text boxes, type the password for this user account.
5. Select an access option for this account:
  - **Read-Only**
  - **Read-Write**
6. Click **OK**.

## Edit a User Account

When you edit a user account, you can change only the access option. You cannot change the user name or password for the account. If you want to change the user name, you must add a new user account and delete the old user account.

From **SSO Agent Configuration Tools**:

1. Select **Edit > User Management**.  
*The User Management Form appears.*
2. Select the account to change.
3. Click **Edit User**.  
*The Edit User dialog box appears.*
4. Select a new access option for this account:
  - **Read-Only**
  - **Read-Write**
5. Click **OK**.

## Delete a User Account

From **SSO Agent Configuration Tools**:

1. Select **Edit > User Management**.  
*The User Management Form appears.*
2. Select the account to delete.
3. Click **Delete User**.  
*The Delete User dialog box appears.*
4. Verify the **User Name** is for the account you want to delete.
5. Click **OK**.

## Configure the SSO Agent

To configure your SSO Agent, you can add, edit, and delete information about your Active Directory domains. When you add or edit a domain, you must specify a user account to use to search your Active Directory server. We recommend that you create a specific user account on your server with permissions to search the directory and with a password that never expires.

### Add a Domain

From **SSO Agent Configuration Tools**:

1. Select **Edit > Add Domain**.  
*The Add Domain dialog box appears.*
2. In the **Domain Name** text box, type the name of the domain.  
For example, type `my-example.com`.
3. In the **NetBIOS Domain Name** text box, type the first part of your domain name, without the top level extension (such as, `.com`).  
For example, type `my-example`.
4. In the **IP Address** text box, type the IP address of the Active Directory server for this domain.

5. In the **Port** text box, type the port to use to connect to this server.  
The default setting is 389.
6. In the **Searching User** section, select an option:
  - **Distinguished Name (DN)** (cn=ssouser,cn=users,dc=domain,dc=com)
  - **User Principal Name (UPN)**
  - **Pre-Windows 2000** (netbiosDomain\ssouser)
7. Type the user information for the option you selected.  
Make sure to specify a user who has permissions to search the directory on your Active Directory server.
8. In the **Password of Searching User** and **Confirm password** text boxes, type the password for the user you specified.  
This password must match the password for this user account on your Active Directory server.
9. To add another domain, click **OK & Add Next**. Repeat Steps 2–8.
10. Click **OK**.  
*The domain name appears in the SSO Agent Configuration Tools list.*

## Edit a Domain

When you edit an SSO domain, you can change all the settings except the domain name. If you want to change the domain name, you must delete the domain and add a new domain with the correct name.

From **SSO Agent Configuration Tools**:

1. Select the domain to change.
2. Select **Edit > Edit Domain**.  
*The Edit Domain dialog box appears.*
3. Update the settings for the domain.
4. Click **OK**.

## Delete a Domain

From **SSO Agent Configuration Tools**:

1. Select the domain to delete.
2. Select **Edit > Delete Domain**.  
*A confirmation message appears.*
3. Click **Yes**.

## Install the WatchGuard Single Sign-On (SSO) Client

As a part of the WatchGuard Single Sign-On (SSO) solution, you can install the WatchGuard SSO client. The SSO client installs as a Windows service that runs under the Local System account on a workstation to verify the credentials of the user currently logged in to that computer. When a user tries to authenticate, the SSO agent sends a request to the SSO client for the user's credentials. The SSO client then returns the credentials of the user who is logged in to the workstation.

The SSO client listens on port 4116.

If you configure multiple Active Directory domains, your users must install the SSO client. For more information, see *Configure Active Directory Authentication* on page 348.

Because the SSO client installer is an MSI file, you can choose to automatically install it on your users' computers when they log on to your domain. You can use Active Directory Group Policy to automatically install software when users log on to your domain. For more information about software installation deployment for Active Directory group policy objects, see the documentation for your operating system.

## Download the SSO Client Software

1. Use your web browser to go to <http://www.watchguard.com/>.
2. Log in with your LiveSecurity Service user name and password.
3. Click the **Software Downloads** link.
4. Select your device type and model number.
5. Download the WatchGuard Authentication Client software and save the file to a convenient location.

## Install the SSO Client Service

1. Double-click **WG-Authentication-Client.msi** to start the Authentication Client Setup Wizard. On some operating systems, you might need to type a local administrator password to run the installer.
2. To install the software, use the instructions on each page and complete the wizard.

To see which drives are available to install the client, and how much space is available on each of these drives, click **Disk Cost**.

3. Click **Close** to exit the wizard.

After the wizard completes, the WatchGuard Authentication Client service starts automatically. Each time the computer starts, the service starts automatically.

## Enable Single Sign-On (SSO)

Before you can configure SSO, you must:

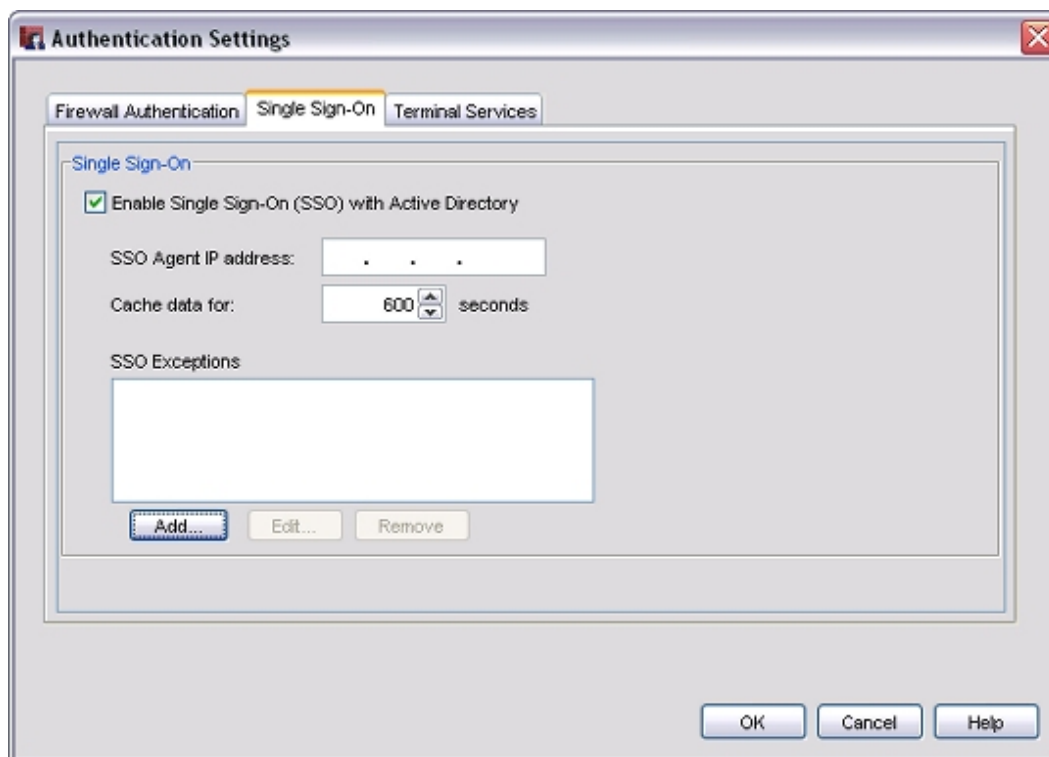
- Configure your Active Directory server
- *Install the WatchGuard Single Sign-On (SSO) Agent*
- *Install the WatchGuard Single Sign-On (SSO) Client (Optional)*

## Enable and Configure SSO

To enable and configure SSO from Policy Manager:

1. Select **Setup > Authentication > Authentication Settings**.  
*The Authentication Settings dialog box appears.*
2. Select the **Single Sign-On** tab.
3. Select the **Enable Single Sign-On (SSO) with Active Directory** check box.





4. In the **SSO Agent IP address** text box, type the IP address of your SSO Agent.
5. In the **Cache data for** text box, type or select the amount of time the SSO Agent caches data.
6. In the **SSO Exceptions** list, add or remove the IP addresses or ranges to exclude from SSO queries.

For more information about SSO exceptions, see the *Define SSO Exceptions* on page 321 section.

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

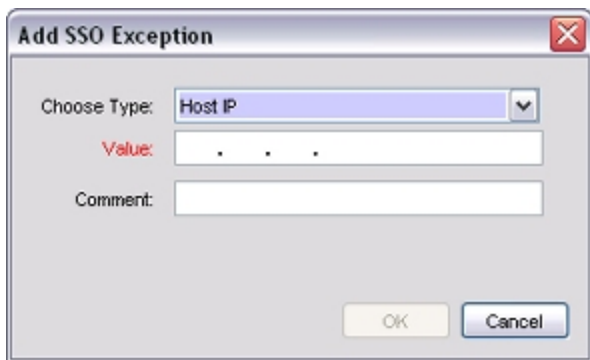
## Define SSO Exceptions

If your network includes devices with IP addresses that do not require authentication, such as network servers, print servers, or computers that are not part of the domain, or if you have users on your internal network who must manually authenticate to the authentication login portal, we recommend that you add their IP addresses to the SSO Exceptions list. Each time a connection attempt occurs from an IP address that is not in the SSO Exceptions list, the XTM device contacts the SSO agent to try to associate the IP address with a user name. This takes about 10 seconds. You can use the SSO Exceptions list to prevent this delay for each connection, to reduce unnecessary network traffic, and enable users to authenticate and connect to your network without delay.

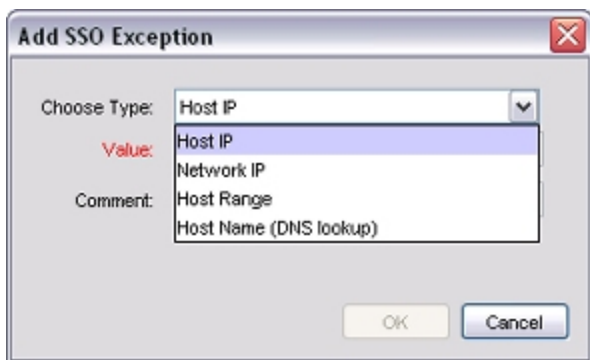
When you add an entry to the SSO Exceptions list, you can choose to add a host IP address, network IP address, subnet, host DNS name, or a host range.

To add an entry to the SSO Exceptions list:

1. Below the **SSO Exceptions** list, click **Add**.  
*The Add SSO Exception dialog box appears.*



2. From the **Choose Type** drop-down list, select the type of entry to add to the SSO Exceptions list:
  - Host IP
  - Network IP
  - Host Range
  - Host Name (DNS lookup)



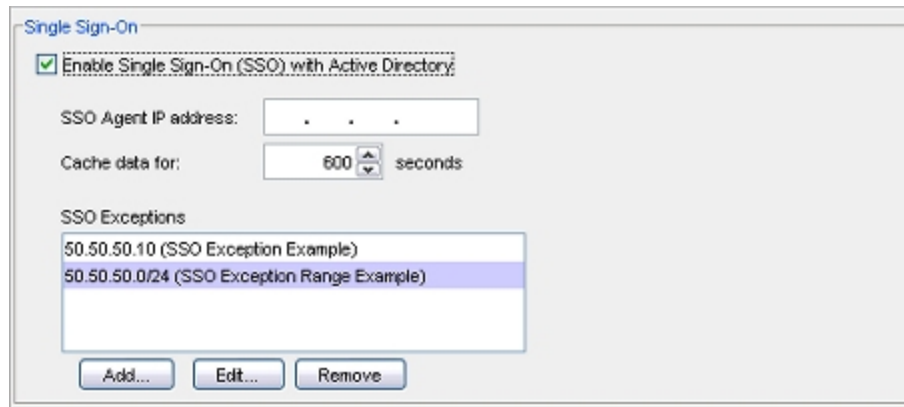
3. In the **Value** text box, type the IP address for the type you selected.
 

If you selected the type **Host Range**, in the **Value** text box, type the IP address at the start of the range.

In the **To** text box, type the IP address at the end of the range.
4. (Optional) In the **Comment** text box, type a description to include with this exception in the SSO Exceptions list.
 

*The Comment text box does not appear for the Host Name type.*
5. Click **OK**.
 

*The IP address or range appears in the SSO Exceptions list.*



To modify an entry in the SSO Exceptions list:

1. From the **SSO Exceptions** list, select an entry.
2. Click **Edit**.

*The Edit SSO exception IP dialog box appears.*

3. Change the settings for the SSO exception.
4. Click **OK**.

*The updated entry appears in the SSO Exceptions list.*



5. Click **OK**.

To remove an entry from the SSO Exceptions list:

1. From the **SSO Exceptions** list, select an entry.
  2. Click **Remove**.
- The selected entry is removed from the SSO Exceptions list.*
3. Click **OK**.

## Install and Configure the Terminal Services Agent

When you have more than one user who connects to your Terminal Server or Citrix server and then connects to your network or the Internet, it can be difficult to control the individual traffic flows from these users based on their user names or group memberships. This is because when one user authenticates to the XTM device, the XTM device maps that user to the IP address of the Terminal Server or Citrix server. Then, when another user sends traffic from the Terminal Server or Citrix server IP address, it appears to the XTM device that this traffic also came from the first user that authenticated. There is no way for the XTM device to distinguish which of the several users who are concurrently logged on to your Terminal Server or Citrix generated any particular traffic.

To make sure that your users are correctly identified, you must:

1. Install the WatchGuard Terminal Services Agent on your Terminal Server (2003 or 2008) or Citrix server.
2. Configure your XTM device to redirect users to the authentication page for authentication.
3. Enable Terminal Services settings in your XTM device configuration file.

After you complete these configuration settings, when each Terminal Server or Citrix server user authenticates to your XTM device, the XTM device sends the Terminal Services Agent a user session ID for each user who logs in. The Terminal Services Agent monitors traffic generated by individual users and reports the user session ID to the XTM device for each traffic flow generated by a Terminal Server or Citrix server client. Your XTM device can then correctly identify each user and apply the correct security policies to the traffic for each user, based on user or group names.

When you use the Terminal Services Agent, your XTM device can enforce policies based on user or group names only for traffic that is authenticated. If traffic comes to the XTM device without session ID information, the XTM device manages the traffic in the same way it manages any other traffic for which it does not have the username mapped to an IP address. If there is a policy in your configuration file that can process traffic from that IP address, the XTM device uses that policy to process the traffic. If there is no policy that matches the source IP address of the traffic, the XTM device uses the *unhandled packet* rules to process the traffic.

For more information about how to configure settings for unhandled packets, see *About Unhandled Packets* on page 532.

If you use the Terminal Services Agent, your XTM device cannot automatically redirect users to the authentication portal.

To enable your XTM device to correctly process system related traffic from the Terminal Server or Citrix server, the Terminal Services Agent uses a special user account named *Backend-Service*, which is part of the Terminal Services Agent. The Terminal Services Agent identifies the traffic generated by system processes (instead of user traffic) with the Backend-Service user account. You can add this user to the **Authorized Users and Groups** list in your XTM device configuration and then use it in a policy to allow traffic to and from your server. For example, you can add a custom packet filter policy that is similar to the default Outgoing policy. Configure the policy to use the TCP-UDP protocol and allow traffic from the *Backend-Service* user account to *Any-External*.

For more information about how to add the Backend-Service user account to your XTM device configuration, see *Use Authorized Users and Groups in Policies* on page 360. Make sure to select **Any** from the **Auth Server** drop-down list.

For more information about how to add a policy, see *Add Policies to Your Configuration* on page 372.

Make sure the updates on your Terminal Server or Citrix server are scheduled to run as the system, local service, or network service user account. The Terminal Services Agent recognizes these user account as the Backend-Service account and allows the traffic. If you schedule updates to run as a different user account, that user must manually authenticate to the application portal for the server to receive the updates. If that user is not authenticated to the authentication portal, the traffic is not allowed and the server does not receive the update.

Before you install the Terminal Services Agent on your Terminal Server or Citrix server, make sure that terminal services or remote desktop services is enabled on your server, and open ports 4131–4134.

You cannot use the Terminal Services Agent with Single Sign-On (SSO). For more information about SSO, see *About Single Sign-On (SSO)*.

The Terminal Services Agent cannot control ICMP, NetBIOS, or DNS traffic. It also does not control traffic to port 4100 for Firebox Authentication. To control this traffic, you must add specific policies to your XTM device configuration file to allow ICMP, NetBIOS, or DNS traffic, and to allow Firebox Authentication.

## Install the Terminal Services Agent

You can install the Terminal Services Agent on a Terminal Server or Citrix server with either a 32-bit or a 64-bit operating system. There are two versions of the Terminal Services Agent installer available: one for a 32-bit operating system and one for a 64-bit operating system. Make sure you select the correct installer for your operating system:

- 32-bit installer — **TO\_AGENT\_32.exe**
- 64-bit installer — **TO\_AGENT\_64.exe**

To install the Terminal Services Agent on your server:

1. Log in to the WatchGuard web site and go to the Software Downloads page.
2. Get the latest version of the TO Agent Installer (**TO\_AGENT\_32.exe** or **TO\_AGENT\_64.exe**) and copy it to the server where you have installed Terminal Services or a Citrix server.
3. Double-click the installer file to start the installer.  
*The TO Agent wizard appears.*
4. To start the wizard, click **Next**.
5. Complete the wizard to install the TO Agent on your server.
6. Reboot your Terminal Server or Citrix server.

## Configure the Terminal Services Agent

After you install the Terminal Services Agent or TO (Traffic Owner) Agent on your Terminal Server or Citrix server, you can use the TO Settings tool to configure the settings for the TO Agent.

Because it is not necessary for the TO Agent to monitor traffic that is not controlled by the XTM device, you can specify a single destination IP address or a range of destination IP addresses for traffic that you do not want the TO Agent to monitor.

1. Select **Start > All programs > WatchGuard > TO Agent > Set Tool**.  
*The TO Setting Tool dialog box appears, with the XTM Device Setting tab selected.*

2. In the **Device IP Address** text box, type the IP address of the XTM device interface for the Terminal Server.  
If the terminal server is on the *Trusted* interface, type the trusted interface IP address.  
If the Terminal Server is on the *External* interface, type the external interface IP address.
3. Click **OK**.
4. To create log messages for the TO Agent, select the **Enable logging of TO Agent processes** check box.
5. To add destinations for traffic that you do not want the TO Agent to monitor, select the **Destination Exception List** tab.
6. Click **Add**.  
*The Add Destination Exception dialog box appears.*
7. From the **Choose Type** drop-down list, select an option:
  - **Host IP Address**
  - **Network IP Address**
  - **IP Address Range**
8. If you select **Host IP Address**, type the **IP Address** for the exception.  
If you select **Network IP Address**, type the **IP Address** and **Mask** for the exception.  
If you select **IP Address Range**, type the **Range from** and **Range to** for the exception.
9. Click **Add**.  
*The information you specified appears in the Destination Exception List.*
10. To add more addresses to the **Destination Exception List**, repeat Steps 4–7.
11. To view the available log files for the TO Agent, click **View Logs**.  
*An Explorer window opens with the available log files you can review.*
12. Click **Close**.

For detailed steps to complete the Terminal Services configuration for your XTM device, see *Configure Terminal Services Settings* on page 326.

## Configure Terminal Services Settings

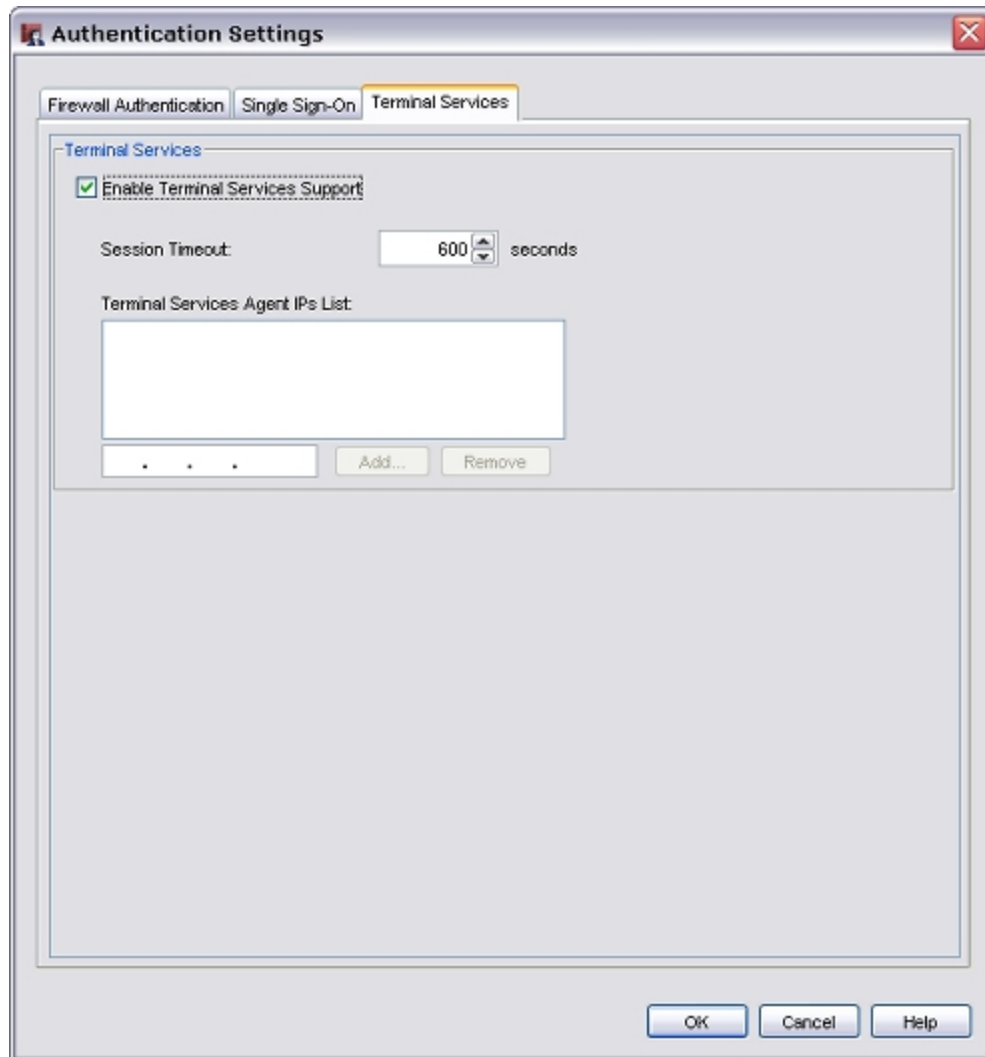
To enable your users to authenticate to your XTM device over a Terminal Server or Citrix server, you must configure the authentication settings for terminal services. When you configure these settings, you set the maximum length of time a session can be active and specify the IP address of your Terminal Server or Citrix server.

When you configure the Terminal Services Settings, if your users authenticate to your XTM device, the XTM device reports the actual IP address of each user who logs in. This enables your XTM device to correctly identify each user who logs in to your network, so the correct security policies can be applied to each user's traffic.

You can use any of your configured authentication server methods (for example, Firebox authentication, Active Directory, or RADIUS) with terminal services.

To configure Authentication Settings for terminal services:

1. *Open Policy Manager.*
2. Select **Setup > Authentication > Authentication Settings**.  
*The Authentication Settings dialog box appears with the Firewall Authentication tab selected by default.*
3. Select the **Terminal Services** tab.
4. Select the **Enable Terminal Services Support** check box.  
*The terminal services settings are enabled.*



5. In the **Session Timeout** text box, type or select the maximum length of time in seconds that the user can send traffic to the external network.  
If you select zero (0) seconds, the session does not expire and the user can stay connected for any length of time.
6. To add a Terminal Server or Citrix server to the **Terminal Services Agent IPs List** list, in the text box, type the IP address of the server and click **Add**.  
*The IP address appears in the Terminal Services Agent IPs List list.*
7. To remove a server IP address from the **Terminal Services Agent IPs List** list, select an IP address in the list and click **Remove**.
8. Click **OK**.

## Authentication Server Types

The Fireware XTM OS supports six authentication methods:

- *Configure Your XTM Device as an Authentication Server*
- *Configure RADIUS Server Authentication*
- *Configure VASCO Server Authentication*
- *Configure SecurID Authentication*
- *Configure LDAP Authentication*
- *Configure Active Directory Authentication*

You can configure one or more authentication server types for an XTM device. If you use more than one type of authentication server, users must select the authentication server type from a drop-down list when they authenticate.

### About Third-Party Authentication Servers

If you use a third-party authentication server, you do not have to keep a separate user database on the XTM device. You can configure a third-party server, install the authentication server with access to your XTM device, and put the server behind the device for security. You then configure the device to forward user authentication requests to that server. If you create a user group on the XTM device that authenticates to a third-party server, make sure you create a group on the server that has the same name as the user group on the device.

For detailed information about how to configure an XTM device for use with third-party authentication servers, see:

- *Configure RADIUS Server Authentication*
- *Configure VASCO Server Authentication*
- *Configure SecurID Authentication*
- *Configure LDAP Authentication*
- *Configure Active Directory Authentication*

### Use a Backup Authentication Server

You can configure a primary and a backup authentication server with any of the third-party authentication server types. If the XTM device cannot connect to the primary authentication server after three attempts, the primary server is marked as inactive and an alarm message is generated. The device then connects to the backup authentication server.

If the XTM device cannot connect to the backup authentication server, it waits ten minutes, and then tries to connect to the primary authentication server again. The inactive server is marked as active after the specified time interval is reached.

For detailed procedures to configure primary and backup authentication servers, see the configuration topic for your third-party authentication server.



# Configure Your XTM Device as an Authentication Server

If you do not use a third-party authentication server, you can use your XTM device as an authentication server, also known as Firebox authentication. When you configure Firebox authentication, you create users accounts for each user in your company, and then divide these users into groups for authentication. When you assign users to groups, make sure to associate them by their tasks and the information they use. For example, you can have an accounting group, a marketing group, and a research and development group. You can also have a new employee group with more controlled access to the Internet.

When you create a group, you set the authentication procedure for the users, the system type, and the information they can access. A user can be a network or one computer. If your company changes, you can add or remove users from your groups.

The Firebox authentication server is enabled by default. You do not have to enable it before you add users and groups.

## Types of Firebox Authentication

You can configure your XTM device to authenticate users with four different types of authentication:

- [Firewall Authentication](#)
- [Mobile VPN with PPTP Connections](#)
- [Mobile VPN with IPSec Connections](#)
- [Mobile VPN with SSL Connections](#)

When authentication is successful, the XTM device links these items:

- User name
- Firebox User group (or groups) of which the user is a member
- IP address of the computer used to authenticate
- Virtual IP address of the computer used to connect with Mobile VPN

## Firewall Authentication

To enable your users to authenticate, you create user accounts and groups. When a user authenticates with the XTM device, the user credentials and computer IP address are used to find whether a policy applies to the traffic that the computer sends and receives.

To create a Firebox user account:

1. *Define a New User for Firebox Authentication.*
2. *Define a New Group for Firebox Authentication* and put the new user in that group.
3. Create a policy that allows traffic only to or from a list of Firebox user names or groups.  
This policy is applied only if a packet comes from or goes to the IP address of the authenticated user.

To authenticate with an HTTPS connection to the XTM device over port 4100:

1. Open a web browser and go to `https://<IP address of a XTM device interface>:4100/`  
*The login page appears.*



2. Type the **Username** and **Password**.
3. From the **Domain** drop-down list, select the domain to use for authentication.  
*This option only appears if you can choose from more than one domain.*
4. Click **Login**.

If the credentials are valid, the user is authenticated.

Firewall authentication takes precedence over Single Sign-On, and replaces the user credentials and IP address from your Single Sign-On session with the user credentials and IP address you select for Firewall authentication. For more information about how to configure Single Sign-On, see *About Single Sign-On (SSO)* on page 312.

## Mobile VPN with PPTP Connections

When you activate Mobile VPN with PPTP on your XTM device, users included in the Mobile VPN with PPTP group can use the PPTP feature included in their computer operating system to make a PPTP connection to the device.

Because the XTM device allows the PPTP connection from any Firebox user that gives the correct credentials, it is important that you make a policy for PPTP sessions that includes only users you want to allow to send traffic over the PPTP session. You can also add a group or individual user to a policy that restricts access to resources behind the XTM device. The XTM device creates a pre-configured group called *PPTP-Users* for this purpose.

To configure a Mobile VPN with PPTP connection:

1. From Policy Manager, select **VPN > Mobile VPN > PPTP**.
2. Select the **Activate Mobile VPN with PPTP** check box.
3. Make sure the **Use RADIUS authentication to authenticate Mobile VPN with PPTP users** check box is not selected.

If this check box is selected, the RADIUS authentication server authenticates the PPTP session.

If you clear this check box, the XTM device authenticates the PPTP session.

The XTM device checks to see whether the user name and password the user types in the VPN connection dialog box match the user credentials in the Firebox User database that is a member of the PPTP-Users group.

*If the credentials supplied by the user match an account in the Firebox User database, the user is authenticated for a PPTP session.*

4. Create a policy that allows traffic only from or to a list of Firebox user names or groups.  
*The XTM device does not look at this policy unless traffic comes from or goes to the IP address of the authenticated user.*

## Mobile VPN with IPSec Connections

When you configure your XTM device to host Mobile VPN with IPSec sessions, you create policies on your device and then use the Mobile VPN with IPSec client to enable your users to access your network. After the XTM device is configured, each client computer must be configured with the Mobile VPN with IPSec client software.

When the user's computer is correctly configured, the user makes the Mobile VPN connection. If the credentials used for authentication match an entry in the Firebox User database, and if the user is in the Mobile VPN group you create, the Mobile VPN session is authenticated.

To set up authentication for Mobile VPN with IPSec:

1. *Configure a Mobile VPN with IPSec Connection.*
2. *Install the Mobile VPN with IPSec Client Software.*

## Mobile VPN with SSL Connections

You can configure the XTM device to host Mobile VPN with SSL sessions. When the XTM device is configured with a Mobile VPN with SSL connection, users included in the Mobile VPN with SSL group can install and use the Mobile VPN with SSL client software to make an SSL connection.

Because the XTM device allows the SSL connection from any of your users who give the correct credentials, it is important that you make a policy for SSL VPN sessions that includes only users you want to allow to send traffic over SSL VPN. You can also add these users to a Firebox User Group and make a policy that allows traffic only from this group. The XTM device creates a pre-configured group called *SSLVPN-Users* for this purpose.

To configure a Mobile VPN with SSL connection:

1. From Policy Manager, select **VPN > Mobile VPN > SSL**.  
*The Mobile VPN with SSL Configuration dialog box appears.*
2. *Configure the XTM Device for Mobile VPN with SSL.*

## Define a New User for Firebox Authentication

You can use Policy Manager to specify which users can authenticate to your XTM device.

1. Select **Setup > Authentication > Authentication Servers**.  
*The Authentication Servers dialog box appears.*



2. On the **Firebox** tab, in the **Users** section, click **Add**.  
*The Setup Firebox User dialog box appears.*

3. Type the **Name** and (optional) a **Description** of the new user.
4. Type and confirm the **Passphrase** you want the person to use to authenticate.


**Note** When you set this passphrase, the characters are masked and it does not appear in simple text again. If you lose the passphrase, you must set a new passphrase.

5. In the **Session Timeout** text box, type or select the maximum length of time the user can send traffic to the external network.

The minimum value for this setting is one (1) seconds, minutes, hours, or days. The maximum value is 365 days.

6. In the **Idle Timeout** text box, type or select the length of time the user can stay authenticated when idle (not passing any traffic to the external network).

The minimum value for this setting is one (1) seconds, minutes, hours, or days. The maximum value is 365 days.

7. To add a user to a Firebox Authentication Group, select the user name in the **Available** list.
8. Click  to move the name to the **Member** list.  
Or, you can double-click the user name in the **Available** list.  
*The user is added to the user list. You can then add more users.*
9. To close the **Setup Firebox User** dialog box, click **OK**.  
*The Firebox Users tab appears with a list of the new users.*

## Define a New Group for Firebox Authentication

You can use Policy Manager to specify which user groups can authenticate to your XTM device.

1. Select **Setup > Authentication > Authentication Servers**.


*The Authentication Servers dialog box appears.*

2. Select the **Firebox** tab.

3. In the **User Groups** section, click **Add**.

*The Setup Firebox Group dialog box appears.*



4. Type a name for the group.
5. (Optional) Type a description for the group.
6. To add a user to the group, select the user name in the **Available** list. Click  to move the name to the **Member** list.  
*You can also double-click the user name in the Available list.*
7. After you add all necessary users to the group, click **OK**.

You can now configure policies and authentication with these users and groups, as described in *Use Authorized Users and Groups in Policies* on page 360.

# Configure RADIUS Server Authentication

RADIUS (Remote Authentication Dial-In User Service) authenticates the local and remote users on a company network. RADIUS is a client/server system that keeps the authentication information for users, remote access servers, VPN gateways, and other resources in one central database.

For more information on RADIUS authentication, see *How RADIUS Server Authentication Works* on page 337.

## Authentication Key

The authentication messages to and from the RADIUS server use an authentication key, not a password. This authentication key, or shared secret, must be the same on the RADIUS client and server. Without this key, there is no communication between the client and server.

## RADIUS Authentication Methods

For web and Mobile VPN with IPsec or SSL authentication, RADIUS supports only PAP (Password Authentication Protocol) authentication.

For authentication with PPTP, RADIUS supports only MSCHAPv2 (Microsoft Challenge-Handshake Authentication Protocol version 2).

For authentication with WPA Enterprise and WPA2 Enterprise authentication methods, RADIUS supports the EAP (Extensible Authentication Protocol) framework.

## Before You Begin

Before you configure your XTM device to use your RADIUS authentication server, you must have this information:


- Primary RADIUS server — IP address and RADIUS port
- Secondary RADIUS server (optional) — IP address and RADIUS port
- Shared secret — Case-sensitive password that is the same on the XTM device and the RADIUS server
- Authentication methods — Set your RADIUS server to allow the authentication method your XTM device uses: PAP, MS CHAP v2, WPA Enterprise, WPA2 Enterprise, or WPA/WPA2 Enterprise

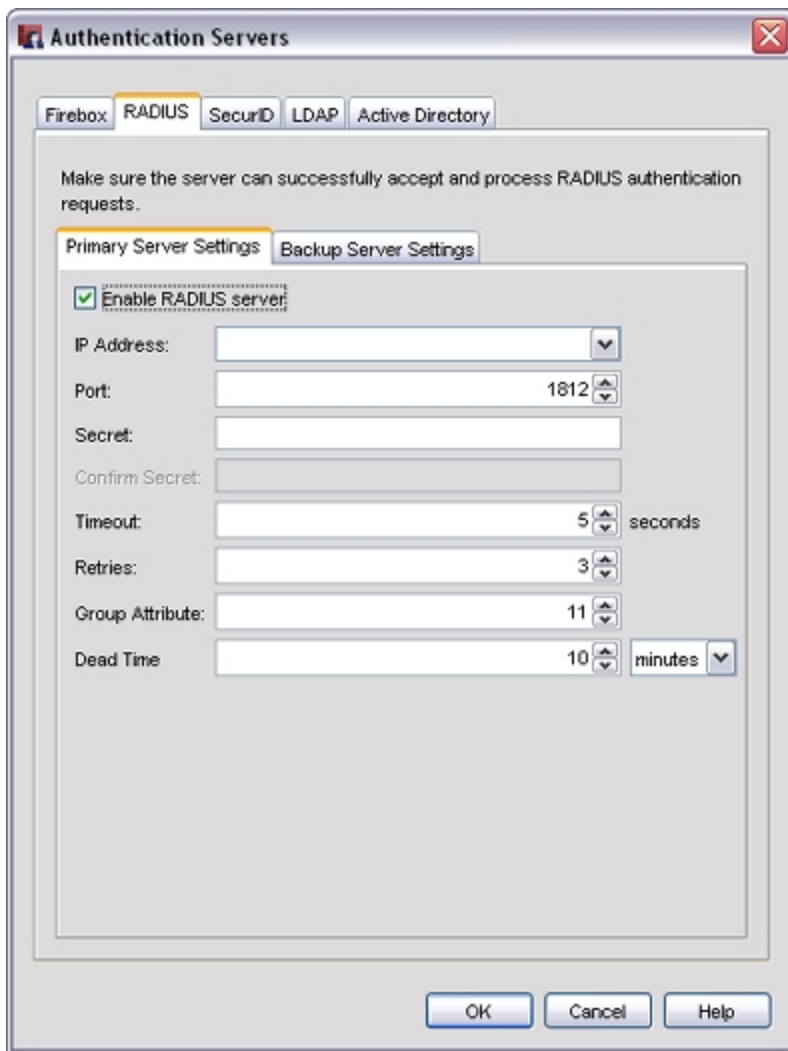
## Use RADIUS Server Authentication with Your XTM Device

To use RADIUS server authentication with your XTM device, you must:

- Add the IP address of the XTM device to the RADIUS server as described in the documentation from your RADIUS vendor.
- Enable and specify the RADIUS server in your XTM device configuration.
- Add RADIUS user names or group names to your policies.

To enable and specify the RADIUS server(s) in your configuration, from Policy Manager:

1. Click .  
Or, select **Setup > Authentication > Authentication Servers**.  
*The Authentication Servers dialog box appears.*
2. Select the **RADIUS** tab.



3. Select the **Enable RADIUS server** check box.
4. In the **IP Address** text box, type the IP address of the RADIUS server.
5. In the **Port** text box, make sure that the port number RADIUS uses for authentication appears. The default port number is 1812. Older RADIUS servers might use port 1645.
6. In the **Secret** text box, type the shared secret between the XTM device and the RADIUS server. The shared secret is case-sensitive, and it must be the same on the XTM device and the RADIUS server.
7. In the **Confirm Secret** text box, type the shared secret again.
8. Type or select the **Timeout** value.

The timeout value is the amount of time the XTM device waits for a response from the authentication server before it tries to connect again.

9. In the **Retries** text box, type or select the number of times the XTM device tries to connect to the authentication server (the timeout is specified above) before it reports a failed connection for one authentication attempt.
10. In the **Group Attribute** text box, type or select an attribute value. The default group attribute is FilterID, which is RADIUS attribute **11**.



The group attribute value is used to set the attribute that carries the User Group information. You must configure the RADIUS server to include the Filter ID string with the user authentication message it sends to the XTM device. For example, *engineerGroup* or *financeGroup*. This information is then used for access control. The XTM device matches the FilterID string to the group name configured in the XTM device policies.

11. In the **Dead Time** text box, type or select the amount of time after which an inactive server is marked as active again. Select **minutes** or **hours** from the drop-down list to change the duration.

After an authentication server has not responded for a period of time, it is marked as inactive. Subsequent authentication attempts will not try this server until it is marked as active again.

12. To add a backup RADIUS server, select the **Backup Server Settings** tab, and select the **Enable a backup RADIUS server** check box.
13. Repeat Steps 4–11 to configure the backup server. Make sure the shared secret is the same on the primary and backup RADIUS server.

For more information, see *Use a Backup Authentication Server* on page 328.

14. Click **OK**.
15. *Save the Configuration File.*

## How RADIUS Server Authentication Works

RADIUS is a protocol that was originally designed to authenticate remote users to a dial-in access server. RADIUS is now used in a wide range of authentication scenarios. RADIUS is a client-server protocol, with the XTM device as the client and the RADIUS server as the server. (The RADIUS client is sometimes called the Network Access Server or NAS.) When a user tries to authenticate, the XTM device sends a message to the RADIUS server. If the RADIUS server is properly configured to have the XTM device as a client, RADIUS sends an *accept* or *reject* message back to the XTM device (the Network Access Server).

When the XTM device uses RADIUS for an authentication attempt:

1. The user tries to authenticate, either through a browser-based HTTPS connection to the XTM device over port 4100, or through a connection using Mobile VPN with PPTP or IPSec. The XTM device reads the user name and password.
2. The XTM device creates a message called an Access-Request message and sends it to the RADIUS server. The XTM device uses the RADIUS shared secret in the message. The password is always encrypted in the Access-Request message.
3. The RADIUS server makes sure that the Access-Request message is from a known client (the XTM device). If the RADIUS server is not configured to accept the XTM device as a client, the server discards the Access-Request message and does not send a message back.
4. If the XTM device is a client known to the RADIUS server and the shared secret is correct, the server looks at the authentication method requested in the Access-Request message.
5. If the Access-Request message uses an allowed authentication method, the RADIUS server gets the user credentials from the message and looks for a match in a user database. If the user name and password match an entry in the database, the RADIUS server can get additional information about the user from the user database (such as remote access approval, group membership, logon hours, and so on).
6. The RADIUS server checks to see whether it has an access policy or a profile in its configuration that matches all the information it has about the user. If such a policy exists, the server sends a response.

7. If any of the previous conditions fail, or if the RADIUS server has no matching policy, it sends an Access-Reject message that shows authentication failure. The RADIUS transaction ends and the user is denied access.
8. If the Access-Request message meets all the previous conditions, RADIUS sends an Access-Accept message to the XTM device.
9. The RADIUS server uses the shared secret for any response it sends. If the shared secret does not match, the XTM device rejects the RADIUS response.

To see diagnostic log messages for authentication, *Set the Diagnostic Log Level* and change the log level for the **Authentication** category.

10. The XTM device reads the value of any FilterID attribute in the message. It connects the user name with the FilterID attribute to put the user in a RADIUS group.
11. The RADIUS server can put a large amount of additional information in the Access-Accept message. The XTM device ignores most of this information, such as the protocols the user is allowed to use (such as PPP or SLIP), the ports the user can access, idle timeouts, and other attributes.
12. The XTM device only requires the FilterID attribute (RADIUS attribute number 11). The FilterID is a string of text that you configure the RADIUS server to include in the Access-Accept message. This attribute is necessary for the XTM device to assign the user to a RADIUS group, however, it can support some other Radius attributes such as Session-Timeout (RADIUS attribute number 27) and Idle-Timeout (RADIUS attribute number 28).

For more information on RADIUS groups, see the subsequent section.

## About RADIUS Groups

When you configure RADIUS authentication, you can set the Group Attribute number. Fireware XTM reads the Group Attribute number from Policy Manager to tell which RADIUS attribute carries RADIUS group information. Fireware XTM recognizes only RADIUS attribute number 11, FilterID, as the Group Attribute. When you configure the RADIUS server, do not change the Group Attribute number from its default value of 11.

When the XTM device gets the Access-Accept message from RADIUS, it reads the value of the FilterID attribute and uses this value to associate the user with a RADIUS group. (You must manually configure the FilterID in your RADIUS configuration.) Thus, the value of the FilterID attribute is the name of the RADIUS group where the XTM device puts the user.

The RADIUS groups you use in Policy Manager are not the same as the Windows groups defined in your domain controller, or any other groups that exist in your domain user database. A RADIUS group is only a logical group of users the XTM device uses. Make sure you carefully select the FilterID text string. You can make the value of the FilterID match the name of a local group or domain group in your organization, but this is not necessary. We recommend you use a descriptive name that helps you remember how you defined your user groups.

## Practical Use of RADIUS Groups

If your organization has many users to authenticate, you can make your XTM device policies easier to manage if you configure RADIUS to send the same FilterID value for many users. The XTM device puts those users into one logical group so you can easily administer user access. When you make a policy in Policy Manager that allows only authenticated users to access a network resource, you use the RADIUS Group name instead of adding a list of many individual users.

For example, when Mary authenticates, the FilterID string RADIUS sends is *Sales*, so the XTM device puts Mary in the *Sales* RADIUS group for as long as she is authenticated. If users John and Alice subsequently authenticate, and RADIUS puts the same FilterID value *Sales* in the Access-Accept messages for John and Alice, then Mary, John, and Alice are all in the *Sales* group. You can make a policy in Policy Manager that allows the group *Sales* to access a resource.

You can configure RADIUS to return a different FilterID, such as *IT Support*, for the members of your internal support organization. You can then make a different policy to allow *IT Support* users to access resources.

For example, you might allow the *Sales* group to access the Internet using a Filtered-HTTP policy. Then you can filter their web access with WebBlocker. A different policy in Policy Manager can allow the *IT Support* users to access the Internet with the Unfiltered-HTTP policy, so that they access the web without WebBlocker filtering. You use the RADIUS group name (or user names) in the **From** field of a policy to show which group (or which users) can use the policy.

## Timeout and Retry Values

An authentication failure occurs when no response is received from the primary RADIUS server. After three authentication attempts fail, Fireware XTM uses the secondary RADIUS server. This process is called *failover*.

**Note** *This number of authentication attempts is not the same as the Retry number. You cannot change the number of authentication attempts before failover occurs.*

The XTM device sends an Access-Request message to the first RADIUS server in the list. If there is no response, the XTM device waits the number of seconds set in the **Timeout** box, and then it sends another Access-Request. This continues for the number of times indicated in the **Retry** box (or until there is a valid response). If there is no valid response from the RADIUS server, or if the RADIUS shared secret does not match, Fireware XTM counts this as one failed authentication attempt.

After three authentication attempts fail, Fireware XTM uses the secondary RADIUS server for the next authentication attempt. If the secondary server also fails to respond after three authentication attempts, Fireware XTM waits ten minutes for an administrator to correct the problem. After ten minutes, Fireware XTM tries to use the primary RADIUS server again.

## WPA and WPA2 Enterprise Authentication

To add another layer of security when your users connect to your wireless network, you can enable enterprise authentication methods on your XTM wireless device. When you configure an enterprise authentication method, the client must have the correct authentication method configured to successfully connect to the XTM device. The XTM wireless device then sends authentication requests to the configured authentication server (RADIUS server or Firebox-DB). If the authentication method information is not correct, the user cannot connect to the device, and is not allowed access to your network.

In Fireware XTM v11.4 and later, the available enterprise authentication methods are WPA Enterprise and WPA2 Enterprise. These authentication methods are based on the IEEE 802.1X standard, which uses the EAP (Extensible Authentication Protocol) framework to enable user authentication to an external RADIUS server or to your XTM device (Firebox-DB). The WPA Enterprise and WPA2 Enterprise authentication methods are more secure than WPA/WPA2 (PSK) because users must first have the correct authentication method configured, and then authenticate with their own enterprise credentials instead of one shared key that is known by everyone who uses the wireless access point.

You can use the WPA Enterprise and WPA2 Enterprise authentication methods with XTM wireless devices. For more information about how to configure your XTM wireless device to use enterprise authentication, see *Set the Wireless Authentication Method* on page 196.

## Configure VASCO Server Authentication


VASCO server authentication uses the VACMAN Middleware or IDENTIKEY Server software to authenticate remote users on a company network through a RADIUS or web server environment. VASCO also supports multiple authentication server environments. The VASCO one-time password token system enables you to eliminate the weakest link in your security infrastructure—the use of static passwords.

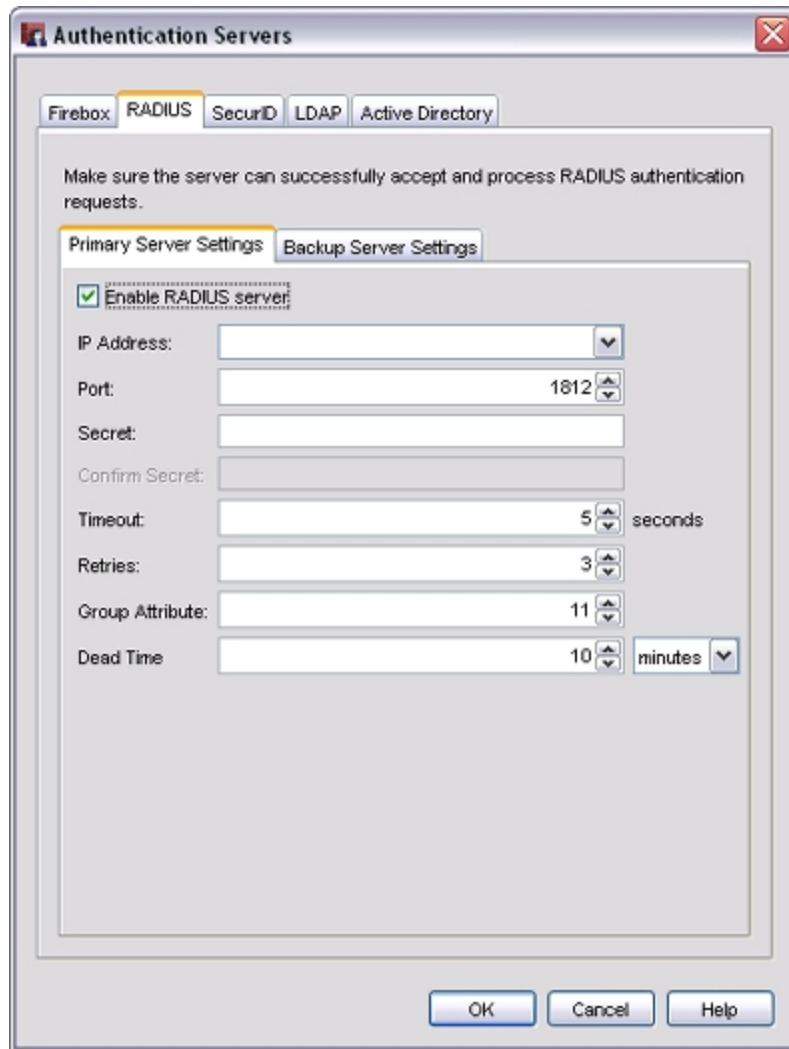
To use VASCO server authentication with your XTM device, you must:

- Add the IP address of the XTM device to the VACMAN Middleware or IDENTIKEY server, as described in the documentation from your VASCO vendor.
- Enable and specify the VACMAN Middleware or IDENTIKEY server in your XTM device configuration.
- Add user names or group names to the policies in Policy Manager.

To configure VASCO server authentication, use the RADIUS server settings. The **Authentication Servers** dialog box does not have a separate tab for VACMAN Middleware or IDENTIKEY servers.

From Policy Manager:

1. Click .  
Or, select **Setup > Authentication > Authentication Servers**.  
*The Authentication Servers dialog box appears.*
2. Select the **RADIUS** tab.



3. To enable the VACMAN Middleware or IDENTIKEY server, select the **Enable RADIUS server** check box.
4. In the **IP Address** text box, type the IP address of the VACMAN Middleware or IDENTIKEY server.
5. In the **Port** text box, make sure that the port number VASCO uses for authentication appears. The default port number is 1812.
6. In the **Secret** text box, type the shared secret between the XTM device and the VACMAN Middleware or IDENTIKEY server.  
The shared secret is case-sensitive, and it must be the same on the XTM device and the server.
7. In the **Confirm Secret** text box, type the shared secret again.
8. In the **Timeout** text box, type or select the amount of time the XTM device waits for a response from the authentication server before it tries to connect again.
9. In the **Retries** text box, type or select the number of times the XTM device tries to connect to the authentication server before it reports a failed connection for one authentication attempt.
10. Type or select the **Group Attribute** value. The default group attribute is FilterID, which is VASCO attribute **11**.

The group attribute value is used to set which attribute carries the user group information. You must configure the VASCO server to include the Filter ID string with the user authentication message it sends to the XTM device. For example, *engineerGroup* or *financeGroup*. This information is then used for access control. The XTM device matches the FilterID string to the group name configured in the XTM device policies.

11. In the **Dead Time** text box, type or select the amount of time after which an inactive server is marked as active again. Select **minutes** or **hours** from the drop-down list to change the duration.

After an authentication server has not responded for a period of time, it is marked as inactive. Subsequent authentication attempts do not try to connect to this server until it is marked as active again.

12. To add a backup VACMAN Middleware or IDENTIKEY server, select the **Backup Server Settings** tab, and select the **Enable a backup RADIUS server** check box.
13. Repeat Steps 4–11 to configure the backup server. Make sure the shared secret is the same on the primary and secondary VACMAN Middleware or IDENTIKEY server.


For more information, see *Use a Backup Authentication Server* on page 328.

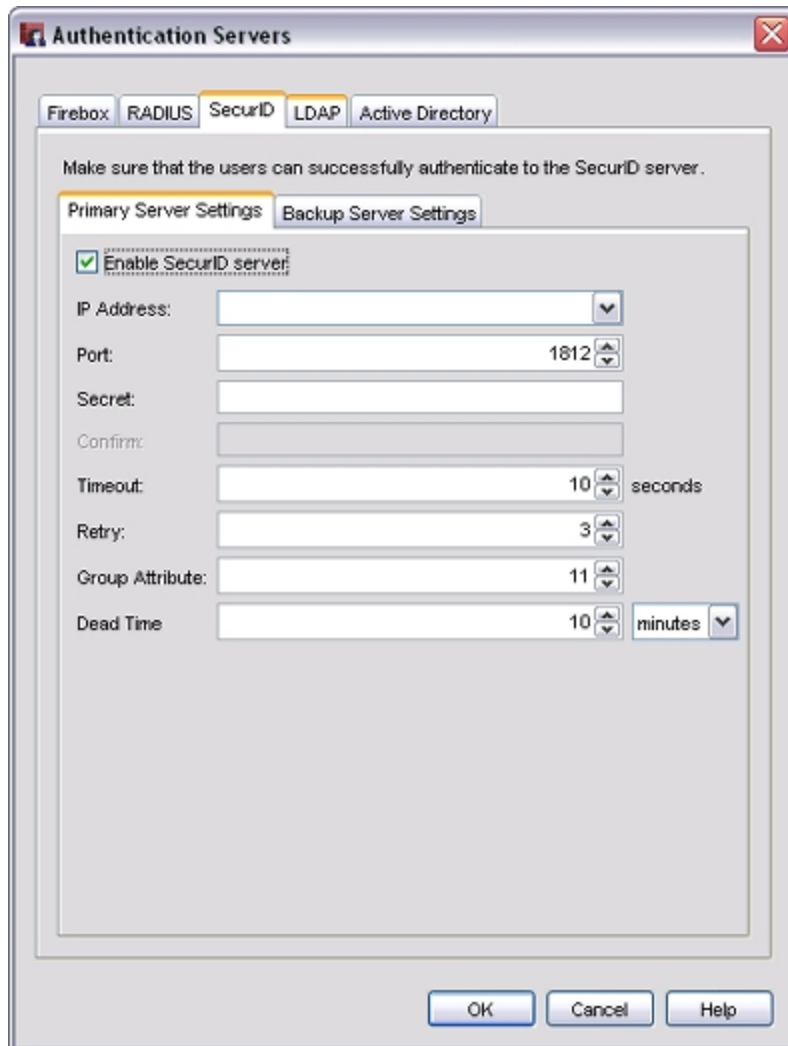
14. Click **OK**.
15. *Save the Configuration File.*

## Configure SecurID Authentication

To use SecurID authentication, you must configure the RADIUS, VASCO, and ACE/Server servers correctly. The users must also have an approved SecurID token and a PIN (personal identification number). Refer to the RSA SecurID documentation for more information.

From Policy Manager:

1. Click .  
Or, select **Setup > Authentication > Authentication Servers**.  
*The Authentication Servers dialog box appears.*
2. Select the **SecurID** tab.



The screenshot shows the 'Authentication Servers' dialog box with the 'SecurID' tab selected. The dialog box has a title bar with a close button. Below the title bar are tabs for 'Firebox', 'RADIUS', 'SecurID', 'LDAP', and 'Active Directory'. The 'SecurID' tab is active. Below the tabs is a message: 'Make sure that the users can successfully authenticate to the SecurID server.' There are two sub-tabs: 'Primary Server Settings' (selected) and 'Backup Server Settings'. Under 'Primary Server Settings', there is a checked checkbox for 'Enable SecurID server'. Below this are several fields: 'IP Address' (a text box with a dropdown arrow), 'Port' (a spinner box set to 1812), 'Secret' (a text box), 'Confirm' (a text box), 'Timeout' (a spinner box set to 10 with the unit 'seconds'), 'Retry' (a spinner box set to 3), 'Group Attribute' (a spinner box set to 11), and 'Dead Time' (a spinner box set to 10 with the unit 'minutes'). At the bottom of the dialog box are three buttons: 'OK', 'Cancel', and 'Help'.

3. Select the **Enable SecurID server** check box.
4. In the **IP Address** text box, type the IP address of the SecurID server.
5. Click the **Port** field up or down arrow to set the port number to use for SecurID authentication.  
The default number is 1812.

6. In the **Secret** text box, type the shared secret between the XTM device and the SecurID server. The shared secret is case-sensitive and must be the same on the XTM device and the SecurID server.
7. In the **Confirm** text box, type the shared secret again.
8. In the **Timeout** text box, type or select the amount of time that the XTM device waits for a response from the authentication server before it tries to connect again.
9. In the **Retry** text box, type or select the number of times the XTM device tries to connect to the authentication server before it reports a failed connection for one authentication attempt.
10. In the **Group Attribute** text box, type or select the group attribute value. We recommend that you do not change this value.

The group attribute value is used to set the attribute that carries the user group information. When the SecurID server sends a message to the XTM device that a user is authenticated, it also sends a user group string. For example, *engineerGroup* or *financeGroup*. This information is then used for access control.

11. In the **Dead Time** text box, type or select the amount of time after which an inactive server is marked as active again. Select **minutes** or **hours** from the adjacent drop-down list to change the duration.

After an authentication server has not responded for a period of time, it is marked as inactive. Subsequent authentication attempts do not use this server until it is marked as active again, after the dead time value is reached.

12. To add a backup SecurID server, select the **Backup Server Settings** tab, and select the **Enable a backup SecurID server** check box.
13. Repeat Steps 4–11 to configure the backup server. Make sure the shared secret is the same on the primary and backup SecurID servers.

For more information, see *Use a Backup Authentication Server* on page 328.

14. Click **OK**.
15. *Save the Configuration File.*




## Configure LDAP Authentication

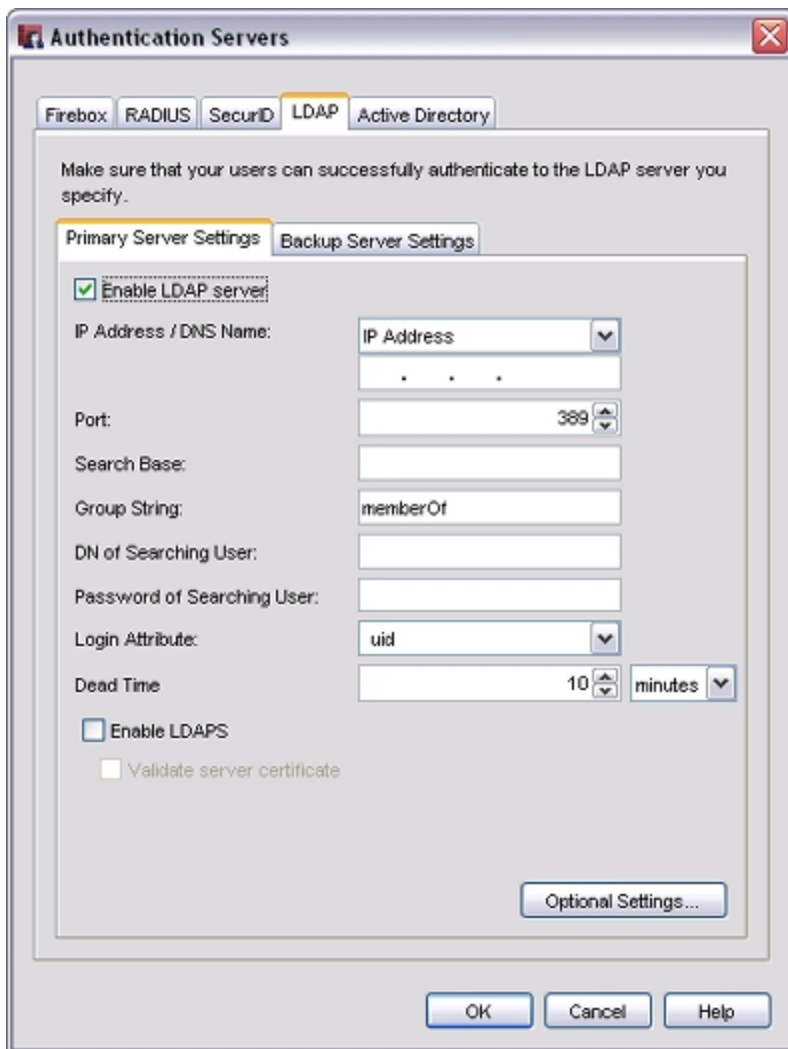
You can use an LDAP (Lightweight Directory Access Protocol) authentication server to authenticate your users with the XTM device. LDAP is an open-standard protocol for using online directory services, and it operates with Internet transport protocols, such as TCP. Before you configure your XTM device for LDAP authentication, make sure you check the documentation from your LDAP vendor to see if your installation supports the *memberOf* (or equivalent) attribute. When you configure your primary and backup LDAP server settings, you can select whether to specify the IP address or the DNS name of your LDAP server.

If your users authenticate with the LDAP authentication method, their distinguished names (DN) and passwords are not encrypted. To use LDAP authentication and encrypt user credentials, you can select the LDAPS (LDAP over SSL) option. When you use LDAPS, the traffic between the LDAP client on your XTM device and your LDAP server is secured by an SSL tunnel. When you enable this option, you can also choose whether to enable the LDAPS client to validate the LDAP server certificate, which prevents man-in-the-middle attacks. If you choose to use LDAPS and you specify the DNS name of your server, make sure the search base you specify includes the DNS name of your server. The standard LDAPS port is 636. For Active Directory Global Catalog queries, the SSL port is 3269.

When you configure the LDAP authentication method, you set a search base to specify where in the authentication server directories the XTM device can search for an authentication match. For example, if your user accounts are in an OU (organizational unit) you refer to as *accounts* and your domain name is *example.com*, your search base is `ou=accounts,dc=example,dc=com`.

From Policy Manager:

1. Click .  
Or, select **Setup > Authentication > Authentication Servers**.  
*The Authentication Servers dialog box appears.*
2. Select the **LDAP** tab.
3. Select the **Enable LDAP server** check box  
*The LDAP server settings are enabled.*



3. From the **IP Address/DNS Name** drop-down list, select whether to use the IP address or DNS name to contact your primary LDAP server.
4. In the **IP Address/DNS Name** text box, type the IP address or DNS name of the primary LDAP server for the XTM device to contact with authentication requests.  
The LDAP server can be located on any XTM device interface. You can also configure your device to use an LDAP server on a remote network through a VPN tunnel.
5. In the **Port** text box, select the TCP port number for the XTM device to use to connect to the LDAP server. The default port number is 389.  
If you enable LDAPS, you must select port 636.
6. In the **Search Base** text box, type the search base settings in the standard format: ou=organizational unit,dc=first part of distinguished server name,dc=any part of the distinguished server name that appears after the dot.  
For example: ou=accounts,dc=example,dc=com
7. In the **Group String** text box, type the group string attribute.

This attribute string holds user group information on the LDAP server. On many LDAP servers, the default group string is *uniqueMember*; on other servers, it is *member*.

8. In the **DN of Searching User** text box, type the distinguished name (DN) for a search operation.  
You can add any user DN with the privilege to search LDAP/Active Directory, such as *Administrator*. Some administrators create a new user that only has searching privileges for use in this field.
9. In the **Password of Searching User** text box, type the password associated with the distinguished name for a search operation.
10. In the **Login Attribute** text box, type the LDAP login attribute to use for authentication.  
The login attribute is the name used for the bind to the LDAP database. The default login attribute is *uid*. If you use *uid*, the **DN of Searching User** and the **Password of Searching User** text boxes can be empty.
11. In the **Dead Time** text box, type or select the amount of time after which an inactive server is marked as active again. Select **minutes** or **hours** from the adjacent drop-down list to set the duration.  
After an authentication server has not responded for a period of time, it is marked as inactive. Subsequent authentication attempts do not try this server until it is marked as active again.
12. To enable secure SSL connections to your LDAP server, select the **Enable LDAPS** check box.
13. To verify the certificate of the LDAP server is valid, select the **Validate server certificate** check box.
14. To specify optional attributes for the primary LDAP server, click **Optional Settings**.  
For more information about how to configure optional settings, see the subsequent section.
15. To add a backup LDAP server, select the **Backup Server Settings** tab, and select the **Enable a backup LDAP server** check box.
16. Repeat Steps 3–14 to configure the backup server. Make sure the shared secret is the same on the primary and backup LDAP servers.  
For more information, see *Use a Backup Authentication Server* on page 328.
17. Click **OK**.
18. *Save the Configuration File.*

## About LDAP Optional Settings

Fireware XTM can get additional information from the directory server (LDAP or Active Directory) when it reads the list of attributes in the server's search response. This lets you use the directory server to assign extra parameters to the authenticated user sessions, such as timeouts and Mobile VPN with IPsec address assignments. Because the data comes from LDAP attributes associated with individual user objects, you are not limited to the global settings in Policy Manager. You can set these parameters for each individual user.

For more information, see *Use Active Directory or LDAP Optional Settings* on page 356.

## Configure Active Directory Authentication

Active Directory is the Microsoft® Windows-based application of an LDAP directory structure. Active Directory lets you expand the concept of domain hierarchy used in DNS to an organizational level. It keeps information and settings for an organization in a central, easy-to-access database. You can use an Active Directory authentication server to enable your users to authenticate to the XTM device with their current network credentials. You must configure both your XTM device and the Active Directory server for Active Directory authentication to work correctly.

When you configure Active Directory authentication, you can specify one or more Active Directory domains that your users can select when they authenticate. For each domain, you can add up to two Active Directory servers: one primary server and one backup server. If the first server you add fails, the second server is used to complete authentication requests. When you add an Active Directory server, you can select whether to specify the IP address or the DNS name of each server.


If you configure more than one Active Directory domain and you use Single Sign-On (SSO), to enable your users to select from the available Active Directory domains and authenticate, your users must install the SSO client. For more information, see *About Single Sign-On (SSO)* on page 312 and *Install the WatchGuard Single Sign-On (SSO) Client* on page 319.

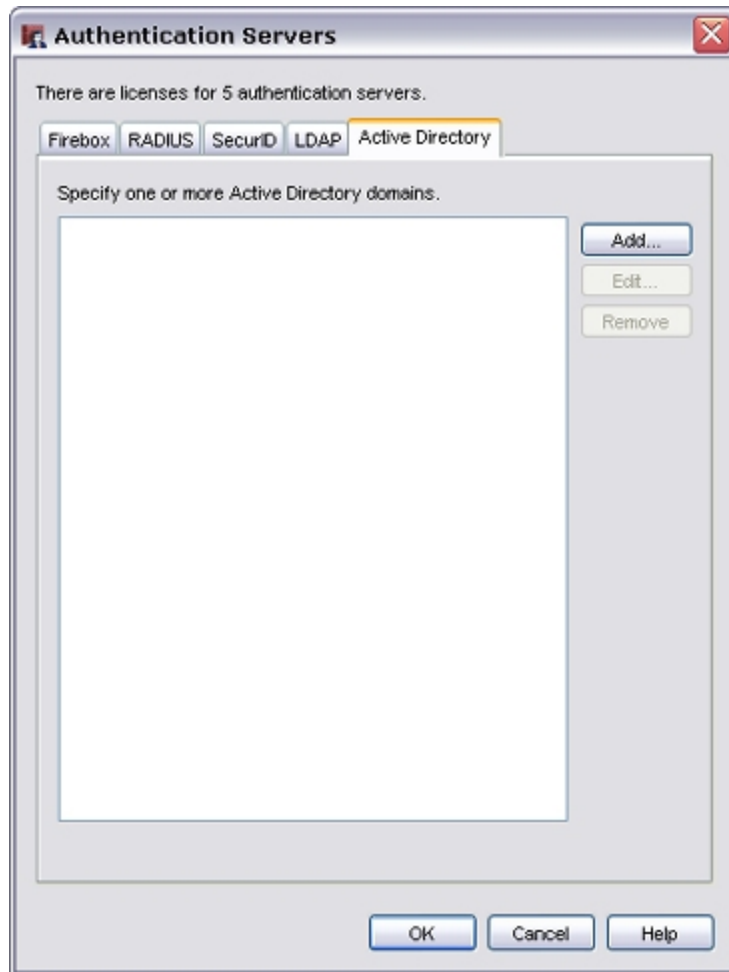
If your users authenticate with the Active Directory authentication method, their distinguished names (DN) and passwords are not encrypted. To use Active Directory authentication and encrypt user credentials, you can select the LDAPS (LDAP over SSL) option. When you use LDAPS, the traffic between the LDAPS client on your XTM device and your Active Directory server is secured by an SSL tunnel. When you enable this option, you can also choose whether to enable the LDAPS client to validate the Active Directory server certificate. If you choose to use LDAPS and you specify the DNS name of your server, make sure the search base you specify includes the DNS name of your server.

The Active Directory server can be located on any XTM device interface. You can also configure your XTM device to use an Active Directory server available through a VPN tunnel. For more information, see *Authentication to an Active Directory Server Through a BOVPN Tunnel*.

Before you begin, make sure your users can successfully authenticate to your Active Directory server. You can then use Policy Manager to configure your XTM device. You can add, edit, or delete the Active Directory domains and servers defined in your configuration.

### Add an Active Directory Authentication Domain and Server

1. Click .  
Or, select **Setup > Authentication > Authentication Servers**.  
*The Authentication Servers dialog box appears.*
2. Select the **Active Directory** tab.  
*The Active Directory settings appear.*



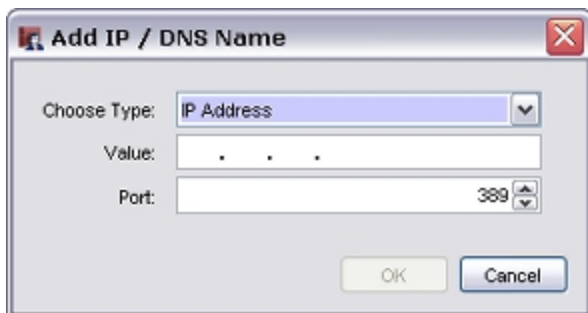
3. Click **Add**.

*The Add Active Directory Domain dialog box appears.*



4. In the **Domain Name** text box, type the domain name to use for this Active Directory server.
5. Click **Add**.

The *Add IP/DNS Name* dialog box appears.



6. From the **Choose Type** drop-down list, select **IP Address** or **DNS Name**.
7. In the **Value** text box, type the IP address or DNS name of this Active Directory server.
8. In the **Port** text box, type or select the TCP port number for the device to use to connect to the Active Directory server.

The default port number is 389. If you enable LDAPS, you must select port 636.

If your Active Directory server is a global catalog server, it can be useful to change the default port. For more information, see *Change the Default Port for the Active Directory Server* on page 355.

9. Click **OK**.

*The IP address or DNS name you added appears in the Add Active Directory Domain dialog box.*

10. To add another Active Directory server to this domain, repeat Steps 3–9. You can add up to two servers.

Make sure the shared secret is the same on all the Active Directory servers you specify.

For more information, see *Use a Backup Authentication Server* on page 328.

**Add Active Directory Domain**

Make sure that your users can successfully authenticate to the Active Directory servers you specify.

Domain Name:

IP Address / DNS Name:

IP / DNS	Port
50.50.50.1	389
50.50.50.11	389

Buttons: Add... Remove

Search Base:

Group String:

DN of Searching User:

Password of Searching User:

Login Attribute:

Dead Time:

Enable LDAPS  
 Validate server certificate

Optional Settings...

OK Cancel Help

11. In the **Search Base** text box, type the location in the directory to begin the search.

The standard format for the search base setting is: *ou=<name of organizational unit>,dc=<first part of the distinguished server name>,dc=<any part of the distinguished server name that appears after the dot>*.

To limit the directories on the authentication server where the XTM device can search for an authentication match, you can set a search base. We recommend that you set the search base to the root of the domain. This enables you to find all users and all groups to which those users belong.

For more information, see *Find Your Active Directory Search Base* on page 354.

12. In the **Group String** text box, type the attribute string that is used to hold user group information on the Active Directory server. If you have not changed your Active Directory schema, the group string is always `memberOf`.
13. In the **DN of Searching User** text box, type the distinguished name (DN) for a search operation.

If you keep the login attribute of `sAMAccountName`, you do not have to type anything in this text box.

If you change the login attribute, you must add a value in the **DN of Searching User** text box. You can use any user DN with the privilege to search LDAP/Active Directory, such as *Administrator*. However, a weaker user DN with only the privilege to search is usually sufficient.

14. In the **Password of Searching User** text box, type the password associated with the distinguished name for a search operation.
15. In the **Login Attribute** text box, type or select an Active Directory login attribute to use for authentication.

The login attribute is the name used for the bind to the Active Directory database. The default login attribute is *sAMAccountName*. If you use *sAMAccountName*, you do not have to specify a value for the **DN of Searching User** and **Password of Searching User** settings.

16. In the **Dead Time** text box, type or select a time after which an inactive server is marked as active again.
17. From the **Dead Time** drop-down list, select **minutes** or **hours** to set the duration.

After an authentication server has not responded for a period of time, it is marked as inactive. Subsequent authentication attempts do not try this server until it is marked as active again.

18. To enable secure SSL connections to your Active Directory server, select the **Enable LDAPS** check box.
19. To verify the certificate of the Active Directory server is valid, select the **Validate server certificate** check box.
20. To specify optional attributes for the primary LDAP server, click **Optional Settings**.

For more information about how to configure optional settings, see the subsequent section.

21. To add another Active Directory domain, repeat Steps 3–20. Make sure the shared secret is the same on all the Active Directory domains you specify.
22. Click **OK**.
23. *Save the Configuration File.*

## About Active Directory Optional Settings

Fireware XTM can get additional information from the directory server (LDAP or Active Directory) when it reads the list of attributes in the server's search response. This lets you use the directory server to assign extra parameters to the authenticated user sessions, such as timeouts and Mobile VPN with IPsec address assignments. Because the data comes from LDAP attributes associated with individual user objects, you are not limited to the global settings in Policy Manager. You can set these parameters for each individual user.

For more information, see *Use Active Directory or LDAP Optional Settings* on page 356.

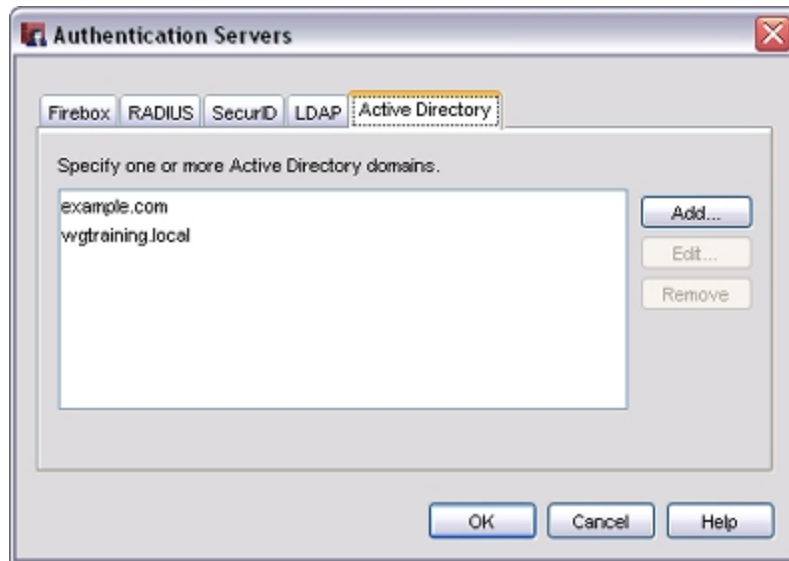
## Edit an Existing Active Directory Domain

When you edit an Active Directory domain, you cannot change the details of the Active Directory servers configured in the domain. Instead, you must add a new server. If there are two servers in the list, you must remove one of the servers before you can add a new one.

From the Authentication Servers dialog box:

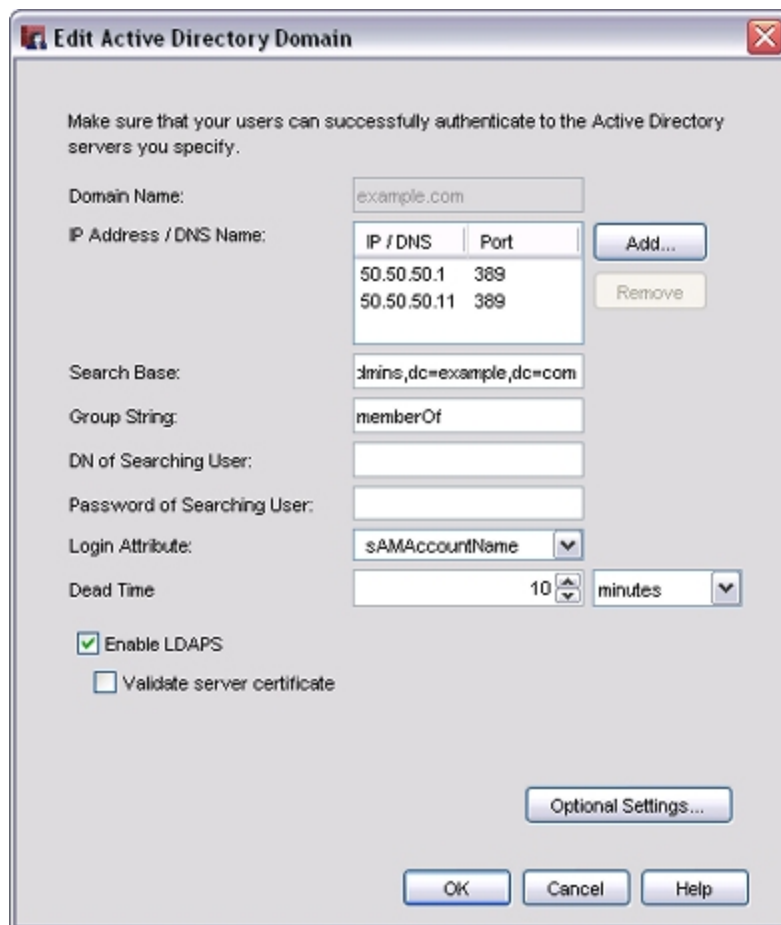
1. In the **Active Directory domains** list, select the server to change.





2. Click **Edit**.

*The Edit Active Directory Domain dialog box appears.*



3. To add an IP address or DNS name to the server for this domain, click **Add** and follow the instructions in Steps 5–9 of the previous section.
4. To remove an IP address or DNS name from the server for this domain, select the entry in the **IP Address / DNS Name** list and click **Remove**.
5. Update the settings for your Active Directory server.

## Delete an Active Directory Domain

From the **Authentication Servers** dialog box:

1. In the **Active Directory domains** list, select the domain to delete.
2. Click **Remove**.  
*A confirmation message appears.*
3. Click **Yes**.

## Find Your Active Directory Search Base

When you configure your XTM device to authenticate users with your Active Directory server, you add a *search base*. The search base is the place the search starts in the Active Directory hierarchical structure for user account entries. This can help to make the authentication procedure faster.

Before you begin, you must have an operational Active Directory server that contains account information for all users for whom you want to configure authentication on the XTM device.

From your Active Directory server:

1. Select **Start > Administrative Tools > Active Directory Users and Computers**.
2. In the **Active Directory Users and Computers** tree, find and select your domain name.
3. Expand the tree to find the path through your Active Directory hierarchy.

Domain name components have the format *dc=domain name component*, are appended to the end of the search base string, and are also comma-delimited.

For each level in your domain name, you must include a separate domain name component in your Active Directory search base. For example, if your domain name is *prefix.example.com*, the domain name component in your search base is *DC=prefix,DC=example,DC=com*.

To make sure that the Active Directory search can find any user object in your domain, specify the root of the domain. For example, if your domain name is *kunstlerandsons.com*, and you want the Active Directory search to find any user object in the entire domain, the search base string to add is:

```
dc=kunstlerandsons,dc=com.
```

If you want to limit the search to begin in some container beneath the root of the domain, specify the fully-qualified name of the container in comma-delimited form, starting with the name of the base container and progressing toward the root of the domain. For example, assume your domain in the tree looks like this after you expand it:



Also assume that you want the Active Directory search to begin in the **Sales** container that appears in the example. This enables the search to find any user object inside the **Sales** container, and inside any containers within the **Sales** container.

The search base string to add in the XTM device configuration is:

```
ou=sales,ou=accounts,dc=kunstlerandsons,dc=com
```

The search string is not case-sensitive. When you type your search string, you can use either uppercase or lowercase letters.

This search does not find user objects inside the **Development** or **Admins** containers, or inside the **BuiltIn**, **Computers**, **Domain Controllers**, **ForeignSecurityPrincipals**, or **Users** containers.

## DN of Searching User and Password of Searching User Fields

You must complete these fields only if you select an option for the **Login Attribute** that is different from the default value, *sAMAccountName*. Most organizations that use Active Directory do not change this. When you leave this field at the default *sAMAccountName* value, users supply their usual Active Directory login names for their user names when they authenticate. This is the name you see in the **User logon name** text box on the **Account** tab when you edit the user account in **Active Directory Users and Computers**.

If you use a different value for the **Login Attribute**, a user who tries to authenticate gives a different form of the user name. In this case, you must add *Searching User credentials* to your XTM device configuration.


## Change the Default Port for the Active Directory Server

If your WatchGuard device is configured to authenticate users with an Active Directory (AD) authentication server, it connects to the Active Directory server on the standard LDAP port by default, which is TCP port 389. If the Active Directory servers that you add to your WatchGuard device configuration are set up to be Active Directory global catalog servers, you can tell the WatchGuard device to use the global catalog port—TCP port 3268—to connect to the Active Directory server.

A *global catalog server* is a domain controller that stores information about all objects in the forest. This enables the applications to search Active Directory, but not have to refer to specific domain controllers that store the requested data. If you have only one domain, Microsoft recommends that you configure all domain controllers as global catalog servers.

If the primary or secondary Active Directory server you use in your WatchGuard device configuration is also configured as a global catalog server, you can change the port the WatchGuard device uses to connect to the Active Directory server to increase the speed of authentication requests. However, we do not recommend that you create additional Active Directory global catalog servers just to speed up authentication requests. The replication that occurs among multiple global catalog servers can use significant bandwidth on your network.

## Configure the XTM Device to Use the Global Catalog Port

1. From Policy Manager, click .  
Or, select **Setup > Authentication > Authentication Servers**.  
*The Authentication Servers dialog box appears.*
2. Select the **Active Directory** tab.
3. In the **Port** text box, clear the contents and type **3268**.
4. Click **OK**.
5. *Save the Configuration File.*

## Find Out if Your Active Directory Server is Configured as a Global Catalog Server

1. Select **Start > Administrative Tools > Active Directory Sites and Services**.
2. Expand the **Sites** tree and find the name of your Active Directory server.
3. Right-click **NTDS Settings** for your Active Directory server and select **Properties**.

If the **Global Catalog** check box is selected, the Active Directory server is configured to be a global catalog.

## Use Active Directory or LDAP Optional Settings

When Fireware XTM contacts the directory server (Active Directory or LDAP) to search for information, it can get additional information from the list of attributes in the search response returned by the server. This lets you use the directory server to assign extra parameters to the authenticated user session, such as timeouts and Mobile VPN address assignments. Because the data comes from LDAP attributes associated with individual user objects, you can set these parameters for each individual user and you are not limited to the global settings in Policy Manager.

## Before You Begin

To use these optional settings you must:

- Extend the directory schema to add new attributes for these items.
- Make the new attributes available to the object class that user accounts belong to.
- Give values to the attributes for the user objects that should use them.

Make sure you carefully plan and test your directory schema before you extend it to your directories. Additions to the Active Directory schema, for example, are generally permanent and cannot be undone. Use the Microsoft® web site to get resources to plan, test, and implement changes to an Active Directory schema. Consult the documentation from your LDAP vendor before you extend the schema for other directories.

## Specify Active Directory or LDAP Optional Settings

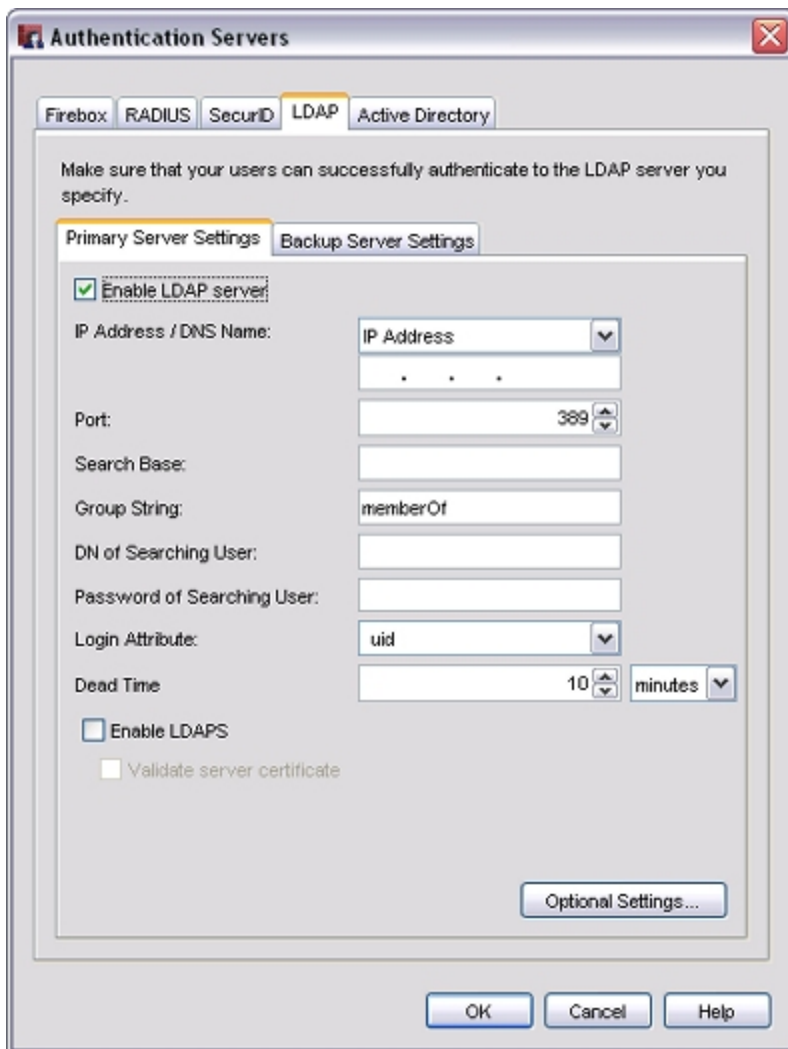
You can use Policy Manager to specify the additional attributes Fireware XTM looks for in the search response from the directory server.

1. Select **Setup > Authentication > Authentication Servers**.

*The Authentication Servers dialog box appears.*

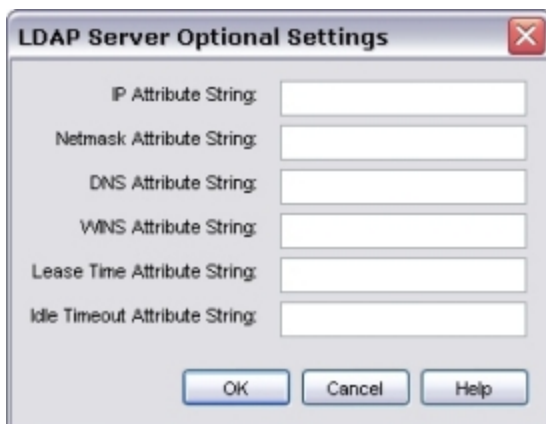


2. Click the **LDAP** tab or the **Active Directory** tab and make sure the server is enabled.



- 3. Click **Optional Settings**.

*The LDAP Server Optional Settings dialog box appears.*



- 4. Type the attributes you want to include in the directory search in the string fields.

*IP Attribute String*

*This field applies only to Mobile VPN clients.*

Type the name of the attribute for Fireware XTM to use to assign a virtual IP address to the Mobile VPN client. This must be a single-valued attribute and an IP address in decimal format. The IP address must be within the pool of virtual IP addresses you specify when you create the Mobile VPN Group.

If the XTM device does not see the IP attribute in the search response or if you do not specify an attribute in Policy Manager, it assigns the Mobile VPN client a virtual IP address from the virtual IP address pool you create when you make the Mobile VPN Group.

#### *Netmask Attribute String*

*This field applies only to Mobile VPN clients.*

Type the name of the attribute for Fireware XTM to use to assign a subnet mask to the Mobile VPN client's virtual IP address. This must be a single-valued attribute and a subnet mask in decimal format.

The Mobile VPN software automatically assigns a netmask if the XTM device does not see the netmask attribute in the search response or if you do not specify one in Policy Manager.

#### *DNS Attribute String*

*This field applies only to Mobile VPN clients.*

Type the name of the attribute Fireware XTM uses to assign the Mobile VPN client one or more DNS addresses for the duration of the Mobile VPN session. This can be a multi-valued attribute and must be a normal dotted-decimal IP address. If the XTM device does not see the DNS attribute in the search response, or if you do not specify an attribute in Policy Manager, it uses the WINS addresses you enter when you *Configure WINS and DNS Servers*.

#### *WINS Attribute String*

*This field applies only to Mobile VPN clients.*

Type the name of the attribute Fireware XTM should use to assign the Mobile VPN client one or more WINS addresses for the duration of the Mobile VPN session. This can be a multi-valued attribute and must be a normal dotted-decimal IP address. If the XTM device does not see the WINS attribute in the search response or if you do not specify an attribute in Policy Manager, it uses the WINS addresses you enter when you *Configure WINS and DNS Servers*.

#### *Lease Time Attribute String*

*This applies to Mobile VPN clients and to clients that use Firewall Authentication.*

Type the name of the attribute for Fireware XTM to use to control the maximum duration a user can stay authenticated (session timeout). After this amount of time, the user is removed from the list of authenticated users. This must be a single-valued attribute. Fireware XTM interprets the attribute's value as a decimal number of seconds. It interprets a zero value as *never time out*.

#### *Idle Timeout Attribute String*

*This applies to Mobile VPN clients and to clients that use Firewall Authentication.*

Type the name of the attribute Fireware XTM uses to control the amount of time a user can stay authenticated when no traffic is passed to the XTM device from the user (idle timeout). If no traffic passes to the device for this amount of time, the user is removed from the list of authenticated users. This must be a single-valued attribute. Fireware XTM interprets the attribute's value as a decimal number of seconds. It interprets a zero value as *never time out*.

5. Click **OK**.

*The attribute settings are saved.*

## Use a Local User Account for Authentication

Any user can authenticate as a Firewall user, PPTP user, or Mobile VPN user, and open a PPTP or Mobile VPN tunnel if PPTP or Mobile VPN is enabled on the XTM device. However, after authentication or a tunnel has been successfully established, users can send traffic through the VPN tunnel only if the traffic is allowed by a policy on the XTM device. For example, a Mobile VPN-only user can send traffic through a Mobile VPN tunnel. Even though the Mobile VPN-only user can authenticate and open a PPTP tunnel, he or she cannot send traffic through that PPTP tunnel.

If you use Active Directory authentication and the group membership for a user does not match your Mobile VPN policy, you can see an error message that says *Decrypted traffic does not match any policy*. If you see this error message, make sure that the user is in a group with the same name as your Mobile VPN group.

## Use Authorized Users and Groups in Policies

You can use specified user and group names when you create policies in Policy Manager. For example, you can define all policies to only allow connections for authenticated users. Or, you can limit connections on a policy to particular users.

The term *authorized users and groups* refers to users and groups that are allowed to access network resources.

## Define Users and Groups for Firebox Authentication

If you use your XTM device as an authentication server and want to define users and groups that authenticate to the XTM device, see *Define a New User for Firebox Authentication* on page 332 and *Define a New Group for Firebox Authentication* on page 334.

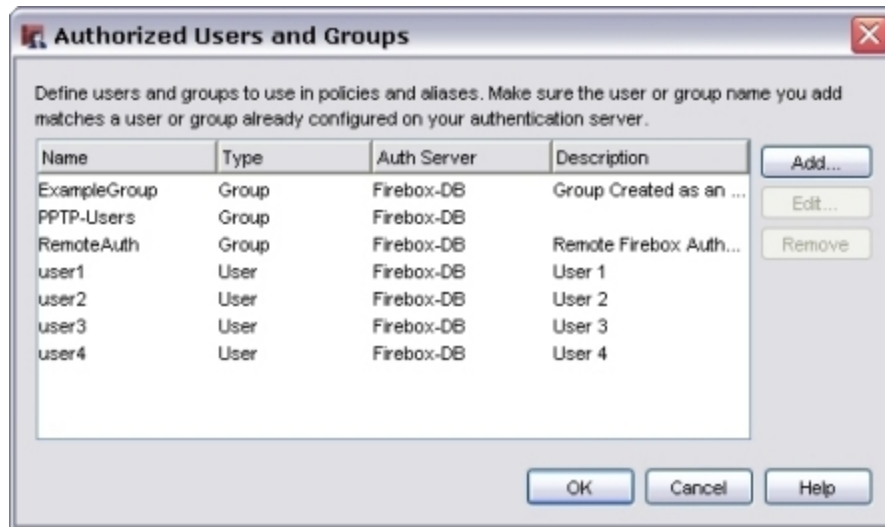
## Define Users and Groups for Third-Party Authentication

You can use Policy Manager to define the users and groups to use for third-party authentication. When you create a group, if you use more than one Active Directory domain for authentication, you must specify the domain that you want users in the group to use to authenticate.

1. Create a group on your third-party authentication server that contains all the user accounts on your system.
2. Select **Setup > Authentication > Authorized Users/Groups**.

*The Authorized Users and Groups dialog box appears.*





3. Click **Add**.

The *Define New Authorized User or Group* dialog box appears.



4. Type a user or group name you created on the authentication server.
5. (Optional) Type a description for the user or group.
6. Select **Group** or **User**.
7. From the **Auth Server** drop-down list, select your authentication server type.

Select **RADIUS** for authentication through a RADIUS or VACMAN Middleware server, or **Any** for authentication through any other server. For Active Directory authentication, select the specific domain to use for this user or group.

8. Click **OK**.

## Add Users and Groups to Policy Definitions

Any user or group that you want to use in your policy definitions must be added as an authorized user. All users and groups you create for Firebox authentication, and all Mobile VPN users, are automatically added to the list of authorized users and groups on the **Authorized Users and Groups** dialog box. You can add any users or groups from third-party authentication servers to the authorized user and group list with the previous procedure. You are then ready to add users and groups to your policy configuration.

1. From Policy Manager, select the **Firewall** tab.
2. Double-click a policy.  
*The Edit Policy Properties dialog box appears.*
3. On the **Policy** tab, below the **From** box, click **Add**.  
*The Add Address dialog box appears.*
4. Click **Add User**.  
*The Add Authorized Users or Groups dialog box appears.*



5. From the left **Type** drop-down list, select whether the user or group is authorized as a Firewall, PPTP, or SSL VPN user.

For more information on these authentication types, see *Types of Firebox Authentication* on page 329.

6. From the right **Type** drop-down list, select either **User** or **Group**.
7. If your user or group appears in the **Groups** list, select the user or group and click **Select**.  
*The Add Address dialog box reappears with the user or group in the Selected Members or Addresses box.*

Click **OK** to close the **Edit Policy Properties** dialog box.

8. If your user or group does not appear in the **Groups** list, see *Define a New User for Firebox Authentication* on page 332, *Define a New Group for Firebox Authentication* on page 334, or the previous *Define users and groups for third-party authentication* procedure, and add the user or group.

After you add a user or group to a policy configuration, WatchGuard System Manager automatically adds a WatchGuard Authentication policy to your XTM device configuration. Use this policy to control access to the authentication portal web page.

For instructions to edit this policy, see *Use Authentication to Restrict Incoming Traffic* on page 306.

# 13 Policies

---

## About Policies

The *security policy* of your organization is a set of definitions to protect your computer network and the information that goes through it. The XTM device denies all packets that are not specifically allowed. When you add a *policy* to your XTM device configuration file, you add a set of rules that tell the XTM device to allow or deny traffic based upon factors such as source and destination of the packet or the TCP/IP port or protocol used for the packet.

As an example of how a policy could be used, suppose the network administrator of a company wants to log in remotely to a web server protected by the XTM device. The network administrator manages the web server with a Remote Desktop connection. At the same time, the network administrator wants to make sure that no other network users can use Remote Desktop. To create this setup, the network administrator adds a policy that allows RDP connections only from the IP address of the network administrator's desktop computer to the IP address of the web server.

A policy can also give the XTM device more instructions on how to handle the packet. For example, you can define logging and notification settings that apply to the traffic, or use NAT (Network Address Translation) to change the source IP address and port of network traffic.

## Packet Filter and Proxy Policies

Your XTM device uses two categories of policies to filter network traffic: *packet filters* and *proxies*. A packet filter examines each packet's IP and TCP/UDP header. If the packet header information is legitimate, then the XTM device allows the packet. Otherwise, the XTM device drops the packet.

A proxy examines both the header information and the content of each packet to make sure that connections are secure. This is also called *deep packet inspection*. If the packet header information is legitimate and the content of the packet is not considered a threat, then the XTM device allows the packet. Otherwise, the XTM device drops the packet.

## Add Policies to Your XTM device

The XTM device includes many pre-configured packet filters and proxies that you can add to your configuration. For example, if you want a packet filter for all Telnet traffic, you add a pre-defined Telnet policy that you can modify for your network configuration. You can also make a custom policy for which you set the ports, protocols, and other parameters.

When you configure the XTM device with the Quick Setup Wizard, the wizard adds several packet filters: Outgoing (TCP-UDP), FTP, ping, and up to two WatchGuard management policies. If you have more software applications and network traffic for the XTM device to examine, you must:

- Configure the policies on your XTM device to let the necessary traffic through
- Set the approved hosts and properties for each policy
- Balance the requirement to protect your network against the requirements of your users to get access to external resources

We recommend that you set limits on outgoing access when you configure your XTM device.

**Note** *In all documentation, we refer to both packet filters and proxies as policies. Information on policies refers to both packet filters and proxies unless otherwise specified.*

## About Policy Manager

Fireware XTM Policy Manager is a WatchGuard software tool that lets you create, edit, and save configuration files. When you use Policy Manager, you see a version of your configuration file that is easy to examine and change.

For more information on how to open Policy Manager, see *Open Policy Manager* on page 366.

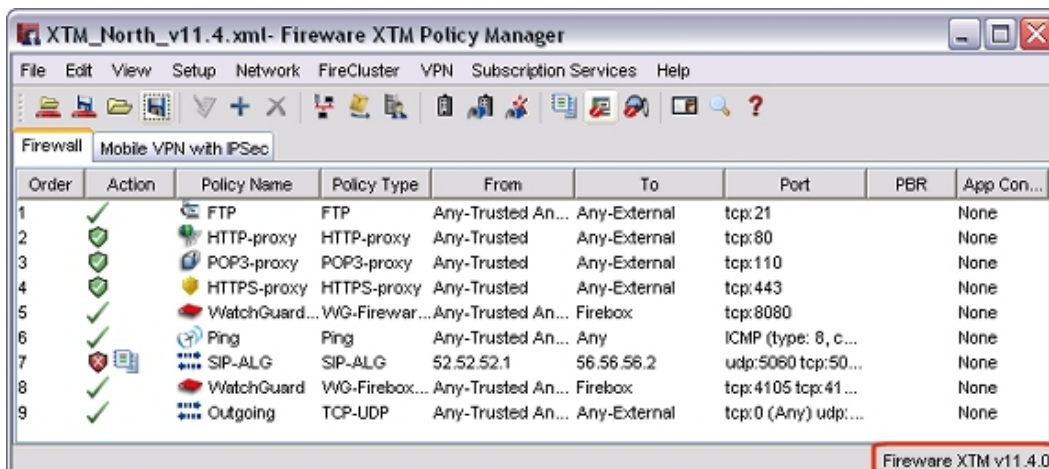
## Policy Manager Window

Policy Manager has two tabs: The **Firewall** tab and the **Mobile VPN with IPSec** tab.

- The **Firewall** tab includes policies that are used for general firewall traffic on the XTM device. It also includes BOVPN policies so you can see the order in which the XTM device examines network traffic and applies a policy rule. (To change the order, see *About Policy Precedence* on page 383.)
- The **Mobile VPN with IPSec** tab includes policies that are used with Mobile VPN with IPSec tunnels.

In Policy Manager, a list of the policies you have configured and their basic settings appear by default. You can also view the policies as a group of large icons to help you identify a policy visually. To switch between these two views, see *About Policy Manager Views* on page 367.

Policy Manager also includes basic information about the open configuration file at the bottom right of the window. Details include information about the management mode and the Fireware XTM OS version number for the configuration file you have open. The version number can help you identify whether the configuration file is for a Fireware XTM OS v11.0–11.3.x or a Fireware XTM OS v11.4 or later device.



## Policy Icons

Policy Manager contains icons for the policies that are defined on the XTM device. You can double-click the icon or its associated entry to edit the properties for that policy. The appearance of the icons shows their status and type:

- Enabled policies that allow traffic appear with a green check mark, or with a green bar and a check mark in Large Icons view.
- Enabled policies that deny traffic have a red X, or a red bar with an X in Large Icons view.
- Disabled policies have a black circle with a line, or a gray bar in Large Icons view.
- An icon with a shield symbol on the left side is a proxy policy.

The names of policies appear in color, based on policy type:

- Managed policies appear in gray with a white background.
- BOVPN policies (such as BOVPN-allow.out) appear in green with a white background.
- Mixed BOVPN and firewall policies (such as Ping or Any-PPTP) appear in blue with a white background.
- All other policies appear in black with a white background.

To change these default colors, see *Change Colors Used for Policy Manager Text* on page 369.



To find a specific policy in Policy Manager, see *Find a Policy by Address, Port, or Protocol* on page 371.

## Open Policy Manager


You open Policy Manager from WatchGuard System Manager. You can choose to open Policy Manager for a specific Firebox or XTM device, or you can open Policy Manager with a new configuration file.

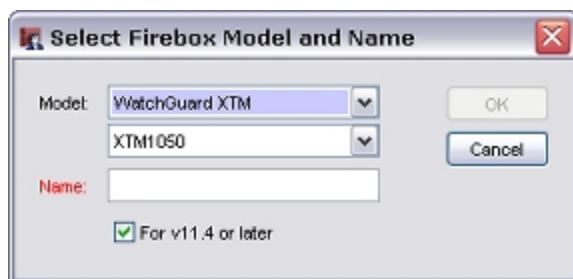
If the XTM device you select is a managed device, Policy Manager puts a lock on the device in WatchGuard System Manager to prevent simultaneous changes from a different user. The lock is released when you close Policy Manager, or if you open Policy Manager for a different device.

To open Policy Manager for a specific device:

1. Open WatchGuard System Manager.
2. Click  and connect to an XTM device.  
*The selected device appears in the Device Status tab.*
3. Select the XTM device and click .  
*Policy Manager appears with the current configuration file for the device.*

To open Policy Manager with a new configuration file:


1. Open WatchGuard System Manager.
2. Click .  
Or, select **Tools > Policy Manager**.  
*The Policy Manager dialog box appears.*
3. Select **Create a new configuration file for**.
4. From the **Firebox** drop-down list, select a type of device for the new configuration file.
5. Click **OK**.  
*The Select Firebox Model and Name dialog box appears.*




6. From the **Model** drop-down lists, select the model information for your XTM device.
7. In the **Name** text box, type a name for the new configuration file.
8. If the configuration file is for an XTM device that runs Fireware XTM OS v11.4 or later, make sure the **For v11.4 or later** check box is selected.  
If the configuration file is for an XTM device that runs Fireware XTM OS v11.3.x or earlier, clear the **For v11.4 or later** check box.
9. Click **OK**.

After Policy Manager is open, you can open an existing configuration file for any device. You can choose to connect to an XTM device and download the current configuration file for the device, or you can open a configuration file that is saved on your management computer.

To download the current configuration file for a device:

1. Click .  
Or, select **File > Open > Firebox**.  
*The Open Firebox dialog box appears.*
2. In the **Firebox Address or Name** text box, type the IP address or name of the device.
3. In the **Status Passphrase** text box, type the read-only passphrase for the device.
4. Click **OK**.

To open a saved configuration file:

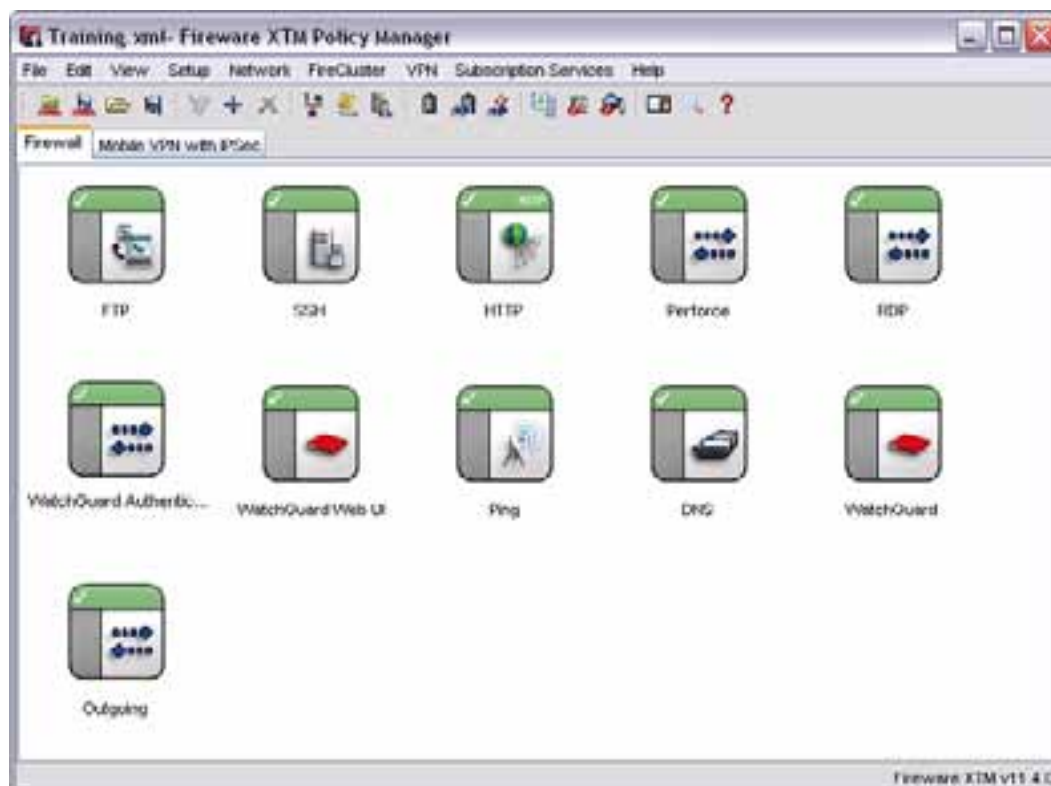
1. Click .  
Or, select **File > Open > Configuration File**.  
*The Open dialog box appears.*
2. Select the configuration file and click **Open**.  
*The selected configuration file opens in Policy Manager.*

## About Policy Manager Views

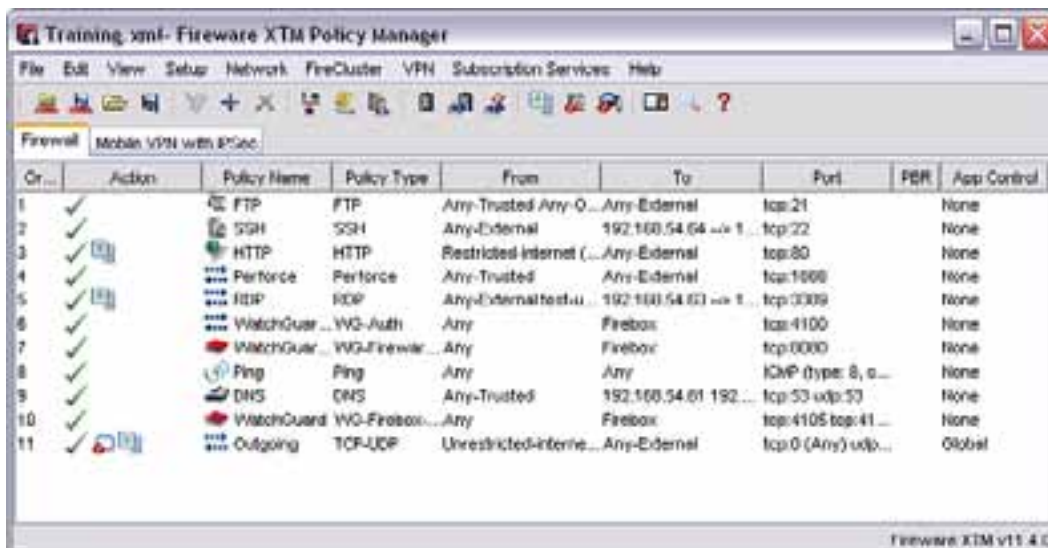
Policy Manager has two views: *Large Icons* and *Details*. The default Large Icons view shows each policy as an icon. In the Details view, each policy is a row of information divided among several columns. You can see configuration information, such as source and destination addresses, assigned ports, policy-based routing, and application control settings, as well as whether notification, scheduling, and QoS/Traffic Management are configured.

To change to the Details view:

Select **View > Details**.



*Large Icons View*



Details View

This information appears for each policy:

**Order**

The order in which the policies are sorted, and how traffic flows through the policies. Policy Manager automatically sorts policies from the most specific to the most general. If you want to switch to manual-order mode, select **View > Auto-order mode** so that the check mark disappears. Then, select the policy whose order you want to change and drag it to its new location.

For more information on policy order, see *About Policy Precedence*.

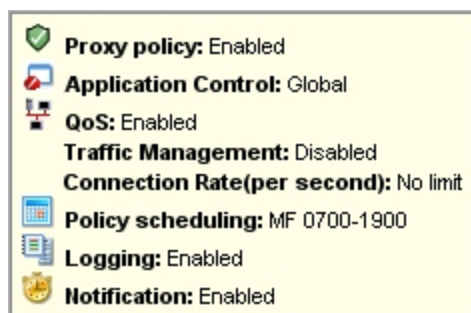
**Action**

The action taken by the policy for traffic that matches the policy definition. The symbols in this column also indicate whether the policy is a packet filter policy or a proxy policy, and the settings that are configured for the policy:

- — Packet filter policy; traffic is allowed
- — Packet filter policy; traffic is denied
- — Disabled packet filter policy
- — Proxy policy; traffic is allowed
- — Proxy policy; traffic is denied
- — Disabled proxy policy
- — Application Control is configured
- — Traffic Management/ QoS is configured
- — Scheduling is configured
- — Logging is enabled
- — Notification is enabled

To see the details about the icons that appear in the **Action** column for a policy, you can hover over the icons and the list of enabled actions and definitions appears.





#### *Policy Name*

Name of the policy, as defined in the **Name** text box in the **New Policy Properties** or **Edit Policy Properties** dialog box.

For more information, see *Add a Policy from the List of Templates* on page 374.

#### *Policy Type*

The protocol that the policy manages. Packet filters include the protocol name only. Proxies include the protocol name and *-proxy*. ALGs include the protocol name and *-ALG*.

#### *From*

The source addresses for this policy.

#### *To*

The destination addresses for this policy.

#### *Port*

Protocols and ports used by the policy.

#### *PBR*

The interface numbers that are used for failover in the policy-based routing settings for the policy.

#### *App Control*

The Application Control action enabled for the policy.

For more information, see *Enable Application Control in a Policy*.

## Change Colors Used for Policy Manager Text

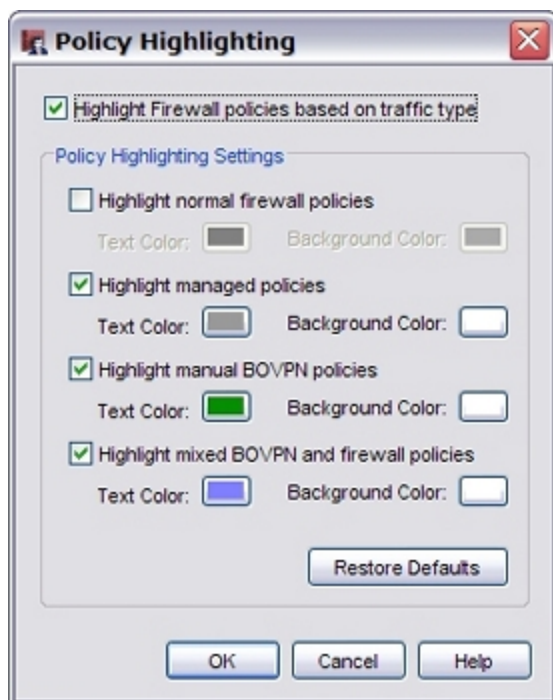
The default setup for Policy Manager is for the names of policies (or the entire row in Details view) to appear highlighted in color based on traffic type:

- Managed policies appear in gray with a white background.
- BOVPN policies (such as BOVPN-allow.out) appear in green with a white background.
- Mixed BOVPN and firewall policies (such as Ping or Any-PPTP) appear in blue with a white background.
- All other policies (normal policies) are not highlighted. They appear in black.

You can use default colors or colors that you select. You can also disable policy highlighting.

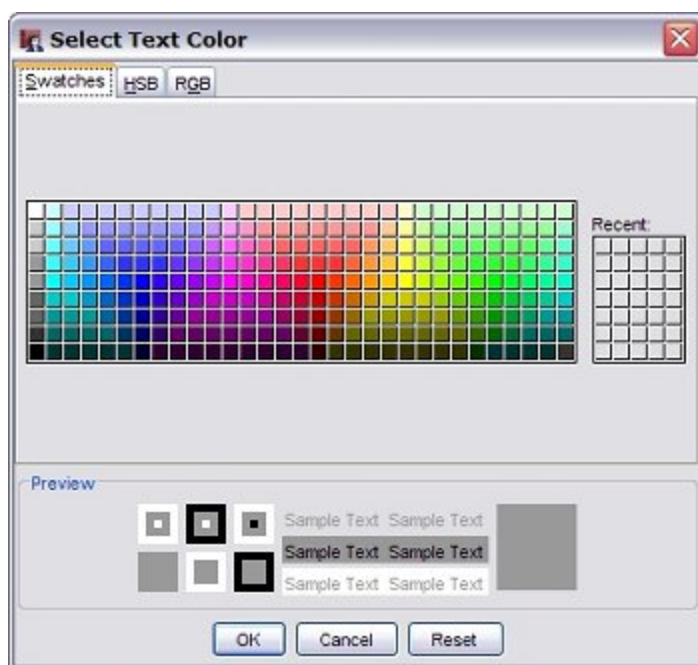
1. Select **View > Policy Highlighting**.

*The Policy Highlighting dialog box appears.*



2. To enable policy highlighting, select the **Highlight Firewall policies based on traffic type** check box. Clear this check box to disable policy highlighting.
3. To select different colors for the text or background of the policy names for normal, managed, BOVPN, or mixed policies, click the **Text Color** or **Background Color** block.

*The Select Text Color or Select Background Color dialog box appears.*



4. Click one of the three tabs, **Swatches**, **HSB**, or **RGB** to specify the color you want:
  - **Swatches** — Click one the small swatches of the available colors.
  - **HSB** — Select **H** (hue), **S** (saturation), or **B** (brightness) and then type or select the value for each setting.
  - **RGB** — Type or select the value for the **Red**, **Green**, or **Blue** settings.  
When you specify a color, a sample of the color appears in the **Sample** block at the bottom of the dialog box.
5. When you are satisfied with the color, click **OK**.
6. Click **OK** on the **Policy Highlighting** dialog box for the changes to take effect.

## Find a Policy by Address, Port, or Protocol

You can locate a policy in Policy Manager with the address, port, or protocol information for the policy.

1. Select **Edit > Find**.  
*The Find Policies dialog box appears.*



2. Select **Address**, **Port Number**, or **Protocol** to specify a policy component.
3. In the **Search all configured policies for** text box, type the string to search for.  
For address and protocol searches, Policy Manager performs a partial string search. You can type only a partial string. Policy Manager shows all policies that contain the string.
4. Click **Find**.  
*The policies that match the search criteria appear in the Policies found box .*
5. To edit a policy that is returned for a search, double-click the policy name.

## Add Policies to Your Configuration

To add a policy, you choose from the list of policy templates in Policy Manager. A policy template contains the policy name, a short description of the policy, and the protocol/port used by the policy.

- To see the list of policy types to choose from, see *See the List of Policy Templates* on page 372.
- To add one of the policies in the list to your configuration, see *Add a Policy from the List of Templates* on page 374.
- To see or modify the definition of a policy template, see *See Template Details and Modify Policy Templates* on page 376.
- To use the policy import/export function to copy policies from one XTM device to another, see *Import and Export Custom Policy Templates* on page 390. This is helpful if you manage several XTM devices and have custom policies for them.


The XTM device includes a default definition for each policy included in the XTM device configuration file. The default definition consists of settings that are appropriate for most installations. However, you can modify them for your particular business purposes, or if you want to include special policy properties such as Traffic Management actions and operating schedules.

After you add a policy to your configuration, you define rules to:

- Set allowed traffic sources and destinations
- Make filter rules
- Enable or disable the policy
- Configure properties such as Traffic Management, NAT, and logging

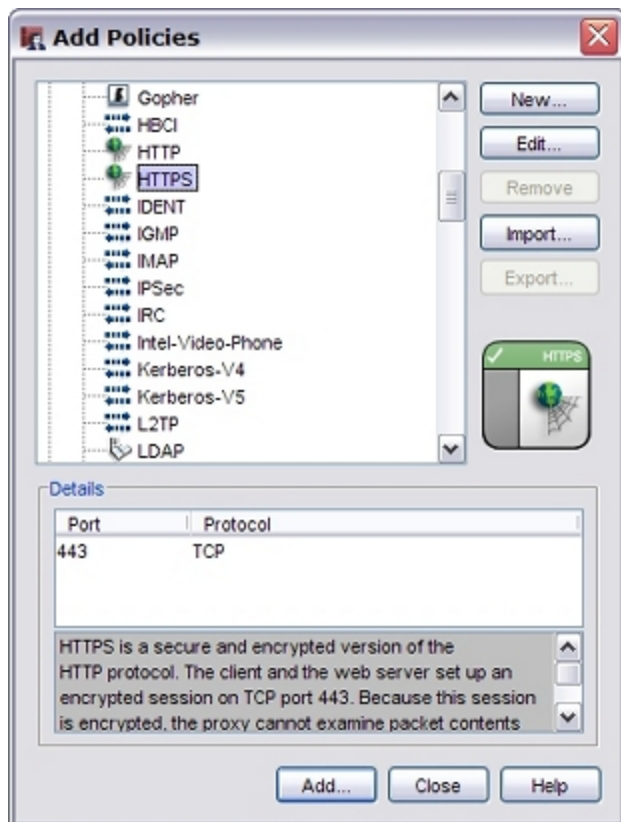
For more information on policy configuration, see *About Policy Properties* on page 391.

## See the List of Policy Templates

1. Click .  
Or, select **Edit > Add Policies**.  
*The Add Policies dialog box appears.*
2. Expand the **Packet Filters** or **Proxies** folder.  
*A list of templates for packet filters or proxies appears.*



3. To see basic information about a policy template, select it.  
*The icon for the policy appears at the right side of the dialog box and basic information about the policy appears in the Details section.*

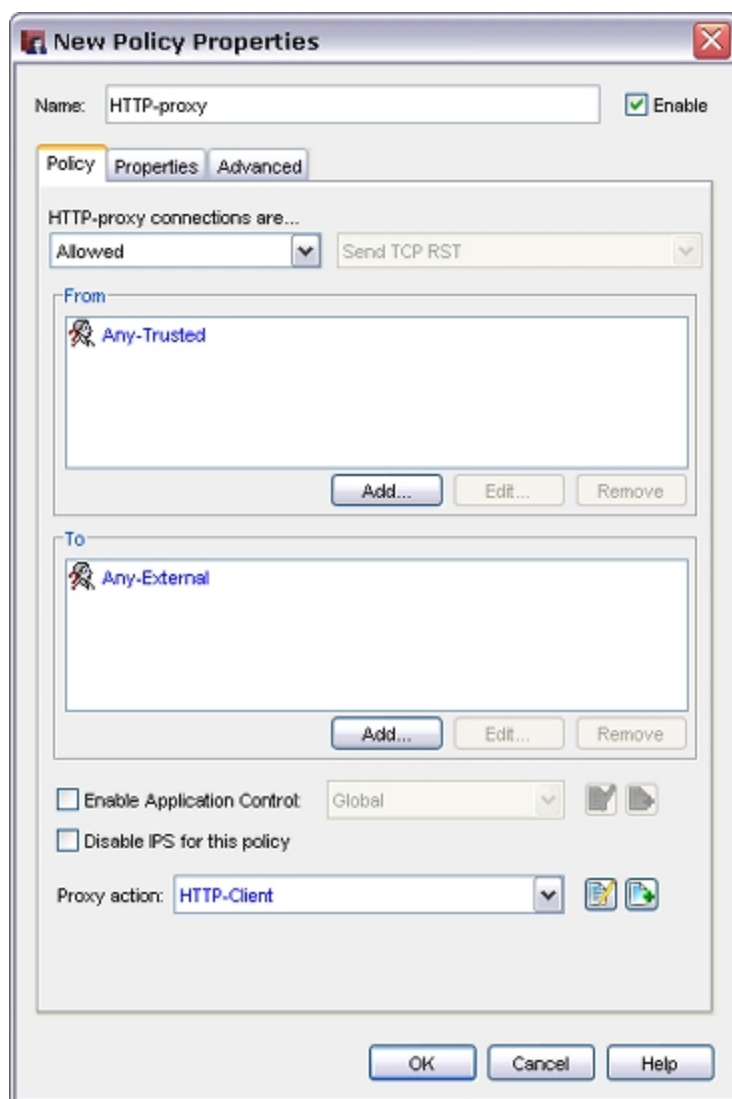


## Add a Policy from the List of Templates

Your XTM device includes a default definition for each policy included in the XTM device configuration. The default definition settings are appropriate for most installations, however, you can modify them to include special policy properties, such as QoS actions and operating schedules.

In the **Add Policies** dialog box:

1. Expand the **Packet Filters**, **Proxies**, or **Custom** folder.  
*A list of templates for packet filter or proxy policies appears.*
2. Select a policy and click **Add**.  
*The New Policy Properties dialog box appears, with the Policy tab selected.*



3. To change the name of the policy, in the **Name** text box, type a new name.
4. Configure the access rules and other settings for the policy.
5. Click **OK** to close the **Properties** dialog box.

*You can add more than one policy while the Policies dialog box is open.*

6. Click **Close**.

*The new policy appears in Policy Manager.*

For more information on policy properties, see *About Policy Properties* on page 391.

For more information about how to configure proxy actions, see *About Proxy Actions*.

For more information about how to configure application control actions, see *Configure Application Control Actions*.

When you configure the access rules for your policy, you can choose to use an alias. For more information about aliases, see *About Aliases* on page 378 and *Create an Alias* on page 379.

## Add More than One Policy of the Same Type

If your security policy requires it, you can add the same policy more than one time. For example, you can set a limit on web access for most users, while you give full web access to your management team. To do this, you add two different policies with different properties:

1. Add the first policy.
2. Change the name of the policy to a name that matches your security policy and add the related information.

*In this example, you can name the first policy "restricted\_web\_access."*

3. Click **OK**.

*The New Policy Properties dialog box for the policy appears.*

4. Add the second policy.

5. Click **OK**.

*The New Policy Properties dialog box for the policy appears.*

For more information on policy properties, see *About Policy Properties* on page 391.

## See Template Details and Modify Policy Templates

The relevant from the policy template appears in the Details section of the **Add Policies** dialog box. If you want to see more detail, you can open the template to edit it. There are two types of policy templates: predefined and custom. For pre-defined policies (those included in the Packet Filters and Proxies lists in the **Add Policies** dialog box), you can edit only the **Description** information on the policy template. You cannot edit or delete pre-defined policies. You can only change or delete a custom policy template.

For more information on custom policies, see *About Custom Policies*.

To see a policy template:

1. In the **Add Policies** dialog box, select a policy template.
2. Click **Edit**.

*The Policy Template dialog box appears.*





## Disable or Delete a Policy

As your network security requirements change, you can disable or delete the policies in your configuration.

You can disable a policy in two places in Policy Manager: the main **Firewall** or **Mobile VPN with IPSec** tabs, or the **Edit Policy Properties** dialog box.

To disable a policy on the **Firewall** or **Mobile VPN with IPSec** tab:


1. Select the **Firewall** or **Mobile VPN with IPSec** tab.
2. Right-click a policy and select **Disable Policy**.  
*The right-click menu option changes to Enable Policy.*

To disable a policy in the **Edit Policy Properties** dialog box:

1. Double-click a policy.  
*The Edit Policy Properties dialog box appears.*
2. Clear the **Enable** check box.
3. Click **OK**.

## Delete a Policy

To remove a policy, you must first remove it from Policy Manager. Then you save the new configuration to the XTM device.

1. Select a policy.
2. Click .  
Or, select **Edit > Delete Policy**.  
*A confirmation dialog box appears.*
3. Click **Yes**.
4. To save the configuration to the XTM device, select **File > Save > To Firebox**.
5. Type the configuration passphrase and select the **Save to Firebox** check box.
6. Click **Save**.

## About Aliases

An alias is a shortcut that identifies a group of hosts, networks, or interfaces. When you use an alias, it is easy to create a security policy because the XTM device allows you to use aliases when you create policies.

Default aliases in Policy Manager include:

- **Any** — Any source or destination aliases that correspond to XTM device interfaces, such as *Trusted* or *External*.
- **Firebox** — An alias for all XTM device interfaces.
- **Any-Trusted** — An alias for all XTM device interfaces configured as *Trusted* interfaces, and any network you can get access to through these interfaces.
- **Any-External** — An alias for all XTM device interfaces configured as *External*, and any network you can get access to through these interfaces.
- **Any-Optional** — Aliases for all XTM device interfaces configured as *Optional*, and any network you can get access to through these interfaces.
- **Any-BOVPN** — An alias for any BOVPN (IPSec) tunnel.  
When you use the BOVPN Policy wizard to create a policy to allow traffic through a BOVPN tunnel, the wizard automatically creates *.in* and *.out* aliases for the incoming and outgoing tunnels.

Alias names are different from user or group names used in user authentication. With user authentication, you can monitor a connection with a name and not as an IP address. The person authenticates with a user name and a password to get access to Internet protocols.

For more information about user authentication, see *About User Authentication* on page 303.

## Alias Members

You can add these objects to an alias:

- Host IP
- Network IP
- A range of host IP addresses
- DNS name for a host
- Tunnel address — defined by a user or group, address, and name of the tunnel
- Custom address — defined by a user or group, address, and XTM device interface
- Another alias
- An authorized user or group

## Create an Alias

To create an alias to use with your security policies:

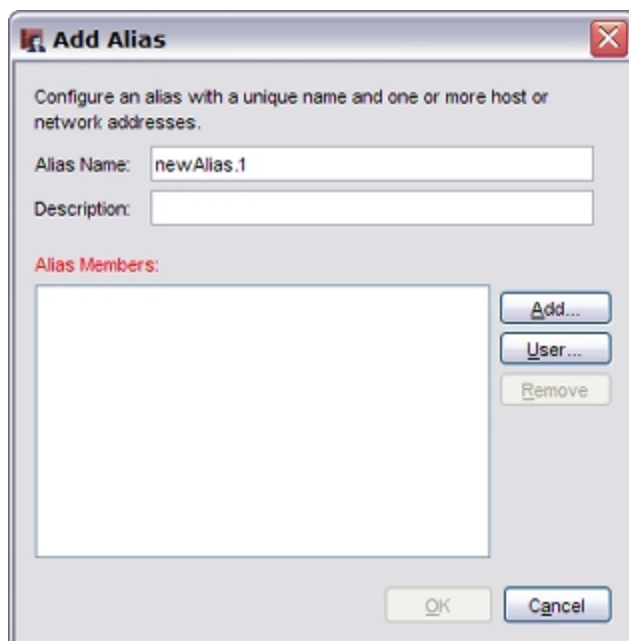
1. Select **Setup > Aliases**.

*The Aliases dialog box appears. Pre-defined aliases appear in blue and user-defined aliases appear in black.*



2. Click **Add**.

*The Add Alias dialog box appears.*



3. In the **Alias Name** text box, type a unique name to identify the alias.  
*This name appears in lists when you configure a security policy.*
4. In the **Description** text box, type a description of the alias.
5. Click **OK**.

## Add an Address, Address Range, DNS Name, or Another Alias to the Alias

1. In the **Add Alias** dialog box, click **Add**.  
*The Add Member dialog box appears.*
2. From the **Choose Type** drop-down list, select the type of member you want to add.
3. Type the address or name in the **Value** text box.
4. Click **OK**.  
*The new member appears in the Alias Members section of the Add Alias dialog box.*
5. To add more members, repeat Steps 1–4.
6. Click **OK**.

## Add an Authorized User or Group to the Alias

1. In the **Add Alias** dialog box, click **User**.  
*The Add Authorized Users or Groups dialog box appears.*
2. In the left **Type** drop-down list, select whether the user or group you want to add is authorized as a Firewall user, a PPTP user, or an SSL VPN user.
3. In the right **Type** drop-down list, select **User** to add a user, or **Group** to add a group.
4. If the user or group appears in the list at the bottom of the **Add Authorized Users or Groups** dialog box, select the user or group and click **Select**.

If the user or group does not appear in the list, it is not yet defined as an authorized user or group. You must define it as an authorized user or group before you add it to an alias.

5. Repeat Steps 1–4 to add more members as needed.  
Or, use the previous procedure to add an address, address range, DNS name, or another alias to the alias.
6. Click **OK**.

For information on how to define an authorized user or group, see:

- *Define a New User for Firebox Authentication*
- *Define a New Group for Firebox Authentication*
- *Use Authorized Users and Groups in Policies*

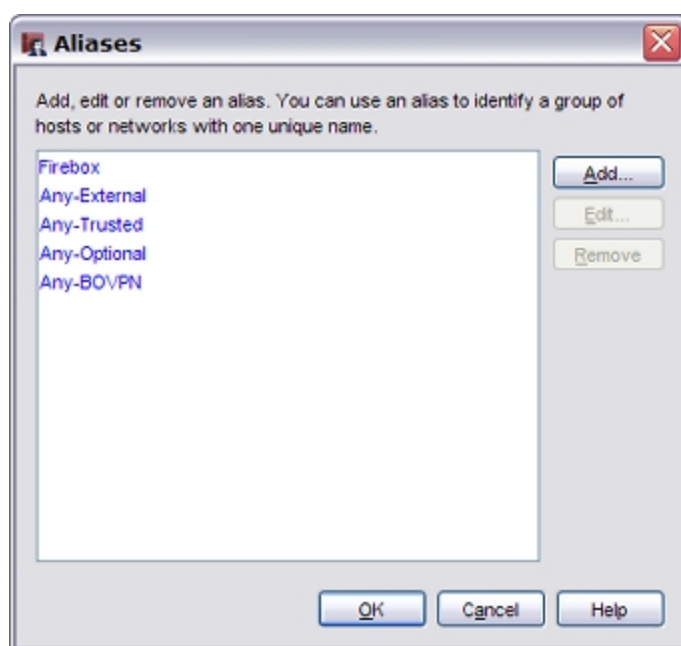
## Edit an Alias

You can edit user-defined aliases from the **Aliases** dialog box, or from within a policy that uses the alias.

To edit an alias from the **Aliases** dialog box:

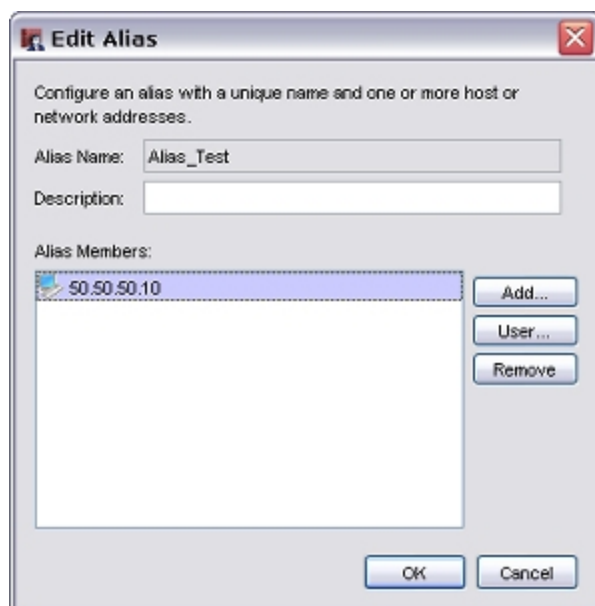
1. Select **Setup > Aliases**.

*The Aliases dialog box appears. Pre-defined aliases appear in blue and user-defined aliases appear in black.*



2. From the **Aliases** list, select the user-defined alias to change.
3. Click **Edit**.

*The Edit Alias dialog box appears.*



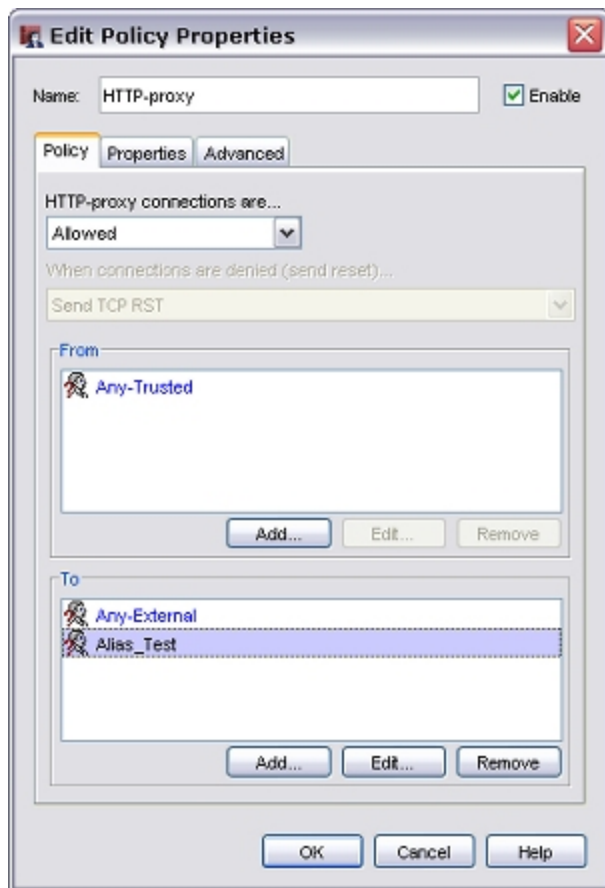
4. To add a member to the **Alias Members** list, click **Add** or **User**.  
For more information, see the previous sections.

To remove a member from the **Alias Members** list, select the entry and click **Remove**

5. Click **OK**.

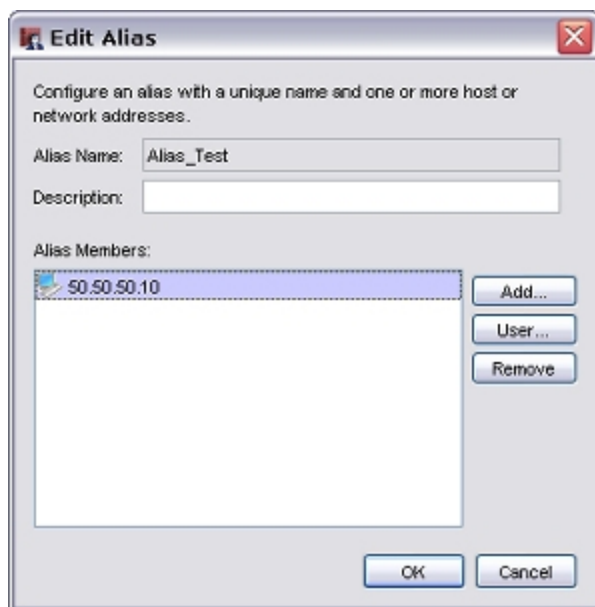
To edit an alias from within a policy:

1. Edit a policy with the user-defined alias you want to change.  
*The Edit Policy Properties dialog box appears.*



2. In the **From** or **To** list, select the alias to change.
3. Click **Edit**.

*The Edit Alias dialog box appears.*



4. To add a member to the **Alias Members** list, click **Add** or **User**.

For more information, see the previous sections.

To remove a member from the **Alias Members** list, select the member and click **Remove**.

5. Click **OK**.

## About Policy Precedence

Precedence is the sequence in which the XTM device examines network traffic and applies a policy rule. The XTM device automatically sorts policies from the most detailed to the most general. It compares the information in the packet to the list of rules in the first policy. The first rule in the list to match the conditions of the packet is applied to the packet. If the detail level in two policies is equal, a proxy policy always takes precedence over a packet filter policy.

## Automatic Policy Order

The XTM device automatically gives the highest precedence to the most specific policies and the lowest to the least specific. The XTM device examines specificity of the subsequent criteria in the following order. If it cannot determine the precedence from the first criterion, it moves to the second, and so on.

1. Policy specificity
2. Protocols set for the policy type
3. Traffic rules of the **To** list
4. Traffic rules of the **From** list
5. Firewall action (Allowed, Denied, or Denied (send reset)) applied to the policies
6. Schedules applied to the policies
7. Alphanumeric sequence based on policy type
8. Alphanumeric sequence based on policy name

The subsequent sections include more details about what the XTM device does within these eight steps.

## Policy Specificity and Protocols

The XTM device uses these criteria in sequence to compare two policies until it finds that the policies are equal, or that one is more detailed than the other.

1. An Any policy always has the lowest precedence.
2. Check for the number of TCP 0 (any) or UDP 0 (any) protocols. The policy with the smaller number has higher precedence.
3. Check for the number of unique ports for TCP and UDP protocols. The policy with the smaller number has higher precedence.
4. Add up the number of unique TCP and UDP ports. The policy with the smaller number has higher precedence.
5. Score the protocols based on their IP protocol value. The policy with the smaller score has higher precedence.

If the XTM device cannot set the precedence when it compares the policy specificity and protocols, it examines traffic rules.

## Traffic Rules

The XTM device uses these criteria in sequence to compare the most general traffic rule of one policy with the most general traffic rule of a second policy. It assigns higher precedence to the policy with the most detailed traffic rule.

1. Host address
2. IP address range (smaller than the subnet being compared to)
3. Subnet
4. IP address range (larger than the subnet being compared to)
5. Authentication user name
6. Authentication group
7. Interface, XTM device
8. Any-External, Any-Trusted, Any-Optional
9. Any

For example, compare these two policies:

(HTTP-1) From: Trusted, user1

(HTTP-2) From: 10.0.0.1, Any-Trusted

*Trusted* is the most general entry for HTTP-1. *Any-Trusted* is the most general entry for HTTP-2. Because *Trusted* is included in the *Any-Trusted* alias, HTTP-1 is the more detailed traffic rule. This is correct despite the fact that HTTP-2 includes an IP address, because the XTM device compares the most general traffic rule of one policy to the most general traffic rule of the second policy to set precedence.

If the XTM device cannot set the precedence when it compares the traffic rules, it examines the firewall actions.



## Firewall Actions

The XTM device compares the firewall actions of two policies to set precedence. Precedence of firewall actions from highest to lowest is:

1. Denied or Denied (send reset)
2. Allowed proxy policy
3. Allowed packet-filter policy

If the XTM device cannot set the precedence when it compares the firewall actions, it examines the schedules.

## Schedules

The XTM device compares the schedules of two policies to set precedence. Precedence of schedules from highest to lowest is:

1. Always off
2. Sometimes on
3. Always on

If the XTM device cannot set the precedence when it compares the schedules, it examines the policy types and names.

## Policy Types and Names

If the two policies do not match any other precedence criteria, the XTM device sorts the policies in alphanumeric sequence. First, it uses the policy type. Then, it uses the policy name. Because no two policies can be the same type and have the same name, this is the last criteria for precedence.

## Set Precedence Manually

You can switch to manual-order mode and change the policy precedence for your XTM device or template.

1. Select **View > Auto-Order Mode**.  
The checkmark disappears and a confirmation message appears.
2. Click **Yes** to confirm that you want to switch to manual-order mode.  
When you switch to manual-order mode, the Policy Manager window changes to the Details view.  
You cannot change the order of policies if you are in Large Icons view.
3. To change the order of a policy, select it and drag it to the new location.

## Create Schedules for XTM Device Actions

A schedule is a set of times for which a feature is active or disabled. You must use a schedule if you want a policy or WebBlocker action to automatically become active or inactive at the times you specify. You can apply a schedule you create to more than one policy or WebBlocker action if you want those policies or actions to be active at the same times.

For example, an organization wants to restrict certain types of network traffic during normal business hours. The network administrator could create a schedule that is active on weekdays, and set each policy in the configuration to use the same schedule.

To create a schedule:

1. Select **Setup > Actions > Schedules**.

*The Schedules dialog box appears.*



2. To edit a schedule, select the schedule name in the **Schedule** dialog box and click **Edit**.  
To create a new schedule from an existing one, select the schedule name and click **Clone**.  
To create a new schedule, click **Add**.

*The New Schedule dialog box appears. The chart in the dialog box shows days of the week along the x-axis (horizontal) and increments of the day on the y-axis (vertical).*

**New Schedule**

Name:

Description:

Mode:

Hour	Sun	Mon	Tue	Wed	Thu	Fri	Sat
06:00							
07:00							
08:00							
09:00							
10:00							
11:00							
12:00							
13:00							
14:00							
15:00							
16:00							
17:00							
18:00							
19:00							
20:00							

: Operational Hour  
 : Non-operational Hour

OK Cancel Help

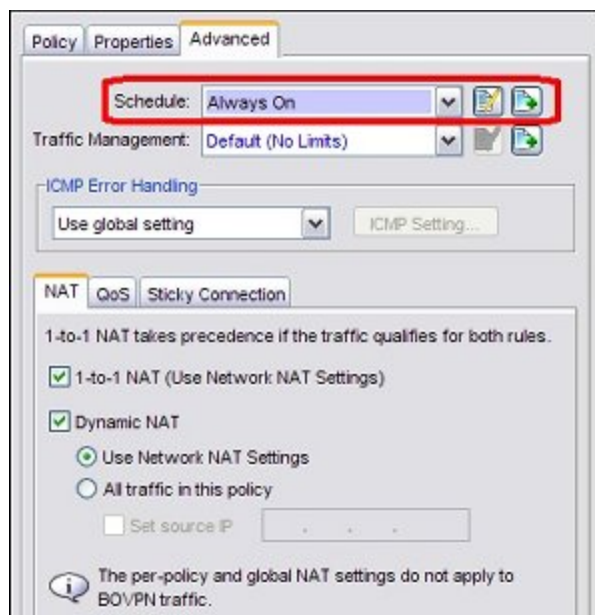
- Type a schedule name and description.  
*Make sure that the name is easy to remember.*  
*The schedule name appears in the Schedules dialog box.*
- In the **Mode** drop-down list, select the time increment for the schedule: one hour, 30 minutes, or 15 minutes.  
*The chart on the left of the New Schedule dialog box shows your entry in the drop-down list.*
- Click boxes in the chart to change them to operational hours (when the policy is active) or non-operational hours (when the policy is not in effect).
- Click **OK** to close the **New Schedule** dialog box.
- Click **Close** to close the **Schedules** dialog box.

## Set an Operating Schedule

You can set an operating schedule for a policy so that it runs at the times you specify. Schedules can be shared by more than one policy.

To modify a policy schedule:

- Select any policy and double-click it.  
*The Edit Policy Properties dialog box appears.*
- Click the **Advanced** tab.
- In the **Schedule** drop-down list, select a predefined schedule.  
Or, click an adjacent icon to create a custom schedule.



4. Click OK.

## About Custom Policies

If you need to allow for a protocol that is not included by default as a XTM device configuration option, you must define a custom traffic policy. You can add a custom policy that uses:

- TCP ports
- UDP ports
- An IP protocol that is not TCP or UDP, such as GRE, AH, ESP, ICMP, IGMP, and OSPF. You identify an IP protocol that is not TCP or UDP with the IP protocol number.

To create a custom policy, you must first create or edit a custom policy template that specifies the ports and protocols used by policies of that type. Then, you create one or more policies from that template to set access rules, logging, QoS, and other settings.

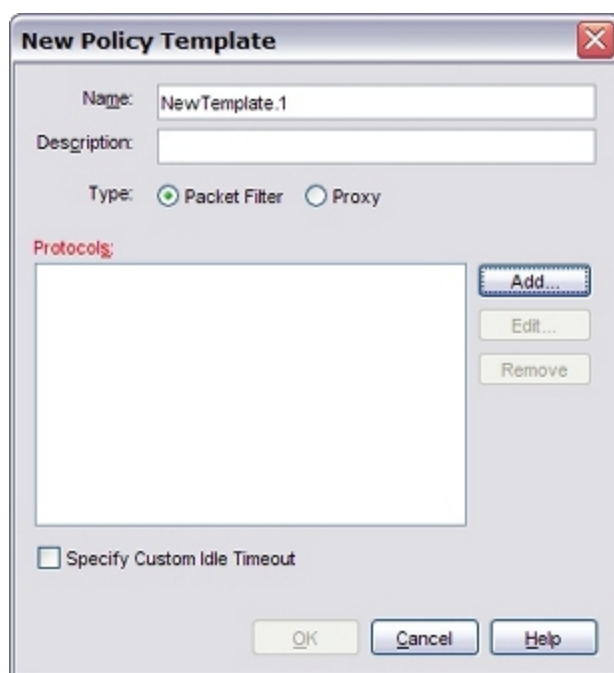
## Create or Edit a Custom Policy Template

To add specialized policies to your configuration files, you can create custom policy templates. These templates can be packet filter or proxy policies and use any available protocol. When you add a custom policy template to your configuration file, make sure to specify a unique name for the policy. A unique name helps you to find the policy when you want to change or remove it. This name must not be the same as any other policy name in the policies list for your device.

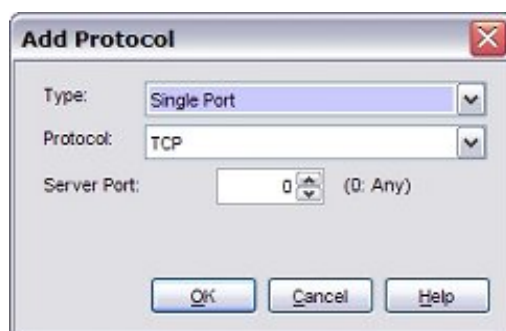
From Policy Manager:

1. Click **+**.  
Or, select **Edit > Add Policies**.  
*The Add Policies dialog box appears.*

2. Click **New**.  
Or, select a custom policy template and click **Edit**.  
*The New Policy Template dialog box appears.*



3. In the **Name** text box, type the name of the custom policy.  
The name appears in the policies list in the **Policy Name** column.
4. In the **Description** text box, type a description of the policy.  
*This appears in the Details section when you click the policy name in the list of User Filters.*
5. Select the type of policy: **Packet Filter** or **Proxy**.
6. If you select **Proxy**, choose the proxy protocol from the adjacent drop-down list.
7. To add protocols for this policy, click **Add**.  
*The Add Protocol dialog box appears.*



8. From the **Type** drop-down list, select **Single Port** or **Port Range**.
9. From the **Protocol** drop-down list, select the protocol for this new policy.  
If you select **Single Port**, you can select **TCP**, **UDP**, **GRE**, **AH**, **ESP**, **ICMP**, **IGMP**, **OSP**, **IP**, or **Any**.  
If you select **Port Range**, you can select **TCP** or **UDP**. The options below the drop-down list change for each protocol.

**Note** *Fireware XTM does not pass IGMP multicast traffic through the XTM device, or between XTM device interfaces. It passes IGMP multicast traffic only between an interface and the XTM device.*

10. If you selected **Single Port**, in the **Server Port** text box, type or select the port for this new policy. If you selected **Port Range**, in the **Start Server Port** and **End Server Port** text boxes, type or select the starting server port and the ending server port.
11. Click **OK**.  
*The policy template is added to the Custom policies folder.*

You can now use the policy template you created to add one or more custom policies to your configuration. Use the same procedure as you would for a predefined policy.

## Import and Export Custom Policy Templates

If you manage several XTM devices and have custom policies for them, you can use the policy import/export function to save time. You can define the templates on one XTM device, export them to an ASCII file, and then import them to another XTM device.

The XTM device where you created the policies must run the same version of WSM as the version of Policy Manager you use to import the policies. You cannot import a template from a previous version into the current version.

1. On the first XTM device, define custom policy templates.
2. Click **Export**.  
You do not have to select the custom policies. The Export function automatically exports all custom policies regardless of which policy is actually selected.
3. In the **Save** dialog box, select where you want to save the policy templates file. Type a name for the file and click **Save**.  
*The default location is My Documents > My WatchGuard.*
4. From Policy Manager on a different XTM device, in the **Add Policies** dialog box, click **Import**.
5. Find the file you created in Step 3 and click **Open**.
6. If custom policy templates are already defined in the current Policy Manager, you are asked whether you want to replace the existing templates or append the imported templates to the existing templates. Click **Replace** or **Append**.  
If you click **Replace**, the existing templates are deleted and replaced with the new templates.  
If you click **Append**, both the existing and the imported templates are listed in alphabetical order under **Custom**.

---

## About Policy Properties

Each policy type has a default definition, which consists of settings that are appropriate for most organizations. However, you can modify policy settings for your particular business purposes, or add other settings such as traffic management and operating schedules.

Mobile VPN policies are created and operate in the same way as firewall policies. However, you must specify a Mobile VPN group to which the policy applies.

To set properties for an existing policy, in Policy Manager, double-click a policy to open the **Edit Policy Properties** dialog box. When you add a new policy to your configuration, the **New Policy Properties** dialog box automatically appears for you to set policy properties.

## Policy Tab

Use the **Policy** tab to set basic information about a policy, such as whether it allows or denies traffic, and which devices it manages. You can use the Policy tab settings to create access rules for a policy, or configure policy-based routing, static NAT, or server load balancing. You can also configure proxy and ALG actions on this tab, which offer different options for each proxy policy and ALG.

For more information on the options for this tab, see the following topics:

- *Set Access Rules for a Policy* on page 392
- *Configure Policy-Based Routing* on page 395
- *Configure Static NAT* on page 179
- *Configure Server Load Balancing* on page 182
- *About Proxy Actions* on page 403 (proxy policies and ALGs only)

## Properties Tab

The **Properties** tab shows the port and protocol to which the policy applies, as well as a description of the policy that you set. You can use the settings on this tab to set logging, notification, automatic blocking, and timeout preferences.

For more information on the options for this tab, see the following topics:

- *Set Logging and Notification Preferences* on page 723
- *Block Sites Temporarily with Policy Settings* on page 538
- *Set a Custom Idle Timeout* on page 399

## Advanced Tab


The **Advanced** tab includes settings for NAT and Traffic Management (QoS), as well as multi-WAN and ICMP options. You can also set an operating schedule for a policy and apply traffic management actions.

For more information on the options for this tab, see the following topics:

- *Set an Operating Schedule* on page 387
- *Add a Traffic Management Action to a Policy* on page 521
- *Set ICMP Error Handling* on page 399
- *Apply NAT Rules* on page 399
- *Enable QoS Marking or Prioritization Settings for a Policy* on page 516
- *Set the Sticky Connection Duration for a Policy* on page 400

## Proxy Settings

Proxy policies have predefined rulesets that provide a good balance of security and accessibility for most installations. If a default ruleset does not meet all of your business needs, you can add, delete, or modify rules.

To modify the settings and rulesets for a proxy action, on the **Policy** tab, to the right of the **Proxy action** drop-down list, click  and select a category of settings.

For more information, see *About Rules and Rulesets* on page 408 and the *About* topic for the specific policy type.

*About the DNS-Proxy* on page 419

*About the POP3-Proxy* on page 467

*About the FTP-Proxy* on page 428

*About the SIP-ALG* on page 480

*About the H.323-ALG* on page 434

*About the SMTP-Proxy* on page 488

*About the HTTP-Proxy* on page 440

*About the TCP-UDP-Proxy* on page 506

*About the HTTPS-Proxy* on page 459

## Set Access Rules for a Policy

To configure access rules for a policy, select the **Policy** tab of the **Edit Policy Properties** dialog box.

The **Connections are** drop-down list defines whether traffic that matches the rules in the policy is allowed or denied. To configure how traffic is handled, select one of these settings:

### *Allowed*

The XTM device allows traffic that uses this policy if it matches the rules you set in the policy. You can configure the policy to create a log message when network traffic matches the policy.

### *Denied*

The XTM device denies all traffic that matches the rules in this policy and does not send a notification to the device that sent the traffic. You can configure the policy to create a log message when a computer tries to use this policy. The policy can also automatically add a computer or network to the Blocked Sites list if it tries to start a connection with this policy.

For more information, see *Block Sites Temporarily with Policy Settings* on page 538.

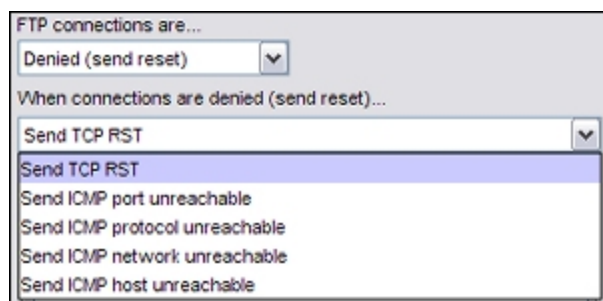


*Denied (send reset)*

The XTM device denies all traffic that matches the rules in this policy. You can configure it to create a log message when a computer tries to use this policy. The policy can also automatically add a computer or network to the Blocked Sites list if it tries to start a connection with this policy

For more information, see *Block Sites Temporarily with Policy Settings* on page 538.

With this option, the XTM device sends a packet to tell the device which sent the network traffic that the session is refused and the connection is closed. You can set a policy to return other errors instead, which tell the device that the port, protocol, network, or host is unreachable. We recommend that you use these options with caution to ensure that your network operates correctly with other networks.



The **Policy** tab also includes:

- A **From** list (or *source*) that specifies who can send (or cannot send) network traffic with this policy.
- A **To** list (or *destination*) that specifies who the XTM device can route traffic to if the traffic matches (or does not match) the policy specifications.

For example, you could configure a ping packet filter to allow ping traffic from all computers on the external network to one web server on your optional network. However, when you open the destination network to connections over the port or ports that the policy controls, you can make the network vulnerable. Make sure you configure your policies carefully to avoid vulnerabilities.

To add members to your access specifications:

1. Adjacent to the **From** or the **To** member list, click **Add** .  
*The Add Address dialog box appears.*



The **Available Members** list contains the members you can add to the **From** or **To** lists. A member can be an alias, user, group, IP address, or range of IP addresses.

2. Select a member you want to add and click **Add**, or double-click an entry in this list.

To add hosts, users, aliases, or tunnels to the policy that do not appear in the **Available Members** list, see *Add New Members for Policy Definitions* on page 394.

3. To add other members to the **From** or **To** list, repeat the previous steps.
4. Click **OK**.

The source and destination can be a host IP address, host range, host name, network address, user name, alias, VPN tunnel, or any combination of those objects.

For more information on the aliases that appear in the **From** and **To** list, see *About Aliases* on page 378.

For more information about how to create a new alias or edit a user-defined alias, see *Create an Alias* on page 379.

## Add New Members for Policy Definitions

To add hosts, aliases, or tunnels to the **Available Members** list:

1. Click **Add Other**.  
*The Add Member dialog box appears.*
2. In the **Choose Type** drop-down list, select the host range, host IP address, or network IP address to add.
3. In the **Value** text box, type the correct network address, range, or IP address.



4. Click **OK**.

*The member or address appears in the Selected Members and Addresses list.*

To add a user or group to the **Available Members** list:

1. Click **Add User**.  
*The Add Authorized Users or Groups dialog box appears.*
2. Select the type of user or group, select the authentication server, and whether you want to add a user or group.



3. Click **Select**.

If the user or group you want to add does not appear in the list, it is not yet defined as an authorized user or group. To define a new authorized user or group, see *Use Authorized Users and Groups in Policies* on page 360.

## Configure Policy-Based Routing

To send network traffic, a router usually examines the destination address in the packet and looks at the routing table to find the next-hop destination. In some cases, you want to send traffic to a different path than the default route specified in the routing table. You can configure a policy with a specific external interface to use for all outbound traffic that matches that policy. This technique is known as policy-based routing. Policy-based routing takes precedence over other multi-WAN settings.

Policy-based routing can be used when you have more than one external interface and have configured your XTM device for multi-WAN. With policy-based routing, you can make sure that all traffic for a policy always goes out through the same external interface, even if your multi-WAN configuration is set to send traffic in a round-robin configuration. For example, if you want email to be routed through a particular interface, you can use policy-based routing in the SMTP-proxy or POP3-proxy definition.

**Note** To use policy-based routing, you must have Fireware XTM with a Pro upgrade. You must also configure at least two external interfaces.

## Policy-Based Routing, Failover, and Failback


When you use policy-based routing with multi-WAN failover, you can specify whether traffic that matches the policy uses another external interface when failover occurs. The default setting is to drop traffic until the interface is available again.

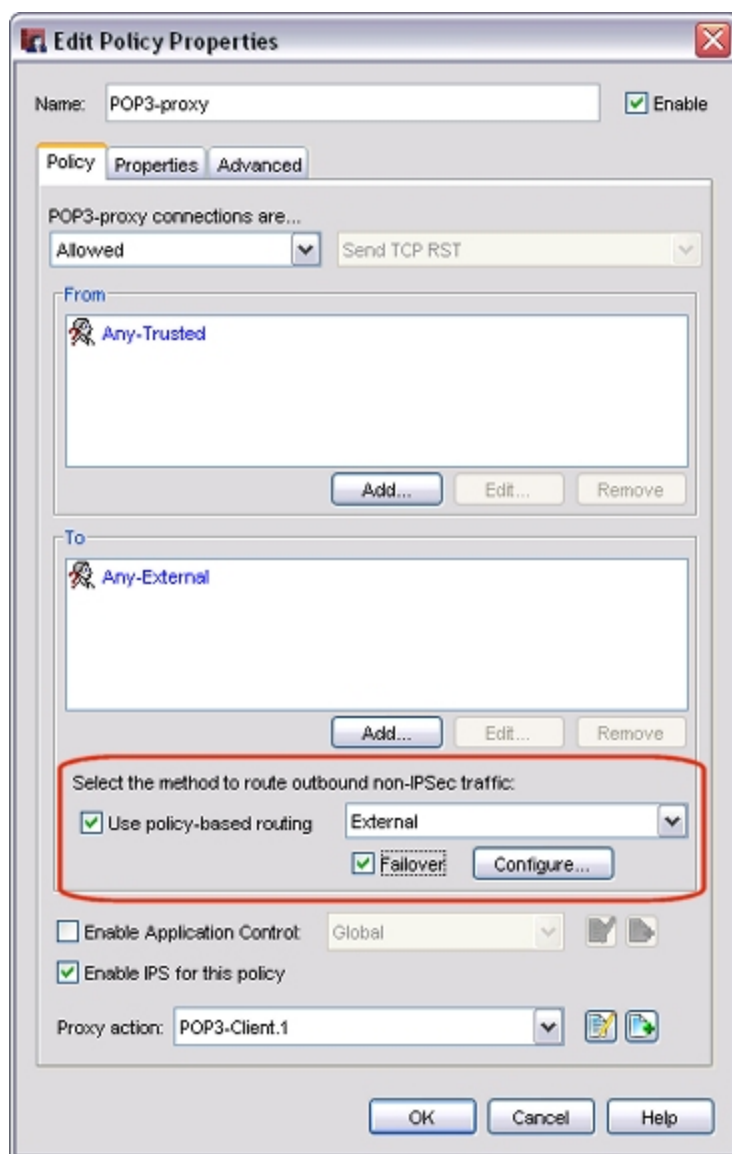
Failback settings (defined on the **Multi-WAN** tab of the **Network Configuration** dialog box) also apply to policy-based routing. If a failover event occurs, and the original interface later becomes available, the XTM device can send active connections to the failover interface, or it can fail back to the original interface. New connections are sent to the original interface.

## Restrictions on Policy-Based Routing

- Policy-based routing is available only if multi-WAN is enabled. If you enable multi-WAN, the **Edit Policy Properties** dialog box automatically includes fields to configure policy-based routing.
- By default, policy-based routing is not enabled.
- Policy-based routing does not apply to IPSec traffic, or to traffic destined for the trusted or optional network (incoming traffic).

## Add Policy-Based Routing to a Policy

1. Open Policy Manager.
2. Select a policy and click .  
Or, double-click a policy.  
*The Edit Policy Properties dialog box appears.*
3. Select the **Use policy-based routing** check box.



4. To specify the interface to send outbound traffic that matches the policy, select the interface name from the adjacent drop-down list. Make sure that the interface you select is a member of the alias or network that you set in the **To** list for your policy.
5. (Optional) Configure policy-based routing with multi-WAN failover as described below. If you do not select **Failover** and the interface you set for this policy is becomes inactive, traffic is dropped until the interface becomes available again.
6. Click **OK**.

## Configure Policy-Based Routing with Failover

You can set the interface you specified for this policy as the primary interface, and define other external interfaces as backup interfaces for all non-IPSec traffic. If the primary interface you set for a policy is not active, traffic is sent to the backup interface or interfaces you specify.

1. In the **Edit Policy Properties** dialog box, select **Failover**.
2. To specify backup interfaces for this policy, click **Configure**.  
*The Policy Failover Configuration dialog box appears.*

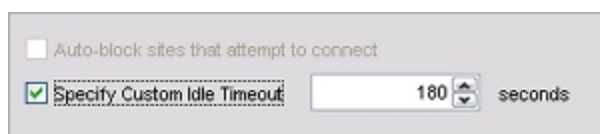


3. In the **Include** column, select the check box for each interface you want to use in the failover configuration. Use the **Move Up** and **Move Down** buttons to set the order for failover. The first interface in the list is the primary interface.
4. Click **OK** to close the **Policy Failover Configuration** dialog box.
5. Click **OK** to close the **Edit Policy Properties** dialog box.
6. *Save the Configuration File.*

## Set a Custom Idle Timeout

*Idle timeout* is the maximum length of time that a connection can stay active when no traffic is sent. By default, the XTM device closes network connections after 8 hours for a packet filter policy and 10 minutes for a proxy policy. When you enable the custom idle timeout setting for a policy, the XTM device closes the connection after the length of time that you specify. The default custom idle timeout setting is 180 seconds (3 minutes).

1. In the **Policy Properties** dialog box, select the **Properties** tab.
2. Select the **Specify Custom Idle Timeout** check box.



3. In the adjacent text box, type or select the number of seconds before a timeout occurs.

## Set ICMP Error Handling

You can set the ICMP error handling settings associated with a policy. These settings override the global ICMP error handling settings.

To change the ICMP error handling settings for the current policy:

1. From the **ICMP Error Handling** drop-down list, select **Specify setting**.
2. Click **ICMP Setting**.
3. In the **ICMP Error Handling Settings** dialog box, select the check boxes to configure individual settings.
4. Click **OK**.

For more information on global ICMP settings, see *Define XTM Device Global Settings* on page 76.

## Apply NAT Rules

You can apply Network Address Translation (NAT) rules to a policy. You can select 1-to-1 NAT or Dynamic NAT.

1. In the **Edit Policy Properties** dialog box, select the **Advanced** tab.
2. Select one of the options described in the subsequent sections.

### 1-to-1 NAT

With this type of NAT, the XTM device uses private and public IP ranges that you set, as described in *About 1-to-1 NAT* on page 168.

### Dynamic NAT

With this type of NAT, the XTM device maps private IP addresses to public IP addresses. All policies have dynamic NAT enabled by default.

Select **Use Network NAT Settings** if you want to use the dynamic NAT rules set for the XTM device.

Select **All traffic in this policy** if you want to apply NAT to all traffic in this policy.

In the **Set Source IP** field, you can select a dynamic NAT source IP address for any policy that uses dynamic NAT. This makes sure that any traffic that uses this policy shows a specified address from your public or external IP address range as the source. This is helpful if you want to force outgoing SMTP traffic to show your domain's MX record address when the IP address on the XTM device external interface is not the same as your MX record IP address.

1-to-1 NAT rules have higher precedence than dynamic NAT rules.

## Set the Sticky Connection Duration for a Policy

The sticky connection setting for a policy overrides the global sticky connection setting. You must enable multi-WAN to use this feature.

1. In the **Policy Properties** dialog box, select the **Advanced** tab.
2. Select the **Sticky Connection** tab.
3. To use the global multi-WAN sticky connection setting, clear the **Override Multi-WAN sticky connection setting** check box.
4. To set a custom sticky connection value for this policy, select the **Enable sticky connection** check box.
5. In the **Enable sticky connection** text box, type the amount of time in minutes to maintain the connection.



# 14 Proxy Settings

---

## About Proxy Policies and ALGs

All WatchGuard policies are important tools for network security, whether they are packet filter policies, proxy policies, or application layer gateways (ALGs). A packet filter examines each packet's IP and TCP/UDP header, a proxy monitors and scans whole connections, and an ALG provides transparent connection management in addition to proxy functionality. Proxy policies and ALGs examine the commands used in the connection to make sure they are in the correct syntax and order, and use deep packet inspection to make sure that connections are secure.

A proxy policy or ALG opens each packet in sequence, removes the network layer header, and examines the packet's payload. A proxy then rewrites the network information and sends the packet to its destination, while an ALG restores the original network information and forwards the packet. As a result, a proxy or ALG can find forbidden or malicious content hidden or embedded in the data payload. For example, an SMTP proxy examines all incoming SMTP packets (email) to find forbidden content, such as executable programs or files written in scripting languages. Attackers frequently use these methods to send computer viruses. A proxy or ALG can enforce a policy that forbids these content types, while a packet filter cannot detect the unauthorized content in the packet's data payload.

If you have purchased and enabled additional subscription services (Gateway AntiVirus, Intrusion Prevention Service, spamBlocker, WebBlocker), WatchGuard proxies can apply these services to network traffic.

## Proxy Configuration

Like packet filters, proxy policies include common options to manage network traffic, including traffic management and scheduling features. However, proxy policies also include settings that are related to the specified network protocol. These settings are configured with *rulesets*, or groups of options that match a specified action. For example, you can configure rulesets to deny traffic from individual users or devices, or allow VoIP (Voice over IP) traffic that matches the codecs you want. When you have set all of the configuration options in a proxy, you can save that set of options as a user-defined proxy action and use it with other proxies.

Fireware XTM supports proxy policies for many common protocols, including DNS, FTP, H.323, HTTP, HTTPS, POP3, SIP, SMTP, and TCP-UDP. For more information on a proxy policy, see the section for that policy.

*About the DNS-Proxy on page 419*

*About the POP3-Proxy on page 467*

*About the FTP-Proxy on page 428*

*About the SIP-ALG on page 480*

*About the H.323-ALG on page 434*

*About the SMTP-Proxy on page 488*

*About the HTTP-Proxy on page 440*

*About the TCP-UDP-Proxy on page 506*

*About the HTTPS-Proxy on page 459*

## Proxy and AV Alarms

An alarm is an event that triggers a *notification*, which is a mechanism to tell a network administrator about a condition in the network. In a proxy definition, an alarm might occur when traffic matches, or does not match, a rule in the proxy. An alarm might also occur when the **Actions to take** selections are set to an action other than **Allow**.

For example, the default definition of the FTP-proxy has a rule that denies the download of files whose file types match any of these patterns: .cab, .com, .dll, .exe, and .zip. You can specify that an alarm is generated whenever the XTM device takes the **Deny** action because of this rule.

For each proxy action, you can define what the XTM device does when an alarm occurs.

AV alarm settings are only available if Gateway AntiVirus applies to the proxy. Gateway AntiVirus is available for the SMTP, POP3, HTTP, FTP, or TCP-UDP proxies. For all other proxies, you can only configure the proxy alarm settings.

From the **Proxy Action Configuration** dialog box:

1. From the **Categories** section of the proxy definition, select **Proxy and AV Alarms**.
2. Configure the XTM device to send an SNMP trap, a notification to a network administrator, or both. The notification can either be an email message to a network administrator or a pop-up window on the administrator's management computer.

For more information on the Proxy and AV alarms settings, see *Set Logging and Notification Preferences* on page 723.

3. To change settings for one or more other categories in this proxy, go to the topic on the next category you want to modify.
4. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

## About Proxy Actions

A proxy action is a specific group of settings, sources, or destinations for a type of proxy. Because your configuration can include several proxy policies of the same type, each proxy policy uses a different proxy action. Each proxy policy has predefined, or default, proxy actions for clients and servers. For example, you can use one proxy action for packets sent to a POP3 server protected by the XTM device, and a different proxy action to apply to email messages retrieved by POP3 clients. You can clone, edit, and delete proxy actions in your XTM device configuration. You can also import and export proxy actions.

Fireware XTM proxy actions are divided into two categories: *predefined* proxy actions, which appear in blue, and *user-defined* proxy actions, which appear in black. The predefined proxy actions are configured to balance the accessibility requirements of a typical company, with the need to protect your computer assets from attacks. You cannot change the settings of predefined proxy actions. Instead, you must clone (copy) the existing predefined proxy action definition and save it as a new, user-defined proxy action. For example, if you want to change a setting in the POP3-Client proxy action, you must save it with a different name, such as POP3-Client.1.

You can create many different proxy actions for either clients or servers, or for a specified type of proxy policy. However, you can assign only one proxy action to each proxy policy. For example, a POP3 policy is linked to a *POP3-Client* proxy action. If you want to create a POP3 proxy action for a POP3 server, or an additional proxy action for POP3 clients, you must add new POP3 proxy policies to Policy Manager that use those new proxy actions.

## Set the Proxy Action in a Proxy Policy

From Policy Manager:

1. [Add or edit a proxy policy](#).  
*The New/Edit Policy Properties dialog box appears, with the Policy tab selected.*
2. From the **Proxy action** drop-down list, select the proxy action to use with this proxy policy.
3. Click **OK**.

## Clone, Edit, or Delete Proxy Actions

To manage the proxy actions for your XTM device, you can clone, edit, and delete proxy actions. You can clone, edit, or delete any user-defined proxy action. You cannot make changes to predefined proxy actions, or delete them. You also cannot delete user-defined proxy actions that are used by a policy.

If you want to change the settings in a predefined proxy action, you can clone it and create a new, user-defined proxy action with the same settings. You can then edit the proxy action to modify the settings as necessary. If you choose to edit a predefined proxy action, you cannot save your changes. Instead, you are prompted to clone the changes you have made to a new, user-defined proxy action.

When you edit a proxy action, you can change the rules and rulesets, and the associated actions. Each the proxy action includes proxy action rules, which are organized into categories. Some categories are further subdivided into subcategories of rules.

For more information on the available proxy action settings for each proxy, see the *About* topic for that proxy.

*About the DNS-Proxy on page 419*

*About the POP3-Proxy on page 467*

*About the FTP-Proxy on page 428*

*About the SIP-ALG on page 480*

*About the H.323-ALG on page 434*

*About the SMTP-Proxy on page 488*

*About the HTTP-Proxy on page 440*

*About the TCP-UDP-Proxy on page 506*

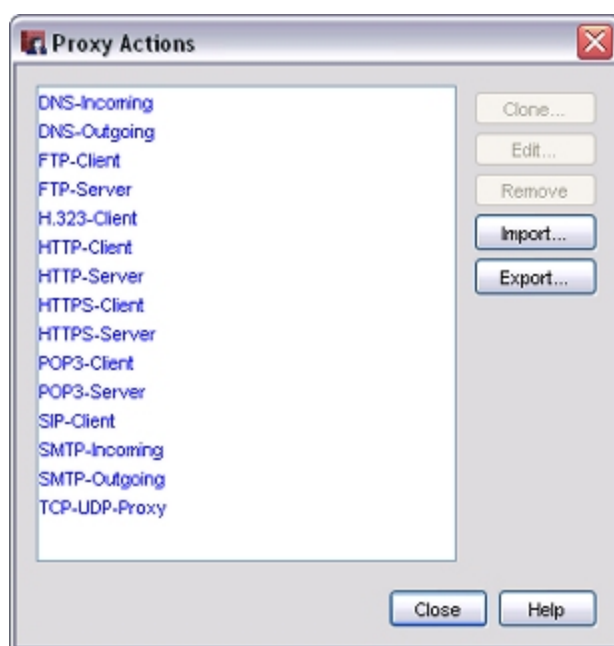
*About the HTTPS-Proxy on page 459*

## Clone or Edit a Proxy Action

You can clone both predefined and user-defined proxy actions. But, you can only edit a user-defined proxy action.

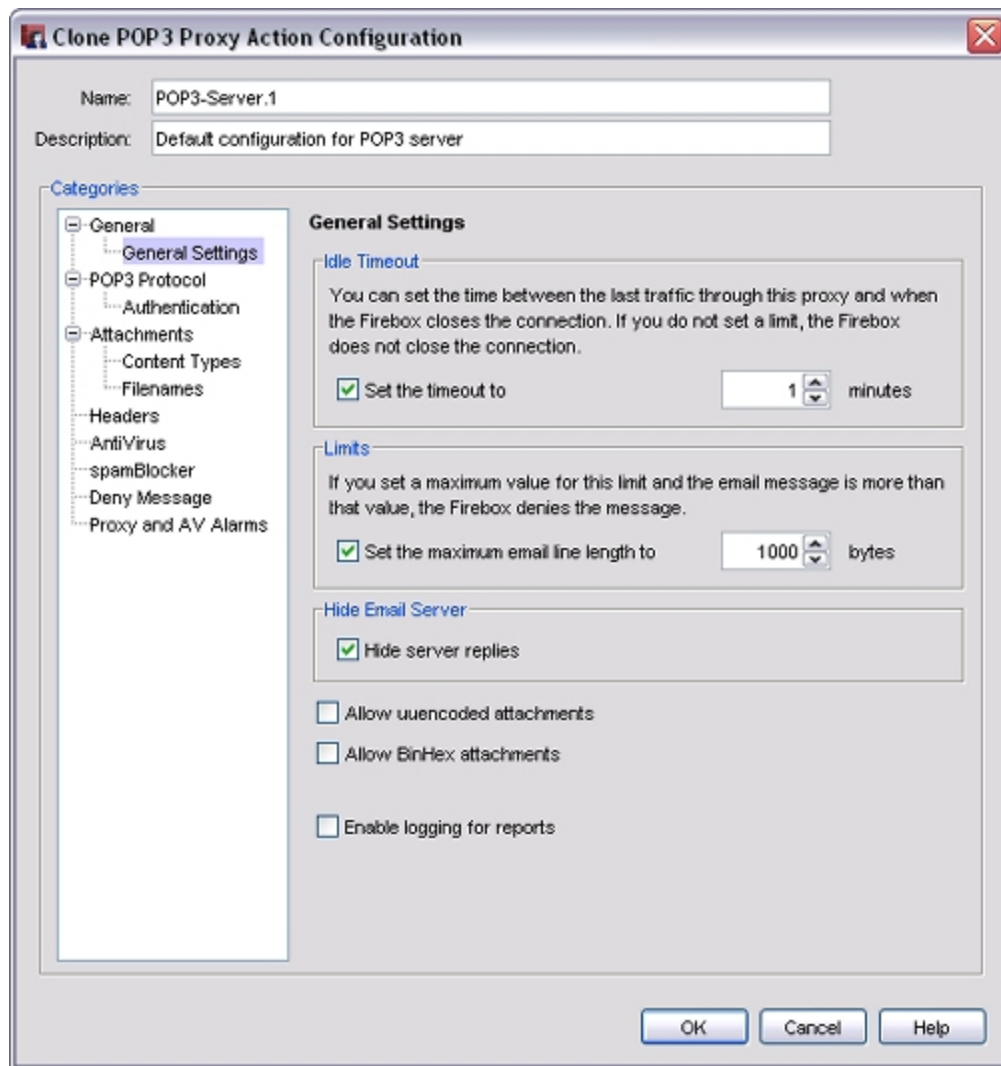
1. Select **Setup > Actions > Proxies**.

*The Proxy Actions dialog box appears.*

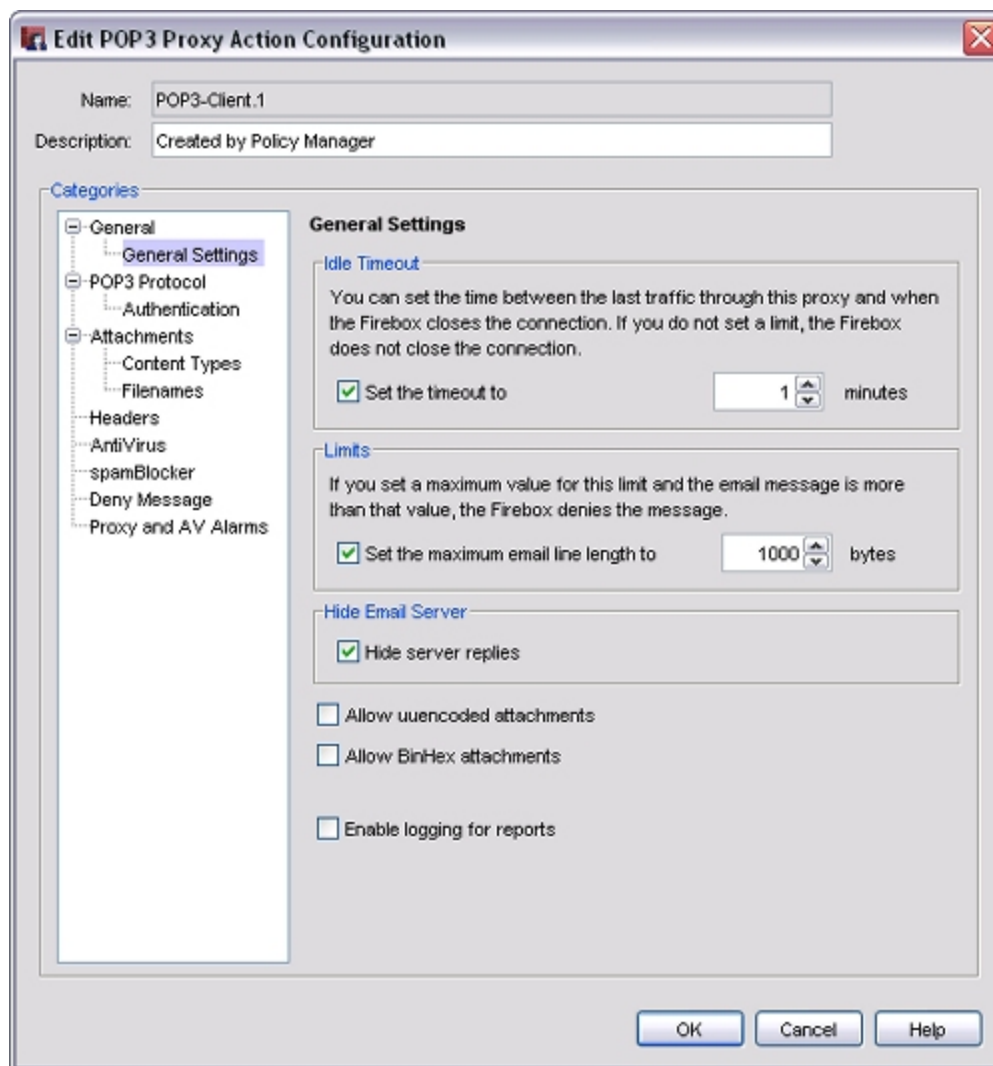


2. Select the proxy action to clone or edit.
3. Click **Clone** or **Edit**.

*If you selected to clone a proxy action, the Clone Proxy Action Configuration dialog box appears, with the available categories displayed in the Categories tree.*



If you selected to edit a proxy action, the Edit Proxy Action Configuration dialog box appears, with the available categories displayed in the Categories tree.

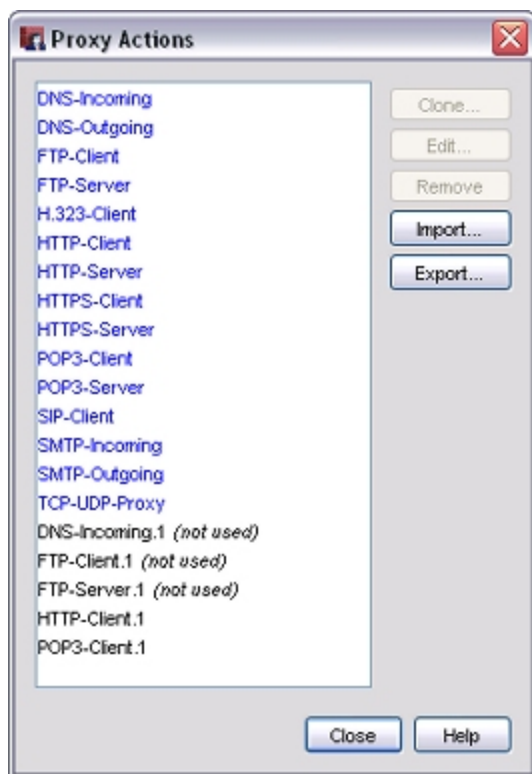


4. From the **Categories** tree, select a category.  
*The page for the selected category appears.*
5. Edit the rules and settings for the proxy action for all the necessary categories.
6. Click **OK**.

## Delete a Proxy Action

You cannot delete predefined proxy actions. You can only delete user-defined proxy actions that are not used by a policy.

1. Select **Setup > Actions > Proxies**.  
*The Proxy Actions dialog box appears.*



2. Select the proxy action to delete.
3. Click **Remove**.  
*A confirmation dialog box appears.*
4. To delete the proxy action, click **Yes**.  
*The proxy action is removed from your device configuration.*

## Import or Export Proxy Actions

If you manage several XTM devices and want to add the same proxy actions to each one, you can save time and use the proxy action import/export function. This enables you to define the proxy actions on one XTM device, export them to a text file, and then import the proxy actions on another XTM device.

For more information, see *Import and Export User-Defined Proxy Actions* on page 407.

## Import and Export User-Defined Proxy Actions

If you manage several XTM devices and have user-defined proxy actions for them, you can use the policy action import/export function to save time. You can define custom proxy actions on one XTM device, export them to an ASCII file, and then import them to another XTM device.

The XTM device for which you created the policies must run the same version of WSM as the version of Policy Manager you use to import the proxy actions. You cannot import a proxy action from an old version into the current version.

1. On the first XTM device, create the user-defined proxy actions.
2. In the **Proxy Actions** dialog box, click **Export**.  
You do not need to select the user-defined actions. The Export function automatically exports all custom actions regardless of which proxy action is actually selected.
3. In the **Save** dialog box, select where you want to save the proxy actions file.  
*The default location is My Documents > My WatchGuard.*
4. Type a name for the file and click **Save**.
5. In Policy Manager on a different XTM device, in the **Proxy Actions** dialog box, click **Import**.
6. Find the file you created in Step 3 and click **Open**.
7. If user-defined proxy actions are already defined in the current Policy Manager, you are asked whether you want to replace the existing actions or append the imported actions to the existing ones. Click **Replace** or **Append**.
  - **Replace** — The existing user-defined proxy actions are deleted and replaced with the new actions.
  - **Append** — Both the existing and the imported actions appear in the dialog box.

## About Rules and Rulesets

When you configure a proxy policy or ALG (application layer gateway), you must select a proxy action to use. You can use either a predefined proxy action or create a new proxy action. Each proxy action contains rules. Rules are sets of criteria to which a proxy compares traffic.

A rule consists of a type of content, pattern, or expression, and the action of the XTM device when a component of the packet's content matches that content, pattern, or expression. Rules also include settings for when the XTM device sends alarms or creates a log entry. A ruleset is a group of rules based on one feature of a proxy such as the content types or filenames of email attachments. The process to create and modify rules is consistent in each proxy policy or ALG.

Your XTM device configuration includes default sets of rules in each proxy actions used by each proxy policy. Separate sets of rules are provided for clients and servers, to protect both your trusted users and your public servers. You can use the default configuration for these rules, or you can customize them for your particular business purposes. You cannot modify or delete predefined proxy actions. If you want to make changes to a predefined proxy action, you can clone it a new proxy action and then make the necessary changes in the new proxy action.

## About Working with Rules and Rulesets

When you configure a proxy or ALG, you can see the rulesets for that proxy in the **Categories** list. These rulesets change when you change the proxy action on the **Properties** tab of a proxy configuration window. For example, the rules for the FTP-Client action have different settings than the rules for the FTP-Server action.

WatchGuard provides a set of predefined rulesets that provide a good balance of security and accessibility for most installations. If a default ruleset does not meet all of your business needs, you can *Add, Change, or Delete Rules*.



## Simple and Advanced Views


You can see rules in proxy definitions in two ways: simple view and advanced view.

- Simple view — Select this view to configure wildcard pattern matching with simple regular expressions.
- Advanced view — Shows the action for each rule. Select this view to use special buttons to edit, clone (use an existing rule definition to start a new one), delete, or reset rules. You can also use the advanced view to configure exact match and Perl-compatible regular expressions.

After you have used the advanced view, you can only change to the simple view if all enabled rules have the same action, alarm, or log settings. For example, if you have five rules with four set to **Allow** and one set to **Deny**, you must continue to use the advanced view.

## Configure Rulesets and Change the View

To configure rulesets for a policy in Policy Manager:

1. Double-click a policy or add a new policy.  
*The Policy Properties dialog box appears with the Policy tab selected.*
2. Adjacent to the **Proxy action** drop-down list, click .
3. To change the view, click **Change View**.
4. *Add, Change, or Delete Rules.*

## Add, Change, or Delete Rules

You can use either the simple or advanced view of the ruleset to add rules. Use the simple view to configure wildcard pattern matching with simple regular expressions. Use the advanced view to configure exact match and Perl-compatible regular expressions. In the advanced view you can also review the action for each rule and edit, clone (use an existing rule definition to create a new rule), delete, or reset rules.

For more information, see *About Rules and Rulesets* on page 408 and *About Regular Expressions* on page 413.

When you configure a rule, you select the actions the proxy takes for each packet. Different actions appear for different proxies or for different features of a particular proxy. This list includes all possible actions:

### *Allow*

Allows the connection.

### *Deny*

Denies a specific request but keeps the connection if possible. Sends a response to the client.

### *Drop*

Denies the specific request and drops the connection. Does not send a response to the sender. The XTM device sends only a TCP reset packet to the client. The client's browser might display "The connection was reset" or "The page cannot be displayed" but the browser does not tell the user why.

### *Block*

Denies the request, drops the connection, and blocks the site. For more information on blocked sites, see *About Blocked Sites* on page 535.

All traffic from the site's IP address is denied for the amount of time specified in Policy Manager at **Setup > Default Threat Protection > Blocked Sites**, on the **Auto-Blocked** tab. Use this action only if you want to stop all traffic from the offender for this time.

### *Strip*

Removes an attachment from a packet and discards it. The other parts of the packet are sent through the XTM device to its destination.

### *Lock*

Locks an attachment, and wraps it so that it cannot be opened by the user. Only the administrator can unlock the file.

### *AV Scan*

Scans the attachment for viruses. If you select this option, Gateway AntiVirus is enabled for the policy.

## **Add Rules (Simple View)**

To add a new rule in simple view:

1. In the **Pattern** text box, type a pattern that uses simple regular expression syntax.  
*The wildcard for zero or more than one character is "\*" . The wildcard for one character is "?" .*
2. Click **Add**.  
*The new rule appears in the Rules box.*
3. Select the **Actions to take**:
  - In the **If matched** drop-down list, set the action to take if the contents of a packet match one of the rules in the list.
  - In the **None matched** drop-down list, set the action to take if the contents of a packet do not match a rule in the list.
4. To configure an alarm for this event, select the **Alarm** check box.  
An alarm notifies users when a proxy rule applies to network traffic. To set the options for the alarm, select **Proxy Alarm** from the **Categories** list on the left side of a Proxy Configuration window. You can send an SNMP trap, send email, or open a pop-up window.
5. To create a message for this event in the traffic log, select the **Log** check box.

## **Add Rules (Advanced View)**

You use the advanced view to configure exact match and Perl-compatible regular expressions. For information on how to work with regular expressions, see *About Regular Expressions* on page 413.

1. In the **Proxy Action Configuration** dialog box, click **Add**.  
*The New Rule dialog box appears.*



2. In the **Rule Name** text box, type the name of the rule.  
*This text box is blank when you add a rule, can be changed when you clone a rule, and cannot be changed when you edit a rule.*
3. In the **Rule Settings** drop-down list, select an option:
  - **Exact Match** — Select when the contents of the packet must match the rule text exactly.
  - **Pattern Match** — Select when the contents of the packet must match a pattern of text, can include wildcard characters.
  - **Regular Expression** — Select when the contents of the packet must match a pattern of text with a regular expression.
4. In the **Rule Settings** text box, type the text of the rule.  
If you selected **Pattern Match** as the rule setting, use an asterisk (\*), a period (.), or a question mark (?) as wildcard characters.
5. In the **Rule Actions** section, in the **Action** drop-down list, select the action the proxy takes for this rule.
6. To create an alarm for this event, select the **Alarm** check box. An alarm tells users when a proxy rule applies to network traffic.
7. To create a message for this event in the traffic log, select the **Log** check box.

## Cut and Paste Rule Definitions

You can copy and paste content in text boxes from one proxy definition to another. For example, suppose you write a custom deny message for the POP3 proxy. You can select the deny message, copy it, and paste it into the **Deny Message** text box for the SMTP proxy.

When you copy between proxy definitions, you must make sure the text box you copy from is compatible with the proxy you paste it into. You can copy rulesets only between proxies or categories within these four groups. Other combinations are not compatible.

Content Types	Filenames	Addresses	Authentication
HTTP Content Types	FTP Download	SMTP Mail From	SMTP Authentication
SMTP Content Types	FTP Upload	SMTP Mail To	POP3 Authentication
POP3 Content Types	HTTP URL Paths		
	SMTP Filename		
	POP3 Filenames		

## Import or Export Rulesets

You can import and export entire rulesets between proxy definitions. For more information, see *Import and Export Rulesets* on page 416.

## Change the Order of Rules

The order that rules are shown in the **Rules** list is the same as the order in which traffic is compared to the rules. The proxy compares traffic to the first rule in the list and continues in sequence from top to bottom. When traffic matches a rule, the XTM device performs the related action. It performs no other actions, even if the traffic matches a rule later in the list. Make sure you use the advanced view of rules.

To change the sequence of rules in a proxy action:

1. To see the advanced view of rules, click **Change View**.
2. Select the rule whose order you want to change.
3. Click **Up** or **Down** to move the rule up or down in the list.

## Change the Default Rule

If traffic does not match any of the rules you have defined for a proxy category, the XTM device uses the *default rule*. This rule appears at the bottom of any list of rules when you use the advanced view.

To modify the default rule:

1. Select the default rule and click **Edit**.  
*The Edit Default Rule dialog box appears.*



2. You can change the action for the default rule, and whether the action triggers an alarm or a log message.  
You cannot change the name “Default” or the order of the rule. It must be the last rule in the list.
3. Click **OK**.

## About Regular Expressions

A regular expression is a group of letters, numbers, and special characters used to match data. You can use Perl-compatible regular expressions (PCRE) in your XTM device configuration to match certain types of traffic in proxy actions. For example, you can use one regular expression to block connections to some web sites and allow connections to other web sites. You can also deny SMTP connections when the recipient is not a valid email address for your company. For example, if you want to block parts of a web site that violate your company’s Internet use policy, you can use a regular expression in the URL Paths category of the HTTP proxy configuration.

### General Guidelines

- Regular expressions in Fireware are case-sensitive — When you create a regular expression, you must be careful to match the case of the letters in your regular expression to the letters of the text you want to match. You can change the regular expression to not be case-sensitive when you put the (?) modifier at the start of a group.
- Regular expressions in Fireware are different from MS-DOS and Unix wildcard characters — When you change files using MS-DOS or the Windows Command Prompt, you can use ? or \* to match one or more characters in a file name. These simple wildcard characters do not operate the same way in Fireware.

For more information on how wildcard characters operate in Fireware, see the subsequent sections.

## How to Build a Regular Expression

The most simple regular expression is made from the text you want to match. Letters, numbers, and other printable characters all match the same letter, number, or character that you type. A regular expression made from letters and numbers can match only a character sequence that includes all of those letters and numbers in order.

Example: fat matches fat, fatuous, and infatuated, as well as many other sequences.

**Note** *Fireware accepts any character sequence that includes the regular expression. A regular expression frequently matches more than one sequence. If you use a regular expression as the source for a Deny rule, you can block some network traffic by accident. We recommend that you fully test your regular expressions before you save the configuration to your XTM device.*

To match different sequences of characters at the same time, you must use a special character. The most common special character is the period (.), which is similar to a wildcard. When you put a period in a regular expression, it matches any character, space, or tab. The period does not match line breaks (`\r\n` or `\n`).

Example: f..t matches foot, feet, f&#t, f -t, and f\t3t.

To match a special character, such as the period, you must add a backslash (\) before the character. If you do not add a backslash to the special character, the rule may not operate correctly. It is not necessary to add a second backslash if the character usually has a backslash, such as `\t` (tab stop).

You must add a backslash to each of these special characters to match the real character: `? . * | + $ \ ^ ( ) [`

Example: `\$9\.` matches \$9.99

## Hexadecimal Characters

To match hexadecimal characters, use `\x` or `%0x%`. Hexadecimal characters are not affected by the case-insensitive modifier.

Example: `\x66` or `%0x66%` matches f, but cannot match F.

## Repetition

To match a variable amount of characters, you must use a repetition modifier. You can apply the modifier to a single character, or a group of characters. There are four types of repetition modifiers:

- Numbers inside curly braces (such as `{2,4}`) match as few as the first number, or as many as the second number.  
Example: `3{2,4}` matches 33, 333, or 3333. It does not match 3 or 33333.
- The question mark (?) matches zero or one occurrence of the preceding character, class, or group.  
Example: `me?et` matches met and meet.
- The plus sign (+) matches one or more occurrences of the preceding character, class, or group.  
Example: `me+t` matches met, meet, and meeeeeeeet.
- The asterisk (\*) matches zero or more occurrences of the preceding character, class, or group.  
Example: `me*t` matches mt, met, meet, and meeeeeeeet.

To apply modifiers to many characters at once, you must make a group. To group a sequence of characters, put parentheses around the sequence.

Example: `ba(na)*` matches `ba`, `bana`, `banana`, and `banananananana`.

## Character Classes

To match one character from a group, use square brackets instead of parentheses to create a character class. You can apply repetition modifiers to the character class. The order of the characters inside the class does not matter.

The only special characters inside a character class are the closing bracket (`]`), the backslash (`\`), the caret (`^`), and the hyphen (`-`).

Example: `gr[ae]y` matches `gray` and `grey`.

To use a caret in the character class, do not make it the first character.

To use a hyphen in the character class, make it the first character.

A negated character class matches everything but the specified characters. Type a caret (`^`) at the beginning of any character class to make it a negated character class.

Example: `[Qq][^u]` matches `Qatar`, but not `question` or `Iraq`.

## Ranges

Character classes are often used with character ranges to select any letter or number. A range is two letters or numbers, separated by a hyphen (`-`), that mark the start and finish of a character group. Any character in the range can match. If you add a repetition modifier to a character class, the preceding class is repeated.

Example: `[1-3][0-9]{2}` matches `100` and `399`, as well as any number in between.

Some ranges that are used frequently have a shorthand notation. You can use shorthand character classes inside or outside other character classes. A negated shorthand character class matches the opposite of what the shorthand character class matches. The table below includes several common shorthand character classes and their negated values.

Class Equivalent to	Negated Equivalent to
<code>\w</code> Any letter or number <code>[A-Za-z0-9]</code>	<code>\W</code> Not a letter or number
<code>\s</code> Any whitespace character <code>[\t\r\n]</code>	<code>\S</code> Not whitespace
<code>\d</code> Any number <code>[0-9]</code>	<code>\D</code> Not a number

## Anchors

To match the beginning or end of a line, you must use an anchor. The caret (^) matches the beginning of a line, and the dollar sign (\$) matches the end of a line.

Example: `^am.*$` matches ampere if ampere is the only word on the line. It does not match dame.

You can use `\b` to match a word boundary, or `\B` to match any position that is not a word boundary.

There are three kinds of word boundaries:

- Before the first character in the character sequence, if the first character is a word character (`\w`)
- After the last character in the character sequence, if the last character is a word character (`\w`)
- Between a word character (`\w`) and a non-word character (`\W`)

## Alternation

You can use alternation to match a single regular expression out of several possible regular expressions. The alternation operator in a regular expression is the pipe character (|). It is similar to the boolean operator *OR*.

Example: `m(oo|a|e)n` matches the first occurrence of moon, man, or men.

## Common Regular Expressions

Match the PDF content type (MIME type)

`^%PDF-`

Match any valid IP address

`(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)`

Match most email addresses

`[A-Za-z0-9._-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,4}`

## Import and Export Rulesets

If you manage several XTM devices, you can import and export rulesets between them. This saves time because you must define the rules only once. You define the rules once for one proxy definition, export them to an XML file, and then import them to a new proxy definition.

1. Create the rulesets for one proxy or category.
2. If necessary, click **Change View** to see the advanced view of the ruleset.
3. Click **Export**.
4. In the **Save** dialog box, select where you want to save the XML file.  
*The default location is My Documents > My WatchGuard.*
5. Type a name for the file and click **Save**.
6. In the new proxy definition, click **Import**.
7. Find the file you created in Step 2 and click **Open**.



8. If rules are already defined in the new proxy, you are asked whether you want to clear the old ruleset first.
  - Click **Yes** to delete the existing rules and replace them with the new ones.
  - Click **No** to include both the existing and the imported rules in the ruleset.

## Copy Rulesets Between Different Proxies or Categories

Some rulesets can be used in more than one proxy or category. For example, you can export the Content Types ruleset of an HTTP proxy action, and then import it to the Content Types ruleset of an SMTP proxy action. Or, you can export the SMTP Mail From ruleset to the SMTP Mail To ruleset.

For more information about the the groups that you can copy rulesets between, see *Cut and Paste Rule Definitions* on page 412.

## Use Predefined Content Types

You can restrict HTTP network traffic and POP3 or SMTP email attachments by content type. You can use the Content Type categories of these proxy policies to allow or deny the content types you specify.

1. From any proxy category, click **Predefined**.  
*The Select Content Type dialog box appears.*
2. Select one or more common content types that you want to add to the Content Types ruleset.  
*Use the Control and/or Shift keys to select multiple content types at the same time.*
3. Click **OK**.


## Add a Proxy Policy to Your Configuration

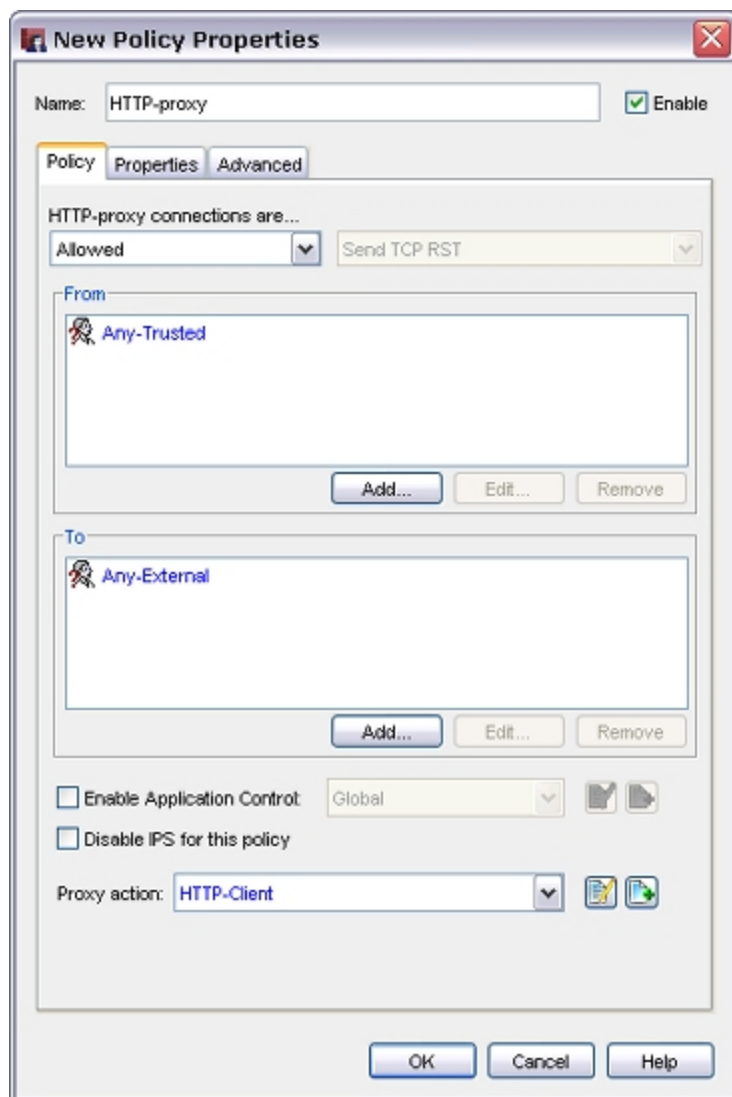
When you add a proxy policy or ALG (application layer gateway) to your Fireware XTM configuration, you specify types of content that the XTM device must find as it examines network traffic. If the content matches (or does not match) the criteria you set in the proxy or ALG definition, the traffic is either allowed or denied.

You can use the default settings of the proxy policy or ALG, or you can change these settings to match network traffic in your organization. You can also create additional proxy policies or ALGs to manage different parts of your network.

It is important to remember that a proxy policy or ALG requires more processor power than a packet filter. If you add a large number of proxy policies or ALGs to your configuration, network traffic speeds might decrease. However, a proxy or ALG uses methods that packet filters cannot use to catch dangerous packets. Each proxy policy includes several settings that you can adjust to create a balance between your security and performance requirements.

You can use Policy Manager to add a proxy policy.

1. Click .  
Or, select **Edit > Add Policies**.  
*The Add Policies dialog box appears.*
2. Expand the **Proxies** folder.  
*A list of proxy policies appears.*
3. Select a proxy policy. Click **Add**.  
*The New Policy Properties dialog box appears.*



For more information on the basic properties of all policies, see *About Policy Properties* on page 391.

Proxy policies and ALGs have default proxy action rulesets that provide a good balance of security and accessibility for most installations. If a default proxy action ruleset does not match the network traffic you want to examine, you can add a new proxy action, or clone an existing proxy action to modify the rules. You cannot modify a default predefined proxy action. For more information, see *About Rules and Rulesets* on page 408 and the *About* topic for the type of policy you added.

*About the DNS-Proxy* on page 419  
*About the FTP-Proxy* on page 428  
*About the H.323-ALG* on page 434  
*About the HTTP-Proxy* on page 440  
*About the HTTPS-Proxy* on page 459

*About the POP3-Proxy* on page 467  
*About the SIP-ALG* on page 480  
*About the SMTP-Proxy* on page 488  
*About the TCP-UDP-Proxy* on page 506

## About the DNS-Proxy

The Domain Name System (DNS) is a network system of servers that translates numeric IP addresses into readable, hierarchical Internet addresses, and vice versa. DNS enables your computer network to understand, for example, that you want to reach the server at 200.253.208.100 when you type a domain name into your browser, such as [www.example.com](http://www.example.com). With Fireware XTM, you have two methods to control DNS traffic: the DNS packet filter and the DNS-proxy policy. The DNS-proxy is useful only if DNS requests are routed through your XTM device.

When you create a new configuration file, the file automatically includes an Outgoing packet filter policy that allows all TCP and UDP connections from your trusted and optional networks to external. This allows your users to connect to an external DNS server with the standard TCP 53 and UDP 53 ports. Because Outgoing is a packet filter, it is unable to protect against common UDP outgoing trojans, DNS exploits, and other problems that occur when you open all outgoing UDP traffic from your trusted networks. The DNS-proxy has features to protect your network from these threats. If you use external DNS servers for your network, the DNS-Outgoing ruleset offers additional ways to control the services available to your network community.

To add the DNS-proxy to your XTM device configuration, see *Add a Proxy Policy to Your Configuration* on page 417.

If you must change the proxy definition, you can use the **New/Edit Proxy Policies** dialog box to modify the definition. This dialog box has three tabs: **Policy**, **Properties**, and **Advanced**.

### Policy Tab

- **DNS-proxy connections are**— Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)** and define who appears in the **From** and **To** list (on the **Policy** tab of the proxy definition). See *Set Access Rules for a Policy* on page 392.
- **Use policy-based routing** — See *Configure Policy-Based Routing* on page 395.
- You can also configure static NAT or configure server load balancing. See *Configure Static NAT* on page 179 and *Configure Server Load Balancing* on page 182.
- **Proxy action** — Select the proxy action to use for this policy. You can also edit the rulesets for proxy actions.

### Properties Tab

- To edit or add a comment to this policy configuration, type the comment in the **Comment** text box.
- To define the logging settings for the policy, click **Logging** and *Set Logging and Notification Preferences* on page 723.
- If you set the **DNS-proxy connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use DNS.  
For more information, see *Block Sites Temporarily with Policy Settings* on page 538.
- To change the idle timeout that is set by the XTM device or authentication server, see *Set a Custom Idle Timeout*.

## Advanced Tab

You can also configure these options in your proxy definition:

- *Set an Operating Schedule*
- *Add a Traffic Management Action to a Policy*
- *Set ICMP Error Handling*
- *Apply NAT Rules* (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- *Enable QoS Marking or Prioritization Settings for a Policy*
- *Set the Sticky Connection Duration for a Policy*

## Configure the Proxy Action

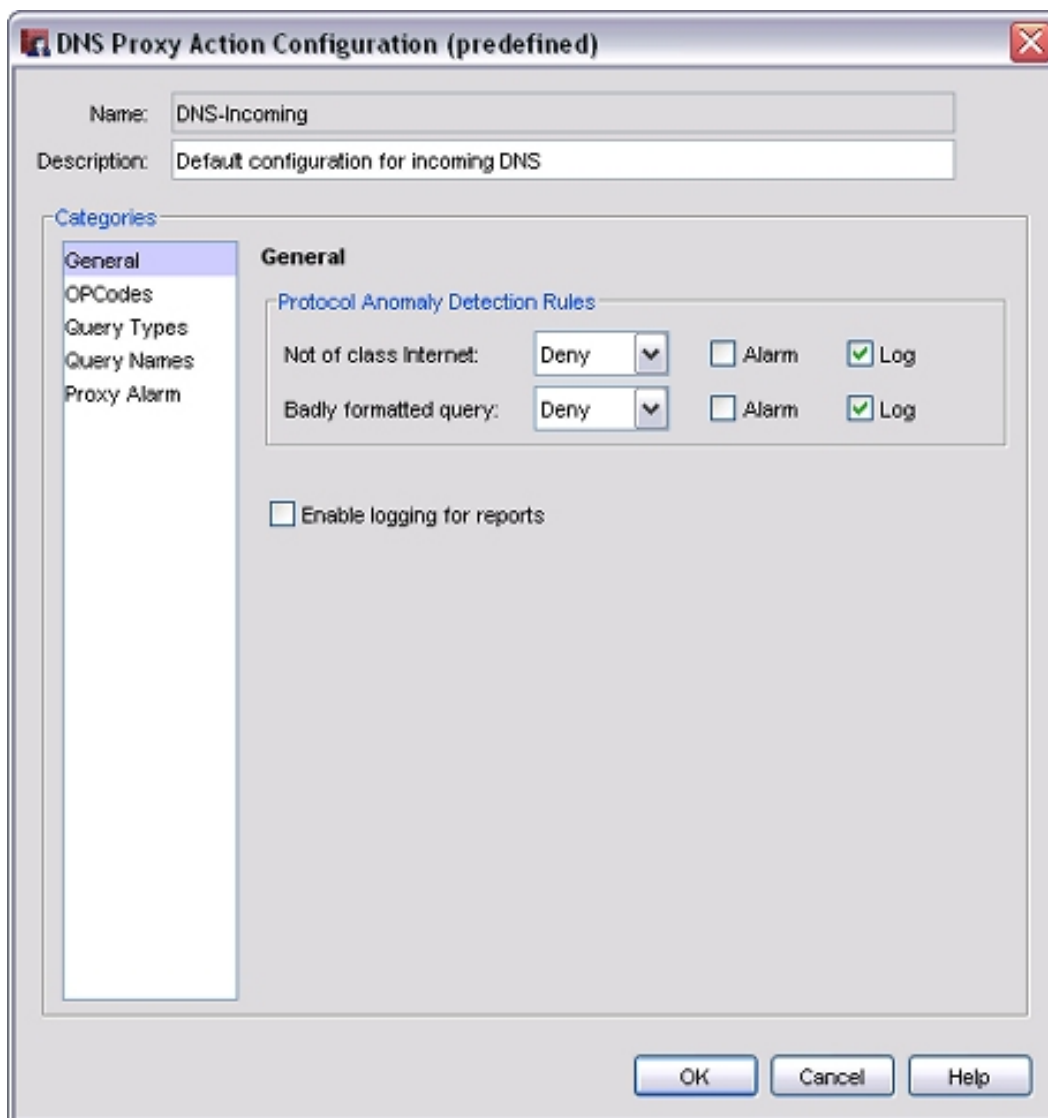
You can choose a predefined proxy action or configure a user-defined proxy action for this proxy. For more information about how to configure proxy actions, see *About Proxy Actions* on page 403.

For the DNS-proxy, you can configure these categories of settings for a proxy action:

- *DNS-Proxy: General Settings*
- *DNS-Proxy: OPcodes*
- *DNS-Proxy: Query Types*
- *DNS-Proxy: Query Names*
- *Proxy and AV Alarms* (SNMP traps and notification are disabled by default)

## DNS-Proxy: General Settings

On the **General** page of the **DNS Proxy Action Configuration** dialog box, you can change the settings of the two protocol anomaly detection rules. We recommend that you do not change the default rule settings. You can also select whether to create a traffic log message for each transaction.



#### *Not of class Internet*

Select the action when the proxy examines DNS traffic that is not of the Internet (IN) class. The default action is to deny this traffic. We recommend that you do not change this default action.

#### *Badly formatted query*

Select the action when the proxy examines DNS traffic that does not use the correct format.

#### *Alarm*

An alarm is a mechanism to tell users when a proxy rule applies to network traffic.

To configure an alarm for this event, select the **Alarm** check box.

To set the options for the alarm, from the **Categories** tree, select **Proxy Alarm**. Alarm notifications are sent in an SNMP trap, email, or a pop-up window.

For more information about proxy alarms, see *Proxy and AV Alarms*.

For more information about notification messages, see *Set Logging and Notification Preferences*.

*Log*

Select this check box to send a message to the traffic log for this event.

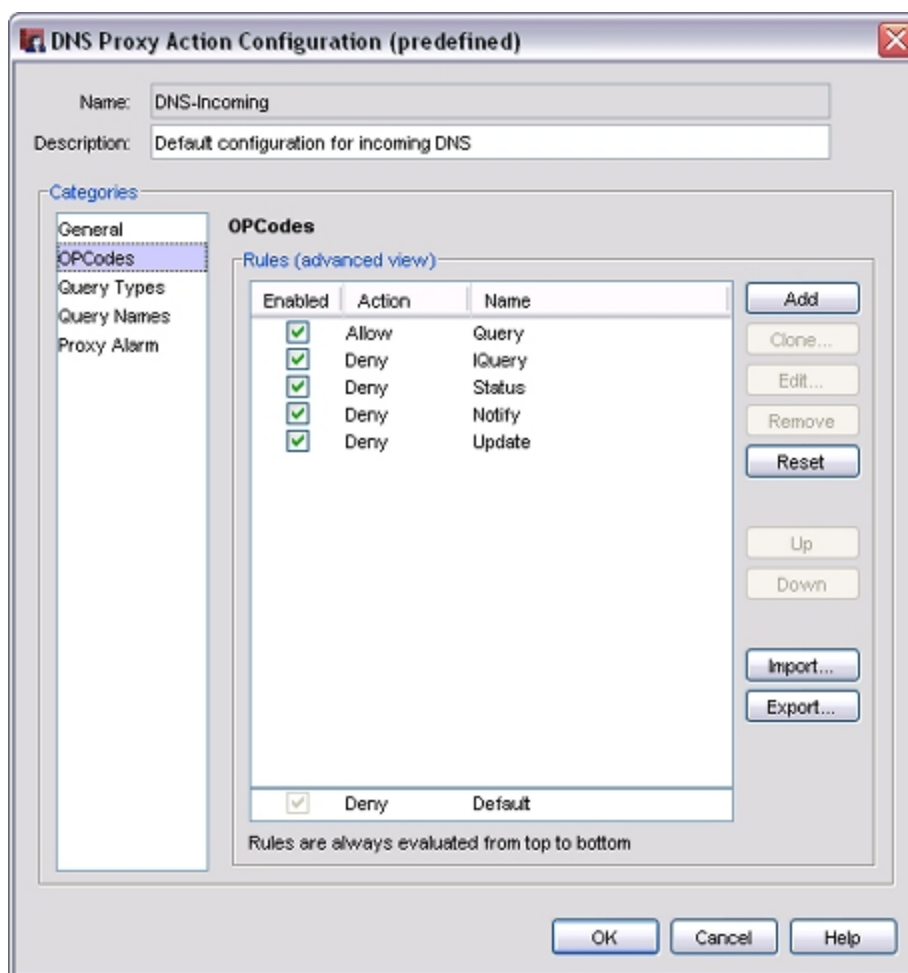
*Enable logging for reports*

Select this check box to create a traffic log message for each transaction. This option creates a large log file, but this information is very important if your firewall is attacked. If you do not select this check box, detailed information about DNS-proxy connections does not appear in your reports.

## DNS-Proxy: OPcodes

DNS OPcodes (operation codes) are commands given to the DNS server that tell it to do some action, such as a query (Query), an inverse query (IQuery), or a server status request (STATUS). They operate on items such as registers, values in memory, values stored on the stack, I/O ports, and the bus. You can add, delete, or modify rules in the default ruleset. You can allow, deny, drop, or block specified DNS OPcodes.

1. In the **Categories** tree, select **OPcodes**.



2. To enable a rule in the list, select the adjacent **Enabled** check box.  
To disable a rule, clear the **Enabled** check box.

**Note** *If you use Active Directory and your Active Directory configuration requires dynamic updates, you must allow DNS OPcodes in your DNS-Incoming proxy action rules. This is a security risk, but can be necessary for Active Directory to operate correctly.*

## Add a New OPcodes Rule

1. Click **Add**.  
*The New OPcodes Rule dialog box appears.*
2. Type a name for the rule.  
*Rule names can have no more than 200 characters.*
3. Click the arrows to set the **OPCode** value. DNS OPcodes have an integer value.

For more information on the integer values of DNS OPcodes, see RFC 1035.

## Delete or Modify Rules

1. Add, delete, or modify rules, as described in *Add, Change, or Delete Rules* on page 409.
2. To change settings for one or more other categories in this proxy, go to the topic on the next category you want to modify.
3. Click **OK**.

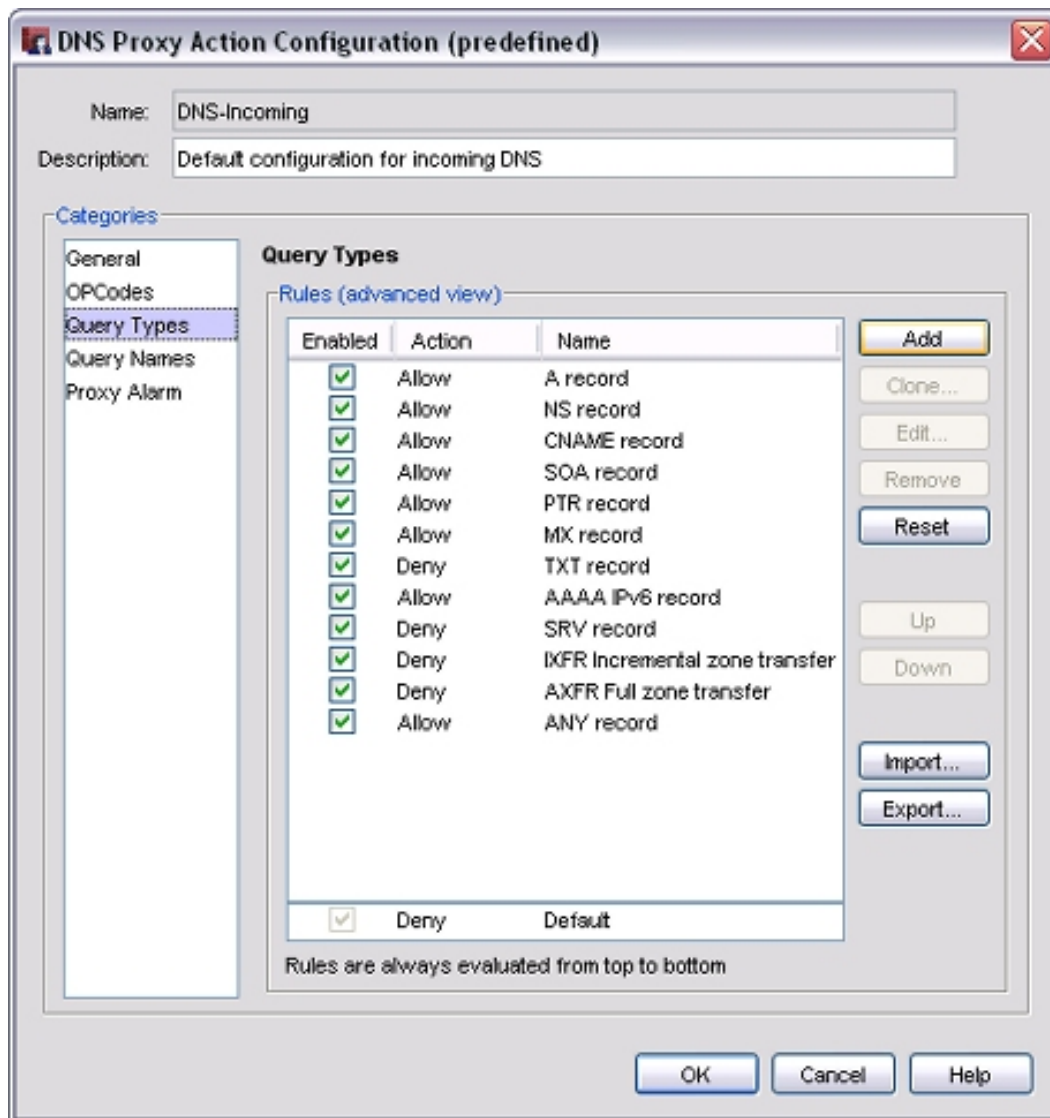
If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

## DNS-Proxy: Query Types

A DNS query type can configure a resource record by type (such as a CNAME or TXT record) or as a custom type of query operation (such as an AXFR Full zone transfer). You can add, delete, or modify rules. You can allow, deny, drop, or block specified DNS query types.

1. In the **Categories** tree, select **Query Types**.



- To enable a rule, select the **Enabled** check box adjacent to the action and name of the rule.

## Add a New Query Types Rule

- To add a new query types rule, click **Add**.  
*The New Query Types Rule dialog box appears.*
- Type a name for the rule.  
*Rules can have no more than 200 characters.*
- DNS query types have a resource record (RR) value. Use the arrows to set the value.  
*For more information on the values of DNS query types, see RFC 1035.*
- Configure the rule action.  
*For more information, see Add, Change, or Delete Rules.*
- To change settings for other categories in this proxy, go to the topic for the next category you want to modify and follow the instructions.
- Click **OK**.



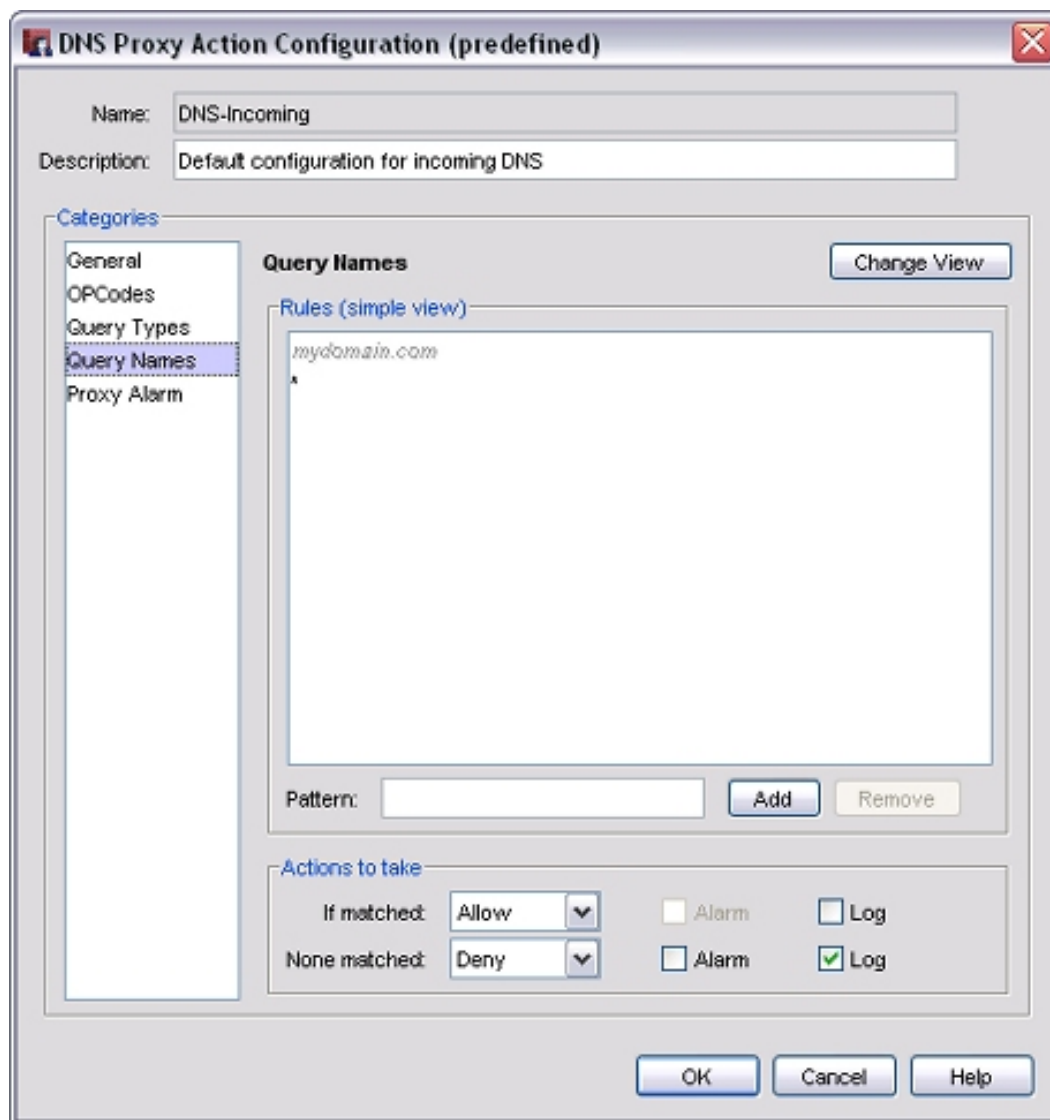
If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

## DNS-Proxy: Query Names

A DNS query name refers to a specified DNS domain name, shown as a fully qualified domain name (FQDN). You can add, delete, or modify rules.

1. In the **Categories** tree, select **Query Names**.



2. Configure the rule action.  
For more information, see *Add, Change, or Delete Rules*.

3. To change settings for other categories in this proxy, go to the topic for the next category you want to modify and follow the instructions.
4. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

## About MX (Mail eXchange) Records

An MX (Mail eXchange) record is a type of DNS record that gives one or more host names of the email servers that are responsible for and authorized to receive email for a given domain. If the MX record has more than one host name, each name has a number that tells which is the most preferred host and which hosts to try next if the most preferred host is not available.

### MX Lookup

When an email server sends email, it first does a DNS query for the MX record of the recipient's domain. When it gets the response, the sending email server knows the host names of authorized mail exchangers for the recipient's domain. To get the IP addresses associated with the MX host names, a mail server does a second DNS lookup for the A record of the host name. The response gives the IP address associated with the host name. This lets the sending server know what IP address to connect to for message delivery.

### Reverse MX Lookup

Many anti-spam solutions, including those used by most major ISP networks and web mail providers such as AOL, MSN, and Yahoo!, use a reverse MX lookup procedure. Different variations of the reverse lookup are used, but the goals are the same: the receiving server wants to verify that the email it receives does not come from a spoofed or forged sending address, and that the sending server is an authorized mail exchanger for that domain.

To verify that the sending server is an authorized email server, the receiving email server tries to find an MX record that correlates to the sender's domain. If it cannot find one, it assumes that the email is spam and rejects it.

The domain name that the receiving server looks up can be:

- Domain name in the email message's **From:** header
- Domain name in the email message's **Reply-To:** header
- Domain name the sending server uses as the FROM parameter of the MAIL command. (An SMTP command is different from an email header. The sending server sends the MAIL FROM: command to tell the receiving sender who the message is from.)
- Domain name returned from a DNS query of the connection's source IP address. The receiving server sometimes does a lookup for a PTR record associated with the IP address. A PTR DNS record is a record that maps an IP address to a domain name (instead of a normal A record, which maps a domain name to an IP address).

Before the receiving server continues the transaction, it makes a DNS query to see whether a valid MX record for the sender's domain exists. If the domain has no valid DNS MX record, then the sender is not valid and the receiving server rejects it as a spam source.

## MX Records and Multi-WAN

Because outgoing connections from behind your XTM device can show different source IP addresses when your XTM device uses multi-WAN, you must make sure that your DNS records include MX records for each external IP address that can show as the source when you send email. If the list of host names in your domain's MX record does not include one for each external XTM device interface, it is possible that some remote email servers could drop your email messages.

For example, Company XYZ has an XTM device configured with multiple external interfaces. The XTM device uses the Failover multi-WAN method. Company XYZ's MX record includes only one host name. This host name has a DNS A record that resolves to the IP address of the XTM device primary external interface.

When Company XYZ sends an email to test@yahoo.com, the email goes out through the primary external interface. The email request is received by one of Yahoo's many email servers. That email server does a reverse MX lookup to verify the identify of Company XYZ. The reverse MX lookup is successful, and the email is sent.

If a WAN failover event occurs at the XTM device, all outgoing connections from Company XYZ start to go out the secondary, backup external interface. In this case, when the Yahoo email server does a reverse MX lookup, it does not find an IP address in Company XYZ's MX and A records that matches, and it rejects the email. To solve this problem, make sure that:

- The MX record has multiple host names, at least one for each external XTM device interface.
- At least one host name in the MX record has a DNS A record that maps to the IP address assigned to each XTM device interface.

## Add Another Host Name to an MX Record

MX records are stored as part of your domain's DNS records. For more information on how to set up your MX records, contact your DNS host provider (if someone else hosts your domain's DNS service) or consult the documentation from the vendor of your DNS server software.

## About the FTP-Proxy

FTP (File Transfer Protocol) is used to send files from one computer to a different computer over a TCP/IP network. The FTP client is usually a computer. The FTP server can be a resource that keeps files on the same network or on a different network. The FTP client can be in one of two modes for data transfer: active or passive. In active mode, the server starts a connection to the client on source port 20. In passive mode, the client uses a previously negotiated port to connect to the server. The FTP-proxy monitors and scans these FTP connections between your users and the FTP servers they connect to.

With an FTP-proxy policy, you can:

- Set the maximum user name length, password length, file name length, and command line length allowed through the proxy to help protect your network from buffer overflow attacks.
- Control the type of files that the FTP-proxy allows for downloads and uploads.

The TCP/UDP proxy is available for protocols on non-standard ports. When FTP uses a port other than port 20, the TCP/UDP proxy relays the traffic to the FTP-proxy. For information on the TCP/UDP proxy, see *About the TCP-UDP-Proxy* on page 506.

For detailed instructions on how to add the FTP-proxy to your XTM device configuration, see *Add a Proxy Policy to Your Configuration* on page 417.

If you must change the proxy definition, you can use the **New/Edit Proxy Policies** dialog box to modify the definition. This dialog box has three tabs: **Policy**, **Properties**, and **Advanced**.

## Policy Tab

To set access rules and other options, select the **Policy** tab.

- **FTP-proxy connections are** — Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)**. Define who appears in the **From** and **To** lists.  
For more information, see *Set Access Rules for a Policy*.
- **Use policy-based routing** — To use policy-based routing in your proxy definition, see *Configure Policy-Based Routing*.
- You can also configure static NAT or configure server load balancing.  
For more information, see *Configure Static NAT* on page 179 or *Configure Server Load Balancing* on page 182.
- **Proxy action** — Select the proxy action to use for this policy. You can also edit the rulesets for proxy actions.

## Properties Tab

- To edit or add a comment to this policy configuration, type the comment in the **Comment** text box.
- To define the logging settings for the policy, click **Logging** and *Set Logging and Notification Preferences* on page 723.
- If you set the **FTP-proxy connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use FTP.  
For more information, see *Block Sites Temporarily with Policy Settings* on page 538.
- To change the idle timeout that is set by the XTM device or authentication server, see *Set a Custom Idle Timeout*.

## Advanced Tab

You can also configure these options in your proxy definition:

- *Set an Operating Schedule*
- *Add a Traffic Management Action to a Policy*
- *Set ICMP Error Handling*
- *Apply NAT Rules* (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- *Enable QoS Marking or Prioritization Settings for a Policy*
- *Set the Sticky Connection Duration for a Policy*

## Configure the Proxy Action

You can choose a predefined proxy action or configure a user-defined proxy action for this proxy. For more information about how to configure proxy actions, see *About Proxy Actions* on page 403.

For the FTP-proxy, you can configure these categories of settings for a proxy action:

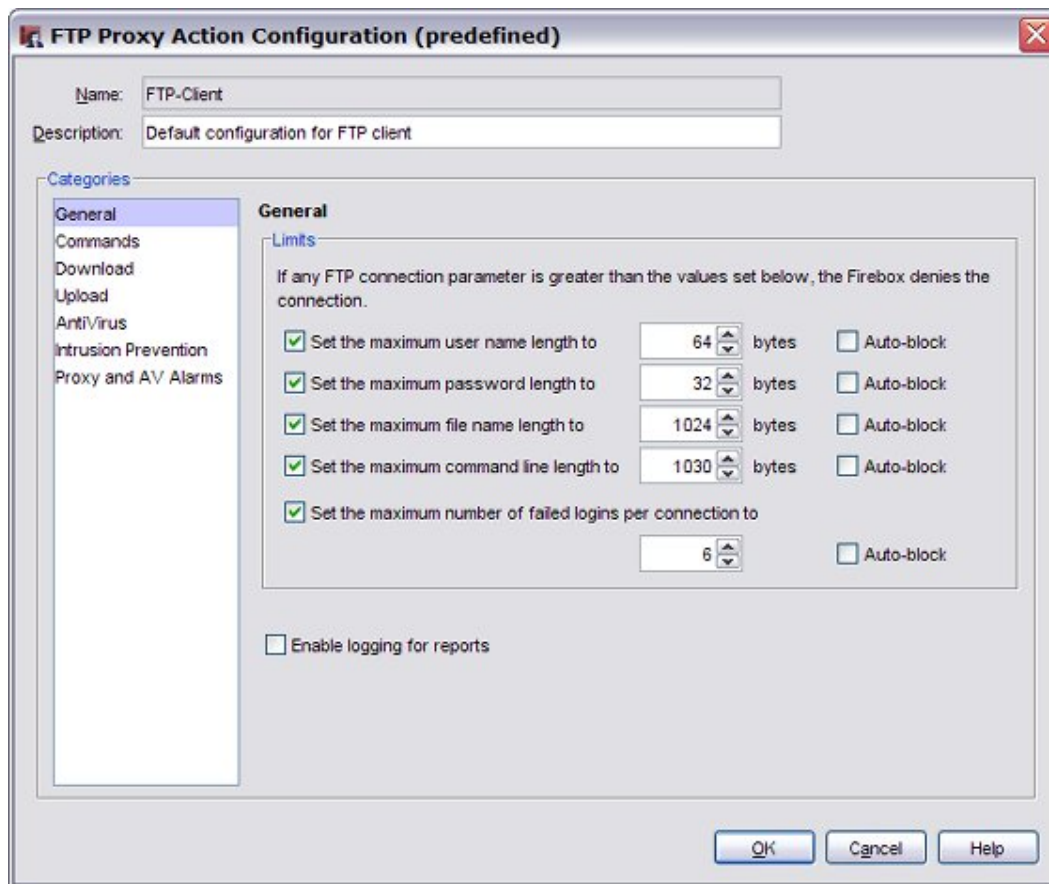
- *FTP-Proxy: General Settings*
- *FTP-Proxy: Commands*
- *FTP-Proxy: Content*
- *FTP-Proxy: AntiVirus*
- *Proxy and AV Alarms*

## FTP-Proxy: General Settings

On the **General** page of the **FTP Proxy Action Configuration** dialog box, you can set basic FTP parameters including maximum user name length.

1. In the **Categories** tree, select **General**.

*The General page appears.*



2. To set limits for FTP parameters, select the applicable check boxes. These settings help to protect your network from buffer overflow attacks.

*Set the maximum user name length to*

Sets a maximum length for user names on FTP sites.

*Set the maximum password length to*

Sets a maximum length for passwords used to log in to FTP sites.

*Set the maximum file name length to*

Sets the maximum file name length for files to upload or download.

*Set the maximum command line length to*

Sets the maximum length for command lines used on FTP sites.

*Set the maximum number of failed logins per connection to*

Allows you to limit the number of failed connection requests to your FTP site. This can protect your site against brute force attacks.

3. In the text box for each setting, type or select the limit for the selected parameter.
4. For each setting, select or clear the **Auto-block** check box.  
If someone tries to connect to an FTP site and exceeds a limit whose **Auto-block** check box is selected, the computer that sent the commands is added to the temporary Blocked Sites List.
5. To create a log message for each transaction, select the **Enable logging for reports** check box.  
You must select this option to get detailed information on FTP traffic.
6. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
7. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

## FTP-Proxy: Commands

FTP has a number of commands to manage files. You can configure rules to put limits on some FTP commands. To put limits on commands that can be used on an FTP server protected by the XTM device, you can configure the FTP-Server proxy action.

The default configuration of the FTP-Server proxy action blocks these commands:

```

ABOR*  HELP*  PASS*  REST*  STAT*  USER*
APPE*  LIST*  PASV*  RETR*  STOR*  XCUP*
CDUP*  MKD*   PORT*  RMD*   STOU*  XCWD*
CWD*   NLST*  PWD*   RNFR*  SYST*  XMKD*
DELE*  NOOP*  QUIT*  RNT0*  TYPE*  XRMD*

```

Use the FTP-Client proxy action to put limits on commands that users protected by the XTM device can use when they connect to external FTP servers. The default configuration of the FTP-Client is to allow all FTP commands.

You can add, delete, or modify rules. You usually should not block these commands, because they are necessary for the FTP protocol to work correctly.

Protocol Command	Client Command	Description
USER	n/a	Sent with login name
PASS	n/a	Sent with password
PASV	pasv	Select passive mode for data transfer
SYST	syst	Print the server's operating system and version. FTP clients use this information to correctly interpret and show a display of server responses.

To add, delete, or modify rules:

1. In the **Categories** tree, select **Commands**.
2. *Add, Change, or Delete Rules.*
3. If you want to change settings for one or more other categories in this proxy, go to the topic for the next category you want to modify.
4. If you are finished with your changes to this proxy definition, click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

## FTP-Proxy: Content

You can control the type of files that the FTP-proxy allows for downloads and uploads. For example, because many hackers use executable files to deploy viruses or worms on a computer, you could deny requests for \*.exe files. Or, if you do not want to let users upload Windows Media files to an FTP server, you could add \*.wma to the proxy definition and specify that these files are denied. Use the asterisk (\*) as a wildcard character.

Use the FTP-Server proxy action to control rules for an FTP server protected by the XTM device. Use the FTP-Client proxy action to set rules for users connecting to external FTP servers.

1. In the **Categories** tree, select **Upload** or **Download**.
2. *Add, Change, or Delete Rules.*
3. If you want uploaded files to be scanned for viruses by Gateway AntiVirus, from the **Actions to take** drop-down list, select **AV Scan** for one or more rules.
4. To change settings for one or more other categories in this proxy, see the topics on the categories you want to modify.
5. When you are finished with your changes to this proxy action definition, click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.



## FTP-Proxy: AntiVirus

If you have purchased and enabled the Gateway AntiVirus feature, the fields in the AntiVirus category set the actions necessary if a virus is found in a file that is uploaded or downloaded.

- To use the proxy definition screens to activate Gateway AntiVirus, see *Activate Gateway AntiVirus from Proxy Definitions* on page 1171.
- To use the **Subscription Services** menu in Policy Manager to activate Gateway AntiVirus, see *Activate Gateway AntiVirus with a Wizard from Policy Manager* on page 1168.
- To configure Gateway AntiVirus for the FTP-proxy, see *Configure Gateway AntiVirus Actions* on page 1172.

When you enable Gateway AntiVirus, you must set the actions to be taken if a virus or error is found in an uploaded or downloaded file. The options for antivirus actions are:

### *Allow*

Allows the packet to go to the recipient, even if the content contains a virus.

### *Deny*

Deny the file and send a deny message.

### *Drop*

Drops the packet and drops the connection. No information is sent to the source of the message.

### *Block*

Blocks the packet, and adds the IP address of the sender to the Blocked Sites list.

Gateway AntiVirus scans each file up to a specified kilobyte count. Any additional bytes in the file are not scanned. This allows the proxy to partially scan very large files without a large effect on performance. Enter the file scan limit in the **Limit scanning to first** field.

For information about the default and maximum scan limits for each XTM device model, see *About Gateway AntiVirus Scan Limits* on page 1181.

## About the H.323-ALG

If you use Voice-over-IP (VoIP) in your organization, you can add an H.323 or SIP (Session Initiation Protocol) ALG (Application Layer Gateway) to open the ports necessary to enable VoIP through your XTM device. An ALG is created in the same way as a proxy policy and offers similar configuration options. These ALGs have been created to work in a NAT environment to maintain security for privately addressed conferencing equipment protected by your XTM device.

H.323 is commonly used on videoconferencing equipment. SIP is commonly used with IP phones. You can use both H.323 and SIP ALGs at the same time, if necessary. To determine which ALG to add, consult the documentation for your VoIP devices or applications.

## VoIP Components

It is important to understand that you usually implement VoIP by using either:

### *Peer-to-peer connections*

In a peer-to-peer connection, each of the two devices knows the IP address of the other device and connects to the other directly, without the use of a proxy server to route their calls. If both peers are behind the XTM device, the XTM device can route the call traffic correctly.

### *Hosted connections*

Connections hosted by a call management system (PBX)

With H.323, the key component of call management is known as a *gatekeeper*. A gatekeeper manages VoIP calls for a group of users, and can be located on a network protected by your XTM device or at an external location. For example, some VoIP providers host a gatekeeper on their network that you must connect to before you can place a VoIP call. Other solutions require you to set up and maintain a gatekeeper on your network.

Coordinating the many components of a VoIP installation can be difficult. We recommend you make sure that VoIP connections work successfully before you add a H.323 or SIP ALG. This can help you to troubleshoot any problems.

## ALG Functions

When you enable an H.323-ALG, your XTM device:

- Automatically responds to VoIP applications and opens the appropriate ports
- Makes sure that VoIP connections use standard H.323 protocols
- Generates log messages for auditing purposes

Many VoIP devices and servers use NAT (Network Address Translation) to open and close ports automatically. The H.323 and SIP ALGs also perform this function. You must disable NAT on your VoIP devices if you configure an H.323 or SIP ALG.

To change the ALG definition, you can use the **New/Edit Proxy Policies** dialog box. This dialog box has three tabs: **Policy**, **Properties**, and **Advanced**.

For more information on how to add a proxy to your configuration, see *Add a Proxy Policy to Your Configuration* on page 417.

## Policy Tab

- **H.323-ALG connections are** — Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)** and define who appears in the **From** and **To** list (on the **Policy** tab of the ALG definition). For more information, see *Set Access Rules for a Policy* on page 392.
- **Use policy-based routing** — If you want to use policy-based routing in your proxy definition, see *Configure Policy-Based Routing* on page 395.
- You can also configure static NAT or configure server load balancing. For more information, see *Configure Static NAT* on page 179 and *Configure Server Load Balancing* on page 182.
- **Proxy action** — Select the proxy action to use for this policy. You can also edit the rulesets for proxy actions.

## Properties Tab

- To edit or add a comment to this policy configuration, type the comment in the **Comment** text box.
- To define the logging settings for the policy, click **Logging** and *Set Logging and Notification Preferences* on page 723.
- If you set the **H.323-ALG connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use H.323. For more information, see *Block Sites Temporarily with Policy Settings* on page 538.
- To change the idle timeout that is set by the XTM device or authentication server, see *Set a Custom Idle Timeout*.

## Advanced Tab

You can also configure these options in your proxy definition:

- *Set an Operating Schedule*
- *Add a Traffic Management Action to a Policy*
- *Set ICMP Error Handling*
- *Apply NAT Rules* (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- *Enable QoS Marking or Prioritization Settings for a Policy*
- *Set the Sticky Connection Duration for a Policy*

## Configure the Proxy Action

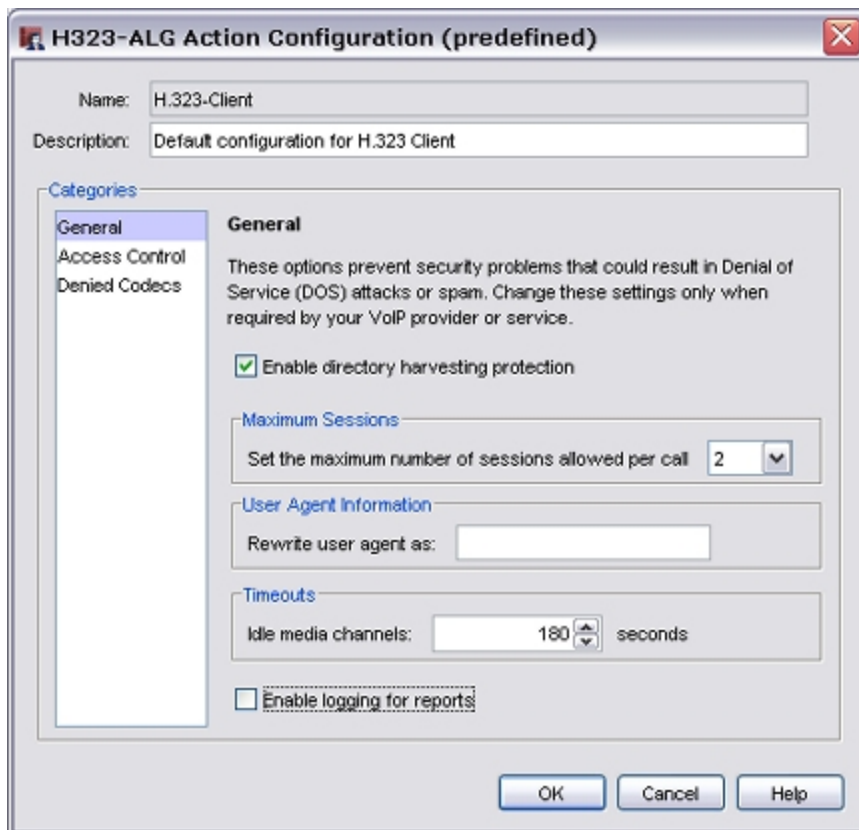
You can choose a predefined proxy action or configure a user-defined proxy action for this proxy. For more information about how to configure proxy actions, see *About Proxy Actions* on page 403.

For the H.323-ALG, you can configure these categories of settings for a proxy action:

- *H.323-ALG: General Settings*
- *H.323-ALG: Access Control*
- *H.323 ALG: Denied Codecs*

## H.323-ALG: General Settings

On the **H323-ALG Action Configuration** dialog box, in the **General** category, you can set security and performance options for the H.323-ALG (Application Layer Gateway).



### *Enable directory harvesting protection*

Select this check box to prevent attackers from stealing user information from VoIP gatekeepers protected by your XTM device. This option is enabled by default.

### *Maximum sessions*

Use this feature to restrict the maximum number of audio or video sessions that can be created with a single VoIP call. For example, If you set the number of maximum sessions to one and participate in a VoIP call with both audio and video, the second connection is dropped. The default value is two sessions, and the maximum value is four sessions. The XTM device creates a log entry when it denies a media session above this number.

### *User agent information*

To have outgoing H.323 traffic identify as a client you specify, in the **Rewrite user agent as** text box, type a new user agent string. To remove the false user agent, clear the text box.

### Timeouts

When no data is sent for a specified amount of time on a VoIP audio, video, or data channel, your XTM device closes that network connection. The default value is 180 seconds (three minutes) and the maximum value is 3600 seconds (sixty minutes).

To specify a different time interval, in the **Idle media channels** text box, type the amount in seconds.

### Enable logging for reports

To send a log message for each connection request managed by the H.323-ALG, select this check box. This option is necessary to create accurate reports on H.323 traffic.

## H.323-ALG: Access Control

On the **Access Control** page of the H.323-ALG (Application Layer Gateway) configuration, you can create a list of users who are allowed to send VoIP network traffic.

**H323-ALG Action Configuration (predefined)**

Name: H.323-Client  
Description: Default configuration for H.323 Client

**Categories**

- General
- Access Control
- Denied Codecs

**Access Control**

Enable access control for VoIP

**Default Settings**

Allow users to:

Start VoIP calls       Log

Receive VoIP calls       Log

**Access Levels**

The access levels you set here take precedence over the default settings.

Address of Record      Access level

     Start calls Only      Add

Name	Access Level	Log

Remove

OK      Cancel      Help

### Enable access control for VoIP

Select this check box to enable the access control feature. When enabled, the H.323-ALG allows or restricts calls based on the options you set.

### Default Settings

To enable all VoIP users to start calls by default, select the **Start VoIP calls** check box.

To enable all VoIP users to receive calls by default, select the **Receive VoIP calls** check box.

To create a log message for each H.323 VoIP connection started or received, select the adjacent **Log** check box.

#### *Access Levels*

To create an exception to the default settings you specified, type the **Address of Record** (the address that shows up in the TO and FROM headers of the packet) for the exception. This is usually an H.323 address in the format *user@domain*, such as *myuser@example.com*.

From the **Access Levels** drop-down list, select an access level and click **Add**.

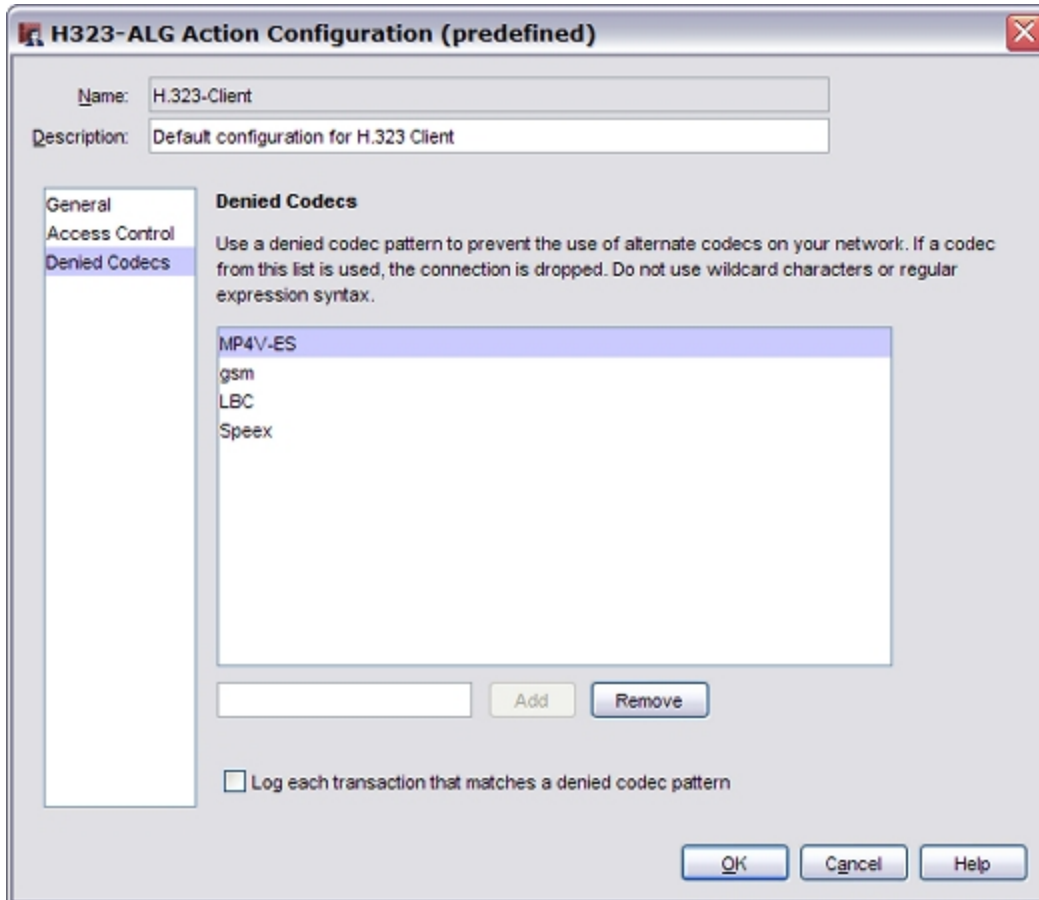
You can allow users to **Start calls only**, **Receive calls only**, **Start and receive calls**, or give them **No VoIP access**. These settings apply only to H.323 VoIP traffic.

To delete an exception, select it in the list and click **Remove**.

Connections made by users who have an access level exception are logged by default. If you do not want to log connections made by a user with an access level exception, clear the **Log** check box adjacent to the exception name in the list.

## H.323 ALG: Denied Codecs

On the **Denied Codecs** page, you can set the VoIP voice, video, and data transmission codecs that you want to deny on your network.



### *Denied Codecs list*

Use this feature to deny one or more VoIP codecs. When an H.323 VoIP connection is opened that uses a codec specified in this list, your XTM device closes the connection automatically. This list is empty by default. We recommend that you add a codec to this list if it consumes too much bandwidth, presents a security risk, or if it is necessary to have your VoIP solution operate correctly. For example, you may choose to deny the G.711 or G.726 codecs because they use more than 32 Kb/sec of bandwidth, or you may choose to deny the Speex codec because it is used by an unauthorized VOIP codec.

To add a codec to the list, type the codec name or unique text pattern in the text box and click **Add**. Do not use wildcard characters or regular expression syntax. The codec patterns are case sensitive.

To delete a codec from the list, select it and click **Remove**.

*Log each transaction that matches a denied codec pattern*

To send a log message when your XTM device denies H.323 traffic that matches a codec in this list, select this option.

## About the HTTP-Proxy

Hyper Text Transfer Protocol (HTTP) is a request/response protocol between clients and servers. The HTTP client is usually a web browser. The HTTP server is a remote resource that stores HTML files, images, and other content. When the HTTP client starts a request, it establishes a TCP (Transmission Control Protocol) connection on Port 80. An HTTP server listens for requests on Port 80. When it receives the request from the client, the server replies with the requested file, an error message, or some other information.

The HTTP-proxy is a high-performance content filter. It examines Web traffic to identify suspicious content that can be a virus or other type of intrusion. It can also protect your HTTP server from attacks.

With an HTTP-proxy filter, you can:

- Adjust timeout and length limits of HTTP requests and responses to prevent poor network performance, as well as several attacks.
- Customize the deny message that users see when they try to connect to a web site blocked by the HTTP-proxy.
- Filter web content MIME types.
- Block specified path patterns and URLs.
- Deny cookies from specified web sites.

You can also use the HTTP-proxy with the WebBlocker security subscription. For more information, see *About WebBlocker* on page 1065.

To enable your users to download Windows updates through the HTTP-proxy, you must change your HTTP-proxy settings. For more information, see *Enable Windows Updates Through the HTTP-Proxy*.

The TCP/UDP proxy is available for protocols on non-standard ports. When HTTP uses a port other than Port 80, the TCP/UDP proxy sends the traffic to the HTTP-proxy. For more information on the TCP/UDP proxy, see *About the TCP-UDP-Proxy* on page 506.

To add the HTTP-proxy to your XTM device configuration, see *Add a Proxy Policy to Your Configuration* on page 417.

If you must change the proxy definition, you can use the **New/Edit Proxy Policies** dialog box to modify the definition. This dialog box has three tabs: **Policy**, **Properties**, and **Advanced**.

You can also configure subscription service settings for the HTTP-proxy. For more information, see:

- *Get Started with WebBlocker*
- *Configure Gateway AntiVirus Actions*
- *Configure Reputation Enabled Defense*
- *Configure Application Control for Policies*



## Policy Tab

- **HTTP-proxy connections are** — Specify whether connections are **Allowed, Denied, or Denied (send reset)** and select the users, computers, or networks that appear in the **From** and **To** list (on the **Policy** tab of the proxy definition). For more information, see *Set Access Rules for a Policy* on page 392.
- **Use policy-based routing** — To use policy-based routing in your proxy definition, see *Configure Policy-Based Routing* on page 395.
- You can also configure static NAT or configure server load balancing.  
For more information, see *Configure Static NAT* on page 179 and *Configure Server Load Balancing* on page 182.
- **Proxy action** — Select the proxy action to use for this policy. You can also edit the rulesets for proxy actions.

## Properties Tab

- To define the logging settings for the policy, click **Logging** and *Set Logging and Notification Preferences* on page 723.
- If you set the **HTTP-proxy connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block devices that try to connect on port 80.  
For more information, see *Block Sites Temporarily with Policy Settings* on page 538.
- To change the idle timeout that is set by the XTM device or authentication server, see *Set a Custom Idle Timeout*.

## Advanced Tab

You can also configure these options in your proxy definition:

- *Set an Operating Schedule*
- *Add a Traffic Management Action to a Policy*
- *Set ICMP Error Handling*
- *Apply NAT Rules* (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- *Enable QoS Marking or Prioritization Settings for a Policy*
- *Set the Sticky Connection Duration for a Policy*

## Configure the Proxy Action

You can choose a predefined proxy action or configure a user-defined proxy action for this proxy. For more information about how to configure proxy actions, see *About Proxy Actions* on page 403.

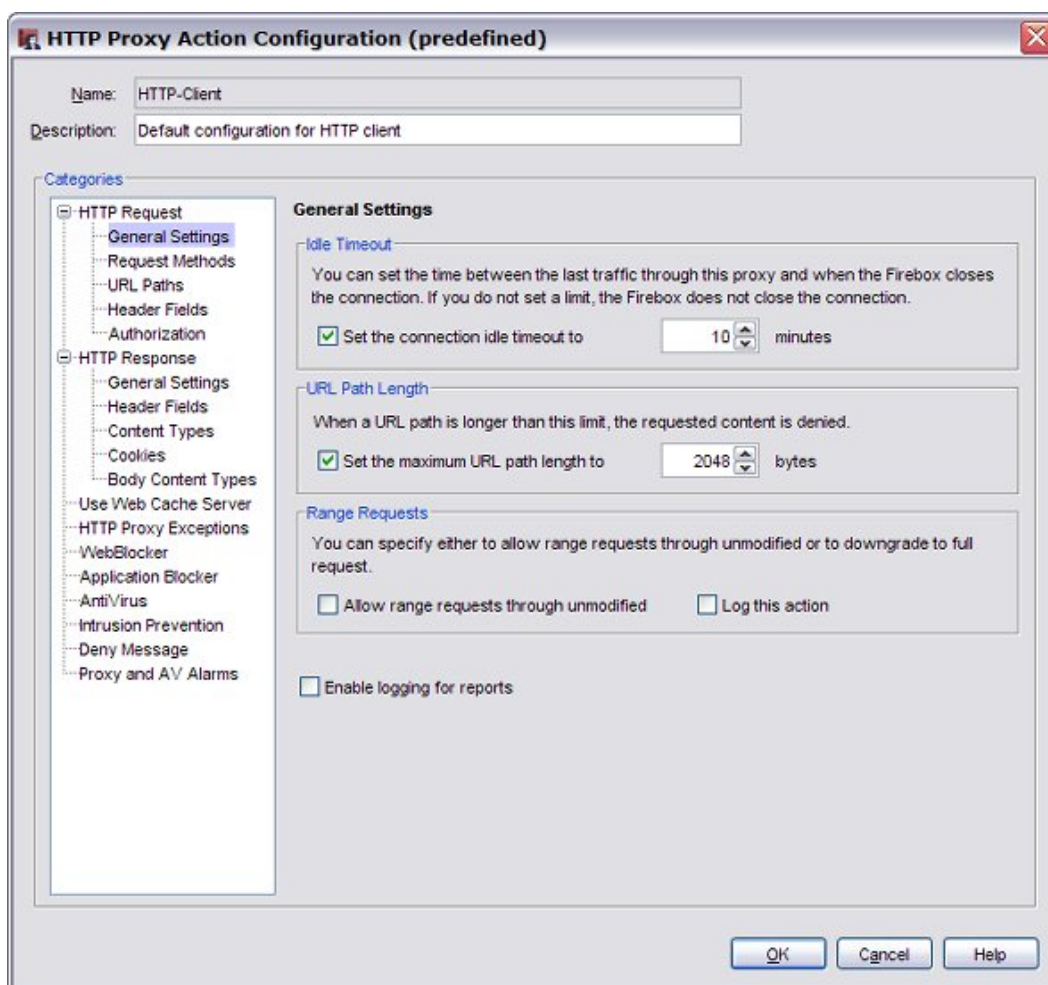
For the HTTP-proxy, you can configure these categories of settings for a proxy action:

- *HTTP Request: General Settings* on page 442
- *HTTP Request: Request Methods* on page 444
- *HTTP Request: URL Paths* on page 445
- *HTTP Request: Header Fields* on page 445
- *HTTP Request: Authorization* on page 446
- *HTTP Response: General Settings* on page 447
- *HTTP Response: Header Fields* on page 448
- *HTTP Response: Content Types* on page 449

- *HTTP Response: Cookies* on page 451
- *HTTP Response: Body Content Types* on page 452
- *Use a Caching Proxy Server* on page 457
- *HTTP-Proxy: Exceptions* on page 452
- *HTTP-Proxy: WebBlocker* on page 453
- *HTTP-Proxy: Deny Message* on page 455
- *Proxy and AV Alarms* on page 402

## HTTP Request: General Settings

On the **HTTP Proxy Action Configuration** dialog box **General Settings** page, you can set basic HTTP parameters such as idle time out and URL length.



### Idle Timeout

This option controls performance.

To close the TCP socket for the HTTP when no packets have passed through the TCP socket in the amount of time you specify, select the **Set the connection idle timeout to** check box. In the adjacent text box, type or select the number of minutes before the proxy times out.

Because every open TCP session uses a small amount of memory on the XTM device, and browsers and servers do not always close HTTP sessions cleanly, we recommend that you keep this check box selected. This makes sure that stale TCP connections are closed and helps the XTM device save memory. You can lower the timeout to five minutes and not reduce performance standards.

#### *URL Path Length*

To set the maximum number of characters allowed in a URL, select the **Set the maximum URL path link to** check box.

In this area of the proxy, *URL* includes anything in the web address after the top-level-domain. This includes the slash character but not the host name (*www.myexample.com* or *myexample.com*). For example, the URL *www.myexample.com/products* counts nine characters toward this limit because */products* has nine characters.

The default value of 2048 is usually enough for any URL requested by a computer behind your XTM device. A URL that is very long can indicate an attempt to compromise a web server. The minimum length is 15 bytes. We recommend that you keep this setting enabled with the default settings. This helps protect against infected web clients on the networks that the HTTP-proxy protects.

#### *Range Requests*

To allow range requests through the XTM device, select this check box. Range requests allow a client to request subsets of the bytes in a web resource instead of the full content. For example, if you want only some sections of a large Adobe file but not the whole file, the download occurs more quickly and prevents the download of unnecessary pages if you can request only what you need.

Range requests introduce security risks. Malicious content can hide anywhere in a file and a range request makes it possible for any content to be split across range boundaries. The proxy can fail to see a pattern it is looking for when the file spans two GET operations. If you have a subscription for Gateway AntiVirus (Gateway AV) or the signature-based Intrusion Prevention Service (IPS), and you enable either of those subscription services, Firewall denies range requests regardless of whether this check box is selected.

We recommend that you do not select this check box if the rules you make in the Body Content Types section of the proxy are designed to identify byte signatures deep in a file, instead of just in the file header.

To add a traffic log message when the proxy takes the action indicated in the check box for range requests, select the **Log this action** check box.

#### *Enable logging for reports*

To create a traffic log message for each transaction, select this check box. This option creates a large log file, but this information is very important if your firewall is attacked. If you do not select this check box, you do not see detailed information about HTTP-proxy connections in reports.

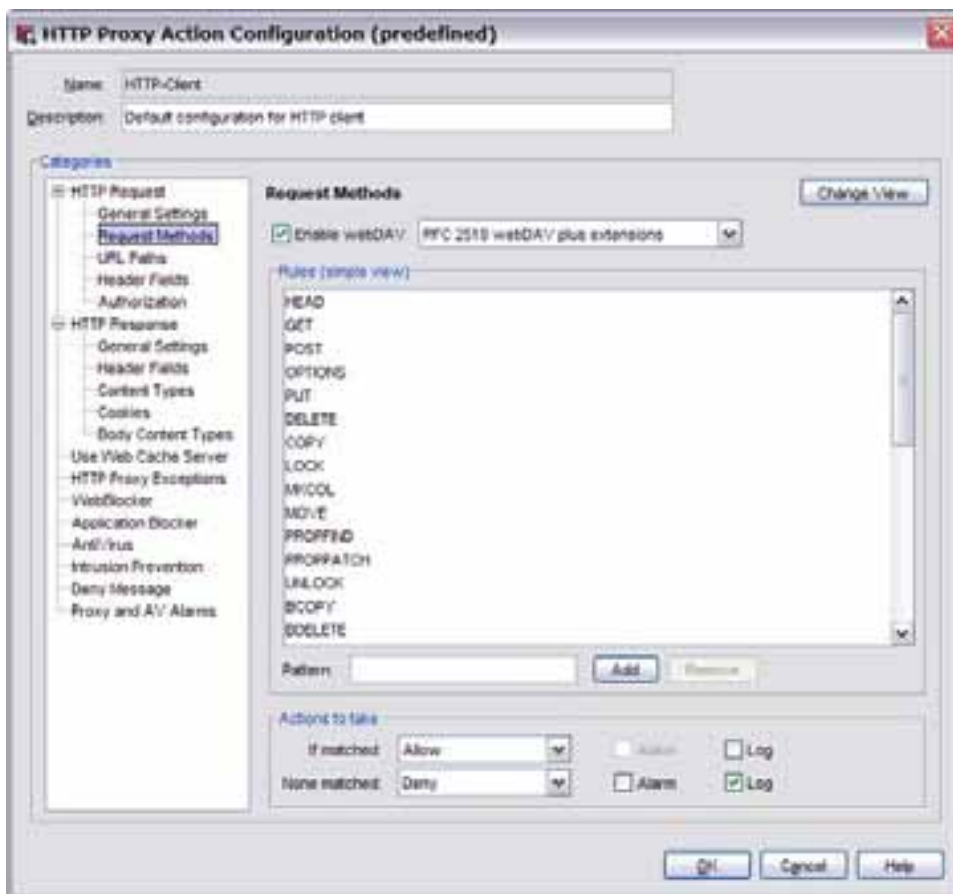
## HTTP Request: Request Methods

Most browser HTTP requests are in one of two categories: GET or POST operations. Browsers usually use GET operations to download objects such as a graphic, HTML data, or Flash data. More than one GET is usually sent by a client computer for each page, because web pages usually contain many different elements. The elements are put together to make a page that appears as one page to the end user.

Browsers usually use POST operations to send data to a web site. Many web pages get information from the end user such as location, email address, and name. If you disable the POST command, the XTM device denies all POST operations to web servers on the external network. This feature can prevent your users from sending information to a web site on the external network.

Web-based Distributed Authoring and Versioning (webDAV) is a set of HTTP extensions that allows users to edit and manage files on remote web servers. WebDAV is compatible with Outlook Web Access (OWA). If webDAV extensions are not enabled, the HTTP proxy supports these request methods: HEAD, GET, POST, OPTIONS, PUT, and DELETE. For HTTP-Server, the proxy supports these request methods by default: HEAD, GET, and POST. The proxy also includes these options (disabled by default): OPTIONS, PUT, and DELETE.

1. In the **Categories** tree, select **HTTP Request > Request Methods**.  
*The Rules (simple view) list appears.*



2. To enable your users to use these extensions, select the **Enable webDAV** check box.  
 Many extensions to the base webDAV protocol are also available. If you enable webDAV, from the

adjacent check box, select whether you want to enable only the extensions described in RFC 2518 or if you want to include an additional set of extensions to maximize interoperability.

3. *Add, Change, or Delete Rules.*
4. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
5. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

## HTTP Request: URL Paths

A URL (Uniform Resource Locator) identifies a resource on a remote server and gives the network location on that server. The URL path is the string of information that comes after the top level domain name. You can use the HTTP-proxy to block web sites that contain specified text in the URL path. You can add, delete, or modify URL path patterns. Here are examples of how to block content with HTTP request URL paths:

- To block all pages that have the host name `www.test.com`, type the pattern: `www.test.com*`
- To block all paths containing the word `sex`, on all web sites: `*sex*`
- To block URL paths ending in `.test`, on all web sites: `*.test`

**Note** *If you filter URLs with the HTTP request URL path ruleset, you must configure a complex pattern that uses full regular expression syntax from the advanced view of a ruleset. It is easier and gives better results to filter based on header or body content type than it is to filter by URL path.*

To block web sites with specific text in the URL path:

1. In the **Categories** tree, select **HTTP Request > URL paths**.  
*The Rules (simple view) list appears.*
2. *Add, Change, or Delete Rules.*
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

## HTTP Request: Header Fields

This ruleset supplies content filtering for the full HTTP header. By default, the HTTP proxy uses exact matching rules to strip *Via* and *From* headers, and allows all other headers. This ruleset matches the full header, not only the name.

To match all values of a header, type the pattern: “[header name]:\*”. To match only some values of a header, replace the asterisk (\*) wildcard with a pattern. If your pattern does not start with an asterisk (\*) wildcard, include one space between the colon and the pattern when you type in the **Pattern** text box. For example, type: [header name]: [pattern], not [header name]:[pattern].

The default rules do not strip the *Referer* header, but do include a disabled rule to strip this header. To enable the rule to strip the header, select **Change View**. Some web browsers and software applications must use the Referer header to operate correctly.

1. In the **Categories** tree, select **HTTP Request > Header Fields**.  
*The Rules (simple view) list appears.*
2. *Add, Change, or Delete Rules.*
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

## HTTP Request: Authorization

This rule sets the criteria for content filtering of HTTP Request Header authorization fields. When a web server starts a *WWW-Authenticate* challenge, it sends information about which authentication methods it can use. The proxy puts limits on the type of authentication sent in a request. It uses only the authentication methods that the web server accepts. With a default configuration, the XTM device allows Basic, Digest, NTLM, and Passport1.4 authentication, and strips all other authentication. You can add, delete, or modify rules in the default ruleset.

1. In the **Categories** tree, select **HTTP Request > Authorization**.  
*The Rules (simple view) list appears.*
2. *Add, Change, or Delete Rules.*
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

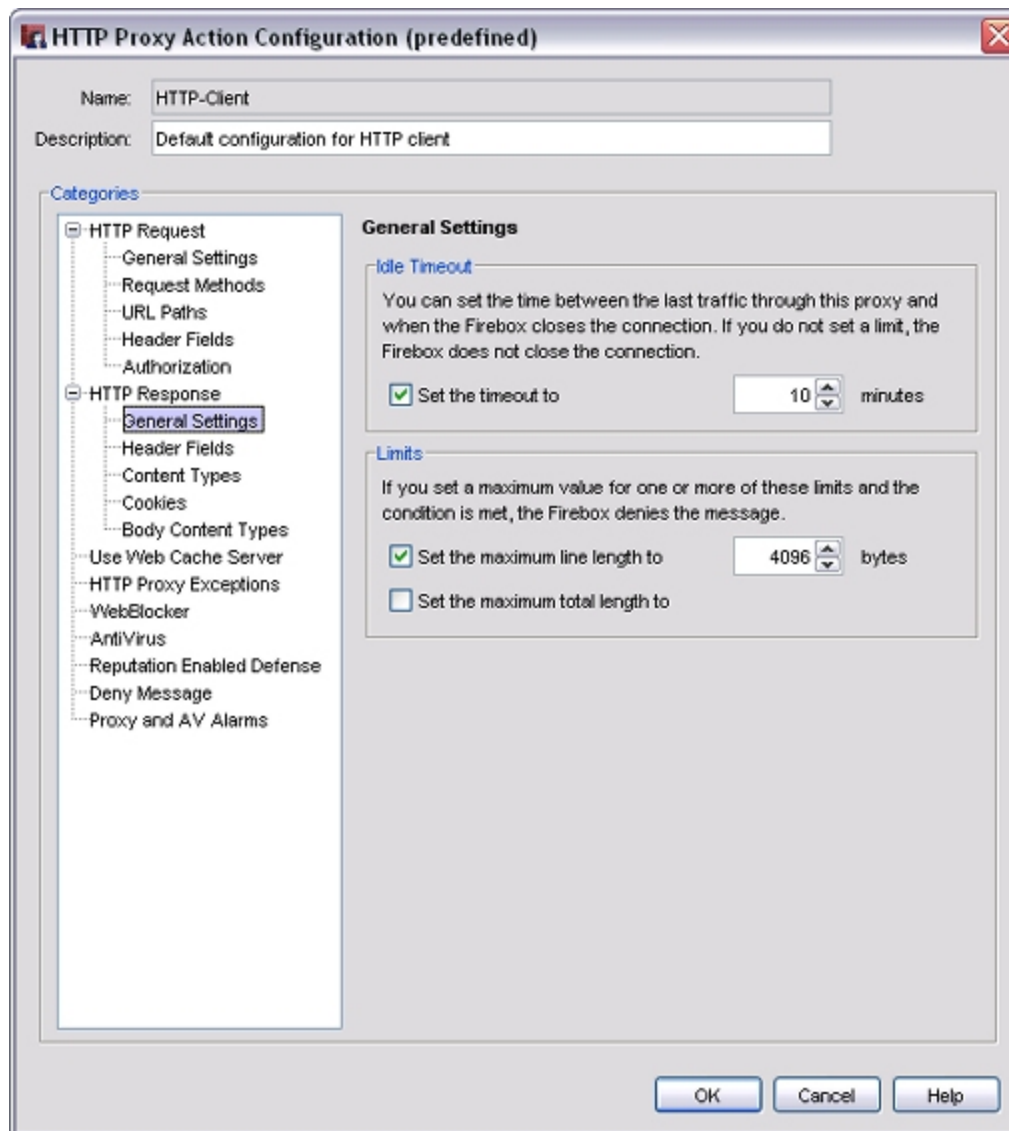
For more information on predefined proxy actions, see *About Proxy Actions*.

## HTTP Response: General Settings

On the **General Settings** page, you can configure basic HTTP parameters such as idle time out, and limits for line and total length.

1. In the **Categories** tree, select **HTTP Response > General Settings**.

*The General Settings page appears.*



2. To set limits for HTTP parameters, select the applicable check boxes. Type or select a value for the limits.

*Set the timeout to*

Controls how long the XTM device HTTP proxy waits for the web server to send the web page. When a user clicks a hyperlink or types a URL in a web browser, it sends an HTTP request to a remote server to get the content. In most browsers, a message similar to *Contacting site...*, appears in the status bar. If the remote server does not respond, the HTTP client continues to send the request until it receives an answer or until the request times out. During this time, the HTTP proxy continues to monitor the connection and uses valuable network resources.

*Set the maximum line length to*

Controls the maximum allowed length of a line of characters in HTTP response headers. Use this property to protect your computers from buffer overflow exploits. Because URLs for many commerce sites continue to increase in length over time, you may need to adjust this value in the future.

*Set the maximum total length to*

Controls the maximum length of HTTP response headers. If the total header length is more than this limit, the HTTP response is denied.

3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

## HTTP Response: Header Fields

This ruleset controls which HTTP response header fields the XTM device allows. You can add, delete, or modify rules. Many of the HTTP response headers that are allowed in the default configuration are described in RFC 2616. For more information, see <http://www.ietf.org/rfc/rfc2616.txt>.

1. In the **Categories** tree, select **HTTP Response > Header Fields**.  
*The Header Fields page appears.*
2. *Add, Change, or Delete Rules.*
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.



## HTTP Response: Content Types

When a web server sends HTTP traffic, it usually adds a MIME type, or content type, to the packet header that shows what kind of content is in the packet. The HTTP header on the data stream contains this MIME type. It is added before the data is sent.

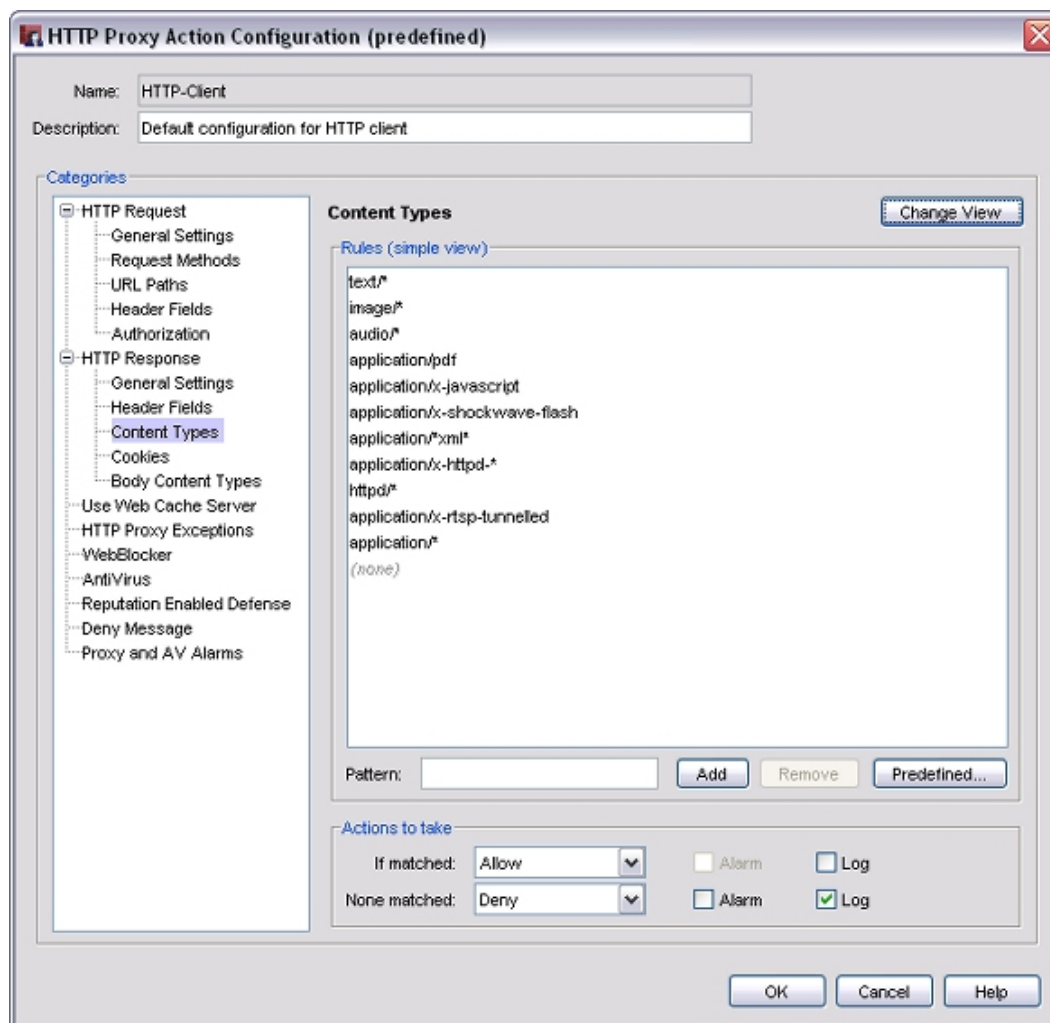
Certain kinds of content that users request from web sites can be a security threat to your network. Other kinds of content can decrease the productivity of your users. By default, the XTM device allows some safe content types, and denies MIME content that has no specified content type. The HTTP proxy includes a list of commonly used content types that you can add to the ruleset. You can also add, delete, or modify the definitions.

The format of a MIME type is **type/subtype**. For example, if you wanted to allow JPEG images, you would add `image/jpeg` to the proxy definition. You can also use the asterisk (\*) as a wildcard. To allow any image format, you add `image/*`.

For a list of current, registered MIME types, see <http://www.iana.org/assignments/media-types>.

## Add, Delete, or Modify Content Types

1. In the **Categories** tree, select **HTTP Response > Content Types**.  
*The Rules (simple view) list appears.*



2. Add, Change, or Delete Rules.
3. To add content types, click **Predefined** .  
*The Select Content Type dialog box appears.*
4. Select the type or types you want to add, and click **OK**.  
*The new types appear in the Rules box.*
5. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
6. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

## Allow Web Sites with a Missing Content Type

By default, the XTM device denies MIME content that has no specified content type. In most cases, we recommend that you keep this default setting. Sites that do not supply legitimate MIME types in their HTTP responses do not follow RFC recommendations and could pose a security risk. However, some organizations need their employees to get access to web sites that do not have a specified content type.

You must make sure that you change the proxy action used by the correct policy or policies. You can apply the change to any policy that uses an HTTP client proxy action. This could be an HTTP-proxy policy, the Outgoing policy (which also applies an HTTP client proxy action), or the TCP-UDP policy.

To allow web sites with a missing content type:

1. In the **Categories** tree, select **Content Types**.
2. Click **Change View**.  
*The Advanced View appears.*
3. In the **Rules (advanced view)** list, select the check box adjacent to the **Allow (none)** rule.

## HTTP Response: Cookies

HTTP cookies are small files of alphanumeric text that web servers put on web clients. Cookies monitor the page a web client is on, to enable the web server to send more pages in the correct sequence. Web servers also use cookies to collect information about an end user. Many web sites use cookies for authentication and other legitimate functions, and cannot operate correctly without cookies.

The HTTP proxy gives you control of the cookies in HTTP responses. You can configure rules to strip cookies, based on your network requirements. The default rule for the HTTP-Server and HTTP-Client proxy action allows all cookies. You can add, delete, or modify rules.

The proxy looks for packets based on the domain associated with the cookie. The domain can be specified in the cookie. If the cookie does not contain a domain, the proxy uses the host name in the first request. For example, to block all cookies for nosy-adware-site.com, use the pattern: \*.nosy-adware-site.com. If you want to deny cookies from all subdomains on a web site, use the wildcard symbol (\*) before and after the domain. For example, \*example.com\* blocks all subdomains of example.com, such as images.example.com and mail.example.com.

## Change Settings for Cookies

1. In the **Categories** tree, select **HTTP Response > Cookies**.  
*The Rules (simple view) list appears.*
2. *Add, Change, or Delete Rules.*
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

## HTTP Response: Body Content Types

This ruleset gives you control of the content in an HTTP response. The XTM device is configured to deny Java bytecodes, Zip archives, Windows EXE/DLL files, and Windows CAB files. The default proxy action for outgoing HTTP requests (HTTP-Client) allows all other response body content types. You can add, delete, or modify rules. We recommend that you examine the file types that are used in your organization and allow only those file types that are necessary for your network.

1. In the **Categories** tree, select **HTTP Response > Body Content Types**.  
*The Rules (simple view) list appears.*
2. *Add, Change, or Delete Rules.*
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

## HTTP-Proxy: Exceptions

For certain web sites, you can use HTTP-proxy exceptions to bypass HTTP-proxy rules, but not bypass the proxy framework. Traffic that matches HTTP-proxy exceptions still goes through the standard proxy handling used by the HTTP-proxy. However, when a match occurs, some proxy settings are not included.

### Excluded Proxy Settings

These settings are not included:

- HTTP request — range requests, URL path length, all request methods, all URL paths, request headers, authorization pattern matching
- HTTP response — response headers, content types, cookies, body content types

Request headers and response headers are parsed by the HTTP-proxy even when the traffic matches the HTTP-proxy exception. If a parsing error does not occur, all headers are allowed. Also, antivirus scanning, IPS scanning, and WebBlocker are not applied to traffic that matches an HTTP-proxy exception.

### Included Proxy Settings

These settings are included:

- HTTP request — Idle timeout
- HTTP response — Idle timeout, maximum line length limit, maximum total length limit

All transfer-encoding parsing is still applied to allow the proxy to determine the encoding type. The HTTP-proxy denies all invalid or malformed transfer encoding.

## Define Exceptions

You can add host names or patterns as HTTP-proxy exceptions. For example, if you block all web sites that end in `.test` but want to allow your users to go to the site `www.example.test`, you can add `www.example.test` as an HTTP-proxy exception.

When you define exceptions, you specify the IP address or domain name of sites to allow. The domain (or host) name is the part of a URL that ends with `.com`, `.net`, `.org`, `.biz`, `.gov`, or `.edu`. Domain names can also end in a country code, such as `.de` (Germany) or `.jp` (Japan).

To add a domain name, type the URL pattern without the leading "http://". For example, to allow your users to go to the Example web site `http://www.example.com`, type `www.example.com`. If you want to allow all subdomains that contain `example.com`, you can use the asterisk (\*) as a wildcard character. For example, to allow users to go to `www.example.com`, and `support.example.com` type `*.example.com`.

1. In the **Categories** tree, select **HTTP Proxy Exceptions**.  
*The HTTP Proxy Exceptions page appears.*
2. In the text box, type the host name or host name pattern. Click **Add**.
3. Repeat this process to add more exceptions.
4. To add a traffic log message each time the HTTP-proxy takes an action on a proxy exception, select the **Log each transaction that matches an HTTP proxy exception** check box.
5. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
6. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

## HTTP-Proxy: WebBlocker

To apply consistent settings for web site content blocking, you can associate a WebBlocker configuration with your HTTP-proxy.

In the **HTTP Proxy Action Configuration** dialog box:

1. In the **Categories** tree, select **WebBlocker**.  
*The WebBlocker page appears.*
2. From the **WebBlocker** drop-down list, select a configuration.

Or, to create a new WebBlocker configuration, click .

For more information, see *About WebBlocker* on page 1065 and *Get Started with WebBlocker* on page 1073.

## HTTP-Proxy: AntiVirus

If you have purchased and enabled the Gateway AntiVirus feature, you can specify the actions the XTM device takes if a virus is found in a web site or when the device cannot scan a web site.

- To use the proxy definition screens to activate Gateway AntiVirus, see *Activate Gateway AntiVirus from Proxy Definitions* on page 1171.
- To use the **Tasks** menu in Policy Manager to activate Gateway AntiVirus, see *Activate Gateway AntiVirus with a Wizard from Policy Manager* on page 1168.
- To configure Gateway AntiVirus for the HTTP-proxy, see *Configure Gateway AntiVirus Actions* on page 1172.

When you enable Gateway AntiVirus, you must set the actions to take if a virus or error is found in a web page.

The options for antivirus actions are:

### *Allow*

Allows the packet to go to the recipient, even if the content contains a virus.

### *Drop*

Drops the packet and drops the connection. No information is sent to the source of the message.

### *Block*

Blocks the packet, and adds the IP address of the sender to the Blocked Sites list.

Gateway AntiVirus scans each file up to the kilobyte count you specify. Any additional bytes in the file are not scanned. This allows the proxy to partially scan very large files without a large effect on performance.

For information about the default and maximum scan limits for each XTM device model, see *About Gateway AntiVirus Scan Limits* on page 1181.

To specify the antivirus actions:

1. In the **Categories** tree, select **AntiVirus**.  
*The AntiVirus page appears.*
2. From the **When a virus is detected** drop-down list, select an action: **Allow, Drop, Block**.
3. From the **When a scan error occurs** drop-down list, select an action: **Allow, Drop, Block**.
4. For each action, to send an alarm message when the action you specified occurs, select the **Alarm** check box.
5. For each action, to send a log message when the action you specified occurs, select the **Log** check box.
6. In the **Limit scanning to first** text box, type or select the file scan limit in kilobytes.
7. Click **OK**.

## HTTP-Proxy: Reputation Enabled Defense

If you have purchased and enabled Reputation Enabled Defense, the check boxes in this category set the actions necessary to allow or block content based on the reputation score of a URL.

To configure the actions for Reputation Enabled Defense in the HTTP-proxy definition, see *Configure Reputation Enabled Defense*.

## HTTP-Proxy: Deny Message

When content is denied, the XTM device sends a default deny message that replaces the denied content. You can change the text of that deny message. You can customize the deny message with standard HTML. You can also use Unicode (UTF-8) characters in the deny message. The first line of the deny message is a component of the HTTP header. You must include an empty line between the first line and the body of the message.

You get a deny message in your web browser from the XTM device when you make a request that the HTTP-proxy does not allow. You also get a deny message when your request is allowed, but the HTTP-proxy denies the response from the remote web server. For example, if a user tries to download an .exe file and you have blocked that file type, the user sees a deny message in the web browser. If the user tries to download a web page that has an unknown content type and the proxy policy is configured to block unknown MIME types, the user sees an error message in the web browser.

The default deny message appears in the **Deny Message** text box. To change this to a custom message, use these variables:

*%(transaction)%*

Select *Request* or *Response* to show which side of the transaction caused the packet to be denied.

*%(reason)%*

Includes the reason the XTM device denied the content.

*%(method)%*

Includes the request method from the denied request.

*%(url-host)%*

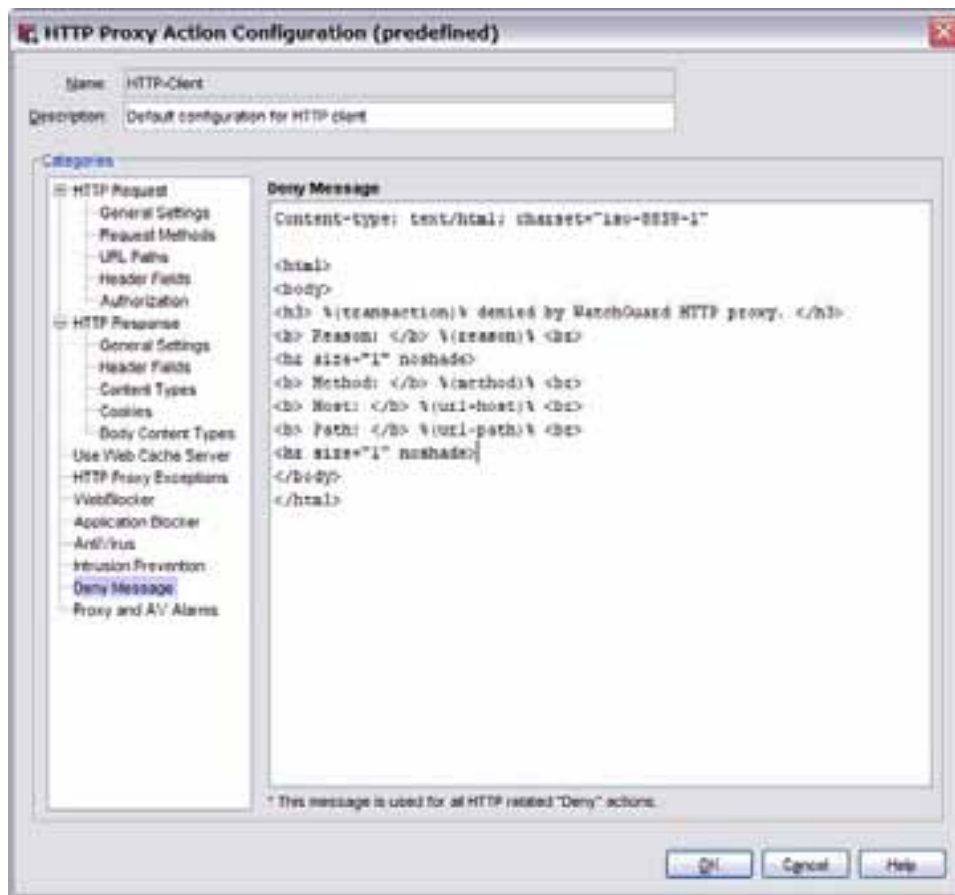
Includes the server host name from the denied URL. If no host name was included, the IP address of the server is included.

*%(url-path)%*

Includes the path component of the denied URL.

To configure the Deny Message:

1. In the **Categories** tree, select **Deny Message**.  
*The Deny Message page appears.*



2. In the **Deny Message** text box, type the deny message.
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.



## Enable Windows Updates Through the HTTP-Proxy

Windows Update servers identify the content they deliver to a computer as a generic binary stream (such as octet stream), which is blocked by the default HTTP proxy rules. To allow Windows updates through the HTTP-proxy, you must edit your HTTP-Client proxy ruleset to add HTTP-proxy exceptions for the Windows Update servers.

1. Make sure that your XTM device allows outgoing connections on port 443 and port 80.  
These are the ports that computers use to contact the Windows Update servers.
2. In the **Categories** tree, select **HTTP Proxy Exceptions**.
3. In the text box, type or paste each of these domains, and click **Add** after each one:  
windowsupdate.microsoft.com  
download.windowsupdate.com  
update.microsoft.com  
download.microsoft.com  
ntservicepack.microsoft.com  
wustat.windows.com  
v4.windowsupdate.microsoft.com  
v5.windowsupdate.microsoft.com
4. Click **OK**.

## If You Still Cannot Download Windows Updates

If you have more than one HTTP-proxy policy, make sure that you add the HTTP exceptions to the correct policy and proxy action.

Microsoft does not limit updates to only these domains. Examine your logs for denied traffic to a Microsoft-owned domain. If you do not have a WatchGuard Log Server, run Windows Update and then monitor the *Device Log Messages (Traffic Monitor)*. Look for any traffic denied by the HTTP-proxy. The log line should include the domain. Add any new Microsoft domain to the HTTP-proxy exceptions list, and then run Windows Update again.


## Use a Caching Proxy Server

Because your users can look at the same web sites frequently, a caching proxy server increases the traffic speed and decreases the traffic volume on the external Internet connections. Although the HTTP-proxy on the XTM device does not cache content, you can use a caching proxy server with the HTTP proxy. All XTM device proxy and WebBlocker rules continue to have the same effect.

The XTM device connection with a proxy server is the same as with a client. The XTM device changes the GET function to: GET / HTTP/1.1 to GET www.mydomain.com / HTTP/1.1 and sends it to a caching proxy server. The proxy server moves this function to the web server in the GET function.

## Use an External Caching Proxy Server

To set up your HTTP-proxy to work with an external caching proxy server:

1. Configure a proxy server, such as Microsoft Proxy Server 2.0.
2. Open Policy Manager.
3. Double-click the **HTTP-proxy** policy.  
*The Edit Policy Properties dialog box appears, with the Policy tab selected.*
4. Adjacent to the **Proxy action** drop-down list, click .  
*The HTTP Proxy Action Configuration dialog box appears.*
5. In the **Categories** tree, select **Use Web Cache Server**.  
*The Use Web Cache Server page appears.*
6. Select the **Use external caching proxy server for HTTP traffic** check box.
7. Type the **IP address** and **Port** for the external caching proxy server.
8. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
9. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

## Use an Internal Caching Proxy Server

You can also use an internal caching proxy server with your XTM device.

To use an internal caching proxy server:

1. Configure the HTTP-proxy action with the same settings as for an external proxy server.
2. In the same HTTP-proxy policy, allow all traffic from the users on your network whose web requests you want to route through the caching proxy server.
3. Add an HTTP packet filter policy to your configuration.
4. Configure the HTTP packet filter policy to allow traffic from the IP address of your caching proxy server to the Internet.
5. If necessary, manually move this policy up in your policy list so that it has a higher precedence than your HTTP-proxy policy.

## About the HTTPS-Proxy

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a request/response protocol between clients and servers used for secure communications and transactions. You can use the HTTPS-proxy to secure a web server protected by your XTM device, or to examine HTTPS traffic requested by clients on your network. By default, when an HTTPS client starts a request, it establishes a TCP (Transmission Control Protocol) connection on port 443. Most HTTPS servers listen for requests on port 443.

HTTPS is more secure than HTTP because HTTPS uses a digital certificate to encrypt and decrypt user page requests as well as the pages that are returned by the web server. Because HTTPS traffic is encrypted, the XTM device must decrypt it before it can be examined. After it examines the content, the XTM device encrypts the traffic with a certificate and sends it to the intended destination.

You can export the default certificate created by the XTM device for this feature, or import a certificate for the XTM device to use instead. If you use the HTTPS-proxy to examine web traffic requested by users on your network, we recommend that you export the default certificate and distribute it to each user so that they do not receive browser warnings about untrusted certificates. If you use the HTTPS-proxy to secure a web server that accepts requests from an external network, we recommend that you import the existing web server certificate for the same reason.

When an HTTPS client or server uses a port other than port 443 in your organization, you can use the TCP/UDP proxy to relay the traffic to the HTTPS-proxy. For information on the TCP/UDP proxy, see *About the TCP-UDP-Proxy* on page 506.

To add the HTTPS-proxy to your XTM device configuration, see *Add a Proxy Policy to Your Configuration* on page 417.

If you must change the proxy definition, you can use the **New/Edit Proxy Policies** dialog box to modify the definition. This dialog box has three tabs: **Policy**, **Properties**, and **Advanced**.

### Policy Tab

- **HTTPS-proxy connections are** — Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)**. Define who appears in the **From** and **To** lists.  
For more information, see *Set Access Rules for a Policy* on page 392.
- **Use policy-based routing** — To use policy-based routing in your proxy definition, see *Configure Policy-Based Routing* on page 395.
- You can also configure static NAT or configure server load balancing.  
For more information, see *Configure Static NAT* on page 179 and *Configure Server Load Balancing* on page 182.
- **Proxy action** — Select the proxy action to use for this policy. You can also edit the rulesets for proxy actions.

## Properties Tab

- To edit or add a comment to this policy configuration, type the comment in the **Comment** text box.
- To define the logging settings for the policy, click **Logging** and *Set Logging and Notification Preferences* on page 723.
- If you set the **HTTPS-proxy connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use HTTPS. For more information, see *Block Sites Temporarily with Policy Settings* on page 538.
- To change the idle timeout that is set by the XTM device or authentication server, see *Set a Custom Idle Timeout*.

## Advanced Tab

You can use several other options in your proxy definition:

- *Set an Operating Schedule*
- *Add a Traffic Management Action to a Policy*
- *Set ICMP Error Handling*
- *Apply NAT Rules* (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- *Enable QoS Marking or Prioritization Settings for a Policy*
- *Set the Sticky Connection Duration for a Policy*

## Configure the Proxy Action

You can choose a predefined proxy action or configure a user-defined proxy action for this proxy. For more information about how to configure proxy actions, see *About Proxy Actions* on page 403.

For the HTTPS-proxy, you can configure these categories of settings for a proxy action:

- *HTTPS-Proxy: General Settings*
- *HTTPS-Proxy: Content Inspection*
- *HTTPS-Proxy: Certificate Names*
- *HTTPS-Proxy: WebBlocker*
- *Proxy and AV Alarms*

## HTTPS-Proxy: General Settings

On the **HTTPS Proxy Action Configuration** dialog box **General Settings** page, you can configure basic HTTPS parameters such as alarms, idle timeout, and logging.



### Proxy Alarm

You can define the proxy to send an SNMP trap, a notification to a network administrator, or both. The notification can either be an email message to a network administrator or a pop-up window on the management computer.

For more information about Proxy and AV alarm settings, see *Set Logging and Notification Preferences* on page 723.

*Idle Timeout*

Configure these settings to specify how long the HTTPS proxy waits for the web client to make a request from the external web server after it starts a TCP/IP connection, or after an earlier request for the same connection. If the time period exceeds this setting, the HTTPS proxy closes the connection.

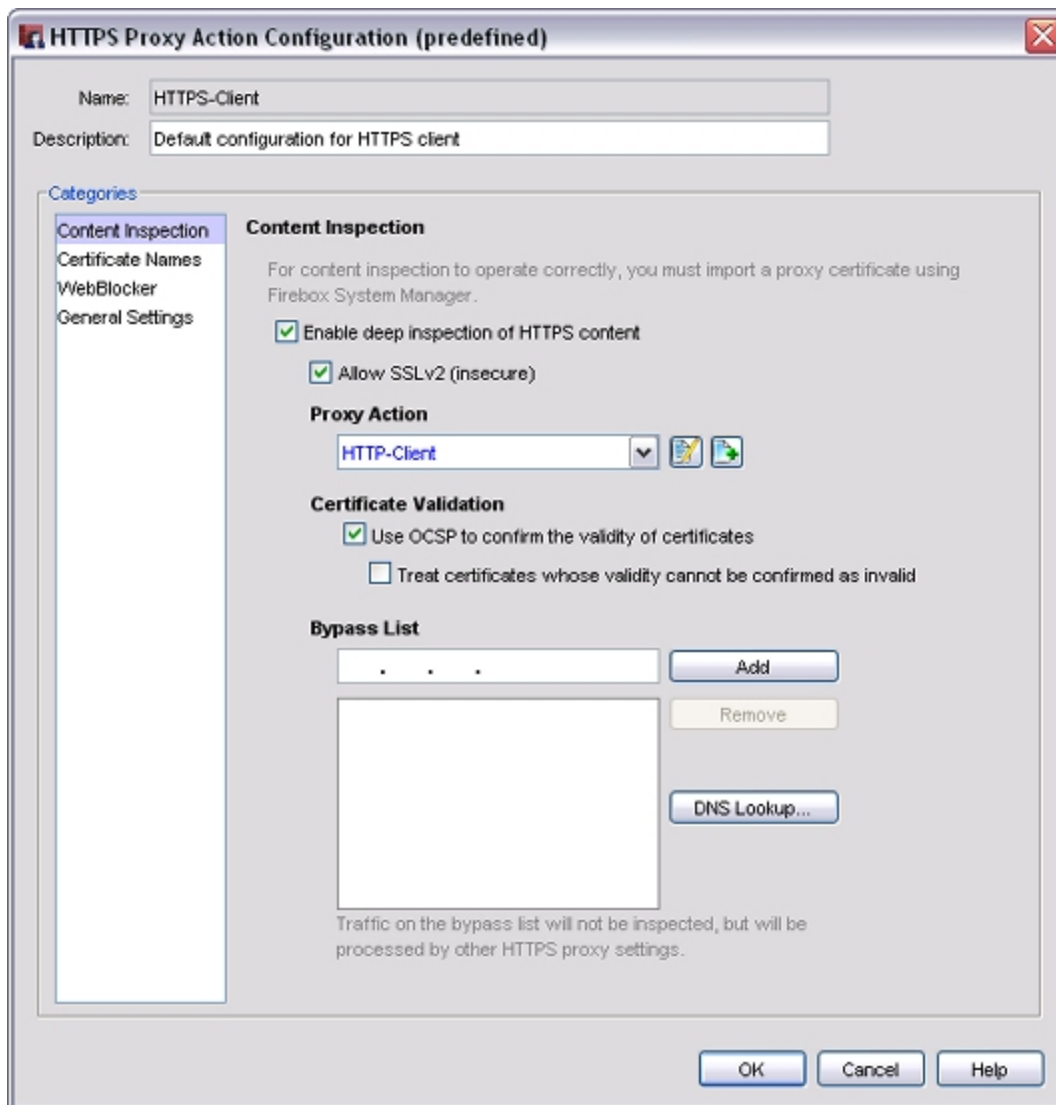
To enable this feature, select the **Connection timeout** check box. In the adjacent text box, type or select the number of minutes before the proxy times out.

*Enable logging for reports*

To create a traffic log message for each transaction, select this check box. This option increases the size of your log file, but this information is very important if your firewall is attacked. If you do not select this check box, you do not see detailed information about HTTPS proxy connections in reports.

## HTTPS-Proxy: Content Inspection

You can enable and configure deep inspection of HTTPS content on the HTTPS-Proxy Action Configuration **Content Inspection** page.



### *Enable deep inspection of HTTPS content*

When this check box is selected, the XTM device decrypts HTTPS traffic, examines the content, and encrypts the traffic again with a new certificate. The content is examined by the HTTP-proxy policy that you choose on this page.

**Note** *If you have other traffic that uses the HTTPS port, such as SSL VPN traffic, we recommend that you evaluate this option carefully. The HTTPS-proxy attempts to examine all traffic on TCP port 443 in the same way. To ensure that other traffic sources operate correctly, we recommend that you add those sources to the **Bypass List**. See the subsequent section for more information.*

By default, the certificate used to encrypt the traffic is generated automatically by the XTM device. You can also upload your own certificate to use for this purpose. If the original web site or your web server has a self-signed or invalid certificate, or if the certificate was signed by a CA the XTM device does not recognize, clients are presented with a browser certificate warning. Certificates that cannot be properly re-signed appear to be issued by *Fireware HTTPS-proxy: Unrecognized Certificate* or simply *Invalid Certificate*.

We recommend that you import the certificate you use, as well as any other certificates necessary for the client to trust that certificate, on each client device. When a client does not automatically trust the certificate used for the content inspection feature, the user sees a warning in their browser, and services like Windows Update do not operate correctly.

Some third-party programs store private copies of necessary certificates and do not use the operating system certificate store, or transmit other types of data over TCP port 443. These programs include:

- Communications software, such as AOL Instant Messenger and Google Voice
- Remote desktop and presentation software, including LiveMeeting and WebEx
- Financial and business software, such as ADP, iVantage, FedEx, and UPS

If these programs do not have a method to import trusted CA certificates, they do not operate correctly when content inspection is enabled. Contact your software vendor for more information about certificate use or technical support, or add the IP addresses of computers that use this software to the Bypass list.

For more information, see *About Certificates* on page 853 or *Use Certificates for the HTTPS-Proxy* on page 880.

#### *Enable SSLv2 (insecure)*

SSLv3, SSLv2, and TLSv1 are protocols used for HTTPS connections. SSLv2 is not as secure as SSLv3 and TLSv1. By default, the HTTPS-proxy only allows connections that negotiate the SSLv3 and TLSv1 protocols. If your users connect to client or server applications that only support SSLv2, you can allow the HTTPS-proxy to use the SSLv2 protocol for connections to these web sites.

To enable this option, select the **SSLv2 (insecure)** check box. This option is disabled by default.

#### *Proxy Action*

Select an HTTP-proxy policy for the XTM device to use when it inspects decrypted HTTPS content.

When you enable content inspection, the HTTP-proxy action WebBlocker settings override the HTTPS-proxy WebBlocker settings. If you add IP addresses to the bypass list for content inspection, traffic from those sites is filtered with the WebBlocker settings from the HTTPS-proxy.

For more information on WebBlocker configuration, see *About WebBlocker* on page 1065.

#### *Use OCSP to confirm the validity of certificates*

Select this check box to have the XTM device automatically check for certificate revocations with OCSP (Online Certificate Status Protocol). When this feature is enabled, the XTM device uses information in the certificate to contact an OCSP server that keeps a record of the certificate status. If the OCSP server responds that the certificate has been revoked, the XTM device disables the certificate.



If you select this option, there can be a delay of several seconds as the XTM device requests a response from the OCSP server. The XTM device keeps between 300 and 3000 OCSP responses in a cache to improve performance for frequently visited web sites. The number of responses stored in the cache is determined by your XTM device model.

#### *Treat certificates whose validity cannot be confirmed as invalid*

When this option is selected and an OCSP responder does not send a response to a revocation status request, the XTM device considers the original certificate as invalid or revoked. This option can cause certificates to be considered invalid if there is a routing error or a problem with your network connection.

#### *Bypass list*

The XTM device does not inspect content sent to or from IP addresses on this list. To add a web site or hostname, type its IP address in the text box and click the **Add** button.

When you enable content inspection, the HTTP proxy action WebBlocker settings override the HTTPS proxy WebBlocker settings. If you add IP addresses to the bypass list for content inspection, traffic from those sites is filtered with the WebBlocker settings from the HTTPS-proxy.

For more information on WebBlocker configuration, see *About WebBlocker* on page 1065.

#### *DNS Lookup*

To quickly find the IP address for a web site or hostname:

1. Click **DNS Lookup**.
2. Type the domain name or hostname and click **Lookup**.  
*If the domain name or hostname is valid, the valid IP addresses appear.*
3. Select the check box for each IP address that you want to add. Click **OK**.
4. To select all or none of the IP addresses, click the check box at the top of the list.

## HTTPS-Proxy: Certificate Names

Certificate names are used to filter content for an entire site. The XTM device allows or denies access to a site if the domain of an HTTPS certificate matches an entry in this list.

For example, if you want to deny traffic from any site in the *example.com* domain, add a Certificate Names rule with the pattern *\*.example.com* and set the **If matched** action to **Deny**.

1. In the **Categories** tree, select **Certificate Names**.  
*The Rules (simple view) list appears.*
2. *Add, Change, or Delete Rules.*
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

## HTTPS-Proxy: WebBlocker

You can associate a WebBlocker configuration with your HTTPS-proxy to apply consistent settings for web site content blocking.

In the **HTTPS Proxy Action Configuration** dialog box:

1. In the **Categories** tree, select **WebBlocker**.  
*The WebBlocker page appears.*
2. From the **WebBlocker** drop-down list, select a configuration.

Or, to create a new WebBlocker configuration, click .

For more information, see *About WebBlocker* on page 1065 and *Get Started with WebBlocker* on page 1073.

---

## About the POP3-Proxy

POP3 (Post Office Protocol v.3) is a protocol that moves email messages from an email server to an email client on a TCP connection over port 110. Most Internet-based email accounts use POP3. With POP3, an email client contacts the email server and checks for any new email messages. If it finds a new message, it downloads the email message to the local email client. After the message is received by the email client, the connection is closed.

With a POP3-proxy filter you can:

- Adjust timeout and line length limits to make sure the POP3-proxy does not use too many network resources, and to prevent some types of attacks.
- Customize the deny message that users see when an email sent to them is blocked.
- Filter content embedded in email with MIME types.
- Block specified path patterns and URLs.

To add the POP3-proxy to your XTM device configuration, see *Add a Proxy Policy to Your Configuration* on page 417.

If you must change the proxy definition, you can use the **New/Edit Proxy Policies** dialog box to modify the definition. This dialog box has three tabs: **Policy**, **Properties**, and **Advanced**.

## Policy Tab

- **POP3-proxy connections are** — Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)**. Define who appears in the **From** and **To** lists.  
For more information, see *Set Access Rules for a Policy* on page 392.
- **Use policy-based routing** — To use policy-based routing in your proxy definition, see *Configure Policy-Based Routing* on page 395.
- You can also configure static NAT or configure server load balancing.  
For more information, see *Configure Static NAT* on page 179 and *Configure Server Load Balancing* on page 182.
- **Proxy action** — Select the proxy action to use for this policy. You can also edit the rulesets for proxy actions.

## Properties Tab

- To edit or add a comment to this policy configuration, type the comment in the **Comment** text box.
- To define the logging settings for the policy, click **Logging** and *Set Logging and Notification Preferences* on page 723.
- If you set the **POP3-proxy connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use POP3.  
For more information, see *Block Sites Temporarily with Policy Settings* on page 538.
- To change the idle timeout that is set by the XTM device or authentication server, see *Set a Custom Idle Timeout*.

## Advanced Tab

You can use several other options in your proxy definition:

- *Set an Operating Schedule*
- *Add a Traffic Management Action to a Policy*
- *Set ICMP Error Handling*
- *Apply NAT Rules* (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- *Enable QoS Marking or Prioritization Settings for a Policy*
- *Set the Sticky Connection Duration for a Policy*

## Configure the Proxy Action

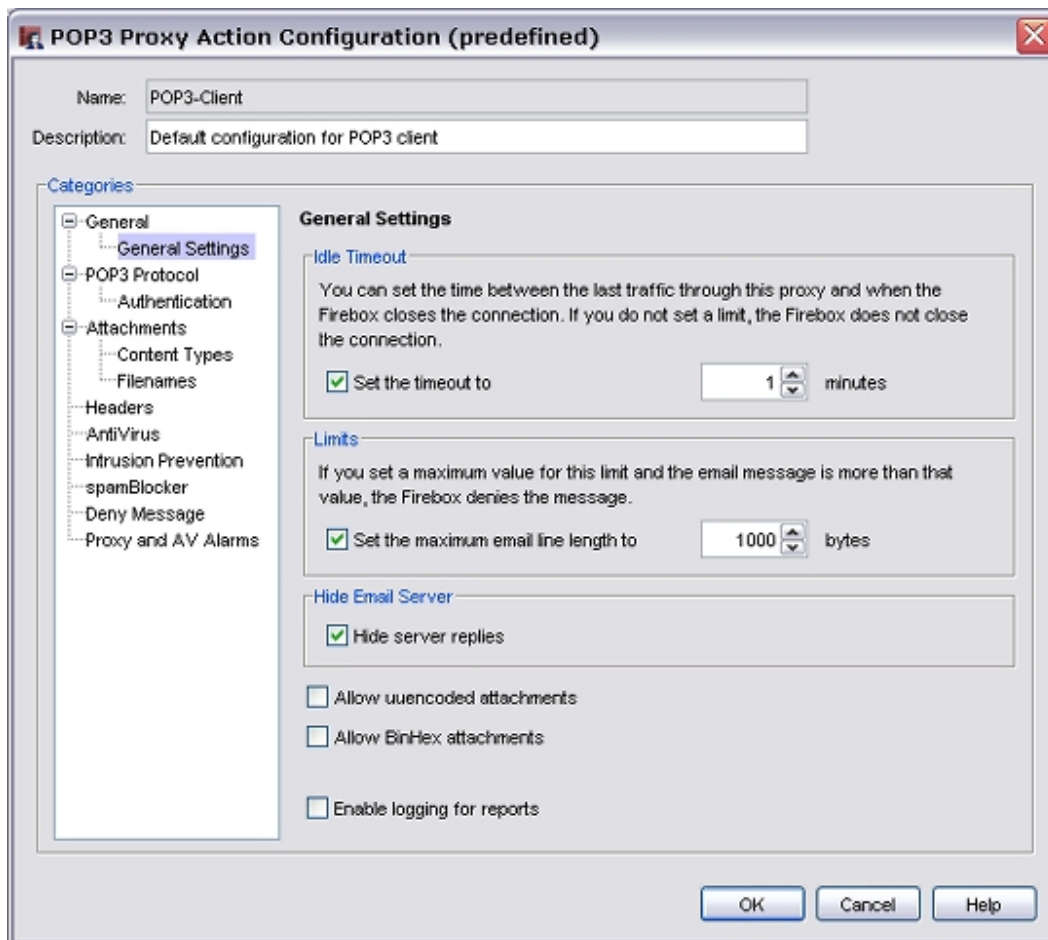
You can choose a predefined proxy action or configure a user-defined proxy action for this proxy. For more information about how to configure proxy actions, see *About Proxy Actions* on page 403.

For the POP3-proxy, you can configure these categories of settings for a proxy action:

- *POP3-Proxy: General Settings*
- *POP3-Proxy: Authentication*
- *POP3-Proxy: Content Types*
- *POP3-Proxy: File Names*
- *POP3-Proxy: Headers*
- *POP3-Proxy: Deny Message*
- *POP3-Proxy: AntiVirus*
- *POP3-Proxy: spamBlocker*
- *Proxy and AV Alarms*

## POP3-Proxy: General Settings

On the **POP3 Proxy Action Configuration** dialog box **General Settings** page, you can adjust time out and line length limits as well as other general parameters for the POP3-proxy.



### *Set the timeout to*

To limit the number of minutes that the email client tries to open a connection to the email server before the connection is closed, select this check box. In the adjacent text box, type or select the number of minutes for the timeout value. This makes sure the proxy does not use too many network resources when the POP3 server is slow or cannot be reached.

### *Set the maximum email line length to*

To prevent some types of buffer overflow attacks, select this check box. In the adjacent text box, type or select the limit of the line length. Very long line lengths can cause buffer overflows on some email systems. Most email clients and systems send relatively short lines, but some web-based email systems send very long lines. However, it is unlikely that you will need to change this setting unless it prevents access to legitimate mail.

*Hide server replies*

To replace the POP3 greeting strings in email messages, select this check box. These strings can be used by hackers to identify the POP3 server vendor and version.

*Allow uuencoded attachments*

To enable the POP3-proxy to allow uuencoded attachments in email messages, select this check box. Uuencode is an older program used to send binary files in ASCII text format over the Internet. UUencoded attachments can be security risks because they appear as ASCII text files, but can actually contain executable files.

*Allow BinHex attachments*

To enable the POP3-proxy to allow BinHex attachments in email messages, select this check box. BinHex, which is short for binary-to-hexadecimal, is a utility that converts a file from binary format to ASCII text format.

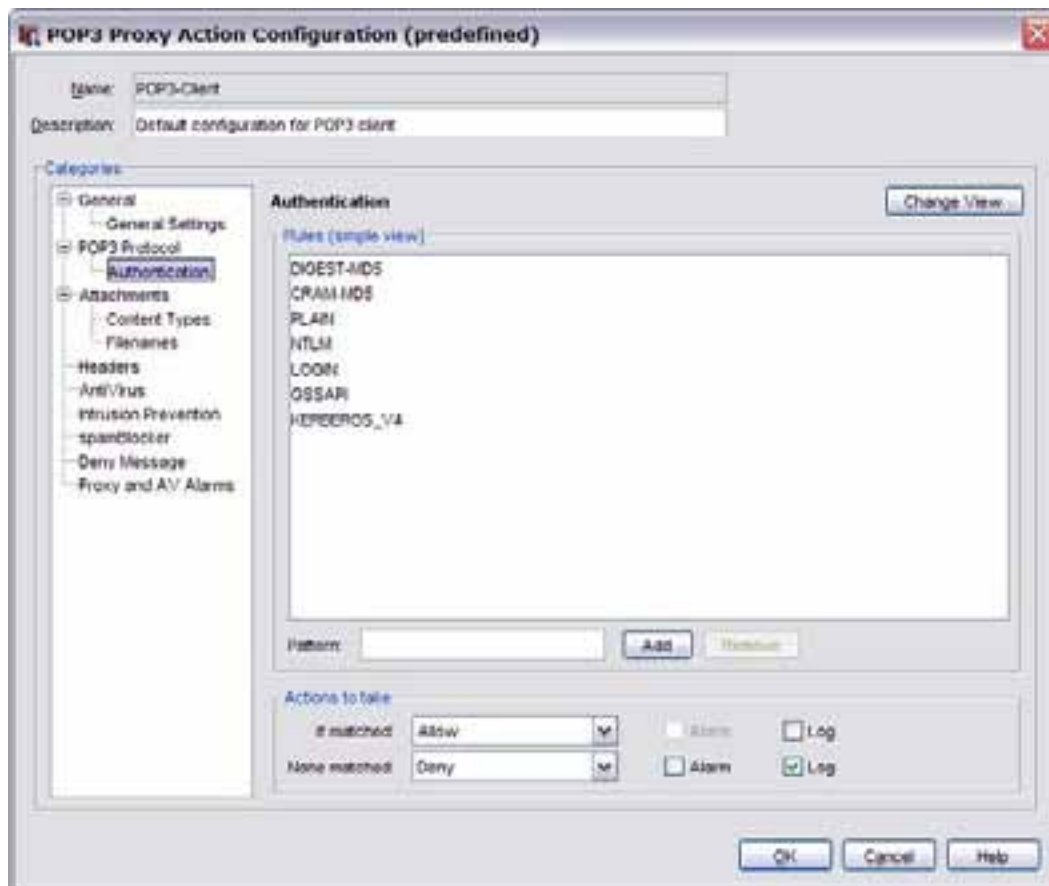
*Enable logging for reports*

To enable the POP3-proxy to send a log message for each POP3 connection request, select this check box. To use WatchGuard Reports to create reports of POP3 traffic, you must select this check box.

## POP3-Proxy: Authentication

A POP3 client must authenticate to a POP3 server before they exchange information. You can set the types of authentication for the proxy to allow and the action to take for types that do not match the criteria. You can add, delete, or modify rules.

1. In the **Categories** tree, select **Authentication**.



2. *Add, Change, or Delete Rules.*
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

## POP3-Proxy: Content Types

The headers for email messages include a Content Type header to show the MIME type of the email and of any attachments. The content type or MIME type tells the computer the types of media the message contains. Certain kinds of content embedded in email can be a security threat to your network. Other kinds of content can decrease the productivity of your users.

You can enable the POP3-proxy to automatically detect the content type of an email message and any attachments. If you do not enable this option, the POP3-proxy uses the value stated in the email header, which clients sometimes set incorrectly. Because hackers often try to disguise executable files as other content types, we recommend that you enable content type auto detection to make your installation more secure.

For example, a .pdf file attached to an email might have a content type stated as application/octet-stream. If you enable content type auto detection, the POP3-proxy recognizes the .pdf file and uses the actual content type, application/pdf. If the proxy does not recognize the content type after it examines the content, it uses the value stated in the email header, as it would if content type auto detection were not enabled.

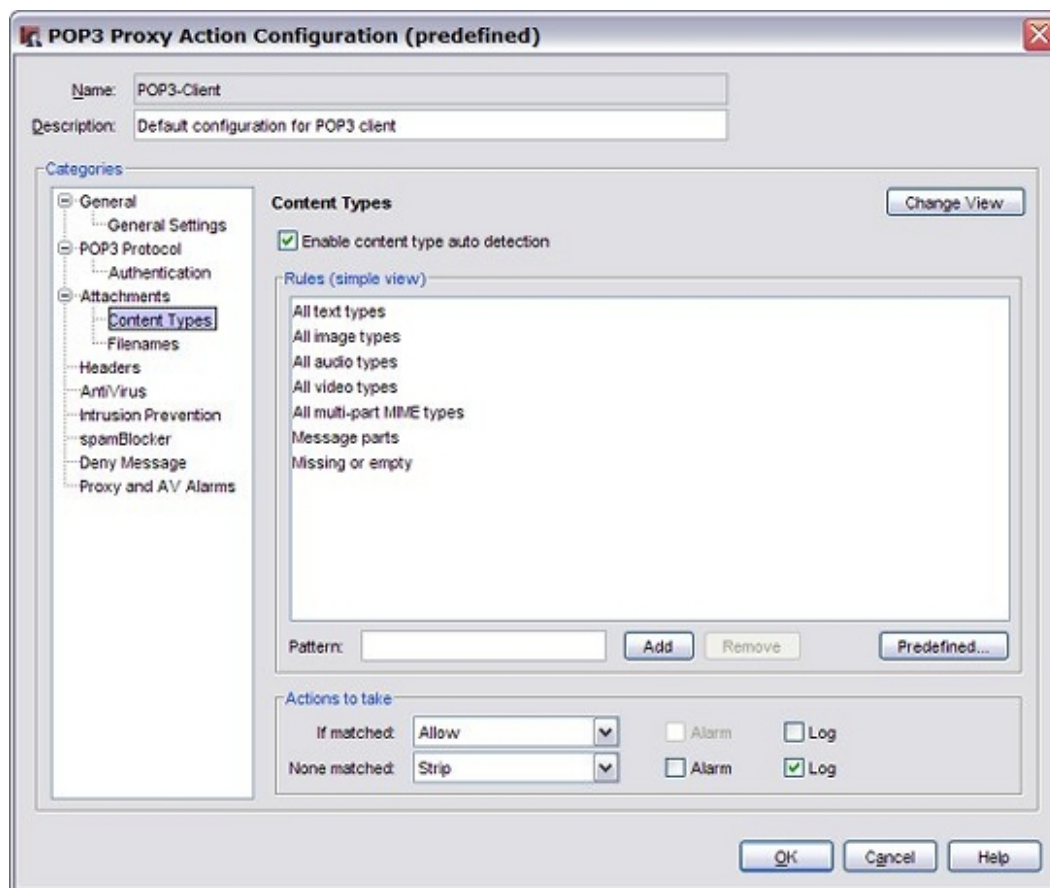
You can add, delete, or modify rules. You can also set values for content filtering and the action to take for content types that do not match the criteria. For the POP3-Server proxy action, you set values for incoming content filtering. For the POP3-Client action, you set values for outgoing content filtering.

When you specify the MIME type, make sure to use the format type/subtype. For example, if you want to allow JPEG images, you add `image/jpeg`. You can also use the asterisk (\*) as a wildcard. To allow any image format, add `image/*` to the list.

To specify the content types for automatic detection:

1. In the **Categories** tree, select **Attachments > Content Types**.  
*The Content Types page appears.*





2. To enable the POP3 proxy to examine content and determine the content type, select the **Enable content type auto detection** check box.  
If you do not select this option, the POP3 proxy uses the value stated in the email header.
3. *Add, Change, or Delete Rules.*
4. To add a predefined content type, click **Predefined**.  
*A list of content types appears, with short descriptions of the content types.*
5. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
6. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

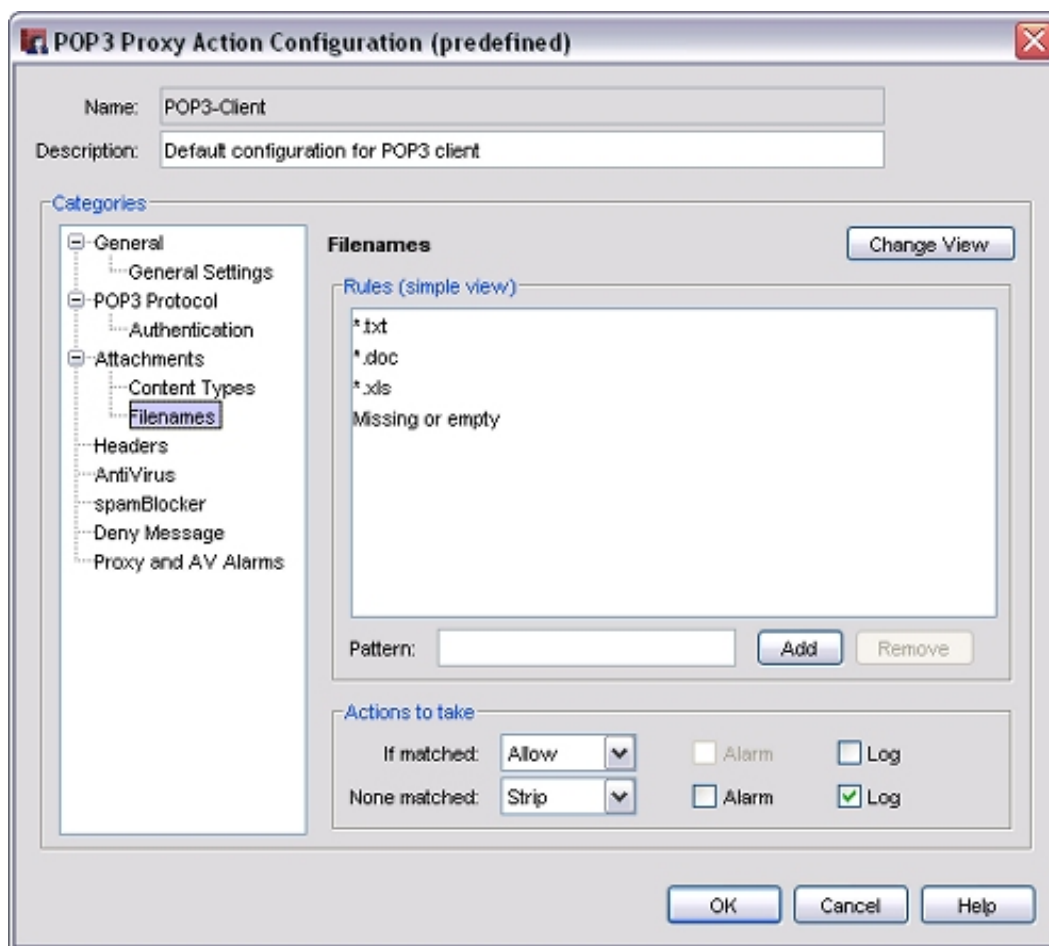
For more information on predefined proxy actions, see *About Proxy Actions*.

## POP3-Proxy: File Names

You can use this ruleset in a POP3-Server proxy action to put limits on file names for incoming email attachments. Or, you can use the ruleset for the POP3-Client proxy action to put limits on file names for outgoing email attachments. You can add, delete, or modify rules.

1. In the **Categories** tree, select **Attachments > Filenames**.

*The Filenames page appears.*



2. Add, Change, or Delete Rules.
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

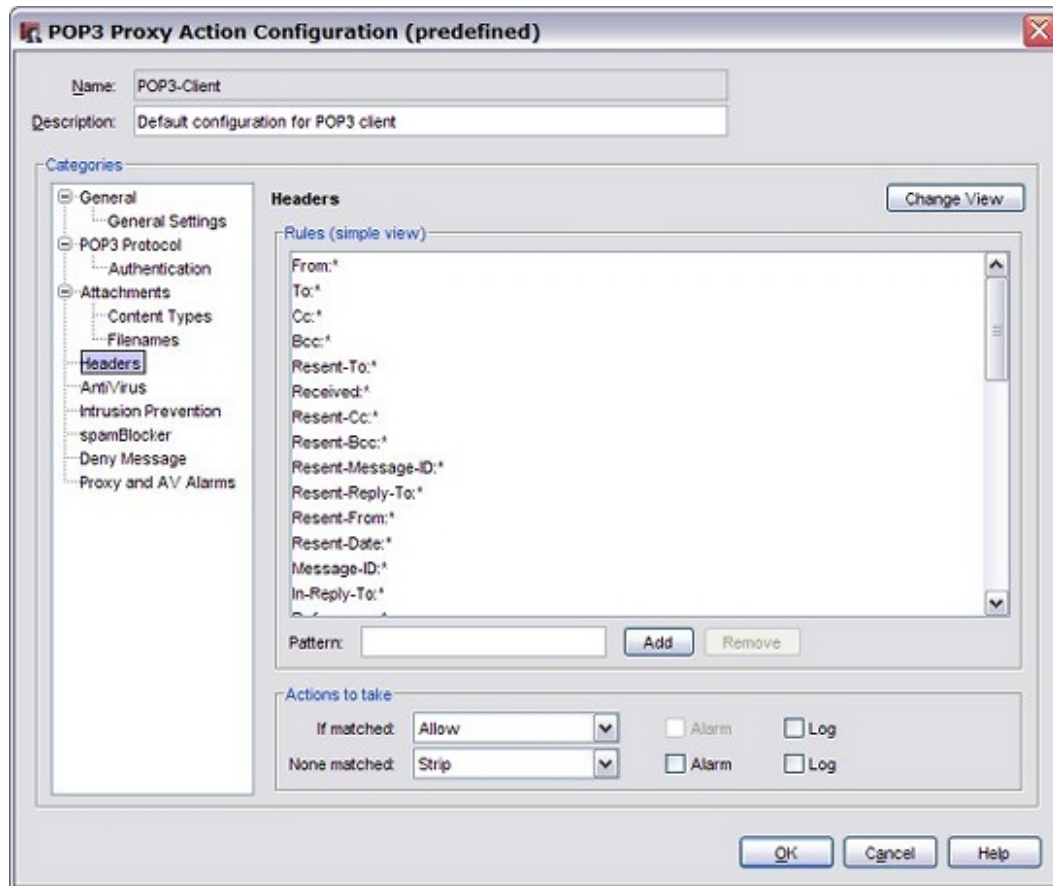
For more information on predefined proxy actions, see *About Proxy Actions*.

## POP3-Proxy: Headers

The POP3-proxy examines email headers to find patterns common to forged email messages, as well as those from legitimate senders. You can add, delete, or modify rules.

1. In the **Categories** tree, select **Headers**.

*The Headers page appears.*



2. *Add, Change, or Delete Rules.*
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

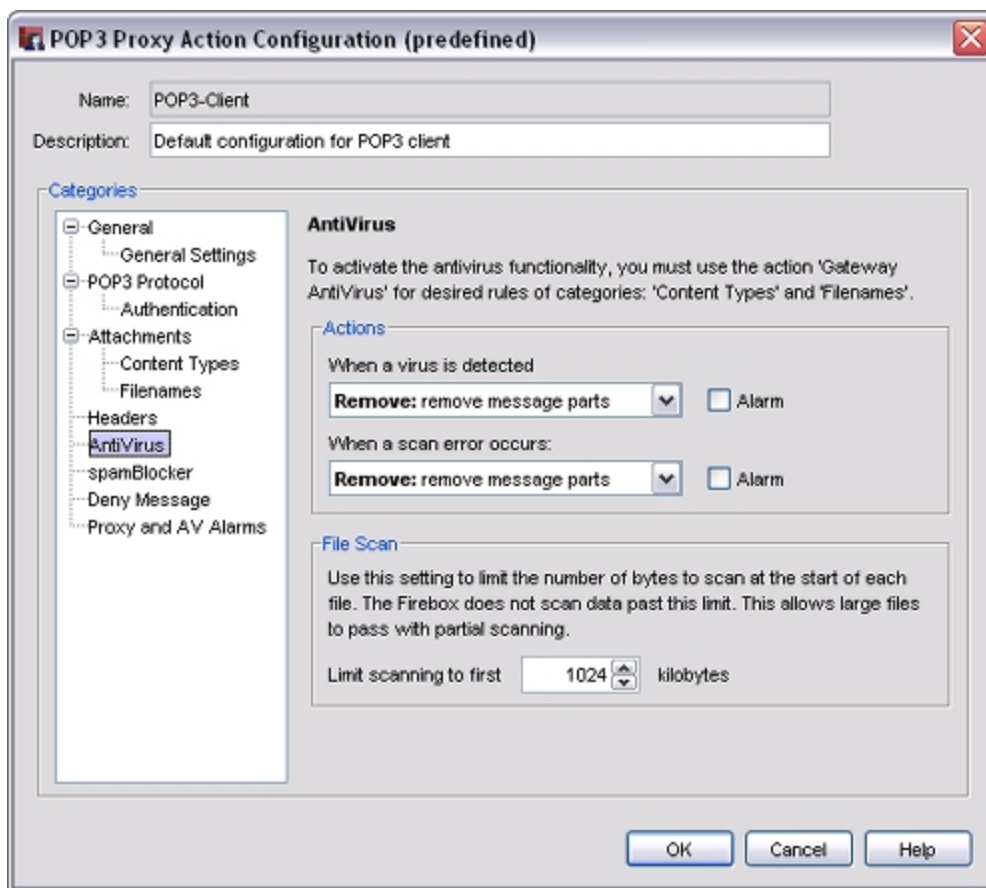
For more information on predefined proxy actions, see *About Proxy Actions*.

## POP3-Proxy: AntiVirus

If you have purchased and enabled the Gateway AntiVirus feature, you can configure the actions the POP3-proxy takes when a virus is found in an email message. You can also specify the actions the XTM device takes when an email message contains an attachment that the XTM device cannot scan.

- To use the proxy definition screens to activate Gateway AntiVirus, see *Activate Gateway AntiVirus from Proxy Definitions* on page 1171.
- To use the **Subscription Services** menu in Policy Manager to activate Gateway AntiVirus, see *Activate Gateway AntiVirus with a Wizard from Policy Manager* on page 1168.
- To configure Gateway AntiVirus for the POP3-proxy, see *Configure Gateway AntiVirus Actions* on page 1172.

When you enable Gateway AntiVirus, you must set the actions to be taken if a virus or error is found in an email message or attachment.



The options for antivirus actions are:

*Allow*

Allows the packet to go to the recipient, even if the content contains a virus.

### Lock

Locks the attachment. This is a good option for files that cannot be scanned by the XTM device. A file that is locked cannot be opened easily by the user. Only the administrator can unlock the file. The administrator can use a different antivirus tool to scan the file and examine the content of the attachment. For information about how to unlock a file locked by Gateway AntiVirus, see *Unlock a File Locked by Gateway AntiVirus* on page 1179.

### Remove

Removes the attachment and allows the message through to the recipient.

**Note** If you set the configuration to allow attachments, your configuration is less secure.

### File Scan

Gateway AntiVirus scans each file up to the kilobyte count you specify in the **Limit scanning to first** text box. Any additional bytes in the file are not scanned. This allows the proxy to partially scan very large files without a large effect on performance.

For information about the default and maximum scan limits for each XTM device model, see *About Gateway AntiVirus Scan Limits* on page 1181.

## POP3-Proxy: Deny Message

When content is denied, the XTM device sends a default *deny message* that replaces the denied content. This message appears in a recipients email message when the proxy blocks an email. You can change the text of that deny message. The first line of the deny message is a section of the HTTP header. You must include an empty line between the first line and the body of the message.

The default deny message appears in the **Deny Message** text box. To change this to a custom message, use these variables:

*%(reason)%*

Includes the reason the XTM device denied the content.

*%(filename)%*

Includes the file name of the denied content.

*%(virus)%*

Includes the name or status of a virus for Gateway AntiVirus users.

*%(action)%*

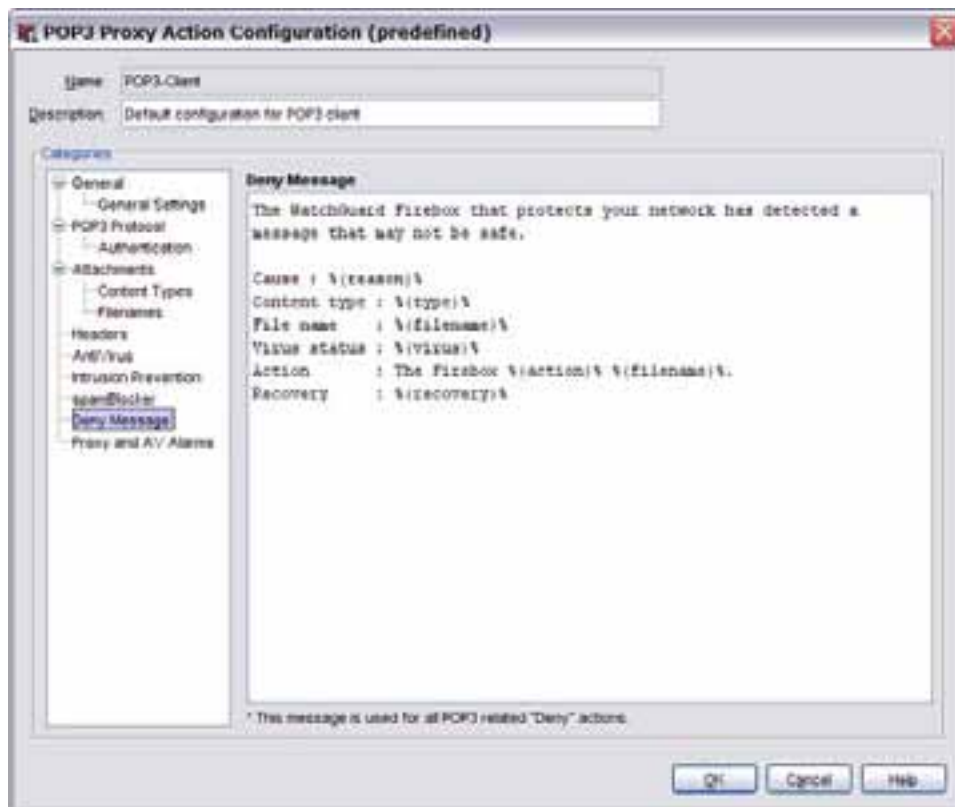
Includes the name of the action taken. For example: lock or strip.

*%(recovery)%*

Includes whether you can recover the attachment.

To configure the deny message:

1. In the **Categories** tree, select **Deny Message**.  
*The Deny Message page appears.*



2. In the **Deny Message** text box, type a custom plain text message in standard HTML.
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **OK**.

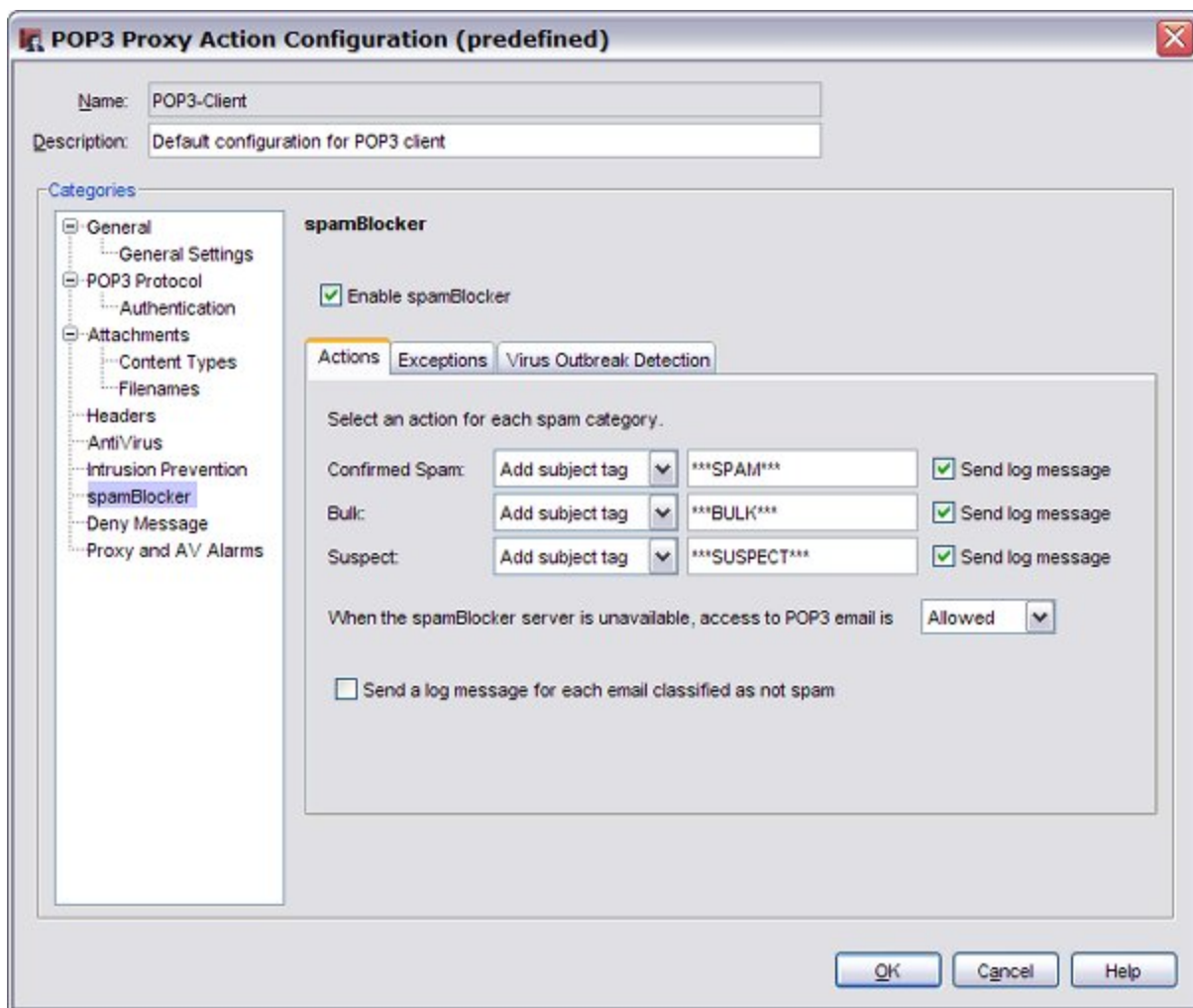
If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

## POP3-Proxy: spamBlocker

Unwanted email, also known as spam, can quickly fill your Inbox. A large volume of spam decreases bandwidth, degrades employee productivity, and wastes network resources. The WatchGuard spamBlocker option increases your capacity to catch spam at the edge of your network when it tries to enter your system. If you have purchased and enabled the spamBlocker feature, the fields in the spamBlocker category set the actions for email messages identified as spam.

Although you can use the proxy definition screens to activate and configure spamBlocker, it is easier to use the **Subscription Services** menu in Policy Manager. For more information, see *About spamBlocker* on page 1141.



## About the SIP-ALG

If you use Voice-over-IP (VoIP) in your organization, you can add a SIP (Session Initiation Protocol) or H.323 ALG (Application Layer Gateway) to open the ports necessary to enable VoIP through your XTM device. An ALG is created in the same way as a proxy policy and offers similar configuration options. These ALGs have been created to work in a NAT environment to maintain security for privately-addressed conferencing equipment behind the XTM device.

H.323 is commonly used on videoconferencing equipment. SIP is commonly used with IP phones. You can use both H.323 and SIP-ALGs at the same time, if necessary. To determine which ALG you need to add, consult the documentation for your VoIP devices or applications.

## VoIP Components

It is important to understand that you usually implement VoIP with either:

### *Peer-to-peer connections*

In a peer-to-peer connection, each of the two devices knows the IP address of the other device and connects to the other directly without the use of a proxy server to route their calls. If both peers are behind the XTM device, the XTM device can route the call traffic correctly.

### *Hosted connections*

Connections hosted by a call management system (PBX)

In the SIP standard, two key components of call management are the *SIP Registrar* and the *SIP Proxy*. Together, these components manage connections hosted by the call management system. The WatchGuard SIP-ALG opens and closes the ports necessary for SIP to operate. The WatchGuard SIP-ALG supports SIP trunks. It can support both the SIP Registrar and the SIP Proxy when used with a call management system that is external to the XTM device.

It can be difficult to coordinate the many components of a VoIP installation. We recommend you make sure that VoIP connections work successfully before you add an H.323 or SIP-ALG. This can help you to troubleshoot any problems.

## Instant Messaging Support

There are no configuration steps necessary to use instant messaging (IM) with the SIP-ALG. We support these types of IM:

- Page-based IM — Supported as part of the default SIP protocol.
- Session-based IM — Available through our support of MSRP (MessagingSession Relay Protocol) over TCP.



---

## ALG Functions

When you enable a SIP-ALG, your XTM device:

- Automatically responds to VoIP applications and opens the appropriate ports
- Makes sure that VoIP connections use standard SIP protocols
- Generates log messages for auditing purposes
- Supports SIP presence through the use of the SIP *Publish* method. This allows softphone users to see peer status.

Many VoIP devices and servers use NAT (Network Address Translation) to open and close ports automatically. The H.323 and SIP-ALGs also perform this function. You must disable NAT on your VoIP devices if you configure an H.323 or SIP-ALG.

For instructions to add the SIP-ALG to your XTM device configuration, see *Add a Proxy Policy to Your Configuration* on page 417.

If you must change the proxy definition, you can use the **New/Edit Proxy Policies** dialog box to modify the definition. This dialog box has three tabs: **Policy**, **Properties**, and **Advanced**.

## Policy Tab

- **SIP-ALG connections are** — Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)**. Define who appears in the **From** and **To** lists.  
For more information, see *Set Access Rules for a Policy* on page 392.
- **Use policy-based routing** — To use policy-based routing in your proxy definition, see *Configure Policy-Based Routing* on page 395.
- You can also configure static NAT or configure server load balancing.  
For more information, see *Configure Static NAT* on page 179 and *Configure Server Load Balancing* on page 182.
- **Proxy action** — Select the proxy action to use for this policy. You can also edit the rulesets for proxy actions.

## Properties Tab

- To edit or add a comment to this policy configuration, type the comment in the **Comment** text box.
- To define the logging settings for the policy, click **Logging** and *Set Logging and Notification Preferences* on page 723.
- If you set the **SIP-ALG connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use SIP.  
For more information, see *Block Sites Temporarily with Policy Settings* on page 538.
- To change the idle timeout that is set by the XTM device or authentication server, see *Set a Custom Idle Timeout*.

## Advanced Tab

You can use several other options in your SIP-ALG definition:

- *Set an Operating Schedule*
- *Add a Traffic Management Action to a Policy*
- *Set ICMP Error Handling*
- *Apply NAT Rules* (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- *Enable QoS Marking or Prioritization Settings for a Policy*
- *Set the Sticky Connection Duration for a Policy*

## Configure the Proxy Action

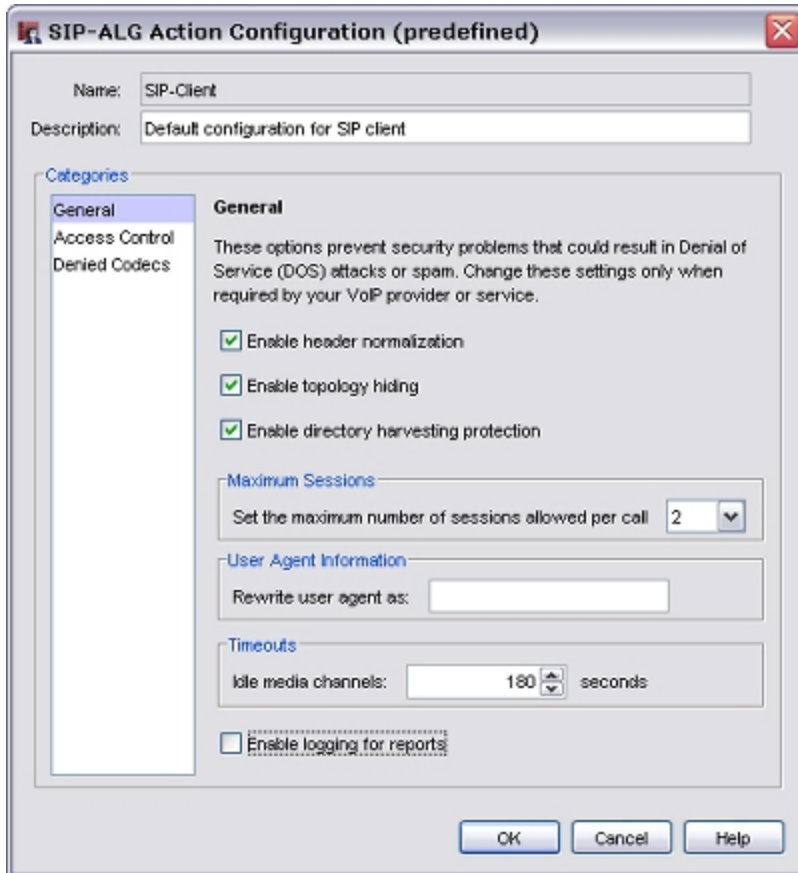
You can choose a predefined proxy action or configure a user-defined proxy action for this proxy. For more information about how to configure proxy actions, see *About Proxy Actions* on page 403.

For the SIP-ALG, you can configure these categories of settings for a proxy action:

- *SIP-ALG: General Settings*
- *SIP-ALG: Access Control*
- *SIP-ALG: Denied Codecs*

## SIP-ALG: General Settings

On the **SIP-ALG Action Configuration** dialog box **General** page, you can set security and performance options for the SIP-ALG (Application Layer Gateway).



### *Enable header normalization*

To deny malformed or extremely long SIP headers, select this check box. While these headers often indicate an attack on your XTM device, you can disable this option if necessary for your VoIP solution to operate correctly.

### *Enable topology hiding*

This feature rewrites SIP traffic headers to remove private network information, such as IP addresses. We recommend that you select this option unless you have an existing VoIP gateway device that performs topology hiding.

### *Enable directory harvesting protection*

To prevent attackers from stealing user information from VoIP gatekeepers protected by your XTM device, select this check box. This option is enabled by default.

#### *Maximum sessions*

Use this feature to restrict the maximum number of audio or video sessions that can be created with a single VoIP call.

For example, if you set the number of maximum sessions to one and participate in a VoIP call with both audio and video, the second connection is dropped. The default value is two sessions and the maximum value is four sessions. The XTM device sends a log message when it denies a media session above this number.

#### *User agent information*

To identify outgoing H.323 traffic as a client you specify, type a new user agent string in the **Rewrite user agent as** text box.

To remove the false user agent, clear the text box.

#### *Timeouts*

When no data is sent for a specified amount of time on a VoIP audio, video, or data channel, your XTM device closes that network connection. The default value is 180 seconds (three minutes) and the maximum value is 600 seconds (ten minutes).

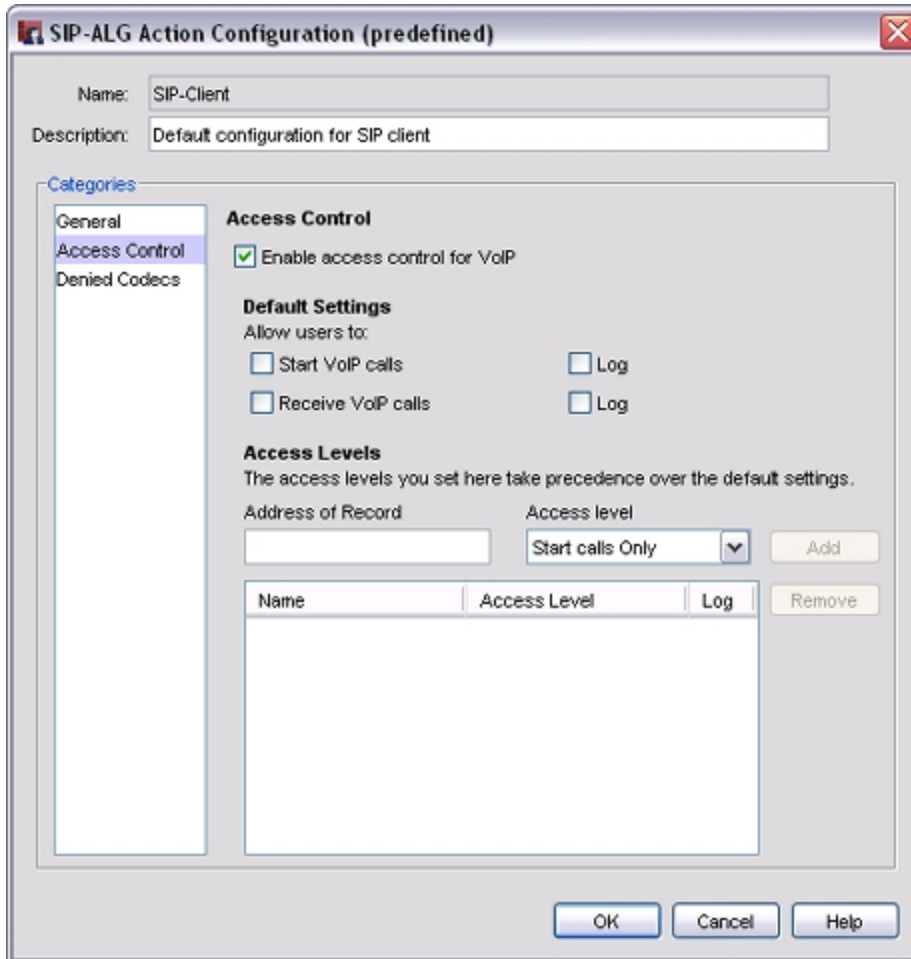
To specify a different time interval, type or select the time in seconds in the **Idle media channels** text box.

#### *Enable logging for reports*

To send a log message for each connection request managed by the SIP-ALG, select this check box. To create accurate reports on SIP traffic, you must select this check box.

## SIP-ALG: Access Control

On the **SIP-ALG Action Configuration** dialog box **Access Control** page, you can create a list of users who are allowed to send VoIP network traffic.



### *Enable access control for VoIP*

To enable the access control feature, select this check box. When enabled, the SIP-ALG allows or restricts calls based on the options you set.

### *Default Settings*

To allow all VoIP users to start calls by default, select the **Start VoIP calls** check box.

To allow all VoIP users to receive calls by default, select the **Receive VoIP calls** check box.

To create a log message for each SIP VoIP connection that is started or received, select the adjacent **Log** check box.

### Access Levels

To create an exception to the default settings you specified, type the **Address of Record** (the address that shows up in the TO and FROM headers of the packet) for the exception. This is usually a SIP address in the format *user@domain*, such as *myuser@example.com*.

From the **Access Level** drop-down list, select an access level and click **Add**.

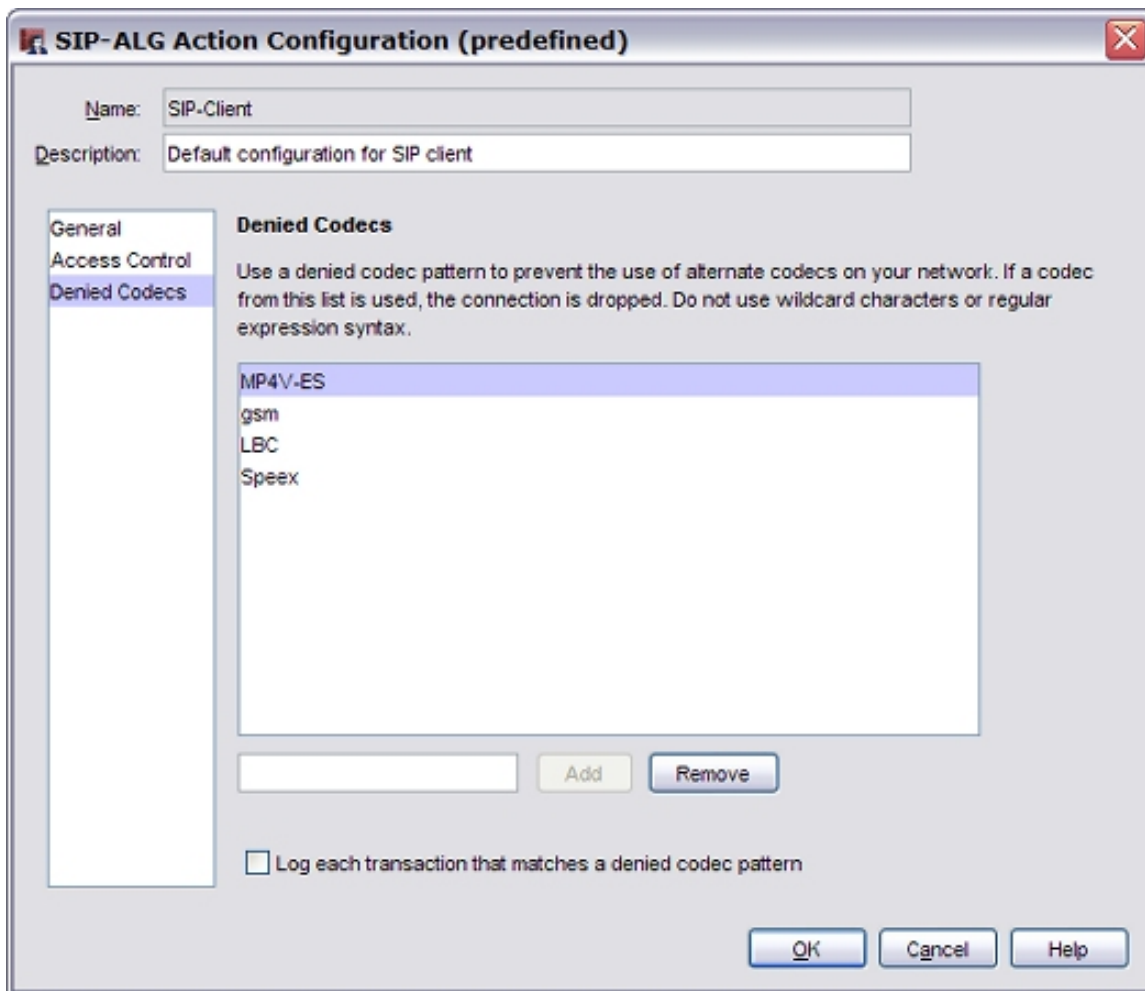
You can select whether to allow users to **Start calls only**, **Receive calls only**, **Start and receive calls**, or give them **No VoIP access**. These settings apply only to SIP VoIP traffic.

To delete an exception, select it in the list and click **Remove**.

Connections made by users who have an access level exception are logged by default. If you do not want to log connections made by a user with an access level exception, clear the **Log** check box adjacent to the exception.

## SIP-ALG: Denied Codecs

On the **Denied Codecs** page, you can set the VoIP voice, video, and data transmission codecs that you want to deny on your network.



### *Denied Codecs list*

Use this feature to deny one or more VoIP codecs. When a SIP VoIP connection is opened that uses a codec specified in this list, your XTM device closes the connection automatically.

This list is empty by default. We recommend that you add a codec to this list if it consumes too much bandwidth, presents a security risk, or if it is necessary to have your VoIP solution operate correctly.

For example, you may choose to deny the G.711 or G.726 codecs because they use more than 32 Kb/sec of bandwidth, or you may choose to deny the Speex codec because it is used by an unauthorized VOIP application.

To add a codec to the list, type the codec name or unique text pattern in the text box and click **Add**. Do not use wildcard characters or regular expression syntax. The codec patterns are case sensitive.

To delete a codec from the list, select it and click **Remove**.

### *Log each transaction that matches a denied codec pattern*

Select this option to create a log message when your XTM device denies SIP traffic that matches a codec in this list.

## About the SMTP-Proxy

SMTP (Simple Mail Transport Protocol) is a protocol used to send email messages between email servers and also between email clients and email servers. It usually uses a TCP connection on Port 25. You can use the SMTP-proxy to control email messages and email content. The proxy scans SMTP messages for a number of filtered parameters, and compares them against the rules in the proxy configuration.

With an SMTP-proxy filter you can:

- Adjust timeout, maximum email size, and line length limit to make sure the SMTP-proxy does not use too many network resources and can prevent some types of attacks.
- Customize the deny message that users see when an email they try to receive is blocked.
- Filter content embedded in email with MIME types and name patterns.
- Limit the email addresses that email can be addressed to and automatically block email from specific senders.

To add the SMTP-proxy to your XTM device configuration, see *Add a Proxy Policy to Your Configuration* on page 417.

If you must change the proxy definition, you can use the **New/Edit Proxy Policies** dialog box to modify the definition. This dialog box has three tabs: **Policy**, **Properties**, and **Advanced**.

## Policy Tab

- **SMTP-proxy connections are** — Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)**. Define who appears in the **From** and **To** lists.  
For more information, see *Set Access Rules for a Policy* on page 392.
- **Use policy-based routing** — To use policy-based routing in your proxy definition, see *Configure Policy-Based Routing* on page 395.
- You can also configure static NAT or configure server load balancing.  
For more information, see *Configure Static NAT* on page 179 and *Configure Server Load Balancing* on page 182.
- **Proxy action** — Select the proxy action to use for this policy. You can also edit the rulesets for proxy actions.

## Properties Tab

- To edit or add a comment to this policy configuration, type the comment in the **Comment** text box.
- To define the logging settings for the policy, click **Logging** and *Set Logging and Notification Preferences* on page 723.
- If you set the **SMTP-proxy connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use SMTP.  
For more information, see *Block Sites Temporarily with Policy Settings* on page 538.
- To change the idle timeout that is set by the XTM device or authentication server, see *Set a Custom Idle Timeout*.



## Advanced Tab

You can use several other options in your proxy definition:

- *Set an Operating Schedule*
- *Add a Traffic Management Action to a Policy*
- *Set ICMP Error Handling*
- *Apply NAT Rules* (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- *Enable QoS Marking or Prioritization Settings for a Policy*
- *Set the Sticky Connection Duration for a Policy*

## Configure the Proxy Action

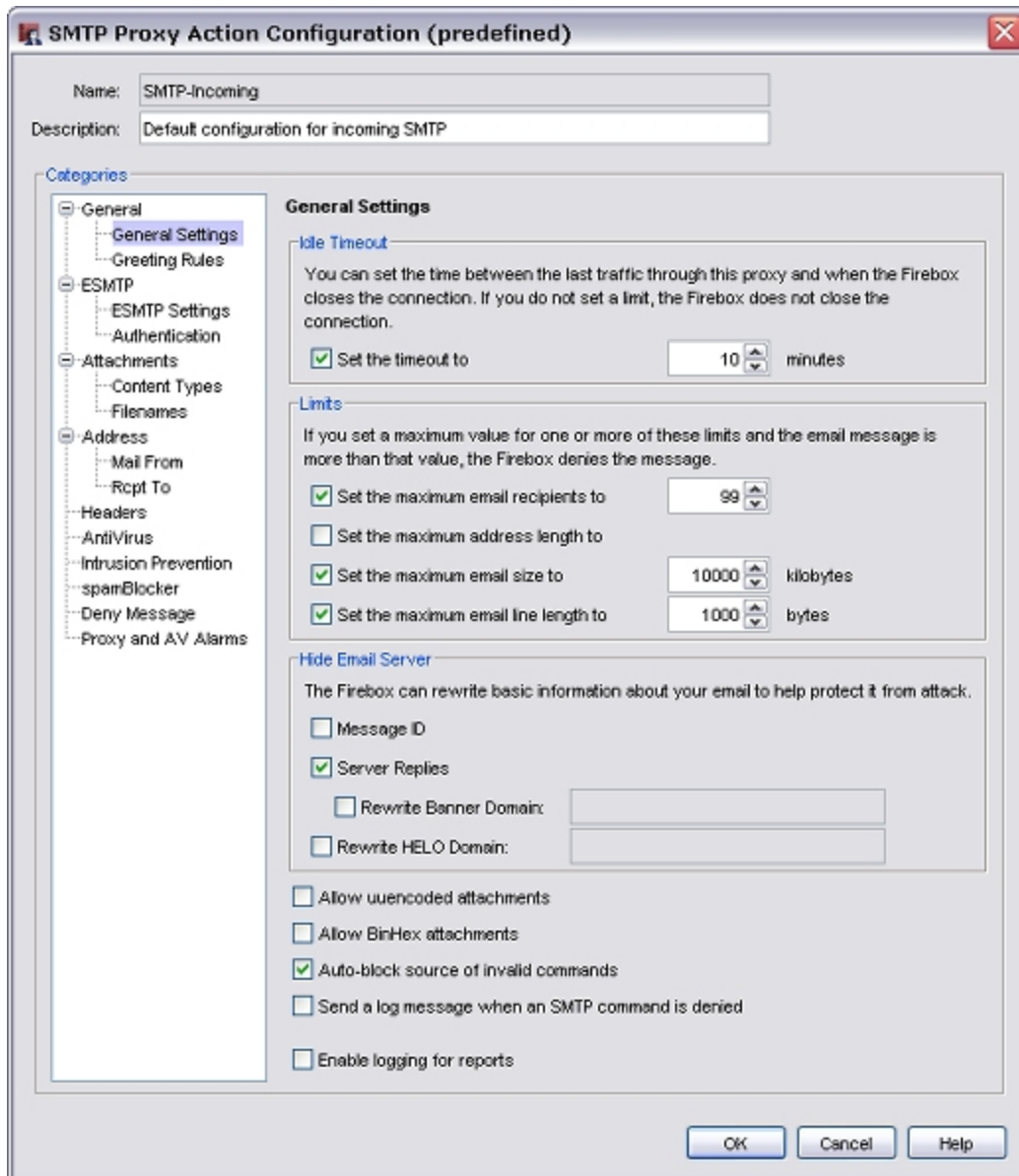
You can choose a predefined proxy action or configure a user-defined proxy action for this proxy. For more information about how to configure proxy actions, see *About Proxy Actions* on page 403.

For the SMTP-proxy, you can configure these categories of settings for a proxy action:

- *SMTP-Proxy: General Settings*
- *SMTP Proxy: Greeting Rules*
- *SMTP-Proxy: ESMTP Settings*
- *SMTP-Proxy: Authentication*
- *SMTP-Proxy: Content Types*
- *SMTP-Proxy: File Names*
- *SMTP-Proxy: Mail From/Rcpt To*
- *SMTP-Proxy: Headers*
- *SMTP-Proxy: AntiVirus*
- *SMTP-Proxy: Deny Message*
- *SMTP-Proxy: spamBlocker*
- *Proxy and AV Alarms*

## SMTP-Proxy: General Settings

On the **SMTP Proxy Action Configuration** dialog box **General Settings** page, you can set basic SMTP-proxy parameters such as idle timeout, message limits, and email message information.



### Idle timeout

You can set the length of time an incoming SMTP connection can be idle before the connection times out. The default value is 10 minutes.

### Set the maximum email recipients

To set the maximum number of email recipients to which a message can be sent, select this check box. In the adjacent text box that appears, type or select the number of recipients.

The XTM device counts and allows the specified number of addresses through, and then drops the other addresses. For example, if you set the value to 50 and there is a message for 52 addresses, the first 50 addresses get the email message. The last two addresses do not get a copy of the message. The XTM device counts a distribution list as one SMTP email address (for example, support@example.com). You can use this feature to decrease spam email because spam usually includes a large recipient list. When you enable this option, make sure you do not also deny legitimate email.

#### *Set the maximum address length to*

To set the maximum length of email addresses, select this check box. In the adjacent text box that appears, type or select the maximum length for an email address in bytes.

#### *Set the maximum email size to*

To set the maximum length of an incoming SMTP message, select this check box. In the adjacent text box that appears, type or select the maximum size for each email in kilobytes.

Most email is sent as 7-bit ASCII text. The exceptions are Binary MIME and 8-bit MIME. 8-bit MIME content (for example, MIME attachments) is encoded with standard algorithms (Base64 or quote-printable encoding) to enable them to be sent through 7-bit email systems. Encoding can increase the length of files by as much as one third. To allow messages as large as 10 KB, you must set this option to a minimum of 1334 bytes to make sure all email gets through.

#### *Set the maximum email line length to*

To set the maximum line length for lines in an SMTP message, select this check box. In the adjacent text box that appears, type or select the length in bytes for each line in an email.

Very long line lengths can cause buffer overflows on some email systems. Most email clients and systems send short line lengths, but some web-based email systems send very long lines.

#### *Hide Email Server*

You can replace MIME boundary and SMTP greeting strings in email messages. These are used by hackers to identify the SMTP server vendor and version.

Select the **Message ID** and **Server Replies** check boxes.

If you have an email server and use the SMTP-Incoming proxy action, you can set the SMTP-proxy to replace the domain that appears in your SMTP server banner with a domain name you select. To do this, you must select the **Server Replies** and **Rewrite Banner Domain** check boxes. In the **Rewrite Banner Domain** text box, type the domain name to use in your banner.

If you use the SMTP-Outgoing proxy action, you can set the SMTP-proxy to replace the domain shown in the HELO or EHLO greetings. A HELO or EHLO greeting is the first part of an SMTP transaction, when your email server announces itself to a receiving email server. To do this, select the **Rewrite HELO Domain** check box. In the **Rewrite HELO Domain** text box, type the domain name to use in your HELO or EHLO greeting.

*Allow uuencoded attachments*

To enable the SMTP-proxy to allow uuencoded attachments to email messages, select this check box. Uuencode is an older program used to send binary files in ASCII text format over the Internet. UUencode attachments can be security risks because they appear as ASCII text files but can actually contain executable files.

*Allow BinHex attachments*

To enable the SMTP-proxy to allow BinHex attachments to email messages, select this check box. BinHex, which is short for binary-to-hexadecimal, is a utility that converts a file from binary to ASCII format.

*Auto-block sources of invalid commands*

To add senders of invalid SMTP commands to the Blocked Sites list, select this check box. Invalid SMTP commands often indicate an attack on your SMTP server.

*Send a log message when an SMTP command is denied*

To send a log message for connection requests that are denied by the SMTP-proxy, select this checkbox.

*Enable logging for reports*

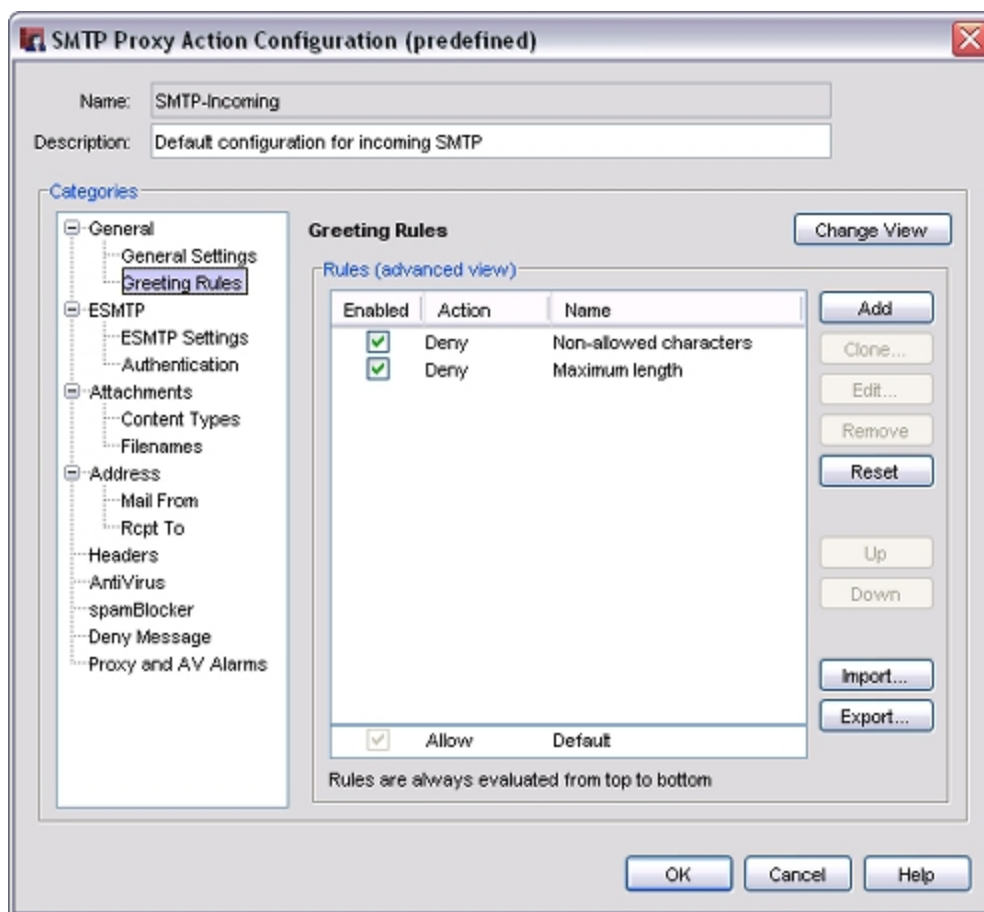
To send a log message for each connection request through the SMTP-proxy, select this check box. To create accurate reports on SMTP traffic, you must select this check box.

## SMTP Proxy: Greeting Rules

The proxy examines the initial HELO/EHLO responses when the SMTP session is initialized. The default rules for the SMTP-Incoming proxy action make sure that packets with greetings that are too long, or include characters that are not correct or expected, are denied. You can add, delete, or modify rules.

1. In the **Categories** tree, select **Greeting Rules**.

*The Greeting Rules page appears.*



2. *Add, Change, or Delete Rules.*
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

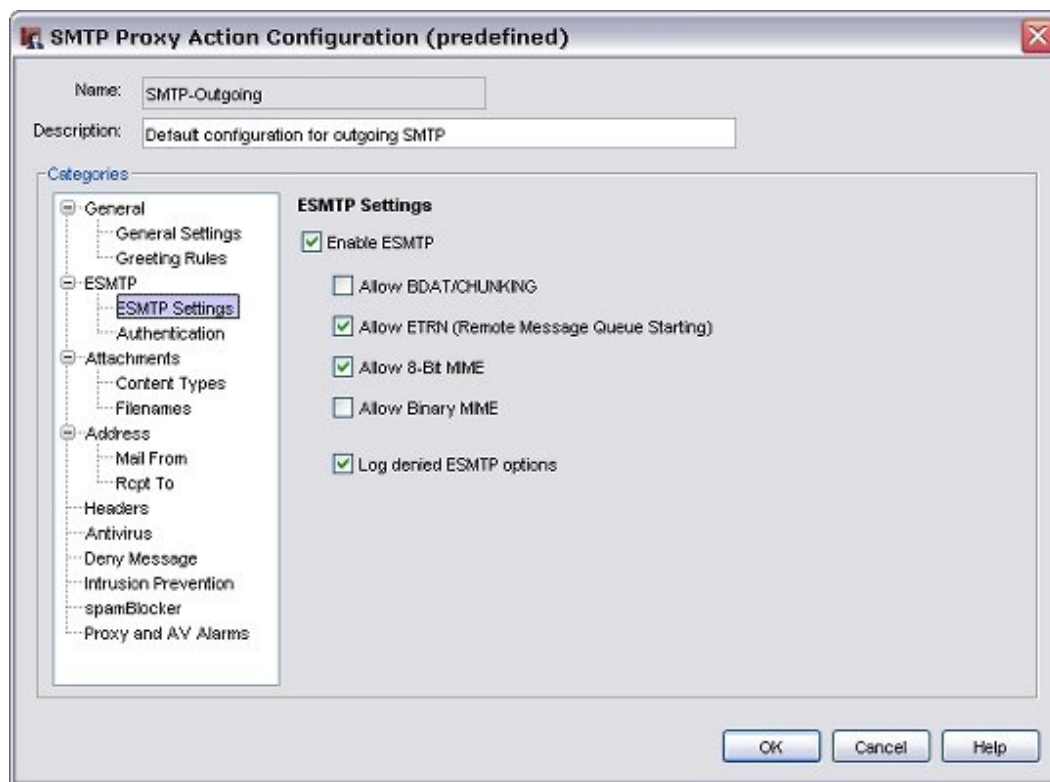
For more information on predefined proxy actions, see *About Proxy Actions*.

## SMTP-Proxy: ESMTP Settings

On the **ESMTP Settings** page, you can set the filtering for ESMTP content. Although SMTP is widely accepted and widely used, some parts of the Internet community want more functionality in SMTP. ESMTP gives a method for functional extensions to SMTP, and to identify servers and clients that support extended features.

1. In the **Categories** tree, select **ESMTP Settings**.

*The ESMTP Settings page appears.*



2. Configure these options:

### *Enable ESMTP*

Select this check box to enable all fields. If you clear this check box, all other check boxes on this page are disabled. When the options are disabled, the settings for each options are saved. If this option is enabled again, all the settings are restored.

### *Allow BDAT/CHUNKING*

Select this check box to allow BDAT/CHUNKING. This enables large messages to be sent more easily through SMTP connections.

### *Allow ETRN (Remote Message Queue Starting)*

This is an extension to SMTP that allows an SMTP client and server to interact to start the exchange of message queues for a given host.

### *Allow 8-Bit MIME*

Select this check box to allow transmission of 8-bit data messages. When this option is disabled, messages encoded with 8-bit MIME are denied by the SMTP-proxy. Enable this option only if your email server has the ability to send 8-bit data transmissions.

#### *Allow Binary MIME*

Select to allow the Binary MIME extension, if the sender and receiver accept it. Binary MIME prevents the overhead of base64 and quoted-printable encoding of binary objects sent that use the MIME message format with SMTP. We do not recommend you select this option as it can be a security risk.

#### *Log denied ESMTP options*

Select this check box to create a log message for unknown ESMTP options that are stripped by the SMTP-proxy. Clear this check box to disable this option.

3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

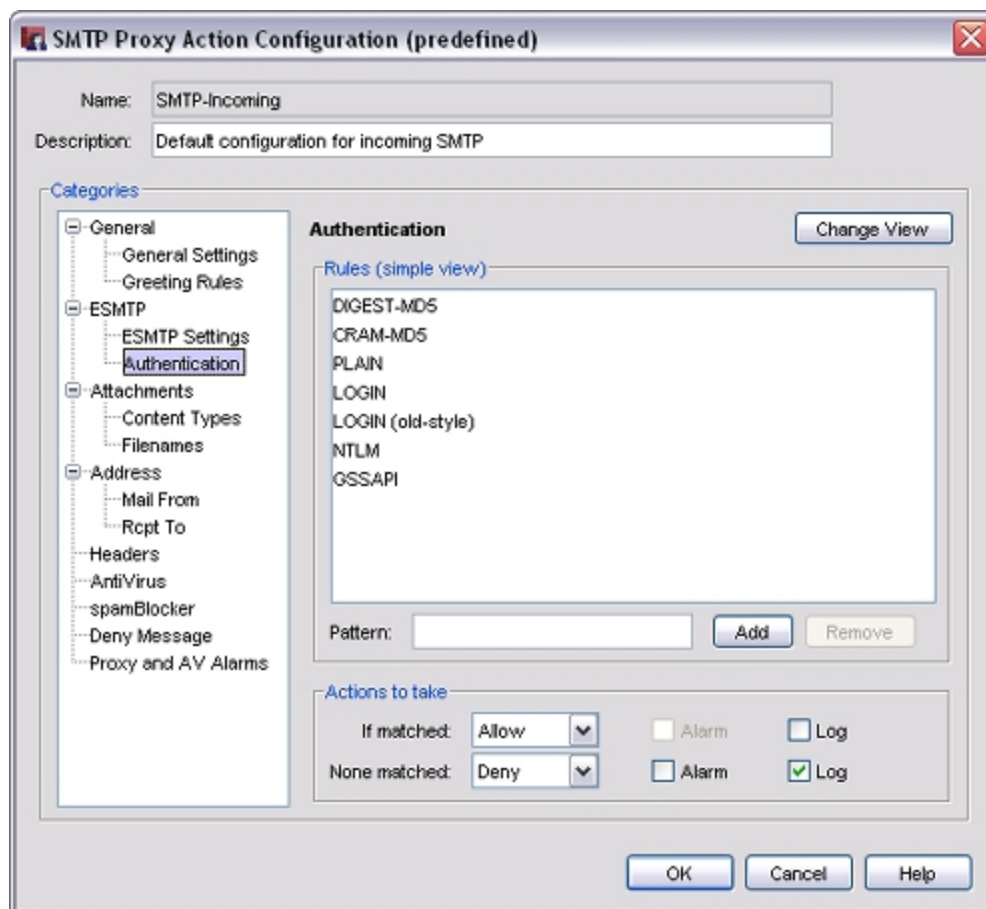
For more information on predefined proxy actions, see *About Proxy Actions*.

## **SMTP-Proxy: Authentication**

This ruleset allows these ESMTP authentication types: DIGEST- MD5, CRAM-MD5, PLAIN, LOGIN, LOGIN (old style), NTLM, and GSSAPI. The default rule denies all other authentication types. The RFC that tells about the SMTP authentication extension is RFC 2554.

If the default ruleset does not meet all of your business needs, you can add, delete, or modify rules:

1. In the **Categories** tree, select **ESMTP > Authentication**.  
*The Authentication page appears.*



2. Add, Change, or Delete Rules.
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.



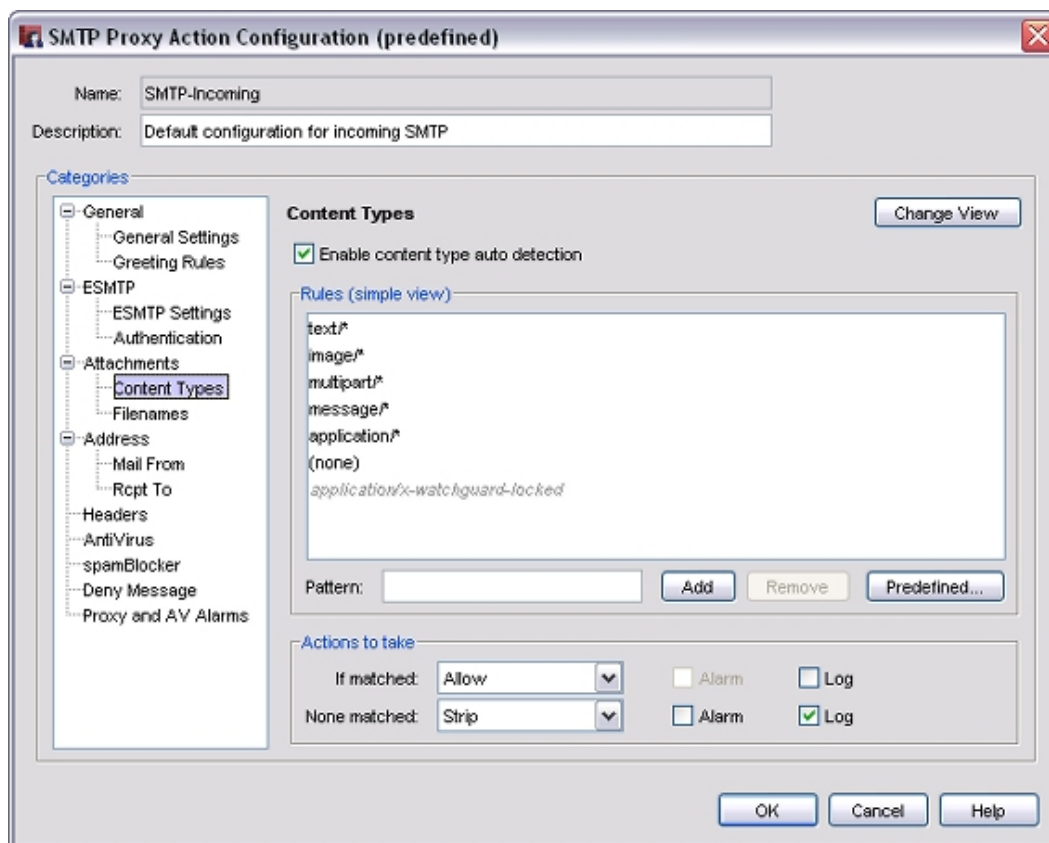
## SMTP-Proxy: Content Types

Certain kinds of content embedded in email can be a security threat to your network. Other kinds of content can decrease the productivity of your users. You can use the ruleset for the SMTP-Incoming proxy action to set values for incoming SMTP content filtering. You can use the ruleset for the SMTP-Outgoing proxy action to set values for outgoing SMTP content filtering. The SMTP-proxy allows these content types: text/\*, image/\*, multipart/\*, and message/\* . You can add, delete, or modify rules.

You can also configure the SMTP-proxy to automatically examine the content of email messages to determine the content type. If you do not enable this option, the SMTP-proxy uses the value stated in the email header, which clients sometimes set incorrectly. For example, an attached .pdf file might have a content type stated as application/octet-stream. If you enable content type auto detection, the SMTP-proxy recognizes the .pdf file and uses the actual content type, application/pdf. If the proxy does not recognize the content type after it examines the content, it uses the value stated in the email header, as it would if content type auto detection were not enabled. Because hackers often try to disguise executable files as other content types, we recommend that you enable content type auto detection to make your installation more secure.

1. In the **Categories** tree, select **Content Types**.

*The Content Types page appears.*



2. To enable the SMTP-proxy to examine content to determine content type, select the **Enable content type auto detection** check box.

3. To add a predefined content type to the ruleset, follow the steps in the subsequent section.
4. *Add, Change, or Delete Rules.*
5. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
6. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

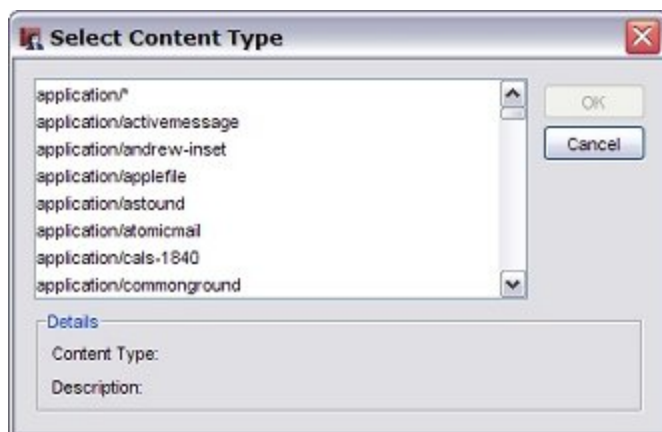
For more information on predefined proxy actions, see *About Proxy Actions*.

## Add Common Content Types

The proxy definition includes several content types that you can easily add to the Content Type ruleset.

To add a content type:

1. Click **Predefined**.  
*The Select Content Type dialog box appears.*

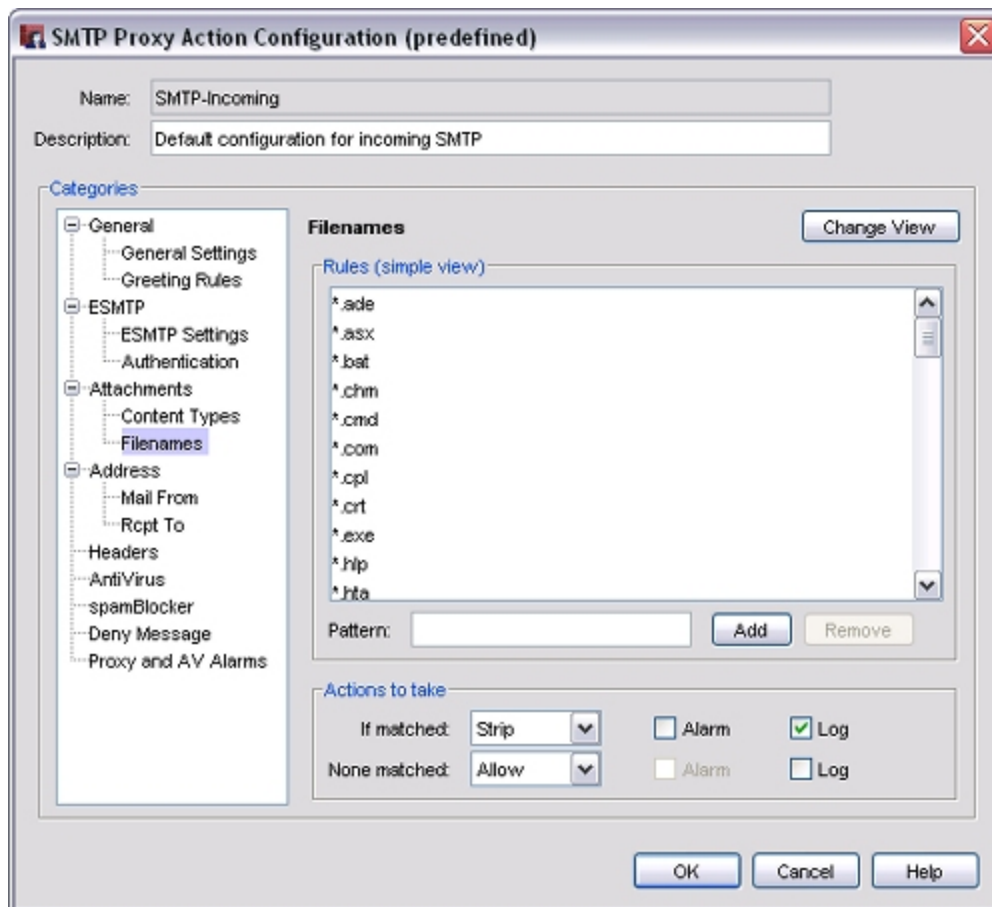


2. Select one or more content types in the list.
3. Click **OK**.

## SMTP-Proxy: File Names

You can use the ruleset for the SMTP-Incoming proxy action to put limits on file names for incoming email attachments. You use the ruleset for the SMTP-Outgoing proxy action to put limits on file names for outgoing email attachments. You can add, delete, or modify rules.

1. In the **Categories** tree, select **Attachments > Filenames**.  
*The ESMTP Settings page appears.*



2. Add, Change, or Delete Rules.
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

## SMTP-Proxy: Mail From/Rcpt To

You can use the **Address: Mail From** ruleset to put limits on email and to allow email into your network only from specified senders. The default configuration is to allow email from all senders. You can add, delete, or modify rules.

The **Address: Rcpt To** ruleset can limit the email that goes out of your network to only specified recipients. The default configuration allows email to all recipients out of your network. On an SMTP-Incoming proxy action, you can use the **Rcpt To** ruleset to make sure your email server can not be used for email relaying. For more information, see *Protect Your SMTP Server from Email Relaying* on page 504.

You can also use the **Rewrite A** option in a rule to configure the XTM device to change the *From* and *To* components of your email address to a different value. This feature is also known as *SMTP masquerading*.

Other options available in the **Mail From** and **Rcpt To** rulesets:

*Block source-routed addresses*

Select this check box to block a message when the sender address or recipient address contains source routes. A source route identifies the path a message must take when it goes from host to host. The route can identify which mail routers or *backbone* sites to use. For example, @backbone.com:freddyb@something.com means that the host named Backbone.com must be used as a relay host to deliver mail to freddyb@something.com. By default, this option is enabled for incoming SMTP packets and disabled for outgoing SMTP packets.

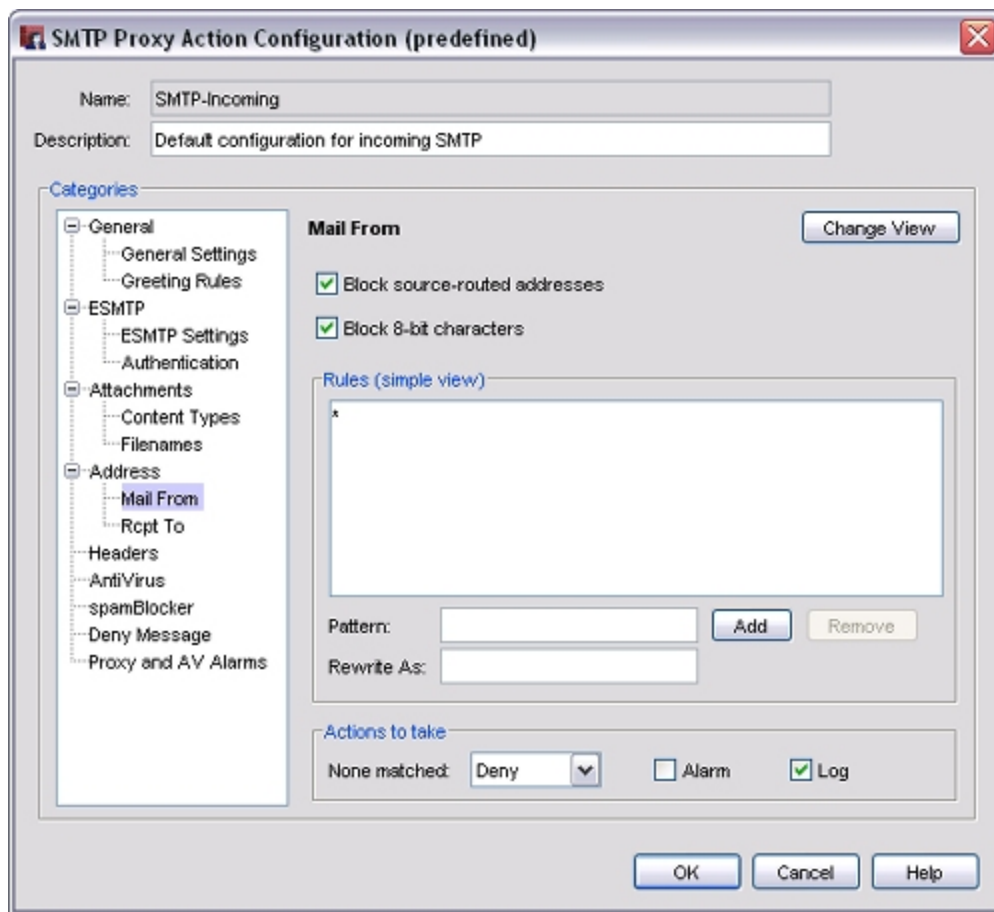
*Block 8-bit characters*

Select this check box to block a message that has 8-bit characters in the sender user name or recipient user name. This allows an accent on an alphabet character. By default, this option is enabled for incoming SMTP packets and disabled for outgoing SMTP packets.

To configure the SMTP proxy to put limits on the email traffic through your network:

1. In the **Categories** tree, select **Address > Mail From** or **Address > Rcpt To**.

*The Mail From or Rcpt To page appears.*



2. *Add, Change, or Delete Rules.*
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

## SMTP-Proxy: Headers

Header rulesets allow you to set values for incoming or outgoing SMTP header filtering. You can add, delete, or modify rules.

1. In the **Categories** tree, select **Headers**.  
*The Headers page appears.*
2. *Add, Change, or Delete Rules.*
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

## SMTP-Proxy: AntiVirus

If you have purchased and enabled the Gateway AntiVirus feature, the options in the AntiVirus category set the actions necessary if a virus is found in an email message. It also sets actions for when an email message contains an attachment that the SMTP-proxy cannot scan.

- To use the proxy definition screens to activate Gateway AntiVirus, see *Activate Gateway AntiVirus from Proxy Definitions* on page 1171.
- To use the **Subscription Services** menu in Policy Manager to activate Gateway AntiVirus, see *Activate Gateway AntiVirus with a Wizard from Policy Manager* on page 1168.
- To configure Gateway AntiVirus for the SMTP-proxy, see *Configure Gateway AntiVirus Actions* on page 1172.

When you enable Gateway AntiVirus, you must set the actions to be taken if a virus or error is found in an email message or attachment. The options for antivirus actions are:

### *Allow*

Allows the packet to go to the recipient, even if the content contains a virus.

### *Lock*

Locks the attachment. This is a good option for files that cannot be scanned by the SMTP-proxy. A file that is locked cannot be opened easily by the user. Only the administrator can unlock the file. The administrator can use a different antivirus tool to scan the file and examine the content of the attachment. For information about how to unlock a file locked by Gateway AntiVirus, see *Unlock a*

*File Locked by Gateway AntiVirus* on page 1179.

#### *Quarantine*

When you use the SMTP proxy with the spamBlocker security subscription, you can send email messages with viruses or possible viruses to the Quarantine Server. For more information on the Quarantine Server, see *About the Quarantine Server* on page 1225. For information on how to set up Gateway AntiVirus to work with the Quarantine Server, see *Configure Gateway AntiVirus to Quarantine Email* on page 1181.

#### *Remove*

Removes the attachment and allows the message through to the recipient.

#### *Drop*

Drops the packet and drops the connection. No information is sent to the source of the message.

#### *Block*

Blocks the packet, and adds the IP address of the sender to the Blocked Sites list.

**Note** *If you set the configuration to allow attachments, your configuration is less secure.*

Gateway AntiVirus scans each file up to a specified kilobyte count. Any additional bytes in the file are not scanned. This allows the proxy to partially scan very large files without a large effect on performance. Enter the file scan limit in the **Limit scanning to first** field.

For information about the default and maximum scan limits for each SMTP-proxy model, see *About Gateway AntiVirus Scan Limits* on page 1181.

## SMTP-Proxy: Deny Message

When content is denied, the XTM device sends a default *deny message* that replaces the denied content. This message appears in a recipients email message when the proxy blocks an email. You can change the text of that deny message. The first line of the deny message is a section of the HTTP header. You must include an empty line between the first line and the body of the message.

The default deny message appears in the **Deny Message** text box. To change this to a custom message, use these variables:

*%(reason)%*

Includes the reason the XTM device denied the content.

*%(type)%*

Includes the type of content that was denied.

*%(filename)%*

Includes the file name of the denied content.

*%(virus)%*

Includes the name or status of a virus for Gateway AntiVirus users.

`%(action)%`

Includes the name of the action taken. For example: lock or strip.

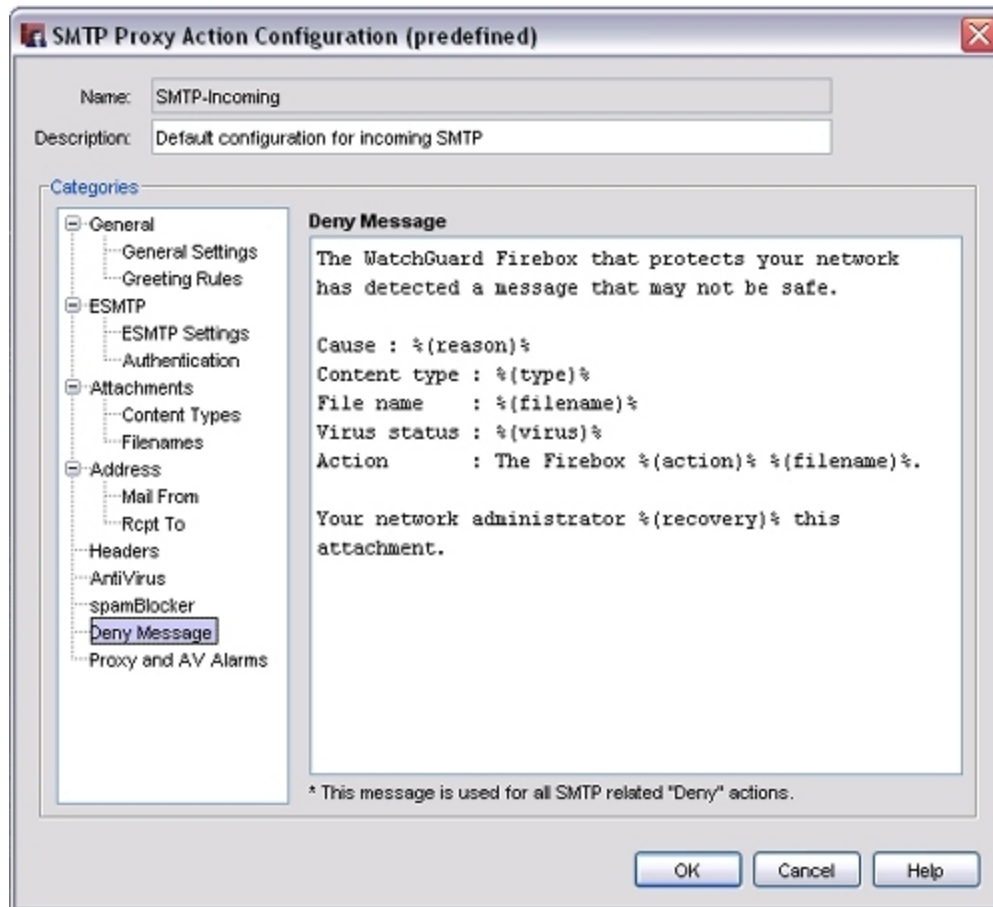
`%(recovery)%`

Includes whether you can recover the attachment.

To configure the deny message:

1. In the **Categories** tree, select **Deny Message**.

The *Deny Message* page appears.



2. In the **Deny Message** text box, type a custom plain text message in standard HTML.
3. To change settings for other categories in this proxy, see the topic for the next category you want to modify.
4. Click **OK**.

If you modified a predefined proxy action, when you save the changes you are prompted to clone (copy) your settings to a new action.

For more information on predefined proxy actions, see *About Proxy Actions*.

## SMTP-Proxy: spamBlocker

Unwanted email, also known as spam, can quickly fill your Inbox. A large volume of spam decreases bandwidth, degrades employee productivity, and wastes network resources. The WatchGuard spamBlocker option increases your capacity to catch spam at the edge of your network when it tries to enter your system. If you have purchased and enabled the spamBlocker feature, the fields in the spamBlocker category set the actions for email messages identified as spam.

Although you can use the proxy definition screens to activate and configure spamBlocker, it is easier to use the **Subscription Services** menu in Policy Manager. For more information, see *About spamBlocker* on page 1141.

## Configure the SMTP-Proxy to Quarantine Email

The WatchGuard Quarantine Server provides a safe, full-featured quarantine mechanism for any email messages suspected or known to be spam or to contain viruses. This repository receives email messages from the SMTP-proxy and filtered by spamBlocker.

To configure the SMTP-proxy to quarantine email:

1. Add the SMTP proxy to your configuration and enable spamBlocker in the proxy definition.  
Or, enable spamBlocker and select to enable it for the SMTP-proxy.
2. When you set the actions spamBlocker applies for different categories of email (as described in *Configure spamBlocker* on page 1146), make sure you select the **Quarantine** action for at least one of the categories. When you select this action, you are prompted to configure the Quarantine Server if you have not already done so.

You can also select the **Quarantine** action for email messages identified by Virus Outbreak Detection as containing viruses. For more information, see *Configure Virus Outbreak Detection Actions for a Policy* on page 1151.

## Protect Your SMTP Server from Email Relaying


Email relaying, also called *mail spamming* or open mail relay, is an intrusion in which a person uses your email server, address, and other resources, to send large amounts of spam email. This can cause system crashes, equipment damage, and financial loss.

If you are not familiar with the issues involved with mail relaying, or are unsure whether your email server is vulnerable to mail relaying, we recommend you research your own email server and learn its potential vulnerabilities. The XTM device can give basic mail relay protection if you are unsure of how to configure your email server. However, you find out how to use your email server to prevent email relaying.

To protect your server, you change the configure of the SMTP-proxy policy that filters traffic from the external network to your internal SMTP server to include your domain information. When you type your domain, you can use the wildcard \* character. Then, any email address that ends with *@your-domain-name* is allowed. If your email server accepts email for more than one domain, you can add more domains. For example, if you add both *\*@example.com* and *\*@\*.example.com* to the list, your email server will accept all email destined to the top-level *example.com* domain and all email destined to sub-domains of *example.com*. For example, *rnd.example.com*.



Before you start this procedure, you must know the names of all domains that your SMTP email server receives email for.

1. *Open Policy Manager.*
2. Double-click the SMTP-proxy policy that filters traffic from the external network to an internal SMTP server.  
*The Edit Policy Properties dialog box appears with the Policy tab selected.*
3. Adjacent to the **Proxy action** drop-down list, click .  
*The SMTP-proxy Action Configuration dialog box appears.*
5. In the **Categories** tree, select **Address > Rcpt To**.
6. In the **Pattern** text box, type \* @[your-domain-name].
7. In the **Actions to Take** section, from the **None Matched** drop-down list, select **Deny**.  
*Any email destined to an address other than the domains in the list is denied.*
8. Click **OK** to close the **SMTP Proxy Action Configuration** dialog box.
9. Click **OK** again to close the SMTP policy definition.
10. Click **Close** to close the **Edit Policy Properties** dialog box.
11. *Save the Configuration File.*
12. Click **Add**.  
*Your domain appears in the Rules list.*

Another way to protect your server is to type a value in the **Rewrite As** text box in this dialog box. The XTM device then changes the From and To components of your email address to a different value. This feature is also known as *SMTP masquerading*.

## About the TCP-UDP-Proxy

The TCP-UDP-proxy is included for these protocols on non-standard ports: HTTP, HTTPS, SIP, and FTP. For these protocols, the TCP-UDP proxy relays the traffic to the correct proxies for the protocols or enables you to allow or deny traffic. For other protocols, you can select to allow or deny traffic. You can also use this proxy policy to allow or deny IM (instant messaging) and P2P (peer-to-peer) network traffic. The TCP-UDP proxy is intended only for outgoing connections.

To add the TCP-UDP-proxy to your XTM device configuration, see *Add a Proxy Policy to Your Configuration* on page 417.

If you must change the proxy definition, you can use the **New/Edit Proxy Policies** dialog box to modify the definition. This dialog box has three tabs: **Policy**, **Properties**, and **Advanced**.

### Policy Tab

- **TCP-UDP-proxy connections are** — Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)**, and define who appears in the **From** and **To** list (on the **Policy** tab of the proxy definition). For more information, see *Set Access Rules for a Policy* on page 392.
- **Use policy-based routing** — To use policy-based routing in your proxy definition, see *Configure Policy-Based Routing* on page 395.
- You can also configure static NAT or configure server load balancing. For more information, see *Configure Static NAT* on page 179 and *Configure Server Load Balancing* on page 182.
- **Proxy action** — Select the proxy action to use for this policy. You can also edit the rulesets for proxy actions.

### Properties Tab

- To edit or add a comment to this policy configuration, type the comment in the **Comment** text box.
- To define the logging settings for the policy, click **Logging** and *Set Logging and Notification Preferences* on page 723.
- If you set the **SMTP-proxy connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use TCP-UDP. For more information, see *Block Sites Temporarily with Policy Settings* on page 538.
- To change the idle timeout that is set by the XTM device or authentication server, see *Set a Custom Idle Timeout*.

## Advanced Tab

You can use several other options in your proxy definition:

- *Set an Operating Schedule*
- *Add a Traffic Management Action to a Policy*
- *Set ICMP Error Handling*
- *Apply NAT Rules* (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- *Enable QoS Marking or Prioritization Settings for a Policy*
- *Set the Sticky Connection Duration for a Policy*

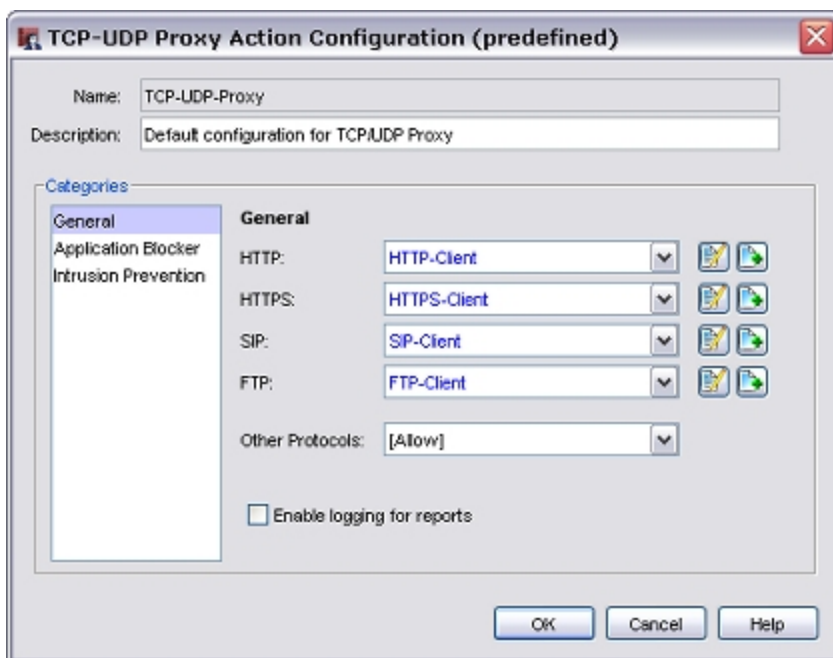
## Configure the Proxy Action

You can choose a predefined proxy action or configure a user-defined proxy action for this proxy. For more information about how to configure proxy actions, see *About Proxy Actions* on page 403.

For the TCP-UDP-proxy, you can configure the general settings for a proxy action. For more information, see *TCP-UDP-Proxy: General Settings*.

## TCP-UDP-Proxy: General Settings

On the **TCP-UDP Proxy Action Configuration** dialog box **General** page, you set basic parameters for the TCP-UDP-proxy.



### *Proxy actions to redirect traffic*

The TCP-UDP-proxy can pass HTTP, HTTPS, SIP, and FTP traffic to proxy policies that you have already created when this traffic is sent over non-standard ports.

For each of these protocols, from the adjacent drop-down list, select the proxy policy to use to manage this traffic.

If you do not want your XTM device to use a proxy policy to filter a protocol, select **Allow** or **Deny** from the adjacent drop-down list.

**Note** To ensure that your XTM device operates correctly, you cannot select the **Allow** option for the FTP protocol.

### *Enable logging for reports*

To send a log message for each connection request through the TCP-UDP-proxy, select this check box. To create accurate reports on TCP-UDP traffic, you must select this check box.

# 15 Traffic Management and QoS

---

## About Traffic Management and QoS

In a large network with many computers, the volume of data that moves through the firewall can be very large. A network administrator can use Traffic Management and Quality of Service (QoS) actions to prevent data loss for important business applications, and to make sure mission-critical applications take priority over other traffic.

Traffic Management and QoS provide a number of benefits. You can:

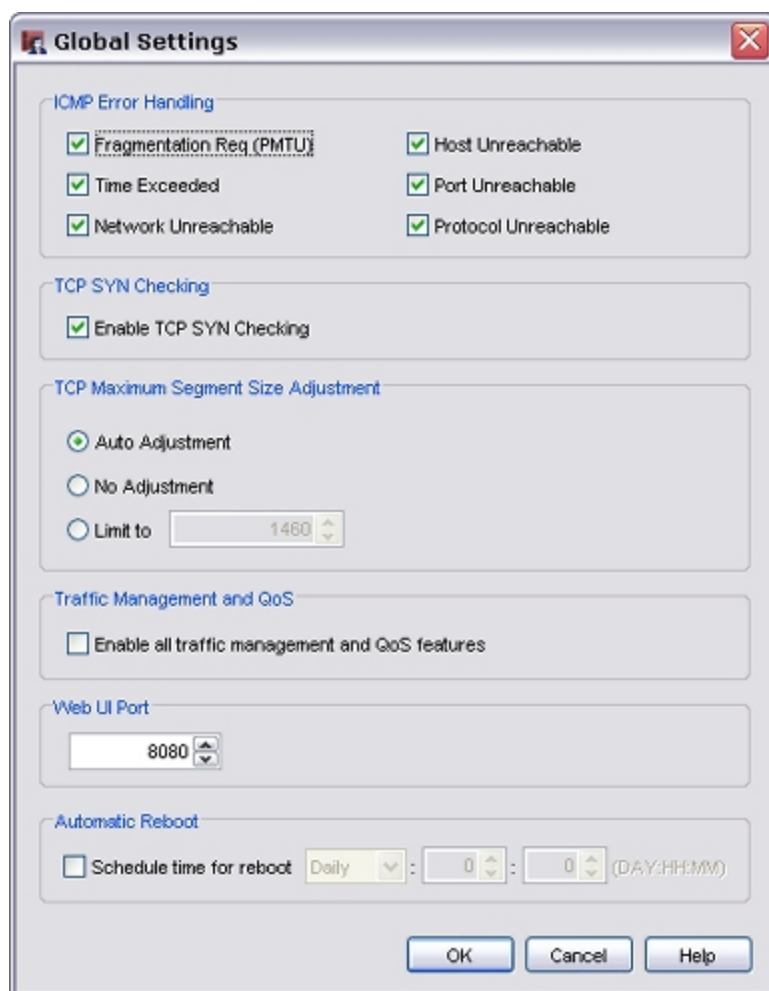
- Guarantee or limit bandwidth
- Control the rate at which the XTM device sends packets to the network
- Prioritize when to send packets to the network

To apply traffic management to policies, you define a Traffic Management action, which is a collection of settings that you can apply to one or more policy definitions. This way you do not need to configure the traffic management settings separately in each policy. You can define additional Traffic Management actions if you want to apply different settings to different policies.

## Enable Traffic Management and QoS

For performance reasons, all traffic management and QoS features are disabled by default. You must enable these features in Global Settings before you can use them.

1. Select **Setup > Global Settings**.  
*The Global Settings window appears.*



2. Select the **Enable all traffic management and QoS features** check box.
3. Click **OK**.
4. *Save the Configuration File.*

## Guarantee Bandwidth

Bandwidth reservations can prevent connection timeouts. A traffic management queue with reserved bandwidth and low priority can give bandwidth to real-time applications with higher priority when necessary without disconnecting. Other traffic management queues can take advantage of unused reserved bandwidth when it becomes available.

For example, suppose your company has an FTP server on the external network and you want to guarantee that FTP always has at least 200 kilobytes per second (KBps) through the external interface. You might also consider setting a minimum bandwidth from the trusted interface to make sure that the connection has end-to-end guaranteed bandwidth. To do this, you would create a Traffic Management action that defines a minimum of 200 KBps for FTP traffic on the external interface. You would then create an FTP policy and apply the Traffic Management action. This will allow *ftp put* at 200 KBps. If you want to allow *ftp get* at 200 KBps, you must configure the FTP traffic on the trusted interface to also have a minimum of 200 KBps.

As another example, suppose your company uses multimedia materials (streaming media) to train external customers. This streaming media uses RTSP over port 554. You have frequent FTP uploads from the trusted to external interface, and you do not want these uploads to compete with your customers ability to receive the streaming media. To guarantee sufficient bandwidth, you could apply a Traffic Management action to the external interface for the streaming media port.

The guaranteed bandwidth setting works with the **Outgoing Interface Bandwidth** setting configured for each interface to make sure you do not guarantee more bandwidth than actually exists. This setting also helps you make sure the sum of your guaranteed bandwidth settings does not fill the link such that non-guaranteed traffic cannot pass. For example, suppose the link is 1 Mbps and you try to use a Traffic Management action that guarantees 973 Kbps (0.95 Mbps) to the FTP policy on that link. With these settings, the FTP traffic could use so much of the available bandwidth that other types of traffic cannot use the interface. If you try to configure the XTM device this way, Policy Manager warns you that you are approaching the limit set for the **Outgoing Interface Bandwidth** setting for that interface.

## Restrict Bandwidth

To preserve the bandwidth that is available for other applications, you can restrict the amount of bandwidth for certain traffic types or applications. This can also discourage the use of certain applications when users find that the speed of the application's performance is significantly degraded.

The **Maximum Bandwidth** setting in a Traffic Management action enables you to set a limit on the amount of traffic allowed by the Traffic Management action.

For example, suppose that you want to allow FTP downloads but you want to limit the speed at which users can download files. You can add a Traffic Management action that has the Maximum bandwidth set to a low amount on the trusted interface, such as 100 kbps. This can help discourage FTP downloads when the users on the trusted interface find the FTP experience is unsatisfactory.

## QoS Marking

QoS marking creates different classes of service for different kinds of outbound network traffic. When you *mark* traffic, you change up to six bits on packet header fields defined for this purpose. Other devices can make use of this marking and provide appropriate handling of a packet as it travels from one point to another in a network.

You can enable QoS marking for an individual interface or an individual policy. When you define QoS marking for an interface, each packet that leaves the interface is marked. When you define QoS marking for a policy, all traffic that uses that policy is also marked.

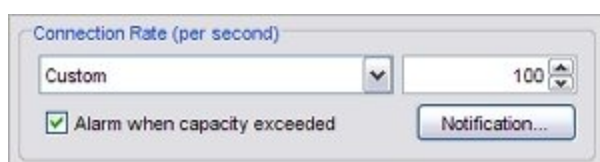
## Traffic priority

You can assign different levels of priority either to policies or for traffic on a particular interface. Traffic prioritization at the firewall allows you to manage multiple class of service (CoS) queues and reserve the highest priority for real-time or streaming data. A policy with high priority can take bandwidth away from existing low priority connections when the link is congested so traffic must compete for bandwidth.

## Set Connection Rate Limits

To improve network security, you can create a limit on a policy so that it only filters a specified number of connections per second. If additional connections are attempted, the traffic is denied and a log message is created. You can also create an alarm for when this happens. You can configure the alarm to make the XTM device send an event notification to the SNMP management system, or to send a notification in the form of an email message or a pop-up window on the management computer.

1. Double-click a policy to edit it.  
*The Edit Policy Properties dialog box appears.*
2. Select the **Advanced** tab.
3. From the **Connection Rate** drop-down list, select the maximum number of connections per second. The default configuration puts no limits on the connection rate.



4. To receive a notification when the connection rate is exceeded, select the **Alarm when capacity exceeded** check box.
5. Click **Notification** and set the notification parameters, as described in *Set Logging and Notification Preferences* on page 723.
6. Click **OK**.

## About QoS Marking

Today's networks often consist of many kinds of network traffic that compete for bandwidth. All traffic, whether of prime importance or negligible importance, has an equal chance of reaching its destination in a timely manner. Quality of Service (QoS) marking gives critical traffic preferential treatment to make sure it is delivered quickly and reliably.

QoS functionality must be able to differentiate the various types of data streams that flow across your network. It must then *mark* data packets. QoS marking creates different classifications of service for different kinds of network traffic. When you mark traffic, you change up to six bits on packet header fields defined for this purpose. The XTM device and other QoS-capable devices can use this marking to provide appropriate handling of a packet as it travels from one point to another in a network.

Fireware XTM supports two types of QoS marking: IP Precedence marking (also known as Class of Service) and Differentiated Service Code Point (DSCP) marking. For more information on these marking types and the values you can set, see *Marking Types and Values* on page 514.

### Before you begin

- Make sure your LAN equipment supports QoS marking and handling. You may also need to make sure your ISP supports QoS.
- The use of QoS procedures on a network requires extensive planning. You can first identify the theoretical bandwidth available and then determine which network applications are high priority, particularly sensitive to latency and jitter, or both.



## QoS marking for interfaces and policies

You can enable QoS marking for an individual interface or an individual policy. When you define QoS marking for an interface, each packet that leaves the interface is marked. When you define QoS marking for a policy, all traffic that uses that policy is also marked. The QoS marking for a policy overrides any QoS marking set on an interface.

For example, suppose your XTM device receives QoS-marked traffic from a trusted network and sends it to an external network. The trusted network already has QoS marking applied, but you want the traffic to your executive team to be given higher priority than other network traffic from the trusted interface. First, set the QoS marking for the trusted interface to one value. Then, add a policy with QoS marking set for the traffic to your executive team with a higher value.

## QoS marking and IPSec traffic

If you want to apply QoS to IPSec traffic, you must create a specific firewall policy for the corresponding IPSec policy and apply QoS marking to that policy.

You can also choose whether to preserve existing marking when a marked packet is encapsulated in an IPSec header.

To preserve marking:

1. Select **VPN > VPN Settings**.  
*The VPN Settings dialog box appears.*
2. Select the **Enable TOS for IPSec** check box.
3. Click **OK**.  
*All existing marking is preserved when the packet is encapsulated in an IPSec header.*

To remove marking:

1. Select **VPN > VPN Settings**.  
*The VPN Settings dialog box appears.*
2. Clear the **Enable TOS for IPSec** check box.
3. Click **OK**.  
*The TOS bits are reset and marking is not preserved.*

## Marking Types and Values

Fireware XTM supports two types of QoS Marking: IP Precedence marking (also known as Class of Service) and Differentiated Service Code Point (DSCP) marking. IP Precedence marking affects only the first three bits in the IP type of service (TOS) octet. DSCP marking expands marking to the first six bits in the IP TOS octet. Both methods allow you to either preserve the bits in the header, which may have been marked previously by an external device, or change them to a new value.

DSCP values can be expressed in numeric form or by special keyword names that correspond to per-hop behavior (PHB). Per-hop behavior is the priority applied to a packet when it travels from one point to another in a network. Fireware DSCP marking supports three types of per-hop behavior:

### *Best-Effort*

Best-Effort is the default type of service and is recommended for traffic that is not critical or real-time. All traffic falls into this class if you do not use QoS Marking.

### *Assured Forwarding (AF)*

Assured Forwarding is recommended for traffic that needs better reliability than the best-effort service. Within the Assured Forwarding (AF) type of per-hop behavior, traffic can be assigned to three classes: Low, Medium, and High.

### *Expedited Forwarding (EF)*

This type has the highest priority. It is generally reserved for mission-critical and real-time traffic.

Class-Selector (CSx) code points are defined to be backward compatible with IP Precedence values. CS1–CS7 are identical to IP Precedence values 1–7.

The subsequent table shows the DSCP values you can select, the corresponding IP Precedence value (which is the same as the CS value), and the description in PHB keywords.

DSCP Value	Equivalent IP Precedence value (CS values)	Description: Per-hop Behavior keyword
0		Best-Effort (same as no marking)
8	1	Scavenger*
10		AF Class 1 - Low
12		AF Class 1 - Medium
14		AF Class 1 - High
16	2	
18		AF Class 2 - Low
20		AF Class 2 - Medium
22		AF Class 2 - High
24	3	

DSCP Value	Equivalent IP Precedence value (CS values)	Description: Per-hop Behavior keyword
26		AF Class 3 - Low
28		AF Class 3 - Medium
30		AF Class 3 - High
32	4	
34		AF Class 4 - Low
36		AF Class 4 - Medium
38		AF Class 4 - High
40	5	
46		EF
48	6	Internet Control
56	7	Network Control

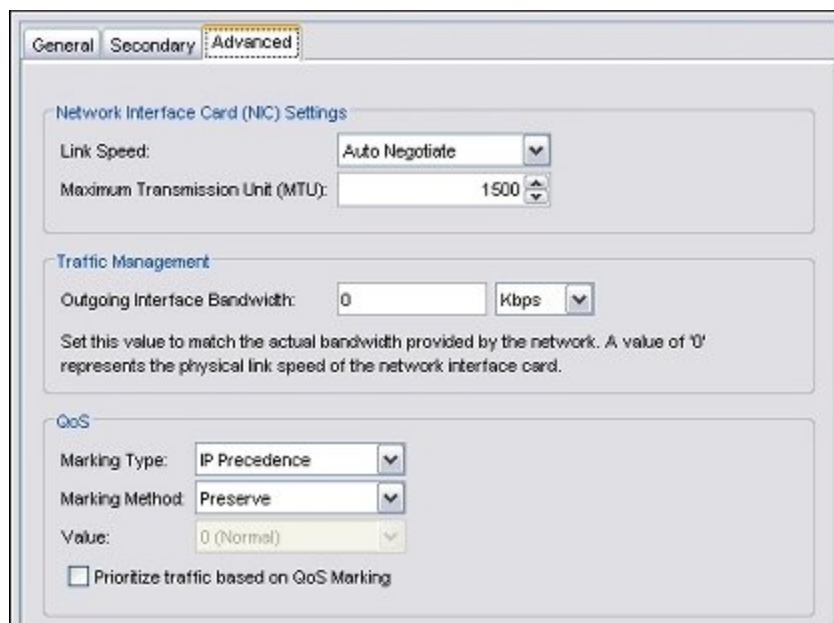
\* The Scavenger class is used for the lowest priority traffic (for example, media sharing or gaming applications). This traffic has a lower priority than Best-Effort.

For more information on DSCP values, see this RFC: <http://www.rfc-editor.org/rfc/rfc2474.txt>.

## Enable QoS Marking for an Interface

You can set the default marking behavior as traffic goes out of an interface. These settings can be overridden by settings defined for a policy.

1. Select **Setup > Global Settings**.  
*The Global Settings dialog box appears.*
2. Select the **Enable all traffic management and QoS features** check box. Click **OK**.  
*You might want to disable these features at a later time if you do performance testing or network debugging.*
3. Select **Network > Configuration**.  
*The Network Configuration dialog box appears.*
4. Select the interface for which you want to enable QoS Marking. Click **Configure**.  
*The Interface Settings dialog box appears.*
5. Select the **Advanced** tab.



6. In the **Marking Type** drop-down list, select either **DSCP** or **IP Precedence**.
7. In the **Marking Method** drop-down list, select the marking method:
  - **Preserve** — Do not change the current value of the bit. The XTM device prioritizes the traffic based on this value.
  - **Assign** — Assign the bit a new value.
  - **Clear** — Clear the bit value (set it to zero).
8. If you selected **Assign** in the previous step, select a marking value.  
 If you selected the **IP precedence** marking type you can select values from 0 (normal priority) through 7 (highest priority).  
 If you selected the **DSCP** marking type, the values are 0–56.  
 For more information on these values, see *Marking Types and Values* on page 514.
9. Select the **Prioritize traffic based on QoS Marking** check box.
10. Click **OK**.

## Enable QoS Marking or Prioritization Settings for a Policy

In addition to marking the traffic that leaves a XTM device interface, you can also mark traffic on a per-policy basis. The marking action you select is applied to all traffic that uses the policy. Multiple policies that use the same marking actions have no effect on each other. XTM device interfaces can also have their own QoS Marking settings. To use QoS Marking or prioritization settings for a policy, you must override any per-interface QoS Marking settings.

1. Double-click the icon for the policy whose traffic you want to mark.  
*The Edit Policy Properties dialog box appears.*
2. Select the **Advanced** tab.
3. Select the **QoS** tab.
4. To enable the other QoS and prioritization option, select the **Override per-interface settings** check box.
5. Complete the settings as described in the subsequent sections.

6. Click **OK**.
7. *Save the Configuration File*



## QoS Marking Settings

For more information on QoS marking values, see *Marking Types and Values* on page 514.

1. From the **Marking Type** drop-down list, select either **DSCP** or **IP Precedence**.
2. From the **Marking Method** drop-down list, select the marking method:
  - **Preserve** — Do not change the current value of the bit. The XTM device prioritizes the traffic based on this value.
  - **Assign** — Assign the bit a new value.
  - **Clear** — Clear the bit value (set it to zero).
3. If you selected **Assign** in the previous step, select a marking value.  
 If you selected the **IP precedence** marking type you can select values from 0 (normal priority) through 7 (highest priority).  
 If you selected the **DSCP** marking type, the values are 0–56.
4. From the **Prioritize Traffic Based On** drop-down list, select **QoS Marking**.

## Prioritization Settings

Many different algorithms can be used to prioritize network traffic. Firewall XTM uses a high performance, class-based queuing method based on the Hierarchical Token Bucket algorithm. Prioritization in Firewall XTM is applied per policy and is equivalent to CoS (class of service) levels 0–7, where 0 is normal priority (default) and 7 is the highest priority. Level 5 is commonly used for streaming data such as VoIP or video conferencing. Reserve levels 6 and 7 for policies that allow system administration connections to make sure they are always available and avoid interference from other high priority network traffic. Use the Priority Levels table as a guideline when you assign priorities.

1. From the **Prioritize Traffic Based On** drop-down list, select **Custom Value**.
2. From the **Value** drop-down list, select a priority level.

## Priority Levels

We recommend that you assign a priority higher than 5 only to WatchGuard administrative policies, such as the WatchGuard policy, the WG-Logging policy, or the WG-Mgmt-Server policy. Give high priority business traffic a priority of 5 or lower.

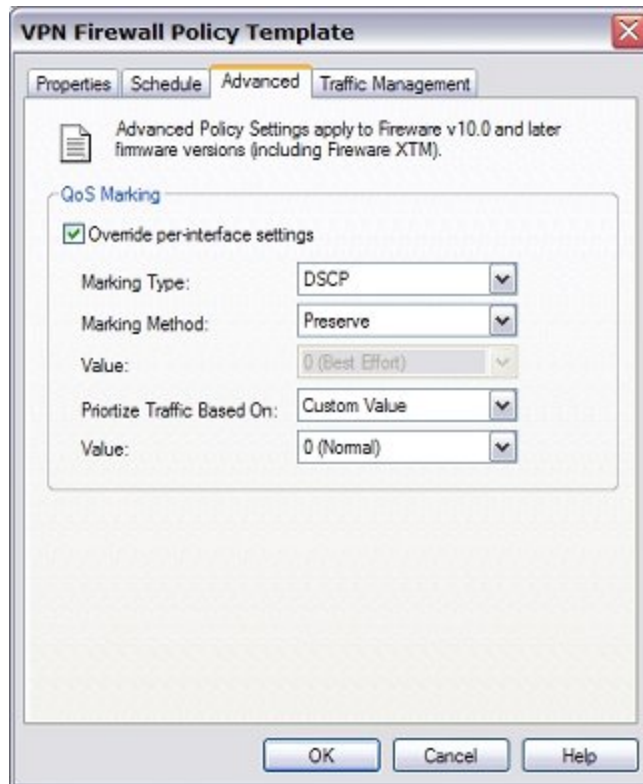
Priority	Description
0	Routine (HTTP, FTP)
1	Priority
2	Immediate (DNS)
3	Flash (Telnet, SSH, RDP)
4	Flash Override
5	Critical (VoIP)
6	Internetwork Control (Remote router configuration)
7	Network Control (Firewall, router, switch management)

## Enable QoS Marking for a Managed BOVPN Tunnel

To use QoS with a managed BOVPN tunnel, you must create a VPN firewall policy template and apply that template to the managed BOVPN tunnel. You cannot edit the default *Any* policy for managed BOVPN tunnels.

You can use QoS marking in a VPN firewall policy template to set different priorities for managed BOVPN tunnels that use different policy templates. The marking action you select is applied to all traffic that uses the policy template.

1. Open WatchGuard System Manager and connect to a Management Server.
2. Select the **Device Management** tab.
3. Expand **Managed VPNs** and expand **VPN Firewall Policy Templates**.
4. Select a VPN firewall policy template in the tree to edit it, or *Add VPN Firewall Policy Templates*.
5. In the **Settings** section, click **Configure**.  
*The VPN Firewall Policy Template dialog box appears.*
6. Select the **Advanced** tab.



7. Select the **Override per-interface settings** check box.
8. From the **Marking Type** drop-down list, select either **DSCP** or **IP Precedence**.
9. From the **Marking Method** drop-down list, select the marking method:
  - **Preserve** — Do not change the current value of the bit. The XTM device prioritizes the traffic based on this value.
  - **Assign** — Assign the bit a new value.
  - **Clear** — Clear the bit value (set it to zero).
10. If you selected **Assign** in the previous step, select a marking value.  
 If you selected the **IP precedence** marking type you can select values from 0 (normal priority) through 7 (highest priority).  
 If you selected the **DSCP** marking type, the values are 0–56.
11. In the **Prioritize Traffic Based On** drop-down list, select the traffic prioritization method:
  - **Custom Value** — Use a custom value to prioritize the traffic.
  - **QoS Marking** — Prioritize traffic based on QoS marking settings for this policy template.
12. If you selected **Custom Value**, in the **Value** drop-down list, select a priority level.  
  
 For more information about traffic priority values, see the table in *Enable QoS Marking or Prioritization Settings for a Policy*.
13. Click **OK**.

# Traffic Control and Policy Definitions

## Define a Traffic Management Action

Traffic Management actions can enforce bandwidth restrictions and guarantee a minimum amount of bandwidth for one or more policies. Each Traffic Management action can include settings for multiple interfaces. For example, on a Traffic Management action used with an HTTP policy for a small organization, you can set the minimum guaranteed bandwidth of a trusted interface to 250 kbps and the maximum bandwidth to 1000 kbps. This limits the speeds at which users can download files, but ensures that a small amount of bandwidth is always available for HTTP traffic. You can then set the minimum guaranteed bandwidth of an external interface to 150 kbps and the maximum bandwidth to 300 kbps to manage upload speeds at the same time.

## Determine Available Bandwidth


Before you begin, you must determine the available bandwidth of the interface used for the policy or policies you want to guarantee bandwidth. For external interfaces, you can contact your ISP (Internet Service Provider) to verify the service level agreement for bandwidth. You can then use a speed test with online tools to verify this value. These tools can produce different values depending on a number of variables. For other interfaces, you can assume the link speed on the XTM device interface is the theoretical maximum bandwidth for that network. You must also consider both the sending and receiving needs of an interface and set the threshold value based on these needs. If your Internet connection is asymmetric, use the uplink bandwidth set by your ISP as the threshold value.

## Determine the Sum of Your Bandwidth

You must also determine the sum of the bandwidth you want to guarantee for all policies on a given interface. For example, on a 1500 kbps external interface, you might want to reserve 600 kbps for all the guaranteed bandwidth and use the remaining 900 kbps for all other traffic.

All policies that use a given Traffic Management action share its connection rate and bandwidth settings. When they are created, policies automatically belong to the default Traffic Management action, which enforces no restrictions or reservations. If you create a Traffic Management action to set a maximum bandwidth of 10 Mbps and apply it to an FTP and an HTTP policy, all connections handled by those policies must share 10Mbps. If you later apply the same Traffic Management action to an SMTP policy, all three must share 10 Mbps. This also applies to connection rate limits and guaranteed minimum bandwidth. Unused guaranteed bandwidth reserved by one Traffic Management action can be used by others.

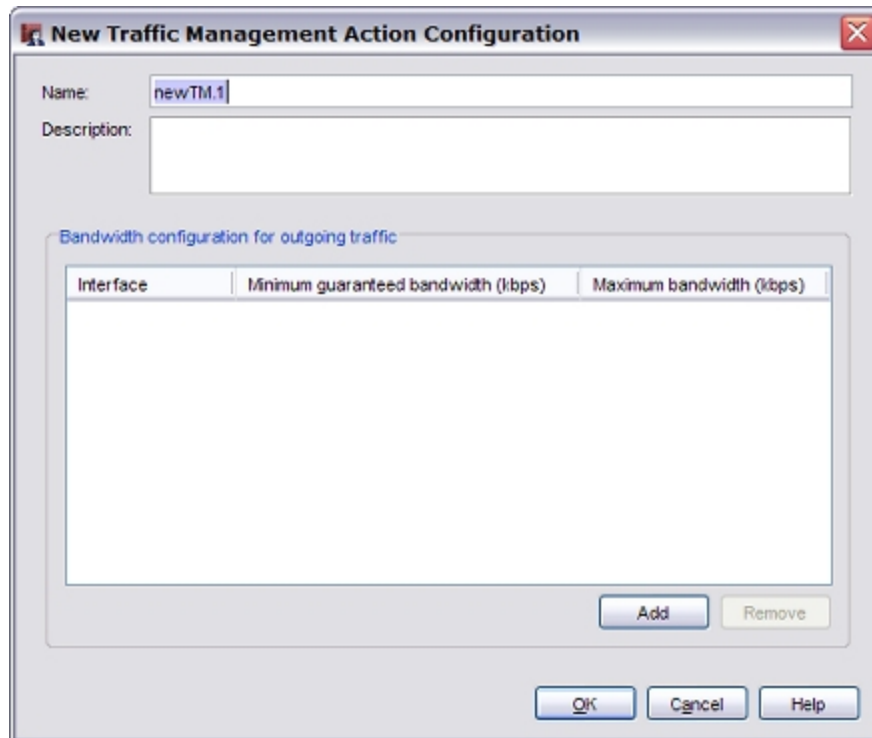
## Create or Modify a Traffic Management Action

1. Double-click the policy for which you want to guarantee a minimum bandwidth. Select the **Advanced** tab. Click .

Or, select **Setup > Actions > Traffic Management** and click **Add**.

*The New Traffic Management Action Configuration dialog box appears.*





2. In the **Bandwidth configuration for outgoing traffic** section, click **Add**.  
*An interface drop-down list appears.*
3. In the **Interface** column, click the drop-down list to select the interface for which you want to set a minimum bandwidth.

If you select an **External** interface, the action applies to upload speeds.

If you select a **Trusted** or **Optional** interface, the action applies to download speeds.

4. Double-click in the **Minimum guaranteed bandwidth** and **Maximum bandwidth** columns to edit the settings. Type a number to set the minimum or maximum bandwidth in kilobits per second.
5. Click **OK**.
6. If you defined the traffic action from a policy definition, the new traffic action now appears in **Traffic Management** on the **Advanced** tab.

If you defined the traffic actions from **Setup > Actions > Traffic Management**, you must *Add a Traffic Management Action to a Policy* for it to have an effect on your network.

## Add a Traffic Management Action to a Policy

After you *Define a Traffic Management Action*, you can add it to policy definitions. You can also add any existing traffic management actions to policy definitions.

1. Double-click the policy for which you want to guarantee a minimum bandwidth.
2. Select the **Advanced** tab.
3. In the **Traffic Management** drop-down list, select a traffic management action to apply to the policy.
4. Click **OK** to close the **Edit Policy Properties** dialog box.

If the sum of all guaranteed bandwidths for an interface approaches or exceeds the bandwidth limit you set for the interface, a warning message appears.

*The new action appears in the Traffic Management Actions dialog box.*



If you want to track the bandwidth used by a policy, go to the **Service Watch** tab of Firebox System Manager and specify **Bandwidth** instead of **Connections**. For more information, see *Visual Display of Policy Usage (Service Watch)* on page 764.

**Note** *If you have a multi-WAN configuration, bandwidth limits are applied separately to each interface.*

## Add a Traffic Management Action to Multiple Policies

When the same traffic management action is added to multiple policies, the maximum and minimum bandwidth apply to each interface in your configuration. If two policies share an action that has a maximum bandwidth of 100 kbps on a single interface, then all traffic on that interface that matches those policies is limited to 100 kbps total.

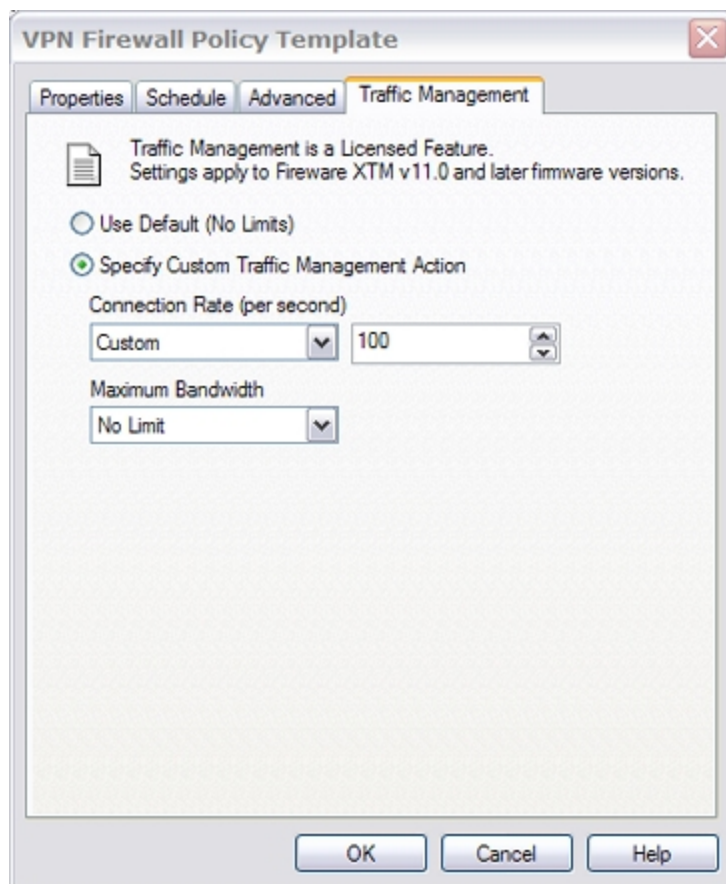
If you have limited bandwidth on an interface used for several applications, each with unique ports, you might need all the high priority connections to share one traffic management action. If you have lots of bandwidth to spare, you could create separate traffic management actions for each application.

## Add a Traffic Management Action to a BOVPN Firewall Policy

To use traffic management with a managed BOVPN tunnel, you must create a VPN firewall policy template and apply that template to the managed BOVPN tunnel. You cannot edit the default *Any* policy for managed BOVPN tunnels.

You can use traffic management in a VPN firewall policy template to set different bandwidth limits for managed BOVPN tunnels that use different policy templates. The marking action you select is applied to all traffic that uses the policy template.

1. Open WatchGuard System Manager and connect to a management server.
2. Select the **Device Management** tab.
3. Expand **Managed VPNs** and expand **VPN Firewall Policy Templates**.
4. Select a VPN firewall policy template in the tree to edit it, or *Add VPN Firewall Policy Templates*.
5. In the **Settings** section, click **Configure**.  
*The VPN Firewall Policy Template dialog box appears.*
6. Select the **Traffic Management** tab.



7. Select the **Specify Custom Traffic Management Action** check box.
8. Define the custom traffic management action as described in *Define a Traffic Management Action* on page 520.
9. Click **OK**.



# 16 Default Threat Protection

---

## About Default Threat Protection

WatchGuard Fireware XTM OS and the policies you create give you strict control over access to your network. A strict access policy helps keep hackers out of your network. But, there are other types of attacks that a strict policy cannot defeat. Careful configuration of default threat protection options for the XTM device can stop threats such as SYN flood attacks, spoofing attacks, and port or address space probes.

With default threat protection, a firewall examines the source and destination of each packet it receives. It looks at the IP address and port number and monitors the packets to look for patterns that show your network is at risk. If a risk exists, you can configure the XTM device to automatically block a possible attack. This proactive method of intrusion detection and prevention keeps attackers out of your network.

To configure default threat protection, see:

- *About Default Packet Handling Options*
- *About Blocked Sites*
- *About Blocked Ports*

You can also purchase an upgrade for your XTM device to use signature-based intrusion prevention. For more information, see *About Gateway AntiVirus* on page 1167.

## About Default Packet Handling Options

When your XTM device receives a packet, it examines the source and destination for the packet. It looks at the IP address and the port number. The device also monitors the packets to look for patterns that can show your network is at risk. This process is called *default packet handling*.

Default packet handling can:

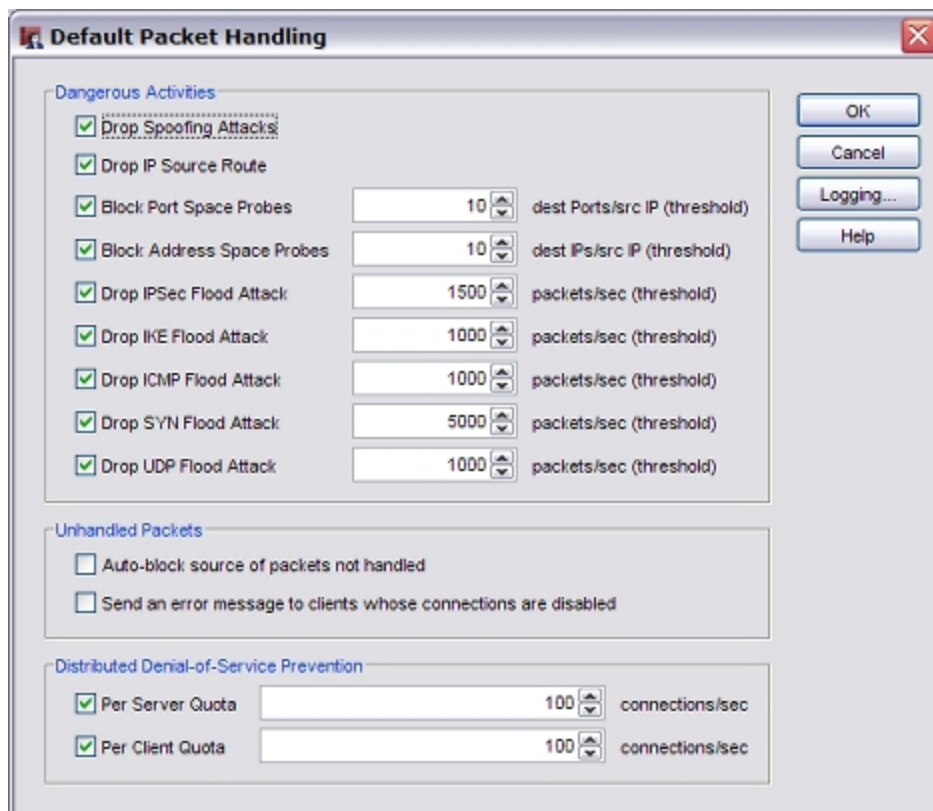
- Reject a packet that could be a security risk, including packets that could be part of a spoofing attack or SYN flood attack
- Automatically block all traffic to and from an IP address
- Add an event to the log file
- Send an SNMP trap to the SNMP management server
- Send a notification of possible security risks

Most default packet handling options are enabled in the default XTM device configuration. You can use Policy Manager to change the thresholds at which the XTM device takes action. You can also change the options selected for default packet handling.

1. Click .

Or, select **Setup > Default Threat Protection > Default Packet Handling**.

*The Default Packet Handling dialog box appears.*



Activity	Threshold	Unit
Drop Spoofing Attacks		
Drop IP Source Route		
Block Port Space Probes	10	dest Ports/src IP (threshold)
Block Address Space Probes	10	dest IPs/src IP (threshold)
Drop IPsec Flood Attack	1500	packets/sec (threshold)
Drop IKE Flood Attack	1000	packets/sec (threshold)
Drop ICMP Flood Attack	1000	packets/sec (threshold)
Drop SYN Flood Attack	5000	packets/sec (threshold)
Drop UDP Flood Attack	1000	packets/sec (threshold)

**Unhandled Packets**

- Auto-block source of packets not handled
- Send an error message to clients whose connections are disabled

**Distributed Denial-of-Service Prevention**

- Per Server Quota: 100 connections/sec
- Per Client Quota: 100 connections/sec

2. Select the check boxes for the traffic patterns you want to take action against, as explained in these topics:
  - *About Spoofing Attacks* on page 527
  - *About IP Source Route Attacks* on page 528
  - *About Port Space and Address Space Probes* on page 529
  - *About Flood Attacks* on page 531
  - *About Unhandled Packets* on page 532
  - *About Distributed Denial-of-Service Attacks* on page 533

## Set Logging and Notification Options

The default device configuration tells the XTM device to send a log message when an event occurs that is specified in the **Default Packet Handling** dialog box.

To configure an SNMP trap or notification:

1. Click **Logging**.  
*The Logging and Notification dialog box appears.*
2. Configure notification settings as described in *Set Logging and Notification Preferences* on page 723.

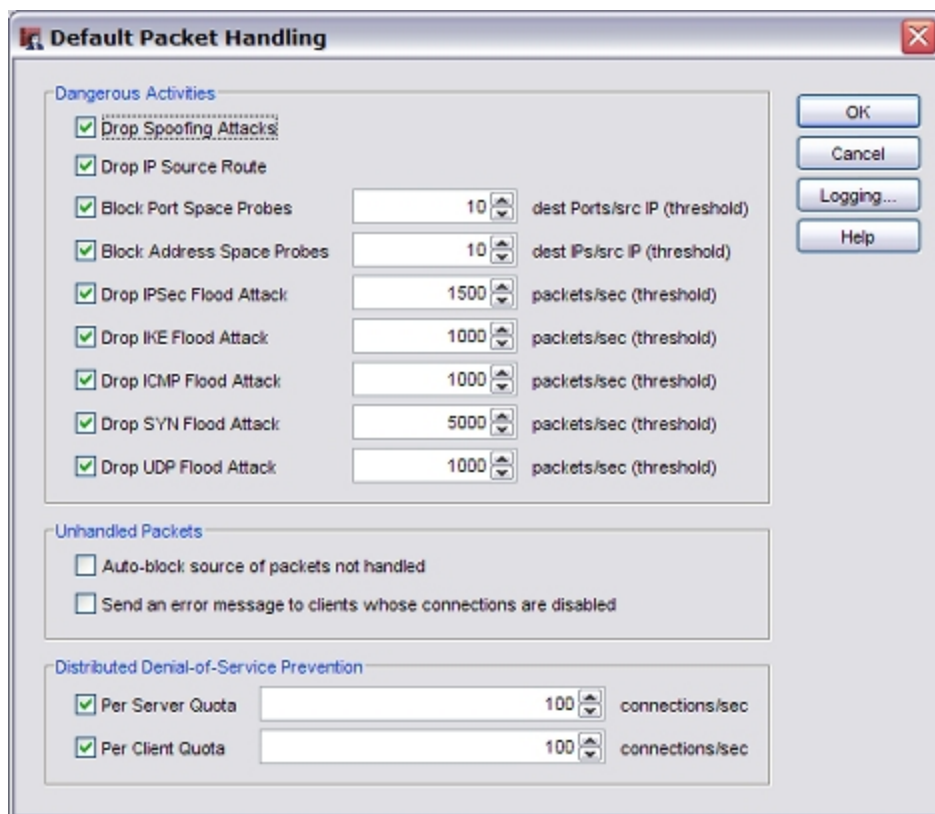
## About Spoofing Attacks

One method that attackers use to enter your network is to make an *electronic false identity*. This is an *IP spoofing* method that attackers use to send a TCP/IP packet with a different IP address than the computer that first sent it.

When anti-spoofing is enabled, the XTM device verifies the source IP address of a packet is from a network on the specified interface.

The default configuration of the XTM device is to drop spoofing attacks. From Policy Manager, you can change the settings for this feature:

1. Click .  
Or, select **Setup > Default Threat Protection > Default Packet Handling**.  
*The Default Packet Handling dialog box appears.*



2. Select or clear the **Drop Spoofing Attacks** check box.
3. Click **OK**.

## About IP Source Route Attacks

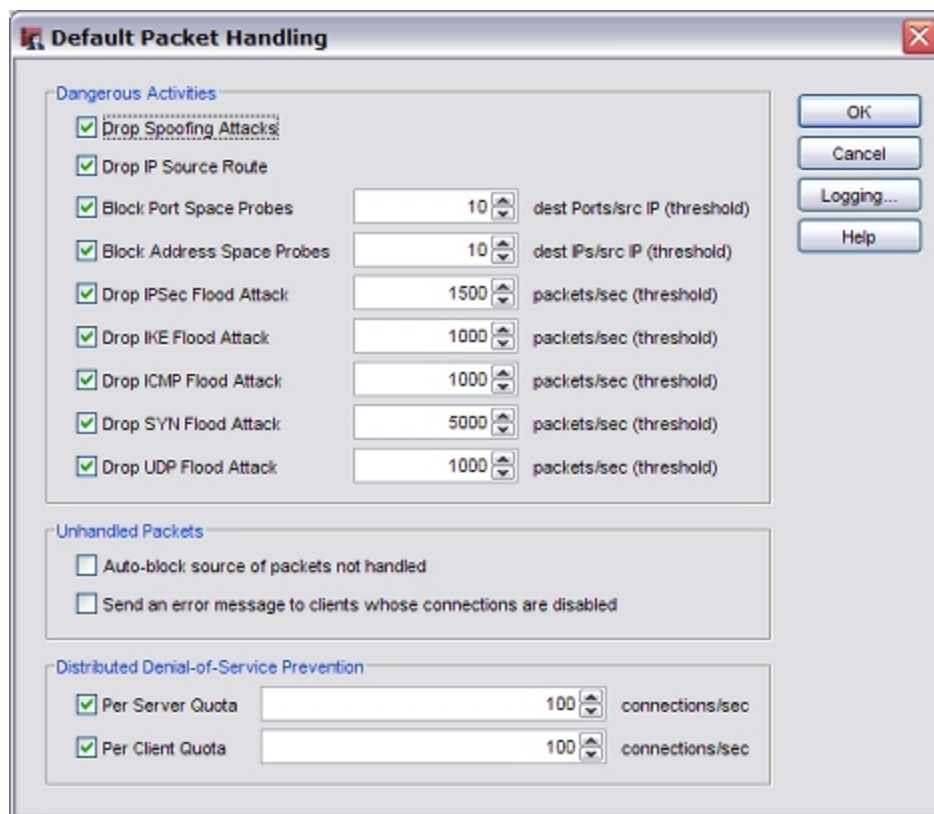
To find the route that packets take through your network, attackers use IP source route attacks. The attacker sends an IP packet and uses the response from your network to get information about the operating system of the target computer or network device.

The default configuration of the XTM device is to drop IP source route attacks. From Policy Manager, you can change the settings for this feature.

1. Click .
  - Or, select **Setup > Default Threat Protection > Default Packet Handling**.

*The Default Packet Handling dialog box appears.*





2. Select or clear the **Drop IP Source Route** check box.
3. Click **OK**.

## About Port Space and Address Space Probes

Attackers frequently look for open ports as starting points to launch network attacks. A *port space probe* is TCP or UDP traffic that is sent to a range of ports. These ports can be in sequence or random, from 0 to 65535. An *address space probe* is TCP or UDP traffic that is sent to a range of network addresses. Port space probes examine a computer to find the services that it uses. Address space probes examine a network to see which network devices are on that network.

For more information about ports, see *About Ports* on page 8.

## How the XTM Device Identifies Network Probes

An address space probe is identified when a computer sends a specified number of packets to different IP addresses assigned to an XTM device interface. To identify a port space probe, your XTM device counts the number of packets sent from one IP address to any XTM device interface IP address. The addresses can include the primary IP addresses and any secondary IP addresses configured on the interface. If the number of packets sent to different IP addresses or destination ports in one second is larger than the number you select, the source IP address is added to the Blocked Sites list.

When the **Block Port Space Probes** and **Block Address Space Probes** check boxes are selected, all incoming traffic on all interfaces is examined by the XTM device. You cannot disable these features for specified IP addresses, specified XTM device interfaces, or different time periods.

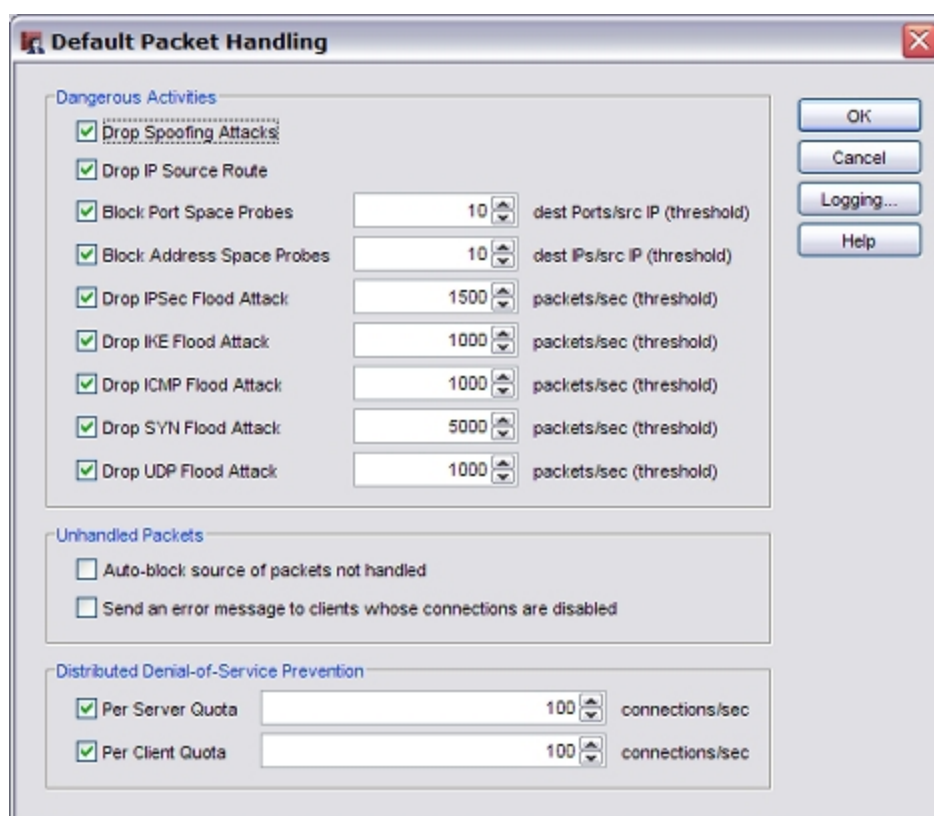
## To Protect Against Port Space and Address Space Probes

The default configuration of the XTM device blocks network probes. You can use Policy Manager to change the settings for this feature, and change the maximum allowed number of address or port probes per second for each source IP address (the default value is 50).

1. Click .

Or, select **Setup > Default Threat Protection > Default Packet Handling**.

The *Default Packet Handling* dialog box appears.



2. Select or clear the **Block Port Space Probes** and the **Block Address Space Probes** check boxes.
3. Click the arrows to select the maximum number of address or port probes to allow per second from the same IP address. The default for each is 10 per second. This means that a source is blocked if it initiates connections to 10 different ports or hosts within one second.
4. Click **OK**.

To block attackers more quickly, you can set the threshold for the maximum allowed number of address or port probes per second to a lower value. If the number is set too low, the XTM device could also deny legitimate network traffic. You are less likely to block legitimate network traffic if you use a higher number, but the XTM device must send TCP reset packets for each connection it drops. This uses bandwidth and resources on the XTM device and provides the attacker with information about your firewall.

## About Flood Attacks

In a flood attack, attackers send a very high volume of traffic to a system so it cannot examine and allow permitted network traffic. For example, an ICMP flood attack occurs when a system receives too many ICMP ping commands and must use all of its resources to send reply commands. The XTM device can protect against these types of flood attacks:

- IPSec
- IKE
- ICMP
- SYN
- UDP

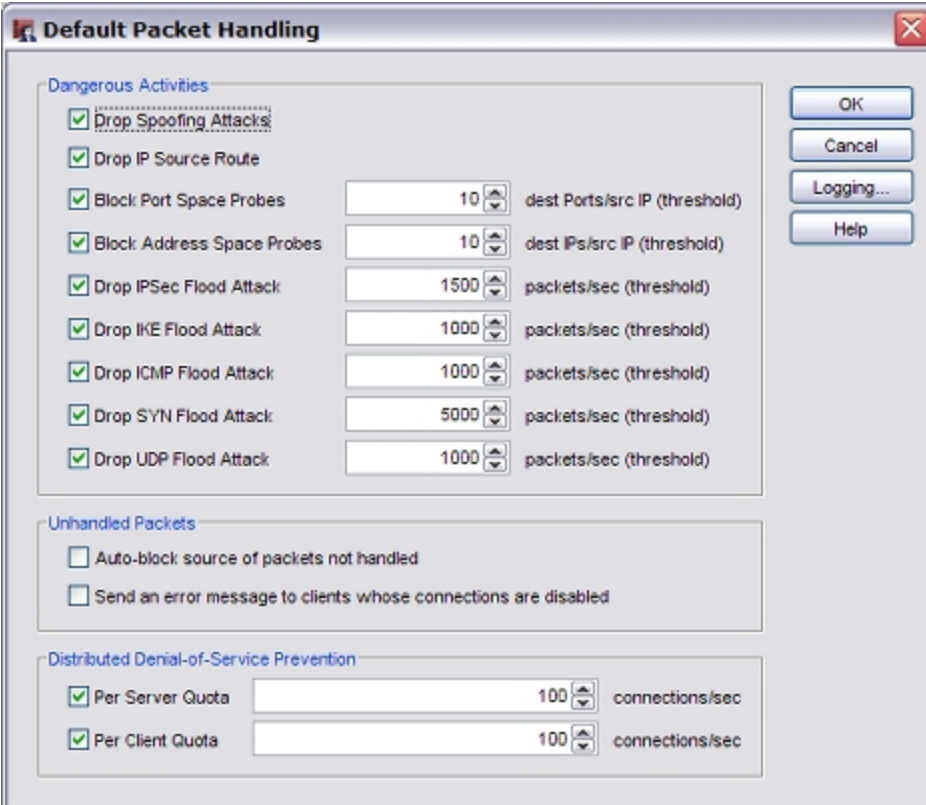
Flood attacks are also known as Denial of Service (DoS) attacks. The default configuration of the XTM device is to block flood attacks.

You can use Policy Manager to change the settings for this feature, or to change the maximum allowed number of packets per second.

1. Click .

Or, select **Setup > Default Threat Protection > Default Packet Handling**.

*The Default Packet Handling dialog box appears.*



Activity	Threshold	Unit
Drop Spoofing Attacks		
Drop IP Source Route		
Block Port Space Probes	10	dest Ports/src IP (threshold)
Block Address Space Probes	10	dest IPs/src IP (threshold)
Drop IPSec Flood Attack	1500	packets/sec (threshold)
Drop IKE Flood Attack	1000	packets/sec (threshold)
Drop ICMP Flood Attack	1000	packets/sec (threshold)
Drop SYN Flood Attack	5000	packets/sec (threshold)
Drop UDP Flood Attack	1000	packets/sec (threshold)

Setting	Value	Unit
Per Server Quota	100	connections/sec
Per Client Quota	100	connections/sec

2. Select or clear the **Flood Attack** check boxes.
3. Click the arrows to select the maximum allowed number of packets per second for each source IP address.  
For example, if the setting is 1000, the XTM device blocks a source if it receives more than 1000 packets per second from that source.
4. Click **OK**.


## About the SYN Flood Attack Setting

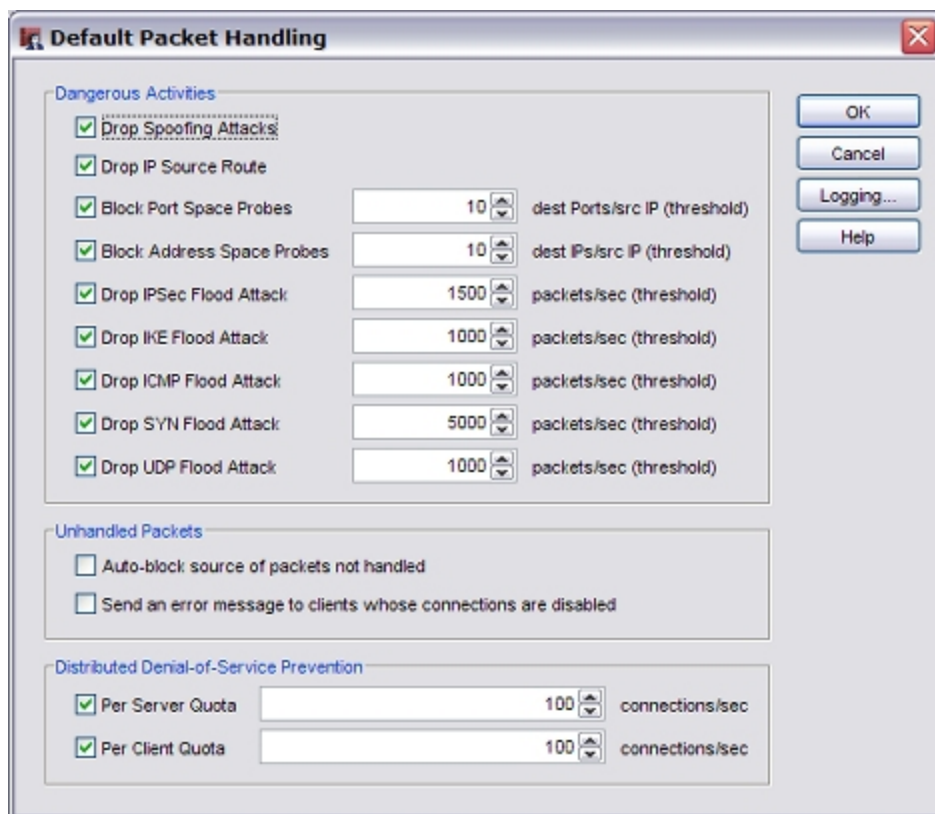
For SYN flood attacks, you can set the threshold at which the XTM device reports a possible SYN flood attack, but no packets are dropped if only the number of packets you selected are received. At twice the selected threshold, all SYN packets are dropped. At any level between the selected threshold and twice that level, if the `src_IP`, `dst_IP`, and `total_length` values of a packet are the same as the previous packet received, then it is always dropped. Otherwise, 25% of the new packets received are dropped.

For example, you set the SYN flood attack threshold to 18 packets/sec. When the XTM device receives 18 packets/sec, it reports a possible SYN flood attack to you, but does not drop any packets. If the device receives 20 packets per second, it drops 25% of the received packets (5 packets). If the device receives 36 or more packets, the last 18 or more are dropped.

## About Unhandled Packets

An *unhandled* packet is a packet that does not match any policy rule. By default, the XTM device always denies unhandled packets. From Policy Manager, you can change the device settings to further protect your network.

1. Click .  
Or, select **Setup > Default Threat Protection > Default Packet Handling**.  
*The Default Packet Handling dialog box appears.*



2. Select or clear the check boxes for these options:

*Auto-block source of packets not handled*

Select to automatically block the source of unhandled packets. The XTM device adds the IP address that sent the packet to the temporary Blocked Sites list.

*Send an error message to clients whose connections are disabled*

Select to send a TCP reset or ICMP error back to the client when the XTM device receives an unhandled packet.

## See Statistics on Unhandled Packets

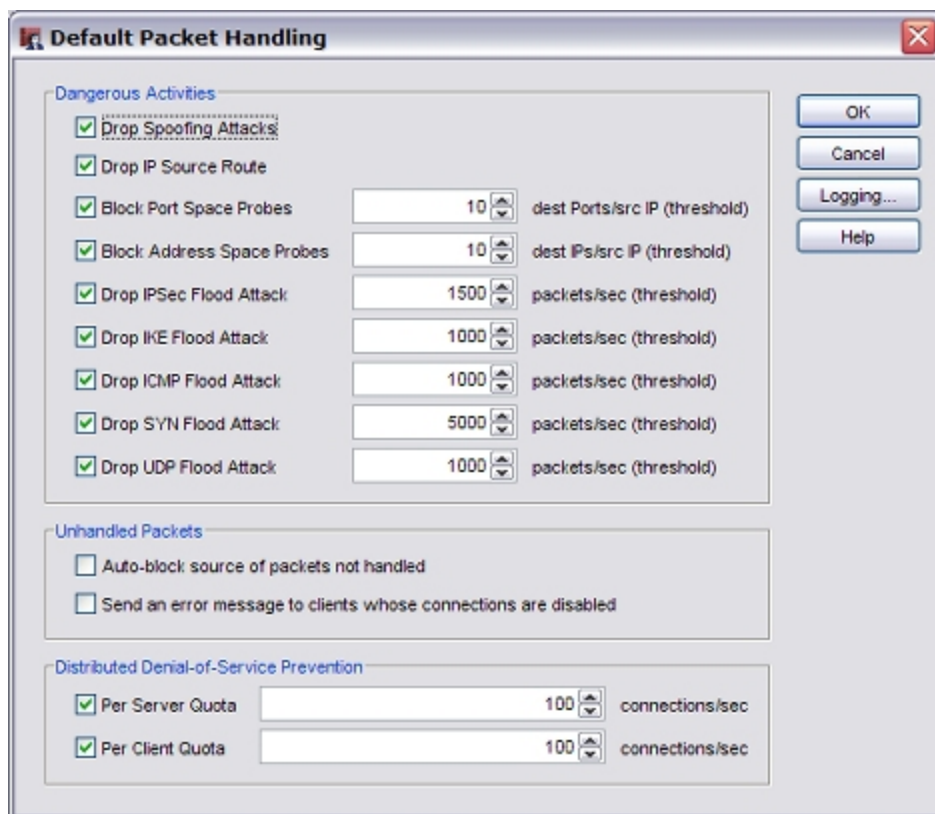
You can see statistics on unhandled packets received by the XTM device on the *Visual Display of Policy Usage (Service Watch)* in Firebox System Manager. From the **Show connections by** drop-down list, you can select to show connections by rule instead of policy.

## About Distributed Denial-of-Service Attacks

Distributed Denial of Service (DDoS) attacks are very similar to flood attacks. In a DDoS attack, many different clients and servers send connections to one computer system to try to flood the system. When a DDoS attack occurs, legitimate users cannot use the targeted system.

The default configuration of the XTM device is to block DDoS attacks. From Policy Manager, you can change the settings for this feature, and change the maximum allowed number of connections per second.

1. Click .  
Or, select **Setup > Default Threat Protection > Default Packet Handling**.  
The *Default Packet Handling* dialog box appears.



2. Select or clear the **Per Server Quota** and **Per Client Quota** check boxes.
3. Click the arrows to set the **Per Server Quota** and the **Per Client Quota**.

#### *Per Server Quota*

The Per Server Quota applies a limit to the number of connections per second from any external source to the XTM device external interface. This includes connections to internal servers allowed by a static NAT policy. For example, when the Per Server Quota is set to the default value of 100, the XTM device drops the 101st connection request received in a one second time frame from an external IP address. The IP address is not added to the blocked sites list.

#### *Per Client Quota*

The Per Client Quota applies a limit to the number of outbound connections per second from any source protected by the XTM device to any one destination. For example, when the Per Client Quota is set to the default value of 100, the XTM device drops the 101st connection request received in a one second time frame from an IP address on the trusted or optional network to any one destination IP address.

## About Blocked Sites

A blocked site is an IP address that cannot make a connection through the XTM device. You tell the XTM device to block specific sites you know, or think, are a security risk. After you find the source of suspicious traffic, you can block all connections from that IP address. You can also configure the XTM device to send a log message each time the source tries to connect to your network. From the log file, you can see the services that the sources use to launch attacks.

The XTM device denies all traffic from a blocked IP address. You can define two different types of blocked IP addresses: permanent and auto-blocked.

### Permanently Blocked Sites

Network traffic from permanently blocked sites is always denied. These IP addresses are stored in the Blocked Sites list and must be added manually. For example, you can add an IP address that constantly tries to scan your network to the Blocked Sites list to prevent port scans from that site.

To block a site, see *Block a Site Permanently* on page 536.

### Auto-Blocked Sites/Temporary Blocked Sites List

Packets from auto-blocked sites are denied for the amount of time you specify. The XTM device uses the packet handling rules specified for each policy to determine whether to block a site. For example, if you create a policy that denies all traffic on port 23 (Telnet), any IP address that tries to send Telnet traffic through that port is automatically blocked for the amount of time you specify.

To automatically block sites that send denied traffic, see *Block Sites Temporarily with Policy Settings* on page 538.

You can also automatically block sites that are the source of packets that do not match any policy rule. For more information, see *About Unhandled Packets* on page 532.

### Blocked Site Exceptions

If the XTM device blocks traffic from a site you believe to be safe, you can add the site to the Blocked Site Exceptions list, so that traffic from that site is not automatically blocked.

To add a blocked site exception, see *Create Blocked Site Exceptions*.

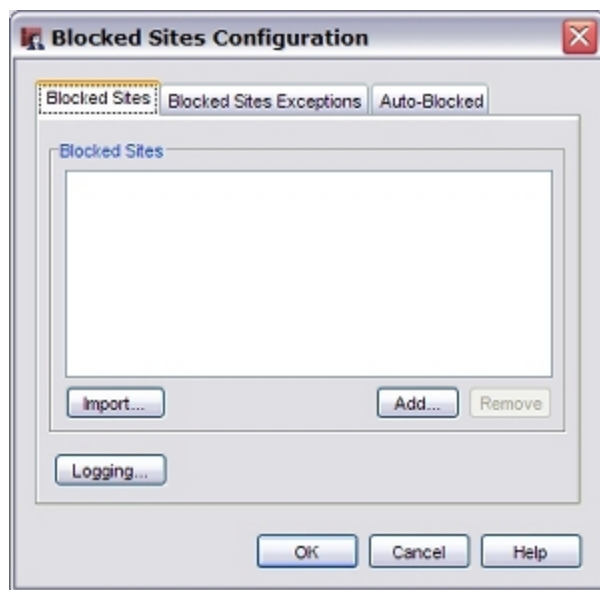
## Block a Site Permanently

You can use Policy Manager to permanently add sites to the Blocked Sites list.

1. Click .

Or, select **Setup > Default Threat Protection > Blocked Sites**.

*The Blocked Sites Configuration dialog box appears.*



2. Click **Add**.

*The Add Site dialog box appears.*



3. From the **Choose Type** drop-down list, select a method to identify the blocked site. Options are: **Host IP**, **Network IP**, **Host Range**, or **Host Name (DNS lookup)**.
4. Type the value.  
The value shows whether this is an IP address or a range of IP addresses. If you must block an address range that includes one or more IP addresses assigned to the XTM device, you must first add these IP addresses to the Blocked Sites Exceptions list.  
To add exceptions, see *Create Blocked Site Exceptions* on page 537.
5. (Optional) Type a comment to provide information about the site.
6. Select **OK**.  
*The new site appears in the Blocked Sites list.*



## Configure Logging for Blocked Sites

You can configure the XTM device to make a log entry or send a notification message if a computer tries to use a blocked site.

From the Blocked Sites Configuration dialog box:

1. Click **Logging**.  
*The Logging and Notification dialog box appears.*
2. Configure notification settings as described in *Set Logging and Notification Preferences* on page 723.

## Create Blocked Site Exceptions

When you add a site to the Blocked Site Exceptions list in Policy Manager, the traffic from that site is not blocked by the auto-blocking feature.

1. Select **Setup > Default Threat Protection > Blocked Sites**.
2. Select the **Blocked Sites Exceptions** tab.



3. Click **Add**.  
*The Add Site dialog box appears.*
4. From the **Choose Type** drop-down list, select a member type. Options are: **Host IP**, **Network IP**, **Host Range**, or **Host Name (DNS lookup)**.
5. Type the member value.  
*The member type shows whether this is an IP address or a range of IP addresses. When you type an IP address, type all the numbers and the period. Do not use the tab or arrow keys.*
6. Click **OK**.

## Import a List of Blocked Sites or Blocked Sites Exceptions

If you manage several XTM devices and want to use the same blocked sites or blocked sites exceptions for more than one device, you can create a list of the sites to block in a plain text (.txt) file and import the file into each device.

The IP addresses in the text file must be separated by spaces or line breaks. Use slash notation to specify networks. To indicate a range of addresses, separate the start and end addresses with a hyphen. An example text import file might look like this:

```
2.2.2.2 5.5.5.0/24
3.3.3.3-3.3.3.8
6.6.6.6 7.7.7.7
```

You can use Policy Manager to import the IP addresses to the Blocked Sites or Blocked Sites Exceptions list for the current XTM device.

1. Select **Setup > Default Threat Protection > Blocked Sites**.  
*The Blocked Sites Configuration dialog appears.*
2. To import blocked sites from a file, click the **Blocked Sites** tab.  
Or, to import blocked sites exceptions, click the **Blocked Site Exceptions** tab.
3. Click **Import**.  
*The Select a File dialog box appears.*
4. Browse to select the file. Click **Select a File**.  
*The sites in the file appear in the Blocked Sites or Blocked Sites Exceptions list.*
5. Click **OK**.

## Block Sites Temporarily with Policy Settings

You can use Policy Manager to temporarily block sites that try to use a denied service. IP addresses from the denied packets are added to the Temporary Blocked sites list for 20 minutes (by default).

1. Double-click the policy for the denied service.  
*The Edit Policy Properties dialog box appears.*
2. On the **Policy** tab, make sure you set the **Connections Are** drop-down list to **Denied** or **Denied (send reset)**.
3. On the **Properties** tab, select the **Auto-block sites that attempt to connect** check box. By default, IP addresses from the denied packets are added to the Temporary Blocked Sites list for 20 minutes.

If you enable logging of temporary blocked sites, the log messages can help you make decisions about which IP addresses to block permanently. To enable logging of denied packets:

1. In the policy definition, select the **Properties** tab
2. Click **Logging**.
3. Select the **Send log message** check box.  
For more information about logging, see *Set Logging and Notification Preferences* on page 723.

## Change the Duration that Sites are Auto-Blocked

You can use Policy Manager to enable the auto-block feature.

Select **Setup > Default Threat Protection > Default Packet Handling**.

For more information, see *About Unhandled Packets* on page 532.

You can also use policy settings to auto-block sites that try to use a denied service. For more information, see *Block Sites Temporarily with Policy Settings* on page 538.

You can use Policy Manager to set the duration that sites are blocked automatically.

1. Select **Setup > Default Threat Protection > Blocked Sites**.
2. Select the **Auto-Blocked** tab.



3. To change the amount of time a site is auto-blocked, in the **Duration for Auto-Blocked sites** text box, type or select the number of minutes to block a site. The default is 20 minutes.
4. Click **OK**.

## About Blocked Ports

You can block the ports that you know can be used to attack your network. This stops specified external network services. Blocking ports can protect your most sensitive services.

When you block a port, you override all of the rules in your policy definitions. To block a port, see *Block a Port* on page 541.

## Default Blocked Ports

In the default configuration, the XTM device blocks some destination ports. You usually do not need to change this default configuration. TCP and UDP packets are blocked for these ports:

### *X Window System (ports 6000-6005)*

The X Window System (or X-Windows) client connection is not encrypted and is dangerous to use on the Internet.

### *X Font Server (port 7100)*

Many versions of X Windows operate X Font Servers. The X Font Servers operate as the super-user on some hosts.

### *NFS (port 2049)*

NFS (Network File System) is a frequently used TCP/IP service where many users use the same files on a network. New versions have important authentication and security problems. To supply NFS on the Internet can be very dangerous.

**Note** *The portmapper frequently uses port 2049 for NFS. If you use NFS, make sure that NFS uses port 2049 on all your systems.*

### *rlogin, rsh, rcp (ports 513, 514)*

These services give remote access to other computers. They are a security risk and many attackers probe for these services.

### *RPC portmapper (port 111)*

The RPC Services use port 111 to find which ports a given RPC server uses. The RPC services are easy to attack through the Internet.

### *port 8000*

Many vendors use this port, and many security problems are related to it.

### *port 1*

The TCPmux service uses Port 1, but not frequently. You can block it to make it more difficult for tools that examine ports.

### *port 0*

This port is always blocked by the XTM device. You cannot allow traffic on port 0 through the device.


**Note** *If you must allow traffic through any of the default blocked ports to use the associated software applications, we recommend that you allow the traffic only through a VPN tunnel or use SSH (Secure Shell) with those ports.*

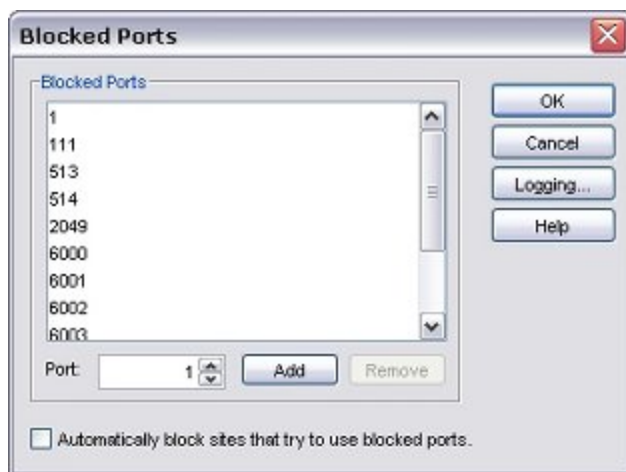
## Block a Port

You can use Policy Manager to add a port number to the Blocked Ports list.

**Note** *Be very careful if you block port numbers higher than 1023. Clients frequently use these source port numbers.*

To add a port number to the Blocked Ports list:

1. Click .  
Or, select **Setup > Default Threat Protection > Blocked Ports**.  
*The Blocked Ports dialog box appears.*
2. In the **Port** text box, type or select the port number to block.
3. Click **Add**.  
*The new port number appears in the Blocked Ports list.*



## Block IP Addresses That Try to Use Blocked Ports

You can configure the XTM device to automatically block an external computer that tries to use a blocked port. In the **Blocked Ports** dialog box, select the **Automatically block sites that try to use blocked ports** check box.

## Set Logging and Notification for Blocked Ports

You can configure the XTM device to make a log entry when a computer tries to use a blocked port. You can also set up notification for when a computer tries to get access to a blocked port.

From the **Blocked Ports** dialog box:

1. Click **Logging**.  
*The Logging and Notification dialog box appears.*
2. Configure notification settings as described in *Set Logging and Notification Preferences* on page 723.



# 17 WatchGuard Server Setup

---

## About WatchGuard Servers

When you install the WatchGuard System Manager software, you can choose to install one or more of the WatchGuard servers. You can also run the installation program and select to install only one or more of the servers, without WatchGuard System Manager. When you install a server, the WatchGuard Server Center program is automatically installed. WatchGuard Server Center is a single application you can use to set up and configure all your WatchGuard System Manager servers. You can also use WatchGuard Server Center to backup and restore your Management Server.

The five WatchGuard servers are:

- Management Server
- Log Server
- Report Server
- Quarantine Server
- WebBlocker Server

To set up WatchGuard servers, see *Set Up WatchGuard Servers* on page 545.

For WatchGuard System Manager installation instructions, see *Install WatchGuard System Manager Software* on page 20.

For information about how to backup and restore your Management Server, see *Back Up or Restore the Management Server Configuration* on page 576.

Each server has a specific function:

#### *Management Server*

The Management Server operates on a Windows computer. With this server, you can manage all firewall devices and create virtual private network (VPN) tunnels with a simple drag-and-drop function. The basic functions of the Management Server are:

- Certificate authority to distribute certificates for Internet Protocol Security (IPSec) tunnels
- VPN tunnel configuration management
- Management for multiple XTM devices

For more information about the Management Server, see *About the WatchGuard Management Server* on page 557.

#### *Log Server*

The Log Server collects log messages from each XTM device and stores them in a PostgreSQL database. The log messages are encrypted when they are sent to the Log Server. The log message format is XML (plain text). The types of log message that the Log Server collects include traffic log messages, event log messages, alarms, and diagnostic messages.

For more information about Log Servers, see *Set Up a Log Server* on page 691.

#### *Report Server*

The Report Server periodically consolidates data collected by your Log Servers from your XTM devices, and stores them in a PostgreSQL database. The Report Server then generates the reports you specify. When the data is on the Report Server, you can review it with Report Manager or Reporting Web UI.

For more information about reports and the Report Server, see *About the Report Server* on page 805.

For more information about Report Manager, see *About WatchGuard Report Manager* on page 830.

For more information about how to configure Reporting Web UI, see *Configure Reporting Web UI Settings* on page 823.

For more information about how to use Reporting Web UI, see the *Reporting Web UI Help*.

#### *Quarantine Server*

The Quarantine Server collects and isolates email messages that spamBlocker identifies as possible spam.

For more information on the Quarantine Server, see *About the Quarantine Server* on page 1225.

#### *WebBlocker Server*

The WebBlocker Server operates with the HTTP proxy to deny user access to specified categories of web sites. When you configure an XTM device, you set the web site categories you want to allow or block.

For more information about WebBlocker and the WebBlocker Server, see *About WebBlocker* on page 1065.



# Set Up WatchGuard Servers

WatchGuard Server Center is a single application you can use to set up and configure all your WatchGuard servers.

After you have installed WatchGuard System Manager (WSM) and the WatchGuard servers, the WatchGuard Server Center Setup Wizard creates the WatchGuard servers you installed on your computer. The wizard includes only the screens that correspond to the components you have installed. For example, if you installed the Log Server and the Report Server, but not the Quarantine Server, the wizard includes only the pages related to the Log Server and Report Server settings. The pages used to create a domain list for the Quarantine Server do not appear in the wizard.

If you did not install or configure some of the WatchGuard servers, you can install or configure them later. You can launch the WatchGuard System Manager Installer from the main configuration page of each server that is not installed. You can also launch the WatchGuard Server Center Setup Wizard from the main configuration page of each server that is not configured.


For more information, see *Install or Configure WatchGuard Servers from WatchGuard Server Center* on page 553.

## Before You Begin

Before you run the wizard, make sure you have all of the necessary information:

- If you want to use a gateway Firebox to protect the Management Server, the IP address of the external interface for that XTM device.
- The Management Server license key.  
To find the license key, see *Find Your Management Server License Key* on page 548.
- If you want to set up Quarantine Server, the domain name or names for which Quarantine Server will accept email messages.
- If you want to set up Log Server, the IP address of the device you will use as a Log Server.

## Start the Wizard

1. In the system tray, right-click  and select **Open WatchGuard Server Center**.  
If you do not see this icon, you did not install any WatchGuard server software.  
To rerun the installation process and install one or more servers, see *Install WatchGuard System Manager Software* on page 20.  
*The WatchGuard Server Center Setup Wizard starts.*
2. Review the Welcome page to make sure you have all the information required to complete the wizard.
3. Click **Next**.  
*The General Settings - Identify your organization name page appears.*

## General Settings

1. In the **Organization name** text box, type the name to use for your organization.  
  
This name is used for the certificate authority on the Management Server, as described in *Configure the Certificate Authority on the Management Server* on page 560.

2. Click **Next**.  
*The General Settings - Set Administrator passphrase page appears.*
3. Type and confirm the **Administrator passphrase**.  
This passphrase must be at least 8 characters.  
The Administrator passphrase is used to control access to the management computer (the computer on which WSM is installed).
4. Click **Next**.

## Management Server Settings

These settings appear in the wizard only if you installed the Management Server.

1. If you have a gateway Firebox for the Management Server, click **Yes**.  
Although a gateway Firebox is optional, we recommend that you use a gateway Firebox to protect the Management Server from the Internet.  
For more information, see *About the Gateway Firebox* on page 548.
2. Type the external IP address and passphrases for the gateway Firebox.
3. Click **Next**.  
*The Management Server - Enter a license key page appears.*
4. Type the license key for Management Server and click **Add**.  
For information about how to find the license key, see *Find Your Management Server License Key* on page 548.
5. Click **Next**.

**Note** *When an interface whose IP address is bound to the Management Server goes down and then restarts, we recommend that you restart the Management Server.*

## Log Server and Report Server Settings

These settings appear in the wizard only if you installed the Log Server.

1. Type and confirm the **Encryption key** to use for the secure connection between the XTM device and the Log Servers.  
  
The allowed range for the encryption key is 8–32 characters. You can use all characters but spaces and slashes (/ or \).
2. In the **Database location** text box, type the path to the folder where you want to keep all log files, report files, and report definition files.  
Or, click **Browse** and select a folder. Make sure you select a location that has plenty of free disk space.  
  
We recommend that you select the built-in directory location for Log Server and Report Server files, C:\Documents and Settings\WatchGuard\logs, which is automatically added to your management computer when you install the Log Server.

**Note** *Select the location carefully. After you have installed the database you cannot change the directory location through the Log Server user interface. If you must change the location, follow the steps in the topic, [Move the Log Data Directory](#) on page 704.*

3. Click **Next**.

## Quarantine Server Settings

These settings appear in the wizard only if you installed the Quarantine Server.

The domain list is the set of domain names for which the Quarantine Server accepts email messages. The Quarantine Server only sends messages for the users in the domains that are included in the domain list. Messages sent to users that are not in one of these domains are deleted.

1. To add a domain, type the domain name in the top text box and click **Add**.  
*The domain name appears in the window.*  
  
To remove a domain, select the domain name from the list and click **Remove**.  
*The domain name is removed from the window.*
2. Click **Next**.

## WebBlocker Server Settings

These settings appear in the wizard only if you installed the WebBlocker Server.

You can choose to download the WebBlocker database now, or wait and download it later. The WebBlocker database has more than 220 MB of data. Your connection speed controls the download speed, which can be more than 30 minutes. Make sure the hard disk drive has a minimum of 250 MB of free space.

1. To download the database now, select **Yes** and click **Download**.  
  
To download the database later, select **No**.
2. Click **Next**.

## Review and Finish

On the **Review Settings** page, review your settings to make sure they are correct.

To make changes to your settings:

1. Click **Back** until you reach the page to change.
2. Make any necessary changes.
3. Click **Next** until you return to the **Review Settings** page.

If your settings are correct:

1. Click **Next**.  
*The server configuration progress indicator appears.*
2. When the configuration is complete, click **Next**.  
*The WatchGuard Server Center Setup Wizard is complete page appears.*
3. Click **Finish**.  
*WatchGuard Server Center appears.*

From WatchGuard Server Center, you can:

- *Monitor the Status of WatchGuard Servers*
- [Configure the WatchGuard Management Server](#)
- *Set Up a Log Server*

- *Set Up the Report Server*
- *Configure the Quarantine Server*
- *Set Up the WebBlocker Server*
- *Change the Administrator Passphrase*

## About the Gateway Firebox

The gateway Firebox helps protect your Management Server from the Internet. When you set up your Management Server, you choose whether to use a gateway Firebox. We recommend that you use a gateway Firebox.

When you add an IP address for your gateway Firebox, the wizard does three things:

- Uses this IP address to configure the gateway Firebox to allow connections to the Management Server.

The Management Server policy is automatically added to the configuration file. This policy opens TCP ports 4110, 4112, and 4113 to allow connections to the Management Server.

If you do not type an IP address here, you must configure a firewall between the Management Server and the Internet to allow connections to the Management Server on TCP ports 4110, 4112, and 4113.

- If you have an earlier version of WatchGuard System Manager, and have a Firebox or XTM device configured as a DVCP server, the wizard gets the DVCP server information from the gateway Firebox and moves these settings to your Management Server.
- The wizard sets the IP address for the Certificate Revocation List (CRL).

After the Management Server is set up, the devices you add as managed clients use this IP address to connect to the Management Server. This IP address must be the public IP address your Management Server shows to the Internet.

If you do not specify an IP address, the wizard uses the current IP address on your Management Server computer for the CRL IP address. If this is not the IP address your computer shows to the Internet because it is behind a device that does NAT (Network Address Translation), you must edit the CRL and to use the public IP address of your Management Server. If you use a gateway Firebox that does NAT, make sure that it is the same version as your Management Server. For example, if your Management Server is v11.0, your gateway Firebox with NAT must be v11.0 or higher.

For more information, see *Update the Management Server with a New Gateway Address* on page 569.

## Find Your Management Server License Key

For most XTM 2 Series, 5 Series, 8 Series, or 1050 devices, WatchGuard System Manager includes a license key that allows you to manage up to four devices. If you have a VPN Manager license key from a previous Firebox or XTM device purchase, you can use the VPN Manager license key for the WatchGuard Management Server. If you do not have either a WatchGuard System Manager license key that includes the ability to manage more than one XTM device, or a VPN Manager license key, you must purchase a license key from a WatchGuard reseller to use the WatchGuard Management Server.

To find your WatchGuard System Manager or VPN Manager license key:

1. Open a browser and go to the *Manage Products* area of the LiveSecurity web site:  
<https://www.watchguard.com/archive/manageproducts.asp>

- If you are not already logged in, you must log in with your LiveSecurity credentials.
2. Scroll to the bottom of the page.
  3. Adjacent to **WatchGuard System Manager** or **VPN Manager**, click **View Details**.  
A list of available license keys appears. If more than one license key appears in the list, you can use any of them.  
The license key has one of these formats:
    - WSMGR-X-000392-yyyyyyyy
    - VPNMGR-X-024535-yyyyyyyy
- The X character shows how many devices you can manage with each key. The “y” characters are a string of alphanumeric characters.
4. Use one of these keys when you run the WatchGuard Server Center Setup Wizard to set up your Management Server.

## Monitor the Status of WatchGuard Servers

You can see either brief or full information about your WatchGuard servers.

### See Which Servers are Running

To only see whether one or more servers are currently running:


1. Right-click  in the system tray.
2. Select **Server Status**.

*The WatchGuard Server Center Status dialog box appears with a list of the servers installed and whether each server is currently running.*

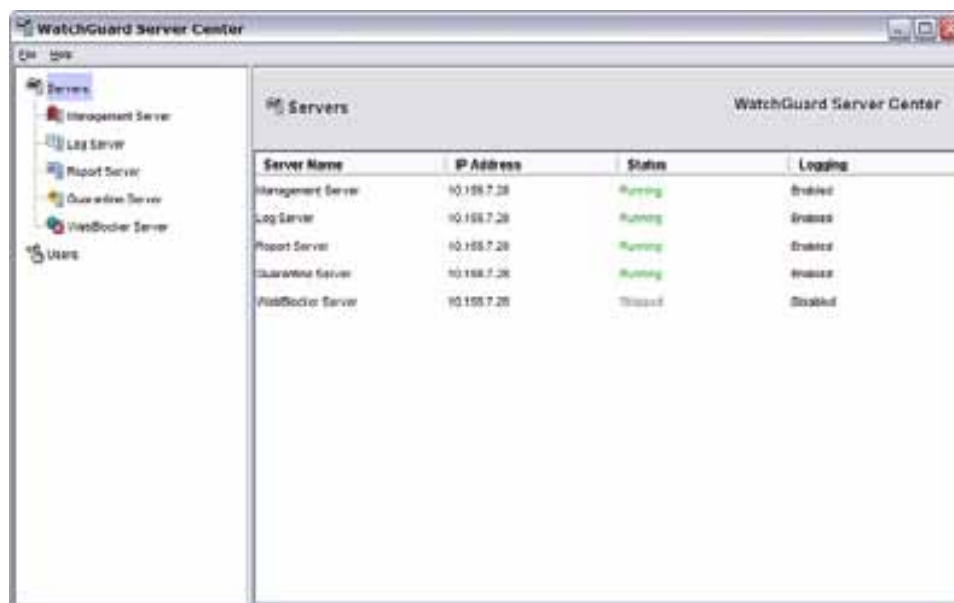


## See Complete Information for Servers

From the Management Server computer:

1. Right-click  in the system tray.
2. Select **Open WatchGuard Server Center**.

*WatchGuard Server Center appears.*



For each server, the **Servers** page shows:

- The server IP address
- Whether it is online or offline
- Whether logging is enabled or disabled

## Configure Your WatchGuard Servers

After you run the WatchGuard Server Center Setup Wizard to set up your servers, you can configure each server in more detail.

For more information, see:


- *About the WatchGuard Management Server* on page 557
- *Set Up a Log Server* on page 691
- *Set Up the Report Server* on page 806
- *Configure the Quarantine Server* on page 1228
- *Set Up the WebBlocker Server* on page 1066

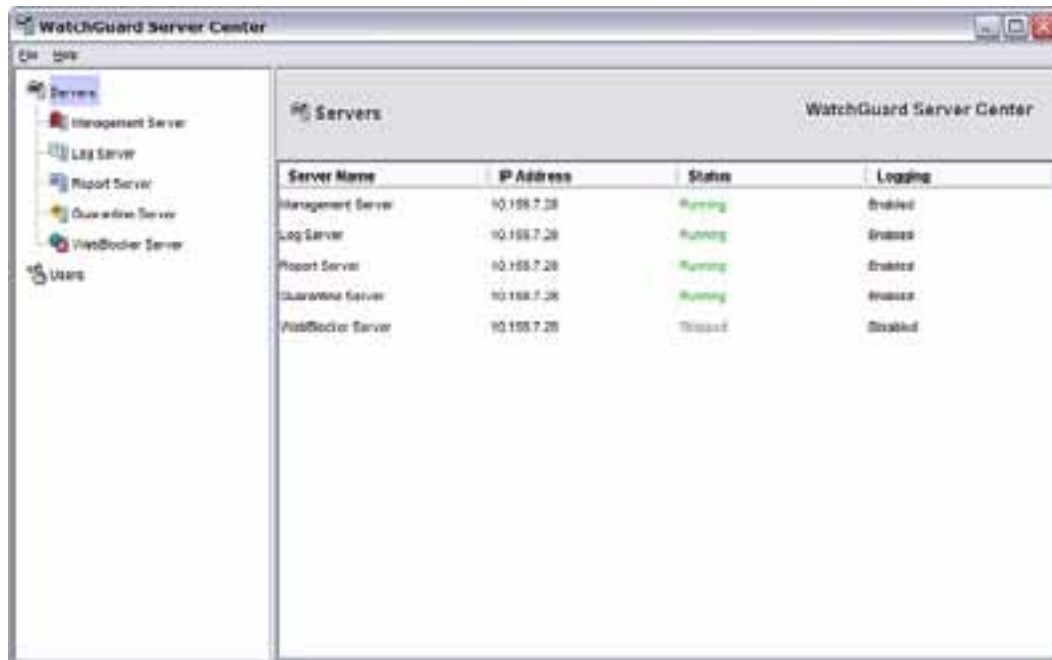
You can also set up role-based administration. For more information, see *About Role-Based Administration* on page 665.

# Open WatchGuard Server Center

You can use WatchGuard Server Center to manage all your WatchGuard servers.

To open WatchGuard Server Center:

1. Right-click  in the system tray and select **Open WatchGuard Server Center**.  
*The Connect to WatchGuard Server Center dialog box appears.*
2. Type your **Username** and **Administrator passphrase**.
3. Click **Login**.  
*WatchGuard Server Center appears.*



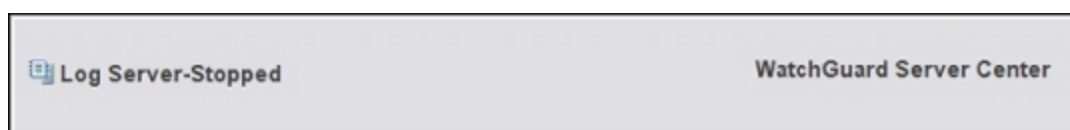
4. From the **Servers** tree, select the server you want to configure.
  - [Management Server](#)
  - [Log Server](#)
  - [Report Server](#)
  - [Quarantine Server](#)
  - [WebBlocker Server](#)

## Stop and Start Your WatchGuard Servers

You can manually stop or start WatchGuard servers at any time. You do not have to disconnect from the servers.

To stop the service, from WatchGuard Server Center:

1. In the **Servers** tree, select the server you want to stop.  
For example, **Log Server**.
2. Right-click the server and select **Stop Server**.  
*A warning message appears.*
3. Click **Yes** to confirm you want to stop the service for the selected server.  
*The service stops and the Stopped message appears at the top of the server page.*  
*For example, if you stopped Log Server, Log Server-Stopped appears.*



To start the service, from WatchGuard Server Center:

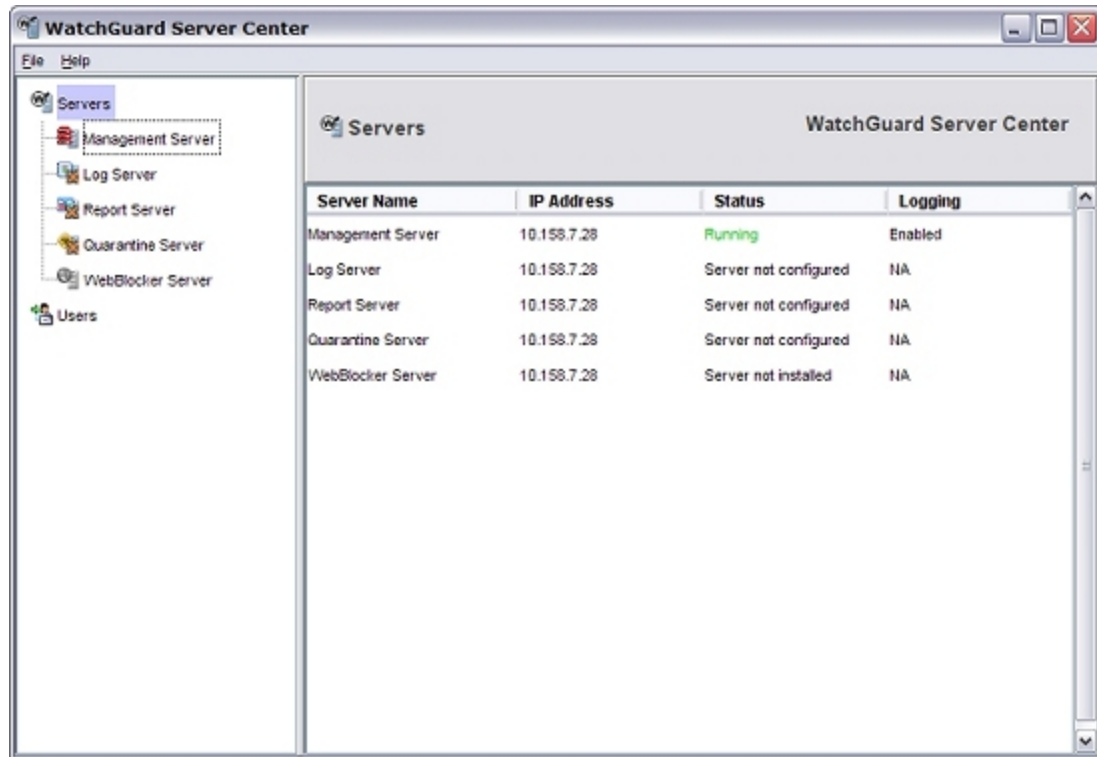
1. In the **Servers** tree, select the server you want to start.  
For example, **Log Server**.
2. Right-click the server and select **Start Server**.  
*The service starts and the server name appears at the top of the server page.*  
*For example, if you started Log Server, Log Server appears.*



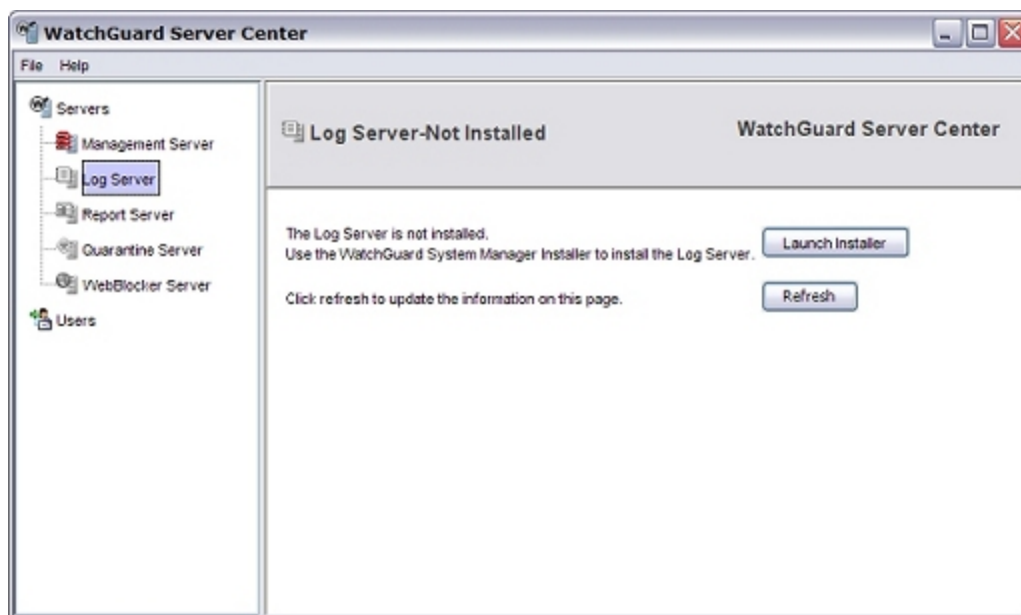
# Install or Configure WatchGuard Servers from WatchGuard Server Center

If you have already installed and configured one or more WatchGuard servers, you can use WatchGuard Server Center (WSC) to install or configure any of the WatchGuard servers you have not already installed or configured.

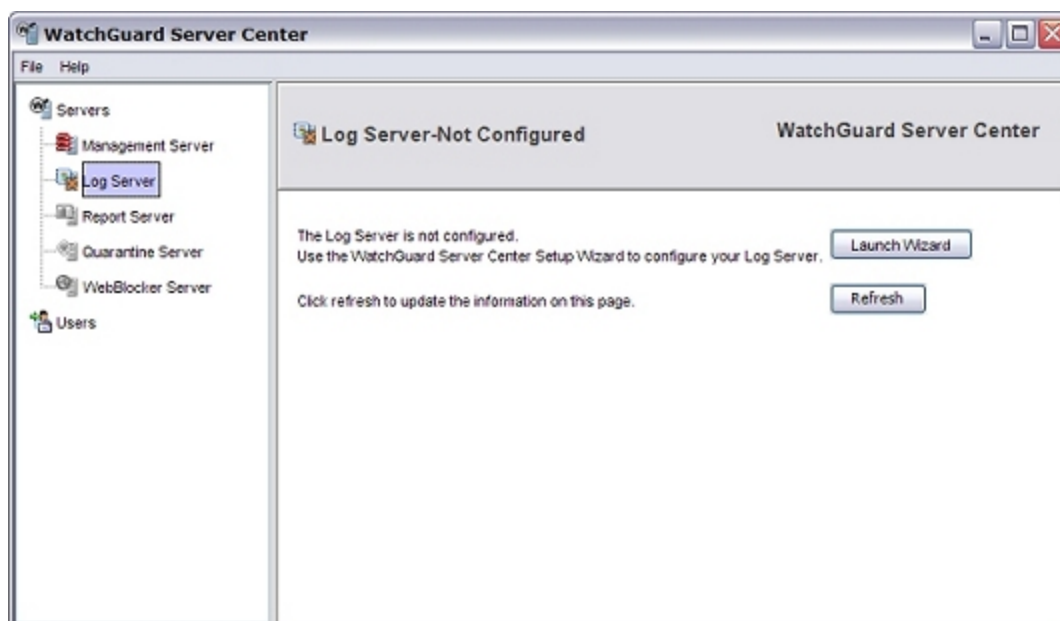
1. *Open WatchGuard Server Center.*  
*The main Servers page appears.*



2. In the **Servers** tree, select the server you want to install or configure.  
*The selected server page appears. In the examples below, you see the Log Server main page.*



*Log Server not installed*



*Log Server not configured*

3. To install the server, click **Launch Installer**.  
*The WatchGuard System Manager Installer appears.*  
  
To configure the server, click **Launch Wizard**.  
*The WatchGuard Server Center Setup Wizard appears.*
4. If you selected to install the server, follow the instructions in *Install WatchGuard System Manager Software* on page 20 to complete the installation wizard.

If you selected to configure the server, follow the instructions in *Set Up WatchGuard Servers* on page 545 for the server you selected.

5. Click **Refresh** to update the server page.
6. If you installed the server, repeat Steps 3–5 to configure the server.



If you configured the server, you can now use WSC to *Set Up WatchGuard Servers*.

## Exit or Open WatchGuard Server Center


After you install any WatchGuard server, the WatchGuard Server Center icon automatically appears in the system tray. This enables you to easily access WatchGuard Server Center. When you close WatchGuard Server Center, the application continues to run in the background and the icon remains in your system tray.

You can choose to exit the application so it no longer runs in the background and then open it again later. When you exit the application, the WatchGuard Server Center icon is removed from your system tray.

To exit WatchGuard Server Center and remove the icon from the system tray:

1. In the system tray, right-click .
2. Select **Exit**.  
*A message appears to confirm you want to exit.*
3. Click **Yes**.  
 *disappears from the system tray.*

To restore the WatchGuard Server Center the icon to the system tray and open WatchGuard Server Center:

1. Select **Start > All Programs > WatchGuard System Manager 11.x > WatchGuard Server Center**.  
 *appears in the system tray.*
2. *Open WatchGuard Server Center.*



# 18 Management Server Setup and Administration

---

## About the WatchGuard Management Server

The WatchGuard Management Server enables you to centrally manage multiple Firebox or XTM devices and VPN tunnels of a distributed enterprise from one easy-to-use management interface. You can manage different types of Firebox or XTM devices: WatchGuard XTM, Firebox X Core, Firebox X Peak, Firebox X Edge, Firebox III, and SOHO 6.

The computer that is configured as the Management Server also operates as a Certificate Authority (CA). The CA gives certificates to managed Firebox or XTM devices when they contact the Management Server to receive configuration updates.

## Install the Management Server

You can install the Management Server software on any computer that uses the Windows operating system. You do not have to install it on the computer that is your management computer (the computer on which you install the WatchGuard System Manager software). We recommend that you install the Management Server software on a computer with a static IP address that is behind an XTM device with a static external IP address. Otherwise, the Management Server may not operate correctly.

When you run the WatchGuard System Manager Setup program to *Install WatchGuard System Manager Software*, you choose which client and server components you want to install. In the **Server Components** list, make sure you select **Management Server**.

If you have already installed WatchGuard System Manager (WSM) and did not install the Management Server, you can still install the Management Server.

1. *Install WatchGuard System Manager Software.*
2. Select only the **WatchGuard Management Server** check box. Do not select the check box for any components you do not want to install.
3. Complete the Setup wizard.

## Set up and Configure the Management Server


For instructions to set up the Management Server, and other WatchGuard System Manager servers, see *Set Up WatchGuard Servers* on page 545.

For instructions to configure the Management Server after set up is completed, see *Configure Settings for the Management Server* on page 558.

## Configure Settings for the Management Server

You can use the WatchGuard Server Center to configure the settings for your Management Server. You can update the Management Server license key, and configure settings for notification, logging, Active Directory, and the configuration history.

On the computer that has the Management Server software installed:

1. Right-click  in the system tray and select **Open WatchGuard Server Center**.  
*The Connect to WatchGuard Server Center dialog box appears.*
2. Type your **Username** and **Administrator passphrase**. Click **Login**.  
*WatchGuard Server Center appears.*
3. In the **Servers** tree, select **Management Server**.  
*The Management Server page appears.*

**Management Server** **WatchGuard Server Center**

[Certificates](#) | [Server Settings](#) | [Active Directory](#) | [Logging](#) | [Configuration History](#)

**Certificate Authority**

Configure the properties for your CA certificate.

Common Name:

Organization:

Certificate Lifetime:  Days

Key Bits:

**Client**

Configure the properties for your client certificate.

Certificate Lifetime:  Days

Key Bits:

**Certificate Revocation List**

Configure the properties for the Certificate Revocation List (CRL).

Distribution IP Address:

Publication Interval:  Hours

Send CA service log messages to Windows Event Viewer

4. Configure the default settings as appropriate for your network.
  - To change certificate authority, client, and revocation list settings, select the [Certificates tab](#).
  - To add or remove a license key, specify device monitoring settings, or change the notification settings, select the [Server Settings tab](#).
  - To enable and configure Active Directory settings, select the [Active Directory tab](#).
  - To configure the settings for logging, select the [Logging tab](#).
  - To specify the number of configuration files to save for each managed device or configuration template, select the [Configuration History tab](#).
5. Click **Apply** to save your changes.

## Configure the Certificate Authority on the Management Server

You can configure the certificate authority (CA) on the Management Server. However, administrators do not usually change the properties of the CA certificate.

From WatchGuard Server Center on your management computer:

1. In the **Servers** tree, select **Management Server**.  
*The Management Server pages appear.*
2. Select the **Certificates** tab.

The screenshot shows the 'Management Server' configuration page in the 'WatchGuard Server Center'. The 'Certificates' tab is selected, and the 'Certificate Authority' section is expanded. The 'Certificate Authority' section contains the following fields: 'Common Name' (WatchGuard Certificate Authority), 'Organization' (WatchGuard), 'Certificate Lifetime' (1000 Days), and 'Key Bits' (2048). The 'Client' section contains 'Certificate Lifetime' (365 Days) and 'Key Bits' (1024). The 'Certificate Revocation List' section contains 'Distribution IP Address' (192.168.131.65) with 'Add' and 'Remove' buttons, and 'Publication Interval' (720 Hours). There is a checkbox for 'Send CA service log messages to Windows Event Viewer' which is unchecked. At the bottom right, there are 'Reset', 'Apply', and 'Help' buttons.

3. Configure the certificates settings as described in the subsequent sections.
4. Click **Apply** to save your changes.



## Set Properties for the Certificate Authority

In the **Certificate Authority** section:

1. In the **Common Name** text box, type the name you want to appear in the CA certificate.
2. In the **Organization** text box, type an organization name for the CA certificate.
3. In the **Certificate Lifetime** text box, type the number of days after which the CA certificate will expire.  
A longer certificate lifetime could give an attacker more time to attack it.
4. From the **Key Bits** drop-down list, select the strength to apply to the certificate. The higher the number of the **Key Bits** setting, the stronger the cryptography that protects the key.

## Set Properties for Client Certificates

In the **Client** section:

1. In the **Certificate Lifetime** text box, type the number of days after which the client certificate expires.  
A longer certificate lifetime could give an attacker more time to attack it.
2. From the **Key Bits** drop-down list, select the strength to apply to the certificate.  
The higher the number of the **Key Bits** setting, the stronger the cryptography that protects the key.

## Set Properties for the Certification Revocation List (CRL)

In the **Certificate Revocation List** section:

1. From the **Distribution IP Address** window, select an IP address from the list, or click **Add** to add a new address.

You can also select an IP address and click **Remove** to delete it from the list.

By default, the distribution IP address is the address of the gateway Firebox. This is also the IP address the remote managed XTM devices use to connect to the Management Server. If the external IP address of your device changes, you must change this value.

2. Type the **Publication Interval** for the CRL in hours.

This is the period after which the CRL is automatically published.

The default setting is zero (0), which means that the CRL is published every 720 hours (30 days). The CRL is also updated after a certificate is revoked.

## Send Diagnostic Log Messages for the Certification Authority

To enable the Management Server to send diagnostic log messages to Windows Event Viewer:

Select the **Send CA Service log messages to Windows Event Viewer** check box.

To see the log messages, open Windows Event Viewer:

1. From the Windows desktop, select **Start > Run**.
2. Type eventvwr.  
The log messages appear in the **Application** section of the Event Viewer.

## Configure License Key, Device Monitoring, and Notification Settings

From WatchGuard Server Center, you add or remove a license key, and configure logging and notification settings for your WatchGuard Management Server.

1. In the **Servers** tree, select **Management Server**.
2. Select the **Server Settings** tab.

*The Server Settings page appears.*

The screenshot shows the 'Management Server' configuration page in the 'WatchGuard Server Center'. The 'Server Settings' tab is selected. The page indicates that there are currently 50 licenses. A 'License Keys' section contains a text area with a masked key and an 'Add' button. Below this is a 'Device Monitoring' section with the following options:

- Enable device health monitoring
  - Launch factor:
  - Send an email notification when a device does not contact the server
  - Send an email notification when a device configuration file is changed
- Send Management Server service log messages to Windows Event Viewer
- Log audit information at startup
- Require users to enter a comment when they save to a Fireware XTM device

At the bottom of the page are 'Reset', 'Apply', and 'Help' buttons.

3. Configure settings for your Management Server as described in the subsequent sections.
4. Click **Apply** to save your changes.

## Add or Remove a Management Server License

To add a Management Server license:

1. In the **License Keys** text box, type or paste the Management Server license key.
2. Click **Add**.

*The license key appears in the License Keys list.*

To remove a Management Server license key:

1. In the **License Keys** list, select the license key to remove.
2. Click **Remove**.

For more information on Management Server license keys, see *Find Your Management Server License Key* on page 548.

## Configure Device Monitoring Settings

You can configure the Management Server to monitor the connection status of your managed devices, send a notification message when a managed device is out of contact with the server, and select whether to send an email notification when the configuration file for a managed device is updated.

### *Enable device health monitoring*

Select this check box to enable the Management Server to monitor the connection status of your managed devices.

In the **Launch factor** text box, type the number of times a device can fail to contact the server before a notification message is sent.

### *Send an email notification when a device does not contact the server*

Select this check box to enable the Management Server to send a notification message when a managed device is out of contact with the Management Server for the specified launch factor interval.

### *Send an email notification when a device configuration file is changed.*

Select this check box to enable the Management Server to send a notification message when the configuration file for a managed device is updated.

For information about how to specify where the notification message is sent, see *Configure Logging Settings for Your WatchGuard Servers* on page 708.

## Control Configuration Change Settings

You can set several global configuration parameters to control the log messages sent from the Management Server to the Log Server.

### *Send Management Server service log messages to Windows Event Viewer*

Select this check box to enable the Management Server to send diagnostic log messages to the Windows Event Viewer. You can also configure logging settings for the Management Server on the **Logging** tab.

### *Log audit information at startup*

Select this check box if you want the Management Server to collect log information on managed devices, VPN resources, VPN firewall policy templates, security templates or Device Configuration Templates, and managed VPN tunnels when it starts up. You must select this check box to get accurate information in Report Manager for managed Firebox or XTM devices.

### *Require users to enter a comment when they save to a Fireware XTM device*

Select this check box to require users to type a comment before they save configuration changes they make in Policy Manager to a managed Firebox or XTM device.

## Enable and Configure Active Directory Authentication

If you want to use an Active Directory server to authenticate users, you use the **Active Directory** tab in the **Management Server** page to define connection information for the Active Directory server.

**Note** *To use Active Directory authentication with your Management Server, you must enable LDAPS (LDAP over SSL) in the Active Directory domain. For more information, visit the Microsoft web site or review the documentation for your Active Directory server.,*

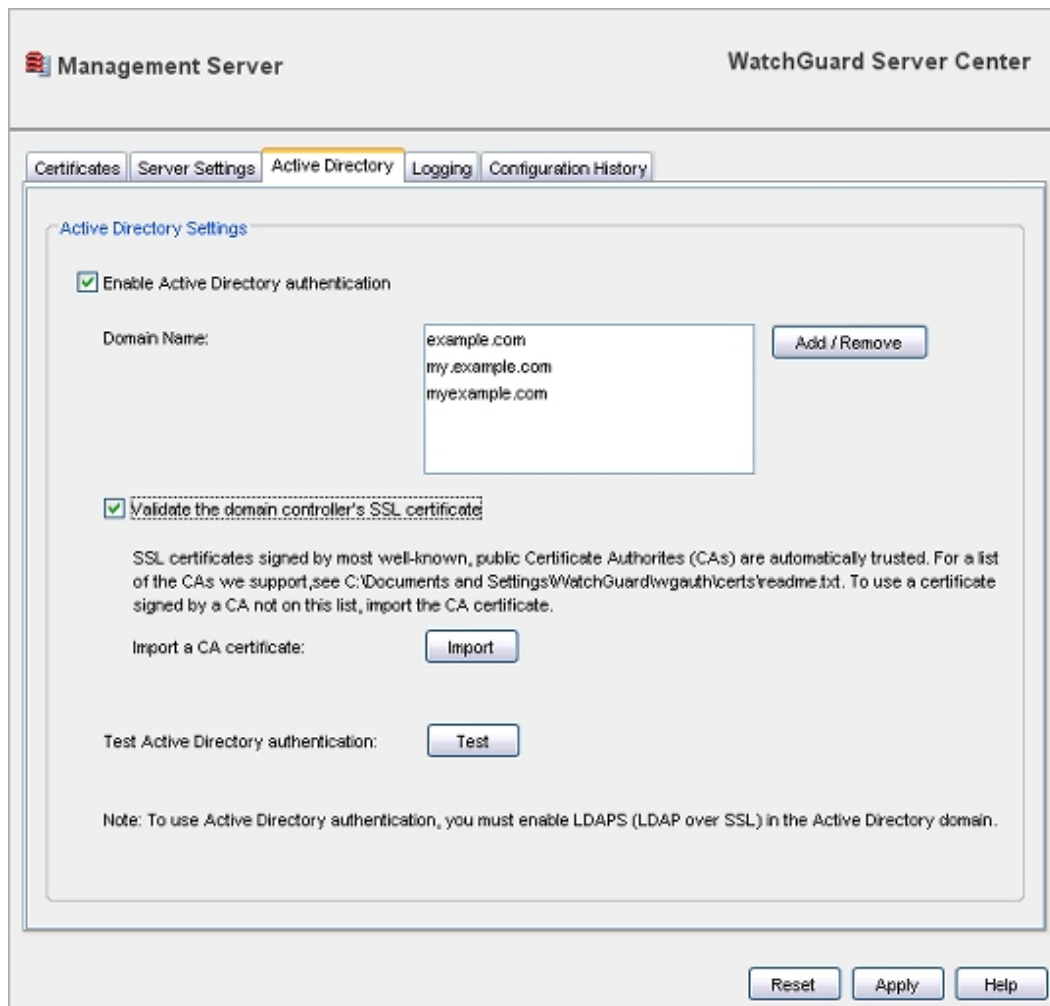
Although the primary administrator account is always managed by the Management Server, you can use an Active Directory server to manage other user accounts. When a user from an external authentication server logs in to the Management Server, the server sends that information to the external Active Directory server. The Active Directory server tells the Management Server whether the user is valid and what groups he or she belongs to. The Management Server then compares the user and groups with its list of users and groups and the role policies they are associated with.

To enable and configure Active Directory authentication, from WatchGuard Server Center:

1. In the **Servers** tree, select **Management Server**.
2. Select the **Active Directory** tab.  
*The Active Directory page appears.*
3. Select the **Enable Active Directory authentication** check box.
4. To add, edit, or remove a domain in the **Domain Name** list, click **Add / Remove**. You can have multiple domain names in this list.  
*The Add Domains dialog box appears.*



5. To add a domain name to the list, in the **Specify domain name** text box, type the Active Directory domain.  
*The Active Directory domain controller uses SSL to connect to the Active Directory server.*
6. Click **Add**.
7. To add more domain names to the list, repeat Steps 4–6.
8. To remove a domain name from the list, select a domain name in the list and click **Remove**.
9. When you are finished, click **OK** to close the **Add Domains** dialog box.  
*The domain names you selected appear in the Domain Name list.*
10. To verify the SSL certificate, select the **Validate the domain controller's SSL certificate** check box.



11. To import a CA certificate, click **Import**.
12. To test your connection for Active Directory authentication, click **Test**.
13. Click **Apply** to save your changes.

## Configure Logging Settings for the Management Server

On the Management Server **Logging** page, you can configure where the Management Server sends log message data. You can choose to send log messages to the WatchGuard Log Server, Windows Event Viewer, and/or a log file.

From WatchGuard Server Center:

1. In the **Servers** tree, select **Management Server**.
2. Select the **Logging** tab.

*The Logging page appears.*

The screenshot shows the 'Management Server' configuration page in 'WatchGuard Server Center'. The 'Logging' tab is selected. The page is titled 'Choose the destination for Management Server log messages'. There are three main sections:

- WatchGuard Log Server:** A checkbox labeled 'Send log messages to WatchGuard Log Server(s)' is unchecked. Below it is a table with two columns: 'Priority' and 'Log Server Address'. To the right of the table are buttons for 'Add', 'Edit', 'Remove', 'Up', and 'Down'. Below the table is a 'Select a log level' dropdown menu set to 'Warning'.
- Windows Event Viewer:** A checkbox labeled 'Send log messages to Windows Event Viewer' is checked. Below it is a 'Select a log level' dropdown menu set to 'Warning'.
- File path:** A checkbox labeled 'Send log messages to a file' is unchecked. Below it is a 'File location' text box containing 'C:\Documents and Settings\Administrator\My Documents\log.txt' and a 'Browse...' button. Below the text box is a 'Select a log level' dropdown menu set to 'Warning'.

At the bottom right of the page are three buttons: 'Reset', 'Apply', and 'Help'.

3. Configure the logging settings for your Management Server.

For detailed information, see *Configure Logging Settings for Your WatchGuard Servers* on page 708.

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

## Define Configuration History Settings

Your WatchGuard Management Server stores the configuration files for all the Fully Managed devices and for all the Device Configuration Templates it manages. When you make changes to the configuration of a Fully Managed device, the Management Server downloads the configuration file from the device and stores a copy of it. When you make changes to a Device Configuration Template, the Management Server also stores a copy of the template. The history for each saved device configuration file or template includes the revision number, timestamp, the user who made the change, the audit comment for the change, and the OS version for the device or template.

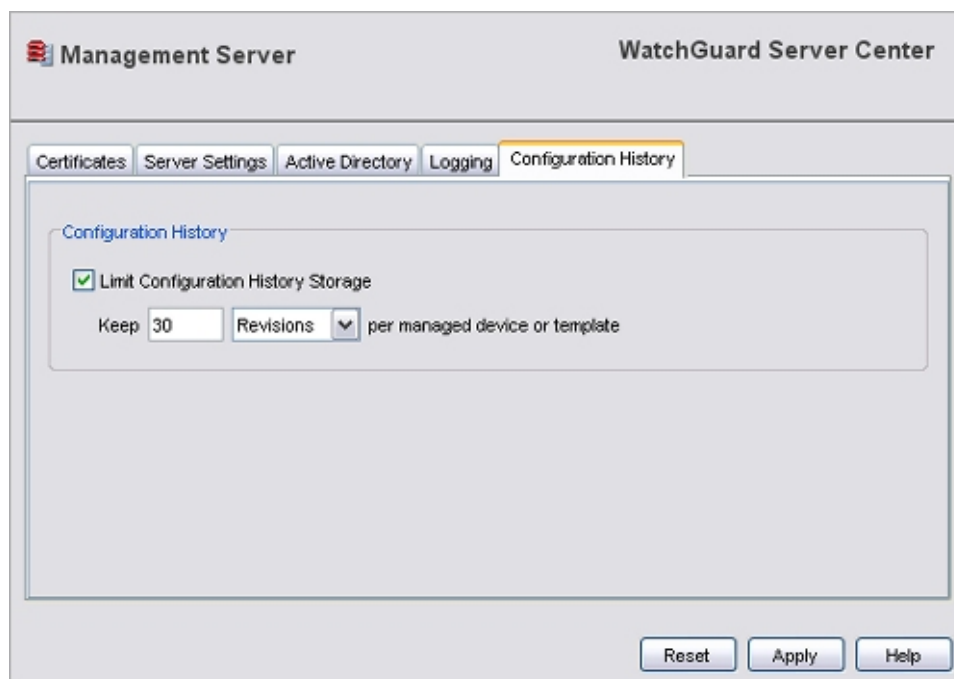
If you change a device from Fully Managed mode to Basic Managed mode, the configuration history already saved on the Management Server remains on the server but, future changes to the device configuration file are not saved. If you delete a Device Configuration Template, the history for that template is also deleted.

You can select to limit the number of configuration files the Management Server stores for all Fully Managed devices and Device Configuration Templates, and specify how many files it saves, by either the number of files or the total disk space the files can use on the Management Server.

To define the settings for configuration history storage:

1. In the **Servers** tree, select **Management Server**.
2. Select the **Configuration History** tab.

*The Configuration History page appears.*



3. To specify the number of files to store for each device, select the **Limit Configuration History Storage** check box.
4. In the **Keep** text box, type the value for the option you selected. The amount you specify is stored for each Fully Managed device or template.



5. From the drop-down list, select an option:
  - **Revisions** — The history includes only the specified number of files.
  - **Megabytes** — The history includes files up to the specified number of megabytes in disk space on the Management Server.
6. Click **Apply** to save your changes.

## Update the Management Server with a New Gateway Address


When you use the WatchGuard Server Center Setup Wizard to set up your Management Server, you use the IP address of the gateway Firebox that protects the Management Server from the Internet. This same IP address is used as the Certificate Revocation List (CRL) Distribution IP address. If you want to change the IP address on your gateway Firebox, you must first change the CRL Distribution IP address on your Management Server, and update all managed devices with this information. If you do not do this, you cannot keep a connection to each of your managed devices.

**Note** *If you have managed Branch Office VPN (BOVPN) tunnels configured on your Management Server, and the gateway Firebox is the endpoint in any of these tunnels, you must remove those VPN tunnels before you start this procedure. When you are done with this procedure, you must create the VPN tunnels again.*

When you configure a managed XTM device, you give the managed device the IP address of the gateway Firebox. The managed device uses this IP address to find the Management Server. The WG-Mgmt-Server policy on the gateway Firebox sets up an SNAT policy to make sure that any connection from a managed XTM device to the Management Server is sent correctly through the external interface of the XTM device.

To change the IP address on your gateway Firebox, you must update your Management Server configuration, update each managed XTM device, and edit the SNAT configuration of the WG-Mgmt-Server policy.

From the Management Server computer:

1. Right-click  and select **Open WatchGuard Server Center**.  
*WatchGuard Server Center appears.*
2. In the **Servers** tree, select **Management Server**.  
*The Management Server page appears.*

**Management Server** **WatchGuard Server Center**

**Certificate Authority**

Configure the properties for your CA certificate.

Common Name:

Organization:

Certificate Lifetime:  Days

Key Bits:

**Client**

Configure the properties for your client certificate.

Certificate Lifetime:  Days

Key Bits:

**Certificate Revocation List**

Configure the properties for the Certificate Revocation List (CRL).

Distribution IP Address:

Publication Interval:  Hours

Send CA service log messages to Windows Event Viewer

3. Select the **Certificates** tab.
4. In the **Certificate Revocation List** section, add a new IP address for your gateway Firebox and remove the existing IP address.
5. Click **Apply**.
6. On your management computer, open WatchGuard System Manager and connect to your Management Server.
7. Select the **Device Management** tab.
8. Right-click a managed device and select **Update Device**.
9. Below **Update Client Settings**, make sure that the **Reset Server Configuration** and **Expire Lease** check boxes are selected.  
Make sure the **Issue/Reissue Firebox's IPsec Certificate and CA's Certificate** check box is also selected.
10. Repeat Steps 3–6 for each device managed by your Management Server.
11. Start Policy Manager for the configuration file of the gateway Firebox.
12. Select **Network > Configuration** and change the IP address of the external interface of the device to the new IP address.
13. Double-click the **WG-Mgmt-Server** policy.  
*The Edit Policy Properties dialog box appears.*

14. In the **To** section, select the SNAT entry and click **Remove**.
15. In the **To** section, click **Add**.  
*The Add Address dialog box appears.*
16. Click **Add SNAT**.  
*The SNAT dialog box appears.*
17. Click **Add**.  
*The Add SNAT dialog box appears.*
18. In the **SNAT Name** text box, type a unique name for this SNAT object.
19. (Optional) In the **Description** text box, type a description to help you identify this SNAT object.
20. Select an option: **Static NAT** or **Server Load Balancing**.
21. Click **Add**.  
*The Add Static NAT/Server Load Balancing dialog box appears.*
22. From the **External IP Address** drop-down list, select the new IP address for your gateway Firebox.
23. In the **Internal IP Address** text box, type the IP address of your Management Server.
24. Click **OK** to close each dialog box and save your changes.
25. *Save the Configuration File.*

When the XTM device restarts, connections between the Management Server and the managed XTM devices start again. You can now re-create any BOVPN tunnels for which the gateway Firebox is a VPN endpoint.

## Change the IP Address of a Management Server

Your managed XTM devices must always be able to contact your Management Server. If you change the IP address on your Management Server, or change the IP address on the external interface of the gateway Firebox, the managed devices could lose contact with the Management Server. When you change the IP address of your Management Server, you must also change the IP addresses for the Certificate Revocation List (CRL) Distribution and your managed XTM devices.

The CRL Distribution IP address is the IP address that the Management Server gives to managed XTM devices. The managed client devices then use this IP address to connect to the Management Server. The CRL Distribution IP address must be the same as the external IP address that managed clients use to connect to the Management Server.

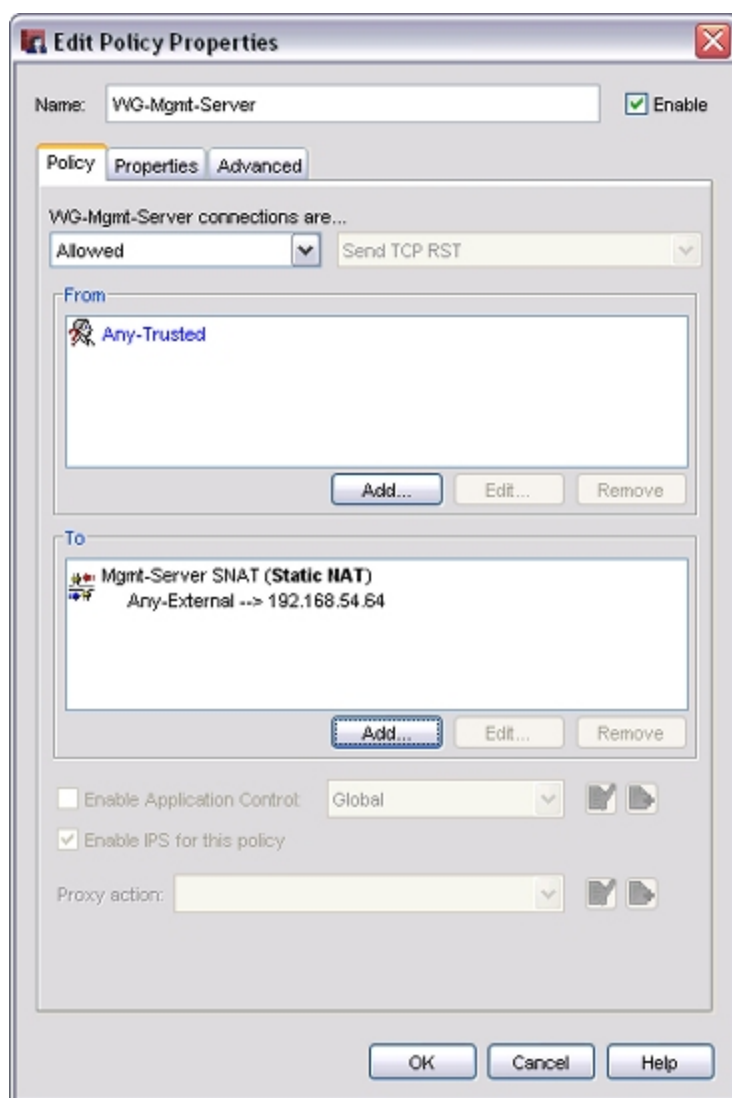
If the Management Server uses a private IP address, the CRL Distribution IP address is the IP address on the external interface of the gateway Firebox. If the Management Server uses a public IP address, and is not behind a gateway Firebox, the CRL Distribution IP address is the public, external IP address of the Management Server.

When you configure a managed XTM device, you give the managed XTM device the IP address of the gateway Firebox. The managed XTM device uses this IP address to find the Management Server. The WG-Mgmt-Server policy on the gateway Firebox sets up a NAT policy to make sure that any connection from a managed XTM device to the Management Server is sent correctly through the external interface of the XTM device. To change the IP address on your Management Server, you must edit the WG-Mgmt-Server policy NAT configuration.

## If Your Management Server is Configured with a Private IP Address

1. From Policy Manager, open the configuration of the gateway Firebox that protects your Management Server from the Internet.
2. Double-click the **WG-Mgmt-Server** policy.

*The Edit Policy dialog box appears.*



3. Select the SNAT entry in the **To** section of the WG-Mgmt-Server policy and click **Remove**.
4. In the **To** section, click **Add**.  
*The Add Address dialog box appears.*
5. Click **Add SNAT**.  
*The SNAT dialog box appears.*
6. Click **Add**.  
*The Add SNAT dialog box appears, with the Static NAT option selected by default.*

7. In the **SNAT Name** text box, type a name for the SNAT action.
8. Click **Add**.  
*The Add Static NAT dialog box appears.*
9. From the **External IP Address** drop-down list, make sure the IP address for your gateway Firebox is selected.
10. In the **Internal IP Address** text box, type the new IP address of your Management Server.
11. Click **OK** to close each of the dialog boxes.
12. *Save the Configuration File.*


## If Your Management Server is Configured with a Public IP Address

1. From Policy Manager, open the configuration of the gateway Firebox that protects your Management Server from the Internet.
2. Double-click the **WG-Mgmt-Server** policy.  
*The Edit Policy dialog box appears.*
3. Select the NAT entry in the **To** dialog box of the WG-Mgmt-Server policy. Click **Remove**.
4. Below the **To** list, click **Add**.  
*The Add Address dialog box appears.*
5. Click **Add Other**.  
*The Add Member dialog box appears.*
6. From the **Choose Type** drop-down list, select **Host IP**.
7. In the **Value** text box, type the new public IP address on the Management Server.
8. Click **OK** to close each of the dialog boxes.
9. *Save the Configuration File.*

## Update the Certificate Revocation List (CRL) Distribution IP Address

You can only update the CRL distribution IP address for your Management Server if it is configured with a public IP address.

From the Management Server computer:

1. Right-click  and select **Open WatchGuard Server Center**.  
*The Connect to WatchGuard Server Center dialog box appears.*
2. Type the Administrator passphrase and click **Login**.  
*The WatchGuard Server Center appears.*
3. In the **Servers** tree, select **Management Server**.
4. Select the **Certificates** tab.
5. If there is an IP address in the **Certificate Revocation List** section, select the address from the **Distribution IP Address** list and click **Remove**.
6. Click **Add** to add a new address.  
*The CRL IP Address dialog box appears.*
7. In the **IP Address** text box, type the new IP address of the Management Server.
8. Click **OK**.  
*The IP address appears in the Distribution IP Address list.*
9. Click **Apply**.  
*A dialog box appears to confirm you want to update the Management Server with your changes.*

10. Click **OK**.  
*A Comments dialog box appears.*
11. (Optional) Add comments for the audit logs.
12. Click **OK**.  
*The Management Server is updated with the changes.*

## Update Managed XTM Devices

You must update all of your managed client devices to finish the IP address change.

1. In WatchGuard System Manager, connect to your Management Server.
2. Select the **Device Management** tab.
3. Right-click a managed device and select **Update Device**.
4. Below **Update Client Settings**, make sure that the **Reset Server Configuration** and **Expire Lease** check boxes are selected.
5. Repeat Steps 3–4 for each device managed by the Management Server.

## Change the Administrator Passphrase

The Administrator passphrase is the master passphrase for all of your WatchGuard servers. In previous versions of WatchGuard System Manager, the Administrator passphrase referred to two passphrases: the Master passphrase and the Server Management passphrase. These passphrases have been replaced by the Administrator passphrase in the 11.x release.

The Administrator passphrase is the passphrase for the *admin* user. The *admin* user is automatically created when you complete the WatchGuard Server Center Setup wizard. After you have set up WatchGuard Server Center, you can change the Administrator passphrase at any time.

**Note** You cannot change the user name of the **admin** user. You can only change the passphrase.

For more information about the WatchGuard Server Center Setup wizard, see *Set Up WatchGuard Servers* on page 545.

For more information about how to edit users, see *Define or Remove Users or Groups* on page 671.

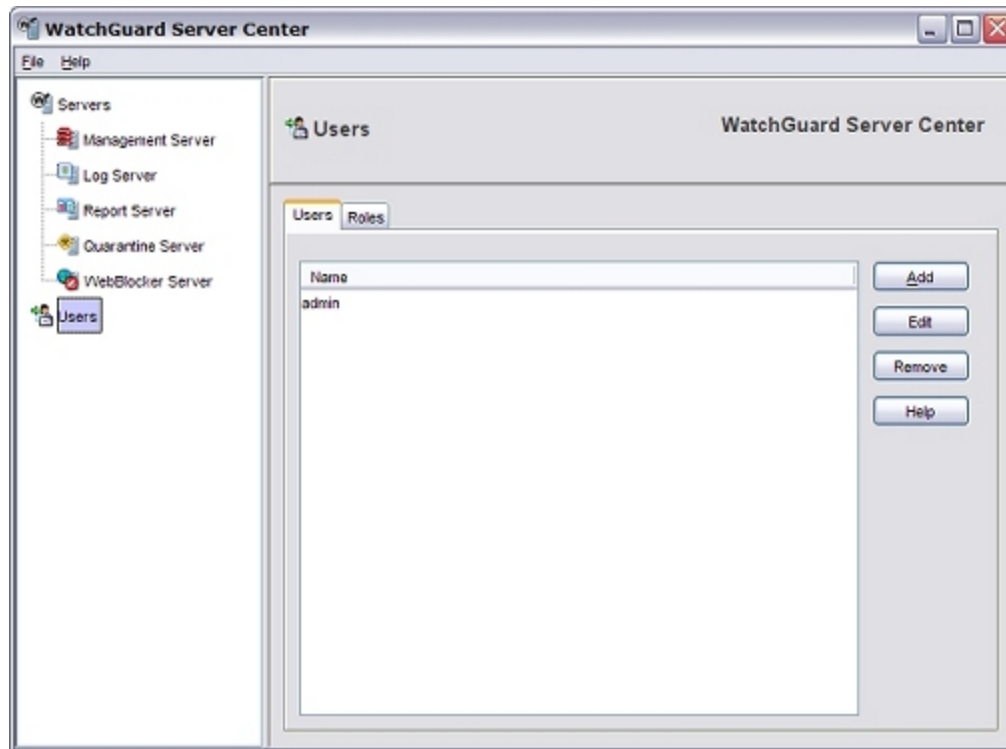
We recommend that you back up your Management Server configuration immediately after you change the Administrator passphrase. When you create a backup configuration file, the current Administrator passphrase is stored in the file. You must use this passphrase when you restore the configuration file. If you change your Administrator passphrase, and then restore a backup configuration file with an old Administrator passphrase, the old passphrase is restored with the server configuration.

For more information about how to restore a backup configuration file, see *Back Up or Restore the Management Server Configuration* on page 576.

Before you change the Administrator passphrase, make sure the **admin** user has logged out of the Management Server.

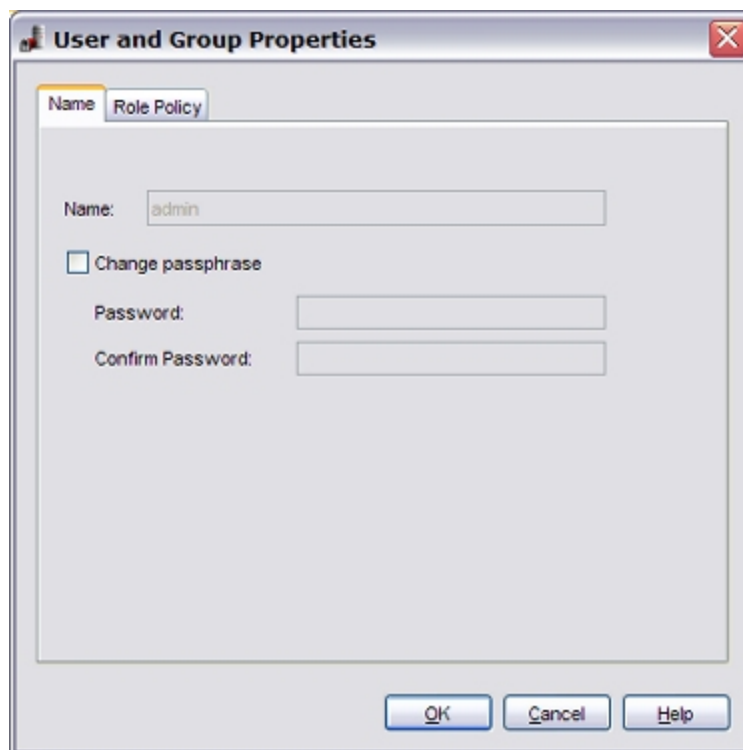
From WatchGuard Server Center:

1. In the left navigation bar, select **Users**.  
*The Users page appears.*



2. On the **Users** tab, in the **Name** list, select **admin**.
3. Click **Edit**.

*The User and Group Properties dialog box appears.*



4. Select the **Change passphrase** check box.
5. Type and confirm the new passphrase.
6. Click **OK**.


## Back Up or Restore the Management Server Configuration

The Management Server contains the configuration information for all managed Firebox or XTM devices and VPN tunnels. It is a good idea to create regular and frequent backup files for the Management Server and keep them in a safe place. You can use these backup files to restore the Management Server in case of hardware failure. You can also use backup files if you want to move the Management Server to a new computer.

When you create a backup configuration file, the current Administrator passphrase is stored in the file. You must use this passphrase to restore the configuration file. If you change your Administrator passphrase, make sure you remember the passphrase for your backup file. When you restore a backup configuration file with an old Administrator passphrase, that passphrase is restored with the server configuration.

### Back up Your Configuration


From the computer where you installed the Management Server:

1. Right-click  and select **Backup/Restore Management Server**.  
*The Management Server Backup/Restore Wizard starts.*
2. Click **Next**.  
*The Select an action screen appears.*
3. Select **Back up settings**.
4. Click **Next**.  
*The Specify a backup file screen appears.*
5. Click **Browse** and select a location for the backup file.  
Make sure you save the configuration file to a location you can access later to restore the configuration.
6. Click **Next**.  
*The Management Server Backup/Restore Wizard is complete screen appears.*
7. Click **Finish** to exit the wizard.

### Restore Your Configuration

Before you begin, make sure you have the correct Administrator passphrase for your backup file.

From the computer where you installed the Management Server:

1. Right-click  and select **Backup/Restore Management Server**.  
*The Management Server Backup/Restore Wizard starts.*
2. Click **Next**.  
*The Select an action screen appears.*
3. Select **Restore settings**.
4. Click **Next**.  
*The Specify a backup file screen appears.*




5. Click **Browse** and select the backup file.
6. In the **Administrator passphrase** text box, type the administrator passphrase that was used to create the backup file.
7. Click **Next**.  
*The Management Server Backup/Restore Wizard is complete screen appears.*
8. Click **Finish** to exit the wizard.

## Move the Management Server to a New Computer


To move Management Server software to a new computer, you first back up the Management Server configuration on the current computer, then you restore the configuration on the new computer. Make sure you have the Administrator passphrase from the backup configuration. You must also make sure that the new Management Server has the same IP address as the former Management Server.

### Back up, Move, and Restore Your Management Server

From the computer where the Management Server is installed:

1. Right-click  and select **Backup/Restore Management Server**.  
*The WatchGuard Server Center Backup/Restore Wizard starts.*
2. Use the wizard to back up your Management Server configuration.  
For more information, see *Back Up or Restore the Management Server Configuration* on page 576.

Make sure you save the configuration file to a location you can access from the new computer.

3. On the new computer, run the WatchGuard System Manager Setup program.
4. Under the **Server Components** section, make sure you select **Management Server**.
5. Right-click  on the new computer and select **Backup/Restore Management Server**.  
*The WatchGuard Server Center Backup/Restore Wizard starts.*
6. Use the wizard to restore your Management Server configuration.  
For more information, see *Back Up or Restore the Management Server Configuration* on page 576.

### Configure Other Installed WatchGuard Servers

When you restore a configuration to your new Management Server installation, you do not have to complete the WatchGuard Server Center Setup Wizard when you open WatchGuard Server Center and access your Management Server. However, if you have installed other WatchGuard servers on your new management computer, the configuration does not restore settings for these servers. You must run the Server Center Setup Wizard to configure the other servers.

Before you begin, make sure you have all the necessary information to set up the WatchGuard servers you installed. For more details about the information necessary to complete the Server Center Setup Wizard, see *Set Up WatchGuard Servers* on page 545.

From WatchGuard Server Center:


1. In the **Servers** tree, select any server with the status **Server not configured**.
2. Click the **Click here to launch setup wizard for [WatchGuard] Server** link.  
The link text specifies the name of the server you selected, but the Wizard sets up all installed WatchGuard servers.  
*A dialog box appears that tells you the wizard will launch.*
3. Click **OK**.  
*The WatchGuard Server Center Setup Wizard appears.*
4. Click **Next**.
5. Complete the Server Center Setup Wizard.
6. Click **Refresh** on the server page of the selected server.  
*The server information appears and the server is started.*
7. In the **Servers** list, select another installed server.

The **Click here to launch setup wizard for [WatchGuard] Server** link appears on the server page. Do not click this link. The server is already set up.

8. Click **Refresh**.  
*The server information appears and the server is started.*
9. Repeat Steps 7–8 for each WatchGuard server you installed.

## Use WSM to Connect to your Management Server

To connect to your Management Server from WatchGuard System Manager:

1. Click .  
Or, select **File > Connect to Server**.  
Or, right-click anywhere in the WatchGuard System Manager window and select **Connect to > Server**.  
*The Connect to Management Server dialog box appears.*




2. From the **Management Server** drop-down list, select a server by its host name or IP address.  
Or, type the IP address or host name.  
When you type an IP address, type all the numbers and the periods. Do not use the Tab or arrow keys.
3. Type your user name for your user account on the Management Server.
4. Type the passphrase for your user account.  
If you use the default admin account, the passphrase is the Administrator passphrase.

5. If necessary, change the **Timeout** value.  
This value sets the time (in seconds) that WatchGuard System Manager listens for data from the Management Server before it sends a message that it cannot connect.  
If you have a slow network or Internet connection to the device, you can increase the timeout value.  
This value is the duration you must wait for a timeout message if you try to connect to a Management Server that is not available.
6. Click **Login**.  
*The server appears in the WatchGuard System Manager window.*

**Note** *In some previous versions of WatchGuard security products, the WatchGuard Management Server was called the DVCP Server.*

## Disconnect from the Management Server

1. Select the Management Server.
  2. Click .
- Or, select **File > Disconnect**.  
Or, right-click and select **Disconnect**.

## Import or Export a Management Server Configuration

You can use WatchGuard System Manager (WSM) to export your Management Server configuration file to a DVCP file. You can then use a text editor to open the file and view it. You can also import a saved DVCP configuration file to your Management Server.

A saved configuration file is not a substitute for a backup of your Management Server. For more information about how to back up your Management Server, see *Back Up or Restore the Management Server Configuration* on page 576.

### Export a Configuration

1. Open WSM and [connect to your Management Server](#).
2. Select **File > Export to File**.  
*The Save As dialog box appears. The default file name is [Management Server IP address].dvcp.*
3. To select a different name for the file, in the **File name** text box, type a new name.
4. Select a location to save the file.
5. Click **Save**.

### Import a Configuration

1. Open WSM and [connect to your Management Server](#).
2. Select **File > Import from File**.  
*The Open dialog box appears.*
3. Browse to select a configuration file.
4. Click **Open**.



# 19 Centralized Management

---

## About WatchGuard System Manager

WatchGuard System Manager (WSM) has menus and icons you can use to start other tools. WSM also has two tabs that you can use to monitor and manage your XTM devices and environment: **Device Status** and **Device Management**.





### Device Status

Information about a device you connect to appears in the **Device Status** tab. The information that appears includes the status, IP address, and MAC address for each Ethernet interface, and the installed certificates. It also includes the status of all virtual private network (VPN) tunnels that are configured in WSM.

Expanded information for each XTM device includes the IP address and subnet mask of each XTM device interface. It also includes:

- IP address and subnet mask of the default gateway (for external interfaces only)
- MAC (Media Access Control) address of the interface
- Number of packets sent and received on each interface since the last XTM device restart

Each device can be in one of four possible states, as indicated by the device icon:

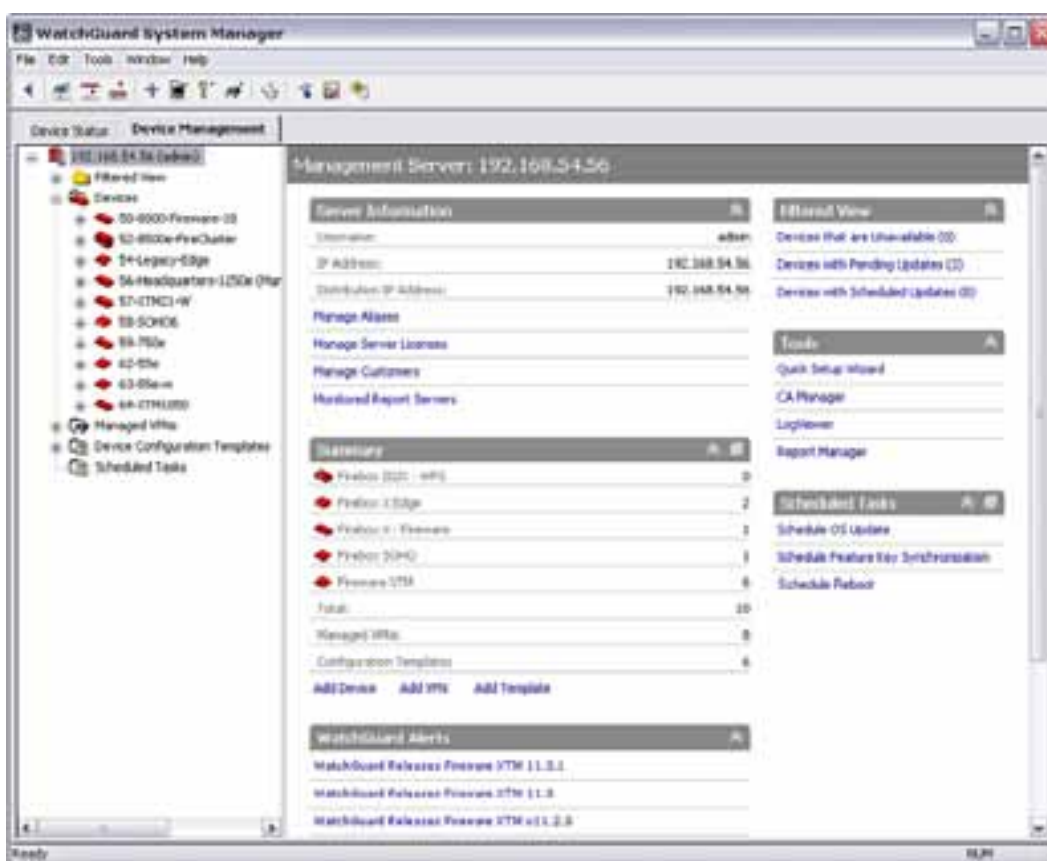
-  — (Normal operation) The device is successfully sending data to WatchGuard System Manager.
-  — The device has a dynamic IP address and has not yet contacted the Management Server.
-  — WatchGuard System Manager cannot make a network connection to the device at this time.
-  — The device is being contacted for the first time or has not been contacted yet.

The **Device Status** tab also includes information on Branch Office VPN tunnels and Mobile VPN tunnels.

## Device Management

The **Device Management** tab has a navigation pane on the left and an information pane on the right. The navigation pane shows the connected WatchGuard Management Servers and their managed devices, managed VPNs, VPN Firewall Policy Templates, Security Templates, Device Configuration Templates, and Scheduled Tasks. If you expand a device list, you see the VPN resources (networks) behind the device. For more information see, *Add VPN Resources* on page 901.

**Note** You only see the **Device Management** tab when you connect to a Management Server. For more information, see *Use WSM to Connect to your Management Server*.



The information pane on the right shows more detailed information for any item you select in the navigation pane and enables you to complete certain tasks.

### Management Server

To see or change information about the Management Server, select the **Management Server** in the navigation pane. The available information about the Management Server appears in the right pane and includes:

- User name and IP address of the user logged in to the Management Server  
*This user name is also included in parentheses after the IP address of the Management Server in the left navigation pane.*
- *Manage Aliases for Firebox X Edge Devices*

- *Manage Server Licenses*
- **Customers** — You can change the Contact List, as described in *Set Device Management Properties*
- *Review and Manage the Monitored Report Servers List*
- List of managed devices, VPN tunnels, and Device Configuration  
For more information, see *Add and Manage VPN Tunnels and Resources* on page 615 and *Create Device Configuration Templates* on page 633.
- **WatchGuard Alerts** — Recent LiveSecurity Broadcasts that are information alerts  
*If you click an alert, you must log in with your LiveSecurity Service account information to see the full text of the alert.*
- **Filtered View** — Information about managed devices, grouped by status and currently scheduled tasks  
For more information, see *About Filtered View* on page 609.
- **WatchGuard System Manager tools** available for this Management Server  
For more information, see *Start WatchGuard System Manager Tools*.
- List of currently scheduled tasks  
For more information, see *Review, Cancel, or Delete Scheduled Tasks*.

### *Devices*

To see a list of managed devices for the Management Server, select **Devices** in the navigation pane. The **Devices** page appears and shows information about all the devices managed by this Management Server.

To see detailed information about a device, in the **Devices** list, select the device. Or, on the **Devices** page, double-click a device. The **Device Page** for the selected device appears.

For more information, see *Review Information for Managed Devices*,

### *Managed VPNs*

To see a list of existing VPN tunnels and add new VPN tunnels, select **Managed VPNs** in the navigation pane. On the **Managed VPNs** page, you can review basic details about your managed VPN tunnels. Double-click a managed VPN in the list to go to the **Managed VPN** page for that VPN tunnel. You can also click **Add** to *Add and Manage VPN Tunnels and Resources*.

To see information about an existing Managed VPN tunnel, click a managed VPN in the **Managed VPNs** tree. On the **Managed VPN** settings page, you can review the tunnel settings. Click **Configure** to *Add and Manage VPN Tunnels and Resources*.

## About the Device Management Page

You can use the device management page to configure management settings for your managed devices.

1. Use WSM to Connect to your Management Server.
2. On the **Device Management** tab, select **Devices**.  
*The Devices page appears.*
3. Double-click a device in the list.  
Or, expand **Devices**, and click a device in the list.  
*The Device management page for the selected device appears.*

From the Device Management page you can:

- See if the device configuration file is locked

If another Management Server user account has opened the configuration file in Policy Manager, the device configuration file is locked. An alert appears at the top of the page to indicate the file is locked. You cannot make changes to the device configuration file until the other user unlocks the file (closes Policy Manager for this device).

- See general device information
- See, add, edit, or remove VPN tunnels for the device

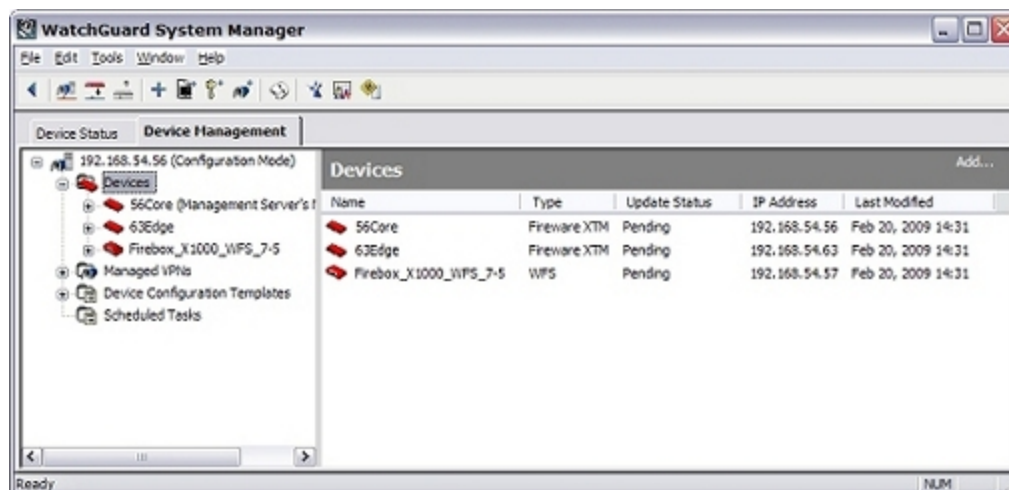
For more information about this section of the page, see *Add and Manage VPN Tunnels and Resources* on page 615.

- See, add, edit, or remove VPN resources for the device
- Verify the connection status of the device
- Launch tools you can use to monitor, define, or manage the device

## Review Information for Managed Devices

On the WatchGuard System Manager **Devices** page, you can review the complete list of managed devices and information for each one.

1. Use WSM to Connect to your Management Server.
2. From the navigation pane, select **Devices**. list, select a device or folder.  
*Information for that device appears on the Devices page.*





*Name*

The name of the managed device.

*Type*

The type of device or OS installed on the managed device.

*Update Status*

Scheduled device updates and update status appear in this column.

- **Never** — The device has never been updated.
- **Pending** — A change has been made but not synchronized on the device, or an update is in progress.
- **Scheduled** — An update has been scheduled, but has not started.
- **Complete** — The device has been updated. The date/time of the update appears in parenthesis.

*IP Address*

The IP address used to identify the device. If the device has not reported in to the server, **n/a** appears.

*Last Modified*

The time and date when the configuration file for the device was last changed on the server.

To see more information for a specific device:

1. Expand the **Devices** list.
2. Select a device or folder.

*Information for that device appears on the Devices page.*

## Verify the Connection Status of a Device

When a device is managed by your Management Server, it regularly contacts the server to verify the device is still online and connected to the server. You can see the device connection status on the **Device** page for that device. You can use this information to help you diagnose connection issues with the managed devices in your network.

Connection status information appears in the **Heartbeat** section and includes the date and time that the device last verified the connection to the Management Server, as well as the current connection status of the device: **Alive** or **Unavailable**. A status of **Alive** indicates that your device is in contact with the Management Server. A status of **Unavailable** indicates your device is not in contact with the Management Server.

When a device has a status of **Unavailable**, the **Heartbeat** section header changes to the alert color, and the device appears in the Filtered View **Unavailable** category. For more information about Filtered View, see *About Filtered View* on page 609.

To verify the connection status of a device:

1. *Use WSM to Connect to your Management Server.*  
*The Device Management tab appears.*

2. In the Management Server tree, select **Devices**.  
*The Devices page appears.*
3. On the **Devices** page, double-click a device in the list.  
Or, in the Management Server tree, expand the **Devices** list, and select a device.  
*The Device management page for the selected device appears, with the Heartbeat section at the top right corner.*
4. To expand the **Heartbeat** section, click the double-arrows at the right of the section.  
*The connection status information appears for this device.*



## About Centralized Management Modes

Centralized Management enables you to control the configurations and settings for your XTM devices from your WatchGuard Management Server. Centralized Management includes two modes: *Basic Managed Mode* and *Fully Managed Mode*. Basic Managed Mode is available for all device models that can be managed by your Management Server. Fully Managed Mode is available for Firebox X Edge and Firewall XTM devices only.

For more information about which XTM device models you can manage with your Management Server, see *Add Managed Devices to the Management Server* on page 590.

In Basic Managed Mode you can use the Management Server to:

- Monitor your Firebox or XTM device
- Manage and monitor VPN tunnels
- Synchronize your feature key
- Update your XTM device OS

In Fully Managed Mode you can use the Management Server to:

- Monitor your Firebox or XTM device
- Manage and monitor VPN tunnels
- Synchronize your feature key
- Update your XTM device OS
- Manage your XTM device configuration with the Management Server
- Schedule configuration updates to your managed devices
- Manage device templates
- Schedule updates to your Device Configuration Templates

When you use WatchGuard System Manager (WSM) to add your device to the Management Server as a managed device, it is automatically in Basic Managed Mode. To change to Fully Managed Mode, use the **Device Mode** section on the WSM **Device** page for your device.

When a device is in Basic Managed Mode, you can still connect directly to the device and manage the configuration file locally with Policy Manager. When a device is in Fully Managed Mode, you can only make changes to the configuration from the Management Server. If you connect directly to the XTM device, the connection and configuration are set to read-only, and you cannot make changes to the configuration

locally. When you make a change to the configuration of a fully managed device, a new copy of the configuration is saved to the Management Server. The configuration history includes the configuration revision number, time the change was made, the user who made the change, an audit comment, and the OS version used by the device.

For more information about how to apply a template to a device, see *Apply Device Configuration Templates to Managed Devices* on page 652.

For more information about how to change the management mode, see *Change the Centralized Management Mode* on page 587.

For more information about how to use WSM to manage your devices, see *About WatchGuard System Manager* on page 581.

## Change the Centralized Management Mode

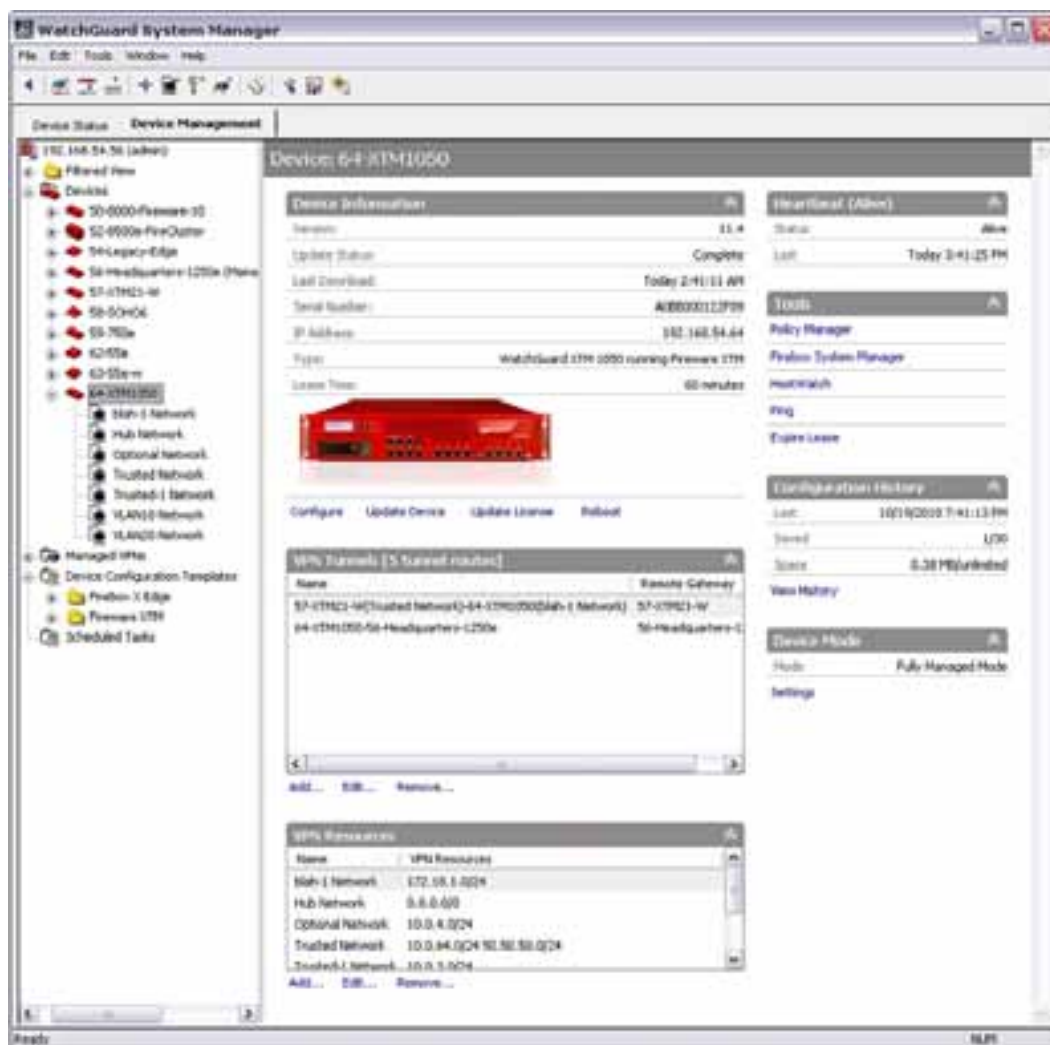
When you add your Firebox or XTM device to your Management Server as a managed device, it is added in *Basic Managed Mode*. You can use WatchGuard System Manager (WSM) to change your Firebox or XTM device to *Fully Managed Mode*.

For more information about management modes, see *About Centralized Management Modes* on page 586.

For more information about Device Configuration Templates, see *Create Device Configuration Templates* on page 633.

To change the management mode:

1. Use WSM to Connect to your Management Server.
2. Expand the **Devices** list and select a Firebox X Edge or Fireware XTM device.  
*The Device page appears for the device you selected. The current Device Mode appears in the Device Mode section.*



3. In the **Device Mode** section, click **Settings**.  
*The Device Mode dialog box appears.*
4. Follow the steps in the subsequent section for the mode you want to select.

## Change to Basic Managed Mode

When you change from Fully Managed Mode to Basic Managed Mode, the Management Server no longer stores a new version of the configuration file when you make a change. The configuration files that are already stored in the configuration history for your device remain on the Management Server.

In the **Device Mode** dialog box:

1. Select **Basic Managed Mode**.



2. Click **OK**.

*Basic Managed Mode appears in the Device Mode section.*

## Change to Fully Managed Mode

When you change from Basic Managed Mode to Fully Managed Mode, the Management Server stores a new version of the configuration file each time you make a change.

In the Device Mode dialog box:

1. Select **Fully Managed Mode**.
2. To apply a configuration template, select the **Use Configuration Template** check box and select a template from the drop-down list.



3. Click **OK**.

*A confirmation message appears.*


4. Click **Yes**.

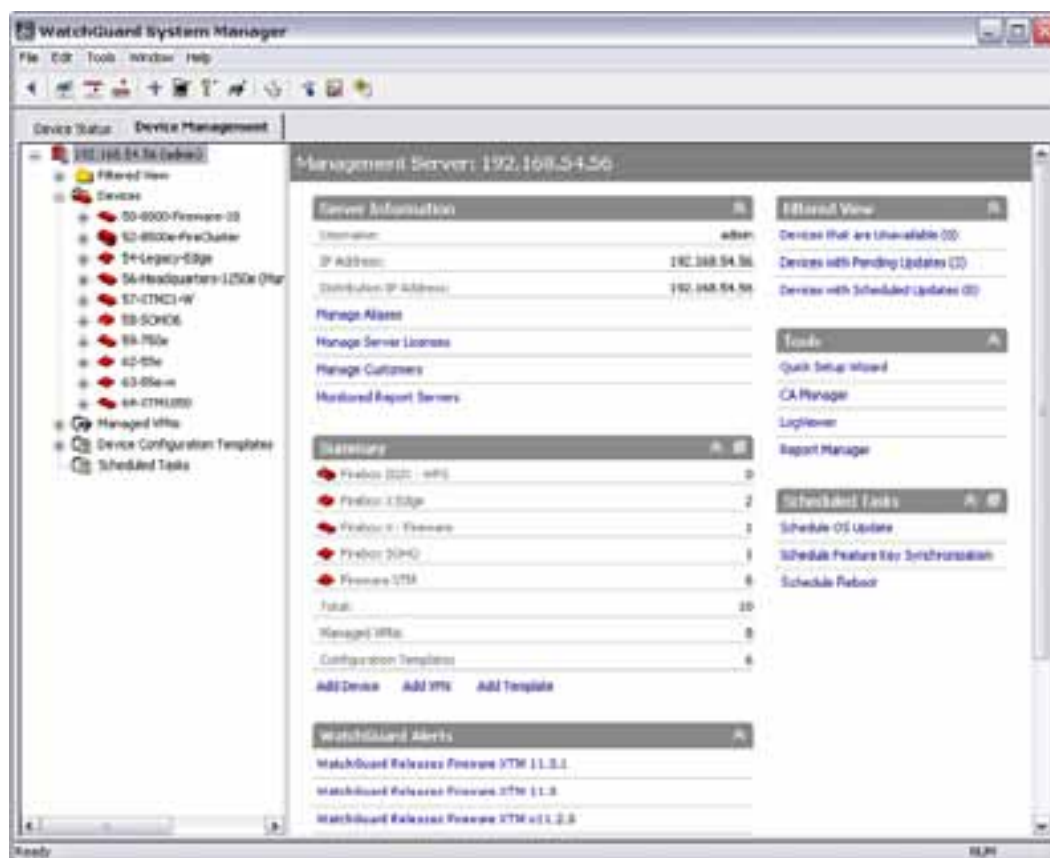
*The Management Server downloads the configuration file. If you selected a configuration template, the template is applied to the device.*


## Add Managed Devices to the Management Server

You can use the Management Server to manage Firebox devices, including Firebox X and WatchGuard XTM devices that use Fireware XTM OS, Firebox X devices that use Fireware OS, Firebox X Edge devices, Firebox III and Firebox X Core devices that use WFS appliance software, and Firebox SOHO devices. You can manage a device with a dynamic IP address if you used Policy Manager to configured it as a managed client. If your device has multiple external interfaces, do not change the interface configuration after you add the device to the Management Server.

From WatchGuard System Manager:

1. To connect to the Management Server, click  .  
Or, select **File > Connect to Server**.  
Or, right-click anywhere in the window and select **Connect to > Server**.  
*The Connect to Management Server dialog box appears.*
2. Type or select the IP address of the Management Server and type the configuration passphrase.
3. Click **Login**.  
*The Management Server page appears.*



4. Click  to add a device.  
Or, on the **Management Server** page, in the **Summary** section, select **Add Device**.  
*The Add Device Wizard starts.*
5. Click **Next**.  
*The first configuration screen appears.*

6. Select an option:
  - **I know the device's current IP address**
  - **I don't know the device's current dynamically allocated IP address**
7. Follow the instructions in the subsequent section for the option you selected.

## If You Know the Current IP Address of the Device

1. Type the **Hostname/IP Address**, **Status Passphrase**, and **Configuration Passphrase** for the device.  
If you select a device that is already managed by another server, a warning message appears. Click **Yes** to overwrite the other configuration and add this device to this Management Server.
2. Click **Next**.  
*The wizard performs device discovery.*
3. If you want to use a name other than the default name, type a **Client Name** for the device.
4. Select the **Device Type** from the drop-down list.
5. Type and confirm the **Shared Secret**.  
The name and shared secret you type here must match the name and shared secret you give the device when you enable it as a managed client.
6. Click **Next**.
7. Type and confirm the **Status Passphrase** and the **Configuration Passphrase**. Click **Next**.
8. Select the tunnel authentication method for the device. Click **Next**.  
*The Configure the Device page appears.*
9. Click **Next**.  
*The Add Device Wizard is complete page appears.*
10. Review the information for your device. Click **Close**.  
*The Add Device Wizard closes and the device appears in WSM in the correct device category in the Summary list and in the Devices list.*

## If You Do Not Know the IP Address of the Device

After you complete the wizard, you can manually configure the device for management. When the device is configured for management, it contacts the Management Server.

For more information, see *Configure an XTM Device as a Managed Device* on page 618 and follow the procedure in the *Set up the Managed Client* section.

1. Click **Next**.  
*The wizard does not perform device discovery and the Enter a name for the device page appears.*
2. If you want to use a name other than the default name, type a **Client Name** for the device.
3. Select the **Device Type** from the drop-down list.
4. Type and confirm the **Shared Secret**.  
The name and shared secret you type here must match the name and shared secret you give the device when you enable it as a managed client.
5. Click **Next**.
6. Type and confirm the **Status Passphrase** and the **Configuration Passphrase**. Click **Next**.  
*The Select the tunnel authentication method page appears.*
7. Select the tunnel authentication method for the device. Click **Next**.  
*The Configure the Device page appears.*
8. Click **Next**.  
*The Add Device Wizard is complete page appears.*
9. Click **Close**.  
*The Add Device Wizard closes and the device appears in WSM in the correct device category in the Summary list and in the Devices list.*

**Note** *If there is a lot of network traffic when the wizard tries to connect to the device, the SSL connection times out. Complete the wizard again when the network is less busy.*



# Set Device Management Properties

You can configure three categories of device management properties from the Device Management page for your XTM device: connection settings, IPSec tunnel preferences, and contact information.

## Connection Settings

1. On the [Device Management page](#), in the **Device Information** section, click **Configure**.  
The *Device Properties dialog box* appears.

The screenshot shows the 'Device Properties' dialog box with the 'Connection Settings' tab selected. The dialog box contains the following fields and options:

- Display Name:** GatewayBox
- Firebox Type:** Firebox X with Fireware
- Device has dynamic external IP address (DHCP, PPPoE)
- Hostname/IP Address:** 192.168.54.50, 10.0.44.1, 10.0.55.1
- Status Passphrase:** [Redacted]
- Configuration Passphrase:** [Redacted]
- Shared Secret:** dEE^327@w~(MMhq(u(#9cmE~eX5L+
- Lease Time:** 60 minutes

Buttons at the bottom: OK, Cancel, Help.

2. In the **Display Name** text box, type the name that you want to appear in WSM for the device.
3. From the **Firebox Type** drop-down list, select the device hardware and, if applicable, the appliance software installed on it.
4. If the device has a static IP address, in the **Hostname/IP Address** field, select or type the entry for your device. This field contains the list of external IP addresses that WSM uses to poll the device and to build VPN tunnels.
5. If the device has a dynamic IP address, select the **Device has dynamic external IP address** check box.
6. In the **Client Name** text box, type the name of the device.

For more information about how to manually set up a device for management, see *Configure an XTM Device as a Managed Device* on page 618.

**Device Properties**

Connection Settings | IPSec Tunnel Preferences | Contact Information

A managed device can participate in VPNs as defined by the list of tunnels. WatchGuard System Manager can also provide real-time status of all configured devices.

Display Name: Box62\_8-6\_Edge

Firebox Type: Firebox X Edge (X10e,X10e-W,X20e,X20e-W,X55e,X55e-W)

Device has dynamic external IP address (DHCP, PPPoE)

Client Name: Box62\_8-6\_Edge

Status Passphrase: ●●●●●●

Configuration Passphrase: ●●●●●●

Shared Secret: 10,Tdk\6=+LZT4n&'3DVQAk@0U}A98

Lease Time: 60 minutes

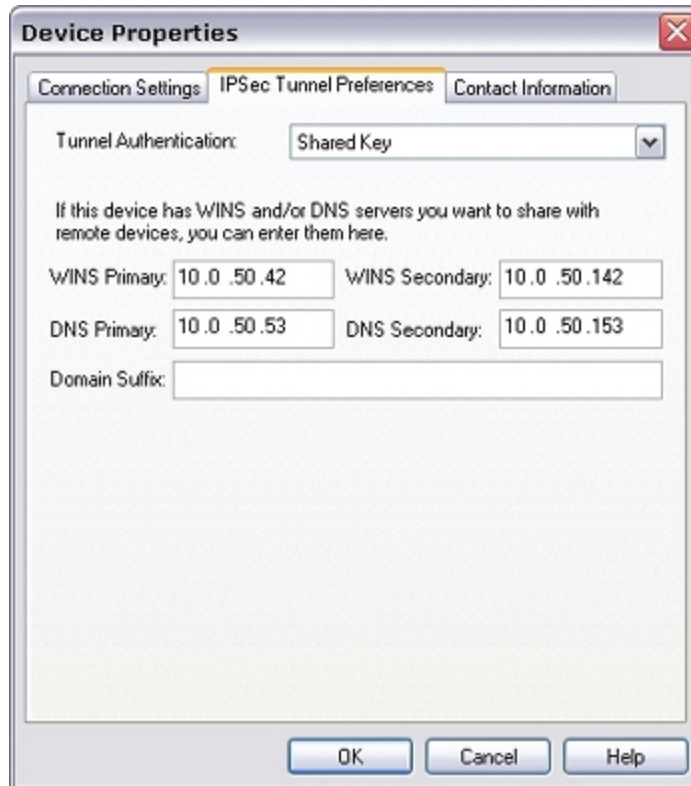
OK Cancel Help

7. Type the status and configuration passphrases for the XTM device.
8. In the **Shared Secret** text box, type the shared secret between the device and the Management Server.
9. In the **Lease Time** text box, type or select the Management Server lease time. This is the time interval at which the managed device contacts the Management Server for updates. The default is 60 minutes.

## IPSec Tunnel Preferences

In the **Device Properties** dialog box:

1. Select the **IPSec Tunnel Preferences** tab.



2. (Does not appear for Edge v10.0 or older) From the **Tunnel Authentication** drop-down list, select either **Shared Key** or **IPSec Firebox Certificate**. The second option uses the certificate for the XTM device.

For more information about certificates, see *Certificates for Branch Office VPN (BOVPN) Tunnel Authentication* on page 876.

3. If you want your managed device to get its WINS and DNS settings through the IPSec BOVPN tunnel, type the primary and secondary addresses for the **WINS** and **DNS** servers. Otherwise, you can leave these fields blank.

You can also type a domain suffix in the **Domain Name** text box for a DHCP client to use with unqualified names such as *kunstler\_mail*.

## Contact Information

On the **Device Management** page for your XTM device, you can see the current entries in the Contact List and edit those entries. If you want to add a new entry in the Contact List for your managed device, you must first add it to the Management Server contact list.

For more information, see *Manage Customer Contact Information* on page 612.

In the **Device Properties** dialog box:

1. Select the **Contact Information** tab.  
*A list of contact information for remote devices appears.*
2. To see entries in the contact list or edit an existing entry, click **Contact List**.  
*The Contact List appears.*
3. To edit an entry, double-click the entry you want to edit.  
*The Contact Information dialog box appears.*



The screenshot shows a 'Contact Information' dialog box with the following fields and values:

Name:	Admin
Phone:	206.613.6600
Cellular:	206-250-6673
Pager:	
Fax:	
E-mail:	admin@mywatchguard.com
Web:	www.mywatchguard.com
Address:	505 Fifth Avenue South Suite 500 Seattle, WA 98104 United States
Notes:	

Buttons: OK, Cancel, Help

4. Make any changes and click **OK**.  
*The updated entry appears in the Contact List dialog box.*
5. Click **OK**.

---

## Schedule Tasks for Managed Devices

You can use WatchGuard System Manager (WSM) to schedule three specific types of tasks for your managed Firebox or XTM devices: OS (operating system) updates, feature key synchronization, and device reboots. OS updates for Firebox or XTM devices must be installed on the Management Server. You can download OS updates from LiveSecurity when you update the WSM software. You can also use WSM to get the most recent feature key for each of your managed Firebox or XTM devices from LiveSecurity. With the Schedule Reboot task, you can select to reboot one or more of your managed Firebox X Edge or XTM devices at a specific time.

When you schedule a task, you can set it to occur immediately or at a time in the future. For example, you can schedule an update for your Firebox or XTM device OS every Friday at midnight, schedule to synchronize your feature key the last day of each month, and reboot specific managed devices on the first of each month.

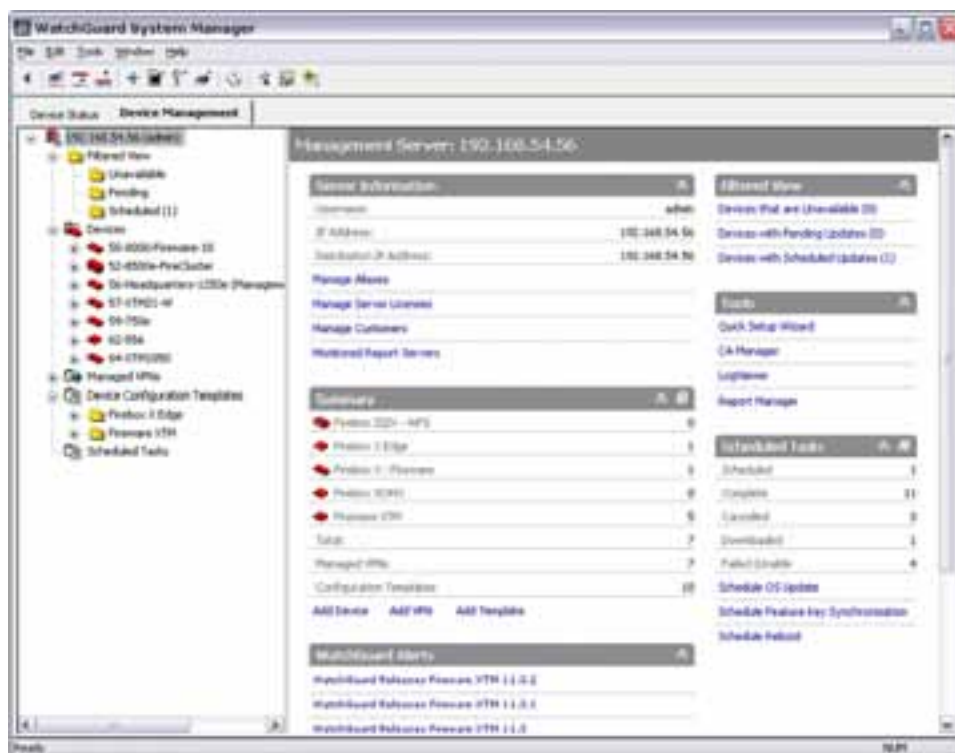
There are a couple of limitations for scheduled OS updates. You cannot schedule an OS update for any device that is a member of a FireCluster. Also, do not include the Management Server gateway Firebox in a scheduled OS update with other devices. If you want to schedule an OS update for your gateway Firebox, make sure to schedule it as a separate task.

You can use WSM to schedule configuration updates to your fully managed Firebox or XTM devices. These configuration updates are scheduled from Policy Manager rather than from the **Scheduled Tasks** page. For more information about how to schedule these updates, see *Update the Configuration For a Fully Managed Device* on page 608.

The current status of all scheduled tasks appears on the **Device Management** tab, in the **Scheduled Tasks** page.

To schedule a new task, from WatchGuard System Manager:

1. Select the **Device Management** tab.
2. In the left navigation bar, select the Management Server for the devices you want to update.  
*The Management Server page appears. The number of scheduled tasks appears in the Scheduled Tasks section at the right side of the page.*



3. In the **Scheduled Tasks** section, select a task to schedule.
4. Use the instructions in the subsequent topics to complete the selected task:
  - *Schedule OS Update*
  - *Schedule Feature Key Synchronization*
  - *Schedule Reboot*

When the task is scheduled, the task appears on the **Scheduled Tasks** page with a separate **Task ID** for each device included in the task. Although each device has a separate row in the list, you cannot select an individual device for a scheduled task. Any actions you take apply to all devices in the scheduled task.

For more information about how to see details for all scheduled tasks, or to cancel or delete a scheduled task, see *Review, Cancel, or Delete Scheduled Tasks* on page 606.

## Schedule OS Update

You can use the WatchGuard System Manager Update OS Wizard to schedule an update of the OS (operating system) for one or more of your managed devices. Before you begin, make sure that the OS update file for the managed device you want to update is installed on your Management Server. You cannot schedule an OS update if the update file is not installed on the Management Server. Before a scheduled OS update for a device is complete, the device reboots.

## Install an OS Update

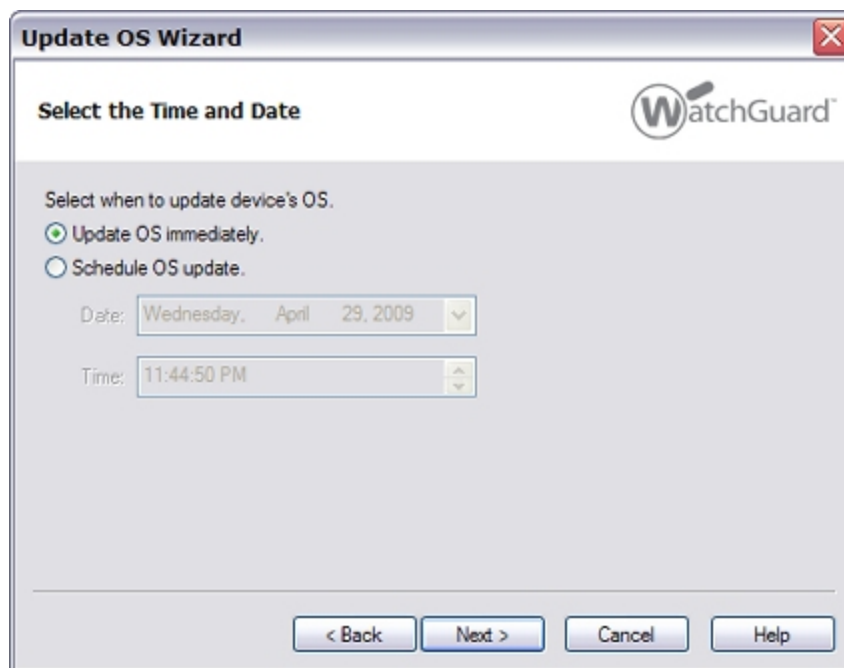
To install the automatic OS update on your Management Server:

1. Open a web browser and go to the [Software Downloads page](#) on the WatchGuard web site.
2. Download the OS update file for your Firebox or XTM device to your management computer (the computer where your Management Server is installed).  
*This is an EXE file. For example, XTM\_OS\_1050\_11\_1.exe.*
3. Go to the location on your management computer where you saved the EXE file, and double-click the file to run it and install the OS on your management computer.

## Schedule an OS Update Task

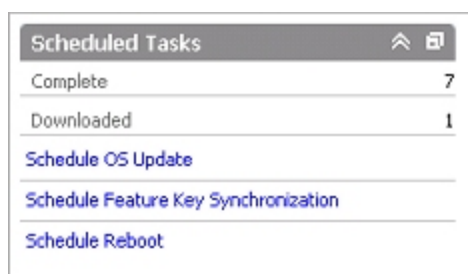
In the **Scheduled Tasks** section:

1. Click **Schedule OS Update**.  
*The Update OS wizard starts.*
2. Read the Welcome message and click **Next**.  
*The Select the device page appears.*
3. Select the **Device Type** from the drop-down list and click **Next**.  
*The Select the devices page appears.*
4. Select the check box for each Firebox or XTM device that you want to update and click **Next**.  
*The Select the OS version page appears.*
5. Select an **OS Version** from the drop-down list and click **Next**.  
*The Select the Time and Date page appears.*



6. To update the OS immediately, select **Update OS immediately**.  
To schedule the update for a future time, select **Schedule OS update**.

7. If you selected **Schedule OS update**, select the date from the **Date** drop-down list, and set the time in the **Time** text box.
8. Click **Next**.  
*The Schedule the OS update page appears.*
9. Click **Next**.  
*The Update OS Wizard is complete page appears.*
10. Click **Close** to finish the wizard.  
*The OS is updated if you selected Update OS immediately, or scheduled if you selected Schedule OS update.  
The number of scheduled tasks appears in the Scheduled Tasks section.*



When the scheduled OS update occurs, the Management Server updates the Firebox or XTM device OS and reboots the device.

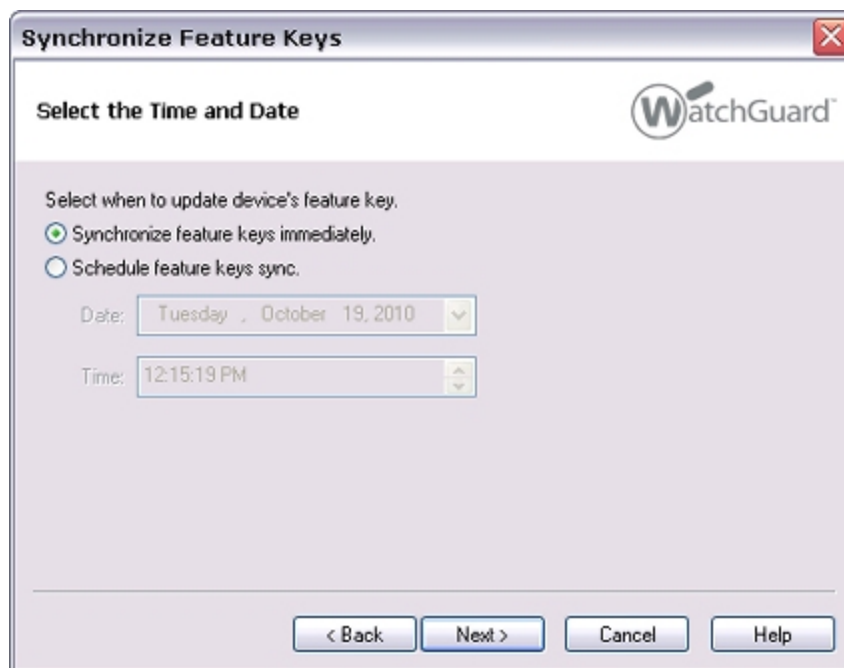


## Schedule Feature Key Synchronization

You can use your Management Server to schedule a feature key synchronization for one or more of your managed devices.

In the **Scheduled Tasks** section:

1. Click **Schedule Feature Key Synchronization**.  
*The Synchronize Feature Keys wizard starts.*
2. Read the Welcome message and click **Next**.  
*The Select the devices page appears.*
3. Select the check box for each managed device with a feature key to synchronize. Click **Next**.  
*The Select the Time and Date page appears.*



4. To synchronize feature keys immediately, select **Synchronize Feature Keys immediately**.  
To schedule the feature keys to synchronize at a future time, select **Schedule feature keys sync**:
  - a. From the **Date** drop-down list, select the date.
  - b. In the **Time** text box, set the time.
5. Click **Next**.  
*The Schedule the Feature Keys Synchronization page appears.*
6. Click **Next**.  
*The Synchronize Feature Keys Wizard is complete page appears.*
7. Click **Close** to finish the wizard.  
*The feature keys are synchronized if you selected Synchronize Feature Keys immediately, or scheduled if you selected Schedule feature keys sync. The number of scheduled tasks appears in the Scheduled Tasks section.*



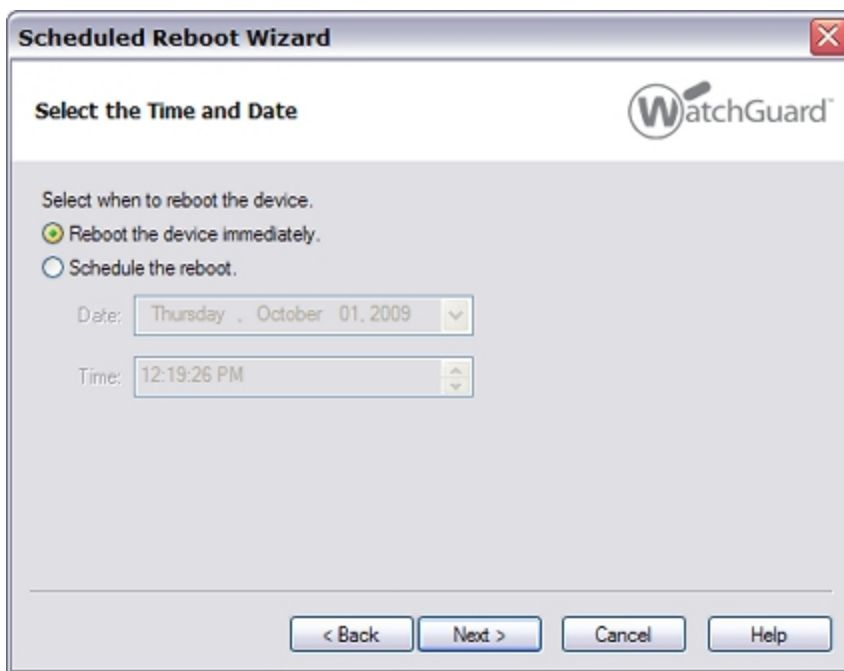
## Schedule Reboot

You can use the WatchGuard System Manager Schedule Reboot wizard to reboot one or more of your managed Firebox X Edge v10.x or Fireware XTM devices. You can choose to schedule a reboot for an individual device, or you can schedule a reboot for a group of devices.

### Schedule a Reboot for an Individual Device

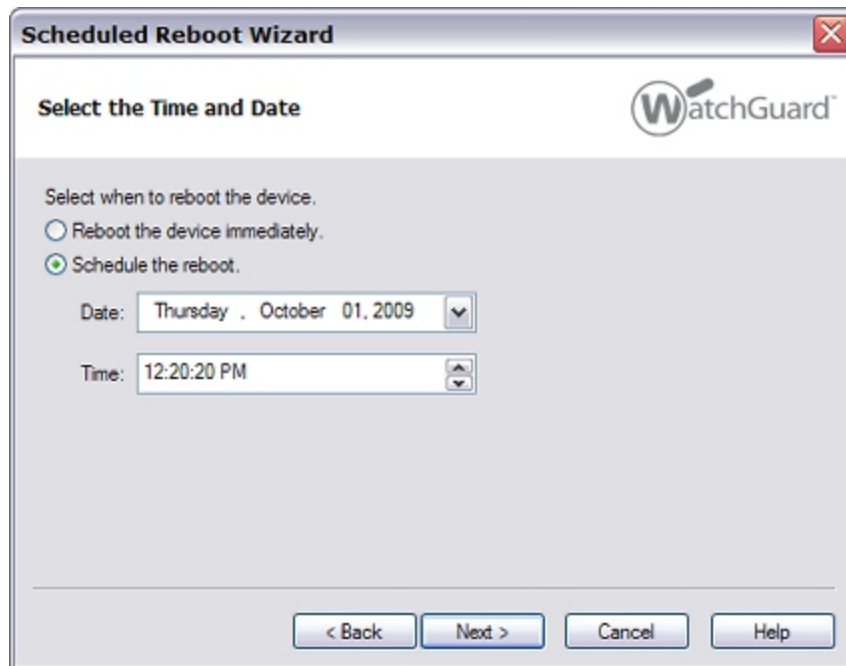
When you schedule a reboot for an individual device, the Schedule Reboot Wizard launches, but you cannot select to include other devices in the scheduled reboot.

1. In the left navigation bar, expand the **Devices** tree.
2. Select the device for which you want to schedule a reboot.
3. Right-click the device, and select **Schedule Reboot**.  
*The Scheduled Reboot Wizard appears.*
4. Read the Welcome message and click **Next**.  
*The Select the Time and Date page appears.*



5. To reboot the device immediately, select **Reboot the device immediately**.  
To schedule the device to reboot at a future time, select **Schedule the reboot**:

- a. From the **Date** drop-down list, select the date.
- b. In the **Time** text box, set the time.

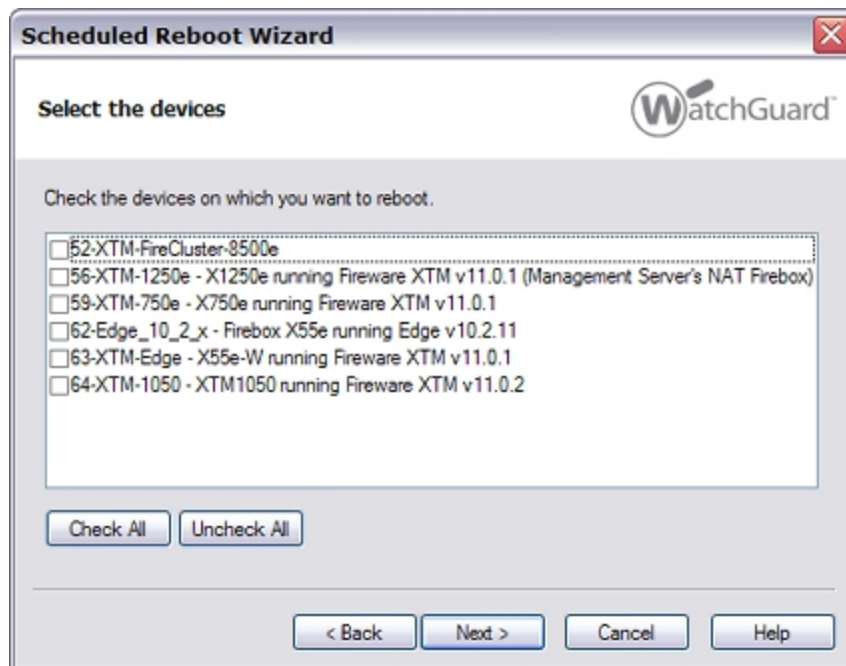


7. Click **Next**.  
*The Schedule the Reboot page appears.*
8. Click **Next**.  
*The Scheduled Reboot Wizard is complete page appears.*
9. Click **Close** to finish the Wizard.  
*The device is rebooted you selected Reboot the device immediately, or scheduled if you selected Schedule the reboot. The number of scheduled tasks appears in the Scheduled Tasks section.*

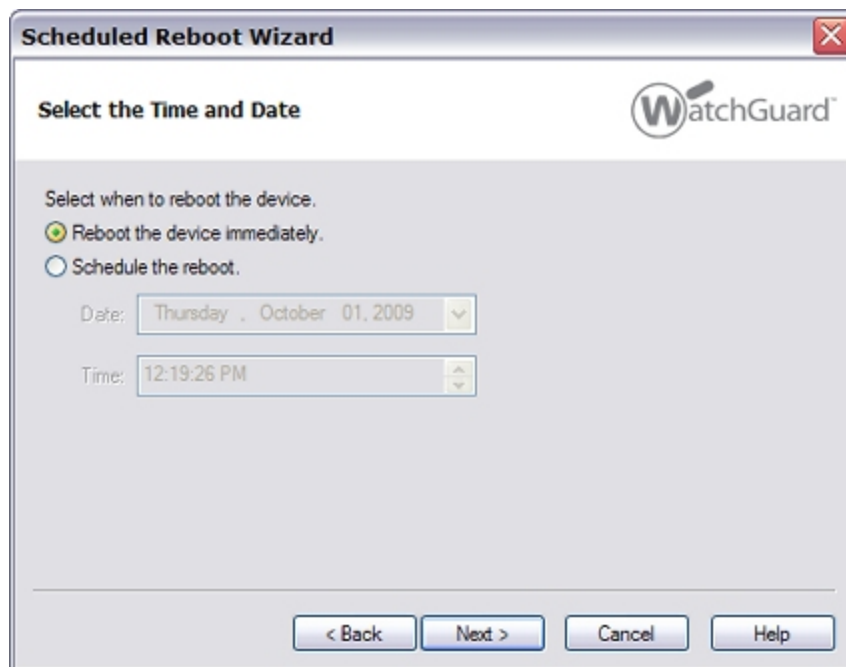
## Schedule a Reboot for One or More Devices

You can schedule a reboot for more than one device at the same time.

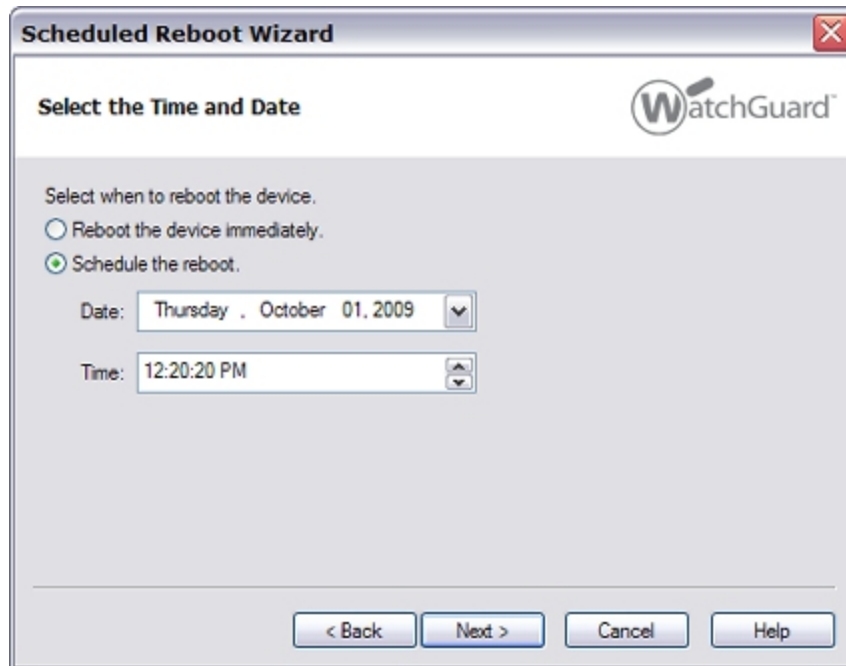
1. On the **Management Server** page, in the **Scheduled Tasks** section, click **Schedule Reboot**.  
Or, in the **Device Management** tree, right-click **Scheduled Tasks** and select **Schedule Reboot**.  
Or, on the **Scheduled Tasks** page, click **Add** and select **Schedule Reboot**.  
*The Scheduled Reboot Wizard appears.*
2. Read the Welcome message and click **Next**.  
*The Select the devices page appears.*



3. Select the check box for each device you want to reboot and click **Next**.  
*The Select the Time and Date page appears.*



4. To reboot the device immediately, select **Reboot the device immediately**.  
To schedule the device to reboot at a future time, select **Schedule the reboot**.
5. If you selected **Schedule the reboot**, select the date from the **Date** drop-down list, and set the time in the **Time** text box.



6. Click **Next**.

*The Schedule the Reboot page appears.*

7. Click **Next**.

*The Scheduled Reboot Wizard is complete page appears.*

8. Click **Close** to finish the wizard.

*The device is rebooted you selected Reboot the device immediately, or scheduled if you selected Schedule the reboot. The number of scheduled tasks appears in the Scheduled Tasks section.*

Scheduled Tasks	
Complete	7
Downloaded	1
<a href="#">Schedule OS Update</a>	
<a href="#">Schedule Feature Key Synchronization</a>	
<a href="#">Schedule Reboot</a>	

## Review, Cancel, or Delete Scheduled Tasks

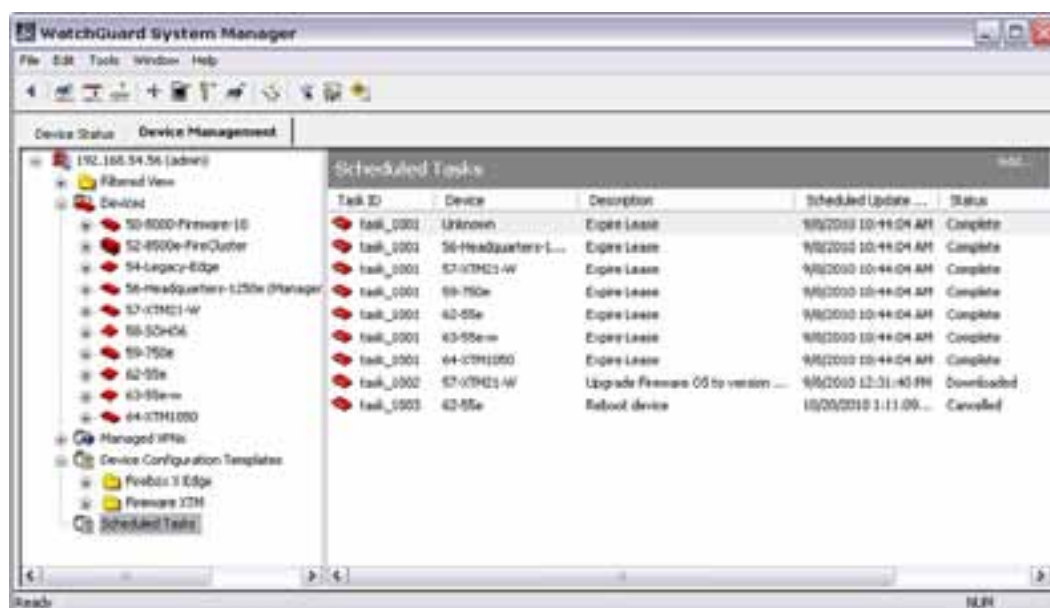
After you have scheduled WatchGuard System Manager (WSM) to update the OS or synchronize the feature keys for your managed devices, you can review, cancel, or delete these Scheduled Tasks. You cannot edit a Scheduled Task. If you want to change the properties of a task you have created, you must delete that task and schedule a new task. When you include more than one device in a scheduled task, any changes you make to the scheduled task affect all the devices included in the task. Each task has a unique Task ID and appears on a separate line for each device, even if more than one device is included in the same update. For this reason, when you select a device in the **Scheduled Tasks** list, all devices included in that scheduled update are selected.

For more information about how to schedule a new task, see *Schedule Tasks for Managed Devices* on page 597.

## Review Scheduled Tasks

1. Open WSM and [connect to a Management Server](#).
2. On the **Device Management** tab, in the left navigation bar, select **Scheduled Tasks**.

*The Scheduled Tasks page appears.*



2. Review the tasks in the **Scheduled Tasks** list.
3. Cancel, delete, or add a new task as necessary.
  - To delete a scheduled task, right-click a device and select **Remove Scheduled Update**.  
*The update is removed from the schedule for all devices included in that update.*
  - To cancel a scheduled update, right-click a device and select **Cancel Scheduled Update**.  
*The task stays in the schedule, but the status changes to Cancelled. You can remove the task later, but you cannot activate it again.*
  - To add a scheduled OS update, click **Add** and select **Add OS Update**.  
Or, right-click and select **Add OS Update**.  
*The Update OS Wizard starts.*

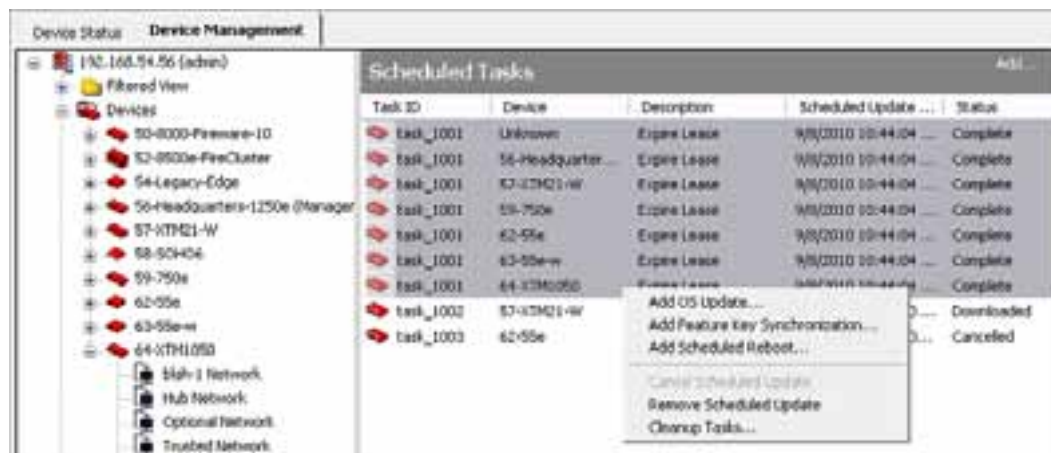
- To schedule Feature Key Synchronization, click **Add** and select **Add Feature Key Synchronization**.  
Or, right-click and select **Add Feature Key Synchronization**.  
*The Synchronize Feature Keys Wizard starts.*
- To schedule a device reboot, click **Add** and select **Schedule Reboot**.  
*The Schedule Reboot Wizard starts.*

## Clean up Scheduled Tasks

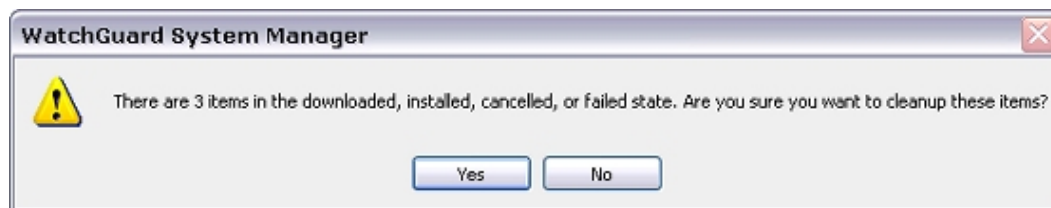
The Scheduled Tasks list shows all the OS Update, Feature Key Synchronization, and Scheduled Reboot tasks for your Management Server. If your Scheduled Tasks list includes tasks with a status of **Cancelled**, **Downloaded**, **Installed**, or **Failed**, you can use the procedure in the previous section to delete each task individually, or you can remove them all at one time.

To clean up all outstanding Scheduled Tasks at one time:

1. Open WSM and [connect to a Management Server](#).
2. On the **Device Management** tab, in the left navigation bar, select **Scheduled Tasks**.  
*The Scheduled Tasks page appears.*
3. In the **Scheduled Tasks** window, right-click anywhere.  
*The right-click menu appears.*



4. Select **Cleanup Tasks**.  
*A warning message appears.*

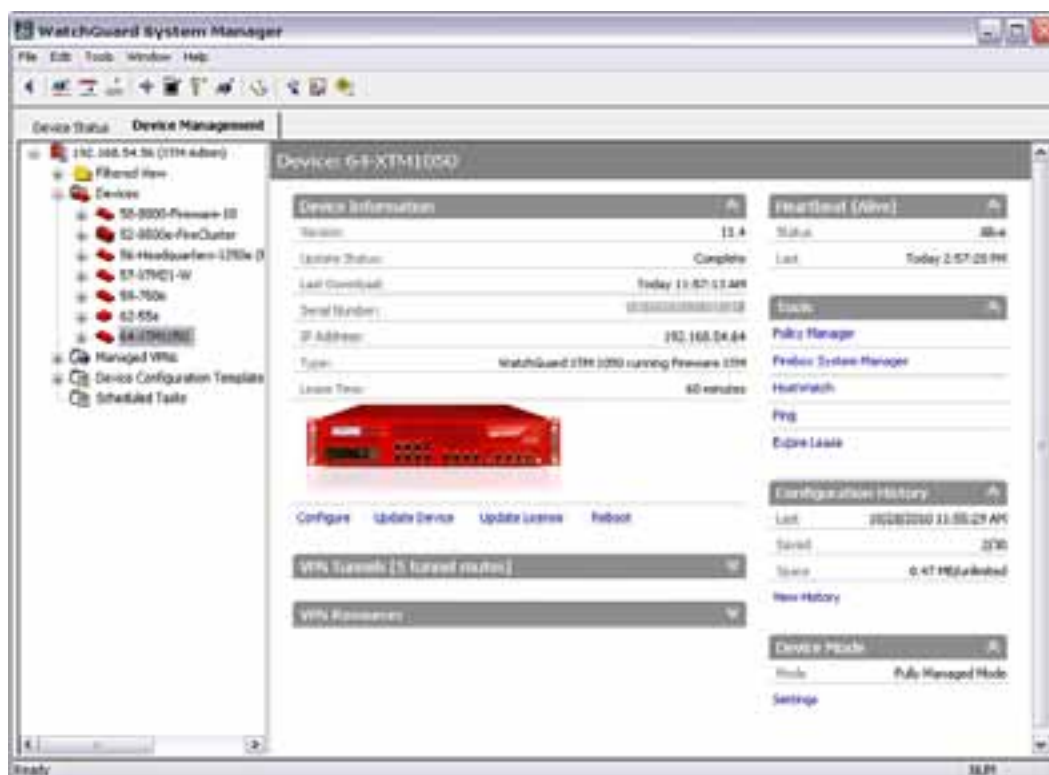


5. Click **Yes**.  
*All downloaded, installed, cancelled, and failed tasks are deleted from the list. Only tasks with a status of Scheduled remain.*

## Update the Configuration For a Fully Managed Device

To change the configuration for any Firebox or XTM device that is fully managed by your Management Server, you must start Policy Manager for that device from the WatchGuard System Manager (WSM) Device Management tab.


1. Use WSM to Connect to your Management Server on page 578
2. Expand the **Devices** list and select a Firebox X Edge or Firewall XTM device.  
*The Device page appears for the device you selected.*



3. In the **Tools** section, click **Policy Manager**.  
*Policy Manager opens the configuration file for the device you selected.*
4. Update the configuration file with your changes.
5. Save the configuration to a file or to the Management Server.


For more information about the available options you can use to save the configuration, see the subsequent sections.

To save the configuration to a file:

1. Click .
- The Save dialog box appears.*
2. In the **File name** text box, type a name for the configuration file.
3. Select the directory where you want to save the configuration file.
4. Click **Save**.  
*The configuration is saved to a file in the location you specified.*



To save the configuration to the Management Server:

1. Click .
 

*The Schedule Configuration Update Wizard appears.*
2. Click **Next** to start the wizard.
 

*The Select the Time and Date page appears.*
3. Select when to update the configuration file:
  - **Update configuration immediately**
  - **Schedule configuration update**
4. If you selected to schedule the update, select the **Date** and **Time** for the update.
5. Click **Next**.
 

*The Schedule Configuration Update Wizard is complete page appears.*
6. Click **Finish** to close the wizard.
 

*A message that the configuration was saved to the Management Server appears. If you scheduled an update, the date for the scheduled update appears in the Update Status field on the Device page for the device, and on the main Devices page.*

## About Filtered View

The Management Server Filtered View enables you to see information about your managed devices, grouped by status, and scheduled tasks. The available categories are:

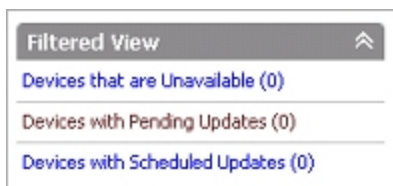
- **Unavailable** — Devices appear in this category when the Management Server cannot connect to them. This information is also available in the **Heartbeat** section of the device page.
- **Pending** — Devices appear in this category if there are scheduled configuration tasks for the device that are in progress.
- **Scheduled** — Devices appear in this category if there are configuration tasks scheduled for the device at a future time.

The scheduled tasks that appear on the pending and scheduled pages include configuration file and managed tunnel updates for an individual device. Scheduled OS updates, template application, lease expiration, and reboot tasks do not appear on the **Filtered View** pages.

You can see these categories in two places: on the **Management Server** page in the **Filtered View** section and on the individual **Filtered View** pages. The **Filtered View** page for each category includes these details:

- Name of the device
- Type of device (OS version)
- Heartbeat status
- Last time the device contacted the Management Server
- IP address of the device
- Time the device configuration was last modified

On the main **Management Server** page, the **Filtered View** section includes a summary of how many devices are included in each category, with the number of each devices in the category in parenthesis.



To see more details about the devices that appear in each filtered view, you can open a **Filtered View** page from the **Management Server** page or from the **Filtered View** list in the left navigation pane.

To open a **Filtered View** page from the **Management Server** page:

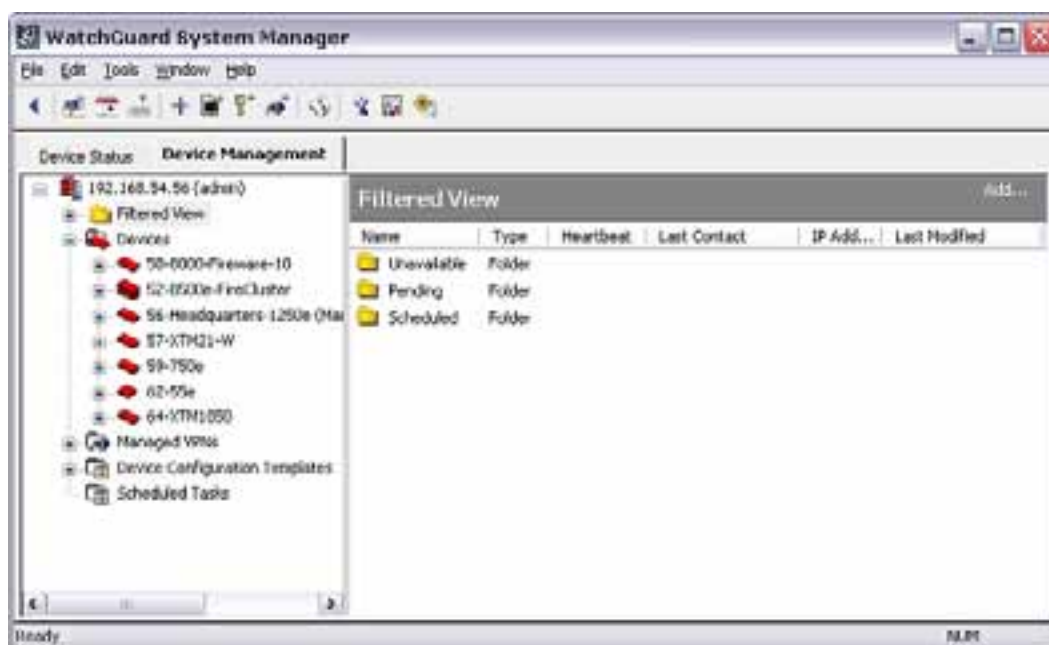
1. Connect to a Management Server and select the **Device Management** tab.
2. In the left navigation pane, select the Management Server.  
*The Management Server page appears.*
3. In the **Filtered View** section, double-click a device category:
  - **Devices that are Unavailable**
  - **Devices with Pending Updates**
  - **Devices with Scheduled Updates**

*The Filtered View page you selected appears.*

To open a **Filtered View** page from the **Filtered View** list in the left navigation pane:

1. Connect to a Management Server and select the **Device Management** tab.
2. In the left navigation pane, select **Filtered View**.

*The Filtered View page appears with the list of available folders.*



3. On the **Filtered View** page, double-click a folder.  
Or, in the left navigation pane, expand the **Filtered View** list and select a folder.  
*The selected Filtered View page appears.*
4. To open the device page for a device that appears on a filtered view page, double-click the device.  
*The device page appears.*

## Manage Server Licenses

You can use WatchGuard System Manager (WSM) to manage the licenses for your Management Server. You can add or delete license keys, and see the current license key information, including how many devices your license keys allow you to manage.

### Review Current License Key Information

1. Start WatchGuard System Manager and Use WSM to Connect to your Management Server.  
*The Management Server page appears.*
2. In the **Server Information** section, click **Manage Server Licenses**.  
Or, select **File > Manage Server Licenses**.  
*The Management Server Licenses dialog box appears.*



### Add or Remove a License Key

To add a license key:

1. In the **Management Server Licenses** dialog box, click **Add**.  
*The Add License Key dialog box appears.*



2. In the **License Key** text box, type or paste the license key.
3. Click **OK**.  
*The license key you added appears in the License Keys window and the number of licensed devices is updated.*

To remove a license key:

1. In the **License Keys** list, select the license key to remove.
2. Click **Remove**.

*The license key is deleted from the License Keys window and the number of licensed devices is updated.*

## Save or Discard Your Changes

After you have added or removed any license keys, you can save or discard your changes.

In the **Management Server Licenses** dialog box:

- To save your changes, click **OK**.
- To close the dialog box and discard any changes, click **Cancel**.

## Manage Customer Contact Information

You can use WatchGuard System Manager (WSM) to manage the *Contact List* for your Management Server. After you add contacts to the Contact List, you can add information for those contacts to each of your managed XTM devices.

For more information about how to add a contact to your managed XTM device, see *Set Device Management Properties* on page 593.

## Add a Contact to the Management Server

You can add a new contact to the Management Server Contact List at any time.

1. *Use WSM to Connect to your Management Server.*  
*The Management Server page appears.*
2. In the **Server Information** section, click **Manage Customers**.  
*The Contact List dialog box appears.*
3. To add a contact to the list, click **Add**.  
*The Contact Information dialog box appears.*
4. Type the necessary information in each text box. All of the information is optional.
5. Click **OK**.  
*The new contact appears in the Contact List.*
6. To add another contact, repeat Steps 3–5.
7. Click **OK** when you are finished.

## Edit a Contact in the Contact List

You can change any of the information for a current entry in the Contact List.

1. *Use WSM to Connect to your Management Server.*  
*The Management Server page appears.*
2. In the **Server Information** section, click **Manage Customers**.  
*The Contact List dialog box appears.*
3. In the **Contact List** dialog box, select the entry you want to change.
4. Click **Edit**.  
*The Contact information dialog box appears.*

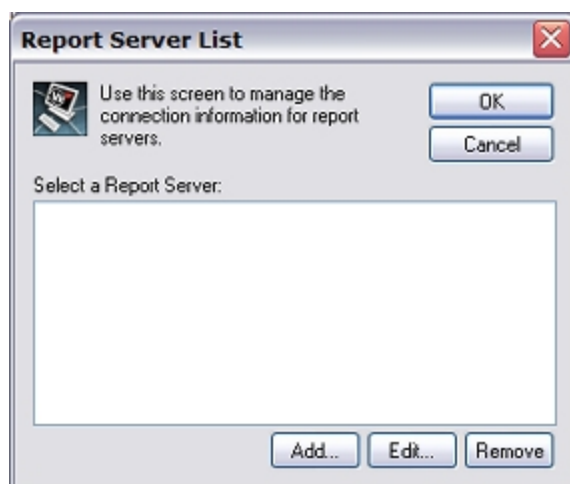
5. Update the necessary information.
6. Click **OK**.
7. Make any necessary changes and click **OK**.  
*The updated entry appears in the Contact List dialog box.*
8. To edit another contact, repeat Steps 1–5.
9. Click **OK**.

## Review and Manage the Monitored Report Servers List

The Monitored Report Servers List is used to configure the list of Report Servers that are on a different computer than your WatchGuard Log Server. When you install the Log Server and Report Server on different computers, your Management Server contacts the Report Servers in the Report Server List to find the associated Log Servers. Then, when you use WatchGuard System Manager (WSM) to connect to Report Manager, it connects to the appropriate Report Server.

You can use WSM to see and manage the connection information for your WatchGuard Report Servers. You can add a new Report Server, change the IP address or port for an existing Report Server, or remove a Report Server from the list.

1. Open WSM and [connect to your Management Server](#).  
*The Management Server page appears.*
2. In the **Server Information** section, click **Monitored Report Servers**.  
*The Report Server List dialog box appears.*



3. Use the instructions in the subsequent sections to add, edit, or remove a Report Server.

## Add a Report Server to the List

1. In the **Report Server List** dialog box, click **Add**.  
*The Report Server dialog box appears.*



2. In the **IP Address** text box, type the IP address of the Report Server.
3. In the **Port** text boxy, type the port to use for Report Server access.
4. Click **OK**.
5. Repeat Steps 1–4 to add more Report Servers to the list.

## Edit Information for a Report Server

1. In the **Report Server List** dialog box, select a report server in the list.
2. Click **Edit**.  
*The Report Server dialog box appears.*



3. Edit the **IP Address** or **Port** for the Report Server.
4. Click **OK**.

## Remove a Report Server from the List

1. In the **Report Server List** dialog box, select the Report Server to remove.
2. Click **Remove**.

*The Report Server is removed from the list.*

## Add and Manage VPN Tunnels and Resources

You can use WatchGuard System Manager to manage VPN tunnels for your managed XTM devices. In the **VPN Tunnels** section of the **Device** page, you can see all tunnels that include the selected XTM device. You can also add, edit, or remove a VPN tunnel.

### See VPN Tunnels

From WatchGuard System Manager:

1. Use *WSM to Connect to your Management Server*.
2. Select the **Device Management** tab.
3. Expand the **Devices** list.
4. Select a device.

*The Device Management page for the selected XTM device appears.*

5. Find the **VPN Tunnels** section.

*This section shows all tunnels for which this device is a VPN endpoint.*

Name	Remote Gateway
57-XTM21-W(Trusted Network)-64-XTM1050(blah-1 Network)	57-XTM21-W
64-XTM1050-56-Headquarters-1250e	56-Headquarters-1250e

Add... Edit... Remove...

### Add a VPN Tunnel

In the **VPN Tunnels** section:

1. Click **Add**.  
*The Add VPN Wizard starts.*
2. Complete the **Add VPN Wizard** to configure your VPN tunnel.

After you add a VPN tunnel to your configuration, the VPN tunnel appears in the list, and the number of configured VPN tunnels appears adjacent to the **VPN Tunnels** section title.

**Note** *If you add more tunnels than your license allows, a warning message that you have exceeded your licensed number of tunnels appears. You must remove enough VPN tunnel routes from your configuration to return to your licensed limit.*

For more information about the Add VPN Wizard, see *Make Managed Tunnels Between Devices* on page 908.

## Edit a VPN Tunnel

After you have added a VPN tunnel, you can use WSM to change the tunnel configuration. You cannot change either of the tunnel endpoints. If you want to change the XTM device that is at one or both ends of the VPN tunnel, you must create a new tunnel.

In the **VPN Tunnels** section:

1. In the **Name** list, select a VPN tunnel.
2. Click **Edit**.  
*The VPN Properties dialog box appears.*
3. Make the changes to your VPN tunnel.

For more information on the changes you can make to your VPN tunnel, see *Edit a Tunnel Definition* on page 908.

4. Click **OK**.  
*The updated VPN tunnel appears in the Name list.*



## Remove a VPN Tunnel

In the **VPN Tunnels** section:

1. In the **Name** list, select a tunnel.
2. Click **Remove**.  
*A confirmation message appears.*
3. If you do not the configuration changes to occur immediately, clear the **Restart devices now to expire leases and download new configuration** check box.
4. Click **Yes**.  
*The VPN tunnel is removed from the list and the device is restarted.*

## Add a VPN Resource

You can configure, and put a limit to, the networks that have access through your VPN tunnels. You can make a VPN between hosts or networks. You can also define VPN resources to configure the networks that are available through a given VPN device.

The **Device Management** tab lists all of your currently defined VPN resources.

For detailed instructions to add VPN resources, see *Add VPN Resources* on page 901.

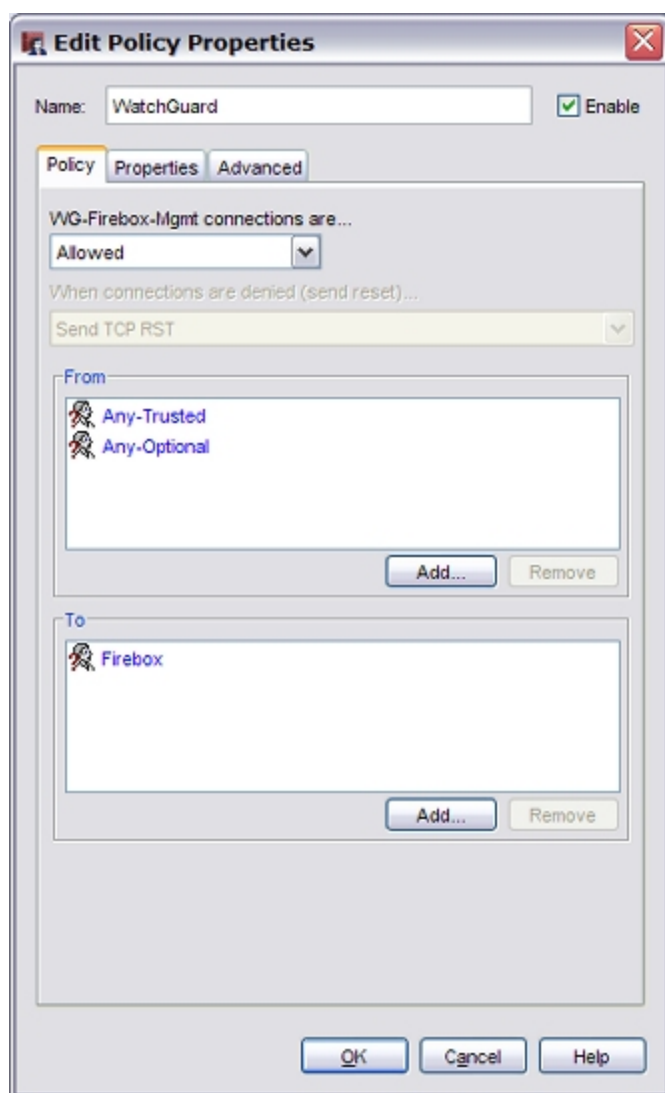
## Configure an XTM Device as a Managed Device

If your XTM device has a dynamic IP address, or if the Management Server cannot connect to it for another reason, you can configure the XTM device as a managed device before you add it to the Management Server. You can then *Add Managed Devices to the Management Server*.

### Edit the WatchGuard Policy

1. Open *Policy Manager* for the XTM device you want to enable as a managed device.
2. Double-click the **WatchGuard** policy to open it.

*The Edit Policy Properties dialog box for the WatchGuard policy appears.*



3. In the **WG-Firebox-Mgmt connections are** drop-down list, make sure **Allowed** is selected.
4. In the **From** section, click **Add**.  
*The Add Address dialog box appears.*
5. Click **Add Other**.  
*The Add Member dialog box appears.*

6. In the **Choose Type** drop-down list, select **Host IP**.
7. In the **Value** text box, type the IP address of the external interface of the gateway Firebox.  
If you do not have a gateway Firebox that protects the Management Server from the Internet, type the static IP address of your Management Server.
8. Click **OK** to close the **Add Member** dialog box.
9. Click **OK** to close the **Add Address** dialog box.
10. Make sure the **To** section includes an entry of either **Firebox** or **Any**.
11. *Save the Configuration File.*

You can now add the device to your Management Server configuration as described in *Add Managed Devices to the Management Server*. When you add this XTM device to the Management Server configuration, the Management Server automatically connects to the static IP address and configures the XTM device as a managed device.

## Set Up the Managed Device

(Optional) If your XTM device has a dynamic IP address, or if the Management Server cannot find the IP address of the XTM device for any reason, you can use this procedure to prepare your XTM device to be managed by the Management Server.

1. Select **Setup > Managed Device Settings**.  
*The Managed Device Settings dialog box appears.*

**Managed Device Settings**

**Centralized Management**

Select this check box to make this a Managed Device. To complete this operation, configure this device for Centralized Management using WatchGuard System Manager.

Managed Device Name:

Management Server IP Address(es):

Shared Secret:

Confirm:

Management Server CA Certificate:

2. To set up an XTM device as a managed device, select the **Centralized Management** check box.
3. In the **Managed Device Name** text box, type the name you want to give the XTM device when you add it to the Management Server configuration.

This name is case-sensitive and must match the name you use when you add the device to the Management Server configuration.

4. In the **Management Server IP Address(es)** list, select the IP address of the Management Server if it has a public IP address.

Or, select the public IP address of the gateway Firebox for the Management Server.

5. To add an address, click **Add**.

The XTM device that protects the Management Server automatically monitors all ports used by the Management Server and forwards any connection on these ports to the configured Management Server. When you use the Management Server Setup Wizard, the wizard adds a *WG-Mgmt-Server* policy to your configuration to handle these connections. If you did not use the Management Server Setup Wizard on the Management Server, or, if you skipped the **Gateway Firebox** step in the wizard, you must manually add the *WG-Mgmt-Server* policy to the configuration of your gateway Firebox.

6. In the **Shared Secret** and the **Confirm** fields, type the shared secret.

The shared secret you type here must match the shared secret you type when you add the XTM device to the Management Server configuration.

7. Click **Import** and import the CA-Admin.pem file as your certificate. This file is in  
  \My Documents\My WatchGuard\certs\[device\_ip\_address].
8. Click **OK**.

When you save the configuration to the XTM device, the XTM device is enabled as a managed device. The managed XTM device tries to connect to the IP address of the Management Server on TCP port 4110. Management connections are allowed from the Management Server to this managed XTM device.

You can now add the device to your Management Server configuration, as described in *Add Managed Devices to the Management Server* on page 590.

You can also use WSM to configure the management mode for your device, as described in *About Centralized Management Modes* on page 586.

## Configure a Firebox III or Firebox X Core Running WFS as a Managed Device

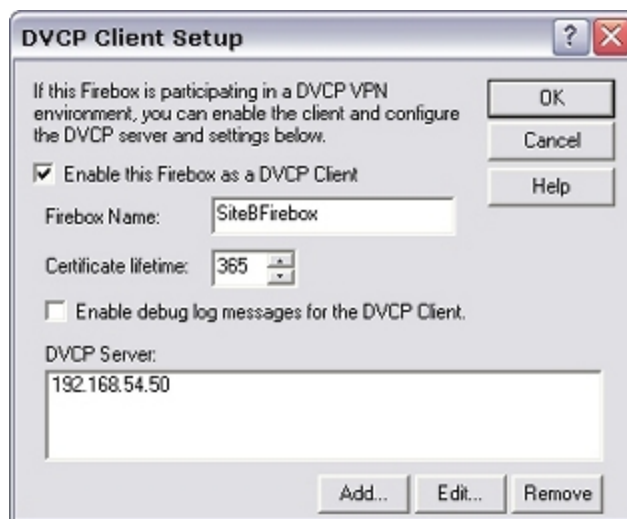
You can configure your Firebox III or Firebox X Core running WFS to be managed by your Management Server.

1. Open Policy Manager for the Firebox you want to enable as a managed device.
2. Double-click the **WatchGuard** policy to open it.  
*The Edit Service Properties dialog box for the WatchGuard policy appears.*
3. On the **Incoming** tab, make sure that incoming WatchGuard connections are set to **Enabled and Allowed**.
4. Below the **From** dialog box, click **Add**.  
*The Add Address dialog box appears.*

5. Click **Add Other**.  
The Add Member dialog box appears.
6. In the **Choose Type** drop-down list, select **Host IP Address**.
7. In the **Value** field, type the IP address of the external interface of the gateway Firebox that protects the Management Server from the Internet.  
If you do not have a gateway Firebox that protects the Management Server from the Internet, type the static IP address of your Management Server.
8. Click **OK** to close the **Add Member** dialog box.
9. Click **OK** to close the **Add Address** dialog box.
10. Make sure the **To** dialog box includes an entry of either **Firebox** or **Any**.

**Note** *If the Firebox you want to manage has a static IP address on its external interface, you can stop here. Save the configuration to this Firebox. You can now add the device to your Management Server configuration. When you add this Firebox to the Management Server configuration, the Management Server automatically connects to the static IP address and configures the Firebox as a managed Firebox client. If the Firebox you want to manage has a dynamic IP address, go on to Step 11.*

11. From Policy Manager, select **Network > DVCP Client**.
12. Select the **Enable this Firebox as a DVCP Client** check box.
13. In the **Firebox Name** field, type the name of the Firebox.  
The Firebox name is case-sensitive. The name you type here must match the name you type when you add this Firebox to the Management Server configuration.



14. To send log messages for the managed client, select the **Enable debug log messages for the DVCP Client** check box.  
We recommend you select this option only when troubleshooting.
15. Click **Add** to add the Management Server the Firebox connects to.  
*The DVCP Server Properties dialog box appears.*
16. In the **IP address** text box, type the IP address of the Management Server if it has a public IP address.  
Or, type the public IP address of the Firebox that protects the Management Server.

The Firebox that protects the Management Server automatically monitors all ports used by the Management Server and forwards any connections on these ports to the configured Management Server. The Firebox protecting the Management Server is configured to do this when you run the Management Server Setup Wizard.

If you did not use the Management Server Setup Wizard on the Management Server, or, if you skipped the *Gateway Firebox* step in the wizard, configure the gateway Firebox to forward TCP ports 4110, 4112, and 4113 to the private IP address of the Management Server.

17. Type the **Shared Secret** to use to connect to the Firebox. The shared secret you type here must match the shared secret you type when you add this device to the Management Server configuration. A Firebox can be a client of only one Management Server.
18. Click **OK** to close the **DVCP Server Properties** dialog box.
19. Click **OK** to close the **DVCP Client Setup** dialog box.
20. Save the configuration file to the Firebox.

When you save the configuration to the Firebox, the Firebox is enabled as a managed client. The managed Firebox client tries to connect to the IP address of the Management Server on TCP port 4110. Management connections are allowed from the Management Server to this managed Firebox client.

You can now add the device to your Management Server configuration as described in *Add Managed Devices to the Management Server* on page 590.

## About Edge (v10.x and Older) and SOHO Devices as Managed Devices

You can use the WatchGuard Management Server to configure and manage many Firebox X Edge and SOHO devices. For Firebox X Edge devices (version 10.x and older), you can enable Fully Managed Mode with WatchGuard System Manager (WSM), which means you can manage policies, updates, and VPNs for many Edge devices from one location. You can use both Edge and SOHO devices as endpoints for managed BOVPN tunnels.

To manage a Firebox X Edge device (version 10.x and older) with the Management Server, you must:

1. Install the Edge — Physically connect it to an Ethernet interface on your computer and run the Quick Setup Wizard to configure it.
2. *Add Managed Devices to the Management Server* — You can import multiple Edge devices at the same time.
3. Define WSM access settings on the Edge — The first three steps are covered in *Prepare a Firebox X Edge (v10.x and Older) for Management*.
4. Configure values to identify the device to the Management Server — *Add Managed Devices to the Management Server*.

To allow connections between your management computer and the Management Server for Firebox X Edge (v10.x or older) devices, you must add the *WG-SmallOffice-Mgmt* packet filter to the configuration on your gateway Firebox. If you have another firewall, make sure that you have a policy to allow traffic from managed Edge devices on TCP port 4109.

If you have added this packet filter to your configuration, and cannot connect to the Edge Web Manager from WSM, you may have a certificate error in your web browser cache. Clear the WatchGuard certificates and all cookies from your web browser certificate store, connect to your Management Server again, and then connect to the Edge Web Manager again.

## Prepare a Firebox X Edge (v10.x and Older) for Management

In its default configuration, Firebox X Edge versions before 11.x cannot be added to a WatchGuard Management Server as a managed device. Before you add a Firebox to the WatchGuard Management Server, you must make sure the device is configured to allow the Management Server to manage it, as described in this topic. You can then add the Firebox X Edge to the Management Server.

To prepare a Firebox X Edge with version 10.x appliance software or older installed for management with the Management Server, you must be able to physically connect the Firebox X Edge to an Ethernet interface on your computer. We recommend that you reset the Edge to factory default settings before you begin this procedure.

### Install the Firebox X Edge

1. On the computer that runs WatchGuard System Manager, change the IP address to 192.168.111.x/24.
2. Start WatchGuard System Manager and select **Tools > Quick Setup Wizard**.  
*The Quick Setup Wizard starts.*
3. Read the **Welcome** page and click **Next**.
4. Select **Firebox X Edge** as the type of Firebox and click **Next**.
5. Connect the network interface on your computer to any LAN port on the Firebox X Edge, and click **Next**.  
Use one of the green Ethernet cables included with the Firebox X Edge. (If no green cable is included with your Firebox X Edge, try the red cable.)
6. Use the instructions on the subsequent page of the wizard to start the Firebox X Edge in safe mode.
7. Use the instructions on the wizard page, and click **Next**.
8. Use the instructions on the **Wait for the Firebox** and **The Wizard found this Firebox** pages. Click **Next** after each page.
9. Accept the License Agreement and click **Next**.
10. Configure the external (WAN 1) interface of the Firebox X Edge. Select **DHCP**, **PPPoE**, or **Static IP addressing**, and click **Next**.  
  
For more information about how to configure the Edge interfaces, see *Configure an External Interface* on page 90.
11. Click **Next** after you configure the interface.
12. Configure the Edge internal interface and click **Next**.
13. Type a status passphrase and a configuration passphrase for your Edge and click **Next**.  
You must type each passphrase two times. This is the passphrase that WatchGuard System Manager uses to connect to and configure the device.
14. Type a user name and passphrase for the device, and click **Next**.  
You must type the passphrase two times. This is the user name and passphrase that you can use to connect to and configure the device with a web browser.
15. Select the time zone settings and click **Next**.

16. Configure the Management Server settings. Type the IP address of the gateway Firebox that protects the Management Server, the name to identify the Firebox in the Management Server interface, and the shared key. Click **Next**.  
The shared key is used by the Management Server to create VPN tunnels between Firebox or XTM devices. You do not have to remember this key.
17. Review the configuration for the Edge and click **Next**.
18. To set up another Edge, select the check box. Click **Finish**.  
If you select this check box, the Quick Setup Wizard populates the fields with the same values as this configuration, so you can easily set up similar Edge devices.

## Import Firebox X Edge Devices into a Management Server

You must connect from the computer and to the same Management Server from which you ran the Quick Setup Wizard. You can import more than one Edge at a time as long as the devices have already been installed, as in the previous step.

1. Start WatchGuard System Manager, and connect to the Management Server for which you configured Edge devices.
2. Select **File > Import Device**.  
*The WatchGuard System Manager dialog box appears.*
3. Select the check boxes in front of each Edge device you want to import.
4. Click **Import**.

The Firebox X Edge devices are imported into the Management Server. The devices appear in the **Imported Devices** folder for the Management Server.

## Define WSM Access Settings on the Edge

1. To connect to the Firebox X Edge System Status page, type `https://` in the browser address bar, and the IP address of the Edge trusted interface.  
*The default URL is: `https://192.168.111.1`*
2. From the navigation bar, select **Administration > WSM Access**.  
*The WatchGuard Management Access page appears.*



3. Select the **Enable remote management** check box.
4. From the **Management Type** drop-down list, select **WatchGuard System Manager**.
5. To enable the Edge for Fully Managed Mode, select the **Use Centralized Management** check box. When the Firebox X Edge is in Fully Managed Mode, access to the Edge configuration pages is set to read-only. The only exception is access to the WSM Access configuration page. If you disable the remote management feature, you get read-write access to the Edge configuration again.

**Note** Do not select the **Use Centralized Management** check box if you use WatchGuard System Manager only to manage VPN tunnels.

6. Type and confirm a **Status Passphrase** for your Firebox X Edge.
7. Type and confirm a **Configuration Passphrase** for your Firebox X Edge. These passphrases must match the passphrases you use when you add the device to the Management Server or the connection will fail.

**Note** If the Firebox X Edge you want to manage has a static IP address on its external interface, you can stop here. Save the configuration to this Firebox. You can now Add Managed Devices to the Management Server. When you add this Edge to the Management Server configuration, the Management Server automatically connects to the Edge and configures it as a managed device. If the Edge you want to manage has a dynamic IP address, continue to the next step.

8. In the **Management Server Address** text box, type the IP address of the Management Server if it has a public IP address. If the Management Server has a private IP address, type the public IP address of the Firebox that protects the Management Server. The Firebox that protects the Management Server automatically monitors all ports used by the

Management Server and will forward any connection on these ports to the configured Management Server. No special configuration is necessary for this to occur.

9. Type the **Client Name** to identify the Edge in the Management Server configuration. This name is case-sensitive and must match the name you use for the Edge when you add it to the Management Server configuration.
10. Type the **Shared Key**. The shared key is used to encrypt the connection between the Management Server and the Firebox X Edge. This shared key must be the same on the Edge and the Management Server. You must get the shared key from your Management Server administrator.
11. Click **Submit** to save this configuration to the Edge. When you save the configuration to the Edge, the Edge is enabled as a managed client. The managed Firebox client tries to connect to the IP address of the Management Server. Management connections are allowed from the Management Server to this managed Firebox client.

You can now add the device to your Management Server configuration as described in *Add Managed Devices to the Management Server* on page 590.

## Configure a Firebox SOHO 6 as a Managed Device

1. Open a web browser and type the IP address of the SOHO 6.
2. If necessary, type the login and passphrase to connect.
3. Select **Administration > VPN Manager Access**.

*The VPN Manager Access page appears.*

4. In the left navigation pane below VPN, click **Managed VPN**.
5. Select the **Enable VPN Manager Access** check box.
6. Type the status passphrase for VPN Manager access. Type the status passphrase again to confirm the passphrase.
7. Type the configuration passphrase for VPN Manager access. Type the configuration passphrase again to confirm the passphrase.

**Note** *If the Firebox SOHO you want to manage has a static IP address on its external interface, you can stop here. Click **Submit** to save your configuration to the SOHO. You can now add*

*the device to your Management Server configuration. When you add this SOHO to the Management Server configuration, the Management Server automatically connects to the static IP address and configures the SOHO as a managed device. If the SOHO you want to manage has a dynamic IP address, proceed to Step 7.*

8. Select the **Enable Managed VPN** check box.
9. From the **Configuration Mode** drop-down list, select **SOHO**.
10. In the **DVCP Server Address** text box, type the IP address of the Management Server if it has a public IP address. If the Management Server has a private IP address, type the public IP address of the Firebox that protects the Management Server.  
The Firebox that protects the Management Server automatically monitors all ports used by the Management Server and forwards any connection on these ports to the configured Management Server. No special configuration is necessary for this to occur.
11. Type the **Client Name** to identify your Firebox SOHO.  
This name is case-sensitive and must match the name you use for the device when you add it to the Management Server configuration.
12. In the **Shared Key** text box, type the key used to encrypt the connection between the Management Server and the Firebox SOHO. This shared key must be the same on the SOHO and the Management Server. You must get the shared key from your Management Server administrator.
13. Click **Submit**.

When you save the configuration to the Firebox SOHO, the SOHO is enabled as a managed client. The managed SOHO client tries to connect to the IP address of the Management Server. Management connections are allowed from the Management Server to this managed SOHO client.

You can now add the device to your Management Server configuration as described in the *Add Managed Devices to the Management Server* on page 590.

## Start WatchGuard System Manager Tools

From the **Device Management** tab, you can start other WatchGuard System Manager (WSM) tools to configure and monitor your devices.

For the Management Server, you can start:

- Quick Setup Wizard
- CA Manager
- LogViewer
- Report Manager

For Firebox or XTM devices and WFS devices, you can start:

- Policy Manager
- Firebox System Manager
- HostWatch
- Ping
- Expire Lease

For more information about the **Expire Lease** tool, see *Expire the Lease for a Managed Device* on page 628.

For Edge devices, you can start:

- Policy Manager (Edge versions 11.x and later)
- Edge Web Manager (Edge versions before 11.0)
- Firebox System Manager
- HostWatch
- Ping
- Expire Lease

To use WatchGuard System Manager tools:

1. Select the **Device Management** tab.
2. Expand the **Devices** tree.
3. Select the device you want to configure or monitor.  
*The Device Management page appears.*
4. In the **Tools** section, click the link for the tool you want to use.  
*The selected tool application starts.*

**Note** *If you are logged in to the Management Server with user credentials that have administrator privileges, when you launch a WSM tool, you are not asked for the Status or Configuration passphrase of the XTM device.*

## Expire the Lease for a Managed Device

You can use the WSM Expire Lease tool to force your managed Firebox X Edge 10.x and Fireware XTM devices to contact the Management Server for new DVCP tunnel information. You can choose to expire the lease for an individual device, or for more than one device at the same time.

## Expire the Lease for One Device

You can choose to expire the lease for an individual device from two locations: the **Tools** section on the **Device** page, or the device context menu.

To expire the lease from the **Device** page:

1. Select the **Device Management** tab.
2. Expand the **Devices** tree and select a device.  
*The Device Management page appears.*
3. In the **Tools** section, click **Expire Lease**.  
*The Expire Lease dialog box appears.*
4. Click **OK**.  
*The Management Server lease for the managed device is automatically expired and any VPN or configuration changes are downloaded. A confirmation dialog box does not appear.*

To expire the lease from the device context menu:

1. Select the **Device Management** tab.
2. Expand the **Devices** tree and select a device.  
*The Device Management page appears.*
3. Right-click the device and select **Expire Lease**.  
*The Expire Lease dialog box appears.*
4. Click **OK**.  
*The Management Server lease for the managed device is automatically expired and any VPN or configuration changes are downloaded. A confirmation dialog box does not appear.*

## Expire the Lease for Many Devices

If you have more than one managed device, you can expire the lease for one or more of your devices at the same time.

1. Select the **Device Management** tab.
2. In the left navigation bar, select the Management Server.  
*The Management Server page appears.*
3. Right-click the Management Server and select Expire Lease.  
*The Expire Lease dialog box appears. By default, the check box for all Firebox X Edge 10.x and Fireware XTM managed devices is selected.*
4. Clear the check box for any device for which you do not want to expire the lease.
5. Click **OK**.  
*The Management Server lease for the managed device is automatically expired and any VPN or configuration changes are downloaded. A confirmation dialog box does not appear.*

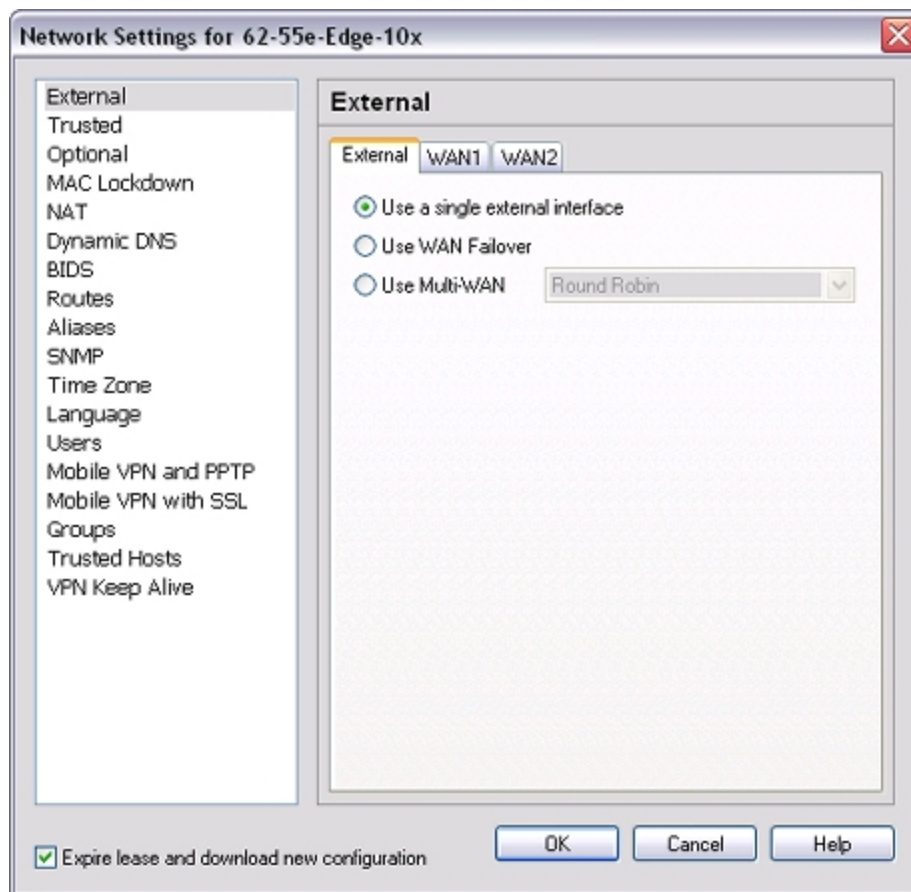
## Configure Network Settings (Edge Devices v10.x and Older Only)

You can use the Management Server to configure unique network settings for Firebox X Edge devices (version 10.x and older only). This procedure loads the current network settings for the Edge device.

**Note** All Firebox X Edge network settings can be configured with the Edge Web Manager.

From WatchGuard System Manager:

1. Select the **Device Management** tab.
2. Expand the **Devices** list.
3. Select a Firebox X Edge device.  
*The Device Management page appears.*
4. In the **Network Settings** section, click **Configure**.  
*The Network Settings dialog box appears.*



5. In the left pane of the dialog box, select a category.  
*The settings for that category appear in the right pane of the dialog box.*
6. Configure the settings for the category.

For more information about network settings for your v10.x Edge device, see the [Firebox X Edge Help v10.x](#) on the WatchGuard web site.

## About the Configuration Template Section

**Note** The management page for a SOHO 6 does not have the **Policy** section.

This section shows the Device Configuration Template to which this Firebox X Edge is subscribed. If a template is not applied to the device, you can drag the device to one of the Device Configuration Templates. You can also click the **Configure** link in this section to configure the Device Configuration Template applied to this device.

For information about Device Configuration Templates, see *Create Device Configuration Templates* on page 633.

## Update or Reboot a Device, or Remove a Device from Management

On the **Device** page for your managed device, you can change the server and client settings, update the IPSec and CA certificates for your device, or reboot your device. You can also remove a device so it is no longer managed by the Management Server.

### Update a Device

From the WatchGuard System Manager **Device Management** page:

1. Expand the **Devices** list.
2. Select the device to update.  
*The Device Management page for the selected device appears.*
3. In the **Device Information** section, click **Update Device**.  
Or, right-click the device and select **Update Device**.  
*The Update Device dialog box appears.*



4. To download the policies on the managed device to the Management Server for the trusted and optional networks, select the **Download Trusted and Optional Network Policies** check box.

We recommend you do this to make sure you have the latest policies when you edit the device configuration, particularly if you have not connected to the device in a long time.

5. To refresh the Management Server configuration on the device after an update (Management Server IP address, hostname, shared secret, and lease time), select the **Reset Server Configuration** check box.

If you have made any changes to the device properties, make sure you select this check box.

6. To expire the Management Server lease for the managed device and download any VPN or configuration changes, select the **Expire Lease** check box.
7. To issue or reissue the IPSec certificate for the XTM device and the Certificate Authority's certificate, select the **Issue/Reissue Firebox's IPSec Certificate and CA's Certificate** check box.  
(This option does not appear for Edge versions before 11.0.)
8. Click **OK**.

## Reboot a Device

From the WatchGuard System Manager **Device Management** page:

1. Expand the **Devices** list.
2. Select the device to reboot.  
*The Device Management page for the selected device appears.*
3. In the **Device Information** section, click **Reboot**.  
*A confirmation message appears.*
4. Click **Yes**.

## Remove a Device from Management

To remove a device so that it is no longer managed by the Management Server and no longer appears in the Management Server window:

1. Expand the **Devices** list.
2. Select the device to remove.
3. Right-click the device and select **Remove**.  
Or, select **Edit > Remove**.  
*A confirmation message appears.*
4. Click **Yes**.
5. Open Policy Manager for this device.
6. Select **Setup > Managed Device Settings**.  
*The Managed Device Settings page appears.*
7. Clear the **Centralized Management** check box.  
*A confirmation message appears.*
8. Click **Yes** to remove the device from management.
9. Save the configuration file.



# Create Device Configuration Templates

A Device Configuration Template is a collection of configuration settings that multiple Firebox or XTM devices can use. When you manage your Firebox or XTM devices with the WatchGuard Management Server, you can create Device Configuration Templates that are stored on the Management Server. You can then use these templates with your managed Firebox or XTM devices. The Management Server uses two different methods to attach a template to a device: *subscription* or *application*. The method that is used depends on your device type and OS version.

The *subscription* method is used for your managed Firebox X Edge e-Series devices, version 10.x and earlier. When you subscribe an Edge device to a Device Configuration Template, the policies and settings configured in the template are added to the individual configuration file for your device. You can view these policies and settings from the device configuration file, but they can only be changed from the Device Configuration Template.

For more information about template subscription, see the topic [Create and subscribe to Device Configuration Templates](#) in the v11.3.x *WatchGuard System Manager Help* on the WatchGuard web site.

The *application* method is used for Fireware XTM devices version 11.x and later. You can apply a template to a single managed XTM device or to a folder of XTM devices. If you apply a template to a folder of devices, the template is only applied to the devices in the folder with the same OS version as the template. For example, if your folder includes Fireware v10.x devices and Fireware XTM v11.3.x devices, and the template is for Fireware v11.3.x, the template is only applied to the devices with v11.3.x OS.

The Management Server includes predefined templates for Firebox X Edge devices of version 10.2 and older. For all other Firebox or XTM devices, you must create new templates. All predefined templates and templates that you create appear in the **Device Configuration Templates** list.

You can use Device Configuration Templates to easily configure standard firewall filters, change the Blocked Sites list, change your WebBlocker configuration, configure logging settings, or apply other policy settings to one or more fully managed devices. There are two different scenarios for how to use XTM v11.4 templates:

- Create complete Device Configuration Templates, including all the settings for your devices.
- Create multiple Device Configuration Templates, each with specific settings that you apply in layers to your devices, as appropriate for each device.

For example, you could create a template that includes only the SMTP-proxy settings for a group of devices deployed in the northern region of your territory.

To help you easily identify the contents of each template you create, make sure to specify a unique, descriptive name for each of your configuration templates.

For Device Configuration Templates created in v11.3.x and older, the policies you add in a template appear in Policy Manager with *T\_* before the policy name (for example, **T\_WatchGuard**). When you upgrade a v11.3.x or older template to v11.4 or later, any policy names that included *T\_* keep the same name after the upgrade. New policies that you add to v11.4 and later templates do not include a *T\_* before the policy name.

When you configure a template, you can also specify whether settings in the template take precedence over settings in an individual device configuration file. By default, template settings automatically override settings in an individual configuration file.

Configuration templates have these restrictions:

- Edge Configuration Templates can only be used with Firebox X Edge devices.
- An Edge device must have OS version 7.5 or later to use Edge Configuration Templates.
- You must use separate templates for Edge devices that run OS versions 7.5, 8.0, 8.5, 8.6, or 10.x.
- Fireware XTM 11.0-11.3.x templates can only be used for XTM devices that run OS versions 11.0–11.3.x,
- Fireware XTM 11.4 and later templates can only be used for XTM devices that run OS version 11.4 and later.

Available configuration templates include:

- Firebox X Edge — Versions 7.5, 8.x, 10.x
- Fireware XTM — Fireware XTM v11.0–11.3.x (for Firebox X Edge e-Series, Core e-Series, Peak e-Series devices) and Fireware XTM v11.4 or later (for XTM devices)

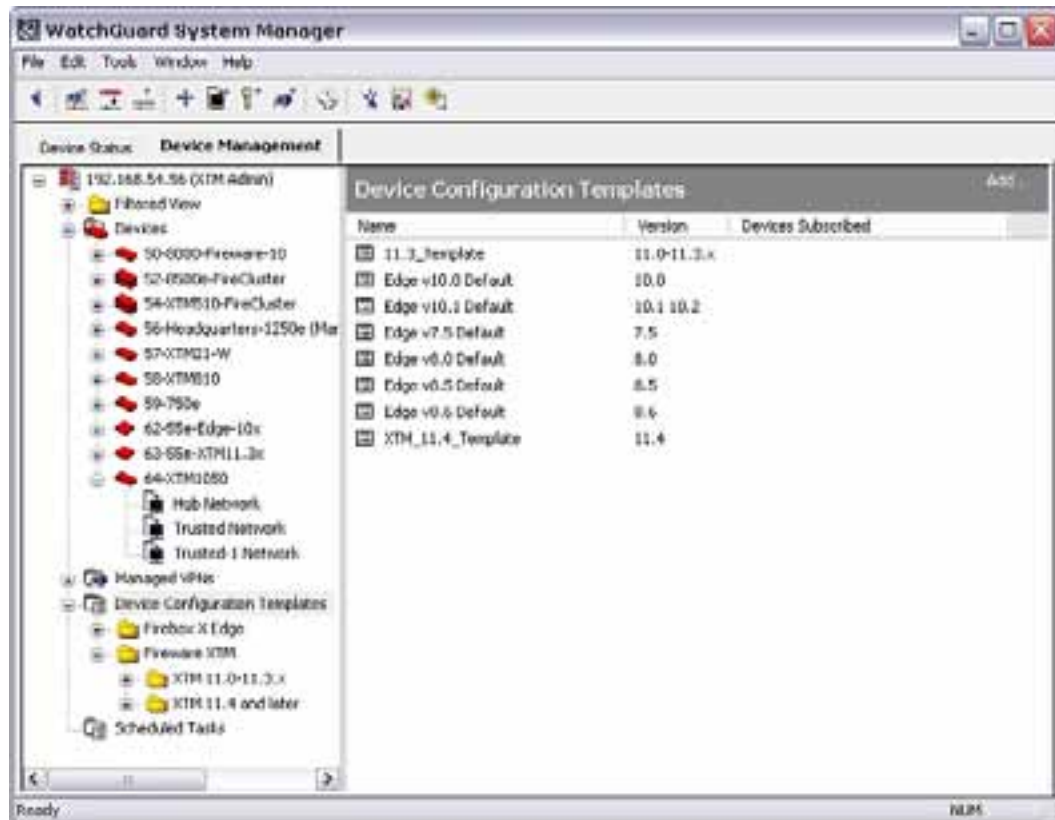
You can make changes to a Device Configuration Template at any time. When you make changes to a Firebox X Edge v 10.2 or older template, the subscribed devices are automatically updated with the changes. When you make a change to a configuration template for an XTM device, the Management Server saves the change in the template configuration history, but the devices that use that template are not automatically updated. You must reapply the template to your devices for the template changes to appear in the configuration file for your devices.

After an XTM Device Configuration Template is applied to a device, you can open Policy Manager from the Management Server to connect directly to the XTM device and change the policies and settings in the device configuration file. The Management Server saves the changes you make in the configuration history for the device.

For more information about the device configuration history, see *About Configuration History and Template Application History*.

## Create a New Device Configuration Template

1. Open WatchGuard System Manager and [connect to your Management Server](#).
2. Select the **Device Management** tab.  
*The Management Server page appears.*
3. In the left navigation bar, select **Device Configuration Templates**.  
*The Device Configuration Templates page appears with the list of currently available templates.*



4. Expand the **Device Configuration Templates** list to see the available templates.
5. Right-click **Device Configuration Templates** and select **Insert Device Configuration Template**.  
Or, click **Add** at the top right of the **Device Configuration Templates** page.  
*The Product Version dialog box appears.*
6. Select the product line and version from the drop-down list. Click **OK**.  
*If you selected an Edge device, the Edge Configuration: Edge Template window appears.*  
*If you selected a Fireware XTM device, you select a name for the template and then Fireware XTM Policy Manager opens with a blank configuration file.*
7. Complete the processes in the subsequent sections to configure the template for the type of device you selected.

## Configure a Template for a Managed Edge Device

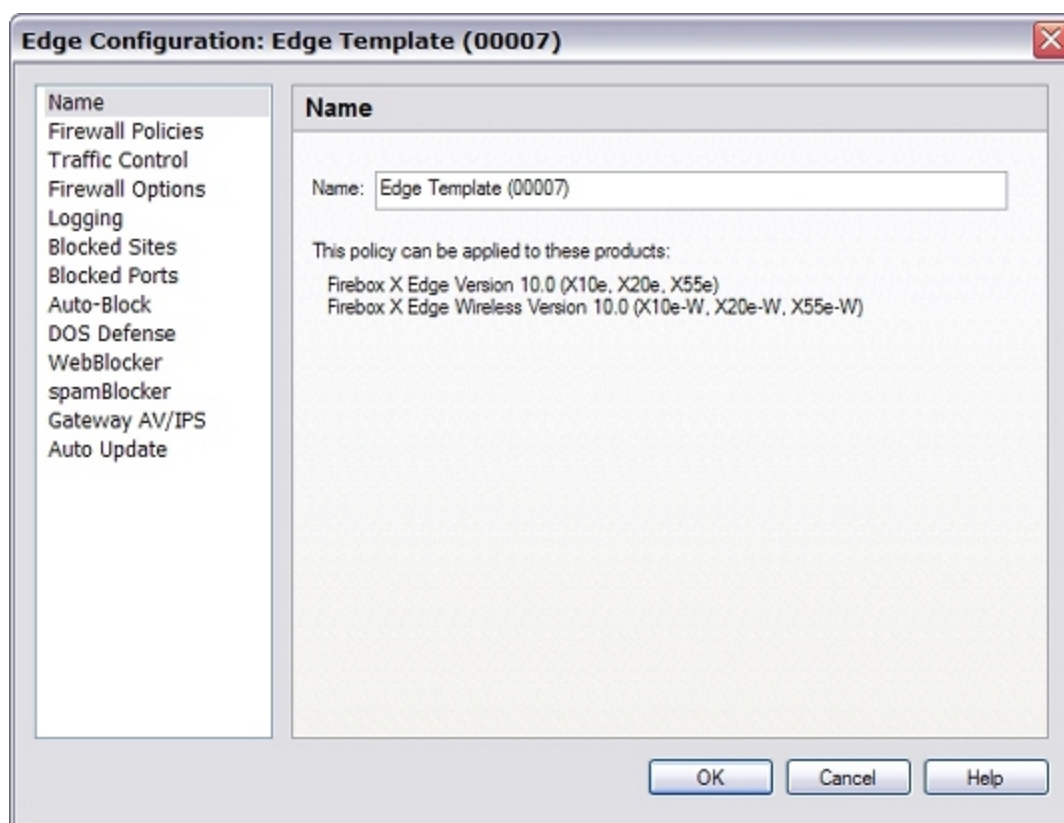
Use the **Edge Configuration: Edge Template** dialog box to define the settings for your Edge configuration template.

**Note** *If you want to use the Edge Web Manager to connect directly to your managed Edge device rather than follow the **Edge Web Manager** link in WSM, you must add a HTTPS policy to your Edge Configuration template. This HTTPS policy must allow incoming traffic from External to an Alias defined on the Edge over TCP port 443.*

To add and configure a new template for your Edge:

1. Select the **Device Configuration Templates** folder.  
*The Device Configuration Templates page appears.*

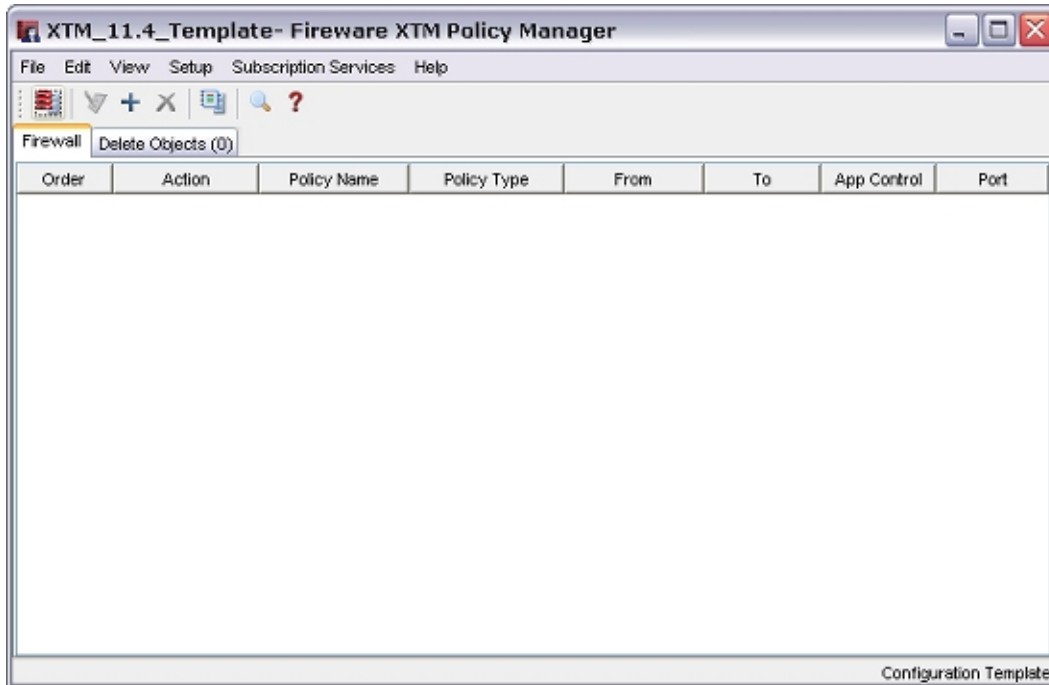
2. Click **Add**.  
*The Edge Configuration Template dialog box appears.*
3. In the **Name** text box, type a name for the template.



4. To configure the template, select the categories in the left pane and add the necessary information for each category.  
*Different categories appear in the list based on the version of the Edge you selected.*  
For more information on the available categories, see the corresponding section in the *Help* or *User Guide*.  
  
For more information about how to add Firewall Policies to the template, see [Add a pre-defined policy with the Add Policy wizard](#) or [Add a custom policy with the Add Policy wizard](#).
5. Click **OK**.  
*The template is saved to the Management Server, and an update is sent to all Firebox X Edge devices that are subscribed to this template.*

## Configure a Template for an XTM Device

When you select to create a template for an XTM device, you use a streamlined version of Fireware XTM Policy Manager to define the settings for your configuration template.



When you configure a template, you can:

- [Add](#), [modify](#), and [delete](#) individual policies
- Set up [Aliases](#) and [Logging](#)
- Set up [Proxy actions](#), and [Schedules](#)
- Configure spamBlocker, Gateway AntiVirus, Intrusion Prevention, WebBlocker, and Quarantine Server settings
- Configure inheritance settings for your devices
- Configure policies to be deleted from your device configuration files
- Configure [SNAT settings](#) (v11.4 and later devices and templates only)

After you apply a template to a device, you can make changes to the aliases in your device configuration file to correctly define the value of the aliases for your device.

Because you can apply a template to more than one fully managed XTM device, it is helpful to be able to automatically delete certain settings from a device configuration file when the template is applied. You can configure the deletion settings when you set up your template configuration file. You can delete policies, services, aliases, proxy actions, WebBlocker settings, Application Control, and schedules. You cannot delete tunnels or license keys, which are stored on the Management Server.

## Add Policies to a Template

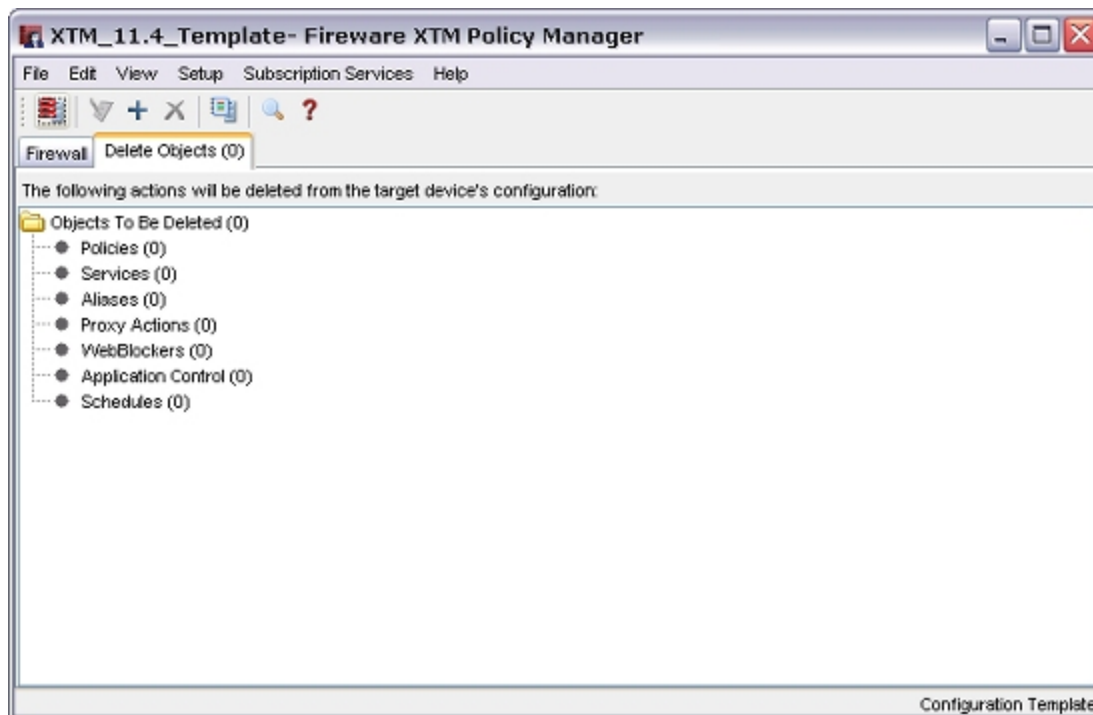
From Fireware XTM Policy Manager:

1. Select the **Firewall** tab.
2. Click **+**.  
Or, select **Edit > Add Policy**.  
*The Add Policies dialog box appears.*
3. Expand the folder for the type of policy you want to add.  
*A list of the selected policies appears.*
4. Select a policy.
5. Click **Add**.  
*The New Policy Properties dialog box appears.*
6. Configure the policy.  
For more information about how to configure a new policy, see *Add a Proxy Policy to Your Configuration* on page 417.
7. Repeat Steps 3–5 to add more policies to your configuration.

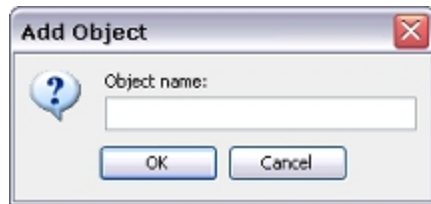
## Specify Objects for Deletion

To specify objects that are deleted from the device configuration file when the template is applied:

1. Select the **Delete Objects** tab.



2. From the **Objects To Be Deleted** tree, select the type of object to delete from the device configuration file.
3. Right-click the object and select **Add Object**.  
*The Add Object dialog box appears.*



4. In the **Object Name** text box, type the name of the object to delete.  
For example, to delete the FTP proxy policy, type FTP-proxy.
5. Click **OK**.  
*The object you specified appears in the list for the type of object you selected.*

## Configure Inheritance Settings

By default, if you apply a template to a device with a configuration file that already includes the same policies and settings as the template, most of the template settings take precedence and override the device configuration settings.

After you have added policies and configured other settings in your template, you can configure your template to specify which device settings the template can override, and for which settings the device configuration file settings take precedence. Each category of settings appears on a different tab:

- **Aliases**
- **Application Control**
- **Other**
- **Policies**
- **Policy Types**
- **Proxy Actions**
- **Schedules**
- **SNAT**
- **WebBlocker**

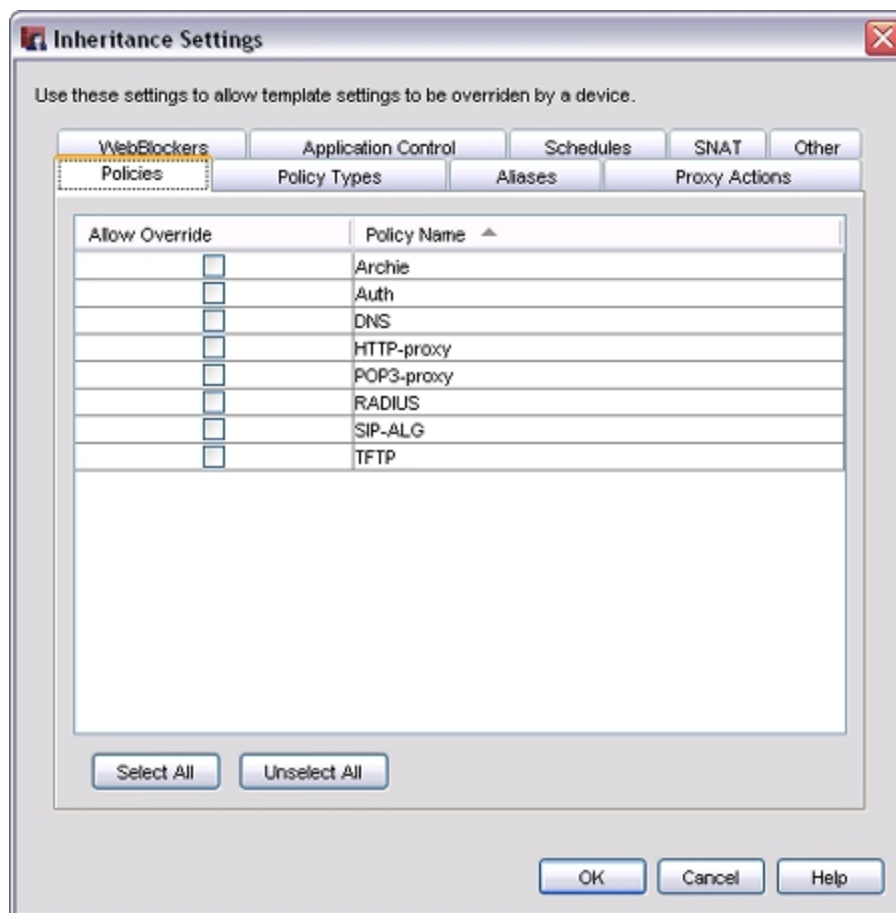
The one exception to the default inheritance settings behavior is the **Other** tab. By default, all of the options on the **Other** tab are selected, so that the device settings automatically override the settings in the template. This is to prevent the template from changing the settings for these options that you have already configured on your device.

Options on the **Other** tab include:

- spamBlocker settings
- Gateway AntiVirus decompression settings
- Intrusion Prevention settings
- Signature Update settings
- Quarantine Server settings
- Reputation Enabled Defense feedback service
- WatchGuard Log Server settings


From Policy Manager for the configuration template file:

1. Select **View > Inheritance Settings**.  
*The Inheritance Settings dialog box appears.*



2. Select a tab.  
*The settings configured in the template for the selected category appear.*
3. To enable the device settings to override a template setting, select the check box for that setting.  
All of the check boxes on the **Other** tab are selected by default.
4. Repeat Steps 2–3 to specify additional override settings.
5. Click **OK**.

## Save the Template

1. Click .  
Or, select **File > Save > To Management Server**.  
*The Schedule Template Update Wizard appears.*
2. Click **Next** to start the wizard.  
*The Select the Time and Date page appears.*
3. Select an option: **Update the template immediately** or **Schedule template update**.
4. If you selected **Schedule template update**, select the **Date** and **Time** that you want the update to occur.
5. Click **Next**.  
*The Schedule Template Update Wizard is complete page appears.*
6. Click **Finish** to exit the wizard.  
*If your Management Server configuration requires that you add a comment when you save your configuration, the Save Comment dialog box appears.*

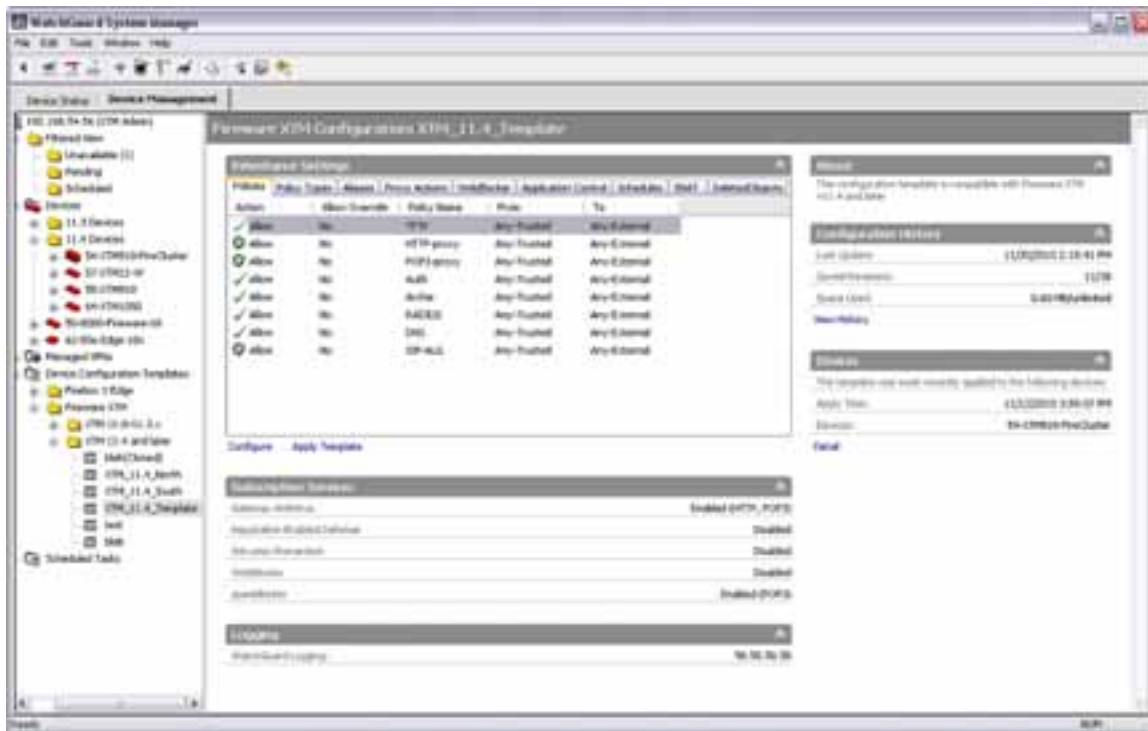


7. If the **Save Comment** dialog box appears, type a comment about your configuration changes.
8. Click **OK**.

The new template appears in the *Device Configuration Templates* list.

## Review XTM Template Settings

After you have configured all the settings for your XTM template, select the template in the **Device Configuration Templates** list. The **Template Settings** page for the template appears with all the settings you configured.



From this page, you can review the template settings, apply the template to an XTM device, and view the configuration history of the template.

The available template settings include:

### *Inheritance Settings*

In the **Inheritance Settings** section, select a tab to review these settings:

- Policies
- Services
- Aliases
- Proxy Actions
- WebBlocker
- Application Control
- Schedules
- Deleted Objects

### *Subscription Services*

The **Subscription Services** section includes the status and general configuration details for each available service.

### *Logging*

The **Logging** section includes details about your WatchGuard Log Server.

### *About*

The **About** section includes device compatibility information for this template.

### *Configuration History*

The **Configuration History** section includes details about when the template was last updated, how many revisions the Management Server currently has saved for the template, and the amount of space the revisions have used on the Management Server.

To see more details in the configuration history for a template, click **View History**.

You cannot make changes to the settings on the **Template Settings** page, but you can open Fireware XTM Policy Manager from this page to change an XTM template. For more information, see the section, *Change an XTM Configuration Template*.

To apply the template to an XTM device, you can use the Apply Template Wizard. For more information, see the subsequent section.


To view the configuration history of the template, you can open the **Configuration History** dialog box. For more information, see *About Configuration History and Template Application History* on page 654.


## **Apply an XTM Template to an XTM Device**

After you have completed the configuration for your XTM Device Configuration Template, you can apply it to your fully managed XTM devices of the same version. For more information about how to apply a template to an XTM device, see *Apply Device Configuration Templates to Managed Devices* on page 652.

## **Change an XTM Configuration Template**

To modify a setting in a Fireware XTM configuration template:

1. In the left navigation menu, select the template.  
*The Template settings page appears.*
2. In the **Inheritance Settings** section, click **Configure**.  
*Policy Manager opens the selected template configuration file.*
3. To modify a policy, select the policy, and click .  
Or, select **Edit > Modify Policy**.  
*The Edit Policy Properties dialog box appears.*
4. Configure the policy.  
For more information about how to modify a policy, see *About Policy Properties* on page 391 or *Add a Proxy Policy to Your Configuration* on page 417.
5. Make any other changes to settings in the template.

- Click .
- Or, select **File > Save > To Management Server**.  
*The template changes are saved to the Management Server.*

For your changes to take effect in your individual device configuration files, you must apply your template changes to your devices with the Apply Template Wizard. For more information, see the previous section.

## Add a Predefined Policy to an Edge Device Configuration Template

You can use the WatchGuard System Manager Add Policy Wizard to add a predefined policy to the Device Configuration Template for your Firebox X Edge device.

- From the **Device Management** tab, select **Device Configuration Templates**.  
*The Device Configuration Templates page appears.*
- Right-click **Device Configuration Templates** and select **Insert Device Configuration Template**.  
Or, click **Add** in the upper-right corner of the page.  
*The Product Version dialog box appears.*
- Select the Edge device and version from the drop-down list. Click **OK**.  
*The Edge Configuration: Edge Template dialog box appears.*
- In the left navigation bar, select **Firewall Policies**.  
*The Firewall Policies page appears.*
- Click **Add**.  
*The Add Policy Wizard starts.*
- Click **Next**.  
*The Select a service for this policy page appears.*



- Select **Choose a predefined service from this list** and select a policy from the list.
- Click **Next**.  
*The Select the traffic direction page appears.*

9. Select the traffic direction: **Outgoing**, **Incoming**, or **Optional**.
10. Click **Next**.  
*The Configure the network resources page appears.*
11. In the **Filter** drop-down list, select to **Deny** or **Allow** traffic.
12. If you selected **Allow**, in the **From** and **To** lists, set the sources and destinations.  
To add a new resource, click **Add** beneath the **From** or **To** list and add the required information.
13. Click **Next**.  
*The Add Policy Wizard is complete page appears.*
14. Click **Finish** to close the wizard.

## Add a Custom Policy to an Edge Device Configuration Template

You can use the Add Policy Wizard to create a custom policy in the Device Configuration Template for your Firebox X Edge device.

1. From the **Device Management** tab, select **Device Configuration Templates**.  
*The Device Configuration Templates page appears.*
2. Right-click **Device Configuration Templates** and select **Insert Device Configuration Template**.  
Or, click **Add** in the upper-right corner of the page.  
*The Product Version dialog box appears.*
3. Select the Edge device and version from the drop-down list. Click **OK**.  
*The Edge Configuration: Edge Template dialog box appears.*
4. In the left navigation bar, select **Firewall Policies**.  
*The Firewall Policies page appears.*
5. Click **Add**.  
*The Add Policy Wizard starts.*
6. Click **Next**.  
*The Select a service for this policy page appears.*



7. Select **Create and use a new custom service**.
8. Click **Next**.

*The Specify Protocols page appears.*

The screenshot shows the 'Add Policy Wizard' dialog box with the 'Specify the protocols' step. The dialog has a title bar with a close button (X) and the WatchGuard logo. Below the title bar, the text 'Specify the protocols.' is displayed. A sub-instruction reads: 'Type the name of this policy and add a list of protocols.' There is a text input field labeled 'Name:'. Below this is a section labeled 'Protocols:' containing a table with two columns: 'Protocol' and 'Port'. The table is currently empty. At the bottom right of the table area are two buttons: 'Add...' and 'Remove'. At the bottom of the dialog are three buttons: '< Back', 'Next >', and 'Cancel'.

9. Type a name for the protocol.
  10. To add a protocol, click **Add**.
- The Add protocol dialog box appears.*

The screenshot shows the 'Add protocol' dialog box. It has a title bar with a close button (X). The dialog contains three fields: 'Type:' with a dropdown menu set to 'Single Port', 'Protocol:' with a dropdown menu set to 'TCP', and 'Server Port:' with a text input field containing '0'. At the bottom are two buttons: 'OK' and 'Cancel'.

11. In the **Type** drop-down list, select whether the protocol uses a **Single Port** or a **Port Range**.
  12. In the **Protocol** drop-down list, select to type of protocol to filter: **TCP**, **UDP**, or **IP**.
  13. Type the **Server Port** number or numbers, or the **IP Protocol** number.
  14. Click **OK** to add the protocol.
  15. Repeat Steps 10–14 to add another protocol.
  16. Click **Next** when all the protocols for this policy are added.
- The Select the traffic direction page appears.*
17. Select the traffic direction: **Outgoing**, **Incoming**, or **Optional**.
  18. Click **Next**.
- The Configure the network resources page appears.*
19. In the **Filter** drop-down list, select to **Deny** or **Allow** traffic.

20. In the **From** and **To** lists, define the sources and destinations.  
To add a new resource, click **Add** beneath the **From** or **To** list and add the required information.
21. Click **Next**.  
*The Add Policy Wizard is complete page appears.*
22. Click **Finish** to close the wizard.

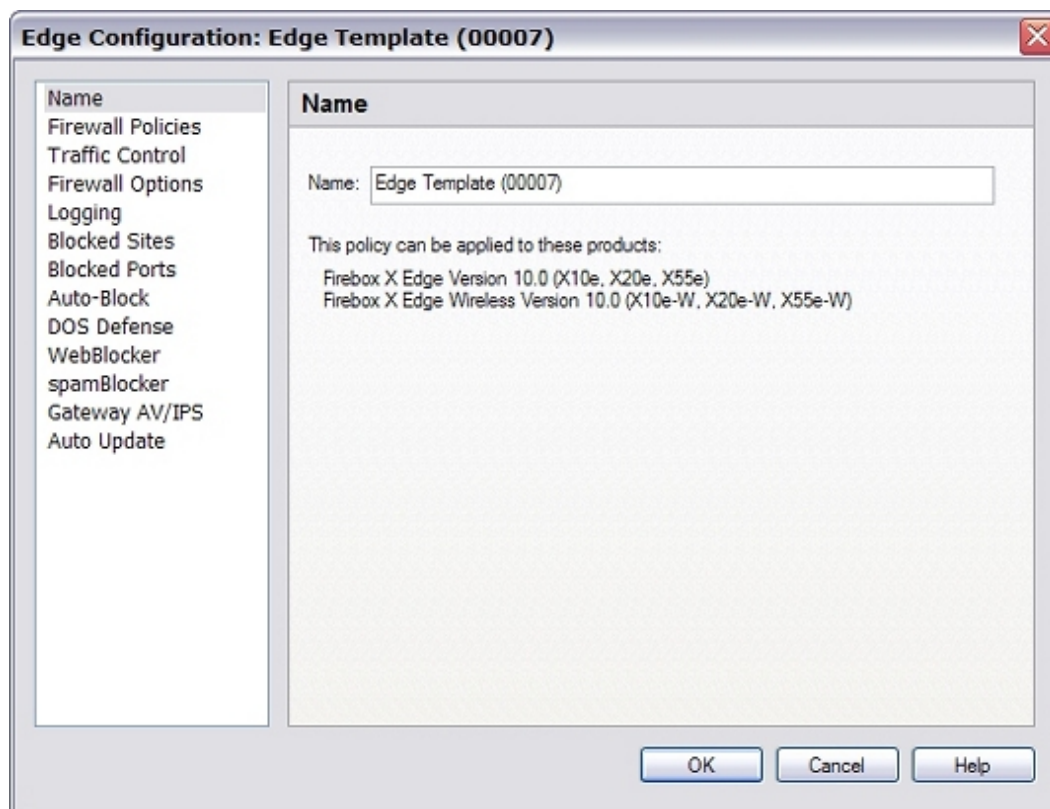
## Change the Name of a Device Configuration Template

When you create a new Device Configuration Templates in WatchGuard System Manager you select a name for that template. You can change the name of each template so you can easily identify to which devices it applies.

1. From the **Device Management** tab, expand the **Device Configuration Templates** list.  
*The list of Device Configuration Templates appears.*
2. Expand the folder for the type of Device Configuration Templates you want to rename.
3. Select the template you want to rename.
4. Follow the steps in the subsequent sections for the type of Device Configuration Template you selected.

## Rename a Firebox X Edge Template

1. Right-click the template and select **Properties**.  
*The Edge Configuration dialog box appears.*
2. In the left navigation bar, select **Name**.  
*The Name page appears.*



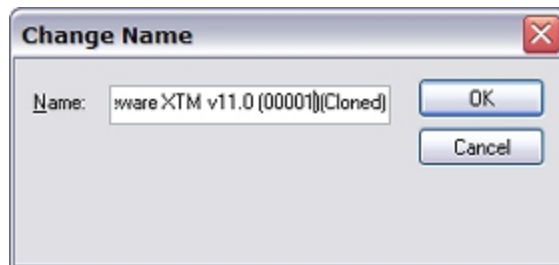
3. In the **Name** text box, type the new name for the template.
4. Click **OK**.

*The name of the template is updated and appears in the Device Configuration Templates list.*

## Rename a Fireware XTM Template

1. Right-click the template and select **Rename**.

*The Change Name dialog box appears.*



2. In the **Name** text box, type a new name for the template.
3. Click **OK**.

*The name of the template is updated and appears in the Device Configuration Templates list.*

## Clone a Device Configuration Template

If you have devices that use similar configurations, but with small differences, you can clone (copy) a template and then customize the cloned template. This enables you to make one template, make a clone for each variation, and then change the cloned templates.

From the WatchGuard System Manager **Device Management** tab:

1. Expand **Device Configuration Templates**.
2. Right-click the Device Configuration Template you want to clone, and select **Clone**.

*The Change Name dialog box appears.*

3. In the **Name** text box, type a new name for the cloned template.
4. Click **OK**.

*The cloned template appears in the Device Configuration Templates list.*

5. Select the new template.

*The template configuration page appears.*

6. Update the template settings.

For information on how to configure template settings, see *Create Device Configuration Templates* on page 633.

## Configure an SNAT Action

An SNAT action is a user-defined action that includes static NAT or server load balancing actions which can be referenced by a policy. An SNAT action is a NAT mapping which replaces the original destination IP address (and optionally, port) with a new destination.

You can add SNAT actions to your XTM Device Configuration Templates v11.4 and later, and apply them to one or more policies in your template or XTM v11.4 or later device configuration. You cannot configure SNAT actions for v11.3.x and earlier devices or templates. For SNAT actions that you add to a template, only static NAT actions are available; server load balancing actions are not available in templates. Each SNAT action you create can have different inheritance settings configured in the template. To reference an SNAT action in a policy, you add it to the *To* (destination) list in the policy.

For more information, see *Configure Static NAT*.

You can add, edit, and delete SNAT actions in your policies. If you edit or remove an SNAT action in a policy, make sure to verify that the policy is still valid.

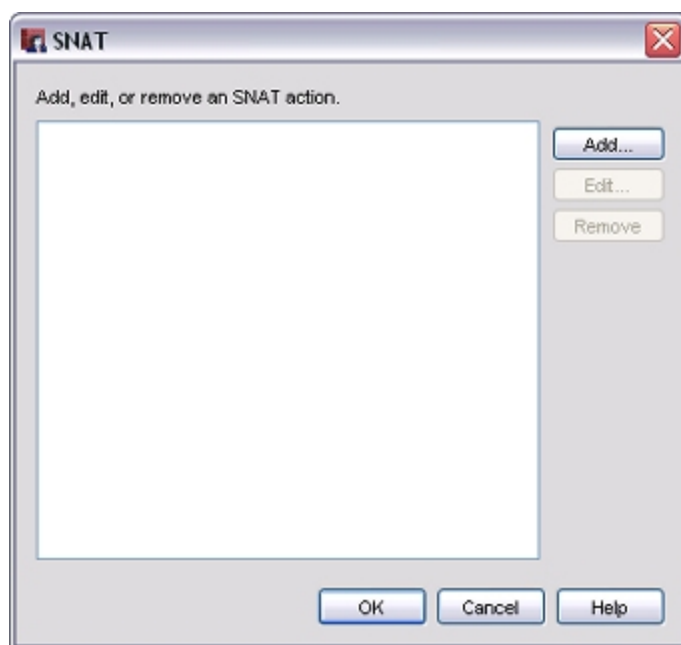
## Add an SNAT Action

When you add an SNAT action to your template, for each NAT member you add to the SNAT action, you specify the external IP address and internal IP address. If you enable port address translation (PAT), you also specify the port to use for the action. This information appears in the SNAT Members list for each action you add to the SNAT action. You can add only one SNAT member to any SNAT action. The external IP address of an SNAT action in a template is restricted to *Any-External*.

To add an SNAT action to a template:

1. Start Policy Manager for your Device Configuration Template.
2. Select **Setup > Actions > SNAT**.

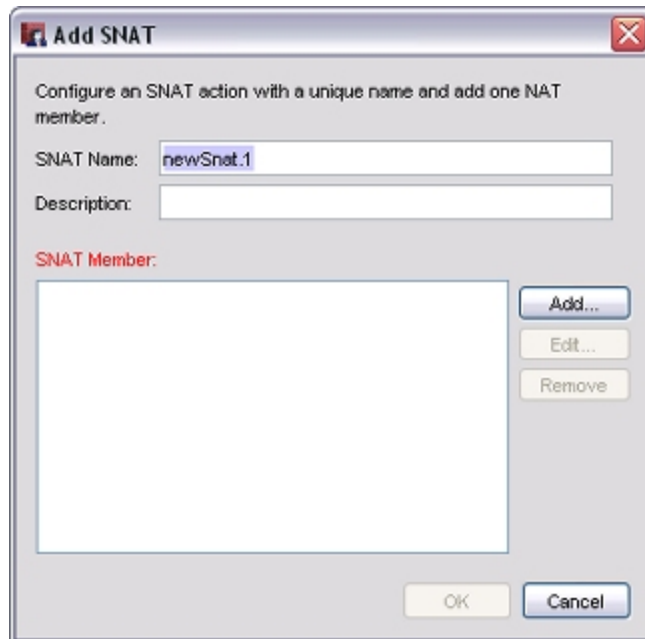
*The SNAT dialog box appears.*



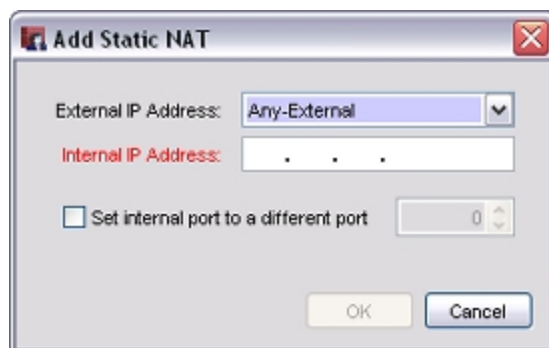
3. Click **Add**.

*The Add SNAT dialog box appears.*

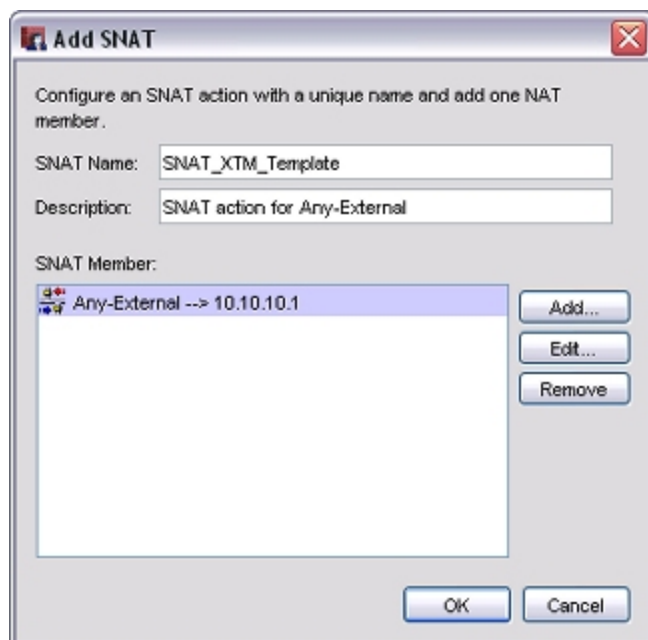




4. In the **SNAT Name** text box, type a name for this SNAT action.
5. (Optional) In the **Description** text box, type an explanatory description to help you identify this SNAT action.
6. To add an SNAT member to the SNAT action, click **Add**.  
*The Add Static NAT dialog box appears.*



7. From the **External IP address** drop-down list, select an external IP address for this SNAT action. For an SNAT action in a template, **Any-External** is the only option.
8. In the **Internal IP Address** text box, type the IP address of the destination on the trusted or optional network.
9. To enable port address translation (PAT), select the **Set internal port to a different port** check box. In the adjacent text box, type or select the port number.
10. Click **OK**.  
*The static NAT route appears in the SNAT Members list.*



11. To change an existing static NAT member, from the **SNAT Members** list, select the member and click **Edit**.
12. To delete a member from the list, from the **SNAT Members** list, select the member and click **Remove**.
13. Click **OK**.

*The SNAT action appears in the SNAT dialog box.*

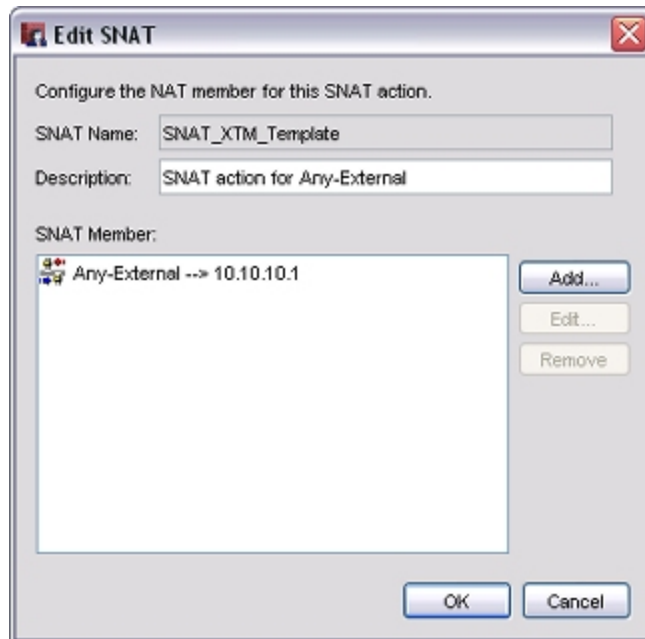
## Edit or Delete an SNAT Action

You can change the settings for the SNAT actions in your templates or remove them from the template. When you edit an SNAT action, you can change only the description and the SNAT members. You cannot change the name of the SNAT action. If you want to change the name of an SNAT action, you must delete the action and create a new action with the new name. You can add only one SNAT member to an SNAT action. If you want to add a new SNAT member to an SNAT action that already includes an SNAT member, you must delete the current SNAT member before you can add the new SNAT member.

To change SNAT action settings:

1. In the **SNAT** dialog box, select an SNAT action. Click **Edit**.

*The Edit SNAT dialog box appears.*



2. Change the details of the SNAT action configuration:
  - To edit a member in the **SNAT Members** list, select an SNAT action. Click **Edit** and change the settings.
  - To remove a member from the **SNAT Members** list, select an SNAT action. Click **Remove**.  
*The member is immediately deleted from the SNAT Member list.*
  - To add an SNAT member, click **Add** and configure the settings for the SNAT member.
  - (Optional) In the **Description** text box, type a new explanatory description for this SNAT action.
3. Click **OK**.

## Apply Device Configuration Templates to Managed Devices

You can use Device Configuration Templates to create a standard set of policies and rules to use for one or more Firebox or XTM devices. You can apply a Device Configuration Template to any of your fully managed XTM devices. You can apply only one template at a time to each device. When you apply a template, the policies and settings defined in the template are added to the device configuration. To apply a template to a device, you can either drag-and-drop the template to each device, or use the Device Configuration Template Settings page to apply a template to your device. You can only apply a template to a device of the same type as the template. For example, if you drag-and-drop a v11.4 or later XTM Device Configuration Template on the **Devices** folder, the template is applied to only the fully managed XTM devices in the list of the same version as the template ( in this case, Fireware XTM OS v11.4 or later), not to the other devices.

### Drag-and-Drop to Apply a Template

You can use drag-and-drop to apply a template to any Firebox or XTM device, or folder of devices.

1. On the **Device Management** tab, expand the **Devices** list.
2. Select a device or folder of devices and drag-and-drop the selected device or folder to a template in the **Device Configuration Templates** list.

Or, drag-and-drop the selected Device Configuration Template to a device or device folder.

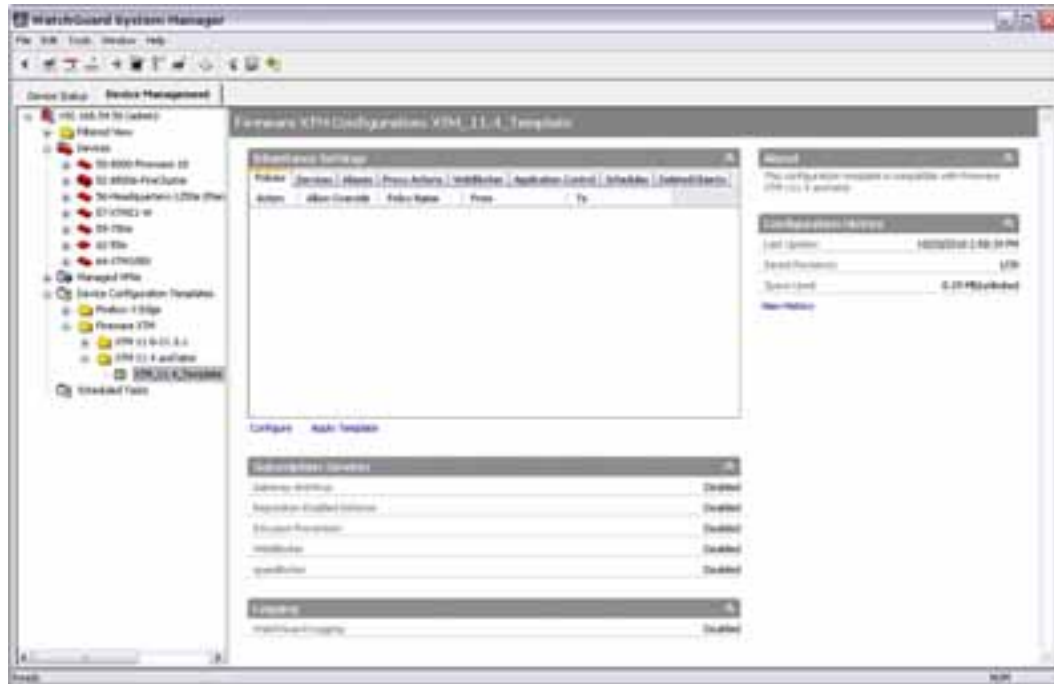
*The template is applied to the selected device or devices of the same type in the folder.*

### Use the Apply Template Wizard for an XTM Device

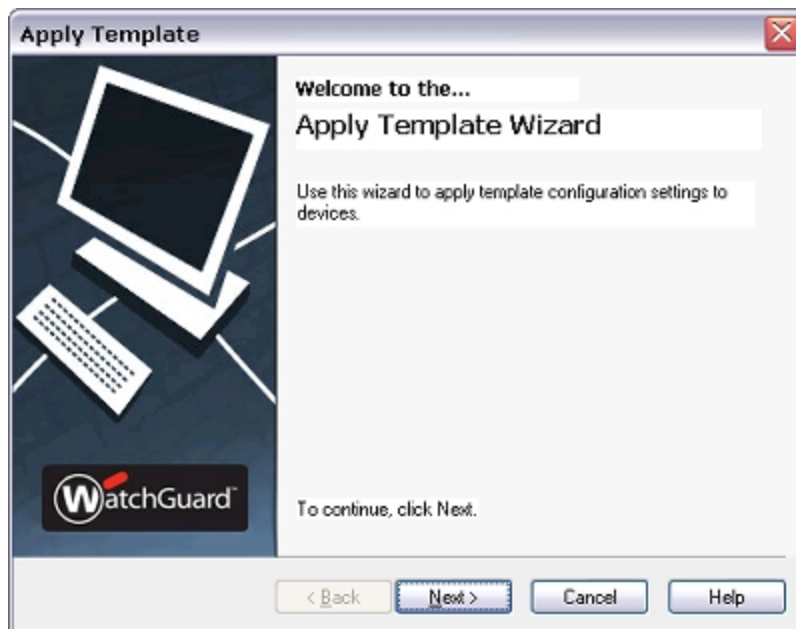
You can use the Apply Template Wizard to simultaneously apply a template to one or more fully managed XTM devices of the same type.

1. In the **Device Configuration Templates** list, select the template to apply to your device.

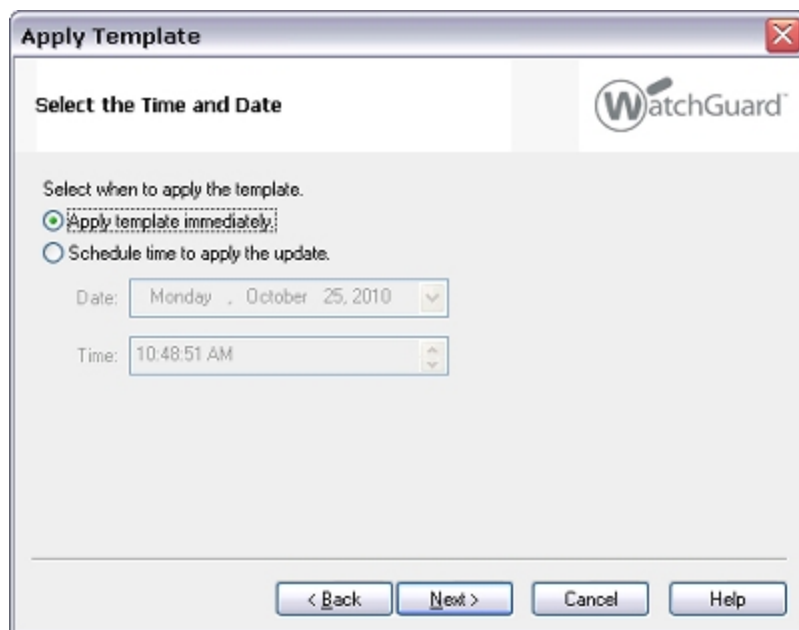
*The selected Device Configuration Template settings page appears.*



- In the **Inheritance Settings** section, click **Apply Template**.  
*The Manage Device List appears.*



- Click **Next**.  
*The Select the devices page appears.*
- Select the check box for each device to which you want to apply this template.
- Click **Next**.  
*The Select time and date page appears.*



6. Select an option to apply the template:
  - **Apply template immediately.**
  - **Schedule time to apply the update.**
    - a. From the **Date** drop-down list, select the day to apply the template.
    - b. In the **Time** text box, type or select the time to apply the template.
7. Click **Next**.

*The Schedule the configuration update page appears.*
8. Click **Next**.

*The Management Server creates the schedule for the template application. The Apply Template Wizard is Complete page appears.*
9. Click **Close**.

*The managed devices you select are subscribed to the Device Configuration Template at the scheduled time.*

## About Configuration History and Template Application History

Each time you update the configuration file for a fully managed device or update a Device Configuration Template, the Management Server stores the new version of the XML configuration file or template in the configuration history for that device or template. You can review the configuration history to see the details of when a file or template was changed, view a configuration file for a device or template to verify the settings in the file, see which devices a template has been applied to and when it was applied, and revert to a previous version of the configuration file for your device or template.

Configuration files saved in the history include all the policies and settings in the XML configuration file, but do not include any managed VPN tunnels, licenses, or certificates for your device. When you configure settings for your Management Server, you can specify the number of files to save in the configuration history for a device or template and require that users add a comment about the changes they made.

For more information about how to configure these settings, see *Define Configuration History Settings* and *Configure License Key, Device Monitoring, and Notification Settings*.

On the settings page for a fully managed device or Device Configuration Template, you can review the basic details of the configuration history: the last time the file was updated in the history, the number of files saved in the history, and the amount of disk space on the Management Server used by the configuration history.

## Review Configuration History and Application History Details

To see more details in the configuration history for a device or template:

1. Open WatchGuard System Manager and connect to a Management Server.
2. In the left navigation pane, select a fully managed device or a configuration template.  
*The settings page for the selected device or template appears.*
3. In the **Configuration History** section, click **View History**.  
*For a fully managed device, the Configuration History dialog box appears. For a Device Configuration Template, the History dialog box appears.*

For a fully managed device, the **Configuration History** dialog box includes this information about the selected device:

- The last time the configuration file was saved to the Management Server.
- The user name of the user who made the change.
- The OS version on the device when the change was made.
- Any comments the user made about the change.
- The amount of disk space on the Management Server used by the configuration history.

For a Device Configuration Template, the **History** dialog box includes two tabs: **Configuration History** and **Application History**.

The **Configuration History** tab includes this information about the selected template:

- The last time the configuration file was saved to the Management Server.
- The user name of the user who made the change.
- The OS version on the device when the change was made.
- Any comments the user made about the change.
- The amount of disk space on the Management Server used by the configuration history.

The **Application History** tab includes these details about the application history of the selected template:

- When a template was applied.
- The user who applied the template.
- The first five devices to which the template was applied.

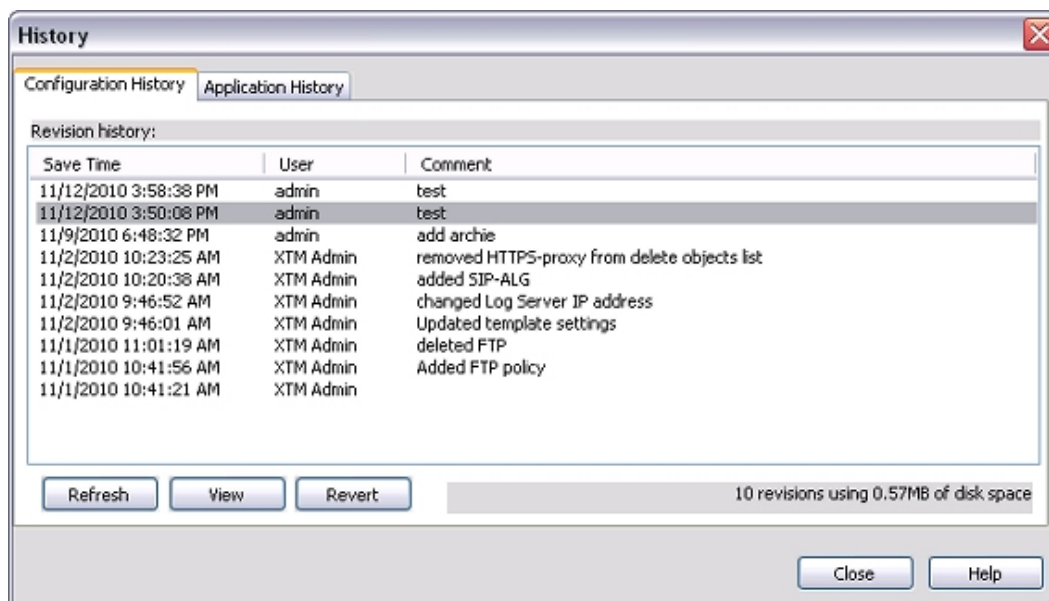
To review the settings in a configuration file for a device or template, you can open a file in the **Revision History** list. You cannot save a configuration file that you have opened from the history. To reapply a configuration file from the configuration history to a device or template, you must revert to an earlier configuration. For more information, see the subsequent section.

To make sure the dialog box includes the most recent changes to the history, such as the time a configuration file was reverted, you can click **Refresh** to update the history information that appears in the list.

To review the settings of a configuration file in the revision history:

1. Select the **Configuration History** tab.

*The Revision history list appears.*



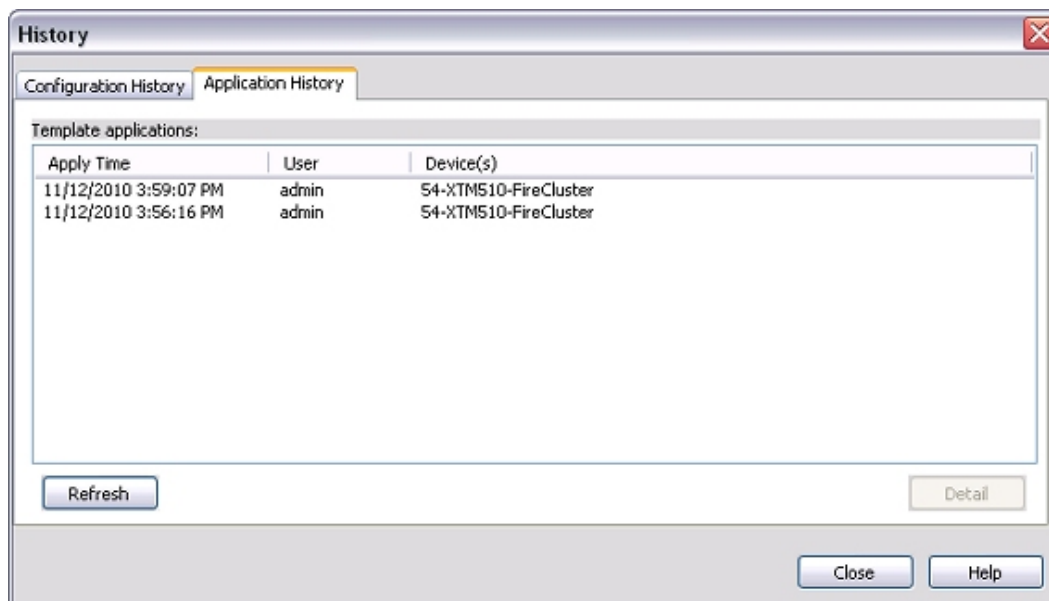
2. To refresh the data in the list, click **Refresh**
3. From the **Revision history** list, select an item.
4. Click **View**.

*Policy Manager opens for the selected configuration file.*

For more information about an applied template, and the complete list of devices to which the template was applied, you can open an item in the **Template applications** list.

1. Select the **Application History** tab.

*The Template applications list appears.*





2. To refresh the data in the list, click **Refresh**
3. From the **Template applications** list, select an item.
4. Click **Detail**.

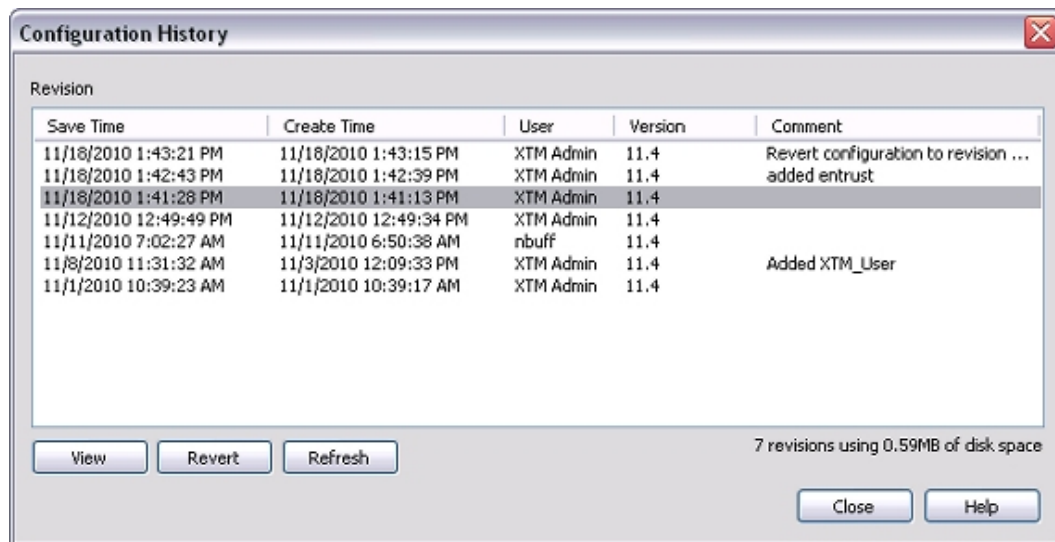
*The Details dialog box appears with all the details about when the template was applied, who applied the templates, and the complete list of devices to which the template was applied.*

## Revert to an Earlier Configuration

You can revert to an earlier configuration file that is included in the **Revision history** list for a device or template. When you revert to an earlier version of a configuration file, the current configuration file is replaced by the earlier version you selected. All the configuration settings in the earlier version are applied to the device or template, except for managed tunnels which are stored separately on the Management Server.

To reapply a configuration file in the history:

1. To refresh the data in the list, click **Refresh**.
2. From the **Revision** list, select an item.



3. Click **Revert**.  
*A confirmation message appears.*
4. Click **Yes**.  
*The Comment dialog box appears.*
5. Type a comment to include in the revision history for the configuration file. Click **OK**.  
*The configuration file is saved to your device and a new entry appears in the Revision History list.*

## Manage Aliases for Firebox X Edge Devices

Aliases are used with your managed Firebox X Edge devices to define a common destination for policy configuration on the Management Server. For example, with aliases, you can create a Device Configuration Template for a mail server, and define that policy to operate with your mail server. Because the mail server can have a different IP address on each Firebox network, you create an alias on the Management Server

called *MailServer*. When you create the Device Configuration Template for the mail server, you use this alias as the destination. Then you define that alias as either the source or destination, to match the direction of the network traffic managed by the policy. In this example, you can configure an incoming *SMTP Allow* policy with *MailServer* as the destination.

For the Device Configuration Template to operate correctly on devices that use the policy, you must configure the *MailServer* alias in the Network Settings for each Firebox X Edge device.

The alias features that were available in WatchGuard System Manager (WSM) 10.x for your 10.x and older Firebox X Edge devices are still available in WSM v11.x. You can use your v11.x Management Server to configure aliases only for v10.x and older Firebox X Edge devices.

You configure an alias in two steps:

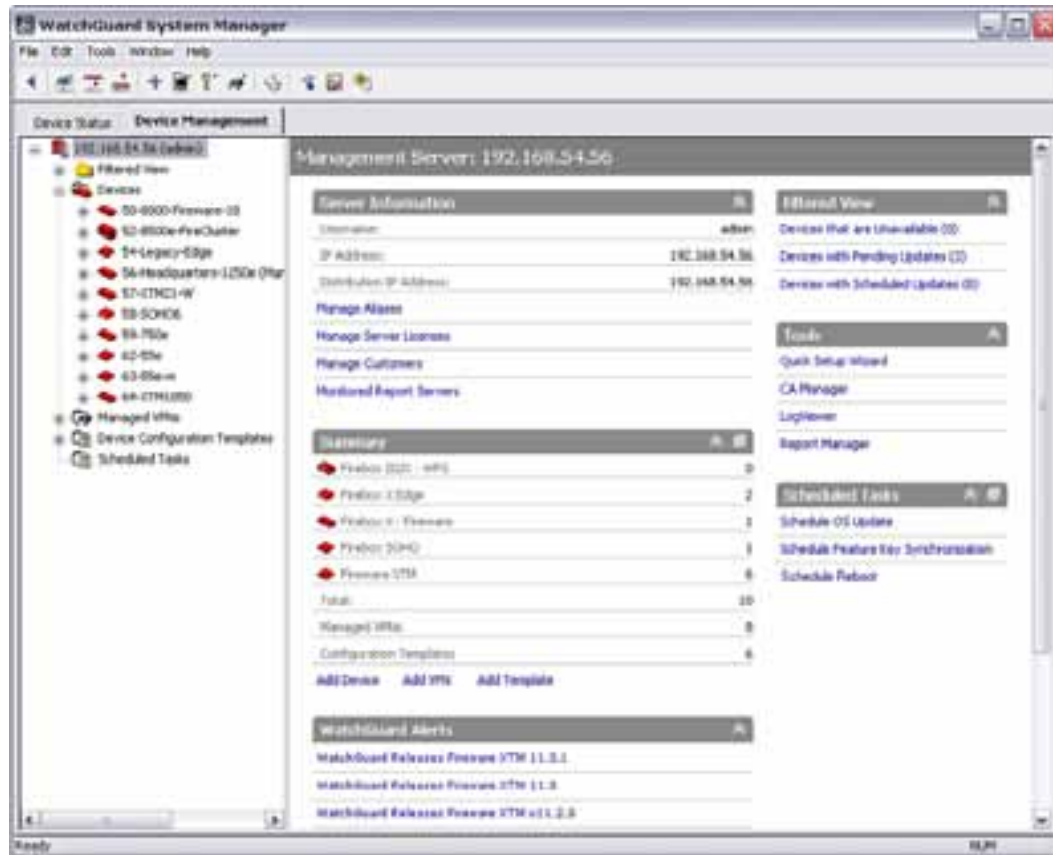
1. *Change the Name of an Alias.*
2. *Define Aliases on a Firebox X Edge Device.*


## Change the Name of an Alias

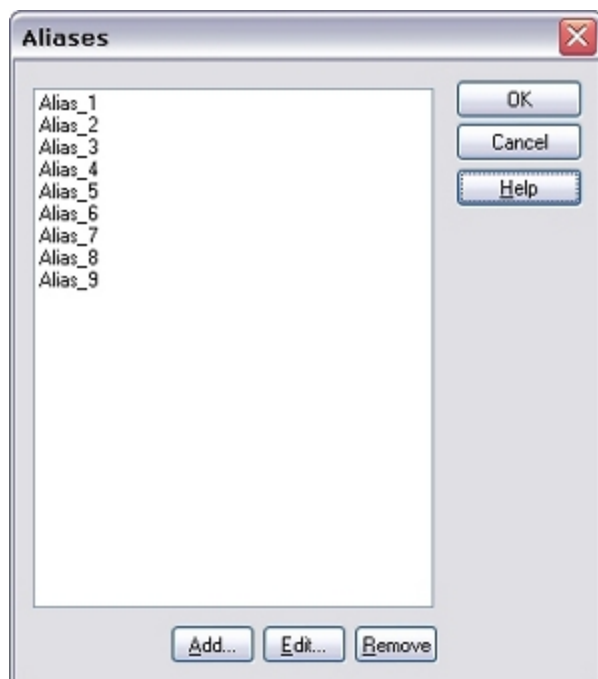
Your Management Server includes a standard set of aliases that you can use with the policies for your Firebox X Edge device (version 10.x and older only). You can add a new alias or rename an existing alias. Before you can add an alias to a policy, you must create or edit the alias on the Management Server.

From the WatchGuard System Manager **Device Management** tab:

1. In the **Device Management** tree, select the Management Server.  
*The Management Server settings page appears.*



2. Click .  
Or, in the **Server Information** section, click **Manage Aliases**.  
*The Aliases dialog box appears.*



3. To add a new alias, click **Add**.  
*The Add Alias dialog box appears.*  
  
To change an existing alias, select an alias and click **Edit**.  
*The Edit Alias Name dialog box appears.*
4. In the **Name** text box, type a name for the alias and click **OK**.
5. Repeat Steps 3–4 to define additional aliases.
6. Click **OK**.

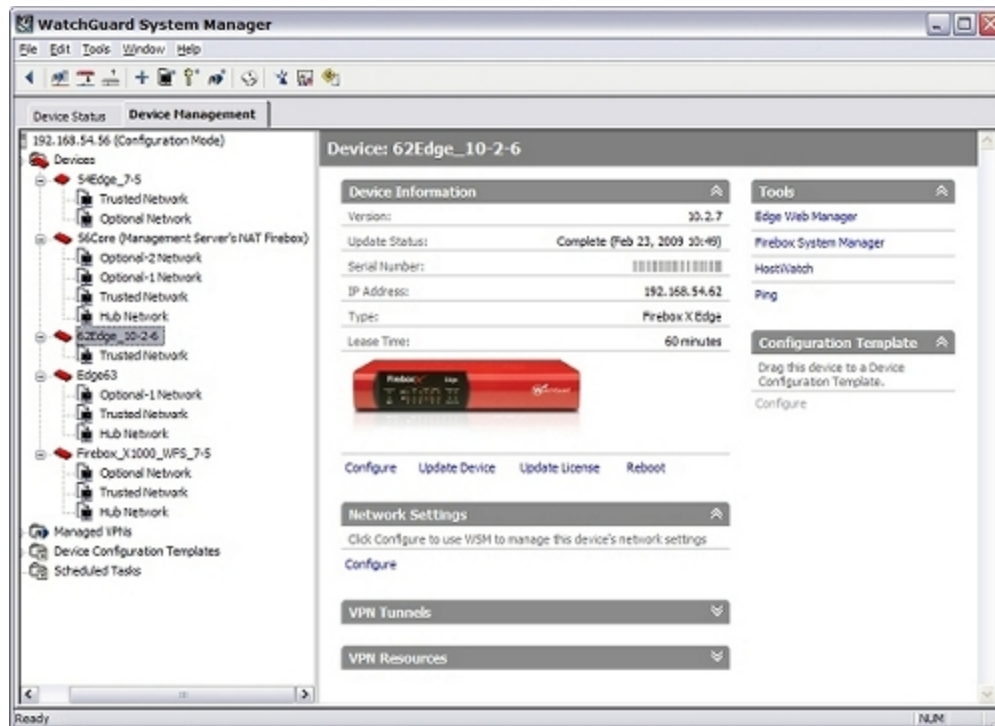
Next, you can assign IP addresses to the aliases, as described in *Define Aliases on a Firebox X Edge Device* on page 660.

## Define Aliases on a Firebox X Edge Device

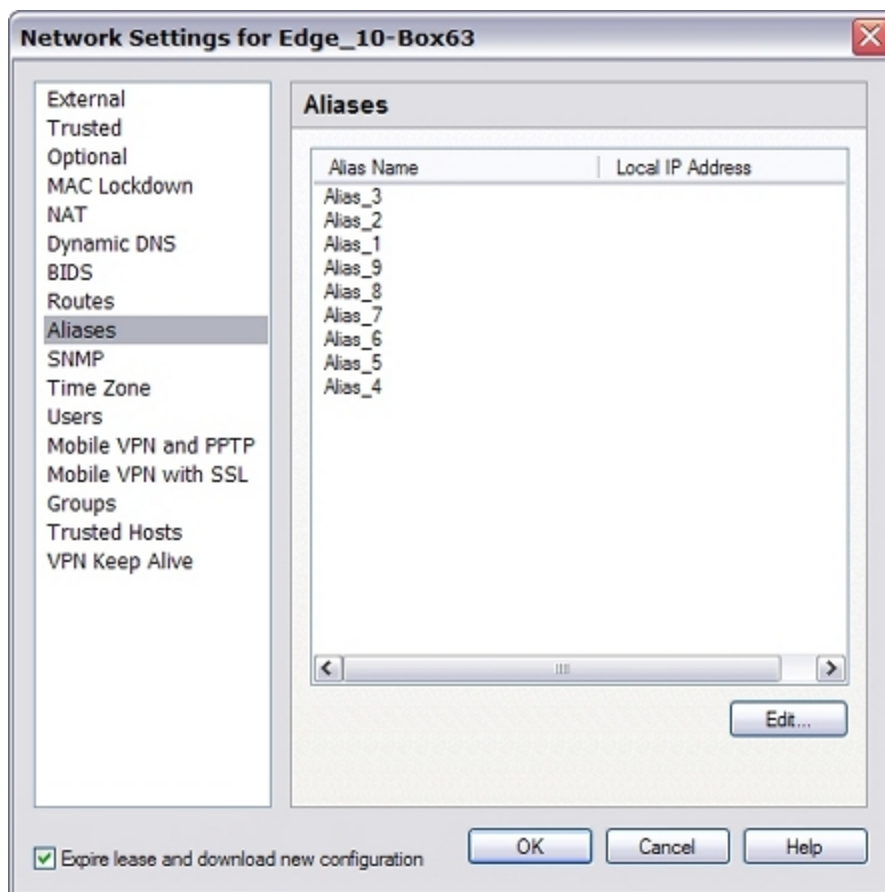
After you have updated the list of aliases on your Management Server, you can define the aliases for use with your Firebox X Edge devices (version 10.x or older only).

From the WatchGuard System Manager **Device Management** tab:

1. Expand the **Devices** tree and select a version 10.x or older Firebox X Edge device.  
*The Device page appears.*



2. In the **Network Settings** section, click **Configure**.  
*The Network Settings dialog box appears.*
3. Click **Aliases**.  
*The Aliases list appears. The list includes those aliases you named on the Management Server and any default aliases.*



4. Select an alias to define and click **Edit**.  
*The Local Alias Setting dialog box appears.*



5. Type the **IP Address** for the local alias on the network of this Firebox X Edge.
6. Click **OK**.
7. To define another alias, repeat Steps 4–6.
8. Click **OK**.

## Remove a Device from Fully Managed Mode

You can remove your Firebox or XTM device from Fully Managed Mode and return it to Basic Managed Mode. When you do this, the Management Server keeps the configuration files that have been saved in the history for the device, but does not save any subsequent changes to the configuration file for the device.

To remove a device from Fully Managed Mode, you can change the Device Management Mode for the device to Basic Managed Mode or completely remove the device from management by the Management Server.

For instructions to change the management mode for a device, see *Change the Centralized Management Mode* on page 587.

For instructions to completely remove a device from management, see *Update or Reboot a Device, or Remove a Device from Management*.





# 20 Role-Based Administration

---

## About Role-Based Administration

Role-based administration enables you to share the configuration and monitoring responsibilities for your organization among several individuals. One or more senior administrators might have full configuration privileges for all devices, while one or more junior administrators have less configuration and monitoring authority or different areas of jurisdiction.

For example, one administrator might have complete configuration and monitoring authority over all of the XTM devices in an organization's Eastern region, but could only monitor the devices deployed in the company's Central and Western regions. Another administrator could have full authority over the Central region, but could only monitor Western and Eastern region devices.

You can use WatchGuard System Manager (WSM) and WatchGuard Server Center to create and implement the different administrator roles for your organization. All the role-based administration settings you create are stored and managed on your Management Server, so they are accessible with WSM or WatchGuard Server Center. When you make a change to role-based administration with WSM, the change automatically appears in WatchGuard Server Center.

**Note** *Role-based administration is only available for Firebox or XTM devices with Fireware XTM v11.0 or later.*

## Roles and Role Policies

A *role* has two parts: a set of tasks, and a set of devices on which these tasks can be performed. Every administrator is assigned one or more roles, such as Super Administrator, Mobile User VPN Administrator, or User Authentication Administrator.

WatchGuard System Manager (WSM) has several predefined roles you can use for your own organization. You can also define custom roles. These roles are recognized by all the WSM tools and WatchGuard servers. For example, if you log in to WSM with read/write permissions, and open Firebox System Manager (FSM), you are not prompted for the configuration passphrase because FSM recognizes that you are logged in with sufficient permissions.

*Role policies* combine the sets of tasks and devices with the users who have the privileges to perform those roles.

## Audit Trail

To keep track of the actions performed by each administrator, WSM stores an audit trail of changes made to a device. These changes are recorded in the Management Server log messages. WSM also has an audit trail that shows all changes made to the entire system, the administrator who made each change, and when each change was made.

## About Predefined Roles

Your XTM device has many predefined administrative roles. You can also define custom roles, as described in *Define Roles and Role Properties* on page 675.

The subsequent table shows all predefined roles and the actions they are allowed to take.

Role	Allowed actions
Branch Office VPN Administrator	View folders and devices in WSM
	View device log messages
	View/create device reports
	Configure device network configuration, policies, and BOVPN tunnels
	Rekey BOVPN tunnels for a device
Device Administrator	View and move folders and devices in WSM
	View/modify folder and device management server properties
	View device log messages
	Define a report of any device
	Set device passphrases
	Configure Reputation Enabled Defense settings
Device Monitor	View folders and devices in WSM
	View device log messages and reports
	View the entire configuration file for a device
	View Reputation Enabled Defense settings

Role	Allowed actions
Legacy admin account	<ul style="list-style-type: none"> <li>View and move folders in WSM</li> <li>View/modify folder and device Management Server properties</li> <li>View/move devices in WSM and monitoring tools</li> <li>View device log messages</li> <li>View/create device reports</li> <li>Set the device configuration (admin) and monitoring (status) passphrase</li> <li>View/modify device configuration file</li> <li>Update device OS</li> <li>Backup/restore device configuration and OS</li> <li>Reboot/restart device</li> <li>Configure device network configuration, Firewall Policies, QoS Settings, BOVPN tunnels, and Mobile VPN tunnels</li> <li>Drop currently active device Mobile VPN user tunnels</li> <li>Configure device external authentication, Firebox users and groups, WebBlocker, spamBlocker, and Quarantine Server settings</li> <li>Update Gateway AV/IPS signatures</li> <li>Rekey device BOVPN tunnels and Mobile VPN tunnels</li> <li>Update the device feature keys</li> <li>Configure Reputation Enabled Defense settings</li> </ul>
Legacy status account	<ul style="list-style-type: none"> <li>View folders in WSM</li> <li>View folder and device Management Server properties</li> <li>View devices in WSM and monitoring tools</li> <li>View device log messages</li> <li>View device reports</li> <li>View device configuration file</li> <li>View Reputation Enabled Defense settings</li> </ul>
Management Server Administrator	<ul style="list-style-type: none"> <li>Define devices, folders, security templates, VPN firewall policies, and customer information</li> <li>Has Certificate Authority access</li> <li>Define a report or view audit log messages of any user</li> <li>Define a report of any device</li> </ul>

Role	Allowed actions
	Configure Reputation Enabled Defense settings
Management Server Monitor	<ul style="list-style-type: none"> <li>View folders and devices in WSM</li> <li>View role policies</li> <li>View security templates</li> <li>View VPN Firewall policies</li> <li>View customer information</li> <li>Access to Certificate Authority</li> <li>View a report or view audit log messages of any user</li> <li>View a report of any device</li> </ul>
Mobile User VPN Administrator	<ul style="list-style-type: none"> <li>View folders and devices in WSM</li> <li>View device log messages</li> <li>View/create device reports</li> <li>Configure device network configuration and Mobile VPN tunnels</li> <li>Drop active Mobile VPN user tunnels for a device</li> <li>Define users and groups for a device</li> <li>Rekey BOVPN tunnels for a device</li> </ul>
MSS Monitor	View devices in monitoring tools
Network Administrator	<ul style="list-style-type: none"> <li>View folders and devices in WSM</li> <li>View device log messages</li> <li>View/create device reports</li> <li>Configure device network configuration</li> </ul>
Security Administrator	<ul style="list-style-type: none"> <li>View folders and devices in WSM</li> <li>View device log messages</li> <li>View/create device reports</li> <li>Configure device network configuration, policies, and QoS settings</li> <li>Update Gateway AV/IPS signatures</li> </ul>

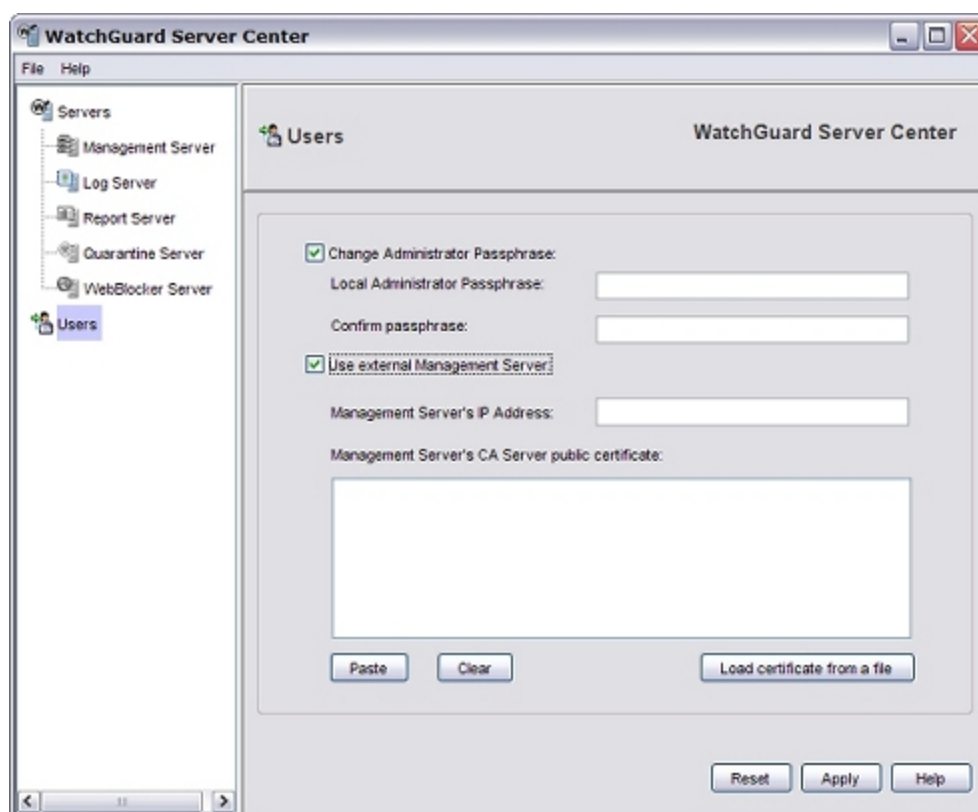
Role	Allowed actions
Super Administrator	Define users, role policies, devices, folders, security templates, VPN firewall policies, and customer information Has Certificate Authority access Define a report or view audit log messages of any user Define a report of any device
User Authentication Administrator	View folders and devices in WSM View device log messages View/create device reports Configure device external authentication Define users and groups for a device
User Services Administrator	View folders and devices in WSM View device log messages View/create device reports Configure WebBlocker, spamBlocker, and Quarantine Server settings for a device

## Use Role-Based Administration with an External Management Server

If you have a WatchGuard Log Server or Report Server installed on a different computer than your Management Server, you can use WatchGuard Server Center to set contact information for the Management Server that you want to use for role-based administration. After you configure these settings, the Log Server or Report Server can contact the selected Management Server for the role and credential information for remote users.

To configure settings for an external Management Server:

1. In the left navigation bar, select **Users**.  
*The Users page appears.*



2. To change the passphrase for the local administrator, select the **Change Administrator Passphrase** check box.
3. Type and confirm the password for the local administrator.
4. Select the **Use external Management Server** check box.
5. Type the **Management Server's IP address**.
6. In the **Management Server's CA Server public certificate** field, copy and paste the content of the certificate for the Management Server.  
Or, click **Load certificate from a file** to select and upload the certificate.
7. Click **Apply**.

## Define or Remove Users or Groups

You can define, edit, and remove users and user groups for role-based administration in WatchGuard System Manager (WSM) and WatchGuard Server Center. You can choose how a user or group is authenticated and define the password for a local user.

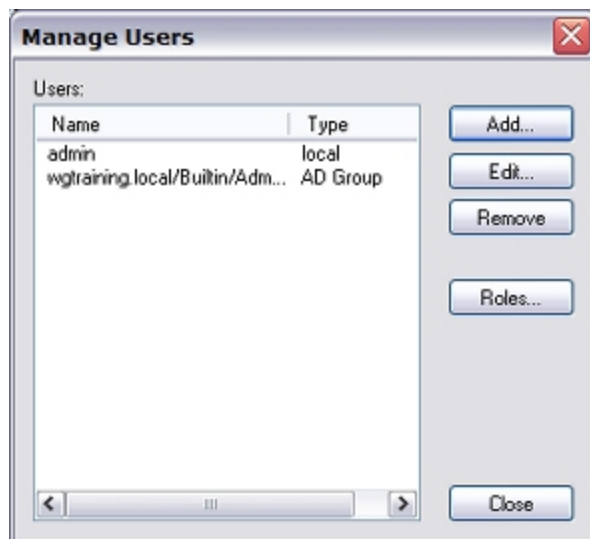
When you edit a user or group, you can change all the details for the user or group, but you cannot change the user or group name. Instead, you must instead remove the existing user or group and then add a new user or group with the new name.

To use an Active Directory server to authenticate a user or group, before you define users or groups, you must *Enable and Configure Active Directory Authentication*.

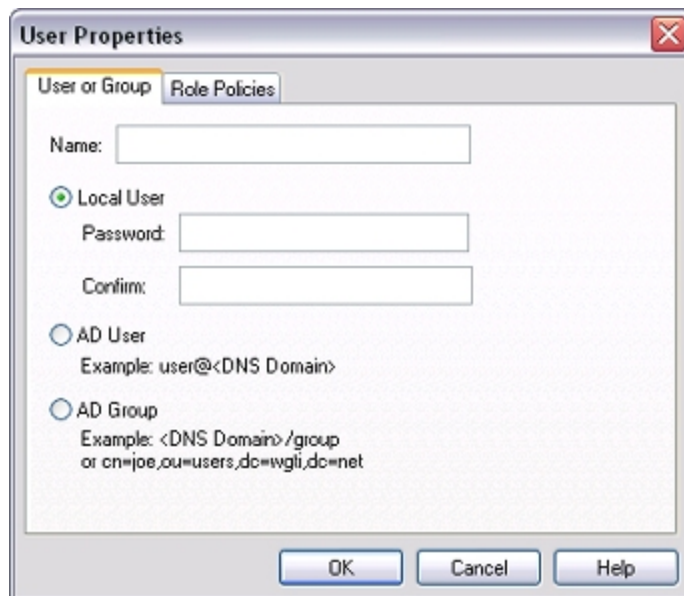
## Use WatchGuard System Manager to Configure Users or Groups

1. Use WSM to Connect to your Management Server.
2. Select **File > Manage Users**.

*The Manage Users dialog box appears.*



3. To add a new user, click **Add**.  
To edit details for an existing user, select a user from the list and click **Edit**.  
*The User Properties dialog box appears.*



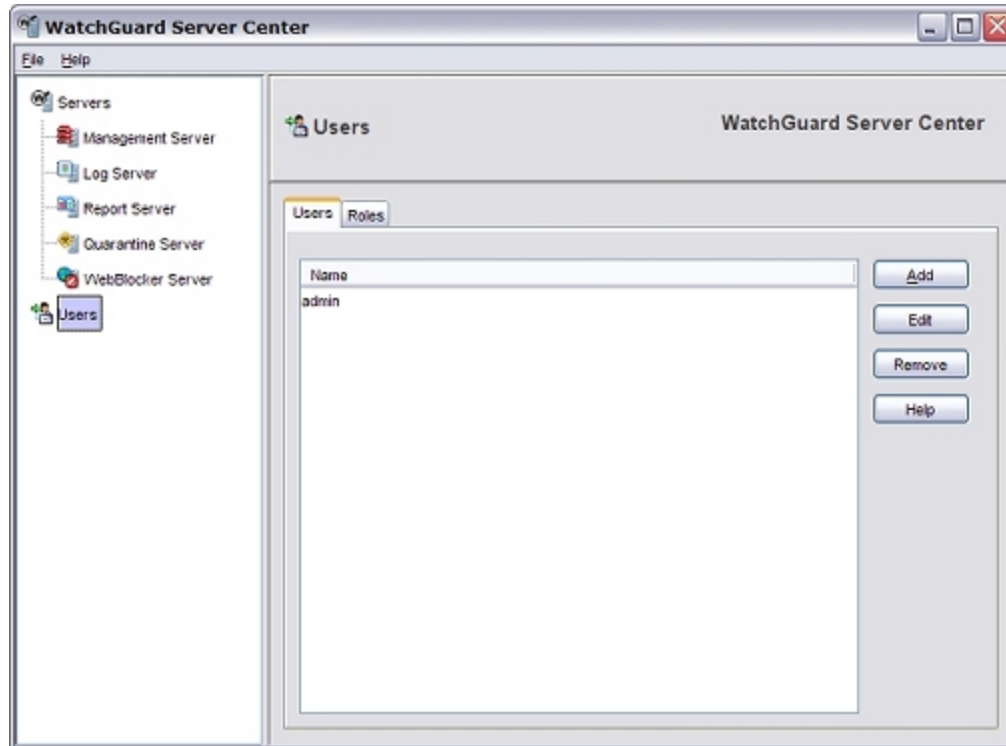
4. On the **User or Group** tab, in the **Name** text box, type a name for the user or group.
5. To define a new user to be authenticated locally, select **Local User**.  
To define a new user to be authenticated to an Active Directory server, select **AD User**.  
This is the principal name for the user in Active Directory.  
To define a new group to be authenticated to an Active Directory server, select **AD Group**.  
This is either the distinguished name or canonical name for the group in Active Directory.
6. If you define or edit a local user, in the **Password** text box, type a new password.
7. In the **Confirm Password** text box, type the password again.
8. If you added a new user or group, select the **Role Policy** tab to assign a Role Policy to the user or group.  
For more information, see *Assign Roles to a User or Group* on page 678.
9. Click **OK**.



## Use WatchGuard Server Center to Configure Users or Groups

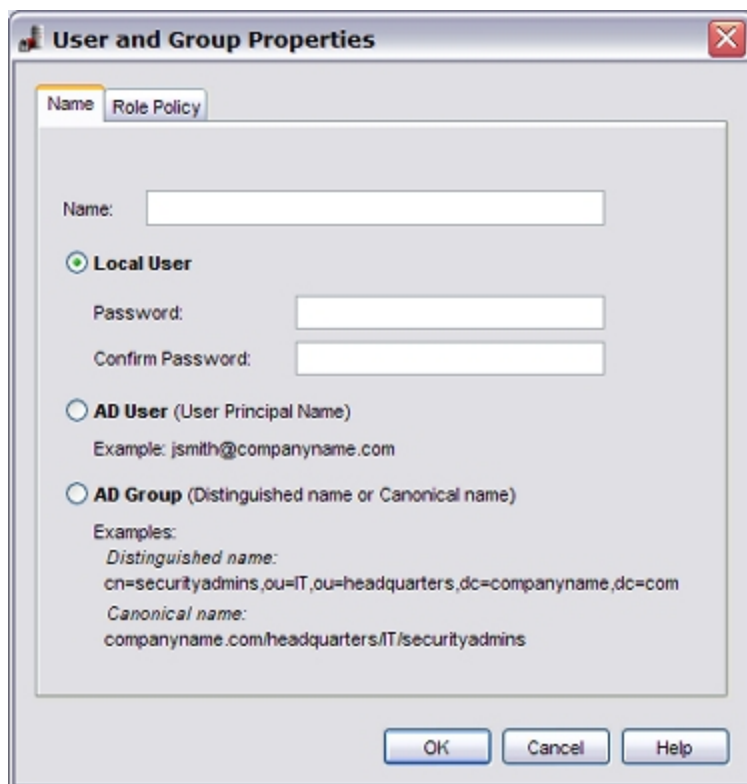
1. In the left navigation bar, select **Users**.

*The Users page appears.*



2. To add a new user, click **Add**.  
To edit details for an existing user, select a user from the list and click **Edit**.

*The User and Group Properties dialog box appears.*



3. In the **Name** text box, type a name for the user or group.
4. To define a new user to be authenticated locally, select **Local User**.  
To define a new user to be authenticated to an Active Directory server, select **AD User**.  
To define a new group to be authenticated to an Active Directory server, select **AD Group**.
5. If you define or edit a local user, in the **Password** text box, type a new password.
6. In the **Confirm Password** text box, type the password again.
7. If you added a new user or group, select the **Role Policy** tab to assign a Role Policy to a user or group.  
For more information, see *Assign Roles to a User or Group* on page 678.
8. Click **OK**.

## Remove a User or Group

You can not remove predefined users or groups. You can only remove user-defined users and groups.

To remove a user or group:

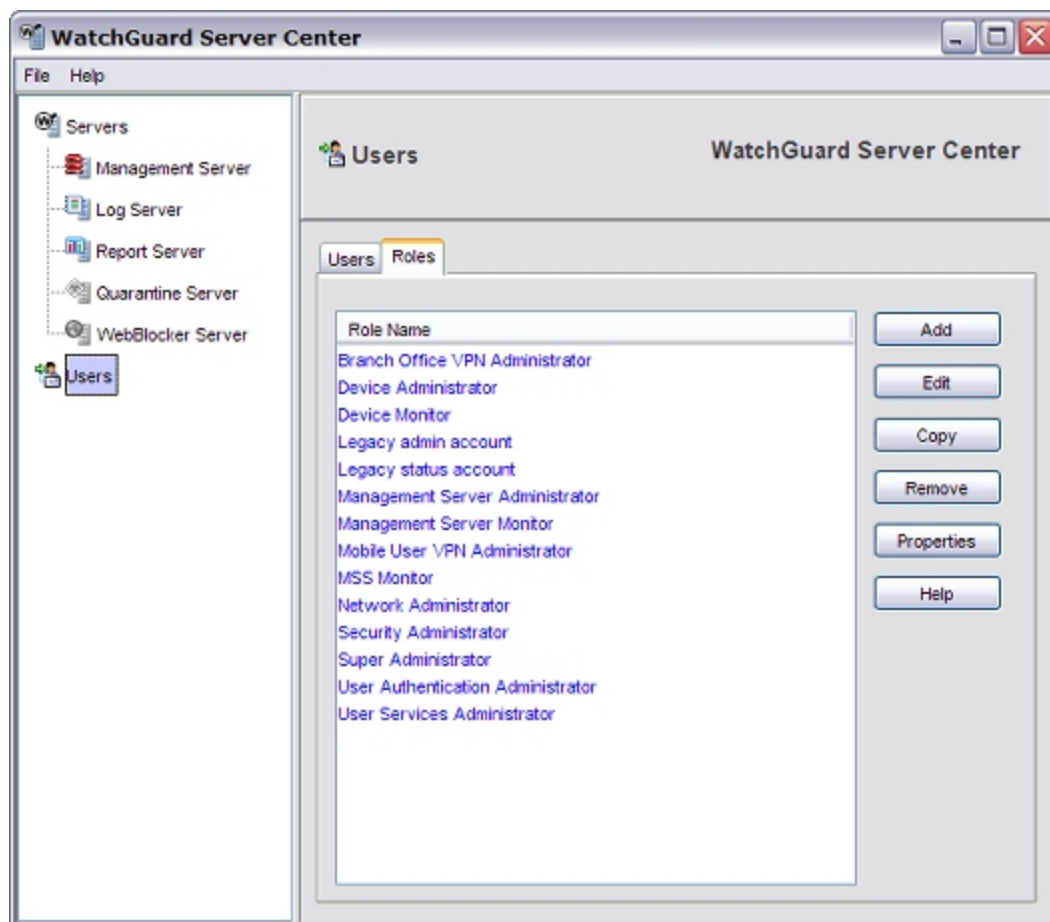
1. In the **Users** list, select the user or group you want to delete.
2. Click **Remove**.  
*A message dialog box appears and asks if you are sure you want to delete the user or group.*
3. Click **Yes**.  
*The user or group is removed from the list.*

## Define Roles and Role Properties

You can use WatchGuard Server Center and WatchGuard System Manager to define and edit roles and role policies on your Management Server for your role-based administration users and user groups. You can only edit user-defined roles. If you want to change a predefined role, copy the role to a new role and make your changes.

### Define Roles in WatchGuard Server Center

1. In the left navigation bar, select **Users**.  
*The Users page appears.*
2. Select the **Roles** tab.  
*Predefined roles appear in blue. Any user-defined roles appear in black.*

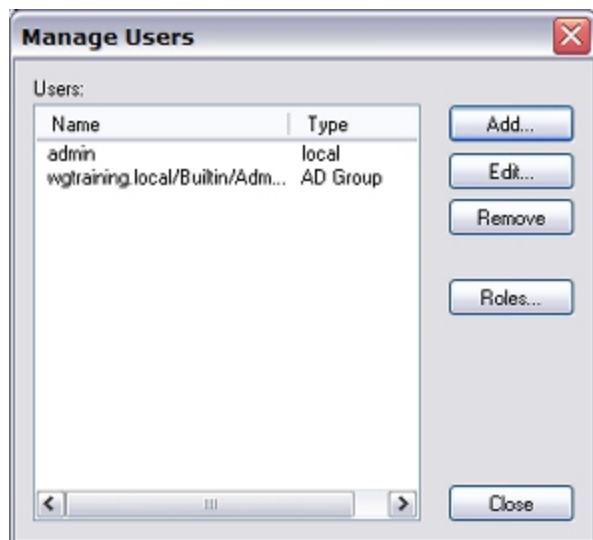


3. Follow the instructions in the subsequent *Configure roles and role policies* section.

## Define Roles in WatchGuard System Manager

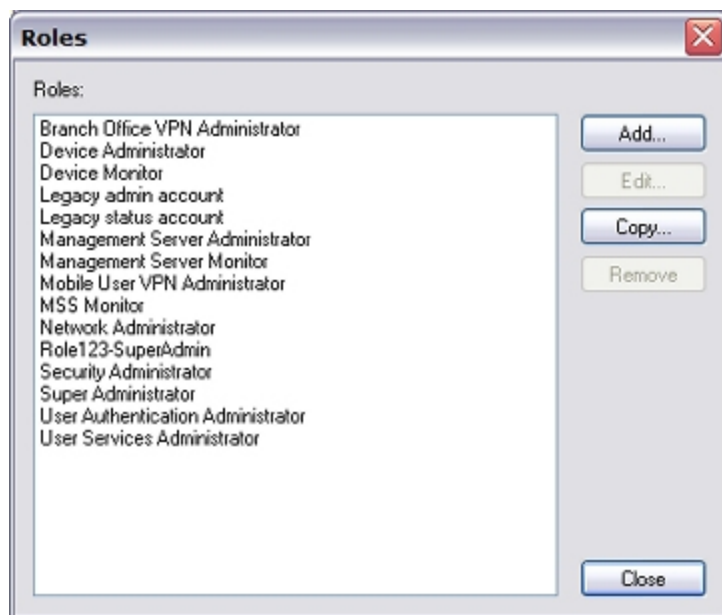
1. Open WatchGuard System Manager and Use *WSM to Connect to your Management Server*.
2. Select **File > Manage Users**.

*The Manage Users dialog box appears.*



3. Click **Roles**.

*The Roles dialog box appears.*



4. Follow the instructions in the subsequent *Configure roles and role policies* section.

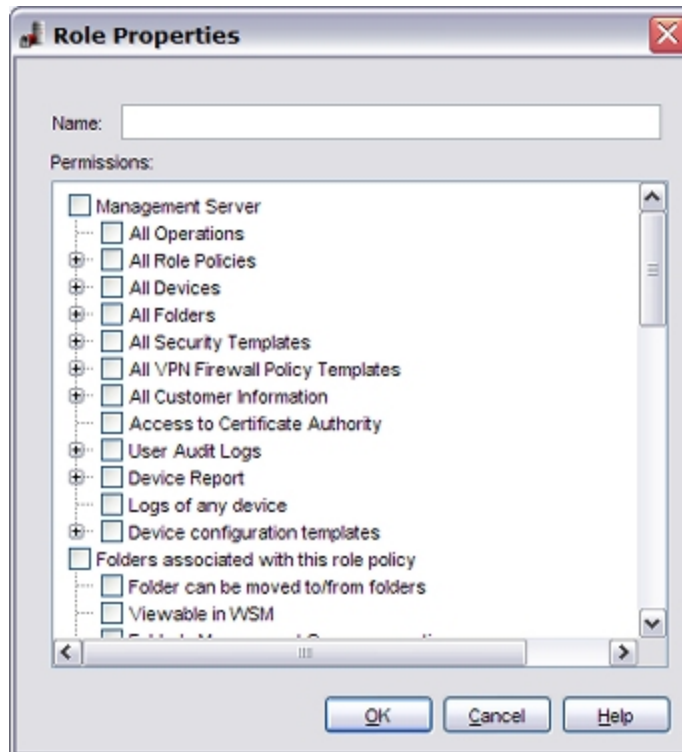
## Configure Roles and Role Properties

1. To define a new role, click **Add**.

To edit an existing role, select the role and click **Edit**.

You can only edit user-defined roles, not predefined roles. If you want to define a new role based on an existing predefined role, select the predefined role, and click **Copy**.

*The Role Properties dialog box appears.*



2. In the **Name** text box, type a name for the new role.
3. In the **Permissions** window, select the set of permissions you want to assign to the role.  
When you select or clear the check box for a top level permission, all the permissions in that list are also selected or removed.
4. Click **OK**.

## Remove a Role

You cannot remove predefined roles from the Management Server. You can only remove user-defined roles.

To remove a user-defined role:

1. Select a role in the list.
2. Click **Remove**.  
*A message dialog box appears and asks if you want to delete the role.*
3. Click **Yes**.  
*The role is removed from the list.*

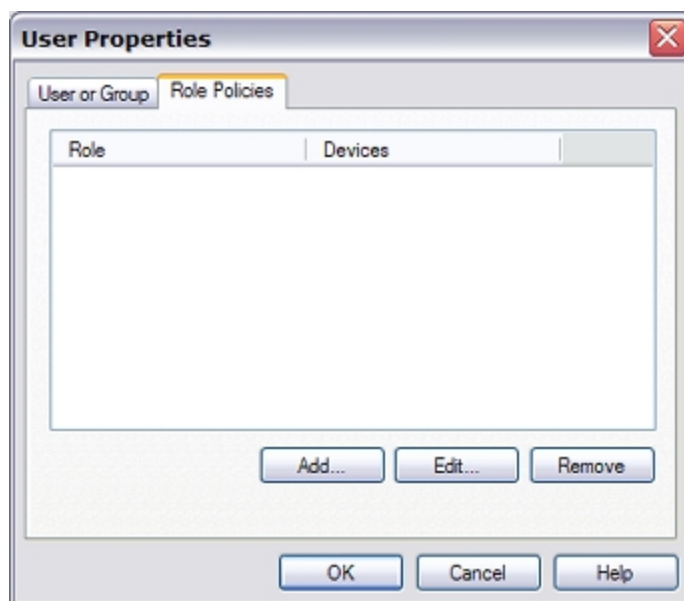
## Assign Roles to a User or Group

A *role policy* combines the tasks and devices that make up a role with one or more users who are assigned to those rules. You can use WatchGuard System Manager or WatchGuard Server Center to assign one or more roles to a user or user group. When you assign more than one role to a user or group, that user or group can complete all of the tasks for all devices from both roles.

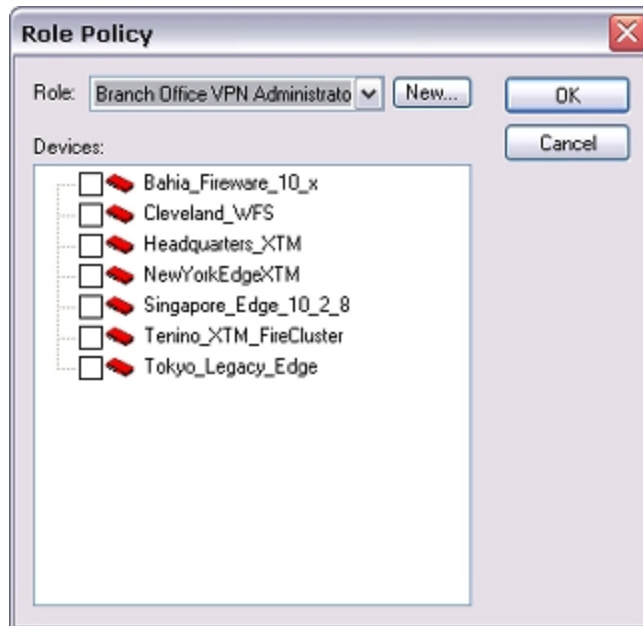
### Assign Roles in WatchGuard System Manager

To add a new role to a user or group, or edit an existing role:

1. Use WSM to Connect to your Management Server.
2. Select **File > Manage Users**.  
*The Manage Users dialog box appears.*
3. Define a user and click **Add**.  
Or, select a user from the **Users** list and click **Edit**.  
*The User Properties dialog box appears.*  
For more information, see *Define or Remove Users or Groups* on page 671.
4. Select the **Role Policies** tab.



5. To add a new role, click **Add**.  
To edit an existing role, select a role from the **Role** list and click **Edit**.  
*The Role Policy dialog box appears.*



- From the **Role** drop-down list, select an existing role.  
Or, click **New** to define a custom role.

For more information, see *Define Roles and Role Properties* on page 675.

- From the **Devices** list, select the check box for each XTM device to include in the role policy.
- Click **OK**.  
*The role appears in the list on the Role Policies tab.*
- Click **OK**.

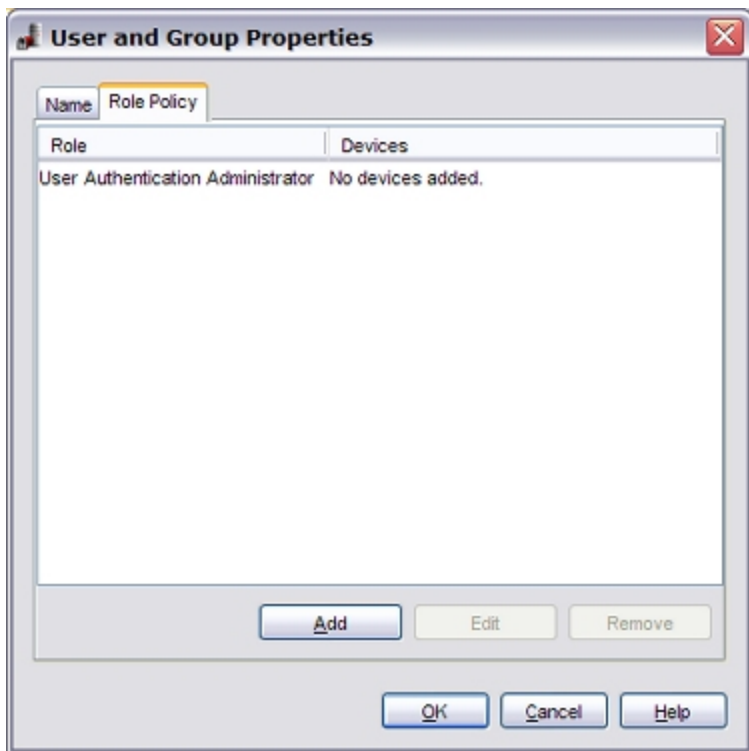
To remove a role from a user or group:

- In the **User Properties** dialog box, select a role in the **Role** list.
- Click **Remove**.  
*A confirmation message appears.*
- Click **Yes** to delete the role from the **Role** list.

## Assign Roles in the WatchGuard Server Center

To add a new role or edit an existing role to a user or group:

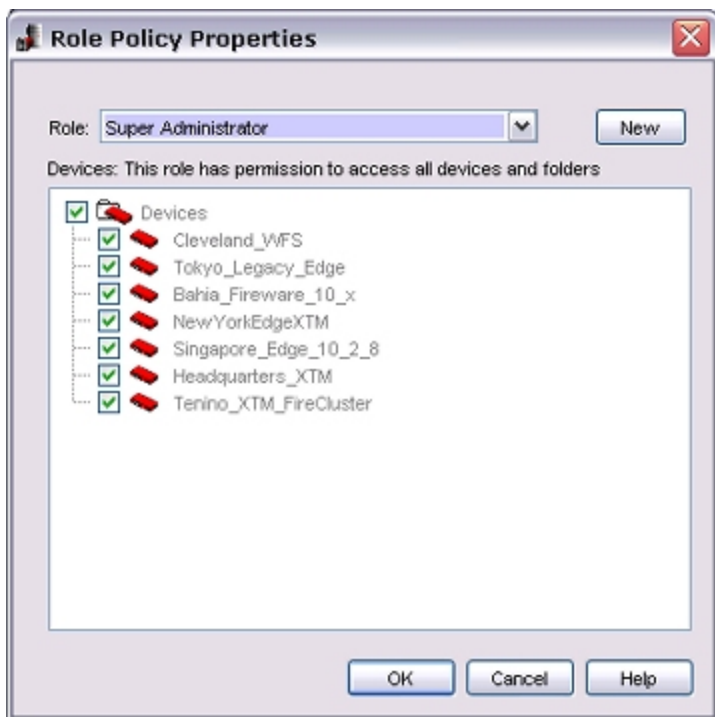
- In the left navigation bar, select **Users**.  
*The Users page appears.*
- Select the **Users** tab.
- Click **Add**.  
*The User and Group Properties dialog box appears.*
- Click the **Role Policy** tab.  
*A list of the roles assigned to the user or group appears. The name of the role or roles appears in the Role column. A comma-delimited list of devices associated with the role appears in the Devices column.*



5. To add a new role policy for the user or group, click **Add**.

To edit an existing role policy, select it and click **Edit**.

*The Role Policy Properties dialog box appears.*





6. From the **Role** drop-down list, select an existing role.  
Or, click **New** to define a custom role.

For more information, see *Define Roles and Role Properties* on page 675.

7. From the **Devices** list, select the check box for the set of devices and folders to assign to this user and role.
8. Click **OK**.

To remove a role from a user or group:

1. In the **User and Group Properties** dialog box, select a role from the **Role** list.
2. Click **Remove**.  
*A confirmation message appears.*
3. Click **Yes** to delete the role from the **Role** list.



# 21 Logging and Notification

---

## About Logging and Log Files

An important feature of network security is to gather messages from your security systems, to examine those records frequently, and to keep them in an archive for future reference. The WatchGuard log message system creates log files with information about security related events that you can review to monitor your network security and activity, identify security risks, and address them.

A *log file* is a list of events, along with information about those events. An *event* is one activity that occurs on the XTM device. An example of an event is when the device denies a packet. Your XTM device can also capture information about allowed events to give you a more complete picture of the activity on your network.

The log message system has several components, which are described below.

## Log Servers

WatchGuard Log Servers collect log message data from each connected device or server. Log Servers receive information on TCP ports 4107 and 4115. Each device that connects to the Log Server first sends its name, serial number, time zone, and software version, then sends log data as new events occur. The serial number (SN) of the XTM device is used to uniquely identify the device in the Log Server database. The Log Server uses multiple instances of the PostgreSQL database to manage its global database. Each instance of the PostgreSQL database appears in Windows Task Manager as a separate PostgreSQL process.

The Log Server uses several processes and modules to collect and store log message data. *wlcollector.exe* is the log collector process. Your XTM device connects to this process for logging on TCP port 4115/4107. *wlcollector.exe* runs two modules: *ap\_collector* and *ap\_notify*. *ap\_collector* gets the logs from the XTM device and puts them in the Log Server database. *ap\_notify* gets alarms from the XTM device and sends the type of notifications you select.

Log messages are sent to the WatchGuard Log Server in XML (plain text) format and are encrypted while in transit. The information collected from firewall devices includes traffic, alarm, event, debug, and performance statistics log messages. This data is not encrypted while stored in the Log Server database.

You can install the WatchGuard Log Server on the computer that is your management computer, or on a different computer. You can also add additional Log Servers for backup and scalability. To do this, use the WatchGuard System Manager (WSM) installation program and select to install only the Log Server component.

After your Log Server has collected the log data from your XTM devices, you can use the WatchGuard Report Server to periodically consolidate the data and generate reports.

For more information about the Report Server and Report Manager, see *About the Report Server* on page 805 and *About WatchGuard Report Manager* on page 830.

## LogViewer

LogViewer is the WatchGuard System Manager tool you use to see log file data. It can show the log data page by page, or search and display by key words or specific log fields.

## Logging and Notification in Applications and Servers

The Log Server can receive log messages from your XTM device or a WatchGuard server. After you have configured your XTM device and Log Server, the device sends log messages to the Log Server. You can enable logging in the various WatchGuard System Manager applications and policies that you have defined for your XTM device to control the level of logs that you see. If you choose to send log messages from another WatchGuard server to the Log Server, you must first enable logging on that server.

For more information about sending log messages from your XTM device, see *Configure Logging and Notification for a Policy* on page 722.

For more information about sending log messages from your WatchGuard server, see *Configure Logging Settings for the Log Server* on page 702.

## About Log Messages

Your XTM device sends log messages to the Log Server. It can also send log messages to a syslog server or keep logs locally on the XTM device. You can choose to send logs to one or both of these locations.

You can use Firebox System Manager to see log messages in the **Traffic Monitor** tab. For more information, see *Device Log Messages (Traffic Monitor)* on page 754.

You can also examine log messages with LogViewer. The log messages are kept on the Log Server in the WatchGuard directory in an SQL database file with a .wgl.xml extension.

To learn more about the different kinds of log messages that the XTM device sends, see *Types of Log Messages* on page 686.

## Log Files

WatchGuard Log Server uses the *wlcollector.log* and *ap\_collector.log* files to store information about device and database connections. This information includes authentication errors, challenge and response mismatches, and database access errors.

These files are stored by default in:

C:\Documents and Settings\WatchGuard\logs\wlogserver\wlcollector\

## Databases

Log information is stored in the PostgreSQL database. Each Log Server has four main database tables that store the log messages for all XTM devices. The Log Server creates fixed-size partitions to store the log information in these databases. To manually modify the contents of the Log Server database, you can use the PostgreSQL command prompt or a third-party application such as *pgadmin*.

When an XTM device connects to the Log Server for the first time, the Log Server updates the global database with information about the new device. Log messages from each device are sent to one of the four Log Server database tables. The data in these tables is used when you look at logs in WatchGuard LogViewer, or create a report with WatchGuard Report Manager. These applications use XMLRPC requests to communicate with the Log Server.

Reports generated by a WatchGuard Report Server are stored as XML files in the C:\Documents and Settings\WatchGuard\wrserver\reports\ directory.

## Performance and Disk Space

You can configure several XTM devices to send log information to a single Log Server. This number is strictly limited only by available disk space. However, the exact number of devices you can connect to your Log Server depends on the size and speed of its hard drives, the amount of available RAM, the number of processors, and the amount of log traffic each connected device sends to the Log Server. You can greatly increase the performance of your Log Server by adding a faster hard drive, more memory, or another processor.

The Log Server includes a setting that you can change to automatically remove old log messages from the database. When you first set up a Log Server, we recommend that you measure how much disk space is used in an average day. Estimate how many days of log messages you can keep before the database takes up too much disk space, then change the settings to match that time interval. When log messages are removed from the database, the disk space is reused when new log entries are created.

The *reindexdb* utility rebuilds the indexes in one or more PostgreSQL database tables for better performance. This utility should be run only at the recommendation of a WatchGuard support representative.

## Types of Log Messages

Your XTM device sends several types of log messages for events that occur on the device. Each message includes the message type in the text of the message. The log messages types are:

- Traffic
- Alarm
- Event
- Debug
- Statistic

## Traffic Log Messages

The XTM device sends traffic log messages as it applies packet filter and proxy rules to traffic that goes through the device.

## Alarm Log Messages

Alarm log messages are sent when an event occurs that triggers the XTM device to run a command. When the alarm condition is matched, the device sends an Alarm log message to the Traffic Monitor and Log Server or syslog server, and then it does the specified action.

You can set some Alarm log messages. For example, you can use Policy Manager to configure an alarm to occur when a specified value matches or is more than a threshold. Other Alarm log messages are set by the appliance software, and you cannot change the value. For example, the XTM device sends an Alarm log message when a network connection on one of the XTM device interfaces fails, or when a *Denial of Service* attack occurs. For more information about Alarm log messages, see the *Log Catalog*.

There are eight categories of Alarm log messages:

- System
- IPS
- AV
- Policy
- Proxy
- Counter
- Denial of Service
- Traffic

The XTM device does not send more than 10 alarms in 15 minutes for the same conditions.

## Event Log Messages

The XTM device sends event log messages because of user activity. Actions that can cause the XTM device to send an event log message include:

- Device start up and shut down
- Device and VPN authentication
- Process start up and shut down

- Problems with the device hardware components
- Any task done by the device administrator

## Debug Log Messages

Debug log messages include diagnostic information that you can use to help troubleshoot problems. There are 27 different product components that can send debug log messages. You can select whether the debug (diagnostic) log messages appear in Traffic Monitor, as described in *Set the Diagnostic Log Level* on page 720.

## Statistic Log Messages

Statistic log messages include information about the performance of the XTM device. By default, the device sends log messages about external interface performance and VPN bandwidth statistics to your log file. You can use these logs to change your XTM device settings as necessary to improve performance. For more information about statistic log messages, see *Define Where the XTM Device Sends Log Messages* on page 711 and *Set Up Performance Statistic Logging* on page 718.

## Log Message Levels

When you enable logging for any of the WatchGuard servers, you can set the level assigned to the log messages from each server. This enables you to select what type of log messages are included in your log files. These log message level options are the same, whether you select to send log messages to a WatchGuard Log Server, Windows Event Viewer, or to a log file.

The available log levels in the **Select a log level** drop-down list are:

### *Error*

(Level: Low)

Includes only log messages for serious errors that cause a service or process to terminate.

### *Warning*

(Level: Medium)

Includes details of normal conditions and process operations. Also includes all details from the *Error* level.

### *Information*

(Level: High)

Includes details about successful log message operations. Also includes all details from the *Error* and *Warning* log levels.

### *Debug*

(Level: Advanced)

Includes detailed log messages from all log levels. We recommend you only select this level when directed to do so by a WatchGuard Technical Support representative, to help diagnose a specific configuration problem.

## About Notification

A notification is a message that an XTM device sends to the administrator when an event occurs at the device that is a possible security threat. The notification can be an email message or a popup window. Notifications can also be sent by way of an SNMP trap.

For more information about SNMP traps, see *About SNMP* on page 67.

Network administrators can configure notifications to be sent for a variety of reasons, and can examine them to help make decisions about how to add more security to the network.

For example, WatchGuard recommends that you configure default packet handling options to send a notification when the XTM device finds a port space probe. To find a port space probe, the XTM device counts the number of packets sent from one IP address to all of the external interface IP addresses on the device. If the number is greater than a configured value, the log host sends a notification to the network administrator about the rejected packets.

For the port space probe example, some possible actions you might take include:

- Block the ports on which the probe was used
- Block the IP address that sent the packets
- Send a notification email message to the network administrator

The XTM device sends notifications only if you enable and configure them on the Log Server that your device uses. For detailed instructions to configure notifications, see *Configure Database Settings* on page 694.

## Quick Start — Set Up Logging for Your Network


You can use the WatchGuard Log Server and policy notification settings to set up logging for your network. The log message data that your XTM devices and Log Servers collect enables you to monitor the activity on your network.

**Note** *This topic provides a general overview of the steps required to set up logging for your network. For more information about each step, follow the link to the detailed topic for each step.*

### Step 1 — Run the WatchGuard Server Center Setup Wizard

The wizard only includes pages for the servers you installed. If you do not see one of the pages included in the subsequent procedure, you did not install that server.

On the computer where you installed the Log Server software:

1. Right-click  in the system tray and select **Open WatchGuard Server Center**.  
*The WatchGuard Server Center Setup Wizard appears.*
2. Review the information on the first page of the wizard to make sure you have all the information necessary to complete the wizard. Click **Next**.
3. Type the name of your organization. Click **Next**.
4. Type and confirm the **Administrator passphrase** to use for all your WatchGuard servers. Click **Next**.
5. (Optional) Type the IP Address of your gateway Firebox. Click **Add**. Click **Next**.
6. (Optional) Type your Management Server License Key. Click **Next**.




7. Type the **Log Server Encryption key** and click **Browse** to select the location of the Log Server database. Click **Next**.
8. Type the Quarantine Server domain name. Click **Add**. Click **Next**.
9. (Optional) Download and install the WebBlocker database. Click **Next**.  
*It can take a long time to download and install the database. You can install the database later if you choose to not install it in the wizard.*
10. Review the settings you have selected. Click **Next**.  
*The wizard configures your servers.*
11. Click **Finish** to exit the wizard.

For more information, see the complete *Set Up WatchGuard Servers* on page 545 topic.

## Step 2 — Configure your Log Server

On the computer where you installed the Log Server software:

1. Right-click  in the system tray and select **Open WatchGuard Server Center**.  
*The WatchGuard Server Center appears.*
2. Type your **Username** and **Administrator passphrase**.
3. In the **Servers** tree, select **Log Server**.  
*The Log Server page appears.*
4. Change the default settings as appropriate for your network.
  - To set the maximum database size, change the encryption key for your Log Server, or delete diagnostic logs from your Log Server database, select the [Server Settings tab](#).
  - To configure settings for database backup and to specify the location of the log data, select the [Database Maintenance tab](#).
  - To configure notification messages settings for your Log Server, select the [Notification tab](#).
  - To view the status of connected devices and configure logging settings, select the [Logging tab](#).
5. Click **OK**.

For more information, see the complete *Set Up a Log Server* on page 691 topic.

## Step 3 — Define where your XTM device sends log messages

On the computer where you installed WSM:

1. Open Policy Manager for the XTM device to configure.
2. Select **Setup > Logging**.
3. Configure the logging settings for the WatchGuard Log Server, syslog server, and Firebox internal storage.

For more information, see the complete *Define Where the XTM Device Sends Log Messages* on page 711 topic.

## Step 4 — Configure Log Servers on your XTM device

1. From Policy Manager, select **Setup > Logging**.  
*The Logging Setup dialog box appears.*
2. Click **Configure**.

3. Select a Log Server from the list.  
If there is more than one server in the list, click **Up** or **Down** to change the order of the currently selected server.  
If the server you want is not in the list, click **Add** and specify the Log Server address and encryption key.
4. Click **OK**.  
*The new priority of the Log Servers appears in the WatchGuard Log Server list.*



For more information, see the complete *Set Log Server Priority* on page 715 topic.

#### Step 5 — Set up notification in your policies

1. From Policy Manager, add a policy or double-click a policy to edit that policy.
2. Select the **Properties** tab.
3. Click **Logging**.
4. Set the parameters for your security policy.

For more information, see *Add Policies to Your Configuration* on page 372 and *Configure Logging and Notification for a Policy* on page 722.

#### Step 6 — Use LogViewer to see log message data

1. From WatchGuard System Manager, click  and open LogViewer.  
*WatchGuard LogViewer appears.*
  2. To connect to a device, click .  
*The Connect to Log Server dialog box appears.*
  3. Type the IP address and passphrase for your Log Server and click **OK**.  
*The Select Firebox/Server dialog box appears.*
  4. Select a device or Log Server from the list and click **OK**.  
To connect to multiple devices at the same time, select more than one device or Log Server.  
*A device window appears for each selected device. The IP address of the device appears in the window title bar. The contents for a XTM device window and a Log Server window are different.*
  5. Select a log message to see more information about the message.  
*The selected log message details appear in the Details pane at the bottom of the device window.*
- If the details pane is not visible, select **View > Details Pane**.

For more information, see the complete *Use LogViewer to See Log Files* on page 727 topic.

## Set Up a Log Server

You can select to install your WatchGuard Log Server on your management computer, or you can install it on a different computer. You can also install additional Log Servers for the purposes of backup and scalability. If you install a WatchGuard server on a computer with a firewall other than Windows Firewall, you must open the ports necessary for the servers to connect through the firewall. If you use Windows Firewall, you do not have to change your configuration.

For more information, see *Install WatchGuard Servers on Computers with Desktop Firewalls* on page 32.

When you install the Log Server, the built-in Log Server PostgreSQL database is automatically installed. This is the default database for the Log Server. After you run the WatchGuard Server Center Setup Wizard to complete the initial configuration for your WatchGuard servers, you can configure your Log Server to use an external PostgreSQL database. This option provides increased scalability for your reports database.

For more information, see *Configure Database Settings* on page 694.

As an added feature, the Log Server can detect some internal failure conditions. When a failure condition is detected, the Log Server creates an Alarm log message that includes details about the failure and sends an email notification to the specified administrator.

For more information, see *Configure Notification Settings* on page 699.

## Install the Log Server

To install the Log Server on a computer other than your management computer:

1. Run the WatchGuard System Manager installation program.
2. Select only the **Log Server** component.
3. Complete the wizard.

## Before You Begin

Before you can configure the Log Server, you must complete the WatchGuard Server Center Setup Wizard. In the wizard, you specify the Log Server encryption key, Log Server database location, and data directory path for log files.

For more information on the setup wizard, see *Set Up WatchGuard Servers* on page 545.


## Configure System Settings

Before you configure your Log Server, make sure that the computer where the Log Server is installed has hibernation disabled so the Log Server does not shut down when the computer hibernates. Also make sure the computer has the same system time as any device configured to send log messages to this server.

1. Click **Start > Control Panel**.
2. Select **Power Options**.
3. Select the **Hibernate** tab and disable hibernation.
4. Verify the Log Server and connected devices are set to the same system time:
  - *Start Firebox System Manager.*
  - Select **Tools > Synchronize Time**.

## Configure the Log Server

On the computer that has the Log Server software installed:

1. Right-click  in the system tray and select **Open WatchGuard Server Center**.  
*The Connect to WatchGuard Server Center dialog box appears.*
2. Type your **Username** and **Administrator passphrase**. Click **Login**.  
*The WatchGuard Server Center appears.*
3. In the **Servers** tree, select **Log Server**.  
*The Log Server page appears.*



4. Change the default settings as appropriate for your network:
  - To set the maximum database size, change the encryption key for your Log Server, or delete diagnostic logs from your Log Server database, select the [Server Settings tab](#).
  - To configure settings for database backup and to specify the location of the log data, select the [Database Maintenance tab](#).
  - To configure notification messages settings for your Log Server, select the [Notification tab](#).
  - To view the status of connected devices and configure logging settings, select the [Logging tab](#).

## Configure Database, Encryption Key, and Diagnostic Log Settings

From WatchGuard Server Center, you can set the maximum database size for your WatchGuard Log Server. You can also change the encryption key for your Log Server, which you set in the WatchGuard Server Center Setup Wizard. When you enable diagnostic logging for your devices, your Log Server database can fill up quickly. To free up space in your Log Server database, you can choose to delete only the diagnostic log messages from your database.

The Log Server saves log files in a fixed-size partition in the database. When the partition reaches the maximum size, the Log Server creates a new partition for the log files. When the Log Server database reaches 95% of the maximum size you specify, it purges partitions until the database size is less than 95% to make room for new log messages.

1. In the **Servers** tree, select **Log Server**.
2. Select the **Server Settings** tab.

*The Server Settings page appears.*

The screenshot shows the 'Log Server' configuration page in the 'WatchGuard Server Center'. The page has a header with the 'Log Server' icon and name on the left, and 'WatchGuard Server Center' on the right. Below the header is a navigation bar with four tabs: 'Server Settings' (selected), 'Database Maintenance', 'Notification', and 'Logging'. The main content area is divided into three sections:

- Database Size:** A form with a text input field containing '100' and 'GB' next to it. To the right, it displays 'Current database size: 0 GB' and 'Available space: 100 GB (100%)'.
- Encryption Key Setting:** A section with the text 'Change the Log Server Encryption key' and a 'Modify' button.
- Diagnostics Logs:** A section with a 'Purge Diagnostics Logs' button and a note below it: 'This will delete appliance generated diagnostics logs of debug or higher level from the Log Server database.'

At the bottom right of the page, there are three buttons: 'Reset', 'Apply', and 'Help'.

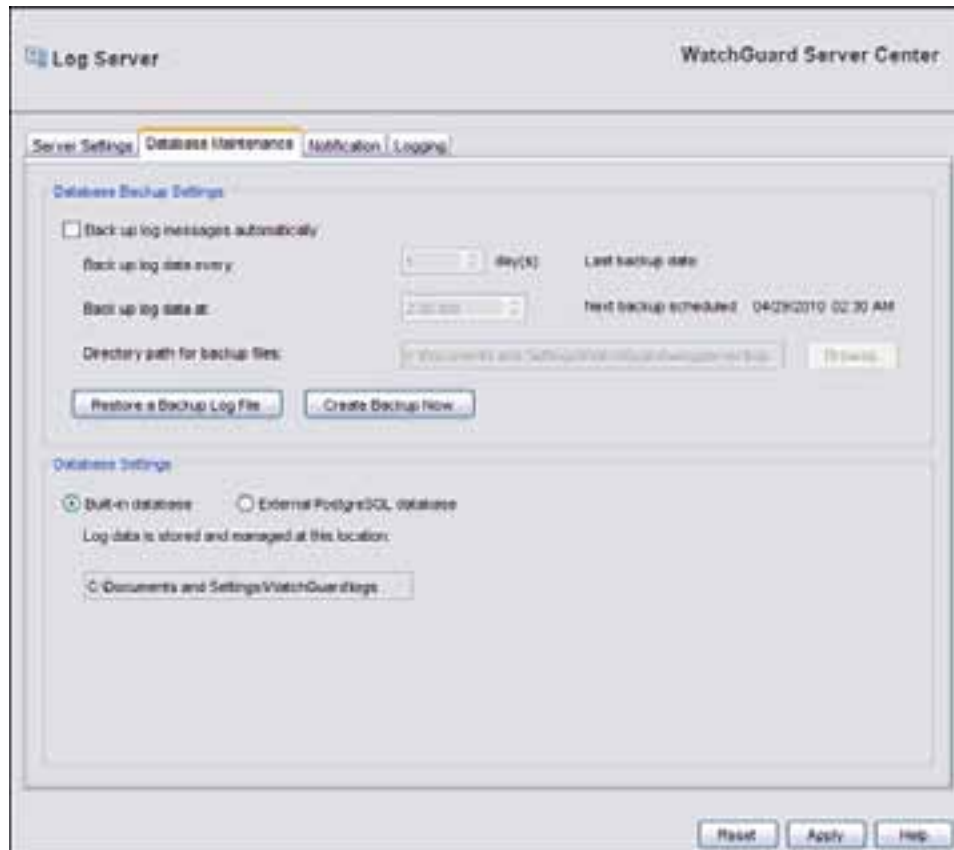
3. In the **Maximum database size** text box, type the maximum size for the Log Server database.  
You can set the database size between 1 and 10,000 GB.  
*The current size of the database and the number of GB currently available appear.*
4. To change the Log Server encryption key:
  - a. Click **Modify**.  
*The Log Server Encryption Key dialog box appears.*
  - b. In the **New key** text box, type a new encryption key for the Log Server.
  - c. Click **OK**.  
*The Log Server Encryption Key dialog box closes and the encryption key is updated to the new value you selected.*
5. To remove device log messages of the Debug level or higher from the Log Server database, click **Purge Diagnostic Logs**.
6. Click **Apply** to save your changes

## Configure Database Settings

From WatchGuard Server Center, you can configure the database backup settings and select the location for your Log Server database. You can choose to use either the built-in PostgreSQL Log Server database or an external PostgreSQL database. If you choose to use an external database, make sure the database is installed before you select it.

For more information about how to install a WatchGuard Log Server and the built-in PostgreSQL database, see *Set Up a Log Server* on page 691 and *Set Up WatchGuard Servers* on page 545.

1. In the **Servers** tree, select **Log Server**.
2. Select the **Database Maintenance** tab.  
*The Database Maintenance page appears.*



3. Use the subsequent sections to configure settings for your Log Server.
4. When you are finished, click **Apply** to save your changes.

## Configure Settings to Back Up Your Log Server Database

You can enable your Log Server to automatically create a backup copy of log messages, specify when and how often the log data is backed up, and select the folder where the backup files are saved. You can also manually create a backup log file at any time and restore a backup log file to your Log Server database.

Each backup file is saved in the directory you specify as a zip file that includes the date in the file name.

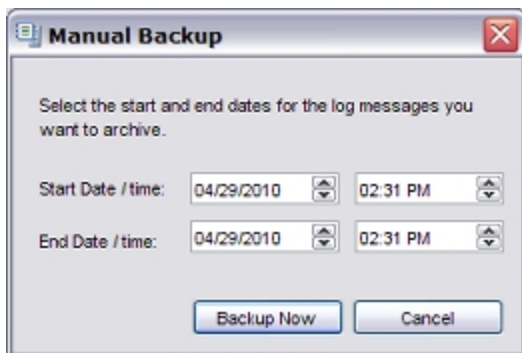
To configure the automatic backup settings for your Log Server:

1. Select the **Back up log messages automatically** check box.
2. In the **Back up log data every** text box, type or select how often to back up log data.  
*The date the last log data backup occurred appears.*
3. In the **Back up log data at** text box, type or select the time of day to back up the log data.  
*The date and time of the next scheduled backup appears.*
4. In the **Directory path for backup files** text box, type the location of the folder where you want to save the backup file.  
Or, click **Browse** to select the folder.

**Note** Because your Log Server backup file is on the same computer as your database log files, we recommend that you configure your Log Server to save the backup files to a drive other than your computer hard drive (such as an external hard drive or a tape drive.) Then, if you have a problem with your computer, you can still get access to your backup files.

To manually create a backup log file:

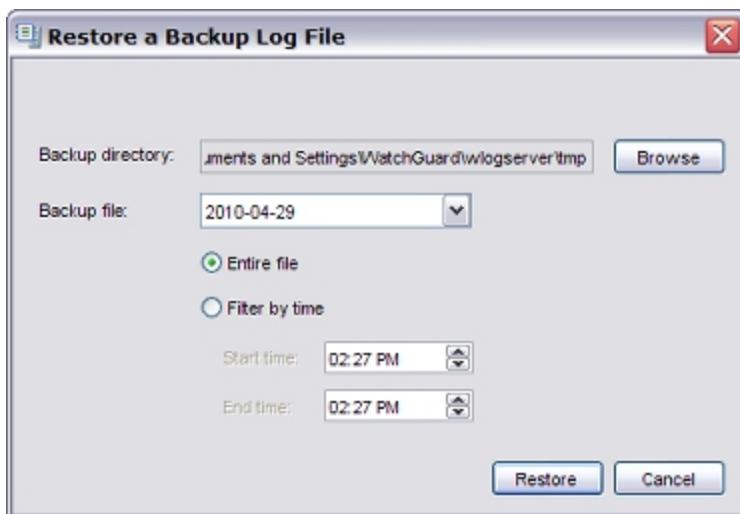
1. Click **Create Backup Now**.  
The Manual Backup dialog box appears.



2. In the **Start Date / time** text boxes, type or select the start of the date range of the log messages to include in the backup file.
3. In the **End Date / time** text boxes, type or select the end of the date range of the log messages to include in the backup file.
4. Click **Backup Now**.  
The backup file is generated and saved to the location you selected. The name of the backup file is the date the file was generated.

To restore a backup log file:

1. Click **Restore a Backup Log File**.  
The Restore a Backup Log File dialog box appears.



2. (Optional) To select the directory where the backup file is stored, click **Browse**.  
This step is not necessary if the backup file is stored in the location you specified in the Directory path for



*backup files text box.*

3. From the **Backup file** drop-down list, select the backup file to restore.
4. To restore all the log messages in the backup file, select **Entire file**.  
To restore only log messages from a certain date range, select **Filter by time** and select the **Start time** and **End time** of the log messages to restore.
5. Click **Restore**.

*The selected logs are restored to the Log Server database.*

## Configure the Database Settings

You can choose to either use the built-in PostgreSQL database that is automatically installed with your Log Server, or you can use an external PostgreSQL database installed on another computer. You can use any PostgreSQL database. This includes a database that was configured with another WatchGuard Log Server.

If you select to use an external PostgreSQL database, make sure your XTM device has a policy configured to allow traffic to and from the port you specify for communication with the external database. If you do not allow traffic to the external database through the specified port, the Log Server cannot connect to the external database. If the external database you select was not installed with a WatchGuard Log Server, the first time the Log Server connects to the database, it configures the structure of the database tables.

Before you configure the Log Server to use an external database, make sure you have this information for the external database:

- IP address of the computer on which the database is installed
- Port number to use to connect to the database
- User name and password for the Database User

**Note** *If you change the **Database Settings**, you must restart the Log Server for the changes to take effect.*

To use the built-in PostgreSQL database:

1. In the **Database Settings** section, select **Built-in database**.  
*The default directory location for your Log Server appears in the text box. This is the location you selected when you ran the WatchGuard Server Center Setup Wizard. You cannot change this location.*
2. Click **Apply**.

To use an external PostgreSQL database:

1. In the **Database Settings** section, select **External PostgreSQL database**.  
*The external database options appear.*

The screenshot shows a 'Database Settings' dialog box. At the top, there are two radio buttons: 'Built-in database' (unselected) and 'External PostgreSQL database' (selected). Below this, a text label reads 'Log data is stored and managed at this location:'. The form contains several input fields: 'Database Name' (empty), 'IP Address' (with three dots for separators), 'Database User' (empty), and 'Password' (empty). To the right of the IP Address field is a 'Port' dropdown menu showing '5432'. A 'Test Connection' button is located to the right of the Password field. At the bottom left, there is a link that says 'For more information, click [Help](#).'

2. In the **Database Name** text box, type the name of the external database.
3. In the **IP Address** text box, type the IP address of the computer on which the database is installed.
4. In the **Port** text box, type or select the port through which the Log Server can contact the external database.
5. In the **Database User** text box, type the user name the Log Server must use to contact the external database.

**Note** *The Database User name and password must not include these characters @ = , / \_ ; # [ ] ' " \* ? ` \ , and cannot be more than 64 characters.*

6. In the **Password** text box, type the password for the user name you selected.
7. To verify these settings are correct, click **Test Connection**.  
*If the Log Server cannot contact the database, an error message appears.*  
*If the Log Server successfully connects to the database, a confirmation message appears.*

## Configure Notification Settings

From WatchGuard Server Center, you can enable your Log Server to send notification messages when the events you specify for policies, devices, and servers occur, or when a failure event occurs on an XTM device or the Log Server. When you select to send notifications for events, you must also specify the email server to use to send the notification messages, and the email accounts to send and receive the messages.

For more information about failure events for a device or the Log Server, see the subsequent section, *Failure Events* on page 700.

1. In the **Servers** tree, select **Log Server**.
2. Select the **Notification** tab.

*The Notification page appears.*

The screenshot shows the 'Log Server' configuration page in the 'WatchGuard Server Center' interface. The 'Notification' tab is selected. The page is divided into three main sections:

- Events:** Contains two checkboxes:
  - Send an email notification for failure events
  - Send an email notification for events from any appliance or server logging to this Log Server
- SMTP Server Settings:**
  - Outgoing email server (SMTP): localhost (Example: smtp.mydomain.com)
  - Send credentials to the email server
  - User name: [text input]
  - Password: [text input]
- Notification Setup:**
  - Send email to: admin@localhost (Example: administrator@mycompany.com)
  - Send email from: [text input] (Example: logServer@mycompany.com)
  - Subject: [text input]
  - [Test Email button]

3. To enable notification for failure events, select the **Send an email notification for failure events** check box.
4. To enable notification for alarm events that occur on a device or server connected to the Log Server, select the **Send an email notification for events from any appliance or server logging to this Log Server** check box.

5. Use the subsequent sections to configure the **SMTP Server Settings** and **Notification Setup** settings.
6. Click **Apply** to save your changes.

## Configure the SMTP Server Settings

When you configure the SMTP Server Settings for your Log Server, the Log server uses your SMTP server to send notification messages for the events you specified. For email notification to work correctly, you must specify the address of an SMTP email server the Log Server can use to send these email messages.

Before you configure the SMTP server settings, make sure you have the correct address for your SMTP server, and, if necessary, the correct user credentials.

In the **SMTP Server Settings** section:

1. In the **Outgoing email server (SMTP)** text box, type the address of your SMTP server.  
*For example, smtp.example.com.*
2. If your email server requires authentication, select the **Send credentials to the email server** checkbox.
3. In the **User name** text box, type the user name for the email server.
4. In the **Password** text box, type the password for the email server.

**Note** *If the user name and password are not required for your SMTP server, you can leave these fields blank.*

## Configure Notification Message Settings

If you select to send an email notification for events, you can specify the email accounts to use to send email notification messages and the subject text for the messages. The email accounts you select must be valid email accounts that your SMTP server recognizes.

In the **Notification Setup** section:

1. In the **Send email to** text box, type the full email address of the account to which you want to send notification message.
2. In the **Send email from** text box, type the full email address of the account from which you want to send notification messages.
3. In the **Subject** text box, type the subject line for the event notification email.
4. To send a test notification email to the address you specified, click **Test Email**.  
*A message appears that tells you if the notification email was sent successfully, or if it failed to send.*

## Failure Events

Log messages can be collected for failure events that occur on your XTM device and on the Log Server.

When a failure event occurs on a device or the Log Server, and you have enabled logging for failure events, a notification message is sent about the failure event. Failure events for the Log Server include PostgreSQL service failures, system failures, and network failures.

For a device, a notification message is sent if the device fails to collect log messages.

For a Log Server, a notification message is sent for these failures:

- Lost database connection

If the connection to the database is lost and cannot be reestablished immediately, a notification message is sent. The server continues to try to connect to the database until the connection succeeds. The server sends a notification email every 15 minutes until the database connects to the server again.

- Database errors

This includes I/O errors, disk-full conditions, and any other database-related failures.

- Database backup errors

This includes any errors that occur when the log data is backed up (for example, I/O errors).

- Heartbeat detection error

When a device is connected to the Log Collector, the Log Server verifies that the log messages from a connected XTM device are being written to the database. If the Log Server detects that a device is connected, but no logs have been written to the database for 15 minutes, it sends a notification message.

- Lost Report Server connection

The Log Server monitors when the Report Server contacts it to collect the log messages. This usually occurs every 15 minutes. If the Report Server does not contact the Log Server for three collection intervals (45 minutes), the Log Server sends a notification message. If the Report Server has not contacted the Log Server since the Log Server was last started, it is not considered a failure condition.

## Configure Logging Settings for the Log Server

From WatchGuard Server Center, you can see the status of your connected XTM devices, and configure Windows Event Viewer and file path settings for your Log Server.

1. In the **Servers** tree, select **Log Server**.
2. Select the **Logging** tab.

*The Logging page appears.*

The screenshot displays the 'Log Server' configuration page in the WatchGuard Server Center. The 'Logging' tab is active. The 'Firebox Status' section contains a table with the following headers: IP Address, Serial Number, Firebox Type, and Firebox Status. Below the table, a message states 'No Firebox devices are currently connected to the Log Server.' There are 'Refresh' and 'Remove' buttons. The 'Windows Event Viewer' section has a checkbox for 'Send log messages to Windows Event Viewer' (unchecked) and a dropdown menu set to 'Warning'. The 'File path' section has a checked checkbox for 'Send log messages to a file', a text field for 'File location' containing 'ts and Settings\WatchGuard\logs\wlogserver', a 'Browse' button, and a dropdown menu set to 'Warning'. At the bottom right, there are 'Reset', 'Apply', and 'Help' buttons.

3. Use the subsequent sections to configure settings for your Log Server.
4. When you are finished, click **Apply** to save your changes.

## See the status of your XTM devices

The **Firebox Status** window shows the list of all XTM devices connected to the Log Server. You can refresh the view to update the list, or delete devices from the list.

1. To see the current status of the device connections, click **Refresh**.  
*A message appears if no XTM devices are connected to the Log Server.*
2. To delete a device from the list, in the **Firebox Status** list, select a device. Click **Remove**.  
*The selected device is removed from the Firebox Status list.*

## Configure Logging to Windows Event Viewer

You can choose to send server log messages to the Windows Event Viewer.

1. Select the **Send log messages to Windows Event Viewer** check box.
2. From the **Select a log level** drop-down list, select the level to assign to the log messages:
  - **Error**
  - **Warning**
  - **Information**
  - **Debug**

For more information about log levels, see *Log Message Levels* on page 687.

## Save Log Messages in a Log File

You can choose to save server log messages in a file that you can review later. This option is enabled by default.

To change the log file settings:

1. To save log messages in a file, make sure the **Send log messages to a file** check box is selected.
2. In the **File Location** text box, type the path to the directory where you want the log file to be stored. Or, click **Browse** to select the directory.
3. From the **Select a log level** drop-down list, select the level to assign to log messages:
  - **Error**
  - **Warning**
  - **Information**
  - **Debug**

For more information about log levels, see *Log Message Levels* on page 687.

## Move the Log Data Directory

You can use the WatchGuard Server Center Setup Wizard to choose a new directory where your log data files are stored. The Log Server then stores all log data files in this directory. After this wizard is complete, you cannot change the log data directory from the WatchGuard Server Center application.

To change the location where the Log Server sends the log data, you must set up the Log Server again. To do this, edit the *wlogserver.ini* file and run the WatchGuard Server Center Setup Wizard again. When you run the wizard again, you specify the new directory location, but the data in the old directory is not moved to the new directory. You must manually move the data from the old directory to the new directory before you use the wizard to specify the new directory for the Log Server.

When you run the WatchGuard Server Center Setup Wizard to reconfigure your Log Server, the screens that appear in the wizard can vary depending on which WatchGuard servers are installed on the computer. The instructions below assume that your computer has only the Management Server, Log Server, and Report Server installed. If you have other WatchGuard servers installed, additional options may appear in the wizard.

For information about these pages, see the complete *Set Up WatchGuard Servers* on page 545 topic.

**Note** *Because the Log Server and the Report Server both use the PostgreSQL database, they also use the same directory. If you have these servers installed on the same computer and you move the database, it is moved for both servers.*

### Step 1 — Stop Services

1. Open WatchGuard Server Center.
2. Stop the Log Server and Report Server.  
For more information, see *Stop and Start Your WatchGuard Servers*.
3. Close the WatchGuard Server Center.
4. Stop the PostgreSQL-8.2 service.
  - From Windows Control Panel, select **Administrative Tools > Services**.  
*The Services window appears.*
  - Select **PostgreSQL-8.2** and click **Stop**.  
*The service stops.*

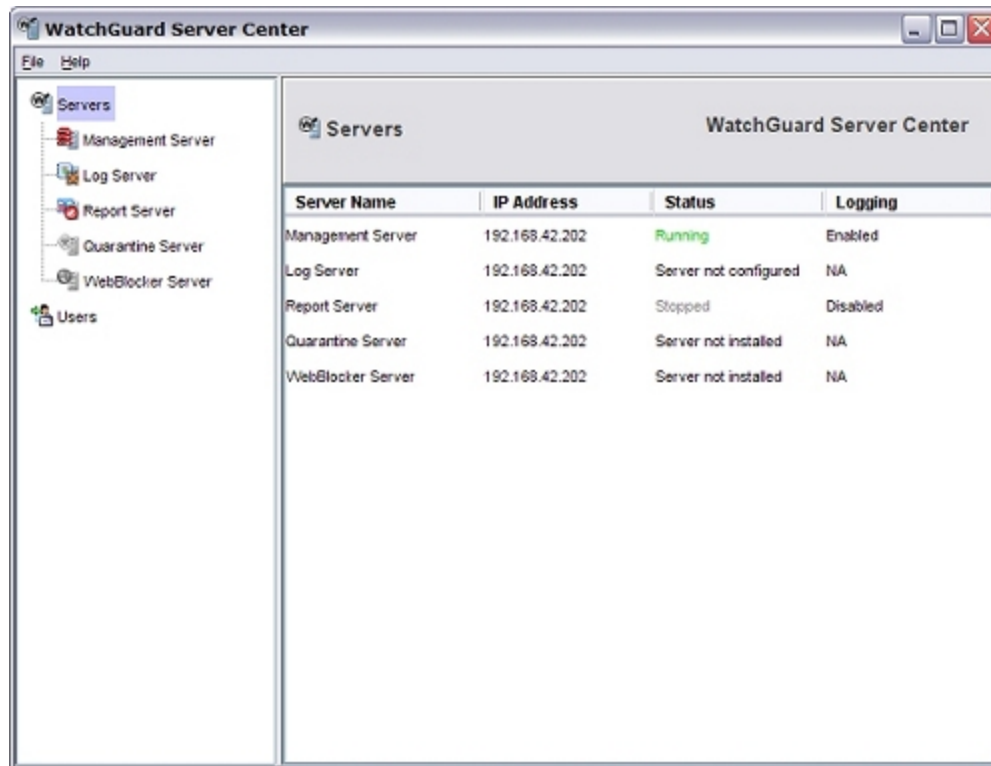
### Step 2 — Move the Log Data

1. Create the new log data directory.  
For example, E:\WatchGuard\logs.
2. Go to the original log data directory folder and copy the entire directory folder. Make sure to include all the folders and files in the directory.  
For example, go to the C:\Documents and Settings\WatchGuard\logs folder and copy the \data folder and all the folders and files in it.
3. Paste the copy of the \data directory in the new location.  
For example, E:\WatchGuard\logs. Make sure you paste the entire copied \data directory in E:\WatchGuard\logs.

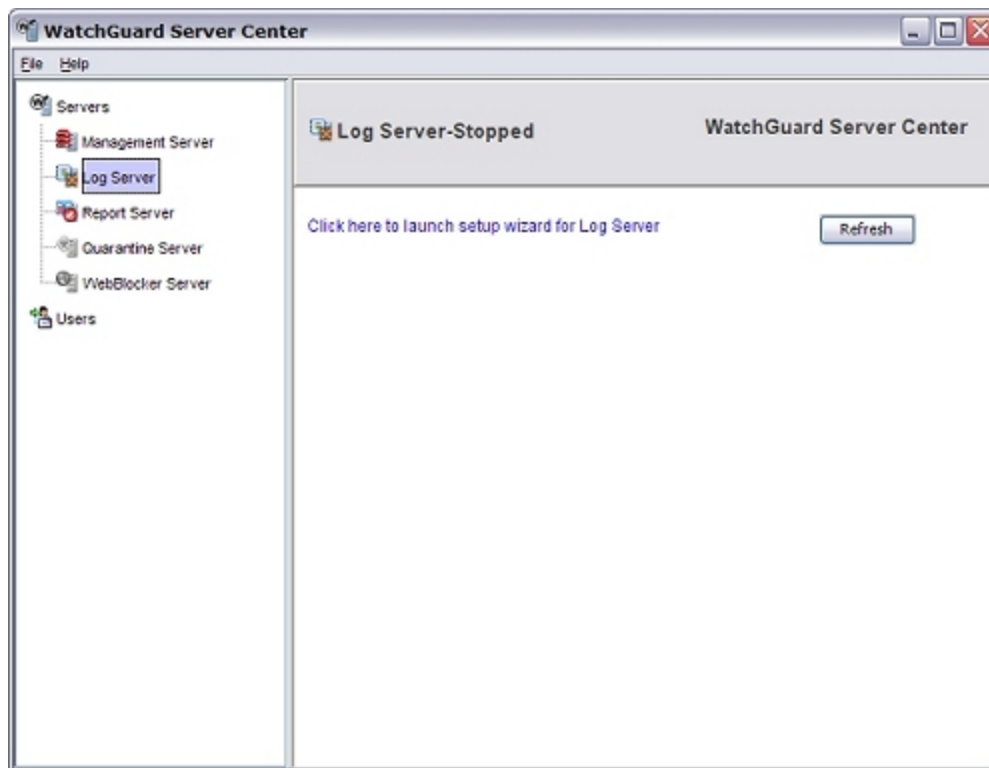


## Step 3 — Run the Setup Wizard

1. Open the C:\Documents and Settings\WatchGuard\wlogserver\wlogserver.ini file and change the **WizardSuccess** value to "0".
2. Delete the pg\_install.ini file.
  - For Windows XP and Windows Server 2003:  
C:\Documents and Settings\WatchGuard\postgresql\pg\_install.ini.
  - For Windows Vista, Windows 7, and Windows Server 2008:  
C:\ProgramData\WatchGuard\postgresql\pg\_install.ini
3. Open WatchGuard Server Center. The **Status** for the Log Server is **Server not configured**.



4. In the **Servers** tree, select **Log Server**.  
*The Log Server page appears.*



5. To launch the WatchGuard Server Center Setup Wizard for the Log Server, click **Click here to launch setup wizard for Log Server**.  
*The WatchGuard Server Center Setup Wizard will launch now message appears.*
6. Click **OK** to launch the wizard.  
*The WatchGuard Server Center Wizard appears.*
7. Click **Next** to start the wizard.  
*The Log Server page appears.*
8. Type and confirm the same **Encryption key** that you set when you originally completed the WatchGuard Server Center Setup Wizard.
9. In the **Database location** list, select the new log data directory location you created in *Step 2* above. Do not include the `\data` folder.  
*For example, E:\WatchGuard\logs.*
10. Click **Next**.
11. Complete the WatchGuard Server Center Wizard.  
*The wizard installs the PostgreSQL program and configures the Log Server with the new Log Server directory location.*

## Final Steps

From WatchGuard Server Center:

1. In the **Servers** tree, select Log Server.  
The Log Server page appears.
2. Click **Refresh**.  
*The Log Server is started and the Log Server configuration pages appear.*

## Update the Report Server Path

(Optional) If your Report Server is not on the same computer as your Log Server, do not complete this procedure.

If your Report Server is on the same computer as your Log Server, the Report Server directory was also moved. You must change the data directory path in the wrserver.ini file to the new location.

1. Make sure WatchGuard Server Center is closed.
2. Open the wrserver.ini file:
  - Windows XP and Windows Server 2003:  
C:\Documents and Settings\WatchGuard\wrserver\wrserver.ini
  - Windows 7, Windows Vista, and Windows Server 2008:  
C:\ProgramData\WatchGuard\wrserver\wrserver.ini
3. Find the DataDir = line and change the path to the new location.  
For example, DataDir = E:\WatchGuard\logs.
4. Save your changes and close the file.
5. Open WatchGuard Server Center.
6. In the **Servers** tree, select **Report Server**.
7. Select the **Database Maintenance** tab.
8. In the **Database Settings** section, verify the new path to the Report Server database appears.

## Start and Stop the Log Server

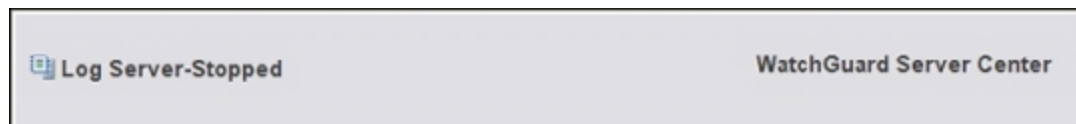
You can manually start or stop the Log Server service at any time. You do not have to disconnect from your Log Server.

To start the service, from WatchGuard Server Center:

1. Select **Log Server** in the **Servers** tree.
2. Right-click **Log Server** and select **Start Server**.  
*The service starts and Log Server appears at the top of the Log Server page.*

To stop the service, from WatchGuard Server Center:

1. Select **Log Server** in the **Servers** tree.
2. Right-click **Log Server** and select **Stop Server**.  
*A warning message appears.*
3. Click **Yes** to confirm you want to stop the Log Server service.  
*The service stops and Log Server-Stopped appears at the top of the Log Server page.*



# Configure Logging Settings for Your WatchGuard Servers

On the WatchGuard Server Center **Logging** pages for the Management Server, Report Server, and Quarantine Server, you can configure where each server sends log message data. You can choose to send log messages to a WatchGuard Log Server, Windows Event Viewer, and a log file.

1. In the **Servers** tree, select the server you want to configure.
2. Select the **Logging** tab.

*The Logging page appears.*

The screenshot shows the 'Logging' configuration page for a WatchGuard server. It is divided into three main sections:

- WatchGuard Log Server:**
  - Checkbox:  Send log messages to WatchGuard Log Server(s)
  - Table with columns: Priority, Log Server Address
  - Buttons: Add, Edit, Remove, Up, Down
  - Select a log level: Warning (dropdown)
- Windows Event Viewer:**
  - Checkbox:  Send log messages to Windows Event Viewer
  - Select a log level: Warning (dropdown)
- File path:**
  - Checkbox:  Send log messages to a file
  - File location: C:\Documents and Settings\WatchGuard\logs\wr- (with a Browse button)
  - Select a log level: Information (dropdown)

3. Use the subsequent sections to configure settings for your server.
4. When you are finished, click **Apply** to save your changes.

## Configure Logging to a WatchGuard Log Server

You can select to send log messages from your servers to one or more WatchGuard Log Servers. When you add more than one Log Server, you can use the Log Server priority list to select the order in which the server connects to each Log Server. If the server cannot connect to the Log Server with the highest priority (Priority 1), it connects to the next Log Server in the list. If the server examines each Log Server in the list and cannot connect, it tries to connect to the first Log Server in the list again.

To enable logging:

1. In the **WatchGuard Log Server** section, select the **Send log messages to WatchGuard Log Server(s)** check box.
2. Click **Add** and add a Log Server to the list.

*The Add Log Server dialog box appears.*



3. In the **Log Server Address** text box, type the IP address of the Log Server.
4. In the **Encryption Key** and **Confirm Key** text boxes, type the encryption key for the Log Server.
5. Click **OK**.  
*The Log Server appears in the list.*
6. To add another Log Server, repeat Steps 2–5.
7. To change information for a Log Server, select a server from the list and click **Edit**.
8. To change the priority of the servers in the list, select a server and click **Up** or **Down**.  
*The selected Log Server moves up or down in the Priority list.*
9. To delete a server from the list, select the server and click **Remove**.
10. From the **Select a log level** drop-down list, select the level that is assigned to log messages:
  - **Error**
  - **Warning**
  - **Information**
  - **Debug**

For more information about log levels, see *Log Message Levels* on page 687.

To disable logging to any WatchGuard Log Servers, clear the **Send log messages to WatchGuard Log Server(s)** check box.

## Configure Logging to Windows Event Viewer

You can choose to send log messages to the Windows Event Viewer.

1. In the **Windows Event Viewer** section, select the **Send log messages to Windows Event Viewer** check box.

2. From the **Select a log level** drop-down list, select the level that is assigned to the log messages:
  - **Error**
  - **Warning**
  - **Information**
  - **Debug**

For more information about log levels, see *Log Message Levels* on page 687.

## Save Log Messages in a Log File

You can choose to save log messages to a file that you can access later. This option is enabled by default.

To change the log file settings:

1. To save log messages in a file, make sure the **Send log messages to a file** check box is selected.
2. Click **Browse** and select the directory where the log file is stored.
3. From the **Select a log level** drop-down list, select the level that is assigned to log messages:
  - **Error**
  - **Warning**
  - **Information**
  - **Debug**

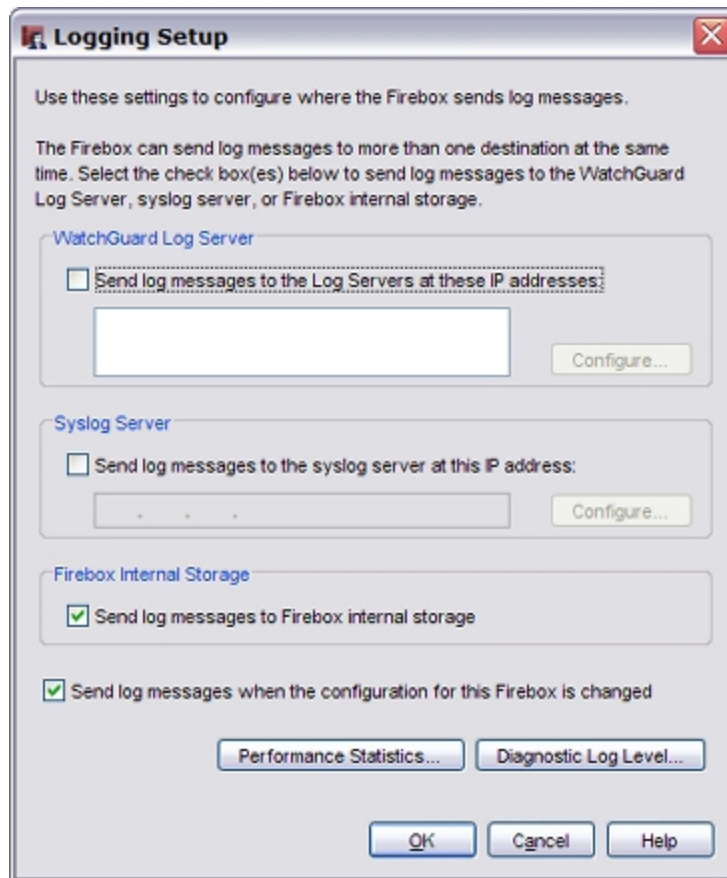
For more information about log levels, see *Log Message Levels* on page 687.

## Define Where the XTM Device Sends Log Messages

From Policy Manager, you can configure your XTM device to log events that occur at the device. You can then examine the log files and make decisions about how to add more security to your network. You must tell the XTM device where to send log messages.

1. Select **Setup > Logging**.

*The Logging Setup dialog box appears.*



2. Configure the logging settings for the WatchGuard Log Server, syslog server, and XTM device internal storage.

### *WatchGuard Log Server*

To send log messages to your WatchGuard Log Servers, select the **Send log messages to the log servers at these IP addresses** check box. An XTM device can send log messages to a WatchGuard Log Server and a syslog server at the same time.

To add or edit the IP addresses for your Log Servers, click **Configure**. You can add up to five Log Servers to the list. For more information, see *Add a Log Server* on page 712.

### *Syslog Server*

To send log messages to your syslog server, select the **Send log messages to the Syslog server at this IP address** check box. An XTM device can send log messages to a WatchGuard Log Server and a syslog server at the same time.

To add or edit the IP addresses for your syslog server, click **Configure**. For more information, see *Configure Syslog* on page 716.

### *Firebox Internal Storage*

To store log messages on the XTM device, select the **Send log messages in Firebox internal storage**.

### *Performance Statistics*

By default, the XTM device sends log messages about external interface performance and VPN bandwidth statistics to your log file. To disable this type of log message, click **Performance Statistics**. For more information, see *Set Up Performance Statistic Logging* on page 718.

### *Diagnostic Log Level*

To set the level of diagnostic logging to write to your log file or to view in Traffic Monitor for each logging category, click **Diagnostic Log Level**. For more information, see *Set the Diagnostic Log Level*.

For more information about Traffic Monitor, see *Device Log Messages (Traffic Monitor)*.

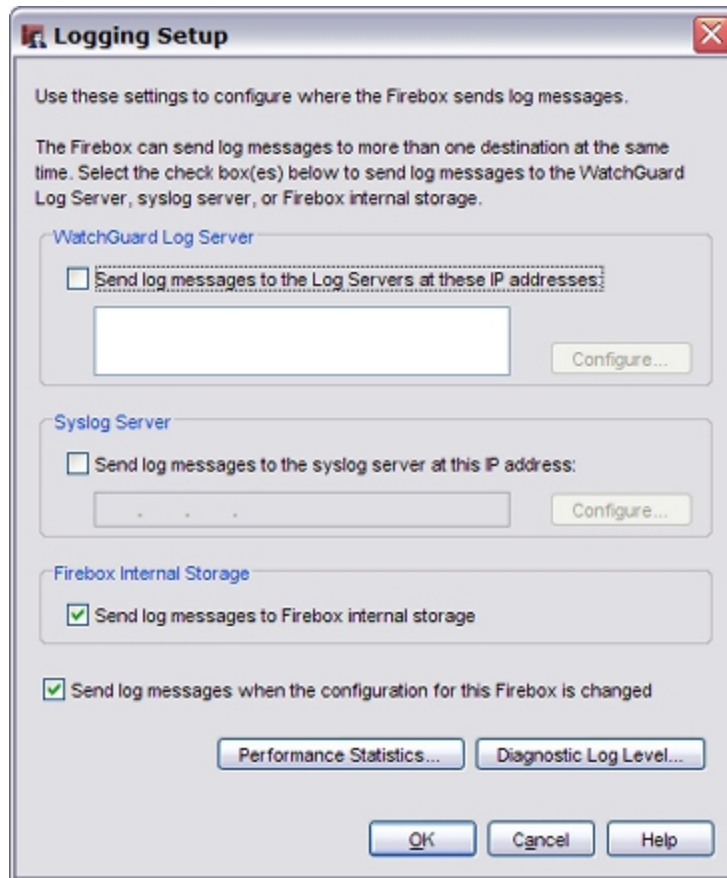
3. To send a log message to the selected log message destinations when the configuration for your XTM device changes, select the **Send log messages when the configuration for this Firebox is changed** check box.
4. Click **OK**.

## **Add a Log Server**

If you select the **Send log messages to the Log Servers at these IP addresses** check box when you *Define Where the XTM Device Sends Log Messages*, you can add one or more Log Servers to the XTM device.

1. From Policy Manager, select **Setup > Logging**.  
*The Logging Setup dialog box appears.*





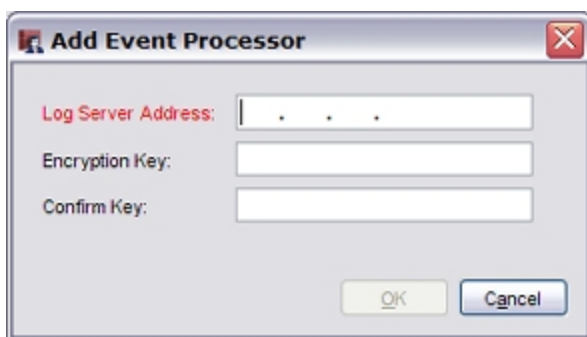
2. Select the **Send log messages to the Log Servers at these IP addresses** checkbox.
3. Click **Configure**.

*The Configure Log Servers dialog box appears.*



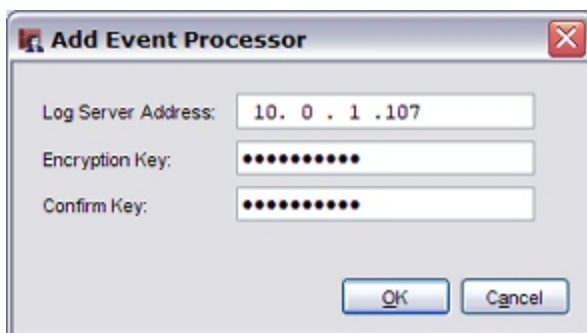
4. Click **Add**.

The *Add Event Processor* dialog box appears.



5. In the **Log Server Address** text box, type the IP address of the Log Server to add.
6. In the **Encryption Key** and **Confirm Key** text boxes, type the Log Server encryption key that you set when you *Set Up a Log Server*.

The allowed range for the encryption key is 8–32 characters. You can use all characters but spaces and slashes (/ or \).



7. Click **OK**.

*The Add Event Processor dialog box disappears.*

## Save the Changes and Verify Logging

1. Click **OK** to close the **Configure Log Servers** dialog box.
2. Click **OK** to close the **Logging Setup** dialog box.
3. *Save the Configuration File.*
4. To verify that the XTM device sends log messages correctly, from WatchGuard System Manager, select **Tools > Firebox System Manager**.

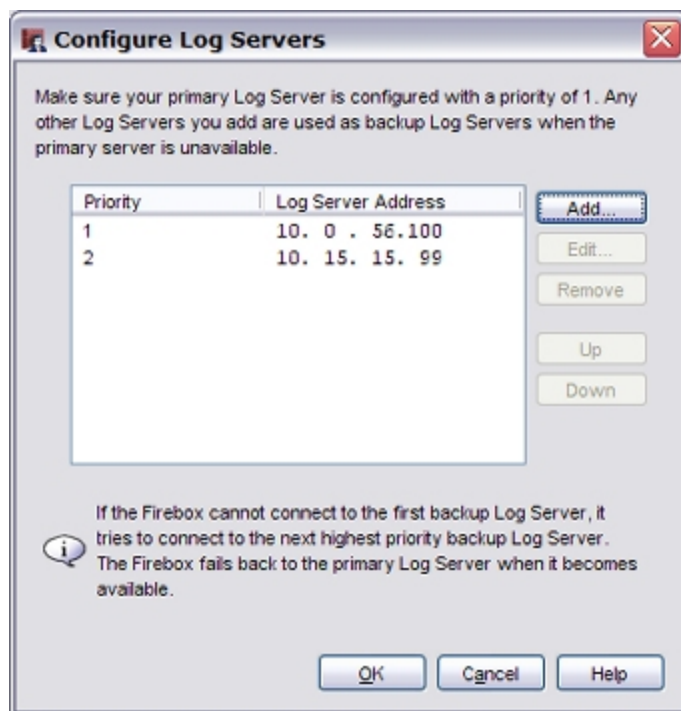
In the **Detail** section, adjacent to **Log Server**, the IP address of the log host appears.

## Set Log Server Priority

The Log Server priority list enables you to select the order the XTM device connects to your Log Servers. From Policy Manager, you can designate one Log Server as the primary (Priority 1) and other Log Servers as backup servers. If the XTM device cannot connect to the primary Log Server, it tries to connect to the next Log Server in the priority list. If the XTM device examines each Log Server in the list and cannot connect to any of them, it tries to connect to the first Log Server in the list again. When the primary Log Server is not available, and the XTM device is connected to a backup Log Server, the XTM device tries to reconnect to the primary Log Server every 6 minutes. This does not affect the XTM device connection to the backup Log Server until the primary Log Server is available.

To create a Log Server priority list:

1. Select **Setup > Logging**.  
*The Logging Setup dialog box appears.*
2. Select the **Send log messages to the Log Servers at these IP addresses** check box.
3. Click **Configure**.  
*The Configure Log Servers dialog box appears.*



4. To change the priority of the Log Servers, select a Log Server from the list and click **Up** or **Down**.
5. Click **OK**.

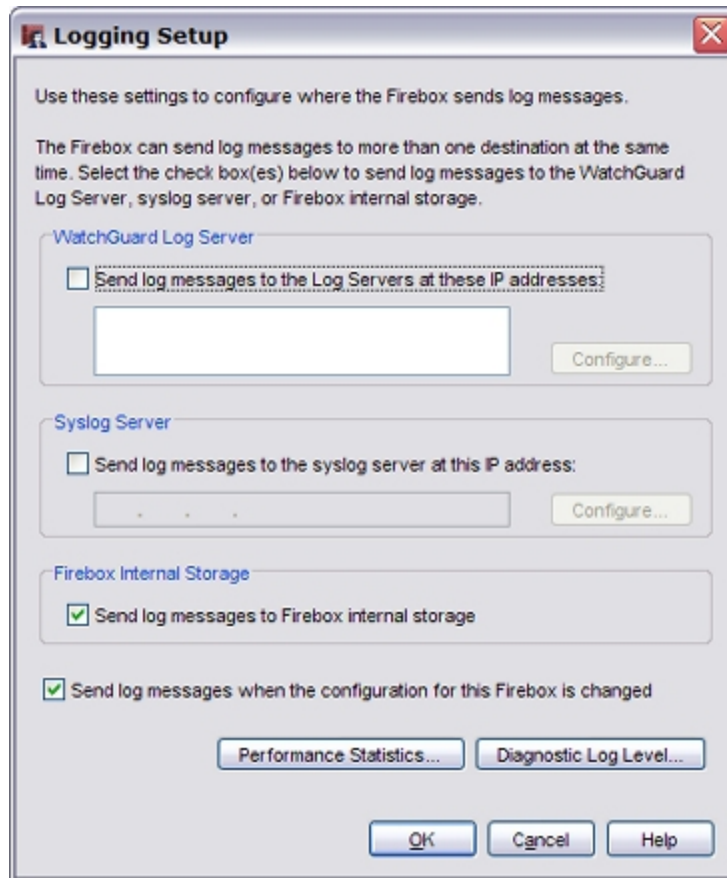
*The Logging Setup dialog box appears. The new priority order of the Log Servers appears in the WatchGuard Log Server list.*

## Configure Syslog

Syslog is a log interface developed for UNIX but also used by a number of computer systems. From Policy Manager, you can configure your XTM device to send log information to a syslog server. An XTM device can send log messages to a WatchGuard Log Server and a syslog server at the same time, or send log messages to only one or the other. Syslog log messages are not encrypted. We recommend that you do not select a syslog host on the external interface.

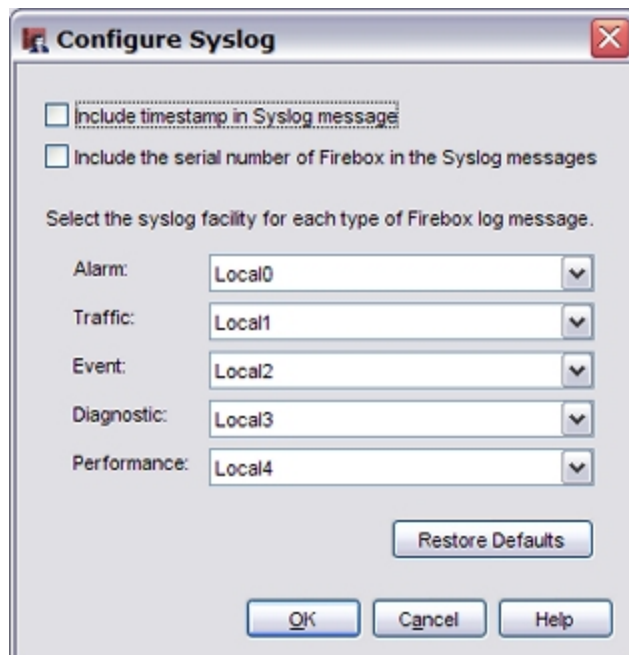
1. Select **Setup > Logging**.

*The Logging Setup dialog box appears.*



2. Select the **Send Log Messages to the Syslog server at this IP address** check box.
3. In the address text box, type the IP address of the syslog server.
4. Click **Configure**.

*The Configure Syslog dialog box appears.*



5. To include the timestamp information from your XTM device in the log message details, select the **Include timestamp in Syslog message** check box.
6. To include the serial number of the XTM device in the log message details, select the **Include the serial number of Firebox in the Syslog messages** check box.
7. For each type of log message, select the syslog facility to which you want it assigned.

If you select **NONE**, details for that message type are not sent to the syslog host.

For information about the different types of messages, see *Types of Log Messages* on page 686.

The syslog facility refers to one of the fields in the syslog packet and to the file syslog sends a log message to. You can use Local0 for high-priority syslog messages, such as alarms. You can use Local1–Local7 to assign priorities for other types of log messages (lower numbers have greater priority). See your syslog documentation for more information on logging facilities.

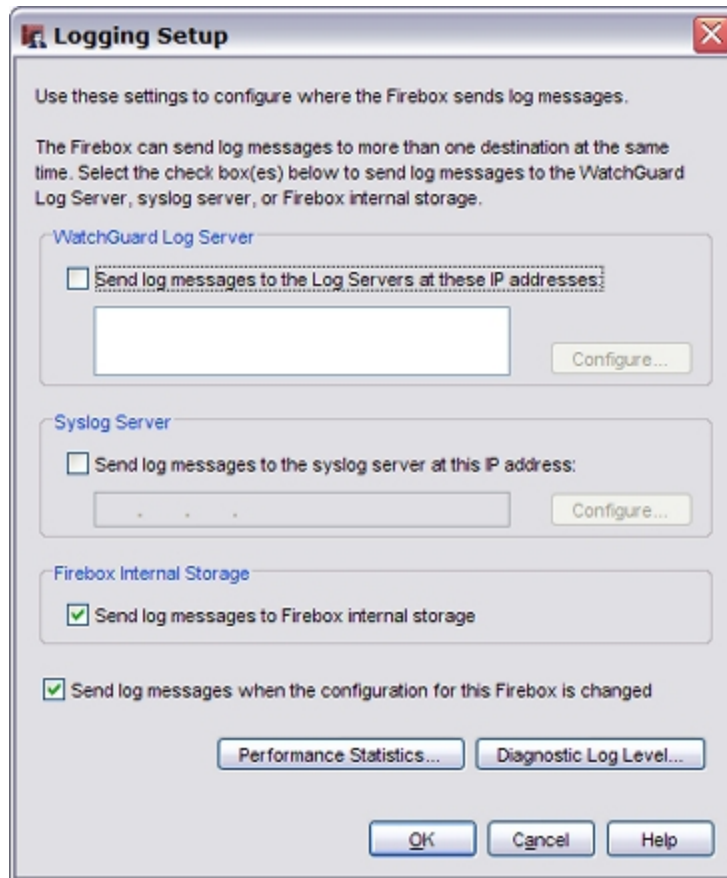
8. To lose your settings and restore the default settings for syslog, click **Restore Defaults**.
9. Click **OK** to close the **Configure Syslog** dialog box.
10. Click **OK** to close the **Logging Setup** dialog box.
11. *Save the Configuration File.*

## Set Up Performance Statistic Logging

From Policy Manager, you can select whether to see performance statistic log data on the Firebox System Manager **Traffic Monitor** tab. To see this log data, performance statistic logging must be enabled. When this option is enabled, the XTM device sends log messages about external interface performance and VPN bandwidth statistics to your Log Server.

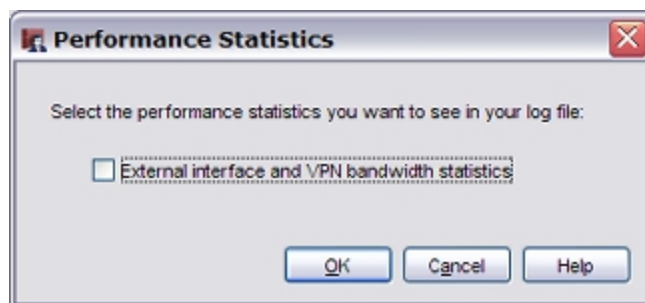
## Enable or Disable Performance Statistic Logging

1. Select **Setup > Logging**.  
*The Logging Setup dialog box appears.*



2. Click **Performance Statistics**.

*The Performance Statistics dialog box appears.*



3. To enable performance statistic logging, select the **External interface and VPN bandwidth statistics** check box.

To disable performance statistic logging, clear the **External interface and VPN bandwidth statistics** check box.

4. Click **OK**.
5. *Save the Configuration File.*

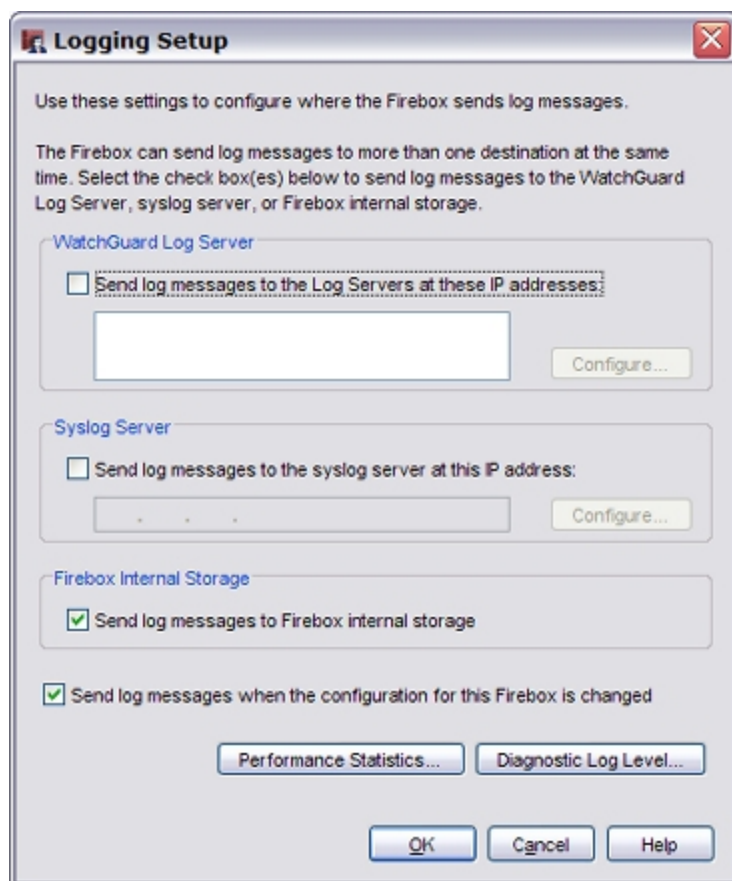
## Set the Diagnostic Log Level

From Policy Manager you can select the level of diagnostic logging to write to your log file or to Traffic Monitor. We do not recommend that you select the highest logging level unless a technical support representative tells you to do so while you troubleshoot a problem. When you use the highest diagnostic log level, the log file can fill up very quickly, and performance of the XTM device is often reduced.

For more information on Traffic Monitor, see *Device Log Messages (Traffic Monitor)* on page 754.

1. Select **Setup > Logging**.

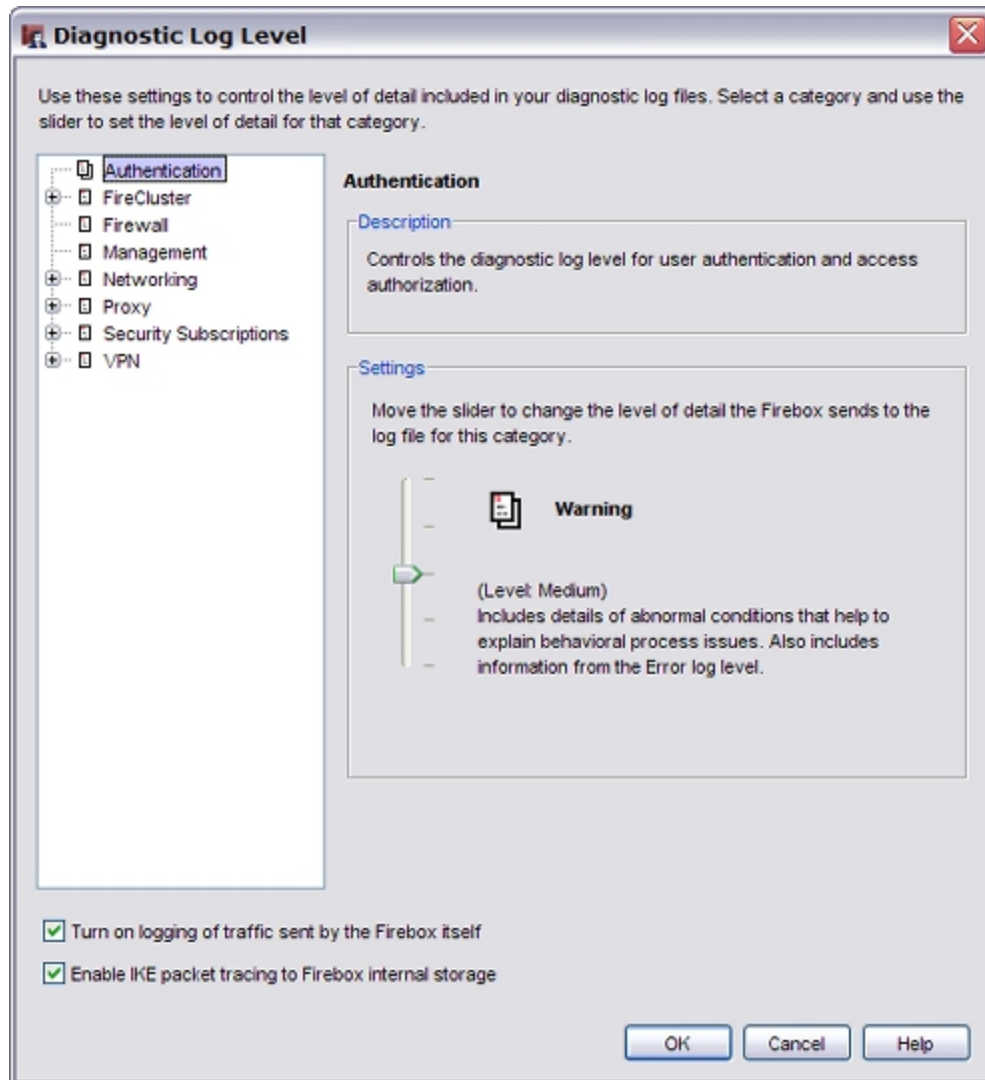
*The Logging Setup dialog box appears.*



2. Click **Diagnostic Log Level**.

*The Diagnostic Log Level dialog box appears.*





3. Select a category from the list.  
*A description of the category appears in the Description box.*
4. Use the **Settings** slider to select the level of detail to include in the log message for each category.

- Off
- Error
- Warning
- Information
- Debug

When **Off** (the lowest level) is selected, diagnostic messages for that category are disabled.

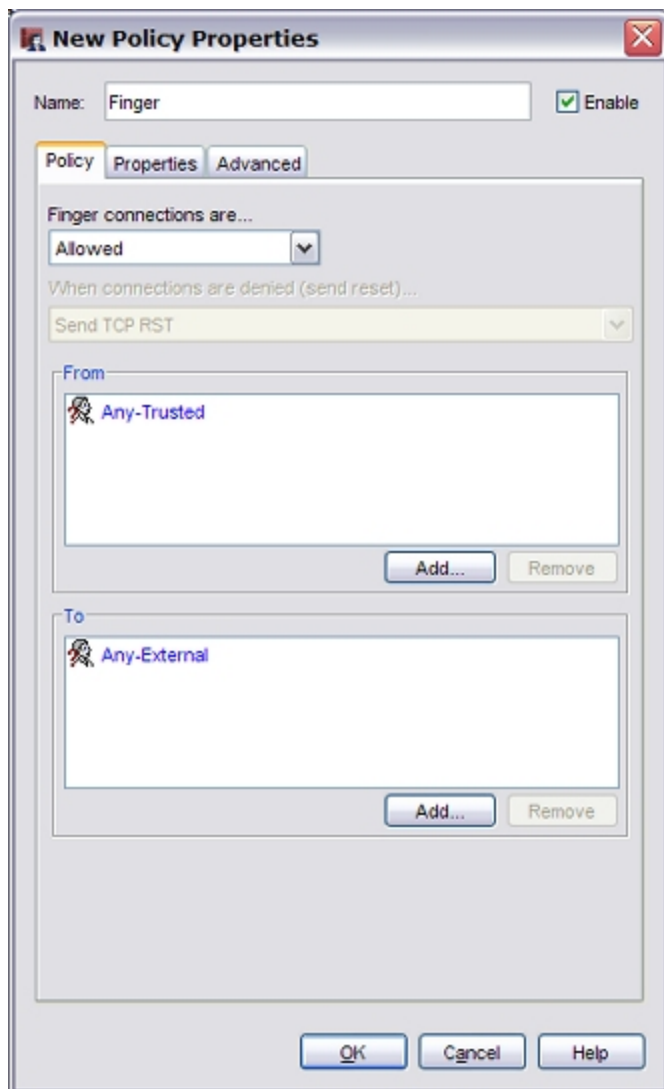
5. To send log messages about traffic sent by the XTM device, select the **Turn on logging of traffic sent by the Firebox itself** check box.
6. To enable the XTM device to collect a packet trace for IKE packets, select the **Enable IKE packet tracing to Firebox internal storage** check box.
7. Click **OK** to save your changes.

*The Diagnostic Log Level dialog box closes and the Logging Settings dialog box appears.*

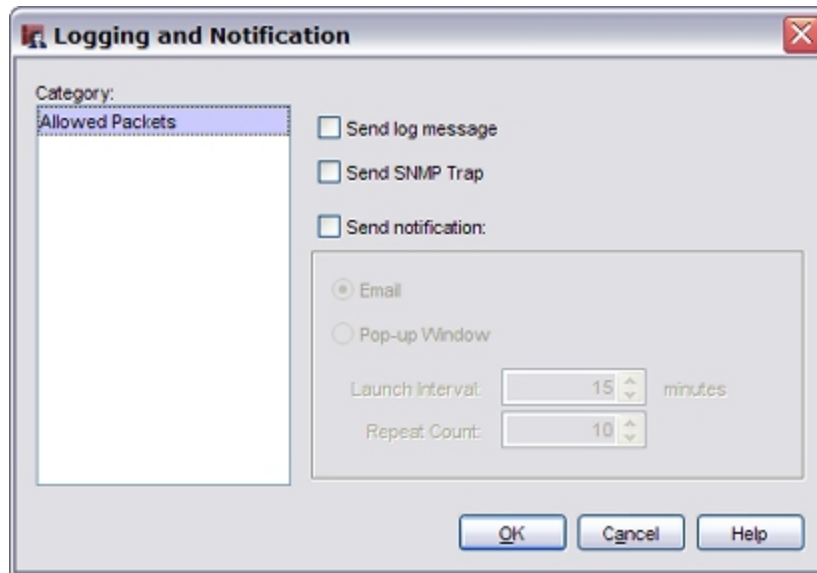
## Configure Logging and Notification for a Policy

You can use Policy Manager to configure the logging and notification settings for each policy in your configuration.

1. [Add a policy](#), or double-click a policy to edit that policy.  
*The New Policy Properties or Edit Policy Properties dialog box appears.*



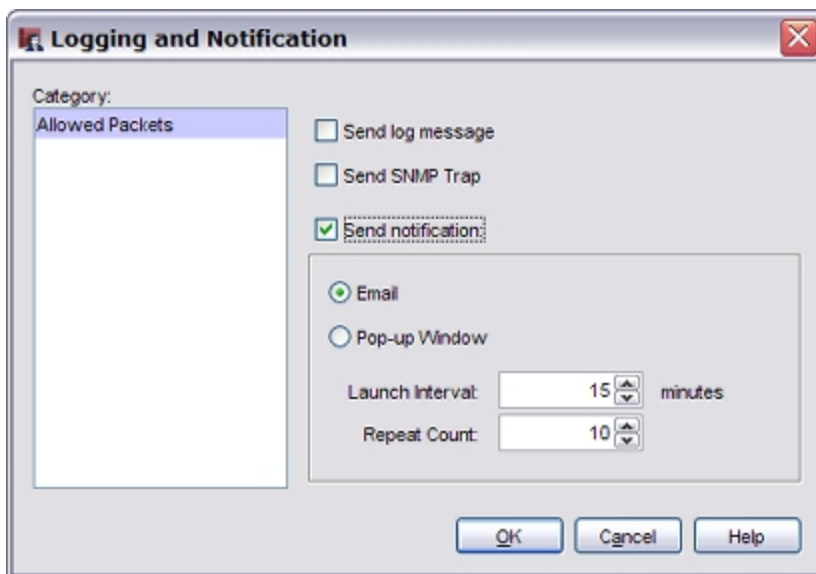
2. Select the **Properties** tab.
3. Click **Logging**.  
*The Logging and Notification dialog box appears.*



4. Set the parameters to match your security policy.  
For information about the options in the **Logging and Notification** dialog box, see *Set Logging and Notification Preferences* on page 723.
5. Click **OK** to save your changes.

## Set Logging and Notification Preferences

The settings for logging and notification are similar throughout the XTM device configuration. For each place you define logging and notification preferences, most or all of the options described below are available.



### *Send Log message*

When you select this check box, the XTM device sends a log message when an event occurs.

You can select to send log messages to a WatchGuard Log Server, syslog server, or XTM device internal storage. For detailed steps to select a destination for your log messages, see *Configure Database, Encryption Key, and Diagnostic Log Settings* on page 693.

#### *Send SNMP trap*

When you select this check box, the XTM device sends an event notification to the SNMP management system. Simple Network Management Protocol (SNMP) is a set of tools used to monitor and manage networks. A SNMP trap is an event notification the XTM device sends to the SNMP management system when a specified condition occurs.

**Note** If you select the **Send SNMP Trap** check box and you have not yet configured SNMP, a dialog box appears and asks you if you want to do this. Click **Yes** to go to the **SNMP Settings** dialog box. You cannot send SNMP traps if you do not configure SNMP.

For more information about SNMP, see *About SNMP* on page 67.

To enable SNMP traps or inform requests, see *Enable SNMP Management Stations and Traps* on page 69.

#### *Send Notification*

When you select this check box, the XTM device sends a notification when the event you specified occurs. For example, when a policy allows a packet.

To configure notification settings, see *About Notification* on page 688.

You can select how the XTM device sends the notification:

- **Email** — The Log Server sends an email message when the event occurs.
- **Pop-up Window** — The Log Server opens a dialog box when the event occurs.

Set the:

**Launch Interval** — The minimum time (in minutes) between different notifications. This parameter prevents more than one notification in a short time for the same event.

**Repeat Count** — This setting tracks how frequently an event occurs. When the number of events reaches the selected value, a special repeat notification starts. This notification creates a repeat log entry about that specified notification. Notification starts again after the number of events you specify in this field occurs.

For example, set the **Launch interval** to 5 minutes and the **Repeat count** to 4. A port space probe starts at 10:00 AM. and continues each minute. This starts the logging and notification mechanisms.

These actions occur at these times:

- 10:00 — Initial port space probe (first event)
- 10:01 — First notification starts (one event)
- 10:06 — Second notification starts (reports five events)
- 10:11 — Third notification starts (reports five events)
- 10:16 — Fourth notification starts (reports five events)

The launch interval controls the time intervals between each event (1, 2, 3, 4, and 5). This was set to 5 minutes. Multiply the repeat count by the launch interval. This is the time interval an event must continue to in order to start the repeat notification.

## Use Scripts, Utilities, and Third-Party Software with the Log Server

You can use several scripts, utilities, and applications from the command line to do certain tasks with the Log Server. You can also use some third-party software with the Log Server. These tasks are designed to help you with problems that arise outside of normal Log Server operations. WatchGuard does not support the use of these scripts and utilities for procedures. Use them solely at your own risk.

You can use scripts, utilities, applications, and third-party software to:

- *Back Up and Restore the Log Server Database*
- *Use Crystal Reports with the Log Server*

In the code examples shown in these topics, *backup.db* is used as a default file name for the contents of your database. You can choose a different filename when you perform the procedure. Additionally, the letter *X* is used in path names to designate letters or numbers that may be different for each user. For example, if the path name includes a directory such as *wsm11.x*, you should look for a directory with a similar name, such as *wsm11.4*. If you have multiple versions of WatchGuard System Manager or Firewall XTM installed, you may have to repeat the procedures for each version.

### Back Up and Restore the Log Server Database

You can use the *pg\_dump* utility to create a file that contains the entire contents of your Log Server database. This file is called a *dump* file. You can use this file to restore the database on the current server, or to move the Log Server to a different server.

1. Open a command prompt.
2. Type `cd \Program Files\WatchGuard\wsm11\postgresql\bin` and press **Enter** to change your working directory.  
*Use the appropriate version number for your WSM installation.*
3. Type `pg_dump -v -f "c:\db.backup" -F c -Z 5 -U wguser wglog` and press **Enter**.
4. When requested, type your Administrator passphrase.  
*The contents of your Log Server database are saved to the specified path and filename, in your current working directory (selected in Step 1).*
5. Copy the backup file to the new Log Server computer (for example, `C:\backup.db`) and stop the Log Server.  
For more information, see *Start and Stop the Log Server* on page 707.
6. At a command prompt, change your current working directory to `\Program Files\WatchGuard\wsm11\postgresql\bin`.
7. Select an option to restore the database:

To restore the database backup on an existing Log Server computer that has a Log Server database installed and configured with the Log Server Setup wizard, type `pg_restore -U wguser -v "c:\db.backup" -c -d wglog` and press **Enter**.

When requested, type your Administrator passphrase and press **Enter**.

*The Log Server database is overwritten with the contents of the database dump file.*

To restore the database backup on a new Log Server computer that does not have a database created and configured with the Log Server Setup wizard, type `pg_restore -U wguser -v "c:\db.backup" -C -d wglog` and press **Enter**.

When requested, type your Administrator passphrase and press **Enter** again.

*The database is created and the backup file contents are imported into the new Log Server.*

8. Start the Log Server.

For more information, see *Start and Stop the Log Server* on page 707.

## Use Crystal Reports with the Log Server

If your organization uses Crystal Reports, you can use the Log Server database as a source of information. You must install software from a third party for this functionality. Also, we recommend that you install Crystal Reports on a separate computer from the Log Server for better performance.

**Note** *In these procedures, we use 192.168.0.1 for the IP address of the Log Server, and 192.168.0.2 for the IP address of the remote client. These are only example IP addresses. Make sure you replace them with the correct IP addresses of your Log Server and remote client when you complete these procedures.*

## Configure Your Log Server Computer

1. Stop the Log Server and the PostgreSQL database services.
2. Open the PostgreSQL configuration file in a text editor:  
**C:\Documents and Settings\WatchGuard\logs\data\postgresql.conf**
3. To allow database connections from other computers, in the *postgresql.conf* file, change the Log Server **listen\_addresses** setting to:  
`listen_addresses = '*'`  
Or,  
`listen_addresses = 'localhost, 192.168.0.1'`  
*If necessary, remove the comment symbol (#) from the beginning of the line.*
4. Save **postgresql.conf**.
5. Open the *pg\_hba.conf* file.
6. Add a line similar to:

```
host    all            all            192.68.0.2/32      md5
```

In this example, 192.168.0.2 is the remote client from which you want to allow access.

7. Restart the PostgreSQL and Log Server services.

## Configure the Crystal Reports Computer

1. Install Crystal Reports on a separate computer from the Log Server computer.
2. [Download](#) and install the ODBC driver for PostgreSQL.
3. From the Windows Start Menu, select **Control Panel > Administrative Tools > Data Sources (ODBC)**.
4. On the **User DSN** tab, click **Add**.
5. Select **PostgreSQL Unicode**.


6. Configure the connection with this information:
  - **Data Source** — PostgreSQL30W
  - **Database** — wglog
  - **Server** — 127.0.0.1
  - **Port** — 5432
  - **User name** — wguser
  - **Password** — [Administrator passphrase]
7. Click **Test** to test the connection.
8. Open Crystal Reports.
9. Select **Database > Log On or Off Server > Create New Connection > ODBC (RDO)**.
10. Select the data source you created in Steps 3–7 and create the connection.

You can also use the WatchGuard Web Services API to export data for Crystal Reports. For more information, see *Use the Web Services API to Retrieve Log and Report Data*.

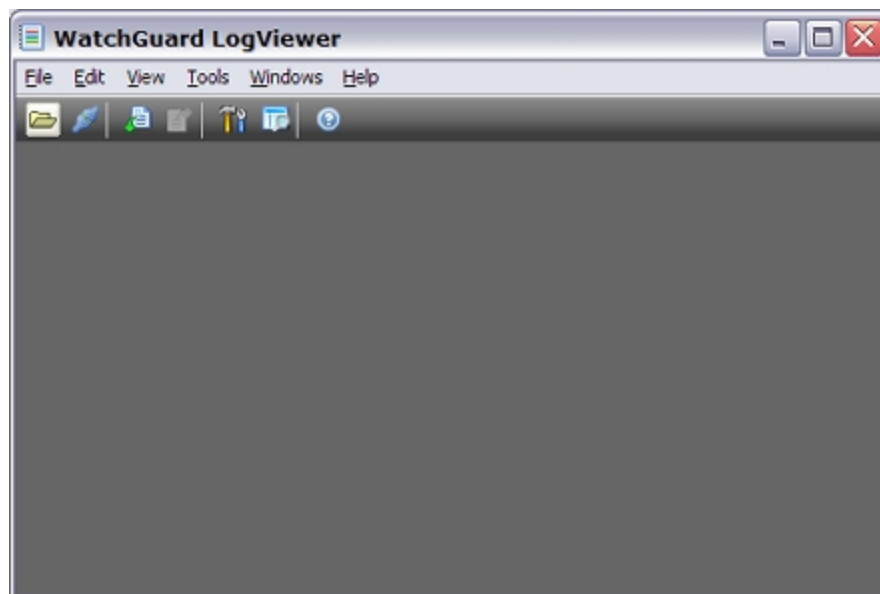
## Use LogViewer to See Log Files

LogViewer is the WatchGuard System Manager tool you use to see log file data. You can use it to review data in the log files currently on your Log Server, or in backup log files. LogViewer can show the log data page by page, or search and display by key words or specific log fields.

### Open LogViewer

1. Open WatchGuard System Manager.
2. Click  on the WatchGuard System Manager toolbar.  
Or, select **Tools > Logs > LogViewer**.


*WatchGuard LogViewer appears.*



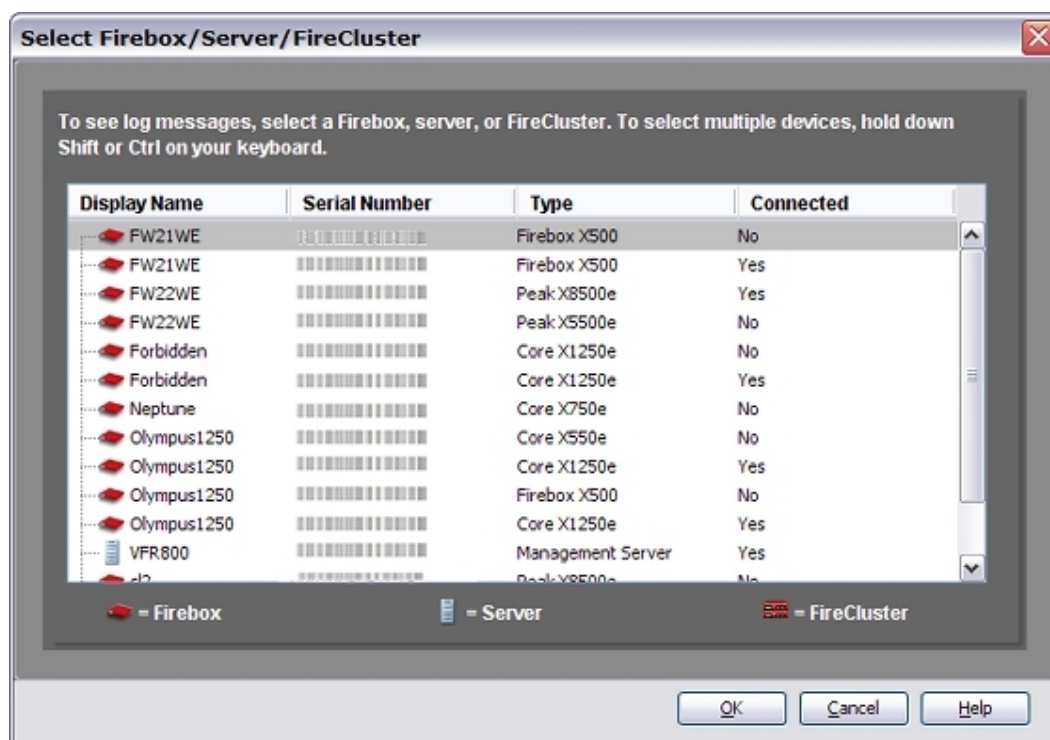
## Connect to a Device

You can connect to XTM devices, Log Servers, or FireClusters. When you connect to an XTM device, you can filter the log data based on the type of log message, date and time, and string searches. When you connect to a Log Server, you can only filter the data by date and time, or simple text string searches. If you select to view log data that has been archived, LogViewer automatically searches the backup files and retrieves the requested log data.

For more information about log message details, see *Set LogViewer User Preferences* on page 730 and *Log Message Details* on page 733.

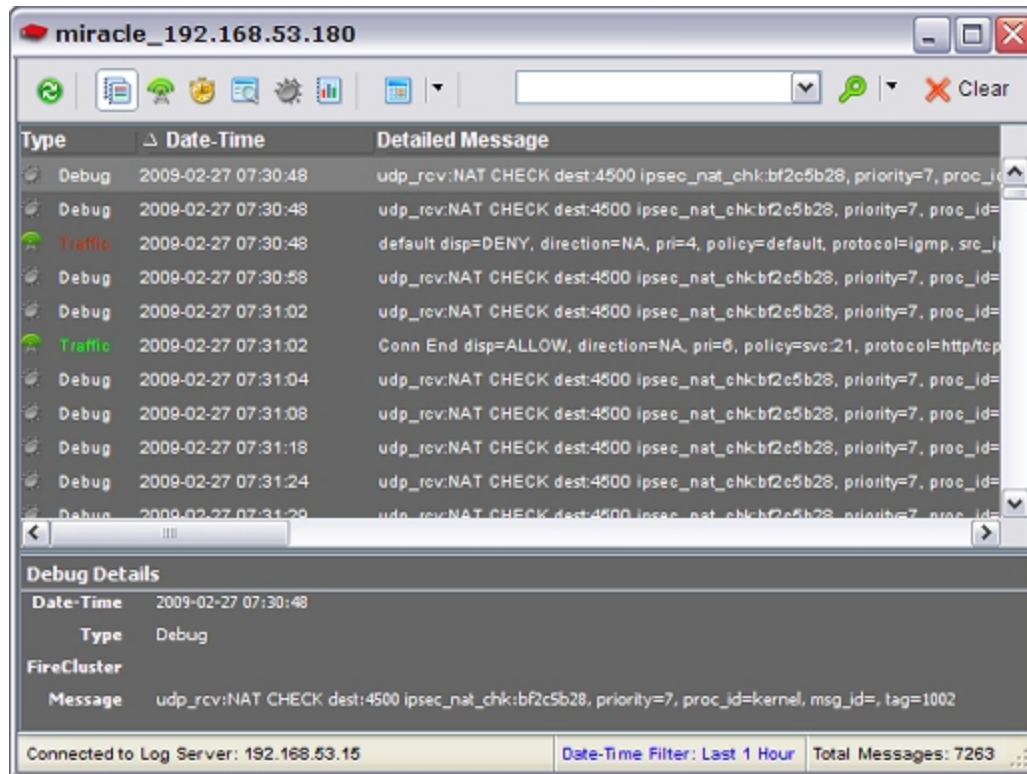
1. Click  on the LogViewer toolbar.  
Or, select **File > Connect to Log Server**.  
*The Connect to Log Server dialog box appears.*
2. Type the IP address, user name, and passphrase for your Log Server.
3. Click **Login**.  
*The Connect to Log Server dialog box disappears. The Select Firebox/Server/FireCluster dialog box appears.*

**Note** *If this is the first time you have connected to this device, server, or cluster, a Certificate Warning appears. You must accept the certificate to proceed and connect.*



4. Select one or more XTM devices, Log Servers, or FireClusters from the list and click **OK**.  
To select multiple devices, hold down Shift or Control on your keyboard.  
*A device window appears for each selected device. The IP address of the device appears in the window title bar. The contents of a XTM device window and a Server window are different.*





5. Select a log message to see more information about the message.  
*The selected log message details appear in the Details pane at the bottom of the device window.*
6. If the details pane is not visible, select **View > Details Pane** to enable it.


For more information about displaying device data, see *Set LogViewer User Preferences* on page 730.

## Open Logs for the Primary Log Server

If you have specified a Primary Log Server, you can open the log files for this server from the main LogViewer window before you connect to it. You can then see the list of XTM devices that are currently logging to the Primary Log Server. You must select a Primary Log Server to enable this option.

For more information about how to select a Primary Log Server, see *Set LogViewer User Preferences* on page 730.

To open logs for the primary Log Server:

1. Open LogViewer.
  2. Click  on the LogViewer toolbar.
- Or, select **File > Open Logs For**.

*The Select Firebox/Server/FireCluster dialog box appears with a list of connected devices.*

For more information on the LogViewer, see *Use LogViewer to See Log Files* on page 727.

## Set LogViewer User Preferences

You can adjust the content and the format of the LogViewer window. You can select a primary Log Server for LogViewer to connect to automatically and adjust the Search feature settings. You can also configure the appearance of the LogViewer window, select the types of logs that appear, and the details included for each message type.

To set LogViewer user preferences:

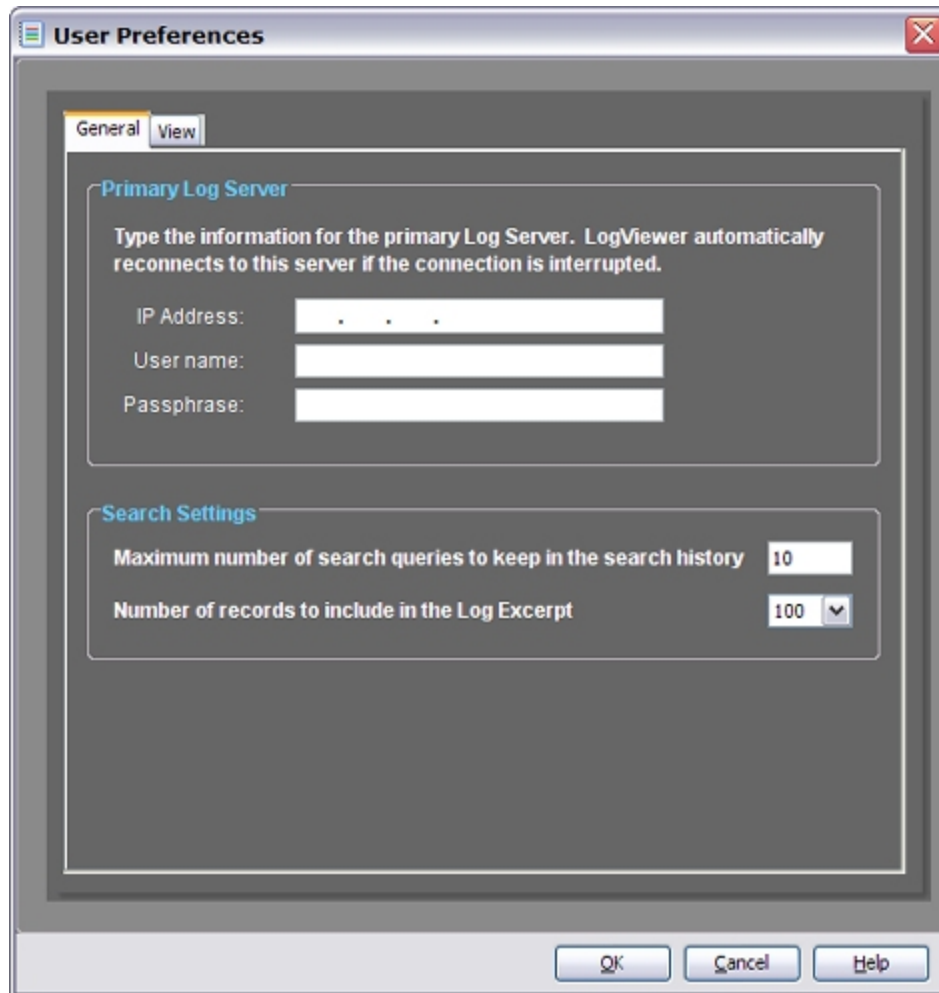
1. Select **View > Preferences**.  
*The User Preferences dialog box appears.*
2. Select a tab to configure the LogViewer window.
  - The **General** tab includes options for setting a primary Log Server and search parameters.
  - The **View** tab includes options to configure the LogViewer window and column settings for each log message type.

## Configure the Primary Log Server and Search Settings

You can specify a Log Server for LogViewer to automatically reconnect to, and configure the settings for the LogViewer Search feature.

From the **User Preferences** dialog box:

1. Select the **General** tab.



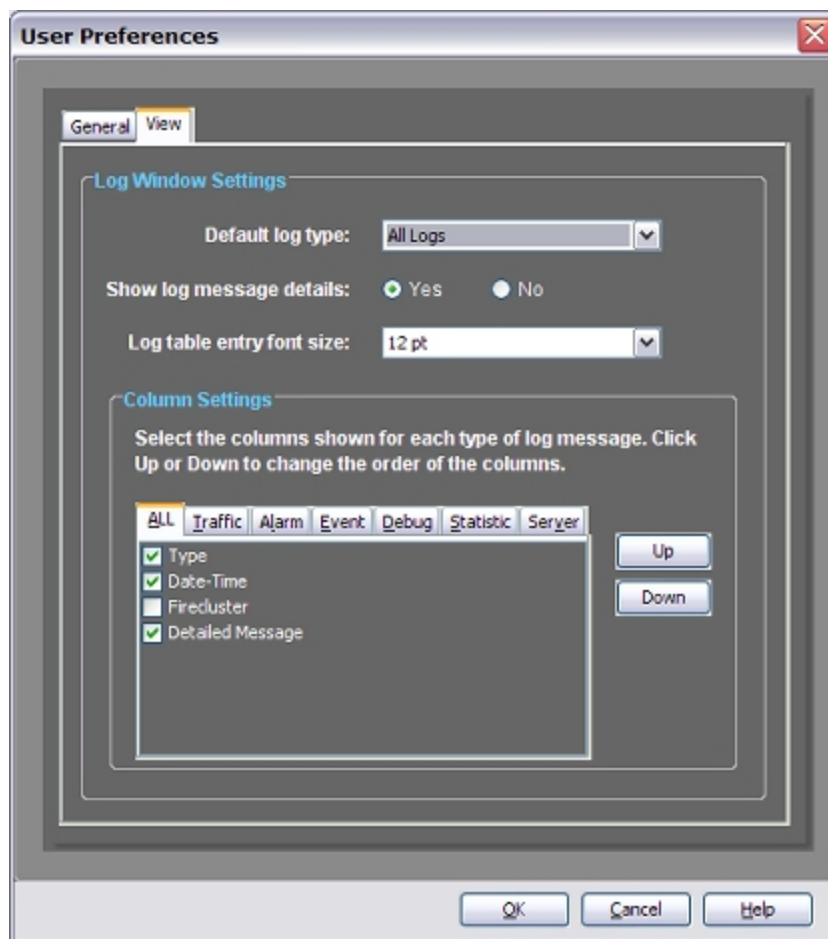
2. To enable LogViewer to automatically reconnect to a specific Log Server, in the **Primary Log Server** section, type the **IP Address**, **User name**, and **Passphrase** for your primary Log Server.  
If you do not want to specify a primary Log Server, keep these fields blank.
3. In the **Maximum number of search queries to keep in the search history** text box, type the maximum number of search queries to keep in your search history.
4. Select the **Number of records to include in the Log Excerpt** from the drop-down list.

## Configure the LogViewer Window and Column Settings

You can also specify the information that appears in the LogViewer windows.

From the **User Preferences** dialog box:

1. Select the **View** tab.



2. Select the type of log messages you want to include from the **Default log type** drop-down list.
3. Select whether to **Show log message details** for the log messages.
4. From the **Log table entry font size** drop-down list, select the font size you want to use for the log table entries.
5. Select the **Column Settings** to include for each type of log message.

Each tab includes a list of available details for that message type. Use these tabs to select which columns of details appear for each message type.

Click **Up** or **Down** to change the order of the columns.

6. Click **OK**.

For more information about the available log message types, see *Log Message Details* on page 733.

## Log Message Details

You can select the details you see in each type of log message by the columns you select to include in the different types of log messages. The subsequent list includes all available columns. Not all columns will appear for all message types.

Log Message Column	Description
Additional Info	Additional details about the log message for proxy logs. For example: hostname, filename, rule_name, content_type.
Alarm ID	The number associated with the alarm.
Alarm Name	The category of the alarm (System, IPS, AV, Policy, Proxy, Probe, Denial of service, or Traffic).
Alarm Type	The type of alarm (email, popup).
Application Provider	The name of the server that provides the data.
Bytes Received	The number of bytes received by a device (WAN or Tunnel) within the statistics log period.
Bytes Sent	The number of bytes sent by a device (WAN or Tunnel) within the statistics log period.
Connection ID	The number of the server connection.
DateTime	The date and time on the server when the log message was received.
Destination Interface	The name of the destination interface.
Destination IP	The destination IP address for this packet.
Destination IP-NAT	The way NAT (Network Address Translation) was handled for the destination IP address for this packet.
Destination Port	The destination port for this packet.
Destination Port-NAT	The way NAT (Network Address Translation) was handled for the destination port for this packet.
Detailed Message	All the log message fields, separated by commas ( , ).
Device	The name of the device that sent out the performance log (WAN or Tunnel).
Direction	The direction of the action. Can be incoming or outgoing.

Log Message Column	Description
Disposition	The packet disposition. Can be deny or allow.
Message	The message field.
Message Code	The code for the message type.
Message Timestamp (s.ms)	The timestamp for the message in <i>seconds.milliseconds</i> format.
Misc. Details	Additional details from the columns you selected to include for the log message type. For example: RC (Return Code), Packet Length, and TTL (packet Time To Live in seconds).
Policy	The name of the policy in Policy Manager that handled this packet.
Priority	The priority level of the log message.
Process ID	The ID for the process completed in the log message action.
Protocol	The protocol used in this packet.
Proxy Action	The name of the proxy action handling this packet. A proxy action is a set of rules for a proxy that can be applied to more than one policy.
Request ID	The ID for the server process requested in the log message.
Return Code	Return code for the packet.
Source Interface	The name you have given the source interface for this packet (as defined in Policy Manager).
Source IP	The source IP address of this packet.
Source IP-NAT	The way NAT (Network Address Translation) was handled for the source IP address for this packet.
Source Port	The source port for this packet.
Source Port-NAT	The way NAT (Network Address Translation) was handled for the source port for this packet.
Type	The type of log message. All logs include a log type in the message: "al" for alarms, "ev" for events, "db" for debug, "pe" for statistic logs, and "tr" for Traffic.


For instructions to select log message details, see *Set LogViewer User Preferences* on page 730.

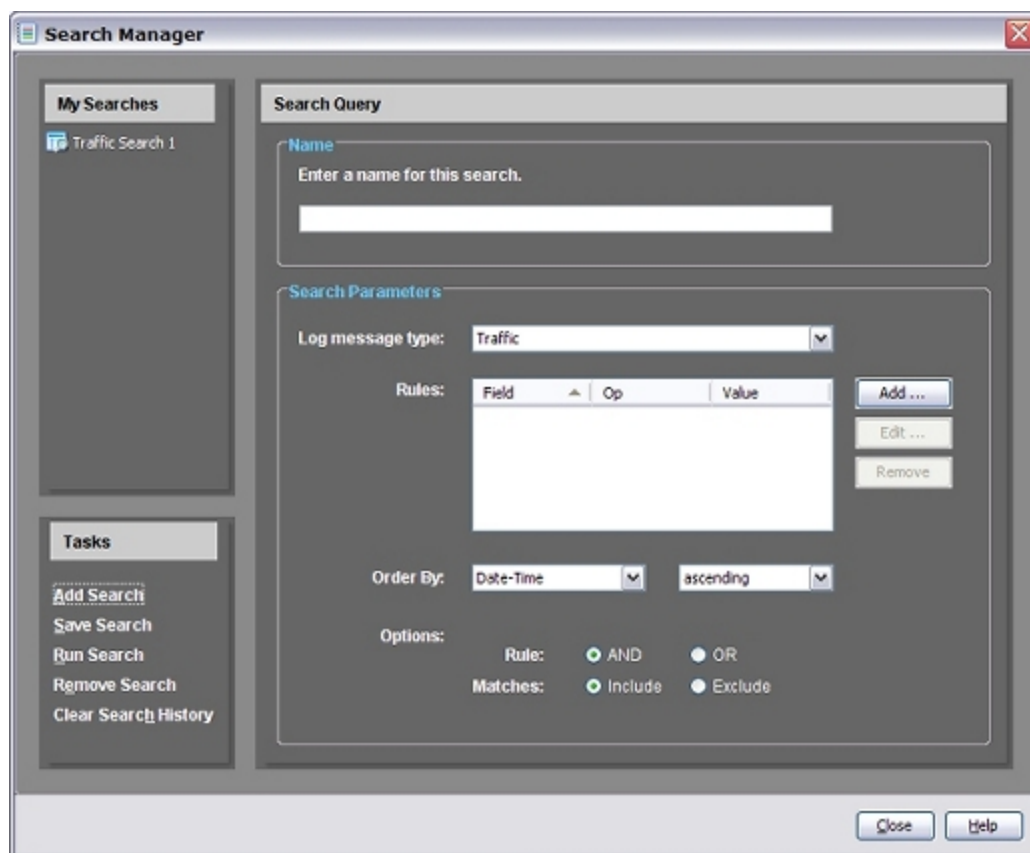
For information about the different types of log messages, see *Types of Log Messages* on page 686.

## Use Search Manager

You can use the LogViewer Search Manager to create rules for searches and then search the data shown in LogViewer. You can create custom searches and save them so you can run them again and again. You can also remove or edit a saved search, and clear the search history.

### Open Search Manager

1. Open LogViewer.  
For information on LogViewer, see *Use LogViewer to See Log Files* on page 727.
2. Click  on the LogViewer toolbar.  
Or, select **Tools > Search Manager**.  
*The Search Manager dialog box appears.*



### Create a Search Query

1. In the **Tasks** pane, click **Add Search**.
2. In the **Name** text box, type a name for your search.
3. Select the **Search Parameters**.  
For more information about search parameters, see *Search Parameter Settings* on page 737.

## Save a search

After you have created a search query, you can save it so you can run it again.

In the **Tasks** pane, click **Save Search**.

*The search name appears in the My Searches list.*

## Remove a Search

When you no longer want to include a saved search in the **My Searches** list, you can remove it. You can remove only one saved search at a time.

1. In the **My Searches** list, select a search.
2. In the **Tasks** pane, click **Remove Search**.

*The search name disappears from the My Searches list.*

## Edit a Search

You can edit a saved search to change the search parameters.

1. In the **My Searches** list, select a search.

*The selected search name appears in the Name field.*

2. Edit the search parameters.
3. In the **Tasks** pane, click **Save Search**.

*The Save Search message appears.*

## Run a Search

You can run a saved or a new search query.

To run a saved search:

1. In the **My Searches** list, select a search.
2. In the **Tasks** pane, click **Run Search**.

*The log messages that match the saved search query parameters appear in the LogViewer window.*

To run a new search query:

1. Define the search query.

For more information, see the *Create a Search Query* section.

2. In the **Tasks** pane, click **Run Search**

*The log messages that match the saved search query parameters appear in the LogViewer window.*

## Clear the Search History

You can remove all recent searches from the search history.

In the **Tasks** pane, click **Clear Search History**.



## Search Parameter Settings

You can use LogViewer Search Manager to define specific search parameters to find particular details in your log files. To create a search query, select from the available options in each field.

For more information about how to run a search query, see *Use Search Manager* on page 735.

To configure **Search Parameters**:

1. Select a type of log message from the **Log message type** drop-down list.
  - **All logs**
  - **Traffic**
  - **Alarm**
  - **Event**
  - **Debug**
  - **Statistic**
  - **Server**
2. To apply column, operator, and value Rules to your search query click **Add** or **Edit**.
  - **Column** — Select a column to search in from the drop-down list.
  - **Operator** — Select the operation to apply in your search: EQUAL TO, NOT EQUAL TO, GREATER THAN ( > ), LESS THAN ( < ), CONTAINS.  
*Some operators are available only for specific columns. If an operator does not appear in the drop-down list, it is not available for the column option you selected.*
  - **Value** — Type a value for the operator to search on.
3. Click **OK** to save your search rule settings.
4. From the **Order By** drop down lists, select the order to display the search results and whether to see the results in **ascending** or **descending** order.  
 You can choose any column that can be sorted and is available for the selected log message type.

5. Select the display **Options** for the search rule.
  - **Rule** — If you choose **AND**, only results that match all rules are displayed. If you choose **OR**, results that match any of the rules are displayed. If there is only one rule in your search, this setting does not apply.
  - **Matches** — Select whether the search query results **Include** or **Exclude** log messages that match the parameters you set in your search rules.








## Filter Log Messages by Type and Time, or Run a String Search

LogViewer includes type and time filters that you can use to show specified types of log message for a time period that you define. You can also use the string search feature to find log messages that include a particular series of characters. This can be useful when you troubleshoot and debug an issue.

### Filter Log Messages by Type and Time

1. To filter the log messages by type, click a log type button.

*LogViewer sorts the log messages and shows only messages of the selected log type.*

  -  — **All logs**
  -  — **Traffic**
  -  — **Alarm**
  -  — **Event**
  -  — **Debug**
  -  — **Statistic**
2. To specify a time filter, click  and select an option:
  - **All Logs**
  - **Last 1 Minute**
  - **Last 5 Minutes**
  - **Last 10 Minutes**
  - **Last 30 Minutes**
  - **Last 1 Hour**
  - **Last 1 Day**
  - **Last 1 Week**
  - **Custom Filter**

*The log message data for the timeframe you selected appears in the LogViewer window*

## Specify a Custom Date-Time Filter

To select a specific date and time range for log message data, from the **Date-Time** drop-down list:

1. Select **Custom Filter**.

*The Custom Date-Time Filter dialog box appears.*

**Custom Date-Time Filter**

Enter the time range for your search.

**Start Date and Time**

January 2009						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Hour: 12 Minute: 46

**End Date and Time**

February 2009						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

Hour: 12 Minute: 46

**Date-Time Range Selected**

2009-01-10 12:46:00 to 2009-02-14 12:46:00

OK Cancel Help

2. From the **Start Date and Time** calendar, select the first day of the date range.
3. In the **Start Date and Time Hour** and **Minute** text boxes, type or select the start of the time range.  
*The selected date and time range appears in the Date-Time Range Selected section.*
4. From the **End Date and Time** calendar, select the last day of the date range.
5. In the **End Date and Time Hour** and **Minute** text boxes, type or select the end of the time range.  
*The selected date and time range appears in the Date-Time Range Selected section.*
6. Click **OK**.  
*The log message data for the timeframe you specified appears in the LogViewer window.*

## Run a String Search

You can *Use Search Manager* to search log messages for specific details, or you can run a string search from LogViewer.

1. In the drop-down list at the top right of the LogViewer window, type a specific text string to find in the logs.



For example, type HTTP Proxy to search for all HTTP Proxy log messages.

2. Click .

To choose how the results appear in LogViewer, click  and select an option:

### *Show only results*

Excludes all log messages that do not match your search from the LogViewer window. The original message you selected is highlighted.

### *Highlight results*

Includes all log messages in the window, but highlights only those that match your search.

### *Recent Saved Searches*

Includes searches you have saved in Search Manager. Select a search from the list to run on the log messages that currently appear in the device window.

*LogViewer searches through the log messages and applies the selected search settings.*

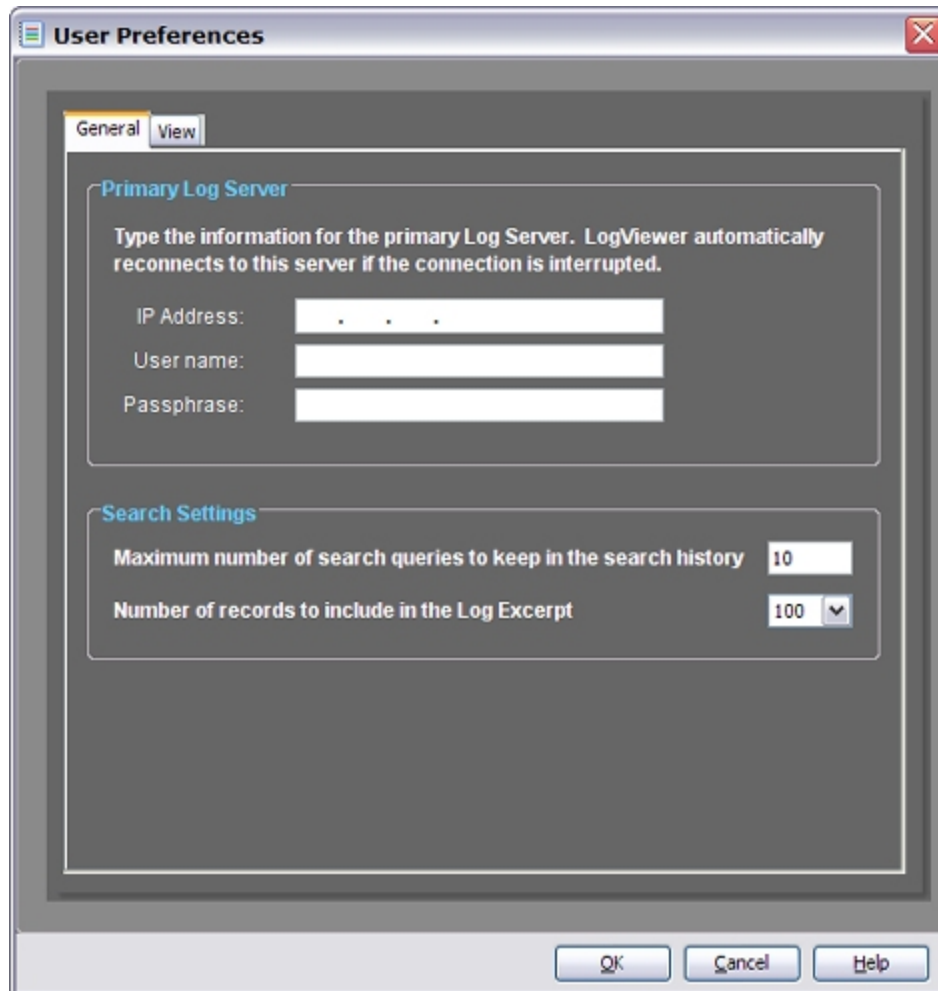
## Use Log Excerpt to Filter Search Results

LogViewer includes search options that you can use to find a specific event that occurred on your XTM device. After you have found a specific log message, you can use Log Excerpt to see the log messages that the Log Server recorded before and after the log message you selected. You can also choose the number of logs (50–250) that you want to see in addition to the selected log message. This can help you review other events that occurred at the same time to troubleshoot a network problem.

You can also use Log Excerpt to compare log messages from two different devices to debug an issue. For example, you can use this feature to review log messages from endpoint devices when you have a problem with a VPN tunnel.

## Set the Number of Log Excerpts


1. Select **View > Preferences**.  
*The User Preferences dialog box appears.*
2. Select the **General** tab.



3. From the **Number of records to be included in the Log Excerpt** drop-down list, select the number of records to include.  
*The default setting is 100.*
4. Click **OK**.


## Use Log Excerpt to Refine Search Results

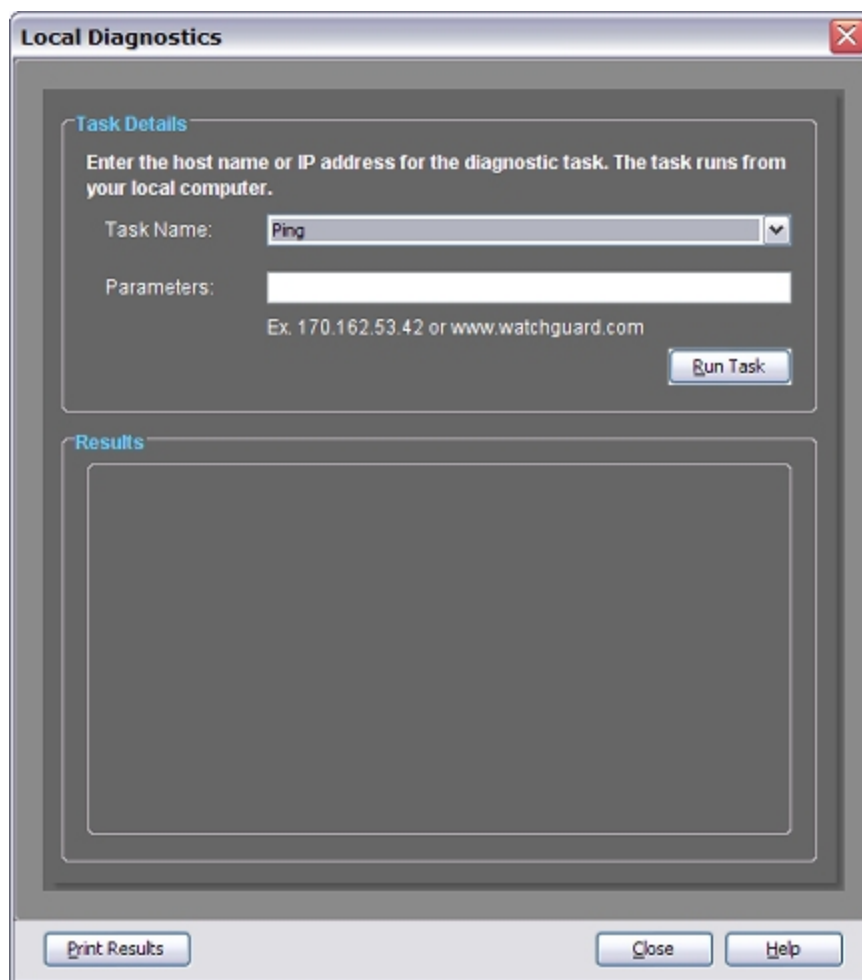
To use Log Excerpt you must run a search query for a text string within the log messages.

1. In LogViewer, [connect to a Log Server, Firebox, or XTM device](#).
2. Select a log message type and [run a string search](#) or [create a custom search query](#).
3. Select a log message in the LogViewer window.
4. Right-click the log message and select **Show Log Excerpt**.  
Or, press the **F5** key.  
*LogViewer filters the search result and shows the number of logs you set around the timestamp for the selected log message.*
5. Click  **Clear** to remove the filters and return to the original view in the LogViewer window.

## Run Local Diagnostic Tasks

You can use LogViewer to run diagnostic tasks on any IP address or host. Diagnostic tasks include **Ping**, **Tracert**, and **NSLookup**.

1. Click  on the LogViewer toolbar.  
Or, select **Tools > Local Diagnostics** and select a task.  
*The Local Diagnostics dialog box appears.*




2. From the **Task name** drop-down list, select a task.
  - **Ping** — Make sure an IP address or host is active.
  - **Tracert** — Trace the route to the IP address or host and see the route transfer time.
  - **NSLookup** — Verify the server name and actual IP address of the selected IP address or host.
3. In the **Parameters** text box, type an IP address or host name.
4. Click **Run Task**.  
*The task results appear in the Results field.*
5. To print the task results, click **Print Results**.  
*The Print dialog box appears.*
6. Select the print parameters and click **Print**.

---

## Import and Export Data to LogViewer


You can use LogViewer to see data from existing database log files, or to export selected data to a database file.

### Import Data

1. On the LogViewer toolbar, click .  
Or, select **File > Import Data**.  
*The Import Data dialog box appears.*
2. Browse to select a database file.
3. Click **Import**.  
*The selected data appears in a new Firebox or Server window.*

For more information about LogViewer Server windows, see *Use LogViewer to See Log Files* on page 727.

### Export Data

1. Select the log messages to export in the LogViewer Firebox or Server window.
2. On the LogViewer toolbar, click .  
Or, select **File > Export Selected Data**.  
*The Export Selected Data dialog box appears with the default file name displayed in the File name text box.*
3. Browse to select a directory where you want to save the database file.
4. To rename the database file, in the **File name** text box, type a new name for the database file.
5. Click **Export**.  
*The database file is saved to the selected directory.*

## Email, Print, or Save Log Messages

After you select one or more log messages in LogViewer, you can email, print, or save them. For more information about how to use LogViewer, see *Use LogViewer to See Log Files* on page 727.

### Send a Log Message in Email

1. Open LogViewer.
2. Select **File > Send Selection As** and select an option:
  - **Comma Separated Values (\*.csv)**
  - **Portable Document Format (\*.pdf)**

*An email message opens with the log message attached in the selected file format.*

### Print a Log Message

1. Open LogViewer.
2. Select **File > Print Selection**.  
*The Print dialog box appears.*
3. Select a printer and the print options.
4. Click **Print**.

## Save a Log Message

1. Open LogViewer.
2. Select **File > Save Selection as** and select an option:
  - **Comma Separated Values (\*.csv)**
  - **Web Page (\*.htm, \*.html)**
  - **Portable Document Format (\*.pdf)**
  - **Extensible Markup Language (\*.xml)**

*The Save dialog box appears.*

3. Select a location and type a file name.
4. Click **Save**.



# 22 Monitor Your Device

---

## About Firebox System Manager (FSM)

WatchGuard Firebox System Manager (FSM) gives you one interface to monitor all of the components of your XTM devices and the work they do. You can see:

- *Basic XTM Device and Network Status (Front Panel)*
- *Device Log Messages (Traffic Monitor)*
- *Visual Display of Bandwidth Usage (Bandwidth Meter)*
- *Visual Display of Policy Usage (Service Watch)*
- *Traffic and Performance Statistics (Status Report)*
- *Authenticated Users (Authentication List)*
- *Manage the Blocked Sites List (Blocked Sites)*
- *Subscription Services Statistics (Subscription Services)*

You can also launch these applications from Firebox System Manager:

- **Policy Manager** is a tool that you can use to make, change, and save configuration files to your XTM devices.  
For more information, see *About Policy Manager* on page 364
- **HostWatch** is a graphical user interface that shows the connections between different XTM device interfaces.  
For more information, see *About HostWatch* on page 782.
- **Performance Console** is a utility that you use to make graphs which show how different parts of the XTM device perform.  
For more information, see *About the Performance Console* on page 789.
- **Communication log** keeps messages about connections between the XTM device and Firebox System Manager.  
For more information, see *Communication Log* on page 797.


You can use Firebox System Manager to:

- *Manage XTM Device Certificates*
- *Start Firebox System Manager*
- *Reboot or Shut Down Your XTM Device*
- *Calculate the Fireware XTM Checksum*
- *See and Synchronize Feature Keys*
- *Synchronize the System Time*
- *Clear the ARP Cache*
- *Clear Alarms*
- *Rekey BOVPN Tunnels*
- *Control FireCluster*
- *Change Passphrases*

## Start Firebox System Manager

You can use Firebox System Manager (FSM) to view the status of your connected XTM device. Before you can use FSM, WatchGuard System Manager must be open and you must be connected to a device. You can open more than one FSM window to show the status of different XTM devices, but you must open each window one at a time.

For more information, see *Start WatchGuard System Manager* on page 29 and *Connect to an XTM Device* on page 29.

1. From WatchGuard System Manager, select the **Device Status** tab.
2. Select the XTM device to examine with Firebox System Manager.
3. Click .

Or, select **Tools > Firebox System Manager**.

*Firebox System Manager appears.*

You might need to wait for a few seconds for Firebox System Manager to connect to the XTM device before you can see status information.

## Disconnect from and Reconnect to a XTM device

You can stop and start the monitored connection to your XTM device while the FSM window is still open. This allows you to stop the flow of data to FSM from the monitored device. You can also start the flow of data again.

To disconnect FSM from the XTM device and stop the monitored connection:

1. Start FSM.
2. Click .

Or, select **File > Disconnect**.

*The device status changes to Not Monitored.*

To connect FSM to the XTM device and start the monitored connection:

1. Start FSM.
2. Click .

Or, select **File > Connect**.

*The device status changes to Connected.*

## Set the Refresh Interval and Pause Display

At the bottom of the window, each Firebox System Manager (FSM) tab includes a drop-down list to set the refresh interval and a **Pause** button to stop the display.

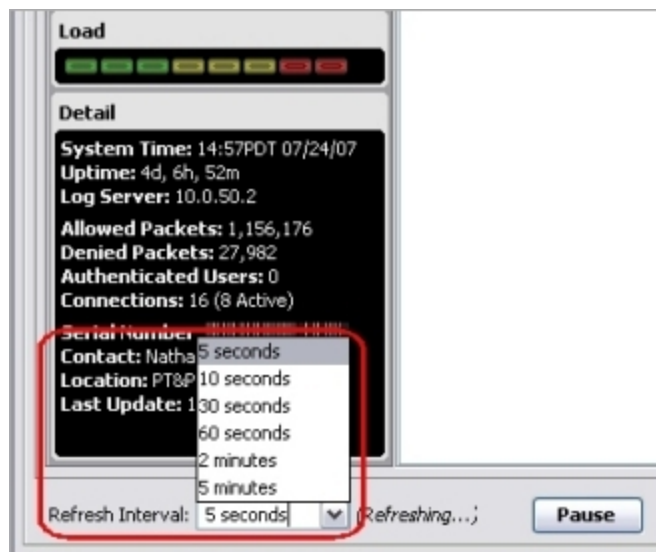
### Refresh Interval

The refresh interval is the polling interval, or the time FSM waits before the display is refreshed. You can change the amount of time (in seconds) that FSM waits before it gets new information from the XTM device and sends the updates to the display.

Before you select an interval, be sure to examine how frequently you want to see new information in relation to the load the selected interval places on the XTM device. A shorter time interval gives a more accurate display, but can have effects on network performance. Be sure to also examine the refresh interval on each tab. When a tab gets new information for its display, the text *Refreshing...* appears adjacent to the **Refresh Interval** drop-down list.

From Firebox System Manager:

Click the **Refresh Interval** drop-down list to select the duration between window refreshes. Or, type a custom value in this field.



### Pause/Continue

To temporarily stop the flow of information from the device:

Click **Pause**.

*The button changes to Continue.*

To refresh the information in the window:

Click **Continue**.

*The button changes to Pause.*

## Basic XTM Device and Network Status (Front Panel)

The **Front Panel** tab of Firebox System Manager shows basic information about your XTM device, your network, and network traffic. It also shows warnings about your device or its components.

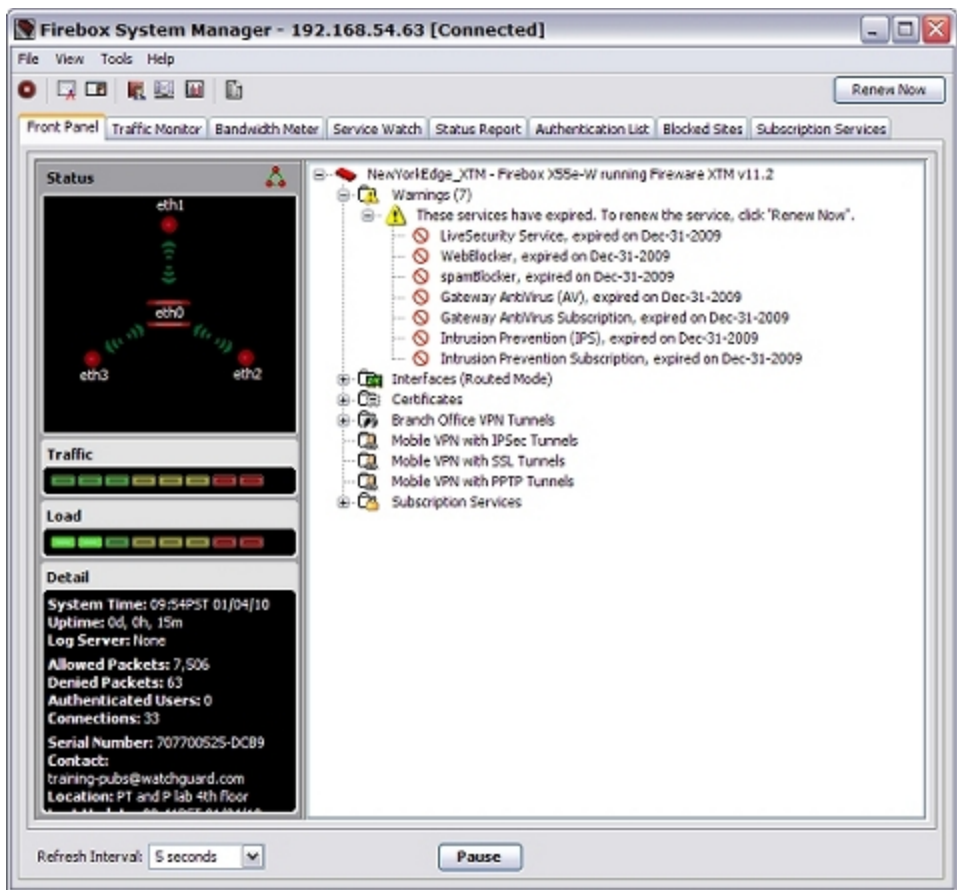
For instructions to open Firebox System Manager, see *Start Firebox System Manager* on page 746.

For details on XTM device and network status, see:

- *Visual Display of Traffic Between Interfaces*
- *Traffic Volume, Processor Load, and Basic Status*
- *XTM Device Status*
- *VPN Tunnel Status and Subscription Services*

## Warnings and Notifications

Any warnings for your XTM device appear on the **Front Panel** tab in the list above all other status information. If there is an action you can take for a warning or notification, a button also appears at the upper-right corner of the window.



*Activate Now*

If the XTM device has not been activated, a notice appears in the **Warnings** list and the **Activate Now** button appears.

Click **Activate Now** to go to the LiveSecurity Service web site where you can get a feature key for the XTM device.

#### *Renew Now*

If any WatchGuard System Manager (WSM) services are soon to expire, a notice appears in the **Warnings** list and the **Renew Now** button appears.

Click **Renew Now** to go to the LiveSecurity Service web site to renew the services.

#### *WAN Fail Back*

If you configure Multi-WAN, but do not enable automatic connection failback, when a WAN failover event occurs, the **WAN Fail Back** button appears.

Click **WAN Fail Back** to fail back to the configured failover connection.

## Expand and Close Tree Views

To expand a part of the display:

Click the **plus icon (+)** adjacent to the entry.  
Or, double-click the entry.

To close a part of the display:

Click the **minus icon (-)** adjacent to the entry.

If a plus or minus icon does not appear, additional information is not available.

## Visual Display of Traffic Between Interfaces

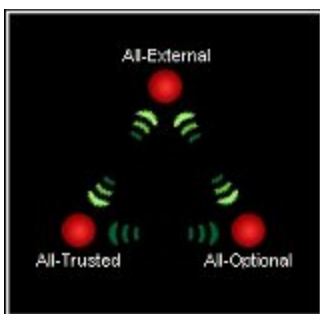
At the upper-left corner of the window, Firebox System Manager (FSM) has a visual display that shows the direction of traffic for the XTM device interfaces. The display also shows whether the current traffic is allowed or denied at each interface. The display can be in the shape of a triangle or a star.

The points of the star and triangle show the traffic that flows through the interfaces. A green point shows traffic is allowed at that interface. A red point shows that either traffic is denied, or that some traffic is denied and other traffic is allowed. Each point shows incoming connections and outgoing connections with different arrows. When traffic flows between the two interfaces, the arrows light up in the direction of the traffic.

## Triangle Display

In the triangle figure, the points of the triangle show the network traffic. The points show only the idle or deny condition. One exception is when there is a lot of default-route VPN traffic. Default-route VPN traffic refers to packets that are sent through a VPN to a XTM device configured as the default gateway for the VPN network. In this case, the FSM traffic level indicator can show very high traffic, but you do not see green lights when more default-route VPN traffic goes in and out of the same interface.

If a XTM device has only three configured interfaces, each corner of the triangle is one interface. If a device has more than three interfaces, each corner of the triangle represents one type of interface. For example, if you have six configured interfaces with one external, one trusted, and four optional interfaces, the *All-Optional* corner in the triangle represents all four of the optional interfaces.



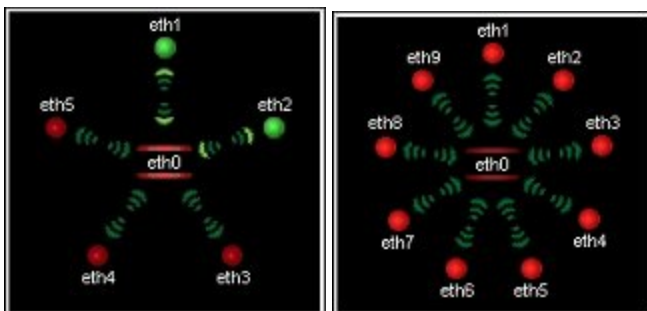
## Star Display

In the star figure, the location where the points come together can show one of two conditions:

- Red (deny) — The XTM device denies a connection on that interface.
- Green (allow) — There is traffic between this interface and a different interface (but not the center) of the star. When there is traffic between this interface and the center, the point between these interfaces appears as green arrows that blink.

The star display shows all traffic in and out of the center interface. An arrow moves from the center interface to a node interface to show the flow of traffic through the XTM device. The traffic comes in through the center interface and goes out through the node interface. For example, if eth1 is at the center and eth2 is at a node, a green arrow shows that traffic flows from eth1 to eth2.

The star display looks different depending on the type of connected XTM device. The number of nodes in the star changes to match the number of interfaces on your device. One interface is located in the center of the star, and then each additional interface appears on a node of the star. For example, if your device has 6 interfaces, the star has 5 nodes, and if your device has 10 interfaces, the star has 9 nodes.



If you use the star figure, you can customize the interface that appears in its center.

To customize the interface:

Click the interface name or its point.

The interface moves to the center of the star. All the other interfaces move clockwise.

If you move an interface to the center of the star, you can see all traffic between that interface and all other interfaces. The default display shows the external interface in the center.

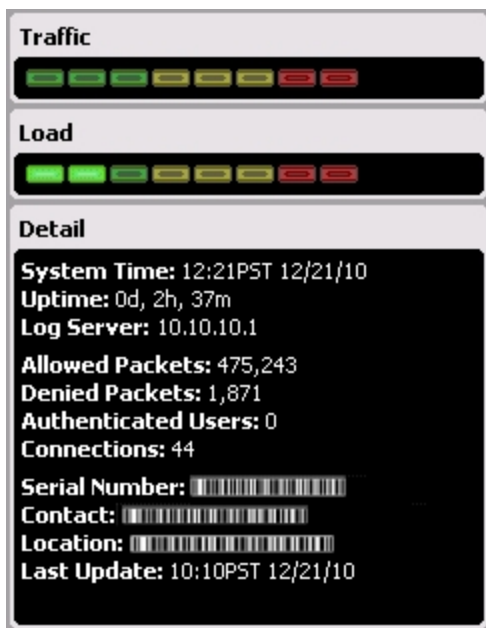
To change the display:

Right-click inside the display area and select **Triangle Mode** or **Star Mode**.

## Traffic Volume, Processor Load, and Basic Status

On the Firebox System Manager **Front Panel** tab, information about the XTM device traffic volume, processor load, and basic device status appears.

Below the **Security Traffic Display** are the **Traffic** volume indicator, processor **Load** indicator, and basic status information (**Detail**). The two bar graphs show the traffic volume and the XTM device capacity.

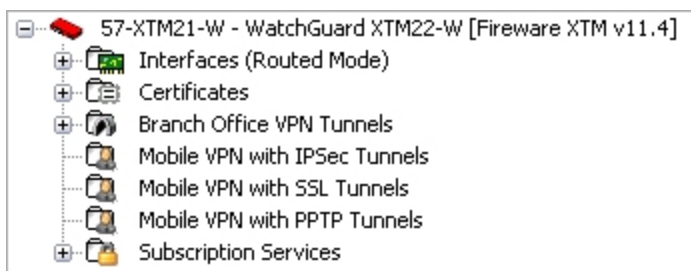


## XTM Device Status

Firebox System Manager (FSM) shows basic status information at the right side of the **Front Panel** tab.

### Status and Warnings

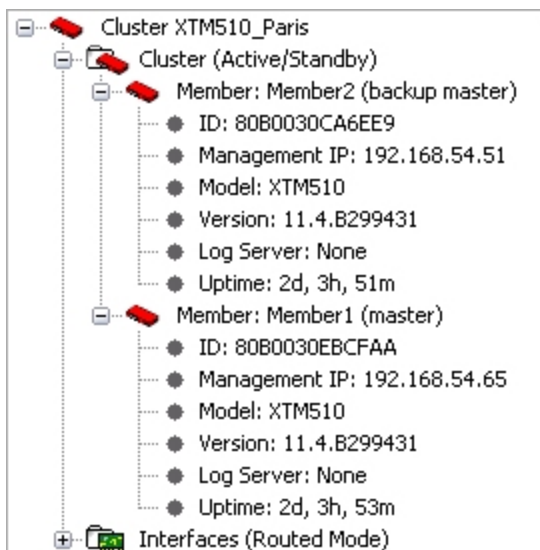
- Status of the XTM device — This includes the device version and patch string.
- Warnings — These appear when updates for Security Services are available, or when Subscription Services or other features are soon to expire.  
To renew, click **Renew Now** at the upper-right of FSM.



### XTM device, FireCluster, and Interface Details

On the **Front Panel** tab, expand the entries to see:

- The IP address of each XTM device interface and the configuration mode of the external interface.
- If FireCluster is configured, whether the FireCluster member devices are available. The time at which the configuration of the member devices was last updated also appears.

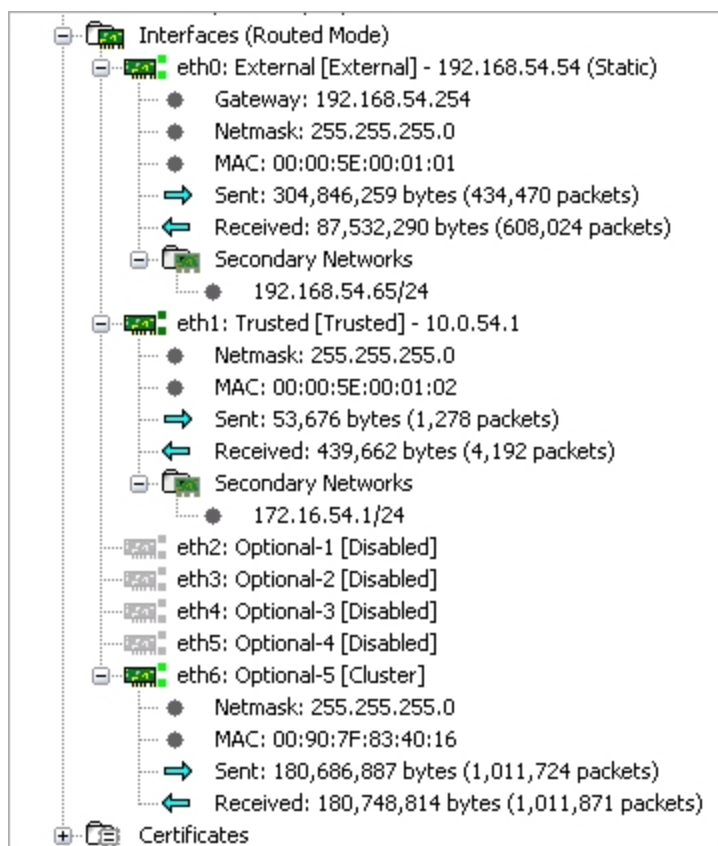


If you expand the entries for each interface again, you can see:

- IP address, gateway, and netmask of each configured interface
- Media Access Control (MAC) address of each interface
- Number of bytes and packets sent and received since the last XTM device restart



- Status of the physical link (an interface or link icon in color means an interface or link is configured, and a dark icon indicates the interface or link is down)



## Certificates and Their Current Status

FSM shows the XTM device certificates and their current status. For valid certificates, FSM shows the validity period and fingerprint.



## Device Log Messages (Traffic Monitor)

You can use Firebox System Manager (FSM) to see log messages from your XTM device as they occur. On some networks, there can be a short delay as log messages are sent.

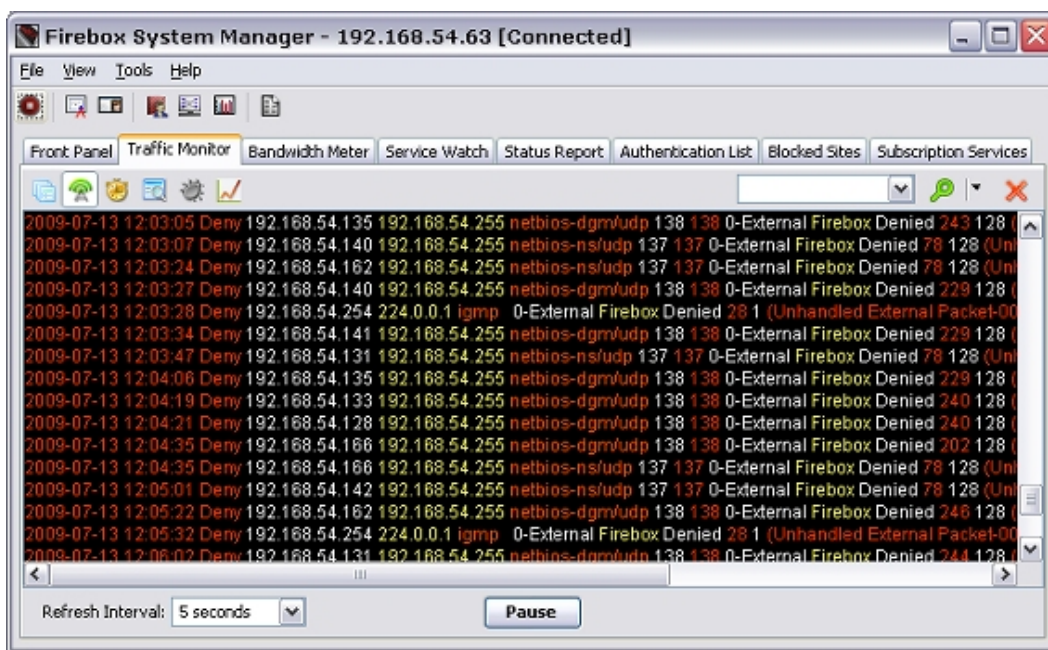
1. Start *Firebox System Manager*.
2. Select the **Traffic Monitor** tab.

Traffic Monitor can help you troubleshoot network performance. For example, you can see which policies are used most or whether external interfaces are constantly used to their maximum capacity.

You can customize Traffic Monitor to:

- *Change Traffic Monitor Settings*
- *Copy Messages to Another Application*
- *Learn More About Traffic Log Messages*
- *Enable Notification for Specific Messages*
- Use the Traffic Monitor icons to display specific *Types of Log Messages*
- *Learn More About Traffic Log Messages* (to help diagnose a problem)







For more information, see *Set the Diagnostic Log Level*.



## Sort and Filter Traffic Monitor Log Messages


You can use the FSM Traffic Monitor buttons to sort the information that you see in the Traffic Monitor. When you select a button, Traffic Monitor shows only log messages of the type you selected. You can also use the filter text box to search the log messages and refine the data you see in Traffic Monitor.


To sort by message type:

1. Select the **Traffic Monitor** tab.
2. To select the type of log message you want to see in Traffic Monitor, click a button:
  -  — All Logs
  -  — Traffic Logs
  -  — Alarm Logs
  -  — Event Logs
  -  — Debug Logs
  -  — Performance Statistics Logs

*FSM sorts the log messages and shows only messages of the type you selected.*

To filter log messages by specified details:

1. Select the **Traffic Monitor** tab.
2. From the filter drop-down list, type or select the information on which you want to search. You can type any value in the filter text box, or select a previously specified value from the drop-down list.
3. From the  drop-down list, select **Highlight Search Results** or **Filter Search Results**.

*The log messages that match the filter search you selected appear in the Traffic Monitor window.*
4. To remove the filter, click .

## Change Traffic Monitor Settings

You can customize the appearance of Traffic Monitor. You can select the background color for the windows, the text color for log types, whether to show logs in color, whether to show the names of the log fields, enable the use of regular expressions when you filter log messages, and set the maximum number of log messages.

To change Traffic Monitor settings:

1. *Start Firebox System Manager.*
2. Select **File > Settings**.

Or, right-click anywhere on the display and select **Settings**.  
*The Settings dialog box appears.*
3. Configure the settings as described in the subsequent sections.
4. Click **OK**.

## Set the Maximum Number of Log Messages

From the **Settings** dialog box, you can change the maximum number of log messages that you want to appear in Traffic Monitor at the same time. When the maximum number is reached, new log messages replace the oldest entries. If you have a slow processor or a small quantity of RAM, a high value can slow your management computer.

If it is necessary to examine a large volume of log messages, we recommend that you *Use LogViewer to See Log Files*.

1. Select the **Traffic Monitor** tab.
2. From the **Maximum Log Messages** drop-down list, select the maximum number of log messages.

## Show Log Field Names

You can enable Traffic Monitor to include labels for log message fields, such as `src_ip`, `dst_ip`, and `src_port`.

1. Select the **Traffic Monitor** tab.
2. Select the **Show Log Field Names** check box.

## Enable Regular Expression Filtering

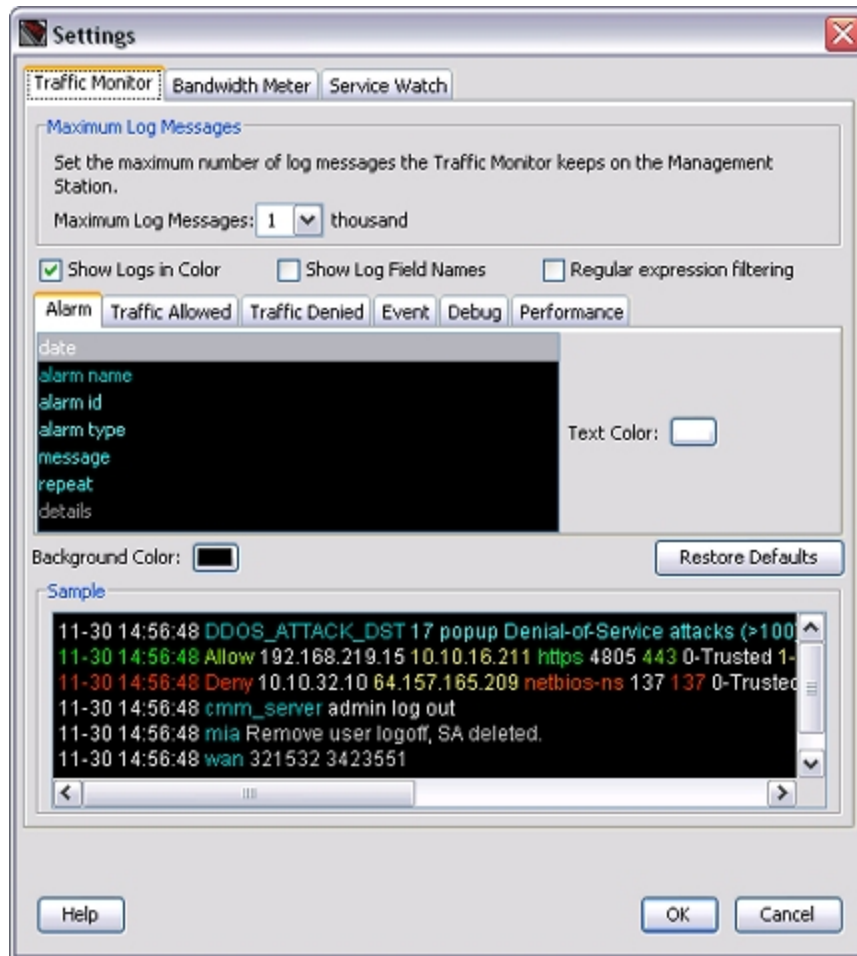
By default, Traffic Monitor filters all log messages with a literal string search. For example, if you type `10.1` in the filter drop-down list, the log messages are filtered to only include entries with the characters `10.1`. To use regular expressions when you filter Traffic Monitor data, you must enable Traffic Monitor to use regular expressions.

1. Select the **Traffic Monitor** tab.
2. Select the **Regular expression filtering** check box.

## Use Color for Log Messages

In Traffic Monitor, you can make messages appear in different colors. You can use different colors to differentiate between types of information. On the **Alarm**, **Traffic Allowed**, **Traffic Denied**, **Event**, **Debug**, and **Performance** tabs, you can select a color for each message type.

1. Select the **Traffic Monitor** tab.



2. To disable all colors in the display, clear the **Show Logs in Color** check box.
3. Select a tab: **Alarm**, **Traffic Allowed**, **Traffic Denied**, **Event**, **Debug**, or **Performance**.
4. Select a log message information category from the list.  
*The current color for the selected category appears in the Text Color color control box.*
5. To change the color, click the **Text Color** color control box.  
*The Traffic Monitor Field Color dialog box appears.*
6. Select a color. A sample of how the color will look in Traffic Monitor appears in the *Sample* window at the bottom of the dialog box.
7. Click **OK** to close the dialog box, or **Reset** to use the previous color.

## Select a Background Color for Traffic Monitor

In the **Settings** dialog box:

1. Select the **Traffic Monitor** tab.
2. Click the **Background Color** color control box.  
*The Traffic Monitor Background Color dialog box appears.*
3. Select a color.  
*A sample of how the color will look in Traffic Monitor appears in the Sample section at the bottom of the dialog box.*

4. Click **OK** to close the dialog box, or **Reset** to go back to the previous color.
5. To cancel your changes and return to the default background color, click **Restore Defaults**.

## Copy Messages to Another Application

You can make a copy of a log message in Firebox System Manager and paste it in a different program.

1. On the **Traffic Monitor** tab, select one or more messages.
2. Right-click the selected message(s) and select **Copy Selection**.  
Or, to copy all of the visible log messages, select **Copy All**.
3. Open the other program and paste the message(s).

You can also use LogViewer to open the log file. LogViewer is the WatchGuard System Manager tool you use to see detailed log file data.

For more information about LogViewer, see *Use LogViewer to See Log Files* on page 727, *Import and Export Data to LogViewer* on page 743, and *Email, Print, or Save Log Messages* on page 743.

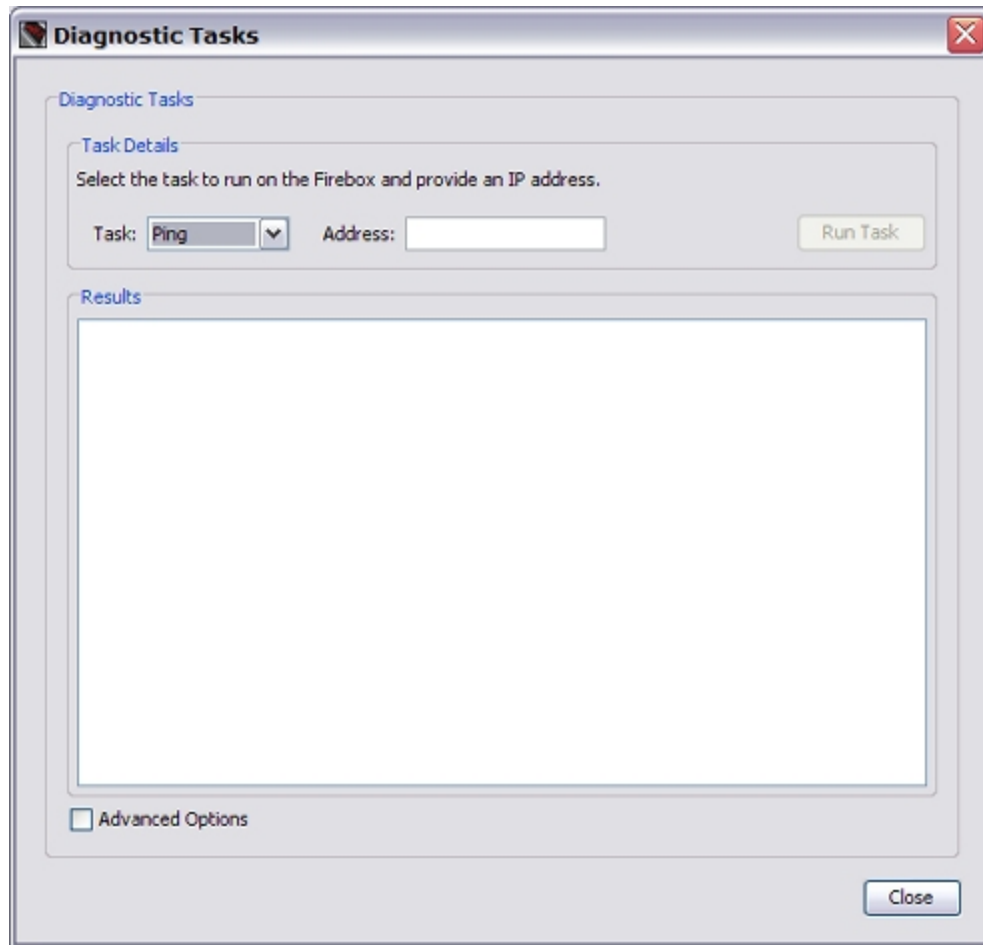
## Learn More About Traffic Log Messages

You can use the Firebox System Manager (FSM) Traffic Monitor Diagnostic Tasks to learn more about a traffic log message, or to review information in your device log messages to help you debug problems on your network. You can ping the source or destination IP address, trace the route to the source or destination IP address, look up DNS information for an IP address, or see information about the packets transmitted across your network (TCP dump). You can also include arguments in your task details to narrow the results.

## Run Diagnostic Tasks

On the FSM **Traffic Monitor** tab, you can run diagnostic tasks to review information in all the log messages from your device. This can help you debug problems on your network.

1. Right-click a message and select **Diagnostic Tasks**.  
*The Diagnostic Tasks dialog box appears.*



2. In the **Task** drop-down list, select the task you want to run.

- **Ping**
- **traceroute**
- **DNS Lookup**
- **TCP Dump**

*If you select Ping, traceroute, or DNS Lookup, the Address text box appears.*

*If you select TCP Dump, the Interface text box appears.*

3. In the **Address** text box, type an IP address.  
Or, select the **Interface** from the drop-down list.
4. To reduce the number of results you see, select the **Advanced Options** check box.  
*The Arguments field appears.*
5. In the **Arguments** text box, type the arguments to include in the search.

Make sure you include the value in the **Address** text box or the **Interface** drop-down list. If you do not include this value in the arguments you type, the search does not run.

To see a list of available arguments, place your cursor over the **Arguments** text box, or keep the text box empty and click **Run Task**.

6. Click **Run Task**.  
*The task information appears in the Results window and the Stop Task button appears.*

7. To stop the diagnostic task, click **Stop Task**.
8. Click **Close** to close the **Diagnostic Tasks** dialog box and return to Traffic Monitor.

## Ping or Trace Route for a Traffic Log Message

You can run a ping or traceroute task on the source or destination IP address for a specific traffic log message to refine the information you see for that message.

1. On the **Traffic Monitor** tab, select a log message.
2. Right-click the message and select a task:
  - **Source IP address > Ping**
  - **Source IP address > Trace Route**
  - **Destination IP address > Ping**
  - **Destination IP address > Trace Route**

*The Diagnostic Tasks dialog box appears with the information for the selected log message and task inserted in the appropriate fields. The selected task starts automatically.*

3. To reduce the number of results you see, select the **Advanced Options** check box.  
*The Arguments field appears.*
4. In the **Arguments** text box, type the arguments and the IP address you want to include in the search. Make sure you type the IP address from the **Address** text box again. To see a list of available arguments, place your cursor over the **Arguments** text box, or keep the text box empty and click **Run Task**.
5. After you have typed any arguments, click **Run Task**.  
*The task information appears in the Results window and the Stop Task button appears.*
6. To stop the diagnostic task, click **Stop Task**.
7. Click **Close** to close the **Diagnostic Tasks** dialog box and return to Traffic Monitor.

## Copy a Log Message IP Address

You can copy the source or destination IP address for a log message in Traffic Monitor to paste in another program or dialog box.

1. On the **Traffic Monitor** tab, select a log message.
2. Right-click the message and select a task:
  - **Source IP address > Copy Source IP address**
  - **Destination IP address > Copy Destination IP address**

*The selected IP address is copied to the system clipboard.*

## Get More Information About IPS Signatures in Traffic Log Messages

If you have enabled logging for Intrusion Prevention Service (IPS) signatures, you can use Traffic Monitor to find more information about the signature IDs associated with traffic log messages.

On the **Traffic Monitor** tab:

1. Select a traffic log message with a signature ID, such as *Detect IPS*.
2. Right-click the log message and select **Lookup Signature Information**.  
*The WatchGuard signature web site appears with details for the signature.*



For more information about IPS and IPS signatures, see *About Intrusion Prevention Service* on page 1187 and *Show IPS Signature Information* on page 1193.

## Enable Notification for Specific Messages

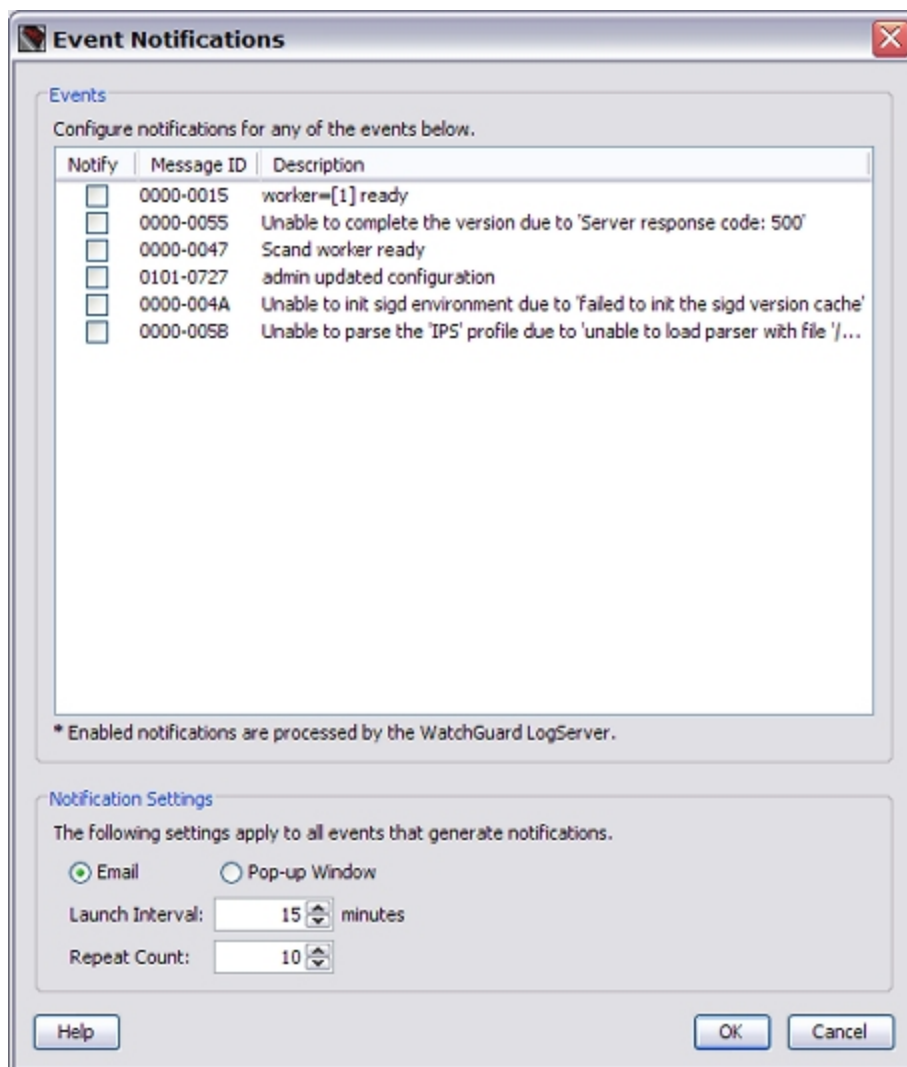
If you want to monitor specific events that occur at your XTM device, you can enable notification for log messages you specify in the Traffic Log. Subsequent log messages with the same message identifier (Message ID) trigger a notification.

Message IDs only appear in the **Event Notifications** dialog box for events that you have already configured for notification, or for events that have actually occurred at the XTM device. The actual event log message from the XTM device is shown in the **Description** column.

From Firebox System Manager:

1. Select the **Traffic Monitor** tab.
2. Right-click any message and select **Event Notifications**.

*The Event Notifications dialog box appears with the Message ID and a description for all available events.*



3. To sort by a column, click the column heading.
4. To receive a notification for a message, select the **Notify** check box for that message.
5. Select the **Notification Settings**.

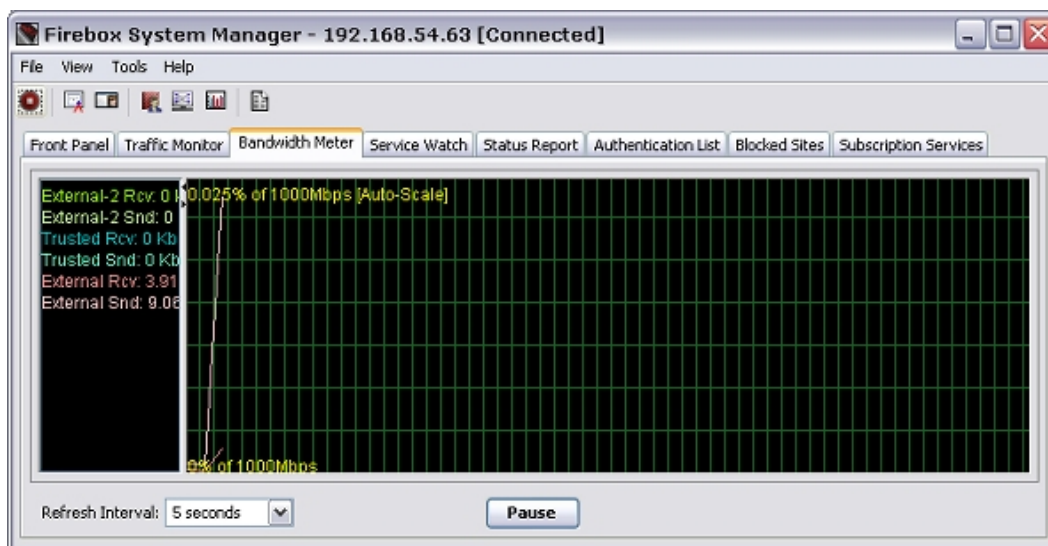
The **Notification Settings** at the bottom of the dialog box apply to all event notifications.

For information about notification options, see *Set Logging and Notification Preferences* on page 723.

6. Click **OK** to save your settings.  
*The Configure Event Notifications dialog box appears with a request for your Configuration passphrase.*
7. Type the **Configuration passphrase** for your XTM device and click **OK**.  
*A message that your configuration for event notifications has been updated appears.*

## Visual Display of Bandwidth Usage (Bandwidth Meter)

You can see the real-time bandwidth for all of the XTM device interfaces on the **Bandwidth Meter** tab. The Y axis (vertical) shows the traffic flow into and out of each interface, at the scale you select. The X axis (horizontal) shows the time. You can click any location on the chart to see more detailed information in a pop-up window about bandwidth use at that time. In addition to physical interfaces, the meter shows traffic on VLAN interfaces.

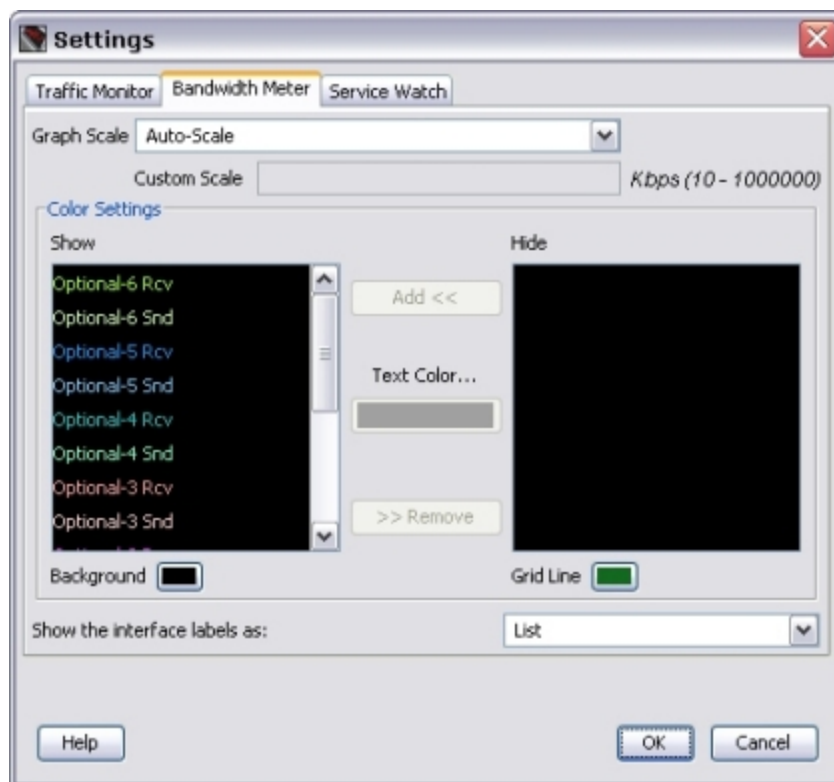


## Change Bandwidth Meter Settings

From Firebox System Manager, you can customize the appearance of the Bandwidth Meter. You can select color settings for text and grid lines, select how the interface labels appear, and set the scale for graphs.

To change the bandwidth display settings:

1. Select the **Bandwidth Meter** tab.
2. Select **File > Settings**.  
Or, right-click anywhere on the display and select **Settings**.  
*The Settings dialog box appears.*



3. From the **Bandwidth Meter** tab, you can customize the display settings with the options in the subsequent sections.
4. When you are finished, click **OK** to save your changes and return to FSM.

## Change the Scale

You can use the **Settings** dialog box to change the scale for the display graphs, or you can right-click anywhere on the Bandwidth Meter tab and select **Graph Scale** to set the scale.

To change the scale of the **Bandwidth Meter** tab:

From the **Graph Scale** drop-down list, select the value that is the best match for the speed of your network.

To set a custom scale.

1. From the **Graph Scale** drop-down list, select **Custom Scale**.
2. In the **Custom Scale** text box, type the value in kilobytes for each second.

## Add and Remove Lines

To add a line to the **Bandwidth Meter** tab:

1. In the **Color Settings** section, select the interface from the **Hide** list.
2. Click the **Text Color** color control box to select a color for the line.
3. Click **Add**.

*The interface name appears in the Show list in the color you selected.*

To remove a line from the **Bandwidth Meter** tab:

1. In the **Color Settings** section, select the interface from the **Show** list.
2. Click **Remove**.

*The interface name appears in the Hide list.*

## Change Colors

To change the display colors for the **Bandwidth Meter** tab:

1. Click the **Background** and **Grid Line** color control boxes to select new colors.  
*The Select Background Color or Select Grid Line color dialog box appears.*
2. Click the **Swatches**, **HSB**, or **RGB** tab and choose a color.  
*An example of the selected color appears in the Preview section.*
3. Click **OK** to confirm your selection and return to the **Settings** dialog box.

## Change Interface Appearance

Interface names appear on the left side of the **Bandwidth Meter** tab. You can view interface names as a list or as a name tag adjacent to the line it identifies.

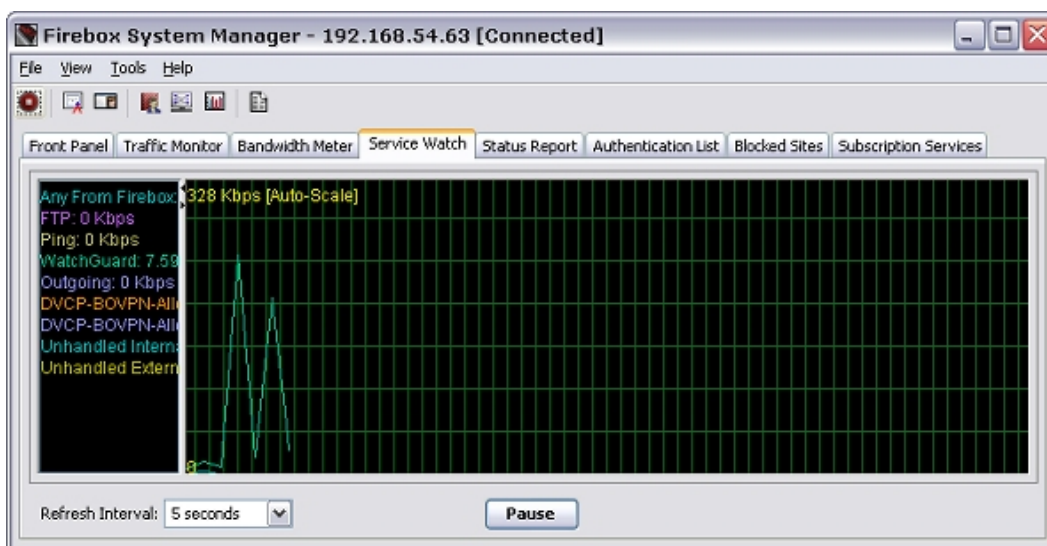
To select the appearance of the interface name:

Click the **Show the interface labels as** drop-down list and select **List** or **Tags**.

To see bandwidth use by policy instead of interface, see *Visual Display of Policy Usage (Service Watch)* on page 764.

## Visual Display of Policy Usage (Service Watch)

You can use Firebox System Manager to see a graph of the policies that are configured in Policy Manager for an XTM device. On the **Service Watch** tab, the Y axis (vertical) shows the number of connections, and the X axis (horizontal) shows the time. You can click any location on the chart to see more detailed information in a pop-up window about policy use at that point in time. You can also configure the appearance of the **Service Watch** tab.



## Change Service Watch Settings

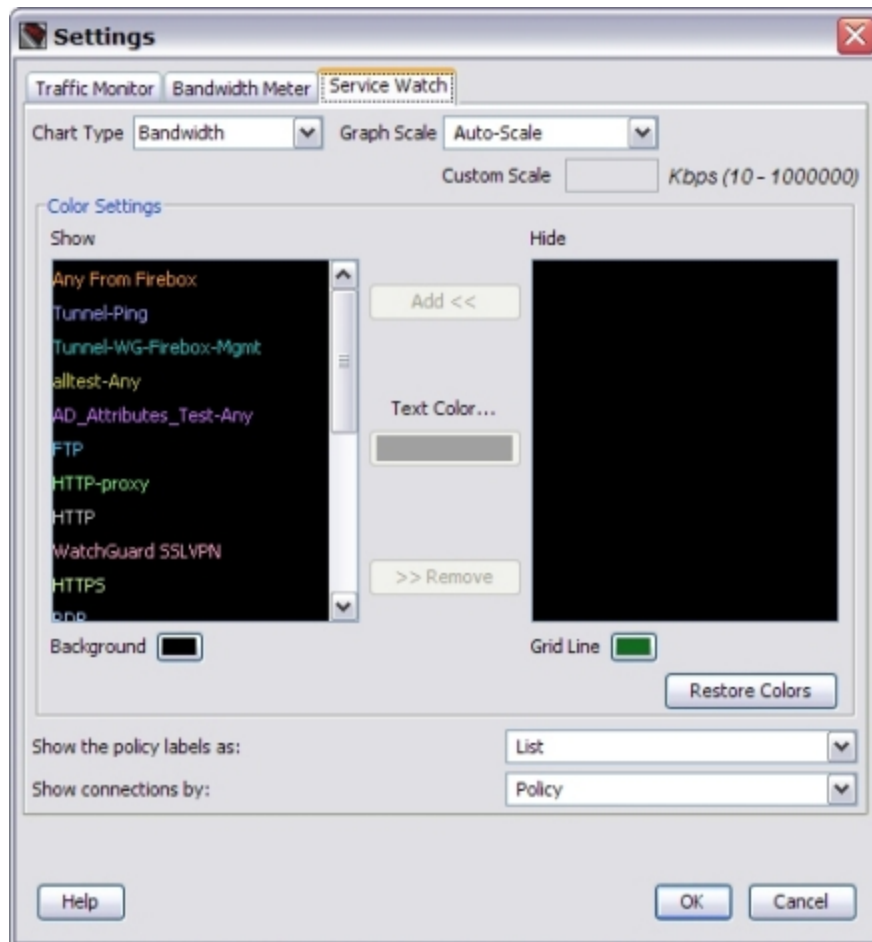
From Firebox System Manager, you can customize the appearance of Service Watch. You can select color settings for text and grid lines, select how the policy labels appear, and set the type and scale for charts.

To change the policy display settings:

1. Select the **Service Watch** tab.
2. Select **File > Settings**.

Or, right-click anywhere on the display and select **Settings**.

*The Settings dialog box appears.*



3. From the **Service Watch** tab, you can customize the Service Watch display settings with the options in the subsequent sections.
4. When you are finished, click **OK** to save your changes and return to FSM.

## Change the Scale

To change the scale of the **Service Watch** tab:

From the **Graph Scale** drop-down list, select the value that is the best match for the volume of traffic on your network.

To set a custom scale.

1. From the **Graph Scale** drop-down list, select **Custom Scale**.
2. In the **Custom Scale** text box, type the number of connections.

## Display Bandwidth Used by a Policy

To see the amount of network capacity in bytes per second used by a policy instead of the number of connections:

From the **Chart Type** drop-down list, select **Bandwidth**.

To see bandwidth use by interface instead of policy, see *Visual Display of Bandwidth Usage (Bandwidth Meter)* on page 762.

## Add and Remove Lines

To add a line to the **Service Watch** tab:

1. In the **Color Settings** section, select the policy from the **Hide** list.
2. Click the **Text Color** color control box to select a color for the line.
3. Click **Add**.

*The policy name appears in the Show list in the color you selected.*

To remove a line from the **Service Watch** tab:

1. In the **Color Settings** section, select the policy from the **Show** list.
2. Click **Remove**.

*The policy name appears in the Hide list.*

## Change Colors

To change the display colors for the **Service Watch** tab:

1. Click the **Background** and **Grid Line** color control boxes to select new colors.  
*The Select Background Color or Select Grid Line color dialog box appears.*
2. Click the **Swatches**, **HSB**, or **RGB** tab and choose a color.  
*An example of the selected color appears in the Preview section.*
3. Click **OK** to confirm your selection and return to the **Settings** dialog box.

## Change How Policy Names Appear

Policy names appear on the left side of the **Service Watch** tab. You can view policy names as a list or as a name tag adjacent to the line it identifies.

To set the appearance of the policy names:

Click the **Show the policy labels as** drop-down list to select **List** or **Tags**.

## Traffic and Performance Statistics (Status Report)


The **Status Report** tab shows statistics about XTM device traffic and performance.

Firebox System Manager - 192.168.54.58 [Connected]

File View Tools Help

Front Panel Traffic Monitor Bandwidth Meter Service Watch **Status Report** Authentication List Blocked Sites Subscription Services

Status report for 'XTM810\_London' from Sun Nov 21 18:28:46 2010

Version : 11.4.B299801  
 Serial #:   
 Model : XTM810

Current local time: Sun Nov 21 18:28:46 2010  
 Current UTC time : Mon Nov 22 02:28:46 2010  
 Uptime : 2d 0h 26m 16s

Firebox Modular Components

Module	Version	Build Number
xtables-addons	11.4	299801
wgversion	11.4	299801
wgplatform	11.4	299801
wgcore	11.4	299801
webui	11.4	299801
vpn-data	11.4	299801
vpn	11.4	299801
rootfs	11.4	299801

Refresh Interval: 30 seconds (Refreshing...)

Pause Support...

To see the Status Report:

1. Start *Firebox System Manager*.
2. Select the **Status Report** tab.

The Status Report includes this information:

*Uptime and version information*

XTM device uptime, the XTM device system software version, the XTM device model, appliance software version, and patch, if applicable. There is also a list of the status and version of the product components on the XTM device.

*Log Servers*

IP addresses of all configured Log Servers.

*Logging options*

Log message options that are configured with the Quick Setup Wizard or Policy Manager.

*Memory and load average*

Statistics on the memory use (shown in bytes of memory) and load average of the XTM device. The load average has three values that typically show an average over the last minute, 5 minutes, and 15 minutes. Values over 1.00 (100%) indicate some threads are queued until resources are available. (A system load that exceeds 1.00 does not mean the system is overloaded.)

*Processes*

Process ID, the name of the process, and the status of the process.

*Network configuration*

Information about the network cards in the XTM device: the interface name, its hardware and software addresses, and its netmask. The display also includes local routing information, IP aliases, and reserved DHCP leases.

*Blocked Sites list, Blocked Sites exceptions*

Current manually blocked sites and any current exceptions. Temporarily blocked site entries appear on the permanent **Blocked Sites** tab.

*Interfaces*

Each XTM device interface; includes information about the interface type configuration (external, trusted, or optional), interface status, and packet count.

*Routes*

XTM device kernel routing table. You use these routes to find which device interface is used for each destination address. ECMP groups and dynamic routes that have been accepted by the dynamic routing daemon also appear here.

*ARP table*

ARP table on the XTM device. The ARP table is used to match IP addresses to hardware addresses. (When an appliance is in drop-in mode, use the contents of the ARP table only to troubleshoot connectivity over secondary networks on the interfaces.)

*Total Dynamic Network Address Translation (DNAT) entries*

Number of used and available entries.



### *Multi-WAN status*

Information on gateways and sticky connections. Also includes the sticky connections table.

### *DHCP client leases*

Information on DHCP client leases on the XTM device. The DHCP lease time is the UTC time listed at the start of the report.

### *Dynamic Routing*

Dynamic routing components in use on the XTM device, if any.

### *DNS Servers*

Address information for DNS servers.

### *Refresh interval*

The rate at which information is updated on this display.

### *Support*

If you are troubleshooting issues with the help of your support representative, you can click **Support** to create a file to help resolve the issues.

## Change the Refresh Interval

The content of the Status Report updates automatically according to the refresh interval.

To change the refresh interval:

1. From the **Refresh Interval** drop-down list, select a different interval.
2. To stop the automatic refresh of the display, click **Pause**.  
*While the display is paused, it does not refresh at the selected interval.*
3. To start the automatic display refresh again, click **Continue**.  
*The display is refreshed immediately and then at to the selected refresh interval.*

## Review Packet Trace Information for Troubleshooting

To see the packet trace information the XTM device collects:

1. Start *Firebox System Manager* and select the **Status Report** tab.
2. Click **Support**.  
*The Support Logs dialog box appears. Firebox System Manager gets the packet trace information from the XTM device.*
3. Click **Browse** to select the location to save diagnostic log files.  
*Support log files are saved in tarzipped (\*.tgz) format.*
4. Click **Retrieve**.  
*The Support Log is saved to the specified location.*
5. Review the details of the packet trace in the support log file.
6. Disable diagnostic logging when you have finished.

## Save the Status Report

You can select parts of the text in the Status Report and copy it to another file, or you can select to save the entire report to a text file.

To save selected parts of the report:

1. Use your cursor to highlight the text.  
Or, right-click the report and select **Select All**.
2. Right-click the highlighted text and click **Copy**.
3. Paste the text you copied in another file.

To save the entire report:

1. Right-click the report and select **Save Status Report to File**.  
*The Save As dialog box appears.*
2. Specify a descriptive name for the report to help you identify it.
3. Select a location where you can locate the report for later use.
4. Click **Save**.

## Authenticated Users (Authentication List)

The Firebox System Manager **Authentication List** tab shows information about all the users that are authenticated to the XTM device. You can sort the information in the Authentication List by any of the columns. You can also end a user authentication session.

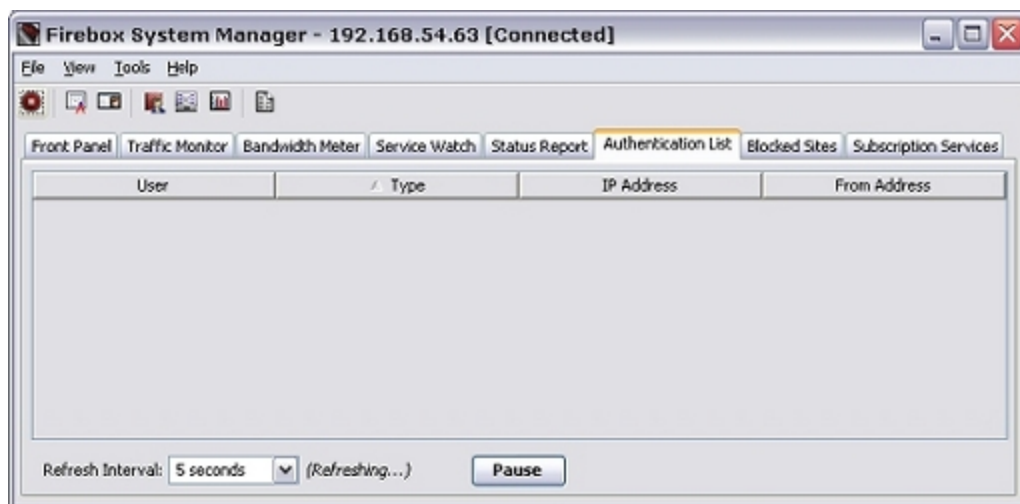
From the **Authentication List** tab, you can also see information about the Outbound Access List for Firebox X Edge devices, and see information about your wireless hotspot connections.

For more information about the Outbound Access List, see [Use the Outbound Access List](#).

For more information about your wireless hotspot connections, see [Wireless Hotspot Connections](#).

To see the Authentication List:

1. *Start Firebox System Manager.*
2. Select the **Authentication List** tab.



Information about each authenticated user appears in these four columns:

*User*

The name of the authenticated user.

*Type*

The type of user who authenticated: Firewall or Mobile User.

*IP Address*

The internal IP address being used by the user. For mobile users, this IP address is the IP address assigned to them by the XTM device.

*From Address*

The IP address on the computer the user authenticates from. For mobile users, this IP address is the IP address on the computer they used to connect to the XTM device. For Firewall users, the IP Address and From Address are the same.

To sort the Authentication List:

Click a column header.

To end a user session:

Right-click the user name and select **Log Off User**.

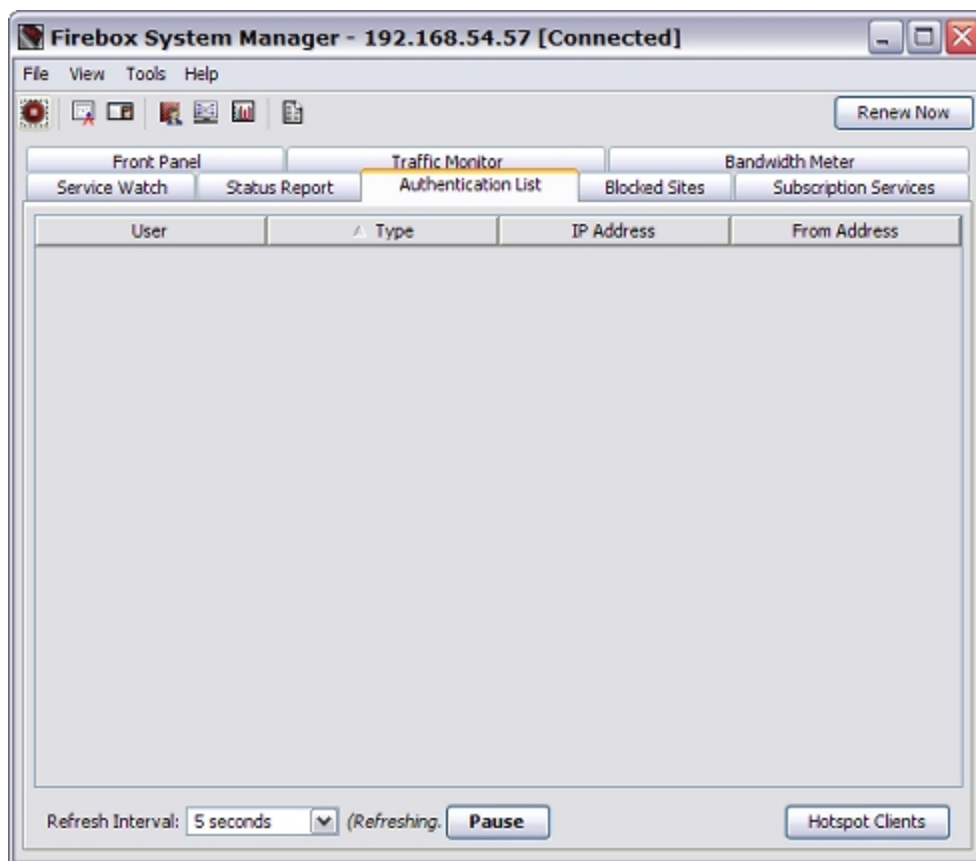
## Wireless Hotspot Connections

When you enable the wireless hotspot feature for your WatchGuard XTM wireless device, you can see information about the number of wireless clients that are connected. You can also disconnect wireless clients.

For more information about how to enable the wireless hotspot feature, see *Enable a Wireless Hotspot*.

To see the wireless hotspot connections:

1. Start *Firebox System Manager* for your wireless device.  
*Firebox System Manager* appears.
2. Select the **Authentication List** tab.



3. Click **Hotspot Clients**.

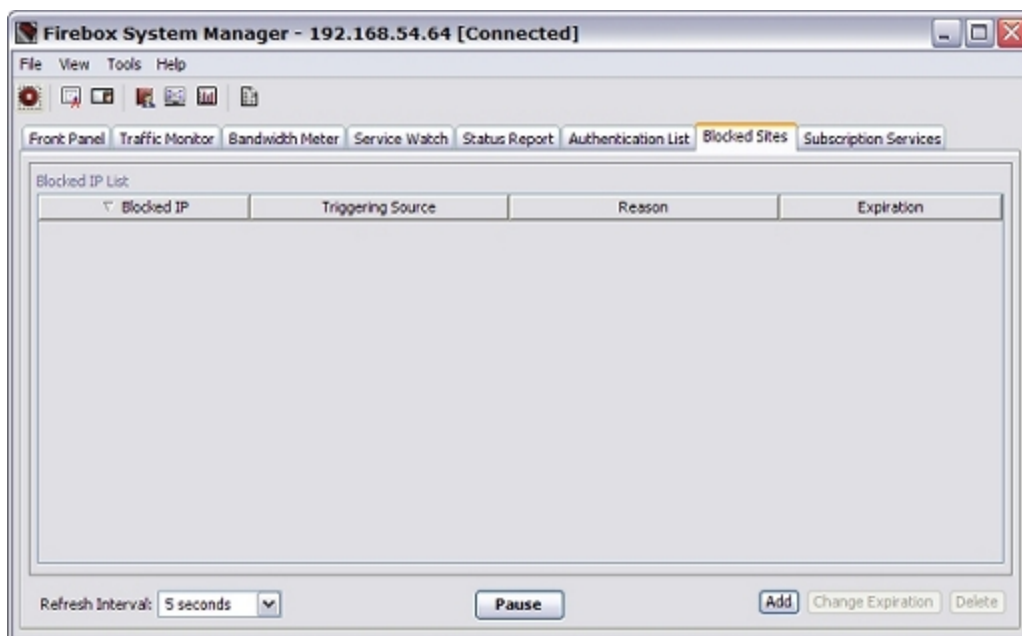
*For each connected wireless client, the IP address and MAC address appear.*

For more information about how to manage wireless hotspot connections, see *See Wireless Hotspot Connections*.

## Manage the Blocked Sites List (Blocked Sites)

The Firebox System Manager (FSM) **Blocked Sites List** tab shows the IP addresses of all the external IP addresses that are temporarily blocked. Many events can cause the XTM device to add an IP address to the **Blocked Sites** tab: a port space probe, a spoofing attack, an address space probe, or an event you configure.

The **Expiration** column for each IP address shows the time when the address is scheduled to be removed from the **Blocked Sites** tab.



You can adjust the default length of time that an IP address stays on the list in the Policy Manager **Blocked Sites** dialog box. For more information, see *Block Sites Temporarily with Policy Settings* on page 538.

## Change the Block Sites List

On the Firebox System Manager **Blocked Sites** tab, you can temporarily change the settings for specific IP addresses on the **Blocked IP List**. You can add a site to the list, change the expiration for a site on the list, or remove a site from the list.

To temporarily add a site to the **Blocked IP List**:

1. Click **Add**.

*The Add Temporary Blocked Site dialog box appears.*



2. Type the IP Address to block.
  3. Type a value in the **Expire After** field and select **Hours**, **Minutes**, or **Seconds** from the drop-down list to set the length of time the address is blocked.
  4. Click **OK**.
- The Add Blocked Site dialog box appears.*
5. Type the configuration passphrase for your XTM device, and click **OK**.

*The IP address appears in the Blocked IP List.*

To change the time that a site is deleted from the **Blocked IP List**:

1. Select a site in the **Blocked IP List** and click **Change Expiration**.

*The Edit Temporary Blocked Site dialog box appears for the selected IP Address.*



2. Verify the **IP Address** value is correct.
3. In the **Expire After** text box, type the new expiration value. From the drop-down list, select **Hours**, **Minutes**, or **Seconds**.
4. Click **OK**.  
*The Update Site dialog box appears.*
5. Type the configuration passphrase for your XTM device, and click **OK**.

To remove a site from the **Blocked IP List**:

1. Select a site from the **Blocked IP List** and click **Delete**.

*The Delete Site(s) dialog box appears.*

2. Type the configuration passphrase for your XTM device, and click **OK**.

*The IP address is removed from the Blocked IP List.*

**Note** You must open the XTM device with the configuration passphrase to remove a site from the list.

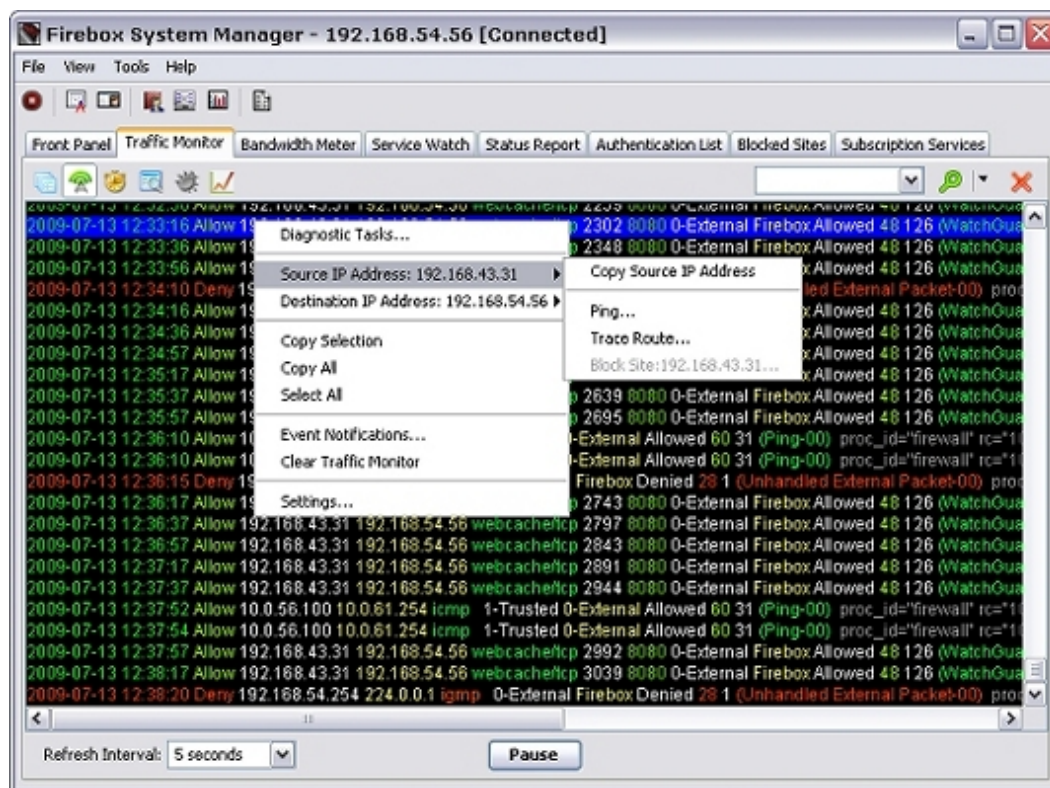
## Blocked Sites and Traffic Monitor

When an IP address is on the Blocked Sites list, a traffic log message that involves this address shows the destination interface as *unknown*. From Firebox System Manager (FSM), you can see the destination interface and add the IP address to the temporarily blocked sites list.

To see the destination interface:

1. Select the **Traffic Monitor** tab.
2. Select a traffic log message.
3. Right-click the message and select **Destination IP Address**.

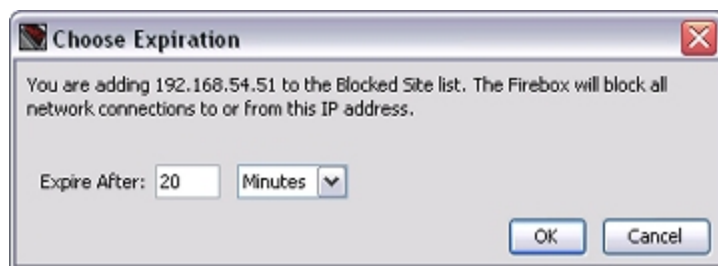
*The Destination IP address and a menu of options appear.*



To save computation cycles, Firewall XTM does not identify the destination interface of a packet if the source or destination IP address is blocked.

To block the destination interface IP address:

1. Select the **Traffic Monitor** tab.
2. Select a message.
3. Right-click the message and select **Destination IP Address**.  
*The Destination IP address and a menu of options appear.*
4. Select **Block Site**.  
*The Choose Expiration dialog box appears.*



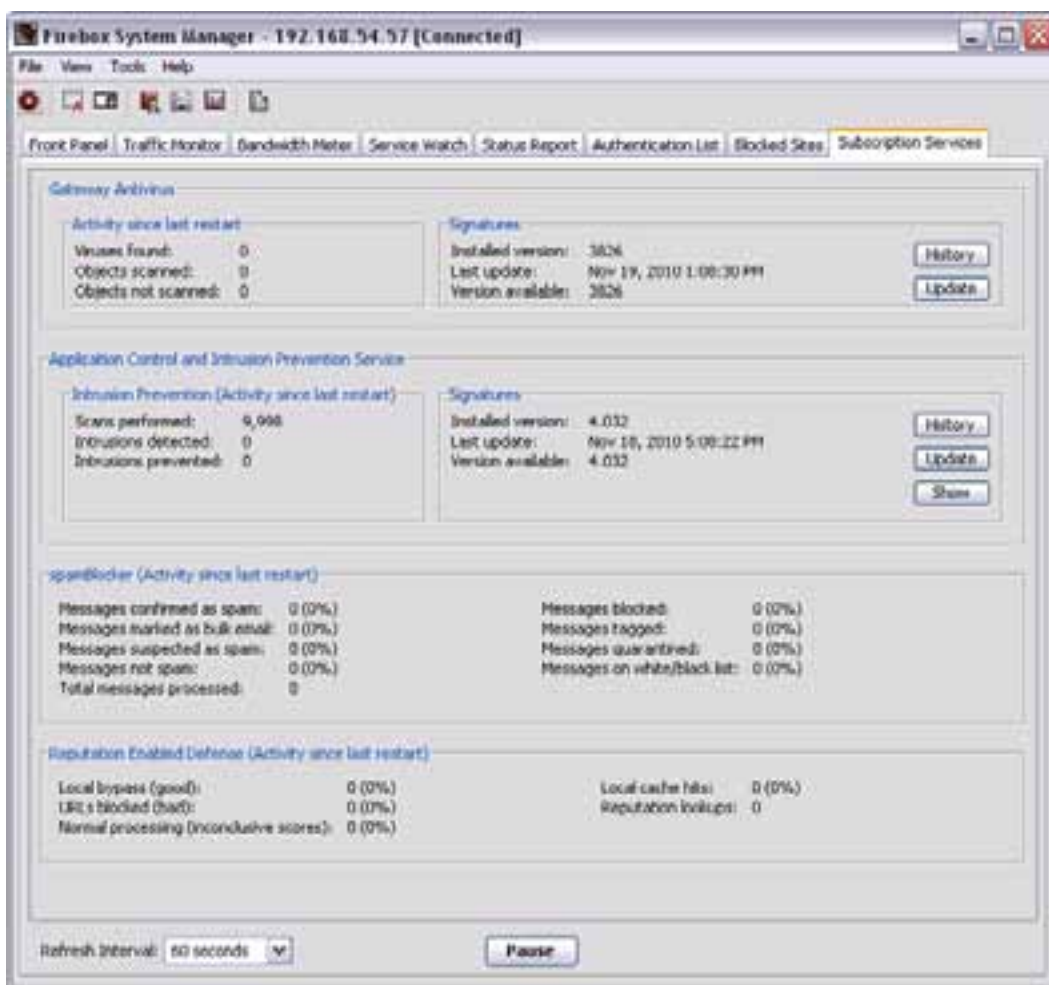
5. To change the amount of time the IP address is blocked, in the **Expire After** text box, type a value. From the drop-down list, select **Hours**, **Minutes**, or **Seconds**.
6. Click **OK**.  
*The Update signature dialog box appears.*
7. Type your configuration passphrase and click **OK**.  
*The IP address is temporarily added to the Blocked Sites list for the specified amount of time.*

# Subscription Services Statistics (Subscription Services)

The Firebox System Manager **Subscription Services** tab includes current XTM device statistics about these subscription services, if installed:

- Gateway AntiVirus Statistics
- Application Control and Intrusion Prevention Service Statistics
- spamBlocker Statistics
- Reputation Enabled Defense Statistics

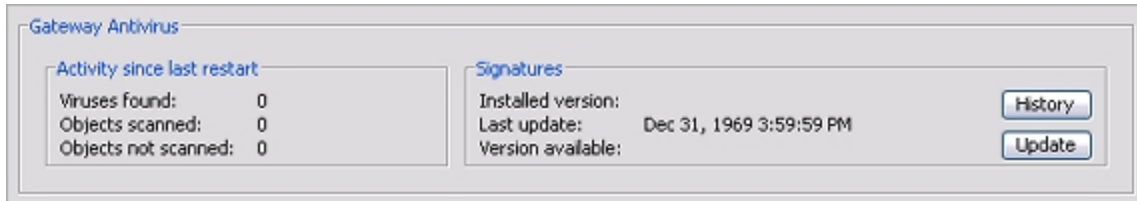
You can also use this page to update the signatures for Gateway AntiVirus and the signatures for Intrusion Prevention Service, as described in *Subscription Services Status and Manual Signatures Updates* on page 780.





## Gateway AntiVirus Statistics

The Firebox System Manager **Subscription Services** tab includes current statistics about the Gateway AntiVirus feature.



### *Activity since last restart*

**Viruses found** — Number of viruses found in scanned files since the last Firebox restart.

**Objects scanned** — Number of files scanned for viruses since the last Firebox restart.

**Objects not scanned** — Number of files not scanned for viruses since the last Firebox restart.

### *Signatures*

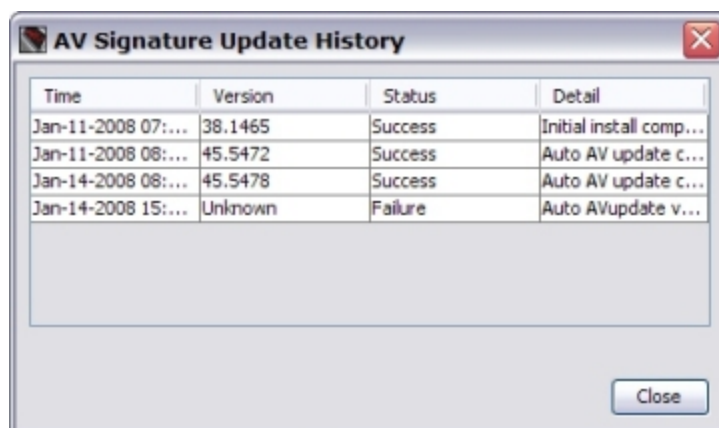
**Installed version** — Version number of the installed signatures.

**Last update** — Date of the last signature update.

**Version available** — The version of the signatures that is currently available.

**Server URL** — URL that the XTM device connects to for updates. Updates are also downloaded from this URL.

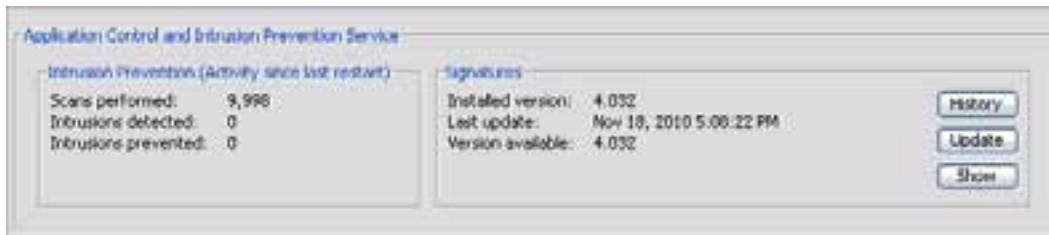
**History** — Click to show a list of all the signature updates. You can select a signature from the list and right-click it to copy information on the selected update, or the entire list of updates.



**Update** — Click to update your virus signatures.

## Application Control and Intrusion Prevention Service Statistics

The **Subscription Services** tab of Firebox System Manager includes current HTTP-proxy statistics about the Application Control and signature-based Intrusion Prevention Service features.



### *Activity since last restart*

**Scans performed** — Number of files scanned for viruses since the last HTTP-proxy restart.

**Intrusions detected** — Number of intrusions found in scanned files since the last HTTP-proxy restart.

**Intrusions prevented** — Number of infected files deleted since the last HTTP-proxy restart.

### *Signatures*

**Installed version** — Version number of the installed signatures.

**Last update** — Date of the last signature update.

**Version available** — If a new version of the signatures is available.

**History** — Click to show a list of all the signature updates. You can select a signature from the list and right-click it to copy information on the selected update, or the entire list of updates.

**Update** — Click to update your intrusion prevention signatures.

**Show** — Click to download and show a list of all current IPS signatures. After you download the signatures, you can look for signatures by signature ID.

## spamBlocker Statistics

The **Subscription Services** tab of Firebox System Manager includes current XTM device statistics about spamBlocker activity that occurred after the last device restart. The statistics include the number and the percentage position for each message type in these categories:

*Messages since last restart that are confirmed as:*

- bulk email
- spam
- suspected spam
- not spam

*Messages since last restart that are:*

- blocked
- tagged
- sent to the Quarantine Server

*Messages since last restart that are blocked or allowed because of a spamBlocker exceptions list that you created:*

- Black list — Exceptions that deny additional sites
- White list — Exceptions that allow additional sites

If you reboot the XTM device, all counters reset to zero.

## Reputation Enabled Defense Statistics

The **Subscription Services** tab of Firebox System Manager includes current XTM device statistics about Reputation Enabled Defense activity that occurred after the last device restart.

*Activity since last restart:*

**Local bypass (good)** — The number and percentage of URL requests that bypassed local Gateway AV scanning because they have a reputation score lower than the Good reputation threshold.

**The number of URLs blocked (bad)** — The number and percentage of URL requests that were blocked without scanning because they have a reputation score higher than the Bad reputation threshold.

**Normal processing (inconclusive scores)** — The number and percentage of URL requests that were processed normally, because they have a reputation score equal to or between the Good reputation and Bad reputation threshold.

**Local cache hits** — The number and percentage of URL requests for which the score was found in the local cache on the XTM device, so no request to the Reputation Enabled Defense server was required.

**Reputation lookups** — The total number of reputation lookup attempts since the last system restart.

**Note** *The total number of **Reputation lookups** can be higher than the combined total number of URLs with good, bad or inconclusive scores. This is because the **Reputation lookups** statistic counts all lookup attempts, whether or not a response was received in time to avoid a local AV scan. If The HTTP proxy does not receive a timely response to a reputation lookup request, it scans the content locally. When this happens, the lookup is added to the **Reputation lookup** total, but is not added to the total of good, bad, or inconclusive scores.*

For more information about the scores for Reputation Enabled Defense, see *About Reputation Enabled Defense*.

## Subscription Services Status and Manual Signatures Updates

The Gateway AntiVirus, Intrusion Prevention Service, and Application Control security services use a frequently-updated set of signatures to identify the latest viruses, threats, and applications. You can configure these services to update signatures automatically. For information about signature update settings see:

- *Configure the Gateway AV Update Server*
- *Configure the IPS Update Server*
- *Configure the Application Control Update Server*

You can also update signatures manually. If the signatures on the XTM device are not current, you are not protected from the latest viruses and intrusions.

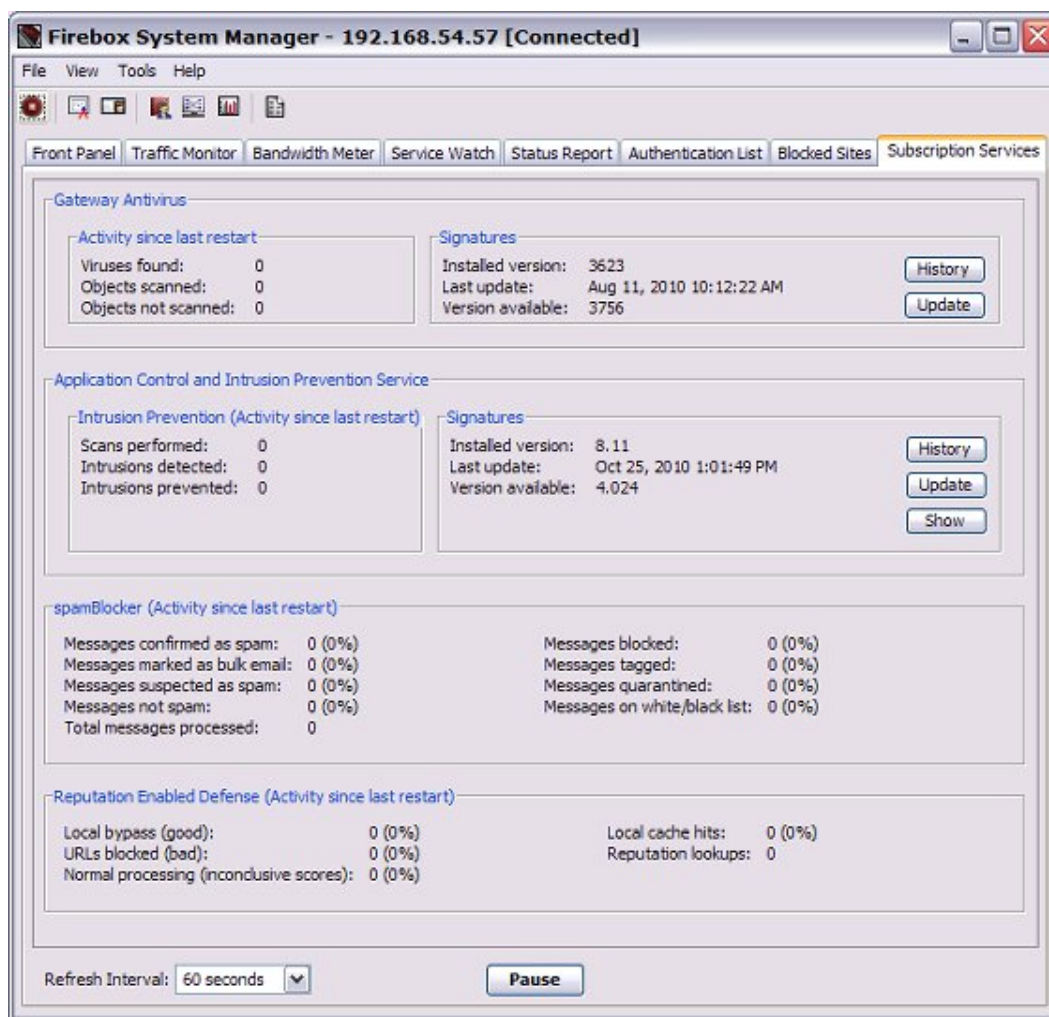
## See Service Status

The **Subscription Services** tab in Firebox System Manager shows you whether protection is active. For each signature-based service, you can see the current signature version installed, and whether a newer version of signatures is available. Feature keys for these features must be installed to see status information.

To see service status:

1. Start Firebox System Manager.
2. Select the **Subscription Services** tab.

*The status of the installed subscription services appears.*



## Update Signatures Manually

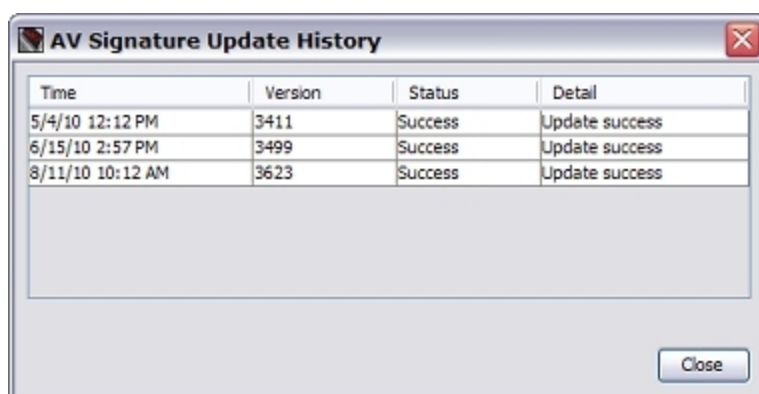
To manually update signatures for a service:

1. Select the **Subscription Services** tab.
2. Click **Update** for the service you want to update.  
*The Update Signature dialog box appears.*
3. Type your configuration passphrase. Click **OK**.  
*The XTM device downloads the most recent available signature update.*

## See the Signature Update History

You can see the history of updates that have been made to each subscription service.

1. Select the **Subscription Services** tab.
2. Adjacent to a subscription service, click **History**.  
*The Update History for the service you selected appears.*



## About HostWatch






HostWatch is a graphical user interface that shows the connections between different XTM device interfaces. HostWatch also gives information about users, connections, ports, and other information.

The top section of the HostWatch window has two sides. You can set the left side to show one interface you want to monitor. The right side shows the connections to and from the interface selected on the left side.

The lines that connect source hosts and destination hosts use colors that show the type of connection. You can change these colors. The default colors are:

- **Red** — The XTM device denies the connection.
- **Blue** — The connection uses a proxy.
- **Green** — The XTM device uses NAT for the connection.
- **Black** — Normal connection (the connection has been accepted, and it does not use a proxy or NAT).

To indicate the type of service, these icons appear adjacent to the server entries.

	Telnet		FTP
	HTTP		Other
	Email		


## DNS Resolution and HostWatch

Domain name server (DNS) resolution does not occur immediately when you start HostWatch. When HostWatch is configured for DNS resolution, it replaces the IP addresses with the host or user names. If the XTM device cannot identify the host or user name, the IP address stays in the HostWatch window.

If you use DNS resolution with HostWatch, the management computer can send a large number of NetBIOS packets (UDP 137) through the Firebox or XTM device. To stop this process, you must disable NetBIOS over TCP/IP in Windows.


## Start HostWatch

To start the HostWatch application:


1. Start *Firebox System Manager*.
2. Click .  
Or, select **Tools > HostWatch**.  
*The display is automatically started.*

## Pause and start the HostWatch display

To pause the HostWatch display:

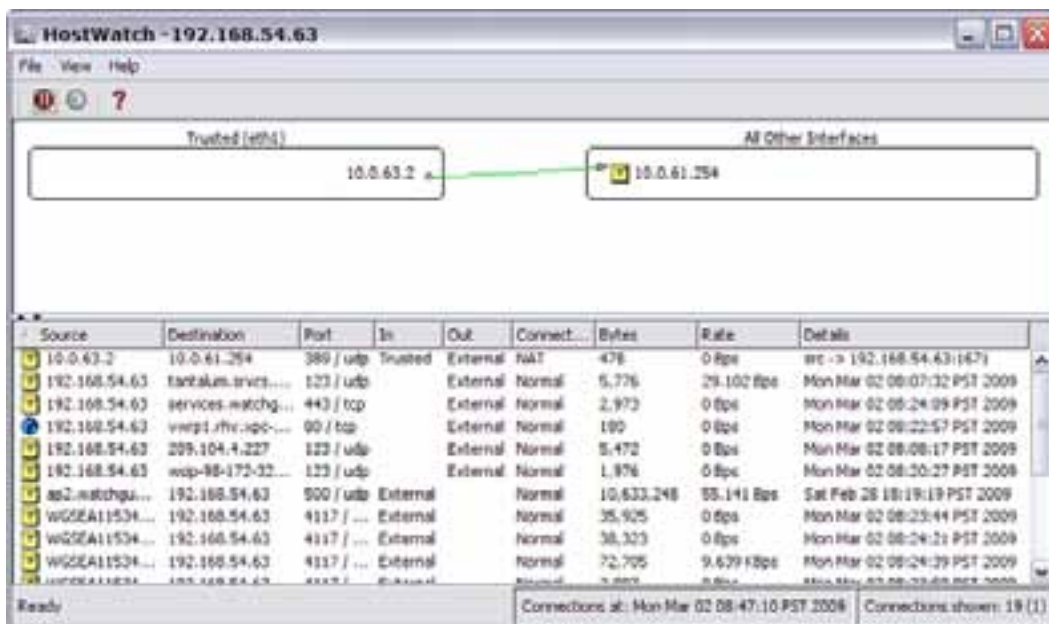
From the HostWatch window, click .  
Or, select **File > Pause**.

To start the HostWatch display:

From the HostWatch window, click .  
Or, select **File > Continue**.

## Select Connections and Interfaces to Monitor

When you first start HostWatch, you see XTM device internal interfaces in the list on the upper-left side of the window. Connections to and from those interfaces appear on the upper-right side of the window, in the **All Other Interfaces** list.



## See Connections

You can also use HostWatch to see information about the connections that involve a selected item, and includes the IP addresses, port number, time, connection type, and direction.

The bottom of the HostWatch window shows all connections to and from all interfaces. The information appears in a table that includes:

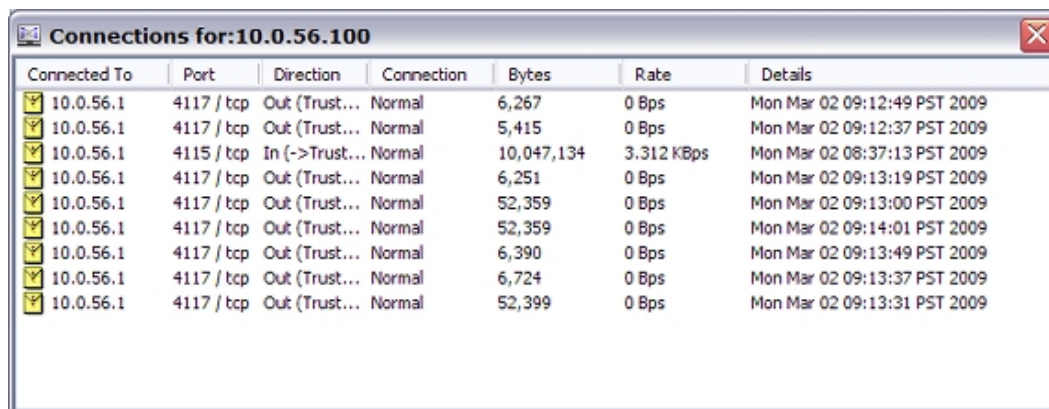
- Source and destination addresses
- Port
- XTM device interface used, and whether traffic was inbound or outbound
- Whether the connection was normal, proxied, or blocked
- Details, such as the time the connection was created or the command used to create the connection



To see connections for an interface:

Double-click an item in either the left or right list.

*The Connections For dialog box appears.*



Connected To	Port	Direction	Connection	Bytes	Rate	Details
10.0.56.1	4117 / tcp	Out (Trust...	Normal	6,267	0 Bps	Mon Mar 02 09:12:49 PST 2009
10.0.56.1	4117 / tcp	Out (Trust...	Normal	5,415	0 Bps	Mon Mar 02 09:12:37 PST 2009
10.0.56.1	4115 / tcp	In (->Trust...	Normal	10,047,134	3.312 KBps	Mon Mar 02 08:37:13 PST 2009
10.0.56.1	4117 / tcp	Out (Trust...	Normal	6,251	0 Bps	Mon Mar 02 09:13:19 PST 2009
10.0.56.1	4117 / tcp	Out (Trust...	Normal	52,359	0 Bps	Mon Mar 02 09:13:00 PST 2009
10.0.56.1	4117 / tcp	Out (Trust...	Normal	52,359	0 Bps	Mon Mar 02 09:14:01 PST 2009
10.0.56.1	4117 / tcp	Out (Trust...	Normal	6,390	0 Bps	Mon Mar 02 09:13:49 PST 2009
10.0.56.1	4117 / tcp	Out (Trust...	Normal	6,724	0 Bps	Mon Mar 02 09:13:37 PST 2009
10.0.56.1	4117 / tcp	Out (Trust...	Normal	52,399	0 Bps	Mon Mar 02 09:13:31 PST 2009

## Select a New Interface to Monitor

To select a new interface from HostWatch:

1. Select **View > Interface**.  
Or, right-click the current interface name.
2. Select the new interface you want to monitor.

To specify the exact interface name or use a regular expression to match multiple interfaces:

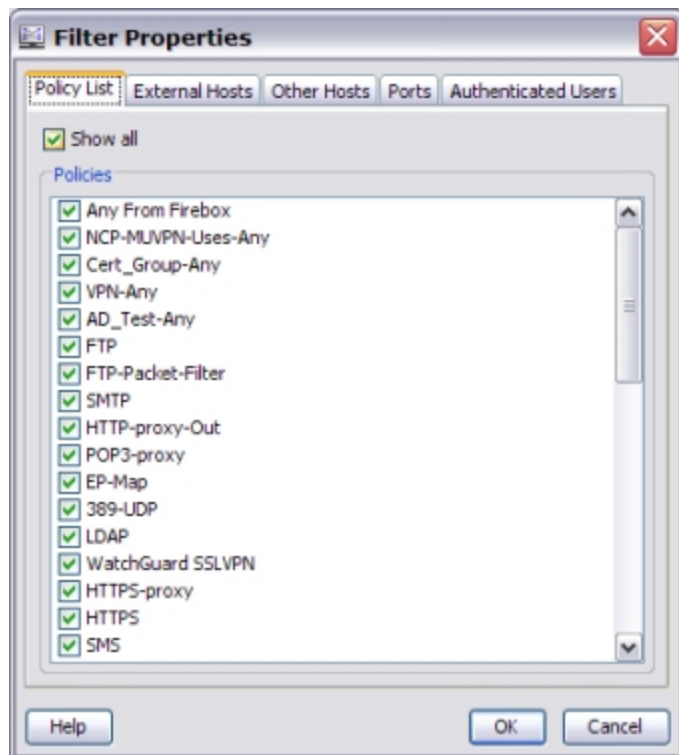
1. Select **View > Interface**.  
Or, right-click the current interface name.
2. Select **Other** from the interface list.  
*You can use this option to see VLANs in HostWatch.*

## Filter Content of the HostWatch Window

By default, HostWatch shows all policies, hosts, ports, and authenticated users. You can change the HostWatch window to show only the content that you specify. You can use this feature to monitor specified policies, hosts, ports, or users.

1. Select **View > Filter**.

*The Filter Properties dialog box appears. The second tab name changes to match the interface you selected to monitor.*



2. Select a tab to monitor.
3. On the tab for each item you want to see, in the **Hosts** or **Authenticated Users** text box, type the IP address, port number, or user name to monitor. Click **Add**.
4. To filter by policies, select the **Policy List** tab and select the check box for each policy you want to monitor.
5. To show all items in the category, select the **Show all** check box on each tab.
6. Click **OK**.

## Change HostWatch Visual Properties

You can change how HostWatch shows information. For example, you can configure HostWatch to show host names instead of addresses.

1. Select **View > Settings**.

*The Settings dialog box appears with the Display tab selected.*



2. Make any changes to the **Display** or **Refresh Interval** settings.
3. To change the line colors for the **NAT**, **Proxy**, **Blocked**, and **Normal** connections, select the **Line Color** tab.

*The Connection Type settings appear.*



4. Adjacent to the **Connection Type** you want to change, click the color button and select a new color.
5. Click **OK**.

## Visit or Block a Site from HostWatch

You can visit a site shown in HostWatch.

1. From the lower window pane, right-click the site and select **Visit Proxied Website**.
2. In the pop-up window that appears, type the address of the site.

You can also block an IP address and add it to the Blocked Sites list:

1. In the top pane, right-click an IP address and select **Block Site: [site address]**.  
Or, right-click a connection in the lower pane and select either **Block Site: [source address]** or **Block Site: [destination address]**.

*The Choose Expiration dialog box appears.*



2. In the **Expire After** text box, type the amount of time for the site to remain blocked. You can select **Hours**, **Minutes**, or **Seconds** from the drop-down list.
3. When prompted, type your configuration passphrase.


The XTM device blocks all network connections to or from this IP address.

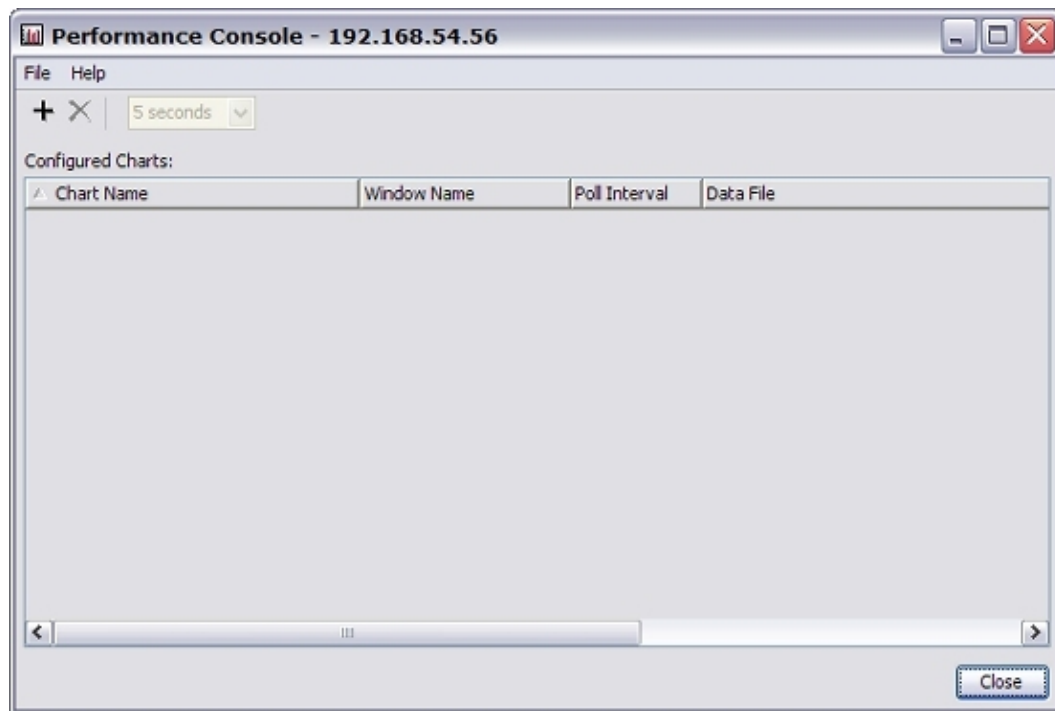
## About the Performance Console

The Performance Console is a utility program you can use to make graphs that show how different parts of the XTM device operate. To collect the information, you define counters that identify the information used to make the graph.

### Start the Performance Console

To start the Performance Console, from Firebox System Manager:

1. Click .  
Or, select **Tools > Performance Console**.  
*The Add Chart dialog box appears.*
2. To close the **Add Chart** dialog box and view the Performance Console, click **Cancel**.  
*The Performance Console dialog box appears.*



3. Or, add a chart and define performance counters.

For more information about the Performance Console and performance counters, see *Define Performance Counters* on page 791.

## Make Graphs with the Performance Console

To make graphs in the Performance Console:

1. *Define Performance Counters.*

For more information about the categories for counters, see the *Types of Counters* section.

2. Modify the chart or add a new one, as described in *Add Charts or Change Polling Intervals* on page 794.

## Types of Counters

You can monitor these types of performance counters:

### *System Information*

Shows how the CPU is used.

### *Interfaces*

Monitor and report on the events of selected interfaces. For example, you can set up a counter that monitors the number of packets a specified interface receives.

### *Policies*

Monitor and report on the events of selected policies. For example, you can set up a counter that monitors the number of packets that a specified policy examines.

### *VPN Peers*

Monitor and report on the events of selected VPN policies.

### *Tunnels*

Monitor and report on the events of selected VPN tunnels.

## Stop Monitoring or Close the Window

You can stop the monitor to save resources and restart it at different time.

1. Click **Stop Monitoring**.  
*The Performance Console no longer receives data for this counter.*
2. Click **Close** to close the chart window.

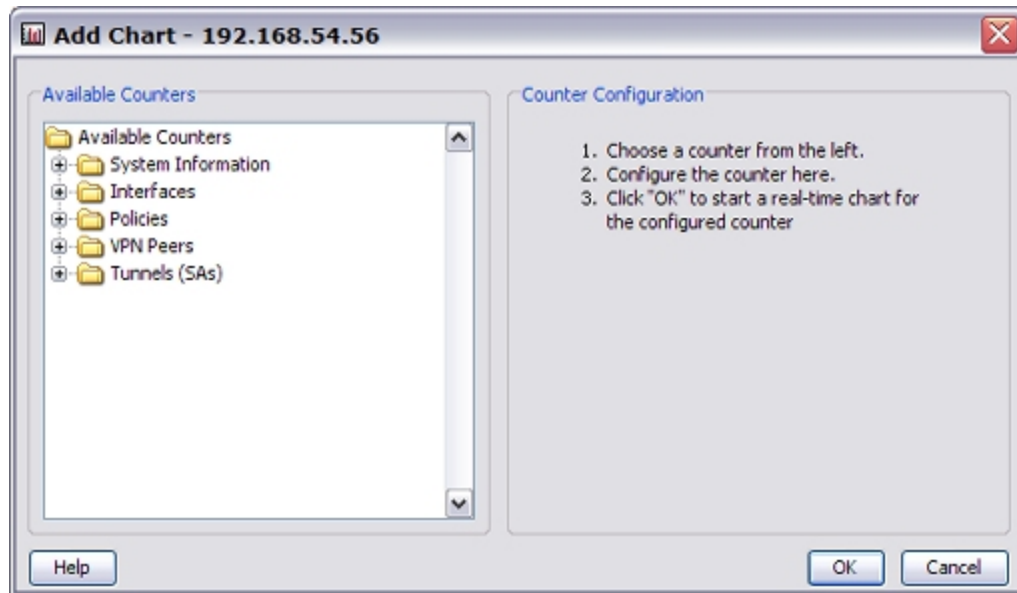
## Define Performance Counters

From Firebox System Manager, you can identify a counter for any of the categories in the Available Counters list.

1. Click .

Or, select **Tools > Performance Console**.

*The Add Chart window appears.*

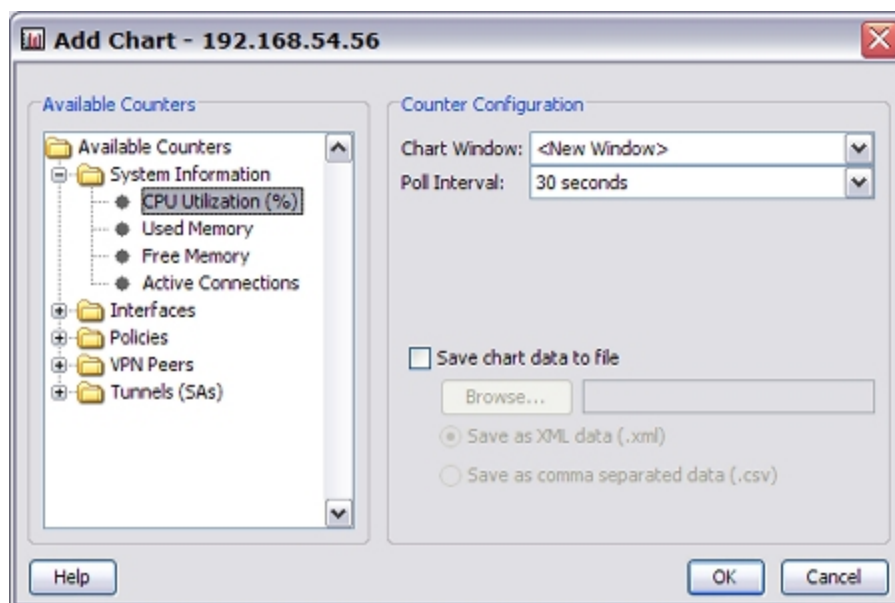


2. In the **Available Counters** list, expand a counter category.

*The available counters for that category appear.*

3. Select a counter. For example, **CPU Utilization**.

*The Counter Configuration fields automatically refresh to show fields for the selected counter.*



4. From the **Chart Window** drop-down list, select **<New Window>** if you want the graph to appear in a new window.  
Or, select the name of an open window to add the graph to that window.
5. From the **Poll Interval** drop-down list, select a time interval.  
This is the amount of time that the Performance Console waits before it checks for updated information from the XTM device.
6. Add configuration information for the counter you selected. The configuration fields correspond to the counter, and different counters have different fields. The available fields include:

#### *Type*

Select the type of graph to create in the drop-down list: **Rate**, **Difference**, or **Raw Value**.

For example, if you want to create a graph of value\_1 at time\_1, value\_2 at time\_2, and so on, by:

- **Rate** — Divide the value difference by the time difference:  $(\text{value\_2}-\text{value\_1})/(\text{time\_2}-\text{time\_1})$ ,  $(\text{value\_3}-\text{value\_2})/(\text{time\_3}-\text{time\_2})$ , and so on.
- **Difference** — Subtract the previous value from the new value: value\_2-value\_1, value\_3-value\_2, and so on.
- **Raw Value** — Use only the value: value\_1, value\_2, and so on. The raw values are generally counters of content such as bytes or packets. Raw values can only increase, not decrease.

#### *Interface*

Select an interface to include in the graph data from the drop-down list.

#### *Policy*

(If you select a Policy counter)

Select a policy from your XTM device configuration to include in the graph data. You can update the policy list that appears in the Performance Console when you click the **Refresh Policy List** button.

#### *Peer IP*

(If you select a VPN Peers counter)

Select the IP address of a VPN endpoint to include in the graph data. You can update the list of VPN endpoints that appears in the Performance Console when you click the **Refresh Peer IP List** button.

#### *Tunnel ID*

(If you select a Tunnels counter)

Select the name of a VPN tunnel to include in the graph data. You can update the list of VPN tunnels that appears in the Performance Console when you click the **Refresh Tunnel ID List** button. If you do not know the tunnel ID for your VPN tunnel, check the Firebox System Manager **Front Panel** tab.

7. To save the data collected by the Performance Console, select the **Save Chart Data to File** check box.

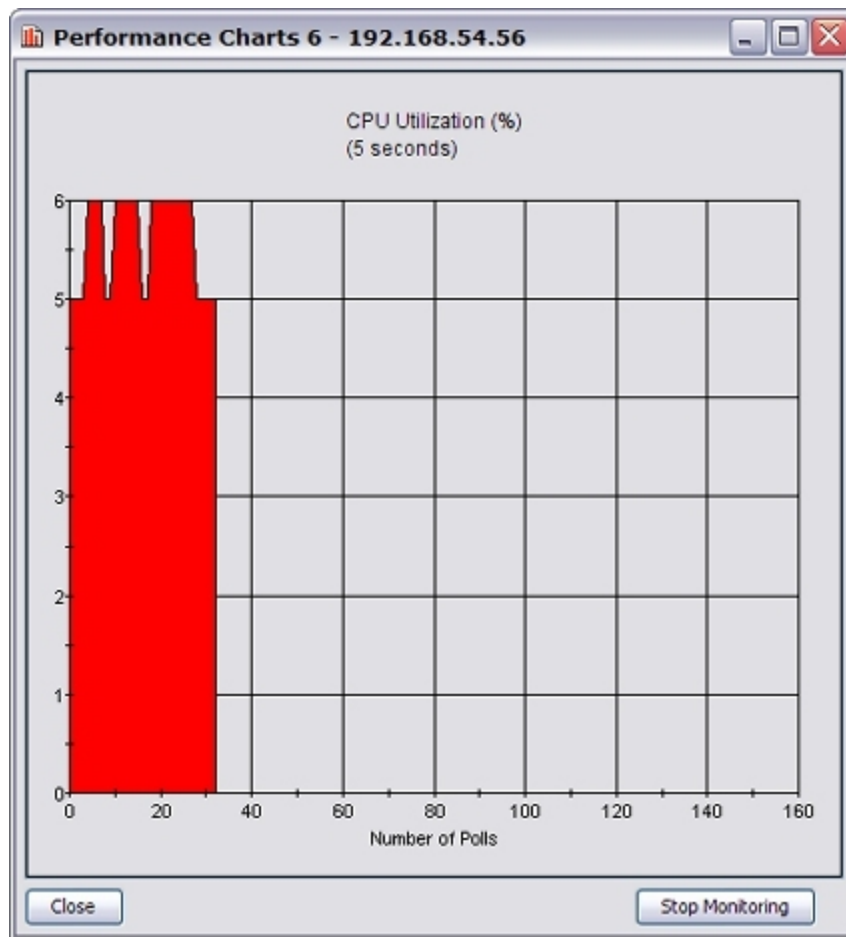


- Click **Browse** to select a location to save the file, and choose whether to save the file as an XML data file or a comma-separated data file.

For example, you can open an XML data file in Microsoft Excel to see the counter value recorded for each polling interval. You can use other tools to merge data from more than one chart

- Click **OK** to start a real-time graph of this counter.

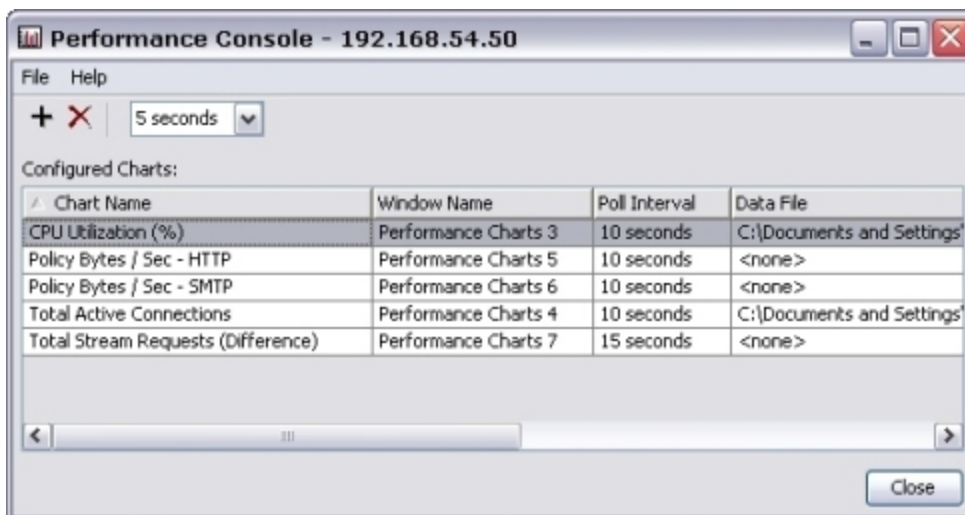
Graphs appear in a real-time chart window. You can show one graph in each window, or show many graphs in one window. Graphs automatically scale to fit the data and refresh every 5 seconds.



**Note** This performance graph shows CPU usage. You can use the same procedure to create graphs for other functions.

## Add Charts or Change Polling Intervals

The main Performance Console window shows a table with all configured and active performance counters. From this window, you can add a new chart or change the polling intervals for configured counters.



### Add a New Chart

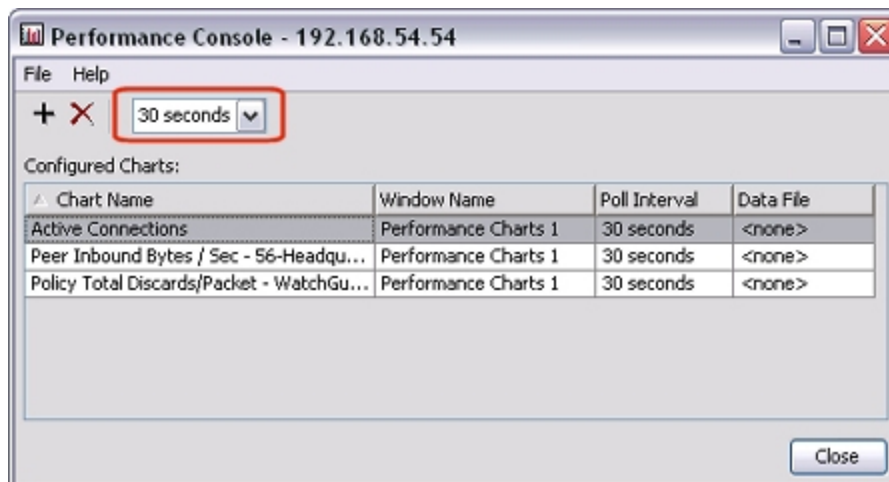
To add a new chart:

1. Click **+**.  
Or, select **File > Add Chart**.  
*The Add Chart dialog box appears.*
2. *Define Performance Counters* for the chart.

### Change the Polling Interval

To change the polling interval for one performance console:


1. From the **Configured Charts** list, select a chart name.



- From the polling interval drop-down list, select the new duration between polls.  
*The new frequency value appears in the Poll Interval column.*

## Delete a Chart

To delete a chart:


- From the **Configured Charts** list, select a chart name.
- Click .  
Or, select **File > Delete Chart**.  
*A confirmation dialog box appears.*
- Click **Yes** to delete the chart.

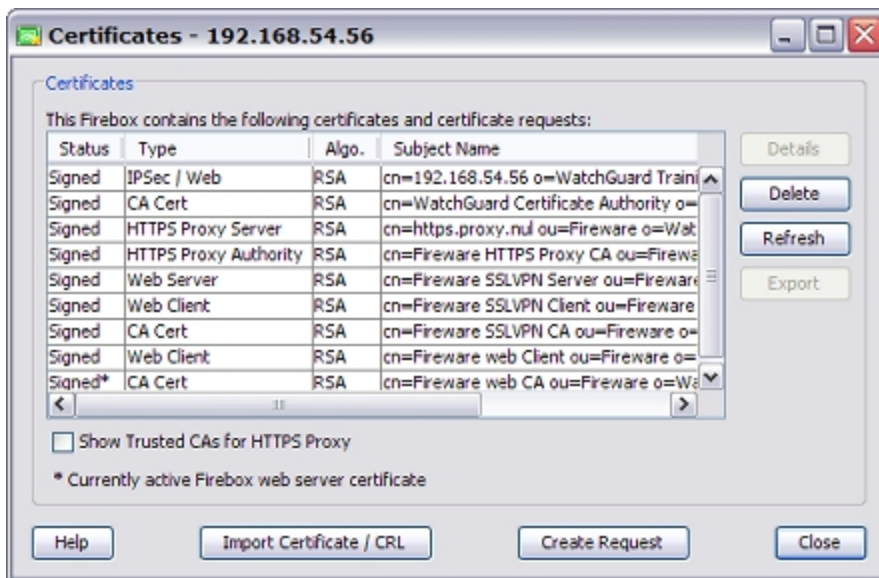
## About Certificates and FSM

Firebox System Manager (FSM) includes a **Certificates** dialog box from which you can do a variety of tasks related to your certificates. You can:

- See a list of the current XTM device certificates and details for each of them.
- Remove a certificate from the XTM device.
- Make a certificate request.
- Import a third-party CA certificate and store it in the certificate trust list.

To open the **Certificates** dialog box:

- Start *Firebox System Manager*.
- Click .  
Or, select **View > Certificates**.  
*The Certificates dialog box appears.*




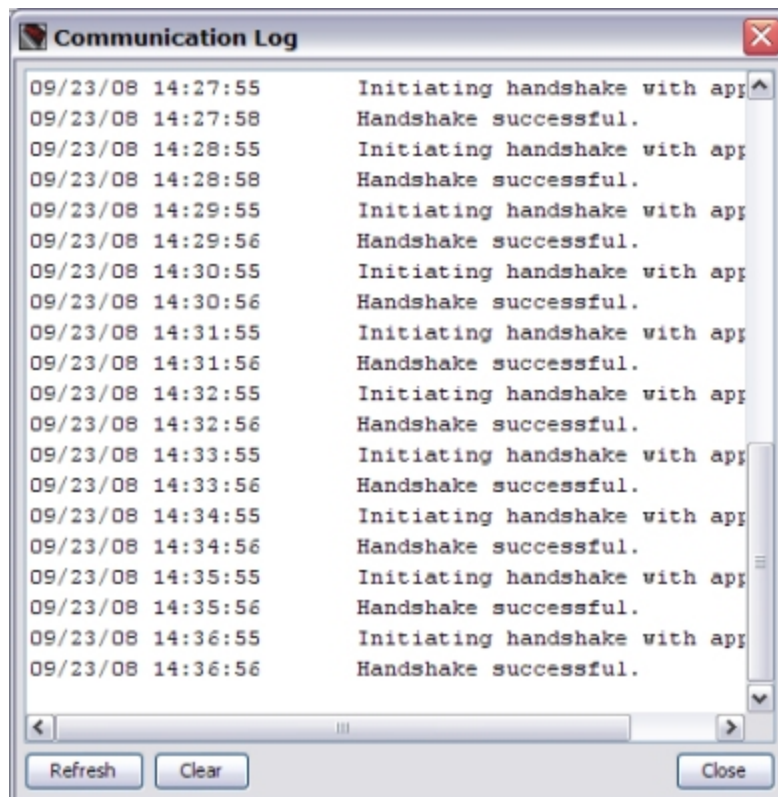
For more information about certificate tasks in FSM, see *Manage XTM Device Certificates* on page 862.

## Communication Log

The Communication Log dialog box contains information such as the success or failure of logins, handshakes, and so on. These are connections between the XTM device and Firebox System Manager.

To see the communication log:

1. Start *Firebox System Manager*.
  2. Click .
- Or, select **View > Communication Log**.  
*The Communication Log dialog box appears.*



The information in the log begins with when initial login is successful, and shows information about the current management session.

3. To reload the log information in the dialog box, click **Refresh**.
4. To delete all information from the Communication Log, click **Clear**.  
*All the information is deleted from the communication log and cannot be restored.*

## Use Firebox System Manager (FSM)

You can use Firebox System Manager tools to complete many tasks on your XTM device. These tasks include:

- *Synchronize the System Time*
- *Reboot or Shut Down Your XTM Device*
- *Clear the ARP Cache*
- *See and Synchronize Feature Keys*
- *Calculate the Fireware XTM Checksum*
- *Clear Alarms*
- *Rekey BOVPN Tunnels*
- *Control FireCluster*
- *Change Passphrases*

### Synchronize the System Time

From Firebox System Manager, you can synchronize the time on the XTM device with the system time on your management computer.

1. Select **Tools > Synchronize Time**.  
*The Synchronize Firebox Time dialog box appears.*



2. Type the device configuration passphrase.
3. Click **OK**.  
*A message that the device time is now synchronized with the management computer appears.*

### Reboot or Shut Down Your XTM Device

You can use Firebox System Manager (FSM) to reboot or shut down your XTM device from a remote location.

#### Reboot Your XTM device

1. *Connect to an XTM Device.*
2. *Start Firebox System Manager.*
3. Select **File > Reboot**.  
*A confirmation message appears.*
4. Click **Yes**.  
*The XTM device reboots.*

## Shut Down Your XTM device

When you shut down a device, the LCD indicator panel, the serial port, and all interfaces of the device are shut down. The power light changes to orange and the fans continue to run, but you cannot communicate with the device. After the device is shut down, you must manually restart the device to resume communication.

To shut down a device:

1. *Connect to an XTM Device.*
2. *Start Firebox System Manager.*
3. Select **File > Shutdown**.  
*A confirmation message appears.*
4. Click **Yes**.  
*The XTM device shuts down.*

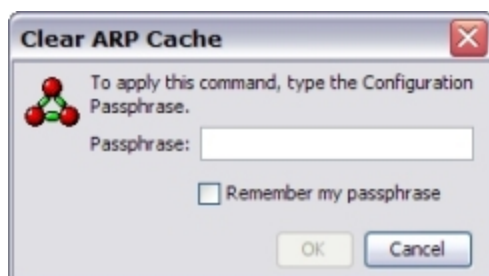
To restart your device after a shut down:

1. To power off the device, press the power button.
2. To power on the device, press the power button again.

## Clear the ARP Cache

The ARP (Address Resolution Protocol) cache on the XTM device keeps the hardware addresses (also known as MAC addresses) of TCP/IP hosts. Before an ARP request starts, the system checks if a hardware address is in the cache. You must clear the ARP cache on the XTM device after installation when your network has a drop-in configuration.

1. From Firebox System Manager, select **Tools > Clear ARP Cache**.



2. Type the device configuration passphrase.
3. Click **OK**.  
*All cache entries are flushed.*


When a XTM device is in drop-in mode, this procedure clears only the content of the ARP table and not the MAC address table. The oldest MAC entries in the MAC table are removed if the table has more than 2000 entries. To clear the MAC address table, you must restart the XTM device.

## See and Synchronize Feature Keys

You can see the feature keys that are installed on your XTM device from Firebox System Manager. You can also get a new feature key from LiveSecurity.

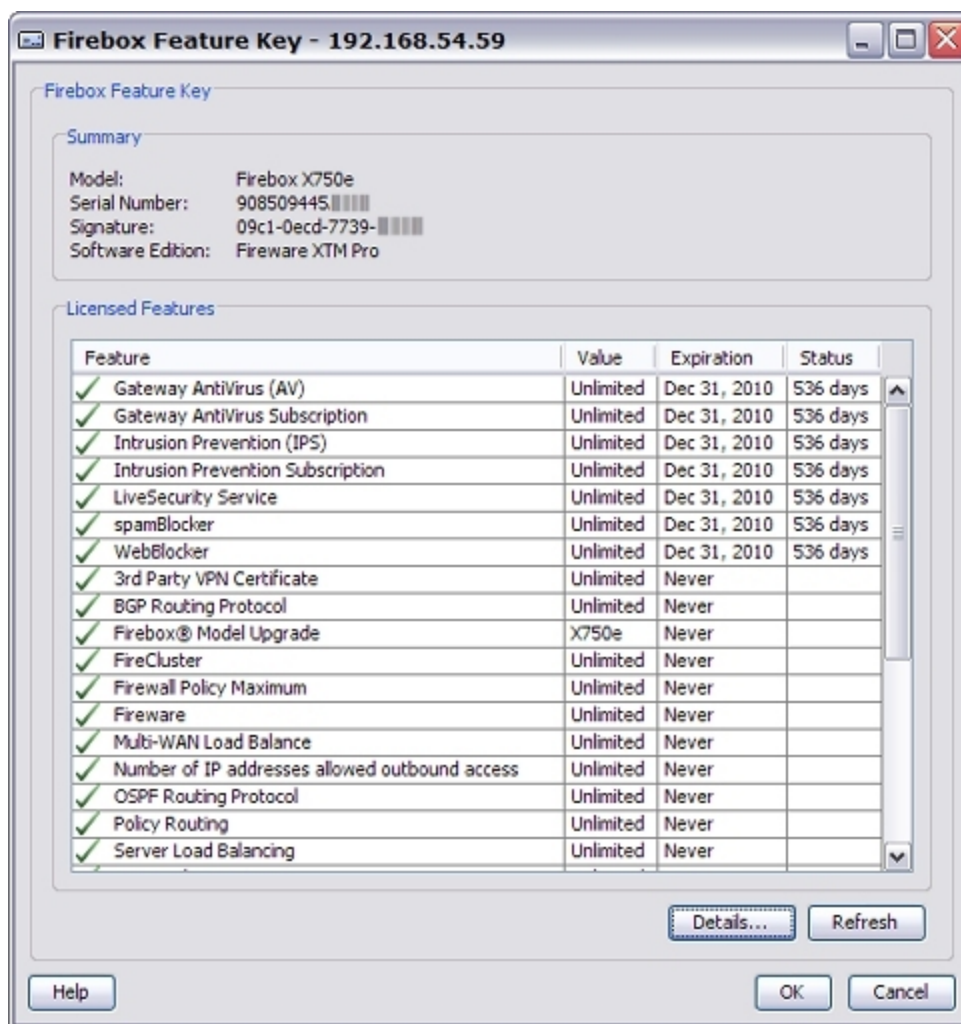
## See Feature Keys

To see your feature keys:

1. Start Firebox System Manager.
2. Click .

Or, select **View > Feature Keys**.

The Firebox Feature Key dialog box appears.



### Feature

The name of the feature, such as *spamBlocker Subscription*.

### Value

The value associate with the feature. For example, the number of VLAN interfaces or BOVPN tunnels allowed.

### Expiration

The expiration date of the feature. If the feature does not expire, **Never** appears in this field.



### Status

For features with expiration dates, the number of days remaining before the feature expires.

### Details

Click to see detailed information for the feature key.



### Refresh

Click to reload the feature key information in the dialog box.

## Synchronize Feature Keys

You can use Firebox System Manager to get a current feature key if you have already created a LiveSecurity user account:

1. Select **Tools > Synchronize Feature Key**.  
*The Synchronize Feature Key dialog box appears.*



2. Type the configuration passphrase.
3. Click **OK**.

*The XTM device connects to the LiveSecurity web site and downloads the current feature key to your XTM device.*

## Calculate the Fireware XTM Checksum

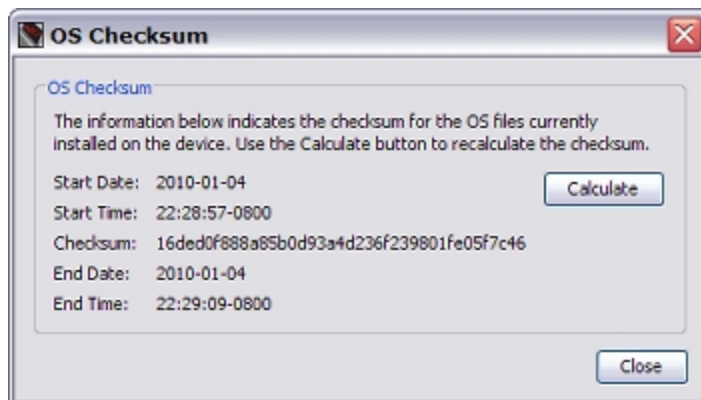
A checksum is used to validate the integrity of data when it is transmitted and stored. You can use this check to verify that your XTM device OS has not been corrupted or modified between the time it was created by WatchGuard and the time you install it on your device. The checksum is provided for the entire Fireware XTM package, not for each file in the package. To find the published checksum for your version of Fireware XTM, see the *Release Notes* for the version of Fireware XTM you installed.

You can use Firebox System Manager (FSM) to calculate the checksum for the version of Fireware XTM installed on your XTM device and then you can compare it to the checksum value for the Fireware XTM package you downloaded.

To use this feature for a FireCluster member, you must be connected to the member. For more information, see *Connect to a Cluster Member* on page 287.

1. Start *Firebox System Manager*.
2. Select **Tools > OS Checksum**.

*The OS Checksum dialog box appears and FSM automatically begins to calculate the checksum. This calculation can take a few moments to complete.*



3. To calculate the checksum again, click **Calculate**.
4. Open the *Release Notes* for the version of Fireware XTM you installed and find the checksum value.
5. Compare the checksum value to the checksum calculated in the **OS Checksum** dialog box.

If the checksum values match, your OS package has not been modified.

If the checksum values do not match, your OS package may be corrupt.

## Clear Alarms

You can clear the alarm list on the XTM device from Firebox System Manager.

1. Start *Firebox System Manager*.
2. Select **Tools > Clear Alarm**.

*The Clear Alarm dialog box appears.*



3. Type the configuration passphrase.
4. Click **OK**.

## Rekey BOVPN Tunnels

The gateway endpoints of BOVPN tunnels must generate and exchange new keys after a set period of time, or after a specified amount of traffic is passed. If you want to immediately generate new keys instead of waiting for them to expire, you can use the rekey options in Firebox System Manager to force BOVPN tunnels to expire immediately. This can be helpful when you troubleshoot tunnel issues.

Because tunnels are triggered by traffic, they are rebuilt when traffic starts to flow through them. If you rekey a tunnel and it has no traffic, it is not automatically rebuilt.

### Rekey One BOVPN Tunnel

1. Select the **Front Panel** tab.
2. From the **Branch Office VPN Tunnels** list, select a tunnel to rekey.
3. Right-click the tunnel and select **Rekey Selected BOVPN Tunnel**.  
*The Rekey BOVPN Tunnels dialog box appears.*
4. Type the device configuration passphrase.
5. Click **OK**.

### Rekey All BOVPN Tunnels

Firebox System Manager has two methods you can use to rekey all BOVPN tunnels at the same time.

Method one:

1. Select the **Front Panel** tab.
2. Right-click anywhere on the Front Panel.
3. Select **Rekey All BOVPN Tunnels**.  
*The Rekey All BOVPN Tunnels dialog box appears.*
4. Type the device configuration passphrase.
5. Click **OK**.

Method two:

1. Select **Tools > Rekey All BOVPN Tunnels**.  
*The Rekey All BOVPN Tunnels dialog box appears.*
2. Type the configuration passphrase.
3. Click **OK**.

## Control FireCluster

You can perform several FireCluster operations from Firebox System Manager.

For more information, see *Monitor and Control FireCluster Members* on page 282.

## Update the Wireless Region for an XTM 2 Series Device

You can update the wireless radio region of a WatchGuard XTM 2 Series device from Firebox System Manager.

To update the wireless country information:

1. Start *Firebox System Manager* for your device.
2. Select **Tools > Update Wireless Radio Region**.

*The 2 Series device contacts a WatchGuard server to determine the current operating region.*

For more information about wireless radio settings on the WatchGuard XTM 2 Series device, see *About Wireless Radio Settings*.

## Change Passphrases

We recommend that you change the XTM device passphrases at regular intervals for additional security. You can change the status and configuration passphrases for your XTM device from Firebox System Manager. You can change both of these passphrases at the same time, or only one passphrase. To do this, you must log in to the XTM device with the configuration passphrase.

**Note** *The status and configuration passphrases must each be at least 8 characters.*

For more information about passphrases, see *About WatchGuard Passphrases, Encryption Keys, and Shared Keys* on page 72.

1. Start *Firebox System Manager*.
2. Select **Tools > Change Passphrases**.

*The Change Passphrases dialog box appears.*



3. Type and confirm the new **Status Passphrase**.
4. Type and confirm the new **Configuration Passphrase**.
5. Click **OK**.

# 23 Reporting

---

## About the Report Server

The Report Server consolidates data collected by your Log Servers from your XTM devices and then generates reports from that data. After the data is on the Report Server, you can use Report Manager or Reporting Web UI to see reports the Report Server generates.

You can choose to use the built-in PostgreSQL database that is installed with your Report Server, or for increased scalability, you can use an external PostgreSQL database that is located on another computer. When you run the WatchGuard Server Center Setup Wizard and set up your Report Server, the built-in database is configured by default.

As an added feature, the Report Server can detect some internal failure conditions. When a failure condition is detected, the Report Server creates an Alarm log message that includes details about the failure and sends an email notification to the specified administrator.

For more information, see *Configure Notification Settings* on page 814.

For more information about the Report Manager, see *About WatchGuard Report Manager*.

For more information about the available reports, see *Predefined Reports List*.

For detailed steps to configure your Report Server, see *Set Up the Report Server*.

## Set Up the Report Server

You can use the WatchGuard System Manager installation program to install the Report Server on the computer where you installed your Management Server (your management computer), or you can install the Report Server software on a different computer. You can also install additional Report Servers for backup.

If you install the Report Server on a computer with a firewall other than Windows Firewall, you must open the ports necessary for the servers to connect through the firewall. Windows Firewall users do not have to modify their firewall configuration.

For more information, see *Install WatchGuard Servers on Computers with Desktop Firewalls* on page 32.

When you install the Report Server, the built-in Report Server PostgreSQL database is automatically installed. This is the default database for the Report Server. After you run the WatchGuard Server Center Setup Wizard to complete the initial configuration for your WatchGuard servers, you can configure your Report Server to use an external PostgreSQL database. This option provides increase scalability for your reports database.

For more information, see *Configure Report Deletion Settings and Database Settings* on page 811.

## Install the Report Server

You can install the Report Server on your management computer or on another computer.

If you choose to install the Report Server on another computer:

1. *Install WatchGuard System Manager Software.*
2. Select to install only the **Report Server** component.


## Before You Begin

Before you can configure the Report Server, you must run the WatchGuard Server Center Setup Wizard to set up the WatchGuard Server Center. For the Report Server, you add the Log Server database location and the Administrator passphrase to the Setup Wizard.

For more information, see *Set Up WatchGuard Servers* on page 545.

## Configure the Report Server

On the computer that has the Report Server software installed:

1. Right-click  in the system tray and select **Open WatchGuard Server Center**.  
*The Connect to WatchGuard Server Center dialog box appears.*
2. Type your **Username** and **Administrator passphrase**. Click **Login**.  
*The WatchGuard Server Center appears.*
3. Select **Report Server** in the **Servers** tree.  
*The Report Server page appears.*



4. Change the default settings as appropriate for your network.
  - To change your default server settings, select the [Server Settings tab](#).
  - To configure settings for report deletion and select an database location, select the [Database Maintenance tab](#).
  - To configure settings for notification messages, select the [Notification tab](#).
  - To change the settings for report generation, select the [Report Generation tab](#).
  - To configure settings for the Reporting Web UI, select the [Reporting Web UI tab](#).
  - To change the settings for logging, select the [Logging tab](#).

## Configure Server Settings

The Report Server gets data from one or more Log Servers and uses it to create reports about the activity on your network. The Report Server can also store the XML report files you create. From WatchGuard Server Center, on the **Server Settings** tab, you can specify the Log Servers that your Report Server can connect to, and select the maximum size for your Report Server database. When the server database reaches the maximum size you select, the oldest reports are deleted to make room for new reports.

1. In the **Servers** tree, select **Report Server**.
2. Select the **Server Settings** tab.

*The Server Settings page appears.*

3. In the **Log Server Settings** section, edit the **Add Log Server(s)** list.
  - To add a Log Server to the list, click **Add**.
  - To change information for a Log Server, select a server from the list and click **Edit**.
  - To delete a server from the list, select the server and click **Remove**.

For more information about how to add or edit Log Servers, see *Configure Log Servers for the Report Server* on page 809.

4. To select the **Directory Path for XML log files**, click **Browse**.
5. In the **Maximum database size** text box, type the maximum size for the Report Server database. You can set the database size to between 1 and 10,000 GB.  
*The current size of the database and the number of GB currently available appear adjacent to this field.*
6. Click **Apply** to save your changes.



## Configure Log Servers for the Report Server

You can select to retrieve log message data from multiple Log Servers to include in your reports. You can add or remove a Log Server, or change the passphrase for a Log Server in the list.

### Add a Log Server

From the WatchGuard Server Center **Report Server** page:

1. Select the **Server Settings** tab.
2. In the **Log Server Settings** section, click **Add**.

*The Add Log Server dialog box appears.*

The image shows a dialog box titled "Add Log Server" with a close button (X) in the top right corner. Inside the dialog, there is a prompt: "Enter Log server IP Address and password." Below this, there are two input fields. The first is labeled "IP Address:" and contains three asterisks. The second is labeled "Password:" and is empty. At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

3. Type the **IP Address** and **Password** for the Log Server.
4. Click **OK**.

### Remove a Log Server

From the WatchGuard Server Center **Report Server** page:

1. Select the **Server Settings** tab.
2. In the **Log Server Settings** list, select the Log Server to delete.
3. Click **Remove**.

*The Log Server is removed from the list.*

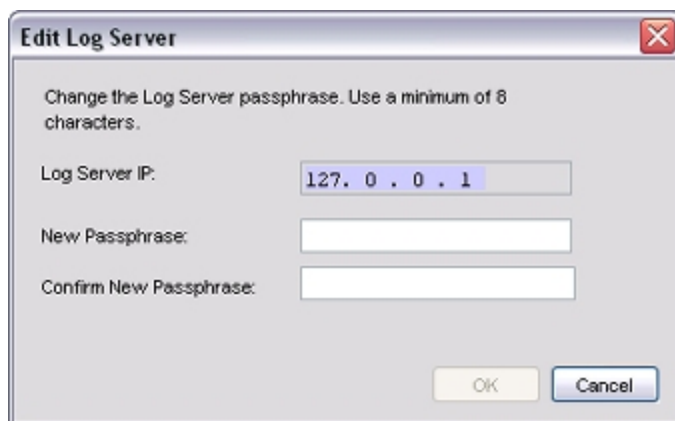
### Edit the Log Server Passphrase

If you change the passphrase for your Log Server, you must update the passphrase that the Report Server uses when it contacts the Log Server to get log message data.

From the WatchGuard Server Center **Report Server** page:

1. Select the **Server Settings** tab.
2. In the **Log Server Settings** list, select a Log Server.
3. Click **Edit**.

*The Edit Log Server dialog box appears.*



4. In the **New Passphrase** and **Confirm New Passphrase** text boxes, type the new passphrase for the Log Server.
5. Click **OK**.  
*The Log Server passphrase is updated.*

## Configure Report Deletion Settings and Database Settings

From WatchGuard Server Center, you can configure the report deletion and database settings for your Report Server. You can choose to use either the built-in Report Server database or an external PostgreSQL database. If you choose to use an external database, make sure the database is installed before you select it.

For more information about how to install a WatchGuard Report Server and the built-in PostgreSQL database, see *Set Up the Report Server* on page 806 or *Set Up WatchGuard Servers* on page 545.

1. In the **Servers** tree, select **Report Server**.
2. Select the **Database Maintenance** tab.

*The Database Maintenance page appears.*

The screenshot shows the 'Report Server' configuration page in the 'WatchGuard Server Center'. The 'Database Maintenance' tab is selected. The 'Report Deletion Settings' section includes a spinner for 'Keep reports on the Report Server for:' set to 30 days, a 'Messages last deleted' field, a 'Delete expired reports at:' spinner set to 11:55 PM, and a 'Next deletion scheduled:' field showing 09/21/2010 11:55 PM. The 'Database Settings' section has two radio buttons: 'Built-in database' (selected) and 'External PostgreSQL database'. Below this is a text field for 'Log data is stored and managed at this location:' containing 'C:\Documents and Settings\WatchGuard\logs'. At the bottom right are 'Reset', 'Apply', and 'Help' buttons.

3. To configure settings for your Report Server, follow the instructions in the subsequent sections.
4. When you are finished, click **Apply** to save your changes.

## Configure Settings for Report Deletion

The Report Server can automatically delete reports at the times you specify. You can select how long to keep reports on the server, from a minimum of 1 day to a maximum of 365 days (one year). The default setting is 30 days. When you change the number of days to keep reports on the server, only reports that are generated after you made the change are affected by the new setting. For example, if you change the setting from 15 days to 30 days, the Report Server does not automatically generate 30 days of reports. It does, however, store reports for 30 days from the date you updated the setting.

In the **Report Deletion Settings** section:

1. In the **Keep reports on the Report Server for** text box, type or select the number of days to store messages on the Report Server.  
To keep the size of your database small, select a smaller number of days.  
*The date messages were last deleted appears.*
2. In the **Delete expired reports at** text box, type or select the time of day to delete expired reports.  
*The date and time of the next scheduled deletion appears.*

## Configure the Database Settings

You can choose to either use the built-in PostgreSQL database that is automatically installed with your Report Server, or an external PostgreSQL database that is located on another computer. You can use any PostgreSQL database. This includes a database that was configured with another WatchGuard Report Server.

If you select to use an external PostgreSQL database, make sure your XTM device has a policy configured to allow traffic to and from the port you specify for communication with the external database. If you do not allow traffic to the external database through the specified port, the Report Server cannot connect to the external database. If the external database you select was not installed with a WatchGuard Report Server, the first time the Report Server connects to the database, it configures the structure of the database tables.

Before you configure an external database, make sure you have this information for the external database:

- IP address of the computer on which the external database is installed
- Port number to use to connect to the database
- User name and password for the Database User

**Note** *If you change the **Database Settings**, you must restart the Report Server for the changes to take effect.*

To use the built-in PostgreSQL database:

In the **Database Settings** section, select **Built-in database**.

*The default directory location for your Report Server appears in the text box. This is the location you selected when you ran the WatchGuard Server Center Setup Wizard. You cannot change this location.*

To use an external PostgreSQL database:

1. In the **Database Settings** section, select **External PostgreSQL** database.  
*The external database options appear.*

The screenshot shows the 'Report Server' configuration interface within the 'WatchGuard Server Center'. The 'Database Settings' section is expanded, showing two radio button options: 'Built-in database' and 'External PostgreSQL database'. The 'External PostgreSQL database' option is selected. Below this, there are several input fields: 'Database Name', 'IP Address' (with three dots for each octet), 'Port' (set to 5432), 'Database User', and 'Password'. A 'Test Connection' button is located to the right of the password field. At the bottom of the configuration area are 'Reset', 'Apply', and 'Help' buttons.

2. In the **Database Name** text box, type the name of the external database.
3. In the **IP Address** text box, type the IP address of the computer where the external database is installed.
4. In the **Port** text box, type or select the port the Report Server must use to contact the external database.
5. In the **Database User** text box, type the user name the Report Server must use to contact the external database.

**Note** The Database User name and password must not include these characters @ = , / \_ ; # [ ] ' " \* ? ` \ and cannot be more than 64 characters.

6. In the **Password** text box, type the password for the user name you selected.
7. To verify these settings are correct, click **Test Connection**.  
*If the Report Server cannot contact the database, an error message appears.*  
*If the Report Server successfully connects to the database, a confirmation message appears.*

## Configure Notification Settings

From WatchGuard Server Center, you can enable your Report Server to send notification messages when failure events occur, and when the Report Server database nears the maximum size you selected. You can also specify the details for the notification messages.

For more information about failure events for the Report Server, see the subsequent section, *Report Server Failure Events* on page 816.

For information about how to set the maximum size of the Report Server database, see *Configure Server Settings* on page 808.

1. In the **Servers** tree, select **Report Server**.
2. Select the **Notification** tab.

*The Notification page appears.*

The screenshot shows the 'Notification' configuration page for the 'Report Server' in the 'WatchGuard Server Center'. The page has a tabbed interface with 'Notification' selected. It contains three main sections: 'Events', 'SMTP Server Settings', and 'Notification Setup'. In the 'Events' section, the 'Enable notifications for failure events' checkbox is unchecked, while the 'Send an email notification if the database reaches the warning threshold' checkbox is checked. The 'Warning threshold' is set to '100%'. In the 'SMTP Server Settings' section, the 'Outgoing email server (SMTP)' is 'localhost', and the 'Send credentials to the email server' checkbox is unchecked. In the 'Notification Setup' section, the 'Send email to' field is 'admin@localhost', the 'Send email from' field is 'vs-server@localhost', and the 'Subject' is 'WatchGuard Report Server Notification'. There is a 'Test Email' button at the bottom right of the form area, and 'Reset', 'Apply', and 'Help' buttons at the bottom of the page.

3. To enable notification message to be sent when a failure event occurs on the Report Server, select the **Enable notifications for failure events** check box.
4. To receive a warning message when the database is near the selected threshold limit, select the **Send an email notification if the database reaches the warning threshold** check box.
5. In the **Warning threshold** text box, type or select the threshold limit.

6. To configure the **SMTP Server Settings** and **Notification Setup** settings, follow the procedures in the subsequent sections.
7. Click **Apply** to save your changes.

## Configure the SMTP Server Settings

For email notification to work correctly, you must specify the address of an SMTP email server the Report Server can use to send email messages.

In the **SMTP Server Settings** section:

1. In the **Outgoing email server (SMTP)** text box, type the address of your SMTP server.
2. If your email server requires authentication, select the **Send credentials to the email server** checkbox.
3. In the **User name** text box, type the user name for the email server.
4. In the **Password** text box, type the password for the email server.

**Note** *If the user name and password are not required for your SMTP server, you can leave these fields blank.*

## Configure Notification Message Settings

You can specify the email accounts to use to send email notification messages and select the subject text for the messages.

In the **Notification Setup** section:

1. In the **Send email to** text box, type the full email address of the account to which you want to send notification message.
2. In the **Send email from** text box, type the full email address of the account from which you want to send notification messages.
3. In the **Subject** text box, type the subject line you want users to see when they receive an event notification email.
4. In the **Body** text box, type the message you want users to see when they receive the notification email.

You can use plain text or HTML in the message body.

5. To send a test notification email to the address you specified, click **Test Email**.

*A message appears that tells you if the notification email was sent successfully, or if it failed to send.*

## Report Server Failure Events

When a failure event occurs on the Report Server, and you have enabled logging for failure events, the Report Server sends a notification message about the failure event. Failure events for the Report Server include PostgreSQL service failures, system failures, and network failures.

A notification message is sent for these failures:

- **Lost database connection**

If the connection to the database is lost and cannot be reestablished immediately, a notification message is sent. The server continues to try to connect to the database until the connection succeeds. The server sends a notification email every 15 minutes until the database connects to the server again.
- **Database errors**

This includes I/O errors, disk-full conditions, and any other database-related failures.
- **Report generation errors**

This includes I/O errors that occur when the XML report file is created.
- **Lost Log Server connection**

If the Report Server cannot connect to the Log Server because the Log Server is not running, or another system error occurs (for example, a network error), the Report Server sends a notification message.



## Configure Report Generation Settings

From WatchGuard Server Center, you can configure the report generation settings for your Report Server. These settings apply to Available Reports and On-Demand Reports.

Reports are generated in XML files that you can view with Report Manager or Reporting Web UI. To control which reports are generated, and when they are generated, you can create groups of reports and report schedules. When you create a report group, you specify which devices to include in the group, the specific types of reports to generate, and the directory where the generated reports are saved. When you create a report schedule, you select the devices and groups for which to generate the reports, the reports to generate, the time to generate them, and whether to generate the reports in PDF or HTML format. You can also specify whether to run the report recurrently, and whether to send a notification message when the report generation is completed to the email addresses you specify.

1. *Configure Report Generation Settings* **Configure Report Generation Settings** In the **Servers** tree, select **Report Server**.
2. Select the **Report Generation** tab.  
*The Report Generation page appears.*



3. In the **Number of records included in summary report** text box, type the number of records you want to appear in your Summary reports. The allowed range is 25–100 records.  
*This setting applies to Summary reports only.*

4. To configure the settings for report schedules and groups, follow the procedures in the subsequent sections.
5. Click **Apply** to save your changes.

## Manage Report Schedules

You can add, edit, and delete schedules for report generation. When you add, edit, or remove a schedule, the Report Server generates a log message about this activity.

For each report schedule, you specify these parameters:

- Devices and groups to include
- Reports to generate
- Time when reports are generated and recurrence
- Format for report output (PDF or HTML)
- Notification email settings for completed reports

If you want to include a report group in your report schedule, you must create the group before you create the schedule. For instructions to create a report group, see the [Manage Groups](#) section.

## Create a Report Schedule

1. In the **Report Schedules** section, click **Add**.  
*The New Schedule dialog box appears with the Schedule Settings tab selected.*



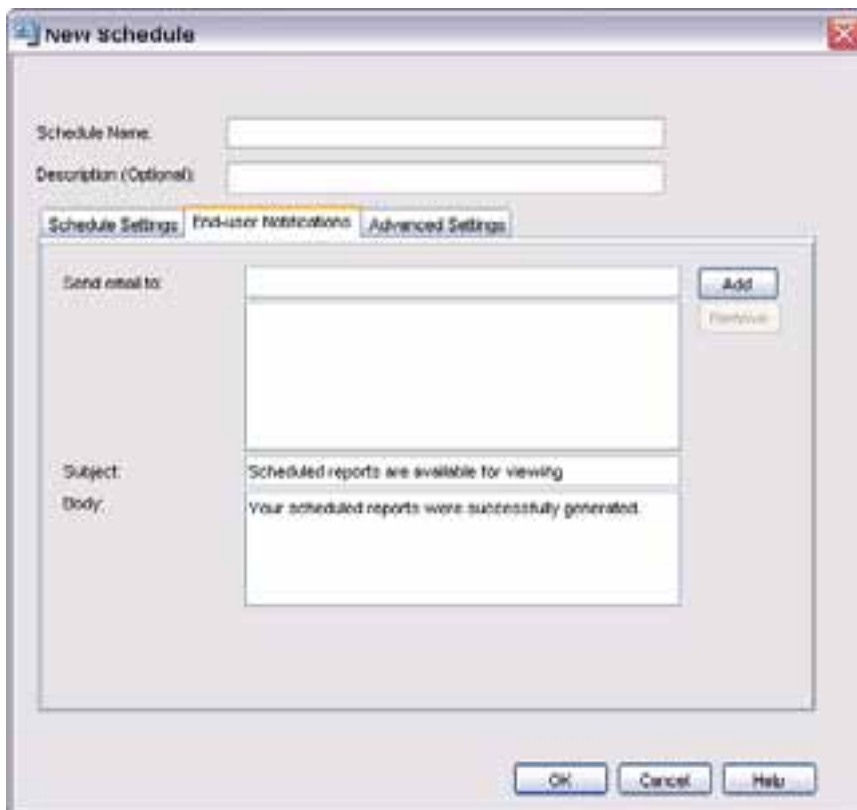
2. In the **Schedule Name** text box, type a name for this schedule.
3. (Optional) In the **Description (Optional)** text box, type a description to help you identify this schedule.
4. In the **Devices** list, select the check box for each device, device group, or FireCluster to include in the group.
5. In the **Report types** list, select the check box for each report you want to generate.
6. From the **Report Schedule** options, select when to run the scheduled report:
  - **Run once at**
  - **Run recurrently**
7. If you select **Run once at**, specify the date and time for the report to run.  
If you select **Run recurrently**, select how often to run the report and specify the range of recurrence:
  - **Daily**
  - **Weekly**
  - **Custom**
8. To configure email notifications for scheduled reports, follow the procedure in the *Configure Email Notifications* section.
9. To configure settings to generate reports for external use, follow the procedure in the *Configure Advanced Settings* section.
10. Click **OK** to save your settings.  
*The schedule appears in the Report Schedules list.*

### Configure Email Notifications

You can specify which end-users receive email notification messages when reports are generated or a schedule is modified.

In the **New Schedule** dialog box:

1. Select the **End-user Notifications** tab.  
*The settings for email notifications appear.*



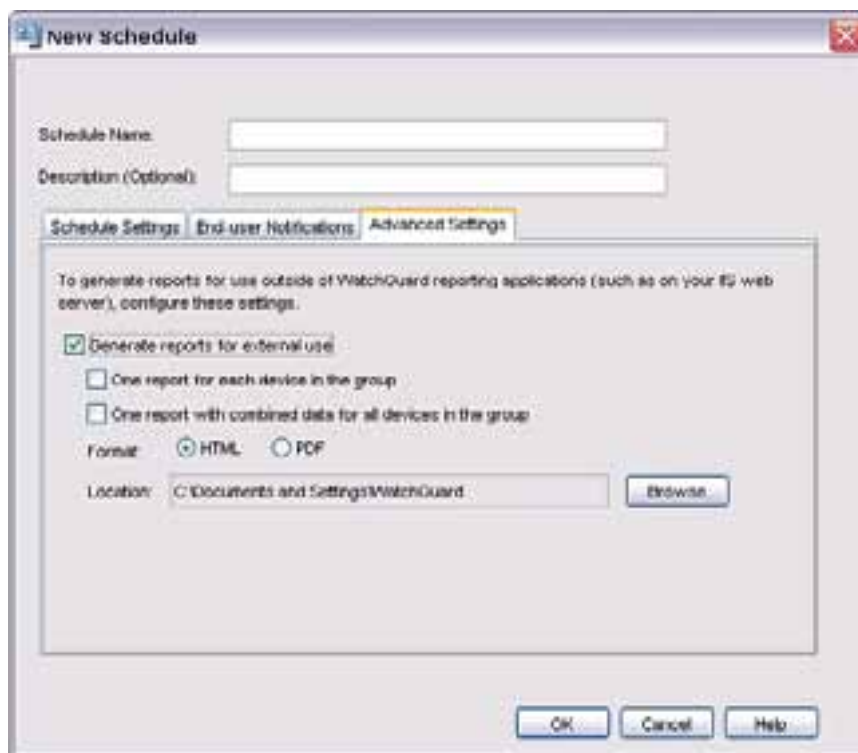
2. In the **Send email to** text box, type the email address where you want to send notifications when a scheduled report is generated or a schedule is modified. Click **Add**.  
*The email address is added to the Send email to list. Repeat this step to add more email addresses.*
3. To delete an email address from the **Send email to** list, select the email address and click **Remove**.
4. In the **Subject** text box, type the text to include in the subject line of the notification messages.
5. In the **Body** text box, type the text of the notification messages.
6. Click **OK**.  
*The new schedule appears in the Report Schedules list.*

### Configure Advanced Settings

To generate reports that you can review in applications other than WatchGuard Report Manager or Reporting Web UI, such as on your web server, you can configure Advanced Settings for your scheduled reports.

In the **New Schedule** dialog box:

1. Select the **Advanced Settings** tab.  
*The Advanced Settings appear.*



2. Select the **Generate reports for external use** check box.
3. Select an option for how reports are generated:
  - **One report for each device in the group**
  - **One report with combined data for all devices in the group**
4. Select a **Format** option for the report: **HTML** or **PDF**.
5. In the **Location** text box, type the path to the directory where you want to save reports.  
Or, click **Browse** and select the directory.

## Change the Settings for a Schedule

On the **Schedule Settings** tab:

1. From the **Report Schedules** list, select a schedule.
2. Click **Edit**.  
*The Edit Schedule dialog box appears.*
3. Modify the report schedule settings.
4. Click **OK**.

## Delete a Schedule

From the **Schedule Settings** tab:

1. From the **Report Schedules** list, select a schedule.
2. Click **Remove**.  
*A confirmation dialog box appears.*
3. Click **Yes**.  
*The schedule is removed from the Report Schedules list.*

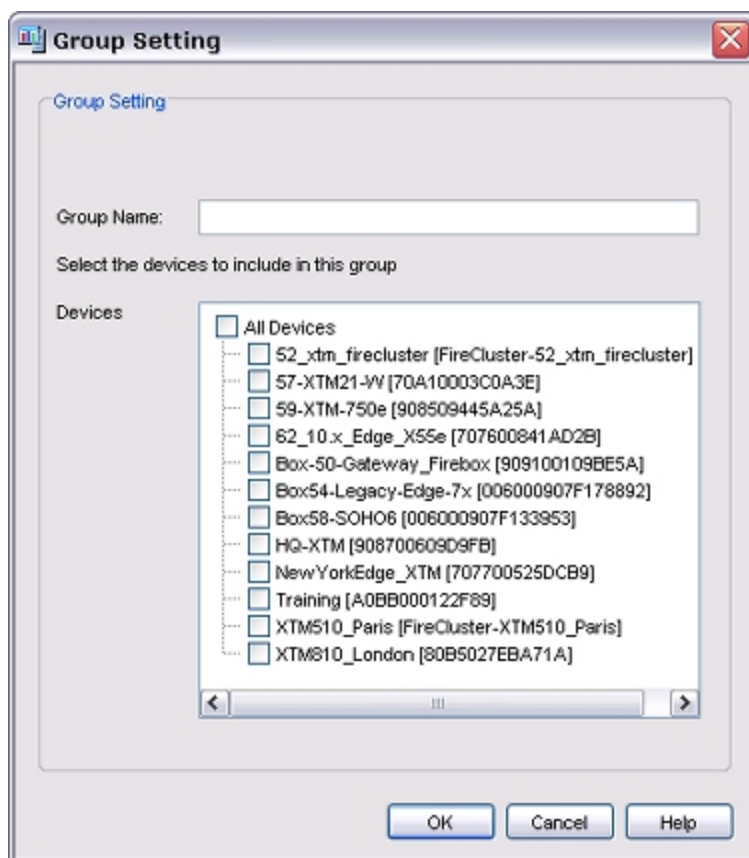
## Manage Groups

You can add, edit, or delete groups of XTM devices to include in the reports generated by the Report Server. When you add, edit, or delete a group, the Report Server generates a log message about the activity.

### Create a Group

1. In the **Report Groups** section, click **Add**.

*The Group Setting dialog box appears.*



2. In the **Group Name** text box, type a descriptive name to identify the group.
3. From the **Devices** list, select the check box for each device to include in the group.
4. Click **OK**.

*The group you added appears in the Group Name list on the Report Generation tab. The devices you included in the group appear in the Selected group members list.*

### Change the Settings for a Group

1. In the **Group Name** list, select a group.
2. Click **Edit**.

*The Group Setting dialog box appears.*

3. Modify the group settings.
4. Click **OK**.

### Delete a Group

1. In the **Group Name** list, select a group.
2. Click **Remove**.  
*A confirmation dialog box appears.*
3. Click **Yes**.  
*The group is removed from the Group Name list.*

## Configure Reporting Web UI Settings

Reporting Web UI is a web-based interface you can configure to enable your users to view the log message data collected from the activity on your network. This log message data is converted into reports that users can review for the specific security devices on your network that you select. Reports are available as either Archived Reports or On-Demand Reports. Archived Reports are reports that are configured to run at a specific date and time. On-Demand Reports are reports that you can generate at any time.

Reporting Web UI is compatible with Firefox 3.0, Internet Explorer 7.0, or Safari. Make sure your users enable JavaScript for their browsers.

Your users can use Reporting Web UI to generate and review any of the standard, predefined report types that you select. The reports that appear in the Web UI depend on which reports you choose to make available. To enable users to see reports, you must first add each user to the WatchGuard Server Center **Users** page.

For more information about how to add a user, see *Use WatchGuard Server Center to Configure Users or Groups* on page 673.

For information about how to use Reporting Web UI, see the [Reporting Web UI Help](#).

From WatchGuard Server Center, you configure the reports that are available in Reporting Web UI. You can also select the header page colors and a logo to customize the look and feel of the Web UI pages. If you do not change the default site customization settings, the default logo and color scheme are used.

To configure settings for Reporting Web UI:

1. In the **Servers** tree, select **Report Server**.
2. Select the **Reporting Web UI** tab.  
*The Reporting Web UI page appears.*



3. In the **Report Availability** section, select the check box for each report type you want to make available to your users in the Web UI.
4. In the **Select the maximum number of days for which users can run reports** text box, type or select the maximum number of days users can select to include in a report.
5. To change the logo and site colors for the Web UI, in the **Site Customization** section:
  - To select a site or report logo, adjacent to the logo you want to update, click **Change**.
  - To select a site header color, adjacent to the element you want to change, click .
  - To change the URL for the logo, in the **Report logo URL** text box, type a new URL.
6. Click **Apply** to save your changes.

## Configure Logging Settings for the Report Server

From WatchGuard Server Center, you can configure where the Report Server sends log message data. You can choose to send log messages to the WatchGuard Log Server, Windows Event Viewer, or a log file.

1. In the **Servers** tree, select **Report Server**.
2. Select the **Logging** tab.  
*The Logging page appears.*



**Report Server** **WatchGuard Server Center**

Server Settings Database Maintenance Notification Report Generation Reporting Web UI **Logging**

Choose the destination for Report Server log messages.

**WatchGuard Log Server**

Send log messages to WatchGuard Log Server(s)

Priority	Log Server Address

Add Edit Remove Up Down

Select a log level: Warning

**Windows Event Viewer**

Send log messages to Windows Event Viewer

Select a log level: Warning

**File path**

Send log messages to a file

File location: C:\Documents and Settings\WatchGuard\logs\lwr Browse

Select a log level: Information

Reset Apply Help

3. Configure settings for your Report Server.

For detailed information about how to configure the Logging settings for your server, see *Configure Logging Settings for Your WatchGuard Servers* on page 708.

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

## Move the Report Directory

You can use the WatchGuard Server Center Setup Wizard to choose the directory where your report data files are stored. The Report Server stores all data files in this directory. After this wizard is complete, you cannot change the data directory from the WatchGuard Server Center application. The Report Server stores the XML report files in a different location that you can change from WatchGuard Server Center.

To change the location where the Report Server stores report data, you must set up the Report Server again. To do this, you edit the *wserver.ini* file and run the WatchGuard Server Center Setup Wizard again. When you run the wizard again, you specify the new directory location, but the data in the old directory is not automatically moved to the new directory. You must manually move the data from the old directory to the new directory location before you use the wizard to specify the new directory for the Report Server.

When you run the WatchGuard Server Center Setup Wizard to reconfigure your Report Server, the pages that appear in the wizard can be different from the pages described in the subsequent procedure. The instructions here assume that your computer has only the Management Server, Log Server, and Report Server installed. If you have other WatchGuard servers installed, additional pages can appear in the wizard.

For information about these pages, see the complete *Set Up WatchGuard Servers* on page 545 topic.

**Note** Because the Log Server and the Report Server both use the PostgreSQL database, if you have these servers installed on the same computer and you move the database, it is moved for both servers.

### Step 1 — Stop Services

1. Open WatchGuard Server Center.
2. Stop and Start Your WatchGuard Servers.
3. Close WatchGuard Server Center.
4. Stop the PostgreSQL-8.2 service.
  - From Windows Control Panel, select **Administrative Tools > Services**.  
*The Services window appears.*
  - Select **PostgreSQL-8.2** and click **Stop**.  
*The service stops.*

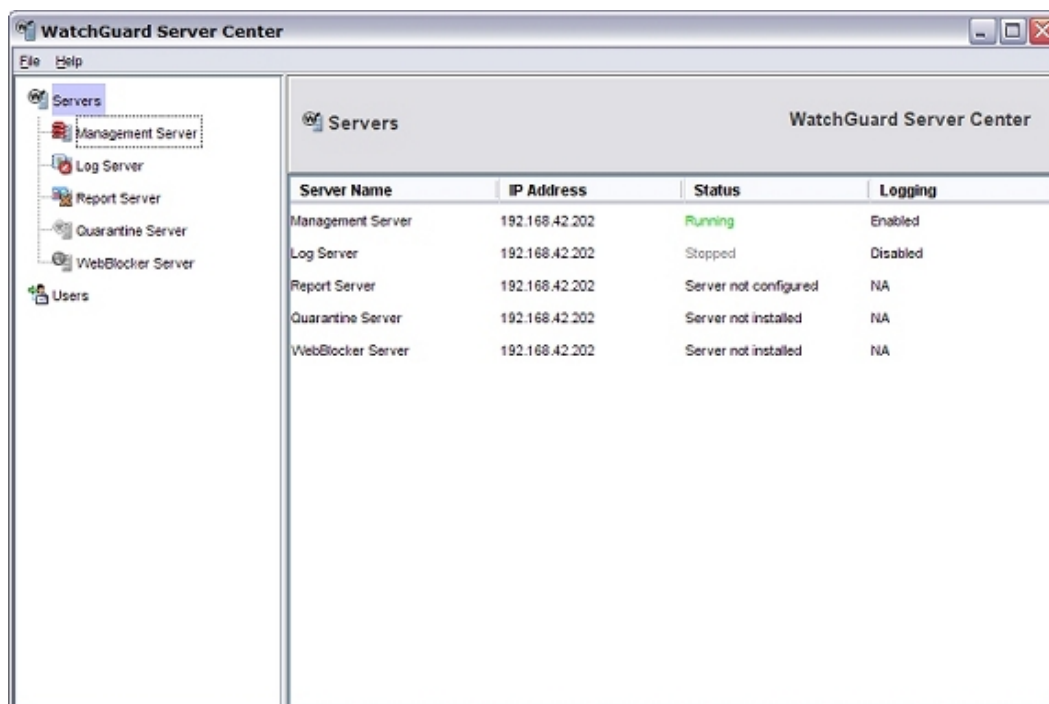
### Step 2 — Move the Report Data

1. Create the new report directory.  
For example, E:\WatchGuard\report\_directory\reports.
2. Go to the original report directory folder and copy the entire directory folder. Make sure to include all the folders and files in the directory.  
For example, go to C:\Documents and Settings\WatchGuard\reports folder. Copy the \data subfolder and all the files in it.
3. Paste the original report directory in the new location.

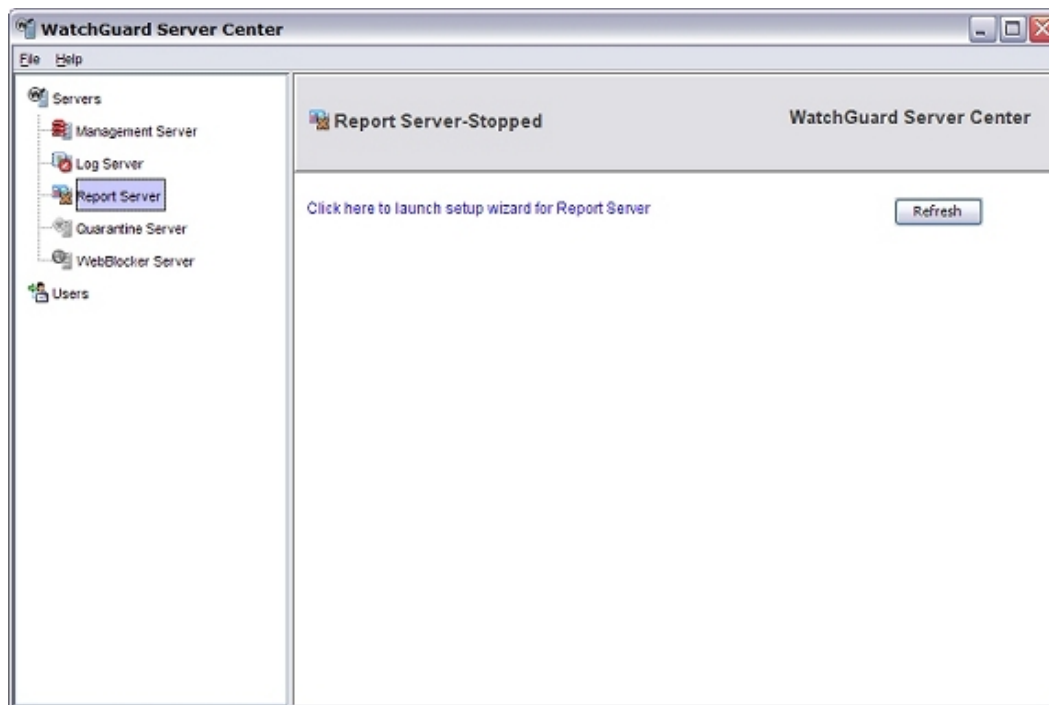
For example, E:\WatchGuard\report\_directory\reports. Make sure you paste the entire report directory. In these examples, this includes the \data folder.

### Step 3 — Run the Setup Wizard

1. Open the C:\Documents and Settings\WatchGuard\wserver\wserver.ini file and change the **WizardSuccess** value to "0".
2. Delete the file: \Program Files\WatchGuard\wsm11.0\postgresql\install\pg\_install.ini.
3. Open WatchGuard Server Center. The **Status** for the Report Server is **Server not configured**.



4. In the **Servers** tree, select **Report Server**.  
*The Report Server page appears.*



5. To launch the WatchGuard Server Center Setup Wizard for the Report Server, click **Click here to launch setup wizard for Report Server**.  
*The WatchGuard Server Center Setup Wizard will launch now message appears.*
6. Click **OK** to launch the wizard.  
*The WatchGuard Server Center Wizard appears.*
7. Click **Next** to start the wizard.  
*The Review Settings page appears.*
8. Review the **Report Server Settings**.
9. Click **Next**.
10. Complete the WatchGuard Server Center Wizard.  
*The wizard installs the PostgreSQL program and configures the Report Server.*

### Final Steps

1. On the **Report Server** page, click **Refresh**.  
*The Report Server is started and the Report Server configuration pages appear.*
2. Restart the Log Server.

## Start or Stop the Report Server

You can start or stop the Report Server service at any time, and still keep the connection to your Report Server.

To start the service, from the WatchGuard Server Center:

1. In the **Servers** tree, select **Report Server**.
2. Right-click **Report Server** and select **Start Server**.  
*The service is stopped and Report Server-appears at the top of the Report Server page.*

To stop the service, from the WatchGuard Server Center:

1. In the **Servers** tree, select **Report Server**.
2. Right-click **Report Server** and select **Stop Server**.  
*A warning message appears.*
3. Click **Yes** to confirm you want to stop the Report Server service.  
*The service is stopped and Report Server-Stopped appears at the top of the Report Server page.*



## About WatchGuard Report Manager

You can use Report Manager to review the data collected from your Log Servers for all your XTM devices. From Report Manager, you can see the available reports for one XTM device, FireCluster, server, or a group of your devices.

WatchGuard Reports are summaries of the log data that is collected from the device and server log files. The Report Server gets the log message data from the Log Server every fifteen minutes. Report Manager then consolidates the log data into a variety of predefined reports so that you can easily examine device actions and events. On the Report Manager **Available Reports** tab, you can see the reports that you have scheduled the Report Server to run. You can also select to run new reports on the **On-Demand Reports** tab.

When you select to run an On-Demand report, the Report Server can only include the log message data it has received from the Log Server. It can take up to a half-hour after a log message is sent for the log message to be available to the Report Server. To make sure your report includes data for the events you want to see, you must account for this delay when you select the parameters for a report.

For more information about these predefined reports, see *Predefined Reports List* on page 835.

You can also use Reporting Web UI (a convenient web-based user interface) to view and generate reports. You configure Reporting Web UI settings when you configure the Report Server.

For more information about how to configure Reporting Web UI, see *Configure Reporting Web UI Settings* on page 823.

For more information about how to use Reporting Web UI, see the *Reporting Web UI Help*.

With the advanced features of Report Manager, you can:

- *Set Report Options* — Report background color, maximum number of records per file, and the directory where reports are stored
- *Select Report Parameters* — Date ranges for reports and filters to streamline report data
- *Select the Report Format* — HTML or PDF
- *Email, Print, or Save a Report*

**Note** *To view reports in Report Manager, you must have Microsoft Internet Explorer version 6.0 or higher or Firefox installed. If you use another web browser as your default web browser, when you select a report it does not appear in the Report Manager window. To view reports with another default browser, you must manually select to view the report in your default web browser window. For more information, see *Select the Report Format* on page 850.*

## Open Report Manager

Open Report Manager from the main WatchGuard System Manager (WSM) interface.

1. Click .

Or, select **Tools > Logs > Report Manager**.

*WatchGuard Report Manager and the Connect to Report Server dialog box appear.*




2. In the **Report Server** text box, type or select the IP address for your Report Server.
3. In the **User Name** text box, type the user name for the administrator.  
The default user name is *admin*.
4. In the **Passphrase** text box, type the Administrator passphrase.  
*You set the Administrator passphrase when you complete the WatchGuard Server Center Setup Wizard.*
5. Click **Login**.  
*Report Manager connects to the Report Server and the available reports appear in the WatchGuard Reports list.*

The first time you connect to a Report Server, an **Accept Certificate** dialog box appears. You must accept the certificate to continue.


## Connect to a Different Report Server

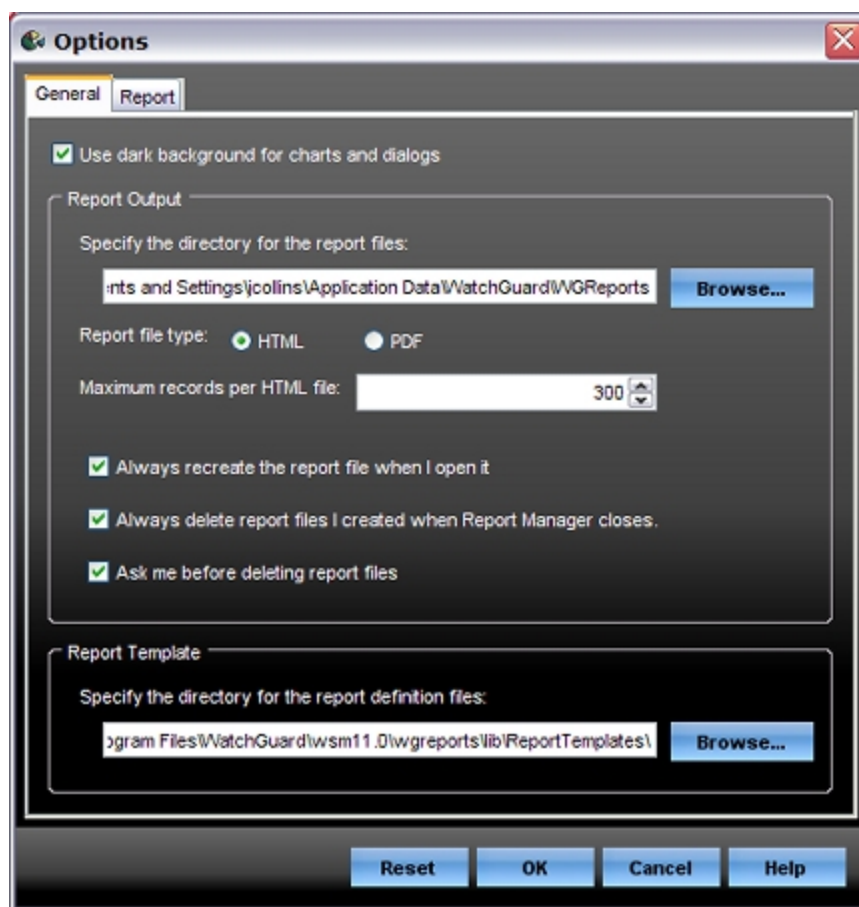
To connect to a different Report Server while Report Manager is open, you must first disconnect from the current Report Server.

1. Select **File > Disconnect**.
2. To connect to a different Report Server, click .

## Set Report Options

From Report Manager, you can change the default settings for report output and the default report template.

1. Click .  
Or, select **View > Options**.  
*The Options dialog box appears with the General tab selected.*



2. To configure the Report Options settings, follow the procedures in the subsequent sections.
3. Click **OK** to save your changes.



## Configure Settings for Charts and Dialog Boxes

You can select to use a dark or light background for charts and dialog boxes. A dark background is selected by default.

To use a light background in all charts and dialog boxes:

1. Select the **General** tab.
2. Clear the **Use dark background for charts and dialogs** check box.

## Configure Settings for Report Output

1. Select the **General** tab.
2. To **Specify the directory for the report files**, click **Browse** and select the folder where you want Report Manager to save the report file on your local hard drive.
3. To specify the default view for report output, select a **Report file type**:
  - **HTML**
  - **PDF**

When you open a report in Report Manager, the report is automatically displayed in this format.

4. To set the maximum number of records to include in each HTML file, in the **Maximum records per HTML file** text box, type or select the number of reports.
5. To configure Report Manager to always create new versions of the selected reports, select the **Always recreate the report file when I open it** check box.

*Large reports might take a long time to generate. This option can take longer, but it provides the most recent data.*

Clear this check box to enable Report Manager to open existing versions of the selected reports.

*This option decreases the time it takes to see a report. Information included in previously created reports might not be the most recent data.*

6. To delete all the reports you created when you close Report Manager, select the **Always delete report files I created when Report Manager closes** check box.
7. To leave report files in the report directory, clear this check box.
8. To configure Report Manager to notify you before report files are deleted, select the **Ask me before deleting report files** check box.  
To configure Report Manager to delete report files without notifying you, clear this check box.

## Select a Location for the Report Template

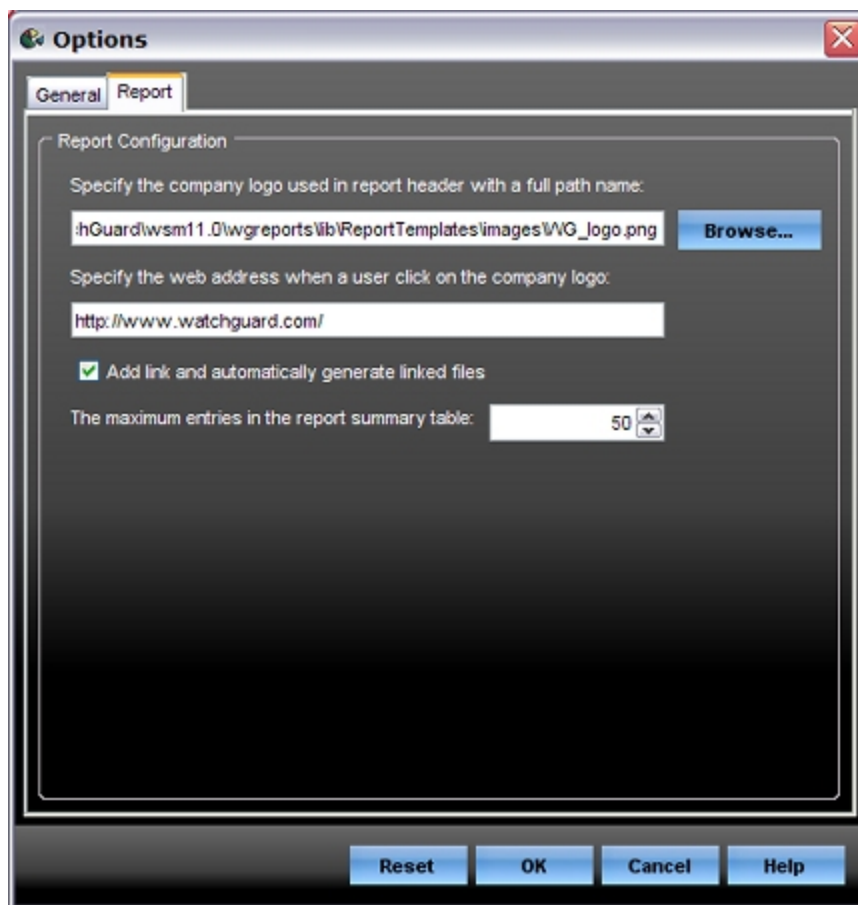
To specify the directory for the report definition files:

1. Select the **General** tab.
2. In the **Report Template** section, click **Browse** and select the directory where you want to save the report definition files.

## Configure Details for Your Reports

You can use the Report Options to add your company logo to your Reports, specify a web site to open when users click your logo, and specify the number of reports included in the Report summary table.

1. Select the **Report** tab.



2. To add your company logo at the top of your reports, in the **Specify the company logo used in report header with a full path name** text box, type the full path to an image file.  
Or, click **Browse** to select the file.
3. To add a web address to go to when you click the company logo on a report, in the **Specify the web address when a user clicks on the company logo** text box, type the full web site address.
4. To add the web address link to the report, select the **Add link and automatically generate linked files** check box.
5. To specify when the Report Server removes entries from the report summary table, in the **The maximum entries in the report summary table** text box, type or select a the number of reports.

## Predefined Reports List

Report Manager includes predefined reports that you can select to show the data your XTM device has collected.

For detailed instructions about how to show reports, see *Select Report Parameters* on page 838 and *View a Report* on page 843.

Report Type	Report Name	Description
Application Control	Application Usage Summary	Summary report of Application Usage data
	Blocked Application Summary	Summary report of applications blocked by Application Control
Client Reports	Top Client Reports	Top client reports by application usage, blocked applications, blocked categories, bandwidth, and connections
	Per Client Web Activity Report	Summary report of Web usage for a specific client (includes charts)
Exceptions	Alarms	All alarm records
	Alarm summary	Summary report of all alarms
	Denied packet summary	Summary report for all denied packets
	Denied packets detail	Detailed report for each incoming or outgoing action
	Denied packets by client	Detailed report of all denied packets, grouped by client
	Denied packets by client summary	Summary report of all denied packets, grouped by client
Firebox Reports	Audit trail	Detailed list of audited configuration changes for an XTM device
	DHCP lease activity	Detailed report of all activity for the DHCP lease
	Firebox statistics	XTM device bandwidth statistics for all interfaces
	Denied User Authentication Report	Detailed list of users denied authentication Includes date, time, and reason for authentication failure
	User Authentication Report	Detailed list of users authenticated Includes login time, logout time, and connection method information

Report Type	Report Name	Description
	External interface bandwidth	Firebox bandwidth statistics summary (for external interfaces) The data sampling interval is based on the report time range. The minimum interval is 1 minute. The published report samples data every 10 minutes.
	Transfer rate for external interfaces and VPN tunnels	These reports are generated when a Bandwidth report is scheduled. They include information about the bandwidth/transfer rate for external interfaces and VPN tunnels.
	VPN tunnel bandwidth	VPN tunnel traffic summary
Gateway AntiVirus Reports	Gateway AntiVirus summary	Gateway AntiVirus action summary
	Detail by protocol	Gateway AntiVirus action details by protocol
	Detail by host (HTTP)	Gateway AntiVirus action details by host
	Detail by virus	Gateway AntiVirus action details by virus
	Detail by email sender	Gateway AntiVirus action details by email sender Available for SMTP or POP3
Intrusion Prevention Service Reports	Intrusion Prevention Service Summary	All intrusion prevention actions
	Detail by IP-spoofed packets	Prevention summary details by IP-spoofed packets
	Detail by protocol	Prevention summary details by protocol
	Detail by severity	Prevention summary details by severity
	Detail by source IP	Prevention summary details by source IP
	Detail by signature	Prevention summary details by signature
Packet-Filter Summaries	Host summary	Summary of packet-filter data by host
	Service summary	Summary of packet-filter data by service
	Daily trend	Summary of packet-filter data by time
	Session summary	Summary of packet-filter data by session

Report Type	Report Name	Description
POP3 Proxy	POP3 server summary	POP3 server activity
	POP3 email summary	POP3 email user activity
	POP3 Proxy detail	All records by time
Proxy Summaries	Proxy Host summary	Proxied traffic summary by host
	Proxy summary	Proxied traffic summary by proxy
	Proxy Daily trend	Proxied traffic summary by time
	Proxy session summary	Proxied traffic summary by session
Reputation Enabled Defense	Reputation Enabled Defense Summary	Summary of Reputation Enabled Defense actions
SMTP Proxy	SMTP server summary	SMTP server activity summary (for internal and external email accounts)
	SMTP email summary	SMTP email activity summary (for internal and external servers)
	SMTP proxy detail	SMTP proxy action records by time
spamBlocker Summary	spamBlocker summary	Statistics by spam type, action, and spam senders and recipients
	spamBlocker by sender	Statistics by sender
Web Audit Reports	Web audit summary	Trends, active clients, most popular domains, WebBlocker information, and web sites blocked by proxy rules Charts are included for the more detailed reports. You can click a chart to see the detailed report.
	Web audit by category	
	Web audit by client	
Web Traffic Reports	Activity trend	Hourly trend data
	Most active clients detail	Top web traffic clients by name and IP address

Report Type	Report Name	Description
	Most popular domains	Top web sites visited by clients
	URL details by time	All URLs in chronological order
	URL details by client	All URLs in order by client
	URL details by domain	All URLs in order by domain
WebBlocker Reports	WebBlocker summary	Statistics and web sites blocked by WebBlocker service
	WebBlocker by category	
	WebBlocker by client	
Wireless Intrusion Detection	Wireless Intrusion Detection Summary	Summary of all Wireless Intrusion Detection actions

## Select Report Parameters

You can use Report Manager to review the log data on your Report Server. To show reports, you must first select the devices and time/date range to include in the report, and then select to view an **Available Report** or generate an **On-Demand Report**. Available reports are reports that you schedule your Report Server to generate at a specific date and time. You can select which report details to include in your Available Reports. On-demand reports are specified WatchGuard reports that you can generate with near real-time information.

For more information about how to create an available report, see *Configure Report Generation Settings* on page 817.

Depending on whether you select the **Available Reports** or **On-Demand Reports** tab, the label for the time/date range drop-down list changes. If you select **Available Reports**, the label is **Generated** and indicates that you can select the time range that the Available Report was generated by the Report Server. If you select **On-Demand Reports**, the label is **Generate**, and indicates that you can select the time range for the log messages to include in your report.

## Select a Device, a Date Range, and a Report List

You can choose to see details for an XTM device, server, or FireCluster in your report. You can also choose to view reports for just one member of a FireCluster. To view a report, you select a device and a date range, and choose whether to view an archived report, or an on-demand report.

1. *Open Report Manager and connect to a Report Server.*

*The Report Manager window appears.*



2. From the **Device** drop-down list, select a device, server, or FireCluster to report on.
3. From the **Generate** or **Generated** drop-down list, select a date range for the report.

For instructions to select to show reports for specific date and time ranges, see the *Specify a date range* section.

4. To select a report list, select the **Available Reports** or **On-Demand Reports** tab.

*The available reports appear for the report list you selected.*

## Specify a Date Range

To refine your report data, you can select to show reports for specific date and time ranges in one report list.

1. From the **Generate** or **Generated** drop-down list, select **Specify a range**.

Or, select **Edit > Specify a range**.

*The Specify a range dialog box appears.*

**Specify a range**

Specify the start date and time, and the end date and time.

**Start:**

January 2009

Sun	Mon	Tue	Wed	Thu	Fri	Sat
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Hour: 0 2 4 6 8 10 12 14 16 18 20 22

Minute: 0 5 10 15 20 25 30 35 40 45 50 55

**End:**

February 2009

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

Hour: 0 2 4 6 8 10 12 14 16 18 20 22

Minute: 0 5 10 15 20 25 30 35 40 45 50 55

**OK** **Cancel**

2. In the **Start** section, select a start date and time.
3. In the **End** section, select an end date and time .
4. Click **OK**.

*The range appears in the Generate or Generated drop-down list.*


**Note** Specified date ranges cannot be saved from session to session. When you close Report Manager, all of the ranges you specified disappear.



---

## Modify a Date Range

You can change the date and time parameters selected for a date range.

1. From the **Generate** or **Generated** drop-down list, select the date range you want to modify.
2. Click .
3. Change the start and end date, and time selections.
4. Click **OK**.

*The Specify a range dialog box appears.*

*The updated range appears in the Generate or Generated drop-down list.*

## Select Reports to Generate

From Report Manager, after you connect to a Report Server and select the device and time period for your report, you can select which types of reports to include when you generate WatchGuard Reports. The reports that appear are populated based on your configuration settings for logging on your devices and servers, and the events that occur at your device. If you selected to log data for a report type, and that type of event occurred at your device, it is included in the list. If you do not see a particular report in the list, you can modify your configuration to collect log data for those reports.

For more information about how to select devices and the time period for your report, see *Select Report Parameters* on page 838.

For more information on logging settings, see *About Logging and Log Files* on page 683.

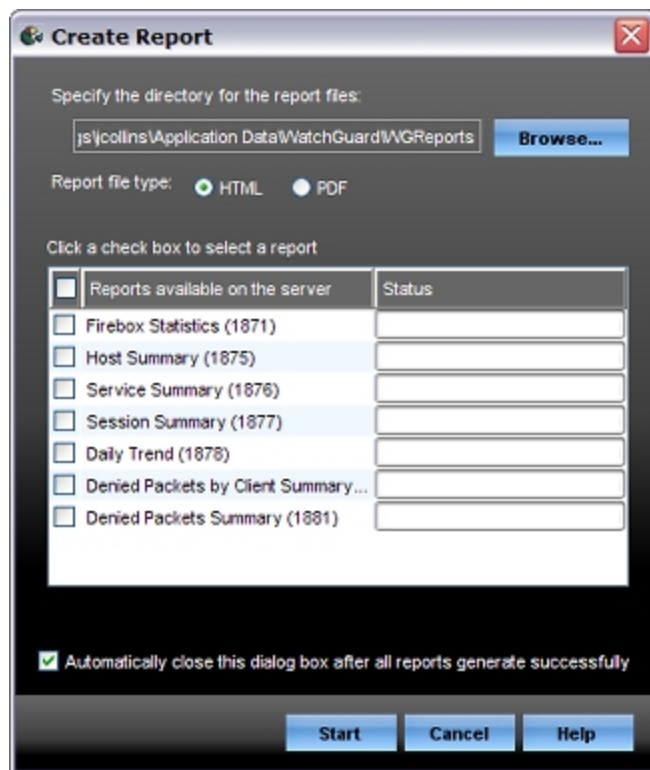
For more information on Log Server settings, see *Configure Logging Settings for the Log Server* on page 702.

For more information on Report Server configuration, see *Set Up the Report Server* on page 806.

## Generate Reports

1. Select **Edit > Create reports**.

*The Create Report dialog box appears.*



2. To change the directory where the report files are saved, click **Browse**.
3. Select the **Report file type**: **HTML** or **PDF**.  
*Report Manager automatically displays the reports in the format you select.*
4. Select the check boxes in the list for each report you want to generate.  
To select all reports in the list, select the **Reports available on the server** check box.
5. If you want the **Create Report** dialog box to remain open after all the reports have successfully generated, clear the **Automatically close this dialog box after all reports generate successfully** check box.
6. Click **Start**.  
*Report Manager generates the selected reports.*

## View a Report

After you have selected your report parameters, and selected which reports to generate, you can use Report Manager to view your reports. Reports are grouped by date and then by report type for all selected devices.



To view a report in Report Manager:

1. *Open Report Manager* and connect to your Report Server.
2. *Select Report Parameters* to choose a device and a date/time range for the report.
3. Select the **Available Reports** or **On-Demand Reports** tab.
4. In the **WatchGuard Reports** list, select a report.

*The Progress dialog box appears and then the selected report appears on the right. If you have selected to view reports in your default browser, the report opens in your browser window.*

Some reports include links to device data. If you selected a report with links to device data, click a link to see the data.

*The device data appears.*

5. To stop report generation, click .
  6. To refresh the selected report, click .
- Or, select **Edit > Update report list**.

For more information about report filter definition and selection, see *Filter Report Data* on page 846.


For more information about report parameter selection, see *Select Report Parameters* on page 838.

For more information about how to select a report to generate, see *Select Reports to Generate* on page 841.

For more information about the available reports, see *Predefined Reports List* on page 835.


## Find a Report in the List

You can use the Report Manager **Find** text box to find a specific report in the list.

1. Select a section of the reports to include in the search.  
*For example, to search all of the displayed reports, click WatchGuard Reports at the top of the list.*
2. In the **Find** text box at the bottom of Report Manager, type a phrase to find within the reports in the list.
3. Click .

Or, press **Enter** on your keyboard.

*If the phrase is included in the displayed reports, the first instance of the report in the list is highlighted, and the report appears.*

4. Click  again to search for more reports in the list.  
*If the phrase is not included in the displayed reports, "Phrase not found" appears below the Find field.*

## Find Details in a Report

You can use the **Find** dialog box to search for specific details in a report.

1. In the **WatchGuard Reports** list, select a report.  
*The report data appears.*
2. Press **Ctrl + F** on your keyboard.  
*The Find dialog box appears.*
3. In the **Find** text box, type a phrase to search on.
4. Select the check box for any additional search parameters. Options include **Case sensitive**, **Wrap Search**, and **Backward**.
5. Click **Find**.

## View Client Web Usage Reports

Client reports are one of many types of reports available on your Report Server as on-demand reports. They include information from proxy log messages about an authenticated user, host name, or an IP address for the device or group you select. There are two types of client reports: *Top Client* and *Per Client*.

### Run a Top Client Report

Log messages for Top Client reports include only IP address information. Because these log messages do not also include the host name and user name parameters, Top Client reports are divided into three selections:

- Top Client by IP address
- Top Client by Host name
- Top Client by Authenticated Users

To view a Top Client report in Report Manager:

1. *Open Report Manager* and connect to your Report Server.
2. From the **Device** drop-down list, select a device, server, or FireCluster.
3. From the **Generate** drop-down list, select a date range for the report.  
*For more information, see [Set Up WatchGuard Servers](#) on page 545.*
4. Select the **On-Demand Reports** tab.
5. In the **WatchGuard Reports** list, select **Top Client Report by [type of report]**.  
*The selected report appears.*

## Run a Per Client Report

The Per Client Report includes a detailed activity summary for the specified client on the device(s) and for the time range you select. You can choose one or more parameters to include in this report. Options include:

- User name or ID
- IP address
- Host name

You must also select a domain for the selected parameters.

To view a Per Client report in Report Manager:

1. *Open Report Manager* and connect to your Report Server.
2. In the **Device** drop-down list, select a device, server, or FireCluster.
3. In the **Generate** drop-down list, select a date range for the report.  
For more information, see *Set Up WatchGuard Servers* on page 545.
4. Select the **On-Demand Reports** tab.
5. In the **WatchGuard Reports** list, select **Per Client Web Activity Report**.

*The Per Client Report Configuration dialog box appears.*

6. Type the **User Name**, **IP Address**, and/or **Host Name** you want to include in the report.
7. In the **Domain** drop-down list, select the authentication server for the domain.
8. Click **OK**.

*A report appears with the information you specified.*

After you select parameters for a Per Client report, you can click the drop-down list to select the same parameter for another report. When you close Report Manager, the parameter history is automatically deleted. You can also manually delete the history.

In the **Per Client Report Configuration** dialog box:

1. Click the drop-down list for the parameter history you want to delete.
2. Select **Clear history**.

*The history is deleted for the selected parameter.*

## Filter Report Data

You can create filters to refine the information included in your reports. The data categories you define for each filter can be combined to give you flexibility in what you see in your reports. When you close Report Manager, your filters are saved, so you can apply them to future reports. You can also modify the values you assign to your filters to change the details you see in your report data. Filters are not available for all reports.

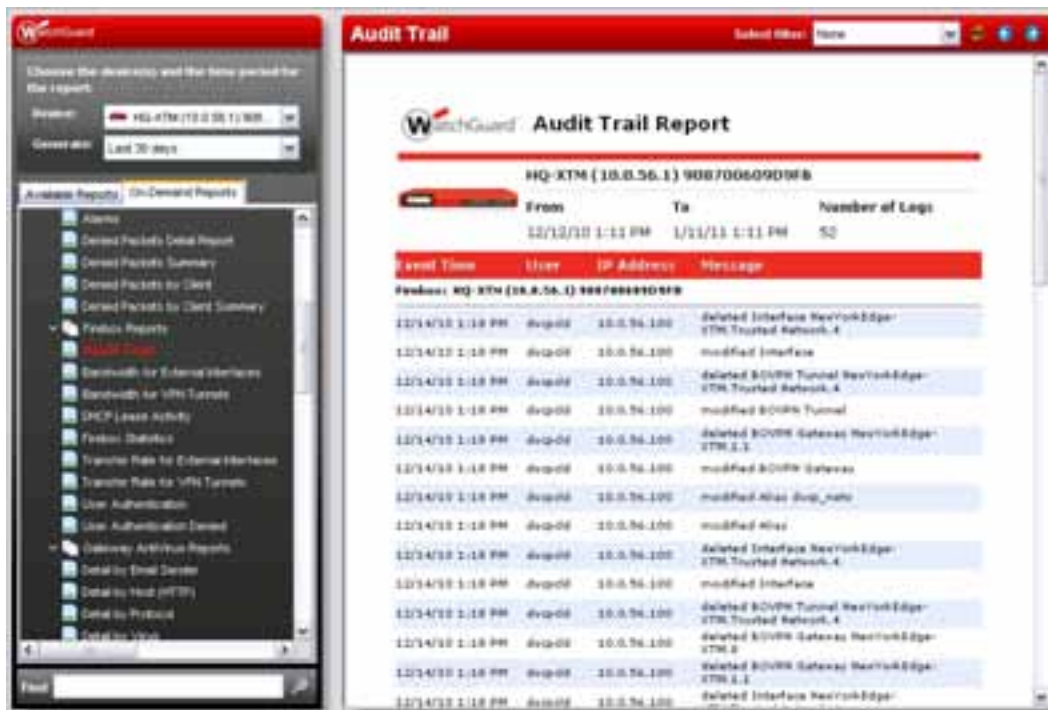
For a list of reports that you can filter, see *Reports You Can Filter*.

You can only filter report data when you view reports in Report Manager. If you view your reports in a web browser, you cannot filter report data.

## Define a Filter

You can define a filter in Report Manager after you select a report.

1. *Select Report Parameters and View a Report.*  
The report appears.



2. From the **Select filter** drop-down list, select **Define a filter**.  
The *Define a filter* dialog box appears.

The 'Define a filter' dialog box features a 'Name' text field at the top. Below it is a 'Filter categories' section with a table containing a 'Data category' column and a 'Values' column. To the right of the table are 'Add', 'Edit', and 'Delete' buttons. The 'Match rule' section has two radio buttons: 'Any data from the selected categories (OR)' (selected) and 'All data from the selected categories (AND)'. The 'Report content' section has two radio buttons: 'Include all records that match the selected categories' (selected) and 'Exclude all records that match the selected categories'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

3. In the **Name** text box, type a name for the filter.
4. To create a data category for the filter, click **Add**.  
*The Define a filter category dialog box appears.*

The 'Define a filter category' dialog box has a 'Data category' dropdown menu set to 'Source IP/Host Name'. Below it is a 'Values' section with a text area and 'Add', 'Delete', 'Up', and 'Down' buttons. The 'Match rule' section has two radio buttons: 'Any data from the specified values (OR)' and 'All data from the specified values (AND)' (selected). At the bottom are 'OK', 'Cancel', and 'Help' buttons.

5. From the **Data category** drop-down list, select an option:

*Source IP/Host Name*

The source IP address or host name included in the log entry.

*Port Number*

The source or destination port included in the log entry.

*User Name*

The user name included in the log entry. The value for this category is not case-sensitive.

*Destination IP/Host Name*

The destination IP address or host name included in the log entry.

6. In the **Values** text box, type a value for the data category.
7. Click **Add**.  
*The value appears in the Values window.*
8. From the **Match rule** section, select an option for the filter category.
9. Click **OK**.  
*The filter category appears in the Filter categories list.*
10. From the **Match rule** section, select an option for the filter.
11. From the **Report content** section, select whether to include or exclude the filtered content.
12. Click **OK**.  
*The filter appears in the Select filter drop-down list.*

## Apply or Remove a Filter

You can only apply a filter to certain reports. For more information, see *Reports You Can Filter* on page 850.

To apply a filter to a report:

1. In the **WatchGuard Reports** tree, select a report.
2. From the **Select filter** drop-down list, select a filter or *Define a Filter*.


If a filter is applied to a report and you select a different report from the **WatchGuard Reports** list, the same filter is automatically applied to the new report you select. You can apply a different filter to the report or remove all filters from the report.

To remove filters from a report:

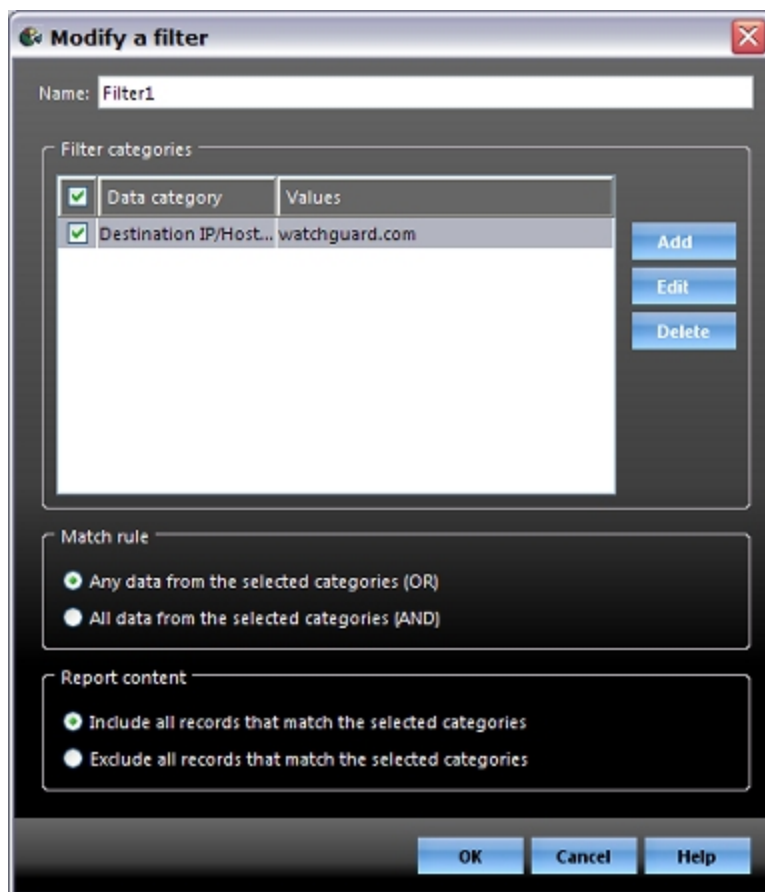
From the **Select filter** drop-down list, select **None**.  
*Unfiltered report data appears in the selected report.*

## Modify a Filter

You can change any of the filter details after you create it.

1. From the **Select filter** drop-down list, select the filter you want to change.
  2. Click .
- The Modify a filter dialog box appears.*





3. To create another data category for the filter, click **Add**.  
*The Define a filter category dialog box appears.*
4. Complete all of the necessary fields and click **OK**.
5. To change a data category, select the category and click **Edit**.  
*The Modify a filter category dialog box appears.*
6. Make any necessary changes and click **OK**.
7. To change the name of the filter, in the **Name** text box, type a new name.
8. Make any changes to the **Match rule** and **Report content** sections.
9. Click **OK**.  
*The modified filter appears in the Select filter drop-down list.*

## Delete Filters

You can clear all the filters in the list, but you cannot delete one filter at a time.

1. From the **Select filters** drop-down list, select **Clear filters**.  
*A confirmation message appears.*
2. Click **OK**.  
*All filters are cleared from the list.*




## Reports You Can Filter

WatchGuard Reports includes an extensive list of reports. The filter in Report Manager is not available for all reports. You can only use the filter with these reports:

- Exceptions
  - Alarms
- Firebox Reports
  - Audit Trail
  - User Authentication
  - User Authentication Denied
- Gateway AntiVirus Reports
  - Detail by Email Sender
  - Detail by Host (HTTP)
  - Detail by Protocol
  - Detail by Virus
- Intrusion Preventions Service Reports
  - Detail by IP-spoofed packets
  - Detail by Protocol
  - Detail by Severity
  - Detail by Signature
  - Detail by Source IP
- Packet-Filter Summaries
  - Daily Trend
  - Service Summary
  - Session Summary
- Web Traffic Reports
  - URL Details by Client
  - URL Details by Domain
  - URL Details by Time
- WebBlocker Reports
  - WebBlocker by Category
  - WebBlocker by Client

## Select the Report Format

You can see your report in HTML or PDF format, or in your default web browser.

1. *View a Report.*
2. Select a format for your report:
  - To see the report in HTML format, click .
  - To see the report in PDF format, click .
  - To see the report in your default web browser, click .

**Note** *If your default web browser is not Internet Explorer or Firefox, you must select to view reports in your default web browser rather than in Report Manager.*

---

## Email, Print, or Save a Report

You can email, print, or save a report directly from Report Manager.

### Send a Report in Email

1. *View a Report.*

2. Click .

Or, select **File > Send to.**

*If the report is in HTML format, an email message opens with a link to the HTML file.*

*If the report is in PDF format, an email message opens with the selected file type attached.*

### Print a Report

1. *View a Report.*

2. Click .

Or, select **File > Print.**

3. If the report is in HTML format, the **Print** dialog box appears.

Select your print parameters and click **Print.**

*If the report is in PDF format, the report appears in a separate window.*

*Print from that application window.*

### Save a Report

1. *View a Report.*

2. Click .

Or, select **File > Save as.**

*The Save dialog box appears.*

3. Select a location, filename, and file type.

4. Click **Save.**

## Use the Web Services API to Retrieve Log and Report Data

With the Web Services API, you can export traffic and alarm messages from your log files, and all data from your Available and On-Demand reports. The Web Services API for Reporting provides a SOAP-based (Simple Object Access Protocol) interface you can use to extract WatchGuard Log Server and Report Server data. Third-party tools that are *Web Services-aware* can use this API to easily connect and extract your log and report file data to generate custom reports. When you generate custom reports, you can combine information from other sources with the extracted data to further customize your reports.

### Installation and Documentation

When you install the Log Server or Report Server, the Web Services Server, the WSDL (Web Services Description Language) file, and associated documentation are automatically installed.

For installation instructions, see *Install WatchGuard System Manager Software*.

The Web Services API files and documentation are installed in this location:

```
C:\Program Files\WatchGuard\wsm11\wsserver\wsdl
```

To use the Web Services API, you must have these files:

- `LogService.wsdl` — WSDL (Web Services Description Language) file
- `LogService.xsd` — Web Services API schema
- `LogService.html` — WSDL reference documentation
- `LogService-UserGuide.pdf` — A user guide for Web Services API for Reporting
- `LogServiceEclipse.pdf` — An interoperability example for Eclipse and Java

You can also search the WatchGuard [Knowledge Base](#) for examples of how you can use the Web Services API to generate reports with third-party tools.

# 24 Certificates and the Certificate Authority

---

## About Certificates

Certificates match the identity of a person or organization with a method for others to verify that identity and secure communications. They use an encryption method called a key pair, or two mathematically related numbers called the *private key* and the *public key*. A certificate includes both a statement of identity and a public key, and is signed by a private key.

The private key used to sign a certificate can be from the same key pair used to generate the certificate, or from a different key pair. If the private key is from the same key pair used to create the certificate, the result is called a *self-signed certificate*. If the private key is from a different key pair, the result is a regular *certificate*. Certificates with private keys that can be used to sign other certificates are called *CA (Certificate Authority) Certificates*. A certificate authority is an organization or application that signs and revokes certificates.

If your organization has a PKI (public key infrastructure) set up, you can sign certificates as a CA yourself. Most applications and devices automatically accept certificates from prominent, trusted CAs. Certificates that are not signed by prominent CAs, such as self-signed certificate are not automatically accepted by many servers or programs, and do not operate correctly with some Firewall XTM features.

## Use Multiple Certificates to Establish Trust

Several certificates can be used together to create a *chain of trust*. For example, the CA certificate at the start of the chain is from a prominent CA, and is used to sign another CA certificate for a smaller CA. That smaller CA can then sign another CA certificate used by your organization. Finally, your organization can use this CA certificate to sign another certificate for use with the HTTPS proxy content inspection feature. However, to use that final certificate at the end of the chain of trust, you must first import all of the certificates in the chain of trust in this order:

1. CA certificate from the prominent CA (as type "Other")
2. CA certificate from the smaller CA (as type "Other")
3. CA certificate from the organization (as type "Other")
4. Certificate used to re-encrypt HTTPS proxy content after inspection (as type "HTTPS Proxy Authority")

It could also be necessary to import all of these certificates on each client device so that the last certificate is also trusted by users.

For more information, see *Manage XTM Device Certificates* on page 862.

## How the XTM device Uses Certificates

Your XTM device can use certificates for several purposes:

- Management session data is secured with a certificate.
- BOVPN or Mobile VPN with IPSec tunnels can use certificates for authentication.
- When content inspection is enabled, the HTTPS-proxy uses a certificate to re-encrypt incoming HTTPS traffic after it is decrypted for inspection.
- You can use a certificate with the HTTPS-proxy to protect a web server on your network.
- When a user authenticates with the XTM device for any purpose, such as a WebBlocker override, the connection is secured with a certificate.
- When RADIUS or Firebox authentication is configured to use WPA Enterprise or WPA2 Enterprise authentication methods.

By default, your XTM device creates self-signed certificates to secure management session data and authentication attempts for Fireware XTM Web UI and for HTTPS proxy content inspection. To make sure the certificate used for HTTPS content inspection is unique, its name includes the serial number of your device and the time at which the certificate was created. Because these certificates are not signed by a trusted CA, users on your network see warnings in their web browsers.

You have three options to remove this warning:

1. You can import certificates that are signed by a CA your organization trusts, such as a PKI you have already set up for your organization, for use with these features. We recommend that you use this option if possible.
2. You can create a custom, self-signed certificate that matches the name and location of your organization.
3. You can use the default, self-signed certificate.

For the second and third options, you can ask network clients to accept these self-signed certificates manually when they connect to the XTM device. Or, you can export the certificates and distribute them with network management tools. You must have WatchGuard System Manager installed to export certificates.

## Certificate Lifetimes and CRLs

Each certificate has a set lifetime when it is created. When the certificate reaches the end of that set lifetime, the certificate expires and can no longer be used automatically. You can also remove certificates manually with Firebox System Manager (FSM).

Sometimes, certificates are *revoked*, or disabled before their lifetime expiration, by the CA. Your XTM device keeps a current list of these revoked certificates, called the Certificate Revocation List (CRL), to verify that certificates used for VPN authentication are valid. If you have WatchGuard System Manager installed, this list can be updated manually with Firebox System Manager (FSM), or automatically with information from a certificate. Each certificate includes a unique number used to identify the certificate. If the unique number on a Web Server, BOVPN, or Mobile VPN with IPSec certificate matches an identifier from its associated CRL, the XTM device disables the certificate.

When content inspection is enabled on an HTTPS proxy, the XTM device can check the OCSP (Online Certificate Status Protocol) responder associated with the certificates used to sign the HTTPS content. The OCSP responder sends the revocation status of the certificate. The XTM device accepts the OCSP response if the response is signed by a certificate the XTM device trusts. If the OCSP response is not signed by a certificate the XTM device trusts, or if the OCSP responder does not send a response, then you can configure the XTM device to accept or reject the original certificate.

For more information about OCSP options, see *HTTPS-Proxy: Content Inspection* on page 463.

## Certificate Authorities and Signing Requests

To create a self-signed certificate, you put part of a cryptographic key pair in a certificate signing request (CSR) and send the request to a CA. It is important that you use a new key pair for each CSR you create. The CA issues a certificate after they receive the CSR and verify your identity. If you have FSM or Management Server software installed, you can use these programs to create a CSR for your XTM device. You can also use other tools, such as OpenSSL or the Microsoft CA Server that comes with most Windows Server operating systems.

If you want to create a certificate for use with the HTTPS proxy content inspection feature, it must be a CA certificate that can re-sign other certificates. If you create a CSR with Firebox System Manager and have it signed by a prominent CA, it can be used as a CA certificate.

If you do not have a PKI set up in your organization, we recommend that you choose a prominent CA to sign the CSRs you use, except for the HTTPS proxy CA certificate. If a prominent CA signs your certificates, your certificates are automatically trusted by most users. WatchGuard has tested certificates signed by VeriSign, Microsoft CA Server, Entrust, and RSA KEON. You can also import additional certificates so that your XTM device trusts other CAs.

For a complete list of automatically trusted CAs, see *Certificate Authorities Trusted by the XTM Device* on page 857.

In WatchGuard System Manager, the Management Server also operates as a CA. The CA gives certificates to managed XTM devices when they contact the Management Server to receive configuration updates.

For more information, see *Configure the Certificate Authority on the Management Server* on page 560.



## Certificate Authorities Trusted by the XTM Device

By default, your XTM device trusts most of the same certificate authorities (CAs) as modern web browsers. We recommend that you import certificates signed by a CA on this list for the HTTPS proxy or Firewall XTM Web UI, so that users do not see certificate warnings in their web browser when they use those features. However, you can also import certificates from other CAs so that your certificates are trusted.

If you have installed WatchGuard System Manager, a copy of each certificate is stored on your hard drive at:

C:\Documents and Settings\WatchGuard\wgauth\certs\README

## Certificate Authority List

C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certification Authority - G2, OU=(c) 1998 VeriSign, Inc. - For authorized use only, OU=VeriSign Trust Network  
 C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting, OU=Certification Services Division, CN=Thawte Personal Premium CA/emailAddress=personal-premium@thawte.com  
 C=ES, L=C/ Muntaner 244 Barcelona, CN=Autoridad de Certificacion Firmaprofesional CIF A62634068/emailAddress=ca@firmaprofesional.com  
 C=HU, ST=Hungary, L=Budapest, O=NetLock Halozatbiztonsagi Kft., OU=Tanusitvanykiadok, CN=NetLock Kozjegyzoi (Class A) Tanusitvanykiado  
 C=ZA, ST=Western Cape, L=Durbanville, O=Thawte, OU=Thawte Certification, CN=Thawte Timestamping CA  
 C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 1999 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 4 Public Primary Certification Authority - G3  
 C=SE, O=AddTrust AB, OU=AddTrust TTP Network, CN=AddTrust Qualified CA Root  
 C=DK, O=TDC Internet, OU=TDC Internet Root CA  
 C=US, O=VeriSign, Inc., OU=Class 2 Public Primary Certification Authority - G2, OU=(c) 1998 VeriSign, Inc. - For authorized use only, OU=VeriSign Trust Network  
 C=US, O=Wells Fargo, OU=Wells Fargo Certification Authority, CN=Wells Fargo Root Certificate Authority  
 OU=GlobalSign Root CA - R2, O=GlobalSign, CN=GlobalSign  
 CN=Test-Only Certificate  
 C=US, O=Entrust, Inc., OU=www.entrust.net/CPS is incorporated by reference, OU=(c) 2006 Entrust, Inc., CN=Entrust Root Certification Authority  
 C=SE, O=AddTrust AB, OU=AddTrust TTP Network, CN=AddTrust Class 1 CA Root  
 C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO Certification Authority  
 O=RSA Security Inc, OU=RSA Security 2048 V3  
 C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting, OU=Certification Services Division, CN=Thawte Personal Basic CA/emailAddress=personal-basic@thawte.com  
 C=FI, O=Sonera, CN=Sonera Class1 CA  
 O=VeriSign Trust Network, OU=VeriSign, Inc., OU=VeriSign International Server CA - Class 3, OU=www.verisign.com/CPS Incorpor.by Ref. LIABILITY LTD.(c)97 VeriSign  
 C=ZA, O=Thawte Consulting (Pty) Ltd., CN=Thawte SGC CA  
 C=US, O=Equifax Secure Inc., CN=Equifax Secure eBusiness CA-1

C=JP, O=SECOM Trust.net, OU=Security Communication RootCA1  
 C=US, O=America Online Inc., CN=America Online Root Certification Authority 1  
 C=HU, L=Budapest, O=NetLock Halozatbiztonsagi Kft., OU=Tanusitvanykiadok,  
 CN=NetLock Uzleti (Class B) Tanusitvanykiado  
 C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network,  
 OU=http://www.usertrust.com, CN=UTN - DATACorp SGC  
 C=BE, O=GlobalSign nv-sa, OU=Root CA, CN=GlobalSign Root CA  
 C=US, O=VeriSign, Inc., OU=Class 2 Public Primary Certification Authority  
 C=CH, O=SwissSign AG, CN=SwissSign Gold CA - G2  
 C=US, O=RSA Data Security, Inc., OU=Secure Server Certification Authority  
 C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root  
 C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 1999 VeriSign, Inc.  
 - For authorized use only, CN=VeriSign Class 3 Public Primary Certification  
 Authority - G3  
 C=US, OU=www.xrampsecurity.com, O=XRamp Security Services Inc, CN=XRamp  
 Global Certification Authority  
 C=PL, O=Unizeto Sp. z o.o., CN=Certum CA  
 C=US, O=Entrust.net, OU=www.entrust.net/CPS incorp. by ref. (limits liab.),  
 OU=(c) 1999 Entrust.net Limited, CN=Entrust.net Secure Server Certification  
 Authority  
 L=ValiCert Validation Network, O=ValiCert, Inc., OU=ValiCert Class 3 Policy  
 Validation Authority,  
 CN=http://www.valicert.com//emailAddress=info@valicert.com  
 C=CH, O=SwissSign AG, CN=SwissSign Platinum CA - G2  
 OU=GlobalSign Root CA - R2, O=GlobalSign, CN=GlobalSign  
 O=Digital Signature Trust Co., CN=DST Root CA X3  
 C=US, O=AOL Time Warner Inc., OU=America Online Inc., CN=AOL Time Warner Root  
 Certification Authority 1  
 C=GB, ST=Greater Manchester, L=Salford, O=Comodo CA Limited, CN=Secure  
 Certificate Services  
 O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at  
 https://www.verisign.com/rpa (c)00, CN=VeriSign Time Stamping Authority CA  
 O=Entrust.net, OU=www.entrust.net/GCCA\_CPS incorp. by ref. (limits liab.),  
 OU=(c) 2000 Entrust.net Limited, CN=Entrust.net Client Certification  
 Authority  
 C=US, O=SecureTrust Corporation, CN=Secure Global CA  
 C=US, O=Equifax, OU=Equifax Secure Certificate Authority  
 O=beTRUSTed, OU=beTRUSTed Root CAs, CN=beTRUSTed Root CA - RSA Implementation  
 C=WW, O=beTRUSTed, CN=beTRUSTed Root CAs, CN=beTRUSTed Root CA  
 C=US, O=GeoTrust Inc., CN=GeoTrust Primary Certification Authority  
 C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certification Authority  
 C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification  
 Services Division, CN=Thawte Premium Server CA/emailAddress=premium-  
 server@thawte.com  
 C=US, O=SecureTrust Corporation, CN=SecureTrust CA  
 OU=Extended Validation CA, O=GlobalSign, CN=GlobalSign Extended Validation CA  
 C=US, O=GeoTrust Inc., CN=GeoTrust Global CA 2  
 C=NL, O=Staat der Nederlanden, CN=Staat der Nederlanden Root CA  
 C=IL, ST=Israel, L=Eilat, O=StartCom Ltd., OU=CA Authority Dep., CN=Free SSL  
 Certification Authority/emailAddress=admin@startcom.org  
 C=US, O=VISA, OU=Visa International Service Association, CN=Visa eCommerce  
 Root  
 O=beTRUSTed, OU=beTRUSTed Root CAs, CN=beTRUSTed Root CA - Entrust

## Implementation

C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc.  
- For authorized use only, CN=VeriSign Class 3 Public Primary Certification  
Authority - G5

C=US, O=Equifax Secure Inc., CN=Equifax Secure Global eBusiness CA-1

C=ES, ST=Barcelona, L=Barcelona, O=IPS Internet publishing Services s.l.,  
O=ips@mail.ips.es C.I.F. B-60929452, OU=IPS CA Chained CAs Certification  
Authority, CN=IPS CA Chained CAs Certification  
Authority/emailAddress=ips@mail.ips.es

DC=com, DC=microsoft, DC=corp, DC=redmond, CN=Microsoft Secure Server  
Authority

C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network,  
OU=http://www.usertrust.com, CN=UTN-USERFirst-Hardware

C=BM, O=QuoVadis Limited, CN=QuoVadis Root CA 3

C=TW, O=Government Root Certification Authority

C=GB, ST=Greater Manchester, L=Salford, O=Comodo CA Limited, CN=Trusted  
Certificate Services

C=US, O=GeoTrust Inc., CN=GeoTrust Universal CA 2

C=US, O=Entrust.net, OU=www.entrust.net/Client\_CA\_Info/CPS incorp. by ref.  
limits liab., OU=(c) 1999 Entrust.net Limited, CN=Entrust.net Client  
Certification Authority

C=FR, O=Certplus, CN=Class 2 Primary CA

C=US, O=Starfield Technologies, Inc., OU=Starfield Class 2 Certification  
Authority

C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting, OU=Certification  
Services Division, CN=Thawte Personal Freemail CA/emailAddress=personal-  
freemail@thawte.com

O=Entrust.net, OU=www.entrust.net/CPS\_2048 incorp. by ref. (limits liab.),  
OU=(c) 1999 Entrust.net Limited, CN=Entrust.net Certification Authority  
(2048)

C=ES, ST=Barcelona, L=Barcelona, O=IPS Internet publishing Services s.l.,  
O=ips@mail.ips.es C.I.F. B-60929452, OU=IPS CA CLASEA1 Certification  
Authority, CN=IPS CA CLASEA1 Certification  
Authority/emailAddress=ips@mail.ips.es

C=US, O=AOL Time Warner Inc., OU=America Online Inc., CN=AOL Time Warner Root  
Certification Authority 2

C=US, O=VeriSign, Inc., OU=Class 1 Public Primary Certification Authority -  
G2, OU=(c) 1998 VeriSign, Inc. - For authorized use only, OU=VeriSign Trust  
Network

C=US, O=VISA, OU=Visa International Service Association, CN=GP Root 2

C=US, O=GeoTrust Inc., CN=GeoTrust Global CA

C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at  
<https://www.verisign.com/rpa> (c)06, CN=VeriSign Class 3 Extended Validation  
SSL CA

C=EU, O=AC Camerfirma SA CIF A82743287, OU=http://www.chambersign.org,  
CN=Global Chambersign Root

C=DE, ST=Hamburg, L=Hamburg, O=TC TrustCenter for Security in Data Networks  
GmbH, OU=TC TrustCenter Class 2 CA/emailAddress=certificate@trustcenter.de

C=US, O=GTE Corporation, OU=GTE CyberTrust Solutions, Inc., CN=GTE CyberTrust  
Global Root

C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at  
<https://www.verisign.com/rpa> (c)05, CN=VeriSign Class 3 Secure Server CA

C=US, O=GTE Corporation, CN=GTE CyberTrust Root

C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 1999 VeriSign, Inc.  
- For authorized use only, CN=VeriSign Class 1 Public Primary Certification  
Authority - G3  
C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network,  
OU=http://www.usertrust.com, CN=UTN-USERFirst-Network Applications  
C=HU, L=Budapest, O=NetLock Halozatbiztonsagi Kft., OU=Tanusitvanykiadok,  
CN=NetLock Minositett Kozjegyzoi (Class QA)  
Tanusitvanykiado/emailAddress=info@netlock.hu  
C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 1999 VeriSign, Inc.  
- For authorized use only, CN=VeriSign Class 2 Public Primary Certification  
Authority - G3  
C=us, ST=Utah, L=Salt Lake City, O=Digital Signature Trust Co., OU=DSTCA X2,  
CN=DST RootCA X2/emailAddress=ca@digsigtrust.com  
C=ES, ST=Barcelona, L=Barcelona, O=IPS Internet publishing Services s.l.,  
O=ips@mail.ips.es C.I.F. B-60929452, OU=IPS CA CLASE3 Certification  
Authority, CN=IPS CA CLASE3 Certification  
Authority/emailAddress=ips@mail.ips.es  
O=RSA Security Inc, OU=RSA Security 1024 V3  
C=US, O=Equifax Secure, OU=Equifax Secure eBusiness CA-2  
C=US, O=thawte, Inc., OU=Certification Services Division, OU=(c) 2006 thawte,  
Inc. - For authorized use only, CN=thawte Primary Root CA  
C=us, ST=Utah, L=Salt Lake City, O=Digital Signature Trust Co., OU=DSTCA X1,  
CN=DST RootCA X1/emailAddress=ca@digsigtrust.com  
C=US, O=Network Solutions L.L.C., CN=Network Solutions Certificate Authority  
C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification  
Services Division, CN=Thawte Server CA/emailAddress=server-certs@thawte.com  
C=US, O=VeriSign, Inc., OU=Class 4 Public Primary Certification Authority -  
G2, OU=(c) 1998 VeriSign, Inc. - For authorized use only, OU=VeriSign Trust  
Network  
C=NL, O=DigiNotar, CN=DigiNotar Root CA/emailAddress=info@diginotar.nl  
C=US, O=America Online Inc., CN=America Online Root Certification Authority 2  
C=ES, ST=Barcelona, L=Barcelona, O=IPS Internet publishing Services s.l.,  
O=ips@mail.ips.es C.I.F. B-60929452, OU=IPS CA Timestamping Certification  
Authority, CN=IPS CA Timestamping Certification  
Authority/emailAddress=ips@mail.ips.es  
C=US, O=DigiCert Inc., CN=DigiCert Security Services CA  
C=US, O=Digital Signature Trust, OU=DST ACES, CN=DST ACES CA X6  
C=DK, O=TDC, CN=TDC OCES CA  
C=US, O=VeriSign, Inc., OU=Class 1 Public Primary Certification Authority  
C=ES, ST=Barcelona, L=Barcelona, O=IPS Internet publishing Services s.l.,  
O=ips@mail.ips.es C.I.F. B-60929452, OU=IPS CA CLASEA3 Certification  
Authority, CN=IPS CA CLASEA3 Certification  
Authority/emailAddress=ips@mail.ips.es  
C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network,  
OU=http://www.usertrust.com, CN=UTN-USERFirst-Client Authentication and Email  
C=GB, ST=Greater Manchester, L=Salford, O=Comodo CA Limited, CN=AAA  
Certificate Services  
L=ValiCert Validation Network, O=ValiCert, Inc., OU=ValiCert Class 1 Policy  
Validation Authority,  
CN=http://www.valicert.com//emailAddress=info@valicert.com  
C=ES, ST=Barcelona, L=Barcelona, O=IPS Internet publishing Services s.l.,  
O=ips@mail.ips.es C.I.F. B-60929452, OU=IPS CA CLASE1 Certification  
Authority, CN=IPS CA CLASE1 Certification

Authority/emailAddress=ips@mail.ips.es  
 C=BM, O=QuoVadis Limited, OU=Root Certification Authority, CN=QuoVadis Root Certification Authority  
 C=US, O=Network Solutions L.L.C., CN=Network Solutions Certificate Authority  
 C=CH, O=SwissSign AG, CN=SwissSign Silver CA - G2  
 C=US, O=Digital Signature Trust Co., OU=DSTCA E2  
 C=US, O=Digital Signature Trust Co., OU=DSTCA E1  
 C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA  
 C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc.,  
 OU=http://certificates.godaddy.com/repository, CN=Go Daddy Secure Certification Authority/serialNumber=07969287  
 C=EU, O=AC Camerfirma SA CIF A82743287, OU=http://www.chambersign.org, CN=Chambers of Commerce Root  
 C=BM, O=QuoVadis Limited, CN=QuoVadis Root CA 2  
 C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert High Assurance EV Root CA  
 C=US, ST=DC, L=Washington, O=ABA.ECOM, INC., CN=ABA.ECOM Root CA/emailAddress=admin@digisigtrust.com  
 C=ES, ST=BARCELONA, L=BARCELONA, O=IPS Seguridad CA, OU=Certificaciones, CN=IPS SERVIDORES/emailAddress=ips@mail.ips.es  
 C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Assured ID Root CA  
 C=ch, O=Swisscom, OU=Digital Certificate Services, CN=Swisscom Root CA 1  
 CN=T\xC3\x9CRKTRUST Elektronik Sertifika Hizmet Sa\xC4\x9Flay\xC4\xB1c\xC4\xB1s\xC4\xB1, C=TR, L=ANKARA, O=(c) 2005  
 T\xC3\x9CRKTRUST Bilgi \xC4\xB0leti\xC5\x9Fim ve Bili\xC5\x9Fim G\xC3\xBCvenli\xC4\x9Fi Hizmetleri A.\xC5\x9E.  
 C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G5  
 C=DE, ST=Hamburg, L=Hamburg, O=TC TrustCenter for Security in Data Networks GmbH, OU=TC TrustCenter Class 3 CA/emailAddress=certificate@trustcenter.de  
 C=HU, L=Budapest, O=NetLock Halozatbiztonsagi Kft., OU=Tanusitvanykiadok, CN=NetLock Expressz (Class C) Tanusitvanykiado  
 C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN-USERFirst-Object  
 C=US, O=The Go Daddy Group, Inc., OU=Go Daddy Class 2 Certification Authority  
 C=US, O=Akamai Technologies Inc, CN=Akamai Subordinate CA 3  
 C=US, O=Network Solutions L.L.C., CN=Network Solutions Certificate Authority  
 C=SE, O=AddTrust AB, OU=AddTrust TTP Network, CN=AddTrust Public CA Root  
 CN=T\xC3\x9CRKTRUST Elektronik Sertifika Hizmet Sa\xC4\x9Flay\xC4\xB1c\xC4\xB1s\xC4\xB1, C=TR, L=Ankara, O=T\xC3\x9CRKTRUST Bilgi \xC4\xB0leti\xC5\x9Fim ve Bili\xC5\x9Fim G\xC3\xBCvenli\xC4\x9Fi Hizmetleri A.\xC5\x9E. (c) Kas\xC4\xB1m 2005  
 C=US, O=GeoTrust Inc., CN=GeoTrust Universal CA  
 C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)06, CN=VeriSign Class 3 Extended Validation SSL SGC CA  
 O=Entrust.net, OU=www.entrust.net/SSL\_CPS incorp. by ref. (limits liab.), OU=(c) 2000 Entrust.net Limited, CN=Entrust.net Secure Server Certification Authority  
 CN=Microsoft Internet Authority  
 L=ValiCert Validation Network, O=ValiCert, Inc., OU=ValiCert Class 2 Policy Validation Authority,

```
CN=http://www.valicert.com//emailAddress=info@valicert.com
C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network,
OU=http://www.usertrust.com, CN=UTN-USERFirst-Hardware
C=SE, O=AddTrust AB, OU=AddTrust External TTP Network, CN=AddTrust External
CA Root
C=FI, O=Sonera, CN=Sonera Class2 CA
O=beTRUSTed, OU=beTRUSTed Root CAs, CN=beTRUSTed Root CA-Baltimore
Implementation
C=IL, O=StartCom Ltd., OU=Secure Digital Certificate Signing, CN=StartCom
Certification Authority
```

## Manage XTM Device Certificates

In Firebox System Manager, you can:

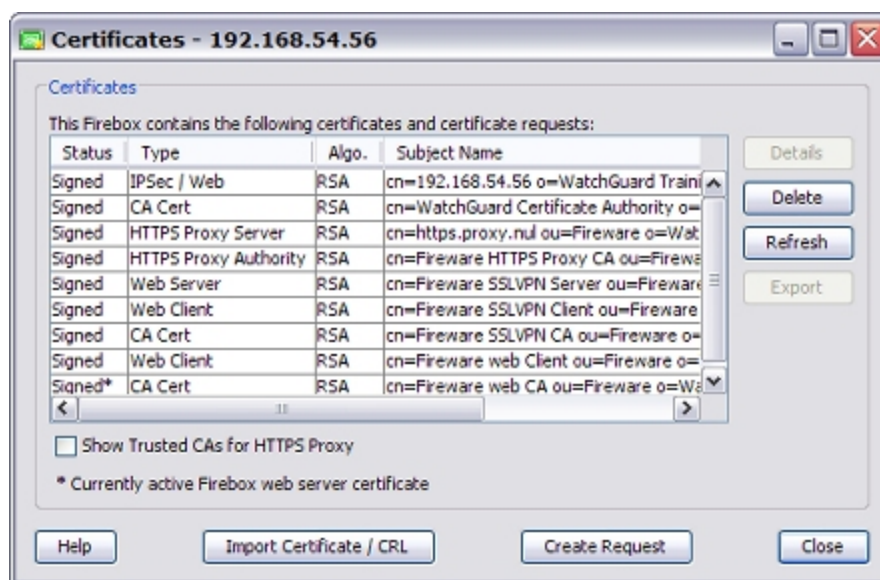
- See a list of the current XTM device certificates and their properties.
- Remove a certificate from the XTM device.
- Create a certificate signing request (CSR).
- Import a certificate or CRL (certificate revocation list).
- Export a certificate for resigning or distribution.

## See Current Certificates

To see the current list of certificates:

1. Open Firebox System Manager.
2. Select **View > Certificates**.

*The Certificates dialog box appears.*



In this dialog box, you can see a list of all certificates and certificate signing requests (CSRs). The list includes:

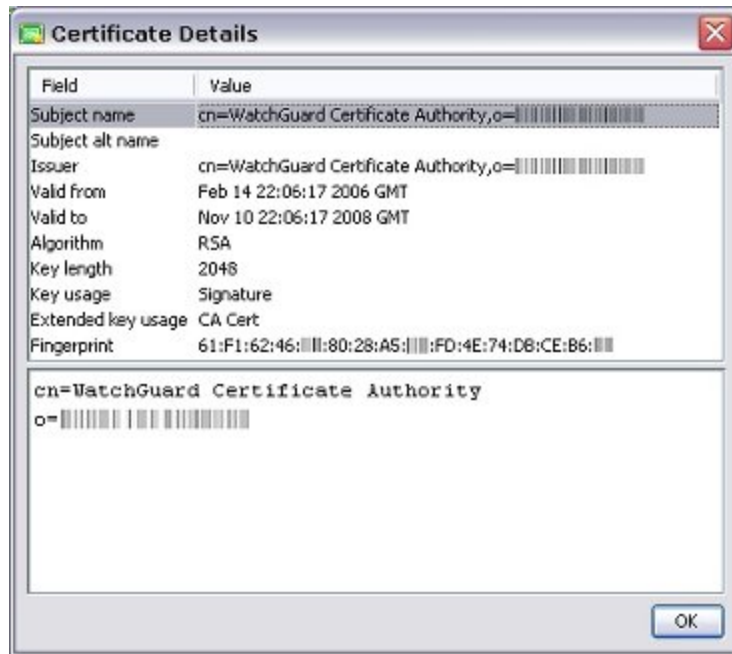
- The status and type of the certificate.
- The algorithm used by the certificate.

- The subject name or identifier of the certificate.

By default, trusted CA certificates do not appear in this list. You can choose to show all of the certificates from trusted CAs.

3. To show all of the certificates from trusted CAs, select the **Show Trusted CAs for HTTPS Proxy** check box.
4. To hide the trusted CA certificates again, clear the **Show Trusted CAs for HTTPS Proxy** check box.
5. To see additional information on a certificate in the list, select the certificate and click **Details**.

*The Certificate Details dialog box appears with information about which CA signed the certificate and the certificate fingerprint. You can use this information to troubleshoot or uniquely identify certificates.*



## Delete a Certificate

When you delete a certificate, it can no longer be used for authentication. If you delete one of the automatically generated certificates, such as the self-signed certificate used by default for the HTTPS proxy, your XTM device creates a new self-signed certificate for this purpose the next time it reboots. The XTM device does not create a new self-signed certificate automatically if you have imported a different certificate.

To remove a certificate from the XTM device:

1. Select the certificate in the **Certificates** dialog box.
2. Click **Delete**.
3. Type the XTM device configuration (read/write) passphrase.
4. Click **OK**.

*The Certificate is deleted.*

## Import a CRL from a File

You can import a certificate revocation list (CRL) that you have previously downloaded from your local computer. CRLs are used only to verify the status of certificates used for VPN authentication.

1. Select **View > Certificates**.  
*The Certificates dialog box appears.*
2. Click **Import Certificate/CRL**.
3. Click the **Import a CRL** tab.



4. Click **Browse** to find the file.
5. Click **Import CRL**.  
*The Import CRL dialog box appears.*
6. Type the configuration passphrase.
7. Click **OK**.  
*The CRL you specified is appended to the CRL on your XTM device.*

## Import a Certificate from a File

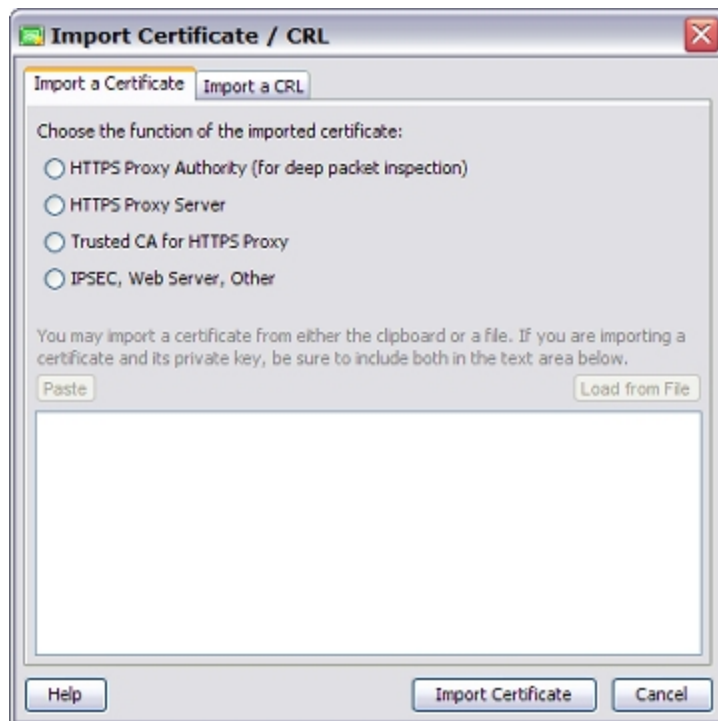
You can import a certificate from the Windows clipboard, or from a file on your local computer. Certificates must be in PEM (base64) format. Before you import a certificate to use with the HTTPS proxy content inspection feature, you must import each previous certificate in the chain of trust with the "Other" type so that the XTM device trusts the certificate. You must import these certificates from first to last, or from most prominent to least prominent, so that the XTM device can connect the certificates in the chain of trust properly.

For more information, see *About Certificates* on page 853 and *Use Certificates for the HTTPS-Proxy* on page 880.

1. Select **View > Certificates**.  
*The Certificates dialog box appears.*
2. Click **Import Certificate/CRL**.
3. Select the option that matches the function of the certificate:



- If the certificate is for an HTTPS proxy policy that manages web traffic requested by users on trusted or optional networks from a web server on an external network, select **HTTPS Proxy Authority (for deep packet inspection)**. A certificate you import for this purpose must be a CA certificate. Make sure you have imported the CA certificate used to sign this certificate with the "Other" category before you import the CA certificate used to re-encrypt traffic with an HTTPS proxy.
- If the certificate is for an HTTPS proxy policy that manages web traffic requested by users on an external network from a web server protected by the XTM device, select **HTTPS Proxy Server**. Make sure you have imported the CA certificate used to sign this certificate with the "Other" category before you import the CA certificate used to re-encrypt traffic from an HTTPS web server.
- For a certificate used to trust HTTPS traffic that is not re-encrypted by the HTTPS proxy, such as a root certificate or intermediate CA certificate used to sign the certificate of an external web server, select **Trusted CA for HTTPS Proxy**.
- If the certificate is for authentication or other purposes, select **IPSec, Web Server, Other**. Select this category if you want to import a certificate to create a chain of trust to a certificate used to re-encrypt network traffic with an HTTPS proxy.



4. Click **Paste** to paste the contents of the clipboard.  
Or, **Load from File** to select a file on your local computer that contains the certificate. If the file also includes a private key, type the password to decrypt the key.
5. Click **Import Certificate**.  
*The certificate is added to the XTM device.*

## Export a Certificate

You can export a certificate for resigning by a trusted CA, or for distribution to clients on your network.


1. Select **View > Certificates**.
2. Select a certificate and click **Export**.
3. Select a location and type a name for the certificate.

*The certificate is saved in PEM format.*

## Manage Management Server Certificates

You can manage and see a list of certificates on the Management Server. You usually use the web-based CA Manager to use this. You can also perform some of these functions from the WatchGuard System Manager window.

### Use the Web-Based CA Manager

1. Open WatchGuard System Manager.
2. Connect to the Management Server.  
*You must type the configuration passphrase to connect.*
3. Click the **Device Management** tab.
4. Click .  
Or, select **Tools > CA Manager**.

The web-based CA Manager has several web pages you can use to manage certificates:

- **Certificate Authority CA Certificate** — Shows the CA (root) certificate. You can save the certificate to a file or copy its contents to the Windows clipboard.
- **Management Server CA Certificate** — Shows the Management Server CA certificate. You can save the certificate to a file or copy its contents to the Windows clipboard.
- **Generate a New Certificate** — Select this option to create a new certificate request (CSR), as described in the *Create a certificate with CA Manager* section of *Create a Certificate with FSM or the Management Server* on page 869.
- **Find and Manage Certificates** — On this page, you can search for certificates by serial number, common name, or organizational unit. You can then view details for, revoke, reinstate, or destroy the certificates returned in the search results.
- **List and Manage Certificates** — To see the full certificate, click its number in the **Serial** column. This page shows detailed information about the certificate, such as its signature algorithm and issuer.
  - To change the status of one or more certificates, select the check box adjacent to each certificate. At the bottom of the page, select an action from the drop-down list and click **Go**.
  - When you revoke a certificate, it is added to the Certificate Revocation List (CRL) and cannot be used for authentication.
  - When you reinstate a certificate, it is removed from the CRL and can be used again. If you remove or destroy a certificate, it is not added to the CRL, but it cannot be used for authentication. The CRL is published to each XTM device when the XTM device connects to the Management Server.
- **Upload Certificate Request** — Use this page to sign a certificate request from a different device. Type in the common name and organizational unit used in the certificate, and then click **Browse** to find the CSR (Certificate Signing Request) file. When you are finished, click **Upload**.

- **Publish a Certificate Revocation List (CRL)** — This option makes the CRL available to each XTM device connected to the Management Server. When a managed XTM device next attempts to validate the certificate, the certificate is disabled. If a revoked certificate was used for VPN authentication, the VPN tunnel is disabled.

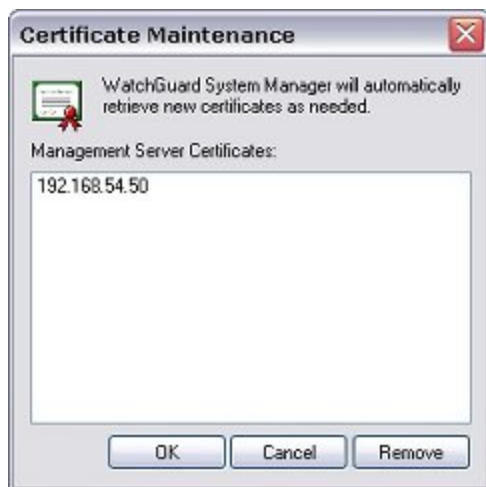
## Manage Certificates with WatchGuard System Manager

You can use WatchGuard System Manager to see certificates used by the Management Server and delete those that are no longer needed.

1. Open WatchGuard System Manager.
2. Connect to the Management Server.  
*You must type the configuration passphrase to connect.*

3. Select **File > Certificates**.

*The Certificate Maintenance dialog box appears with a list of the certificates used by WatchGuard System Manager. WatchGuard automatically gets the certificates it needs.*



4. To delete a certificate, select it and click **Remove**. If the certificate is currently used by the Management Server, you must first disconnect from the server before you delete the certificate.
5. Click **OK**.

**Note** *When you delete a Management Server certificate, you do not delete certificates in Microsoft Internet Explorer.*

# Create a Certificate with FSM or the Management Server

If you have not prepared a certificate, you can create a certificate signing request (CSR) from your XTM device with Firebox System Manager (FSM). You can also create a new certificate for a Mobile VPN with the built-in Certificate Authority (CA) Manager on your Management Server.

## Create a Certificate with FSM

1. Connect to your XTM device and open FSM.
2. Select **View > Certificates**.
3. Click **Create Request**.  
*The Certificate Request Wizard starts.*
4. Click **Next**.
5. Select the purpose of the completed certificate.
  - If the certificate is to be used to re-encrypt inspected content with an HTTPS proxy, select **HTTPS Proxy Authority**.
  - If the certificate is to be used to re-encrypt content for a protected web server with an HTTPS proxy, select **HTTPS Proxy Server**.
  - For all other uses, including VPN, XTM device, or Management Server authentication, select **IPSec, Device, Web Server, Other**.



6. Click **Next**.
7. Type your name, your department, the name of your company, and the city, state or province, and country you are working in. These entries are used to create the subject name.

8. Click **Next**.  
*The wizard creates a subject name based on what you entered in the previous screen.*
9. Type the appropriate information in the **DNS Name**, **IP Address**, and **User Domain Name** text boxes.

10. Click **Next**.
11. By default, the certificate uses RSA encryption, 1024-bit key length, and both encryption and signatures for key usage. Make any necessary changes to these settings. Click **Next**.  
*HTTPS proxy authority and HTTPS proxy server certificates do not have options for key usage.*




12. Click **Next**. Type the type the configuration passphrase.
13. Click **OK** to see the finished CSR.



14. Click **Copy** to copy the Certificate Signing Request to the Windows clipboard. You must send this CSR to a certificate authority for signature before you can use it with your XTM device. When you import the finished certificate, you must first import the CA certificate used to sign the new certificate with the "Other" category.
15. Click **Next**.
16. On the last screen of the wizard, you can:

- Click **Import Now** to import a certificate.  
*The Import Certificate/CRL dialog box appears.*  
For more information on how to use this dialog box, see *Manage XTM Device Certificates* on page 862.
- Click **Finish** to close the wizard.

## Create a Self-Signed Certificate with CA Manager

1. Open WatchGuard System Manager.
2. Connect to the Management Server.  
*You must type the configuration passphrase to connect.*
3. Click the **Device Management** tab for the Management Server.
4. Click .  
Or, select **Tools > CA Manager**.
5. Click **Generate a New Certificate**.
6. Type the common name, password, and certificate lifetime for the subject.
  - For Mobile VPN users, the common name must agree with the user name of the remote user.
  - For Firebox users, the common name must agree with the XTM device identifying information (normally, its IP address).
  - For a generic certificate, the common name is the name of the user.
7. If this certificate is for Mobile VPN users only, type the organizational unit for the subject. The organizational unit must appear in this format:  
GW: <vpn gateway name>  
If you do not know the VPN gateway name, use the value of config.watchguard.id in the configuration file of the gateway Firebox.
8. To download the certificate after it is generated, select the **Download Cert** check box.
9. Click **Generate**.



## Create a CSR with OpenSSL

To create a certificate, you first need to create a Certificate Signing Request (CSR). You can send the CSR to a certification authority, or use it to create a self-signed certificate.

### Use OpenSSL to Generate a CSR

OpenSSL is installed with most GNU/Linux distributions. To download the source code or a Windows binary file, go to <http://www.openssl.org/> and follow the installation instructions for your operating system. You can use OpenSSL to convert certificates and certificate signing requests from one format to another. For more information, see the OpenSSL man page or online documentation.

1. Open a command line interface terminal.
2. To generate a private key file called `privkey.pem` in your current working directory, type `openssl genrsa -out privkey.pem 1024`
3. Type `openssl req -new -key privkey.pem -out request.csr`  
*This command generates a CSR in the PEM format in your current working directory.*
4. When you are prompted for the x509 Common Name attribute information, type your fully-qualified domain name (FQDN). Use other information as appropriate.
5. Follow the instructions from your certificate authority to send the CSR.

To create a temporary, self-signed certificate until the CA returns your signed certificate:

1. Open a command line interface terminal.
2. Type:  
`openssl x509 -req -days 30 -in request.csr -key privkey.pem -out sscert.cert`

This command creates a certificate inside your current directory that expires in 30 days with the private key and CSR you created in the previous procedure.

**Note** *You cannot use a self-signed certificate for VPN remote gateway authentication. We recommend that you use certificates signed by a trusted Certificate Authority.*

## Sign a Certificate with Microsoft CA

Although you can create a self-signed certificate with Firebox System Manager or other tools, you can also create a certificate with the Microsoft Certificate Authority (CA).

Each certificate signing request (CSR) must be signed by a certificate authority (CA) before it can be used for authentication. When you create a certificate with this procedure, you act as the CA and digitally sign your own CSR. For compatibility reasons, however, we recommend that you instead send your CSR to a widely known CA. The root certificates for these organizations are installed by default with most major Internet browsers and XTM devices, so you do not have to distribute the root certificates yourself.

You can use most Windows Server operating systems to complete a CSR and create a certificate. The subsequent instructions are for Windows Server 2003.

## Send the Certificate Request

1. Open your web browser. In the location or address bar, type the IP address of the server where the Certification Authority is installed, followed by `certsrv`.  
For example: `http://10.0.2.80/certsrv`
2. Click the **Request a Certificate** link.
3. Click the **Advanced certificate request** link.
4. Click **Submit a certificate**.
5. Paste the contents of your CSR file into the **Saved Request** text box.
6. Click **OK**.
7. Close your web browser.

## Issue the Certificate

1. Connect to the server where the Certification Authority is installed, if necessary.
2. Select **Start > Control Panel > Administrative Tools > Certification Authority**.
3. In the **Certification Authority (Local)** tree, select **Your Domain Name > Pending Requests**.
4. Select the **CSR** in the right navigation pane.
5. In the **Action** menu, select **All Tasks > Issue**.
6. Close the Certification Authority window.

## Download the Certificate

1. Open your web browser. In the location or address bar, type the IP address of the server where the certification authority is installed, followed by `certsrv`.  
Example: `http://10.0.2.80/certsrv`
2. Click the **View the status of a pending certificate request** link.
3. Click the certificate request with the time and date you submitted.
4. To choose the PKCS10 or PKCS7 format, select **Base 64 encoded**.
5. Click **Download certificate** to save the certificate on your hard drive.

Certification Authority is distributed with Windows Server 2003 as a component. If the Certification Authority is not installed in the Administrative Tools folder of the Control Panel, follow the instructions from the manufacturer to install it.

# Use Certificates for Authentication

You can use certificates for:

- [Mobile VPN with IPsec tunnel authentication](#)
- [BOVPN tunnel authentication](#)

**Note** *Third-party or self-signed certificates cannot be used for Mobile VPN authentication.*

You can also *Configure the Web Server Certificate for Firebox Authentication*. The web server certificate is the certificate that the XTM device uses to secure HTTPS connections for management sessions, WebBlocker overrides, and other purposes.

When you perform any of these procedures, we recommend that you *Connect to an XTM Device* so Policy Manager can download the list of currently installed certificates. If you save changes from a local configuration file and the new settings do not match the certificates on the XTM device, your XTM device may not operate correctly.

## Certificates for Mobile VPN with IPsec Tunnel Authentication

When a Mobile VPN tunnel is created, the identity of each endpoint must be verified. This key can be a passphrase or pre-shared key (PSK) known by both endpoints, or a certificate from the Management Server. Your XTM device must be a managed device to use a certificate for Mobile VPN authentication.

From Policy Manager, you can configure a new Mobile VPN with IPsec tunnel to use certificates.

1. Select **VPN > Mobile VPN > IPsec**.  
*The Mobile VPN with IPsec Configuration dialog box appears.*
2. Click **Add**.  
*The Mobile VPN with IPsec Wizard appears.*
3. Click **Next**.
4. Complete the **Select a user authentication server** page. Click **Next**.
5. Select **Use an RSA certificate issued by your WatchGuard Management Server**.
6. Type the IP address and administration passphrase of your Management Server.
7. Finish the wizard.

From Policy Manager, you can configure an existing Mobile VPN tunnel to use certificates for authentication.

1. Select **VPN > Mobile VPN > IPsec**.
2. Select the Mobile VPN tunnel you want to change. Click **Edit**.
3. Click the **IPsec Tunnel** tab.
4. Select **Use a certificate**.
5. Type the **IP address** of the Management Server or certificate authority (CA). If necessary, adjust the connection timeout.
6. Click **OK**.

When you use certificates, you must give each Mobile VPN user three files:

- The end-user profile (.wgx)
- The client certificate (.p12)
- The CA root certificate (.pem)

When a Mobile VPN user opens the .wgx file, the root and client certificates in the cacert.pem and the .p12 files are automatically loaded.

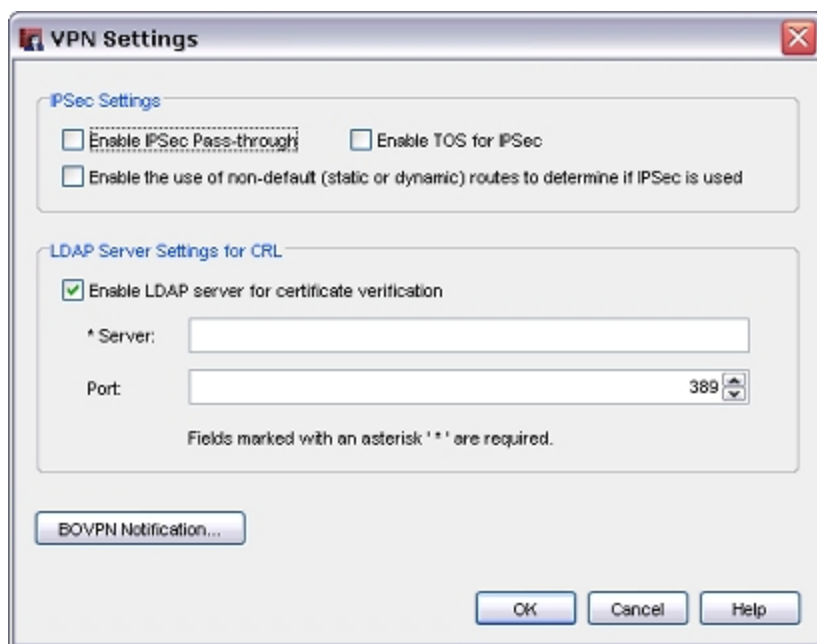
For more information on Mobile VPN with IPsec, see *About Mobile VPN with IPsec* on page 987.

## Verify VPN Certificates with an LDAP Server

You can use an LDAP server to automatically verify certificates used for VPN authentication if you have access to the server. You must have LDAP account information provided by a third-party CA service to use this feature.

1. From Policy Manager, select **VPN > VPN Settings**.

*The VPN Settings dialog box appears.*



2. Select the **Enable LDAP server for certificate verification** check box.
3. In the **Server** text box, type the name or IP address of the LDAP server.
4. (Optional) Type or select the **Port** number.
5. Click **OK**.

*Your XTM device checks the CRL stored on the LDAP server when tunnel authentication is requested.*

## Certificates for Branch Office VPN (BOVPN) Tunnel Authentication

When a BOVPN tunnel is created, the IPsec protocol checks the identity of each endpoint with either a pre-shared key (PSK) or a certificate imported and stored on the XTM device.

To use a certificate for BOVPN tunnel authentication:

1. Select **VPN > Branch Office Gateways**.
2. Click **Add** to create a new gateway.  
Or, select an existing gateway and click **Edit**.

3. Select **Use IPSec Firebox Certificate**.
4. Select the certificate you want to use.
5. Set other parameters as necessary.
6. Click **OK**.

If you use a certificate for BOVPN authentication:

- You must first import the certificate.  
For more information, see *Manage XTM Device Certificates* on page 862.
- Firebox System Manager must recognize the certificate as an IPSec-type certificate.
- Make sure certificates for the devices at each gateway endpoint use the same algorithm. Both endpoints must use either DSS or RSA. The algorithm for certificates appears in the table in the **New Gateway** dialog box in WatchGuard System Manager, and in the **Certificates** dialog box in Firebox System Manager.
- If you do not have a third-party or self-signed certificate, you must use the certificate authority on a WatchGuard Management Server.  
For more information, see *Configure the Certificate Authority on the Management Server* on page 560.

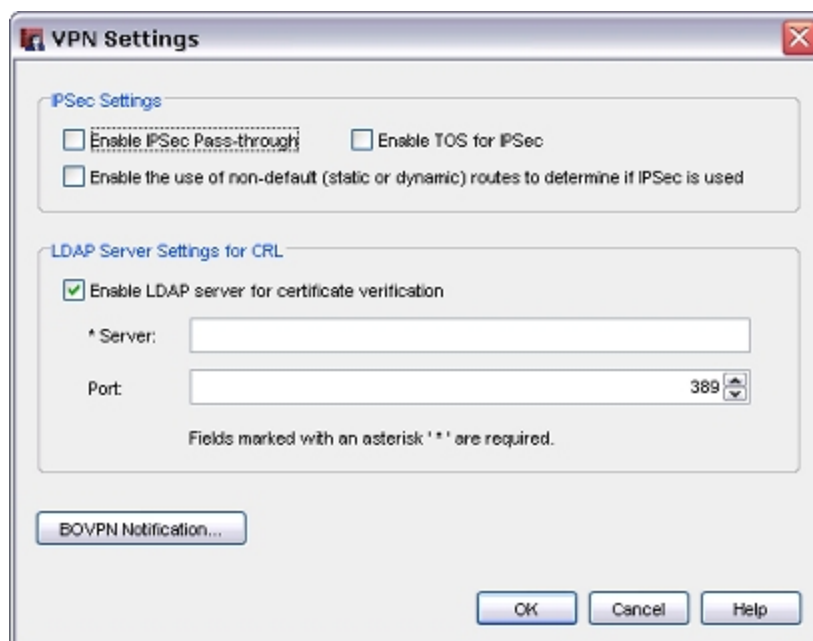
## Verify the Certificate with FSM

1. Select **View > Certificates**.  
*The Certificates dialog box appears.*
2. In the **Type** column, verify *IPSec* or *IPSec/Web* appears.

## Verify VPN Certificates with an LDAP Server

You can use an LDAP server to automatically verify certificates used for VPN authentication if you have access to the server. You must have LDAP account information provided by a third-party CA service to use this feature.

1. Select **VPN > VPN Settings**.  
*The VPN Settings dialog box appears.*



2. Select the **Enable LDAP server for certificate verification** check box.
3. In the **Server** text box, type the name or address of the LDAP server.
4. (Optional) Type the **Port** number.
5. Click **OK**.

*Your XTM device checks the CRL stored on the LDAP server when tunnel authentication is requested.*

## Configure the Web Server Certificate for Firebox Authentication

When users connect to your XTM device with a web browser, they often see a security warning. This warning occurs because the default certificate is not trusted, or because the certificate does not match the IP address or domain name used for authentication. If you have Fireware XTM with a Pro upgrade, you can use a third-party or self-signed certificate that matches the IP or domain name for user authentication. You must import that certificate on each client browser or device to prevent the security warnings.

To see the current web server certificate:

1. Open Firebox System Manager.
2. Select **View > Certificates**. The web server certificate is marked with an asterisk.

To configure the web server certificate for Firebox authentication:

1. Select **Setup > Authentication > Web Server Certificate**.



2. To use the default certificate, select **Default certificate signed by Firebox** and proceed to the last step in this procedure.
3. To use a certificate you have previously imported, select **Third-party certificate**.
4. Select a certificate from the adjacent drop-down list and continue with the last step in this procedure.  
*This certificate must be recognized as a Web certificate.*
5. If you want to create a custom certificate signed by your XTM device, select **Custom certificate signed by Firebox**.
6. Type the **common name** for your organization. This is usually your domain name.

7. (Optional) You can also type an **Organization Name** and an **Organization Unit Name** to identify the part of your organization that created the certificate.
8. Click **Add Domain Names** or **Add Interface IP Addresses**.



9. In the text box at the bottom of the dialog box, type a domain name or IP address of an interface on your XTM device.
10. Click **Add**.
11. Repeat Steps 8–9 to add more domain names.
12. Click **OK**.

## Use Certificates for the HTTPS-Proxy

Many web sites use both the HTTP and HTTPS protocols to send information to users. While HTTP traffic can be examined easily, HTTPS traffic is encrypted. To examine HTTPS traffic requested by a user on your network, you must configure your XTM device to decrypt the information and then encrypt it with a certificate signed by a CA that each network user trusts.



By default, the XTM device re-encrypts the content it has inspected with an automatically generated self-signed certificate. Users without a copy of this certificate see a certificate warning when they connect to a secure web site with HTTPS. If the remote web site uses an expired certificate, or if that certificate is signed by a CA (Certificate Authority) the XTM device does not recognize, the XTM device re-signs the content as *Fireware HTTPS Proxy: Unrecognized Certificate* or simply *Invalid Certificate*.

This section includes information about how to export a certificate from the XTM device and import it on a Microsoft Windows or Mac OS X system to operate with the HTTPS-proxy. To import the certificate on other devices, operating systems, or applications, see the documentation from their manufacturers.

## Protect a Private HTTPS Server

To protect an HTTPS server on your network, you must first import the CA certificate used to sign the HTTPS server certificate, and then import the HTTPS server certificate with its associated private key. If the CA certificate used to sign the HTTPS server certificate is not automatically trusted itself, you must import each trusted certificate in sequence for this feature to operate correctly. After you have imported all of the certificates, configure the HTTPS-proxy.

From Policy Manager:

1. Click .  
Or, select **Edit > Add Policy**.  
*The Add Policies dialog box appears.*
2. Expand the **Proxies** list and select **HTTPS-proxy**. Click **Add**.  
*The New Policy Properties dialog box appears with the Policy tab selected.*
3. Adjacent to the **Proxy action** drop-down list, click .  
*The HTTPS Proxy Action Configuration dialog box appears, with the Content Inspection category selected.*
4. Select the **Enable deep inspection of HTTPS content** check box.
5. From the **Proxy Action** drop-down list, select the HTTP proxy action to use to inspect HTTPS content, or create a new HTTP proxy action to use for this policy.
6. Clear the **Use OCSP to confirm the validity of certificates** check box.
7. In the **Bypass List** text box, type the IP address of a web site for which you do not want to inspect traffic. Click **Add**.
8. (Optional) Repeat Step 7 to add more IP addresses to the **Bypass List**
9. Click **OK** to close the **HTTPS Proxy Action Configuration** dialog box.  
*The Clone Predefined or DVCP-created Object dialog box appears.*
10. In the **Name** text box, type a name for the proxy action.  
For example, type **HTTPS-Client DCI**.
11. Click **OK**.
12. Click **OK** to close the **New Policy Properties** dialog box.
13. In the **Add Policy** dialog box, click **Close**.

For more information, see *Manage XTM Device Certificates* on page 862.



## Examine Content from External HTTPS Servers



If your organization already has a PKI (Public Key Infrastructure) set up with a trusted CA, then you can import a certificate on the XTM device that is signed by your organization CA. If the CA certificate is not automatically trusted itself, you must import each previous certificate in the chain of trust for this feature to operate correctly. For more information, see *Manage XTM Device Certificates* on page 862.

**Note** *If you have other traffic that uses the HTTPS port, such as SSL VPN traffic, we recommend that you evaluate the content inspection feature carefully. The HTTPS-proxy attempts to examine all traffic on TCP port 443 in the same way. To ensure that other traffic sources operate correctly, we recommend that you add those IP addresses to the Bypass List. For more information, see HTTPS-Proxy: Content Inspection on page 463.*

Before you enable this feature, we recommend that you provide the certificate(s) used to sign HTTPS traffic to all of the clients on your network. You can attach the certificates to an email with instructions, or use network management software to install the certificates automatically. Also, we recommend that you test the HTTPS-proxy with a small number of users to ensure that it operates correctly before you apply the HTTPS-proxy to traffic on a large network.

If your organization does not have a PKI, you must copy the default or a custom self-signed certificate from the XTM device to each client device.

From Policy Manager:

1. Click .  
Or, select **Edit > Add Policy**.  
*The Add Policies dialog box appears.*
2. Expand the **Proxies** category and select the **HTTPS-proxy** entry. Click **Add**.  
*The New Policy Properties dialog box appears, with the Policy tab selected.*
3. Adjacent to the **Proxy action** drop-down list, click .  
*The HTTPS Proxy Action Configuration dialog box appears, with the Content Inspection category selected.*
4. Select the **Enable deep inspection of HTTPS content** check box.
5. From the **Proxy Action** drop-down list, select the HTTP proxy action to use to inspect HTTPS content, or create a new HTTP proxy action to use for this policy.
6. Select the options for OCSP certificate validation.
7. In the **Bypass List** text box, type the IP address of a web site for which you do not want to inspect traffic. Click **Add**.
8. (Optional) Repeat Step 7 to add more IP addresses to the **Bypass List**
9. Click **OK** to close the **HTTPS Proxy Action Configuration** dialog box.  
*The Clone Predefined or DVCP-created Object dialog box appears.*
10. In the **Name** text box, type a name for the proxy action.  
For example, type HTTPS-Client DCI.
11. Click **OK**.
12. Click **OK** to close the **New Policy Properties** dialog box.
13. In the **Add Policy** dialog box, click **Close**.

When you enable content inspection, the HTTP proxy action WebBlocker settings override the HTTPS proxy WebBlocker settings. If you add IP addresses to the Bypass list, traffic from those sites is filtered with the WebBlocker settings from the HTTPS proxy.

For more information on WebBlocker configuration, see *About WebBlocker* on page 1065.

## Export the HTTPS Content Inspection Certificate

This procedure exports one certificate from your XTM device in PEM format.

1. Open Firebox System Manager and connect to your XTM device.
2. Select **View > Certificates**.
3. Select the **HTTPS Proxy Authority CA** certificate from the list and click **Export**.
4. Type a name and select a location to save the certificate locally.
5. Copy the saved certificate to the client machine.

If the HTTPS-proxy certificate used for content inspection requires another root or intermediate CA certificate before it can be trusted by network clients, you must also export those certificates. You can also copy the certificates from the original source for distribution.

If you have previously imported the certificate on a client, you can export that certificate directly from the operating system or browser certificate store. In most cases, this exports the certificate in the x.509 format. Windows and Mac OS X users can double-click an x.509 format certificate to import it.

## Import the Certificates on Client Devices

To use certificates you have installed on the XTM device with client devices, you must export the certificates with Firebox System Manager, then import the certificates on each client.

For more information about how to import a certificate, see *Import a Certificate on a Client Device* on page 883.

## Troubleshoot Problems with HTTPS Content Inspection

The XTM device often creates log messages when there is a problem with a certificate used for HTTPS content inspection. We recommend that you check these log messages for more information.

If connections to remote web servers are often interrupted, check to make sure you have imported all of the certificates necessary to trust the CA certificate used to re-encrypt the HTTPS content, as well as the certificates necessary to trust the certificate from the original web server. You must import all of these certificates on the XTM device and each client device for connections to be successful.

## Import a Certificate on a Client Device

When you configure your XTM device to use a custom or third-party certificate for authentication or HTTPS content inspection, you must import that certificate on each client in your network to prevent security warnings. This also allows services like Windows Update to operate correctly.

**Note** *If you normally use Fireware XTM Web UI, you must install Firebox System Manager before you can export certificates.*

## Import a PEM Format Certificate with Windows XP

This process allows Internet Explorer, Windows Update, and other programs or services that use the Windows certificate store on Microsoft Windows XP to get access to the certificate.

1. In the Windows **Start** menu, select **Run**.
2. Type `mmc` and click **OK**.  
*A Windows Management Console appears.*
3. Select **File > Add/Remove Snap-In**.
4. Click **Add**.
5. Select **Certificates**, then click **Add**.
6. Select **Computer account** and click **Next**.
7. Click **Finish**, **Close**, and **OK** to add the certificates module.
8. In the **Console Root** window, expand the **Certificates** tree.
9. Expand the **Trusted Root Certification Authorities** object.
10. Under the **Trusted Root Certification Authorities** object, right-click **Certificates** and select **All Tasks > Import**.
11. Click **Next**.
12. Click **Browse** to find and select the HTTPS Proxy Authority CA certificate you previously exported. Click **OK**.
13. Click **Next**, then click **Finish** to complete the wizard.

## Import a PEM format certificate with Windows Vista

This process allows Internet Explorer, Windows Update, and other programs or services that use the Windows certificate store on Microsoft Windows Vista to get access to the certificate.

1. On the Windows **Start** menu, type `certmgr.msc` in the **Search** text box and press **Enter**.  
*If you are prompted to authenticate as an administrator, type your password or confirm your access.*
2. Select the **Trusted Root Certification Authorities** object.
3. From the **Action** menu, select **All Tasks > Import**.
4. Click **Next**. Click **Browse** to find and select the HTTPS Proxy Authority CA certificate you previously exported. Click **OK**.
5. Click **Next**, then click **Finish** to complete the wizard.

## Import a PEM Format Certificate with Mozilla Firefox 3.x

Mozilla Firefox uses a private certificate store instead of the operating system certificate store. If clients on your network use the Firefox browser, you must import the certificate into the Firefox certificate store even if you have already imported the certificate on the host operating system.

When you have more than one XTM device that uses a self-signed certificate for HTTPS content inspection, clients on your network must import a copy of each XTM device certificate. However, the default self-signed XTM device certificates use the same name, and Mozilla Firefox only recognizes the first certificate you import when more than one certificate has the same name. We recommend that you replace the default self-signed certificates with a certificate signed by a different CA, and then distribute those CA certificates to each client.

1. In Firefox, select **Tools > Options**.  
*The Options dialog box appears.*
2. Click the **Advanced** icon.
3. Select the **Encryption** tab, then click **View Certificates**.  
*The Certificate Manager dialog box appears.*
4. Select the **Authorities** tab, then click **Import**.
5. Browse to select the certificate file, then click **Open**.
6. In the **Downloading Certificate** dialog box, select the **Trust this CA to identify web sites** check box.  
Click **OK**.
7. Click **OK** twice to close the **Certificate Manager** and **Options** dialog boxes.
8. Restart Firefox.

## Import a PEM Format Certificate with Mac OS X 10.5

This process allows Safari and other programs or services that use the Mac OS X certificate store to get access to the certificate.

1. Open the **Keychain Access** application.
2. Select the **Certificates** category.
3. Click the **plus icon (+)** button on the lower toolbar, then find and select the certificate.
4. Select the **System** keychain, then click **Open**. You can also select the System keychain, then drag and drop the certificate file into the list.
5. Right-click the certificate and select **Get Info**.  
*A certificate information window appears.*
6. Expand the **Trust** category.
7. In the **When using this certificate** drop-down list, select **Always Trust**.
8. Close the certificate information window.
9. Type your administrator password to confirm your changes.



# 25 Virtual Private Networks (VPNs)

---

## Introduction to VPNs

To move data safely between two private networks across an unprotected network, such as the Internet, you can create a virtual private network (VPN). You can also use a VPN for a secure connection between a host and a network. The networks and hosts at the endpoints of a VPN can be corporate headquarters, branch offices, or remote users. VPNs use encryption to secure data, and authentication to identify the sender and the recipient of the data. If the authentication information is correct, the data is decrypted. Only the sender and the recipient of the message can read the data sent through the VPN.

A VPN *tunnel* is the virtual path between the two private networks of the VPN. We refer to this path as a tunnel because a tunneling protocol such as IPSec, SSL, or PPTP is used to securely send the data packets. A gateway or computer that uses a VPN uses this tunnel to send the data packets across the public Internet to private IP addresses behind a VPN gateway.

## Branch Office VPN

A Branch Office VPN (BOVPN) is an encrypted connection between two dedicated hardware devices. It is used most frequently to make sure the network communications between networks at two offices is secure. WatchGuard provides two methods to set up a BOVPN:

### *Manual BOVPN*

You can use Policy Manager or Fireware XTM Web UI to manually configure a BOVPN between any two devices that support IPSec VPN protocols.

For more information, see *About Manual Branch Office VPN Tunnels* on page 914.

### *Managed BOVPN*

You can use WatchGuard System Manager to set up a managed BOVPN between any two managed Firebox or XTM devices.

For more information, see *About Managed Branch Office VPN Tunnels* on page 899.

All WatchGuard BOVPNs use the IPSec protocol suite to secure the BOVPN tunnel.

For more information about IPSec VPNs, see *About IPSec VPNs* on page 888.

## Mobile VPN

A Mobile VPN is an encrypted connection between a dedicated hardware device and a laptop or desktop computer. A Mobile VPN allows your employees who telecommute and travel to securely connect to your corporate network. WatchGuard supports three types of Mobile VPNs:

- Mobile VPN with IPSec
- Mobile VPN with PPTP
- Mobile VPN with SSL

For a comparison of these Mobile VPN solutions, see *Select a Mobile VPN*.

## About IPSec VPNs

WatchGuard Branch Office VPN and Mobile VPN with IPSec both use the IPSec protocol suite to establish VPNs between devices or mobile users. Before you configure an IPSec VPN, especially if you configure a manual BOVPN tunnel, it is helpful to understand how IPSec VPNs work.

For more information, see:

- *About IPSec Algorithms and Protocols*
- *About IPSec VPN Negotiations*
- *Configure Phase 1 and Phase 2 Settings*

## About IPSec Algorithms and Protocols

IPSec is a collection of cryptography-based services and security protocols that protect communication between devices that send traffic through an untrusted network. Because IPSec is built on a collection of widely known protocols and algorithms, you can create an IPSec VPN between your XTM device and many other devices that support these standard protocols. The protocols and algorithms used by IPSec are discussed in the subsequent sections.

## Encryption Algorithms

Encryption algorithms protect the data so it cannot be read by a third-party while in transit. Fireware XTM supports three encryption algorithms:

- DES (Data Encryption Standard) — Uses an encryption key that is 56 bits long. This is the weakest of the three algorithms.
- 3DES (Triple-DES) — An encryption algorithm based on DES that uses DES to encrypt the data three times.
- AES (Advanced Encryption Standard) — The strongest encryption algorithm available. Fireware XTM can use AES encryption keys of these lengths: 128, 192, or 256 bits.



## Authentication Algorithms

Authentication algorithms verify the data integrity and authenticity of a message. Fireware XTM supports two authentication algorithms:

- HMAC-SHA1 (Hash Message Authentication Code — Secure Hash Algorithm 1) — SHA-1 produces a 160-bit (20 byte) message digest. Although slower than MD5, this larger digest size makes it stronger against brute force attacks.
- HMAC-MD5 (Hash Message Authentication Code — Message Digest Algorithm 5) — MD5 produces a 128 bit (16 byte) message digest, which makes it faster than SHA-1.

## IKE Protocol

Defined in RFC2409, IKE (Internet Key Exchange) is a protocol used to set up security associations for IPSec. These security associations establish shared session secrets from which keys are derived for encryption of tunneled data. IKE is also used to authenticate the two IPSec peers.

## Diffie-Hellman Key Exchange Algorithm

The Diffie-Hellman (DH) key exchange algorithm is a method used to make a shared encryption key available to two entities without an exchange of the key. The encryption key for the two devices is used as a symmetric key for encrypting data. Only the two parties involved in the DH key exchange can deduce the shared key, and the key is never sent over the wire.

A Diffie-Hellman *key group* is a group of integers used for the Diffie-Hellman key exchange. Fireware XTM can use DH groups 1, 2, and 5. The higher group numbers provide stronger security.

For more information, see *About Diffie-Hellman Groups* on page 925.

## AH

Defined in RFC 2402, AH (Authentication Header) is a protocol that you can use in manual BOVPN Phase 2 VPN negotiations. To provide security, AH adds authentication information to the IP datagram. Most VPN tunnels do not use AH because it does not provide encryption.

## ESP

Defined in RFC 2406, ESP (Encapsulating Security Payload) provides authentication and encryption of data. ESP takes the original payload of a data packet and replaces it with encrypted data. It adds integrity checks to make sure that the data is not altered in transit, and that the data came from the proper source. We recommend that you use ESP in BOVPN Phase 2 negotiations because ESP is more secure than AH. Mobile VPN with IPSec always uses ESP.

## About IPSec VPN Negotiations

The devices at either end of an IPSec VPN tunnel are IPSec peers. When two IPSec peers want to make a VPN between them, they exchange a series of messages about encryption and authentication, and attempt to agree on many different parameters. This process is known as VPN negotiations. One device in the negotiation sequence is the initiator and the other device is the responder.

VPN negotiations happen in two distinct phases: *Phase 1* and *Phase 2*.

### *Phase 1*

The main purpose of Phase 1 is to set up a secure encrypted channel through which the two peers can negotiate Phase 2. When Phase 1 finishes successfully, the peers quickly move on to Phase 2 negotiations. If Phase 1 fails, the devices cannot begin Phase 2.

### *Phase 2*

The purpose of Phase 2 negotiations is for the two peers to agree on a set of parameters that define what traffic can go through the VPN, and how to encrypt and authenticate the traffic. This agreement is called a Security Association.

The Phase 1 and Phase 2 configurations must match for the devices on either end of the tunnel.

## Phase 1 Negotiations

In Phase 1 negotiations, the two peers exchange credentials. The devices identify each other and negotiate to find a common set of Phase 1 settings to use. When Phase 1 negotiations are completed, the two peers have a Phase 1 Security Association (SA). This SA is valid for only a certain amount of time. After the Phase 1 SA expires, if the two peers must complete Phase 2 negotiations again, they must also negotiate Phase 1 again.

Phase 1 negotiations include these steps:

1. The devices exchange credentials.

The credentials can be a certificate or a pre-shared key. Both gateway endpoints must use the same credential method. If one peer uses a pre-shared key, the other peer must also use a pre-shared key, and the keys must match. If one peer uses a certificate, the other peer must also use a certificate.

2. The devices identify each other.

Each device provides a Phase 1 identifier, which can be an IP address, domain name, domain information, or an X500 name. The VPN configuration on each peer contains the Phase 1 identifier of the local and the remote device, and the configurations must match.

3. The peers decide whether to use Main Mode or Aggressive Mode.

Phase 1 negotiations can use one of two different modes: Main Mode or Aggressive Mode. The device that starts the IKE negotiations (the initiator) sends either a Main Mode proposal or an Aggressive Mode proposal. The responder can reject the proposal if it is not configured to use that mode. Aggressive Mode communications take place with fewer packet exchanges. Aggressive Mode is less secure but faster than Main Mode.

4. The peers agree on Phase 1 parameters.

- Whether to use NAT traversal
  - Whether to send IKE keep-alive messages (supported between Firebox or XTM devices only)
  - Whether to use Dead Peer Detection (RFC 3706)
5. The peers agree on Phase 1 Transform settings.

Transform settings include a set of authentication and encryption parameters, and the maximum amount of time for the Phase 1 SA. The settings in the Phase 1 transform must exactly match a Phase 1 transform on the IKE peer, or IKE negotiations fail.

The items you can set in the transform are:

- Authentication — The type of authentication (SHA1 or MD5).
- Encryption — The type of encryption algorithm (DES, 3DES or AES).
- SA Life — The amount of time until the Phase 1 Security Association expires.
- Key Group — The Diffie-Hellman key group.

## Phase 2 Negotiations

After the two IPSec peers complete Phase 1 negotiations, Phase 2 negotiations begin. Phase 2 negotiations is to establish the Phase 2 SA (sometimes called the IPSec SA). The IPSec SA is a set of traffic specifications that tell the device what traffic to send over the VPN, and how to encrypt and authenticate that traffic. In Phase 2 negotiations, the two peers agree on a set of communication parameters. When you configure the BOVPN tunnel in Policy Manager or in Fireware XTM Web UI, you specify the Phase 2 parameters.

Because the peers use the Phase 1 SA to secure the Phase 2 negotiations, and you define the Phase 1 SA settings in the BOVPN Gateway settings, you must specify the gateway to use for each tunnel.

Phase 2 negotiations include these steps:

1. The peers use the Phase 1 SA to secure Phase 2 negotiations.

Phase 2 negotiations can only begin after Phase 1 SA has been established.

2. The peers exchange Phase 2 identifiers (IDs).

Phase 2 IDs are always sent as a pair in a Phase 2 proposal: one indicates which IP addresses behind the local device can send traffic over the VPN, and the other indicates which IP addresses behind the remote device can send traffic over the VPN. This is also known as a *tunnel route*. You can specify the Phase 2 IDs for the local and remote peer as a host IP address, a network IP address, or an IP address range.

3. The peers agree on whether to use Perfect Forward Secrecy (PFS).

PFS specifies how Phase 2 keys are derived. When PFS is selected, both IKE peers must use PFS, or Phase 2 rekeys fail. PFS guarantees that if an encryption key used to protect the data transmission is compromised, an attacker can access only the data protected by that key, not subsequent keys. If the peers agree to use PFS, they must also agree on the Diffie-Hellman key group to use for PFS.

4. The peers agree on a Phase 2 proposal.

The Phase 2 proposal includes the IP addresses that can send traffic over the tunnel, and a group of encryption and authentication parameters. Fireware XTM sends these parameters in a Phase 2 proposal. The proposal includes the algorithm to use to authenticate data, the algorithm to use to encrypt data, and how often to make new Phase 2 encryption keys.

The items you can set in a Phase 2 proposal include:

### *Type*

For a manual BOVPN, you can select the type of protocol to use: Authentication Header (AH) or Encapsulating Security Payload (ESP). ESP provides authentication and encryption of the data. AH provides authentication without encryption. We recommend you select ESP. Managed BOVPN and Mobile VPN with IPSec always use ESP.

### *Authentication*

Authentication makes sure that the information received is exactly the same as the information sent. You can use SHA or MD5 as the algorithm the peers use to authenticate IKE messages from each other. SHA1 is more secure.

### *Encryption*

Encryption keeps the data confidential. You can select DES, 3DES, or AES. AES is the most secure.

### *Force Key Expiration*

To make sure Phase 2 encryption keys change periodically, always enable key expiration. The longer a Phase 2 encryption key is in use, the more data an attacker can collect to use to mount an attack on the key.

## Configure Phase 1 and Phase 2 Settings

You configure Phase 1 and Phase 2 settings for each IPsec VPN you configure.

### Branch Office VPN

For a manual Branch Office VPN (BOVPN), you configure Phase 1 settings when you define a Branch Office gateway, and you configure Phase 2 settings when you define a Branch Office tunnel.

For more information about BOVPN Phase 1 and Phase 2 settings, see:

- *Configure Gateways* on page 918
- *Define a Tunnel* on page 928

For a managed Branch Office VPN, you configure the Phase 1 and Phase 2 settings when you add a Security Template.

For more information, see *Add Security Templates* on page 905

### Mobile VPN with IPsec

For Mobile VPN with IPsec, many of the Phase 1 and Phase 2 settings are set automatically by the Add Mobile VPN with IPsec Wizard. You can also manage these settings in Policy Manager.

For more information, see:

- *Configure the XTM Device for Mobile VPN with IPsec* on page 990
- *Modify an Existing Mobile VPN with IPsec Group Profile*

### Use a Certificate for IPsec VPN Tunnel Authentication

When an IPsec tunnel is created, the IPsec protocol checks the identity of each endpoint with either a pre-shared key (PSK) or a certificate imported and stored on the XTM device. You configure the tunnel authentication method in the VPN Phase 1 settings.

For more information about how to use a certificate for tunnel authentication, see:

- *Certificates for Branch Office VPN (BOVPN) Tunnel Authentication*
- *Certificates for Mobile VPN with IPsec Tunnel Authentication*

## About Mobile VPNs

A *Mobile VPN* enables your employees who telecommute and travel to securely connect to your corporate network. Fireware XTM supports three forms of remote user virtual private networks: Mobile VPN with IPSec, Mobile VPN with PPTP, and Mobile VPN with SSL.

When you use Mobile VPN, you first configure your XTM device and then configure the remote client computers. You use Policy Manager or Fireware XTM Web UI to configure the settings for each user or group of users. For Mobile VPN with IPSec and Mobile VPN with SSL, you use Policy Manager or the Web UI to create an end user profile configuration file that includes all the settings necessary to connect to the XTM device. You can also configure your policies to allow or deny traffic from Mobile VPN clients. Mobile VPN users authenticate either to the XTM device user database or to an external authentication server.

### Select a Mobile VPN

Fireware XTM supports three types of Mobile VPN. Each type uses different ports, protocols, and encryption algorithms.

#### *Mobile VPN with PPTP*

- PPTP (Point-to-Point Tunneling Protocol) — Secures the tunnel between two endpoints
- TCP port 1723 — Establishes the tunnel
- IP protocol 47 — Encrypts the data
- Encryption algorithms — 40 bit or 128 bit

#### *Mobile VPN with IPSec*

- IPSec (Internet Protocol Security) — Secure the tunnel between two endpoints
- UDP port 500 (IKE) — Establishes the tunnel
- UDP port 4500 (NAT Traversal) — Used if the XTM device is configured for NAT
- IP protocol 50 (ESP) or IP Protocol 51 (AH) — Encrypts the data
- Encryption algorithms — DES, 3DES, or AES (128, 192, or 256 bit)

#### *Mobile VPN with SSL*

- SSL (Secure Sockets Layer) — Secures the tunnel between two endpoints
- TCP port 443 or UDP port 443 — Establishes the tunnel and encrypts the data
- Encryption algorithms — Blowfish, DES, 3DES, or AES (128, 192, or 256 bit)

**Note** For Mobile VPN with SSL, you can choose a different port and protocol. For more information, see *Choose the port and protocol for Mobile VPN with SSL*

The type of Mobile VPN you select largely depends on your existing infrastructure and your network policy preferences. The XTM device can manage all three types of mobile VPN simultaneously. A client computer can be configured to use one or more methods. Some of the things to consider when you select what type of Mobile VPN to use are described in the subsequent sections.

## VPN Tunnel Capacity and Licensing

When you select a type of tunnel, make sure to consider the number of tunnels your device supports and whether you can purchase an upgrade to increase the number of tunnels.

Mobile VPN	Maximum VPN tunnels
Mobile VPN with PPTP	50 tunnels
Mobile VPN with IPsec	<ul style="list-style-type: none"> <li>■ Base and maximum tunnels vary by XTM device model.</li> <li>■ License purchase is required to enable the maximum number of tunnels.</li> </ul>
Mobile VPN with SSL	<ul style="list-style-type: none"> <li>■ Base and maximum tunnels vary by XTM device model.</li> <li>■ Pro upgrade for the Fireware XTM OS is required for maximum SSL VPN tunnels.</li> <li>■ To support more than one SSL VPN tunnel you must have a Pro upgrade.</li> </ul>

For the base and maximum number of tunnels supported for Mobile VPN with IPsec and Mobile VPN with SSL, see the detailed specifications for your XTM device model.

To find the number of VPN tunnels currently supported by your XTM device:

1. Open Policy Manager.
2. Select **VPN > Mobile VPN**.
3. Select the type of VPN.

*The number of tunnels your device supports appears in the configuration dialog box for each type of mobile VPN.*

## Authentication Server Compatibility

When you select a Mobile VPN solution, make sure to choose a solution that supports the type of authentication server you use.

Mobile VPN	XTM device	RADIUS	Vasco/RADIUS	Vasco Challenge Response	RSA SecurID	LDAP	Active Directory
Mobile VPN with PPTP	Yes	Yes	No	No	No	No	No
Mobile VPN with IPsec	Yes	Yes	Yes	N/A	Yes	Yes	Yes
Mobile VPN with SSL	Yes	Yes	Yes	N/A	Yes	Yes	Yes

## Client Configuration Steps and Operating System Compatibility

The configuration steps you must complete are different for each Mobile VPN solution. Each VPN solution is also compatible with different operating systems.

### *Mobile VPN with PPTP*

You do not install WatchGuard VPN client software. You must manually configure the network settings on each client computer to set up a PPTP connection.

Compatible with: Windows XP, and Windows Vista.

### *Mobile VPN with IPSec*

You must install the WatchGuard Mobile VPN with IPSec client and manually import the end user profile. The Mobile VPN with IPSec client requires more steps to set up than the Mobile VPN with SSL client.

Compatible with: Windows XP SP2 (32 bit and 64 bit), Windows Vista (32 bit and 64 bit), and Windows 7 (32 bit and 64 bit).

### *Mobile VPN with SSL*

You must install the WatchGuard Mobile VPN with SSL client and configuration file.

Compatible with: Windows XP SP2 (32 bit and 64 bit), Windows Vista (32 bit and 64 bit), Windows 7 (32 bit and 64 bit), Mac OS X 10.6 Snow Leopard, and Mac OS X 10.5 Leopard

## Internet Access Options for Mobile VPN Users

For all three types of Mobile VPN, you have two options for Internet access for your Mobile VPN users:

### *Force all client traffic through tunnel (default-route VPN)*

The most secure option is to require that all remote user Internet traffic is routed through the VPN tunnel to the XTM device. Then, the traffic is sent back out to the Internet. With this configuration (known as default-route VPN), the XTM device is able to examine all traffic and provide increased security, although it uses more processing power and bandwidth.

When you use default-route VPN with Mobile VPN for IPSec or Mobile VPN for PPTP, a dynamic NAT policy must include the outgoing traffic from the remote network. This enables remote users to browse the Internet when they send all traffic to the XTM device.

### *Allow direct access to the Internet (split tunnel VPN)*

Another configuration option is to enable split tunneling. With this option, your users can browse the Internet, but Internet traffic is not sent through the VPN tunnel. Split tunneling improves network performance, but decreases security because the policies you create are not applied to the Internet traffic. If you use split tunneling, we recommend that each client computer have a software firewall.

For more information specific to each type of Mobile VPN, see:

- *Options for Internet Access Through a Mobile VPN with IPSec Tunnel*
- *Options for Internet Access Through a Mobile VPN with PPTP Tunnel*



- *Options for Internet Access Through a Mobile VPN with SSL Tunnel*

## Mobile VPN Setup Overview

When you set up Mobile VPN, you must first configure the XTM device and then configure the client computers. Regardless of which type of Mobile VPN you choose, you must complete the same five configuration steps. The details for each step are different for each type of VPN.

1. Activate Mobile VPN in Policy Manager.
2. Define VPN settings for the new tunnel.
3. Select and configure the method of authentication for Mobile VPN users.
4. Define policies and resources.
5. Configure the client computers.
  - For Mobile VPN with IPsec and Mobile VPN with SSL, install the client software and configuration file.
  - For Mobile VPN with PPTP, manually configure the PPTP connection in the client computer network settings.

For more information and detailed steps to set up each type of Mobile VPN, see:

- *About Mobile VPN with IPsec*
- *About Mobile VPN with PPTP*
- *About Mobile VPN with SSL*



# 26 Managed Branch Office VPN Tunnels

---

## About Managed Branch Office VPN Tunnels

A *VPN (Virtual Private Network)* creates secure connections between computers or networks in different locations. Each connection is known as a *tunnel*. When a VPN tunnel is created, the two tunnel endpoints authenticate with each other. Data in the tunnel is encrypted. Only the sender and the recipient of the traffic can read it.

*Branch Office Virtual Private Networks (BOVPN)* enable organizations to deliver secure, encrypted connectivity between geographically separated offices. The networks and hosts on a BOVPN tunnel can be corporate headquarters, branch offices, remote users, or telecommuters. These communications often contain the types of critical data exchanged inside a corporate firewall. In this scenario, a BOVPN provides confidential connections between these offices. This streamlines communication, reduces the cost of dedicated lines, and maintains security at each endpoint.

With WatchGuard System Manager, you can quickly and easily configure IPsec tunnels that use authentication and encryption. You can see that these tunnels operate with other tunnels and security policies. These tunnels are called *managed BOVPN tunnels*. Another type of tunnel is a *manual BOVPN tunnel*, which is a BOVPN tunnel that you use dialog boxes to define. For information on this type of tunnel, see *About Manual Branch Office VPN Tunnels* on page 914.

## How to Create a Managed BOVPN Tunnel

You can quickly create a manual tunnel between devices with a drag-and-drop procedure and a simple wizard, as described in *Make Managed Tunnels Between Devices* on page 908.

However, you must make sure you have performed these procedures before you create managed tunnels:

1. Add the XTM devices that will be the tunnel endpoints to the Management Server, as described in *Add Managed Devices to the Management Server* on page 590.
2. If you want to use a certificate for VPN authentication, you must first import the certificate. For more information on this, see *Manage XTM Device Certificates* on page 862.

The certificate must be recognized as an "IPSec"-type certificate by Firebox System Manager. To verify this, *Start Firebox System Manager*, select **View > Certificates**, and make sure the **Type** column in the **Certificates** dialog box that appears says "IPSec" or "IPSec/Web." If you do not have a third-party or self-signed certificate, you must use the certificate authority on a Management Server.

For more information, see *Configure the Certificate Authority on the Management Server* on page 560.

## Tunnel Options

You can use several options to customize managed VPN tunnels:

- If the trusted network behind one of the devices has many routed or secondary networks that you want to allow through the tunnel, add them manually as VPN resources for the device as described in *Add VPN Resources* on page 901.
- If you want to restrict the types of traffic you allow through the managed BOVPN, or if you want to restrict the types of traffic that send log messages to the Log Server, you must use a VPN Firewall policy template. Or, you can use a policy template that is already defined on your Management Server. For more information, see *Add VPN Firewall Policy Templates* on page 903.
- The wizard you use to create managed BOVPN tunnels allows you to choose from several settings for encryption. These settings are appropriate for most tunnels. However, if your network has special requirements, you can create your own settings, as described in *Add Security Templates* on page 905.

## VPN Failover

VPN Failover, described in *Configure VPN Failover*, is supported with managed BOVPN tunnels. If you have multi-WAN configured and you create managed tunnels, WSM automatically sets up gateway pairs that include the external interfaces of both ends of your tunnel. No other configuration is necessary.

## Global VPN Settings

Global VPN settings on your XTM device apply to all manual BOVPN tunnels, managed tunnels, and Mobile VPN tunnels. You can use these settings to:

- Enable IPSec pass-through.
- Clear or maintain the settings of packets with Type of Service (TOS) bits set.
- Enable the use of non-default routes to determine if IPSec is used (BOVPN tunnels only).
- Use an LDAP server to verify certificates.
- Configure the XTM device to send a notification when a BOVPN tunnel is down (BOVPN tunnels only).

To change these settings, from Policy Manager, select **VPN > VPN Settings**. For more information on these settings, see *About Global VPN Settings* on page 935.

## BOVPN tunnel Status

You can use Firebox System Manager to see the current status of BOVPN tunnels. This information also appears on the **Device Status** tab of WatchGuard System Manager. For more information, see *VPN Tunnel Status and Subscription Services* on page 910.

## Rekey BOVPN Tunnels

You can use Firebox System Manager to immediately generate new keys for BOVPN tunnels instead of waiting for them to expire. For more information, see *Rekey BOVPN Tunnels* on page 803.

## Add VPN Resources

A VPN resource is a network that is allowed to connect through a VPN tunnel you specify. If a VPN endpoint device has a static IP address, all trusted networks behind the device are automatically allowed to connect. The Management Server creates a default VPN resource for the device that includes all trusted networks.

However, if the trusted network behind a device has many routed or secondary networks that you want to allow through the tunnel, you must add them manually as VPN resources for the device. If an endpoint device has a dynamic IP address, you must either get its current resources, as described below, or add any networks behind that device as VPN resources. The Management Server does not automatically create VPN resources for those networks.

## Get the Current Resources from a Device

If an endpoint device has a dynamic IP address, you can use WatchGuard System Manager to get the policies that already apply to the networks behind the device. Or, you can skip this procedure and add the networks as VPN resources instead.


1. On the **Device Management** tab, select a managed device, then select **Edit > Update Device**.  
*The Update Device dialog box appears.*



2. Select the **Download Trusted and Optional Network policies** check box.
3. Click **OK**.

## Create a New VPN Resource

To make a VPN resource, on the **Device Management** tab:

1. Select the device for which you want to configure a VPN resource and click .

Or, right-click the device and select **Insert VPN Resource**.

*The VPN Resource dialog box for that device appears.*

2. In the **Policy Name** text box, type a name for the policy. This name later appears in the Device Management window and in the Add VPN Wizard.
3. From the **Disposition** drop-down list, select one of these options:

*secure*

Encrypt traffic to and from this resource. This is the most commonly used option.

*bypass*

Sends the traffic in clear text. You might use this option if one XTM device is in drop-in mode and the tunnel routes traffic to the drop-in network. In this case, the drop-in IP address must be bypassed but not blocked or the tunnel cannot negotiate.

*block*

Do not allow the traffic through the VPN. You might use this option to exclude one or more IP addresses from using a VPN that allows a full subnet, but only when given a higher precedence than the full subnet.

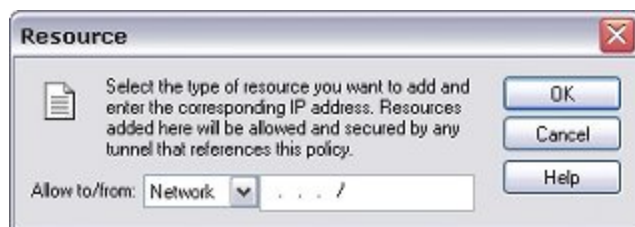
**Note** *If you want to create a VPN resource for a Firebox X Edge that does not use Fireware XTM 11.0 or higher, the **Disposition** drop-down list does not appear because only the **secure** option is supported.*

4. Add, edit, or delete resources.
  - Click **Add** to add an IP address or a network address.
  - Click **Edit** to edit a resource that you have selected in the list.
  - To delete a resource, select the resource in the **Resources** list and click **Remove**.
5. Click **OK**.

## Add a Host or Network

1. From the **VPN Resource** dialog box, click **Add**.

*The Resource dialog box appears.*



2. From the **Allow to/from** drop-down list, select the resource type, and then type the IP address or network address in the adjacent address text box.
3. Click **OK**.

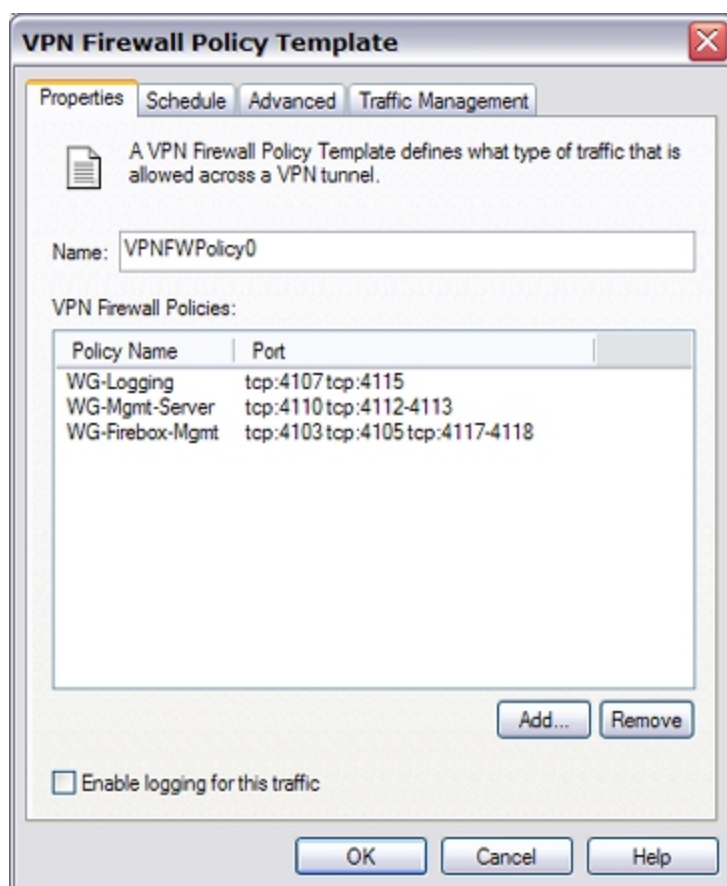
## Add VPN Firewall Policy Templates

You use VPN firewall policy templates to create a set of one or more bidirectional firewall policies that restrict the type the traffic allowed across a VPN. Note that policy templates do not support proxy policies.

If you use the default "Any" VPN firewall policy, a log message is generated for all traffic through the managed VPN tunnel. If you want to control what traffic is recorded in the logs, you must create your own VPN firewall policy template and use the **Enable logging for this traffic** check box. You cannot turn off logging for the default "Any" VPN firewall policy or change it in any way.

To create a VPN Firewall policy template:

1. On the **Device Management** tab, expand **Managed VPNs**, and select **VPN Firewall Policy Templates**.  
*The VPN Firewall Policy Templates page appears with a list of currently defined policy templates, if any are available.*
2. At the upper-right corner of the page, click **Add**.  
*The VPN Firewall Policy Template dialog box appears.*

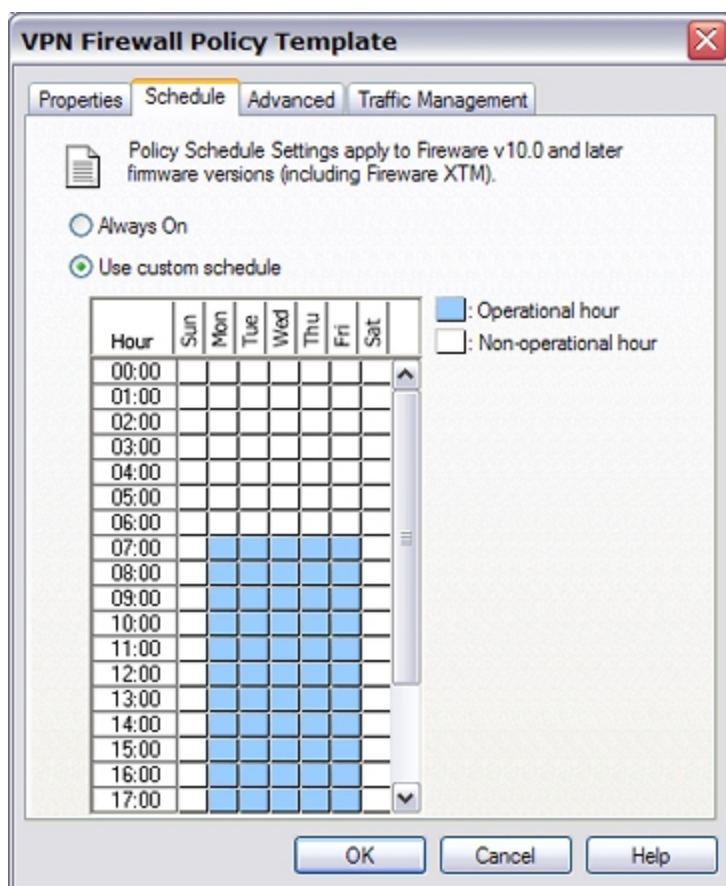


3. In the **Name** text box, type a name for the Policy Template. This is the name that appears in the VPN Firewall Policy Templates list and in the Add VPN Wizard.
4. To add a policy to the template, click **Add**.  
*The Add Policy wizard starts.*
5. Select from a list of pre-defined policies or create a custom policy. If you create a custom policy, on the next page of the wizard, type a name and select a port and protocol for the policy.
6. After you add the policy, you can repeat Steps 2–5 to add more policies.
7. Click **OK**.

## Set a Schedule for the Policy Template

By default, the policy template schedule is set to **Always On**. If you want to restrict the operational hours of this policy, you can configure the policy template to use a custom schedule.

1. Select the **Schedule** tab.  
*The Policy Schedule Settings appear.*
2. To change the operational hours, select **Use custom schedule**.  
*The custom schedule chart appears.*



3. The custom schedule chart shows days of the week along the X-axis (horizontal) and increments of the day on the Y-axis (vertical). Click the boxes in the chart to change them between operational hours (when the policy is active) and non-operational hours (when the policy is not in effect).



## Use QoS Marking in a Policy Template

You can use QoS Marking to mark traffic that uses a VPN firewall policy template. The marking action you select is applied to all traffic that uses the policy.

1. Select the **Advanced** tab.
2. Select the **Override per-interface settings** check box.
3. Configure the QoS Marking settings as described in *Enable QoS Marking for a Managed BOVPN Tunnel* on page 518.

## Configure Traffic Management in a Policy Template

1. Select the **Traffic Management** tab.
2. Select **Specify Custom Traffic Management Action**.
3. Configure the custom traffic management settings as described in *Add a Traffic Management Action to a BOVPN Firewall Policy* on page 522.


## Add Security Templates

A Security Template is a set of configuration information to be used when you create tunnels. When you use Security Templates, you do not need to re-create security settings each time you create a tunnel. These templates include Phase 1 and Phase 2 settings.

For more information on these settings, see *Configure Mode and Transforms (Phase 1 Settings)* on page 922 and *Configure Phase 2 Settings* on page 931.

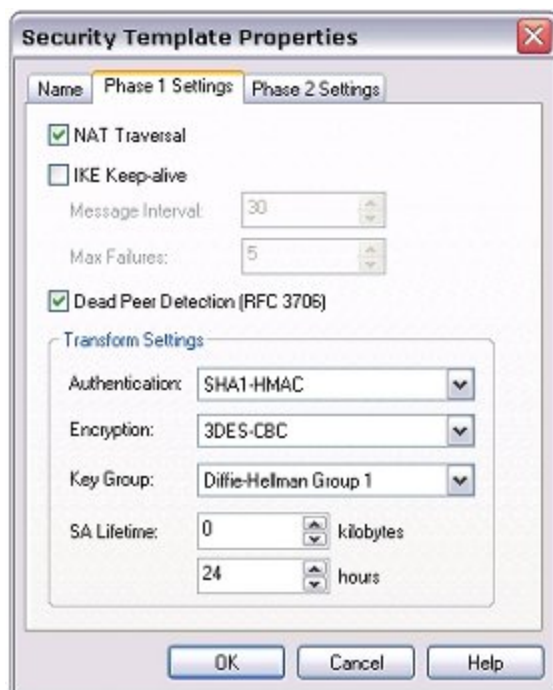
Default Security Templates are supplied for all of the available encryption types. You can use these settings to create secure tunnels that work correctly for most networks. However, if your network has special requirements, you can modify the existing templates or make new templates.

To add a Security Template:

1. On the **Device Management** tab, click .  
Or, select **Edit > Insert Security Template**.  
*The Security Template dialog box appears.*



2. In the **Template Name** text box, type a name for the template. This is the name that appears in the Security Templates list and in the Add VPN Wizard
3. Select the **Phase 1 Settings** tab.



4. If you want to create a BOVPN tunnel between the XTM device and another device that is behind a NAT device, select the **NAT Traversal** check box. NAT Traversal, or UDP Encapsulation, allows traffic to get to the correct destinations when a device does not have a public IP address.
5. If the other VPN endpoint supports it, select the **Dead Peer Detection** check box.

6. If both devices do not support Dead Peer Detection, and if both devices are XTM devices, select the **IKE Keep-alive** check box to enable the Firebox or XTM device to send messages to its IKE peer and keep the VPN tunnel open.
  - To set the **Message Interval**, type the number of seconds or use the value control to select the number of seconds you want.
  - To set the maximum number of times the XTM device tries to send an IKE keep-alive message before it tries to negotiate Phase 1 again, type the number of attempts in the **Max Failures** box.

**Warning** Do not enable both IKE Keep-alive and Dead Peer Detection.

7. From the **Authentication** and **Encryption** drop-down lists, select the authentication method and encryption method.
8. From the **Key Group** drop-down list, select the Diffie-Hellman group you want. Diffie-Hellman groups determine the strength of the master key used in the key exchange process. Higher group numbers are more secure, but more time is required to make the keys. For more information, see *About Diffie-Hellman Groups* on page 925.
9. To change the SA (security association) life, type a number in the **SA Life** text boxes to define the amount of time or traffic that must pass before the SA expires. Type a zero (0) for no limit.
10. Click the **Phase 2 Settings** tab.




11. From the **Authentication** drop-down list, select the authentication method for Phase 2.
12. From the **Encryption** drop-down list, select the encryption method.
13. To force the key to expire, select the **Force Key Expiration** check box. Select the duration and a number of kilobytes after which the key expires.  
If **Force Key Expiration** is disabled, or if it is enabled and both the time and number of kilobytes are set to zero, the XTM device tries to use the key expiration time set for the peer. If this is also disabled or zero, the XTM device uses a default key expiration time of 8 hours.  
The maximum expiration time is one year.
14. Click **OK**.

## Make Managed Tunnels Between Devices

You use the Add VPN Wizard to configure a managed BOVPN tunnel.

Dynamic Firebox and XTM devices must have networks that are configured before you can use this procedure. You must also get the policies from any new dynamic devices before you configure tunnels. For more information, see *Add VPN Resources* on page 901.

On the **Device Management** tab:

1. On one of the tunnel endpoints, select the device name. Drag-and-drop the name to the name of the device at the other tunnel endpoint.  
Or, click .  
Or, select **Edit > Create a new VPN**.  
*The Add VPN wizard starts.*
2. If you used the drag-and-drop procedure in Step 1, the wizard shows the two endpoint devices you selected with drag-and-drop, and the VPN resource that the tunnel uses.  
If you did not use drag-and-drop, select the endpoints from the **Device** drop-down list.
3. From the **VPN Resource** drop-down list, select a VPN resource for each device.  
For more information on VPN resources, see *Add VPN Resources* on page 901.  
To make a null-route VPN tunnel to force all traffic through a VPN, select **Hub Network**. Use this setting as the VPN resource for the device that hosts the null-route VPN. The remote device then sends all traffic through the VPN to the device that has **Hub Network** as the local resource.
4. Click **Next**.
5. From the **Security Template** drop-down list, select the Security Template that matches the type of security and type of authentication you want to use for this tunnel. Select the check box for each DNS and WINS servers you want to use. Click **Next**.  
  
For more information on Security Templates, see *Add Security Templates* on page 905.
6. From the **VPN Firewall Policy Template** drop-down list, select the VPN Firewall Policy Template applicable for the type of traffic you want to allow through this tunnel. If no VPN Firewall Policy Templates have been defined, the default "Any" policy is applied to the tunnel.  
For more information on VPN Firewall Policy Templates, see *Add VPN Firewall Policy Templates* on page 903.
7. Click **Next**.  
*The wizard shows the configuration.*
8. Select the **Restart devices now to download VPN configuration** check box.
9. Click **Finish** to restart both devices and create the VPN tunnel.

## Edit a Tunnel Definition

You can see all your tunnels on the **Device Management** tab of WatchGuard System Manager (WSM). From this page, you can change the tunnel name, Security Template, endpoints, and the policy used for each VPN tunnel.

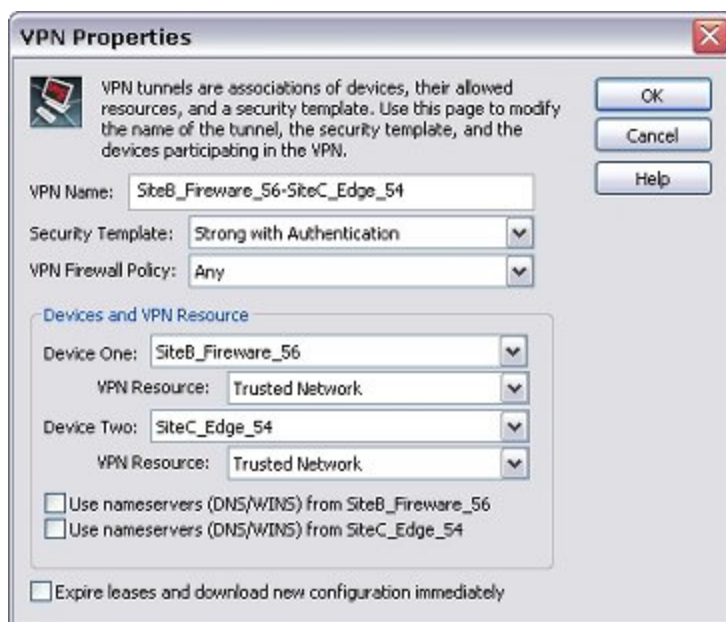
If you want to change the Policy Template or the Security Template for the tunnel, you can drag-and-drop the template name from the tree view at the left side of the **Device Management** tab to the VPN name in the tree view. The new template is applied. For other changes, or to use a dialog box to change a template:

1. On the **Device Management** tab, expand the **Managed VPNs** tree.
2. Right-click the tunnel you want to change and select **Properties**.

*The VPN Properties dialog box appears.*

3. Make the changes you want to the tunnel.
4. Click **OK** to save your changes.

*The changes are applied the next time the tunnel is renegotiated.*



## Remove Tunnels and Devices

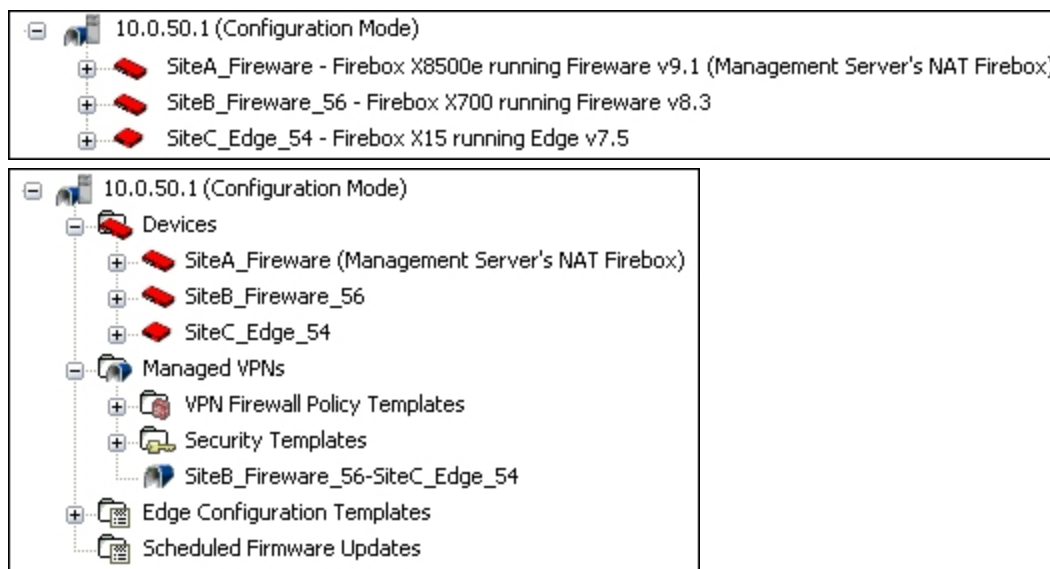
To remove a device from WatchGuard System Manager (WSM), you must first remove the tunnels for which that device is an endpoint.

### Remove a Tunnel

1. Select the **Device Management** tab.
2. Expand **Managed VPNs** to find the tunnel you want to remove.
3. Right-click the tunnel and select **Remove**.
4. Click **Yes** to confirm.
5. To restart the devices that use the tunnel you want to remove. Click **Yes**.

### Remove a Device

1. Select the **Device Status** or **Device Management** tab.

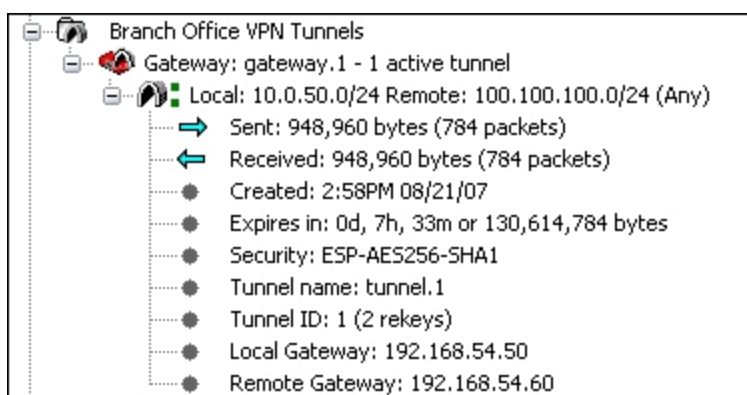


2. If you use the **Device Management** tab, expand **Devices** to find the device you want to remove.
3. Right-click the device and select **Remove**.
4. Click **Yes** to confirm.

## VPN Tunnel Status and Subscription Services

The front panel of Firebox System Manager (FSM) includes statistics about current VPN tunnels.

In the Firebox Status area on the right side of the window is a section on BOVPN tunnels. Firebox System Manager shows the current tunnel status and gateway information for each VPN tunnel as well as data sent and received, creation and expiration information, type of authentication and encryption used, and the number of rekeys.



Each BOVPN tunnel is shown in one of three states:

### *Active*

The BOVPN tunnel operates correctly and passes traffic.

### *Inactive*

The BOVPN tunnel has been created, but no tunnel negotiation has occurred. No traffic has been sent through the VPN tunnel.

### *Expired*

The BOVPN tunnel was active, but is no longer active because the tunnel has no traffic or because the link between the gateways was lost.

This information also appears on the **Device Status** tab in WatchGuard System Manager.

## Mobile VPN Tunnel Status

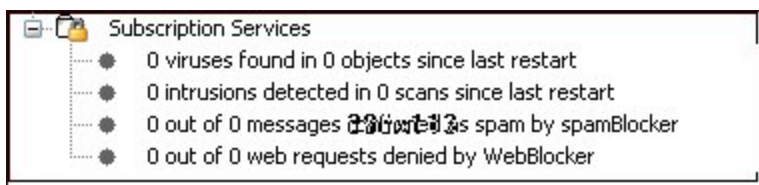
Firebox System Manager shows the user name, IP address information, and the quantity of sent and received packets for the three types of Mobile VPN Tunnels:

- Mobile VPN with IPSec
- Mobile VPN with SSL
- Mobile VPN with PPTP

To disconnect Mobile VPN users, right-click a user and select **Logoff selected user**.

## Subscription Services Status

In the **Subscription Services** section, Firebox System Manager shows the number of viruses found, the number of intrusions, the number of email messages confirmed as spam, and the number of HTTP requests denied by WebBlocker since the last restart.







# 27 Manual Branch Office VPN Tunnels

---

## What You Need to Create a Manual BOVPN

Before you configure a branch office VPN network on your XTM device, read these requirements:

- You must have two XTM devices, or one XTM device and a second device that uses IPSec standards. You must enable the VPN option on the other device if it is not already active.
- You must have an Internet connection.
- The ISP for each VPN device must allow IPSec traffic on their networks.  
Some ISPs do not let you create VPN tunnels on their networks unless you upgrade your Internet service to a level that supports VPN tunnels. Speak with a representative from each ISP to make sure these ports and protocols are allowed:
  - UDP Port 500 (Internet Key Exchange or IKE)
  - UDP Port 4500 (NAT traversal)
  - IP Protocol 50 (Encapsulating Security Payload or ESP)
- If the other side of the VPN tunnel is a XTM device and each device is under management, you can use the Managed VPN option. Managed VPN is easier to configure than Manual VPN. To use this option, you must get information from the administrator of the XTM device on the other side of the VPN tunnel.
- You must know whether the IP address assigned to the external interface of your XTM device is static or dynamic.  
For more information about IP addresses, see *About IP Addresses* on page 3.
- Your XTM device model tells you the maximum number of VPN tunnels that you can create. If your XTM device model can be upgraded, you can purchase a model upgrade that increases the maximum number of supported VPN tunnels.
- If you connect two Microsoft Windows NT networks, they must be in the same Microsoft Windows domain, or they must be trusted domains. This is a Microsoft Networking issue, and not a limitation of the XTM device.
- If you want to use the DNS and WINS servers from the network on the other side of the VPN tunnel, you must know the IP addresses of these servers.  
The XTM device can give WINS and DNS IP addresses to the computers on its trusted network if those computers get their IP addresses from the XTM device with DHCP.

- If you want to give the computers the IP addresses of WINS and DNS servers on the other side of the VPN, you can type those addresses into the DHCP settings in the trusted network setup. For information on how to configure the XTM device to distribute IP addresses with DHCP, see *Configure DHCP in Mixed Routing Mode* on page 94.
- You must know the network address of the private (trusted) networks behind your XTM device and of the network behind the other VPN device, and their subnet masks.

**Note** *The private IP addresses of the computers behind your XTM device cannot be the same as the IP addresses of the computers on the other side of the VPN tunnel. If your trusted network uses the same IP addresses as the office to which it will create a VPN tunnel, then your network or the other network must change their IP address arrangement to prevent IP address conflicts.*

## About Manual Branch Office VPN Tunnels

A *VPN (Virtual Private Network)* creates secure connections between computers or networks in different locations. Each connection is known as a *tunnel*. When a VPN tunnel is created, the two tunnel endpoints authenticate with each other. Data in the tunnel is encrypted. Only the sender and the recipient of the traffic can read it.

*Branch Office Virtual Private Networks (BOVPN)* enable organizations to deliver secure, encrypted connectivity between geographically separated offices. The networks and hosts on a BOVPN tunnel can be corporate headquarters, branch offices, remote users, or telecommuters. These communications often contain the types of critical data exchanged inside a corporate firewall. In this scenario, a BOVPN provides confidential connections between these offices. This streamlines communication, reduces the cost of dedicated lines, and maintains security at each endpoint.

*Manual BOVPN tunnels* provide many additional tunnel options. Another type of tunnel is a *managed BOVPN tunnel*, which is a BOVPN tunnel that you create with a drag-and drop procedure, a wizard, and the use of templates. For information on this type of tunnel, see *About Managed Branch Office VPN Tunnels* on page 899.

## What You Need to Create a VPN

In addition to the VPN requirements, you must have this information to create a manual VPN tunnel:

- You must know whether the IP address assigned to the other VPN device is static or dynamic. If the other VPN device has a dynamic IP address, your XTM device must find the other device by domain name and the other device must use Dynamic DNS.
- You must know the shared key (passphrase) for the tunnel. The same shared key must be used by each device.
- You must know the encryption method used for the tunnel (DES, 3DES, AES-128 bit, AES-192 bit, or AES-256 bit). The two VPN devices must use the same encryption method.
- You must know the authentication method for each end of the tunnel (MD5 or SHA-1). The two VPN devices must use the same authentication method.

For more information, see *What You Need to Create a Manual BOVPN* on page 913.

We recommend that you write down your XTM device configuration and the related information for the other device. See the *Sample VPN Address Information Table* on page 917 to record this information.

## How to Create a Manual BOVPN Tunnel

The basic procedure to create a manual tunnel includes these steps:

1. *Configure Gateways* — Configure the connection points on both the local and remote sides of the tunnel.
2. *Make Tunnels Between Gateway Endpoints* — Configure routes for the tunnel, specify how the devices control security, and make a policy for the tunnel.

Other options you can use for BOVPN tunnels are described in the subsequent sections.

## Custom Tunnel Policies

The XTM device automatically adds new VPN tunnels to the BOVPN-Allow.in and BOVPN-Allow.out policies. This allows all traffic to use the tunnel. You can choose to not use this policy and instead create custom VPN policies to allow only traffic of specific types through the tunnel. For more information, see *Define a Custom Tunnel Policy* on page 938.

## One-Way Tunnels

*Set Up Outgoing Dynamic NAT Through a Branch Office VPN Tunnel* if you want to keep the VPN tunnel open in one direction only. This can be helpful when you make a tunnel to a remote site where all VPN traffic comes from one public IP address.

## VPN Failover

VPN tunnels automatically fail over to the backup WAN interface during a WAN failover. You can configure BOVPN tunnels to fail over to a backup peer endpoint if the primary endpoint becomes unavailable. To do this, you must define at least one backup endpoint, as described in *Configure VPN Failover* on page 959.

## Global VPN Settings

Global VPN settings on your XTM device apply to all manual BOVPN tunnels, managed tunnels, and Mobile VPN tunnels. You can use these settings to:

- Enable IPsec pass-through
- Clear or maintain the settings of packets with Type of Service (TOS) bits set
- Enable the use of non-default routes to determine if IPsec is used
- Use an LDAP server to verify certificates
- Configure the XTM device to send a notification when a BOVPN tunnel is down (BOVPN tunnels only)

To change these settings, from Policy Manager, select **VPN > VPN Settings**. For more information on these settings, see *About Global VPN Settings* on page 935.

## BOVPN Tunnel Status

You can use Firebox System Manager to see the current status of BOVPN tunnels. This information also appears on the **Device Status** tab of WatchGuard System Manager. For more information, see *VPN Tunnel Status and Subscription Services* on page 910.

## Rekey BOVPN Tunnels

You can use Firebox System Manager to immediately generate new keys for BOVPN tunnels instead of waiting for them to expire. For more information, see *Rekey BOVPN Tunnels* on page 803.

## Sample VPN Address Information Table

Item	Description	Assigned by
External IP Address	<p>The IP address that identifies the IPSec-compatible device on the Internet. ISP</p> <p>Example: Site A: 207.168.55.2 Site B: 68.130.44.15</p>	ISP
Local Network Address	<p>An address used to identify a local network. These are the IP addresses of the computers on each side that are allowed to send traffic through the VPN tunnel. We recommend that you use an address from one of the reserved ranges:</p> <p>10.0.0.0/8—255.0.0.0 172.16.0.0/12—255.240.0.0 192.168.0.0/16—255.255.0.0</p> <p>The numbers after the slashes indicate the subnet masks. /24 means that the subnet mask for the trusted network is 255.255.255.0. For more information about slash notation, see <i>About Slash Notation</i> on page 3.</p> <p>Example: Site A: 192.168.111.0/24 Site B: 192.168.222.0/24</p>	You
Shared Key	<p>The shared key is a passphrase used by two IPSec-compatible devices to encrypt and decrypt the data that goes through the VPN tunnel. The two devices use the same passphrase. If the devices do not have the same passphrase, they cannot encrypt and decrypt the data correctly.</p> <p>Use a passphrase that contains numbers, symbols, lowercase letters, and uppercase letters for better security. For example, “Gu4c4mo!3” is better than “guacamole”.</p> <p>Example: Site A: OurSharedSecret Site B: OurSharedSecret</p>	You
Encryption Method	<p>DES uses 56-bit encryption. 3DES uses 168-bit encryption. AES encryption is available at the 128-bit, 192-bit, and 256-bit levels. AES-256 bit is the most secure encryption. The two devices must use the same encryption method.</p> <p>Example: Site A: 3DES Site B: 3DES</p>	You
Authentication	<p>The two devices must use the same authentication method.</p> <p>Example: Site A: MD5 (or SHA-1) Site B: MD5 (or SHA-1)</p>	You

## Configure Gateways

A gateway is a connection point for one or more tunnels. To create a tunnel, you must set up gateways on both the local and remote endpoint devices. To configure these gateways, you must specify:

- Credential method — Either pre-shared keys or an IPSec XTM device certificate.  
For information about using certificates for BOVPN authentication, see *Certificates for Branch Office VPN (BOVPN) Tunnel Authentication* on page 876.
- Location of local and remote gateway endpoints, either by IP address or domain information.
- Settings for Phase 1 of the Internet Key Exchange (IKE) negotiation. This phase defines the security association, or the protocols and settings that the gateway endpoints will use to communicate, to protect data that is passed in the negotiation.

You can use Policy Manager to configure the gateways for each endpoint device.

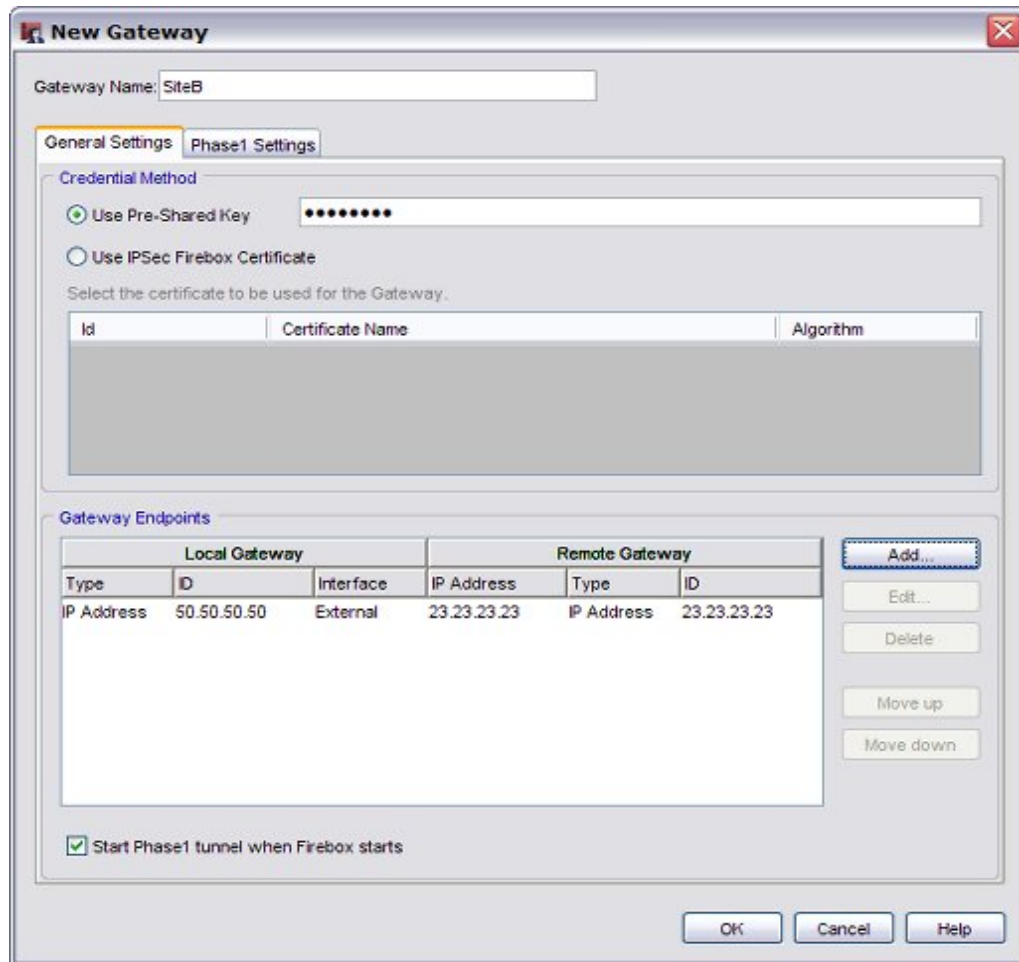
1. Select **VPN > Branch Office Gateways**.

*The Gateways dialog box appears.*



2. To add a gateway, click **Add**.

*The New Gateway dialog box appears.*



3. In the **Gateway Name** text box, type a name to identify the gateway for this XTM device.
4. From the **New Gateway** dialog box, select either **Use Pre-Shared Key** or **Use IPsec Firebox Certificate** to identify the authentication procedure this tunnel uses.

*If you selected Use Pre-Shared Key*

Type or paste the shared key. You must use the same shared key on the remote device. This shared key must use only standard ASCII characters.

*If you selected Use IPsec Firebox Certificate*

The table below the radio button shows current certificates on the XTM device. Select the certificate to use for the gateway.

For more information, see *Certificates for Branch Office VPN (BOVPN) Tunnel Authentication* on page 876.

You can now *Define Gateway Endpoints*.

## Define Gateway Endpoints

Gateway Endpoints are the local and remote gateways that a BOVPN connects. This information tells your XTM device how to identify and communicate with the remote endpoint device when it negotiates the BOVPN. It also tells the XTM device how to identify itself to the remote endpoint when it negotiates the BOVPN.

Any external interface can be a gateway endpoint. If you have more than one external interface, you can configure multiple gateway endpoints to *Configure VPN Failover*.

### Local Gateway

In the Local Gateway section, you configure the gateway ID and the interface the BOVPN connects to on your XTM device. For the gateway ID, if you have a static IP address you can select **By IP Address**. Use **By Domain Information** if you have a domain that resolves to the IP address the BOVPN connects to on your XTM device.

1. In the **Gateway Endpoints** section of the **New Gateway** dialog box, click **Add**.  
*The New Gateway Endpoints Settings dialog box appears.*

**New Gateway Endpoints Settings - SiteB**

A tunnel needs authentication on each side of the tunnel. Provide the configuration details for the gateway endpoints below.

**Local Gateway**

Specify the gateway ID for tunnel authentication.

By IP Address

IP Address: 50.50.50.50

By Domain Information

External interface: External

**Remote Gateway**

Specify the remote gateway IP address for a tunnel.

Static IP address

IP Address: 23.23.23.23

Dynamic IP address

Specify the gateway ID for tunnel authentication.

By IP Address

IP Address: 23.23.23.23

By Domain Information

2. Specify the gateway ID.



- **By IP address** — Select **By IP Address**. Type the IP address of the XTM device interface IP address or select it from the drop-down list. All configured XTM device IP addresses appear in the list.
  - **By Domain Information**—Select **By Domain Information**. Click **Configure** and select the method of domain configuration. Select **By Domain Name** or **By User ID on Domain**.
    - By Domain Name** — Type your domain name and click **OK**.
    - By User ID on Domain** — Type the user name and domain with the format `UserName@DomainName` and click **OK**.
3. From the **External Interface** drop-down list, select the interface on the XTM device with the IP address or domain you choose for the gateway ID.

## Remote Gateway

In the Remote Gateway section, you configure the gateway IP address and gateway ID for the remote endpoint device that the BOVPN connects to. The gateway IP address can be either a **Static IP address** or a **Dynamic IP address**. The gateway ID can be **By Domain Name**, **By User ID on Domain**, or **By x500 Name**. The administrator of the remote gateway device can tell you which to use.

1. Select the remote gateway IP address.
  - **Static IP address** — Select this option if the remote device has a static IP address. For IP Address, type the IP address or select it from the drop-down list.
  - **Dynamic IP address** — Select this option if the remote device has a dynamic IP address.
2. Select the gateway ID.
  - **By IP address** — Select the **By IP Address** radio button. Type the IP address or select it from the drop-down list.
  - **By Domain Information** — Select **By Domain Information**. Click **Configure** and select the method of domain configuration. Select **By Domain Name**, **By User ID on Domain**, or **By x500 Name** and type the name, user ID and domain, or x500 name. Click **OK**.



**Note** If the remote VPN endpoint uses DHCP or PPPoE to get its external IP address, set the ID type of the remote gateway to **Domain Name**. Set the peer name to the fully qualified domain name of the remote VPN endpoint. The XTM device uses the IP address and domain name to find the VPN endpoint. Make sure the DNS server used by the XTM device can identify the name.

3. Click **OK** to close the **New Gateway Endpoints Settings** dialog box.  
The **New Gateway** dialog box appears. The gateway pair you defined appears in the list of gateway endpoints.
4. Go to **Configure Mode and Transforms (Phase 1 Settings)** if you want to use Phase 1 settings other than the default values. Otherwise, click **OK**.

## Configure Mode and Transforms (Phase 1 Settings)

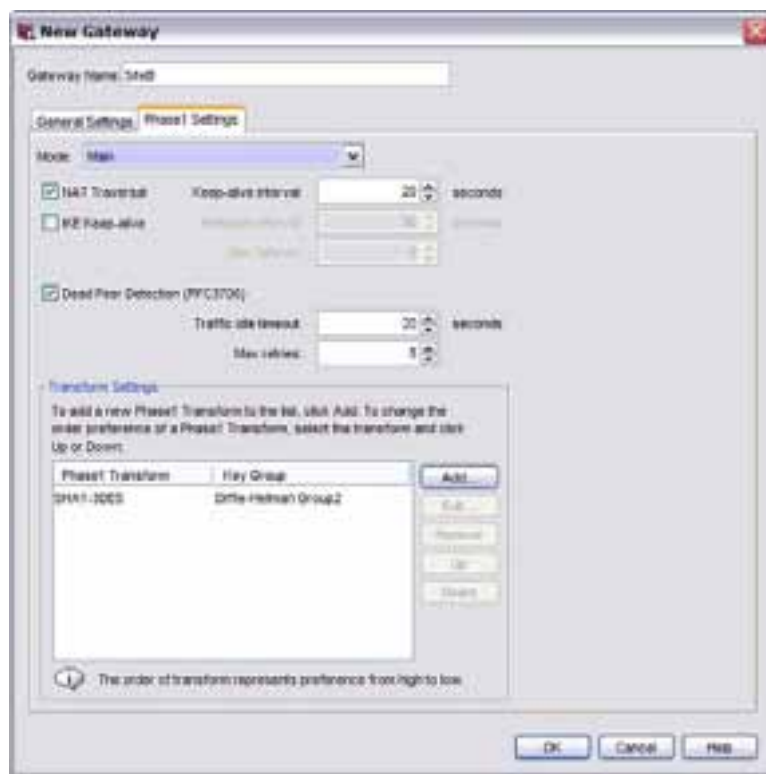
Phase 1 of establishing an IPSec connection is where the two peers make a secure, authenticated channel they can use to communicate. This is known as the ISAKMP Security Association (SA).

A Phase 1 exchange can use either *Main Mode* or *Aggressive Mode*. The mode determines the type and number of message exchanges that take place during this phase.

A transform is a set of security protocols and algorithms used to protect VPN data. During IKE negotiation, the peers make an agreement to use a certain transform.

You can define a tunnel such that it offers a peer more than one transform for negotiation. For more information, see *Add a Phase 1 Transform* on page 924.

1. In the **New Gateway** dialog box, select the **Phase1 Settings** tab.



- From the **Mode** drop-down list, select **Main**, **Aggressive**, or **Main fallback to Aggressive**.

#### *Main Mode*

This mode is more secure, and uses three separate message exchanges for a total of six messages. The first two messages negotiate policy, the next two exchange Diffie-Hellman data, and the last two authenticate the Diffie-Hellman exchange. Main Mode supports Diffie-Hellman groups 1, 2, and 5. This mode also allows you to use multiple transforms, as described in *Add a Phase 1 Transform* on page 924.

#### *Aggressive Mode*

This mode is faster because it uses only three messages, which exchange *About Diffie-Hellman Groups* data and identify the two VPN endpoints. The identification of the VPN endpoints makes Aggressive Mode less secure.

#### *Main fallback to aggressive*

The XTM device attempts Phase 1 exchange with Main Mode. If the negotiation fails, it uses Aggressive Mode.

- If you want to build a BOVPN tunnel between the XTM device and another device that is behind a NAT device, select the **NAT Traversal** check box. NAT Traversal, or UDP Encapsulation, enables traffic to get to the correct destinations.
- To have the XTM device send messages to its IKE peer to keep the VPN tunnel open, select the **IKE Keep-alive** check box.
- In the **Message Interval** text box, type or select the number of seconds that pass before the next IKE Keep-alive message is sent.

**Note** *IKE Keep-alive is used only by XTM devices. Do not enable it if the remote endpoint is a third-party IPsec device.*

- To set the maximum number of times the XTM device tries to send an IKE keep-alive message before it tries to negotiate Phase 1 again, type the number you want in the **Max failures** box.
- Use the **Dead Peer Detection** check box to enable or disable traffic-based dead peer detection. When you enable dead peer detection, the XTM device connects to a peer only if no traffic is received from the peer for a specified length of time and a packet is waiting to be sent to the peer. This method is more scalable than IKE keep-alive messages.

If you want to change the XTM device defaults, in the **Traffic idle timeout** text box, type or select the amount of time (in seconds) that passes before the XTM device tries to connect to the peer. In the **Max retries** text box, type or select the number of times the XTM device tries to connect before the peer is declared dead.

Dead Peer Detection is an industry standard that is used by most IPsec devices. We recommend that you select Dead Peer Detection if both endpoint devices support it.

**Note** *If you configure VPN failover, you must enable DPD. For more information about VPN failover, see *Configure VPN Failover* on page 959*

- The XTM device contains one default transform set, which appears in the **Transform Settings** list. This transform specifies SHA-1 authentication, 3DES encryption, and Diffie-Hellman Group 2. You can:

- Use this default transform set.
- Remove this transform set and replace it with a new one.
- Add an additional transform, as explained in *Add a Phase 1 Transform* on page 924.

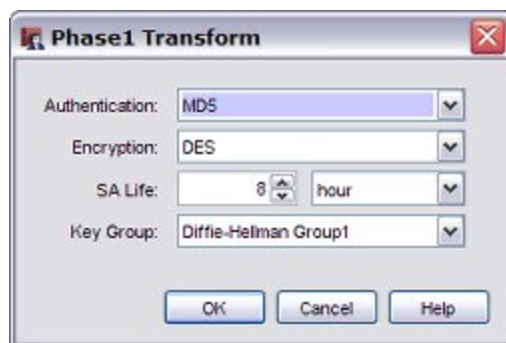
## Add a Phase 1 Transform

You can define a tunnel to offer a peer more than one transform set for negotiation. For example, one transform set might include SHA1-DES-DF1 ([authentication method]-[encryption method]-[key group]) and a second transform might include MD5-3DES-DF2, with the SHA1-DES-DF1 transform as the higher priority transform set. When the tunnel is created, the XTM device can use either SHA1-DES-DF1 or MD5-3DES-DF2 to match the transform set of the other VPN endpoint.

You can include a maximum of nine transform sets. You must specify Main Mode in the Phase 1 settings to use multiple transforms.

1. In the **New Gateway** dialog box, select the **Phase 1 Settings** tab.
2. In the **Transform Settings** section, click **Add**.

*The Phase 1 Transform dialog box appears.*



2. From the **Authentication** drop-down list, select **SHA1** or **MD5** as the type of authentication.
3. From the **Encryption** drop-down list, select **AES (128-bit)**, **AES (192-bit)**, **AES (256-bit)**, **DES**, or **3DES** as the type of encryption.
4. To change the SA (security association) life, type a number in the **SA Life** text box, and select **Hour** or **Minute** from the adjacent drop-down list.
5. From the **Key Group** drop-down list, select a Diffie-Hellman group. Fireware XTM supports groups 1, 2, and 5.  
Diffie-Hellman groups determine the strength of the master key used in the key exchange process. A higher the group number provides greater security, but more time is required to make the keys. For more information, see *About Diffie-Hellman Groups* on page 925.
6. Click **OK**.  
*The Transform appears in the New Gateway dialog box in the Transform Settings list. You can add up to nine transform sets.*
7. Repeat Steps 2–6 to add more transforms. The transform set at the top of the list is used first.
8. To change the priority of a transform set, select the transform set and click **Up** or **Down**.
9. Click **OK**.

## About Diffie-Hellman Groups

Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Higher group numbers are more secure, but require additional time to compute the key.

Fireware XTM supports Diffie-Hellman groups 1, 2, and 5:

- DH Group 1: 768-bit group
- DH Group 2: 1024-bit group
- DH Group 5: 1536-bit group

Both peers in a VPN exchange must use the same DH group, which is negotiated during Phase 1 of the IPsec negotiation process. When you define a manual BOVPN tunnel, you specify the Diffie-Hellman group as part of Phase 1 of creating an IPsec connection. This is where the two peers make a secure, authenticated channel they can use to communicate.

### DH groups and Perfect Forward Secrecy (PFS)

In addition to Phase 1, you can also specify the Diffie-Hellman group in Phase 2 of an IPsec connection. Phase 2 configuration includes settings for a security association (SA), or how data packets are secured when they are passed between two endpoints. You specify the Diffie-Hellman group in Phase 2 only when you select Perfect Forward Secrecy (PFS).

PFS makes keys more secure because new keys are not made from previous keys. If a key is compromised, new session keys are still secure. When you specify PFS during Phase 2, a Diffie-Hellman exchange occurs each time a new SA is negotiated.

The DH group you choose for Phase 2 does not need to match the group you choose for Phase 1.

### How to Choose a Diffie-Hellman Group

The default DH group for both Phase 1 and Phase 2 is Diffie-Hellman Group 1. This group provides basic security and good performance. If the speed for tunnel initialization and rekey is not a concern, use Group 2 or Group 5. Actual initialization and rekey speed depends on a number of factors. You might want to try DH Group 2 or 5 and decide whether the slower performance time is a problem for your network. If the performance is unacceptable, change to a lower DH group.

### Performance Analysis

The following table shows the output of a software application that generates 2000 Diffie-Hellman values. These figures are for a 1.7GHz Intel Pentium 4 CPU.

DH Group	No. of key pairs	Time required	Time per key pair
Group 1	2000	43 sec	21 ms
Group 2	2000	84 sec	42 ms
Group 5	2000	246 sec	123 ms

## Edit and Delete Gateways

To change the definition of a gateway

1. Select **VPN > Branch Office Gateways**.  
Or, right-click on a tunnel icon in the **BOVPN** tab of Policy Manager, and select **Gateway Property**.
2. Select a gateway and click **Edit**.  
*The Edit Gateway dialog box appears.*
3. Make your changes and click **OK**.

To delete a gateway, select the gateway and click **Remove**. You can also select multiple gateways and click **Remove** to delete them all at once.

## Disable Automatic Tunnel Startup

BOVPN tunnels are automatically created each time the XTM device starts. You can use Policy Manager to change this default behavior. A common reason to change it would be if the remote endpoint uses a third-party device that must initiate the tunnel instead of the local endpoint.

To disable automatic startup for tunnels that use a gateway:

1. Select **VPN > Branch Office Gateways**.  
*The Gateways dialog box appears.*
2. Select a gateway and click **Edit**.  
*The Edit Gateway dialog box appears.*
3. Clear the **Start Phase1 tunnel when Firebox starts** check box at the bottom of the dialog box.

## If Your XTM Device is Behind a Device That Does NAT

The XTM device can use NAT Traversal. This means that you can make VPN tunnels if your ISP does NAT (Network Address Translation) or if the external interface of your XTM device is connected to a device that does NAT. We recommend that the XTM device external interface have a public IP address. If that is not possible, follow the subsequent instructions.

Devices that do NAT frequently have some basic firewall features. To make a VPN tunnel to your XTM device when the XTM device is installed behind a device that does NAT, the NAT device must let the traffic through. These ports and protocols must be open on the NAT device:

- UDP port 500 (IKE)
- UDP port 4500 (NAT Traversal)
- IP protocol 50 (ESP)

See the documentation for your NAT device for information on how to open these ports and protocols on the NAT device.

If the external interface of your XTM device has a private IP address, you cannot use an IP address as the local ID type in the Phase 1 settings.

- If the NAT device to which the XTM device is connected has a dynamic public IP address:
  - First, set the device to Bridge Mode. For more information, see *Bridge Mode* on page 103. In Bridge Mode, the XTM device gets the public IP address on its external interface. Refer to the documentation for your NAT device for more information.
  - Set up Dynamic DNS on the XTM device. For information, see *About the Dynamic DNS Service* on page 96. In the Phase 1 settings of the Manual VPN, set the local ID type to **Domain Name**. Enter the DynDNS domain name as the Local ID. The remote device must identify your XTM device by domain name and it must use the DynDNS domain name associated with your XTM device in its Phase 1 configuration.
- If the NAT device to which the XTM device is connected has a static public IP address — In the Phase 1 settings of the Manual VPN, set the local ID type drop-down list to **Domain Name**. Enter the public IP address assigned to the external interface of the NAT device as the local ID. The remote device must identify your XTM device by domain name, and it must use the same public IP address as the domain name in its Phase 1 configuration.

## Make Tunnels Between Gateway Endpoints

After you define gateway endpoints, you can make tunnels between them. To make a tunnel, you must:

- *Define a Tunnel*
- *Configure Phase 2 Settings* for the Internet Key Exchange (IKE) negotiation. This phase sets up security associations for the encryption of data packets.

### Define a Tunnel

From Policy Manager, you can add, edit, and delete Branch Office VPN tunnels.

1. Select **VPN > Branch Office Tunnels**.  
*The Branch Office IPSec Tunnels dialog box appears.*





2. Click **Add**.  
*The New Tunnel dialog box appears.*





3. In the **Tunnel Name** text box, type a name for the tunnel. Make sure the name is unique among tunnel names, Mobile VPN group names, and interface names.
4. From the **Gateway** drop-down list, select the gateway for this tunnel to use.
 

To edit a gateway that already exists, select the name and click . Follow the procedures described in *Configure Gateways* on page 918.

To add a new gateway, click . Follow the procedures described in *Configure Gateways* on page 918.
5. To add the tunnel to the BOVPN-Allow.in and BOVPN-Allow.out policies, select the **Add this tunnel to the BOVPN-Allow policies** check box. These policies allow all traffic that matches the routes for this tunnel.
 

To restrict traffic through the tunnel, clear this check box and use the BOVPN Policy wizard as described in *Define a Custom Tunnel Policy* on page 938 to create custom policies for types of traffic that you want to allow through the tunnel.

You can now *Add Routes for a Tunnel*, *Configure Phase 2 Settings*, or *Enable Multicast Routing Through a Branch Office VPN Tunnel*.

## Edit and Delete a Tunnel

You can use Policy Manager to change or remove a tunnel.

To edit a tunnel:

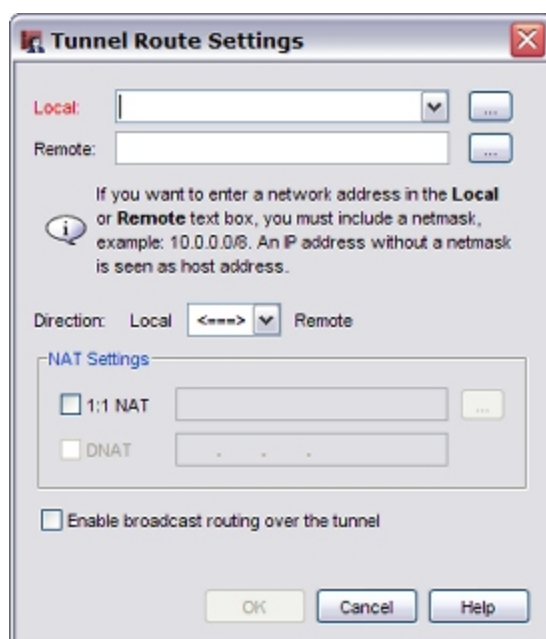
1. Select **VPN > Branch Office Tunnels**.
2. Select the tunnel and click **Edit**.  
*The Edit Tunnel dialog box appears.*
3. Make the changes and click **OK**.

To delete a tunnel:

1. From the **Branch Office IPSec Tunnels** dialog box, select the tunnel.  
You can select one or more tunnels to delete at the same time. .
2. Click **Remove**.

## Add Routes for a Tunnel

1. On the **Addresses** tab of the **New Tunnel** dialog box, click **Add**.  
*The Tunnel Route Settings dialog box appears.*



2. From the **Local** drop-down list, select the local address you want.  
You can also click the button adjacent to the **Local** drop-down list to enter a host IP address, network address, a range of host IP addresses, or a DNS name.
3. In the **Remote** box, type the remote network address.  
You can also click the adjacent button to enter a host IP address, network address, a range of host IP addresses, or a DNS name.
4. In the **Direction** drop-down list, select the direction for the tunnel. The tunnel direction determines which endpoint of the VPN tunnel can start a VPN connection through the tunnel.

5. You can enable 1-to-1 NAT and dynamic NAT for the tunnel if the address types and tunnel direction you selected are compatible. For more information, see *Set Up Outgoing Dynamic NAT Through a Branch Office VPN Tunnel* on page 939 and *Use 1-to-1 NAT Through a Branch Office VPN Tunnel* on page 944.
6. Click **OK**.

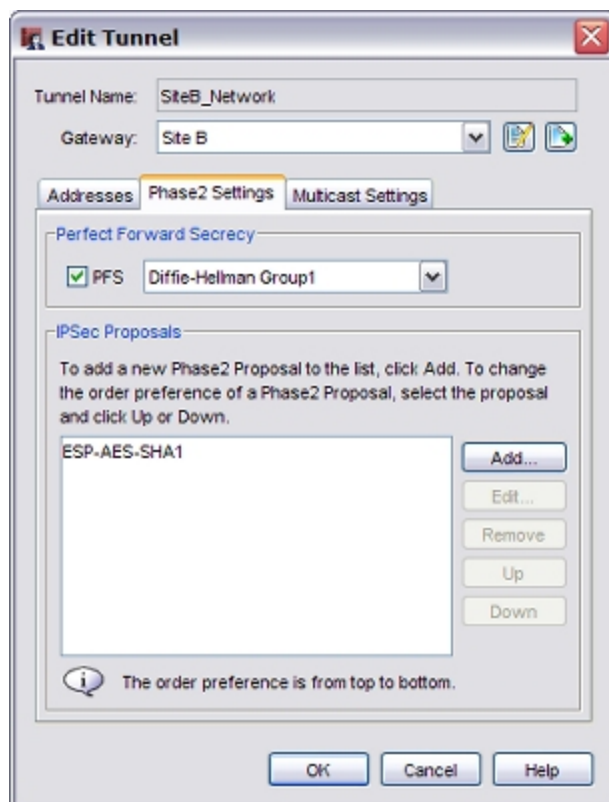
## Configure Phase 2 Settings

Phase 2 settings include settings for a security association (SA), which defines how data packets are secured when they are passed between two endpoints. The SA keeps all information necessary for the XTM device to know what it should do with the traffic between the endpoints. Parameters in the SA can include:

- Encryption and authentication algorithms used.
- Lifetime of the SA (in seconds or number of bytes, or both).
- The IP address of the device for which the SA is established (the device that handles IPSec encryption and decryption on the other side of the VPN, not the computer behind it that sends or receives traffic).
- Source and destination IP addresses of traffic to which the SA applies.
- Direction of traffic to which the SA applies (there is one SA for each direction of traffic, incoming and outgoing).

To configure Phase 2 settings:

1. From the **New Tunnel** dialog box, select the **Phase2 Settings** tab.



2. Select the **PFS** check box if you want to enable Perfect Forward Secrecy (PFS). If you enable PFS, select the Diffie-Hellman group.

Perfect Forward Secrecy gives more protection to keys that are created in a session. Keys made with PFS are not made from a previous key. If a previous key is compromised after a session, your new session keys are secure. For more information, see *About Diffie-Hellman Groups* on page 925.

3. The XTM device contains one default proposal, which appears in the **IPSec Proposals** list. This proposal specifies the ESP data protection method, AES encryption, and SHA-1 authentication. You can either:
  - Use the default proposal.
  - Remove the default proposal and replace it with a new one.
  - Add an additional proposal, as explained in *Add a Phase 2 Proposal* on page 932.

You can add more than one Phase 2 proposal in the Phase 2 Settings tab. However, you cannot add AH and ESP phase 2 proposals to the same Phase 2 configuration.

If you plan to use the IPSec pass-through feature, you must use a proposal with ESP (Encapsulating Security Payload) as the proposal method. IPSec pass-through supports ESP but not AH. For more information on IPSec pass-through, see *About Global VPN Settings* on page 935.

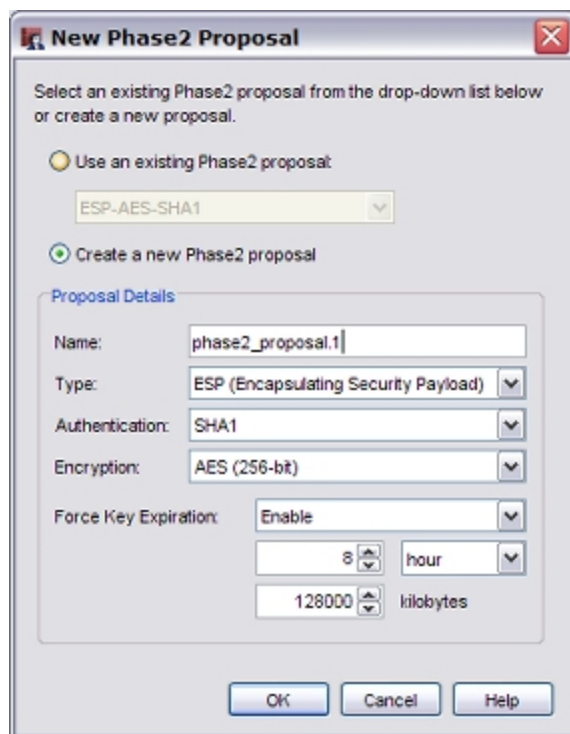
## Add a Phase 2 Proposal

You can define a tunnel to offer a peer more than one proposal for Phase 2 of the IKE. For example, you might specify ESP-3DES-SHA1 in one proposal, and ESP-DES-MD5 for second proposal. When traffic passes through the tunnel, the security association can use either ESP-3DES-SHA1 or ESP-DES-MD5 to match the transform settings on the peer.

You can include a maximum of nine proposals.

To add a new proposal:

1. In the **New Tunnel** or **Edit Tunnel** dialog box, select the **Phase 2 Settings** tab.
2. In the **IPSec Proposals** section, click **Add**.



## Add an Existing Proposal

There are six pre-configured proposals that you can choose. The names follow the format <Type>-<Authentication>-<Encryption>. For all six, Force Key Expiration is enabled for 8 hours or 128000 kilobytes.

To use one of the six pre-configured proposals:

1. Select **Use an existing Phase 2 proposal**.
2. Select the proposal you want to add from the drop-down list and click **OK**.

## Create a New Proposal

1. On the **New Phase2 Proposal** dialog box, select the **Create a new Phase 2 proposal** check box. Or, select **VPN > Phase2 Proposals**. The **Phase2 Proposals** dialog box appears. Click **Add**.
2. In the **Name** text box, type a name for the new proposal.  
If you opened the dialog box from **VPN > Phase 2 Proposals**, an optional **Description** text box appears.  
In the **Description** text box, type a description to identify this proposal (optional).
3. From the **Type** drop-down list, select **ESP** or **AH** as the proposal method. We recommend that you use ESP (Encapsulating Security Payload). The differences between ESP and AH (Authentication Header) are:
  - ESP is authentication with encryption.
  - AH is authentication only. ESP authentication does not include the protection of the IP header, while AH does.

- IPsec pass-through supports ESP but not AH. If you plan to use the IPsec pass-through feature, you must specify ESP as the proposal method. For more information on IPsec pass-through, see *About Global VPN Settings* on page 935.
4. From the **Authentication** drop-down list, select **SHA1**, **MD5**, or **None** for the authentication method.
  5. If you selected **ESP** from the **Type** drop-down list, from the **Encryption** drop-down list, select the encryption method.  
The options are DES, 3DES, and AES 128, 192, or 256 bit, which appear in the list from the most simple and least secure to most complex and most secure.
  6. To make the gateway endpoints generate and exchange new keys after a quantity of time or amount of traffic passes, select the **Force Key Expiration** check box. In the fields below, enter a quantity of time and a number of bytes after which the key expires.  
If Force Key Expiration is disabled, or if it is enabled and both the time and kilobytes are set to zero, the XTM device tries to use the key expiration time set for the peer. If this is also disabled or zero, the XTM device uses a default key expiration time of 8 hours.  
The maximum time before a forced key expiration is one year.
  7. Click **OK**.

## Edit or Clone a Proposal

When you clone a proposal, you copy a proposal that already exists and save it with a new name. You must do this if you want to edit a predefined proposal, because you can change only user-defined proposals.

1. Select **VPN > Phase2 Proposals**.  
*The Phase2 Proposals dialog box appears.*
2. Select a proposal and click **Edit** or **Clone**.
3. Make changes to the fields as described in the **Create a new proposal** section of this topic. Click **OK**.

## Change Order of Tunnels

The order of VPN tunnels is particularly important when more than one tunnel uses the same routes or when the routes overlap. A tunnel higher in the list of tunnels on the **Branch Office IPsec Tunnels** dialog box takes precedence over a tunnel below it when traffic matches tunnel routes of multiple tunnels.

From Policy Manager, you can change the order in which the XTM device attempts connections. You can only change the order of tunnels for manual VPN tunnels.

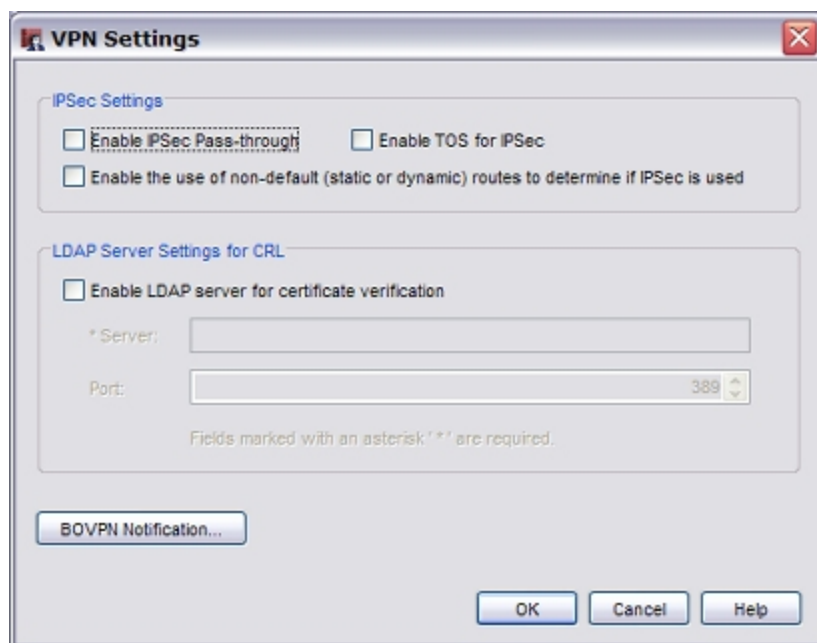
1. Select **VPN > Branch Office Tunnels**.  
*The Branch Office IPsec Tunnels dialog box appears.*
2. Select a tunnel and click **Move Up** or **Move Down** to move it up or down in the list.

## About Global VPN Settings

From Policy Manager, you can select settings that apply to manual BOVPN tunnels, managed BOVPN tunnels, and Mobile VPN with IPsec tunnels.

1. Select **VPN > VPN Settings**.

The *VPN Settings dialog box* appears.



2. Configure the settings for your VPN tunnels, as explained in the subsequent sections.

### Enable IPsec Pass-Through

For a user to make IPsec connections to an XTM device located behind a different XTM device, you must make sure the **Enable IPsec Pass-through** check box is selected. For example, if mobile employees are at a customer location that has a XTM device, they can use IPsec to make IPsec connections to their network. For the local XTM device to correctly allow the outgoing IPsec connection, you must also add an IPsec policy to the configuration.

When you enable IPsec pass-through, a policy called *WatchGuard IPsec* is automatically added to the configuration. The policy allows traffic from any trusted or optional network to any destination. When you disable IPsec pass-through, the *WatchGuard IPsec* policy is automatically deleted.

### Enable TOS for IPsec

Type of Service (TOS) is a set of four-bit flags in the IP header that can tell routing devices to give an IP datagram more or less priority than other datagrams. Firewall XTM gives you the option to allow IPsec tunnels to clear or maintain the settings on packets that have TOS flags. Some ISPs drop all packets that have TOS flags.

If you do not select the **Enable TOS for IPSec** check box, all IPSec packets do not have the TOS flags. If the TOS flags were set before, they are removed when Fireware XTM encapsulates the packet in an IPSec header.

When the **Enable TOS for IPSec** check box is selected and the original packet has TOS flags, Fireware XTM keeps the TOS flags set when it encapsulates the packet in an IPSec header. If the original packet does not have the TOS flags set, Fireware XTM does not set the TOS flag when it encapsulates the packet in an IPSec header.

Make sure to carefully consider whether to select this check box if you want to apply QoS marking to IPSec traffic. QoS marking can change the setting of the TOS flag. For more information on QoS marking, see *About QoS Marking* on page 512.

## Enable the Use of Non-Default (Static or Dynamic) Routes to Determine if IPSec is Used

When this option is not enabled, all packets that match the tunnel route specified in the IPSec gateway are sent through the IPSec VPN. If this option is enabled, the XTM device uses the routing table to determine whether to send the packet through the IPSec VPN tunnel.

*If a default route is used to route a packet*

The packet is encrypted and sent through the VPN tunnel, to the interface specified in the VPN gateway configuration.

*If a non-default route is used to route a packet*

The packet is routed to the interface specified in the non-default route in the routing table. When a non-default route is used, the decision about whether to send the packet through the IPSec VPN tunnel depends on the interface specified in the routing table. If the interface in the non-default route matches the interface in the BOVPN gateway, the packet goes through the BOVPN tunnel configured for that interface. For example, if the BOVPN gateway interface is set to Eth0, and the matched non-default route uses Eth1 as the interface, the packet is not sent through the BOVPN tunnel. However, if the matched non-default route uses Eth0 as the interface, the packet is sent through the BOVPN tunnel.

This feature works with any non-default route (static or dynamic). You can use this feature in conjunction with dynamic routing to enable dynamic network failover from a private network route to an encrypted IPSec VPN tunnel.

For example, consider an organization that sends traffic between two networks, Site A and Site B. They use a dynamic routing protocol to send traffic between the two sites over a private network connection, with no VPN required. The private network is connected to the Eth1 interface of each device. They have also configured a BOVPN tunnel between the two sites to send BOVPN traffic over the local Internet connection, over the Eth0 interface of each device. They want to send traffic over the BOVPN tunnel only if the private network connection is not available.

If they select the **Enable the use of non-default (static or dynamic) routes to determine if IPSec is used** check box in the Global VPN Settings, the XTM device sends traffic over the private network if a dynamic route to that network is present over the Eth1 interface. Otherwise, it sends traffic over the encrypted IPSec BOVPN tunnel on the Eth0 interface.



## Enable LDAP Server for Certificate Verification

When you create a VPN gateway, you specify a credential method for the two VPN endpoints to use when the tunnel is created. If you choose to use an IPsec XTM device certificate, you can identify an LDAP server that validates the certificate. Type the IP address for the LDAP server. You can also specify a port if you want to use a port other than 389.

## BOVPN Notification

Click **BOVPN Notification** to configure the XTM device to send a notification when a BOVPN tunnel is down. A dialog box appears for you to set parameters for the notification.

For information on the options in this dialog box, see *Set Logging and Notification Preferences* on page 723.

This setting does not apply to Mobile VPN with IPsec tunnels.

## Define a Custom Tunnel Policy

Tunnel policies are sets of rules that apply to tunnel connections. By default, a new VPN tunnel is automatically added to the BOVPN-Allow.in and BOVPN-Allow.out policies, which allow all traffic to use the tunnel. From Policy Manager, you can configure the tunnel such that it is not added to this policy. See *Define a Tunnel* to make sure you clear the **Add this tunnel to the BOVPN-Allow policies** check box. Then, create a custom VPN policy to allow specified policy types. You can also keep the default setting and then add other policies for other types of traffic, such as HTTP traffic.

1. Select **VPN > Create BOVPN Policy**.  
*The BOVPN Policy Wizard starts.*
2. Complete the wizard, as described in the subsequent sections.

## Choose a Name for the Policies

The name you choose is prepended to ".in" and ".out" to create the firewall policy names for incoming and outgoing tunnels, respectively. For example, if you use "williams" as the name base, the wizard creates the policies "williams.in" and "williams.out."

## Select the Policy Type

Specify the traffic type allowed to pass through the BOVPN tunnel.

## Select the BOVPN Tunnels

Select the BOVPN tunnels to which the policies created by this wizard apply.

## Create an Alias for the Tunnels

(Optional) As with the policy name, the name you specify is prepended to ".in" and ".out" to create the alias names for incoming and outgoing tunnels, respectively. You can use these aliases in other policies as well.

We recommend that you create an alias when you create policies for many BOVPN tunnels. Include those tunnels in the alias. You can then modify the alias as you add or remove tunnels, rather than create a new policy for each set of tunnels. For information on how to create an alias, see *Create an Alias* on page 379.

## The BOVPN Policy Wizard has Completed Successfully

The final screen shows which policies and aliases were created by the wizard.

## Set Up Outgoing Dynamic NAT Through a Branch Office VPN Tunnel

You can use dynamic NAT (DNAT) through Branch Office VPN (BOVPN) tunnels. Dynamic NAT acts as unidirectional NAT, and keeps the VPN tunnel open in one direction only. This can be helpful when you make a BOVPN tunnel to a remote site where all VPN traffic comes from one public IP address.

For example, suppose you want to create a BOVPN tunnel to a business partner so you can get access to their database server, but you do not want this company to get access to any of your resources. Your business partner wants to allow you access, but only from a single IP address so they can monitor the connection.

You must have the external and trusted network IP addresses of each VPN endpoint to complete this procedure. If you enable dynamic NAT through a BOVPN tunnel, you cannot use the VPN Failover feature for that VPN tunnel.

The step by step instructions below work with any BOVPN that uses dynamic NAT to make all traffic from one endpoint appear to come from a single IP address. The subsequent images show the settings for a BOVPN where all traffic from Site A must come from the public IP of Site A.

### *Site A*

Public IP—50.50.50.50

Trusted Network—10.0.1.1/24

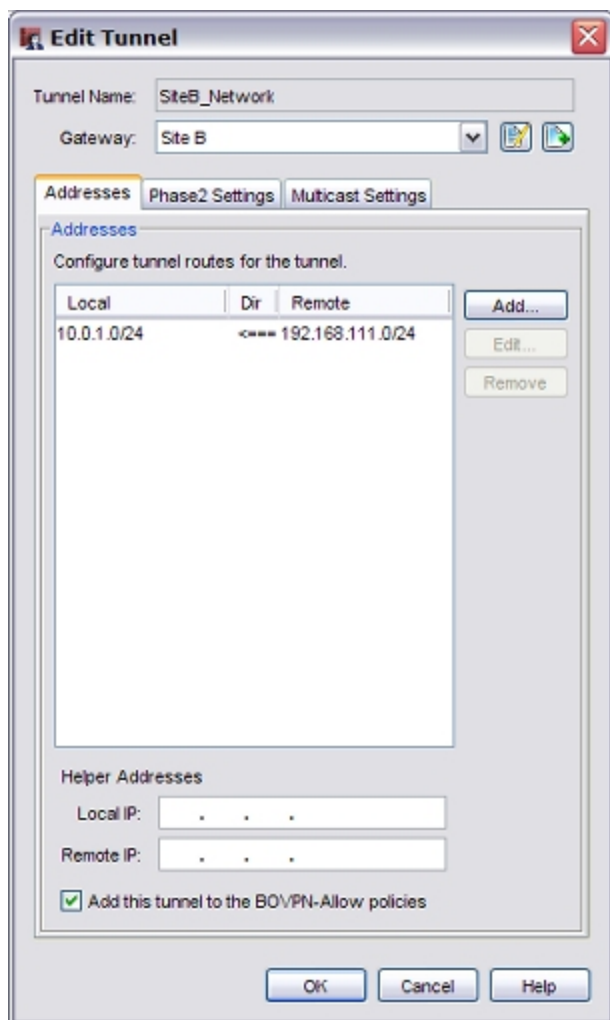
### *Site B*

Public IP—23.23.23.23

Trusted Network—192.168.111.1/24

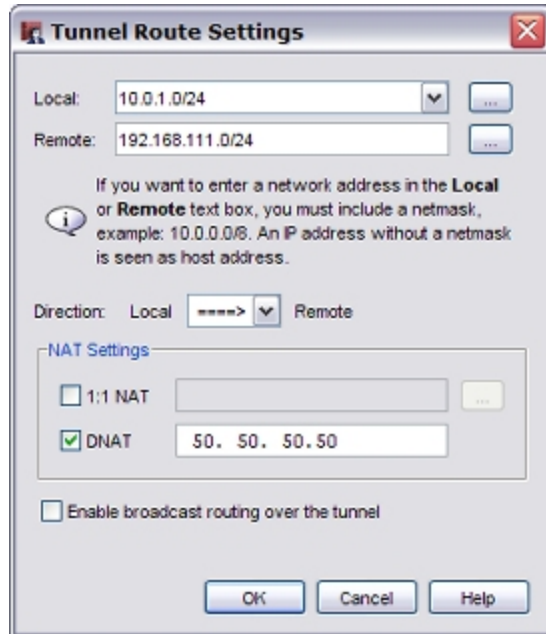
## Configure the Endpoint Where All Traffic Must Appear to Come from a Single Address (Site A)

1. From Policy Manager, configure the gateway for the BOVPN.  
For more information, see *Configure Gateways* on page 918.
2. Select **VPN > Branch Office Tunnels**.
3. Click **Add** to add a new tunnel, or select a tunnel and click **Edit**.  
*The Add Tunnel or Edit Tunnel dialog box appears.*



4. Select the gateway from the **Gateway** drop-down list.
5. On the **Addresses** tab, click **Add**.

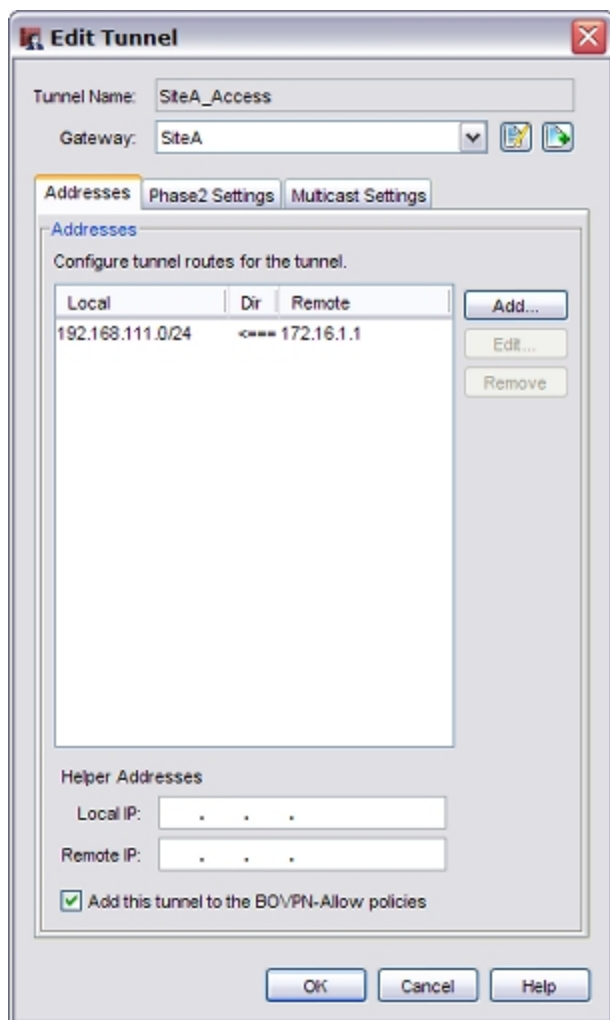
*The Tunnel Route Settings dialog box opens.*



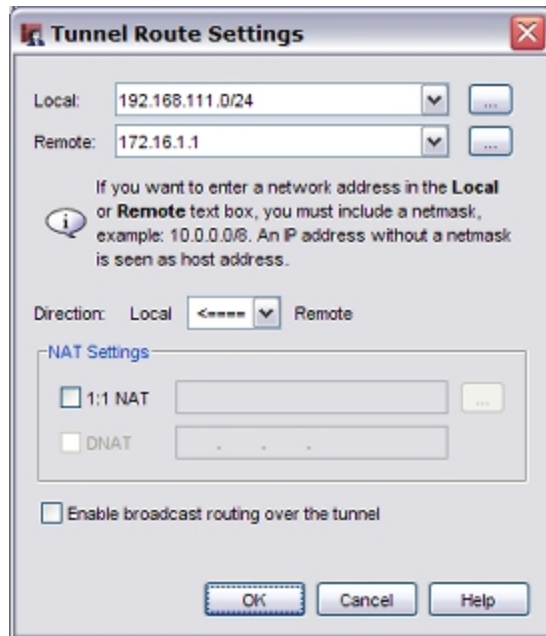
6. From the **Local** drop-down list, select the local address.  
You can also click the button adjacent to the **Local** drop-down list to type a host IP address, network address, a range of host IP addresses, or a DNS name.
7. In the **Remote** box, type the remote network address.  
You can also click the adjacent button to type a host IP address, network address, a range of host IP addresses, or a DNS name.
8. In the **Direction** drop-down list, select the second option where the arrow points to **Remote**.
9. In the **NAT Settings** area, select the **DNAT** check box. In the adjacent text box, type the IP address that the remote network sees as the source for all traffic through the tunnel.
10. Click **OK** twice, click **Close**, and save the changes to the XTM device.

## Configure the Endpoint that Expects All Traffic to Come from a Single IP Address (Site B)

1. From Policy Manager, configure the gateway for the BOVPN. For more information, see *Configure Gateways* on page 918.
2. Select **VPN > Branch Office Tunnels**. Click **Add** to add a new tunnel or select an existing tunnel and click **Edit**.  
*The Add Tunnel or Edit Tunnel dialog box opens.*



3. Select the gateway from the **Gateways** drop-down list.
4. On the **Addresses** tab, click **Add**.  
*The Tunnel Route Settings dialog box opens.*



5. From the **Local** drop-down list, select the local address you want. You can also click the button adjacent to the **Local** drop-down list to type a host IP address, network address, a range of host IP addresses, or a DNS name. This must match the Remote address in step 6 above.
6. In the **Remote** text box, type the remote IP address. You can also click the adjacent button to enter a host IP address. This must match the DNAT address in step 8 above.
7. From the **Direction** drop-down list, select the third option where the arrow points to **Local**.
8. Do not select anything in the **NAT Settings** area.
9. Click **OK** twice, click **Close**, and save the changes to the XTM device.

When the XTM device at the remote site restarts, the two XTM devices negotiate a VPN tunnel. The first XTM device applies dynamic NAT to all traffic sent to the trusted network of the second XTM device. When this traffic reaches the remote site, it arrives as traffic that originated from the DNAT IP address.

## Use 1-to-1 NAT Through a Branch Office VPN Tunnel

When you create a Branch Office VPN (BOVPN) tunnel between two networks that use the same private IP address range, an IP address conflict occurs. To create a tunnel without this conflict, both networks must apply 1-to-1 NAT to the VPN. 1-to-1 NAT makes the IP addresses on your computers appear to be different from their true IP addresses when traffic goes through the VPN.

1-to-1 NAT maps one or more IP addresses in one range to a second IP address range of the same size. Each IP address in the first range maps to an IP address in the second range. In this document, we call the first range the real IP addresses and we call the second range the masqueraded IP addresses. For more information on 1-to-1 NAT, see *About 1-to-1 NAT* on page 168.

### 1-to-1 NAT and VPNs

When you use 1-to-1 NAT through a BOVPN tunnel:

- When a computer in your network sends traffic to a computer at the remote network, the XTM device changes the source IP address of the traffic to an IP address in the masqueraded IP address range. The remote network sees the masqueraded IP addresses as the source of the traffic.
- When a computer at the remote network sends traffic to a computer at your network through the VPN, the remote office sends the traffic to the masqueraded IP address range. The XTM device changes the destination IP address to the correct address in the real IP address range and then sends the traffic to the correct destination.

1-to-1 NAT through a VPN affects only the traffic that goes through that VPN. The rules you see in Policy Manager at **Network > NAT** do not affect traffic that goes through a VPN.

### Other Reasons to Use 1-to-1 NAT Through a VPN

In addition to the previous situation, you would also use 1-to-1 NAT through a VPN if the network to which you want to make a VPN already has a VPN to a network that uses the same private IP addresses you use in your network. An IPSec device cannot route traffic to two different remote networks when the two networks use the same private IP addresses. You use 1-to-1 NAT through the VPN so that the computers in your network appear to have different (masqueraded) IP addresses. However, unlike the situation described at the beginning of this topic, you need to use NAT only on your side of the VPN instead of both sides.

A similar situation exists when two remote offices use the same private IP addresses and both remote offices want to make a VPN to your XTM device. In this case, one of the remote offices must use NAT through its VPN to your XTM device to resolve the IP address conflict.

### Alternative to Using NAT

If your office uses a common private IP address range such as 192.168.0.x or 192.168.1.x, it is very likely that you will have a problem with IP address conflicts in the future. These IP address ranges are often used by broadband routers or other electronic devices in homes and small offices. You should consider changing to a less common private IP address range, such as 10.x.x.x or 172.16.x.x.



## How to Set Up the VPN

1. Select a range of IP addresses that your computers show as the source IP addresses when traffic comes from your network and goes to the remote network through the BOVPN. Consult with the network administrator for the other network to select a range of IP addresses that are not in use. Do not use any of the IP addresses from:
  - The trusted, optional, or external network connected to your XTM device
  - A secondary network connected to a trusted, optional, or external interface of your XTM device
  - A routed network configured in your XTM device policy (**Network > Routes**)
  - Networks to which you already have a BOVPN tunnel
  - Mobile VPN virtual IP address pools
  - Networks that the remote IPSec device can reach through its interfaces, network routes, or VPN routes
2. *Configure Gateways* for the local and remote XTM devices.
3. *Make Tunnels Between Gateway Endpoints*. In the **Tunnel Route Settings** dialog box for each XTM device, select the **1:1 NAT** check box and type its masqueraded IP address range in the adjacent text box.

The number of IP addresses in this text box must be exactly the same as the number of IP addresses in the **Local** text box at the top of the dialog box. For example, if you use slash notation to indicate a subnet, the value after the slash must be the same in both text boxes. For more information, see *About Slash Notation* on page 3.

You do not need to define anything in the **Network > NAT** settings in Policy Manager. These settings do not affect VPN traffic.

## Example

Suppose two companies, Site A and Site B, want to make a Branch Office VPN between their trusted networks. Both companies use a WatchGuard XTM device with Fireware XTM. Both companies use the same IP addresses for their trusted networks, 192.168.1.0/24. Each company's XTM device uses 1-to-1 NAT through the VPN. Site A sends traffic to Site B's masqueraded range and the traffic goes outside Site A's local subnet. Also, Site B sends traffic to the masqueraded range that Site A uses. This solution solves the IP address conflict at both networks. The two companies agree that:

- Site A makes its trusted network appear to come from the 192.168.100.0/24 range when traffic goes through the VPN. This is Site B's masqueraded IP address range for this VPN.
- Site B makes its trusted network appear to come from the 192.168.200.0/24 range when traffic goes through the VPN. This is Site A's masqueraded IP address range for this VPN.

## Define a Branch Office Gateway on Each XTM Device

The first step is to make a gateway that identifies the remote IPSec device. When you make the gateway, it appears in the list of gateways in Policy Manager. To see the list of gateways from Policy Manager, select **VPN > Branch Office Gateways**.

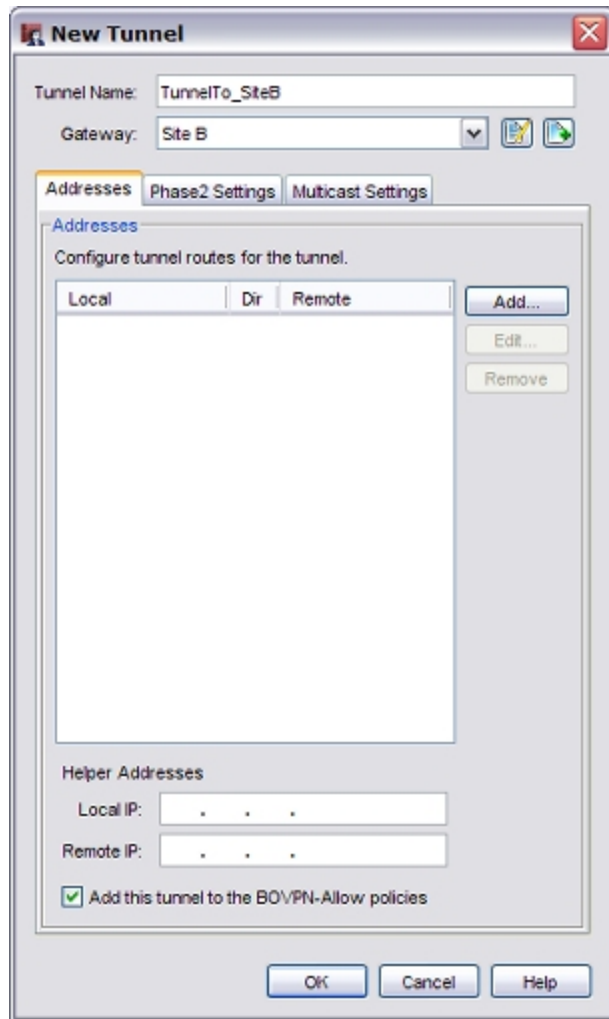


## Configure the Local Tunnel

1. Select **VPN > Branch Office Tunnels**.  
*The Branch Office IPsec Tunnels dialog box appears.*



2. Click **Add**.  
*The New Tunnel dialog box appears.*

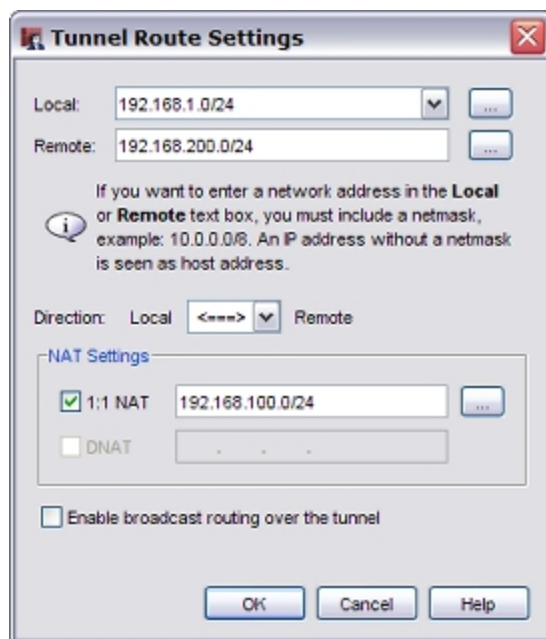


3. Type a descriptive name for the tunnel. The example uses "TunnelTo\_SiteB".
4. From the **Gateway** drop-down list, select the gateway that points to the IPsec device of the remote office. The example uses the gateway called "SiteB".
5. Select the **Phase 2 Settings** tab. Make sure the Phase 2 settings match what the remote office uses for Phase 2.
6. Select the **Addresses** tab. Click **Add** to add the local-remote pair.  
*The Tunnel Route Settings dialog box appears.*
7. and In the **Local** text box, type the real IP address range of the local computers that use this VPN. This example uses 192.168.1.0/24.
8. In the **Remote** text box, type the private IP address range that the local computers send traffic to.

In this example, the remote office Site B uses 1-to-1 NAT through its VPN. This makes Site B's computers appear to come from Site B's masqueraded range, 192.168.200.0/24. The local computers at Site A send traffic to Site B's masqueraded IP address range. If the remote network does not use NAT through its VPN, type the real IP address range in the **Remote** text box.

9. Select the **1:1 NAT** check box and type the masqueraded IP address range for this office. This is the range of IP addresses that the computers protected by this XTM device show as the source IP

address when traffic comes from this XTM device and goes to the other side of the VPN. (The **1:1 NAT** check box is enabled after you type a valid host IP address, a valid network IP address, or a valid host IP address range in the **Local** text box.) Site A uses 192.168.100.0/24 for its masqueraded IP address range.

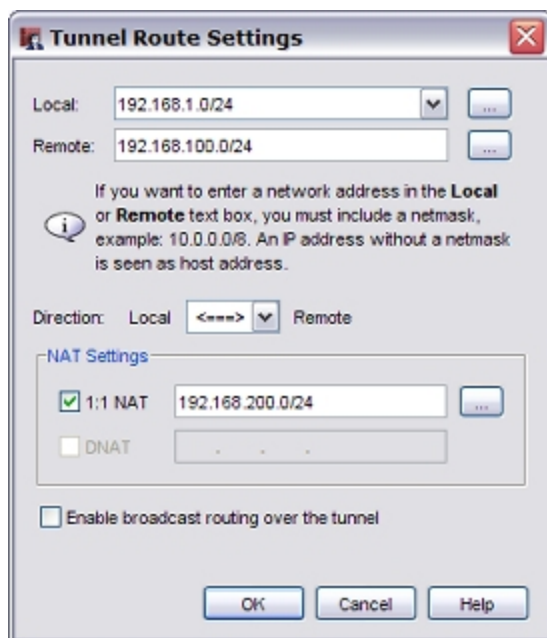


10. Click **OK**. The device adds the new tunnel to the BOVPN-Allow.out and BOVPN-Allow.in policies on the **Firewall** tab of Policy Manager.
11. *Save the Configuration File.*

If you need 1-to-1 NAT on your side of the VPN only, you can stop here. The device at the other end of the VPN must configure its VPN to accept traffic from your masqueraded range.

## Configure the Remote Tunnel

1. Follow Steps 1–6 in the previous procedure to add the tunnel on the remote XTM device. Make sure the Phase 2 settings match.
2. In the **Local** text box, type the real IP address range of the local computers that use this VPN. This example uses 192.168.1.0/24.
3. In the **Remote** text box, type the private IP address range that the computers at the remote office send traffic to. In our example, Site A does 1-to-1 NAT through its VPN. This makes the computers at Site A appear to come from its masqueraded range, 192.168.100.0/24. The local computers at Site B send traffic to the masqueraded IP address range of Site A.
4. Select the **1:1 NAT** check box and type the masqueraded IP address range of this site. This is the range of IP addresses that computers behind this XTM device show as the source IP address when traffic comes from this XTM device and goes to the other side of the VPN. Site B uses 192.168.200.0/24 for its masqueraded IP address range.



5. Click **OK**. The device adds the new tunnel to the BOVPN-Allow.out and BOVPN-Allow.in policies.

## Define a Route for All Internet-Bound Traffic

When you enable remote users to access the Internet through a VPN tunnel, the most secure setup is to require that all remote user Internet traffic is routed through the VPN tunnel to the XTM device. From the XTM device, the traffic is then sent back out to the Internet. With this configuration (known as a hub route or default-route VPN), the XTM device is able to examine all traffic and provide increased security, although more processing power and bandwidth on the XTM device is used. When you use default-route VPN, a dynamic NAT policy must include the outgoing traffic from the remote network. This allows remote users to browse the Internet when they send all traffic to the XTM device.

When you define a default route through a BOVPN tunnel, you must do three things:

- Configure a BOVPN on the remote XTM device (whose traffic you want to send through the tunnel) to send all traffic from its own network address to 0.0.0.0/0.
- Configure a BOVPN on the central XTM device to allow traffic to pass through it to the remote XTM device.
- Add a route on the central XTM device from 0.0.0.0/0 to the network address of the remote XTM device.

Before you begin the procedures in this topic, you must have already created a manual branch office VPN between the central and remote XTM devices. For information on how to do this, see *About Manual Branch Office VPN Tunnels* on page 914.

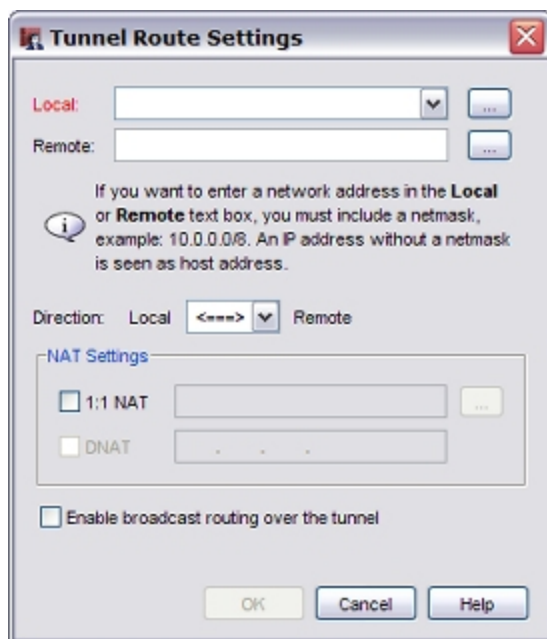
## Configure the BOVPN Tunnel on the Remote XTM Device

1. From Policy Manager, open the configuration file on the remote XTM device.
2. Select **VPN > Branch Office Tunnels**. Find the name of the tunnel to the central XTM device and click **Edit**.

*The Edit Tunnels dialog box appears.*

3. Click **Add**.

*The Tunnel Route Settings dialog box appears.*



4. From the **Local** drop-down list, select or type the trusted network address of the remote XTM device.
5. In the **Remote** text box, type 0.0.0.0/0 and click **OK**.
6. Select any other tunnel to the central XTM device and click **Remove**.
7. Click **OK** and *Save the Configuration File*.

## Configure the BOVPN Tunnel on the Central XTM Device

1. From Policy Manager, open the configuration file on the central XTM device.
2. Select **VPN > Branch Office Tunnels**. Find the name of the tunnel to the remote XTM device and click **Edit**.  
*The Edit Tunnels dialog box appears.*
3. Click **Add**.  
*The Tunnel Route Settings dialog box appears.*
4. Click the button adjacent to the **Local** drop-down list. Select **Network IP** from the **Choose Type** drop-down list. Type 0.0.0.0/0 for **Value** and click **OK**.
5. In the **Remote** text box, type the trusted network address of the remote XTM device and click **OK**.
6. Select any other tunnel to the remote XTM device and click **Remove**.
7. Click **OK** and *Save the Configuration File*.

## Add a Dynamic NAT Entry on the Central XTM Device

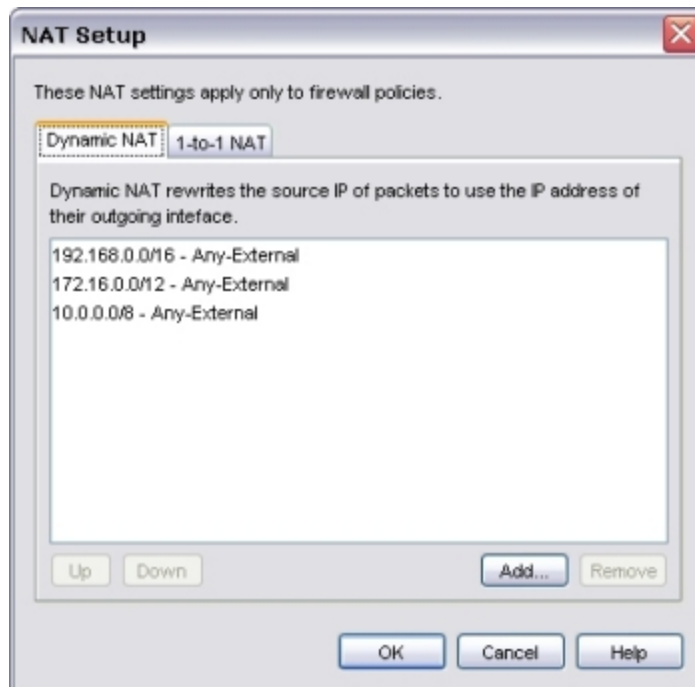
To allow a computer with a private IP address to access the Internet through the XTM device, you must configure the central XTM device to use dynamic NAT. With dynamic NAT, the XTM device replaces the private IP address included in a packet sent from a computer protected by the XTM device with the public IP address of the XTM device itself. By default, dynamic NAT is enabled and active for the three RFC-approved private network addresses:

192.168.0.0/16 - Any-External  
172.16.0.0/12 - Any-External  
10.0.0.0/8 - Any-External

When you set up a default route through a branch office VPN tunnel to another XTM device, you must add a dynamic NAT entry for the subnet behind the remote XTM device if its IP addresses are not within one of the three private network ranges.

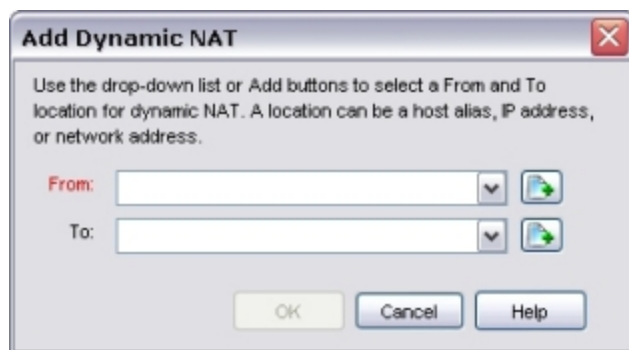
1. Select **Network > NAT**.


*The NAT Setup dialog box appears.*



2. On the **Dynamic NAT** tab of the **NAT Setup** dialog box, click **Add**.

*The Add Dynamic NAT dialog box appears.*



3. Adjacent to the **From** drop-down list, click .
4. In the **Choose Type** drop-down list, select **Network IP**. Type the network IP address of the network behind the remote XTM device in the **Value** field. Click **OK**.
5. In the **To** drop-down list, select **Any-External**.
6. Click **OK** to close the **Add Dynamic NAT** dialog box.
7. Click **OK**.
8. *Save the Configuration File* to the central XTM device.

## Enable Multicast Routing Through a Branch Office VPN Tunnel

You can enable multicast routing through a Branch Office VPN (BOVPN) tunnel to support one-way multicast streams between networks protected by XTM devices. For example, you can use multicast routing through a BOVPN tunnel to stream media from a video on demand (VOD) server to users on the network at the other end of a branch office VPN tunnel.

**Note** *Multicast routing through a BOVPN tunnel is supported only between XTM devices.*

When you enable multicast routing through a BOVPN tunnel, the tunnel sends multicast traffic from a single IP address on one side of the tunnel to an IP Multicast Group address. You configure the multicast settings in the tunnel to send multicast traffic to this IP Multicast Group address through the tunnel.

You must configure the multicast settings on each XTM device differently. You must configure the tunnel on one XTM device to send multicast traffic through the tunnel, and configure the tunnel settings on the other XTM device to receive multicast traffic. You can configure only one origination IP address per tunnel.

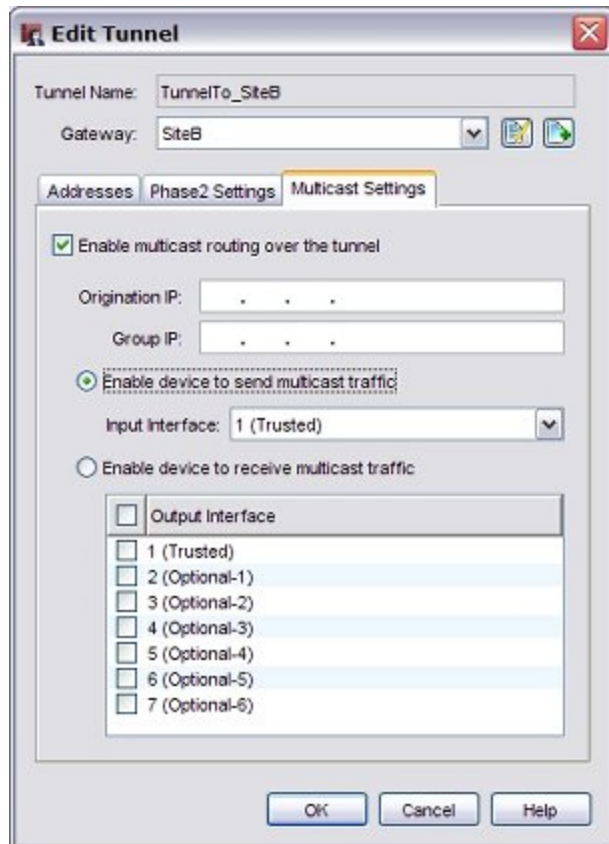
When you enable multicast routing through a BOVPN tunnel, the XTM device creates a GRE tunnel inside the IPsec VPN tunnel between the networks. The XTM device sends the multicast traffic through the GRE tunnel. The GRE tunnel requires an unused IP address on each side of the tunnel. You must configure helper IP addresses for each end of the BOVPN tunnel.



## Enable an XTM Device to Send Multicast Traffic Through a Tunnel

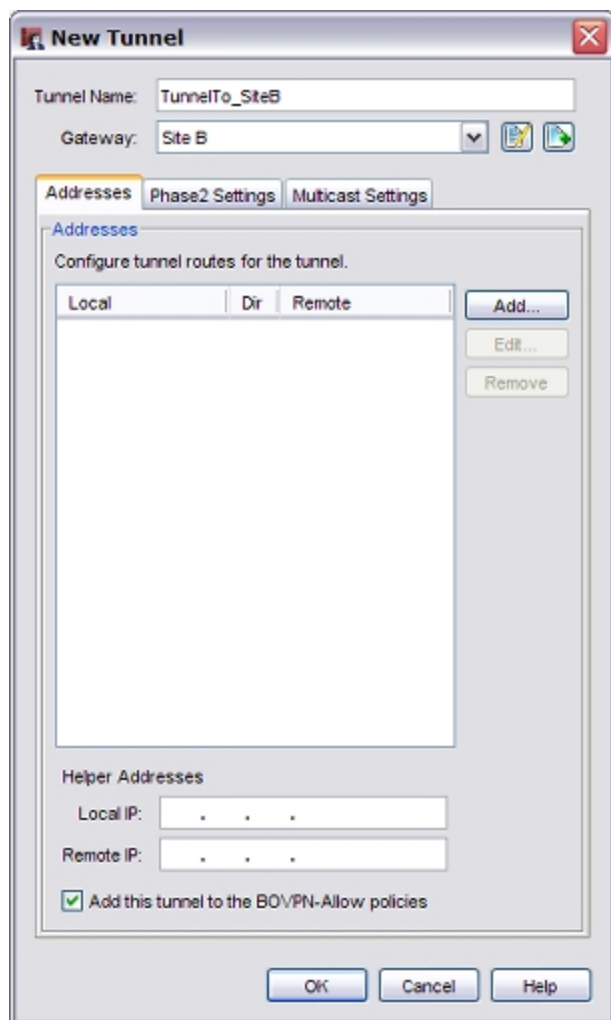
On the XTM device from which the multicast traffic is sent, edit the tunnel configuration to enable the device to send multicast traffic through the BOVPN tunnel.

1. Select **VPN > Branch Office Tunnels**.
2. Select a tunnel and click **Edit**.
3. From the **Edit Tunnel** dialog box, click the **Multicast Settings** tab.



4. Select the **Enable multicast routing over the tunnel** check box.
5. In the **Origination IP** text box, type the IP address of the originator of the traffic.
6. In the **Group IP** text box, type the multicast IP address to receive the traffic.
7. Select **Enable device to send multicast traffic**.
8. From the **Input Interface** drop-down list, select the interface from which the multicast traffic originates.
9. Click the **Addresses** tab.

*The Broadcast/Multicast Tunnel Endpoints settings appear at the bottom of the Addresses tab.*



10. In the **Helper Addresses** section, type IP addresses for each end of the multicast tunnel. The XTM device uses these addresses as the endpoints of the broadcast/multicast GRE tunnel inside the IPsec BOVPN tunnel. You can set Local IP and Remote IP to any unused IP address. We recommend that you use IP addresses that are not used on any network known to the XTM device.
  - In the **Local IP** text box, type an IP address to use for the local end of the tunnel.
  - In the **Remote IP** text box, type an IP address to use for the remote end of the tunnel.

## Enable the Other XTM Device to Receive Multicast Traffic Through a Tunnel

On the XTM device on the network on which you want to receive the multicast traffic, configure the multicast settings to enable the device to receive multicast traffic through the tunnel.

1. Select **VPN > Branch Office Tunnels**.
2. Select a tunnel and click **Edit**.
3. From the **Edit Tunnel** dialog box, click the **Multicast Settings** tab.
4. Select the **Enable multicast routing over the tunnel** check box.
5. In the **Origination IP** text box, type the IP address of the originator of the traffic.
6. In the **Group IP** text box, type the multicast address to receive the traffic.
7. Select **Enable device to receive multicast traffic**.
8. Select the check box for each interfaces that you want to receive the multicast traffic.
9. Select the **Addresses** tab.  
*The Broadcast/Multicast Tunnel Endpoints settings appear at the bottom of the Addresses tab.*
10. In the **Helper Addresses** section, type the opposite IP addresses you typed in the configuration for the other end of the tunnel.
  - In the **Local IP** text box, type the IP address that you typed in the Remote IP field for the XTM device at the other end of the tunnel.
  - In the **Remote IP** text box, type the IP address that you typed in the Local IP field for the XTM device at the other end of the tunnel.

## Enable Broadcast Routing Through a Branch Office VPN Tunnel

You can configure your XTM device to support limited broadcast routing through a Branch Office VPN (BOVPN) tunnel. When you enable broadcast routing, the tunnel supports broadcasts to the limited broadcast IP address, 255.255.255.255. Local subnet broadcast traffic is not routed through the tunnel. Broadcast routing supports broadcast only from one network to another through a BOVPN tunnel.

**Note** *Broadcast routing through a BOVPN tunnel is supported only between XTM devices.*

Broadcast routing through a BOVPN tunnel does not support these broadcast types:

- DHCP/ Bootstrap Protocol (bootp) broadcast
- NetBIOS broadcast
- Server Message Block (SMB) broadcast

For an example that shows which broadcasts can be routed through a BOVPN tunnel, see [Broadcast Routing Through a BOVPN Tunnel](#).

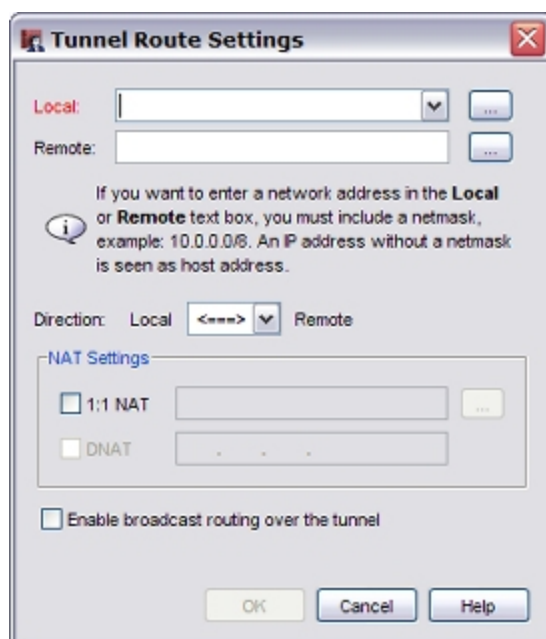
Some software applications require the ability to broadcast to other network devices in order to operate. If devices that need to communicate this way are on networks connected by a BOVPN tunnel, you can enable broadcast routing through the tunnel so the application can find the devices on the network at the other end of the tunnel.

When you enable broadcast routing through a BOVPN tunnel, the XTM device creates a GRE tunnel inside the IPsec VPN tunnel between the networks. The XTM device sends the broadcast traffic through the GRE tunnel. The GRE tunnel requires an unused IP address on each side of the tunnel. So you must configure helper IP addresses for each end of the BOVPN tunnel.

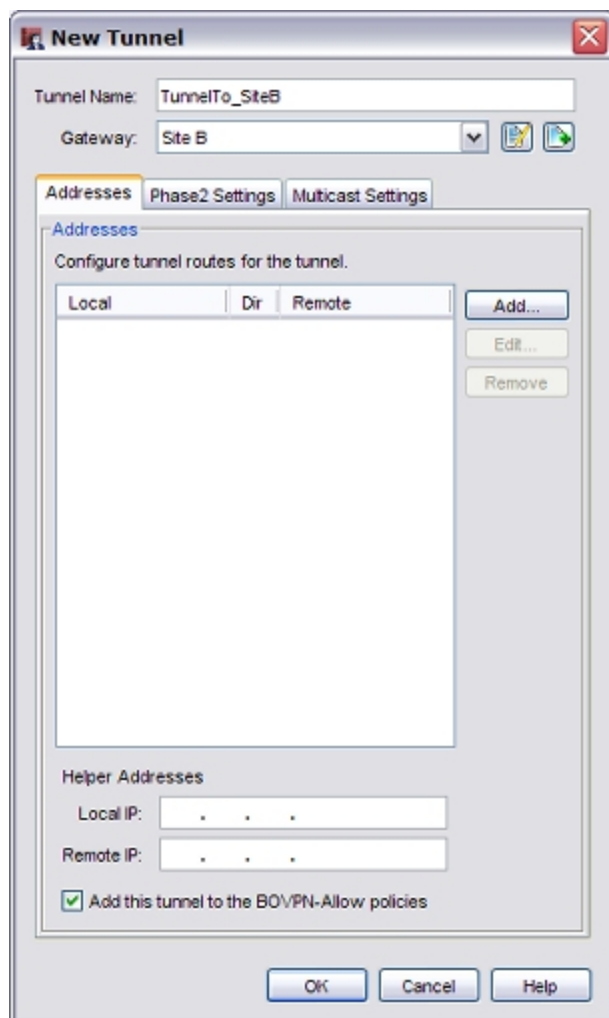
## Enable Broadcast Routing for the Local XTM device

1. Select **VPN > Branch Office Tunnels**.
2. Select a tunnel and click **Edit**.
3. From the **Edit Tunnel** dialog box, select the tunnel route and click **Edit**.

*The Tunnel Route Settings dialog box appears.*



4. Select the **Enable broadcast routing over the tunnel** check box. Click **OK**.  
*The Edit Tunnel dialog box appears. The Helper Addresses appear at the bottom of the Addresses tab.*



5. In the **Helper Addresses** section, type IP addresses for each end of the broadcast tunnel. The XTM device uses these addresses as the endpoints of the broadcast/multicast GRE tunnel inside the IPsec BOVPN tunnel. You can set the **Local IP** and **Remote IP** to any unused IP address. We recommend you use IP addresses that are not used on any network known to the XTM device.
  - In the **Local IP** text box, type an IP address to use for the local end of the tunnel.
  - In the **Remote IP** text box, type an IP address to use for the remote end of the tunnel.

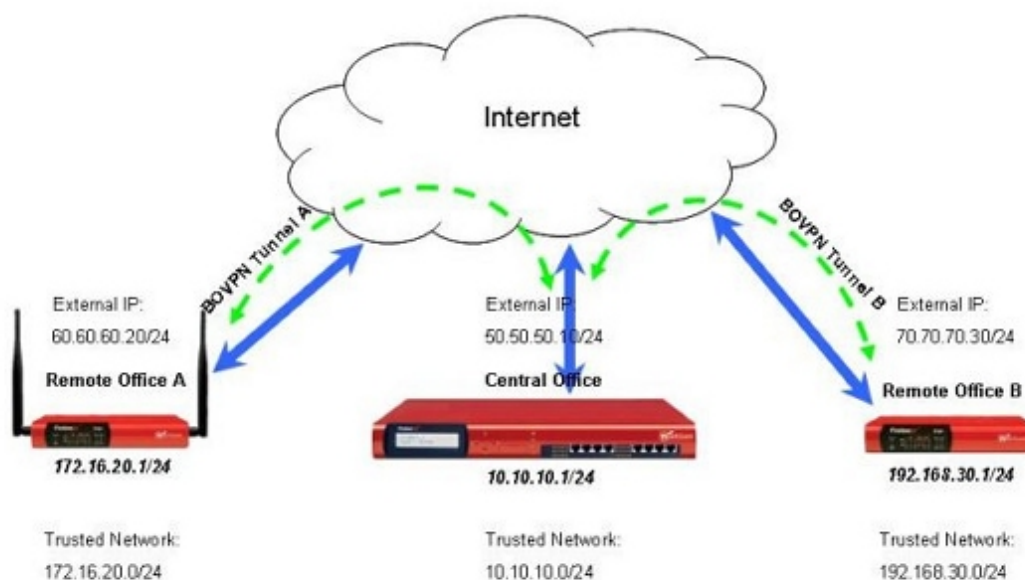
## Configure Broadcast Routing for the XTM Device at the Other End of the Tunnel

1. Repeat Steps 1–4 above to enable broadcast routing for the device at the other end of the tunnel.
2. In the **Helper Addresses** section, type the opposite addresses you typed in the configuration for the other end of the tunnel.
  - In the **Local IP** text box, type the IP address that you typed in the **Remote IP** text box for the device at the other end of the tunnel.
  - In the **Remote IP** text box, type the IP address that you typed in the **Local IP** text box for the device at the other end of the tunnel.

## Branch Office VPN Tunnel Switching

If you have two or more remote Branch Office VPN (BOVPN) tunnels connected to your network, and you want computers on the remote networks to exchange data, you must configure tunnel switching on the central XTM device. When you set up tunnel switching, the central XTM device decrypts packets sent from one VPN, applies the policies configured on the central XTM device, encrypts the packets again, and sends the encrypted packets to their destination on the other VPN.

For example, if you have a XTM device at your Central Office that you use for tunnel switching between BOVPN tunnels to two remote offices, your network configuration might look like this:



In this example, you can use tunnel switching so the Central Office XTM device can pass traffic from the trusted network of Remote Office A to the trusted network of Remote Office B, without a third BOVPN tunnel between the two remote offices. This configuration is useful when you require control of network security at the Central Office, because you can apply policies to traffic between the two tunnels at the Central Office.

For a step-by-step example of how to configure BOVPN tunnel switching, see the *Manual BOVPN Tunnels* section of the *Fireware XTM WatchGuard System Manager Help* at <http://www.watchguard.com/help/docs/wsm/11/en-US/index.html>.

## Configure VPN Failover

Failover is an important function of networks that need high availability. When you have multi-WAN failover configured, VPN tunnels automatically fail over to a backup external interface if a failure occurs. You can also configure VPN tunnels to fail over to a backup endpoint if the primary endpoint becomes unavailable.

**Note** *This topic applies only to manual VPN tunnels. If you have multi-WAN configured and you create managed tunnels, WSM automatically sets up gateway pairs that include the external interfaces of both ends of your tunnel. No other configuration is necessary.*

VPN Failover occurs when one of these two events occur:

- A physical link is down. The XTM device monitors the status of the VPN gateway and the devices identified in the multi-WAN link monitor configuration. If the physical link is down, VPN failover occurs.
- The XTM device detects the VPN peer is not active.

When failover occurs, if the tunnel uses IKE keep-alive IKE continues to send Phase 1 keep-alive packets to the peer. When it gets a response, IKE triggers failback to the primary VPN gateway. If the tunnel uses Dead Peer Detection, failback occurs when a response is received from the primary VPN gateway.

When a failover event occurs, most new and existing connections failover automatically. For example, if you start an FTP “PUT” command and the primary VPN path goes down, the existing FTP connection continues on the backup VPN path. The connection is not lost, but there is some delay. Note that VPN Failover can occur only if:

- Firebox or XTM devices at each tunnel endpoint have Fireware v11.0 or higher installed.
- Multi-WAN failover is configured, as described in *About Using Multiple External Interfaces* on page 141.
- The interfaces of your XTM device are listed as gateway pairs on the remote Firebox or XTM device. If you have already configured multi-WAN failover, your VPN tunnels will automatically fail over to the backup interface.
- DPD is enabled in the Phase 1 settings for the branch office gateway on each end of the tunnel.

VPN Failover does not occur for BOVPN tunnels with dynamic NAT enabled as part of their tunnel configuration. For BOVPN tunnels that do not use NAT, VPN Failover occurs and the BOVPN session continues. With Mobile VPN tunnels, the session does not continue. You must authenticate your Mobile VPN client again to make a new Mobile VPN tunnel.

## Define Multiple Gateway Pairs

To configure manual BOVPN tunnels to fail over to a backup endpoint, you must define more than one set of local and remote endpoints (gateway pairs) for each gateway.

**Note** *If you have multi-WAN configured and you create managed tunnels, WSM automatically sets up gateway pairs that include the external interfaces of both ends of your tunnel. No other configuration is necessary.*

For complete failover functionality for a VPN configuration, you must define gateway pairs for each combination of external interfaces on each side of the tunnel. For example, suppose your primary local endpoint is 23.23.1.1/24 with a backup of 23.23.2.1/24. Your primary remote endpoint is 50.50.1.1/24 with a backup of 50.50.2.1/24. For complete VPN Failover, you would need to define these four gateway pairs:

23.23.1.1 - 50.50.1.1

23.23.1.1 - 50.50.2.1

23.23.2.1 - 50.50.1.1

23.23.2.1 - 50.50.2.1

1. Select **VPN > Branch Office Gateways**. Click **Add** to add a new gateway. Give the gateway a name and define the credential method, as described in *Configure Gateways* on page 918.
2. In the **Gateway Endpoints** section of the **New Gateway** dialog box, click **Add**.  
*The New Gateway Endpoints Settings dialog box appears.*





3. Specify the location of the local and remote gateways. Select the external interface name that matches the local gateway IP address or domain name you add.  
You can add both a gateway IP address and gateway ID for the remote gateway. This can be necessary if the remote gateway is behind a NAT device and requires more information to authenticate to the network behind the NAT device.
4. Click **OK** to close the **New Gateway Endpoints Settings** dialog box.  
*The New Gateway dialog box appears. The gateway pair you defined appears in the list of gateway endpoints.*
5. Repeat this procedure to define additional gateway pairs. You can add up to nine gateway pairs. You can select a pair and click **Up** or **Down** to change the order in which the XTM device attempts connections.
6. Click **OK**.

## Force a Branch Office VPN Tunnel Rekey

Normally, the gateway endpoints must generate and exchange new keys after a specified amount of time or traffic passes, as defined in the **Force Key Expiration** text boxes in the **Phase2 Proposals** dialog box. If you want to immediately generate new keys instead of waiting for them to expire (particularly when you troubleshoot VPN tunnels), you can choose to rekey one or more Branch Office VPN (BOVPN) tunnels.

## To Rekey One BOVPN Tunnel

You can rekey a VPN tunnel either from the front panel of Firebox System Manager or from the **Device Status** tab of WatchGuard System Manager.

1. In the **Branch Office VPN Tunnels** list, select the tunnel you want to rekey.
2. Right-click the tunnel and select **Rekey Selected BOVPN Tunnel**.
3. When prompted, type the configuration passphrase.

## To Rekey all BOVPN Tunnels

In WatchGuard System Manager, you can choose from three methods to rekey all BOVPN tunnels.

### Method One

1. In Firebox System Manager, right-click anywhere on the **Front Panel** tab.
2. Select **Rekey All BOVPN Tunnels**.
3. When prompted, type the configuration passphrase.

### Method Two

1. In Firebox System Manager, select **Tools > Rekey All BOVPN Tunnels**.
2. When prompted, type the configuration passphrase.

### Method Three

1. On the WatchGuard System Manager **Device Status** tab, right-click the **Branch Office VPN Tunnels** list, or any tunnel in the list.
2. Select **Rekey All BOVPN Tunnels**.

## Related Questions About Branch Office VPN Set Up

### Why do I Need a Static External Address?

To make a VPN connection, each device must know the IP address of the other device. If the address for a device is dynamic, the IP address can change. If the IP address changes, connections between the devices cannot be made unless the two devices know how to find each other.

You can use Dynamic DNS if you cannot get a static external IP address. For more information, see *About the Dynamic DNS Service* on page 96.

### How do I Get a Static External IP Address?

You get the external IP address for your computer or network from your ISP or a network administrator. Many ISPs use dynamic IP addresses to make their networks easier to configure and use with many users. Most ISPs can give you a static IP address as an option.

## How do I Troubleshoot the Connection?

If you can send a ping to the trusted interface of the remote Firebox and to the computers on the remote network, the VPN tunnel is up. The configuration of the network software or the software applications are possible causes of other problems.

## Why is Ping not Working?

If you cannot send a ping to the local interface IP address of the remote XTM device, use these steps:

1. Ping the external address of the remote XTM device.

For example, at Site A, ping the IP address of Site B. If you do not receive a response, make sure the external network settings of Site B are correct. Site B must be configured to respond to ping requests on that interface. If the settings are correct, make sure that the computers at Site B have a connection to the Internet. If the computers at site B cannot connect, speak to your ISP or network administrator.

2. If you can ping the external address of each XTM device, try to ping a local address in the remote network.

From a computer at Site A, ping the internal interface IP address of the remote XTM device. If the VPN tunnel is up, the remote XTM device sends the ping back. If you do not receive a response, make sure the local configuration is correct. Make sure that the local DHCP address ranges for the two networks connected by the VPN tunnel do not use any of the same IP addresses. The two networks connected by the tunnel must not use the same IP addresses.

## Improve Branch Office VPN Tunnel Availability

There are Branch Office VPN (BOVPN) installations in which all the settings are correct, but BOVPN connections do not always operate correctly. You can use the information below to help you troubleshoot your BOVPN tunnel availability problems. These procedures do not improve general BOVPN tunnel performance.

Most BOVPN tunnels remain available to pass traffic at all times. Problems are often associated with one or more of these three conditions:

- One or both endpoints have unreliable external connections. High latency, high packet fragmentation, and high packet loss can make a connection unreliable. These factors have a greater impact on BOVPN traffic than on other common traffic, like HTTP and SMTP. With BOVPN traffic, the encrypted packets must arrive at the destination endpoint, be decrypted, and then reassembled before the unencrypted traffic can be routed to the destination IP address.
- One endpoint is not an XTM device, or is an older Firebox with older system software. Compatibility tests between new WatchGuard products and older devices are done with the latest software available for older devices. With older software, you could have problems that have been fixed in the latest software release.  
Because they are based on the IPSec standard, XTM devices are compatible with most third-party endpoints. However, some third-party endpoint devices are not IPSec-compliant because of software problems or proprietary settings.
- If there is a low volume of traffic through the tunnel, or if there are long periods of time when no traffic goes through the tunnel, some endpoints terminate the VPN connection. Firebox devices that run Fireware XTM, and Firebox X Edge devices do not do this. Some third-party devices and Firebox devices with older versions of the WFS software use this condition as a way to terminate tunnels that seem to be dead.

You can install the latest operating system and management software on all XTM devices, but all of the other conditions in this list are out of your control. You can, however, take certain actions to improve the availability of the BOVPN.

Select either IKE Keep-alive or Dead Peer Detection, but not both

Both IKE Keep-alive and Dead Peer Detection settings can show when a tunnel is disconnected. When they find the tunnel has disconnected, they start a new Phase 1 negotiation. If you select both IKE Keep-alive and Dead Peer Detection, the Phase 1 renegotiation that one starts can cause the other to identify the tunnel as disconnected and start a second Phase 1 negotiation. Each Phase 1 negotiation stops all tunnel traffic until the tunnel has been negotiated. To improve tunnel stability, select either IKE Keep-alive or Dead Peer Detection. Do not select both.

Note the following about these settings:

*The **IKE Keep-alive** setting is used only by XTM devices. Do not use it if the remote endpoint is a third-party IPSec device.*

When you enable IKE Keep-alive, the XTM device sends a message to the remote gateway device at a regular interval and waits for a response. **Message interval** determines how often a message is sent. **Max Failures** is how many times the remote gateway device can fail to respond before the XTM device tries to renegotiate the Phase 1 connection.

*Dead Peer Detection is an industry standard that is used by most IPSec devices. Select Dead Peer detection if both endpoint devices support it.*

When you enable Dead Peer Detection, the XTM device monitors tunnel traffic to identify whether a tunnel is active. If no traffic has been received from the remote peer for the amount of time entered for **Traffic idle timeout**, and a packet is waiting to be sent to the peer, the XTM device sends a query. If there is no response after the number of **Max retries**, the XTM device renegotiates the Phase 1 connection. For more information about Dead Peer Detection, see <http://www.ietf.org/rfc/rfc3706.txt>.

The IKE Keep-alive and Dead Peer Detection settings are part of the Phase 1 settings.

1. In Policy Manager, select **VPN > Branch Office Gateways**.
2. Select the gateway and click **Edit**.
3. Click the **Phase 1 Settings** tab.

Use the default settings

The default BOVPN settings provide the best combination of security and speed. Use the default settings when possible. If the remote endpoint device does not support one of the WatchGuard default settings, configure the XTM device to use the default setting from the remote endpoint. These are the default settings for WSM 11.x:

**Note** *If a setting is not displayed in WSM, you cannot change it.*

General Settings	
Mode	Main (Select Aggressive if one of the devices has a dynamic external IP address.)
NAT Traversal	Yes
NAT Traversal Keep-alive Interval	20 seconds
IKE Keep-alive	Disabled
IKE Keep-alive Message Interval	None
IKE Keep-alive Max Failures	None
Dead Peer Detection (RFC3706)	Enabled
Dead Peer Detection Traffic Idle Timeout	20 seconds
Dead Peer Detection Max Retries	5

PHASE 1 Transform Settings	
Authentication Algorithm	SHA-1
Encryption Algorithm	3DES

**PHASE 1 Transform Settings**

SA Life or Negotiation Expiration (hours)	8
SA Life or Negotiation Expiration (kilobytes)	0
Diffie-Hellman Group	2

**PHASE 2 Proposal Settings**

Type	ESP
Authentication Algorithm	SHA-1
Encryption Algorithm	AES (256 bit)
Force Key Expiration	Enable
Phase 2 Key Expiration (hours)	8
Phase 2 Key Expiration (kilobytes)	128000
Enable Perfect Forward Secrecy	No
Diffie-Hellman Group	None

Configure the XTM device to send log traffic through the tunnel

If no traffic goes through a tunnel for a period of time, an endpoint can decide that the other endpoint is unavailable and not try to renegotiate the VPN tunnel immediately. One way to make sure traffic goes through the tunnel at all times is to configure the XTM device to send log traffic through the tunnel. You do not need a Log Server to receive and keep records of the traffic. In this case, you intentionally configure the XTM device to send log traffic to a log server that does not exist. This creates a consistent but small amount of traffic sent through the tunnel, which can help to keep the tunnel more stable.

There are two types of log data: WatchGuard logging and syslog logging. If the XTM device is configured to send log data to both a WatchGuard Log Server and a syslog server, you cannot use this method to pass traffic through the tunnel.

You must choose a Log Server IP address to send the log data to. To choose the IP address, use these guidelines.

- The Log Server IP address you use must be an IP address that is included in the remote tunnel route settings. For more information, see *Add Routes for a Tunnel* on page 930.
- The Log Server IP address should not be an IP address that is used by a real device.

The two types of logging generate different amounts of traffic.

### WatchGuard Logging

No log data is sent until the XTM device has connected to a Log Server. The only types of traffic sent through the tunnel are attempts to connect to a Log Server that are sent every three minutes. This can be enough traffic to help tunnel stability with the least impact on other BOVPN traffic.

### Syslog Logging

Log data is immediately sent to the syslog server IP address. The volume of log data depends on the traffic that the XTM device handles. Syslog logging usually generates enough traffic that packets are always passing through the tunnel. The volume of traffic can occasionally make regular BOVPN traffic slower, but this is not common.

To improve stability and have the least impact on BOVPN traffic, try the WatchGuard Logging option first. If this does not improve the stability of the BOVPN tunnel, try syslog logging. The subsequent procedures assume that both endpoint devices are WatchGuard devices, and that neither endpoint is configured to send log data to either a WatchGuard Log Server or a syslog server. If an endpoint is already configured to send log data that a server collects, do not change those logging settings.

Different options you can try include:

- Configure one endpoint to send WatchGuard log traffic through the tunnel.
- Configure the other endpoint to send WatchGuard log traffic through the tunnel.
- Configure both endpoints to send WatchGuard log traffic through the tunnel.
- Configure one endpoint to send syslog log traffic through the tunnel.
- Configure only the other endpoint to send syslog log traffic through the tunnel.
- Configure both endpoints to send syslog log traffic through the tunnel.

### Send WatchGuard log data through the tunnel

1. Select **Setup > Logging**.
2. Select **Send log messages to the log servers at these IP addresses** and click **Configure**.
3. Click **Add**.  
*The Add Event Processor dialog box appears.*
4. For **Log Server Address**, type the IP address you have selected for the Log Server.
5. Type an **Encryption Key** and type the same key in the **Confirm Key** text box.  
*The allowed range for the encryption key is 8–32 characters. You can use all characters except spaces and slashes (/ or \).*
6. Click **OK** three times.

### Send syslog data through the tunnel

1. Select **Setup > Logging**.
2. Select **Send log messages to the Syslog server at this IP addresses**.
3. Type the IP address you have chosen for the syslog server in the text box.
4. Click **OK**.





# 28 Mobile VPN with PPTP

---

## About Mobile VPN with PPTP

Mobile Virtual Private Networking (Mobile VPN) with Point-to-Point Tunneling Protocol (PPTP) creates a secure connection between a remote computer and the network resources behind the XTM device. Each XTM device supports as many as 50 users at the same time. Mobile VPN with PPTP users can authenticate to the XTM device, or to a RADIUS or VACMAN Middleware authentication server. To use Mobile VPN with PPTP, you must configure the XTM device and the remote client computers.

## Mobile VPN with PPTP Requirements

Before you configure an XTM device to use Mobile VPN with PPTP, make sure you have this information:

- The IP addresses for the remote client to use for Mobile VPN with PPTP sessions.  
For Mobile VPN with PPTP tunnels, the XTM device gives each remote user a virtual IP address. These IP addresses cannot be addresses that the network behind the XTM device uses. The safest procedure to give addresses for Mobile VPN users is to install a "placeholder" secondary network. Then, select an IP address from that network range. For example, create a new subnet as a secondary network on your trusted network 10.10.0.0/24. Select the IP addresses in this subnet for your range of PPTP addresses.
- The IP addresses of the DNS and WINS servers that resolve host names to IP addresses.
- The user names and passwords of users that are allowed to connect to the XTM device with Mobile VPN with PPTP.

## Encryption Levels

For Mobile VPN with PPTP, you can select to use 128-bit encryption or 40-bit encryption. Software versions of Windows XP in the United States have 128-bit encryption enabled. You can get a strong encryption patch from Microsoft for other versions of Windows. The XTM device always tries to use 128-bit encryption first. It can be configured to use 40-bit encryption if the client cannot use a 128-bit encrypted connection.

For more information on how to allow 40-bit encryption, see *Configure Mobile VPN with PPTP* on page 971.

If you do not live in the United States and you want to have strong encryption allowed on your LiveSecurity Service account, send an email message to [supportid@watchguard.com](mailto:supportid@watchguard.com) and include all of the following information:

- Your LiveSecurity Service key number
- Date of purchase for your WatchGuard product
- Name of your company
- Company mailing address
- Telephone number and contact name
- Email address

If you live in the United States and do not already use WatchGuard System Manager (WSM) with strong encryption, you must download the strong encryption software from your Software Downloads page in the LiveSecurity Service web site.

1. Open a web browser and go to [www.watchguard.com](http://www.watchguard.com).
2. Log in to your LiveSecurity Service account.
3. Click **Support**.  
*Your WatchGuard Support Center appears.*
4. In the **Managing Your Products** section, click **Software Downloads**.
5. From the **Choose product family** list, select your XTM device.  
*The Software Downloads page appears.*
6. Download **WatchGuard System Manager with Strong Encryption**.

Before you install the WatchGuard System Manager with Strong Encryption software, you must uninstall any other versions of WatchGuard System Manager from your computer.

**Note** *To keep your current XTM device configuration, do not use the Quick Setup Wizard when you install the new software. Open WatchGuard System Manager, connect to the XTM device, and save your configuration file. Configurations with a different encryption version are compatible.*

## Configure Mobile VPN with PPTP

To configure your XTM device to accept PPTP connections you must first use Policy Manager to activate Mobile VPN with PPTP and configure the settings.

1. Select **VPN > Mobile VPN > PPTP**.

The *Mobile VPN with PPTP Configuration* dialog box appears.

2. Select the **Activate Mobile VPN with PPTP** check box. This allows PPTP remote users to be configured and automatically creates a WatchGuard PPTP policy to allow PPTP traffic sent to the XTM device. We recommend that you do not change the default properties of the WatchGuard PPTP policy.
3. Use the information in the subsequent sections to complete the PPTP configuration.

## Authentication

Mobile VPN with PPTP users can authenticate to the XTM device, or use extended authentication to a RADIUS or VACMAN Middleware server. The instructions to use a VACMAN Middleware server are identical to the instructions to use a RADIUS server. To use the XTM device database, do not select the **Use RADIUS authentication to authenticate Mobile VPN with PPTP users** check box.

To use a RADIUS or VACMAN Middleware server for authentication:

1. Select the **Use RADIUS Authentication to authenticate Mobile VPN with PPTP users** check box.
2. Configure the RADIUS server in the **Authentication Servers** dialog box, as described in *Configure RADIUS Server Authentication* on page 335.  
Or, configure the VASCO server in the **Authentication Servers** dialog box as described in *Configure VASCO Server Authentication* on page 340.
3. On the RADIUS server, create a group named *PPTP-Users*. Add names or groups of PPTP users to this group.

**Note** *To establish the PPTP connection, the user must be a member of a group named PPTP-Users. After the user is authenticated, you can use other groups of which the user is a member to create policies that control access to network resources.*

## Set Encryption for PPTP Tunnels

Versions of Windows XP sold in the United States have 128-bit encryption enabled. You can get a strong encryption patch from Microsoft for other versions of Windows.

- Select **Require 128-bit encryption** if you want to require 128-bit encryption for all PPTP tunnels. We recommend that you use 128-bit encryption for VPN.
- Select **Allow Drop from 128-bit to 40-bit** to allow the tunnels to drop from 128-bit to 40-bit encryption for connections that are less reliable, or when the client cannot use 128-bit encryption. The XTM device always tries to use 128-bit encryption first. It uses 40-bit encryption if the client cannot use the 128-bit encrypted connection. Usually, only customers outside the United States select this check box.
- Select **Do not require encryption** to allow traffic that is not encrypted through the VPN.

## MTU and MRU

The Maximum Transmission Unit (MTU) or Maximum Receive Unit (MRU) sizes are sent to the client as part of the PPTP parameters to use during the PPTP session. We recommend that you do not change MTU or MRU values unless you are sure the change corrects a known problem with your PPTP sessions. Incorrect MTU or MRU values cause traffic through the PPTP VPN to fail.

## Define Timeout Settings for PPTP Tunnels

You can define two timeout settings for PPTP tunnels if you use RADIUS authentication:

### Session Timeout

The maximum length of time the user can send traffic to the external network. If you set this field to zero (0) seconds, minutes, hours, or days, no session timeout is used and the user can stay connected for any length of time.

### Idle Timeout

The maximum length of time the user can stay authenticated when idle (not passing any traffic to the external network interface). If you set this field to zero (0) seconds, minutes, hours, or days, no idle timeout is used and the user can stay idle for any length of time.

If you do not use RADIUS for authentication, the PPTP tunnel uses the timeout settings that you set for each Firebox User. For more information about Firebox user settings, see *Define a New User for Firebox Authentication* on page 332.

## Add to the IP Address Pool

Mobile VPN with PPTP supports as many as 50 users at the same time. The XTM device gives an open IP address to each Mobile VPN user from a group of available addresses, until all of the addresses are in use. When a user closes a session, his or her IP address becomes available again.

You must configure two or more IP addresses for PPTP to operate correctly.

1. In the **IP Address Pool** section, click **Add**.

*The Add Address dialog box appears.*

2. From the **Choose Type** drop-down list, select **Host IP** (for a single IP address) or **Host Range** (for a range of IP addresses).

You can configure up to 50 addresses.

If you select **Host IP**, you must add at least two IP addresses.

If you select **Host Range** and add a range of IP addresses that is larger than 50 addresses, Mobile VPN with PPTP uses the first 50 addresses in the range.

3. In the **Value** field, type the host IP address. If you selected **Host Range**, type the first IP address in the range for **Value** and the last IP address in the range for **To**.  
Make sure that you use IP addresses that are never used by any other device that connects to the XTM device. The IP address or address range appears in the list of addresses available to remote clients.
4. Click **OK**.
5. Repeat Steps 1–4 to configure all the addresses for use with Mobile VPN with PPTP.

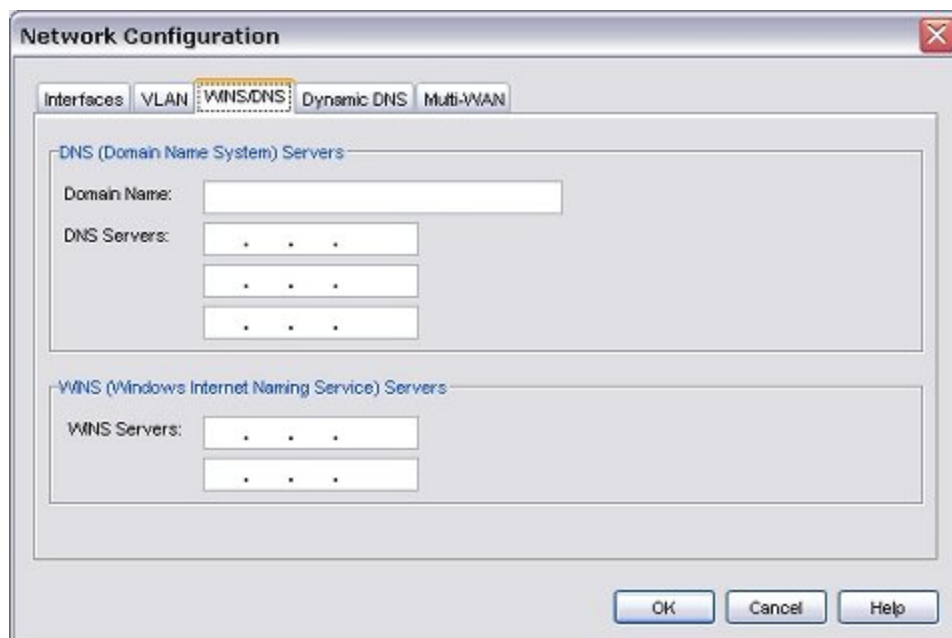
## Save Your Changes

1. Click **OK** to close the **Mobile VPN with PPTP Configuration** dialog box.
2. Save the changes to your XTM device.

## Configure WINS and DNS Servers

Mobile VPN clients use shared Windows Internet Naming Service (WINS) and Domain Name System (DNS) server addresses. DNS changes hostnames into IP addresses, while WINS changes NetBIOS names to IP addresses. The trusted interface of the XTM device must have access to these servers. You can use Policy Manager to enable access to our WINS and DNS servers.

1. Select **Network > Configuration**.
2. Select the **WINS/DNS** tab.  
*The information for the WINS and DNS servers appears.*
3. Type a **Domain Name** for the DNS server.
4. In the **DNS Servers** text boxes, type the addresses for the DNS servers.  
You can type up to three addresses for DNS servers.
5. In the **WINS Servers** text boxes, type the addresses for the WINS servers.  
You can type up to two addresses for WINS servers.



## Add New Users to the PPTP-Users Group

To connect to the XTM device with a PPTP VPN tunnel, mobile users must type their user names and passphrases to authenticate. The XTM device uses this information to authenticate the user to the XTM device.

When you enable PPTP in your XTM device configuration, a default user group is created automatically. This user group is called *PPTP-Users*. You see this group name when you create a new user or add user names or groups to policies. Users must be a member of this group to make a PPTP connection.

For more information on XTM device groups, see *Configure Your XTM Device as an Authentication Server* on page 329.

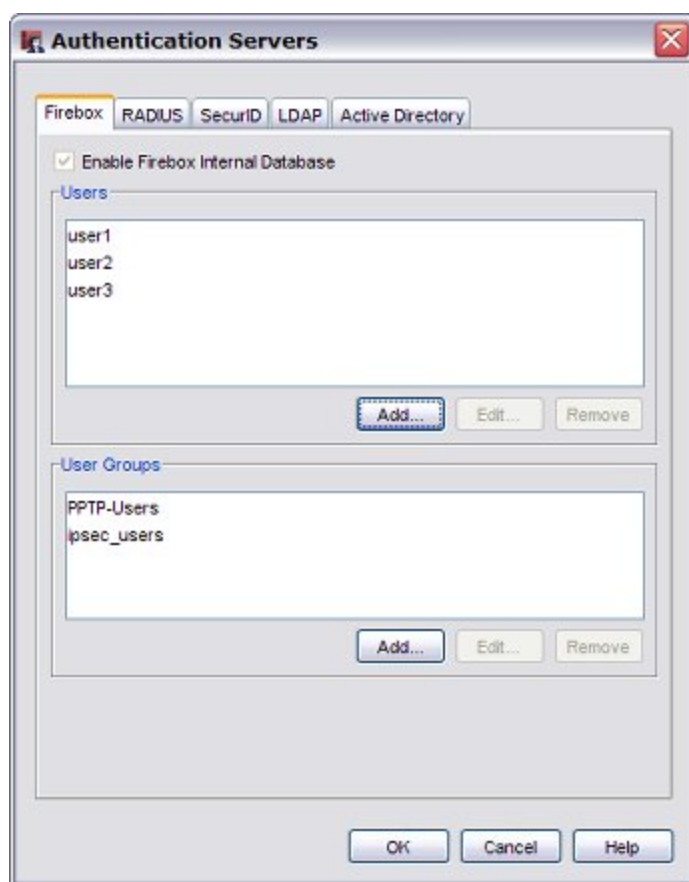
If you use a RADIUS or VACMAN middleware server for authentication, you must create the PPTP-Users group on your authentication server and add users to that group. For more information, see the documentation for your authentication server.

If you use the XTM device for authentication, you must add users and make them members of the PPTP-Users group. You can use Policy Manager to add these users.

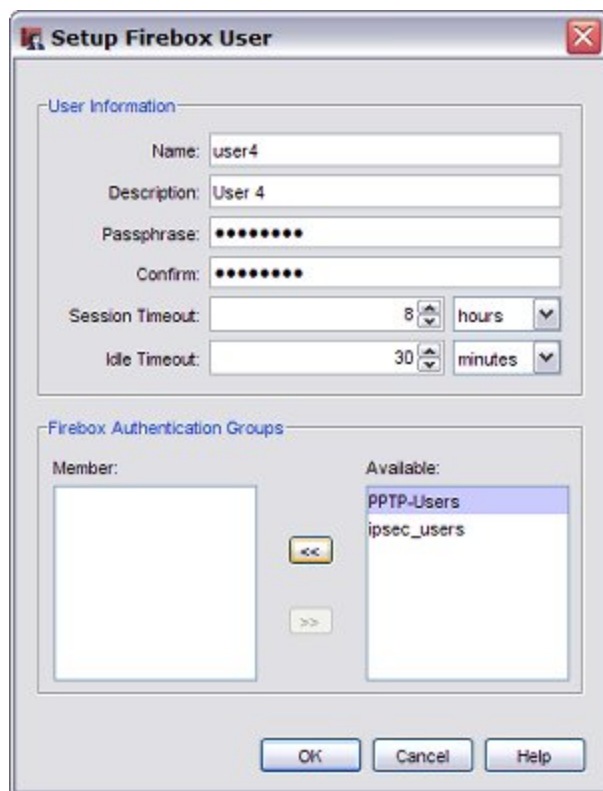
1. Select **Setup > Authentication > Authentication Servers**.


*The Authentication Servers dialog box appears.*

2. Select the **Firebox** tab.



3. To add a new user, in the **Users** section, click the **Add** button.
4. To change properties for a selected user, click **Edit**.



5. For a new user, type a user name and passphrase. Type the passphrase again to confirm it. You can skip this step if the user was created previously.  
*A description is not required. We recommend that you do not change the default values for Session Timeout and Idle Timeout.*
6. To add a user to a Firebox Authentication Group, select the user name in the **Available** list.
7. Click  to move the name to the **Member** list.  
Or, you can double-click the user name in the **Available** list.  
*The user is added to the user list. Repeat Steps 3–6 to add more users.*
8. To close the **Setup Firebox User** dialog box, click **OK**.  
*The Firebox Users tab appears with a list of the new users.*

## Options for Internet Access Through a Mobile VPN with PPTP Tunnel

You can enable remote users to access the Internet through a Mobile VPN tunnel. This option affects your security because this Internet traffic is not filtered or encrypted. You have two options for Mobile VPN tunnel routes: default-route VPN and split tunnel VPN.



## Default-Route VPN

The most secure option is to require that all remote user Internet traffic is routed through the VPN tunnel to the XTM device. Then, the traffic is sent back out to the Internet. With this configuration (known as default-route VPN), the XTM device is able to examine all traffic and provide increased security, although it uses more processing power and bandwidth. When you use default-route VPN, a dynamic NAT policy must include the outgoing traffic from the remote network. This allows remote users to browse the Internet when they send all traffic to the XTM device.

**Note** If you use the "route print" or "ipconfig" commands after you start a Mobile VPN tunnel on a computer with Microsoft Windows installed, you see incorrect default gateway information. The correct information is located on the **Details** tab of the **Virtual Private Connection Status** dialog box.

## Split Tunnel VPN

Another configuration option is to enable split tunneling. This configuration enables users to browse the Internet without the need to send Internet traffic through the VPN tunnel. Split tunneling improves network performance, but decreases security because the policies you create are not applied to the Internet traffic. If you use split tunneling, we recommend that each client computer have a software firewall.

## Default-Route VPN Setup for Mobile VPN with PPTP

In Windows Vista, XP, and 2000, the default setting for a PPTP connection is default-route. Your XTM device must be configured with dynamic NAT to receive the traffic from a PPTP user. Any policy that manages traffic going out to the Internet from behind the XTM device must be configured to allow the PPTP user traffic.

When you configure your default-route VPN:

- Make sure that the IP addresses you have added to the PPTP address pool are included in your dynamic NAT configuration on the XTM device.  
From Policy Manager, select **Network > NAT**.
- Edit your policy configuration to allow connections from the PPTP-Users group through the external interface.  
For example, if you use WebBlocker to control web access, add the PPTP-Users group to the proxy policy that is configured to with WebBlocker enabled.

## Split Tunnel VPN Setup for Mobile VPN with PPTP

On the client computer, edit the PPTP connection properties to not send all traffic through the VPN.

1. For Windows Vista, XP, or 2000, select **Control Panel > Network Connections** and right-click the VPN connection.
2. Select **Properties**.  
*The VPN properties dialog box appears.*
3. Select the **Networking** tab.
4. Select **Internet Protocol (TCP/IP)** in the list box and click **Properties**.  
*The Internet Protocol (TCP/IP) Properties dialog box appears.*

5. On the **General** tab, click **Advanced**.  
*The Advanced TCP/IP Settings dialog box appears.*
6. Windows XP and Windows 2000 — On the **General** tab (XP and Windows 2000), clear the **Use default gateway on remote network** check box.  
Windows Vista — On the **Settings** tab (XP and Windows 2000), clear the **Use default gateway on remote network** check box.

## Configure Policies to Control Mobile VPN with PPTP Client Access

Mobile VPN with PPTP users have no access privileges through a XTM device by default. You must configure policies to allow PPTP users access to network resources. You can add new policies or edit existing policies.

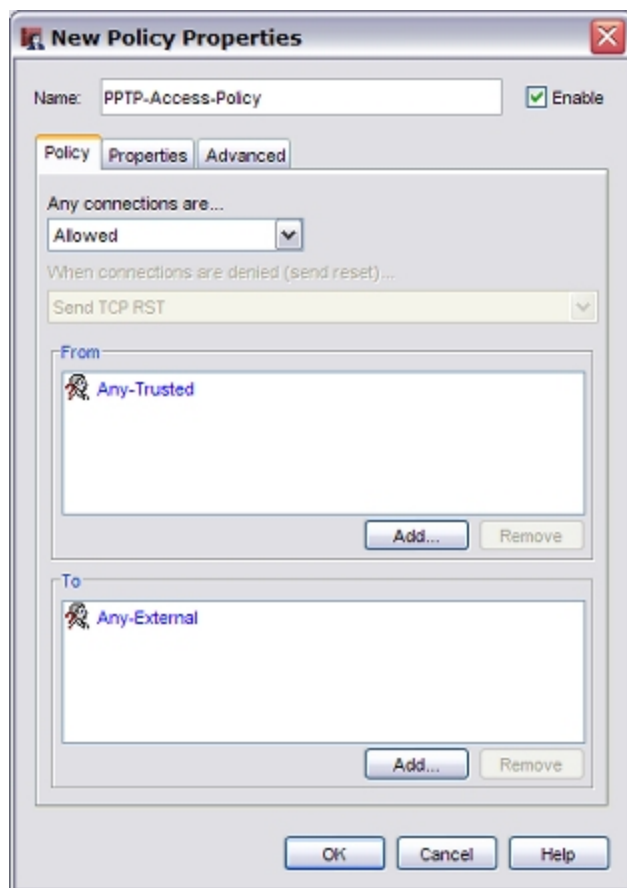
Before you set up the PPTP access policy, you must enable Mobile VPN with PPTP. For instructions, see *Configure Mobile VPN with PPTP* on page 971. When you enable Mobile VPN for PPTP, Policy Manager creates the *PPTP-Users* group you use in the PPTP access policy.

**Note** *If you assign IP addresses from a trusted network to PPTP users, the traffic from the PPTP user is not considered trusted. All Mobile VPN with PPTP traffic is not trusted by default. For this reason, you must create policies to allow PPTP users access to network resources.*

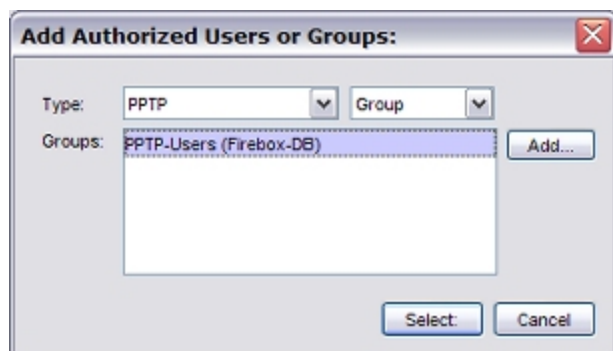
### Allow PPTP Users to Access a Trusted Network

In this example, you use Policy Manager to add an Any policy to give all members of the PPTP-Users group full access to resources on all trusted networks.

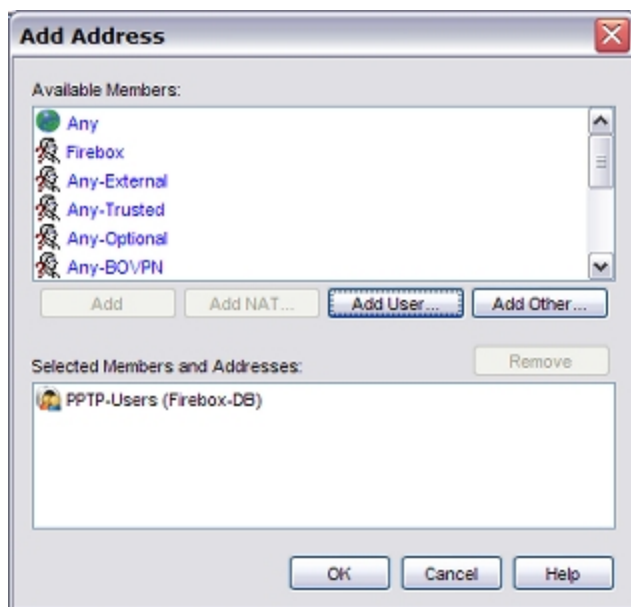
1. Click **+**.  
Or, select **Edit > Add Policies**.  
*The Add Policies dialog box appears.*
2. Click the plus (+) icon to expand the **Packet Filters** list.  
*A list of templates for packet filters appears.*
3. Select **Any** and click **Add**.  
*The New Policy Properties dialog box opens.*



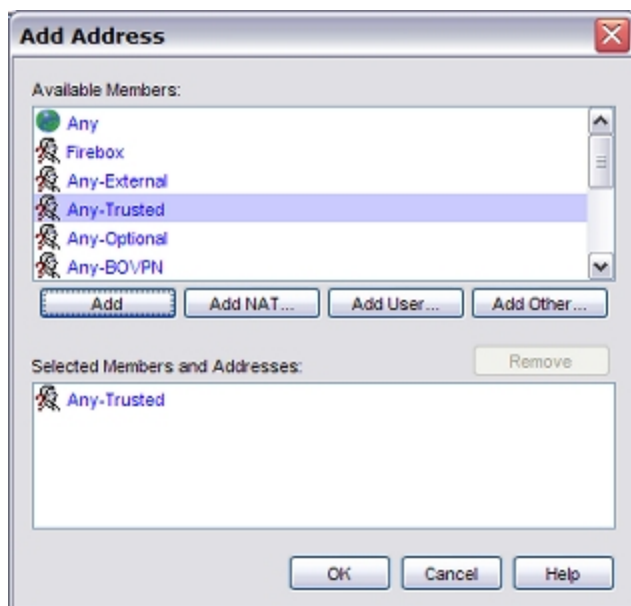
4. In the **Name** text box, type a name for the policy.  
Choose a name to help you identify this policy in your configuration.
5. On the **Policy** tab, in the **From** section, click **Add**.  
*The Add Address dialog box opens.*
6. In the **Selected Members and Addresses** section, select **Any-Trusted** and click **Remove**.
7. Click **Add User**.  
*The Add Authorized Users or Groups dialog box opens.*



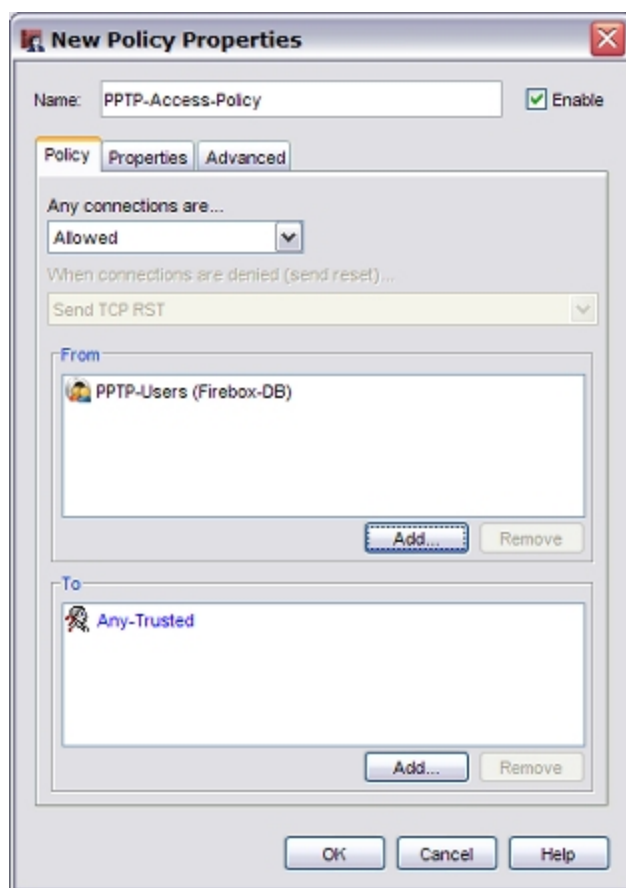
8. From the first **Type** drop-down list, select **PPTP**.
9. From the second **Type** drop-down list, select **Group**.
10. From the **Groups** list, select **PPTP-Users** and click **Select**.  
*PPTP-Users appears as the name of the authentication method in parenthesis.*



11. Click **OK** to close the **Add Address** dialog box.
12. In the **New Policy Properties** dialog box, in the **To** section, click **Add**.  
*The Add Address dialog box opens.*
13. In the **Selected Members and Addresses** list, select **Any-External** and click **Remove**.
14. In the **Available Members** list, select **Any-Trusted** and click **Add**.  
*Any-Trusted appears in the Selected Members and Addresses window.*



15. Click **OK** to close the **Add Address** dialog box.  
*The New Policy Properties dialog appears.*



16. Click **OK** to close the **New Policy Properties** dialog box.
17. Click **Close**.
18. Save your changes.

For more information on policies, see *Add Policies to Your Configuration* on page 372.

## Use Other Groups or Users in a PPTP Policy

Users must be a member of the *PPTP-Users* group to make a PPTP connection. When you configure a policy to give PPTP users access to network resources, you can use the individual user name, or any other group that the user is a member of.

You can use Policy Manager to select a user or group other than PPTP-Users.

1. Double-click the policy to which you want to add the user or group.
2. On the **Policy** tab, in the **From** section, click **Add**.  
*The Add Address dialog box opens.*
3. Click **Add User**.  
*The Add Authorized Users or Groups dialog box opens.*
4. From the first **Type** drop-down list, select **PPTP**.
5. From the second **Type** drop-down list, select either **User** or **Group**.

6. Select the user or group you want to add and click **Select**.  
*The selected user or group appears in the Add Address dialog box in the Selected Members and Addresses window.*
7. Click **OK** to close the **Add Address** dialog box.
8. Click **OK** to close the **New Policy Properties** dialog box.

For more information on how to use users and groups in policies, see *Use Authorized Users and Groups in Policies* on page 360.

## Prepare Client Computers for PPTP

Before you can use your client computers as Mobile VPN with PPTP remote hosts, you must first prepare each computer with Internet access. Then, you can use the instructions in the subsequent sections to:

- Install the necessary version of Microsoft Dial-Up Networking and the necessary service packs
- Prepare the operating system for VPN connections
- Install a VPN adapter (not necessary for all operating systems)

## Prepare a Windows NT or 2000 Client Computer: Install MSDUN and Service Packs

To correctly configure Mobile VPN with PPTP on a computer with Windows NT and 2000, make sure these options are installed:

- MSDUN (Microsoft Dial-Up Networking) upgrades
- Other extensions
- Service packs

For Mobile VPN with PPTP, you must have these upgrades installed:

Encryption	Platform	Application
Base	Windows NT	40-bit SP4
Strong	Windows NT	128-bit SP4
Base	Windows 2000	40-bit SP2*
Strong	Windows 2000	128-bit SP2*

\*40-bit encryption is the default for Windows 2000. If you upgrade from Windows 98 with strong encryption, Windows 2000 automatically sets strong encryption for the new installation.

To install these upgrades or service packs, go to the Microsoft Download Center web site at:

<http://www.microsoft.com/downloads/>

The steps to configure and establish a PPTP connection are different for each version of Microsoft Windows.

To set up a PPTP connection on Windows Vista, see *Create and Connect a PPTP Mobile VPN for Windows Vista* on page 983.

To set up a PPTP connection on Windows XP, see *Create and Connect a PPTP Mobile VPN for Windows XP* on page 984.

To set up a PPTP connection on Windows 2000, see *Create and Connect a PPTP Mobile VPN for Windows 2000* on page 984.

## Create and Connect a PPTP Mobile VPN for Windows Vista

### Create a PPTP Connection

To prepare a Windows Vista client computer, you must configure the PPTP connection in the network settings.

1. From the Windows **Start** menu, select **Settings > Control Panel**.  
*The Start menu in Windows Vista is located in the lower-left corner of the screen.*
2. Click **Network and Internet**.  
*The Network and Sharing Center appears.*
3. In the left column, below **Tasks**, click **Connect to a network**.  
*The New Connection Wizard starts.*
4. Select **Connect to a workplace** and click **Next**.  
*The Connect to a workplace dialog box appears.*
5. Select **No, create a new connection** and click **Next**.  
*The How do you want to connect dialog box appears.*
6. Click **Use my Internet connection (VPN)**.  
*The Type the Internet address to connect to dialog box appears.*
7. Type the hostname or IP address of the XTM device external interface in the **Internet address** field.
8. Type a name for the Mobile VPN (such as "PPTP to XTM") in the **Destination name** text box.
9. Select whether you want other people to be able to use this connection.
10. Select the **Don't connect now; just set it up so I can connect later** check box so that the client computer does not try to connect at this time.
11. Click **Next**.  
*The Type your user name and password dialog box appears.*
12. Type the **User name** and **Password** for this client.
13. Click **Create**.  
*The connection is ready to use dialog box appears.*
14. To test the connection, click **Connect now**.

### Establish the PPTP Connection

To connect a Windows Vista client computer, replace **[name of the connection]** with the actual name you used when configuring the PPTP connection. The user name and password refers to one of the users you added to the PPTP-Users group. For more information, see *Add New Users to the PPTP-Users Group* on page 974.

Make sure you have an active connection to the Internet before you begin.

1. Select **Start > Settings > Network Connections > [name of the connection]**  
*The Windows Vista Start button is located in the lower-left corner of your screen.*
2. Type the user name and password for the connection and click **Connect**.
3. The first time you connect, you must select a network location. Select **Public location**.

## Create and Connect a PPTP Mobile VPN for Windows XP

To prepare a Windows XP client computer, you must configure the PPTP connection in the network settings.

### Create the PPTP Mobile VPN

From the Windows Desktop of the client computer:

1. From the Windows **Start** menu, select **Control Panel > Network Connections**.
2. Select **Create a new connection**.  
Or, click **New Connection Wizard** in Windows Classic view.  
*The New Connection wizard appears.*
3. Click **Next**.
4. Select **Connect to the network at my workplace** and click **Next**.
5. Select **Virtual Private Network connection** and click **Next**.
6. Type a name for the new connection (such as "Connect with Mobile VPN") and click **Next**.
7. Select if Windows ensures the public network is connected:
  - For broadband connection, select **Do not dial this initial connection**.
  - Or,
  - For a modem connection, select **Automatically dial this initial connection**, and then select a connection name from the drop-down list.
8. Click **Next**.  
*The VPN Server Selection screen appears. The wizard includes this screen if you use Windows XP SP2. Not all Windows XP users see this screen.*
9. Type the host name or IP address of the XTM device external interface and click **Next**.  
*The Smart Cards screen appears.*
10. Select whether to use your smart card with this connection profile and click **Next**.  
*The Connection Availability screen appears.*
11. Select who can use this connection profile and click **Next**.
12. Select **Add a shortcut to this connection to my desktop**.
13. Click **Finish**.

### Connect with the PPTP Mobile VPN

1. Start an Internet connection through a dial-up network, or directly through a LAN or WAN.
2. Double-click the shortcut to the new connection on your desktop.  
Or, select **Control Panel > Network Connections** and select your new connection from the Virtual Private Network list.
3. Type the user name and passphrase for the connection.  
For more information about the user name and passphrase, see *Add New Users to the PPTP-Users Group* on page 974.
4. Click **Connect**.

## Create and Connect a PPTP Mobile VPN for Windows 2000

To prepare a Windows 2000 remote host, you must configure the PPTP connection in the network settings.



## Create the PPTP Mobile VPN

From the Windows Desktop of the client computer:

1. From the Windows **Start** menu, select **Settings > Network Connections > Create a New Connection**.  
*The New Connection wizard appears.*
2. Click **Next**.
3. Select **Connect to the network at my workplace** and click **Next**.
4. Click **Virtual Private Network connection**.
5. Type a name for the new connection (such as "Connect with Mobile VPN") and click **Next**.
6. Select to not dial (for a broadband connection), or to automatically dial (for a modem connection) this connection, and click **Next**.
7. Type the host name or IP address of the XTM device external interface and click **Next**.
8. Select **Add a shortcut to this connection to my desktop** and click **Finish**.

## Connect with the PPTP Mobile VPN

1. Start your Internet connection through a dial-up network, or connect directly through a LAN or WAN.
2. Double-click the shortcut to the new connection on your desktop.  
Or, select **Control Panel > Network Connections** and select your new connection from the Virtual Private Network list.
3. Type the user name and passphrase for the connection.  
For more information about the user name and passphrase, see *Add New Users to the PPTP-Users Group* on page 974.
4. Click **Connect**.

## Make Outbound PPTP Connections from Behind an XTM Device

If necessary, you can make a PPTP connection to a XTM device from behind a different XTM device. For example, one of your remote users goes to a customer office that has a XTM device. The user can connect to your network with a PPTP connection. For the local XTM device to correctly allow the outgoing PPTP connection, add the PPTP policy and allow traffic from the network the user is on to the *Any-External* alias.

To add a policy, see *Add Policies to Your Configuration* on page 372.



# 29 Mobile VPN with IPsec

---

## About Mobile VPN with IPsec

Mobile VPN with IPsec is a client software application that is installed on a remote computer. The client makes a secure connection from the remote computer to your protected network through an unsecured network, such as the Internet. The Mobile VPN client uses Internet Protocol Security (IPsec) to secure the connection.

These topics include instructions to help you configure a Mobile VPN tunnel between the Mobile VPN with IPsec client and a XTM device with Fireware XTM installed.

## Configure a Mobile VPN with IPsec Connection

You can configure the XTM device to act as an endpoint for Mobile VPN with IPsec tunnels.

1. Open Policy Manager for your XTM device.
2. Select **VPN > Mobile VPN > IPsec**.

A user must be a member of a Mobile VPN group to be able to make a Mobile VPN with IPsec connection. You create the Mobile VPN group with the Add Mobile VPN with IPsec wizard. When the wizard is finished, Policy Manager does two things:

- Saves an end-user profile (called a .wgx file) on the management computer that created the Mobile VPN account. The user must have this .wgx file to configure the Mobile VPN client computer. If you use a certificate for authentication, .p12 and cacert.pem files are generated. These files can be found in the same location as the .wgx end-user profile.
- Automatically adds an *Any* policy to the **Mobile VPN with IPsec** tab that allows traffic to pass to and from the authenticated Mobile VPN user.

To restrict Mobile VPN client access, delete the *Any* policy and add policies to the **Mobile VPN with IPsec** that allow access to resources. For instructions to add policies, see *About Policy Manager* on page 364.

When the XTM device is configured, the client computer must have the Mobile VPN with IPSec client software installed. For information on how to install the Mobile VPN with IPSec client software, see *Install the Mobile VPN with IPSec Client Software* on page 1018.

When the user computer is correctly configured, the user makes the Mobile VPN connection. If the credentials the user authenticates with match an entry in the XTM device user database, and if the user is in the Mobile VPN group you create, the Mobile VPN session is authenticated.

## System Requirements

Before you configure your XTM device for Mobile VPN with IPSec, make sure you understand the system requirements for the WatchGuard management computer and the mobile user client computer.

### *WatchGuard System Manager with strong encryption*

Because strict export restrictions are put on high encryption software, WatchGuard System Manager is available with two encryption levels. To generate an encrypted end-user profile for Mobile VPN with IPSec, you must make sure you set up your XTM device with the version of WatchGuard System Manager with strong encryption. The IPSec standard requires a minimum of 56-bit encryption. For more information, see *Install WatchGuard System Manager Software* on page 20.

### *Mobile user client computer*

You can install the Mobile VPN with IPSec client software on any computer with Windows 2000 Professional, Windows XP (32-bit and 64-bit), or Windows Vista (32-bit and 64-bit). Before you install the client software, make sure the remote computer does not have any other IPSec VPN client software installed. You must also uninstall any desktop firewall software (other than Microsoft firewall software) from each remote computer. For more information, see *Client Requirements* on page 1018.

**Note** *To distribute the end-user profile as an encrypted (.wgx) file, we recommend that you use WatchGuard System Manager. You can use Firewall XTM Web UI to configure Mobile VPN with IPSec and generate the unencrypted (.ini) end-user profile. For more information about the two types of end-user profile configuration files, see About Mobile VPN Client Configuration Files on page 989.*

## Options for Internet Access Through a Mobile VPN with IPSec Tunnel

You can allow remote users to access the Internet through a Mobile VPN tunnel. This option affects your security because Internet traffic is not filtered or encrypted. You have two options for Mobile VPN tunnel routes: default-route VPN and split tunnel VPN.

### Default-Route VPN

The most secure option is to require that all remote user Internet traffic is routed through the VPN tunnel to the XTM device. From the XTM device, the traffic is then sent back out to the Internet. With this configuration (known as default-route VPN), the XTM device is able to examine all traffic and provide increased security, although the XTM device uses more processing power and bandwidth. When you use

default-route VPN, a dynamic NAT policy must include the outgoing traffic from the remote network. This allows remote users to browse the Internet when they send all traffic to the XTM device.

For more information about dynamic NAT, see *Add Firewall Dynamic NAT Entries* on page 163.

## Split Tunnel VPN

Another configuration option is to enable split tunneling. This configuration allows users to browse the Internet normally. Split tunneling decreases security because XTM device policies are not applied to the Internet traffic, but performance is increased. If you use split tunneling, your client computers should have a software firewall.

## About Mobile VPN Client Configuration Files

With Mobile VPN with IPSec, the network security administrator controls end user profiles. Policy Manager is used to create the Mobile VPN with IPSec group and create an end user profile, with the file extension .wgx or .ini. The .wgx and .ini files contain the shared key, user identification, IP addresses, and settings that are used to create a secure tunnel between the remote computer and the XTM device.

The .wgx file is encrypted with a passphrase that is eight characters or greater in length. Both the administrator and the remote user must know this passphrase. When you use the Mobile VPN with IPSec client software to import the .wgx file, the passphrase is used to decrypt the file and configure the client. The .wgx file does not configure the Line Management settings.

The .ini configuration file is not encrypted. It should only be used if you have changed the **Line Management** setting to anything other than **Manual**. For more information, see **Line Management** on the **Advanced** tab in *Modify an Existing Mobile VPN with IPSec Group Profile* on page 998.

After you use the Add Mobile VPN with IPSec wizard, you can create or re-create a .wgx file at any time. For more information, see *Mobile VPN with IPSec Configuration Files* on page 1011

If you want to lock the profiles for mobile users, you can make them read-only. For more information, see *Lock Down an End User Profile* on page 1011.

## Configure the XTM Device for Mobile VPN with IPsec

You can use Policy Manager to enable Mobile VPN with IPsec for a group of users you have already created, or you can create a new user group. The users in the group can authenticate either to the XTM device, or to a third-party authentication server included in your XTM device configuration.

For more information about how to add users to a group for local Firebox authentication, see *Add Users to a Firebox Mobile VPN Group* on page 996. If you use a third-party authentication server, follow the instructions provided in the documentation from its manufacturer.

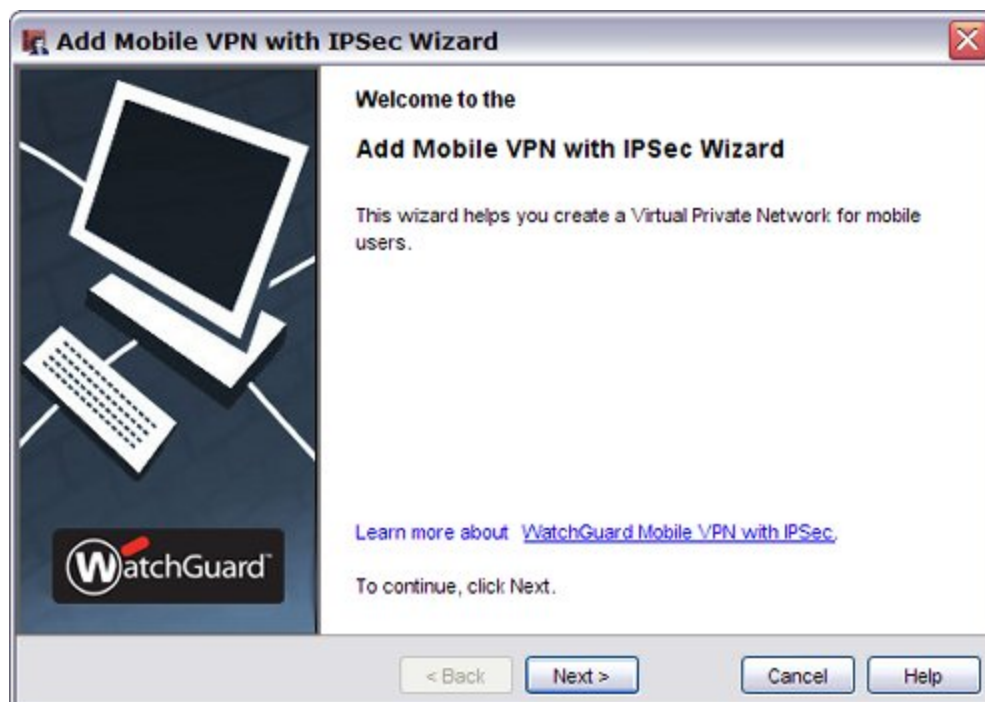
1. Select **VPN > Mobile VPN > IPsec**.

*The Mobile VPN with IPsec Configuration dialog box appears.*



2. Click **Add**.

*The Add Mobile VPN with IPsec Wizard appears.*



3. Click **Next**.

*The Select a user authentication server screen appears.*



4. From the **Authentication Server** drop-down list, select an authentication server.

You can authenticate users to the XTM device (Firebox-DB) or to a RADIUS, VASCO, SecurID, LDAP, or Active Directory server. Make sure that this method of authentication is enabled in Policy Manager. Select **Setup > Authentication > Authentication Servers** to see these settings.

5. In the **Group Name** text box, type the name of the group.

You can type the name of a Mobile VPN group you have already created, or enter a group name for a new Mobile VPN group. Make sure the name is unique among VPN group names, as well as all interface and tunnel names.

For more information about VPN group authentication, see *Types of Firebox Authentication* on page 329.

6. Click **Next**.

*The Select a tunnel authentication method screen appears.*

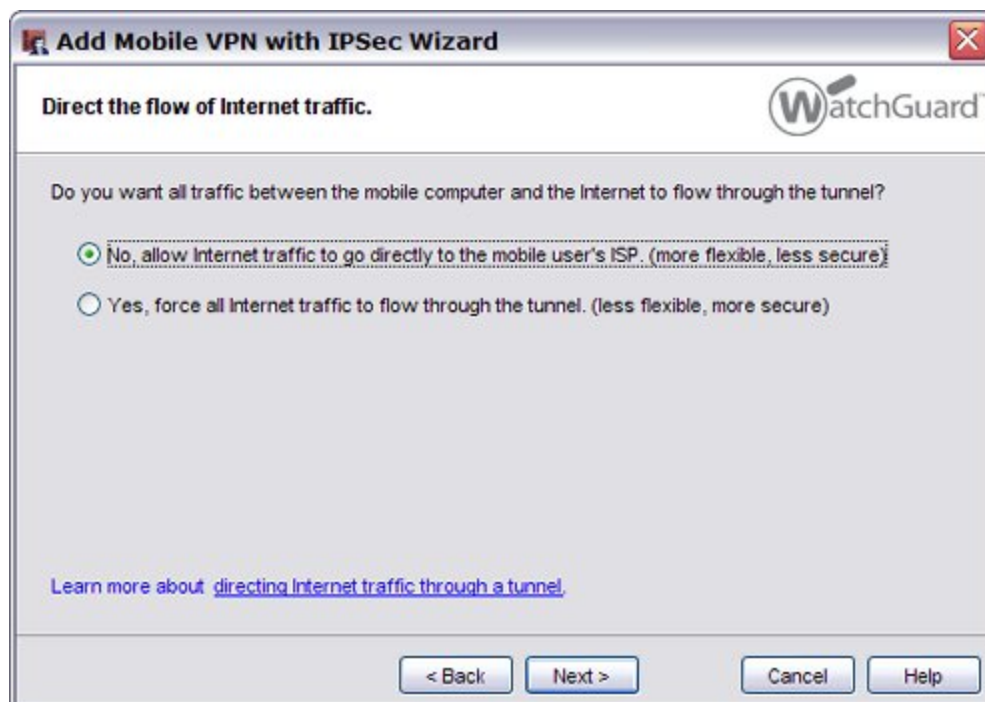
7. Select an option for tunnel authentication:

- **Use this passphrase**  
Type and confirm the passphrase.
- **Use an RSA certificate issued by your WatchGuard Management Server**  
Type the **IP Address** of your Management Server and the **Administration Passphrase**.

8. Click **Next**.

*The Direct the flow of Internet traffic screen appears.*





9. Select an option for Internet traffic:

- **No, allow Internet traffic to go directly to the mobile user's ISP.**  
(Split tunneling)
- **Yes, force all Internet traffic to flow through the tunnel.**  
(Default-route VPN)

For more information about split tunneling and default-route VPN, see *Options for Internet Access Through a Mobile VPN with IPsec Tunnel* on page 988.

10. Click **Next**.

*The Identify the resources accessible through the tunnel screen appears.*



11. Click **Add** to specify the host or network IP addresses that users can connect to through the VPN tunnel.
12. Click **Next**.  
*The Create the virtual IP address pool screen appears.*



13. Click **Add** to add one IP address or an IP address range.  
To add more virtual IP addresses, repeat this step.

Mobile VPN users are assigned one of these IP addresses when they connect to your network. The number of IP addresses should be the same as the number of Mobile VPN users. If High Availability is configured, you must add two virtual IP addresses for each Mobile VPN user. The IP addresses cannot be used for anything else on your network.

14. Click **Next**.

The Add Mobile VPN with IPSec Wizard has completed successfully screen appears.



The Mobile VPN with IPSec group end-user configuration file is available at the location specified on this screen.

15. To add users to the new Mobile VPN with IPSec group, select the **Add users to** check box.
16. Click **Finish**.

## Configure the External Authentication Server

If you create a Mobile VPN user group that authenticates to a third-party server, make sure you create a group on the server that has the same name as the name you added in the wizard for the Mobile VPN group.

If you use Active Directory as your authentication server, the users must belong to an Active Directory *security group* with the same name as the group name you configure for Mobile VPN with IPSec.

For RADIUS, VASCO, or SecurID, make sure that the RADIUS server sends a *Filter-Id* attribute (RADIUS attribute 11) when a user successfully authenticates, to tell the XTM device what group the user belongs to. The value for the *Filter-Id* attribute must match the name of the Mobile VPN group as it appears in Policy Manager. All Mobile VPN users that authenticate to the server must belong to this group.

## Add Users to a Firebox Mobile VPN Group

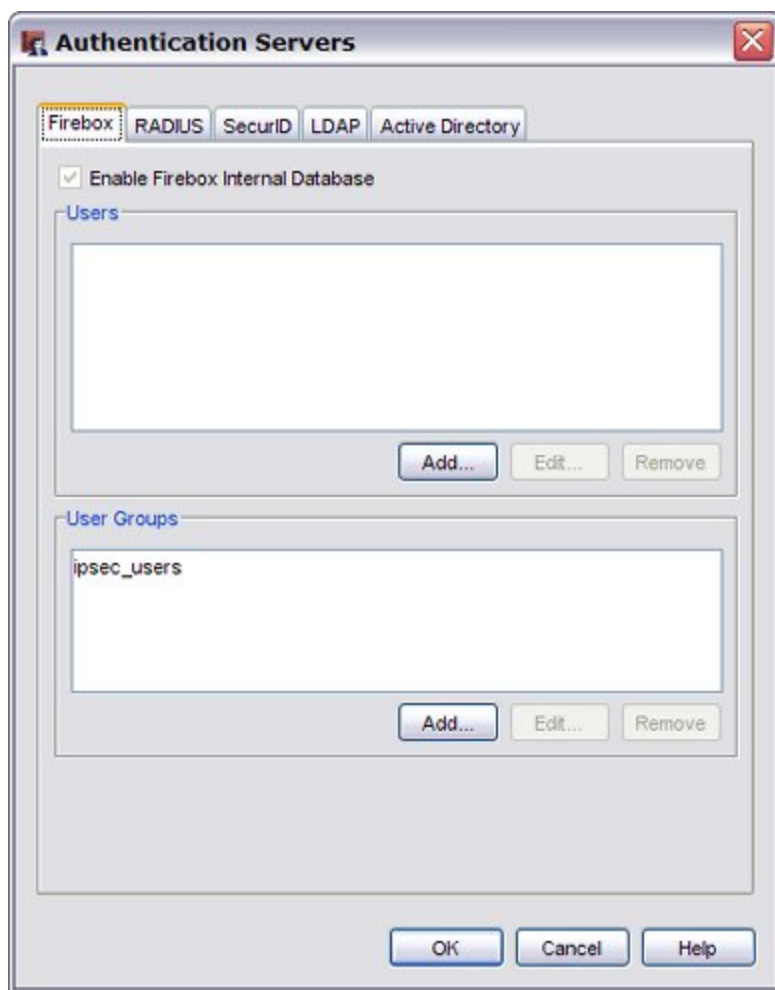
To create a Mobile VPN tunnel with the XTM device, remote users type their user name and password to authenticate. WatchGuard System Manager uses this information to authenticate the user to the XTM device.

To authenticate, users must be part of the group created in the Add Mobile VPN with IPsec Wizard. If you use Firebox authentication, use the instructions below to configure a group in Policy Manager. If you use a third-party authentication server, use the instructions provided in your vendor documentation.

For more information on Firebox groups, see *Types of Firebox Authentication* on page 329.

1. Select **Setup > Authentication > Authentication Servers**.

*The Authentication Servers dialog box appears.*



2. Select the **Firebox** tab.
3. To add a new user, in the **Users** section, click **Add**.

*The Setup Firebox User dialog box appears.*

**Setup Firebox User**

**User Information**

Name:

Description:

Passphrase:

Confirm:

Session Timeout:  hours

Idle Timeout:  minutes

**Firebox Authentication Groups**

Member:

Available: ipsec\_users

<< >>

OK Cancel Help

4. Type a user name and passphrase for the new user. The passphrase must be at least 8 characters long. Type the passphrase again to confirm it.  
*Description is not required. Do not change the values for Session Timeout and Idle Timeout unless the change is necessary.*
5. In the **Firebox Authentication Groups** section, select the group name in the **Available** list and click to make the new user a member of the group you created in the wizard.
6. Click **OK**.  
*The new user appears in the Users list in the Authentication Servers dialog box. The dialog box stays open for you to add more users if you choose.*
7. To close the **Authentication Servers** dialog box, click **OK**.

## Modify an Existing Mobile VPN with IPsec Group Profile

After you use the Mobile VPN with IPsec wizard to create a new .wgx file, you can edit the profile to:

- Change the shared key
- Add access to more hosts or networks
- Restrict access to a single destination port, source port, or protocol
- Change the Phase 1 or Phase 2 settings.

You can use Policy Manager to modify a Mobile VPN with IPsec group profile.

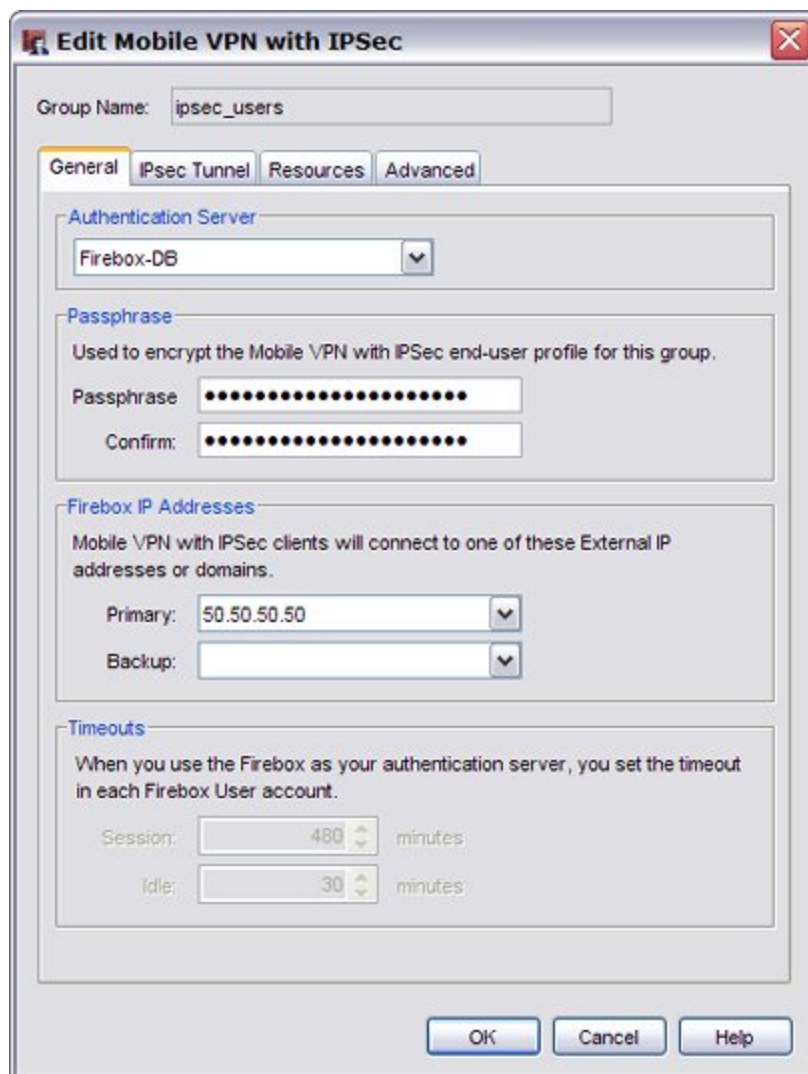
1. Select **VPN > Mobile VPN > IPsec**.

*The Mobile VPN with IPsec Configuration dialog box appears.*



2. Select the group that you want to change from the list.
3. Click **Edit**.

*The Edit Mobile VPN with IPsec dialog box appears.*



4. On the **General** tab, edit the group profile and configure these settings:

#### *Authentication Server*

Select the authentication server to use for this Mobile VPN group. You can authenticate users with the internal XTM device database (Firebox-DB) or with a RADIUS, VASCO, SecurID, LDAP, or Active Directory server.

To configure your authentication server, select **Setup > Authentication > Authentication Servers** from the menu bar in Policy Manager.

#### *Passphrase*

Type a passphrase to encrypt the Mobile VPN profile (.wgx file) that you distribute to users in this group. The shared key can use only standard ASCII characters. If you use a certificate for authentication, this is the PIN for the certificate.

#### *Confirm*

Type the passphrase again.

*Primary*

Select or type the primary external IP address or domain to which Mobile VPN users in this group can connect.

*Backup*

Select or type a backup external IP address or domain to which Mobile VPN users in this group can connect. This backup IP address is optional. If you add a backup IP address, make sure it is an IP address assigned to a XTM device external interface.

*Session*

Select the maximum time in minutes that a Mobile VPN session can be active.

*Idle*

Select the time in minutes before the XTM device closes an idle Mobile VPN session. The session and idle timeout values are the defaults if the authentication server does not use different settings. If you use the XTM device as the authentication server, you must set timeouts in the individual XTM device user accounts.

The session and idle timeouts cannot be longer than the value in the **SA Life** field. To set this field, from the **IPSec Tunnel** tab of the **Edit Mobile VPN with IPSec** dialog box, click **Advanced**. The default value is 8 hours.

5. Select the **IPSec Tunnel** tab.





6. Edit the **IPsec tunnel** tab settings:

*Use the passphrase of the end-user profile as the pre-shared key*

Select this setting to use the passphrase of the end-user profile as the pre-shared key for tunnel authentication. You must use the same shared key on the remote device. Use only standard ASCII characters in the shared key.

*Use a certificate*

Select this setting to use a certificate for tunnel authentication.

For more information, see *Certificates for Mobile VPN with IPsec Tunnel Authentication* on page 875.

*CA IP address*

(This field appears only if you select to use a certificate)

Type the IP address of the Management Server that is configured as the certificate authority.

*Timeout*

(This field appears only if you select to use a certificate)

Type the time in seconds before the certificate authority request times out.

#### *Phase1 Settings*

Select the authentication and encryption methods for the Mobile VPN tunnel.

To configure advanced settings, such as NAT Traversal or the key group, click the **Advanced** button, and see the procedure described in *Define Advanced Phase 1 Settings* on page 1006. The Encryption options are listed from the most simple and least secure to the most complex and most secure.

DES

3DES

AES (128 bit)

AES (192 bit)

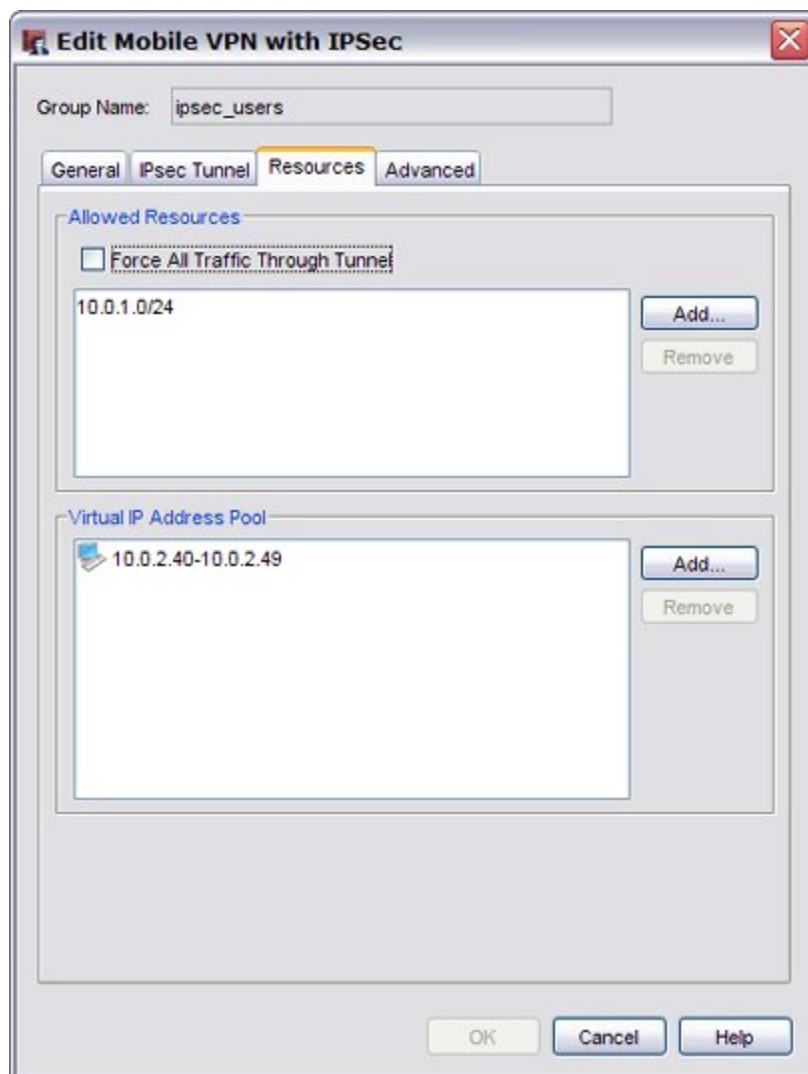
AES (256 bit)

#### *Phase2 Settings*

Select the proposal and key expiration settings for the Mobile VPN tunnel. You can also enable Perfect Forward Secrecy (PFS) and set the Diffie-Hellman group.

To change other proposal settings, click the **Proposal** button, and see the procedure described in *Define Advanced Phase 2 Settings* on page 1008.

7. Select the **Resources** tab.



- Add or remove allowed network resources and virtual IP addresses:

#### *Allowed Resources list*

This list shows the resources that users in the group can get access to on the network.

To add a Host IP address or Network IP address to the network resources list, click **Add**.

To delete a Host IP address or Network IP address from the network resources list, select a resource and click **Remove**

#### *Force All Traffic Through Tunnel*

Select this check box to send all Mobile VPN user Internet traffic through the VPN tunnel.

When this option is selected, Mobile VPN user Internet traffic is sent through the VPN, but web sites can be slower for those users. If this is not selected, Mobile VPN user Internet traffic is not examined by XTM device policies, but users can browse the Internet more quickly.

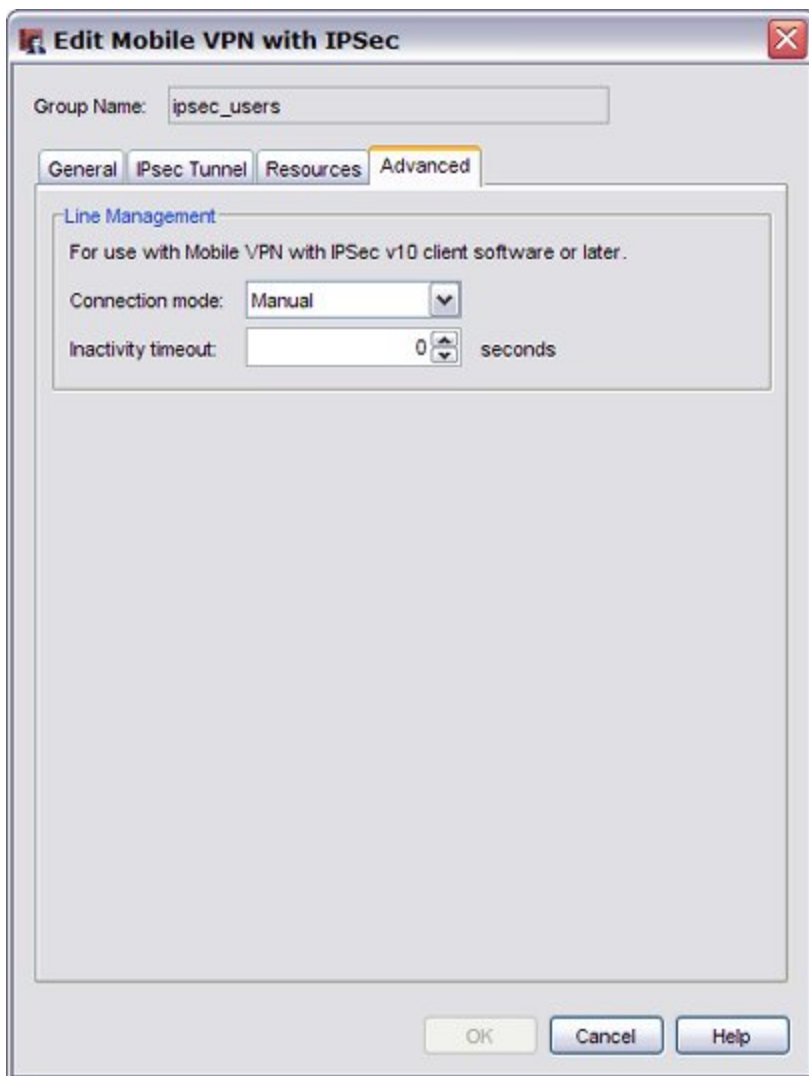
#### *Virtual IP Address Pool*

This list shows the internal IP addresses that are used by Mobile VPN users over the tunnel. These addresses are used only when they are needed.

To add a Host IP address or a Host Range of IP addresses to the virtual IP address pool, click **Add**.

To clear the selected Host IP address or a Host Range of IP addresses from the virtual IP address pool, click **Remove**.

- 9. Select the **Advanced** tab.



- 10. Configure the **Line Management** settings:

*Connection mode*

**Manual** — In this mode, the client does not try to restart the VPN tunnel automatically if the VPN tunnel goes down. This is the default setting.

To restart the VPN tunnel, you must click the **Connect** button in Connection Monitor, or right-click the Mobile VPN icon on your Windows desktop toolbar and click **Connect**.

**Automatic** — In this mode, the client tries to start the connection when your computer sends traffic to a destination that you can reach through the VPN. The client also tries to restart the VPN tunnel automatically if the VPN tunnel goes down.

**Variable** — In this mode, the client tries to restart the VPN tunnel automatically until you click **Disconnect**. After you disconnect, the client does not try to restart the VPN tunnel again until after the next time you click **Connect**.

#### *Inactivity timeout*

If the Connection Mode is set to **Automatic** or **Variable**, the Mobile VPN with IPSec client software does not try to negotiate the VPN connection again for the amount of time you specify.

**Note** *The default Line Management settings are **Manual** and **0 seconds**. If you change either setting, you must use the .ini file to configure the client software.*

11. Click **OK**.

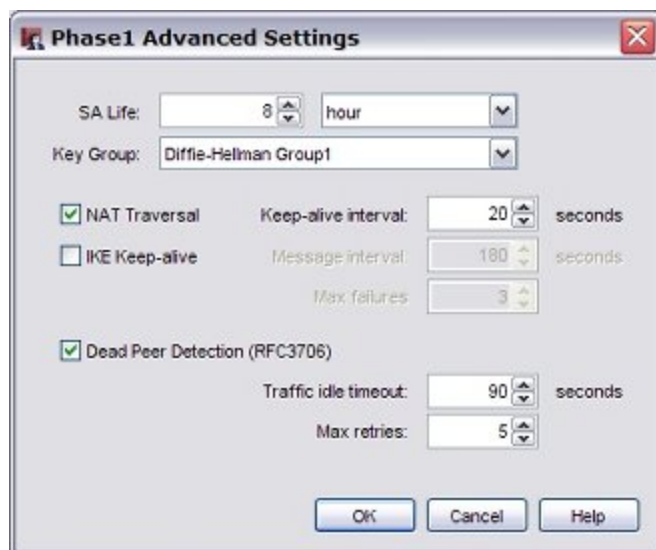
You must save the configuration to the XTM device. End users that are members of the group you edit are not able to connect until they receive a new configuration file and import it into their Mobile VPN with IPSec client software. You must generate the configuration file and then provide it to the end users.

For more information, see *Mobile VPN with IPSec Configuration Files* on page 1011.

## Define Advanced Phase 1 Settings

You can define the advanced Phase 1 settings for your Mobile VPN user profile.

1. From the **IPsec Tunnel** tab of the **Edit Mobile VPN with IPsec** dialog box, select **Advanced**.  
*The Phase1 Advanced Settings dialog box appears.*



2. Configure the setting options for your profile. We recommend you use the default settings.

### *SA Life*

Select a SA (security association) lifetime duration and select **Hour** or **Minute** from the drop-down list. When the SA expires, a new Phase 1 negotiation starts. A shorter SA life is more secure but the SA negotiation can cause existing connections to fail.

### *Key Group*

Select a Diffie-Hellman group. You can choose from groups 1, 2, and 5.

Diffie-Hellman groups determine the strength of the master key used in the key exchange process. Higher group numbers have greater security, but use more time and resources on the client computer and requires the XTM device to make the keys.

### *NAT Traversal*

Select this check box to build a Mobile VPN tunnel between the XTM device and another device that is behind a NAT device. NAT Traversal, or UDP Encapsulation, allows traffic to route to the correct destinations.

### *IKE Keep-alive*

Select this check box only if this group connects to an older Firebox device that does not support Dead Peer Detection. All Firebox devices with Fireware v9.x or lower, Edge v8.x or lower, and all versions of WFS do not support Dead Peer Detection. For these devices, select this check box to enable the device to send messages to its IKE peer to keep the VPN tunnel open. Do not select both IKE Keep-alive and Dead Peer Detection.

*Message interval*

Select the number of seconds for the IKE keep-alive message interval.

*Max failures*

Set the maximum number of times there is no response to the XTM device IKE keep-alive messages before it terminates the VPN connection and starts a new Phase 1 negotiation.

*Dead Peer Detection*

Select this check box to enable Dead Peer Detection (DPD). Your XTM device must support DPD. All XTM devices and all Firebox devices with Fireware v10.x or higher and Edge v10.x or higher support DPD. Do not select both IKE Keep-alive and Dead Peer Detection.

DPD is based on RFC 3706 and uses IPSec traffic patterns to determine if a connection is live before a packet is sent. When you select DPD, the Firebox or XTM device attempts to connect to the peer when traffic has not been received for the selected time period. If DPD determines a peer is unavailable, additional connection attempts are not made.

*Traffic Idle Timeout*

Set the number of seconds the XTM device waits before it attempts to connect to the peer.

*Max retries*

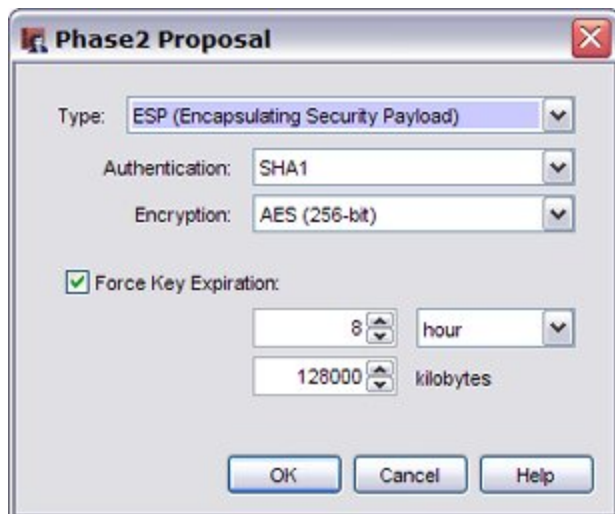
Set the maximum number of times there is no response to before the XTM device determines the peer connection is unavailable, terminates the VPN connection, and starts a new Phase 1 negotiation.

3. Click **OK**.

## Define Advanced Phase 2 Settings

You can define the advanced Phase 2 settings for your Mobile VPN user profile.

1. From the **IPsec Tunnel** tab of the **Edit Mobile VPN with IPsec** dialog box, click **Proposal**.  
*The Phase2 Proposal dialog box appears.*



2. Configure the setting options for your profile. We recommend that you use the default settings.

### *Type*

**ESP** or **AH** are the two proposal method options. Only ESP is supported at this time.

### *Authentication*

Select **SHA1** or **MD5** for the authentication method from the drop-down list.

### *Encryption*

Select an encryption method from the drop-down list. The options are listed from the most simple and least secure to the most complex and most secure.

- DES
- 3DES
- AES (128 bit)
- AES (192 bit)
- AES (256 bit)

### *Force Key Expiration*

Select this check box to regenerate the gateway endpoints and exchange new keys after a specified amount of time or network traffic passes through the gateway.



In **Force Key Expiration** text boxes and drop-down list, select a duration and a number of kilobytes after which the key expires.

If **Force Key Expiration** is disabled, or if it is enabled and both the time and kilobytes are set to zero, the XTM device tries to use the key expiration time set for the peer. If this is also disabled or zero, the XTM device uses the default key expiration time of 8 hours. The maximum time before a key expiration is one year.

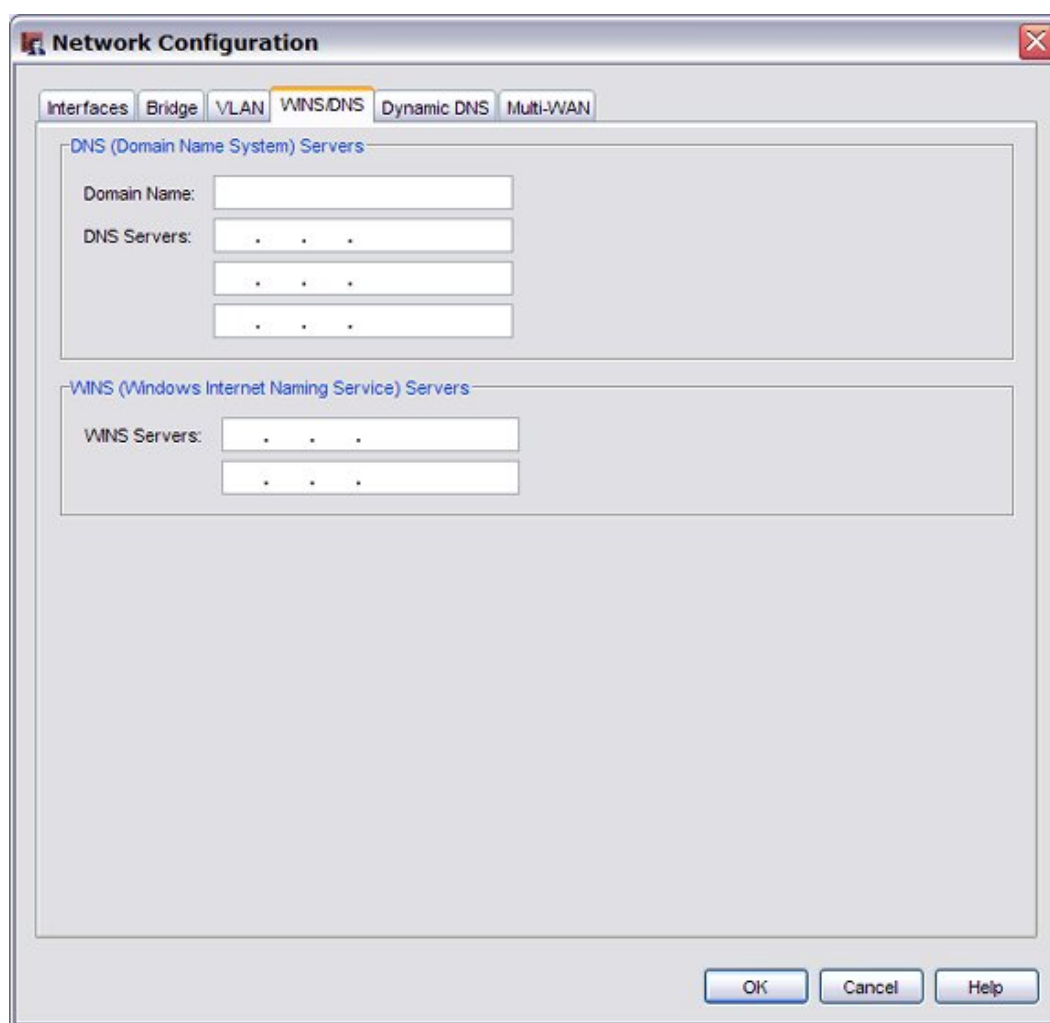
3. Click **OK**.

## Configure WINS and DNS Servers

Mobile VPN clients rely on shared Windows Internet Name Server (WINS) and Domain Name System (DNS) server addresses. DNS translates host names into IP addresses. WINS resolves NetBIOS names to IP addresses. These servers must be accessible from the XTM device trusted interface.

You can use Policy Manager to configure the WINS and DNS servers for you Mobile VPN clients. Make sure you use only an internal DNS server. Do not use external DNS servers.

1. Select **Network > Configuration**.  
*The Network Configuration dialog box appears.*
2. Select the **WINS/DNS** tab.  
*The information for the WINS and DNS servers appears.*



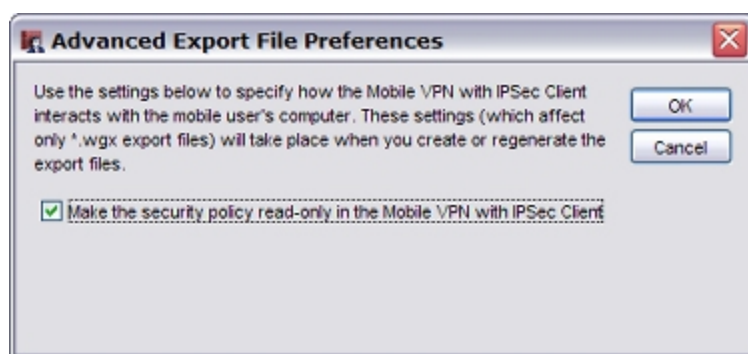
The screenshot shows the 'Network Configuration' dialog box with the 'WINS/DNS' tab selected. The dialog has a title bar with a close button (X) and a menu icon. Below the title bar are several tabs: 'Interfaces', 'Bridge', 'VLAN', 'WINS/DNS' (which is highlighted), 'Dynamic DNS', and 'Multi-WAN'. The main area is divided into two sections. The first section is titled 'DNS (Domain Name System) Servers' and contains a 'Domain Name:' text box and three 'DNS Servers:' text boxes, each with a placeholder of three dots. The second section is titled 'WINS (Windows Internet Naming Service) Servers' and contains two 'WINS Servers:' text boxes, each with a placeholder of three dots. At the bottom right of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

3. Type a domain name for the DNS server.
4. In the **DNS Servers** and **WINS Servers** text boxes, type the addresses for the WINS and DNS servers.
5. Click **OK**.

## Lock Down an End User Profile

You can use Policy Manager to lock down the end user profile so that users can see some settings but not change them, and hide other settings so that users cannot see or change them. We recommend that you lock down all profiles so that users cannot make changes to their profiles. This setting is for .wgx end user profile files. You cannot make .ini end user profile files read only.


1. Select **VPN > Mobile VPN > IPSec**.  
*The Mobile VPN with IPSec Configuration dialog box appears.*
2. Click **Advanced**.  
*The Advanced Export File Preferences dialog box appears.*



3. To give mobile users read-only access to their profiles, select the **Make the security policy read-only in the Mobile VPN with IPSec Client** check box.
4. Click **OK**.

## Save the Profile to a XTM Device

To activate a new Mobile VPN user profile, you must save the configuration file to the XTM device.

From Policy Manager, click .  
Or, select **File > Save > To Firebox**.

## Mobile VPN with IPSec Configuration Files

To configure the Mobile VPN with IPSec client, you import a configuration file. The configuration file is also called the end user profile file. There are two types of configuration files.

### .wgx

The .wgx files are encrypted and can be set so that the mobile user cannot change settings in the Mobile VPN with IPsec client software. For more information, see *Lock Down an End User Profile* on page 1011. A .wgx file cannot set the Line Management settings in the client software. If you configure **Line Management** to anything other than **Manual**, you must use a .ini configuration file.

*.ini*

The *.ini* file should only be used if you have changed the **Line Management** setting to anything other than **Manual**. For more information, see **Line Management** on the **Advanced** tab in *Modify an Existing Mobile VPN with IPSec Group Profile* on page 998. The *.ini* configuration file is not encrypted.

When you first configure a Mobile VPN with IPSec group, or if you make a change to the settings for a group, you must regenerate the configuration file for the group and provide it to mobile users. Mobile VPN configuration files, or profiles, are located in:

```
C:\Documents and Settings\All Users\  
  Shared Watchguard\muvpn\ip_address\config_name\wgx\config_name.wgx
```

and

```
C:\Documents and Settings\All Users\  
  Shared Watchguard\muvpn\ip_address\config_name\ini\config_name.ini
```

If you use certificates for authentication, the certificate files are also created.

You can use Policy Manager to generate an end user profile file for a group.

1. Select **VPN > Mobile VPN > IPSec**.
2. Select the Mobile VPN group and click **Generate**.

You can now distribute the configuration file to the mobile users.

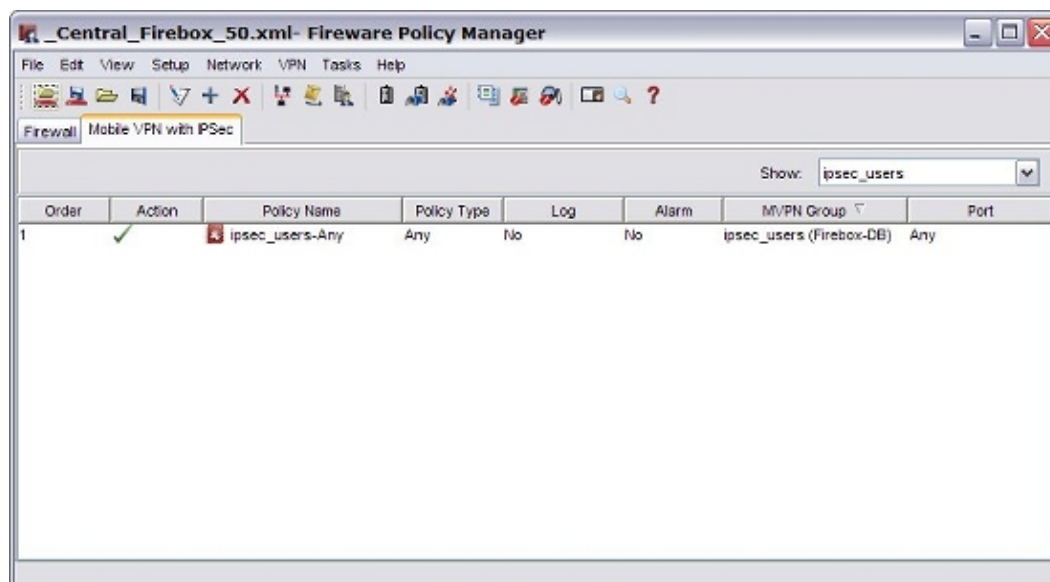
## Configure Policies to Filter Mobile VPN Traffic

In a default configuration, Mobile VPN with IPSec users have full access to XTM device resources with the *Any* policy. The *Any* policy allows traffic on all ports and protocols between the Mobile VPN user and the network resources available through the Mobile VPN tunnel. To restrict VPN user traffic by port and protocol, the *Any* policy on the **Mobile VPN with IPSec** tab can be deleted and replaced with policies that restrict access.

### Add Individual Policies

You can use Policy Manager to create policies that restrict VPN user traffic.

1. Select the **Mobile VPN with IPSec** tab.



- From the **Show** drop-down list, select the name of the Mobile VPN group for which you want to add a policy. You must select a group before you add a policy.
- Add, edit, and delete policies as described in *About Policies* on page 363.
- Save your configuration file to the XTM device after you make these changes.

## Change the View

You can choose to see the policy list as large icons or as a detailed list.

- To see large icons and no details, select **View > Large Icons**.
- To see more information in a detailed list, select **View > Details**.

Under **M/VPN Group**, Policy Manager shows the authentication server for the Mobile VPN group in parentheses.

## Distribute the Software and Profiles

WatchGuard recommends distributing end-user profiles by encrypted email or with another secure method. Each client computer must have:

- ### Software installation package

The **WatchGuard Mobile VPN with IPSec** installation package is located on the WatchGuard LiveSecurity Service web site at: <https://www.watchguard.com/archive/softwarecenter.asp>  
To download software, you must log in to the site with your LiveSecurity Service user name and password.

- ### The end user profile

This file contains the group name, shared key, and settings that allow a remote computer to connect securely over the Internet to a protected, private computer network. The end user profile has the filename **groupname.wgx**. The default location of the .wgx file is:

```
C:\Documents and Settings\All Users\Shared WatchGuard
  \mvpn\\wgx
```

- **Two certificate files, if you use certificates to authenticate**

These are the .p12 file, which is an encrypted file containing the certificate; and cacert.pem, which contains the root (CA) certificate. The .p12 and cacert.pem files can be found in the same location as the .wgx end user profile.

- **User documentation**

Documentation to help the remote user install the Mobile VPN client and import the Mobile VPN configuration file can be found in the *About Mobile VPN Client Configuration Files* topics.

- **Passphrase**

To import the end user profile, the user must type a passphrase. This key decrypts the file and imports the security policy into the Mobile VPN client. The passphrase is set during the creation of the Mobile VPN group in Policy Manager. To change the shared key, see *Modify an Existing Mobile VPN with IPsec Group Profile* on page 998.

**Note** *The end user profile passphrase, user name, and user password are highly sensitive information. For security reasons, we recommend that you do not provide this information by email. Because email is not secure, an unauthorized user can get the information and gain access to your internal network. Give the user the information by telling it to the user, or by some other method that does not allow an unauthorized person to intercept it.*

## Additional Mobile VPN Topics

This section describes special topics for Mobile VPN with IPsec.

### Making Outbound IPsec Connections from Behind an XTM Device

A user might have to make IPsec connections to an XTM device from behind another XTM device. For example, if a mobile employee travels to a customer site that has a XTM device, that user can make IPsec connections to their network. For the local XTM device to correctly manage the outgoing IPsec connection, you must set up an IPsec policy that includes the IPsec packet filter.

For more information on how to enable policies, see *About Policies* on page 363.

Because the IPsec policy enables a tunnel to the IPsec server and does not complete any security checks at the firewall, add only the users that you trust to this policy.

### Terminate IPsec Connections

To fully stop VPN connections, the XTM device must be restarted. Current connections do not stop when you remove the IPsec policy.

## Global VPN Settings

Global VPN settings on your XTM device apply to all manual BOVPN tunnels, managed tunnels, and Mobile VPN tunnels. You can use these settings to:

- Enable IPSec pass-through.
- Clear or maintain the settings of packets with Type of Service (TOS) flags set.
- Use an LDAP server to verify certificates.

To change these settings, from Policy Manager, select **VPN > VPN Settings**. For more information on these settings, see *About Global VPN Settings* on page 935.

## See the Number of Mobile VPN Licenses

From Policy Manager, you can see the number of Mobile VPN licenses that are available with the feature key.

1. From , select **Setup > Feature Keys**.  
*The Firebox Feature Key dialog box appears.*
2. Scroll down to **Mobile VPN Users** in the **Feature** column, and find the number in the **Value** column.  
This is the maximum number of Mobile VPN users that can connect at the same time.

## Purchase Additional Mobile VPN Licenses

WatchGuard Mobile VPN with IPSec is an optional feature. Each XTM device includes a number of Mobile VPN licenses. You can purchase more licenses for Mobile VPN.

Licenses are available through your local reseller, or on the WatchGuard web site:

<http://www.watchguard.com/sales>

## Add Feature Keys

For more information on how to add feature keys, see *About Feature Keys* on page 58.

## Mobile VPN and VPN Failover

You can configure VPN tunnels to fail over to a backup endpoint if the primary endpoint becomes unavailable. For more information on VPN failover, see *Configure VPN Failover* on page 959.

If VPN failover is configured and failover occurs, Mobile VPN sessions do not continue. You must authenticate your Mobile VPN client again to make a new Mobile VPN tunnel.

From Policy Manager, you can configure VPN failover for Mobile VPN tunnels.

1. Select **VPN > Mobile VPN > IPSec**.  
*The Mobile VPN with IPSec Configuration dialog box appears.*
2. Select a mobile user group from the list and click **Edit**.  
*The Edit Mobile VPN with IPSec dialog box appears.*
3. Select the **General** tab.
4. In the **Firebox IP Addresses** section, type a backup WAN interface IP address in the **Backup** text box.  
You can specify only one backup interface for tunnels to fail over to, even if you have additional WAN interfaces.

## Configure Mobile VPN with IPSec to a Dynamic IP Address

We recommend that you use either a static IP address for a XTM device that is a VPN endpoint, or use Dynamic DNS. For more information about Dynamic DNS, see *About the Dynamic DNS Service* on page 96.

If neither of these options are possible, and the external IP address of the XTM device changes, you must either give remote IPSec users a new .wgx configuration file or have them edit the client configuration to include the new IP address each time that the IP address changes. Otherwise, IPSec users cannot connect until they get the new configuration file or IP address.

Use these instructions to configure the XTM device and support the IPSec client users if the XTM device has a dynamic IP address and you cannot use Dynamic DNS.

### Keep a Record of the Current IP Address

From Policy Manager, you can find the current IP address of the XTM device external interface.

1. Select **Network > Configuration**.
2. Look for the interface with type **External** and look at the IP address in the **IP** column. This is the external IP address of the XTM device.

This is the IP address that is saved to the .wgx configuration files. When remote users say that they cannot connect, check the external IP address of the XTM device to see if the IP address has changed.

### Configure the XTM Device and IPSec Client Computers

The XTM device must have an IP address assigned to the external interface before you download the .wgx files. This is the only difference from the normal configuration of the XTM device and IPSec client computers.



## Update the Client Configurations when the Address Changes

When the external IP address of the XTM device changes, the remote Mobile VPN with IPSec client computers cannot connect until they have been configured with the new IP address. You can change the IP address in two ways.

- Give remote users a new .wgx configuration file to import.
- Have remote users manually edit the IPSec client configuration. For this option, you must configure the XTM device so remote users can edit the configuration. For more information, see *Lock down an end user profile* *Lock Down an End User Profile* on page 1011.

From Policy Manager, you can give users a new .wgx configuration file.

1. Select **VPN > Mobile VPN > IPSec**.
2. Select a Mobile VPN user group and click **Generate** to generate and download the .wgx files.
3. Distribute the .wgx files to the remote users.
4. Tell the remote users to *Import the End-User Profile*.

To have users manually edit the client configuration:

1. Give remote users the new external IP address of the XTM device and tell them to perform the next five steps.
2. On the IPSec client computer, select **Start > All Programs > WatchGuard Mobile VPN > Mobile VPN Monitor**.
3. Select **Configuration > Profile Settings**.
4. Select the profile and click **Configure**.
5. In the left column, select **IPSec General Settings**.
6. In the **Gateway** text box, type the new external IP address of the XTM device.

## About the Mobile VPN with IPSec Client

The WatchGuard Mobile VPN with IPSec client is installed on a mobile client computer, whether the user travels or works from home. The user connects with a standard Internet connection and activates the Mobile VPN client to get access to protected network resources.

The Mobile VPN client creates an encrypted tunnel to your trusted and optional networks, which are protected by a XTM device. The Mobile VPN client allows you to supply remote access to your internal networks and not compromise your security.

## Client Requirements

Before you install the client, make sure you understand these requirements and recommendations.

You must configure your XTM device to work with Mobile VPN with IPsec. If you have not, see the topics that describe how to configure your XTM device to use Mobile VPN.

- You can install the Mobile VPN with IPsec client software on any computer with Windows 2000, Windows XP (32-bit and 64-bit), Windows Vista (32-bit and 64-bit), or Windows 7 (32 bit and 64 bit). Before you install the client software, make sure the remote computer does not have any other IPsec VPN client software installed. You must also uninstall any desktop firewall software (other than Microsoft firewall software) from each remote computer.
- If the client computer uses Windows XP, you must log on using an account that has administrator rights to install the Mobile VPN client software and to import the .wgx or .ini configuration file. Administrator rights are not required to connect after the client has been installed and configured.
- If the client computer uses Windows Vista, you must log on using an account that has administrator rights to install the Mobile VPN client software. Administrator rights are not required to import a .wgx or .ini file or to connect after the client has been installed.
- We recommend that you check to make sure all available service packs are installed before you install the Mobile VPN client software.
- WINS and DNS settings for the Mobile VPN client are obtained in the client profile you import when you set up your Mobile VPN client.
- We recommend that you do not change the configuration of any Mobile VPN client setting not explicitly described in this documentation.

## Install the Mobile VPN with IPsec Client Software

The installation process consists of two parts: install the client software on the remote computer, and import the end-user profile into the client. Before you start the installation, make sure you have the following installation components:

- The Mobile VPN installation file
- An end-user profile, with a file extension of .wgx or .ini
- Passphrase
- A cacert.pem and a .p12 file (if you use certificates to authenticate)
- User name and password

**Note** Write the passphrase down and keep it in a secure location. You must use it during the final steps of the installation procedure.

To install the client:

1. Copy the Mobile VPN installation file to the remote computer and extract the contents of the file.
2. Copy the end user profile (the .wgx or .ini file) to the root directory on the remote (client or user) computer. Do not run the installation software from a CD or other external drive.  
*If you use certificates to authenticate, copy the cacert.pem and .p12 files to the root directory.*
3. Double-click the .exe file you extracted in Step 1. This starts the WatchGuard Mobile VPN Installation wizard. You must restart your computer when the installation wizard completes.

For detailed instructions written for Mobile VPN with IPSec client end-users, see *End-User Instructions for WatchGuard Mobile VPN with IPSec Client Installation* on page 1031.

## Import the End-User Profile

When the computer restarts, the WatchGuard Mobile VPN Connection Monitor dialog box appears. When the software starts for the first time after you install it, you see this message:

```
There is no profile for the VPN dial-up!  
Do you want to use the configuration wizard for creating a profile now?
```

Click **No**.

To turn off the Connection Monitor auto-start functionality, select **View > AutoStart > No Autostart**.

To import a Mobile VPN configuration .wgx or .ini file:

1. From your Windows desktop, select **Start > All Programs > WatchGuard Mobile VPN > Mobile VPN Monitor**.
2. From the WatchGuard Mobile VPN Connection Monitor, select **Configuration > Profile Import**.  
*The Profile Import Wizard starts.*
3. On the **Select User Profile** screen, browse to the location of the .wgx or .ini configuration file.
4. Click **Next**.
5. If you use a .wgx file, on the **Decrypt User Profile** screen, type the passphrase. The passphrase is case-sensitive.
6. Click **Next**.
7. On the **Overwrite or add Profile** screen, you can select to overwrite a profile of the same name. This is useful if your network administrator gives you a new .wgx file to import.
8. Click **Next**.
9. On the **Authentication** screen, you can select whether to type the user name and password that you use to authenticate the VPN tunnel.  
If you keep these fields empty, you are prompted to enter your user name and password each time you connect.  
If you type your user name and password, the XTM device stores them and you do not have to enter this information each time you connect. However, this is a security risk. You can also type just your user name and keep the **Password** text box empty.
10. Click **Next**.
11. Click **Finish**.

*The computer is now ready to use Mobile VPN with IPSec.*

## Select a Certificate and Enter the PIN

If you use certificates for authentication, you must add the correct certificate and then configure the Mobile VPN connection profile to use that certificate.

### Add the Certificate

To add the certificate to the Mobile VPN client configuration, you must have a cacert.pem and a .p12 file.

1. Select **Configuration > Certificates**.
2. Click **Add**.
3. On the **User Certificate** tab, select **from PKS#12 file** from the **Certificate** drop-down list.
4. Adjacent to the **PKS#12 Filename** text box, click the button and browse to the location of the .p12 file.
5. Click **OK**.
6. Click **Close**.

## Select the Certificate for the Mobile VPN profile

After you add the certificate, you must select the correct certificate set for the connection profile.

1. Select **Configuration > Profiles**.
2. Select the profile name. Click **Edit**.
3. Click **Identities**.
4. From the **Certificate configuration** drop-down box, select the certificate configuration you added.
5. Select **Connection > Enter PIN**.
6. Type the passphrase and click **OK**.

## Uninstall the Mobile VPN Client

It can become necessary to uninstall the Mobile VPN client. We recommend that you use the Windows **Add/Remove Programs** tool to uninstall the Mobile VPN client. After the Mobile VPN client software is installed the first time, it is not necessary to uninstall the Mobile VPN client software before you apply an upgrade to the client software.

Before you start, disconnect all tunnels and close the Mobile VPN Connection Monitor. From the Windows desktop:

1. Click **Start > Settings > Control Panel**.  
*The Control Panel window appears.*
2. Double-click the **Add/Remove Programs** icon.  
*The Add/Remove Programs window appears.*
3. Select **WatchGuard Mobile VPN** and click **Change/Remove**.  
*The InstallShield Wizard window appears.*
4. Click **Remove** and click **Next**.  
*The Confirm File Deletion dialog box appears.*
5. Click **OK** to completely remove all of the components. If you do not select this check box at the end of the uninstall, the next time you install the Mobile VPN software the connection settings from this installation are used for the new installation.

## Connect and Disconnect the Mobile VPN Client

The WatchGuard Mobile VPN with IPSec client software makes a secure connection from a remote computer to your protected network over the Internet. To start this connection, you must connect to the Internet and use the Mobile VPN client to connect to the protected network.

Start your connection to the Internet through a Dial-Up Networking connection or LAN connection. Then, use the instructions below or select your profile, connect, and disconnect by right-clicking the Mobile VPN icon on your Windows toolbar.

1. From your Windows desktop, select **Start > All Programs > WatchGuard Mobile VPN > Mobile VPN Monitor**.
2. From the **Profile** drop-down list, select the name of the profile you created for your Mobile VPN connections to the XTM device.



3. Click   to connect.

## Disconnect the Mobile VPN Client

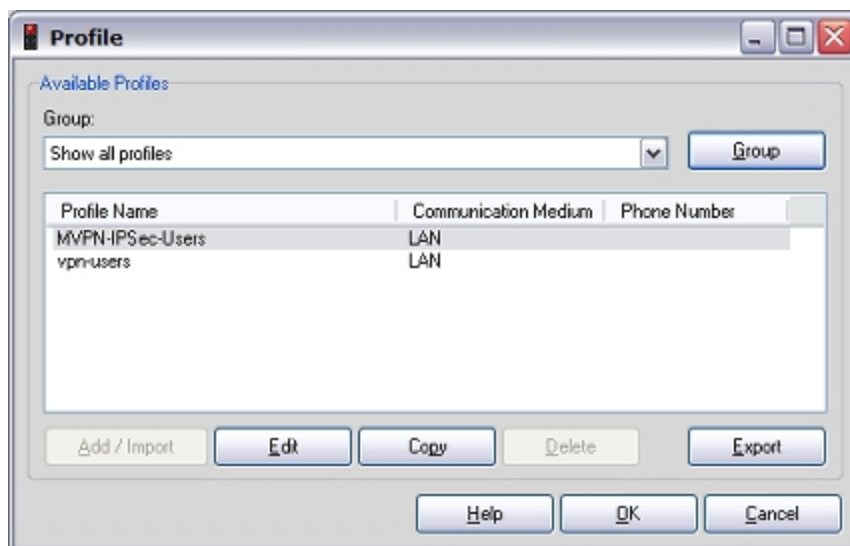
On the Mobile VPN Monitor dialog box, click   to disconnect.

## Control Connection Behavior

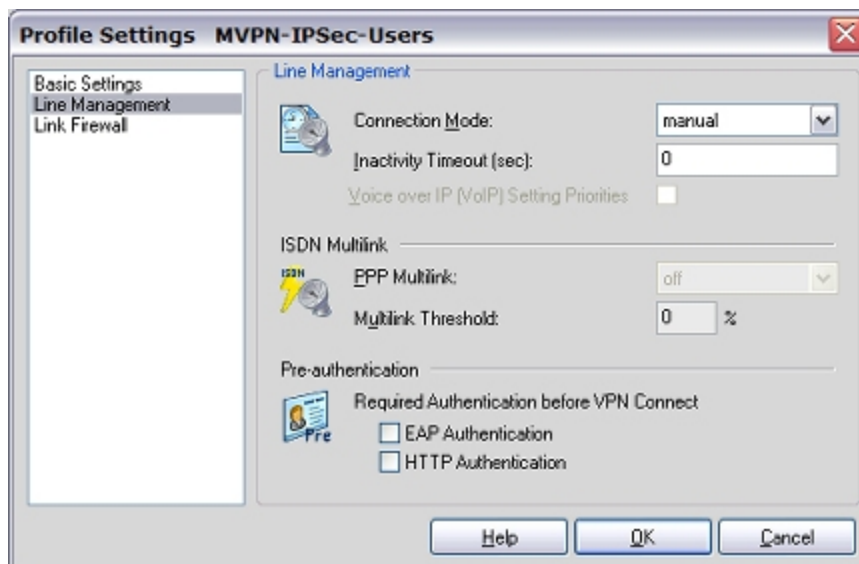
For each profile you import, you can control the action the Mobile VPN client software takes when the VPN tunnel becomes unavailable for any reason. You can configure these settings on the XTM device and use a .ini file to configure the client software. A .wgx file does not change these settings.

From the WatchGuard Mobile VPN Connection Monitor, you can manually set the behavior of the Mobile VPN client when the VPN tunnel becomes unavailable.

1. Select **Configuration > Profiles**.
2. Select the name of the profile and click **Edit**.



3. Select **Line Management**.



4. In the **Connection Mode** drop-down list, select a connection behavior for this profile.

- **Manual** — When you select **manual** connection mode, the client does not try to restart the VPN tunnel automatically if the VPN tunnel goes down. To restart the VPN tunnel, you must click the **Connect** button in Connection Monitor, or right-click the Mobile VPN icon on your Windows desktop toolbar and click **Connect**.
- **Automatic** — When you select **automatic** connection mode, the client tries to start the connection when your computer sends traffic to a destination that you can reach through the VPN. The client also tries to restart the VPN tunnel automatically if the VPN tunnel goes down.
- **Variable** — When you select **variable** connection mode, the client tries to restart the VPN tunnel automatically until you click **Disconnect**. The client does not try to restart the VPN tunnel again until after the next time you click **Connect**.

5. Click **OK**.

## Mobile VPN With IPSec Client Icon

The Mobile VPN with IPSec client icon appears in the Windows desktop system tray to show the status of the desktop firewall, the link firewall, and the VPN network. You can right-click the icon to connect and disconnect your Mobile VPN and see which profile is in use.

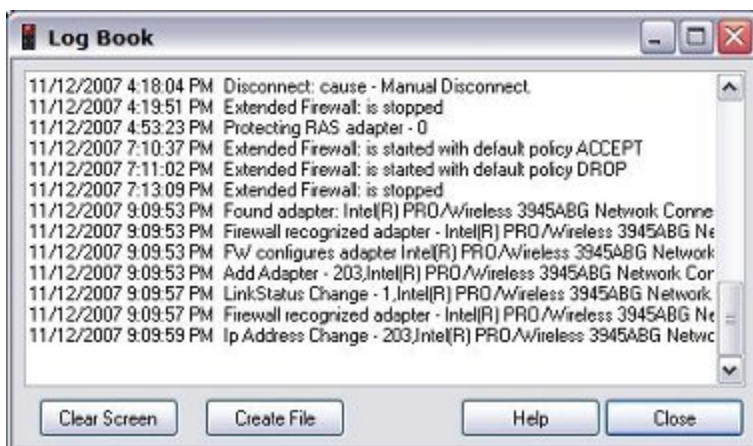


## See Mobile VPN Log Messages

You can use the Mobile VPN client log file to troubleshoot problems with the VPN client connection.

To see Mobile VPN log messages, select **Log > Logbook** from the Connection Monitor.

The Log Book dialog box appears.



## Secure Your Computer with the Mobile VPN Firewall

The WatchGuard Mobile VPN with IPsec client includes two firewall components:

### *Link firewall*

The link firewall is not enabled by default. When the link firewall is enabled, your computer discards any packets received from other computers. You can choose to enable the link firewall only when a Mobile VPN tunnel is active, or enable it all the time.

### *Desktop firewall*

This full-featured firewall can control connections to and from your computer. You can define friendly networks and set access rules separately for friendly and unknown networks.

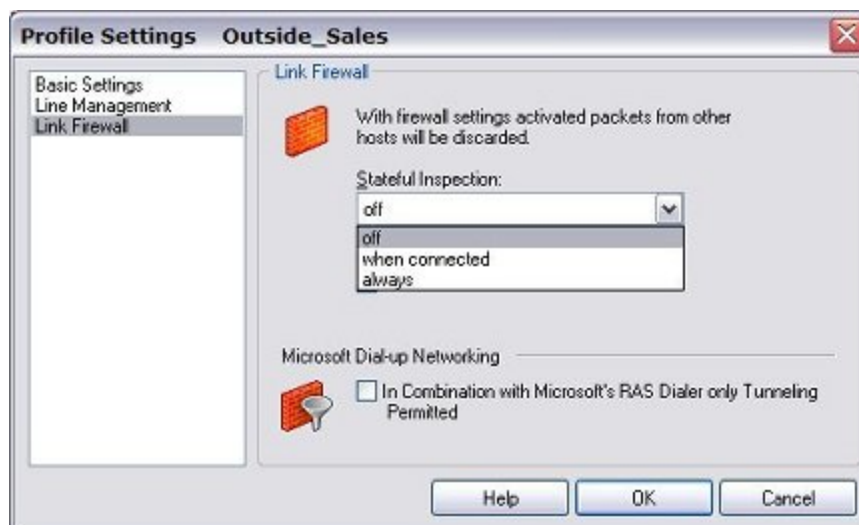
## Enable the Link Firewall

When the link firewall is enabled, the Mobile VPN client software drops any packets sent to your computer from other hosts. It allows only packets sent to your computer in response to packets your computer sends. For example, if you send a request to an HTTP server through the tunnel from your computer, the reply traffic from the HTTP server is allowed. If a host tries to send an HTTP request to your computer through the tunnel, it is denied.

To enable the link firewall:

1. From the WatchGuard Mobile VPN Connection Monitor, select **Configuration > Profiles**.
2. Select the profile you want to enable the link firewall for and select **Edit**.
3. From the left pane, select **Link Firewall**.





- From the **Stateful Inspection** drop-down list, select **when connected** or **always**.

If you select **when connected**, the link firewall operates only when the VPN tunnel is active for this profile.

If you select **always**, the link firewall is always active, whether the VPN tunnel is active or not.

- Click **OK**.

## About the Desktop Firewall

When you enable a rule in your firewall configurations, you must specify what type of network the rule applies to. In the Mobile VPN client, there are three different types of networks:

### *VPN networks*

Networks defined for the client in the client profile they import.

### *Unknown networks*

Any network not specified in the firewall.

### *Friendly networks*

Any network specified in the firewall as a known network.

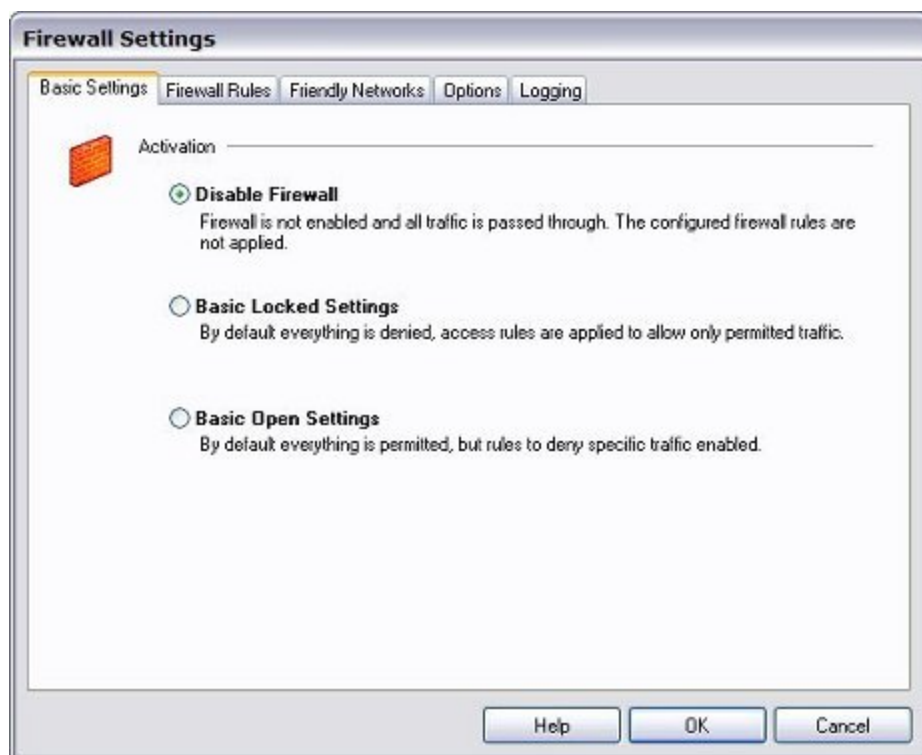
For information about how to enable the desktop firewall, see *Enable the Desktop Firewall* on page 1025.

## Enable the Desktop Firewall

To enable the full-featured desktop firewall:

- From the WatchGuard Mobile VPN Connection Monitor, select **Configuration > Firewall**.  
*The firewall is disabled by default.*
- When you enable the firewall, you must choose between two firewall modes:
  - **Basic Locked Settings** — When you enable this mode, the firewall denies all connections to or from your computer unless you have created a rule to allow the connection.

- **Basic Open Settings** — When you enable this mode, the firewall allows all connections unless you have created a rule to deny the connection.



3. Click **OK**.

After you have enabled the desktop firewall, you can configure your firewall settings.

For more information about how to define friendly networks and create firewall rules, see *Define Friendly Networks* on page 1026 and *Create Firewall Rules* on page 1027.

## Define Friendly Networks

You can generate a firewall rule set for specific known networks that you define. For example, if you want to use the Mobile VPN client on a local network where you want your computer available to other computers, you can add the network address of that LAN as a friendly network. This makes the firewall rules for that LAN different from the firewall rules you create for connections to the Internet and to remote VPN networks.

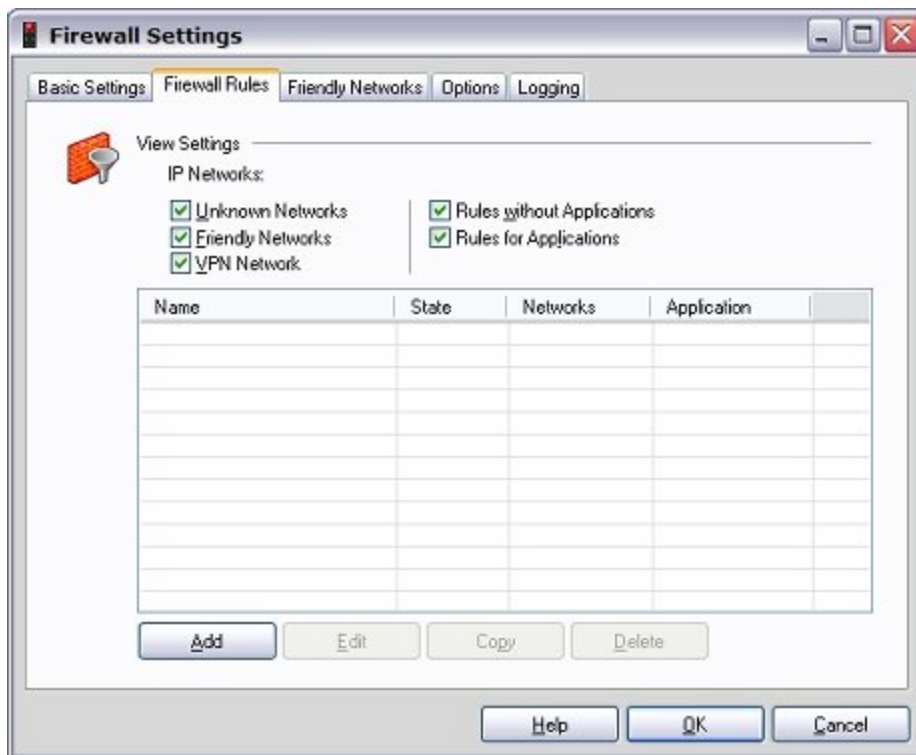
1. From the **Firewall Settings** dialog box, select the **Friendly Networks** tab.
2. Click **Add** to add a new friendly network.

The Automatic Friendly Network detection feature does not operate correctly in this release of the Mobile VPN with IPSec client software.

## Create Firewall Rules

You can create exceptions to the firewall mode you set when you enabled the firewall on the **Firewall Rules** tab of the **Firewall Settings** dialog box. For example, if you selected **Basic Locked Settings** when you enabled the firewall, then the rules you create here allow traffic. If you selected **Basic Open Settings**, then the rules you create here deny traffic. Firewall rules can include multiple port numbers from a single protocol.

Select or clear the check boxes below **View Settings** to show or hide categories of firewall rules. Some options are not available in the Mobile VPN for Windows Mobile version of the desktop firewall.



To create a rule, click **Add**. Use the four tabs in the **Firewall Rule Entry** dialog box to define the traffic you want to control:

- *General Tab*
- *Local Tab*
- *Remote Tab*
- *Applications Tab*

### General Tab

You can define the basic properties of your firewall rules on the **General** tab of the **Firewall Rule Entry** dialog box.

### Rule Name

Type a descriptive name for this rule. For example, you might create a rule called "Web surfing" that includes traffic on TCP ports 80 (HTTP), 8080 (alternate HTTP), and 443 (HTTPS).

### State

To make a rule inactive, select **Disabled**. New rules are enabled by default.

### Direction

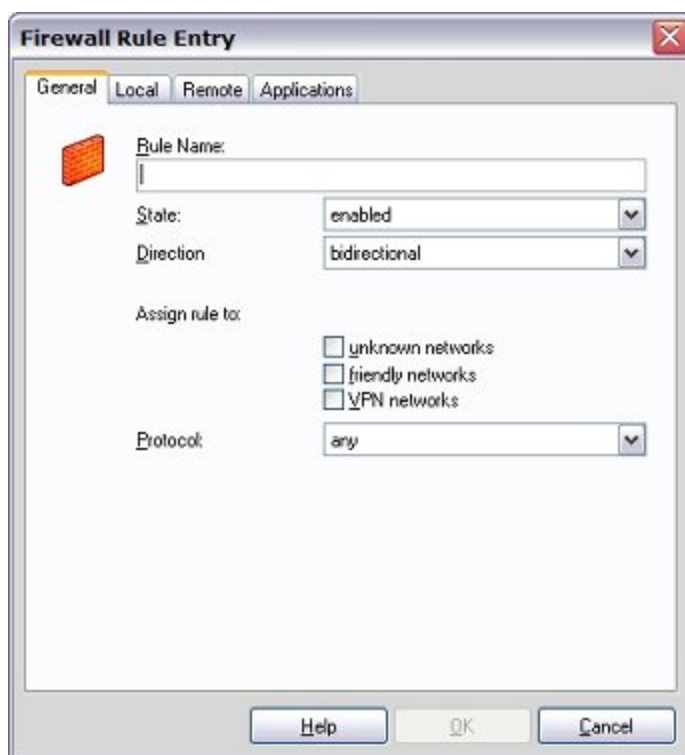
To apply the rule to traffic that comes from your computer, select **outgoing**. To apply the rule to traffic that is sent to your computer, select **incoming**. To apply the rule to all traffic, select **bidirectional**.

### Assign rule to

Select the check boxes adjacent to the network types that this rule applies to.

### Protocol

Use this drop-down list to select the type of network traffic you want to control.

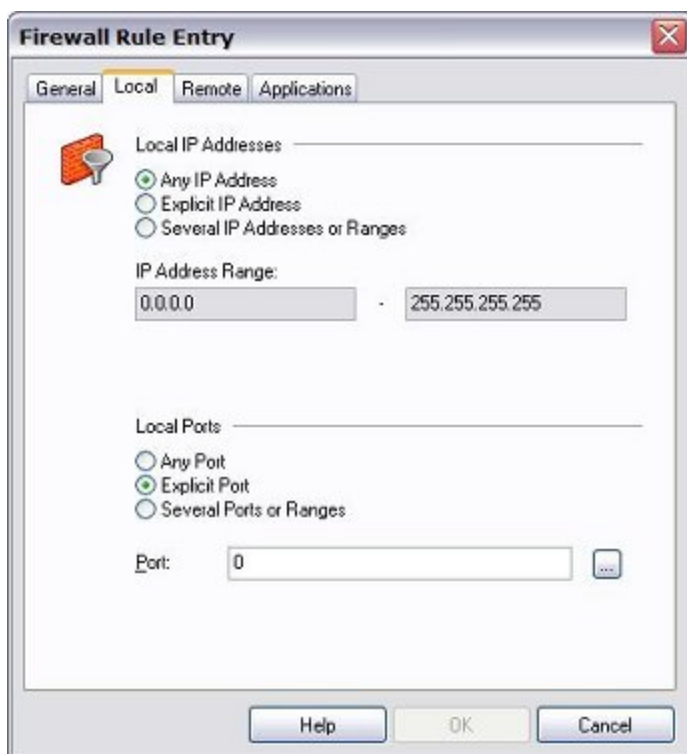


## Local Tab

You can define any local IP addresses and ports that are controlled by your firewall rule on the **Local** tab of the **Firewall Rule Entry** dialog box. We recommend that, in any rule, you configure the **Local IP Addresses** setting to enable the **Any IP address** radio button. If you configure an incoming policy, you can add the ports to control with this policy in the Local Ports settings. If you want to control more than one port in the same

policy, select **Several Ports or Ranges**. Click **New** to add each port.

If you select **Explicit IP Address**, you must specify an IP address. The IP address must not be set to 0.0.0.0.

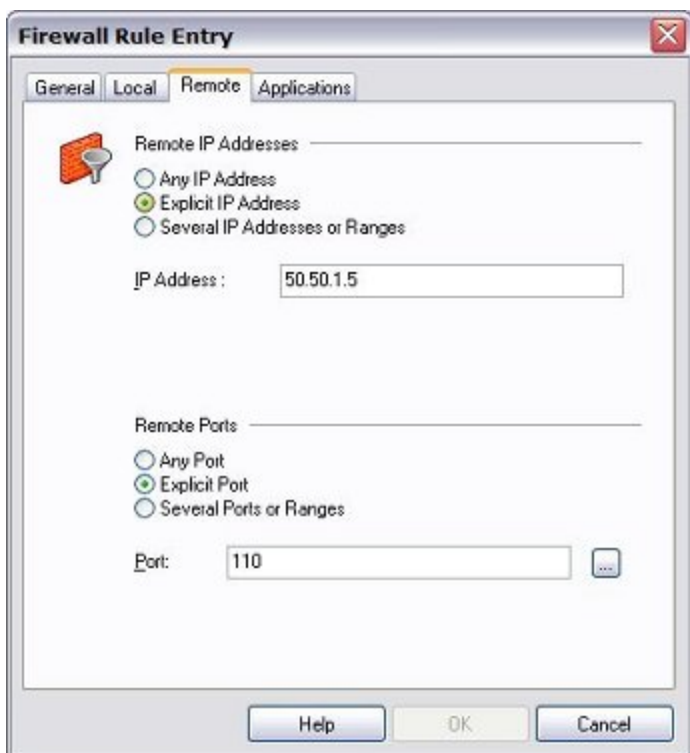


## Remote Tab

You can define any remote IP addresses and ports that are controlled by this rule on the **Remote** tab of the **Firewall Rule Entry** dialog box.

For example, if your firewall is set to deny all traffic and you want to create a rule to allow outgoing POP3 connections, add the IP address of your POP3 server as an **Explicit IP Address** in the **Remote IP Addresses** section. Then, in the **Remote Ports** section, specify port 110 as an **Explicit Port** for this rule.

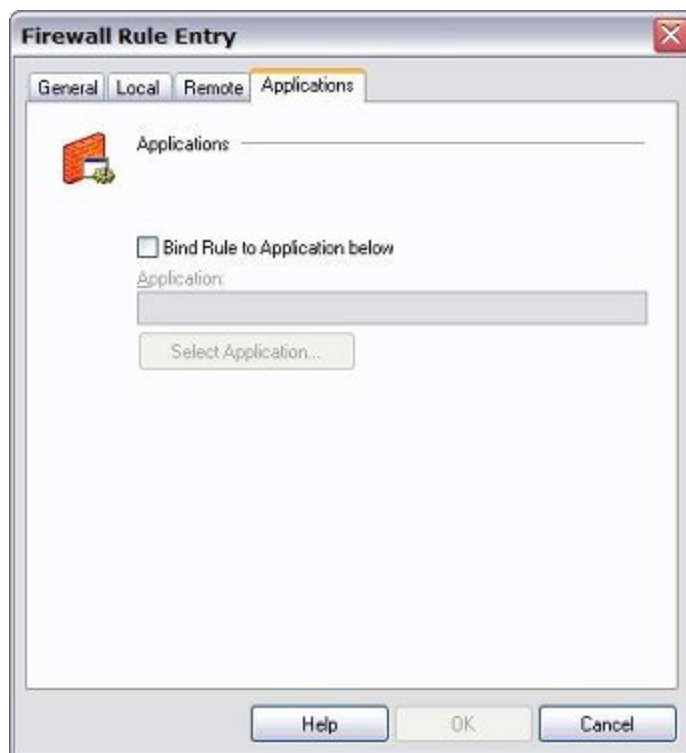
If you select the **Explicit IP Address** radio button, make sure you specify an IP address. The IP address must not be set to 0.0.0.0.



## Applications Tab

You can limit your firewall rule so that it applies only when a specified program is used.

1. On the **Applications** tab of the **Firewall Rule Entry** dialog box, select the **Bind Rule To Application below** check box. This tab is not available in the Mobile VPN for Windows Mobile version of the desktop firewall.



2. Click **Select Application** to browse your local computer for a list of available applications.
3. Click **OK**.

## End-User Instructions for WatchGuard Mobile VPN with IPsec Client Installation

**Note** These instructions are written for Mobile VPN with IPsec client end users. They tell end users to contact their network administrator for instructions on how to install a desktop firewall or configure the firewall that is part of the client software, and for the settings to [control the connection behavior](#) if they do not use a .ini file. You can print these instructions or use them to create a set of instructions for your end users.

The WatchGuard Mobile VPN with IPsec client creates an encrypted connection between your computer and the XTM device with a standard Internet connection. The Mobile VPN client enables you to get access to protected network resources from any remote location with an Internet connection.

Before you install the client, make sure you understand these requirements and recommendations:

- You can install the Mobile VPN with IPsec client software on any computer with Windows XP SP2 (32 bit and 64 bit), Windows Vista (32 bit and 64 bit), or Windows 7 (32 bit and 64 bit) operating system.
- Make sure the computer does not have any other IPsec VPN client software installed.
- Uninstall any desktop firewall software other than Microsoft firewall software from your computer.
- If the client computer uses Windows XP, to install the Mobile VPN client software and to import the .wgx configuration file, you must log on with an account that has administrator rights. Administrator rights are not required to connect after the client has been installed and configured.

- If the client computer uses Windows Vista, to install the Mobile VPN client software, you must log on with an account that has administrator rights. Administrator rights are not required to import a .wgx or .ini file or to connect after the client has been installed.
- We recommend that you check to make sure all available service packs are installed before you install the Mobile VPN client software.
- We recommend that you do not change the configuration of any Mobile VPN client setting not explicitly described in this documentation.

Before you start the installation, make sure you have the following installation components:

- Mobile VPN with IPsec software installation file
- End-user profile, with a .wgx or .ini file extension
- Passphrase (if the end-user profile is a .wgx file or the connection uses certificates for authentication)
- User name and password
- cacert.pem and .p12 certificate file (if the connection uses certificates for authentication)

## Install the Client Software

1. Copy the Mobile VPN .zip file to the remote computer and extract the contents of the file to the root directory on the remote (client or user) computer. Do not run the installation software from a CD or other external drive.
2. Copy the end user profile (the .wgx or .ini file) to the root directory.  
*If you use certificates to authenticate, copy the cacert.pem and .p12 files to the root directory as well.*
3. Double-click the .exe file you extracted in Step 1. This starts the WatchGuard Mobile VPN Installation Wizard. You must restart your computer when the installation wizard completes.
4. Click through the wizard and accept all the default settings.
5. Restart your computer when the installation wizard completes.
6. When the computer restarts, the WatchGuard Mobile VPN Connection Monitor dialog box appears. When the software starts for the first time after you install it, you see this message:  
  
There is no profile for the VPN dial-up!  
Do you want to use the configuration wizard for creating a profile now?
7. Click **No**.
8. Select **View > Autostart > No Autostart** so that the program does not run automatically.

After you install the client software, reinstall the original desktop firewall software or configure the firewall that is part of the client software. If you use a third-party desktop firewall, make sure you configure it to allow traffic to establish the VPN tunnel and the traffic that goes through the tunnel. Contact your network administrator for instructions.

## Import the End User Profile

The end user profile file configures the Mobile VPN client with the settings required to create a VPN tunnel.

To import a Mobile VPN configuration .wgx or .ini file:

1. From your Windows desktop, select **Start > All Programs > WatchGuard Mobile VPN > Mobile VPN Monitor**.
2. From the WatchGuard Mobile VPN Connection Monitor, select **Configuration > Profile Import**.  
*The Profile Import Wizard starts.*



3. On the **Select User Profile** screen, browse to the location of the .wgx or .ini configuration file.
4. Click **Next**.
5. If you use a .wgx file, on the **Decrypt User Profile** screen, type the passphrase. The passphrase is case-sensitive.
6. Click **Next**.
7. On the **Overwrite or add Profile** screen, you can select to overwrite a profile of the same name. This is useful if your network administrator gives you a new .wgx file to import.
8. Click **Next**.
9. On the **Authentication** screen, you can select whether to type the user name and password that you use to authenticate the VPN tunnel.

If you keep these fields empty, you must enter your user name and password each time you connect.

If you type your user name and password, the Firebox stores them and you do not have to enter this information each time you connect. However, this is a security risk. You can also type just your user name and keep the **Password** field empty.

10. Click **Next**.
11. Click **Finish**.

## Select a Certificate and Enter the Passphrase

Complete this section only if you have a cacert.pem and a .p12 file.

1. Select **Configuration > Certificates**.
2. Click **Add**.
3. On the **User Certificate** tab, select **from PKS#12 file** from the **Certificate** drop-down list.
4. Adjacent to the **PKS#12 Filename** text box, click the button and browse to the location of the .p12 file.
5. Click **OK**. Click **Close**.
6. Select **Configuration > Profiles**.
7. Select the profile name. Click **Edit**.
8. Click **Identities**.
9. From the **Certificate configuration** drop-down box, select the certificate configuration you added.
10. Select **Connection > Enter PIN**.
11. Type the passphrase and click **OK**.

## Connect and Disconnect the Mobile VPN Client

Connect to the Internet through a Dial-Up Networking connection or a LAN connection. Then, use the instructions below to select your profile, connect, and disconnect.

To select your profile and connect the Mobile VPN client:


1. From your Windows desktop, select **Start > All Programs > WatchGuard Mobile VPN > Mobile VPN Monitor**.  
*The WatchGuard Mobile VPN dialog box appears.*
2. From the **Profile** drop-down list, select the name of the profile you imported.



3. Click  to connect.

The [Mobile VPN with IPSec client icon](#) appears in the Windows system tray when you are connected.

To disconnect the Mobile VPN client:

1. Restore the Mobile VPN Monitor dialog box.
2. Click  to disconnect.

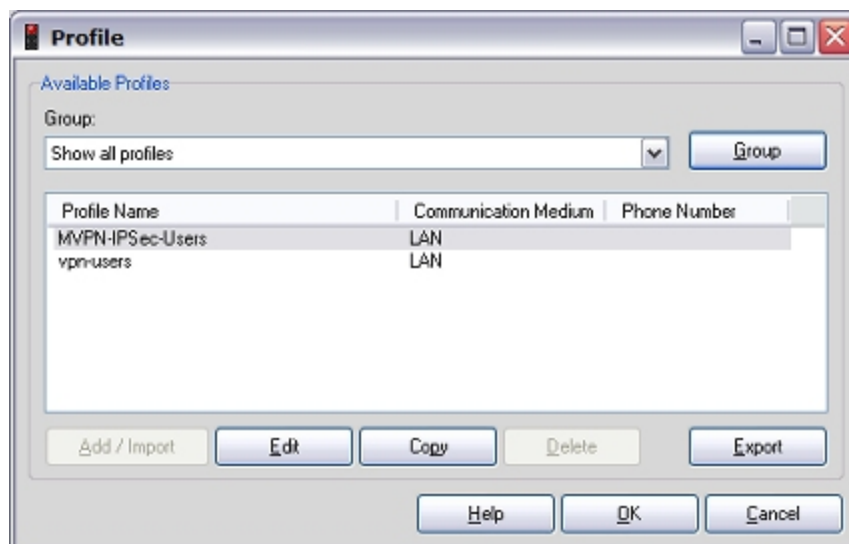
## Control the Connection Behavior

The connection behavior controls the action the Mobile VPN client software takes when the VPN tunnel becomes unavailable for any reason. By default, you must manually reconnect. You are not required to change the connection behavior, but you can select to automatically or variably reconnect. Contact your network administrator for the suggested setting.

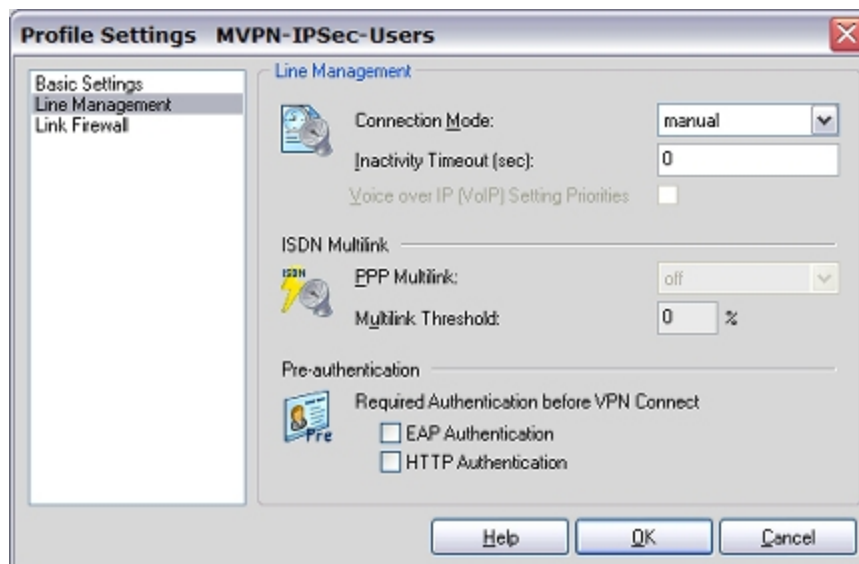
**Note** If you import a .ini file to configure the client software, do not change any of the Line Management settings. The .ini file configures these settings for you.

To set the behavior of the Mobile VPN client when the VPN tunnel becomes unavailable:

1. From the WatchGuard Mobile VPN Connection Monitor, select **Configuration > Profiles**.
2. Select the name of the profile and click **Edit**.



- From the left pane, select **Line Management**.



- Use the **Connection Mode** drop-down list to set a connection behavior for this profile.
  - Manual** — When you select **manual** connection mode, the client does not try to restart the VPN tunnel automatically if the VPN tunnel goes down.  
To restart the VPN tunnel, you must click the **Connect** button in Connection Monitor or right-click the Mobile VPN icon on your Windows desktop toolbar and click **Connect**.
  - Automatic** — When you select **automatic** connection mode, the client tries to start the connection when your computer sends traffic to a destination that you can reach through the VPN. The client also tries to restart the VPN tunnel automatically if the VPN tunnel goes down.
  - Variable** — When you select **variable** connection mode, the client tries to restart the VPN tunnel automatically until you click **Disconnect**. After you disconnect, the client does not try to restart the VPN tunnel again until after the next time you click **Connect**.
- Click **OK**.

## Mobile VPN with IPSec Client Icon

The Mobile VPN with IPSec client icon appears in the Windows system tray to show the VPN connection status. You can right-click the icon to reconnect and disconnect your Mobile VPN, and to see the profile in use.



## Mobile VPN for Windows Mobile Setup

WatchGuard Mobile VPN for Windows Mobile uses the data connection on a device running the Windows Mobile operating system to establish a secure VPN connection to networks protected by an XTM device that supports Mobile VPN with IPSec. Mobile VPN for Windows Mobile has two components:

- **WatchGuard Mobile VPN WM Configurator** runs on a computer that can establish a connection to the Windows Mobile device using Microsoft ActiveSync. The Configurator configures and uploads the client software to the Windows Mobile device.
- The WatchGuard Mobile VPN client software runs on the Windows Mobile device. The **WatchGuard Mobile VPN Service** must be running in order to establish a VPN connection. **WatchGuard Mobile VPN Monitor** allows you to select an uploaded end-user profile and connect the VPN.

Mobile VPN for Windows Mobile uses the same .wgx end-user profile files that are used to configure Mobile VPN with IPSec. To create the end-user profile, see *Configure the XTM Device for Mobile VPN with IPSec* on page 990.

## Mobile VPN WM Configurator and Windows Mobile IPSec Client Requirements

Before you install the client, make sure you understand these requirements and recommendations to work with Mobile VPN with IPSec. If you have not, see the topics that describe how to configure your XTM device to use Mobile VPN.

You must *Configure the XTM Device for Mobile VPN with IPSec*. This process creates the end user profile used to configure the Windows Mobile client software.

The Mobile VPN WM Configurator system requirements are:

Operating System	Microsoft ActiveSync Version
Windows 2000	4.5 or higher
Windows XP (32-bit and 64-bit)	4.5 or higher
Windows Vista	6.1

The Windows Mobile IPSec client device requirements are:

- Windows Mobile 5.0
- Windows Mobile 6.0

Supported devices include:

- Symbol MC70 (Windows Mobile 5 Premium Phone)
- T-Mobile Dash (Windows Mobile 6 Smartphone)
- Samsung Blackjack (Windows Mobile 5 Smartphone)

**Note** The devices in this list have been tested with WatchGuard Mobile VPN for Windows Mobile. A good way to learn if other users have successfully configured other device is to check the WatchGuard user forum, at <http://forum.watchguard.com/>.

To install the Windows Mobile VPN WM Configurator on some operating systems, you must log on to the computer with an account that has administrator rights and import the .wgx configuration file. Administrator rights are not required to upload the client and configuration to the Windows Mobile device.

## Install the Mobile VPN WM Configurator Software

The Mobile VPN WM Configurator software must be installed on a computer that can connect to the Windows Mobile device through ActiveSync. Before you start the installation, make sure you have these installation components:

- The WatchGuard Mobile VPN WM Configurator installation file
- An end user profile, with a file extension of .wgx
- Shared Key
- A .p12 certificate file (if the VPN connects to a Firebox X Core or Peak and use certificates to authenticate)
- User name and password (if the VPN connects to a Firebox X Core or Peak and use Extended Authentication)

**Note** Write the shared key down and keep it in a secure location. You must use it when you import the end-user profile.

To install the Configurator:

1. Copy the Mobile VPN WM Configurator .zip file to the computer and extract the contents of the file.
2. Copy the end user profile (the .wgx file) to the root directory on the remote computer.
3. Double-click the .exe file you extracted in Step 1. This starts the WatchGuard Mobile VPN WM Installation Wizard.
4. Follow the steps in the wizard. In the **InstallShield Wizard Complete** dialog box keep the **Start PDA Installation** check box selected only if the Windows Mobile device is currently connected through ActiveSync.

## Select a Certificate and Enter the PIN

If the VPN uses a certificate to authenticate, you must:

1. Save the .p12 file to the \certs\ directory. The default location is C:\Program Files\WatchGuard\Mobile VPN WM\certs\.
2. Select **Start > All Programs > WatchGuard Mobile VPN > WatchGuard Mobile VPN WM** to start the Configurator.
3. Select **Configuration > Certificates**.
4. On the **User Certificate** tab, select **from PKS#12 file** from the **Certificate** drop-down list.

5. Adjacent to the **PKS#12 Filename** text box, type %installdir%\certs\mycert.p12. Replace mycert.p12 with the name of your .p12 file. Click **OK**.
6. Select **Connection > Enter PIN**.
7. Type the PIN and click **OK**.

*The PIN is the shared key entered to encrypt the file in the Add Mobile VPN with IPSec wizard.*

## Import an End-User Profile

To import a Mobile VPN configuration .wgx file:

1. Select **Start > All Programs > WatchGuard Mobile VPN > WatchGuard Mobile VPN WM** to start the Configurator.
2. Select **Configuration > Profile Import**.  
*The Profile Import Wizard starts.*
3. On the **Select User Profile** screen, browse to the location of the .wgx configuration file supplied by your network administrator. Click **Next**.
4. On the **Decrypt User Profile** screen, type the shared key or passphrase supplied by your network administrator. The shared key is case-sensitive. Click **Next**.
5. On the **Overwrite or add Profile** screen, you can select to overwrite a profile of the same name. This is useful if your network administrator gives you a new .wgx file and you must reimport it. Click **Next**.
6. On the **Authentication** screen, you can type the user name and password that you use to authenticate the VPN tunnel. If you type your user name and password here, the XTM device stores it and you do not have to type this information each time you connect. However, this is a security risk. You can type just your user name and keep the **Password** field empty. This can minimize the amount of data required for the VPN connection.

If you keep the fields empty, you must type your user name and password the first time you connect the VPN. The next time you connect, the user name field is automatically filled with the last user name entered.

7. Click **Next**.

**Note** *If the password you use is your password on an Active Directory or LDAP server and you choose to store it, the password becomes invalid when it changes on the authentication server.*

8. Click **Finish**.

## Install the Windows Mobile Client Software on the Windows Mobile Device

After you import the end user profile to the Configurator, connect the Configurator to the Windows Mobile device. The computer and the Windows Mobile device must have an ActiveSync connection when you start the Configurator.

**Note** *After the WatchGuard Mobile VPN software is installed on your Windows Mobile device you must reboot it.*

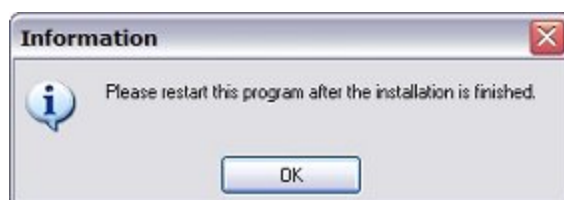
1. Connect your Windows Mobile device to your computer with Microsoft ActiveSync.



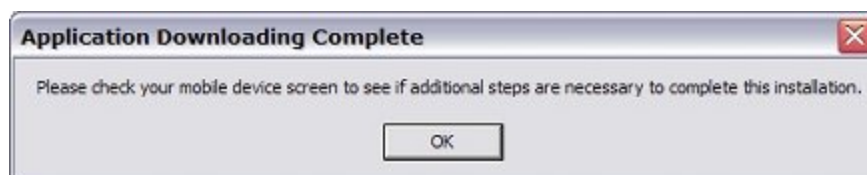
2. To start the Configurator, select **Start > All Programs > WatchGuard Mobile VPN > WatchGuard Mobile VPN WM**.
3. If the WatchGuard Mobile VPN WM software has not been installed on the Windows Mobile device, a **Confirmation** dialog box opens. Click **Yes**.



4. An Information dialog box opens. Click **OK**.



5. The WatchGuard Mobile VPN WM software is installed on the Windows Mobile device. Click **OK**.



6. Reboot the Windows Mobile device.

## Upload the End-User Profile to the Windows Mobile Device

After the Windows Mobile software is installed, you can upload the end-user profile to the Windows Mobile device.

1. Connect your Windows Mobile device to your computer with Microsoft ActiveSync.
2. Select **Start > All Programs > WatchGuard Mobile VPN > WatchGuard Mobile VPN WM** to start the Configurator.
3. From the **Profile** drop-down list, select the profile you want to upload to the Windows Mobile device.



4. Click **Upload**.
5. When the upload is complete, the Configurator status area shows **Upload completed successfully!**





If the VPN uses a certificate to authenticate, you must upload the certificate to the Windows Mobile device. Before you upload the certificate, the Configurator must be set up to use the certificate.

For more information, see [select a certificate and enter the PIN](#).

To upload a certificate:

1. In the Configurator, select **Configuration > Upload PKS#12 File**.
2. Browse to the PKS#12 file and select it. Click **Open**.

## Connect and Disconnect the Mobile VPN for Windows Mobile Client

The WatchGuard Mobile VPN for Windows Mobile client software uses the data connection of a Windows Mobile device to make a secure connection to networks protected by an XTM device. The Windows Mobile device must be able to make a data connection to the Internet.

1. On your Windows Mobile device, select **Start > Programs > WatchGuard Mobile VPN Monitor**. If the WatchGuard Mobile VPN Service is not running, a dialog box opens. Click **Yes** to start the service.



2. The WatchGuard Mobile VPN dialog box opens. Select the end user profile from the drop-down list at the top of the WatchGuard Mobile VPN dialog box.



3. Click **Connect** and type your user name and password. Click **OK**.



**Note** After the first successful VPN connection, the client saves the user name and only asks for a password. To change the user name, click **OK** with the password area clear. A dialog box opens in which you can enter a different user name and password.

4. A yellow line with the word **Connecting** appears between the phone and computer in the WatchGuard Mobile VPN dialog box. The line turns green when the VPN tunnel is ready.



To disconnect the Mobile VPN client:

1. On your Windows Mobile device, select **Start > Programs > WatchGuard Mobile VPN Monitor**.
2. Click **Disconnect**. The green line changes to yellow.



When there is no line between the phone and computer, the VPN is disconnected.



## Secure Your Windows Mobile Device with the Mobile VPN Firewall

The WatchGuard Mobile VPN for Windows Mobile client includes two firewall components:

### Link firewall

The link firewall is not enabled by default. When the link firewall is enabled, your Windows Mobile device drops any packets received from other computers. You can choose to enable the link firewall only when a Mobile VPN tunnel is active, or enable it all the time.

### Desktop firewall

This full-featured firewall can control connections to and from your Windows Mobile device. You can define friendly networks and set access rules separately for friendly and unknown networks.

For more information, see *Enable the Link Firewall* on page 1024 and *Enable the Desktop Firewall* on page 1025.

## Stop the WatchGuard Mobile VPN Service

The WatchGuard Mobile VPN Service must be running on the Windows Mobile device to use the WatchGuard Mobile VPN Monitor to create VPN tunnels. When you close the Monitor, the service does not stop. You must stop the service manually.

1. On your Windows Mobile device, select **Start > Programs > WatchGuard Mobile VPN Service**.  
*The WatchGuard Mobile VPN dialog box appears.*



2. To stop the service, click **Yes**.



## Uninstall the Configurator, Service, and Monitor

To uninstall WatchGuard Mobile VPN for Windows Mobile, you must uninstall software from your Windows computer and your Windows Mobile device.

## Uninstall the Configurator from Your Windows Computer

1. On your Windows computer, select **Start > Control Panel**.
2. Double-click **Add or Remove Programs**.
3. Click **WatchGuard Mobile VPN WM** and click **Change/Remove**.
4. Click **Yes** to uninstall the application.
5. Click **OK** when the uninstall is complete.

## Uninstall the WatchGuard Mobile VPN Service and Monitor from Your Windows Mobile Device

1. On your Windows Mobile device, select **Start > Settings**.
2. In Settings, click the **System** tab and double-click **Remove Programs**.
3. Select **WatchGuard Mobile VPN** and click **Remove**.
4. The **Remove Program** dialog box opens. Click **Yes** to remove the software.  
*A dialog box appears and asks if you want to reboot the device now.*
5. To reboot the device now, click **Yes**.  
To reboot the device later, click **No**.  
The uninstall program does not complete until you reboot the device.



# 30 Mobile VPN with SSL

---

## About Mobile VPN with SSL

The WatchGuard Mobile VPN with SSL client is a software application that is installed on a remote computer. The client makes a secure connection from the remote computer to your protected network through an unsecured network, such as the Internet. The Mobile VPN client uses SSL (Secure Sockets Layer) to secure the connection.

## Configure the XTM Device for Mobile VPN with SSL

From Policy Manager, when you enable Mobile VPN with SSL, an "SSLVPN-Users" user group and a "WatchGuard SSLVPN" policy are created to allow SSL VPN connections from the Internet to your external interface.

## Configure Authentication and Connection Settings

1. Select **VPN > Mobile VPN > SSL**.

The *Mobile VPN with SSL Configuration* dialog box appears.

**Mobile VPN with SSL Configuration**

When you activate Mobile VPN with SSL, an "SSLVPN-Users" user group and a "WatchGuard SSLVPN" policy are created to allow SSL VPN connections from the Internet to your external interface.

Activate Mobile VPN with SSL

General | Advanced

Authentication Server

Firebox-DB

Force users to authenticate after a connection is lost

Firebox IP Addresses

Type or select a Firebox IP address or domain name for SSL VPN users to connect to.

Primary: 50.50.50.50 Backup:

Networking and IP Address Pool

Choose the method the Firebox uses to send traffic through the VPN tunnel. Select **Bridge VPN traffic** if you want to bridge the user to a network you specify. Select **Route VPN traffic** if you want the Firebox to route VPN traffic to specified networks and resources.

Routed VPN traffic

Force all client traffic through tunnel

Allow access to networks connected through Trusted, Optional, and VLANs

Specify allowed resources

Virtual IP Address Pool

Enter a subnet that is not used by computers locally connected to the Firebox. Your Firebox allows 300 Mobile VPN with SSL user(s).

192.168.113. 0 /24

OK Cancel Help

2. Select the **Activate Mobile VPN with SSL** check box.
3. Select an **Authentication Server** from the drop-down list. You can authenticate users with the internal XTM device database (Firebox-DB) or with a RADIUS, VACMAN Middleware, SecurID, LDAP, or Active Directory server.  
Make sure that the method of authentication is enabled (select **Setup > Authentication > Authentication Servers**). For more information, see [Configure user authentication for Mobile VPN with SSL](#).



4. If you select RADIUS or SecurID as your authentication server, you can select the **Force users to authenticate after a connection is lost** check box to require users to authenticate after a Mobile VPN with SSL connection is disconnected. We recommend you select this check box if you use two-factor authentication that uses a one-time password, such as SecurID or Vasco.  
If you do not force users to authenticate after a connection is lost, the automatic connection attempt can fail. The Mobile VPN with SSL client automatically tries to reconnect after a connection is lost with the one-time password the user originally entered, which is no longer correct.
5. From the **Primary** drop-down list, select or type a public IP address or domain name. Mobile VPN with SSL clients connect to this IP address or domain name by default.
6. If your XTM device has more than one WAN connection, select a different public IP address from the **Backup** drop-down list. A Mobile VPN with SSL client connects to the backup IP address when it is unable to establish a connection with the primary IP address.

## Configure the Networking and IP Address Pool Settings

In the **Networking and IP address pool** section, you configure the network resources Mobile VPN with SSL clients can use.

1. From the drop-down list in the **Networking and IP Address Pool** section, select the method the XTM device uses to send traffic through the VPN tunnel.
  - Select **Bridge VPN Traffic** to bridge SSL VPN traffic to a network you specify. When you select this option, you cannot filter traffic between the SSL VPN users and the network that the SSL VPN traffic is bridged to.
  - Select **Routed VPN Traffic** to route VPN traffic to specified networks and resources. This is the default for all WatchGuard XTM devices.
2. Select or clear the **Force all client traffic through the tunnel** check box.
  - Select **Force all client traffic through tunnel** to send all private network and Internet traffic through the tunnel. This option sends all external traffic through the XTM device policies you create and offers consistent security for mobile users. However, because it requires more processing power on the XTM device, access to Internet resources can be very slow for the mobile user. To allow clients to access the Internet when this option is selected, see *Options for Internet Access Through a Mobile VPN with SSL Tunnel* on page 1054.
  - Clear the **Force all client traffic through tunnel** check box to send only private network information through the tunnel. This option gives your users better network speeds by routing only necessary traffic through the XTM device, but access to Internet resources is not restricted by the policies on your XTM device. To restrict Mobile VPN with SSL client access to only specified devices on your private network, select the **Specify allowed resources** radio button. Type the IP address of the network resource in slash notation and click **Add**.
3. Configure the IP addresses the XTM device assigns to Mobile VPN with SSL client connections. The virtual IP addresses in this address pool cannot be part of a network protected by the XTM device, any network accessed through a route or BOVPN, assigned by DHCP to a device behind the XTM device, or used for Mobile VPN with IPSec or Mobile VPN with SSL address pools.

*Routed VPN traffic*

For the Virtual IP Address Pool, keep the default setting of 192.168.113.0/24, or enter a different range. Type the IP address of the subnet in slash notation. IP addresses from this subnet are automatically assigned to Mobile VPN with SSL client connections. You cannot assign an IP address to a user.

The virtual IP addresses in this address pool cannot be part of a network protected by the XTM device, any network accessed through a route or BOVPN, assigned by DHCP to a device behind the XTM device, or used for Mobile VPN with IPSec or Mobile VPN with PPTP address pools.

*Bridge VPN traffic*

From the **Bridge to interface** drop-down list, select the name of the interface to bridge to. In the **Start** and **End** fields, type the first and last IP addresses in the range that is assigned to the Mobile VPN with SSL client connections. The **Start** and **End** IP addresses must be on the same subnet as the bridged interface.

**Note** *The **Bridge to interface** option does not bridge SSL VPN traffic to any secondary networks on the selected interface.*

4. Click **OK**.

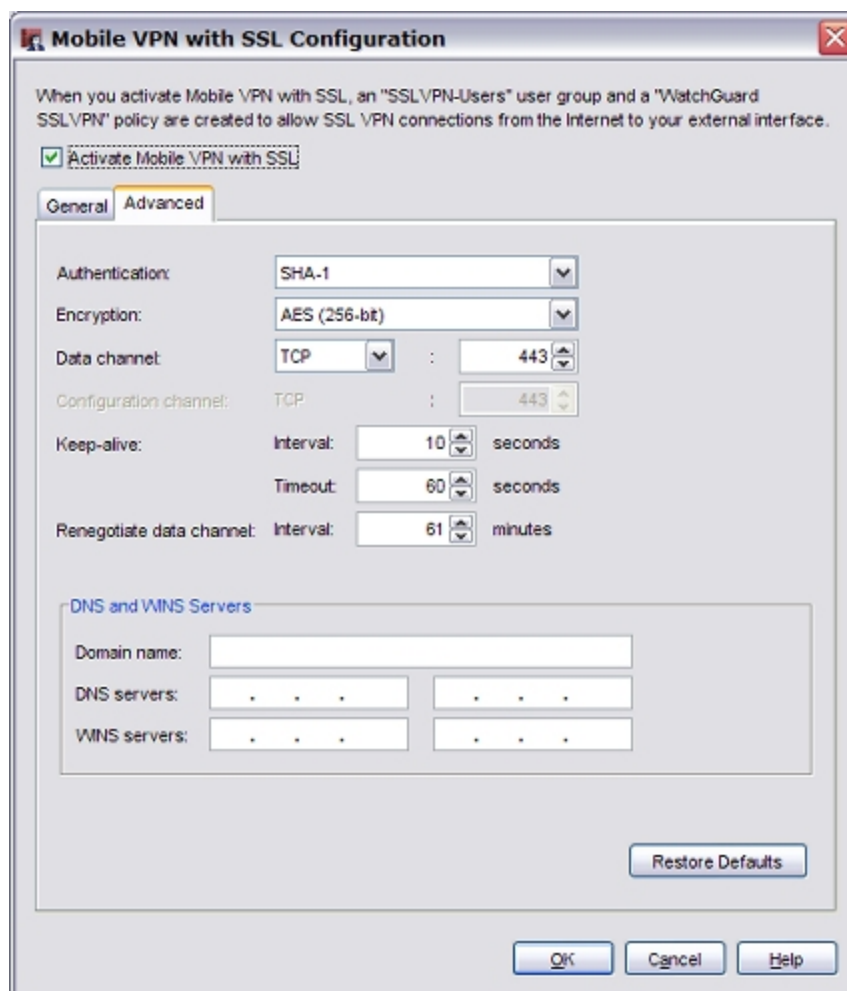
After you save the changes to your XTM device, you must [configure user authentication for Mobile VPN with SSL](#) before users can download and install the software. Any changes you make are distributed to clients automatically the next time they connect using Mobile VPN with SSL.

For more information on using slash notation, see *About Slash Notation* on page 3.

## Configure Advanced Settings for Mobile VPN with SSL

1. Select **VPN > Mobile VPN > SSL**.

The Mobile VPN with SSL Configuration dialog box appears.



2. Click the **Advanced** tab.

The options you can configure on this tab include:

### Authentication

Authentication method used to establish the connection. The options are **MD5**, **SHA**, **SHA-1**, **SHA-256**, and **SHA-512**.

### Encryption

Algorithm that is used to encrypt the traffic. The options are **Blowfish**, **DES**, **3DES**, **AES (128 bit)**, **AES (192 bit)**, or **AES (256 bit)**. The algorithms are shown in order from weakest to strongest, with the exception of Blowfish, which uses a 128-bit key for strong encryption.

For best performance with a high level of encryption, we recommend that you choose MD5 authentication with Blowfish encryption.

### *Data channel*

The protocol and port Mobile VPN with SSL uses to send data after a VPN connection is established. You can use the **TCP** or **UDP** protocol. Then, select a port. The default protocol and port for Mobile VPN with SSL is TCP port 443. This is also the standard protocol and port for HTTPS traffic. Mobile VPN with SSL can share port 443 with HTTPS.

If you change the data channel to use a port other than 443, users must manually type this port in the Mobile VPN with SSL connection dialog box. For example, if you change the data channel to 444, and the XTM device IP address is 50.50.50.50, the user must type 50 . 50 . 50 . 50 : 444 instead of 50 . 50 . 50 . 50 .

If the port is set to the default 443, the user must type only the XTM device's IP address. It is not necessary to type :443 after the IP address.

For more information, see Choose the Port and Protocol for Mobile VPN with SSL.

### *Configuration channel*

The protocol and port Mobile VPN with SSL uses to negotiate the data channel and to download configuration files. If you set the data channel protocol to TCP, the configuration channel automatically uses the same port and protocol. If you set the data channel protocol to UDP, you can set the configuration channel protocol to **TCP** or **UDP**, and you can use a different port than the data channel.

### *Keep-alive*

Defines how often the XTM device sends traffic through the tunnel to keep the tunnel active when no other traffic is being sent through the tunnel.

### *Timeout*

Defines how long the XTM device waits for a response. If there is no response before the timeout value, the tunnel is closed and the client must reconnect.

### *Renegotiate Data Channel*

If a Mobile VPN with SSL connection has been active for the amount of time specified in the **Renegotiate Data Channel** text box, the Mobile VPN with SSL client must create a new tunnel. The minimum value is 60 minutes.

### *DNS and WINS Servers*

You can use DNS or WINS to resolve the IP addresses of resources that are protected by the XTM device. If you want the Mobile VPN with SSL clients to use a DNS or WINS server behind the XTM device instead of the servers assigned by the remote network they are connected to, type the domain name and IP addresses of the DNS and WINS servers on your network. For more information on DNS and WINS, see *Name Resolution for Mobile VPN with SSL* on page 1055.

### *Restore Defaults*

Click to reset the **Advanced** tab settings to their default values. All DNS and WINS server information on the **Advanced** tab is deleted.

## Configure User Authentication for Mobile VPN with SSL

To allow users to authenticate to the XTM device and connect with Mobile VPN with SSL, you must configure user authentication on the XTM device. You can configure your XTM device as an authentication server or use a third-party authentication server. When you enable Mobile VPN with SSL, an SSLVPN-Users group is created automatically.

Users must be a member of the SSLVPN-Users group to make a Mobile VPN with SSL connection. Users cannot connect if they are a member of a group that is part of the SSLVPN-Users group. The user must be a direct member of the SSLVPN-Users group.

For more information, see *Configure Your XTM Device as an Authentication Server* on page 329 and *About Third-Party Authentication Servers* on page 328.


## Configure Policies to Control Mobile VPN with SSL Client Access

When you enable Mobile VPN with SSL, an *Allow SSLVPN-Users* policy is added. It has no restrictions on the traffic that it allows from SSL clients to network resources protected by the XTM device. To restrict Mobile VPN with SSL client access, disable the Allow SSLVPN-Users policy. Then, add new policies to your configuration or add the group with Mobile VPN with SSL access to the **From** section of existing policies.

**Note** *If you assign addresses from a trusted network to Mobile VPN with SSL users, the traffic from the Mobile VPN with SSL user is not considered trusted. All Mobile VPN with SSL traffic is untrusted by default. Regardless of assigned IP address, policies must be created to allow Mobile VPN with SSL users access to network resources.*

## Allow Mobile VPN with SSL Users to Access a Trusted Network

In this example, you use Policy Manager to add an Any policy which gives all members of the SSLVPN-Users group full access to resources on all trusted networks.

1. Click .  
Or, select **Edit > Add Policies**.  
*The Add Policies dialog box appears.*
2. Expand the **Packet Filters** folder.  
*A list of templates for packet filters appears.*
3. Select **Any** and click **Add**.  
*The New Policy Properties dialog box opens.*
4. Type a name for the policy in the **Name** text box. Choose a name that will help you identify this policy in your configuration.
5. On the **Policy** tab, in the **From** section, select **Any-Trusted** and click **Remove**.
6. In the **From** section, click **Add**.  
*The Add Address dialog box appears.*
7. Click **Add User**. From the two **Type** drop-down lists, select **SSL VPN** for the first and **Group** for the second.
8. Select **SSLVPN-Users** and click **Select**.  
*After SSLVPN-Users is the name of the authentication method in parenthesis.*

9. Click **OK** to close the **Add Address** dialog box.
10. In the **To** section, select **Any-External** and click **Remove**.
11. In the **To** section, click **Add**.  
*The Add Address dialog box appears.*
12. In the **Available Members** list, select **Any-Trusted** and click **Add**.
13. Click **OK** twice. Click **Close**.
14. Save the changes to the XTM device.

For more information on policies, see *Add Policies to Your Configuration* on page 372.

## Use Other Groups or Users in a Mobile VPN with SSL Policy

Users must be a member of the SSLVPN-Users group to make a Mobile VPN with SSL connection. You can use policies with other groups to restrict access to resources after the user connects. You can use Policy Manager to select a user or group other than SSLVPN-Users.

1. Double-click the policy to which you want to add the user or group.
2. On the **Policy** tab, in the **From** section, click **Add**.  
*The Add Address dialog box opens.*
3. Click **Add User**.  
*The Add Authorized Users or Groups dialog box opens.*
4. For the two **Type** drop-down lists, select **Firewall** for the first and either **User** or **Group** for the second.
5. Select the user or group you want to add, then click **Select**.
6. Click **OK** twice.

For more information on how to use users and groups in policies, see *Use Authorized Users and Groups in Policies* on page 360.

## Options for Internet Access Through a Mobile VPN with SSL Tunnel

### Force All Client Traffic Through Tunnel

This is the most secure option. It requires that all remote user Internet traffic is routed through the VPN tunnel to the XTM device. From the XTM device, the traffic is then sent back out to the Internet. With this configuration (also known as default-route VPN), the XTM device is able to examine all traffic and provide increased security. However, this requires more processing power and bandwidth from the XTM device. This can affect network performance if you have a large number of VPN users. By default, a policy named *Allow SSLVPN-Users* allows access to all internal resources and the Internet.

### Allow Direct Access to the Internet

If you select **Routed VPN traffic** in the Mobile VPN with SSL configuration, and you do not force all client traffic through the tunnel, you must configure the allowed resources for the SSL VPN users. If you select **Specify allowed resources** or **Allow access to networks connected through Trusted, Optional and VLANs**,

only traffic to those resources is sent through the VPN tunnel. All other traffic goes directly to the Internet and the network that the remote SSL VPN user is connected to. This option can affect your security because any traffic sent to the Internet or the remote client network is not encrypted or subject to the policies you configured on the XTM device.

## Use the HTTP Proxy to Control Internet Access for Mobile VPN with SSL Users

If you configure Mobile VPN with SSL to force all client traffic through the tunnel, you can use HTTP proxy policies to restrict Internet access. The default *Allow SSLVPN-Users* policy has no restrictions on the traffic that it allows from SSL clients to the Internet. To restrict Internet access, you can use an HTTP proxy policy you have already configured, or add a new HTTP proxy policy for SSL clients.

1. Double-click the policy to open the **Edit Policy Properties** dialog box.
2. On the **Policy** tab, click **Add** in the **From** area.
3. Click **Add User**.
4. For **Type**, select **SSL VPN** and **Group**.
5. Select **SSLVPN-Users** and click **Select**.
6. Click **OK** to return to the **Edit Policy Properties** dialog box.
7. Click **OK**. *Save the Configuration File*.

The HTTP proxy policy takes precedence over the Any policy. You can leave the Any policy to handle traffic other than HTTP, or you can use these same steps with another policy to manage traffic from the SSL clients.

For more information on how to configure an HTTP proxy policy, see *About the HTTP-Proxy* on page 440.

## Name Resolution for Mobile VPN with SSL

The goal of a mobile VPN connection is to allow a user to connect to network resources as if they were connected locally. With a local network connection, NetBIOS traffic on the network allows you to connect to devices using the device name. It is not necessary to know the IP address of each network device. However, Mobile VPN tunnels cannot pass broadcast traffic, and NetBIOS relies on broadcast traffic to operate correctly. An alternative method for name resolution must be used.

## Methods of Name Resolution Through a Mobile VPN with SSL Connection

You must choose one of these two methods for name resolution:

### *WINS/DNS (Windows Internet Name Service/Domain Name System)*

A WINS server holds a database of NetBIOS name resolution for the local network. DNS works in a similar way. If your domain uses only Active Directory, you must use DNS for name resolution.

### *LMHOSTS file*

An LMHOSTS file is a manually created file that you install on all computers with Mobile VPN with SSL installed. The file contains a list of resource names and their associated IP addresses.

## Select the Best Method for Your Network

Because of the limited administration requirements and current information it provides, WINS/DNS is the preferred solution for name resolution through a Mobile VPN tunnel. The WINS server constantly listens to the local network and updates its information. If a resource changes its IP address or a new resource is added, nothing on the SSL client must be changed. When the client tries to get access to a resource by name, a request is sent to the WINS/DNS servers and the most current information is given.

If you do not already have a WINS server, the LMHOSTS file is a fast way to provide name resolution to Mobile VPN with SSL clients. Unfortunately, it is a static file and you must edit it manually any time there is a change. Also, the resource name/IP address pairs in the LMHOSTS file are applied to all network connections, not only the Mobile VPN with SSL connection.



## Configure WINS or DNS for Name Resolution

Each network is unique in the resources available and the skills of the administrators. The best resource to learn how to configure a WINS server is the documentation for your server, such as the Microsoft web site. When you configure your WINS or DNS server, note that:

- The WINS server must be configured to be a client of itself.
- Your XTM device must be the default gateway of the WINS and DNS servers.
- You must make sure that network resources do not have more than one IP address assigned to a single network interface. NetBIOS only recognizes the first IP address assigned to a NIC. For more information, refer to <http://support.microsoft.com/kb/q131641/>.

## Add WINS and DNS Servers to a Mobile VPN with SSL Configuration

1. Select **VPN > Mobile VPN > SSL**.
2. Select the **Advanced** tab.
3. Type the primary and secondary addresses for the WINS and DNS servers. You can also type a domain suffix in the **Domain Name** text box for a client to use with unqualified domain names.
4. Click **OK**.
5. *Save the Configuration File.*
6. The next time an SSL client computer authenticates to the XTM device, the new settings are applied to the connection.

## Configure an LMHOSTS File to Provide Name Resolution

When you use an LMHOSTS file to get name resolution for your Mobile VPN clients, no changes to the XTM device or the Mobile VPN client software are necessary. Basic instructions to help you create an LMHOSTS file are shown below. For more information on LMHOSTS files, refer to <http://support.microsoft.com/kb/q150800/>.

### Edit an LMHOSTS File

1. Look for an LMHOSTS file on the Mobile VPN client computer. The LMHOSTS file (sometimes named `lmhosts.sam`) is usually located in:  
`C:\WINDOWS\system32\drivers\etc`
2. If you find an LMHOSTS file in that location, open it with a text editor like Notepad. If you cannot find an LMHOSTS file, create a new file in a text editor.
3. To create an entry in the LMHOSTS file, type the IP address of a network resource, five spaces, and then the name of the resource. The resource name must be 15 characters or less. It should look like this:  
`192.168.42.252        server_name`
4. If you started with an older LMHOSTS file, save the file with its original name. If you created a new file in Notepad, save it with the name `lmhost` in the `C:\WINDOWS\system32\drivers\etc` directory. You must also choose the type "All Files" in the **Save** dialog box, or Notepad appends ".txt" to the file name.
5. Reboot the SSL client computer for the LMHOSTS file to become active.

## Install and Connect the Mobile VPN with SSL Client

The Mobile VPN with SSL software allows users to connect, disconnect, gather more information about the connection, and to exit or quit the client. The Mobile VPN with SSL client adds an icon to the system tray on the Windows operating system, or an icon in the menu bar on Mac OS X. You can use this icon to [control the client software](#).

To use Mobile VPN with SSL, you must:

1. [Verify system requirements](#)
2. [Download the client software](#)
3. [Install the client software](#)
4. [Connect to your private network](#)

**Note** *If a user is unable to connect to the XTM device, or cannot download the installer from the XTM device, you can Manually Distribute and Install the Mobile VPN with SSL Client Software and Configuration File.*

## Client Computer Requirements

You can install the Mobile VPN with SSL client software on computers with these operating systems:

- Microsoft Windows 7
- Microsoft Windows Vista
- Microsoft Windows XP
- Mac OS X 10.5 (Leopard)

If the client computer has Windows Vista or Windows XP, you must log on with an account that has administrator rights to install the Mobile VPN with SSL client software. Administrator rights are not required to connect after the SSL client has been installed and configured. In Windows XP Professional, the user must be a member of the *Network Configuration Operators* group to run the SSL client.

If the client computer has Mac OS X, administrator rights are not required to install or use the SSL client.

## Download the Client Software

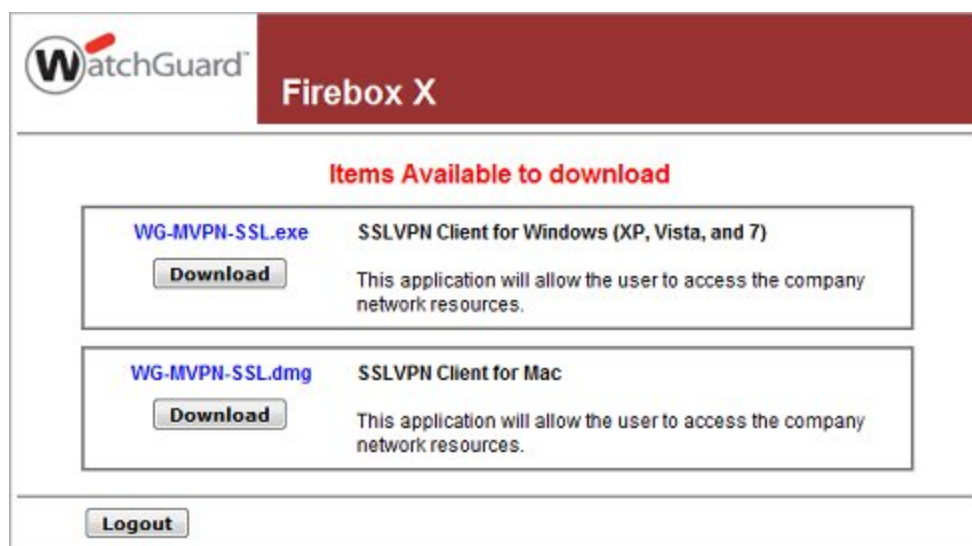
1. Connect to this address with a web browser:

`https://<IP address of an XTM device interface>/sslvpn.html`

or

`https://<Host name of the XTM device>/sslvpn.html`

2. Enter your user name and password to authenticate to the XTM device.  
*The SSL VPN client download page appears.*



3. Click the **Download** button for the installer you want to use. There are two available versions: Windows (WG-MVPN-SSL.exe) and Mac OS X (WG-MVPN-SSL.dmg).
4. Save the file to your desktop or another folder of your choice.

## Install the Client Software

For Microsoft Windows:

1. Double-click **WG-MVPN-SSL.exe**.  
*The Mobile VPN with SSL client Setup Wizard starts.*
2. Accept the default settings on each screen of the wizard.
3. If you want to add a desktop icon or a Quick Launch icon, select the check box in the wizard that matches the option. A desktop or Quick Launch icon is not required.
4. Finish and exit the wizard.

For Mac OS X:

1. Double-click **WG-MVPN-SSL.dmg**.  
*A volume named WatchGuard Mobile VPN is created on your desktop.*
2. In the WatchGuard Mobile VPN volume, double-click **WatchGuard Mobile VPN with SSL Installer V15.mpkg**.  
*The client installer starts.*
3. Accept the default settings on each screen of the installer.
4. Finish and exit the installer.

After you download and install the client software, the Mobile VPN client software automatically connects to the XTM device. Each time you connect to the XTM device, the client software checks for configuration updates.

## Connect to Your Private Network

For Microsoft Windows:

1. Use one of these three methods to start the client software:
  - From the **Start Menu**, select **All Programs > WatchGuard > Mobile VPN with SSL client > Mobile VPN with SSL client**.
  - Double-click the Mobile VPN with SSL icon on your desktop.
  - Click the Mobile VPN with SSL icon in the Quick Launch toolbar.
2. Type the information for the XTM device you want to connect to, and the username and password for the user.

The Server is the IP address of the primary external interface of the XTM device. If you configured Mobile VPN with SSL to use a port other than the default port 443, in the Server field, type the primary external interface followed by a colon and the port number. For example, if Mobile VPN with SSL is configured to use port 444, and the primary external IP address is 50.50.50.1. the Server is 50.50.50.1:444.

3. Click **Connect**.

For Mac OS X:

1. Open a Finder window. Go to **Applications > WatchGuard** and double-click the **WatchGuard Mobile VPN with SSL** application.

*The WatchGuard Mobile VPN with SSL icon appears in the menu bar.*

2. Click the icon in the menu bar and select **Connect**.
3. Type the information for the XTM device you want to connect to, and the username and password for the user.




The Server is the IP address of the primary external interface of the XTM device. If you configured Mobile VPN with SSL to use a port other than the default port 443, in the Server field, type the primary external interface followed by a colon and the port number. For example, if Mobile VPN with SSL is configured to use port 444, and the primary external IP address is 50.50.50.1. the Server is 50.50.50.1:444.

4. Click **Connect**.

The SSL client user must enter their login credentials. Mobile VPN with SSL does not support any Single Sign-On (SSO) services. If the connection between the SSL client and the XTM device is temporarily lost, the SSL client tries to establish the connection again.

## Mobile VPN with SSL Client Controls

When the Mobile VPN with SSL client runs, the WatchGuard Mobile VPN with SSL icon appears in the system tray (Windows) or on the right side of the menu bar (Mac OS X). The VPN connection status is shown by the icon's magnifying glass.

-  The VPN connection is not established.
-  The VPN connection has been established. You can securely connect to resources behind the XTM device.
-  The client is in the process of connecting or disconnecting.

To see the client controls list, right-click the Mobile VPN with SSL icon in the system tray (Windows), or click the Mobile VPN with SSL icon in the menu bar (Mac OS X). You can select the following actions:

#### *Connect/Disconnect*

Start or stop the SSL VPN connection.

#### *View Logs*

Open the connection log file.

#### *Properties*

Windows — Select **Launch program on startup** to start the client when Windows starts. Type a number for **Log level** to change the level of detail included in the logs.

Mac OS X — Shows detailed information about the SSL VPN connection. You can also set the log level.

#### *About*

The WatchGuard Mobile VPN dialog box opens with information about the client software.

#### *Exit (Windows) or Quit (Mac OS X)*

Disconnect from the XTM device and shut down the client.

## Manually Distribute and Install the Mobile VPN with SSL Client Software and Configuration File

If there is some reason your users cannot download the client software from the XTM device, you can manually provide them with the client software and configuration file. You can download the Mobile VPN with SSL client software from the [Software Downloads section](#) of the WatchGuard LiveSecurity web site. Use the steps below to get the SSL VPN configuration file to distribute.

### Get the Configuration File from the XTM device

You must configure the XTM device to use Mobile VPN with SSL before you use this procedure.

1. *Start Firebox System Manager.*
2. Select the **Status Report** tab and click **Support**.
3. Choose a location to save the support .tgz file and click **Retrieve**.
4. Extract the contents of support .tgz to a folder on your computer.

The Mobile VPN with SSL configuration file is located in:

```
Fireware_XTM_Support\support\debug\client.wgssl.
```

### Install and Configure the SSL Client Using the Installation Software and a Configuration File

You must have two files:

- Mobile VPN with SSL VPN client installation software  
WG-MVPN-SSL.exe (Microsoft Windows) or WG-MVPN-SSL.dmg (Mac OS X)

- Mobile VPN with SSL VPN configuration file  
sslvpn\_client.wgssl

For Microsoft Windows:

1. Double-click **WG-MVPN-SSL.exe**.  
*The Mobile VPN with SSL client Setup Wizard starts.*
2. Accept the default settings on each screen of the wizard.
3. If you want to add a desktop icon or a Quick Launch icon, select the check box for that option.  
*A desktop or Quick Launch icon is not required. The client icon is added to the Windows Start menu by default.*
4. Finish and exit the wizard.
5. Use one of these three methods to start the client software:
  - From the **Start Menu**, select **All Programs > WatchGuard > Mobile VPN with SSL client > Mobile VPN with SSL client**.  
*The client installer starts.*
  - Double-click the Mobile VPN with SSL client icon on the desktop.
  - Click the Mobile VPN with SSL client icon in the Quick Launch toolbar.
6. Double-click **sslvpn-client.wgssl** to configure the Mobile VPN with SSL client software.

For Mac OS X:

1. Double-click **WG-MVPN-SSL.dmg**.  
*A volume named WatchGuard Mobile VPN is created on the desktop.*
2. In the WatchGuard Mobile VPN volume, double-click **WatchGuard Mobile VPN with SSL Installer V15.mpkg**.  
*The client installer starts.*
3. Accept the default settings in the installer.
4. Finish and exit the installer.
5. Start the client software. Open a Finder window and go to **Applications > WatchGuard**.
6. Double-click the **WatchGuard Mobile VPN with SSL** application.  
*The WatchGuard Mobile VPN with SSL logo appears in the menu bar.*
7. Double-click **sslvpn-client.wgssl** to configure the Mobile VPN with SSL client software.

## Update the Configuration of a Computer that is Unable to Connect to the XTM Device

You must have an updated sslvpn-client.wgssl file. For information on how to get the sslvpn-client.wgssl file, see [Get the configuration file from the XTM device](#).

1. Double-click **sslvpn-client.wgssl**.  
*The SSL client starts.*
2. Type your user name and password. Click **Connect**.

The SSL VPN connects with the new settings.

## Uninstall the Mobile VPN with SSL Client

You can use the uninstall application to remove the Mobile VPN with SSL client from a computer.

## Windows Vista and Windows XP

1. From the **Start Menu**, select **All Programs > WatchGuard > Mobile VPN with SSL client > Uninstall Mobile VPN with SSL client**.

*The Mobile VPN with SSL client uninstall program starts.*

2. Click **Yes** to remove the Mobile VPN with SSL client and all of its components.
3. When the program is finished, click **OK**.

## Mac OS X

1. In a Finder window, go to the **Applications > WatchGuard** folder.
2. Double-click the **Uninstall WG SSL VPN** application to start the uninstall program.  
*The Mobile VPN with SSL client uninstall program starts.*
3. Click **OK** on the **Warning** dialog box.
4. Click **OK** on the **Done** dialog box.
5. In a Finder window, go to the **Applications** folder.
6. Drag the **WatchGuard** folder to the Trash.





# 31 WebBlocker

---

## About WebBlocker

If you give users unlimited web site access, your company can suffer lost productivity and reduced bandwidth. Uncontrolled Internet surfing can also increase security risks and legal liability. The WebBlocker security subscription gives you control of the web sites that are available to your users.

WebBlocker uses a database of web site addresses controlled by SurfControl, a leading web filter company. When a user on your network tries to connect to a web site, the XTM device examines the WebBlocker database. If the web site is not in the database or is not blocked, the page opens. If the web site is in the WebBlocker database and is blocked, a notification appears and the web site is not displayed.

WebBlocker works with the HTTP and HTTPS proxies to filter web browsing. If you have not configured an HTTP or HTTPS proxy, a proxy is automatically configured and enabled for you when you enable WebBlocker.

The WebBlocker Server hosts the WebBlocker database that the XTM device uses to filter web content. If you use WebBlocker on any XTM device other than an XTM 2 Series, you must first set up a local WebBlocker Server on your management computer. By default, WebBlocker on an XTM 2 Series device uses a WebBlocker Server hosted and maintained by WatchGuard.

The WebBlocker Server is installed as part of the WatchGuard System Manager installation. To learn about how to set up a WebBlocker Server, see *Set Up the WebBlocker Server* on page 1066.

To configure WebBlocker on the XTM device, you must have a WebBlocker license key and register it on the LiveSecurity web site. After you register the license key, LiveSecurity gives you a new feature key.

For more information about feature keys, see *About Feature Keys* on page 58.


# Set Up the WebBlocker Server

## Install the WebBlocker Server software

Make sure you have installed the WebBlocker Server software on your management computer. You usually do this when you select the server components to install in the WatchGuard System Manager Installer. If you did not do this, run the setup procedure as described in *Install WatchGuard System Manager Software* on page 20, but select only the WebBlocker Server component.

## Manage the WebBlocker Server

You manage the WebBlocker Server in the WatchGuard Server Center. To get to the WebBlocker Server general settings:

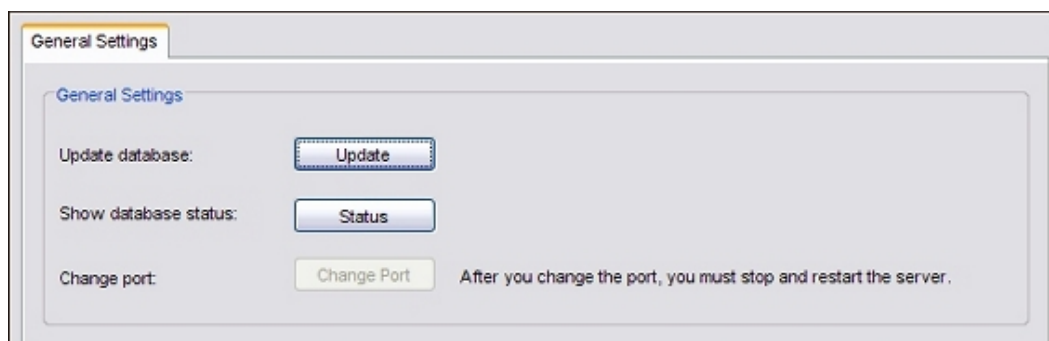
1. Right-click  in the system tray and select **Open WatchGuard Server Center**.  
*The Connect to WatchGuard Server Center dialog box appears.*
2. Type your **Username** and **Administrator passphrase**.
3. Click **Login**.  
*WatchGuard Server Center appears.*
4. In the **Servers** tree, select **WebBlocker Server**.  
*The WebBlocker General Settings page appears.*

The options available on the WebBlocker Server **General Settings** tab depend on whether you have downloaded the full WebBlocker database.

- If you did not download the WebBlocker database yet, a **Download** button appears on the **General Settings** tab.



- After you download the WebBlocker database, an **Update** button appears on the **General Settings** tab.



Use the buttons on the **General Settings** tab to manage the WebBlocker Server.


- Click **Download** to *Download the WebBlocker Database* from WatchGuard.
- Click **Update** to *Keep the WebBlocker Database Updated* with incremental updates from WatchGuard.
- Click **Status** to see the date and time the WebBlocker database was last updated and other status information.
- Click **Change Port** to *Change the WebBlocker Server Port*. We recommend you do not change the port.

## Download the WebBlocker Database

After you first install the WebBlocker server, you must download the full WebBlocker database. You can use this procedure to download a new version of the database at any time.

**Note** *The WebBlocker database has more than 240 MB of data. Your connection speed sets the download speed, which can be more than 30 minutes. Make sure your hard disk drive has a minimum of 250 MB of free space.*

To download the WebBlocker database:

1. Right-click  in the system tray and select **Open WatchGuard Server Center**.  
*The Connect to WatchGuard Server Center dialog box appears.*
2. Type your **Username** and **Administrator passphrase**.
3. Click **Login**.  
*WatchGuard Server Center appears.*
4. In the **Servers** tree, select **WebBlocker Server**.  
*The WebBlocker General Settings page appears.*



5. To download the full WebBlocker database, click **Download**.  
*The Download WebBlocker Database dialog box appears.*



- To download the folder to a location other than the default, click **Browse** and select a new folder. The default database location is C:\Documents and Settings\WatchGuard\wbserver\db. You cannot save the WebBlocker database to a root directory, such as c:\.
- To download the new database, click **Download**.  
*The download progress appears in a separate dialog box.*
- Click **OK** twice to close the database download dialog box and the information dialog box.
- To start the WebBlocker server, right-click **WebBlocker Server** in WatchGuard Server Center, and select **Start Server**.


**Note** *The WebBlocker database does not update automatically. To keep your WebBlocker database up to date, we recommend you use Windows Task Scheduler to set up regular, automatic incremental database updates. To learn how, see Keep the WebBlocker Database Updated on page 1068.*

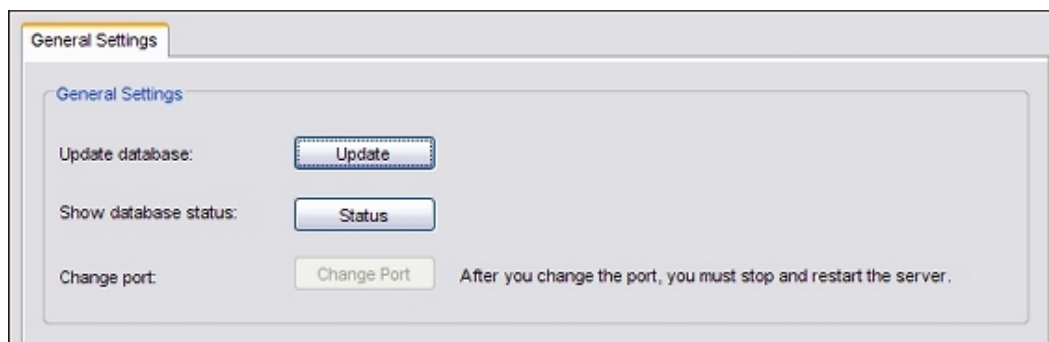
## Keep the WebBlocker Database Updated

The WebBlocker database does not update automatically. You can update the WebBlocker database at any time. To download the full database use the download procedure described in *Download the WebBlocker Database* on page 1067.

To keep your WebBlocker database up to date, we recommend you use Windows Task Scheduler to set up database updates.

## Get an Incremental Update

- Right-click  in the system tray and select **Open WatchGuard Server Center**.  
*The Connect to WatchGuard Server Center dialog box appears.*
- Type your **Username** and **Administrator passphrase**.
- Click **Login**.  
*WatchGuard Server Center appears.*
- In the **Servers** tree, right-click **WebBlocker Server** and select **Stop Server**.  
*A confirmation message appears.*
- Click **Yes**.
- In the WebBlocker **General Settings** tab, click **Update**.



- To start the server, right-click **WebBlocker Server** and select **Start Service**.

## Automate WebBlocker Database Downloads

The best procedure to keep your WebBlocker database updated is to use Windows Task Scheduler. You can use Windows Task Scheduler to schedule the “updatedb.bat” process, which is created automatically for you in your C:\Program Files\WatchGuard\wsm11.0\bin directory.

1. Open the Windows Task Scheduler.  
In Windows XP, select **Start > All Programs > Accessories > System Tools > Scheduled Tasks**.
2. Click **Add Scheduled Task**.  
*The Scheduled Tasks wizard starts.*
3. Click **Next**.  
*A list of programs appears.*
4. Click **Browse** and go to C:\Program Files\WatchGuard\wsm11\bin.
5. Select **updatedb.bat**.
6. Select the time interval at which to do this task. We recommend that you update your database each day. You can update less frequently if you have low bandwidth. Click **Next**.
7. Type the time and frequency to start the procedure. Because the update batch file stops and restarts the WebBlocker Server, we recommend that you schedule updates outside your usual hours of operation.
8. Select a start date. Click **Next**.
9. Type the user name and the passphrase for this procedure. Make sure that this user has access to the necessary files. Click **Next**.
10. Click **Finish**.

## See Database Status

1. In the **Servers** tree, select **WebBlocker Server**.  
*The WebBlocker Server General Settings page appears.*
2. Click **Status**.  
*The WebBlocker Database Status dialog box appears.*




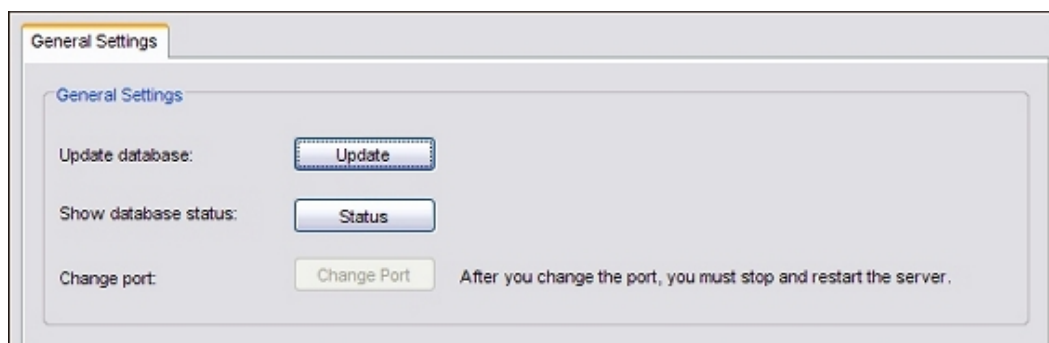
3. Review the status of the database.
4. Click **OK**.

## Change the WebBlocker Server Port

The XTM device sends WebBlocker queries to your WebBlocker Server on UDP port 5003. By default, the XTM device uses TCP port 5003 to verify the connection to your WebBlocker Server. Your WebBlocker Server listens for communications from the XTM device on those ports. We recommend you do not change the port number. The only reason to change the WebBlocker port number is if the computer you want to use as your WebBlocker Server uses other software that listens on TCP or UDP port 5003 (for example, Filemaker Pro).

## Change the WebBlocker Server Listen Port

1. Right-click  in the system tray and select **Open WatchGuard Server Center**.  
*The Connect to WatchGuard Server Center dialog box appears.*
2. Type your **Username** and **Administrator passphrase**.
3. Click **Login**.  
*WatchGuard Server Center appears.*
4. In the **Servers** tree, select **WebBlocker Server**.  
*The WebBlocker General Settings page appears.*



5. Click **Change Port**.  
*The WebBlocker Configuration dialog box appears.*

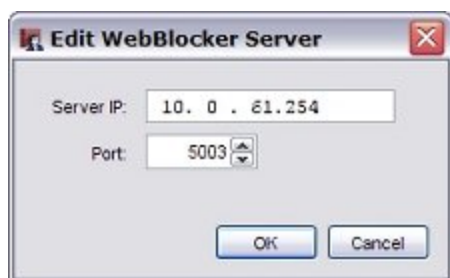


6. In the **Server Listen Port** text box, type or select the new port number. Click **OK**.  
*The port number is changed. The change does not take effect until you stop and restart the WebBlocker Server.*
7. To stop the server, in the **Servers** tree, right-click **WebBlocker Server** and select **Stop Server**.
8. To restart the server, in the **Servers** tree, right-click **WebBlocker Server** and select **Start Server**.

## Change the WebBlocker Server Port Used by the XTM device

After you change the port number for the WebBlocker Server, you must edit the configuration file for each XTM device that uses WebBlocker.

1. Open Policy Manager.
2. Select **Setup > Actions > WebBlocker**.  
*The WebBlocker Configurations dialog box appears.*
3. Select the WebBlocker configuration. Click **Edit**.  
*The Edit WebBlocker Configuration dialog box appears.*
4. Select the WebBlocker Server. Click **Edit**.  
*The Edit WebBlocker Server dialog appears.*



5. In the **Port** field, type or select the port number that you configured in the WebBlocker Server settings.
6. Click **OK** to close each of the open WebBlocker dialog boxes.
7. *Save the Configuration File.*

## Copy the WebBlocker Database from One WebBlocker Server to Another

After you install WebBlocker, you usually download the full WebBlocker database from WatchGuard. If you already have a WebBlocker Server, you can copy the WebBlocker database from that server to the new server. The WebBlocker database is over 250 MB. Dependant on the speed of your Internet connection, it might be faster to copy the WebBlocker database from a local server, than to download the full database from WatchGuard.

### Before You Begin

Before you copy the WebBlocker database, you must install the WebBlocker Server on the second server.

**Note** *You must install the WebBlocker Server in the same location on both servers.*

You usually do this when you select the server components to install in the WatchGuard System Manager Installer. If you did not do this, run the setup procedure as described in *Install WatchGuard System Manager Software* on page 20, but select only the WebBlocker Server component.

These instructions use the default installation location for WatchGuard System Manager 11.0. The version number is part of the installation path. If you use a different version, you must change the path in some of these steps to match your version number. If you installed the server in a different location on both servers, use that path.

## Copy the WebBlocker Database and Configuration Files

1. Copy the contents of `\documents and settings\watchguard\wbserver\db` from the existing server to the same location on the new server.
2. Copy the file `\documents and settings\watchguard\wbserver\conf\CSPConfig.ini` from the existing server to the same location on the new server.
3. On the new server, open `\documents and settings\watchguard\wbserver\wbserver.ini` in a text editor such as Notepad.
4. Add these two lines to the bottom of the file (include the quotes and the line break):  
SurfConfigFile = "  
C:\\Documents and Settings\\WatchGuard\\wbserver\\conf\\CSPConfig.ini"

**Note** *If you do not complete this step, the configuration file is not recognized and the WebBlocker Server does not start.*


5. On the new server, copy the file `\program files\watchguard\wsm11.0\wbserver\conf\license.ini` to the target server directory `\documents and settings\watchguard\wbserver\conf`.

## Run the Utility to Install the WebBlocker Service

Usually, this step is done for you automatically when you download the database. If you copy a local database, you must run this command manually.

1. In the Windows start menu, select **Start > Run**.
2. Type (include the quotation marks):  
"C:\program files\watchguard\wsm11.0\wbserver\bin\wbserver" -config

## Start the WebBlocker Server on the Target Server

1. Right-click  in the system tray and select **Open WatchGuard Server Center**.  
*The Connect to WatchGuard Server Center dialog box appears.*
2. Type your **Username** and **Administrator passphrase**.
3. Click **Login**.  
*WatchGuard Server Center appears.*
4. In the **Servers** tree, right-click **WebBlocker Server**.
5. Select **Start Server**.  
*The WebBlocker server starts and uses the copied database.*

We recommend you use Windows Task Scheduler to set up regular, automatic incremental database updates. For more information, see *Keep the WebBlocker Database Updated* on page 1068.



# Get Started with WebBlocker

## Before You Begin

- If you have not already done so, *Set Up the WebBlocker Server*.
- Download the WebBlocker database for the WebBlocker Server. For instructions, see *Download the WebBlocker Database* on page 1067.
- *Get a Feature Key from LiveSecurity* for WebBlocker, and then import the feature key to your XTM device.

For more information, see *Add a Feature Key to Your XTM Device* on page 62.

## Activate WebBlocker

You can use Policy Manager to activate WebBlocker on your XTM device.

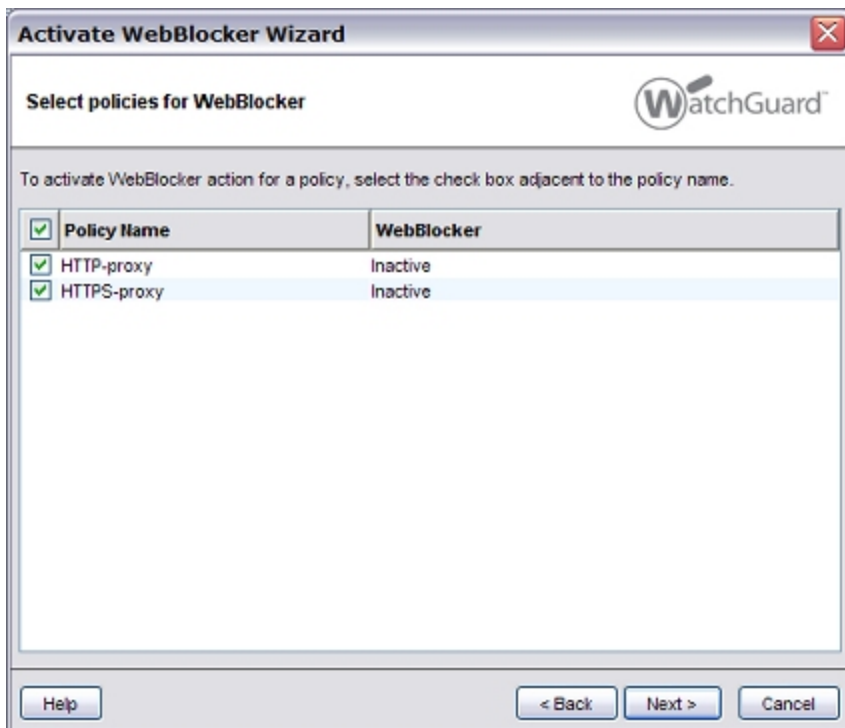
1. *Open Policy Manager*.
2. Select **Subscription Services > WebBlocker > Activate**.  
*The Activate WebBlocker Wizard starts.*
3. Click **Next**.  
*The first page of the wizard appears. The page you see depends on your configuration.*
4. Complete the wizard, as described in the subsequent sections.

## Set Policies for WebBlocker

If you have not yet defined a HTTP-proxy or a HTTPS-proxy policy, this page does not appear. The wizard automatically creates a default HTTP-proxy policy for you.

If you have already created a HTTP-proxy or a HTTPS-proxy policy on your XTM device, it appears on this page. To add a WebBlocker action to a policy in the list, select the check box for that policy.

If you do not select any policies, a new HTTP-proxy policy is created with a WebBlocker action.



## Identify the WebBlocker Servers

If you have a WatchGuard XTM device other than a 2 Series, you must configure at least one WebBlocker Server.



To add a WebBlocker Server:

1. Click **Add**.
2. In the **Server IP** text box, type the IP address of the WebBlocker Server.
3. If necessary, change the port number.

You can add a backup WebBlocker Server that the XTM device can fail over to if it cannot connect to the primary server. The first server in the list is the primary server.

To move a server in the list:

1. Select a server.
2. Click **Move Up** or **Move Down**.

If your device is an XTM 2 Series, WebBlocker uses a WebBlocker Server hosted by WatchGuard by default. You can configure WebBlocker to use a locally configured WebBlocker Server:

1. Select **Custom WebBlocker server**.
2. Click **Add**.
3. In the **Server IP** text box, type the IP address of the WebBlocker Server.
4. If necessary, change the port number.

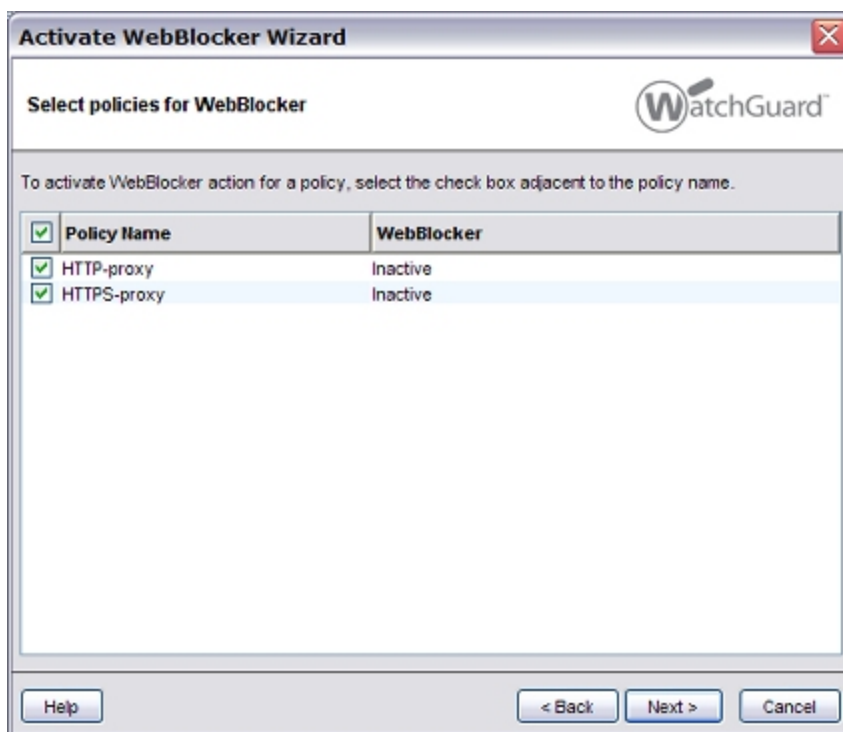


To add a WebBlocker Server after you complete the wizard:

1. Open Policy Manager.
2. Select **Setup > Actions > WebBlocker**.
3. Click **Add**.
4. Select the **Servers** tab.

## Select Categories to Block

You can select to the categories that WebBlocker denies.



- To select the categories to block, select the check box adjacent to each web site category. The **Other** category is enabled by default.  
For more information on WebBlocker categories, see *About WebBlocker Categories* on page 1080.
- To read a description of a category, click the category. The description appears at the bottom of the page.
- If you want to block access to web sites that match all the categories, select the **Deny All Categories** check box.
- To make sure users cannot go to web sites that hide their identities to try to avoid WebBlocker, select to block the **Proxies & Translators** category.

## Use Exception Rules to Restrict Web Site Access

You can choose to use exception rules to restrict web site access instead of categories.

1. Clear the check boxes for all categories.
2. Select **Deny website access**, as described in *About WebBlocker Exceptions* on page 1086.

# Configure WebBlocker

After you use the Activate WebBlocker Wizard to activate WebBlocker and create a basic configuration, you can use Policy Manager to configure additional WebBlocker settings.

## Configure WebBlocker Settings for a Policy

1. Select **Subscription Services > WebBlocker > Configure**.

*The Configure WebBlocker dialog box appears and shows any HTTP or HTTPS policies that were already created.*



2. Select a policy to configure. Click **Configure**.

*The WebBlocker Configuration dialog box for that policy appears.*



The **WebBlocker Configuration** dialog box includes tabs to you can use to:

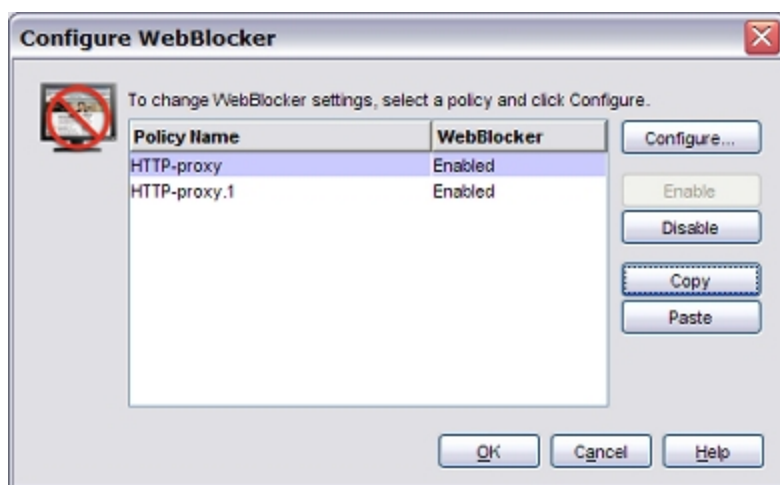
- *Add New WebBlocker Servers or Change Their Order*
- *Change Categories to Block*
- *Add WebBlocker Exceptions*
- *Define Advanced WebBlocker Options*
- *Define WebBlocker Alarms*

## Copy WebBlocker Settings from One Policy to Another

If you have more than one WebBlocker policy, you can copy settings from one policy to another.

1. Select the policy you want to copy settings from, and click **Copy**.

*The Paste button activates.*



2. Select the policy you want to copy the settings to, and click **Paste**.

*The WebBlocker settings are copied to the second policy you selected.*

3. Click **Configure** to view the policy settings.

*The policy settings are the same as for the policy you copied from in Step 1.*

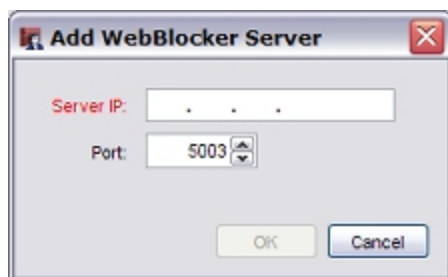
## Add New WebBlocker Servers or Change Their Order

You can add up to five WebBlocker Servers. If the XTM device cannot connect to the first server in the list, it tries to connect to the subsequent one in the list. The first server in the list is the primary server.

### Add a Server

1. On the **Servers** tab of the **WebBlocker Configuration** dialog box, click **Add**.

*The Add WebBlocker Server dialog box appears.*



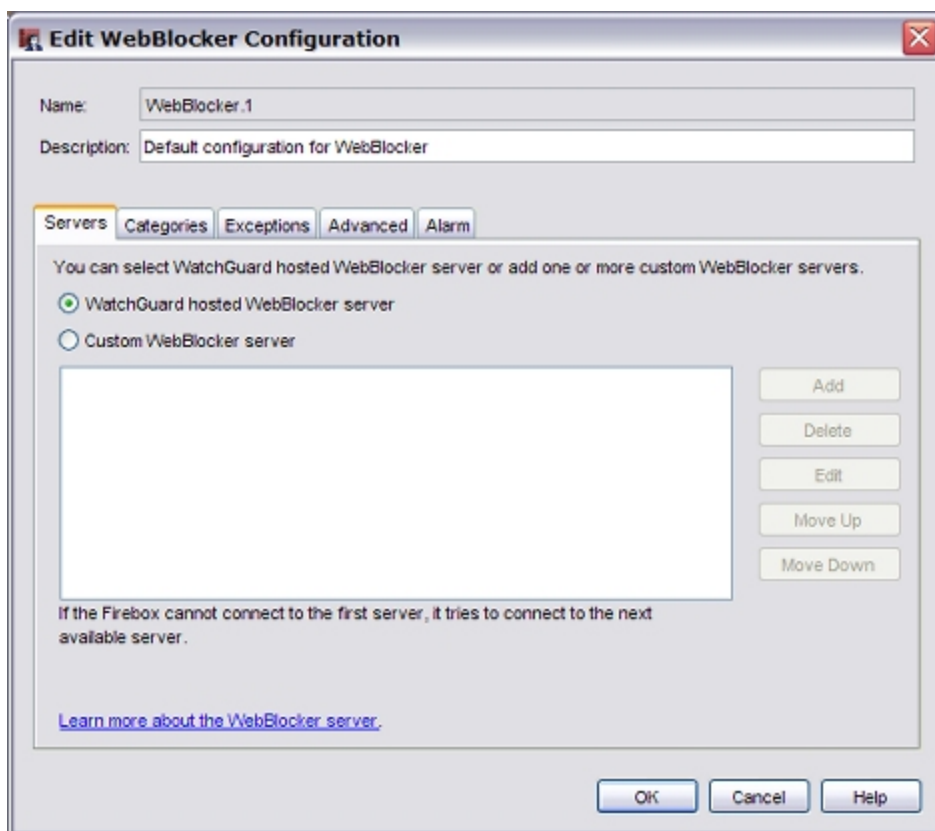
2. Next to **Server IP**, type the IP address of the WebBlocker Server. If necessary, change the port number. Click **OK**.

## Change the Order of Servers

1. You can change the order of the servers to define the order in which the XTM device fails over to backup servers. To move a server higher in the list, select it and click **Move Up**. To move it lower, select it and click **Move Down**.
2. Click **OK**.

For information about server timeout settings, see *Define Advanced WebBlocker Options* on page 1084.

For the XTM 2 Series, WebBlocker uses a WebBlocker Server hosted by WatchGuard by default. If you want WebBlocker to use a locally configured WebBlocker Server, select **Custom WebBlocker server**, and configure a local WebBlocker Server..



## About WebBlocker Categories

The WebBlocker database contains nine category groups, with 54 web site categories.

A web site is added to a category when the contents of the web site meet the correct criteria. Web sites that give opinions or educational material about the subject matter of the category are not included. For example, the **Illegal Drugs** category denies sites that tell how to use marijuana. They do not deny sites with information about the historical use of marijuana.

SurfControl periodically adds new web site categories. The new categories do not appear on the WebBlocker configuration page until WatchGuard updates the software to add the new categories.

To block sites that meet the criteria for a new SurfControl category that is not yet part of a WebBlocker software update, select the **Other** category.

To block sites that do not meet the criteria for any other category, select the **Uncategorized** category.

## Change Categories to Block

When you used the Activate WebBlocker Wizard, you selected categories of web sites you want to block. Click the **Categories** tab on the **WebBlocker Configuration** dialog box to make changes to your original configuration.

This dialog box is very similar to the wizard screen described in *Get Started with WebBlocker* on page 1073. The main difference is that the categories are grouped below headings. For example, the Shopping heading includes Advertisements, Food & Drink, Motor Vehicles, Real Estate, and Shopping. If you want to select all the sites below the Shopping heading, you can select the check box adjacent to Shopping. All the sites below it are automatically selected. If you want to select only one or a few categories below Shopping but not all of them, clear the **Shopping** check box and select only the categories you want to restrict.

For information on WebBlocker categories, see *About WebBlocker Categories* on page 1080.

## Send an Alarm when a Site is Denied

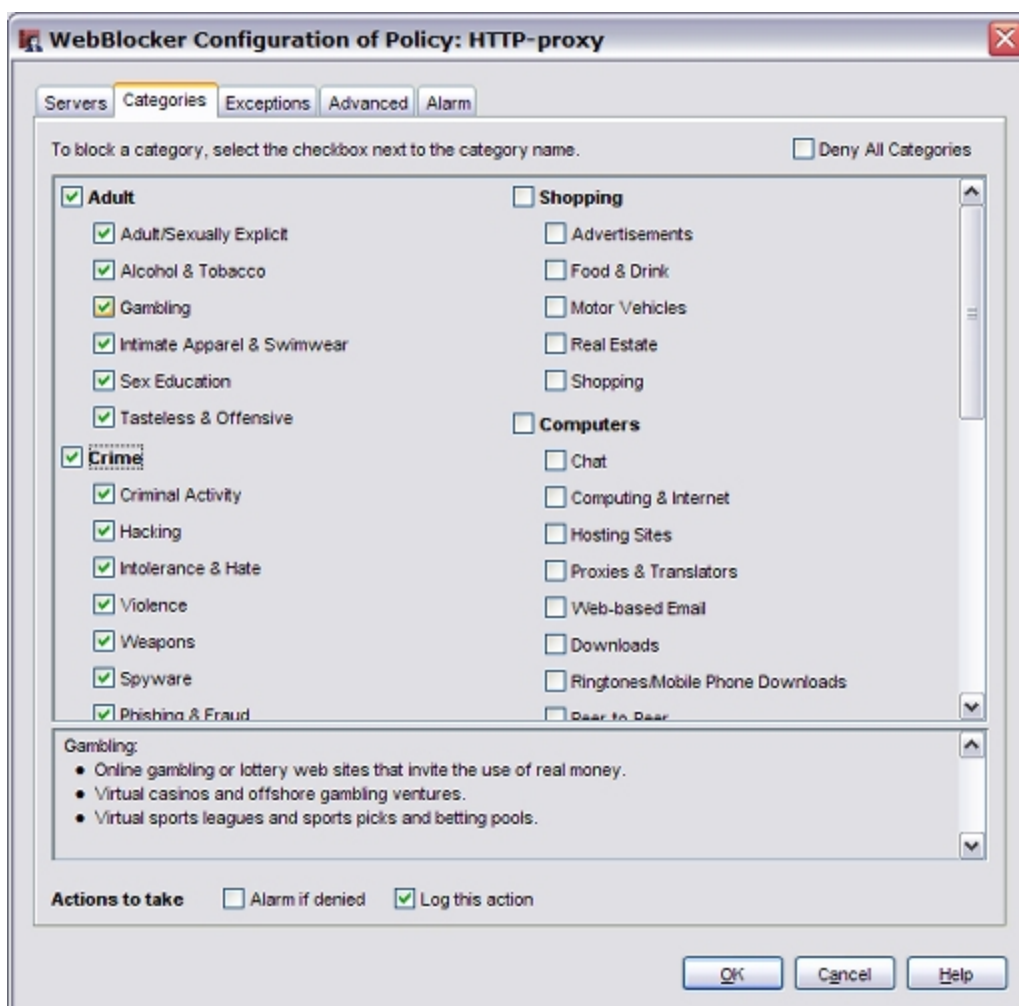
You can define WebBlocker to send an alarm if a user tries to go to a site and is denied. In the **Actions to Take** section at the bottom of the dialog box, select **Alarm if denied**.

To set parameters for the alarms, click the **Alarm** tab. For information on the fields in this dialog box, see *Set Logging and Notification Preferences* on page 723.

## Log WebBlocker Actions

You can define WebBlocker to send a message to the log file if a user tries to go to a site and is denied. In the **Actions to Take** section at the bottom of the dialog box, select **Log this action**.



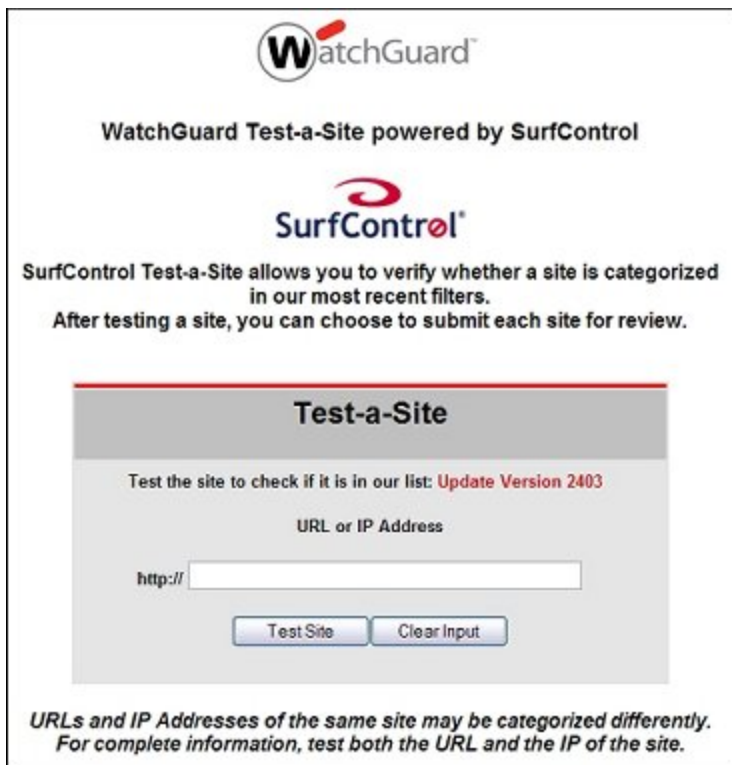


## See Whether a Site is Categorized

To see whether WebBlocker denies access to a web site as part of a category block, go to the Test-a-Site page on the SurfControl web site.

1. Open a web browser and go to [http://mtas2.surfcontrol.com/mtas/WatchGuardTest-a-Site\\_MTAS.asp](http://mtas2.surfcontrol.com/mtas/WatchGuardTest-a-Site_MTAS.asp).

*The WatchGuard Test-a-Site page appears.*



2. Type the URL or IP address of the site to check.
3. Click **Test Site**.

*The WatchGuard Test-a-Site Results page appears.*



## Add, Remove, or Change a Category

If you get a message that the URL you entered is not in the SurfControl list, you can submit it on the Test Results page.

1. On the **Test Results** page, click **Submit A Site**.

*The Submit A Site page appears.*

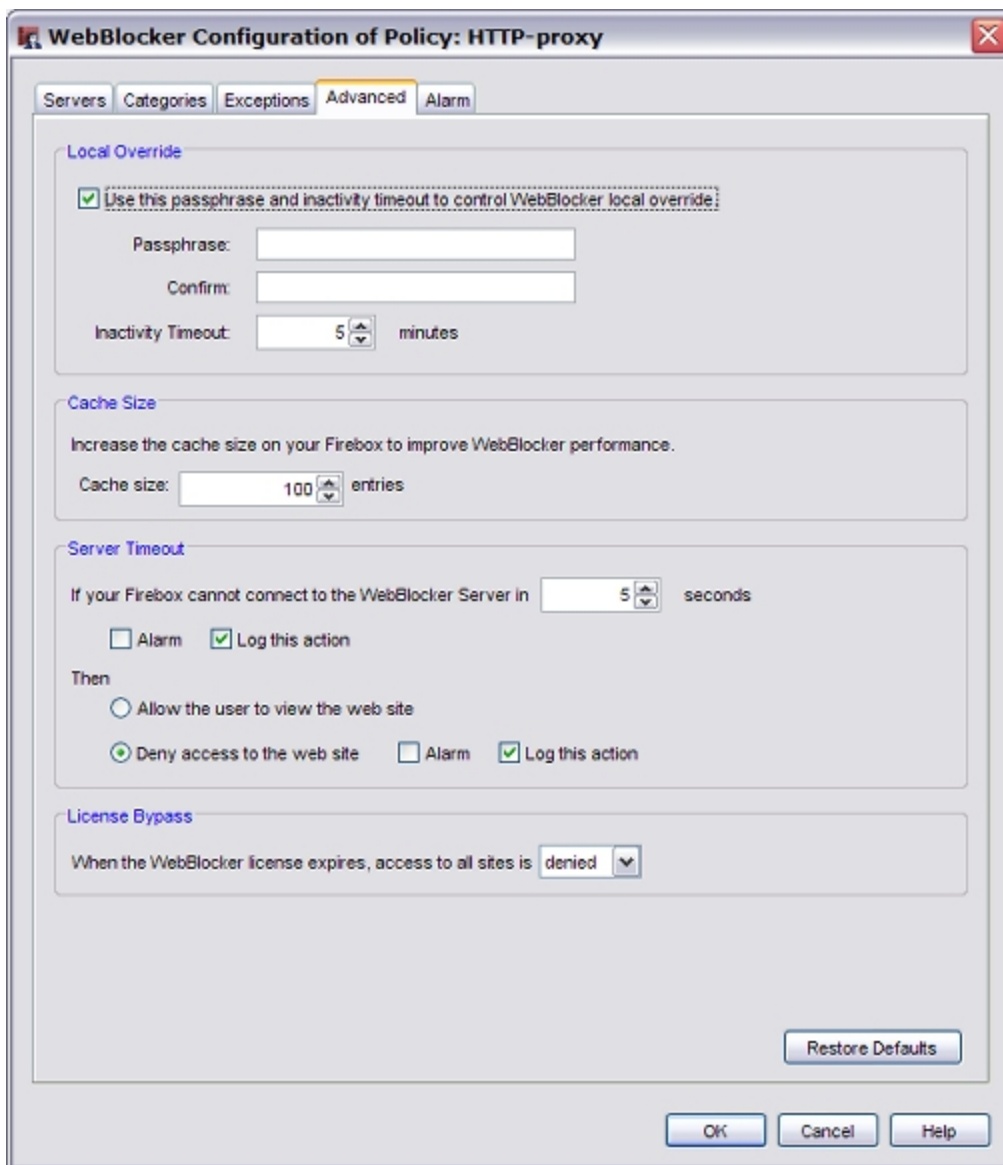


The screenshot shows a web form titled "Submit-a-Site" with a dark blue header. Below the header, there are three radio buttons for selection: "Add a site" (which is selected), "Delete a site", and "Change the category". To the left of these radio buttons is the text "Do You Want To:". Below the radio buttons is a text input field labeled "URL (Internet Address):" with "http://" pre-filled. Below the URL field is a dropdown menu labeled "Choose Category:" with "None" selected. At the bottom of the form are two buttons: "Submit" and "Reset".

2. Select whether you want to **Add a site**, **Delete a site**, or **Change the category**.
3. Type the site URL.
4. To request that the category assigned to a site is changed, select the new category from the drop-down list.
5. Click **Submit**.

## Define Advanced WebBlocker Options

To configure advanced WebBlocker options, select the **Advanced** tab.



## Local Override

If you want to allow users to bypass WebBlocker if they know a passphrase, select the **Use this passphrase and inactivity timeout to enable WebBlocker local override** check box. Type a passphrase in the **Passphrase** text box, and then type the same password again in the **Confirm** text box. If desired, change the **Inactivity Timeout**.

When you enable WebBlocker local override, if a user tries to visit a site that is denied by WebBlocker, the user is prompted to type the override password. When the user types the correct password, WebBlocker allows the user to get to the destination web site until the inactivity timeout is reached or until an authenticated user logs out. This feature operates only with HTTP proxy policies. For more information about local override, see *Use WebBlocker Local Override* on page 1099.

## Cache Size

Change this setting to improve WebBlocker performance.

### *Cache Size*

Use the arrows to change the number of entries in the cache or type in a number.

## Server Timeout

### *If your Firebox cannot connect to the WebBlocker server in*

Set the number of seconds to try to connect to the server before the XTM device times out.

### *Alarm*

Select to send an alarm when the XTM device cannot connect to the WebBlocker Server and times out. To set parameters for the alarms, click the **Alarm** tab. For information about the settings on the **Alarm** tab, see *Set Logging and Notification Preferences* on page 723.

### *Log this action*

Select to send a message to the log file if the XTM device times out.

### *Allow the user to view the web site*

Select if you want to allow the user to see the web site if the XTM device times out and does not connect to the WebBlocker Server.

### *Deny access to the web site*

Select to deny access if the XTM device times out.

The XTM device attempts to reach the WebBlocker Server even when it is unavailable. If you allow web traffic when the server is unavailable, each user who sends a web request must wait the amount of time in the above field to try to connect to the WebBlocker Server and time out. After this number of seconds, the XTM device allows access to the web site. When the XTM device can connect to the WebBlocker Server again, it starts to apply WebBlocker rules again.

To add or delete servers, or to change their order of priority, see *Add New WebBlocker Servers or Change Their Order* on page 1078.

## License Bypass

The license bypass setting controls whether users on your network can get access to web sites if WebBlocker is enabled and the WebBlocker security subscription expires.

From the **When the WebBlocker license expires, access to all sites is** drop-down box, select one of these options:

*denied*

Select to block access to all web sites when the WebBlocker license expires

*allowed*

Select to allow access to all web sites when the WebBlocker license expires

By default, license bypass is configured to block access to all web sites if the WebBlocker security subscription is expired. This is the most secure option if you must block your users from specific types of content.

For information about how to renew your security subscription see *Renew Security Subscriptions* on page 84.

## Define WebBlocker Alarms

To configure notification parameters for WebBlocker alarms, select the **Alarm** tab.

You can send an alarm when the XTM device cannot connect to the WebBlocker Server and times out, or when the XTM device times out and access to a site is denied. For information about the **Alarm** tab settings, see *Set Logging and Notification Preferences* on page 723.

To change server timeout settings, see *Define Advanced WebBlocker Options* on page 1084.

## About WebBlocker Exceptions

WebBlocker could deny a web site that is necessary for your business. You can override WebBlocker when you define a web site usually denied by WebBlocker as an *exception* to allow users to get access to it. For example, suppose employees in your company frequently use web sites that contain medical information. Some of these web sites are forbidden by WebBlocker because they fall into the sex education category. To override WebBlocker, you specify the web site IP address or its domain name. You can also deny sites that WebBlocker usually allows

WebBlocker exceptions apply only to HTTP traffic. If you deny a site with WebBlocker, the site is not automatically added to the Blocked Sites list.

To add WebBlocker exceptions, see *Add WebBlocker Exceptions* on page 1088.

## Define the Action for Sites that do not Match Exceptions

In the **Use category list** section below the list of exception rules, you can configure the action to occur if the URL does not match the exceptions you configure. By default the **Use the WebBlocker category list to determine accessibility** radio button is selected, and WebBlocker compares sites against the categories you selected on the **Categories** tab to determine accessibility.

You can also choose not to use the categories at all and instead use exception rules only to restrict web site access. To do this, click the **Deny website access** radio button.

### *Alarm*

Select to send an alarm when the XTM device denies a WebBlocker exception. To set parameters for the alarms, click the **Alarm** tab. For information on the **Alarm** tab fields, see *Set Logging and Notification Preferences* on page 723.

### *Log this action*

Select to send a message to the log file when the XTM device denies a WebBlocker exception.

## Components of Exception Rules

Exception rules are based on IP addresses or a pattern based on IP addresses. You can have the XTM device block or allow a URL with an exact match. Usually, it is more convenient to have the XTM device look for URL patterns. The URL patterns do not include the leading "http://". To match a URL path on all web sites, the pattern must have a trailing `"/*`.

The host in the URL can be the host name specified in the HTTP request, or the IP address of the server.

Network addresses are not supported, however you can use subnets in a pattern (for example, 10.0.0.\*).

For servers on port 80, do not include the port. For servers on ports other than 80, add  `:port`, for example: 10.0.0.1:8080. You can also use a wildcard for the port—for example, 10.0.0.1:\*—but this does not apply to port 80.

## Exceptions with Part of a URL

You can create WebBlocker exceptions with the use of any part of a URL. You can set a port number, path name, or string that must be blocked for a special web site. For example, if it is necessary to block only `www.sharedspace.com/~dave` because it has inappropriate photographs, you type `"www.sharedspace.com/~dave/*"`. This gives the users the ability to browse to `www.sharedspace.com/~julia`, which could contain content you want your users to see.

To block URLs that contain the word `"sex"` in the path, you can type `"*/sex*"`. To block URLs that contain `"sex"` in the path or the host name, type `"*sex*"`.

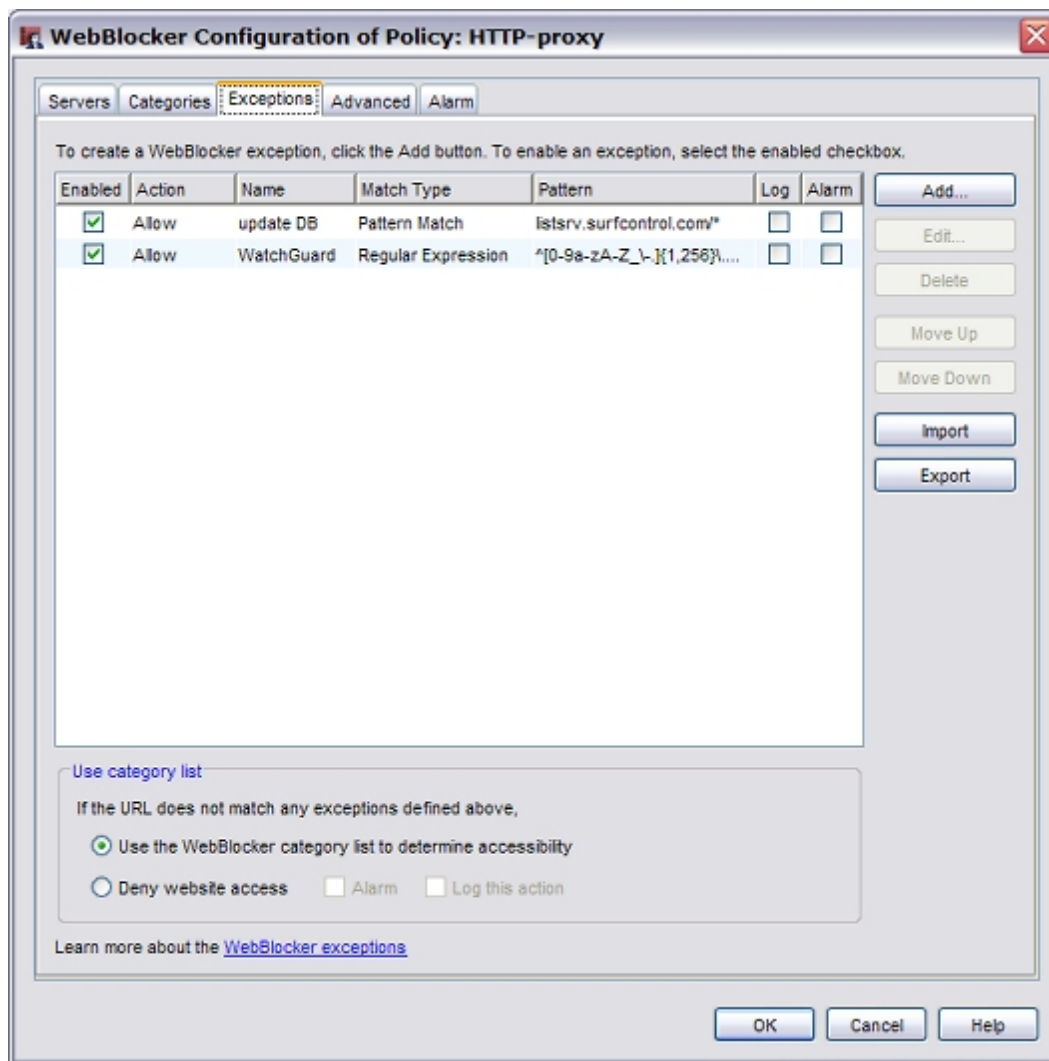
You can block ports in an URL. For example, look at the URL `http://www.hackerz.com/warez/index.html:8080`. This URL has the browser use the HTTP protocol on TCP port 8080 instead of the default method that uses TCP 80. You can block the port by matching `*8080`.

## Add WebBlocker Exceptions

From Policy Manager, you can add an exception that is an exact match of a URL, or you can use the wildcard symbol "\*" in the URL to match any character. For example, if you add "www.example.com" to the Allowed Sites list, and a user types "www.example.com/news", the request is denied. If you add "www.example.com/\*" to the Allowed Sites list, WebBlocker allows requests to go to all URL paths on the www.example.com web site.

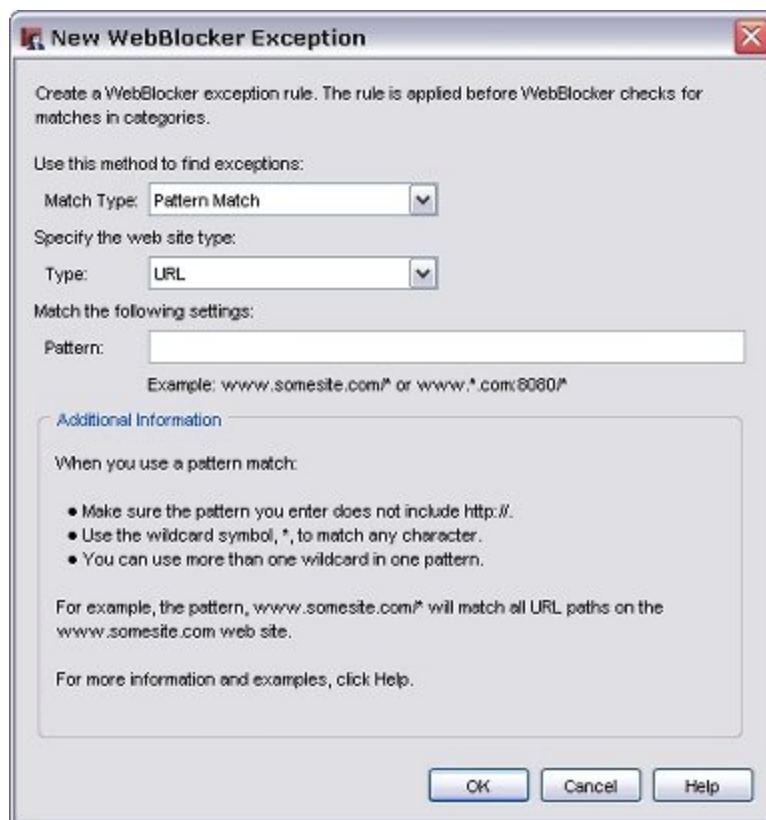
To add exceptions:

1. To create exceptions to the WebBlocker categories, select the **Exceptions** tab.



2. Click **Add** to add a new exception rule.  
*The New WebBlocker Exception dialog box appears.*





- From the **Match Type** drop-down list, select one of these options:

#### *Pattern match*

Pattern matches match a pattern in the URL or address, for example “pattern” in `www.pattern.com`. Make sure to drop the leading “`http://`” and include “`/*`” at the end. Use the wildcard symbol, `*`, to match any character. You can use more than one wildcard in one pattern. For example, the pattern `www.somesite.com/*` will match all URL paths on the `www.somesite.com` web site. To enter a network address, use a pattern match that ends in a wildcard. For example, to match all the web sites at `1.1.1.1` on port `8080`, set the directory to “`*`”.

#### *Exact match*

Exact matches match an exact URL or IP address, character by character. You cannot use wildcards, and you must type each character exactly as you want it to be matched. For example, if you enter an exception to allow `www.yahoo.com` as an exact match only, and a user types “`www.yahoo.com/news`”, the request is denied.

#### *Regular expression*

Regular expression matches use a Perl-compatible regular expression to make a match. For example, `\.[onc][eor][gtm]` matches `.org`, `.net`, `.com`, or any other three-letter combination of one letter from each bracket, in order. Be sure to drop the leading “`http://`” Supports wild cards used in shell script. For example, the expression

“(www)?\.\watchguard\.[com|org|net]” will match URL paths including www.watchguard.com, www.watchguard.net, and www.watchguard.org. The expression 1.1.1.[1-9] will match all IP addresses from 1.1.1.1 to 1.1.1.9. For help on how to use regular expressions, see *About Regular Expressions* on page 413.

4. From the **Type** drop-down list, select the web site type: **URL** or **Host IP Address**.
5. If you chose **URL**, type the pattern, value, or expression, depending on the value you selected for **Match Type**.  
If you chose **Host IP Address**, type the address, port, and directory to be matched.
6. Click **OK** to close the **New WebBlocker Exception** dialog box.
7. Click the **Action** column to activate the **Action** drop-down list. Select whether WebBlocker allows or denies the exception.
8. In the **Name** text box, type a name for the exception. The default name is WB Rule[number].

You can use any of these options for WebBlocker exceptions:

- You can use the drop-down lists for the **Match Type** and **Pattern** fields if you want to change the settings you made in the **New WebBlocker Exception** dialog box.
- Click the **Log** check box if you want a log message when an action is taken on a WebBlocker exception.
- To disable a exception but keep it in your configuration for possible use at a later time, clear the **Enabled** check box.
- In the **Use category list** section below the list of exception rules, you can configure the action to take if the URL does not match the exceptions you configure. The default setting is that the **Use the WebBlocker category list to determine accessibility** radio button is selected, and WebBlocker compares sites against the categories you selected on the **Categories** tab to determine accessibility.
- You can also choose to not use the categories at all, and instead only use exception rules to restrict web site access. To deny access to all sites not listed on the exceptions list, select **Deny website access**.
- To allow access to all sites not listed on the exceptions list, select **Use the WebBlocker category list to determine accessibility**. Then, make sure that no categories are selected on the **Categories** tab.

## Change the Order of Exception Rules

The order that the exception rules appear in the dialog box shows the order in which sites are compared to the rules. WebBlocker compares messages to the first rule in the list and continues in sequence from top to bottom. When a messages matches a rule, WebBlocker performs the related action. It performs no other actions, even if a site matches a rule or rules later in the list.

To change the order of rules, select the rule whose order you want to change. Click the **Up** or **Down** button to move the rule up or down in the list.

## Import or Export WebBlocker Exception Rules

If you manage several XTM devices or use WebBlocker with more than one proxy definition, you can import and export exception rules between them. This saves time because you must define the rules only once.

You can transfer exception rules between proxies or XTM devices in two ways. You can write an ASCII file that defines the rules and import it to other XTM devices or proxies. Or, you can use the WebBlocker user interface to define the exception rules, export the file to an ASCII file, and import that file into another device configuration file or proxy definition.

## Write Rulesets in an ASCII File

You can write rules in a normal ASCII file that uses the standard UTF-8 character set.

You must include only one rule per line. The syntax for rules is:

```
[rule_name, action, enabled|disabled, log|no log, match_type,] pattern_value
```

where:

*rule\_name* is the name of the rule as it appears in the exception list. The default is **WB Rule n**.

*action* = **Allow** or **Deny**. The default action is **Allow**.

**enabled|disabled** = Whether the rule is currently enabled or disabled. The default is **enabled**.

**log|no log** = Specifies whether you want a log message when the action is taken. The default is **no log**.

*match\_type* = Specifies the type of match: exact match, regular expression or pattern match. The default is **pattern match**.

*value* = value to be matched.

The fields enclosed in brackets are optional. If you omit them, the default values are used.

To add comments to a file, precede the comment with a number sign (#). Make sure the comment is on its own line.

Below is an example exceptions file.

```
#
# Here are five exception rules
#
AllowFB, allow, enabled, No Log, *.firebox.net/*
deny, disabled, Log, very.badsite.com/*
ExceptionRule1, *.goodsite.com/"
exact match, 10.0.0.1
*.xyz.*/
```

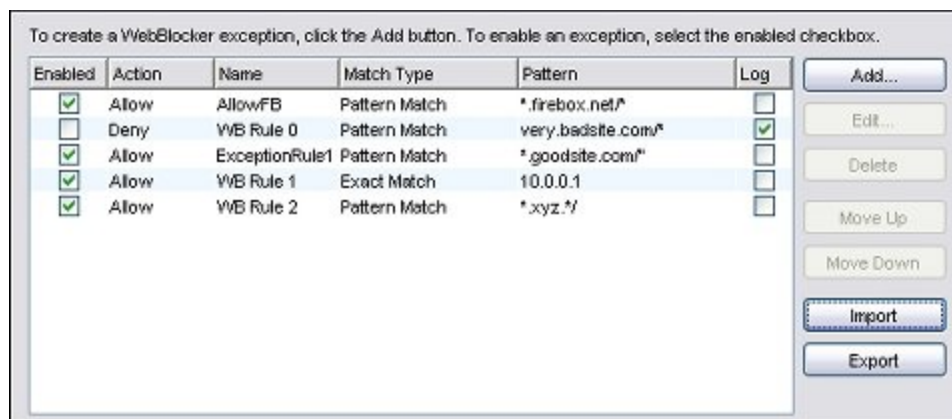
The next section, "Import an ASCII exceptions file", shows how the above file would look if imported into WebBlocker.

## Import an ASCII Exceptions File

1. From the **Exceptions** tab of the **WebBlocker Configuration** dialog box, click **Import**.
2. Find the ASCII file and click **Open**.
3. If exceptions are already defined in WebBlocker, you are asked whether you want to replace the existing rules or append the imported rules to the list of existing rules. Click **Replace** or **Append**.

If you click **Append**, the imported rules appear in the **Exceptions** block beneath any existing rules. If you want to change the order of the exception rules, see *Change the Order of Exception Rules* on page 1090.

If you import the example file in the previous section into WebBlocker, it appears like this:



## Export Rules to an ASCII File

When you export exception rules from a proxy definition, the XTM device saves the current rules to an ASCII text file in the format described above.

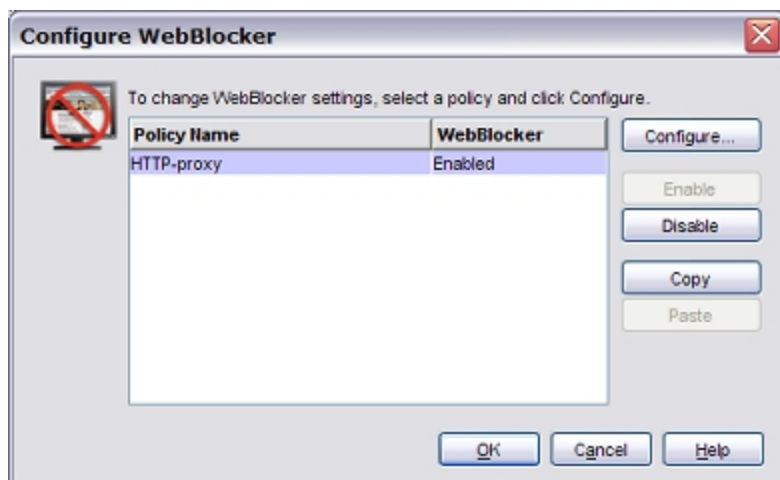
1. From the **Exceptions** tab of the **WebBlocker Configuration** dialog box, define exceptions as described in *Add WebBlocker Exceptions* on page 1088.
2. Click **Export**.
3. In the **Open** dialog box, select where you want to save the exceptions file and click **Save**.  
You can now open another HTTP proxy definition in the same or in a different XTM device configuration file and import the exceptions file.

## Restrict Users to a Specific Set of Web Sites

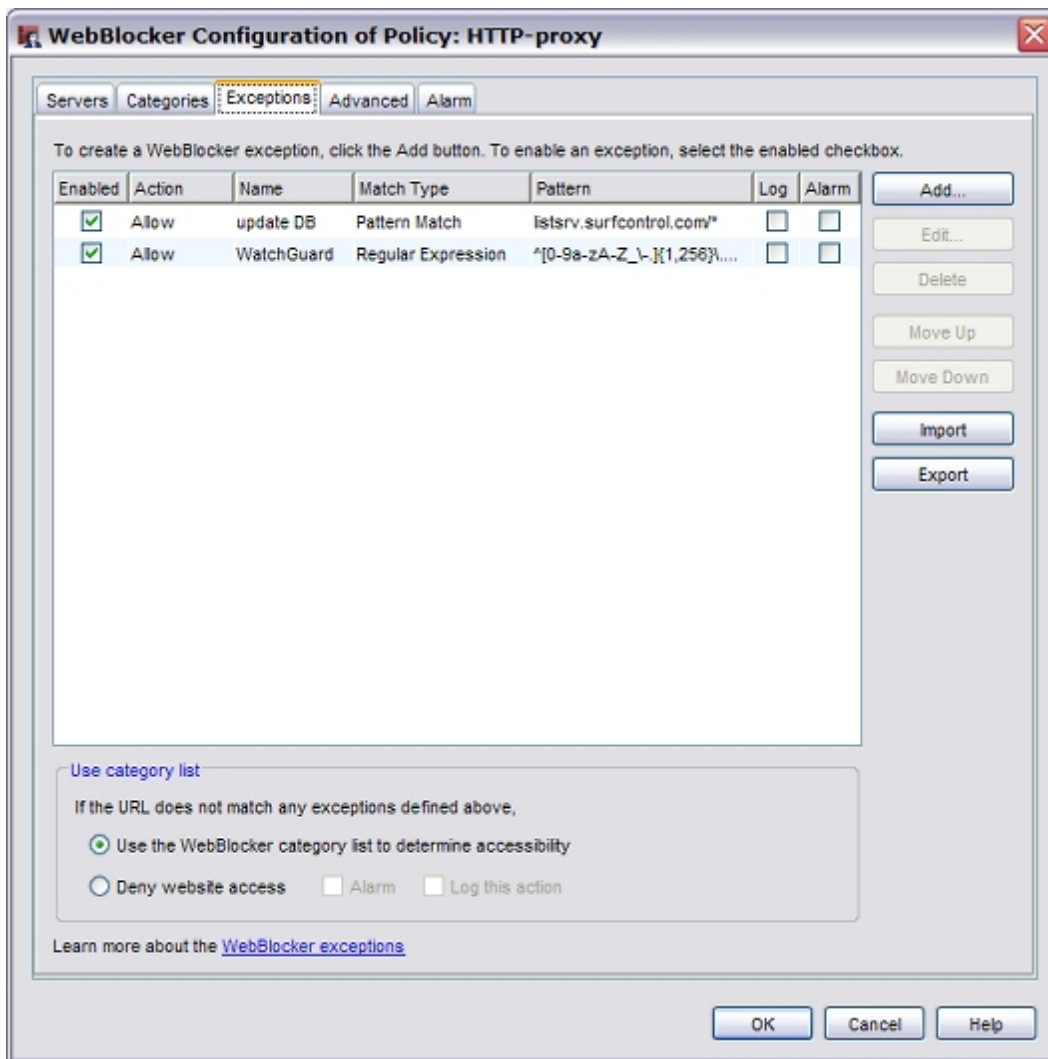
You can configure WebBlocker to give users access to only one web site or only a list of allowed web sites. To do this, you add an allowed exception to the exceptions list for each web site you want users to have access to. Then, you configure WebBlocker to deny access to any site that does not match the allowed sites. In this configuration, WebBlocker does not use the WebBlocker category list to determine access.

From Policy Manager, you can enable users to access only specifically allowed web sites based on a URL pattern.

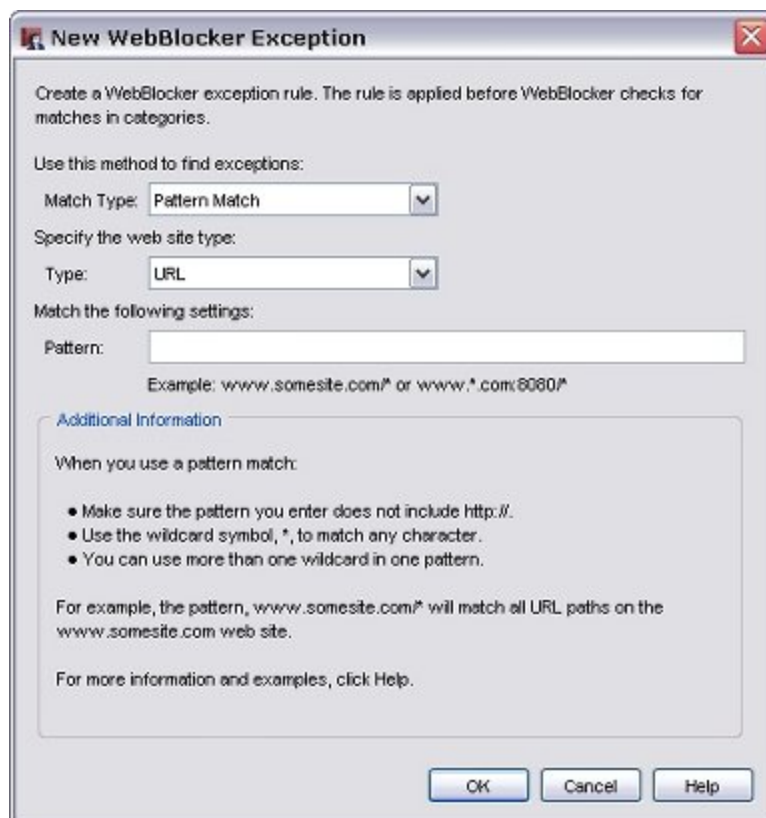
1. Select **Subscription Services > WebBlocker > Configure**.  
*The Configure WebBlocker dialog box appears and shows any HTTP or HTTPS policies that were already created.*



2. Select the policy you want to configure. Click **Configure**.  
*The WebBlocker Configuration dialog box for that policy appears.*
3. Select the **Exceptions** tab.  
*The Exceptions tab shows any exceptions you previously defined.*



4. Click **Add** to add a new exception rule.  
*The New WebBlocker Exception dialog box appears.*



5. From the **Match Type** drop-down list, select **Pattern Match**.
6. From the **Type** drop-down list, select **URL**.
7. In the **Pattern** text box, type the URL pattern that matches the web site you want to allow access to. For example, the pattern `www.mycompany.com/*` allows access to all URL paths on the `www.mycompany.com` web site. When you enter a URL, do not include the leading "http://". Include a forward slash (/) at the end of the URL pattern to match all URL paths on that site. Use the asterisk (\*) wildcard symbol to match any character. You can use more than one wildcard in one pattern.
8. Click **OK** to close the **New WebBlocker Exception** dialog box.  
*The WebBlocker Configuration shows the exception you just added.*



9. If you want to edit the exception you just added, click on the **Name** column in the exception. The default name is WB Rule[ number ].
10. Repeat Steps 2–7 to add allowed exceptions for any other sites you want to allow your users to access.
11. After you have added all the allowed sites to the exceptions list, select **Deny website access**. This setting configures WebBlocker to deny access to all web sites not explicitly allowed on the exception list.
12. Click **OK**.
13. *Save the Configuration File.*



## Use WebBlocker Actions in Proxy Definitions

The basic configuration you created with **Subscription Services > WebBlocker > Configure** is a WebBlocker action (a set of WebBlocker settings) that you can apply to an HTTP or HTTPS proxy definition. From Policy Manager, you can define additional WebBlocker actions if you want to apply different settings to different proxies.

### Define Additional WebBlocker Actions


1. Select **Setup > Actions > WebBlocker**.

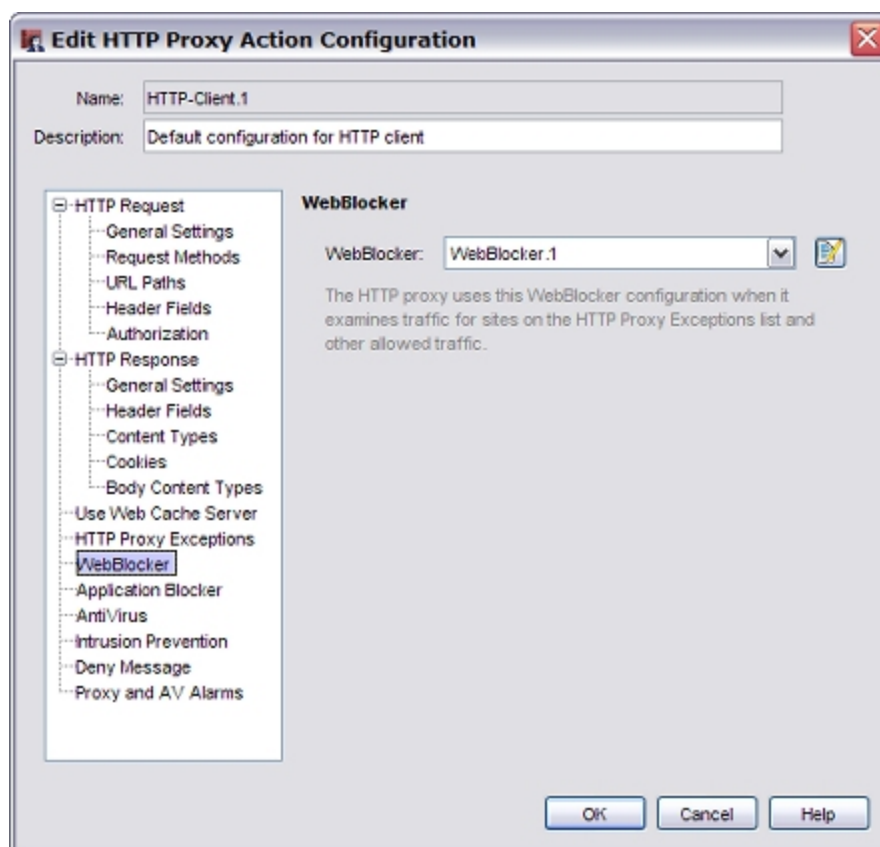
*The WebBlocker Configurations dialog box appears.*



2. Click **Add**. Or, to define a new action based on an existing one, select that action and click **Clone**.
3. Configure the WebBlocker action as described in *Configure WebBlocker* on page 1077.

### Add WebBlocker Actions to a Policy

1. Double-click the HTTP-Proxy policy.  
*The Edit Policy Properties dialog box appears.*
2. Select the **Policy** tab.
3. Adjacent to the **Proxy action** drop-down list, click .  
*The HTTP Proxy Action Configuration dialog box appears.*



4. From the categories list, select **WebBlocker**.
5. From the **WebBlocker** drop-down list, select the WebBlocker action you want to apply.

For two examples of how to use WebBlocker actions with policies, see *Configure WebBlocker Policies for Groups with Firebox Authentication* and *Configure WebBlocker Policies for Groups with Active Directory Authentication* on page 1107.

## Schedule WebBlocker Actions

You can set an operating schedule for the policy. You can use the predefined settings in the drop-down list or create custom schedules. You use these time periods to set rules for when to block different web sites. For example, you can block sports web sites during usual business hours of operation, but allow users to browse at lunch time, evenings, and weekends.

To set a schedule for a policy:

1. Open the policy to edit it, and select the **Advanced** tab.
2. Select a schedule from the drop-down list, or click the **New/Clone** icon to make a new schedule.  
For more information, see *Create Schedules for XTM Device Actions* on page 386.
3. Configure an HTTP policy that uses the schedule.

You can also configure two HTTP or HTTPS policies, but create a schedule for only one of them. Each policy uses one of the proxy actions. Each of these proxy actions points to one of at least two WebBlocker actions.

# About WebBlocker Subscription Services Expiration

If your site uses WebBlocker, you must renew or disable the WebBlocker subscription as soon as it expires to prevent an interruption in web browsing. WebBlocker has a default setting that blocks all traffic when the connections to the server time out. When your WebBlocker expires, it no longer contacts the server. This appears to the XTM device as a server timeout. All HTTP traffic is blocked unless this default was changed before expiration.

To change this setting:

1. In the **WebBlocker Configuration** dialog box, select the **Advanced** tab.
2. In the **License Bypass** section, change the setting to **Allowed**.

## Examples

### Use WebBlocker Local Override

WebBlocker local override is a feature that allows a user to type an override password to go to a web site that is blocked by the WebBlocker policy. For example, in a school, a teacher could use the override password to allow a student to access an approved site that is blocked by WebBlocker content categories.

When a user tries to go to a site that is blocked by the WebBlocker policy, if local override is enabled, the user sees a deny message in the browser.



If the XTM device uses a self-signed certificate for authentication, the user can also see a certificate warning. We recommend that you install a trusted certificate on the XTM device for this purpose, or import the self-signed certificate on each client device.

To get access to the requested site, the user must type the override destination and the override password.

1. In the **Override destination** text box, type the URL to allow access to. By default, the override destination is set to the URL that was blocked. You can use wildcards in the override destination to

allow access to more than one site, or more pages in one site. Examples of override destinations that use wildcards:

*\*.amazon.com*

allows access to all subdomains. of amazon.com

*\*amazon.com*

allows access to all domain names that end with amazon.com, such as images-amazon.com

*www.amazon.com/books-used-books-textbooks/\**

allows access to only pages in that path

2. In the **Override Password** text box, type the override password configured in the WebBlocker profile.
3. Click **Submit**.

After the user types the correct override password, the XTM device allows access to the override destination until an authenticated user logs out, or until there is no traffic to a matching site for the amount of time specified in the WebBlocker local override inactivity timeout. You enable local override and set the local override inactivity timeout in the Advanced tab of the WebBlocker configuration.

For more information about how to configure WebBlocker local override, see *Define Advanced WebBlocker Options* on page 1084.

## Use a WebBlocker Server Protected by Another XTM Device

If you have XTM devices in different office locations, you can configure WebBlocker on a branch office device to use the WebBlocker Server protected by a central XTM device. There are two ways to configure this.

- Send the WebBlocker traffic over a BOVPN tunnel. This traffic is encrypted.
- Send the WebBlocker traffic in clear text through the Internet. This traffic is not encrypted.

In these procedures, the **central XTM device** is the device that protects the WebBlocker Server. The **branch office XTM device** is the device that you want to configure to use the WebBlocker Server protected by the central XTM device.

## Send WebBlocker Traffic Through the BOVPN Tunnel

If you have a BOVPN tunnel between two XTM devices, use these steps to send WebBlocker traffic through the tunnel. We recommend this configuration, because all traffic between the branch office device and the central WebBlocker Server is encrypted.

From Policy Manager, configure the WebBlocker Server address on each branch office XTM device.

1. Select **Subscription Services > WebBlocker > Configure**.  
*The Configure WebBlocker dialog appears.*



2. Select a Policy Name. Click **Configure**.

*The WebBlocker Configuration of Policy dialog box for that policy appears.*



3. Click **Add** to add a new WebBlocker Server IP address.  
Or, select an existing IP address. Click **Edit**.  
*The Edit WebBlocker Server dialog appears.*
4. In the **Server IP** text box, type the real (private) IP address of the WebBlocker Server protected by the central XTM device.

From Policy Manager, add a tunnel route to the WebBlocker Server in each branch office XTM device.

1. Select **VPN > Branch Office Tunnels**.

*The Branch Office IPSec Tunnels dialog appears.*



2. Select the tunnel to the central XTM device. Click **Edit**.  
*The Edit Tunnel dialog appears.*
3. On the **Addresses** tab, click **Add**.  
*The Tunnel Route Settings dialog appears.*



4. In the **Local** text box, type the external IP address of this branch office XTM device.
5. In the **Remote** text box, type the private IP address of the WebBlocker Server.
6. Save the configuration to the device.

From Policy Manager, on the central XTM device, add a tunnel route from the WebBlocker Server to each branch office XTM device.

1. Select **VPN > Branch Office Tunnels**.
2. Click the tunnel to the branch office XTM device to select it. Click **Edit**.

3. On the **Addresses** tab, click **Add**.
4. In the **Local** text box, type the private IP address of the WebBlocker Server.
5. In the **Remote** text box, type the external IP address of the branch office XTM device.
6. If you have more than one branch office XTM device that you want to use this WebBlocker Server, repeat these steps to create a tunnel route from the WebBlocker Server to each branch office XTM device.
7. Save the configuration to the device.

The branch office XTM device can now use the WebBlocker Server protected by the central XTM device over the encrypted VPN tunnel.

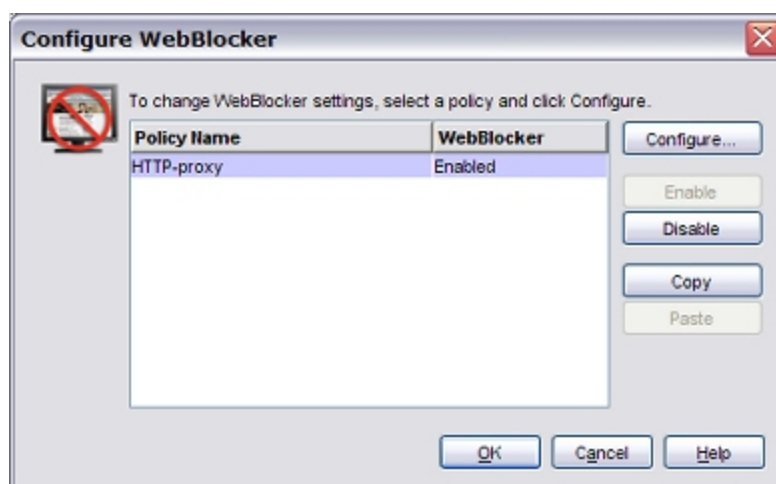
## Send WebBlocker Traffic Unencrypted Over the Internet

We do not recommend you send WebBlocker traffic unencrypted over the Internet. This procedure can be useful if you need a secondary path to the WebBlocker Server when a VPN tunnel is not available. For more about configuring a secondary connection, see [configure a backup connection to the WebBlocker Server](#) below.

From Policy Manager, configure the WebBlocker Server address on each branch office XTM device.

1. Select **Subscription Services > WebBlocker > Configure**.

*The Configure WebBlocker dialog appears.*



2. Select a Policy Name. Click **Configure**.

*The WebBlocker Configuration of Policy dialog for that policy appears.*

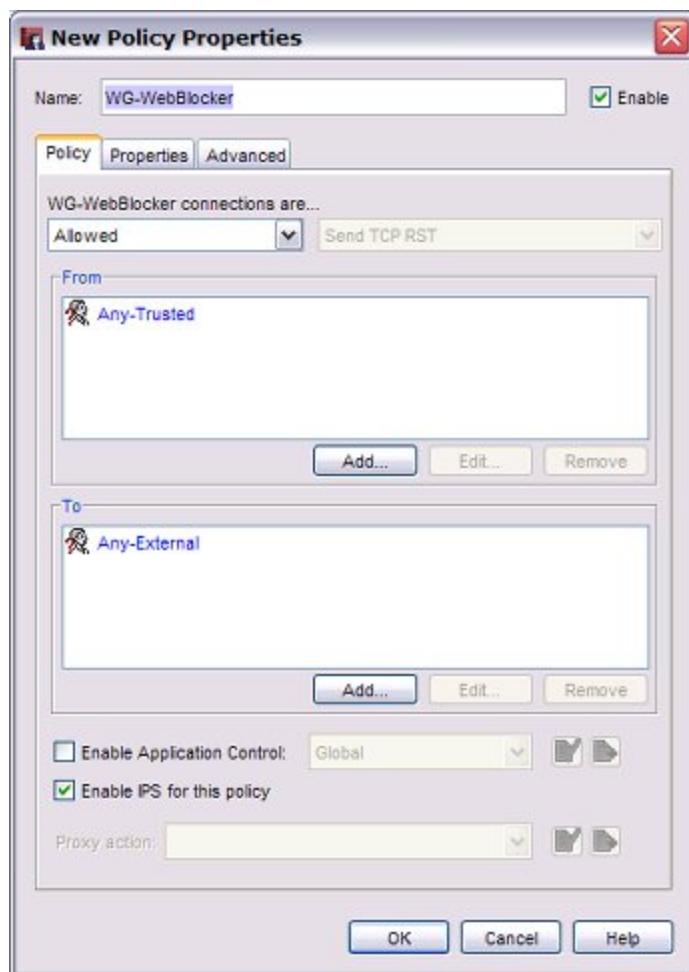


3. Click **Add** to add a new WebBlocker Server IP address.  
Or, select an existing WebBlocker Server IP address. Click **Edit**.  
*The Edit WebBlocker Server dialog appears.*
4. In the **Server IP** text box, type the external IP address of the central XTM device that protects the WebBlocker Server.
5. Click **OK**.
6. Save the configuration to the device.

From Policy Manager, configure the WB-WebBlocker policy on the central XTM device.

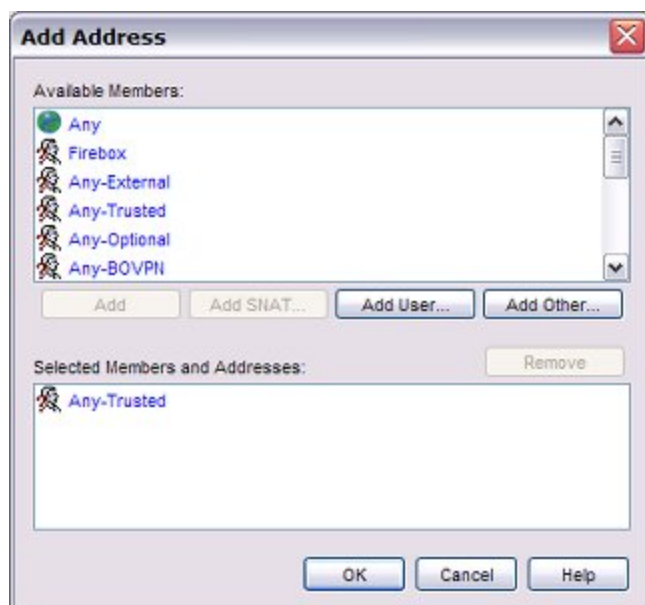
1. Select **Edit > Add Policy**.
2. Expand the **Packet Filters** folder.
3. Double-click the **WG-WebBlocker** policy to add it.  
*The New Policy Properties dialog appears.*





4. In the **From** section, click **Any-Trusted**. Click **Remove**.
5. In the **From** section, click **Add**.

*The Add Address dialog appears.*



6. If the branch office XTM device has a dynamic external IP address, in the **Available Members** list, select **Any-External**. Click **Add**.
7. If the branch office XTM device has a static external IP address, use these steps to add the Host IP address for each XTM device that will use this WebBlocker Server.
  - Click **Add Other**.
  - From the **Choose type** drop-down list, select **Host-IP**.
  - In the **Value** text box, type the external IP address of the branch office XTM device. Click **OK**.
8. Click **OK** to close the **Add Address** dialog box.
9. In the New Policy Properties dialog box, in the **To** section, select **Any-External**. Click **Remove**.
10. Click **Add**.

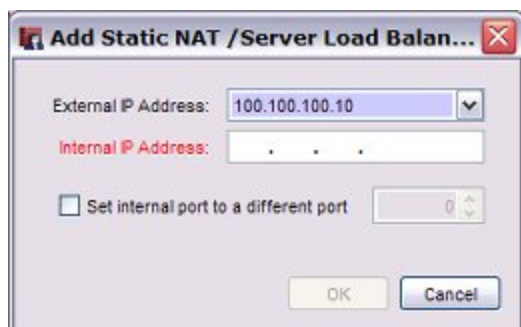
*The Add Address dialog appears.*
11. Click **Add SNAT**.

*The Add SNAT dialog box appears.*
12. Click **Add**.

*The Add SNAT dialog box appears.*



13. In the **SNAT Name** text box, type a name to identify this static NAT action.
14. Click **Add**.



15. From the **External IP Address** drop-down list, select the external interface IP address.
16. In the **Internal IP Address** text box, type the private IP address of the WebBlocker Server. Click **OK**.

17. Save the configuration to the device.

The branch office XTM device can now use the WebBlocker Server protected by the central XTM device.

## Configure a Backup Connection to the WebBlocker Server

If you configure a XTM device to send WebBlocker queries over the VPN tunnel, and the VPN tunnel goes down, WebBlocker loses access to the WebBlocker Server. For redundancy, you can use the Internet as a secondary path to the WebBlocker Server.

If you configure two connections, make sure that you configure WebBlocker on the branch office XTM device to use the private IP address of the WebBlocker Server as the first WebBlocker Server in the list.



With this redundant configuration, WebBlocker on the branch office XTM device always tries to get access to the WebBlocker Server with the VPN tunnel first. If it cannot connect to the WebBlocker Server over the VPN tunnel, it tries to connect outside the tunnel.

## Configure WebBlocker Policies for Groups with Active Directory Authentication

Many organizations want to allow different levels of access to web sites for different groups of users. To do this, you must first set up user authentication. You can then set up different WebBlocker settings for each group of users. At a high level, the steps are:

- Enable and configure Active Directory authentication.
- Define the user groups to match the user group names on your Active Directory server.
- Add policies for each user group. The policy includes WebBlocker configuration settings for that group.
- Remove or modify the default Outgoing policy.
- Configure authentication settings to automatically redirect users to the WatchGuard authentication page.
- (Optional) Configure Single Sign-On (SSO).

## Example Scenario

To show how to set up this configuration, we use a school that wants to set different levels of web access for three groups:

- Students (more restricted access)
- Teachers (less restricted access)
- IT (unrestricted access)


## Configure User Authentication

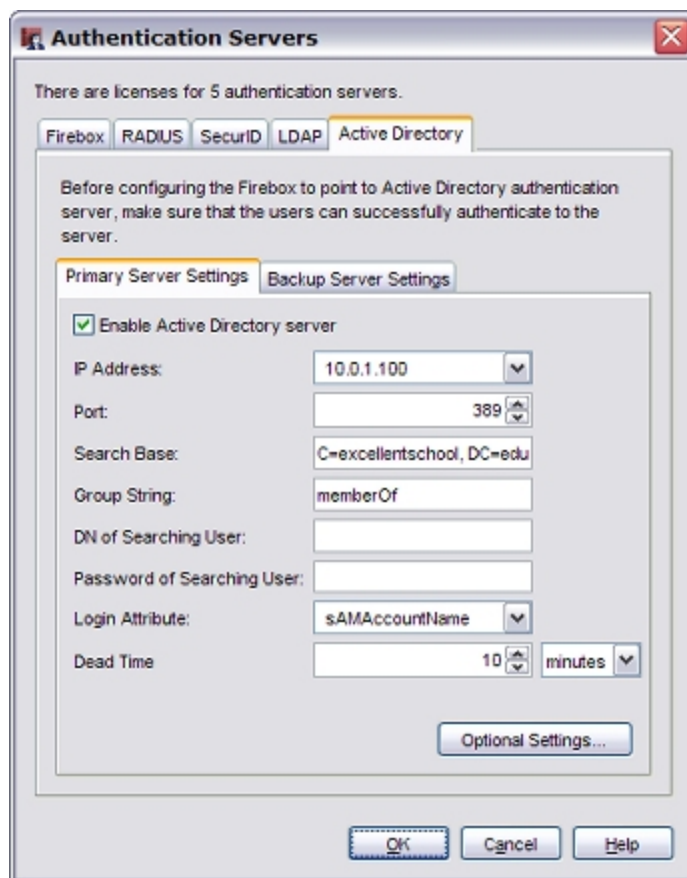
Before you configure WebBlocker settings, you must set up user authentication. You can use any authentication method, such as Active Directory, local authentication, Radius, or LDAP. For more information about the supported authentication methods, see *Authentication Server Types* on page 328. In this example, we assume the school wants to use Active Directory authentication with Single Sign-On.

## Enable Active Directory Authentication

You can use an Active Directory authentication server so that users can authenticate to your XTM device with their current network credentials. Before you configure your XTM device to use Active Directory authentication, make sure your users can successfully authenticate to the Active Directory server.

For this example, we use Policy Manager to configure the device to use the school's Active Directory server at the IP address 10.0.1.100.

1. Click .  
Or, select **Setup > Authentication > Authentication Servers**.  
*The Authentication Servers dialog box appears.*
2. Select the **Active Directory** tab.



3. Select the **Enable Active Directory server** check box.
4. In the **IP Address** text box, type the IP address of the primary Active Directory server.  
For this example, type 10.0.1.100.

The Active Directory server can be located on any XTM device interface. You can also configure the device to use an Active Directory server available through a VPN tunnel.

5. In the **Port** text box, type or select the TCP port number used to connect to the Active Directory server. The default port number is 389.

If your Active Directory server is a global catalog server, it can be useful to change the default port. For more information, see *Change the Default Port for the Active Directory Server* on page 355.

6. In the **Search Base** text box, type the location in the directory to begin the search.

The standard format for the search base setting is: ou=<name of organizational unit>,dc=<first part of the distinguished server name>,dc=<any part of the distinguished server name that appears after the dot>.

You set a search base to put limits on the directories on the authentication server the XTM device uses to search for an authentication match. We recommend that you set the search base to the root of the domain. This enables you to find all users and all groups to which those users belong.

For this example, the root domain name in the Active Directory database is **excellentschool.edu**, so for the Search Base, we type C=excellentschool,DC=edu.

For more information about how to find your search base on the Active Directory server, see *Find Your Active Directory Search Base* on page 354.

7. In the **Group String** text box, type the attribute string that is used to hold user group information on the Active Directory server. If you have not changed your Active Directory schema, the group string is always `memberOf`.
8. In the **DN of Searching User** text box, type the distinguished name (DN) for a search operation.

It is not necessary to enter anything in this text box if you keep the login attribute of `sAMAccountName`. If you change the login attribute, you must add a value in the **DN of Searching User** field to your configuration. You can use any user DN with the privilege to search LDAP/Active Directory, such as *Administrator*. However, a weaker user DN with only the privilege to search is usually sufficient.

9. In the **Password of Searching User** field, type the password associated with the distinguished name for a search operation.
10. In the **Login Attribute** text box, type an Active Directory login attribute to use for authentication.

The login attribute is the name used to connect to the Active Directory database. The default login attribute is `sAMAccountName`. If you use `sAMAccountName`, you can leave the **DN of Searching User** field and the **Password of Searching User** empty.

11. Click the **Dead Time** field up or down arrow to set a time after which an inactive server is marked as active again. Select **minutes** or **hours** from the adjacent drop-down list to set the duration.

After an authentication server has not responded for a period of time, it is marked as inactive. Subsequent authentication attempts do not use this server until it is marked as active again.

12. Click **OK**.
13. *Save the Configuration File.*

## Define the Authorized Users and Groups

Before you can use the Active Directory groups in policies, you must use Policy Manager to define the groups in the XTM device configuration. The group names you add must match the groups on your Active Directory server.

1. Select **Setup > Authentication > Authorized Users/Groups**.  
*The Authorized Users and Groups dialog box appears.*
2. Click **Add**.  
*The Define New Authorized User or Group dialog box appears.*



3. In the **Name** text box, type the name of the group on the Active Directory Server.  
For this example, the students are in the Active Directory group called Students, so we type Students.
4. (Optional) In the **Description** text box, type a description of the group.
5. Make sure that the **Type** is set to **Group**.
6. From the **Auth Server** drop-down list, select **Active Directory**.

Repeat these steps to create groups for **Teachers** and **IT**.

## Create an HTTP-proxy Policy for the Students

The XTM device uses two categories of policies to filter network traffic: *packet filters* and *proxies*.

### *Packet filter policy*

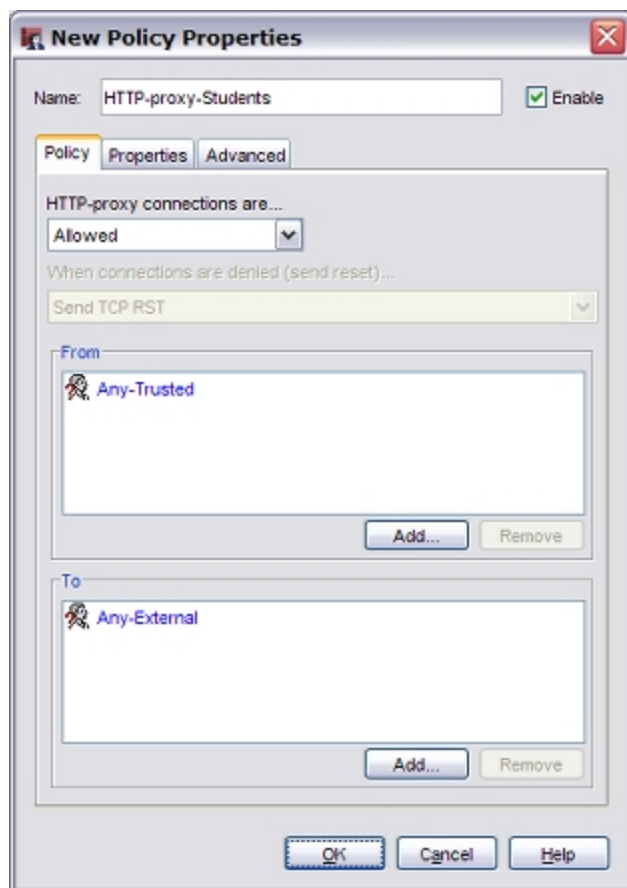
A packet filter examines each packet's IP and TCP/UDP header. If the packet header information is permitted by the packet filter settings, then the XTM device allows the packet. Otherwise, the XTM device drops the packet.

### *Proxy policy*

A proxy examines both the header information and the content of each packet. If the packet header information and the content of the packet is allowed by the proxy settings, then the XTM device allows the packet. Otherwise, the XTM device drops the packet.

To block access to categories of web sites for a group of users, you must use Policy Manager to create an HTTP proxy policy for those users, and define a WebBlocker action for that policy. The HTTP proxy can then inspect the content and allow or deny the users access to a web site based on the WebBlocker categories configured for that policy.

1. Select **Edit > Add Policies**.  
*The Add Policies dialog box appears.*
2. Expand the **Proxies** folder and select **HTTP-proxy**. Click **Add**.  
*The New Policy Properties dialog box appears.*

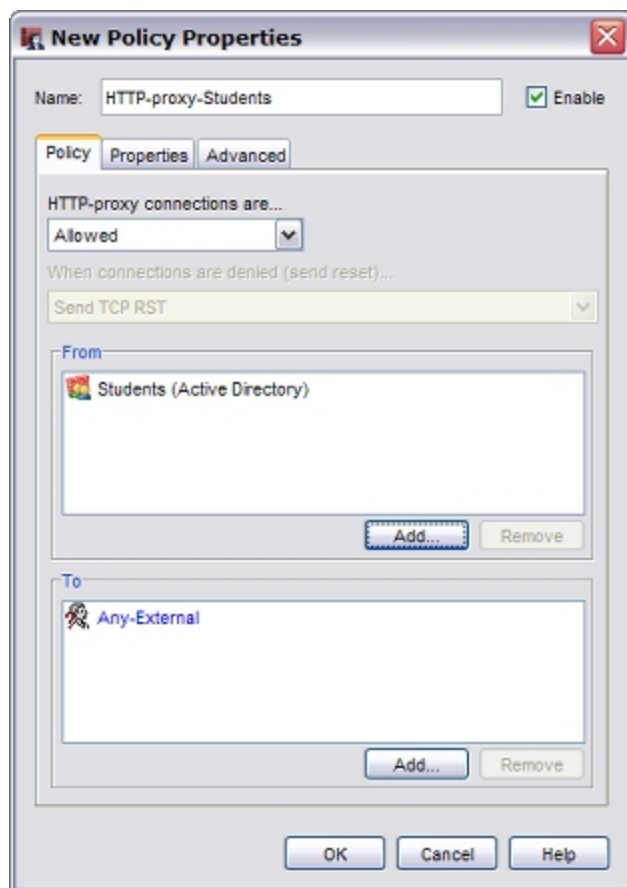



3. Change the name of the proxy policy to describe the group it applies to. In this example, we call the proxy policy **HTTP-proxy-Students**.
4. On the **Policy** tab, in the **From** section, click **Any-Trusted**. Then, click **Remove**.
5. In the **From** section, click **Add** to add the user group for this policy.  
*The Add Address dialog appears.*
6. Click **Add User**. Select **Firewall** and **Group** from the drop-down lists.  
*The Add Authorized Users or Groups dialog box appears.*



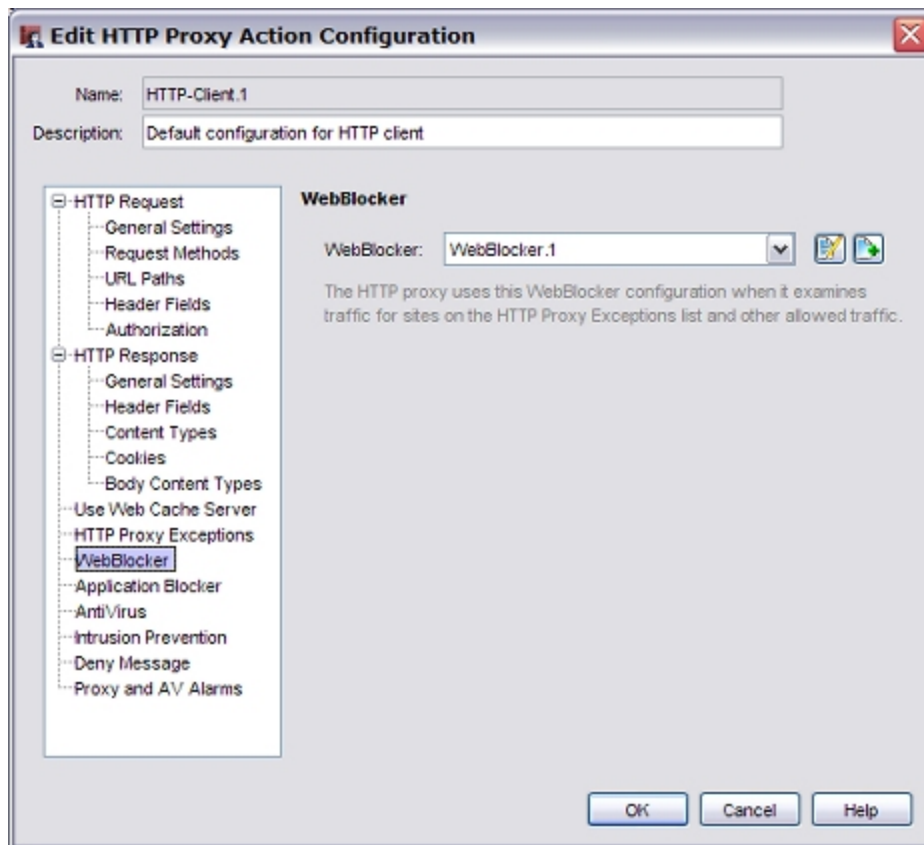
7. Select the **Students** group. Click **Select**, then click **OK**.  
*The New Policy Properties dialog box appears with the group Students (Active Directory) in the From section of the policy.*




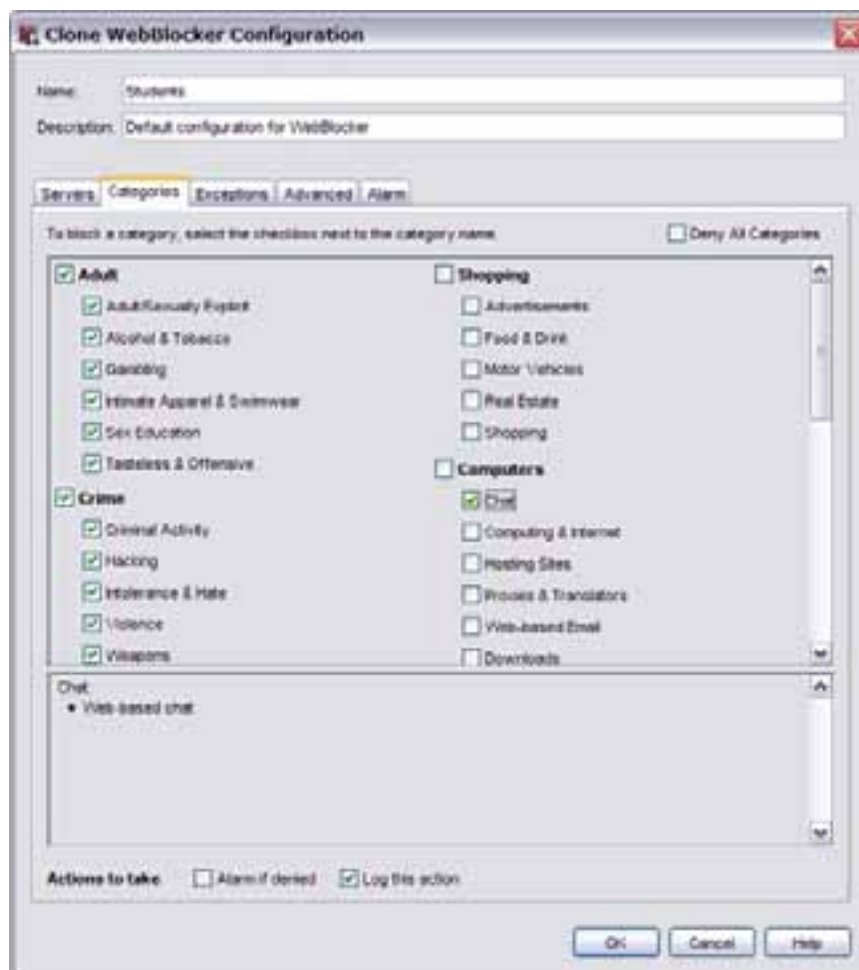


8. Select the **Properties** tab.
9. Click .

*The HTTP Proxy Action Configuration dialog box appears.*



10. From the categories list, select **WebBlocker**.  
*The WebBlocker configuration appears.*
11. Adjacent to the **WebBlocker** drop-down list, click .  
*The New WebBlocker Configuration dialog box appears.*

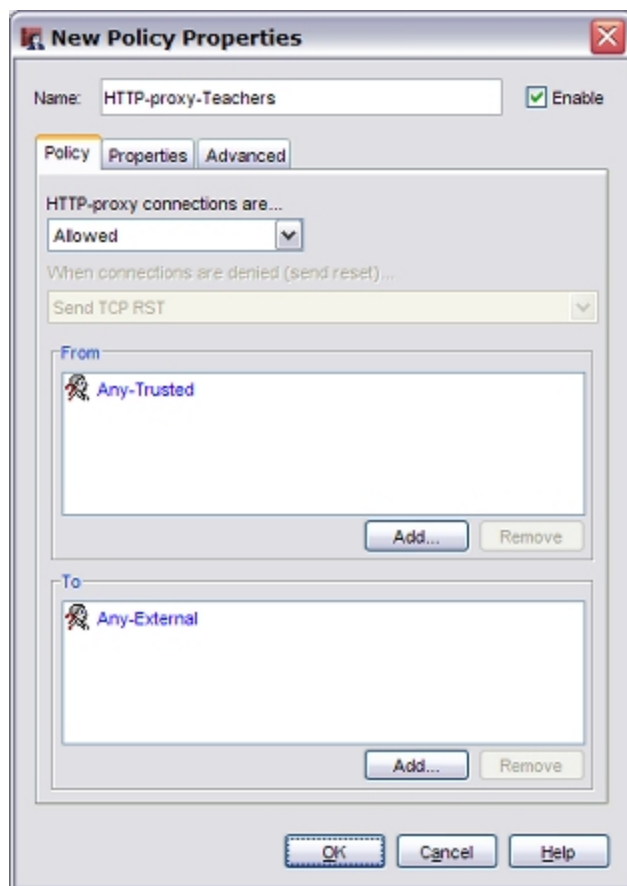


12. In the **Name** text box, type a name for this WebBlocker configuration.  
For this example, give this configuration the name **Students**.
13. On the **Servers** tab, click **Add**, and type the IP address of the WebBlocker server.
14. Select the **Categories** tab to show the categories of content that can be blocked.
15. Select the check box for each content category that you want to block for users in the **Students** group.

## Create an HTTP-proxy Policy for the Teachers

From Policy Manager, repeat the same steps to set up a different policy for the **Teachers** group.

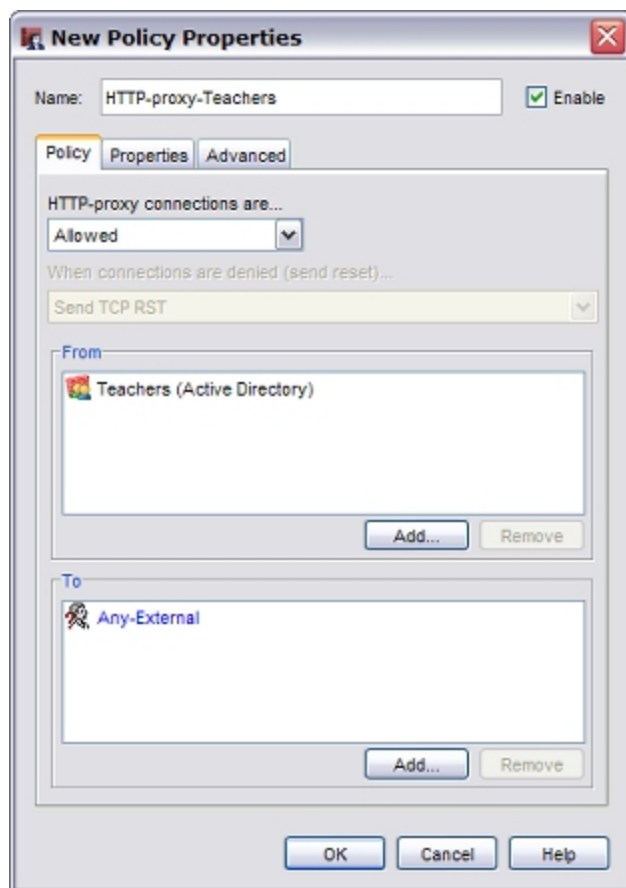
1. Select **Edit > Add Policies**.  
*The Add Policies dialog box appears.*
2. Expand the **Proxies** folder and select **HTTP-proxy**. Click **Add**.  
*The New Policy Properties dialog box appears.*




3. Change the name of the proxy policy to describe the group it applies to.  
In this example, we call the proxy policy HTTP-proxy-Teachers.
4. On the **Policy** tab, in the **From** section, click **Any-Trusted**. Then click **Remove** to remove it.
5. In the **From** section, click **Add** to add the user group for this policy.  
For this example, add the group **Teachers**.
6. Click **Add User**. Select **Firewall** and **Group** from the drop-down lists.  
*The Add Authorized Users or Groups dialog box appears.*




7. Select the **Teachers** group. Click **Select**, then click **OK**.  
*The New Policy Properties dialog box appears with the group Teachers (Active Directory) in the From section of the policy.*

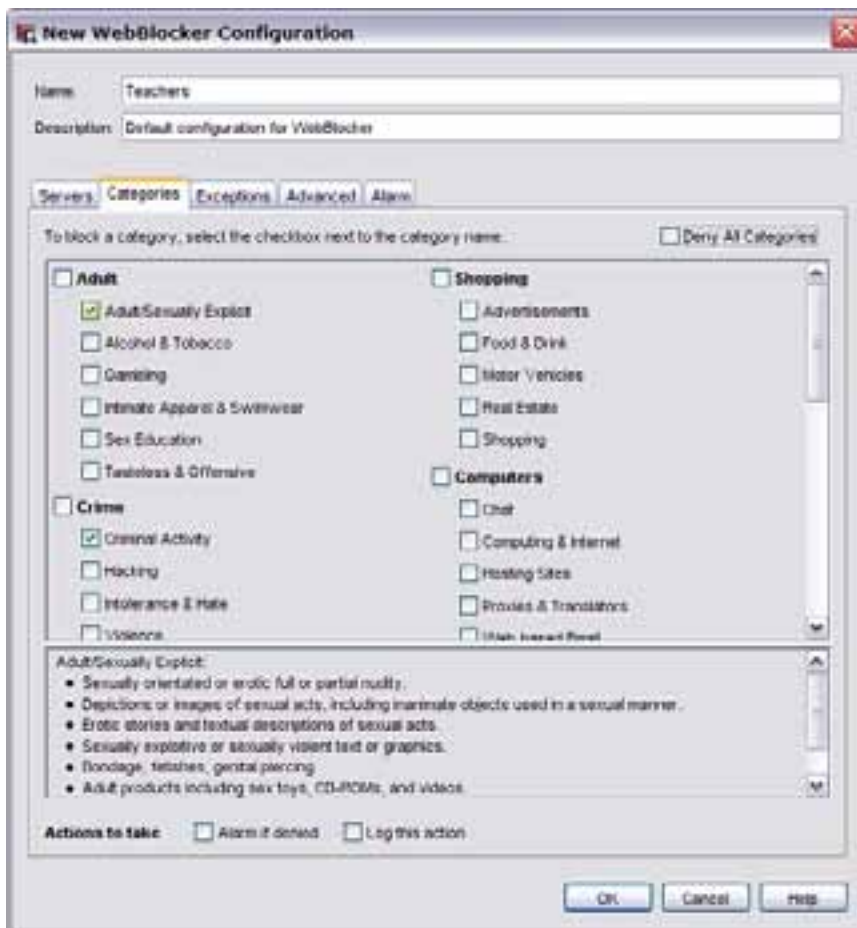


8. In the **New Policy Properties** dialog box, select the **Properties** tab.
9. Click .
 

*The HTTP Proxy Action Configuration dialog box appears.*
10. From the categories list, select **WebBlocker**.
 

*The WebBlocker configuration appears.*
11. Adjacent to the **WebBlocker** drop-down list, click .
 

*The New WebBlocker Configuration dialog box appears.*
12. In the **Name** text box, type a name for this WebBlocker configuration.  
In this example, we use the name Teachers.
13. On the **Servers** tab, click **Add**, and type the IP address of the WebBlocker server.
14. Select the **Categories** tab to see the categories of content that can be blocked.

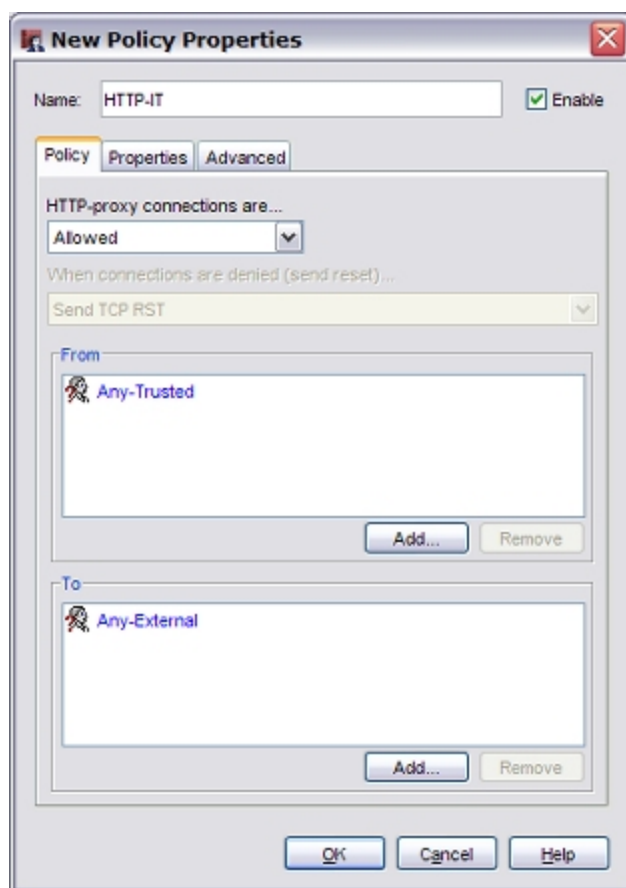


15. Select the check box for each content category that you want to block for users in the **Teachers** group.
16. Click **OK**.

## Create an HTTP Packet Filter Policy for the IT Group

The IT team needs unrestricted access to the Internet. Because we do not need a policy to inspect the content of HTTP packets for these users, we use Policy Manager to create an HTTP packet filter policy instead of an HTTP proxy policy.

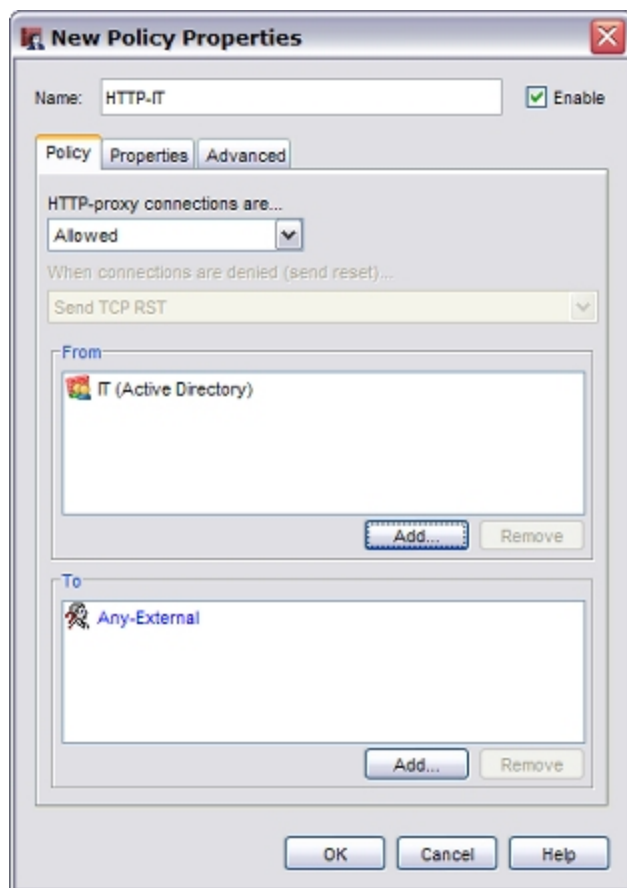
1. Select **Edit > Add Policies**.  
*The Add Policies dialog box appears.*
2. Expand the **Packet Filters** folder and select **HTTP**. Click **Add**.  
*The New Policy Properties dialog box appears.*



3. Change the name of the proxy policy to describe the group it applies to. In this example, we call the proxy policy HTTP-IT.
4. On the **Policy** tab, in the **From** list, select **Any-Trusted**. Then click **Remove** to remove it.
5. In the **From** section, click **Add** to add the user group for this policy. For this example, add the group **IT**.
6. Click **Add User**. Select **Firewall** and **Group** from the drop-down lists. *The Add Authorized Users or Groups dialog box appears.*



7. Select the **IT** group. Click **Select**, then click **OK**. *The New Policy Properties dialog box appears with the group IT (Active Directory) in the From section of the policy.*



8. Click **OK**.

Members of the IT group are no longer affected by WebBlocker restrictions.

## Remove or modify the Outgoing Policy

After you configure your HTTP proxy to add a WebBlocker profile, you must make sure that the default Outgoing policy does not allow network clients to visit web sites without user authentication. To do this, you can use Policy Manager to either remove the Outgoing policy and add any other outgoing network policies you need, or you can edit the Outgoing policy to add your WebBlocker authentication user groups. Both options are explained below.

### Option 1: Remove the Outgoing Policy and Add Other Outgoing Network Policies

This is the option we recommend if you want increased control over outbound network access. You must know what ports and protocols are necessary to meet the needs of your organization.

First, remove the Outgoing policy:

1. Select the **Outgoing** policy.
2. Select **Edit > Delete Policy**.
3. Click **Yes** to confirm.

Then, add a DNS packet filter policy to allow outbound DNS queries:



1. Select **Edit > Add Policies**.  
*The Add Policies dialog box appears.*
2. Expand the **Packet Filters** folder and select **DNS**. Click **Add**.  
*The New Policy Properties dialog box appears.*
3. Add all of your internal networks to the **From** section of the policy.
4. Click **OK** to save the policy.

Finally, add other custom policies:

Add custom policies for any other necessary outgoing traffic. Examples of other custom policies you may want to add include:

- UDP
- SMTP (if you have a mail server)

For information about how to add a custom policy, see *About Custom Policies* on page 388.

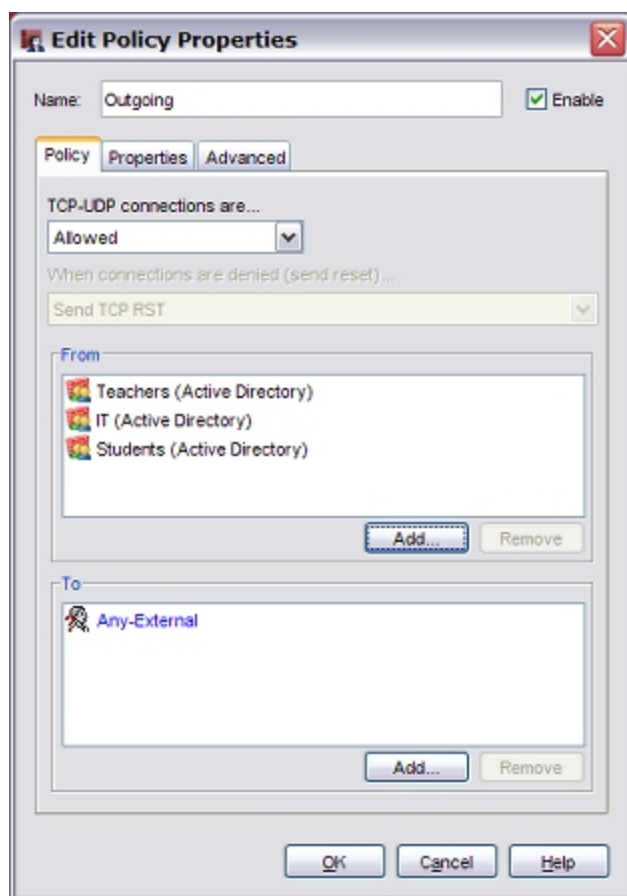
## Option 2: Add Your User Authentication Groups to the Outgoing Policy

If you are not sure what other outgoing ports and protocols are necessary for your business, or if you are comfortable with the same level of outbound control you have when you use the default configuration, you can use Policy Manager to modify the Outgoing policy to add your authentication groups.

1. Double-click the **Outgoing** policy.  
*The Edit Policy Properties dialog box appears.*
2. In the **From** list, select **Any-Trusted**. Click **Remove**.
3. In the **From** list, select **Any-Optional**. Click **Remove**.
4. In the **From** section, click **Add**.  
*The Add Address dialog box appears.*
5. Click **Add User**. Select **Firewall** and **Group** from the drop-down lists.  
*The Add Authorized Users or Groups dialog box appears.*



6. Select one of the user authentication groups you created. Then click **Select**.
7. Repeat Steps 5–6 to add all of the authentication groups.
8. Click **OK**.  
*The Edit Policy Properties dialog appears for the Outgoing policy. The groups appear in the From section of the policy.*



## Automatically Redirect Users to the Login Portal

From Policy Manager, you can configure the global authentication settings to automatically send users who have not yet authenticated to the authentication login portal when they try to get access to the Internet.

1. Select **Setup > Authentication > Authentication Settings**.  
*The Authentication Settings dialog box opens.*
2. Select the **Auto redirect users to authentication page for authentication** check box.

WebBlocker is now configured to use different policies for different groups of authenticated users, and automatically redirects unauthenticated users to an authentication page.

## Configure Single Sign-On (SSO)

When users log on to computers on your network, they must give a user name and password. If you use Active Directory authentication on your XTM device to restrict outgoing network traffic to specified users or groups, they must also log on again when they manually authenticate to the device to access network resources such as the Internet. You can use Single Sign-On (SSO) to have users on the trusted or optional networks automatically authenticate to the XTM device when they log on to their computers.

To use SSO, you must install the SSO agent software on a computer in your domain. For an environment such as a school, where more than one person uses the same computer, we recommend that you install the SSO client software on each computer.

For more information about Single Sign-On, see *About Single Sign-On (SSO)* on page 312

## Configure WebBlocker Policies for Groups with Firebox Authentication

Many organizations want to allow different levels of access to web sites for different groups of users. To do this, you must first set up user authentication. You can then set up different WebBlocker settings for each group of users. At a high level, the steps are:

- Configure user authentication.
- Add the users to groups who you want to have different levels of access.
- Add an HTTP proxy policy for each group of users. The policy includes WebBlocker configuration settings for that group.
- Remove or modify the default Outgoing policy.
- Configure authentication settings to automatically redirect users to the WatchGuard authentication page.

### Example Scenario

To show how to set up this configuration, we use Policy Manager to configure WebBlocker policies for a school that wants to set different levels of web access for three groups:

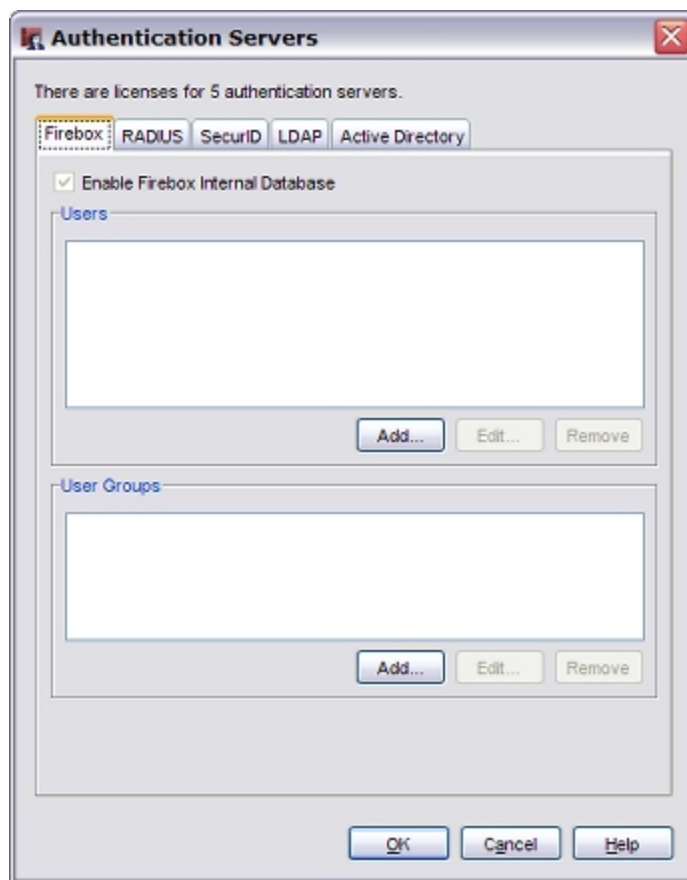
- Students (more restricted access)
- Teachers (less restricted access)
- IT (unrestricted access)

### Configure Authentication

Before you configure WebBlocker settings, you must set up user authentication. You can use any authentication method, such as Active Directory, local authentication, RADIUS, or LDAP. For information about the supported authentication methods, see *Authentication Server Types* on page 328. In this example, we assume the school wants to use Firebox authentication.

### Add users for Firebox Authentication

1. Select **Setup > Authentication > Authentication Servers**.  
*The Authentication Servers dialog box appears.*



2. On the **Firebox** tab, in the **Users** section, click **Add**.  
*The Setup Firebox User dialog box appears.*

3. Type the **Name** and (optional) a **Description** of the new user.  
*The Name is the user name used to authenticate. The name cannot contain a space.*
4. Type and confirm the **Passphrase** for the new user.

**Note** When you set this passphrase, the characters are masked and it does not appear in simple text again. If you lose the passphrase, you must set a new passphrase.

5. In the **Session Timeout** text box, type or select the maximum length of time the user can send traffic to the external network.  
  
The minimum setting for is one (1) seconds, minutes, hours, or days. The maximum value is 365 days.
6. In the **Idle Timeout** text box, type or select the length of time the user can stay authenticated when idle (not passing any traffic to the external network).  
  
The minimum setting is one (1) seconds, minutes, hours, or days. The maximum value is 365 days.
7. To close the **Setup Firebox User** dialog box, click **OK**.  
*The Authentication Servers dialog box appears, with the user name added to the Users list.*

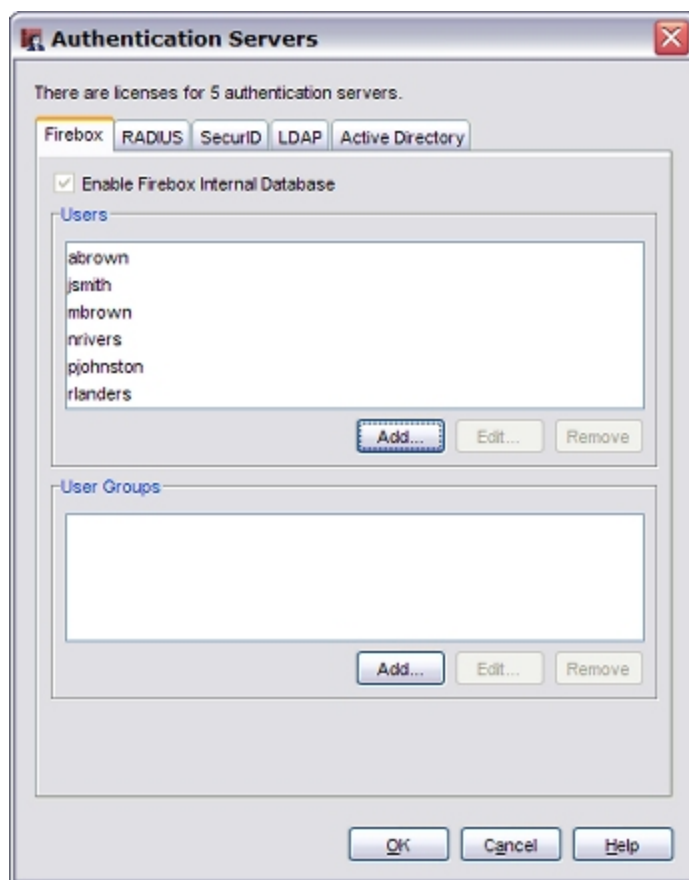
Repeat these steps to add each user to the Firebox authentication database. For this example, add all students, teachers, and members of the IT team.

## Define Firebox Authentication Groups

Next, you must define the user groups that correspond to the different WebBlocker policies you want to use. From Policy Manager, create a group for each different level of web site access you want to allow. In this example, we define three groups, *Teachers*, *Students* and *IT*.

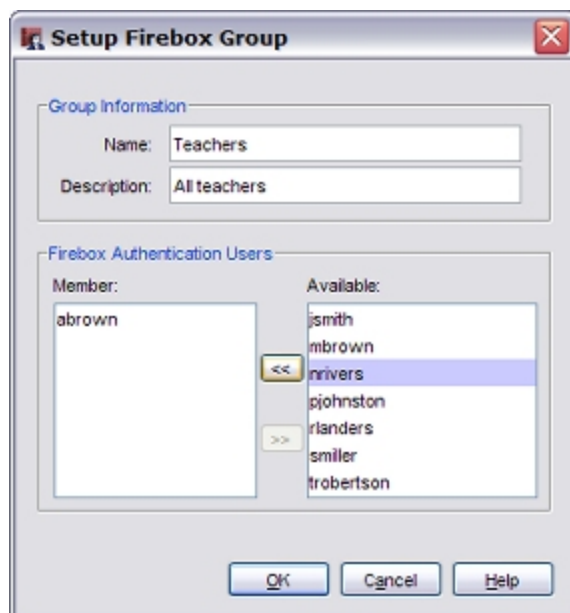
1. Select **Setup > Authentication > Authentication Servers**.


*The Authentication Servers dialog box appears.*

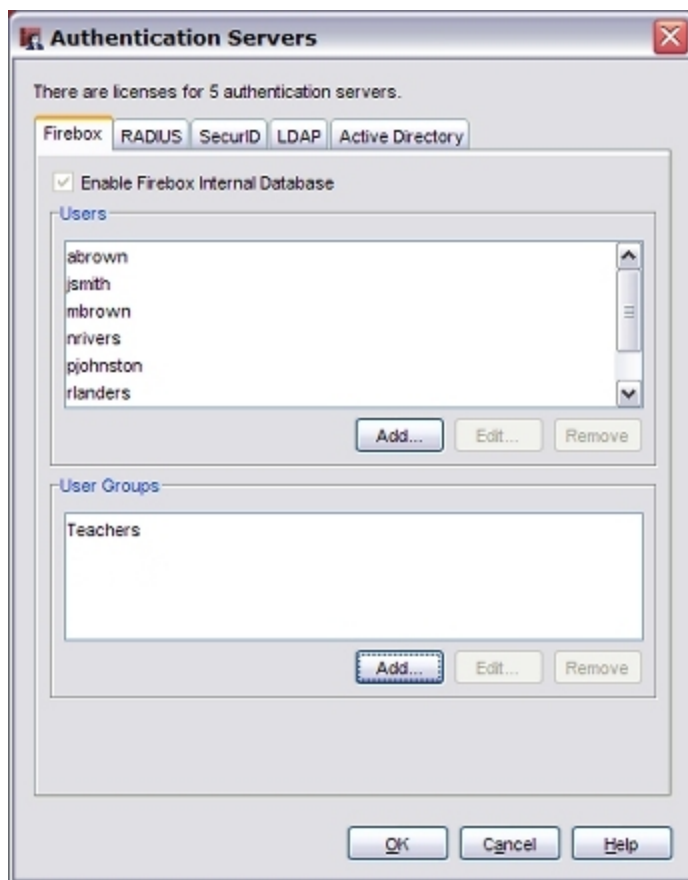


2. In the **User Groups** section, click **Add**.

*The Setup Firebox Group dialog box appears.*



4. Type a name for the group. For this example, the group name is Teachers.
5. (Optional) Type a description for the group.
6. Add the user names of all the teachers to this group. To add a user to the group, select the user name in the **Available** list. Click  to move the name to the **Member** list.  
*You can also double-click the user name in the Available list.*
7. After you add all of the teachers to the group, click **OK**.  
*The Authentication Servers dialog box appears with the Teachers user group added.*



Repeat the same steps to create a group called **Students** that contains the user names of all the students, and a group called **IT** that contains the user names of all members of the IT team.

## Create an HTTP-proxy Policy for the Students

The Firebox uses two categories of policies to filter network traffic: *packet filters* and *proxies*.

### *Packet filter policy*

A packet filter examines each packet's IP and TCP/UDP header. If the packet header information is permitted by the packet filter settings, then the Firebox allows the packet. Otherwise, the Firebox drops the packet.

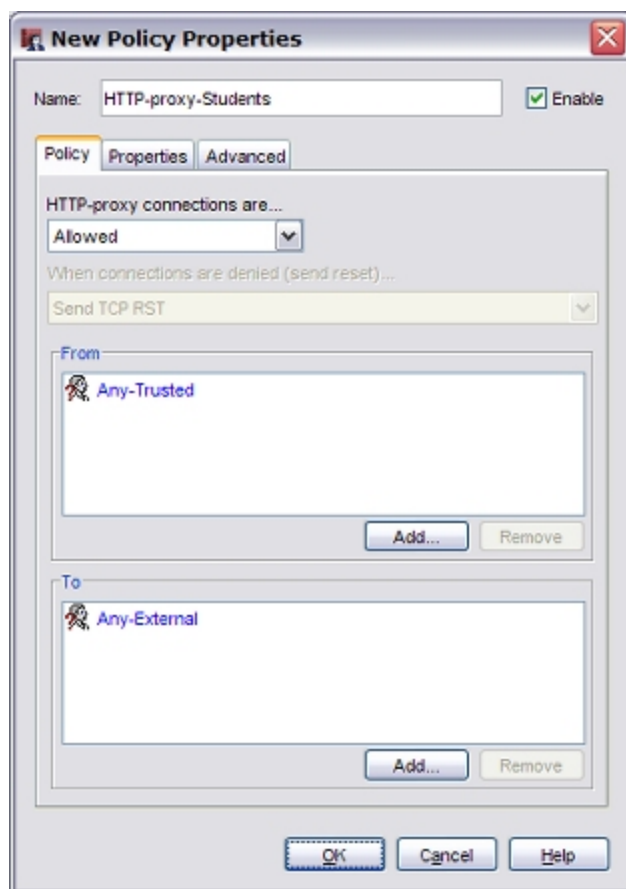
### *Proxy policy*

A proxy examines both the header information and the content of each packet. If the packet header information and the content of the packet is allowed by the proxy settings, then the Firebox allows the packet. Otherwise, the Firebox drops the packet.

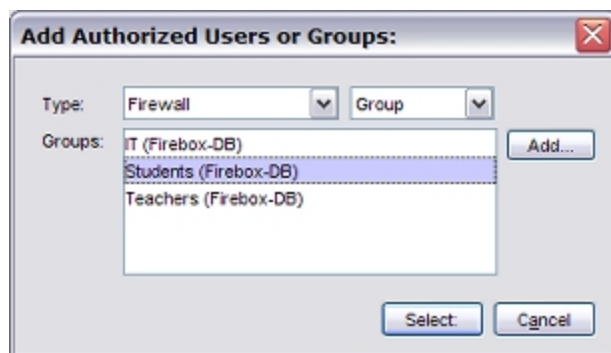
To block access to categories of web sites for a group of users, use Policy Manager to create an HTTP proxy policy for those users, and define a WebBlocker action for that policy. The HTTP proxy can then inspect the content and allow or deny the users access to a web site based on the WebBlocker categories configured for that policy.



1. Select **Edit > Add Policies**.  
*The Add Policies dialog box appears.*
2. Expand the **Proxies** folder and select **HTTP-proxy**. Click **Add**.  
*The New Policy Properties dialog box appears.*

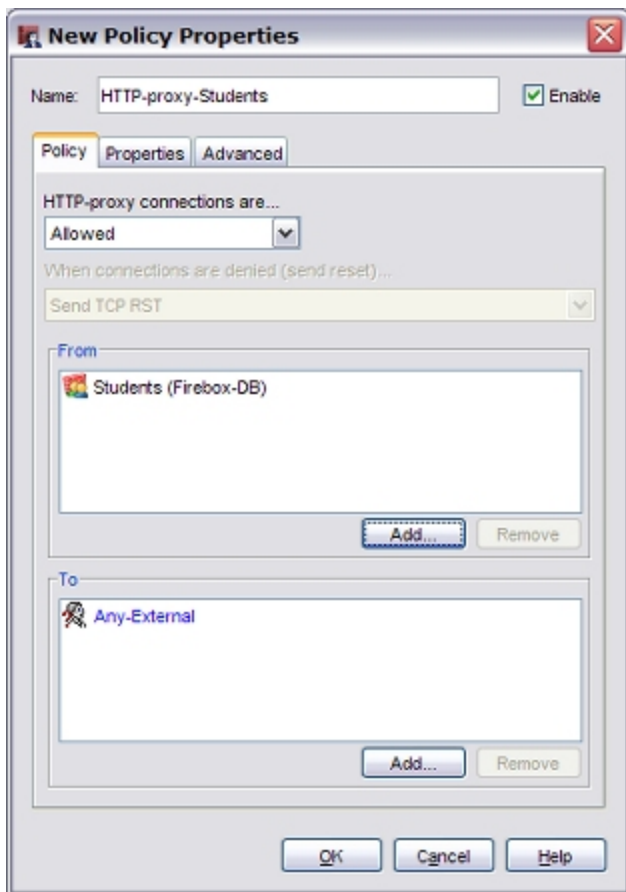



3. Change the name of the proxy policy to describe the group it applies to.  
In this example, we call the proxy policy HTTP-proxy-Students.
4. On the **Policy** tab, in the **From** list, select **Any-Trusted**. Click **Remove**.
5. In the **From** section, click **Add** to add the user group for this policy.  
*The Add Address dialog appears.*
6. Click **Add User**. Select **Firewall** and **Group** from the drop-down lists.  
*The Add Authorized Users or Groups dialog box appears.*



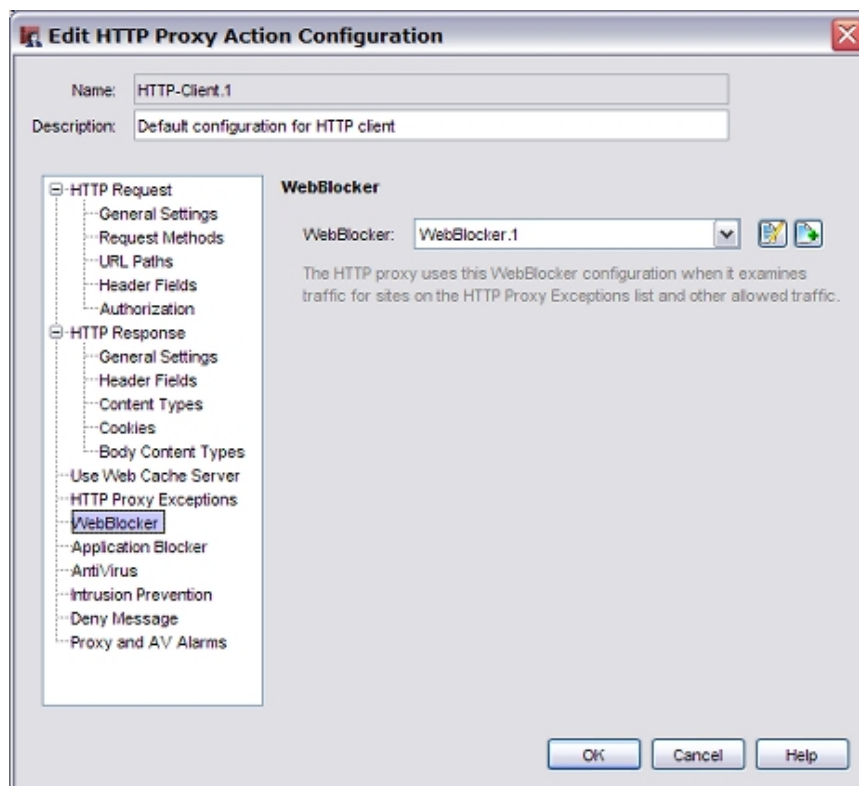
7. Select the **Students** group. Click **Select**, then click **OK**.


*The New Policy Properties dialog box appears with the group Students (Firebox-DB) in the From section of the policy.*

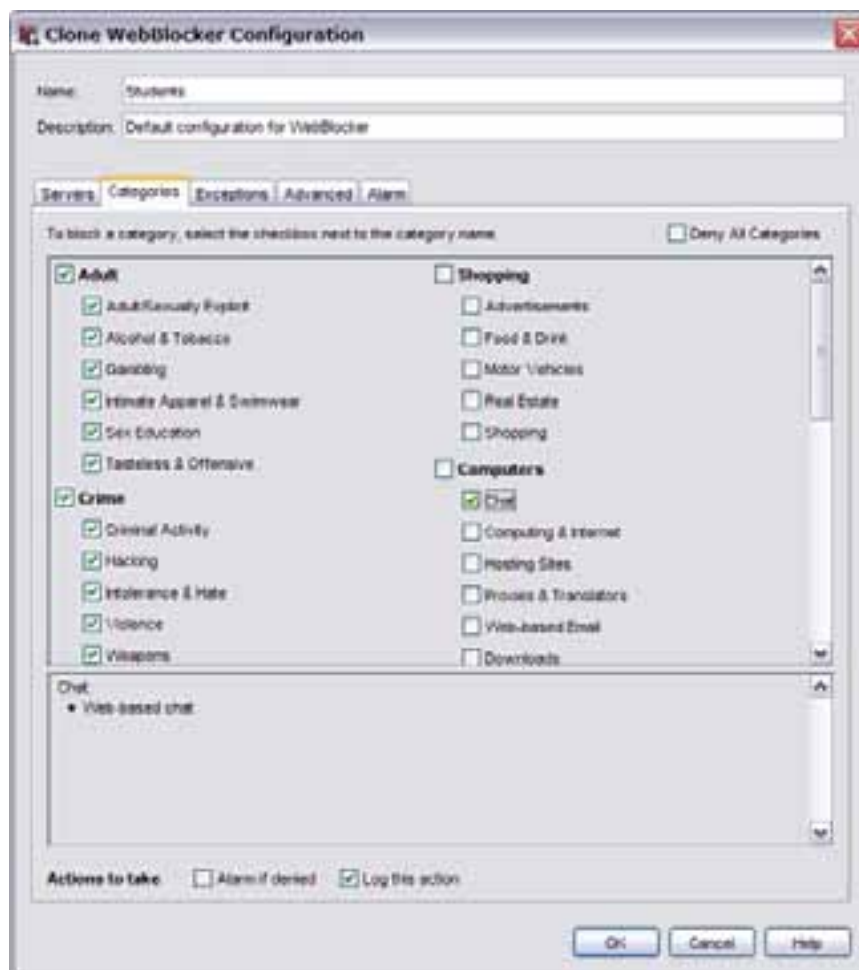


8. Select the **Properties** tab.
9. Click .

*The HTTP Proxy Action Configuration dialog box appears.*



10. From the categories list, select **WebBlocker**.  
*The WebBlocker configuration appears.*
11. Adjacent to the **WebBlocker** drop-down list, click .  
*The New WebBlocker Configuration dialog box appears.*

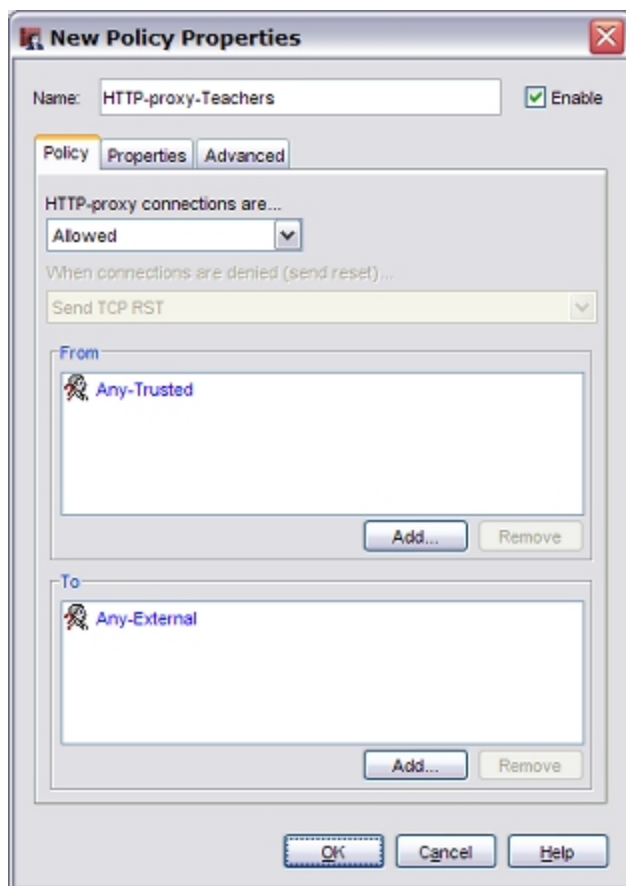


12. In the **Name** text box, type a name for this WebBlocker configuration.  
For this example, give this configuration the name **Students**.
13. On the **Servers** tab, click **Add**, and type the IP address of the WebBlocker server.
14. Select the **Categories** tab to show the categories of content that can be blocked.
15. Select the check box for each content category that you want to block for users in the **Students** group.

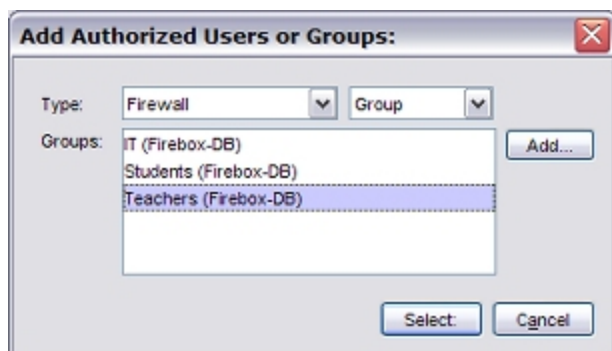
## Create an HTTP-proxy Policy for the Teachers

From Policy Manager, repeat the same steps to set up a different policy for the **Teachers** group.

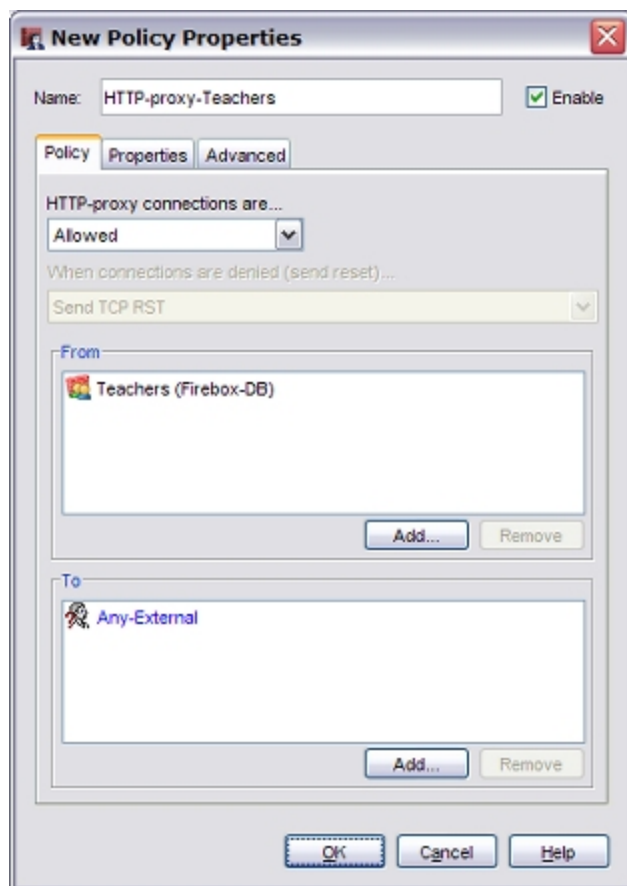
1. Select **Edit > Add Policies**.  
*The Add Policies dialog box appears.*
2. Expand the **Proxies** folder and select **HTTP-proxy**. Click **Add**.  
*The New Policy Properties dialog box appears.*





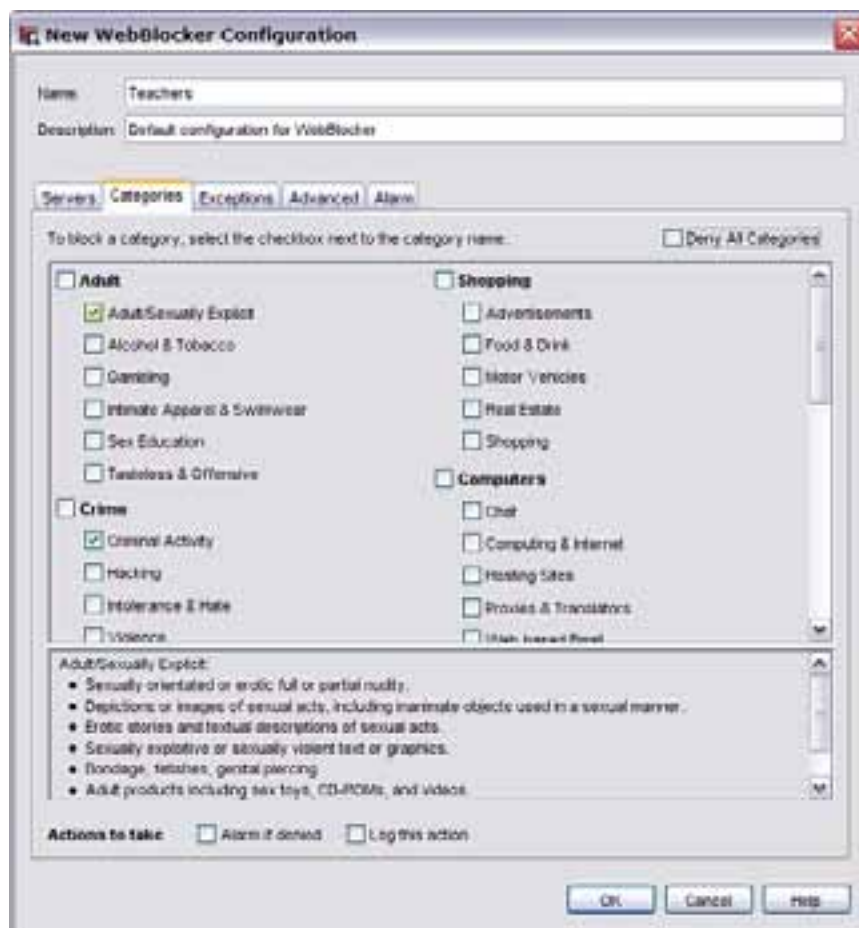
3. In the **Name** text box, type a descriptive name for the proxy policy to describe this group.  
For this example, type HTTP-proxy-Teachers.
4. On the **Policy** tab, in the **From** list, select **Any-Trusted**. Click **Remove**.
5. In the **From** section, click **Add** to add the user group for this policy.  
For this example, add the group **Teachers**.
6. Click **Add User**. Select **Firewall** and **Group** from the drop-down lists.  
*The Add Authorized Users or Groups dialog box appears.*



7. Select the **Teachers** group. Click **Select**. Click **OK**.  
*The New Policy Properties dialog box appears with the group Teachers (Firebox-DB) in the From section of the policy.*



8. Select the **Properties** tab.
9. Click .
- The HTTP Proxy Action Configuration dialog box appears.*
10. From the categories list, select **WebBlocker**.
- The WebBlocker configuration appears.*
11. Adjacent to the **WebBlocker** drop-down list, click .
- The New WebBlocker Configuration dialog box appears.*
12. In the **Name** text box, type a name for this WebBlocker configuration.  
In this example, we use the name Teachers.
13. On the **Servers** tab, click **Add**, then type the IP address of the WebBlocker server.
14. Select the **Categories** tab to see the categories of content that can be blocked.

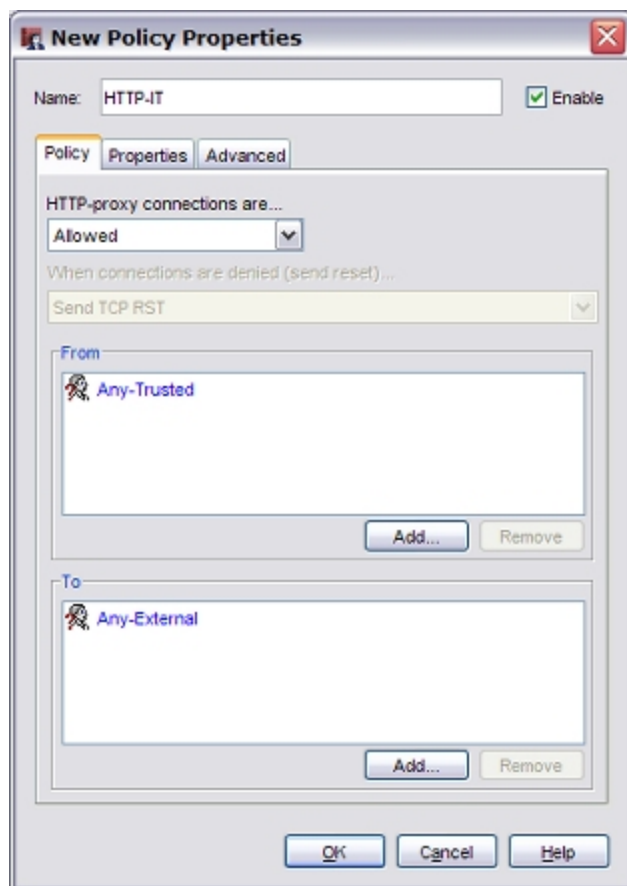


15. Select the check box for each content category that you want to block for users in the **Teachers** group.

## Create an HTTP Packet Filter Policy for the IT Group

The IT team needs unrestricted access to the Internet. Because we do not need a policy to inspect the content of HTTP packets for these users, we use Policy Manager to create an HTTP packet filter policy instead of an HTTP proxy policy.

1. Select **Edit > Add Policies**.  
*The Add Policies dialog box appears.*
2. Expand the **Packet Filters** folder and select **HTTP**. Click **Add**.  
*The New Policy Properties dialog box appears.*

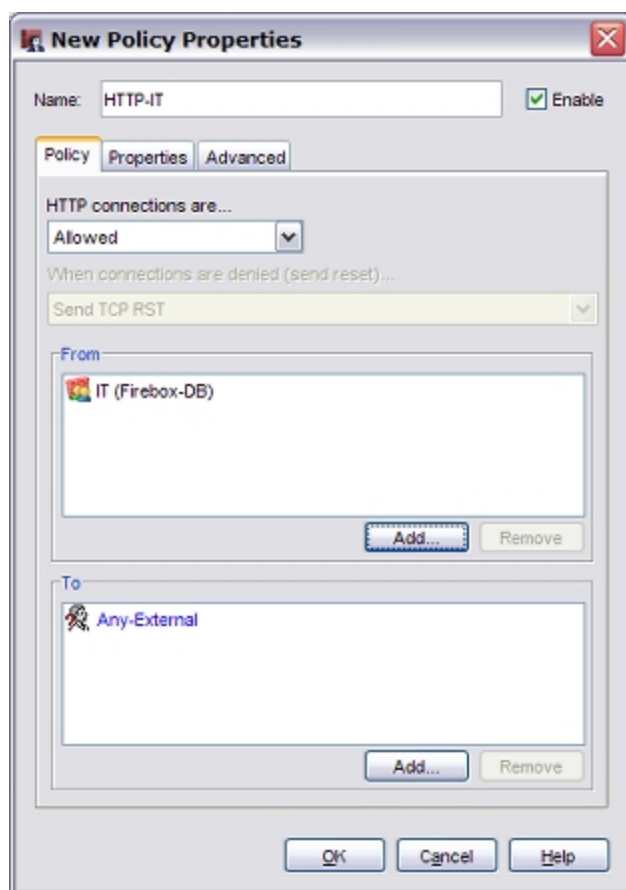


3. Change the name of the proxy policy to describe the group it applies to. In this example, we call the proxy policy HTTP-IT.
4. On the **Policy** tab, in the **From** section, select **Any-Trusted**. Click **Remove**.
5. In the **From** section, click **Add** to add the user group for this policy. For this example, add the group **IT**.
6. Click **Add User**. Select **Firewall** and **Group** from the drop-down lists. *The Add Authorized Users or Groups dialog box appears.*



7. Select the **IT** group. Click **Select**. Click **OK**. *The New Policy Properties dialog box appears with the group IT (Firebox-DB) in the From section of the policy.*





8. Click **OK**.

Members of the IT group are no longer affected by WebBlocker restrictions.

## Remove or Modify the Outgoing Policy

After you configure your HTTP proxy to add a WebBlocker profile, you must make sure that the default Outgoing policy does not allow network clients to visit web sites without user authentication. To do this, you can use Policy Manager to either remove the Outgoing policy and add any other outgoing network policies you need, or you can edit the Outgoing policy to add your WebBlocker authentication user groups. Both options are explained below.

### Option 1: Remove the Outgoing Policy and Add Other Outgoing Network Policies

This is the option we recommend if you want increased control over outbound network access. You must know what ports and protocols are necessary to meet the needs of your organization.

First, remove the Outgoing policy:

1. Select the **Outgoing** policy.
2. Select **Edit > Delete Policy**.
3. Click **Yes** to confirm.

Then, add a DNS packet filter policy to allow outbound DNS queries:

1. Select **Edit > Add Policies**.  
*The Add Policies dialog box appears.*
2. Expand the **Packet Filters** folder and select **DNS**. Click **Add**.  
*The New Policy Properties dialog box appears.*
3. Add all of your internal networks to the **From** section of the policy.
4. Click **OK** to save the policy.

Finally, add other custom policies:

Add custom policies for any other necessary outgoing traffic. Examples of other custom policies you may want to add include:

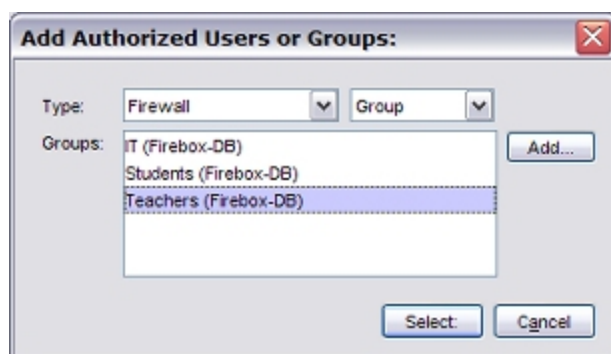
- UDP
- SMTP (if you have a mail server)

For information about how to add a custom policy, see *About Custom Policies* on page 388.

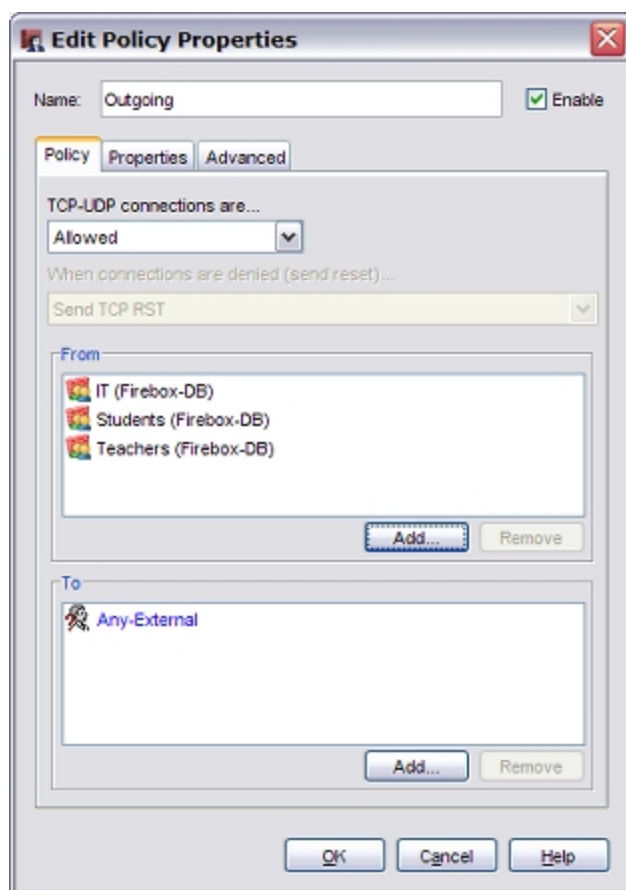
## Option 2: Add Your User Authentication Groups to the Outgoing Policy

If you are not sure what other outgoing ports and protocols are necessary for your business, or if you are comfortable with the same level of outbound control you have when you use the default configuration, you can modify the Outgoing policy to add your authentication groups.

1. Double-click the **Outgoing** policy.  
*The Edit Policy Properties dialog box appears.*
2. In the **From** list, select **Any-Trusted**. Click **Remove**.
3. In the **From** list, select **Any-Optional**. Click **Remove**.
4. In the **From** section, click **Add**.  
*The Add Address dialog box appears.*
5. Click **Add User**. Select **Firewall** and **Group** from the drop-down lists.  
*The Add Authorized Users or Groups dialog box appears.*



6. Select one of the user authentication groups you created. Click **Select**.
7. Repeat Steps 5–6 to add all of the authentication groups.
8. Click **OK**.  
*The Edit Policy Properties dialog appears for the Outgoing policy. The groups appear in the From section of the policy.*



## Automatically Redirect Users to the Login Portal

From Policy Manager, you can configure the global authentication settings to automatically send users who have not yet authenticated to the authentication login portal when they try to get access to the Internet.

1. Select **Setup > Authentication > Authentication Settings**.  
*The Authentication Settings dialog box opens.*
2. Select the **Auto redirect users to authentication page for authentication** check box.

WebBlocker is now configured to use different policies for different groups of authenticated users, and automatically redirects unauthenticated users to an authentication page.



# 32 spamBlocker

---

## About spamBlocker

Unwanted email, also known as spam, fills the average Inbox at an astonishing rate. A large volume of spam decreases bandwidth, degrades employee productivity, and wastes network resources. The WatchGuard spamBlocker option uses industry-leading pattern detection technology from Commtouch to block spam at your Internet gateway and keep it away from your email server.

Commercial mail filters use many methods to find spam. Blacklists keep a list of domains that are used by known spam sources or are open relays for spam. Content filters search for key words in the header and body of the email message. URL detection compares a list of domains used by known spam sources to the advertised link in the body of the email message. However, all of these procedures scan each individual email message. Attackers can easily bypass those fixed algorithms. They can mask the sender address to bypass a blacklist, change key words, embed words in an image, or use multiple languages. They can also create a chain of proxies to disguise the advertised URL.

spamBlocker uses the Recurrent-Pattern Detection (RPD) solution created by Commtouch to detect these hard-to-find spam attacks. RPD is an innovative method that searches the Internet for spam outbreaks in real time. RPD finds the patterns of the outbreak, not only the pattern of individual spam messages. Because it does not use the content or header of a message, it can identify spam in any language, format, or encoding. To see an example of real-time spam outbreak analysis, visit the Commtouch Outbreak Monitor at: <http://www.commtouch.com/Site/ResearchLab/map.asp>

spamBlocker also provides optional virus outbreak detection functionality. For more information, see *Enable and Set Parameters for Virus Outbreak Detection (VOD)* on page 1156.

You can see statistics on current spamBlocker activity on the XTM device, as described in *spamBlocker Statistics* on page 779.

## spamBlocker Requirements

Before you enable spamBlocker, you must have:

- A spamBlocker feature key — To get a feature key, contact your WatchGuard reseller or go to the WatchGuard LiveSecurity web site at:  
<http://www.watchguard.com/store>
- POP3 or SMTP email server — spamBlocker works with the WatchGuard POP3 and incoming SMTP proxies to scan your email. If you have not configured the POP3 or SMTP proxy, they are enabled when you configure the spamBlocker service. If you have more than one proxy policy for POP3 or for SMTP, spamBlocker works with all of them.
- DNS configured on your XTM device — In Policy Manager, select **Network > Configuration**. Select the **WINS/DNS** tab and type the IP addresses of the DNS servers your XTM device uses to resolve host names.
- A connection to the Internet

## spamBlocker Actions, Tags, and Categories

The XTM device uses spamBlocker actions to apply decisions about the delivery of email messages. When a message is assigned to a category, the related action is applied. Not all actions are supported when you use spamBlocker with the POP3 proxy.

### *Allow*

Let the email message go through the XTM device.

### *Add subject tag*

Let the email message go through the XTM device, but insert text in the subject line of the email message to mark it as spam or possible spam. You can keep the default tags or you can customize them, as described in the spamBlocker tags section below. You can also create rules in your email reader to sort the spam automatically, as described in *Create Rules for Your Email Reader* on page 1157.

### *Quarantine (SMTP only)*

Send the email message to the Quarantine Server. Note that the **Quarantine** option is supported only if you use spamBlocker with the SMTP proxy. The POP3 proxy does not support this option.

### *Deny (SMTP only)*

Stop the email message from being delivered to the mail server. The XTM device sends this 571 SMTP message to the sending email server: *Delivery not authorized, message refused*. The **Deny** option is supported only if you use spamBlocker with the SMTP proxy. The POP3 proxy does not support this option.

### *Drop (SMTP only)*

Drop the connection immediately. The XTM device does not give any error messages to the sending server. The **Drop** option is supported only if you use spamBlocker with the SMTP proxy. The POP3 proxy does not support this option.

## spamBlocker tags

If you select the spamBlocker action to add a tag to certain email messages, the XTM device adds a text string to the subject line of the message. You can use the default tags provided, or you can create a custom tag. The maximum length of the tag is 30 characters.

This example shows the subject line of an email message that was found to be spam. The tag added is the default tag: **\*\*\*SPAM\*\*\***.

Subject: **\*\*\*SPAM\*\*\*** Free auto insurance quote

This example shows a custom tag: [SPAM]

Subject: [SPAM] You've been approved!

## spamBlocker Categories

The Commtouch Recurrent-Pattern Detection (RPD) solution classifies spam attacks in its Anti-Spam Detection Center database by severity. spamBlocker queries this database and assigns a category to each email message.

spamBlocker has three categories:

The **Confirmed Spam** category includes email messages that come from known spammers. If you use spamBlocker with the SMTP proxy, we recommend you use the **Deny** action for this type of email. If you use spamBlocker with the POP3 proxy, we recommend you use the **Add subject tag** action for this type of email.

The **Bulk** category includes email messages that do not come from known spammers, but do match some known spam structure patterns. We recommend you use the **Add subject tag** action for this type of email, or the **Quarantine** action if you use spamBlocker with the SMTP proxy.

The **Suspect** category includes email messages that look like they could be associated with a new spam attack. Frequently, these messages are legitimate email messages. We recommend that you consider a suspect email message as a *false positive* and therefore not spam unless you have verified that is not a false positive for your network. We also recommend that you use the **Allow** action for suspect email, or the **Quarantine** action if you use spamBlocker with the SMTP proxy.

## See the spamBlocker Category for a Message

After spamBlocker categorizes a message, it adds the spam category to the full email message header as a spam score.

To find the spam score for a message, open the full email message header.

If you have Microsoft Outlook, open the message, select **View > Options**, and look in the **Internet headers** dialog box.

The spam score appears in this line:

X-WatchGuard-Spam\_Score:

For example:

X-WatchGuard-Spam-Score: 3, bulk; 0, no virus

The first number on this line is the spam category. This number has one of these values:


- 0 - clean
- 1 - clean
- 2 - suspect
- 3 - bulk
- 4 - spam

If you enable Virus Outbreak Detection (VOD) in your spamBlocker configuration, the spam score in the email message header has a second number, the VOD category. This number has one of these values:

- 0 - no virus
- 1 - no virus
- 2 - virus threat possible
- 3 - virus threat high

## Activate spamBlocker

You use a wizard to enable the spamBlocker feature in the SMTP proxy, the POP3 proxy, or both. You can also use this wizard to add a new SMTP proxy or POP3 proxy to your XTM device configuration.

1. Make sure you have met all requirements for spamBlocker, as described in *spamBlocker Requirements* on page 1142.
2. Import the feature key for spamBlocker to the XTM device, as described in *Add a Feature Key to Your XTM Device* on page 62.
3. From WatchGuard System Manager, select the XTM device that you want use spamBlocker.
4. Click .  
Or, select **Tools > Policy Manager**.  
*Policy Manager appears for the device you selected.*
5. Select **Subscription Services > spamBlocker > Activate**.  
*The Activate spamBlocker wizard starts.*





6. Click through the wizard and add the information it asks for. The wizard has either one or two screens depending on how your XTM device is currently configured.

## Apply spamBlocker Settings to Your Policies

This screen appears if you already have one or more SMTP or POP3 proxy policies defined on your XTM device. From the list, select the proxy policies for which you want to enable spamBlocker. The **Select** check box is dimmed for any policies that already have spamBlocker enabled.

## Create New Proxy Policies

This screen appears if your XTM device does not yet have proxy policies created for either SMTP or POP3, or if your XTM device has either SMTP or POP3 but not both. The wizard can create one or both of these policies for you. For either policy, you must have at least one external interface with a static IP address.

- To create a POP3 policy, select the **POP3** check box.
- To create an SMTP policy, select the **Incoming SMTP** check box. Type the email server IP address.
- The SMTP policy created by this wizard contains “Any-External” in the **From** list and a static NAT entry in the **To** list. The static NAT entry uses the first static external IP address configured on the XTM device. It enables static NAT for the email server IP address you enter in the wizard. If this default static NAT SMTP policy is not the best choice for your organization, you can use Policy Manager to create an SMTP policy before you use the wizard.

For information on how to add a policy to Policy Manager, see *Add a Policy from the List of Templates* on page 374.

After the wizard is finished, you can click the check box at the bottom of the screen to begin to configure spamBlocker, as described in *Configure spamBlocker* on page 1146.

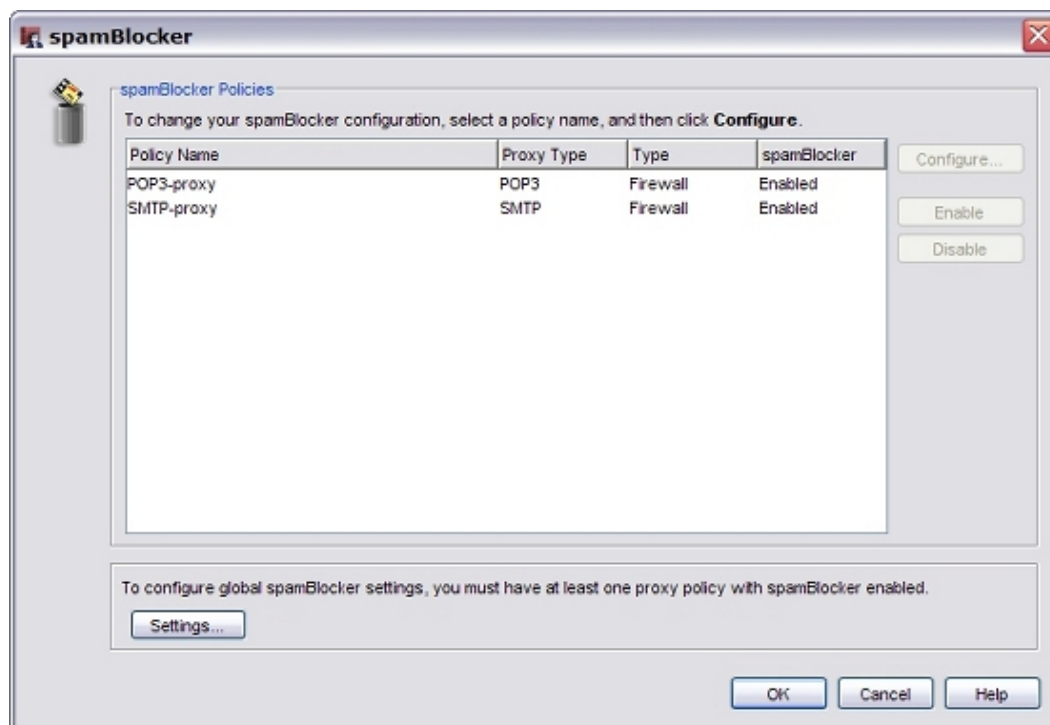
## Configure spamBlocker

After you use the Activate spamBlocker Wizard to activate spamBlocker, you can set other configuration parameters.

If you did not select the check box in the final screen of the Activate spamBlocker Wizard to configure spamBlocker, you can activate spamBlocker from Policy Manager.

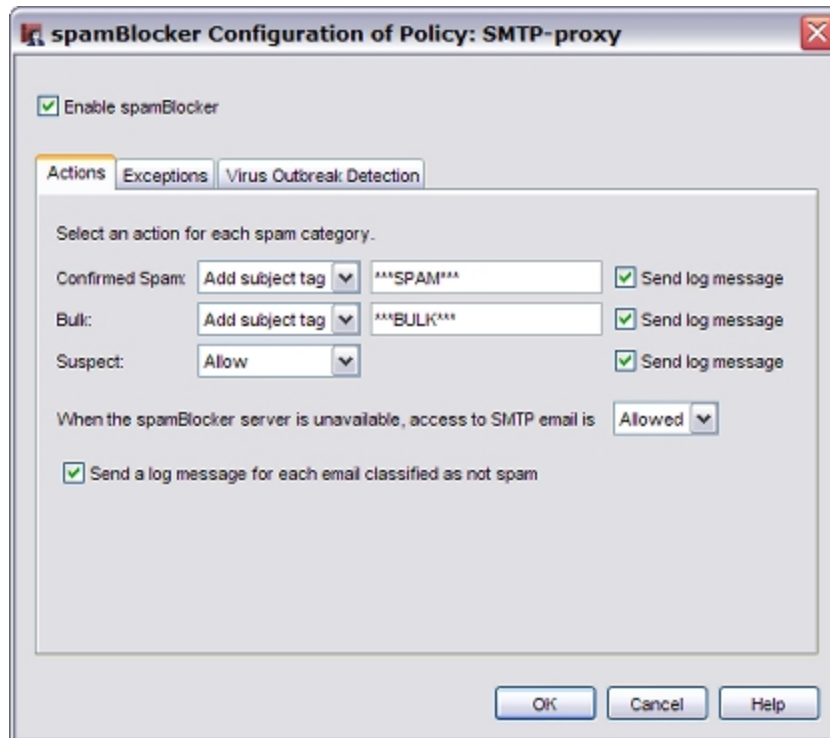
1. Select **Subscription Services > spamBlocker > Configure**.

*The spamBlocker dialog box appears with a list of the SMTP and POP3 proxies on your XTM device, and whether spamBlocker is enabled for each one.*



2. Select a policy. Click **Configure**.

*The spamBlocker Configuration page for that policy appears.*



3. Select the **Enable spamBlocker** check box.
4. Set the actions spamBlocker applies for each category of email in the drop-down lists adjacent to **Confirmed spam**, **Bulk**, and **Suspect**. If you select **Add subject tag** for any category, you can change the default tag that appears in the text box to the right of the drop-down list. For more information on spamBlocker tags, see *spamBlocker Actions, Tags, and Categories* on page 1142.
5. If you want to send a log message each time spamBlocker takes an action, select the **Send log message** check box for the action. If you do not want to record log messages for an action, clear this check box.
6. The **When the spamBlocker server is unavailable, access to POP3/SMTP email is** drop-down list specifies how the XTM device handles incoming email when the spamBlocker server cannot be contacted. We recommend you use the default **Allowed** action.
  - If you set this option to **Denied** for the POP3 or SMTP proxy, it causes a conflict with Microsoft Outlook. When Outlook starts a connection to the email server, spamBlocker tries to contact the spamBlocker server. If the spamBlocker server is not available, spamBlocker stops the email download. When this happens, a cycle starts. Outlook tries to download email and spamBlocker stops the download. This continues until the XTM device can connect to the spamBlocker server, or the request is dropped because the proxy times out, or you cancel the request.
  - If you set this option to **Denied** with the SMTP proxy, the XTM device sends this 450 SMTP message to the sending email server: "Mailbox is temporarily unavailable."
7. The **Send log message for each email classified as not spam** check box specifies whether a message is added to the log file if an email message is scanned by spamBlocker but is not designated as Confirmed Spam, Bulk, or Suspect. Select this check box if you want to add a message to the log file in this situation.
8. (Optional) Add spamBlocker exception rules, as described in *About spamBlocker Exception* on page 1148.

9. Configure Virus Outbreak Detection actions, as described in *Configure Virus Outbreak Detection Actions for a Policy* on page 1151.
10. Click **OK**.

**Note** *If you have any perimeter firewall between the XTM device that uses spamBlocker and the Internet, it must not block HTTP traffic. The HTTP protocol is used to send requests from the XTM device to the spamBlocker server.*

After you enable spamBlocker for a proxy action or policy, you can define global spamBlocker settings. These settings apply to all spamBlocker configurations. Click **Settings** to see or modify the global spamBlocker configuration settings. For more information, see *Set Global spamBlocker Parameters* on page 1153.

## About spamBlocker Exceptions

You can create an exception list to the general spamBlocker actions that is based on the sender's or recipient's address. For example, if you want to allow a newsletter that spamBlocker identifies as Bulk email, you can add that sender to the exception list and use the **Allow** action regardless of the spamBlocker category the sender is assigned to. Or, if you want to apply a tag to a sender that spamBlocker designates as safe, you can add that to the exceptions list as well.

Make sure you use the sender's actual address that is listed in the "Mail-From" field in the email message header, which may not match the address in the "From:" field that you see at the top of the email message. To get the actual address for an exception, get the full email message header (from Microsoft Outlook, with the message open, select **View > Options** and look in the **Internet headers** box). The addresses of the sender and recipient are in these lines:

```
X-WatchGuard-Mail-From:  
X-WatchGuard-Mail-Recipients:
```

Use care when you add wildcards to an exception. Spammers can spoof header information. The more specific the addresses in your exception list, the more difficult it will be to spoof them.

To add an exception rule, see *Add spamBlocker Exception Rules* on page 1148.

To change the order of the rules listed in the dialog box, see *Change the Order of Exceptions* on page 1150.

You can also add exception rules by writing them in an ASCII file and importing them into your XTM device configuration. See *Import and Export spamBlocker Exception Rules* on page 1150.

## Add spamBlocker Exception Rules

After you enable spamBlocker, you can use Policy Manager to define exceptions that allow email from specific senders to bypass spamBlocker.

1. Select **Subscription Services > spamBlocker > Configure**.
2. Select a proxy policy and click **Configure**. Select the **Exceptions** tab.



- Click **Add**. Select a rule action: **Allow**, **Add subject tag**, **Quarantine**, **Deny**, or **Drop**. (Remember that the POP3 proxy supports only the **Allow** and **Add subject tag** actions in spamBlocker.)



- Type a sender, a recipient, or both. You can type the full email address or use wildcards. Make sure you use the actual address of the sender. You can find this address in the "Mail-From" field in the email message header. This address may not match the address in the "From:" field that you see at the top of the email message. To get the actual address for an exception, get the full email message header (from Microsoft Outlook, with the message open, select **View > Options** and look in the **Internet headers** box). The addresses of the sender and recipient are in these lines:  
X-WatchGuard-Mail-From:  
X-WatchGuard-Mail-Recipients:  
Use care when you add wildcards to an exception. Spammers can spoof header information. The more specific the addresses in your exception list, the more difficult it will be to spoof them.
- Click **OK**.  
*The exception is added to the bottom of the exceptions list.*

6. To send a log message each time an email matches one of the exceptions, select the **Send log message for each email that matches one of the above exceptions** check box.

The exceptions are processed in the order they appear in the list. To *Change the Order of Exceptions*, click **Up** and **Down**.

## Change the Order of Exceptions

The order that the spamBlocker exception rules appear in the dialog box shows the order in which email messages are compared to the rules. The proxy policy compares messages to the first rule in the list and continues in sequence from top to bottom. When a message matches a rule, the XTM device performs the related action. It performs no other actions, even if the message matches a rule or rules later in the list.

To change the order of rules, select the rule whose order you want to change. Click **Up** or **Down** to move the selected rule up or down in the list.

## Import and Export spamBlocker Exception Rules

If you manage several XTM devices, or use spamBlocker with more than one proxy definition, you can import and export exception rules between them. This saves time because you must define the rules only once.

You can transfer exception rules between proxies or XTM devices in two ways.

- You can write an ASCII file that defines the rules and import it to other XTM devices or proxy policies.
- You can use the spamBlocker user interface to define the exception rules, export the file to an ASCII file, and import that file into another XTM device configuration file or proxy definition.

## Write Rulesets in an ASCII File

You can write rules in a normal ASCII file that uses the standard UTF-8 character set.

You must include only one rule per line. The syntax for rules is:

*[action, <tag>], sender [, recipient]*

where:

*action* = Allow, Add subject tag <tag>, Quarantine, Deny, or Drop. (Quarantine, Deny, and Drop are not supported by the POP3 proxy.) The default action is Allow.

*tag* = The identifier you want to add to the email messages. The identifier must be enclosed in angle brackets.

*sender* = Email address (abc@mywatchguard.com) or pattern (\*@firebox.net). The default is all senders.

*recipient* = Email address (abc@mywatchguard.com) or pattern (\*@firebox.net). The default is all recipients.

The fields enclosed in brackets are optional. If you omit them, the default values are used.

To add comments to a file, precede the comment with a number sign (#). Make sure the comment is on its own line.

Here is an example of a spamBlocker exception rules file:

```
# allow all email from firebox.net
*@firebox.net

# use **SPAM** tag on all email from xyz.com
Add subject tag, <**SPAM**>, *@xyz.com

# deny all email from unknown.com to abc@mywatchguard.com
Deny, *@unknown.com, abc@mywatchguard.com
```

## Import an ASCII Exceptions File

1. From the **Exceptions** section of the **spamBlocker Configuration** dialog box, click **Import**.
2. Find the ASCII file and click **Open**.
3. If exceptions are already defined in spamBlocker, you are asked whether you want to replace the existing rules or append the imported rules to the list of existing rules. Click **Replace** or **Append**. If you click **Append**, the imported rules appear in the **Exceptions** block under any existing rules. If you want to change the order of the exception rules, see *Change the Order of Exceptions* on page 1150.

**Note** If you import a rule with the **Deny** exception into the POP3 proxy, you get an error message.

## Export Rules to an ASCII File

When you export exception rules from a proxy definition, the XTM device saves the current rules to an ASCII text file.

1. In the **spamBlocker Configuration** dialog box, on the **Exceptions** tab, define exceptions as described in *Add spamBlocker Exception Rules* on page 1148.
2. Click **Export**.
3. In the **Open** dialog box, select where you want to save the exceptions file and click **Save**. You can now open another SMTP or POP3 proxy definition in the same or in a different XTM device configuration file and import the exceptions file.

## Log Exceptions

Select the **Send log message for each email that matches one of the above exceptions** check box if you want a message written to the log file each time an email message matches an exception rule.

## Configure Virus Outbreak Detection Actions for a Policy

Virus Outbreak Detection (VOD) is a technology that uses traffic analysis technology to identify email virus outbreaks worldwide within minutes and then provides protection against those viruses. Provided by Commtouch, an industry leader in email spam and virus protection, VOD is incorporated into the spamBlocker subscription service. After you enable spamBlocker you can use Policy Manager to configure Virus Outbreak Detection.

To configure Virus Outbreak Detection actions:

1. Select **Subscription Services > spamBlocker > Configure**.
2. Make sure Virus Outbreak Detection is enabled:
  - On the **spamBlocker** dialog box, click **Settings**.
  - On the **spamBlocker Settings** dialog box, select the **General Settings** tab.
  - Select the **Enable Virus Outbreak Detection (VOD)** check box.  
For more information, see *Enable and Set Parameters for Virus Outbreak Detection (VOD)* on page 1156.
  - Click **OK**.
3. On the **spamBlocker** dialog box, select a proxy policy and click **Configure**. Select the **Virus Outbreak Detection** tab.



4. From the **When a virus is detected** drop-down list, select the action the XTM device takes if VOD detects a virus in an email message.
5. From the **When a scan error occurs** drop-down list, select the action the XTM device takes when VOD cannot scan an email message or attachment.  
Attachments that cannot be scanned include binhex-encoded messages, certain encrypted files, or files that use a type of compression that we do not support such as password-protected Zip files.
6. Select the **Log this action** check boxes to send a log message when a virus is detected or when a scan error occurs.
7. Select the **Alarm** check boxes to send an alarm when a virus is detected or when a scan error occurs.

The SMTP proxy supports the **Allow**, **Lock**, **Remove**, **Quarantine**, **Drop**, and **Block** actions. The POP3 proxy supports only the **Allow**, **Lock**, and **Remove** actions.

For more information on these actions, see *spamBlocker Actions, Tags, and Categories* on page 1142.



## Configure spamBlocker to Quarantine Email

The WatchGuard Quarantine Server provides a safe, full-featured quarantine mechanism for any email messages suspected or known to be spam or to contain viruses. This repository receives email messages from the SMTP proxy and filtered by spamBlocker.

To configure spamBlocker to quarantine email:

1. When you run the Activate spamBlocker Wizard (as described in *Activate spamBlocker* on page 1144), you must make sure you use spamBlocker with the SMTP proxy. The POP3 proxy does not support the Quarantine Server.
2. When you set the actions spamBlocker applies for different categories of email (as described in *Configure spamBlocker* on page 1146), make sure you select the Quarantine action for at least one of the categories. When you select this action, you are prompted to configure the Quarantine Server if you have not already done so.

You can also select the **Quarantine** action for email messages identified by Virus Outbreak Detection to contain viruses. For more information, see *Configure Virus Outbreak Detection Actions for a Policy* on page 1151.

## About Using spamBlocker with Multiple Proxies

You can configure more than one SMTP or POP3 proxy policy to use spamBlocker. This lets you create custom rules for different groups in an organization. For example, you can allow all email to your management employees and use a spam tag for the marketing team.

If you want to use more than one proxy policy with spamBlocker, your network must use one of these configurations:

- Each proxy policy must send email to a different internal email server.
- You must set the external source or sources that can send email for each proxy policy.

## Set Global spamBlocker Parameters

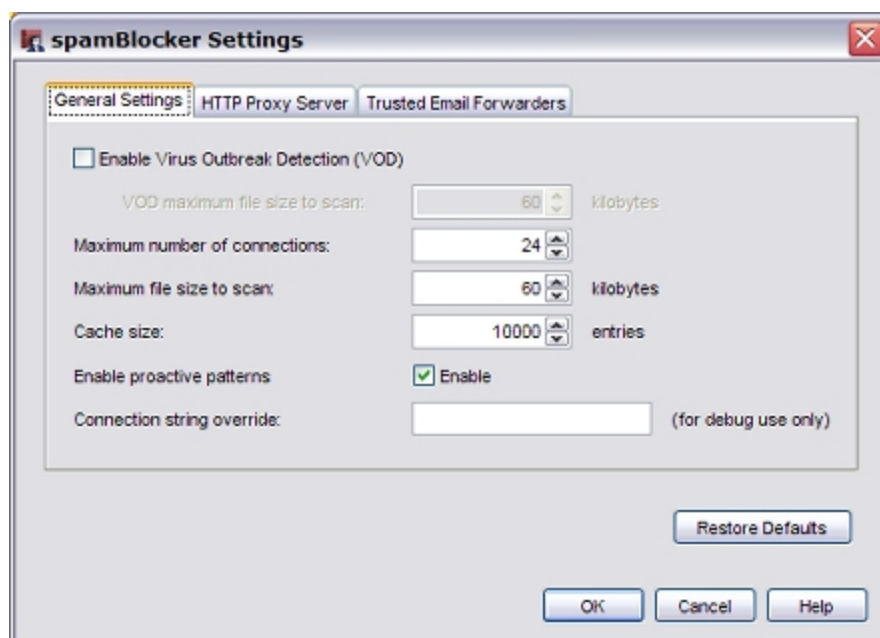
You can use global spamBlocker settings to optimize spamBlocker for your own installation. Because most of these parameters affect the amount of memory that spamBlocker uses on the XTM device, you must balance spamBlocker performance with other XTM device functions.

**Note** *To configure global spamBlocker settings, you must enable spamBlocker for at least one proxy policy.*

From Policy Manager, you can configure the global parameters for spamBlocker.

1. Select **Subscription Services > spamBlocker > Configure**.
2. Click **Settings**.

*The spamBlocker Settings dialog box appears.*



3. spamBlocker creates a connection for each message it processes. This connection includes information about the message that is used to generate its spam score. spamBlocker sets a default maximum number of connections that can be simultaneously buffered according to your XTM device model. You can use the **Maximum number of connections** text box to increase or decrease this value. If the amount of traffic handled by your proxy policies is low, you can increase the number of supported connections for spamBlocker without affecting performance. If you have limited available memory on the XTM device, you may want to decrease the value in this field.
4. In the **Maximum file size to scan** text box, type or select the number of bytes of an email message to be passed to spamBlocker to be scanned. Usually, 20–40K is enough for spamBlocker to correctly detect spam. However, if image-based spam is a problem for your organization, you can increase the maximum file size to block more image-based spam.  
For information about the default and maximum scan limits for each XTM device model, see *About spamBlocker and VOD Scan Limits* on page 1157.
5. In the **Cache size** text box, enter the number of entries spamBlocker caches locally for messages that have been categorized as spam and bulk. A local cache can improve performance because network traffic to Commtouch is not required. Usually, you do not have to change this value. You can set the **Cache size** to 0 to force all email to be sent to Commtouch. This is most often used only for troubleshooting.
6. Clear the **Enabled** check box adjacent to **Proactive Patterns** if you want to disable the Commtouch CT Engine Proactive Patterns feature. This feature is automatically enabled. This feature uses a large amount of memory while the local database is updated. If you have limited memory or processor resources, you may want to disable this feature.
7. The **Connection string override** text box is used only when you must troubleshoot a spamBlocker problem with a technical support representative. Do not change this value unless you are asked to give additional debug information for a technical support problem.
8. You can also define several other optional parameters for spamBlocker:
  - *Enable and Set Parameters for Virus Outbreak Detection (VOD)*
  - *Use an HTTP Proxy Server for spamBlocker*

- *Add Trusted Email Forwarders to Improve Spam Score Accuracy*

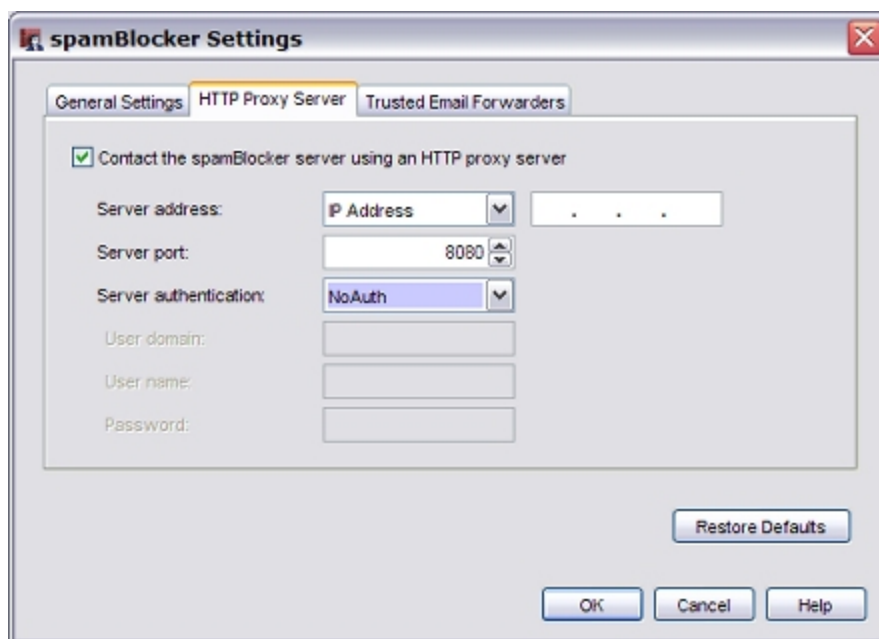
9. Click **OK**.

To restore the default spamBlocker settings at any time, click **Restore Defaults**.

## Use an HTTP Proxy Server for spamBlocker

If spamBlocker must use an HTTP proxy server to connect to the CommTouch server through the Internet, you must configure the HTTP proxy server settings on the **spamBlocker Settings** dialog box.

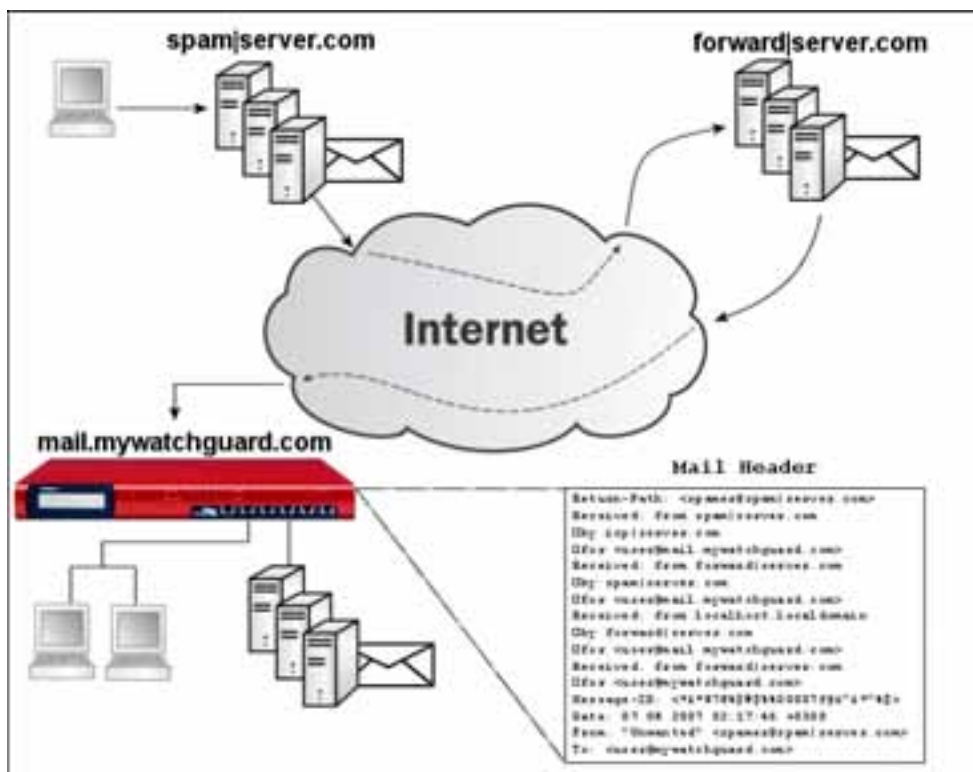
1. In the spamBlocker dialog box, click **Settings**.
2. Click the **HTTP Proxy Server** tab.



3. On the **HTTP Proxy Server** tab, select the **Contact the spamBlocker using an HTTP Proxy server** check box.
4. Use the other fields in this tab to set up parameters for the proxy server, which include the address of the proxy server, the port the XTM device must use to contact the proxy server, and authentication credentials for the XTM device to use for proxy server connections (if required by the proxy server).

## Add Trusted Email Forwarders to Improve Spam Score Accuracy

Part of the spam score for an email message is calculated using the IP address of the server that the message was received from. If an email forwarding service is used, the IP address of the forwarding server is used to calculate the spam score. Because the forwarding server is not the initial source email server, the spam score can be inaccurate.



To improve spam scoring accuracy, you can enter one or more host names or domain names of email servers that you trust to forward email to your email server. If you use SMTP, enter one or more host names or domain names for SMTP email servers that you trust to forward messages to your email server. If you use POP3, enter domain names for known or commonly used POP3 providers that you trust to download messages from.

After you add one or more trusted email forwarders, spamBlocker ignores the trusted email forwarder in email message headers. The spam score is calculated using the IP address of the source email server.

1. From the **spamBlocker Settings** dialog box, select the **Trusted Email Forwarders** tab.
2. Type a host or domain name in the text box at the bottom of the dialog box. Click **Add**.  
If you add a domain name, make sure you add a leading period (.) to the name, as in `.firebox.net`.
3. (Optional) Repeat Step 2 to add more trusted email forwarders.
4. Click **OK**.

## Enable and Set Parameters for Virus Outbreak Detection (VOD)

Virus Outbreak Detection (VOD) is a technology that identifies email virus outbreaks worldwide within minutes and then provides protection against those viruses. Provided by Commtouch, an industry leader in email spam and virus protection, VOD catches viruses even faster than signature-based systems.

To enable and configure VOD:

1. In the **spamBlocker Settings** dialog box, select the **General Settings** tab.

2. Select the **Enable Virus Outbreak Detection (VOD)** check box.
3. By default, VOD scans inbound email messages up to a default size limit that is optimal for the XTM device model. You can increase or decrease this limit with the arrows adjacent to **VOD maximum file size to scan**.

For information about the default and maximum scan limits for each XTM device model, see *About spamBlocker and VOD Scan Limits* on page 1157.

VOD uses the larger of the maximum file size values set for VOD or spamBlocker. If the global spamBlocker value of the **Maximum file size to scan** field set on the **spamBlocker Settings** dialog box is greater than the **VOD maximum file size to scan** value, VOD uses the global spamBlocker value. For information about spamBlocker global settings, see *Set Global spamBlocker Parameters* on page 1153.

In the proxy definitions for spamBlocker, you can set the actions for spamBlocker to take when a virus is found, as described in *Configure Virus Outbreak Detection Actions for a Policy* on page 1151.

## About spamBlocker and VOD Scan Limits

spamBlocker scans each file up to a specified kilobyte count. Any additional bytes in the file are not scanned. This allows the proxy to partially scan very large files without a large effect on performance. The default and maximum scan limits can be different for each XTM device model.

### File Scan Limits by XTM Device Model, in Kilobytes

Model	Minimum	Maximum	Default
XTM 2 Series	1	1000	60
XTM 5 Series	1	2000	100
XTM 8 Series	1	2000	100
XTM 1050	1	2000	100

For information about how to set the maximum file size to scan for spamBlocker and VOD, see *Set Global spamBlocker Parameters* on page 1153 and *Enable and Set Parameters for Virus Outbreak Detection (VOD)* on page 1156

## Create Rules for Your Email Reader

To use the **Tag** action in spamBlocker, it is best to configure your email reader to sort messages. Most email readers, such as Outlook, Thunderbird, and Mac Mail, allow you to set rules that automatically send email messages with tags to a subfolder. Some email readers also let you create a rule to automatically delete the message.

Because you can use a different tag for each spamBlocker category, you can set a different rule for each category. For example, you can set one rule to move any email message with the **\*\*\*BULK\*\*\*** tag in the subject line to a Bulk subfolder in your Inbox. You can set another rule that deletes any email message with the **\*\*\*SPAM\*\*\*** tag in the subject line.

For instructions on how to configure the Microsoft Outlook email client, see *Send Spam or Bulk Email to Special Folders in Outlook* on page 1158. For information about how to use this procedure on other types of email clients, look at the user documentation for those products.

**Note** *If you use spamBlocker with the SMTP proxy, you can have spam email sent to the Quarantine Server. For more information on the Quarantine Server, see About the Quarantine Server on page 1225.*

## Send Spam or Bulk Email to Special Folders in Outlook

This procedure shows you the steps to create rules for bulk and suspect email in Microsoft Outlook. You can have email with a “spam” or “bulk” tag delivered directly to special folders in Outlook. When you create these folders, you keep possible spam email out of your usual Outlook folders, but you can get access to the email if it becomes necessary.

Before you start, make sure that you configure spamBlocker to add a tag for spam and bulk email. You can use the default tags, or create custom tags. The steps below describe how to create folders with the default tags.

1. From your Outlook Inbox, select **Tools > Rules and Alerts**.
2. Click **New Rule** to start the Rules wizard.
3. Select **Start from a blank rule**.
4. Select **Check messages when they arrive**. Click **Next**.
5. Select the condition check box: **with specific words in the subject**. Then, in the bottom pane, edit the rule description by clicking on **specific**.
6. In the **Search Text** dialog box, type the spam tag as **\*\*\*SPAM\*\*\***. If you use a custom tag, type it here instead.
7. Click **Add** and then click **OK**.
8. Click **Next**.
9. The wizard asks what you want to do with the message. Select the **move it to the specified folder** check box. Then, in the bottom pane, click **specified** to select the destination folder.
10. In the **Choose a Folder** dialog box, click **New**.
11. In the folder name field, type **Spam**. Click **OK**.
12. Click **Next** two times.
13. To complete the rule setup, type a name for your spam rule and click **Finish**.
14. Click **Apply**.

Repeat these steps to create a rule for bulk email, using the bulk email tag. You can send bulk email to the same folder, or create a separate folder for bulk email.

## Send a Report about False Positives or False Negatives

A false positive email message is a legitimate message that spamBlocker incorrectly identifies as spam. A false negative email message is a spam message that spamBlocker does not correctly identify as spam. If you find a false positive or false negative email message, you can send a report directly to Commtouch. You can also send a report about a false positive for a solicited bulk email message. This is a message that spamBlocker identifies as bulk email when a user actually requested the email message.

**Note** Do not send a report about a false positive when the email is assigned to the Suspect category. Because this is not a permanent category, Commtouch does not investigate error reports for suspected spam.

You must have access to the email message to send a false positive or false negative report to Commtouch. You must also know the category (Confirmed Spam, Bulk) into which spamBlocker put the email message. If you do not know the category, see the "Find the category a message is assigned to" section below.

1. Save the email as a .msg or .eml file.  
You cannot forward the initial email message because Commtouch must see the email header. If you use email software such as Microsoft Outlook or Mozilla Thunderbird, you can drag and drop the email message into a computer desktop folder. If you use email software that does not have drag-and-drop functionality, you must select **File > Save As** to save the email message to a folder.
2. Create a new email message addressed to:  
reportfp@blockspam.biz for false positives  
reportfn@blockspam.biz for false negatives  
reportso@blockspam.biz for false positive solicited bulk email
3. Type the following on the subject line of your email message:  
FP Report <Your Company Name> <Date of submission> for false positives  
FN Report <Your Company Name> <Date of submission> for false negatives  
FP Report <Your Company Name> <Date of submission> for false positive solicited bulk email
4. Attach the .msg or .eml file to the email message and send the message.

If you have many messages to tell Commtouch about, you can put them all into one Zip file. Do not put the Zip file into a Zip archive. The Zip file can be compressed to only one level for Commtouch to analyze it automatically.

## Use RefID Record Instead of Message Text

If you want to send a report to Commtouch but cannot send the initial email message because the information in the message is confidential, you can use the RefID record from the email header instead. The RefID record is the reference number for the transaction between the XTM device and the Commtouch Detection Center.

spamBlocker adds an X-WatchGuard-Spam-ID header to each email. The header looks like this:

X-WatchGuard-Spam-ID: 0001.0A090202.43674BDF.0005-G-gg8BuArWNRyK9/VK03E51A==

The long sequence of numbers and letters after X-WatchGuard-Spam-ID: part of the header is the RefID record.

Instead of attaching the initial email, put the RefID record in the body of your email message. If you have more than one email message you want to send a report about, put each RefID record on a separate line.

To see email headers if you use Microsoft Outlook:

1. Open the email message in a new window or select it in Outlook.
2. If you open the email in a separate window, select **View > Options**.  
If you highlight the email in Outlook, right-click the email message and select **Options**.  
The headers appear at the bottom of the Message Options window.

To see email headers if you use Microsoft Outlook Express:

1. Open the email message in a new window or highlight it in Outlook Express.
2. If you open the email in a separate window, select **File > Properties**.  
If you highlight the email in Outlook Express, right-click the email and select **Properties**.
3. Click the **Details** tab to view the headers.

To see email headers if you use Mozilla Thunderbird:

1. Open the email messages in a new window.
2. Select **View > Headers > All**.

## Find the Category a Message is Assigned To

Message tags are the only way to know which category a message is assigned to. Change the action to **Add subject tag** and use a unique sequence of characters to add to the beginning of the email subject line. For more information on how to use spamBlocker tags, see *spamBlocker Actions, Tags, and Categories* on page 1142.



# 33 Reputation Enabled Defense

---

## About Reputation Enabled Defense

You can use the Reputation Enabled Defense (RED) security subscription to increase the performance and enhance the security of your XTM device.

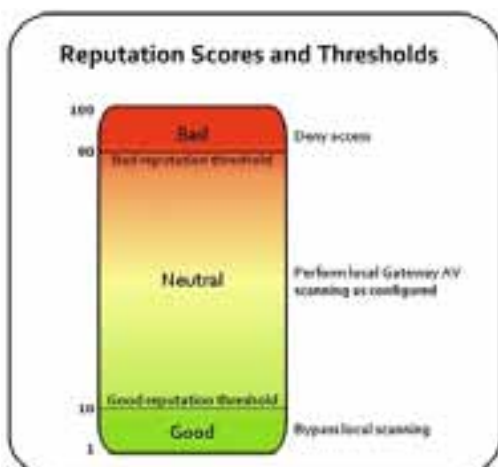
WatchGuard RED uses a cloud-based WatchGuard reputation server that assigns a reputation score between 1 and 100 to every URL. When a user goes to a web site, RED sends the requested web address (or URL) to the WatchGuard reputation server. The WatchGuard server responds with a reputation score for that URL. Based on the reputation score, and on locally configured thresholds, RED determines whether the XTM device should drop the traffic, allow the traffic and scan it locally with Gateway AV, or allow the traffic without a local Gateway AV scan. This increases performance, because Gateway AV does not need to scan URLs with a known good or bad reputation.

## Reputation Thresholds

There are two reputation score thresholds you can configure:

- **Bad reputation threshold** — If the score for a URL is higher than the Bad reputation threshold, the HTTP proxy denies access without any further inspection.
- **Good reputation threshold** — If the score for a URL is lower than the Good reputation threshold and Gateway AntiVirus is enabled, the HTTP proxy bypasses the Gateway AV scan.

If the score for a URL is equal to or between the configured reputation thresholds and Gateway AV is enabled, the content is scanned for viruses.



## Reputation Scores

The reputation score for a URL is based on feedback collected from devices around the world. It incorporates scan results from two leading anti-malware engines: Kaspersky and AVG. Reputation Enabled Defense uses the collective intelligence of the cloud to keep Internet browsing safe and to optimize performance at the gateway.

A reputation score closer to 100 indicates that the URL is more likely to contain a threat. A score closer to 1 indicates that the URL is less likely to contain a threat. If the RED server does not have a previous score for a web address, it assigns a neutral score of 50. The reputation score changes from the default score of 50 based on a number of factors.

These factors can cause the reputation score of a URL to increase, or move toward a score of 100:

- Negative scan results
- Negative scan results for a referring link

These factors can cause the reputation score of a URL to decrease, or move toward a score of 1:

- Multiple clean scans
- Recent clean scans

Reputation scores can change over time. For increased performance, the XTM device stores the reputation scores for recently accessed web addresses in a local cache.

## Reputation Lookups

The XTM device uses UDP port 10108 to send reputation queries to the WatchGuard reputation server. UDP is a best-effort service. If the XTM device does not receive a response to a reputation query soon enough to make a decision based on the reputation score, the HTTP proxy does not wait for the response, but instead processes the HTTP request normally. In this case the content is scanned locally if Gateway AV is enabled.

**Note** A reputation score of -1 means that your device did not get a response soon enough to make a decision based on the reputation score.

Reputation lookups are based on the domain and URL path, not just the domain. Parameters after escape or operator characters, such as & and ? are ignored.

For example, for the URL:

```
http://www.example.com/example/default.asp?action=9&parameter=26
```

the reputation lookup is:

```
http://www.example.com/example/default.asp
```

Reputation Enabled Defense does not do a reputation lookup for sites listed in the HTTP Proxy Exceptions area of the HTTP proxy action.

## Reputation Enabled Defense Feedback

If Gateway AntiVirus is enabled, you can choose if you want to send the results of local Gateway AV scans to the WatchGuard server. You can also choose to upload Gateway AV scan results to WatchGuard even if Reputation Enabled Defense is not enabled or licensed on your device. All communications between your network and the Reputation Enabled Defense server are encrypted.

We recommend that you enable the upload of local scan results to WatchGuard to improve overall coverage and accuracy of Reputation Enabled Defense.

## Configure Reputation Enabled Defense

You can enable Reputation Enabled Defense (RED) to increase the security and performance of the HTTP proxy policies on your XTM device.

### Before You Begin

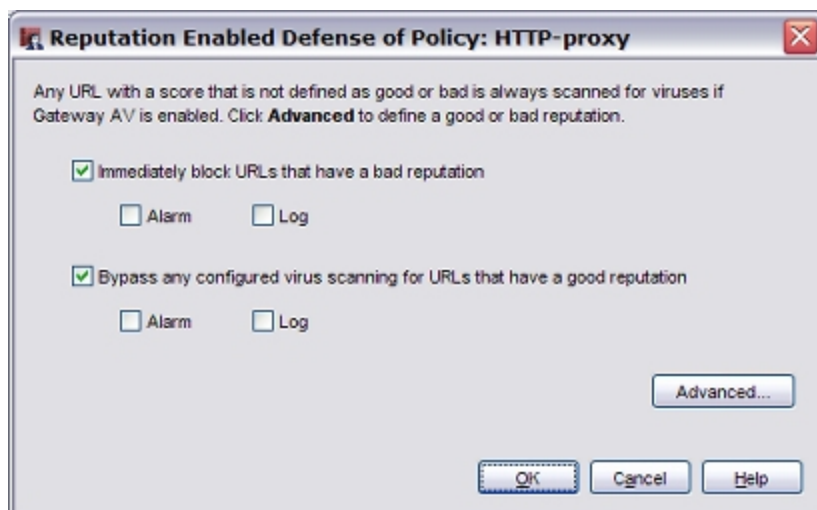
Reputation Enabled Defense is a subscription service. Before you can configure RED, you must *Get a Feature Key from LiveSecurity* on page 59 and *Add a Feature Key to Your XTM Device* on page 62.

**Note** *The XTM device sends reputation queries over UDP port 10108. Make sure this port is open between your XTM device and the Internet.*

### Enable Reputation Enabled Defense

To enable Reputation Enabled Defense on your XTM device:

1. In Policy Manager, select **Subscription Services > Reputation Enabled Defense**.  
*The Reputation Enabled Defense dialog box appears.*
2. Select the HTTP-proxy policy you want to enable RED for and click **Enable**. You must configure at least one HTTP proxy policy to use RED.  
*The Reputation Enabled Defense status changes to Enabled.*
3. Click **Configure**.  
*The Reputation Enabled Defense settings for that policy appear.*

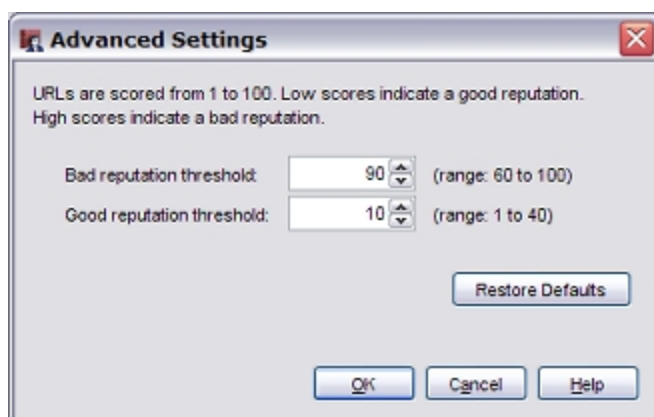


4. Select the **Immediately block URLs that have a bad reputation** check box to block access to sites that score higher than the configured Bad reputation threshold.
5. Select the **Bypass any configured virus scanning for URLs that have a good reputation** check box to have Gateway AntiVirus ignore sites that have a score lower than the configured Good reputation threshold.
6. If you want to trigger an alarm for an action, select the **Alarm** check box for that RED action. If you do not want an alarm, clear the **Alarm** check box for that action.
7. If you want to record log messages for an action, select the **Log** check box for that RED action. If you do not want to record log messages for a RED response, clear the **Log** check box for that action.

## Configure the Reputation Thresholds

You can change the reputation thresholds in the Advanced settings.


1. In the Reputation Enabled Defense settings dialog box, click **Advanced**.  
*The Advanced Settings dialog box appears.*



2. In the **Bad reputation threshold** text box, type or select the threshold score for bad reputation.  
*The proxy can block access to sites with a reputation higher than this threshold.*
3. In the **Good reputation threshold** text box, type or select the threshold score for good reputation.  
*The proxy can bypass a Gateway AntiVirus scan for sites with a reputation score lower than this threshold.*

4. Click **Restore Defaults** if you want to reset the reputation thresholds to the default values.
5. Click **OK**.


You can also configure Reputation Enabled Defense from the **Edit Policy Properties** dialog box:

1. Double-click on the policy.
2. Select the **Policy** tab.
3. Adjacent to the **Proxy action** drop-down list, click .
4. Select **Reputation Enabled Defense** from the **Categories** list.

## Configure Alarm Notification for RED Actions

An alarm is a mechanism to tell users when a proxy rule applies to network traffic. If you enable alarms for a proxy action, you must also configure the type of alarm to use in the proxy policy.

To configure the alarm type to use for an HTTP proxy policy:

1. Double-click the policy.
2. Select the **Properties** tab.
3. Click .
4. Select the **Proxy and AV Alarms** category.
5. Configure the Proxy/AV Alarms settings as described in *Set Logging and Notification Preferences* on page 723.

## Send Gateway AV Scan Results to WatchGuard

When you enable Reputation Enabled Defense, the default configuration allows your XTM device to send the results of local Gateway AntiVirus scans to WatchGuard servers. This action helps to improve Reputation Enabled Defense results for all Fireware XTM users. If you have Gateway AntiVirus, but do not have Reputation Enabled Defense, you can still send Gateway AntiVirus scan results to WatchGuard.

To see or change the feedback setting, select **Subscription Services > Reputation Enabled Defense**.

The **Send encrypted scan results to WatchGuard servers to improve overall coverage and accuracy** check box controls whether the XTM device sends results of Gateway AntiVirus scans to the WatchGuard servers. This check box is selected by default when you configure Reputation Enabled Defense.

- Select this check box to send Gateway AntiVirus scan results to WatchGuard.
- Clear this check box if you do not want to send Gateway AntiVirus scan results.

We recommend that you allow the XTM device to send anti-virus scan results to WatchGuard. This can help improve performance, because the scan results help to improve the accuracy of the reputation scores. All feedback sent to the WatchGuard Reputation Enabled Defense service is encrypted.



# 34 Gateway AntiVirus

---

## About Gateway AntiVirus

Hackers use many methods to attack computers on the Internet. Viruses, including worms and Trojans, are malicious computer programs that self-replicate and put copies of themselves into other executable code or documents on your computer. When a computer is infected, the virus can destroy files or record key strokes.

To help protect your network from viruses, you can purchase the Gateway AntiVirus subscription service. Gateway AntiVirus operates with the SMTP, POP3, HTTP, FTP, and TCP-UDP proxies. When a new attack is identified, the features that make the virus unique are recorded. These recorded features are known as the signature. Gateway AV uses these signatures to find viruses when content is scanned by the proxy.

When you enable Gateway AV for a proxy, Gateway AV scans the content types configured for that proxy. Gateway AV/IPS can scan these compressed file types: .zip, .gzip, .tar, .jar, .rar, .chm, .lha, .pdf, XML/HTML container, OLE container (Microsoft Office documents), MIME (mainly email messages in EML format), .cab, .arj, .ace, .bz2 (Bzip), .swf (flash; limited support).

**Note** *WatchGuard cannot guarantee that Gateway AV can stop all viruses, or prevent damage to your systems or networks from a virus.*

You can see statistics on current Gateway AntiVirus activity on the XTM device, as described in *Gateway AntiVirus Statistics* on page 777.

## Install and Upgrade Gateway AV

To install Gateway AntiVirus, you must *Get a Feature Key from LiveSecurity* on page 59 and *Add a Feature Key to Your XTM Device* on page 62.

New viruses appear on the Internet frequently. To make sure that Gateway AV gives you the best protection, you must update the signatures frequently. You can configure the XTM device to update the signatures automatically from WatchGuard, as described in *Configure the Gateway AV Update Server* on page 1183. You can also *Subscription Services Status and Manual Signatures Updates*.

## About Gateway AntiVirus and Proxy Policies

Gateway AV can work with the WatchGuard SMTP, POP3, HTTP, FTP, and TCP-UDP proxies. When you enable Gateway AV, these proxies examine various types of traffic and perform an action that you specify, such as to drop the connection or to block the packet and add its source address to the Blocked Sites list.

Gateway AV scans different types of traffic according to which proxy policies you use the feature with:

- SMTP or POP3 proxy — Gateway AV looks for viruses and intrusions encoded with frequently used email attachment methods. You can also use Gateway AV and the SMTP proxy to send virus-infected email to the Quarantine Server. For more information, see *About the Quarantine Server* on page 1225 and *Configure Gateway AntiVirus to Quarantine Email* on page 1181.
- HTTP proxy — Gateway AV looks for viruses in web pages that users try to download.
- TCP-UDP proxy — This proxy scans traffic on dynamic ports. It recognizes traffic for several different types of proxies, including HTTP and FTP. The TCP-UDP proxy then sends traffic to the appropriate proxy to scan for viruses or intrusions.
- FTP proxy — Gateway AV looks for viruses in uploaded or downloaded files.
- DNS proxy — Gateway AV looks for viruses in DNS packets.

Each proxy that uses Gateway AV is configured with options that are special to that proxy. For example, the categories of items you can scan is different for each proxy.

For all proxies, you can limit file scanning up to a specified kilobyte count. The default scan limit and maximum scan limits are different for each XTM device model. The XTM device scans the start of each file up to the specified kilobyte count. This allows large files to pass with partial scanning.

For more information about the default and maximum scan limits for each XTM device model, see *About Gateway AntiVirus Scan Limits* on page 1181.

**Note** To make sure Gateway AV has current signatures, you can enable automatic updates for the Gateway AV server, as described in *Configure the Gateway AV Update Server* on page 1183.


## Activate Gateway AntiVirus

There are two ways you can activate Gateway AntiVirus:

- *Activate Gateway AntiVirus with a Wizard from Policy Manager*
- *Activate Gateway AntiVirus from Proxy Definitions*

When you use the Activate Gateway AntiVirus wizard, you can create proxies in one step and enable Gateway AntiVirus for several proxies at the same time. If you plan to use Gateway AntiVirus for more than one proxy, you can save time if you use the wizard.

### Activate Gateway AntiVirus with a Wizard from Policy Manager

1. From WatchGuard System Manager, select the XTM device on which you want to use Gateway AntiVirus.
2. Click .

Or, select **Tools > Policy Manager**.

*Policy Manager appears for the selected device.*



3. Select **Subscription Services > Gateway AntiVirus > Activate**.

The *Activate Gateway AntiVirus wizard* starts.



4. Click **Next**.
5. Complete the wizard. The wizard shows different pages depending on whether you already have proxy policies in your configuration. If you do not, the wizard helps you create one or more proxy policies.

## Apply Gateway AntiVirus Settings to Your Policies

This screen includes a list of proxy policies that are already on your XTM device. From the list, select the proxy policies for which you want to enable Gateway AntiVirus. The **Select** check boxes for any policies that are disabled or that have Gateway AntiVirus already enabled appear dimmed.

You can also automatically enable Gateway AntiVirus for the SMTP, POP3, HTTP, FTP, or TCP proxies if you change settings in the proxy definition, as described in *Activate Gateway AntiVirus from Proxy Definitions* on page 1171.



## Create New Proxy Policies

This screen appears if your XTM device does not yet have policies created for Incoming SMTP, POP3, TCP, FTP, or HTTP Client.

To create a policy, select the corresponding check box. If you select SMTP, enter the email server IP address.


If you select to create an SMTP policy, the wizard creates a default SMTP policy, which is a static NAT policy. To create this default SMTP policy, you must have at least one external interface with a static IP address or PPPoE. Only one policy is created even if you have more than one external interface. The **To** list of the policy has a static NAT entry (the static IP address of the first external interface to the specified email service IP address). If this default policy does not meet your requirements, you can create an SMTP policy in Policy Manager before you run this wizard.



## Activate Gateway AntiVirus from Proxy Definitions

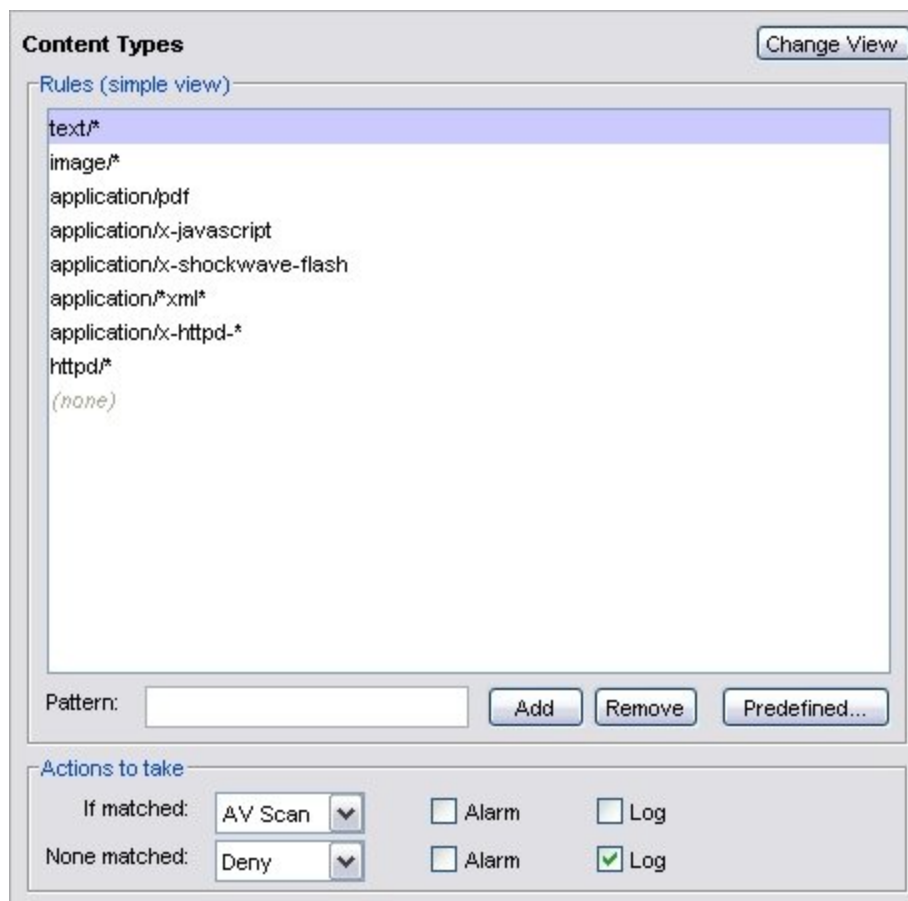
Gateway AV can scan traffic that matches rules in several categories for each proxy. For example, for the SMTP and POP3 proxies, Gateway AV can scan traffic that matches rules in the Content Types and File Names categories.

From Policy Manager, you can activate Gateway AntiVirus while you edit a proxy definition.

1. Add an SMTP, POP3, HTTP, FTP, or TCP-UDP proxy you want to use with Gateway AntiVirus.  
For information on how to add policies, see *Add a Proxy Policy to Your Configuration* on page 417.
2. Double-click the policy.  
*The Edit Policy Properties dialog appears.*
3. Select the **Policy** tab.
4. Click  adjacent to the **Proxy action** drop-down list.
5. From the **Categories** list on the left side of the Proxy Action Configuration dialog box, select one of these categories.

FTP Proxy	SMTP Proxy	POP3 Proxy	HTTP Proxy	TCP-UDP Proxy (HTTP/SMTP traffic on dynamic ports)
Download	Content Types	Content Types	Requests: URL Paths	Request: URL Paths
Upload	File names	File names	Responses: Content Types, Body Content Types	Responses: Content Types, Body Content Types

6. From the **If matched** or **None matched** drop-down lists, select **AV Scan** if you want traffic that matches, or does not match, a given rule to be scanned for viruses. (For information on how to configure rules in a proxy definition, see *Add, Change, or Delete Rules* on page 409.)



7. Click **OK**.

Gateway AntiVirus is automatically activated and enabled for the proxy. To use Gateway AntiVirus with other proxies, you must repeat this procedure for each one.

## Configure Gateway AntiVirus Actions

When you enable Gateway AntiVirus, you must set the actions to be taken if a virus or error is found in an email message (SMTP or POP3 proxies), web page (HTTP proxy), or uploaded or downloaded file (FTP proxy). When Gateway AntiVirus is enabled, it scans each file up to a specified kilobyte count. Any additional bytes in the file are not scanned. This allows the proxy to partially scan very large files without a large effect on performance.

The options for antivirus actions are:

### *Allow*

Allows the packet to go to the recipient, even if the content contains a virus.

### *Deny*

*(FTP proxy only)*

Denies the file and send a deny message.

### *Lock*

*(SMTP and POP3 proxies only)*

Locks the attachment. This is a good option for files that cannot be scanned by the XTM device. A file that is locked cannot be opened easily by the user. Only the administrator can unlock the file. The administrator can use a different antivirus tool to scan the file and examine the content of the attachment.

For information about how to unlock a file locked by Gateway AntiVirus, see *Unlock a File Locked by Gateway AntiVirus* on page 1179.

### *Quarantine*

*(SMTP proxy only)*

When you use the SMTP proxy with the spamBlocker security subscription, you can send email messages with viruses, or possible viruses, to the Quarantine Server. For more information on the Quarantine Server, see *About the Quarantine Server* on page 1225. For information on how to set up Gateway AntiVirus to work with the Quarantine Server, see *Configure Gateway AntiVirus to Quarantine Email* on page 1181.

### *Remove*

*(SMTP and POP3 proxies only)*

Removes the attachment and allows the message through to the recipient.

### *Drop*

*(Not supported in POP3 proxy)*

Drops the packet and drops the connection. No information is sent to the source of the message.

### *Block*

*(Not supported in POP3 proxy)*

Blocks the packet, and adds the IP address of the sender to the Blocked Sites list.

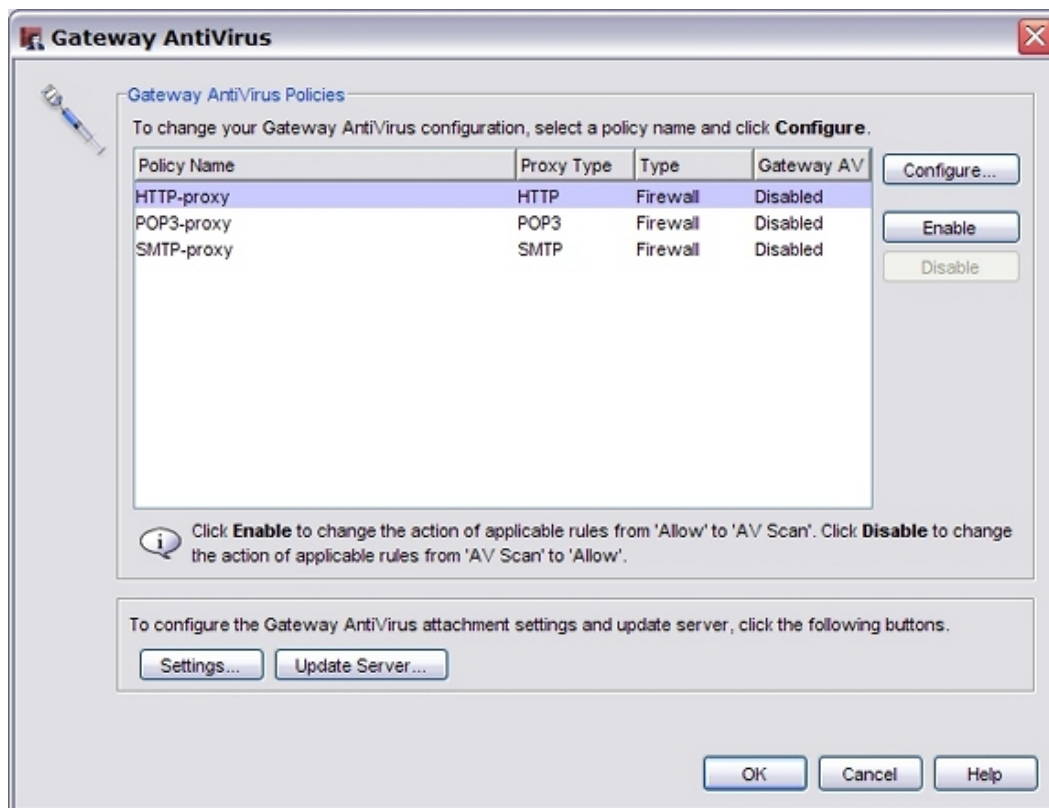
### *AV Scan*

This action can be applied within a ruleset to initiate an AV Scan of the content that matches a rule, or as the default action if the content does not match any rule in the rule category.

## Configure Gateway AntiVirus actions for a Proxy Policy

1. Select **Subscription Services > Gateway AntiVirus > Configure**.

*The Gateway AntiVirus dialog box appears.*

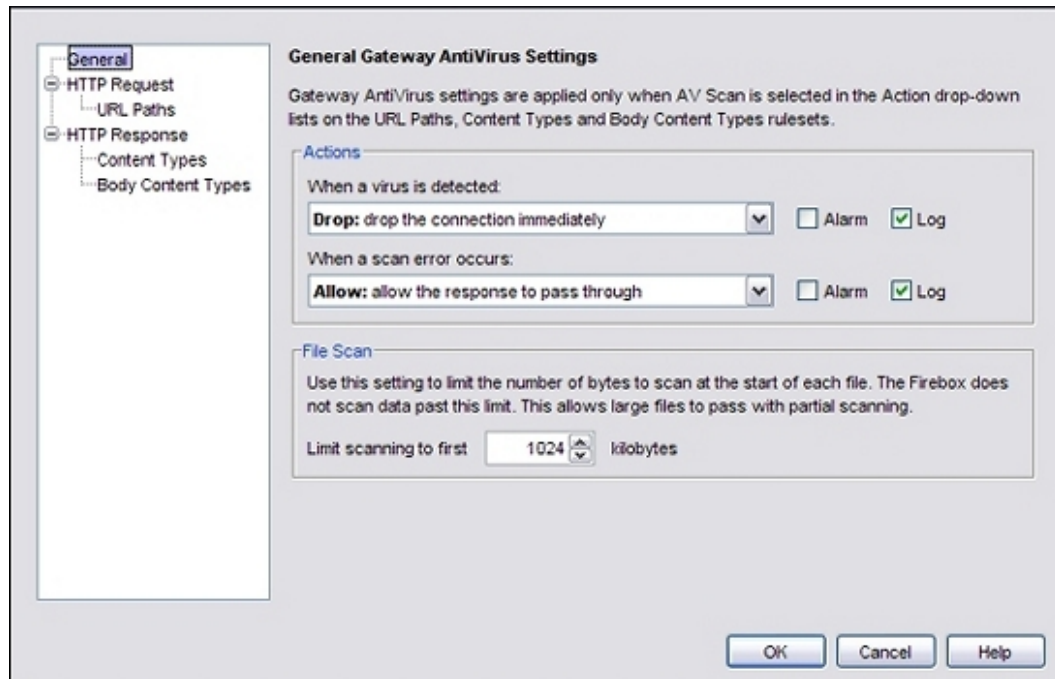


2. Select the policy you want to enable Gateway AntiVirus for and click **Enable**.

*The Gateway AV status changes to Enabled.*


3. Click **Configure**.

*The General Gateway AntiVirus Settings for that policy appear.*



4. From the **When a virus is detected** drop-down list, select the action the XTM device takes if a virus is detected in an email message, file, or web page. See the beginning of this section for a description of the actions.
5. From the **When a scan error occurs** drop-down list, select the action the XTM device takes when it cannot scan an object or an attachment. Attachments that cannot be scanned include binhex-encoded messages, certain encrypted files, or files that use a type of compression that Gateway AV does not support such as password-protected Zip files. See the beginning of this section for a description of the actions.
6. To create log messages for the action, select the **Log** check box for the antivirus response. If you do not want to record log messages for an antivirus response, clear the **Log** check box.
7. To trigger an alarm for the action, select the **Alarm** check box for the antivirus response. If you do not want to set an alarm, clear the **Alarm** check box for that action.
8. In the **Limit scanning to first** text box, type the file scan limit.  
For information about the default and maximum scan limits for each XTM device model, see *About Gateway AntiVirus Scan Limits* on page 1181.

You can also configure Gateway AntiVirus actions in the **Edit Policy Properties** dialog box.

1. Double-click the policy.
2. Select the **Properties** tab.
3. Click .
4. From the **Categories** list, select **AntiVirus**.

## Configure Gateway AntiVirus Actions in Policy Rulesets

For the HTTP proxy, the General Gateway AntiVirus settings only apply when AV Scan is selected in the **Action** drop-down lists on the **URL Paths**, **Content Types**, and **Body Content Types** rulesets for the policy. By default, the Activate Gateway AntiVirus Wizard sets the default action for content that does not match a proxy rule to **AV Scan**. You can improve Gateway AV performance if you change the default action for content that does not match one of the configured proxy rules.

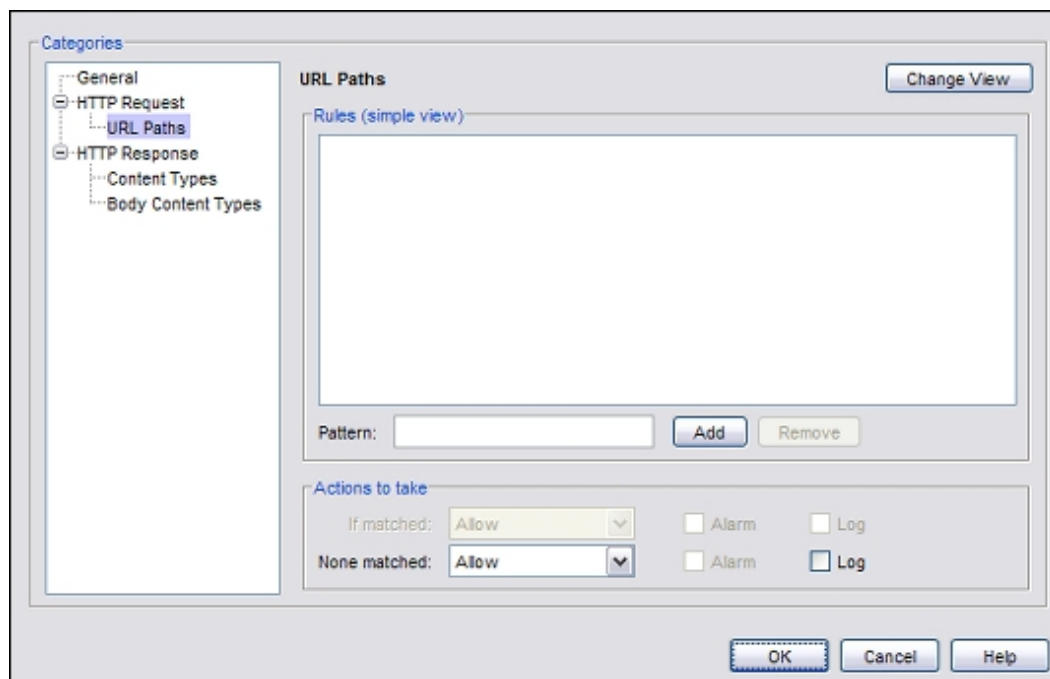
To optimize performance, you can configure Gateway AV actions for the HTTP proxy to make the proxy more selective about which content types to scan. When you set the **None matched** action to **AV Scan** for the **URL Paths**, **Content Types**, or **Body Content Types** categories, the HTTP proxy scans all objects that do not match a rule.

To set the actions for HTTP proxy rulesets, follow the instructions in the subsequent section. You can also use the instructions to configure the Gateway AV actions by content type for the POP3 and SMTP proxies.

### Configure AV Actions Based on URL Paths

1. In the **Categories** tree, expand **HTTP Request** and select **URL Paths**.

*The URL Paths rules and actions settings appear.*



2. From the **None matched** drop-down list, select **Allow**.

*With this setting, URLs that do not match a rule in the list are not scanned by Gateway AV.*

If you add rules to the **URL Paths Rules** list, you can set the **If matched** action to **AV Scan** to scan the content if the URL matches a rule in the list.

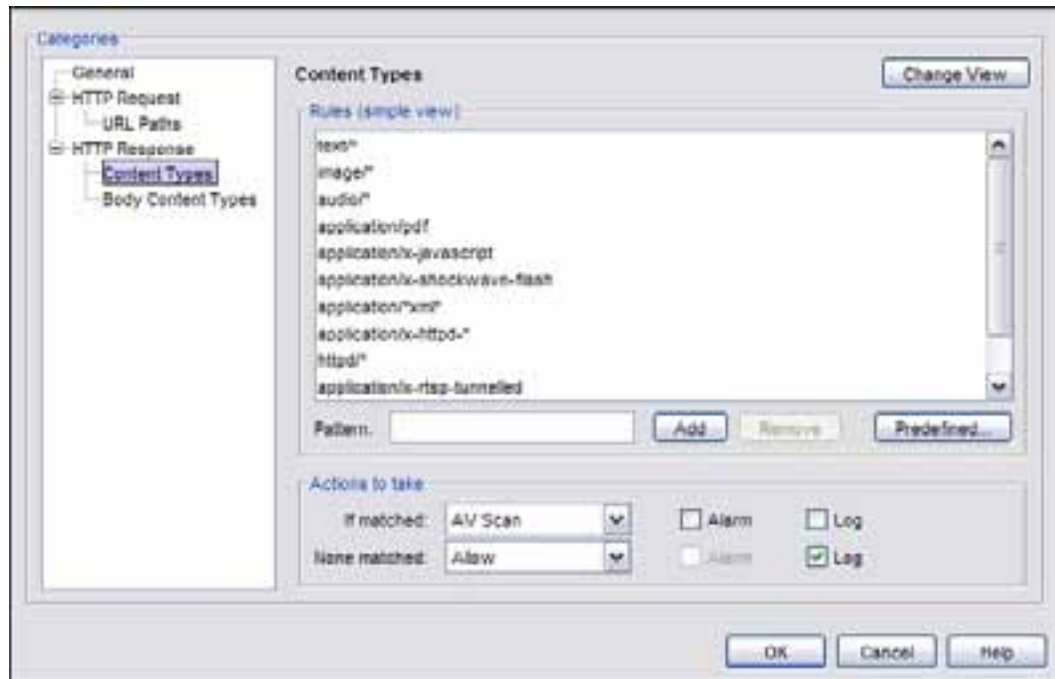
- For information about actions, see *Add, Change, or Delete Rules*.
- For information about how to add URL Paths, see *HTTP Request: URL Paths*.



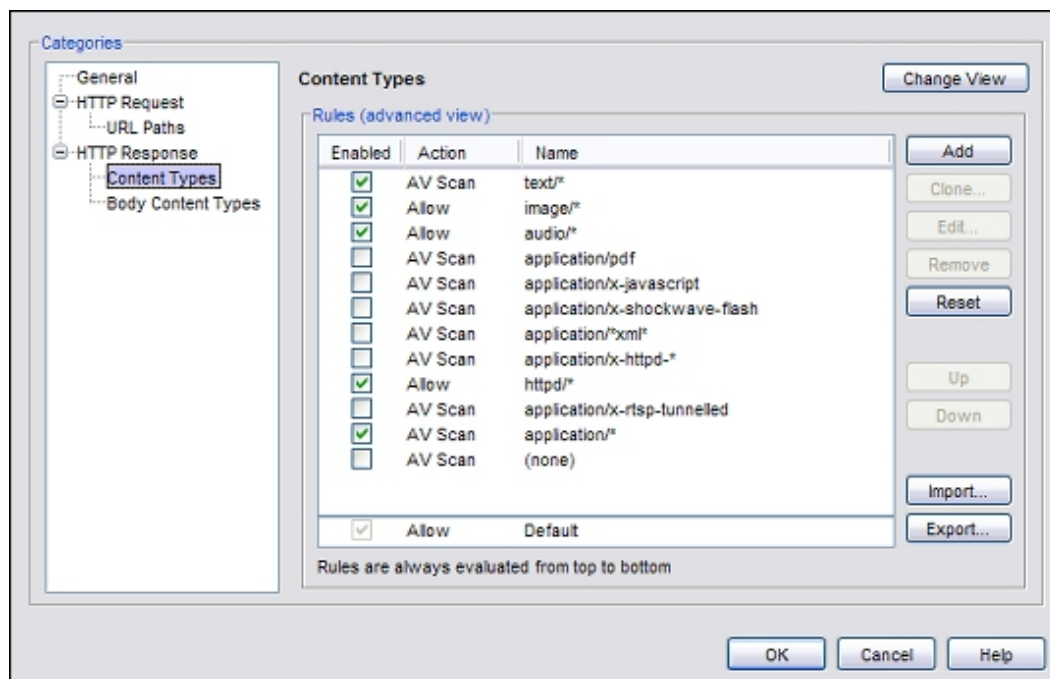
## Configure AV Actions Based on Content Types

You can configure the actions for Content Type rules to scan the content types that are most likely to contain a virus, and to not scan other content types. To set the actions more granularly based on content type, use the advanced view of the rules.

1. In the **Categories** tree, expand **HTTP Response** and select **Content Types**.



2. From the **None matched** drop-down list, select **Allow**.  
Or, select an option other than the default (**AV Scan**).
3. Click **Change View**.  
*The Content Type Rules settings change to the advanced view.*



- To select which rules to use, select or clear the **Enabled** check box for each rule .
- For each enabled rule, double-click the rule to select the **Action** to take for that rule.

*The Edit Content Type Rule dialog box appears.*

- To scan all content that matches the rule, set the action to **AV Scan**.
- To allow content that matches the rule without an AV scan, set the action to **Allow**.

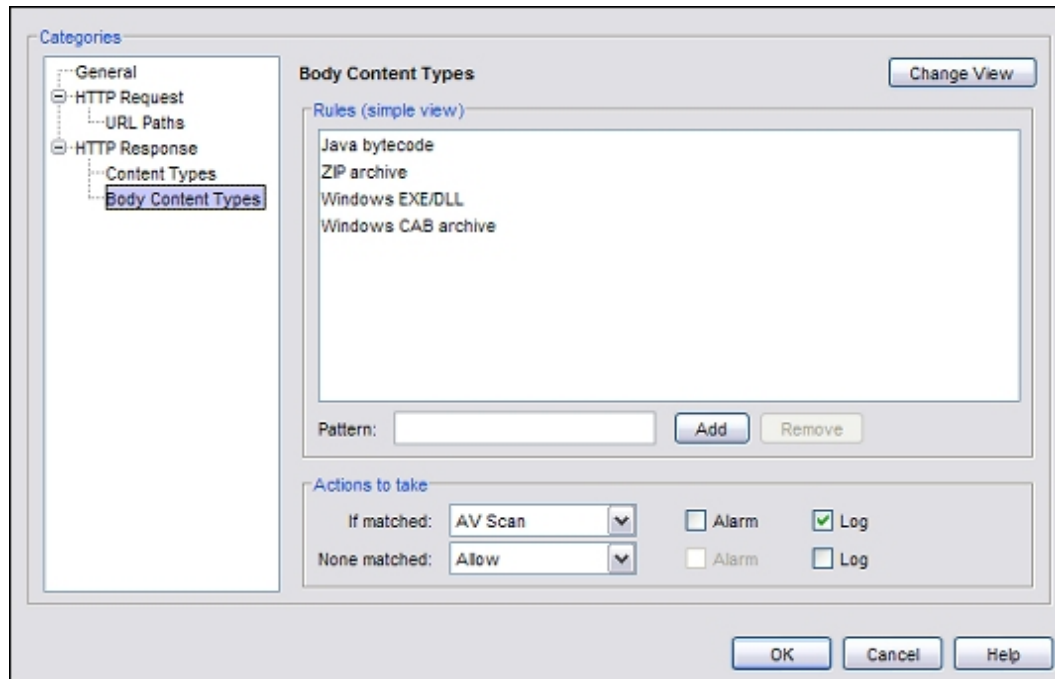
For example, you could set the action to **AV Scan** only for **text/\*** and **application/\*** content types, and set the action to **Allow** for other content types that are less likely to pose a threat.

For information about HTTP Response Content Types, see *HTTP Response: Content Types*.

## Configure AV Actions Based on Body Content Types

You can also configure the actions for the Body Content Types rules.

- In the **Categories** tree, expand **HTTP Response** and select **Content Types**.




2. From the **None matched** drop-down list, select **Allow**.  
Or, select an option other than the default (**AV Scan**).
3. From the **If matched** drop-down list, select **AV Scan**.  
Or, click **Change View** to set rules individually for different body content types.

For information about HTTP Response Body Content Types, see *HTTP Response: Body Content Types*.

## Configure Alarm Notification for Antivirus Actions

You can configure an alarm notification to tell users when a proxy rule applies to network traffic. If you enable alarms for a proxy antivirus action, you must also configure the type of alarm to use in the proxy policy.

To configure the alarm type to use for a proxy policy:

1. Double-click the policy to edit.
2. Select the **Properties** tab.
3. Click .
4. Select the **Proxy and AV Alarms** category.
5. Configure the Proxy/AV Alarms settings as described in *Set Logging and Notification Preferences* on page 723.

## Unlock a File Locked by Gateway AntiVirus

WatchGuard System Manager provides an executable file to unlock attachments locked by Gateway AntiVirus. When Gateway AntiVirus locks a file, the locked file remains attached to the email message, but the file has an appended file extension of .clk. So, for example, if the original file attachment name was example.zip, the locked file attachment name is example.zip.clk. To unlock a file, you must save the attached .clk file to the computer where you have installed WatchGuard System Manager.

The executable file utility to unlock a file is located in:

C:\Program Files\WatchGuard\wsm11\bin\unlock.exe

To open a locked file:

1. Save the file attachment to a location on the computer where WatchGuard System Manager is installed. It may be easiest if you copy the file to the same location as the unlock.exe utility.
2. Open a command prompt.
3. Type **Unlock** <path and filename of locked file>.

For example, if the locked file is called example.zip.clk, and it is located in the root directory (C:\), you type:

```
unlock c:\example.zip.clk
```

The utility saves the unlocked file, without the .clk file extension to the local directory. In this example, the utility writes the unlocked file, example.zip, to the C:\Program Files\WatchGuard\wsm11\bin\ directory.

After you unlock the file, we recommend that you use a different antivirus tool to scan the file and examine the content of the attachment.

## Configure Gateway AntiVirus to Quarantine Email

The WatchGuard Quarantine Server provides a safe, full-featured quarantine mechanism for any email messages suspected or known to be spam or to contain viruses. This repository receives email messages from the SMTP proxy and filtered by spamBlocker.

To configure Gateway AntiVirus to quarantine email:

1. When you run the Activate Gateway AntiVirus Wizard (as described in *Activate Gateway AntiVirus* on page 1168), you must make sure you use Gateway AntiVirus with the SMTP proxy. The POP3 proxy does not support the Quarantine Server.
2. When you set the actions spamBlocker applies for different categories of email (as described in *Configure spamBlocker* on page 1146), make sure you select the **Quarantine** action for at least one of the categories. When you select this action, you are prompted to configure the Quarantine Server if you have not already done so.

You can also select the **Quarantine** action for email messages identified by Virus Outbreak Detection to contain viruses. For more information, see *Configure Virus Outbreak Detection Actions for a Policy* on page 1151.

## About Gateway AntiVirus Scan Limits

Gateway AntiVirus scans each file up to a specified kilobyte count. Any additional bytes in the file are not scanned. This allows the proxy to partially scan very large files without a large effect on performance. The default and maximum scan limits can be different for each XTM device model.

### File Scan Limits by XTM Device Model, in Kilobytes

Model	Minimum	Maximum	Default
XTM 2 Series	250	5120	512
XTM 5 Series	250	30720	1024
XTM 8 Series	250	30720	1024
XTM 1050	250	30720	1024

For information about how to set the scan limit, see *Configure Gateway AntiVirus Actions* on page 1172.

## Update Gateway AntiVirus Settings

The XTM device has several settings for the Gateway AntiVirus engine regardless of which proxy it is configured to work with. For more information, see *Configure Gateway AV Decompression Settings* on page 1182.

It is important to update the signatures for Gateway AntiVirus/Intrusion Prevention Service. You can update the signatures in two ways:

- *Configure the Gateway AV Update Server* to enable automatic updates
- Update the signatures manually in Firebox System Manager, as described in *Subscription Services Status and Manual Signatures Updates* on page 780.

## If you Use a Third-Party Antivirus Client

If you use a third-party antivirus service on computers that are protected by your XTM device, you could have problems with updates for the third-party service. When the client for that secondary service tries to update its signature database on port 80, the WatchGuard Gateway AV service, working through the HTTP proxy, recognizes the signatures and strips them before they download to the client. The secondary service cannot update its database. To avoid this problem, you must add *HTTP-Proxy: Exceptions* to the policy that denies the update traffic. You must know the host name of the third-party signature database. Then you can add that host name as an allowed exception.

To configure an exception on the XTM device that protects the computers that want to download IPS or antivirus signatures:

1. Open the definition of the HTTP proxy policy that denies the update traffic.
2. From the **Categories** section, select **HTTP Proxy Exceptions**.
3. In the text box adjacent to **Add**, type the host name of the update server. If you want to allow all subdomains to bypass the proxy, use the wildcard symbol (\*) before and after the host name. For example, *\*watchguard.com\** allows all subdomains of watchguard.com, such as *antivirus.watchguard.com* and *updates.watchguard.com*.
4. Click **Add**. Repeat Steps 4–5 for additional exceptions you want to add.
5. Click **OK** twice to close both dialog boxes.
6. *Save the Configuration File*.

## Configure Gateway AV Decompression Settings

Gateway AV can scan inside compressed files if you enable decompression in the Gateway AV configuration settings.

1. From Policy Manager, select **Subscription Services > Gateway AntiVirus > Configure**.  
*The Gateway AntiVirus dialog box appears.*
2. From the **Gateway AntiVirus** dialog box, click **Settings**.  
*The Gateway AV Decompression Settings dialog box appears.*

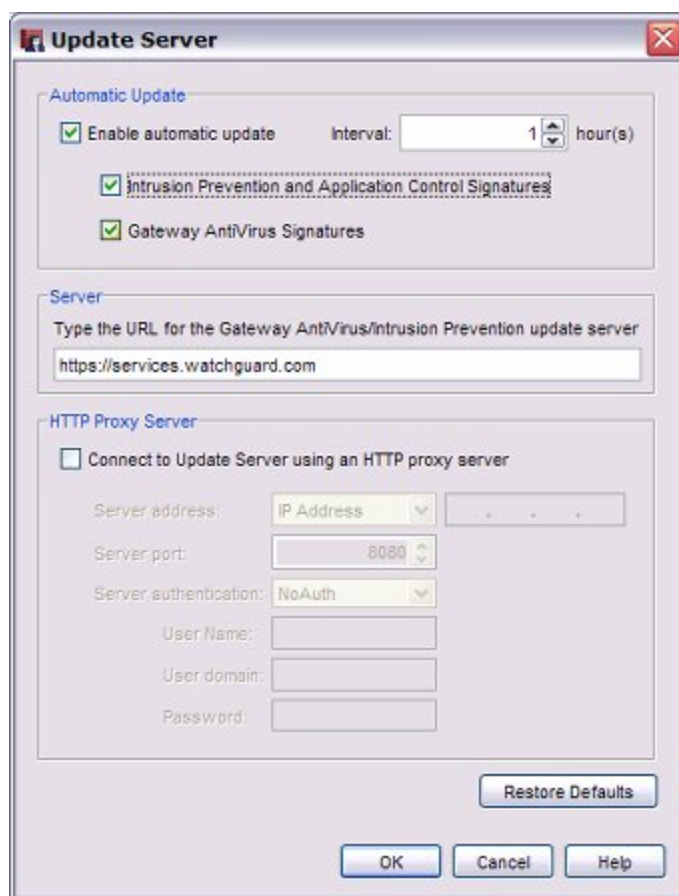


3. To scan inside compressed attachments, select the **Enable Decompression** check box. Select or type the number of compression levels to scan. If you enable decompression, we recommend that you keep the default setting of three levels, unless your organization must use a larger value. If you specify a larger number, your XTM device could send traffic too slowly. Gateway AntiVirus supports up to six levels. If Gateway AntiVirus detects that the archive depth is greater than the value set in this field, it will generate a scan error for the content.  
Compressed attachments that cannot be scanned include encrypted files or files that use a type of compression that we do not support such as password-protected Zip files. To set the action for the XTM device when it finds a message it cannot scan, select an action for **When a scan error occurs** in the **General** category of the policy configuration.
4. Click **Restore Defaults** if you want to reset the user interface to default settings.
5. Click **OK**.

## Configure the Gateway AV Update Server

Gateway AntiVirus downloads signature updates from a signature update server. Gateway AV, IPS, and Application Control use the same signature update server. When you configure the signature update server for any of these subscription services, the settings apply to all three services.

1. From Policy Manager, select **Subscription Services > Gateway AntiVirus > Configure**.  
or, select **Subscription Services > Intrusion Prevention > Configure**.
2. Click **Update Server**.  
*The Update Server dialog box appears.*



3. To enable automatic updates for the server, select the **Enable automatic update** check box. Enter the number of hours between automatic updates in the **Interval** drop-down list.
  - If you want the XTM device to download a new set of Intrusion Prevention and Application Control signatures at this interval, select the **Intrusion Prevention and Application Control Signatures** check box.
  - If you want the XTM device to download a new set of Gateway AV signatures at this interval, select the **Gateway AV Signatures** check box.
4. Do not change the URL of the update server for Gateway AV or IPS unless you are told to do so by WatchGuard. If you change the URL accidentally or incorrectly, click **Restore Defaults** to return to the default setting.
5. Click **OK**.

## Connect to the Update Server Through an HTTP Proxy Server

If your XTM device must connect through an HTTP proxy to get to the signature update server, you must add information about the HTTP proxy server to your update server configuration.

1. From the **Gateway AntiVirus** dialog box, click **Update Server**.
2. Select the **Contact the Update Server using an HTTP proxy server** check box.
3. From the **Server address** drop-down list, select whether you identify your HTTP proxy server by host name or IP address. Type the host name or IP address in the adjacent text box.



4. Most HTTP proxy servers receive requests on port 8080. If your HTTP proxy uses a different port, enter it in the **Server port** text box.
5. From the **Server authentication** drop-down list, select the type of authentication your HTTP proxy server uses. Select **NoAuth** if your HTTP proxy does not require authentication. If your HTTP proxy server requires **NTLM** or **Basic** authentication, enter your user name, user domain, and password in the text boxes.
6. Click **OK**.

## Block Access from the Trusted Network to the Update Server

If you do not want to allow all users on your trusted network to have unfiltered access to the IP address of the signature database, you can use an internal server on your trusted network to receive the updates. You can create a new HTTP proxy policy with *HTTP-Proxy: Exceptions* or an HTTP packet filter policy that allows traffic only from the IP address of your internal server to the signature database.

## Update Signatures Manually

For information about how to see the status of Gateway AntiVirus signature updates, and how to manually force an update to the most current signatures, see *Subscription Services Status and Manual Signatures Updates*.



# 35 Intrusion Prevention Service

---

## About Intrusion Prevention Service

Intrusions are direct attacks on your computer. Usually the attack exploits a vulnerability in an application. These attacks are created to cause damage to your network, get sensitive information, or use your computers to attack other networks.

Intrusion Prevention Service (IPS) provides real-time protection from threats, including spyware, SQL injections, cross-site scripting, and buffer overflows. When a new attack is identified, the features that make the intrusion attack unique are recorded. These recorded features are known as the signature. IPS uses these signatures to identify intrusion attacks.

By default, when you enable and configure IPS, the IPS configuration applies globally to all traffic. You can also choose to disable IPS on a per-policy basis.

## IPS Threat Levels

IPS categorizes IPS signatures into five threat levels, based on the severity of the threat. The severity levels, from highest to lowest are:

- Critical
- High
- Medium
- Low
- Information

When you enable IPS, the default setting is to drop and log traffic that matches the Critical, High, Medium, or Low threat levels. Traffic that matches the information threat level is allowed and not logged by default.

## Add the IPS Upgrade

To enable IPS on your XTM device, you must:

1. *Get a Feature Key from LiveSecurity* on page 59
2. *Add a Feature Key to Your XTM Device* on page 62
3. *Configure Intrusion Prevention*

## Keep IPS Signatures Updated

New intrusion threats appear on the Internet frequently. To make sure that IPS gives you the best protection, you must update the signatures frequently. You can configure the XTM device to update the signatures automatically from WatchGuard, as described in *Configure the IPS Update Server*.

**Note** *The XTM 2 Series models have a smaller number of IPS signatures than the other XTM device models.*

## See IPS Status

You can see statistics on current IPS activity and update the IPS signatures in Firebox System Manager. For more information, see *Application Control and Intrusion Prevention Service Statistics* on page 778.

## Configure Intrusion Prevention

To use Intrusion Prevention Service (IPS), you must have a feature key to enable the service.

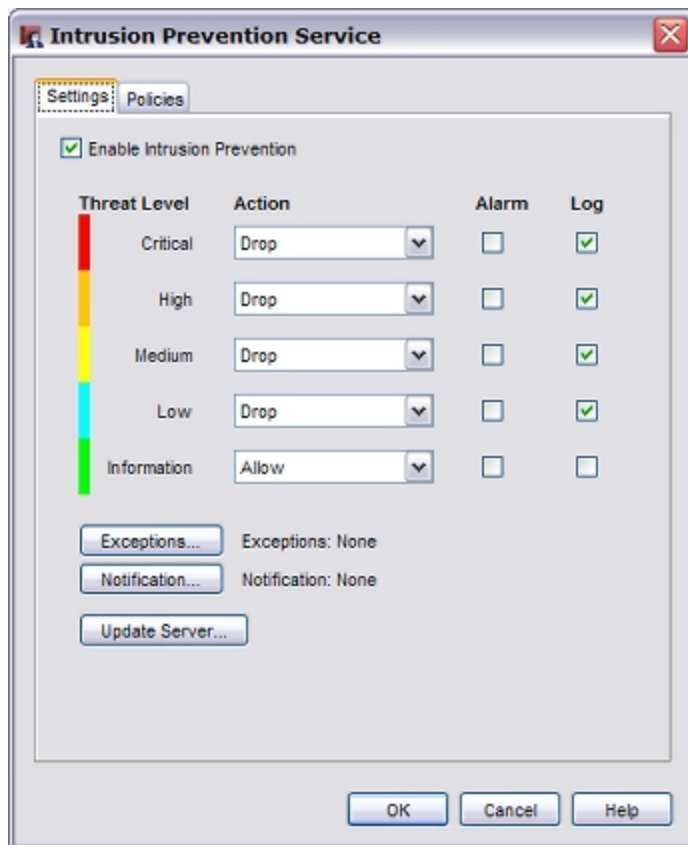
For more information, see:

- *Get a Feature Key from LiveSecurity* on page 59
- *Add a Feature Key to Your XTM Device* on page 62

## Enable IPS and Configure IPS Actions

To enable IPS:

1. Select **Subscription Services > Intrusion Prevention**.  
*The Intrusion Prevention Service dialog box appears.*



2. Select the **Enable Intrusion Prevention** check box.
3. For each threat level, select the action. Available actions are:
  - **Allow** — Allows the connection.
  - **Drop** — Denies the request and drops the connection. No information is sent to the source of the message.
  - **Block** — Denies the request, drops the connection, and adds the IP address of the sender to the Blocked Sites list.
4. For each threat level, select the **Log** check box if you want to send a log message for an IPS action. Or, clear the **Log** check box if you do not want to log IPS actions for that threat level.
5. For each threat level, select the **Alarm** check box if you want to trigger an alarm for an IPS action. Or, clear the **Alarm** check box if you do not want to trigger an alarm for that threat level.
6. Click **Save**.

## Configure other IPS Settings

Click **Exceptions** to add signatures to the exceptions list. For more information, see *Configure IPS Exceptions*.

Click **Notification** to configure notification settings for IPS. For more information, see *Set Logging and Notification Preferences*.

Click **Update Server** to configure signature update settings. For more information, see *Configure the IPS Update Server*.

Click the **Policies** tab to disable or enable IPS for each policy. For more information, see *Disable or Enable IPS for a Policy*

## Configure the IPS Update Server

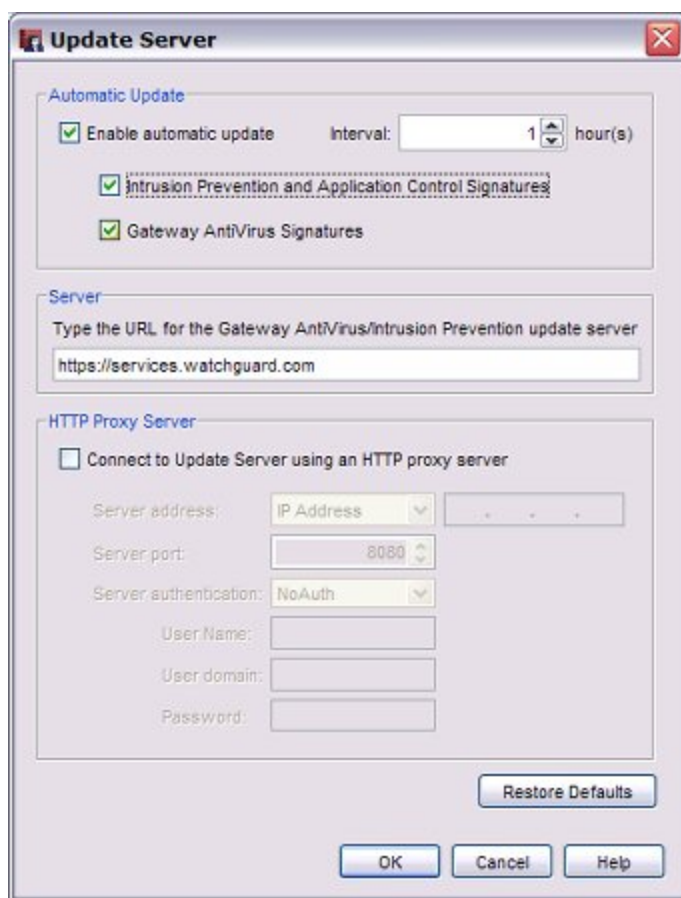
The Intrusion Prevention Service (IPS) downloads signature updates from a signature update server. Gateway AV, IPS, and Application Control use the same update server settings. When you configure the update server for any one of these subscription services, the settings apply to all three services.

IPS and Application Control signature updates are delivered together in one file.

## Configure Automatic Signature Updates

1. Select **Subscription Services > Intrusion Prevention**.
2. Click **Update Server**.

*The Update Server dialog box appears.*



3. To enable automatic signature updates, select the **Enable automatic update** check box. This option is enabled by default.
4. From the **Interval** drop-down list, enter the number of hours between automatic updates.
5. Select the **Intrusion Prevention and Application Control Signatures** check box to automatically update signatures at the selected update interval.

Do not change the **Update server URL** unless you are told to do so by WatchGuard. If you change the URL accidentally or incorrectly, click **Restore Default** to return to the default setting.

## Connect to the Update Server Through an HTTP Proxy Server

If your XTM device must connect through an HTTP proxy to get to the signature update server, you must add information about the HTTP proxy server to your update server configuration.

1. In the **ProxyServer** section, select the **Connect to Update server using an HTTP proxyserver** checkbox.
2. From the **Server address** drop-down list, select whether you identify your HTTP proxy server by host name or IP address. Type the host name or IP address in the adjacent text box.
3. Most HTTP proxy servers receive requests on port 8080. If your HTTP proxy uses a different port, type it in the **Server port** text box.
4. From the **Server authentication** drop-down list, select the type of authentication your HTTP proxy server uses.
  - If your HTTP proxy does not require authentication, select **NoAuth**
  - If your HTTP proxy server requires **NTLM** or **Basic** authentication, type your **User name**, **Domain**, and **Password** in the text boxes
5. Click **OK**.

## Block Access from the Trusted Network to the Update Server

If you do not want to allow all users on your trusted network to have unfiltered access to the IP address of the signature database, you can use an internal server on your trusted network to receive the updates. You can create a new HTTP proxy policy with *HTTP-Proxy: Exceptions* or an HTTP packet filter policy that allows traffic only from the IP address of your internal server to the signature database.

## Update Signatures Manually

For information about how to see the status of IPS signature updates and how to manually force an update to the most current signatures, see *Subscription Services Status and Manual Signatures Updates*.

## Configure IPS Exceptions

When you enable the IPS feature, the XTM device examines traffic to look for patterns of traffic that match the signatures of known intrusions. When an IPS signature match occurs, the XTM device denies the content and the intrusion is blocked. If you want to allow traffic that is blocked by an IPS signature, you can find the identification number for the signature (the signature ID) and add the signature ID to the IPS exception list.

## Find the IPS Signature ID

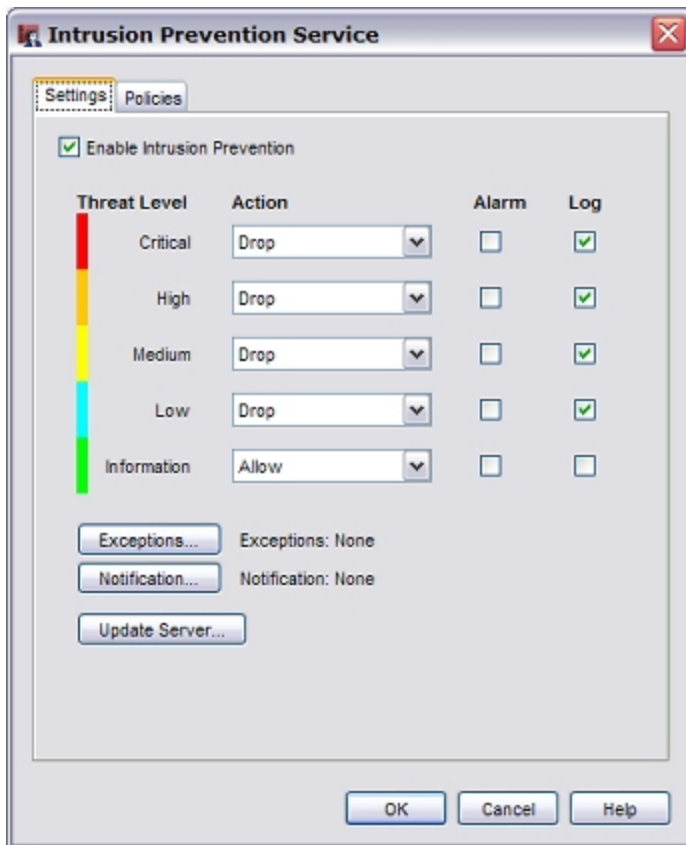
When the XTM device blocks a connection based on a match with an IPS signature, the signature ID appears in the log file if you have enabled logging for IPS. To see which IPS signature blocked the connection, look in the log file for the IPS signature ID number. If a connection that you want to allow is blocked by an IPS signature, use the signature ID to add an IPS exception to allow that connection.

In the Firebox System Manager, you can look up the IPS signature ID to see information about the threat a signature ID represents. For information about how to look up an IPS signature, see *Show IPS Signature Information*.

## Add an IPS Signature Exception

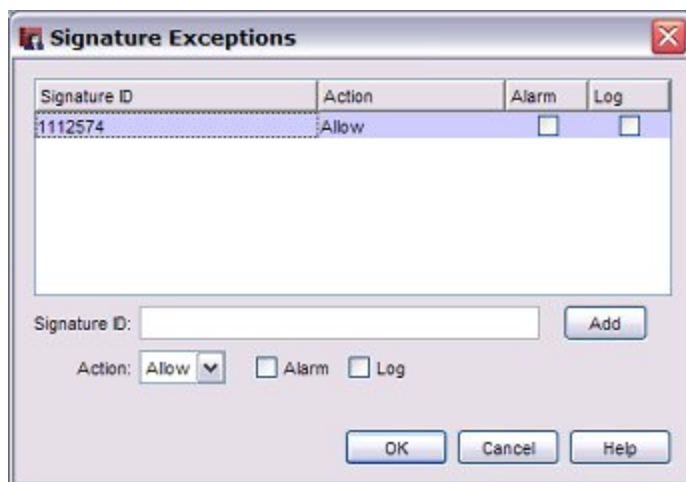
To add an IPS signature exception:

1. Select **Subscription Services > Intrusion Prevention**.  
*The Intrusion Prevention Service dialog box appears.*



2. Click **Exceptions**.  
*The Signature Exceptions dialog box appears.*





3. In the **Signature ID** text box, type the ID of the signature you want to add.
4. From the **Action** drop-down list, select the action you want IPS to take for this signature. The available actions are:
  - **Allow** — Allows the connection.
  - **Drop** — Denies the request and drops the connection. No information is sent to the source of the message.
  - **Block** — Denies the request, drops the connection, and adds the IP address of the sender to the Blocked Sites list.
5. Select the **Log** check box if you want to send a log message for this IPS exception.
6. Select the **Alarm** check box if you want to send an alarm for this IPS exception.
7. Click **Add**.

*The exception is added to the Signature Exceptions list.*

To edit settings for an exception, click the **Action**, **Alarm** or **Log** column in the Signature Exceptions table to edit the setting.

To remove an exception, click the exception and click **Remove**.

## Show IPS Signature Information

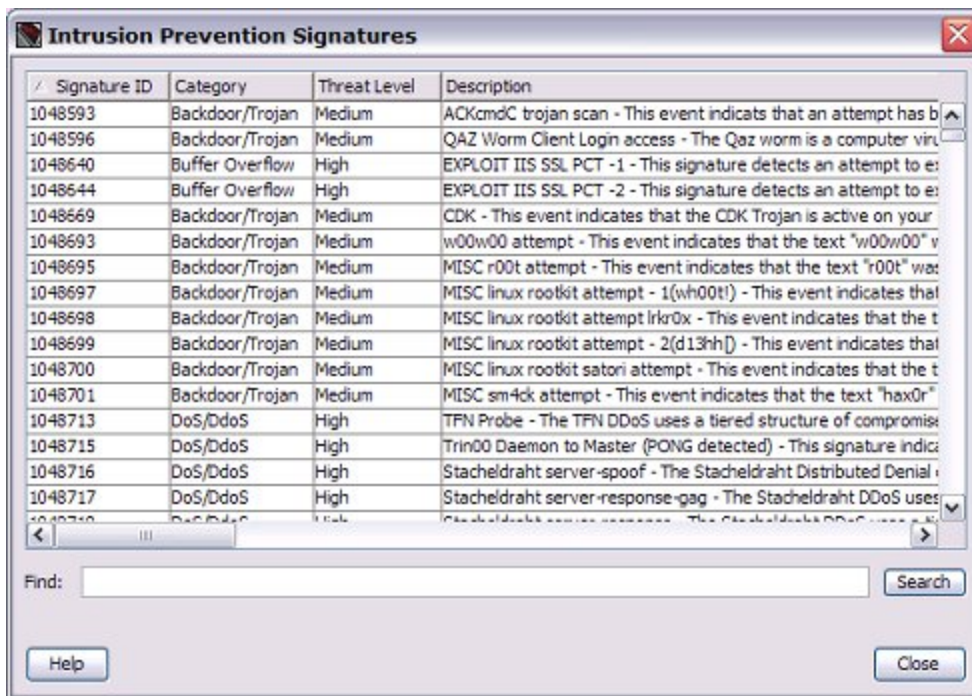
When the XTM device denies content based on a match with an IPS signature, the signature ID appears in the log file. To see more information about the signature ID that blocked the content, you can look up the IPS signature ID number in Firebox System Manager. Or, you can search for more signature details on the WatchGuard IPS Security Portal.

## Find IPS Signature Information in Firebox System Manager

To look up information about an IPS signature:

1. Open Firebox System Manager.
2. Select the **Subscription Services** tab.
3. In the **Intrusion Prevention** section, click **Show**.

*The Intrusion Prevention Signatures dialog box appears.*



The Intrusion Prevention Signatures dialog box shows all signatures, sorted by signature ID.

- The **Signature ID** is the ID that appears in the log file when content is blocked by this signature.
  - The **Category** is the type of threat.
  - The **Threat Level** indicates the severity of the threat.
  - The **Description** column contains a short description of the threat.
4. To search for signatures that contain a specific word or signature ID, type the text to search for in the **Find** text box. Click **Search**.
- The signatures that match your search are highlighted in the list.*

If a connection that you want to allow is blocked by an IPS signature, you can use the signature ID to add an IPS exception.

The threat levels are the same five threat levels you see in the IPS configuration. For information about how to change the action for each threat level, see *Configure Intrusion Prevention*.

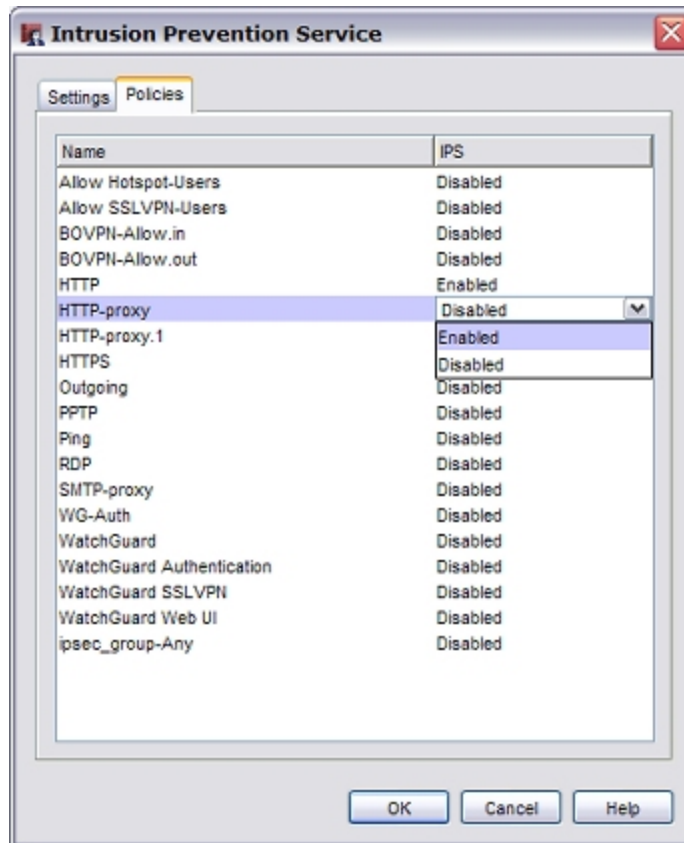
You can also look up information about an IPS signature on the WatchGuard IPS Security Portal. For more information, see *Look up IPS Signatures on the IPS Security Portal*

## Disable or Enable IPS for a Policy

When you enable IPS, it is automatically enabled for all policies. You can choose to disable it for a specific policy in the IPS configuration or when you edit a policy.

To disable or enable IPS for a policy:

1. Select **Subscription Services > Intrusion Prevention**.  
*The Intrusion Prevention Service dialog box appears.*
2. Select the **Policies** tab.  
*The list of configured policies appears.*



3. To disable IPS for a policy, click the IPS column for that policy.  
*A drop-down list appears, with the choices Enabled or Disabled.*
4. Select **Disabled** to disable IPS for the selected policy.  
Or, click **Enabled** to enable IPS for the policy.
5. Click **OK**.

You can also choose to enable or disable IPS when you edit a policy:

1. In Policy Manager, add or edit a policy.  
*The Policy Properties dialog box appears with the Policy tab selected.*
2. Select the **Enable IPS for this policy** check box.  
Or, clear the check box to disable it.
3. Click **OK**.



# 36 Application Control

---

## About Application Control

Application Control is a subscription service that enables you to monitor and control the use of applications on your network. Application Control uses signatures that can identify and block over 1500 applications. In the Application Control action, you select the applications by name, and choose to block or allow traffic for each application. Then you apply the Application Control action to the applicable policy. You do not need to create or maintain your own custom rules to identify applications. The Application Control service provides frequent updates to application signatures to keep the protection current.

You can use Application Control to block the usage of specific applications, and you can report on application use and use attempts. For some applications, you can block specific application behaviors, such as file transfer.

When Application Control blocks content that matches an Application Control action, the user who requested the content sees that the content is not available, but does not get a message that the content was blocked by Application Control.

## Add the Application Control Upgrade

To enable Application Control on your XTM device, you must:

1. *Get a Feature Key from LiveSecurity* on page 59
2. *Add a Feature Key to Your XTM Device* on page 62
3. *Configure Application Control Actions*

## Keep Application Control Signatures Updated

New applications appear on the Internet frequently. To make sure that Application Control can recognize the latest applications, you must update the signatures frequently. You can configure the XTM device to update the signatures automatically from WatchGuard, as described in *Configure the Application Control Update Server*.

**Note** *The XTM 2 Series models have a smaller number of Application Control signatures than the other XTM device models.*

## How Application Control Identifies Applications

Application Control uses several methods to identify traffic associated with specific applications:

- Simple pattern matching of patterns in the packets.
- Simple L4 port-based rules for applications in the Network Protocols category. Applications can be identified by their use of well known ports.
- Examination of the SSL certificates that are used.
- Behavior correlation of related signatures. When the first few packets arrive, Application Control can identify that the traffic is Facebook. As it examines more packets, it could further identify the traffic as a Facebook application.

The most complex applications to identify are applications such as Skype that use their own implementation of encrypted communication. Unlike other VoIP applications, Skype is based on peer-to-peer technology. There is no central infrastructure. The entire Skype directory of users is distributed among all the nodes in the network. Once a user registers with the service and downloads the client, their system could potentially become a node in the network, even if it is not actively making a call. Skype was designed to get around firewalls and it dynamically uses a combination of ports.

Together with signatures, Application Control uses a patent pending algorithm to identify these encrypted applications such as Skype, Winny, and Thunder. Application Control examines traffic characteristics such as packet sizes, patterns of DNS lookups, and the patterns of different ports that are used.

## Application Control — Begin with Monitoring

When you start to use Application Control, we recommend that you first configure your policies to send log messages for all application use so that you get a true understanding of the applications that are used on the network. To monitor application use, you can enable Application Control and logging for all policies that match the application traffic. After you enable Application Control and logging for a policy, all application activity for traffic through that policy is recorded in the log database and available for the Application Control reports, even if the Global Application Control action is empty.

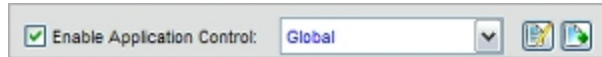
## Monitor Application Use

To monitor application use:

1. Create an Application Control action that does not block any applications.  
*The Global action is empty by default, so it does not block applications.*

For more information, see *Configure Application Control Actions*.

2. Apply the empty Application Control action to the policies that handle traffic you want to monitor.



For information about how to enable Application Control, see *Enable Application Control in a Policy*.

For information about which policies to configure, see *Policy Guidelines for Application Control*.

3. Enable logging in each policy that has Application Control enabled.

For information about how to enable logging in a policy, see *Configure Logging and Notification for a Policy*.

**Note** *If you do not enable logging for a policy that has Application Control enabled, Application Control saves log information only for blocked applications.*

## Application Control Reports

After you have enabled Application Control and logging in your policies, you can use Report Manager to run Application Control reports that summarize information about the applications used on your network.

**Note** *To run Application Control reports, you must set up a Log Server and a Report Server. For more information about WatchGuard servers, see *About WatchGuard Servers*.*

Report Manager includes these predefined reports for Application Control:

### Application Control Reports

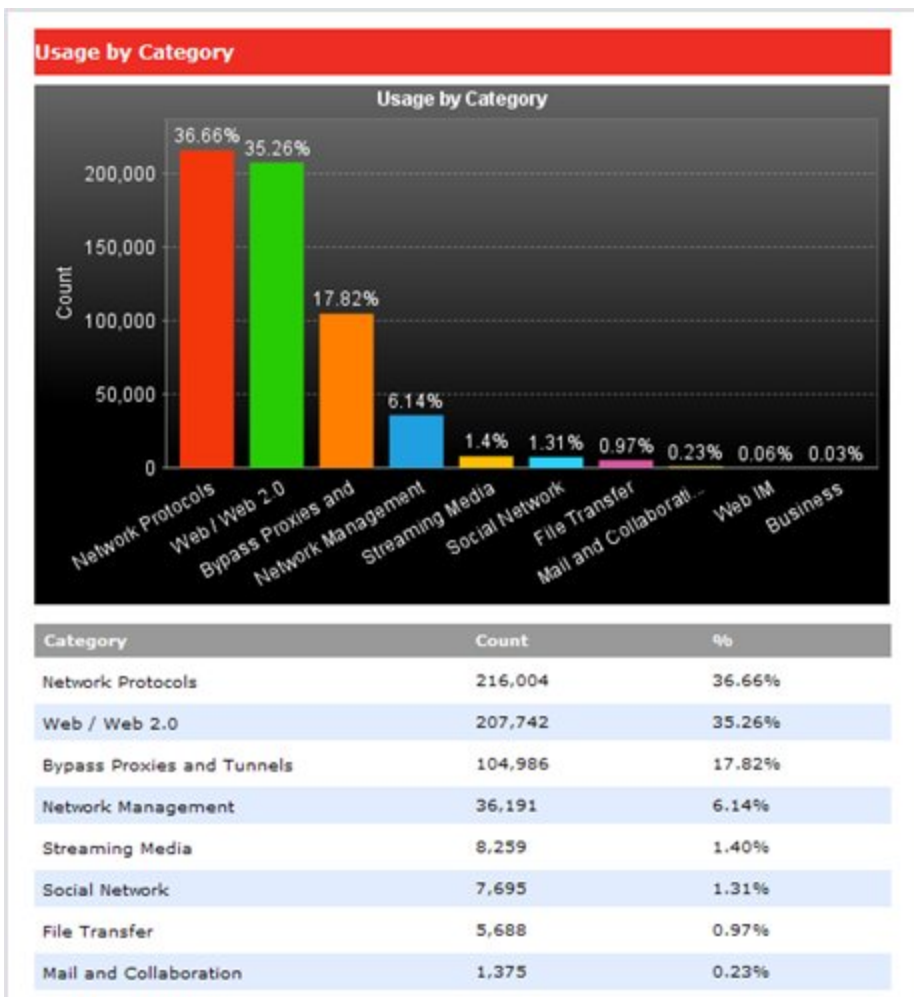
- Application Usage Summary
- Blocked Application Summary

### Client Reports — Show which users use the applications

- Top Clients by Application Usage
- Top Clients by Blocked Applications
- Top Clients by Blocked Categories

Client reports show the names of users who use applications if you have configured authentication on the firewall.

Before you configure Application Control to block applications, we recommend that you examine the Application Usage Summary and the Top Clients by Application Usage reports.



When you look at the Application Usage reports, consider these questions:

- Does the report show any application categories that seem to conflict with corporate policy?
- Are the applications appropriate for business use?
- Which users use the applications? Fireware XTM provides reports that show application use by client. The authentication capabilities in Fireware XTM enable you to see client reports by user name rather than by IP address. You can also identify user traffic in Terminal Services environments.

For information about how to configure Terminal Services, see *Configure Terminal Services Settings*.

If the reports show an application that you are not familiar with, you can look up information about the application on the WatchGuard Application Control Security Portal at <http://www.watchguard.com/SecurityPortal/AppDB.aspx>.

For more information about Report Manager, see *About WatchGuard Report Manager*.



## Policy Guidelines for Application Control

To monitor or block application usage, you must enable Application Control for all policies that handle the application traffic. WatchGuard does not recommend that you apply the Global Application Control action to every policy. Because of the performance implications, you don't want — or need — to enable Application Control for every policy.

We recommend that you enable Application Control for these types of policies:

- Any outbound policy that handles HTTP or HTTPS traffic
- VPN policies that use 0.0.0.0/0 routes (default-route VPNs)
- Any outbound policy if you are not sure how the policy is used
- Policies that use the 'Any' protocol
- Policies that use an 'Any-\*' alias, for example Allow 'Any-Trusted' to 'Any-External', on a specific port/protocol

It is not necessary to enable Application Control for a policy if you control the network on both sides of a traffic flow the policy handles. Some examples of these types of policies include:

- POS systems
- Intranet web applications
- Internal databases and traffic in a DMZ

It usually not necessary to enable Application Control for policies that are restricted by port and protocol and that allow only a known service. Some examples of these types of policies include:

- Default WatchGuard policies
- DNS traffic
- RDP
- VoIP - SIP and H.323 application layer gateways

To block evasive applications that dynamically use different ports, you must enable Application Control to block those applications in all of your policies. For more information about evasive applications, see *Manage Evasive Applications*.

For some examples of how to use Application Control with policies, see *Application Control Policy Examples*.

## Global Application Control Action

The Global Application Control action is created by default and cannot be removed. You can configure the Global Application Control action to control overall corporate policy. For example you can:

- Block all games
- Block use of peer-to-peer applications

The Global Application Control action does not apply to traffic unless you enable Application Control for policies in your configuration. You can assign the Global Application Control action directly to a policy, or you can use the Global Application Control action as a secondary action if traffic does not match the applications configured in a user-defined Application Control action assigned to a policy.

You can create more specific application actions to implement rules that apply to user groups or to specific interfaces. For example, you might want to apply some specific rules to allow one department to have access to an application.

If you know that an application is specifically restricted to a specific port, you can apply an Application Control action to a packet filter or proxy policy on that port only. If not, you must apply the Application Control action to an outgoing policy that covers all ports to make sure that you capture all possible traffic for the application.

## Configure Application Control Actions

To block application traffic, you need to create Application Control actions. You apply these actions to one or more policies to enforce consistent rules for application usage. An Application Control action contains a list of applications and associated actions. For each application, you can specify whether to drop or allow the connection. You also configure what action to take if traffic that does not match the applications is detected.

For each application, you can choose one of these actions:

- **Drop** — Block the selected application.
- **Allow** — Allow the selected application

For some applications, you can control specific application behaviors. For each behavior, you can set the action to **Drop** or **Allow**. The behaviors you can control depend on the application. The application behaviors you can control are:

- **Authority** — Log in
- **Access** — Command to access a server or peer
- **Communicate** — Communicate with server or peer (chat)
- **Connect** — Unknown command (P2P connect to peer)
- **Games** — Games
- **Media** — Audio and video
- **Transfer** — File transfer

For each Application Control action, you configure an action to take if traffic does not match the configured applications. You can set this action to:

- **Allow** — Allow traffic that does not match the configured applications
- **Drop** — Drop traffic that does not match the configured applications
- **Use Global Action** — Use the Global Application Control action if traffic does not match

When you set the action to take if traffic does not match to **Use Global action**, Application Control uses the **Global** Application Control action for any traffic that does not match. You can also assign the Global Application Control action to a policy. The **Global** Application Control action is created by default and cannot be removed.

## Connect to the XTM Device To Get The Latest Signatures

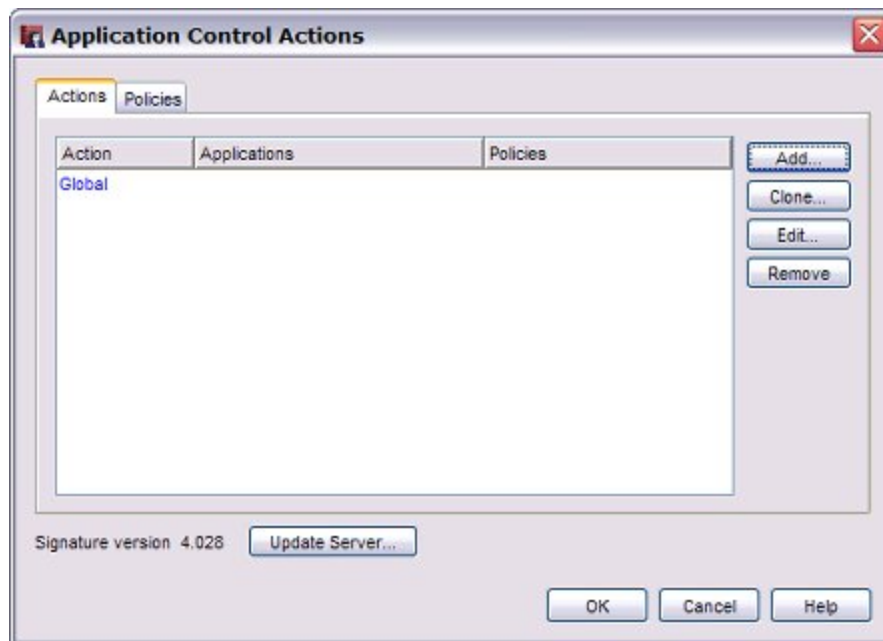
The list of applications you can control is based on a set of application signatures that Application Control uses to identify the application. The list of applications changes over time as the signature set is updated. As part of the Application Control security subscription, your XTM device automatically downloads updated application signatures from a WatchGuard server. Your management computer gets the updated application signature set when you connect to the device. To make sure that your management computer has the most recent Application Control signatures, connect to your device with WatchGuard System Manager before you use Policy Manager to edit Application Control actions.

## Add or Edit Application Control Actions

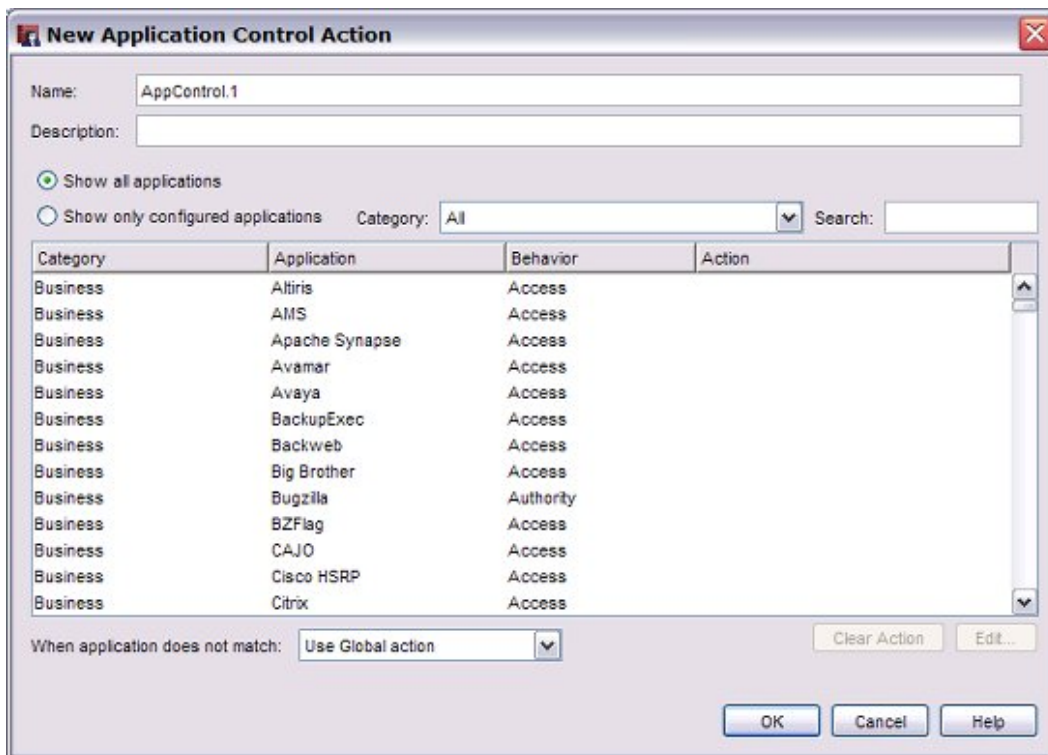
To see and edit all of the Application Control actions:

1. Select **Subscription Services > Application Control**.

*The Application Control Actions page appears.*



2. To create a new Application Control action, click **Add**.  
Or, to edit an action, click the action name and click **Edit**.  
*The Application Control Action Settings page appears.*



3. If this is a new action, in the **Name** text box, type the name for the action. Optionally, type a **Description**.
4. To filter the application list, use these options:
  - **Show all applications** — Show all applications you can configure.
  - **Show only configured applications** — Show the applications that have an action configured
  - **Category** — Filter by application category
  - **Search** — Search for applications that contain a specific word or phrase
5. To configure an application for this Application Control action, click an application in the list. Then click **Edit**.

*The Application Control Configuration dialog box appears.*



6. From the **Set the action for all behaviors** drop-down box, select the action to take for this application

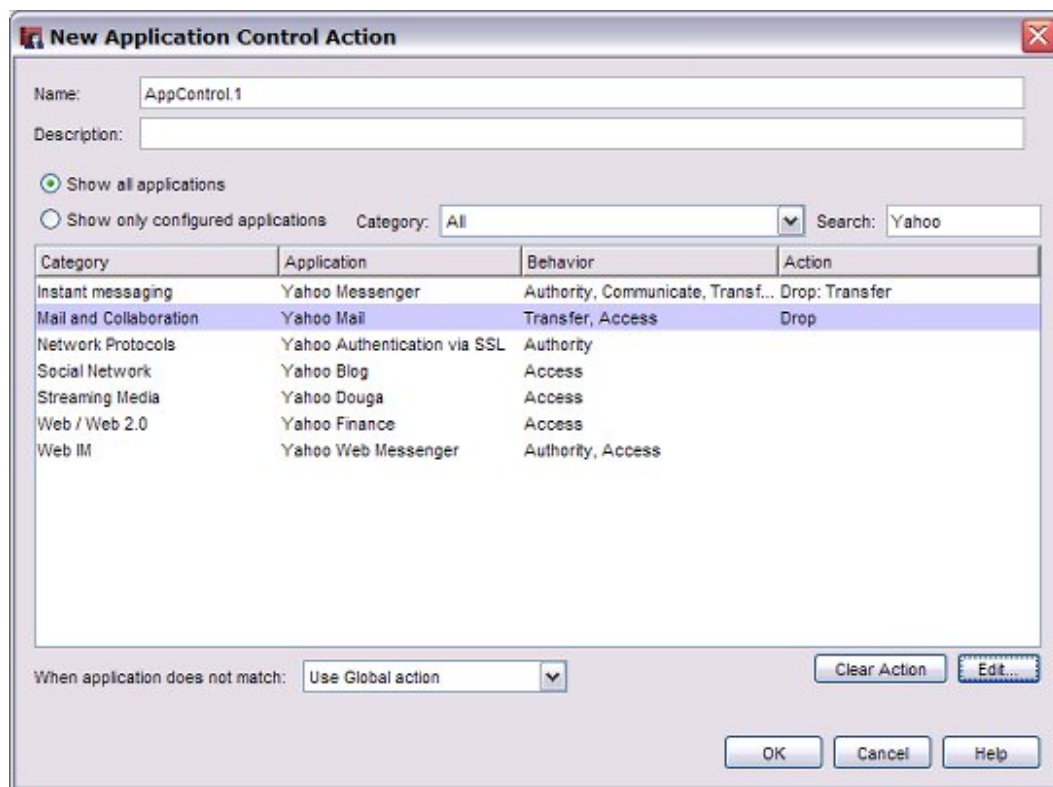
- Select **Drop** to block the selected application.
- Select **Allow** to allow the selected application.

Or, select **Set the action for specific behaviors**. Select the check box for each behavior to control. Select **Drop** or **Allow** for each selected behavior.

**Note** *If you select multiple applications, you can set the action to apply to all selected applications, but you cannot set the action for specific behaviors.*

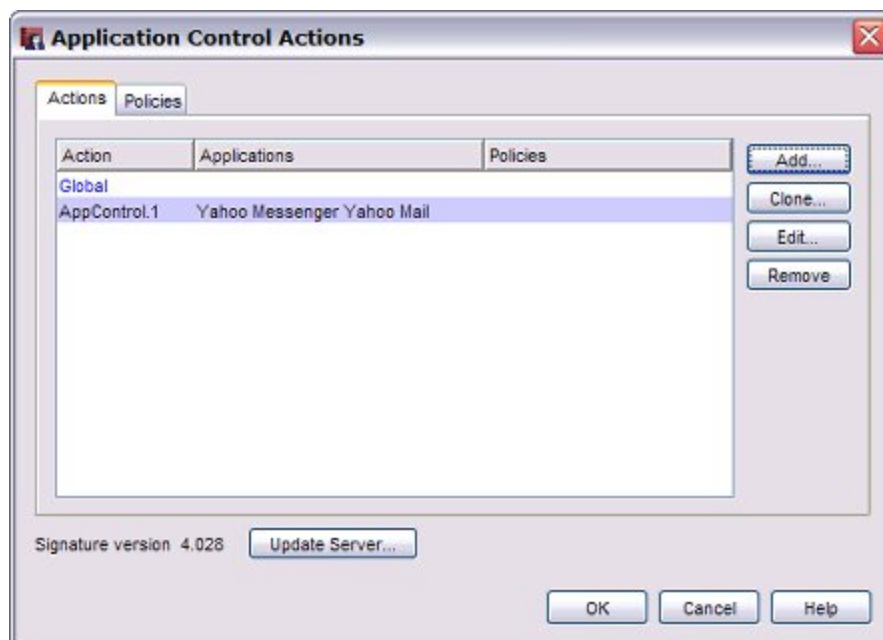
7. Click **OK**.

*The configured action appears in the Action column.*



8. Click **OK** to save the Application Control action.

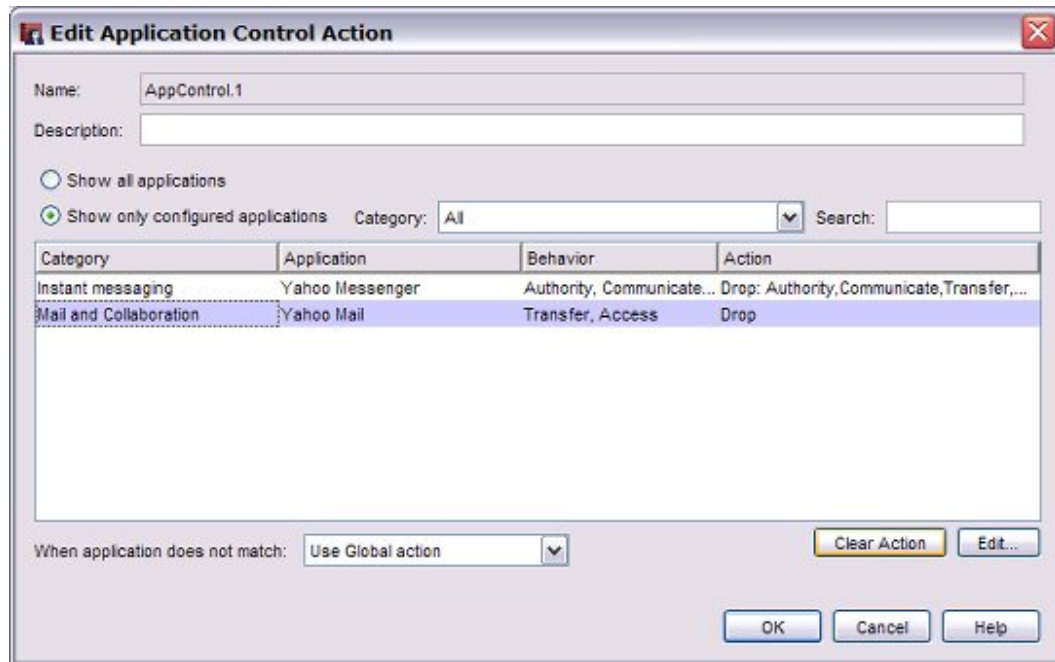
*The Application Control action is added to the list, but is not yet applied to any policy.*



## Remove Configured Applications From an Application Control Action

To remove a configured application from an Application Control action:

1. Select **Subscription Services > Application Control**.  
*The Application Control Actions page appears.*
2. Select the Application Control action to edit. Click **Edit**.  
*The settings for the selected Application Control Action appear.*
3. To show only the configured applications, select **Show only configured applications**  
*The list updates to show only the applications configured for this Application Control action.*



4. Select one or more configured applications you want to remove from this Application Control action.
5. To clear the action for the selected applications, click **Clear Action**.  
*The action for the selected applications is cleared. The application is removed from the configured applications list.*
6. Click **OK** to save the Application Control action.

## Apply an Application Control Action to a Policy

When you create an Application Control action, it is not automatically applied to your policies. There are two ways you can apply an application control to a policy.

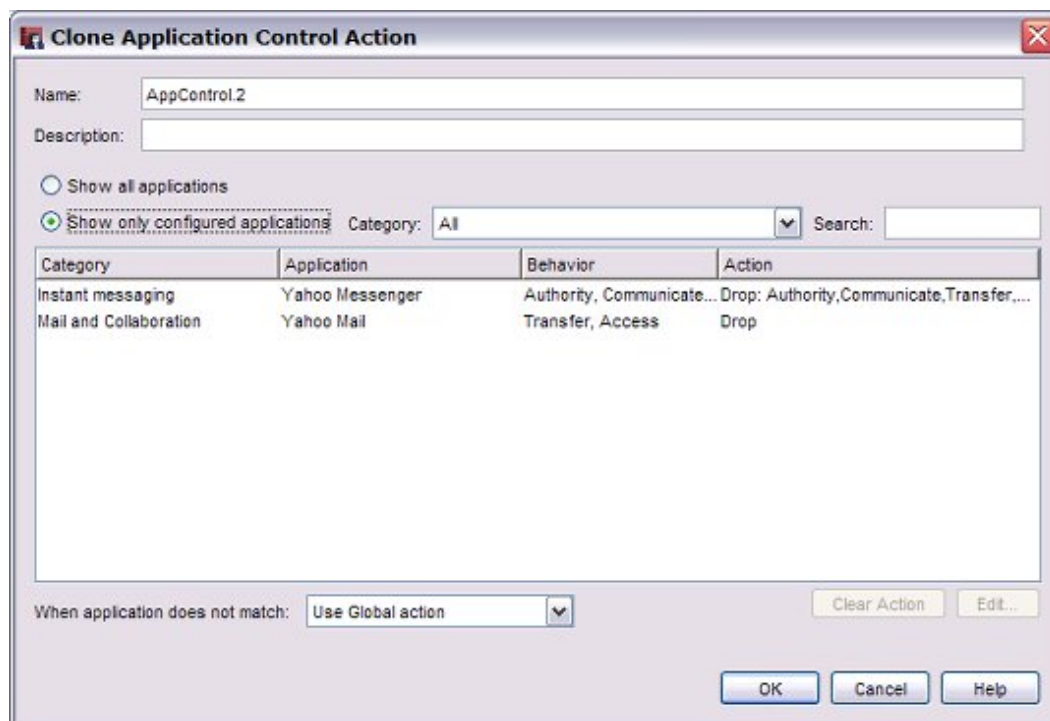
- Select which Application Control action to enable for each policy on the **Policies** tab of the Application Control Actions dialog box, .  
For more information, see *Configure Application Control for Policies*.
- Change the Application Control action when you edit a policy  
For more information, see *Enable Application Control in a Policy*.

## Clone an Application Control Action

To create an Application Control action that is similar to one that you have already created, you can clone (copy) an existing Application Control action.

In the **Application Control Actions** dialog box:

1. Select the **Actions** tab.
2. Click an existing Application Control action to select it.
3. Click **Clone**.  
*The Clone Application Control Action dialog box appears.*



4. In the **Name** text box, you can edit the name of this action. Optionally, edit the **Description**.
5. Select **Show only configured applications** to see the applications already configured in this action.
6. Edit the Application Control action as described in the previous section
7. Click **OK** to save the new Application Control action.

## Remove Application Control Actions

From the Application Control Actions dialog box, you can remove any Application Control action that is not used in a policy. To remove an application, click the Application Control action. Then click **Remove**.



## Use Categories

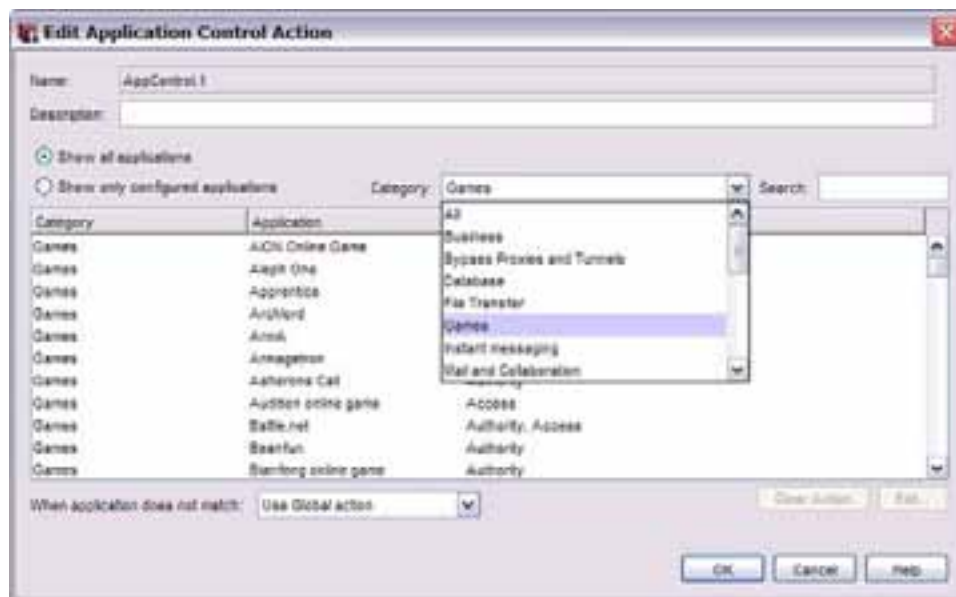
Categories are used to classify applications in Application Control reports. Categories also provide a convenient way to find applications when you edit an Application Control action. There is also a search option if you want to find a specific application.

You can select a group of applications by category to conveniently restrict use of a set of applications that do not have legitimate business value. A good example is the **Games** application category.

To block all applications in the Games category for an Application Control action:

1. From the **Category** drop-down list, select **Games**.

*All Applications in the Games category appear.*



2. Select the first application in the list. Press the **Shift** key while you select the last application.  
*All applications in the category are selected.*
3. Click **Edit** to set the action for the selected applications to **Drop**.
4. Click **OK**.

If you configure Application Control to block all applications in a category, be aware of everything that is included in the category and the expected consequences. For example, SWF (Shockwave Flash) is included in the streaming media category. Flash is used widely in many web sites to deliver content.

We do not recommend that you configure Application Control to block general categories like Web / Web 2.0, Business, or Network Protocols. It is highly likely that there could be an application blocked that may not have the consequences that you intend.

It is a good practice to set up Application Control to send log messages and report on all activity for a period of time before you configure any actions that block applications.

**Note** When you configure an Application Control action to block all applications in a category, this selects all applications currently in the category. Application Control signatures are updated frequently. If new applications are added to the category later, these new applications are not automatically blocked by Application Control.

## Configure Application Control for Policies

Application Control is configured globally, but is not used by a policy unless you enable it. After you create an Application Control action in the Application Control configuration, you can change the Application Control action enabled for each policy.

1. Select **Subscription Services > Application Control**.  
*The Application Control Actions dialog box appears.*
2. Select the **Policies** tab.  
*A list of configured policies appears. The Action column shows which Application Control action is enabled for each policy.*



3. To change the Application Control action for a policy, select the **Action** column for that policy.  
*The available Application Control actions appear in the drop-down list.*
4. From the drop-down list, select an Application Control action.  
Or, to disable Application Control for the selected policy, select **None**.
5. Click **OK**.

When you enable Application Control for a policy, the XTM device always identifies and creates a log message for applications dropped due to an Application Control action. If you want the XTM device to create a log message for all identified applications, even those that are not dropped, you must enable logging in each policy that has Application Control enabled.

For information about how to enable logging in a policy, see *Configure Logging and Notification for a Policy*.

## Enable Application Control in a Policy

To enable Application Control in the policy configuration:

1. In Policy Manager, add or edit a policy.  
*The Policy Properties dialog box appears with the Policy tab selected.*
2. Select the **Enable Application Control** check box.



3. From the adjacent drop-down list, select the Application Control action to use for this policy.
4. Click **OK**.

When you enable Application Control for a policy, the XTM device always identifies and creates a log message for applications dropped due to an Application Control action. If you want the XTM device to create a log message for all identified applications, even those that are not dropped, you must enable logging in each policy that has Application Control enabled.

For information about how to enable logging in a policy, see *Configure Logging and Notification for a Policy*.


## Edit or Clone Application Control Actions

When you enable Application Control for a policy, you can use an existing Application Control action or create a new action based on one of the existing actions.


**Note** *An Application Control action can be used by more than one policy. If you edit an existing Application Control action, those changes apply to all policies that use that action.*

If you want to modify an existing Application Control action for this policy but do not want to affect other policies, clone the action. This creates a new copy of the action that you can edit for this policy.

To view and edit the selected Application Control action in a policy:

1. Adjacent to the **Enable Application Control** drop-down list, click .
2. Edit the Application Control action as described in *Configure Application Control Actions*.
3. Click **OK** to save the edited rule to this policy.

To clone the selected application control action in a policy:

1. Adjacent to the **Enable Application Control**, click .  
*The Clone Application Control Action dialog box appears.*
2. Edit the new Application Control action as described in *Configure Application Control Actions*.
3. Click **OK**.  
*The new application control action is enabled for the policy.*

## Get Information About Applications

When you configure Application Control, or when you look at Application Control reports, you might see application names you are not familiar with. To get information about any application that Application Control can identify, you can look up the application on the WatchGuard Application Control Security Portal at <http://www.watchguard.com/SecurityPortal/AppDB.aspx>.

On the Application Control Security Portal page, you can:

- See a list of all applications that Application Control can identify.
- Search for an application by name.
- See a description of the application and supported application behaviors.

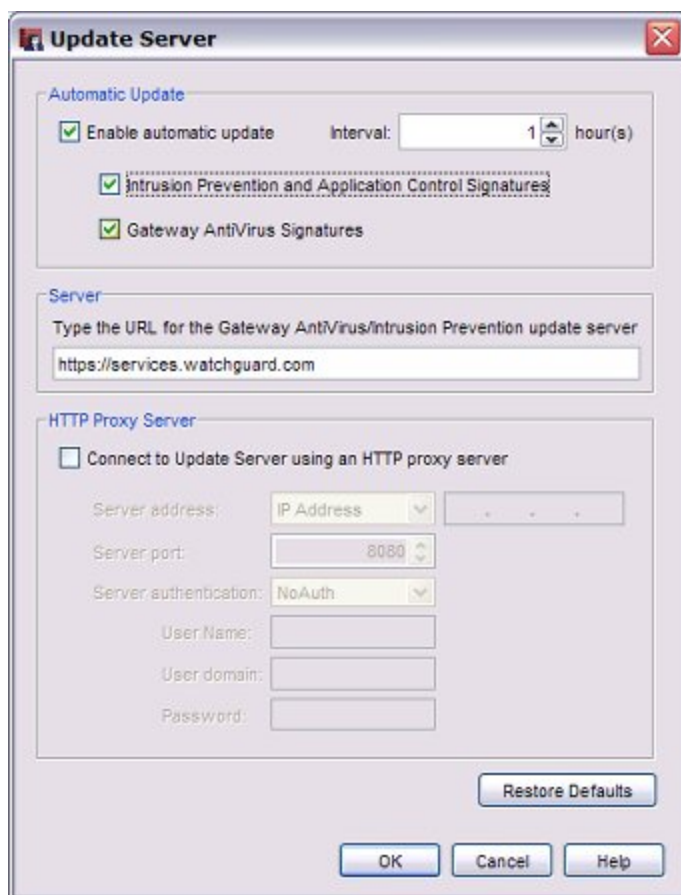
## Configure the Application Control Update Server

Application Control downloads signature updates from a signature update server. Gateway AV, IPS, and Application Control use the same update server settings. When you change configuration of the update server for any of these subscription services, the settings apply to all three services.

### Configure Signature Updates

1. Select **Subscription Services > Application Control**.
2. Click **Update Server**.

*The Update Server dialog box appears.*



3. To enable automatic signature updates, select the **Enable automatic update** check box. This option is enabled by default.
4. From the **Interval** drop-down list, enter the number of hours between automatic updates.
5. Select the **Intrusion Prevention and Application Control Signatures** check box to automatically update signatures at the selected update interval.

Do not change the **Update server URL** unless you are told to do so by WatchGuard. If you change the URL accidentally or incorrectly, click **Restore Defaults** to return to the default setting.

## Connect to the Update Server Through an HTTP Proxy Server

If your XTM device must connect through an HTTP proxy to get to the signature update server, you must add information about the HTTP proxy server to your update server configuration.

1. In the **ProxyServer** section, select the **Connect to Update server using an HTTP proxyserver** checkbox.
2. In the **Server address** text box, type the IP address or host name of your HTTP proxy server.
3. Most HTTP proxy servers receive requests on port 8080. If your HTTP proxy uses a different port, type it in the **Server port** field.
4. From the **Server authentication** drop-down list, select the type of authentication your HTTP proxy server uses.
  - If your HTTP proxy does not require authentication, select **NoAuth**.
  - If your HTTP proxy server requires **NTLM** or **Basic** authentication, type your **User name**, **Domain**, and **Password** in the text boxes.
5. Click **OK**.

## Block Access from the Trusted Network to the Update Server

If you do not want to allow all users on your trusted network to have unfiltered access to the IP address of the signature database, you can use an internal server on your trusted network to receive the updates. You can create a new HTTP proxy policy with *HTTP-Proxy: Exceptions* or an HTTP packet filter policy that allows traffic only from the IP address of your internal server to the signature database.

## Update Signatures Manually

For information about how to see the status of Application Control signature updates, and how to manually force an update to the most current signatures, see *Subscription Services Status and Manual Signatures Updates*.

## Application Control and Proxies

There is some duplication of the functions available in the Application Control service and in the WatchGuard proxy policies. In general, the proxies perform different and more detailed inspection and provide more granular control over the type of content. For example with the HTTP proxy, you can

- Adjust timeout and length limits of HTTP requests and responses to prevent poor network performance, as well as several attacks
- Customize the deny message that users see when they try to connect to a web site blocked by the HTTP proxy

- Filter web content MIME types
- Block specified path patterns and URLs
- Deny cookies from specified web sites

Proxies are also used to provide Gateway AntiVirus, WebBlocker, and Reputation Enabled Defense services.

By default, the HTTP proxy action blocks the download of these content types:

- Java bytecode
- ZIP archives
- Windows EXE/DLL files
- Windows CAB archive

The Application Control feature does not override settings in the proxy policy configuration. For example, if you allow YouTube in Application Control, but the proxy policy is already configured with an action to block streaming video, YouTube videos are still blocked.

## Application Control and WebBlocker

If both WebBlocker and Application Control are configured in the same policy, and the traffic matches for a web site and application, the Application Control action triggers first. For example, consider facebook.com. All access to facebook.com can be blocked in WebBlocker if the “personals and dating” category is blocked.

One advantage of WebBlocker is that it displays a specific warning message in the user’s browser when a site is blocked. If your company policy is to restrict all access to Facebook, it may be appropriate to block it in WebBlocker. You can either block the “personals and dating” category or add a WebBlocker exception. Application Control provides more granular control over applications and their associated subfunctions. With Application Control, it is possible to allow access to Facebook, but not allow access to Facebook Games.

## Manage SSL Applications

Many web-based applications are accessible through SSL (HTTPS), as well as through HTTP. Organizations offer encrypted SSL connections to provide more security to users. SSL encryption can also make applications more difficult for Application Control to detect. When you block applications that are accessible through SSL, you might also need to specifically block the SSL login for that application to make sure that you block all access to that application.

For example, when you select to block the application **Google-Finance**, this blocks Google's financial applications. But it does not block Google Finance over SSL. To block that, you must also block the application **Google Authentication via SSL**. It is important to understand that, once you block Google Authentication over SSL, you lose control over the granularity of all Google SSL applications to block. For example, access to Google Docs and Gmail over SSL is also blocked.

Similar behavior occurs for some Microsoft and Yahoo applications when they are accessed over SSL. There are corresponding signatures for Authentication over SSL for Microsoft and Yahoo and many other applications in the Application Control application list. To granularly manage these types of applications, you might want to block Authentication over SSL. Then you can use the application signatures to granularly configure the applications that can be used over the http access that is allowed.

## Manage Evasive Applications

Some applications use dynamic ports and protocols, encryption, and other techniques to make the application traffic difficult to detect and manage. For these types of applications, there can be some limitations to the application behaviors that Application Control can manage.

One example of this type of evasive application is Skype, a popular peer-to-peer (P2P) network application. The Skype client uses a dynamic combination of ports that include outbound ports 80 and 443. Skype traffic is very difficult to detect and block because it is encrypted, and because the Skype client is able to bypass many network firewalls.

For information about how to block Skype, see *Block User Logins to Skype*.

### Block User Logins to Skype

You can configure Application Control to block a user login to the Skype network. It is important to understand that Application Control can only block the Skype login process. It cannot block traffic for a Skype client that has already logged in and has an active connection. For example:

- If a remote user logs in to Skype when the computer is not connected to your network, and then the user connects to your network while the Skype client is still active, Application Control cannot block the Skype traffic until the user logs off the Skype network or restarts their computer.
- When you first configure Application Control to block Skype, any users that are already logged in to the Skype network are not blocked until they log off the Skype network, or restart their computers.

To configure an Application Control action to block user logins to Skype:

1. Select **Subscription Services > Application Control**.  
*The Application Control Actions page appears.*
2. Double-click the Application Control action you want to edit.

3. From the list of applications, select the **Skype** application. To quickly find the Skype application, type "skype" in the search text box.
4. Click **Edit**.



5. Set the action for all behaviors to **Drop**.
6. Click **OK** to save the action for the Skype application.
7. Click **OK** to save the Application Control action.

After you configure the Application Control action to block Skype, you must apply this Application Control action to all policies in your configuration. You can do this when you edit the policy, or on the **Policies** tab of the Application Control dialog box.

If you have a high precedence policy that allows all DNS, you must configure the DNS policy to use the Application Control action that blocks Skype.

## Manage Applications that Use Multiple Protocols

Many applications today, especially instant messaging and peer-to-peer applications, use multiple protocols and techniques to transfer files. For example, there are many clients that use the BitTorrent protocol and other protocols to transfer files. To fully block applications that use multiple protocols, you must configure Application Control with a combination of actions. This is best illustrated as an example.

### Example: Block FlashGet

When you select the BitTorrent Series application in an Application Control action, Application Control uses a set of rules that identify the BitTorrent protocol for peer-to-peer file sharing.

FlashGet is a client application that is used for file sharing. The FlashGet client application can use the BitTorrent peer-to-peer protocol to download files, or it can use simple HTTP downloads, FTP file transfer, or the proprietary FlashGet protocol.

If you do not block, but only record activity in the log files, BitTorrent downloads that are triggered by the FlashGet client appear in the log files and reports as both FlashGet and BitTorrent application activity, at different times.

To block all possible file transfers by the FlashGet client, you must configure Application Control to block FlashGet, and also to block BitTorrent Series, Web File Transfer, and FTP Applications. It is important to understand that if you block BitTorrent Series, Application Control also blocks BitTorrent use by all other applications. There is no way to block BitTorrent use by FlashGet, but allow it for other applications.



If you block FlashGet, but do not block BitTorrent or Web File Transfer, downloads through BitTorrent or HTTP are not blocked, even if the downloads are started by the FlashGet client.

If you block Web File Transfer or FTP Applications, this functionality is blocked for all applications. There is no way to block HTTP file transfers or FTP file transfers for FlashGet but allow it for other applications.

## File Transfer Applications and Protocols

The table below shows some common applications and the variety of protocols that they use for file transfer. The names of applications and protocols in the table correspond to application names in Application Control.

Category	Application	Protocols and Applications Used
P2P	Thunder Series	Thunder Private Protocol Web File Transfer ASFV1, MP4, MMS, FLV, RMVB, SWF, AVI, MP3, WMA, MOV, WMA, ASF BitTorrent Series FTP Applications
P2P	BitTorrent	BitTorrent Series Web File Transfer ASFV1, MP4, MMS, FLV, RMVB, SWF, AVI, MP3, WMA, MOV, WMA, ASF FTP Applications
P2P	FlashGet	BitTorrent Series Web File Transfer ASFV1, MP4, MMS, FLV, RMVB, SWF, AVI, MP3, WMA, MOV, WMA, ASF FTP Applications
P2P	QQDownload	BitTorrent Series Web File Transfer ASFV1, MP4, MMS, FLV, RMVB, SWF, AVI, MP3, WMA, MOV, WMA, ASF FTP Applications QQ Private Protocol
MEDIA	QQLive	QQLive ASFV1, MP4, MMS, FLV, RMVB, SWF, AVI, MP3, WMA, MOV, WMA, ASF QQ Private Protocol QQ/TM
MEDIA	PPTV	PPTV (PPLive) ASFV1, MP4, MMS, FLV, RMVB, SWF, AVI, MP3, WMA, MOV, WMA, ASF

Category	Application	Protocols and Applications Used
MEDIA	PPStream	PPStream ASFV1, MP4, MMS,FLV,RMVB, SWF,AVI,MP3, WMA, MOV, WMA, ASF
MEDIA	UUSee	UUSee ASFV1, MP4, MMS,FLV,RMVB, SWF,AVI,MP3, WMA, MOV, WMA, ASF
IM	QQ	QQ/TM QQ Private Protocol
GAME	QQ/QQFO	QQ Game QQ Private Protocol

To fully block all file transfers through applications that use multiple protocols and applications, you must block the application, and you must block all protocols and applications the application uses. There are some common applications and protocols that you may not want to block because they are used by many applications.

For a description of any of the applications or protocols in this table, you can look up the application on the WatchGuard Application Control Security Portal at <http://www.watchguard.com/SecurityPortal/AppDB.aspx>.

## Monitor Downloads and File Transfers

Application Control includes two general purpose applications called **Web File Transfer** and **FTP Applications** that you can use to record log messages for common download and file transfer activity.

### *Web File Transfer*

Web File Transfer is a general application that detects the download of common file formats that are often downloaded through popular P2P and File Transfer programs, including: bz2 ,doc , exe , gz, pdf, ppt, rar , rpm, tar, xls, zip, torrent, dll, manifest, xdap, deploy, xps, , xaml, application, mkv, and dat. It also covers HTTP upload of files.

### *FTP Applications*

FTP Applications is an application that detects a range of FTP commands —pass, list, eprt, epsv, create directory, delete directory, get (binary and ascii), put (binary and ascii), passive and active file transfer.

These applications are best used to generate log messages of activity. Consider the implications carefully before you decide to block these applications.

## Manage Facebook Applications

Some applications, such as Facebook, contain multiple application types that Application Control can identify. You can use Application Control to granularly control which applications your users can use.

Facebook is a social networking site that includes a large number of features and applications. You can use Application Control to block some or all Facebook applications. For example, you can configure an Application Control action that allows Facebook, but blocks the use of Facebook games or IM. Or you can block the use of all Facebook applications.

You can see the list of Facebook applications when you configure an Application Control action for your device, or you can search for *facebook* in the Application Control security portal at <http://www.watchguard.com/SecurityPortal/AppDB.aspx>.



Category	Application	Behavior
Web IM	Facebook Web IM	Communicate
Social Network	Facebook	Authentic, Access
Social Network	Facebook Games	Access
Social Network	Facebook Applications	Access
Social Network	Facebook This is	Access
Social Network	Facebook Post	Access
Social Network	Facebook Sites	Transfer
Social Network	Facebook Photos	Transfer
Social Network	Facebook Comments	Access

Application Control can identify and block different types of Facebook activity.

*Facebook Web IM*

Identifies Facebook chat sessions.

*Facebook*

Identifies attempts to log in to Facebook or see Facebook web pages.

*Facebook Game*

Identifies the top 25 most popular Facebook games.

*Facebook Applications*

Identifies all applications available through the Facebook apps directory.

*Facebook Plug-in*

Identifies all Facebook social plug-ins that can be embedded in other sites on the Internet. This includes plug-ins such as **Like** and **Comments**. To see the current list of Facebook social plug-ins, see <http://developers.facebook.com/plugins>.

*Facebook Post*

Identifies information posts to Facebook. This includes:

- Post a message to the wall
- Share status
- Share a link

*Facebook Video*

Identifies video uploads to Facebook.

*Facebook Picture*

Identifies photo uploads to Facebook.

*Facebook EditProfile*

Identifies Facebook user profile updates.

To block Facebook applications:

1. Create or edit an Application Control action.
2. In the search text box, type facebook.  
*The list of applications is filtered to show only the Facebook applications.*
3. Select one or more Facebook applications to block.
4. Select **Edit**. Set the action for the selected applications to **Block**.
5. Apply the Application Control action to your policies.

# Application Control Policy Examples

You can use the **Global** Application Control action with other Application Control actions to allow or block different applications based on the time of day, or based on the user name or user group. To do this, you create Application Control actions that block or allow different sets of applications. Then you apply different Application Control actions to different policies as described in the examples below.

Each of the examples below enables Application Control actions for a single type of policy. If your configuration includes other policy types, such as TCP-UDP, or Outgoing, you can use the same steps to set up a two-tiered Application Control configuration for those policies. The policies you need to apply an Application Control action to depend on which policies exist in your configuration, and which applications you want to block. For example, if you want to block an application that you know uses FTP, you must enable the Application Control action for the FTP policy.

For recommendations on which types of policies to configure for Application Control, see *Policy Guidelines for Application Control*.

## Allow an Application For a Group of Users

If the Global Application Control action blocks an application, you can create a separate Application Control action to allow that same application for a department or other user group. For example, if you want to block the use of MSN instant messaging for most users, but you want to allow this application for the people in the Sales department, you can create different Application Control actions and policies to get this result.

If you already have an **HTTP** packet filter policy that applies to all users, you can use these steps to allow different applications for the Sales department.

1. Configure the **Global** Application Control action to block MSN instant messaging, and any other applications you do not want to allow.
2. Apply the **Global** Application Control action to the existing **HTTP** packet filter policy.
3. Create a new Application Control action to allow MSN instant messaging. For example, you could call this action, **AllowIM**. Configure this action to use the **Global** action when the application does not match.
4. Create an HTTP policy for the users in the Sales department. For example, you could call this policy **HTTP-Sales**. For information about how to create a policy for a group of users, see *Use Authorized Users and Groups in Policies*.
5. Apply the **AllowIM** Application Control action to the **HTTP-Sales** policy.
6. Enable logging for the **HTTP** and **HTTP-Sales** policies.  
*You must enable logging to see information about Application Control in the log files and reports.*

In this example, the two resulting HTTP policies could look like this:

*Policy: HTTP-Sales*

HTTP connections are: **Allowed**  
From: **Sales** To: **Any-External**  
Application Control: **AllowIM**

*Policy: HTTP*

HTTP connections are: **Allowed**  
From: **Any-Trusted** To: **Any-External**  
Application Control: **Global**

The **AllowIM** Application Control action applied to the **HTTP-Sales** policy acts as an exception to the Global Application Control action. The users in the Sales group can use MSN instant messaging, but cannot use any other applications blocked by the **Global** Application Control action.

If this device configuration included other policies, such as HTTP-Proxy, TCP-UDP, or Outgoing, that could be used for IM traffic, you can repeat the steps above to set up a two-tiered Application Control configuration for other policies.

## Block Applications During Business Hours

You can use Application Control with policies to block different applications based on the time of day. For example, you might want to block the use of games during business hours. To block applications during certain hours, you can use Application Control with policies that have an operating schedule.

If you already have an **HTTP-Proxy** policy that does not have an operating schedule, use these steps to add a new policy and Application Control action to block applications during business hours.

1. Configure the **Global** Application Control action to block applications you want to always block.
2. Apply the **Global** Application Control action to the existing **HTTP-Proxy** policy.
3. Create a schedule called **Business-Hours** that defines the business hours. For more information about schedules, see *Create Schedules for XTM Device Actions*.
4. Create a new HTTP-Proxy policy that uses the **Business-Hours** schedule you configured. For example, you could call the new policy **HTTP-Proxy-Business**. For more information about how to set the schedule for a policy, see *Set an Operating Schedule*.
5. Create an Application Control action that blocks the applications you want to block during business hours. For example, you could call this action **Business**.
6. Apply the **Business** Application Control action to the **HTTP-Proxy-Business** policy.
7. Enable logging for the **HTTP-Proxy** and **HTTP-Proxy-Business** policies.  
*You must enable logging to see information about Application Control in the log files and reports.*

In this example, the two resulting policies could look like this:

*Policy: HTTP-Proxy-Business*

HTTP connections are: **Allowed**  
From: **Sales** To: **Any-External**  
Application Control: **Business**

*Policy: HTTP-Proxy*

HTTP connections are: **Allowed**  
From: **Any-Trusted** To: **Any-External**  
Application Control: **Global**

The **Business** Application Control action in the **HTTP-Proxy-Business** policy blocks games only during business hours. All other applications in the **Global** Application Control action are blocked at all times of day.

If this device configuration included other policies, such as HTTP, TCP-UDP, or Outgoing, that might be used for games traffic, you can repeat the steps above to set up a two-tiered Application Control configuration for other policies.

## Application Control and Policy Precedence

When you apply different Application Control actions to multiple policies of the same type, it is helpful to understand policy precedence, so you know which policies apply to which types of traffic. The XTM device automatically sorts policies from the most detailed to the most general. The first rule in the list to match the conditions of the packet is applied to the packet.

For more information about policy precedence, see *About Policy Precedence*.





# 37 Quarantine Server

---

## About the Quarantine Server

The WatchGuard Quarantine Server provides a safe mechanism to quarantine any email messages suspected or known to be spam or to contain viruses. The Quarantine Server is a repository for email messages that the SMTP proxy decides to quarantine based on analysis by spamBlocker or Gateway AntiVirus. Granular control allows you to configure preferences for mail disposition, storage allocation, and other parameters.

**Note** *The SMTP proxy requires a Quarantine Server if you configure it to quarantine emails that spamBlocker classifies as spam, or if you configure Gateway AntiVirus to quarantine emails from a specified category.*

The Quarantine Server provides tools for both users and administrators. Users get regular email message notifications from the Quarantine Server when they have email stored on the Quarantine Server. Users can then click a link in the email message to go to the Quarantine Server web site. On the Quarantine Server web site, they see the sender and the subject of the suspicious email messages. For spam email, the user can release any email messages they choose to their email inbox, and delete the other messages. Administrators can configure the Quarantine Server to automatically delete future messages from a specific domain or sender, or those that contain specified text in the subject line.

The administrator can see statistics on Quarantine Server activity, such as the number of messages quarantined during a specific range of dates, and the number of suspected spam messages.

The SMTP proxy adds messages to different categories based on analysis by spamBlocker and Gateway AntiVirus. The Quarantine Server displays these classifications for quarantined messages:

- Suspected spam — The message could be spam, but there is not enough information to decide.
- Confirmed spam — The message is spam.
- Bulk — The message was sent as commercial bulk email .
- Virus — The message contains a virus.
- Possible virus — The message might contain a virus, but there is not enough information to decide.

# Set Up the Quarantine Server


## Install the Quarantine Server Software

Make sure you have installed the Quarantine Server software on your management computer. You usually do this when you select server components to install when you set up WatchGuard System Manager. If you did not do this, run the setup procedure again as described in *Install WatchGuard System Manager Software* on page 20, but select only the Quarantine Server component.

## Run the WatchGuard Server Center Setup Wizard

The WatchGuard Server Center Setup Wizard sets up the Quarantine Server and any other servers you have installed. The WatchGuard Server Center Setup Wizard starts automatically the first time that you open WatchGuard Server Center.

On the computer where you installed the Quarantine Server software:


1. Right-click  in the system tray and select **Open WatchGuard Server Center**.  
*The WatchGuard Server Center Setup Wizard appears.*
2. Review the information on the first page of the wizard to make sure you have all the information necessary to complete the wizard. Click **Next**.
3. Type the name of your organization. Click **Next**.
4. Type and confirm the **Administrator passphrase** to use for all your WatchGuard servers. Click **Next**.
5. (Optional) Type the IP Address of your gateway XTM device. Click **Add**. Click **Next**.
6. (Optional) Type your Management Server License Key. Click **Next**.
7. Type the **Log Server Encryption key**. Click **Next**.
8. Type the domain for which you want to quarantine messages. Click **Add**. Click **Next**.
9. (Optional) Download and install the WebBlocker database. Click **Next**.  
*It can take a long time to download and install the database. You can install the database later if you choose to not install it in the wizard.*
10. Review your settings. Click **Next**.  
*The wizard configures your servers.*
11. Click **Finish** to exit the wizard.

For more information, see the complete *Set Up WatchGuard Servers* on page 545.

**Note** *If you install the Quarantine Server software after you have already configured other WatchGuard servers, the wizard does not start automatically when you open the WatchGuard Server Center. To configure the Quarantine Server, you must open WatchGuard Server Center, select the Quarantine Server, and click **Launch Wizard**.*

## Configure the Quarantine Server Settings

On the computer where you installed the Quarantine Server software:

1. Right-click  in the system tray and select **Open WatchGuard Server Center**.  
*The WatchGuard Server Center appears.*
2. Type your **Username** and administrator **Passphrase**.
3. In the **Servers** tree, select **Quarantine Server**.  
*The Quarantine Server page appears.*
4. Change the default settings as appropriate for your network.
  - To change the Server Settings, see *Configure Database and SMTP Server Settings* on page 1229.
  - To change the Database Maintenance settings, see *Configure Deletion Settings and Accepted Domains* on page 1231.
  - To change the Notification settings, see *Configure User Notification Settings* on page 1232.
  - To change the Logging settings, see *Configure Logging Settings for the Quarantine Server* on page 1234.
  - To change the rules that determine how mail gets quarantined, see *Configure Quarantine Server Rules* on page 1235.
5. When you are finished, click **OK**.


## Configure the XTM Device to Quarantine Email

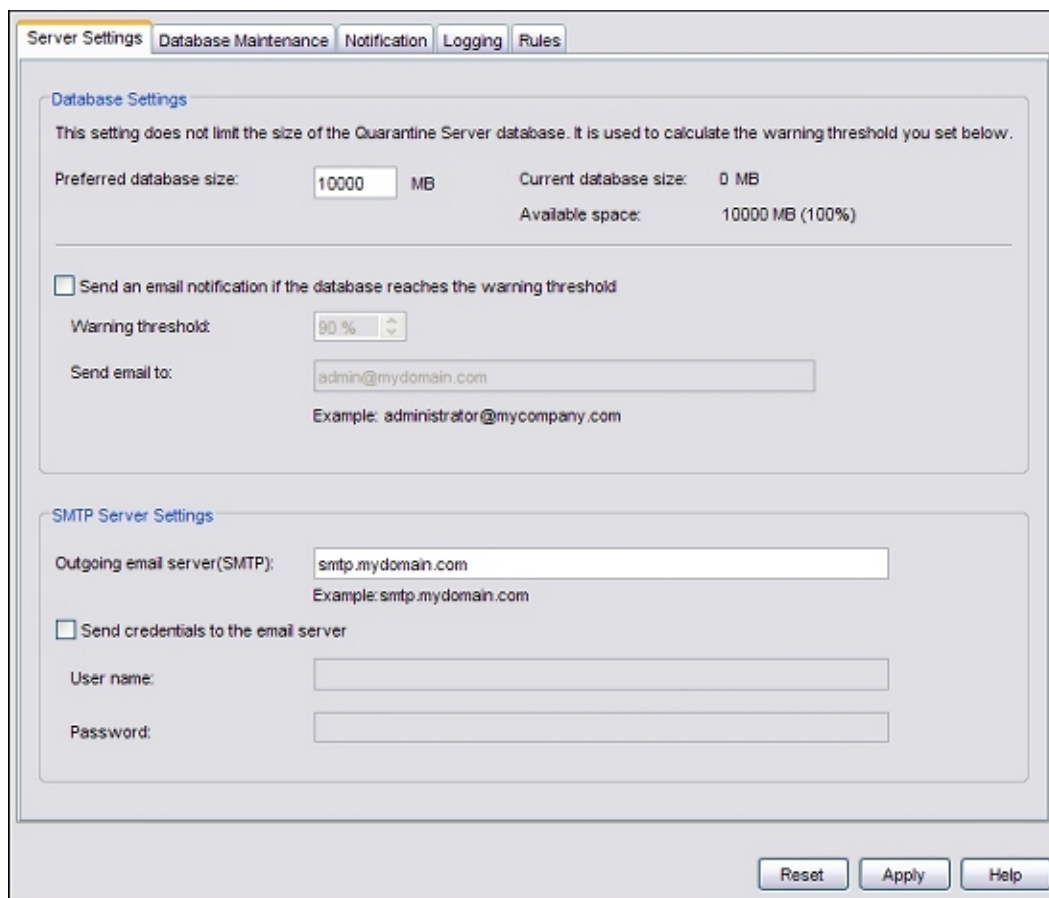
After you install and configure Quarantine Server, you must update the XTM device configuration to send email to the Quarantine Server.

1. Configure the Quarantine Server IP address as described in *Define the Quarantine Server Location on the XTM Device* on page 1237.
2. Set up spamBlocker and Gateway AntiVirus actions for the SMTP proxy to quarantine the mail.  
For more information, see *Configure spamBlocker to Quarantine Email* on page 1153, and *Configure Gateway AntiVirus to Quarantine Email* on page 1181.

# Configure the Quarantine Server

To open the Quarantine Server settings page:

1. Right-click  in the system tray and select **Open WatchGuard Server Center**.
2. Type the Administrator passphrase.  
*The WatchGuard Server Center appears.*
3. In the **Servers** tree, select **Quarantine Server**.  
*The Quarantine Server Configuration settings appear.*



Server Settings Database Maintenance Notification Logging Rules

**Database Settings**

This setting does not limit the size of the Quarantine Server database. It is used to calculate the warning threshold you set below.

Preferred database size:  MB Current database size: 0 MB  
Available space: 10000 MB (100%)

Send an email notification if the database reaches the warning threshold

Warning threshold:

Send email to:   
Example: administrator@mycompany.com

**SMTP Server Settings**

Outgoing email server(SMTP):   
Example: smtp.mydomain.com

Send credentials to the email server

User name:


Password:

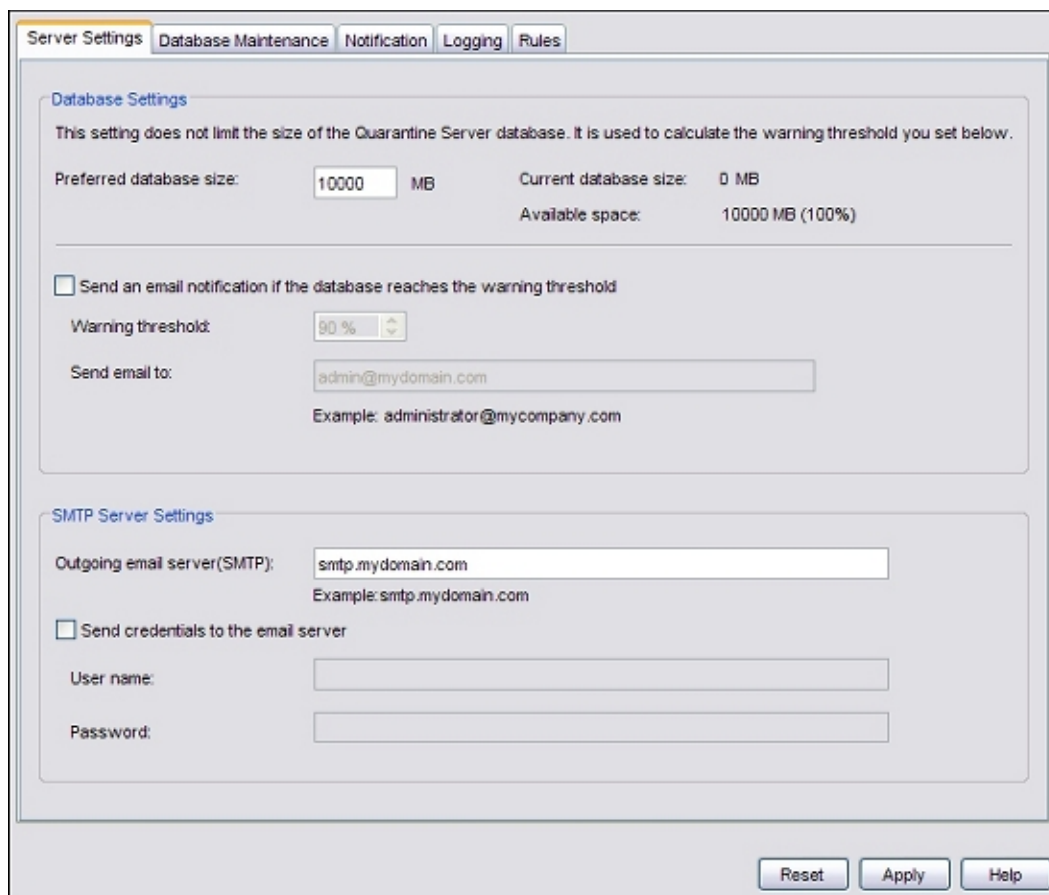
Reset Apply Help

When you configure the Quarantine Server, you can:

- *Configure Database and SMTP Server Settings.*
- *Configure Deletion Settings and Accepted Domains* — When to delete or how long to keep messages, and add and delete user domains. Only users in the domains that are in this list can have their messages sent to the Quarantine Server.
- *Configure User Notification Settings* — The message sent to users that tells them they have messages on the Quarantine Server.
- *Configure Logging Settings for the Quarantine Server.*
- *Configure Quarantine Server Rules* — Add, change, or delete the rules that determine messages to that the Quarantine Server will automatically delete.

## Configure Database and SMTP Server Settings

1. Right-click  in the system tray and select **Open WatchGuard Server Center**.
2. Type the Administrator paraphrase.  
*The WatchGuard Server Center appears.*
3. In the **Servers** tree, select **Quarantine Server**.  
*The Quarantine Server Configuration settings appear.*



The screenshot shows the 'Server Settings' window with tabs for 'Database Maintenance', 'Notification', 'Logging', and 'Rules'. The 'Database Settings' section includes a text box for 'Preferred database size' set to '10000 MB', 'Current database size' at '0 MB', and 'Available space' at '10000 MB (100%)'. Below this is a checkbox for 'Send an email notification if the database reaches the warning threshold', a 'Warning threshold' dropdown set to '90%', and a 'Send email to:' text box containing 'admin@mydomain.com'. The 'SMTP Server Settings' section has an 'Outgoing email server(SMTP):' text box with 'smtp.mydomain.com' and a checkbox for 'Send credentials to the email server'. Below the checkbox are 'User name:' and 'Password:' text boxes. At the bottom right are 'Reset', 'Apply', and 'Help' buttons.

## Database Settings

### *Preferred database size*

This setting is for email notifications. It does not limit the maximum size of the Quarantine Server database. It is used to calculate the warning threshold for notification messages.

Type the preferred database size for the Quarantine Server database warning notification messages. The database size range is 1–10000 MB. The default setting is 10000 MB.

*The dialog box shows the current size of the database and the amount of unused space.*

### *Send an email notification if the database reaches the warning threshold*

Select this check box to receive a warning message when the database is near the selected limit.

### *Warning threshold*

Specify when the database sends you a threshold warning message.

### *Send email to*

Type the full email address of the account where you want to send the notifications.

For example, suppose that you select to receive a warning message. If you set the default warning threshold to 90%, and set the preferred database size to 1000 MB, the Quarantine Server sends a warning message when the Quarantine Server database size reaches 900 MB.

## SMTP Server Settings

### *Outgoing email server (SMTP)*

Type the address of the outgoing SMTP email server.

### *Send credentials to the email server*

If your email server requires authentication, select this check box.


### *User name*

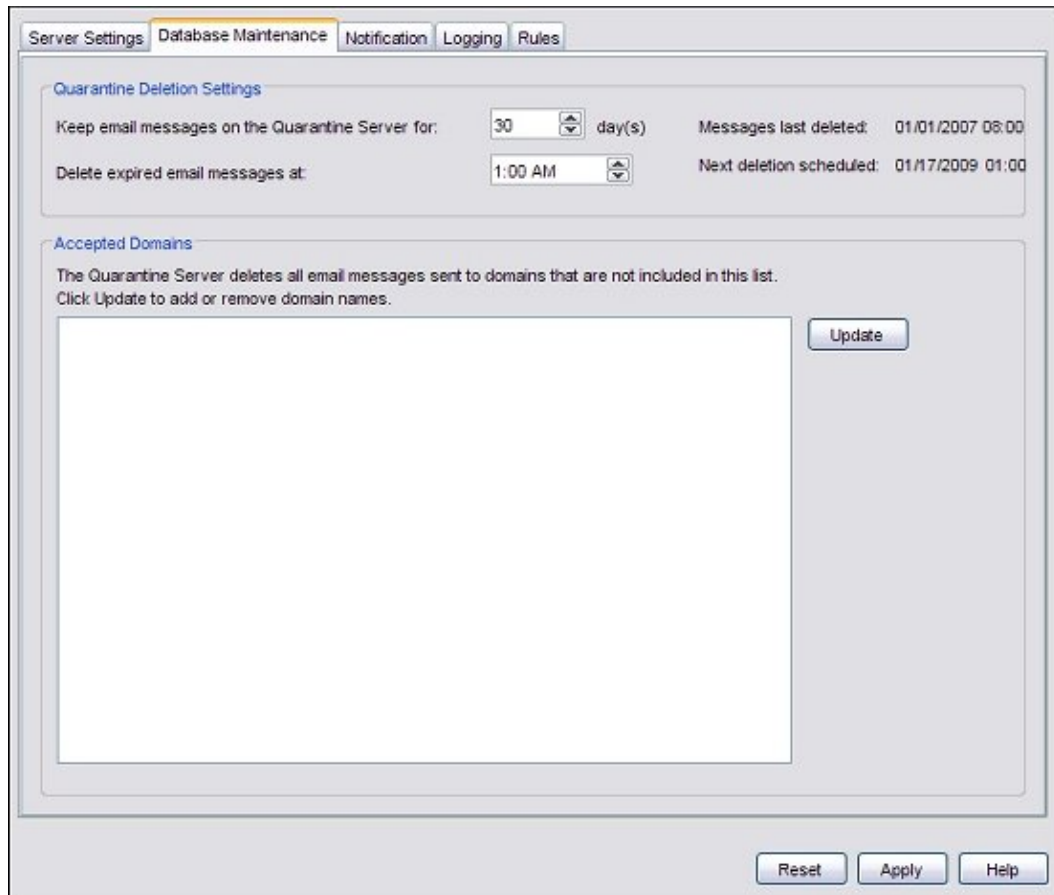
Type the user name for the email server. If the user name is not required for your SMTP server, you can keep this field blank.

### *Password*

Type the password for the email server. If the password is not required for your SMTP server, you can keep this field blank.

## Configure Deletion Settings and Accepted Domains

1. Right-click  in the system tray and select **Open WatchGuard Server Center**.
2. Type the Administrator passphrase.  
*The WatchGuard Server Center appears.*
3. In the **Servers** tree, select **Quarantine Server**.  
*The Quarantine Server Configuration settings appear.*
4. Select the **Database Maintenance** tab.



Server Settings Database Maintenance Notification Logging Rules

**Quarantine Deletion Settings**

Keep email messages on the Quarantine Server for: 30 day(s) Messages last deleted: 01/01/2007 08:00

Delete expired email messages at: 1:00 AM Next deletion scheduled: 01/17/2009 01:00

**Accepted Domains**

The Quarantine Server deletes all email messages sent to domains that are not included in this list.  
Click Update to add or remove domain names.

Update

Reset Apply Help

5. In the **Keep email messages on the Quarantine Server for** text box, type the number of days to maintain messages on the Quarantine Server. By default, email messages are kept for 30 days.
6. In the **Delete expired messages at** text box, enter the time of day to delete expired messages after the number of days in the previous field has passed.

## Add or Remove Accepted Domains

The **Database Maintenance** tab of the **Quarantine Server Configuration** dialog box shows the domain names for which the Quarantine Server accepts email messages. Only users in the domains that are in the list can have messages sent to the Quarantine Server for them. Messages sent to users that are not in one of these domains are deleted.

1. To add or remove a domain name from the server, click **Update**.


*The Add Domains dialog box appears.*



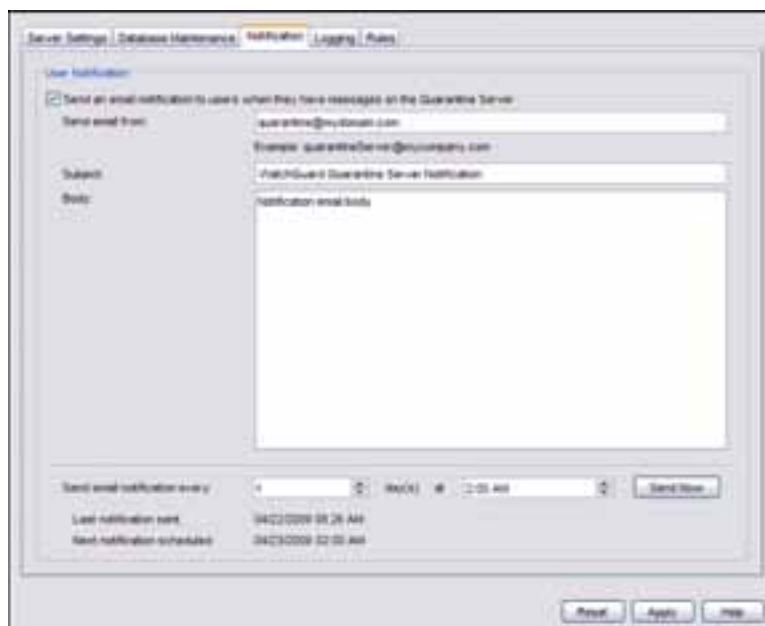
2. To add a domain, in the **Specify domain name** text box, type the domain and click **Add**.
3. To remove a domain, select it from the list and click **Remove**.

## Configure User Notification Settings

Users receive periodic email messages on their email client that include a list of the messages currently stored for them on the Quarantine Server. You can specify the account from which these messages are sent. You can also specify the title and body of the message. You can configure the interval at which the Quarantine Server sends notifications, although it cannot be more than once a day. You can also set the hour and minute of the day.

1. Right-click  in the system tray and select **Open WatchGuard Server Center**.
2. Type the Administrator passphrase.  
*The WatchGuard Server Center appears.*
3. In the **Servers** tree, select **Quarantine Server**.  
*The Quarantine Server Configuration settings appear.*
4. Select the **Notification** tab.





5. To enable notification (and the options on this dialog box), select the **Send an email notification to users when they have messages on the Quarantine Server** check box.
6. In the **Send email from** text box, type the full email address of the account you want to send the notification message from.

The email address must end in a valid top-level domain (TLD).

7. In the **Subject** text box, type a name for the subject of the notification messages. The default is *WatchGuard Quarantine Server Notification*.
8. In the **Body** text box, type the body of the notification message. You can use either text or HTML in the message body.

**Note** *The notification email is always in HTML format, with links to the quarantined messages. The notification message does not display properly in email readers that do not support HTML in the message body.*

9. In the **Send email notification every** text box, type or select a time interval for notification and the time of day you want the notifications sent. By default, email notification is sent once a day. To immediately send notifications to all users, click **Send Now**.

**Note** *Some email readers flag the notification message sent by the Quarantine Server as a "scam" or "phishing" email. This is because these readers classify any URL that uses an IP address as suspect. The URL that gives users access to the Quarantine Server includes the IP address of the Quarantine Server instead of a hostname.*

## Configure Logging Settings for the Quarantine Server

From WatchGuard Server Center, you can configure where the Quarantine Server sends log message data. You can choose to send log messages to a WatchGuard Log Server, Windows Event Viewer, or to a log file.

1. In the **Servers** tree, select **Quarantine Server**.
2. Select the **Logging** tab.

*The Logging page appears.*

The screenshot shows the 'Quarantine Server' configuration page in the 'WatchGuard Server Center'. The 'Logging' tab is selected. The page is titled 'Choose the destination for Quarantine Server log messages.' and contains three sections:

- WatchGuard Log Server:** An unchecked checkbox labeled 'Send log messages to the WatchGuard Log Server(s)'. Below it is a table with columns 'Priority' and 'Log Server Address:'. To the right of the table are buttons for 'Add', 'Edit', 'Remove', 'Up', and 'Down'. Below the table is a 'Select a log level:' dropdown menu set to 'Warning'.
- Windows Event Viewer:** A checked checkbox labeled 'Send the log messages to Windows Event Viewer'. Below it is a 'Select a log level:' dropdown menu set to 'Warning'.
- File path:** An unchecked checkbox labeled 'Send log messages to a file'. Below it is a 'File location:' text field containing ':Documents and Settings\WatchGuard\logs\lwqserver' and a 'Browse' button. Below the text field is a 'Select a log level:' dropdown menu set to 'Warning'.

At the bottom right of the page are three buttons: 'Reset', 'Apply', and 'Help'.


3. Configure settings for your Quarantine Server.

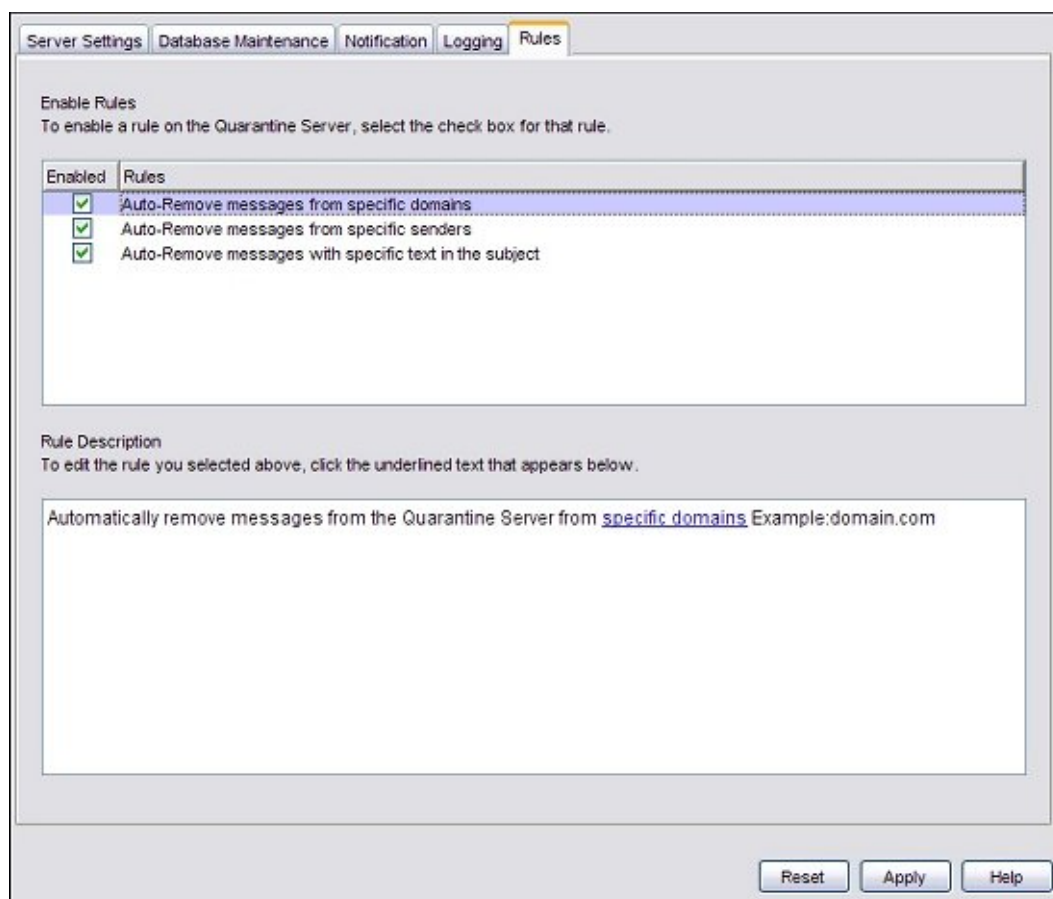
For more information about server configuration, see *Configure Logging Settings for Your WatchGuard Servers* on page 708.

4. When you are finished, click **Apply** to save your changes.

## Configure Quarantine Server Rules

You set up rules to automatically remove email messages if they come from a specified domain or sender, or if they contain specified text in the subject line.

1. Right-click  in the system tray and select **Open WatchGuard Server Center**.
2. Type the Administrator passphrase.  
*The WatchGuard Server Center appears.*
3. In the **Servers** tree, select **Quarantine Server..**  
*The Quarantine Server Configuration settings appear.*
4. Select the **Rules** tab.
5. Select the rule to modify.  
*The description of the rule appears in the Rule Description section.*



6. Click the underlined words in the rule description to check for a domain, sender, or text string in the subject line.  
*The Edit Auto-Remove Rule dialog box appears.*



7. To add a new domain, sender, or string, type it in the **Enter text to match** text box and click **Add**.
8. To remove a domain, sender, or string, select it from the list and click **Remove**.

There are three restrictions on the rules you can create:

- Rules do not support wildcard characters. For example, you cannot create the rule *Auto-Remove messages from \*.gov* to auto-remove email from all domains with the .gov extension.
- When you remove a domain, sender, or string, Quarantine Server deletes only subsequent email messages that match this rule. It does not delete current messages in the database that match the new rule.
- Rules which auto-block messages that match a specified text string apply only to text in the subject line. If the text is in the body of the message, but not in the subject line, the message is not removed.

## Define the Quarantine Server Location on the XTM Device

You must define the location of the Quarantine Server in the XTM device configuration. You can use Policy Manager to specify the IP address of the of the Quarantine Server where the XTM device sends email messages to be quarantined.

1. Select **Subscription Services > Quarantine Server**.

*The Quarantine Server dialog box appears.*



2. Type the IP address for the Quarantine Server. We recommend that you do not change the Quarantine Server port unless asked to do so by a WatchGuard technical support representative.
3. To send all email messages that spamBlocker or Gateway AntiVirus handles to the Quarantine Server, select the **Enable debugging for SMTP** check box.  
If an email message is not handled by spamBlocker because it matches a spamBlocker exception, it is not sent to the Quarantine Server.
4. If you want to cancel the changes you made in this dialog box and return to the default entries, click **Restore Defaults**.

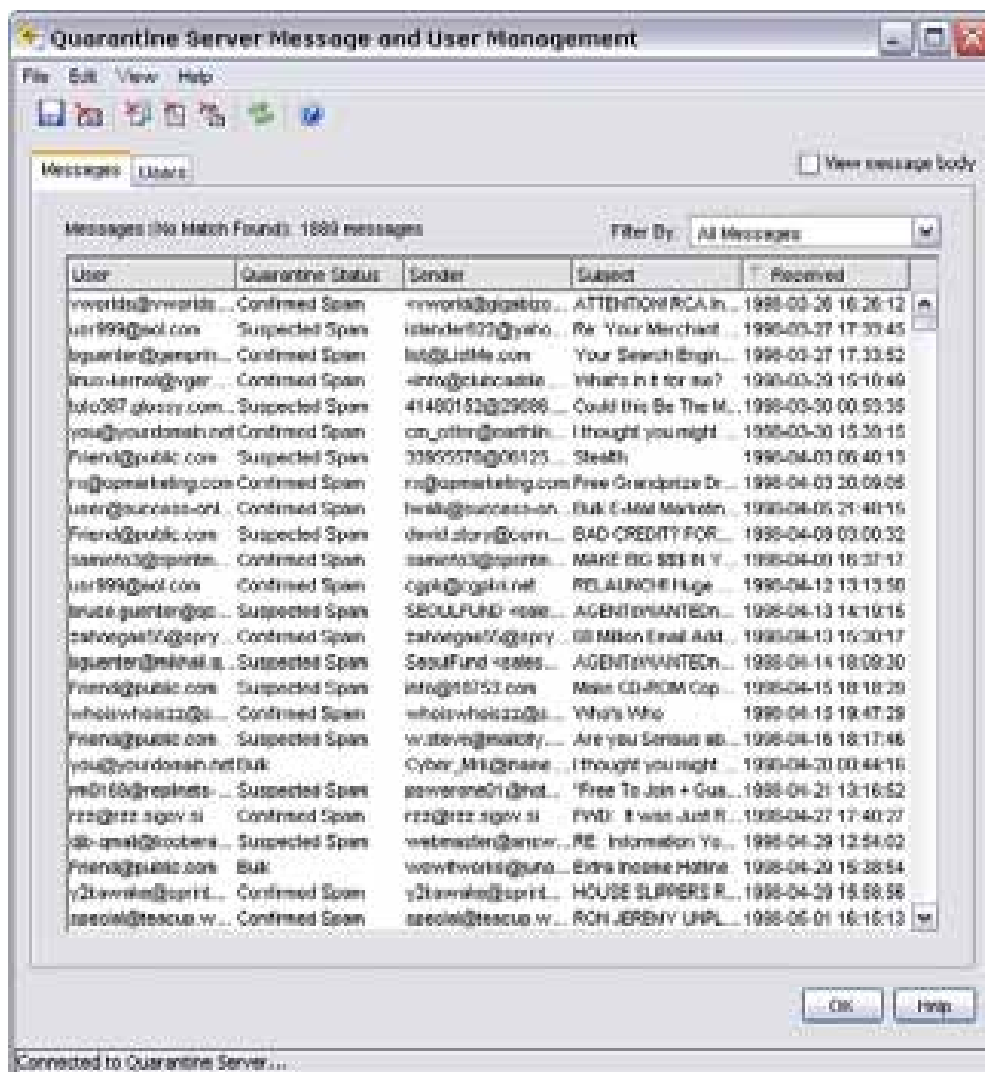
## About the Quarantine Server Client

The Quarantine Server Client allows you to manage Quarantine Server messages and users. You start the Quarantine Server Client from WatchGuard System Manager.

1. Click .  
Or, select **Tools > Quarantine Server Client**.



2. In the **Name/IP Address** text box, type or select a server by its hostname or IP address.  
If your Quarantine Server is installed on the same computer as WatchGuard System Manager, you can type **localhost** in the **Name/IP Address** text box.
3. In the **Username** text box, type the user name.  
This user must have Super Administrator privileges.  
For information about role-based administration, see *About Role-Based Administration* on page 665.
4. In the **Password** text box, type the password for the Super Administrator user.
5. Click **OK**.  
*The Quarantine Server Message and User Management dialog box appears.*



From the **Quarantine Server Message and User Management** dialog box, you can:

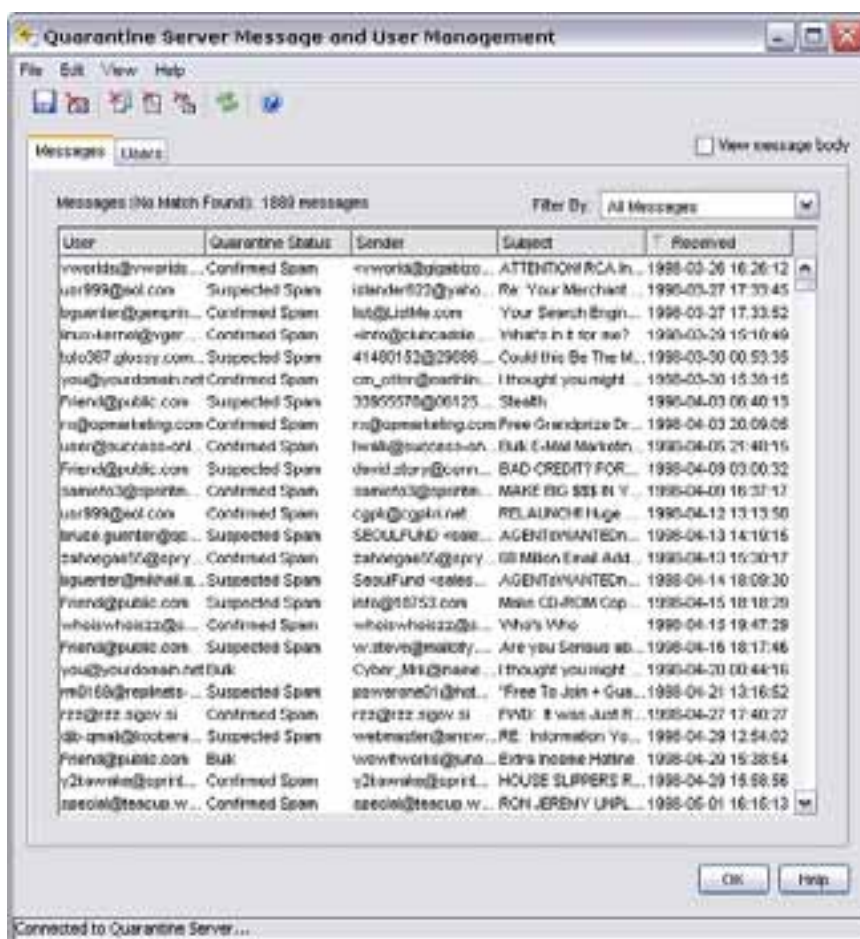
- *Manage Quarantined Messages*
- *Manage Quarantine Server Users*
- *Get Statistics on Quarantine Server Activity*

## Manage Quarantined Messages

You can see all messages on the Quarantine Server in the Quarantine Server Client. You can sort messages by user, quarantine status, sender, subject, and date/time received.

## View Quarantined Messages

To launch the Quarantine Server client from WatchGuard System Manager, select **Tools > Quarantine Server Client**. For details, see *About the Quarantine Server Client* on page 1238. The **Quarantine Server Message and User Management** dialog box appears. The quarantined messages appear in the **Messages** tab.



## Set Message Viewing Options


Click on any column heading to sort the list of messages. You can use the **Filter By** drop-down list to see all messages, or only those with a specified quarantine status.

To see the body of a message, select the **View message body** check box. Select any message. A second pane appears at the bottom of the dialog box that shows the message body. You can also select any message and select **Edit > View Message Body**, or right-click any message and select **View Message Body**.



## Save Messages to a Local File

You can save a copy of a message on the Quarantine Server to a file.


1. On the **Messages** tab of the **Quarantine Server Message and User Management** dialog box, select the message you want to save. You can save only one message at a time.
2. Click .  
Or, select **File > Save As**.  
Or, right-click the message and select **Save As**.
3. Type or select the location where you want to save the file. Click **Save**.

## Release Quarantined Messages to the Recipient

You can only release spam email messages to users. You cannot release messages that contain or are suspected to contain viruses.

1. On the **Messages** tab, select the message or messages you want to release.
  - To select a range of messages, click the first message, hold down the Shift key, and click the last message in the range.
  - To select multiple messages that are not in a range, hold down Ctrl as you select each message.
  - To select all messages, select **Edit >Select All**. Or, right-click any message and select **Select All**.
2. Select **Edit > Release Message**.  
Or, right-click a selected message and select **Release Message**.  
*After the message is sent to the user, the message is removed from the Messages tab.*

## Delete Messages Manually

1. On the **Messages** tab, select the message or messages you want to delete.
  - To select a range of messages, click the first message, hold down the Shift key, and click the last message in the range.
  - To select multiple messages that are not in a range, hold down Ctrl as you select messages.
  - To select all messages, select **Edit >Select All**.  
Or, right-click any message and select **Select All**.
2. Click .  
Or, select **Edit > Delete**.

## Delete Messages Automatically

You can have Quarantine Server automatically delete all future email messages from a specified domain or sender, or automatically delete messages that contain specified text in the subject line. All subsequent messages sent to any user with these properties are automatically deleted.

1. On the **Messages** tab, select the message or messages with the properties that you want to automatically delete.
  - To select a range of messages, click the first message, press the **Shift** key, and click the last message in the range.
  - To select multiple messages that are not in a range, hold down **Ctrl** as you select messages.
  - To select all messages, select **Edit > Select All**. Or, right-click any message and select **Select All**.
2. Choose an option for automatic deletion.
  - From the **Edit** menu, select **Auto-Remove > Sender Domain**, **Auto-Remove > Sender**, or **Auto-Remove > Subject**. These options are also available from the right-click (context) menu.
  - You can also use the equivalent icons to select these options.

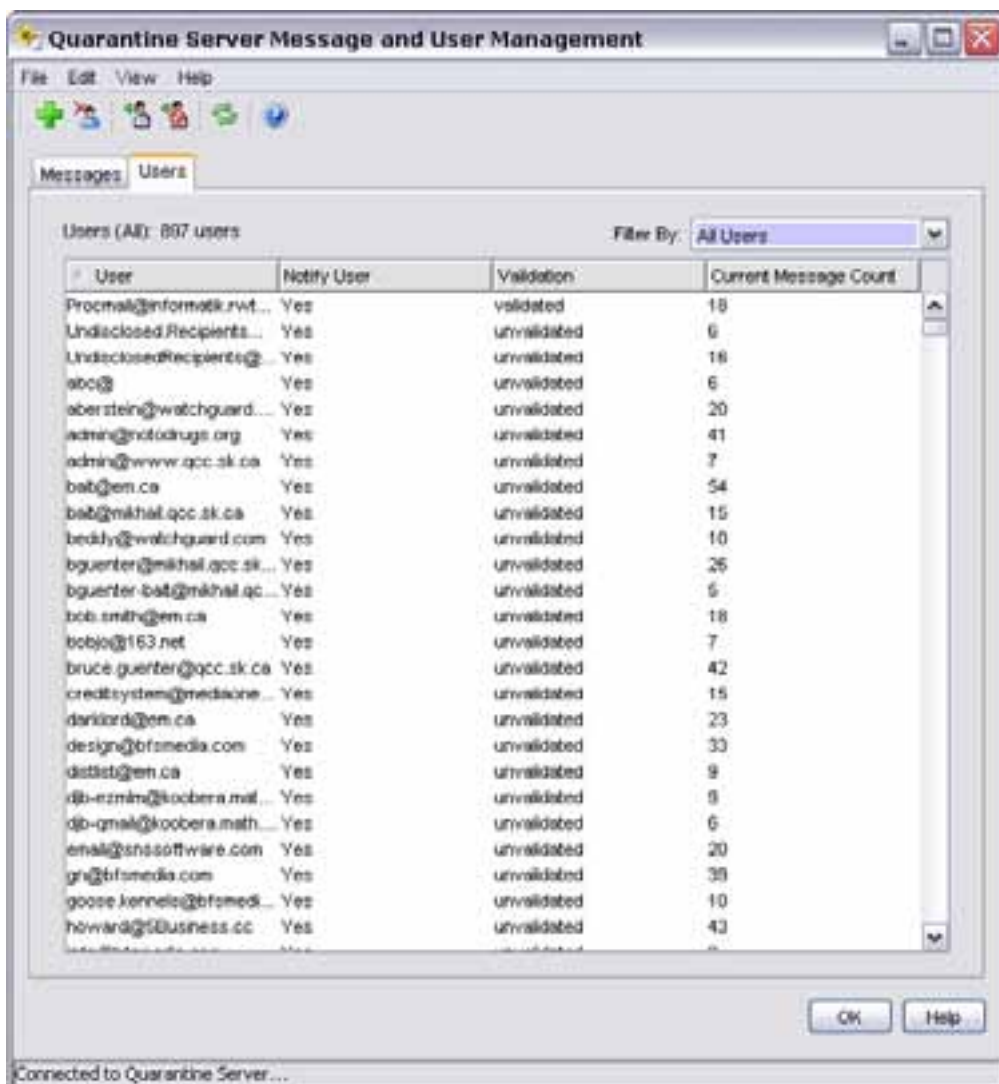
## Manage Quarantine Server Users

Quarantine Server maintains a list of all users who have an email message stored on the Quarantine Server. You can use the Quarantine Server Client to view, add, and delete users, and to change user notification settings.

### View Quarantine Server Users

To start the Quarantine Server Client from WatchGuard System Manager, select **Tools > Quarantine Server Client**. For more information, see *About the Quarantine Server Client* on page 1238.

When the **Quarantine Server Message and User Management** dialog box appears, select the **Users** tab.



The **Users** tab shows:

- Email addresses of users that can have email messages sent to the Quarantine Server.
- If users are notified when they have email on the Quarantine Server.
- If users are validated or unvalidated. A user is validated when he or she gets a message in an email client about messages on the Quarantine Server, and the user clicks the link to go to the Quarantine Server. Many "users" shown on the Quarantine Server are never validated, because the email address does not match a real user.
- The number of messages currently on the Quarantine Server that are addressed to that user. If you want to see only validated or unvalidated users, from the **Filter by** drop-down list, select **Validated Users** or **Unvalidated Users**.

## Add Users

Users are automatically added when messages are sent to the Quarantine Server for them. Use this procedure to manually add users:


1. Launch the Quarantine Server Client.  
*The Quarantine Server Message and User Management dialog box appears.*
2. From the **Quarantine Server Message and User Management** dialog box, click the **Users** tab.
3. Select **Edit > Add User**.  
*The Add User dialog box appears.*



4. Type the full email address of the user, such as name@example.com.
5. Select **Send notification for this user** or **Do not send notification** to specify if you want the user to be notified when the Quarantine Server receives a message for him or her.
6. Click **OK**.  
For more information, see *About the Quarantine Server Client* on page 1238.



## Remove Users

When you remove a user, all email messages stored on the Quarantine Server for that user are also deleted.

1. From the **Quarantine Server Message and User Management** dialog box, select the **Users** tab.
  2. Select the user you want to delete and click .
- Or, select **Edit > Delete**.

## Change the Notification Option for a User

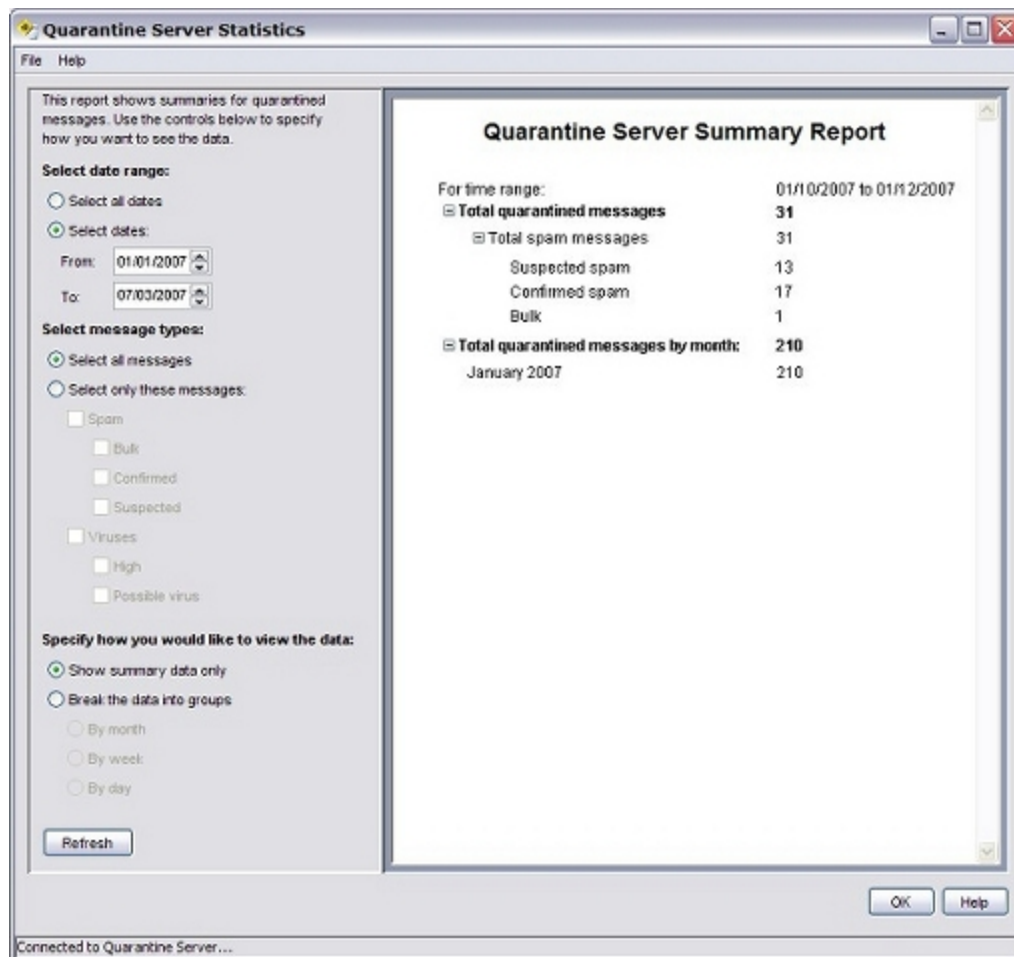
You can automatically notify users when they have email messages stored on the Quarantine Server.

1. From the **Quarantine Server Message and User Management** dialog box, select the **Users** tab.
2. To enable notification for a user, select the user and click .  
Or, select **Edit > Notify User > Yes**.
3. To disable notification for a user, select the user and click .  
Or, select **Edit > Notify User > No**.

## Get Statistics on Quarantine Server Activity

Quarantine Server stores the total number of messages, the reason each message was quarantined, and the number of messages deleted manually or automatically. You can see these statistics from the Quarantine Server Client.

1. To launch the Quarantine Server client from WatchGuard System Manager, select **Tools > Quarantine Server Client**. For details, see *About the Quarantine Server Client* on page 1238. *The Quarantine Server Message and User Management dialog box appears.*
2. From the **Quarantine Server Message and User Management** dialog box, select **View > Statistics**.



## See Statistics from Specific Dates

You can limit the statistics to see only messages from a specified range of dates:

1. From the **Quarantine Server Statistics** dialog box, select **Select dates**.
2. Type the start and end dates in the **From** and **To** fields.

## See Specific Types of Messages

You can specify whether you want to see statistics only for messages that are suspected spam, confirmed spam, or part of bulk mailings, or that contain or possibly contain viruses. Select the **Select only these messages** radio button, then choose the type or types of messages you want to see.

## Group Statistics by Month, Week, or Day

By default, only summary data is shown. You can see the data grouped by month, week, or day.

1. From the **Quarantine Server Statistics** dialog box, select **Break the data into groups**.
2. Select an option: **By Month**, **By Week**, or **By Day**.

## Export and Print Statistics

To export Quarantine Server statistics to a Microsoft Excel spreadsheet (.xls) format:

From the **Quarantine Server Statistics** dialog box, select **File > Export to Excel**.

To export Quarantine Server statistics to comma-separated values (.csv) format:

From the **Quarantine Server Statistics** dialog box, select **File > Export to Csv**.

To print Quarantine Server statistics:

From the **Quarantine Server Statistics** dialog box, select **File > Print**.

# Configure User Notification with Microsoft Exchange Server 2003 or 2007

Microsoft Exchange Server has specific authentication requirements that you must consider when you configure your Quarantine Server. If you use a Microsoft Exchange Server 2003 or 2007 as your SMTP server and you want to enable user notification on your Quarantine Server, you might have to complete some additional configuration tasks. The tasks you must complete depend on whether or not your Microsoft Exchange Server requires authentication. The subsequent sections are two examples of methods you can use to change your configuration settings on the Quarantine Server and the Microsoft Exchange Server. The first example is for servers that do not require authentication. The second is for servers that do require authentication.


**Note** WatchGuard provides interoperability instructions to help our customers configure WatchGuard products to work with products created by other organizations. If you need more information or technical support about configuring a non-WatchGuard product, see the documentation and support resources for that product.

In these examples, the IP address of the Quarantine Server is 192.168.2.100. The Microsoft Exchange Server (SMTP/POP3) is installed on the same computer.

## Configure User Notification if Your Microsoft Exchange Server Does Not Require Authentication

Use these configuration settings if your Microsoft Exchange Server is configured to not require authentication.

### Configure the Quarantine Server

1. Right-click  in the system tray and select **Open WatchGuard Server Center**.
2. Type the Administrator passphrase.  
*The WatchGuard Server Center appears.*
3. In the **Servers** tree, select **Quarantine Server**.  
*The Quarantine Server Server Settings page appears.*
4. In the **SMTP Server Settings** section, in the **Outgoing e-mail server (SMTP)** text box, type the domain name or IP address of the SMTP server. For this example, type 192.168.2.100.
5. Make sure the **Use login information for the E-mail server** check box is not selected.
6. Select the **Notification** tab.
7. Select the **Send an email notification to users when they have messages on the Quarantine Server** check box.
8. Configure the **User Notification** settings for the notification email.
9. Click **OK**.

*The Quarantine Server sends an email to all user accounts that have ever had an email quarantined.*

For information about user notification settings, see *Configure User Notification Settings*.

## Configure the Microsoft Exchange Server (2007)

To enable your Exchange server to accept email notifications from the Quarantine Server, use the Exchange Management Console to configure a Receive Connector to receive messages from the Quarantine Server. Before you begin this procedure, make sure all other settings on the Exchange Server are configured correctly for email delivery.


1. Open the Exchange Management Console.
2. From the console tree on the left pane, click the **Server Configuration** node to expand it.
3. Below the Server Configuration node, click the **Hub Transport** node.
4. In the work pane, select the **Receive Connectors** tab.
5. Select **Create new Receive Connector**.
6. Select the **Network** tab.
7. In the **Receive mail from remote servers that have these IP addresses** list, click **Add**.
8. Add the IP address of your Quarantine Server. For this example, add 192.168.2.100.
9. Select the **Permission Groups** tab.
10. Select **Anonymous users**.
11. Do not change the other settings.

After you complete these configuration changes, the Quarantine Server scheduled notification and Send Now notification should operate.

## Configure User Notification if Your Microsoft Exchange Server Requires Authentication

Use these configuration settings if your Microsoft Exchange Server is configured to require authentication.

### Configure the Quarantine Server

1. Right-click  in the system tray and select **Open WatchGuard Server Center**.
2. Type the Administrator passphrase.  
*The WatchGuard Server Center appears.*
3. In the **Servers** tree, select **Quarantine Server**  
*The Quarantine Server Server Settings page appears.*
4. In the **SMTP Server Settings** section, in the **Outgoing e-mail server (SMTP)** text box, type the domain name or IP address of the SMTP server. For this example, type 192.168.2.100.
5. Select the **Use login information for the E-mail server** check box.
6. In the **User name** text box, type an the email address of a user who is a Domain Admin on the Microsoft Exchange Server. For this example, type ricky@wgrd-tech.com.
7. In the **Password** text box, type the email password for this user.
8. Select the **Notification** tab.
9. Select the **Send an email notification to users when they have messages on the Quarantine Server** check box.
10. Configure the **User Notification** settings for the notification email.
11. Click **OK**.  
*The Quarantine Server sends an email to all user accounts that have ever had an email quarantined.*

For information about user notification settings, see *Configure User Notification Settings*.



## Configure the Microsoft Exchange Server (2007)

To enable your Exchange server to accept email notifications from the Quarantine Server, we recommend you use the settings in the subsequent steps.

1. Open the Exchange Management Console.
2. From the console tree on the left pane, click the **Server Configuration** node to expand it.
3. Below the Server Configuration node, click the **Hub Transport** node.
4. In the work pane, select the **Receive Connectors** tab.
5. Select **Create new Receive Connector**.
6. Select the **Network** tab.
7. In the **Receive mail from remote servers that have these IP addresses** list, click **Add**.
8. Add the IP address of your Quarantine Server. For this example, add 192.168.2.100.
9. Select the **Permission Groups** tab.
10. Select **Exchange Servers**.
11. Select the **Authentication** tab.
12. Select **Basic Authentication**.
13. Make sure the user you added to the Quarantine Server configuration is a member of the **Domain Admins** group. For this example, make sure the user ricky is a member of Domain Admins.

After you complete these configuration changes, the Quarantine Server scheduled notification and Send Now notification should operate.

