



UAG Series

UAG2100 / UAG4100 / UAG5100

Unified Access Gateway

Version 4.10
Edition 1, 03/2015

User's Guide

Default Login Details

LAN IP Address	http://172.16.0.1 (LAN1) http://172.17.0.1 (LAN2)
User Name	admin
Password	1234

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

The Quick Start Guide shows how to connect the UAG and access the Web Configurator wizards. (See the wizard real time help for information on configuring each screen.) It also contains a package contents list.

- CLI Reference Guide

The CLI Reference Guide explains how to use the Command-Line Interface (CLI) to configure the UAG.

Note: It is recommended you use the Web Configurator to configure the UAG.

- Web Configurator Online Help

Click the help icon in any screen for help in configuring that screen and supplementary information.

Contents Overview

Introduction	20
Hardware Installation and Connection	36
Printer Deployment	42
Installation Setup Wizard	50
Quick Setup Wizards	64
Dashboard	80
Monitor	91
Licensing	131
Wireless	136
Interfaces	154
Trunks	195
Policy and Static Routes	203
DDNS	214
NAT	219
VPN 1-1 Mapping	226
HTTP Redirect	231
SMTP Redirect	235
ALG	239
UPnP	241
IP/MAC Binding	248
Layer 2 Isolation	253
IPnP	257
Web Authentication	259
RTLS	286
Security Policy	289
Billing	304
Printer	322
Free Time	332
SMS	336
IPSec VPN	338
Bandwidth Management	366
Application Patrol	376
Content Filtering	381
Zones	395
User/Group	399
AP Profile	414
MON Profile	430
Application	435
Addresses	442

Services	447
Schedules	453
AAA Server	459
Authentication Method	464
Certificates	467
ISP Accounts	483
System	486
Log and Report	534
File Manager	549
Diagnostics	560
Packet Flow Explore	572
Reboot	581
Shutdown	582
Troubleshooting	583

Table of Contents

Contents Overview	3
Table of Contents	5
Chapter 1	
Introduction.....	20
1.1 Overview	20
1.2 Default Zones, Interfaces, and Ports	21
1.3 Management Overview	21
1.4 Web Configurator	22
1.4.1 Web Configurator Access	23
1.4.2 Web Configurator Screens Overview	23
1.4.3 Navigation Panel	26
1.4.4 Tables and Lists	32
1.5 Stopping the UAG	35
Chapter 2	
Hardware Installation and Connection	36
2.1 Rack-mounting (UAG5100)	36
2.2 Wall Mounting (UAG2100 and UAG4100)	37
2.3 Front Panel	38
2.3.1 Front Panel LEDs	39
2.4 Rear Panel	40
2.4.1 UAG2100 or UAG4100	40
2.4.2 UAG5100	41
Chapter 3	
Printer Deployment.....	42
3.1 Overview	42
3.2 Attach the Printer to the UAG	42
3.3 Set up an Internet Connection on the UAG	42
3.4 Allow the UAG to Monitor and Manage the Printer	43
3.5 Turn on Web Authentication on the UAG	46
3.6 Generate a Free Guest Account	47
Chapter 4	
Installation Setup Wizard	50
4.1 Welcome Screen	50
4.2 Internet Settings	50
4.2.1 Internet Settings: Ethernet	52

4.2.2 Internet Settings: PPPoE	53
4.2.3 Internet Settings: PPTP	54
4.2.4 Internet Settings - Second WAN Interface	55
4.3 Wireless Settings	56
4.3.1 Wireless and Radio Settings	56
4.4 Web Authentication Settings	57
4.5 Printer Settings	58
4.5.1 Printer List and Printout Settings	59
4.6 Billing Settings	59
4.6.1 Billing Profile	60
4.6.2 Account Generator Settings	61
4.7 Free Time Settings	62
4.8 Device Registration	63
Chapter 5	
Quick Setup Wizards	64
5.1 Quick Setup Overview	64
5.2 WAN Interface Quick Setup	65
5.2.1 Choose an Ethernet Interface	65
5.2.2 Select WAN Type	65
5.2.3 Configure WAN IP Settings	66
5.2.4 ISP and WAN Connection Settings	66
5.2.5 Quick Setup Interface Wizard: Summary	68
5.3 VPN Setup Wizard	70
5.3.1 Welcome	70
5.3.2 VPN Setup Wizard: Wizard Type	71
5.3.3 VPN Express Wizard - Scenario	71
5.3.4 VPN Express Wizard - Configuration	72
5.3.5 VPN Express Wizard - Summary	72
5.3.6 VPN Express Wizard - Finish	73
5.3.7 VPN Advanced Wizard - Scenario	74
5.3.8 VPN Advanced Wizard - Phase 1 Settings	75
5.3.9 VPN Advanced Wizard - Phase 2	76
5.3.10 VPN Advanced Wizard - Summary	77
5.3.11 VPN Advanced Wizard - Finish	78
Chapter 6	
Dashboard	80
6.1 Overview	80
6.1.1 What You Can Do in this Chapter	80
6.2 The Dashboard Screen	80
6.2.1 The CPU Usage Screen	86
6.2.2 The Memory Usage Screen	86

6.2.3 The Active Sessions Screen	87
6.2.4 The VPN Status Screen	88
6.2.5 The DHCP Table Screen	88
6.2.6 The Number of Login Users Screen	89
Chapter 7	
Monitor.....	91
7.1 Overview	91
7.1.1 What You Can Do in this Chapter	91
7.2 The Port Statistics Screen	92
7.2.1 The Port Statistics Graph Screen	93
7.3 The Interface Status Screen	94
7.4 The Traffic Statistics Screen	97
7.5 The Session Monitor Screen	99
7.6 The DDNS Status Screen	101
7.7 The IP/MAC Binding Monitor Screen	101
7.8 The Login Users Screen	102
7.9 The Dynamic Guest Screen	103
7.10 The UPnP Port Status Screen	105
7.11 The USB Storage Screen	106
7.12 The Ethernet Neighbor Screen	107
7.13 The AP List Screen	109
7.13.1 Station Count of AP	110
7.14 The Radio List Screen	112
7.14.1 AP Mode Radio Information	114
7.15 The Station List Screen	115
7.16 Detected Device	116
7.17 The Printer Status Screen	118
7.18 The VPN 1-1 Mapping Status Screen	118
7.18.1 VPN 1-1 Mapping Statistics	119
7.19 The IPSec Monitor Screen	120
7.19.1 Regular Expressions in Searching IPSec SAs	121
7.20 The App Patrol Screen	121
7.21 The Content Filter Screen	123
7.22 The Log Screen	125
7.22.1 View AP Log	127
7.22.2 Dynamic Users Log	129
Chapter 8	
Licensing.....	131
8.1 Overview	131
8.1.1 What You Can Do in this Chapter	131
8.1.2 What you Need to Know	131

8.2 Registration Screen	132
8.3 Service Screen	132
8.4 App Patrol Signature Update Screen	133
Chapter 9	
Wireless	136
9.1 Overview	136
9.1.1 What You Can Do in this Chapter	136
9.1.2 What You Need to Know	136
9.2 Controller Screen	137
9.3 AP Management Screen	137
9.3.1 Edit AP List	139
9.3.2 Port Setting Edit	140
9.3.3 VLAN Add/Edit	141
9.3.4 AP Policy	143
9.4 MON Mode	144
9.4.1 Add/Edit Rogue/Friendly List	145
9.5 Load Balancing	146
9.5.1 Disassociating and Delaying Connections	147
9.6 DCS	148
9.7 Auto Healing	151
9.8 Technical Reference	152
9.8.1 Dynamic Channel Selection	152
9.8.2 Load Balancing	153
Chapter 10	
Interfaces	154
10.1 Interface Overview	154
10.1.1 What You Can Do in this Chapter	154
10.1.2 What You Need to Know	154
10.2 Port Role Screen	156
10.3 Ethernet Summary Screen	157
10.3.1 Ethernet Edit	159
10.3.2 Object References	165
10.3.3 Add/Edit DHCP Extended Options	166
10.4 PPP Interfaces	168
10.4.1 PPP Interface Summary	169
10.4.2 PPP Interface Add or Edit	170
10.5 VLAN Interfaces	174
10.5.1 VLAN Interface Summary Screen	175
10.5.2 VLAN Interface Add/Edit	176
10.6 Bridge Interfaces	181
10.6.1 Bridge Interface Summary	183

10.6.2 Bridge Interface Add/Edit	184
10.7 Virtual Interfaces	189
10.7.1 Virtual Interfaces Add/Edit	190
10.8 Interface Technical Reference	191
Chapter 11	
Trunks.....	195
11.1 Overview	195
11.1.1 What You Can Do in this Chapter	195
11.1.2 What You Need to Know	195
11.2 The Trunk Summary Screen	198
11.2.1 Configuring a User-Defined Trunk	199
11.2.2 Configuring the System Default Trunk	201
Chapter 12	
Policy and Static Routes	203
12.1 Policy and Static Routes Overview	203
12.1.1 What You Can Do in this Chapter	203
12.1.2 What You Need to Know	203
12.2 Policy Route Screen	205
12.2.1 Policy Route Add/Edit Screen	207
12.3 IP Static Route Screen	211
12.3.1 Static Route Add/Edit Screen	211
12.4 Policy Routing Technical Reference	212
Chapter 13	
DDNS.....	214
13.1 DDNS Overview	214
13.1.1 What You Can Do in this Chapter	214
13.1.2 What You Need to Know	214
13.2 The DDNS Screen	215
13.2.1 The Dynamic DNS Add/Edit Screen	216
Chapter 14	
NAT.....	219
14.1 NAT Overview	219
14.1.1 What You Can Do in this Chapter	219
14.1.2 What You Need to Know	219
14.2 The NAT Screen	220
14.2.1 The NAT Add/Edit Screen	221
14.3 NAT Technical Reference	224
Chapter 15	
VPN 1-1 Mapping	226

15.1 VPN 1-1 Mapping Overview	226
15.1.1 What You Can Do in this Chapter	226
15.1.2 What You Need to Know	226
15.2 The VPN 1-1 Mapping General Screen	227
15.2.1 The VPN 1-1 Mapping Edit Screen	228
15.3 The VPN 1-1 Mapping Profile Screen	229
Chapter 16	
HTTP Redirect	231
16.1 Overview	231
16.1.1 What You Can Do in this Chapter	231
16.1.2 What You Need to Know	231
16.2 The HTTP Redirect Screen	232
16.2.1 The HTTP Redirect Edit Screen	233
Chapter 17	
SMTP Redirect	235
17.1 Overview	235
17.1.1 What You Can Do in this Chapter	235
17.1.2 What You Need to Know	235
17.2 The SMTP Redirect Screen	236
17.2.1 The SMTP Redirect Edit Screen	237
Chapter 18	
ALG	239
18.1 ALG Overview	239
18.1.1 What You Can Do in this Chapter	239
18.1.2 What You Need to Know	239
18.1.3 Before You Begin	240
18.2 The ALG Screen	240
Chapter 19	
UPnP	241
19.1 Overview	241
19.2 What You Need to Know	241
19.2.1 NAT Traversal	241
19.2.2 Cautions with UPnP	242
19.3 UPnP Screen	242
19.4 Technical Reference	243
19.4.1 Using UPnP in Windows XP Example	243
19.4.2 Web Configurator Easy Access	245
Chapter 20	
IP/MAC Binding	248

20.1 IP/MAC Binding Overview	248
20.1.1 What You Can Do in this Chapter	248
20.1.2 What You Need to Know	248
20.2 IP/MAC Binding Summary	249
20.2.1 IP/MAC Binding Edit	250
20.2.2 Static DHCP Edit	251
20.3 IP/MAC Binding Exempt List	251
Chapter 21	
Layer 2 Isolation	253
21.1 Overview	253
21.1.1 What You Can Do in this Chapter	253
21.2 Layer-2 Isolation General Screen	254
21.3 White List Screen	254
21.3.1 Add/Edit White List Rule	255
Chapter 22	
IPnP	257
22.1 Overview	257
22.1.1 What You Can Do in this Chapter	257
22.2 IPnP Screen	258
Chapter 23	
Web Authentication	259
23.1 Overview	259
23.1.1 What You Can Do in this Chapter	259
23.1.2 What You Need to Know	260
23.2 Web Authentication	260
23.2.1 General Screen	260
23.2.2 User-aware Access Control Example	264
23.2.3 Authentication Type Screen	271
23.2.4 Custom Web Portal / User Agreement File Screen	276
23.3 Walled Garden	277
23.3.1 General Screen	278
23.3.2 URL Base Screen	278
23.3.3 Domain/IP Base Screen	280
23.3.4 Walled Garden Login Example	282
23.4 Advertisement Screen	283
23.4.1 Adding/Editing an Advertisement URL	284
Chapter 24	
RTLS	286
24.1 Overview	286

24.1.1 What You Can Do in this Chapter	286
24.2 Before You Begin	287
24.3 Configuring RTLS	287
Chapter 25	
Security Policy	289
25.1 Overview	289
25.1.1 What You Can Do in this Chapter	289
25.1.2 What You Need to Know	290
25.2 Security Policy Control Screen	291
25.2.1 Configuring the Security Policy Control Screen	292
25.2.2 Add/Edit Policy Control Rule	294
25.3 Session Control Screen	296
25.3.1 Add/Edit a Session Limit Rule	298
25.4 Security Policy Configuration Example	299
25.5 Security Policy Example Applications	301
Chapter 26	
Billing	304
26.1 Overview	304
26.1.1 What You Can Do in this Chapter	304
26.1.2 What You Need to Know	304
26.2 The General Screen	305
26.3 The Billing Profile Screen	307
26.3.1 The Account Generator Screen	308
26.3.2 The Account Redeem Screen	311
26.3.3 The Billing Profile Add/Edit Screen	313
26.4 The Discount Screen	314
26.4.1 The Discount Add/Edit Screen	316
26.5 The Payment Service General Screen	316
26.5.1 The Payment Service Desktop View / Mobile View Screen	318
Chapter 27	
Printer	322
27.1 Overview	322
27.1.1 What You Can Do in this Chapter	322
27.2 The General Setting Screen	322
27.2.1 Add/Edit Printer Rule	324
27.3 The Printout Configuration Screen	325
27.4 The Printer Manager Screen	326
27.4.1 Edit Printer Manager	327
27.4.2 Reports Overview	328
27.4.3 Key Combinations	328

27.4.4 Daily Account Summary	328
27.4.5 Monthly Account Summary	329
27.4.6 Account Report Notes	330
27.4.7 System Status	330
Chapter 28	
Free Time.....	332
28.1 Overview	332
28.1.1 What You Can Do in this Chapter	332
28.2 The Free Time Screen	332
Chapter 29	
SMS.....	336
29.1 Overview	336
29.1.1 What You Can Do in this Chapter	336
29.2 The SMS Screen	336
Chapter 30	
IPSec VPN.....	338
30.1 Virtual Private Networks (VPN) Overview	338
30.1.1 What You Can Do in this Chapter	338
30.1.2 What You Need to Know	339
30.1.3 Before You Begin	339
30.2 The VPN Connection Screen	340
30.2.1 The VPN Connection Add/Edit Screen	341
30.3 The VPN Gateway Screen	347
30.3.1 The VPN Gateway Add/Edit Screen	348
30.4 IPSec VPN Background Information	354
Chapter 31	
Bandwidth Management.....	366
31.1 Overview	366
31.1.1 What You Can Do in this Chapter	366
31.1.2 What You Need to Know	366
31.2 The Bandwidth Management Screen	370
31.2.1 The Bandwidth Management Add/Edit Screen	372
Chapter 32	
Application Patrol.....	376
32.1 Overview	376
32.1.1 What You Can Do in this Chapter	376
32.1.2 What You Need to Know	376
32.2 Application Patrol Profile	377

32.2.1 Add/Edit Application Patrol Profile	378
32.2.2 Add/Edit Application Patrol Profile Rule Application	380
Chapter 33	
Content Filtering.....	381
33.1 Overview	381
33.1.1 What You Can Do in this Chapter	381
33.1.2 What You Need to Know	381
33.1.3 Before You Begin	382
33.2 Content Filter Profile Screen	383
33.2.1 Add/Edit Content Filter Profile	385
33.3 Content Filter Trusted Web Sites Screen	391
33.4 Content Filter Forbidden Web Sites Screen	392
33.5 Content Filter Technical Reference	393
Chapter 34	
Zones	395
34.1 Zones Overview	395
34.1.1 What You Can Do in this Chapter	395
34.1.2 What You Need to Know	395
34.2 The Zone Screen	396
34.2.1 Add/Edit Zone	397
Chapter 35	
User/Group.....	399
35.1 Overview	399
35.1.1 What You Can Do in this Chapter	399
35.1.2 What You Need To Know	399
35.2 User Summary Screen	401
35.2.1 User Add/Edit Screen	402
35.3 User Group Summary Screen	405
35.3.1 Group Add/Edit Screen	405
35.4 User/Group Setting Screen	406
35.4.1 Default User Settings Edit Screens	409
35.4.2 User Aware Login Example	410
35.5 MAC Address Screen	411
35.5.1 Add/Edit MAC Address	412
35.6 User /Group Technical Reference	413
Chapter 36	
AP Profile.....	414
36.1 Overview	414
36.1.1 What You Can Do in this Chapter	414

36.1.2 What You Need To Know	414
36.2 Radio Screen	415
36.2.1 Add/Edit Radio Profile	417
36.3 SSID Screen	420
36.3.1 SSID List	420
36.3.2 Add/Edit SSID Profile	422
36.3.3 Security List	424
36.3.4 Add/Edit Security Profile	425
36.3.5 MAC Filter List	428
36.3.6 Add/Edit MAC Filter Profile	428
Chapter 37	
MON Profile	430
37.1 Overview	430
37.1.1 What You Can Do in this Chapter	430
37.1.2 What You Need To Know	430
37.2 MON Profile	430
37.2.1 Add/Edit MON Profile	431
37.3 Technical Reference	433
Chapter 38	
Application	435
38.1 Overview	435
38.1.1 What You Can Do in this Chapter	436
38.2 Application Screen	436
38.2.1 Add Application Rule	437
38.3 Application Group Screen	440
38.3.1 Add Application Group Rule	441
Chapter 39	
Addresses	442
39.1 Overview	442
39.1.1 What You Can Do in this Chapter	442
39.1.2 What You Need To Know	442
39.2 Address Summary Screen	442
39.2.1 Address Add/Edit Screen	443
39.3 Address Group Summary Screen	444
39.3.1 Address Group Add/Edit Screen	445
Chapter 40	
Services	447
40.1 Overview	447
40.1.1 What You Can Do in this Chapter	447

40.1.2 What You Need to Know	447
40.2 The Service Summary Screen	448
40.2.1 The Service Add/Edit Screen	449
40.3 The Service Group Summary Screen	450
40.3.1 The Service Group Add/Edit Screen	451
Chapter 41	
Schedules.....	453
41.1 Overview	453
41.1.1 What You Can Do in this Chapter	453
41.1.2 What You Need to Know	453
41.2 The Schedule Summary Screen	454
41.2.1 The One-Time Schedule Add/Edit Screen	455
41.2.2 The Recurring Schedule Add/Edit Screen	456
41.3 The Schedule Group Summary Screen	457
41.3.1 The Schedule Group Add/Edit Screen	457
Chapter 42	
AAA Server.....	459
42.1 Overview	459
42.1.1 RADIUS Server	459
42.1.2 What You Can Do in this Chapter	459
42.1.3 What You Need To Know	459
42.2 RADIUS Server Summary	460
42.2.1 Adding/Editing a RADIUS Server	460
Chapter 43	
Authentication Method.....	464
43.1 Overview	464
43.1.1 What You Can Do in this Chapter	464
43.1.2 Before You Begin	464
43.2 Authentication Method Objects	464
43.2.1 Creating an Authentication Method Object	465
Chapter 44	
Certificates.....	467
44.1 Overview	467
44.1.1 What You Can Do in this Chapter	467
44.1.2 What You Need to Know	467
44.1.3 Verifying a Certificate	469
44.2 The My Certificates Screen	470
44.2.1 The My Certificates Add Screen	471
44.2.2 The My Certificates Edit Screen	473

44.2.3 The My Certificates Import Screen	476
44.3 The Trusted Certificates Screen	477
44.3.1 The Trusted Certificates Edit Screen	479
44.3.2 The Trusted Certificates Import Screen	481
Chapter 45	
ISP Accounts.....	483
45.1 Overview	483
45.1.1 What You Can Do in this Chapter	483
45.2 ISP Account Summary	483
45.2.1 ISP Account Edit	484
Chapter 46	
System.....	486
46.1 Overview	486
46.1.1 What You Can Do in this Chapter	486
46.2 Host Name	487
46.3 USB Storage	487
46.4 Date and Time	488
46.4.1 Pre-defined NTP Time Servers List	491
46.4.2 Time Server Synchronization	491
46.5 Console Port Speed	492
46.6 DNS Overview	493
46.6.1 DNS Server Address Assignment	493
46.6.2 Configuring the DNS Screen	493
46.6.3 Address Record	496
46.6.4 PTR Record	496
46.6.5 Adding an Address/PTR Record	496
46.6.6 CNAME Record	497
46.6.7 Adding a CNAME Record	497
46.6.8 Domain Zone Forwarder	498
46.6.9 Adding a Domain Zone Forwarder	498
46.6.10 MX Record	499
46.6.11 Adding a MX Record	500
46.6.12 Adding a DNS Service Control Rule	500
46.7 WWW Overview	501
46.7.1 Service Access Limitations	501
46.7.2 System Timeout	501
46.7.3 HTTPS	502
46.7.4 Configuring WWW Service Control	502
46.7.5 Service Control Rules	505
46.7.6 Customizing the WWW Login Page	506
46.7.7 HTTPS Example	511

46.8 SSH	518
46.8.1 How SSH Works	519
46.8.2 SSH Implementation on the UAG	520
46.8.3 Requirements for Using SSH	520
46.8.4 Configuring SSH	520
46.8.5 Secure Telnet Using SSH Examples	521
46.9 Telnet	523
46.9.1 Configuring Telnet	523
46.10 FTP	524
46.10.1 Configuring FTP	524
46.11 SNMP	525
46.11.1 Supported MIBs	526
46.11.2 SNMP Traps	527
46.11.3 Configuring SNMP	527
46.12 Authentication Server	528
46.12.1 Add/Edit Trusted RADIUS Client	530
46.13 Language	531
46.14 ZyXEL One Network (ZON) Utility	531
46.14.1 ZyXEL One Network (ZON) System Screen	532
Chapter 47	
Log and Report	534
47.1 Overview	534
47.1.1 What You Can Do In this Chapter	534
47.2 Email Daily Report	534
47.3 Log Settings Screens	536
47.3.1 Log Settings Summary	537
47.3.2 Edit System Log Settings	538
47.3.3 Edit Log on USB Storage Setting	542
47.3.4 Edit Remote Server Log Settings	543
47.3.5 Log Category Settings Screen	545
Chapter 48	
File Manager	549
48.1 Overview	549
48.1.1 What You Can Do in this Chapter	549
48.1.2 What you Need to Know	549
48.2 The Configuration File Screen	551
48.3 The Firmware Package Screen	555
48.4 The Shell Script Screen	557
Chapter 49	
Diagnostics	560

49.1 Overview	560
49.1.1 What You Can Do in this Chapter	560
49.2 The Diagnostics Screen	560
49.2.1 The Diagnostics Files Screen	561
49.3 The Packet Capture Screen	562
49.3.1 The Packet Capture Files Screen	565
49.4 The Core Dump Screen	566
49.4.1 The Core Dump Files Screen	566
49.5 The System Log Screen	567
49.6 The Network Tool Screen	568
49.7 The Wireless Frame Capture Screen	569
49.7.1 The Wireless Frame Capture Files Screen	571
Chapter 50	
Packet Flow Explore.....	572
50.1 Overview	572
50.1.1 What You Can Do in this Chapter	572
50.2 The Routing Status Screen	572
50.3 The SNAT Status Screen	578
Chapter 51	
Reboot	581
51.1 Overview	581
51.1.1 What You Need To Know	581
51.2 The Reboot Screen	581
Chapter 52	
Shutdown.....	582
52.1 Overview	582
52.1.1 What You Need To Know	582
52.2 The Shutdown Screen	582
Chapter 53	
Troubleshooting.....	583
53.1 Resetting the UAG	589
53.2 Getting More Troubleshooting Help	590
Appendix A Customer Support	591
Appendix B Legal Information.....	597
Index	604

Introduction

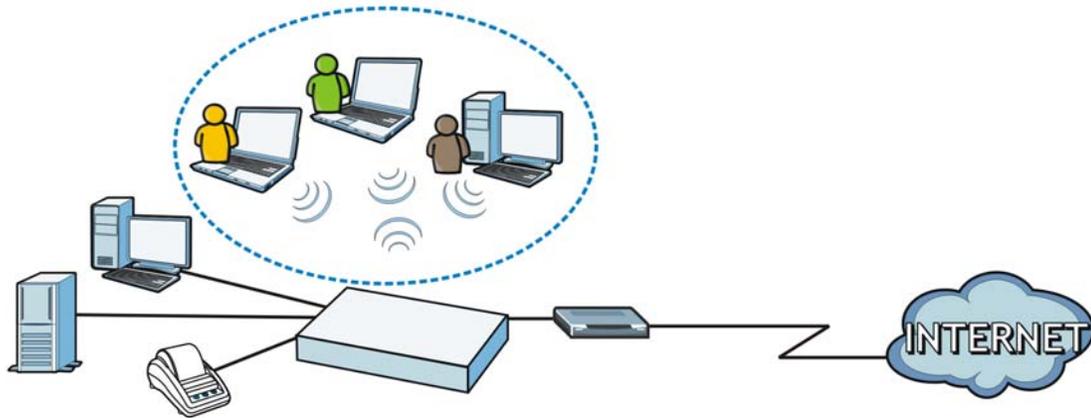
1.1 Overview

This User's Guide covers the following models: UAG2100, UAG4100 and UAG5100.

Table 1 UAG Series Comparison Table

FEATURES	UAG2100	UAG4100	UAG5100
SMS Service Subscription	√		
IPSec VPN (Site-to-Site)			√
Content Filtering			√
Application Patrol			√
Local AP (Built-in Wireless LAN Module)	√	√	
Drop-in Mode			√

The UAG is a comprehensive service gateway. The UAG combines an IEEE 802.11n wireless access point, router, 4-port switch and service gateway in one box. If you have a "statement printer", such as SP350E, you can connect it directly to the UAG, allowing you to easily print subscriber statements. The UAG is ideal for offices, coffee shops, libraries, hotels and airport terminals catering to subscribers that seek Internet access. You should have an Internet account already set up and have been given usernames, passwords etc. required for Internet access.



You can use web authentication to allow guests to access the network only after they authenticate with the UAG through a specifically designated login web page. You can also forward the authenticated client's e-mail messages to a specific SMTP server.

The UAG also provides bandwidth management, NAT, port forwarding, policy routing, DHCP server and many other powerful features. The UAG's security features include security policies and certificates.

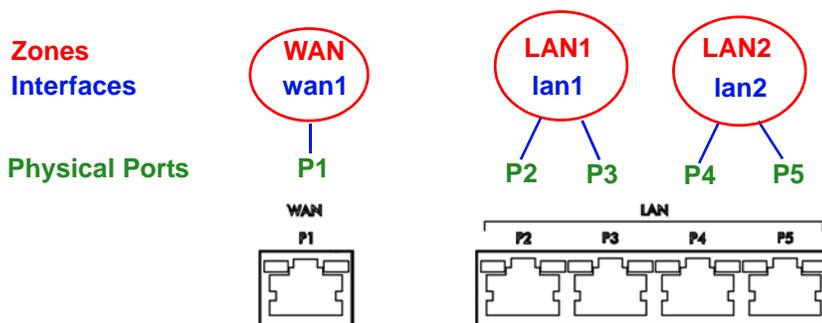
The UAG lets you set up multiple networks for your company. The UAG also provides two separate LAN networks. You can set ports to be part of the LAN1 or LAN2.

1.2 Default Zones, Interfaces, and Ports

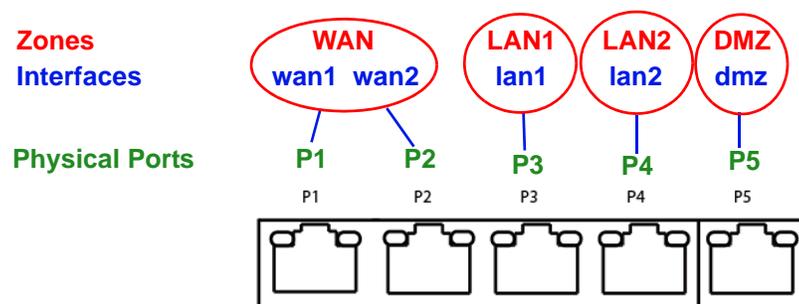
The default configurations for zones, interfaces, and ports are as follows. References to interfaces may be generic rather than the specific name used in your model. For example, this guide may use “the WAN interface” rather than “P1”.

Figure 1 Zones, Interfaces, and Physical Ethernet Ports

UAG2100 / UAG4100



UAG5100



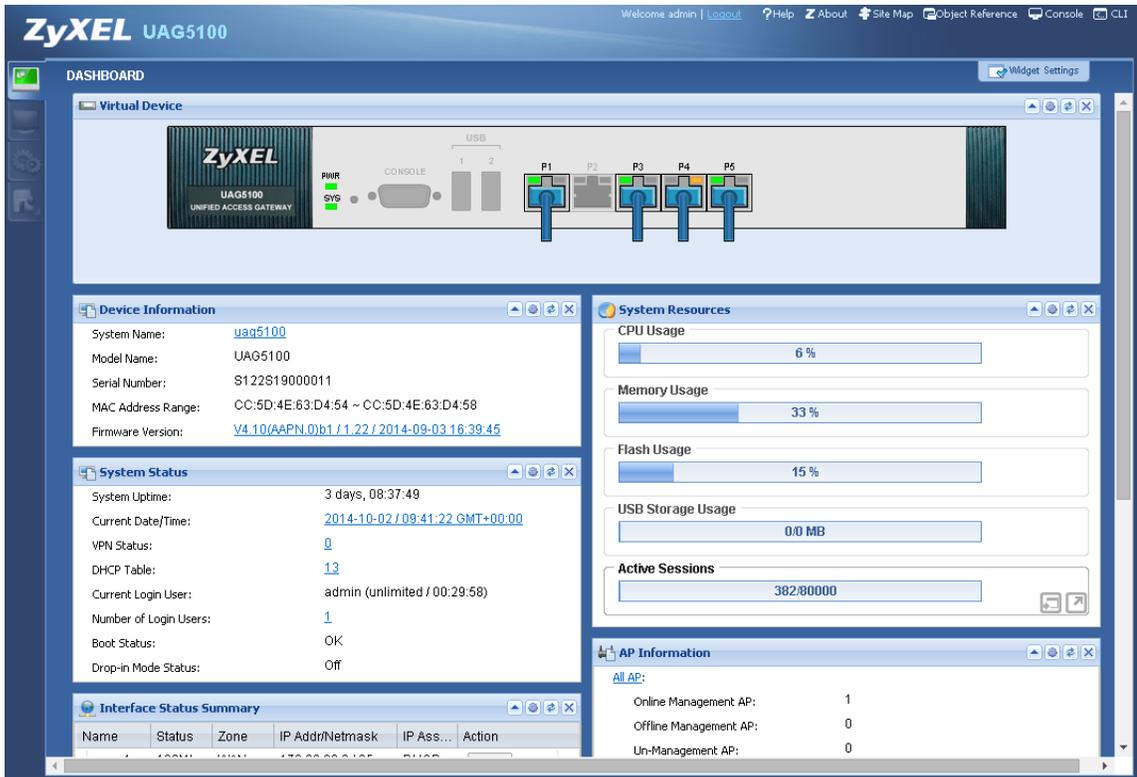
1.3 Management Overview

You can manage the UAG in the following ways.

Web Configurator

The Web Configurator allows easy UAG setup and management using an Internet browser. This User’s Guide provides information about the Web Configurator.

Figure 2 Managing the UAG: Web Configurator



Command-Line Interface (CLI)

The CLI allows you to use text-based commands to configure the UAG. Access it using remote management (for example, SSH or Telnet) or via the physical or Web Configurator console port. See the Command Reference Guide for CLI details. The default settings for the console port are:

Table 2 Console Port Default Settings

SETTING	VALUE
Speed	115200 bps
Data Bits	8
Parity	None
Stop Bit	1
Flow Control	Off

1.4 Web Configurator

In order to use the Web Configurator, you must:

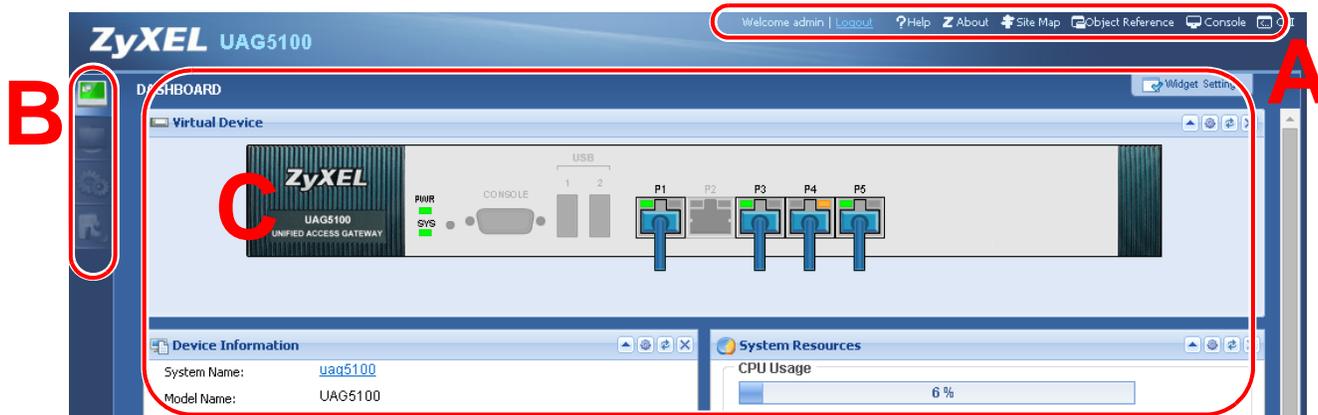
- Use one of the following web browser versions or later: Internet Explorer 6.0, Firefox 8.0, Chrome 14.0, Safari 4.0
- Allow pop-up windows (blocked by default in Windows XP Service Pack 2)
- Enable JavaScripts, Java permissions, and cookies

The recommended screen resolution is 1024 x 768 pixels.

1.4.1 Web Configurator Access

- 1 Make sure your UAG hardware is properly connected. See the Quick Start Guide.
- 2 In your browser go to <http://172.16.0.1> or <http://172.17.0.1>. The **Login** screen appears.

- 3 Type the user name (default: "admin") and password (default: "1234").
- 4 Click **Login**. If you logged in using the default user name and password, the **Update Admin Info** screen appears. Otherwise, the dashboard appears.
- 5 Follow the directions in the **Update Admin Info** screen. If you change the default password, the **Login** screen appears after you click **Apply**. If you click **Ignore**, the **Installation Setup Wizard** opens if the UAG is using its default configuration; otherwise the dashboard appears.



1.4.2 Web Configurator Screens Overview

This guide uses the UAG5100 screens as an example. The screens may vary slightly for different models.

The Web Configurator screen is divided into these parts (as illustrated on [page 23](#)):

- **A** - title bar

- **B** - navigation panel
- **C** - main window

1.4.2.1 Title Bar

Figure 3 Title Bar



The title bar icons in the upper right corner provide the following functions.

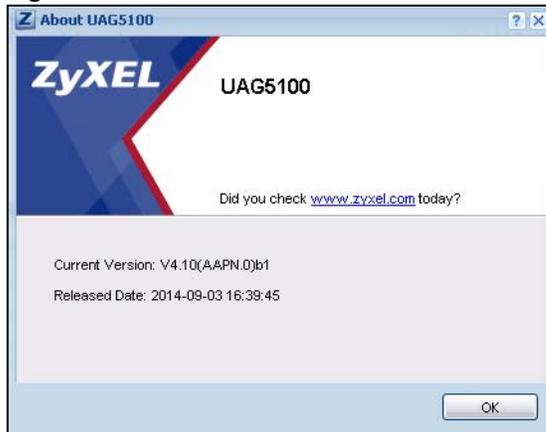
Table 3 Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
Logout	Click this to log out of the Web Configurator.
Help	Click this to open the help page for the current screen.
About	Click this to display basic information about the UAG.
Site Map	Click this to see an overview of links to the Web Configurator screens.
Object Reference	Click this to check which configuration items reference an object.
Console	Click this to open a Java-based console window from which you can run command line interface (CLI) commands. You will be prompted to enter your user name and password. See the Command Reference Guide for information about the commands.
CLI	Click this to open a popup window that displays the CLI commands sent by the Web Configurator to the UAG.

About

Click **About** to display basic information about the UAG.

Figure 4 About



The following table describes labels that can appear in this screen.

Table 4 About

LABEL	DESCRIPTION
Boot Module	This shows the version number of the software that handles the booting process of the UAG.
Current Version	This shows the firmware version of the UAG.
Released Date	This shows the date (yyyy-mm-dd) and time (hh:mm:ss) when the firmware is released.
OK	Click this to close the screen.

Site Map

Click **Site MAP** to see an overview of links to the Web Configurator screens. Click a screen's link to go to that screen.

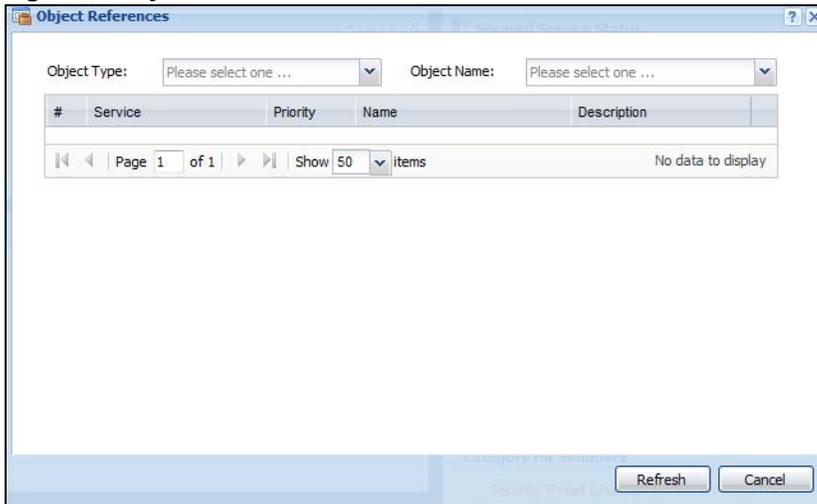
Figure 5 Site Map



Object Reference

Click **Object Reference** to open the **Object Reference** screen. Select the type of object and the individual object and click **Refresh** to show which configuration settings reference the object.

Figure 6 Object Reference



The fields vary with the type of object. The following table describes labels that can appear in this screen.

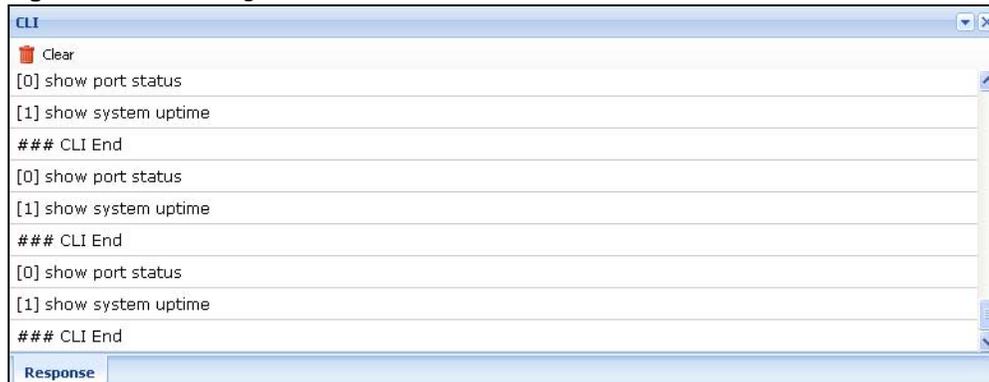
Table 5 Object References

LABEL	DESCRIPTION
Object Name	This identifies the object for which the configuration settings that use it are displayed. Click the object's name to display the object's configuration screen in the main window.
#	This field is a sequential value, and it is not associated with any entry.
Service	This is the type of setting that references the selected object. Click a service's name to display the service's configuration screen in the main window.
Priority	If it is applicable, this field lists the referencing configuration item's position in its list, otherwise N/A displays.
Name	This field identifies the configuration item that references the object.
Description	If the referencing configuration item has a description configured, it displays here.
Refresh	Click this to update the information in this screen.
Cancel	Click Cancel to close the screen.

CLI Messages

Click **CLI** to look at the CLI commands sent by the Web Configurator. Open the pop-up window and then click some menus in the web configurator to display the corresponding commands.

Figure 7 CLI Messages

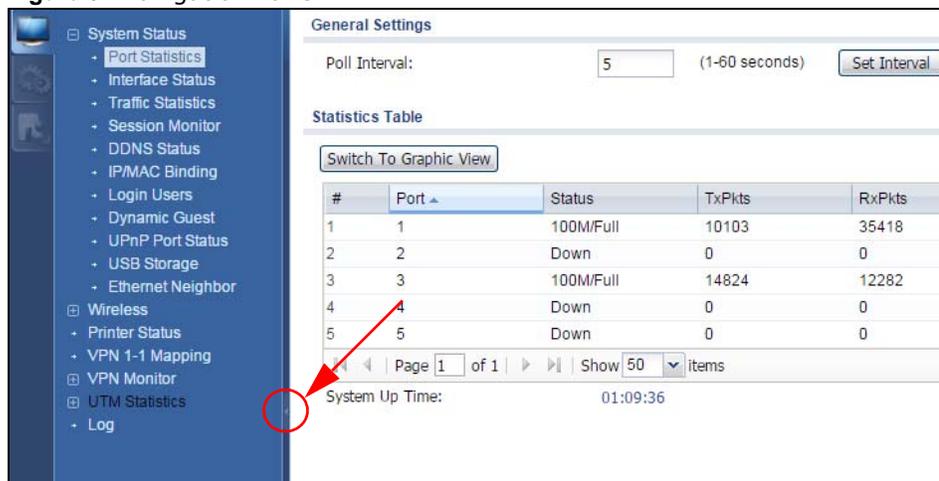


Click **Clear** to remove the currently displayed information.

See the Command Reference Guide for information about the commands.

1.4.3 Navigation Panel

Use the navigation panel menu items to open status and configuration screens. Click the arrow in the middle of the right edge of the navigation panel to hide the panel or drag to resize it. The following sections introduce the UAG's navigation panel menus and their screens.

Figure 8 Navigation Panel

Dashboard

The dashboard displays general device information, system status, system resource usage, licensed service status, and interface status in widgets that you can re-arrange to suit your needs. See [Chapter 6 on page 80](#) for details on the dashboard.

Monitor Menu

The monitor menu screens display status and statistics information.

Table 6 Monitor Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
System Status		
Port Statistics		Display packet statistics for each physical port.
Interface Status		Display general interface information and packet statistics.
Traffic Statistics		Collect and display traffic statistics.
Session Monitor		Display the status of all current sessions.
DDNS Status		Display the status of the UAG's DDNS domain names.
IP/MAC Binding		List the devices that have received an IP address from UAG interfaces using IP/MAC binding.
Login Users		List the users currently logged into the UAG.
Dynamic Guest		List the dynamic guest accounts in the UAG's local database.
UPnP Port Status		List the NAT port mapping rules that UPnP creates on the UAG.
USB Storage		Display details about a USB device connected to the UAG.
Ethernet Neighbor		View and manage the UAG's neighboring devices via Smart Connect (Layer Link Discovery Protocol (LLDP)).
Wireless		
AP Information	AP List	Display information about the connected APs.
	Radio List	Display information about the radios of the connected APs.

Table 6 Monitor Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
Station Info		Display information about the connected stations.
Detected Device		Display information about suspected rogue APs.
Printer Status		
Printer Status		Display information about the connected statement printers.
VPN 1-1 Mapping		
VPN 1-1 Mapping		Display the status of the active users to which the UAG applied a VPN 1-1 mapping rule.
Statistics		Display statistics for each of the VPN 1-1 mapping rules.
VPN Monitor		
IPSec		Display and manage the active IPSec SAs.
UTM Statistics		
App Patrol		Displays application patrol statistics.
Content Filter		Collect and display content filter statistics.
Log		List log entries.
View Log		List log entries for the UAG.
View AP Log		Allow you to query connected APs and view log entries for them.
Dynamic Users Log		Display the UAG's dynamic guest account log messages.

Configuration Menu

Use the configuration menu screens to configure the UAG's features.

Table 7 Configuration Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
Quick Setup		Quickly configure WAN interfaces.
Licensing		
Registration	Registration	Register the device and activate trial services.
	Service	View the licensed service status and upgrade licensed services.
Signature Update	App Patrol	Update application patrol signatures immediately or by a schedule.
Wireless		
Controller	Configuration	Configure how the UAG handles APs that newly connect to the network.
AP Management	Mgmt. AP List	Edit wireless AP information, remove APs, and reboot them.
	AP Policy	Configure the AP controller's IP address on the managed APs and determine the action the managed APs take if the current AP controller fails.
MON Mode	Rogue/Friendly AP List	Configure how the UAG monitors rogue APs.
Load Balancing		Configure load balancing for traffic moving to and from wireless clients.
DCS		Configure dynamic wireless channel selection.

Table 7 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
Auto Healing		Enable auto healing to extend the wireless service coverage area of the managed APs when one of the APs fails.
Network		
Interface	Port Role	Use this screen to set the UAG's flexible ports as LAN1 or LAN2.
	Ethernet	Manage Ethernet interfaces and virtual Ethernet interfaces.
	PPP	Create and manage PPPoE and PPTP interfaces.
	VLAN	Create and manage VLAN interfaces and virtual VLAN interfaces.
	Bridge	Create and manage bridges and virtual bridge interfaces.
	Trunk	Create and manage trunks (groups of interfaces) for load balancing.
Routing	Policy Route	Create and manage routing policies.
	Static Route	Create and manage IP static routing information.
DDNS		Define and manage the UAG's DDNS domain names.
NAT		Set up and manage port forwarding rules.
VPN 1-1 Mapping	General	Enable and configure VPN 1-1 mapping to assign a public IP address to each of users that match the rules.
	Profile	Configure a pool profile which defines the public IP address that the UAG assigns to the matched users and the interface through which the user's traffic is forwarded.
HTTP Redirect		Set up and manage HTTP redirection rules.
SMTP Redirect		Set up and manage SMTP redirection rules.
ALG		Configure FTP pass-through settings.
UPnP		enable UPnP and NAT-PMP on your UAG.
IP/MAC Binding	Summary	Configure IP to MAC address bindings for devices connected to each supported interface.
	Exempt List	Configure ranges of IP addresses to which the UAG does not apply IP/MAC binding.
Layer 2 Isolation	General	Enable layer-2 isolation on the UAG and the internal interface(s).
	White List	Enable and configure the white list.
IPnP		Enable IPnP on the UAG and the internal interface(s).
Web Authentication	Web Authentication	Define rules to force user authentication for network access.
	Walled Garden	Create walled garden links that display in the login screen.
	Advertisement	Enable and set advertisement links.
RTLS	Real Time Location System	Use the managed APs as part of an Ekahau RTLS to track the location of Ekahau Wi-Fi tags.
Security Policy	Policy Control	Create and manage level-3 traffic rules and apply UTM profiles.
	Session Control	Limit the number of concurrent client NAT/security policies sessions.
Billing	General	Configure the general billing settings, such as the accounting method.
	Billing Profile	Configure the billing profiles for the web-based account generator and each button on the connected statement printer.
	Discount	Configure discount price plans.
	Payment Service	Enable online payment service and configure the service pages.

Table 7 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
Printer	General Setting	Configure the printer list, enable printer management and customize the account printout.
	Printer Manager	Detect the connected statement printers, change their IP addresses and/or add them to the managed printer list.
Free Time	Free Time	Allow users to get a free account for Internet surfing during the specified time period.
SMS	SMS	Enable the SMS service to send dynamic guest account information in text messages.
VPN		
IPSec VPN	VPN Connection	Configure IPSec tunnels.
	VPN Gateway	Configure IKE tunnels.
BWM	BWM	Enable and configure bandwidth management rules.
UTM Profile		
App Patrol	Profile	Manage different types of traffic in this screen. Create App Patrol template(s) of settings to apply to a traffic flow using a security policy.
Content Filter	Profile	Create and manage the detailed filtering rules for content filtering profiles and then apply to a traffic flow using a security policy.
	Trusted Web Sites	Create a list of allowed web sites that bypass content filtering policies.
	Forbidden Web Sites	Create a list of web sites to block regardless of content filtering policies.
Object		
Zone		Configure zones used to define various policies.
User/Group	User	Create and manage users.
	Group	Create and manage groups of users.
	Setting	Manage default settings for all users, general settings for user sessions, and rules to force user authentication.
	MAC Address	Configure the MAC addresses of wireless clients for MAC authentication using the local user database.
AP Profile	Radio	Create and manage wireless radio settings files that can be associated with different APs.
	SSID	Create and manage wireless SSID, security, and MAC filtering settings files that can be associated with different APs.
MON Profile		Create and manage rogue AP monitoring files that can be associated with different APs.
Application	Application	Create and manage template(s) of services to apply to policies as an object.
	Application Group	Create and manage groups of applications to apply to policies as a single object.
Address	Address	Create and manage host, range, and network (subnet) addresses.
	Address Group	Create and manage groups of addresses.
Service	Service	Create and manage TCP and UDP services.
	Service Group	Create and manage groups of services.
Schedule	Schedule	Create one-time and recurring schedules.
	Schedule Group	Create and manage groups of schedules.

Table 7 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
AAA Server	RADIUS	Configure the RADIUS settings.
Auth. Method	Authentication Method	Create and manage ways of authenticating users.
Certificate	My Certificates	Create and manage the UAG's certificates.
	Trusted Certificates	Import and manage certificates from trusted sources.
ISP Account	ISP Account	Create and manage ISP account information for PPPoE/PPTP interfaces.
System		
Host Name		Configure the system and domain name for the UAG.
USB Storage	Settings	Configure the settings for the connected USB devices.
Date/Time		Configure the current date, time, and time zone in the UAG.
Console Speed		Set the console speed.
DNS		Configure the DNS server and address records for the UAG.
WWW	Service Control	Configure HTTP, HTTPS, and general authentication.
	Login Page	Configure how the login and access user screens look.
SSH		Configure SSH server and SSH service settings.
TELNET		Configure telnet server settings for the UAG.
FTP		Configure FTP server settings.
SNMP		Configure SNMP communities and services.
Auth. Server		Configure the UAG to act as a RADIUS server.
Language		Select the Web Configurator language.
ZON		Enable or disable ZDP discovery and LLDP discovery on the UAG.
Log & Report		
Email Daily Report		Configure where and how to send daily reports and what reports to send.
Log Settings		Configure the system log, e-mail logs, and remote syslog servers.

Maintenance Menu

Use the maintenance menu screens to manage configuration and firmware files, run diagnostics, and reboot or shut down the UAG.

Table 8 Maintenance Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
File Manager	Configuration File	Manage and upload configuration files for the UAG.
	Firmware Package	View the current firmware version and to upload firmware.
	Shell Script	Manage and run shell script files for the UAG.

Table 8 Maintenance Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
Diagnostics	Diagnostic	Collect diagnostic information.
	Packet Capture	Capture packets for analysis.
	Core Dump	Connect a USB device to the UAG and save a process's core dump to the attached USB storage device if the process terminates abnormally (crashes).
	System Log	Connect a USB device to the UAG and archive the UAG system logs to it here.
	Network Tool	Identify problems with the connections. You can use Ping or TraceRoute to help you identify problems.
	Wireless Frame Capture	Capture wireless frames from APs for analysis.
Packet Flow Explore	Routing Status	Check how the UAG determines where to route a packet.
	SNAT Status	View a clear picture on how the UAG converts a packet's source IP address and check the related settings.
Reboot		Restart the UAG.
Shutdown		Turn off the UAG.

1.4.4 Tables and Lists

Web Configurator tables and lists are flexible with several options for how to display their entries.

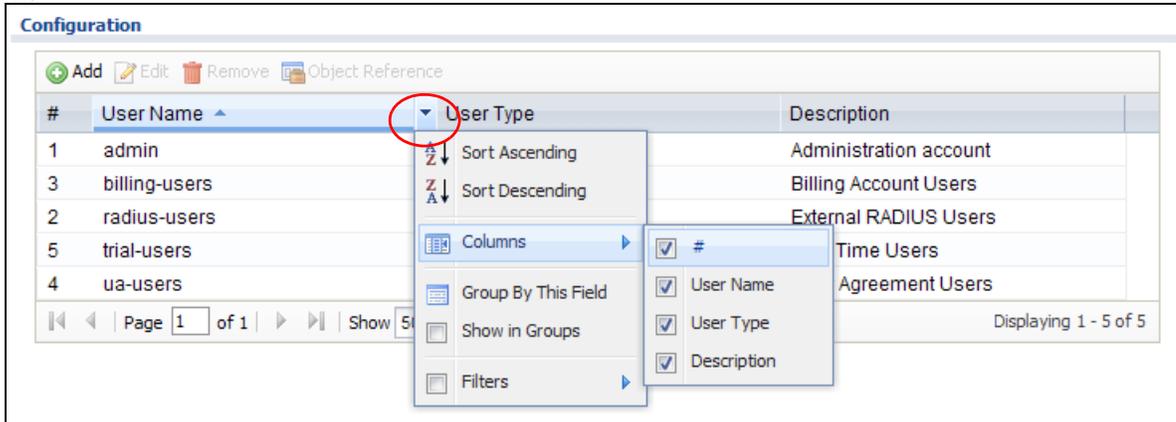
Click a column heading to sort the table's entries according to that column's criteria.

Figure 9 Sorting Table Entries by a Column's Criteria

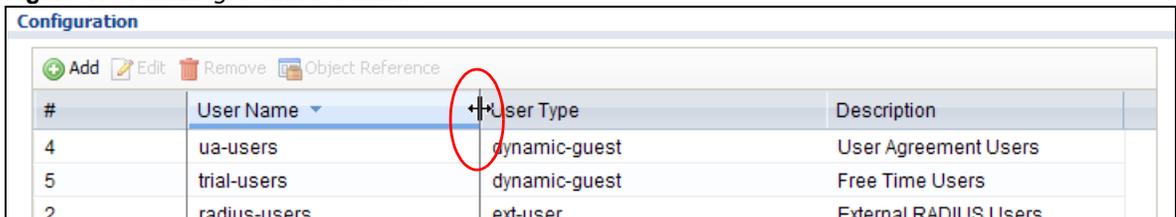
#	User Name	User Type	Description
1	admin	admin	Administration account
3	billing-users	dynamic-guest	Billing Account Users

Click the down arrow next to a column heading for more options about how to display the entries. The options available vary depending on the type of fields in the column. Here are some examples of what you can do:

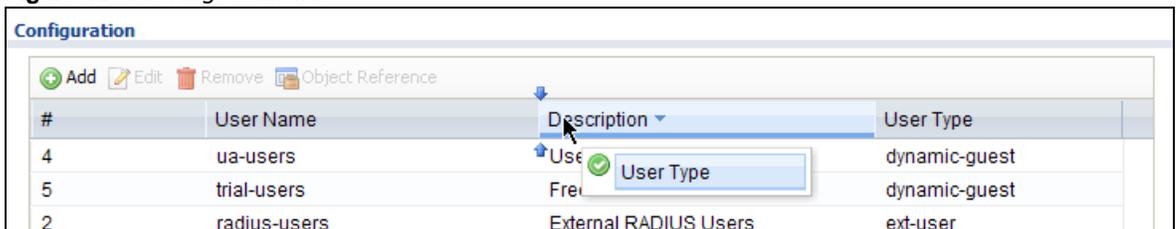
- Sort in ascending or descending (reverse) alphabetical order
- Select which columns to display
- Group entries by field
- Show entries in groups
- Filter by mathematical operators (<, >, or =) or searching for text

Figure 10 Common Table Column Options

Select a column heading cell's right border and drag to re-size the column.

Figure 11 Resizing a Table Column

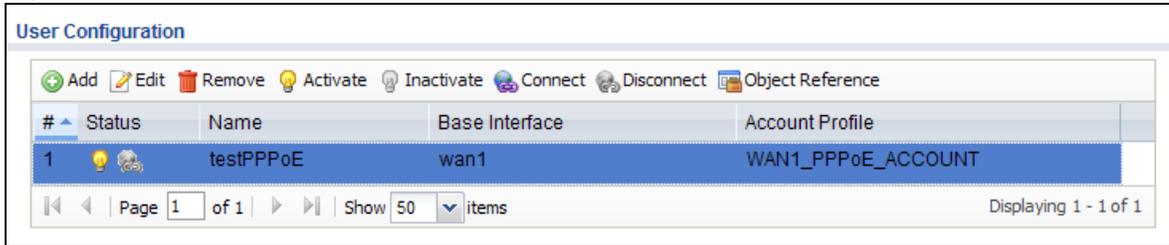
Select a column heading and drag and drop it to change the column order. A green check mark displays next to the column's title when you drag the column to a valid new location.

Figure 12 Moving Columns

Use the icons and fields at the bottom of the table to navigate to different pages of entries and control how many entries display at a time.

Figure 13 Navigating Pages of Table Entries

The tables have icons for working with table entries. You can often use the [Shift] or [Ctrl] key to select multiple entries to remove, activate, or deactivate.

Figure 14 Common Table Icons

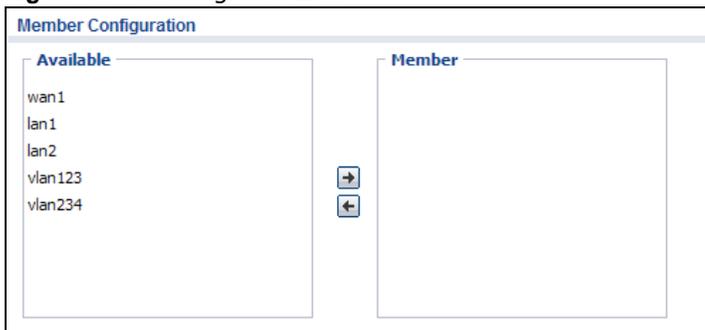
Here are descriptions for the most common table icons.

Table 9 Common Table Icons

LABEL	DESCRIPTION
Add	Click this to create a new entry. For features where the entry's position in the numbered list is important (features where the UAG applies the table's entries in order like security policy for example), you can select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings. In some tables you can just click a table entry and edit it directly in the table. For those types of tables small red triangles display for table entries with changes that you have not yet applied.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
Connect	To connect an entry, select it and click Connect .
Disconnect	To disconnect an entry, select it and click Disconnect .
Object Reference	Select an entry and click Object Reference to check which settings use the entry.
Move	To change an entry's position in a numbered list, select it and click Move to display a field to type a number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed. For example, if you type 6, the entry you are moving becomes number 6 and the previous entry 6 (if there is one) gets pushed up (or down) one.

Working with Lists

When a list of available entries displays next to a list of selected entries, you can often just double-click an entry to move it from one list to the other. In some lists you can also use the [Shift] or [Ctrl] key to select multiple entries, and then use the arrow button to move them to the other list.

Figure 15 Working with Lists

1.5 Stopping the UAG

Always use **Maintenance > Shutdown > Shutdown** or the `shutdown` command before you turn off the UAG or remove the power. Not doing so can cause the firmware to become corrupt.

Hardware Installation and Connection

2.1 Rack-mounting (UAG5100)

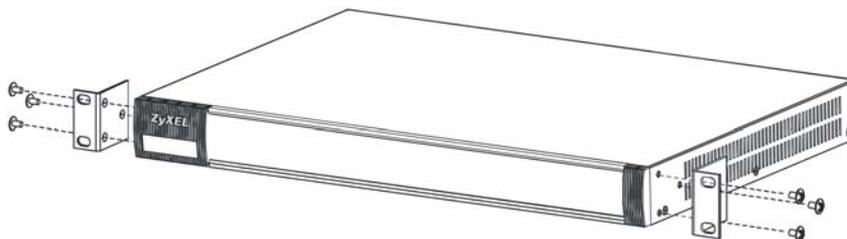
Use the following steps to mount the UAG on an EIA standard size, 19-inch rack or in a wiring closet with other equipment using a rack-mounting kit. Make sure the rack will safely support the combined weight of all the equipment it contains and that the position of the UAG does not make the rack unstable or top-heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

Note: Leave 10 cm of clearance at the sides and 20 cm in the rear.

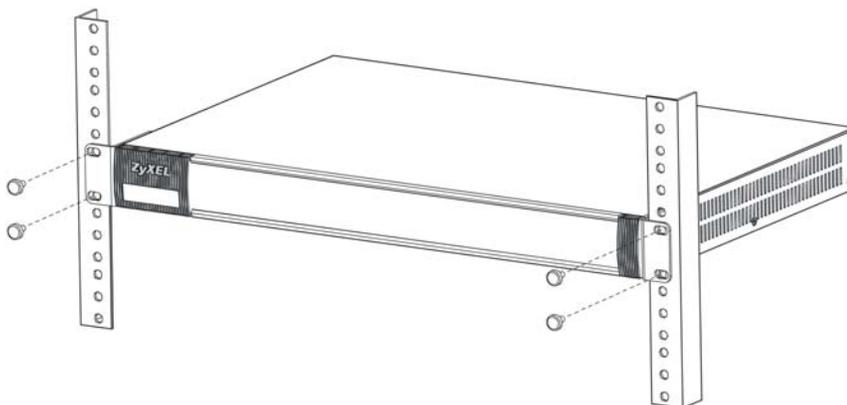
Use a #2 Phillips screwdriver to install the screws.

Note: Failure to use the proper screws may damage the unit.

- 1 Align one bracket with the holes on one side of the UAG and secure it with the included bracket screws (smaller than the rack-mounting screws).
- 2 Attach the other bracket in a similar fashion.



- 3 After attaching both mounting brackets, position the UAG in the rack and up the bracket holes with the rack holes. Secure the UAG to the rack with the rack-mounting screws.



2.2 Wall Mounting (UAG2100 and UAG4100)

You may need screw anchors if mounting on a concrete or brick wall.

Table 10 Wall Mounting Information

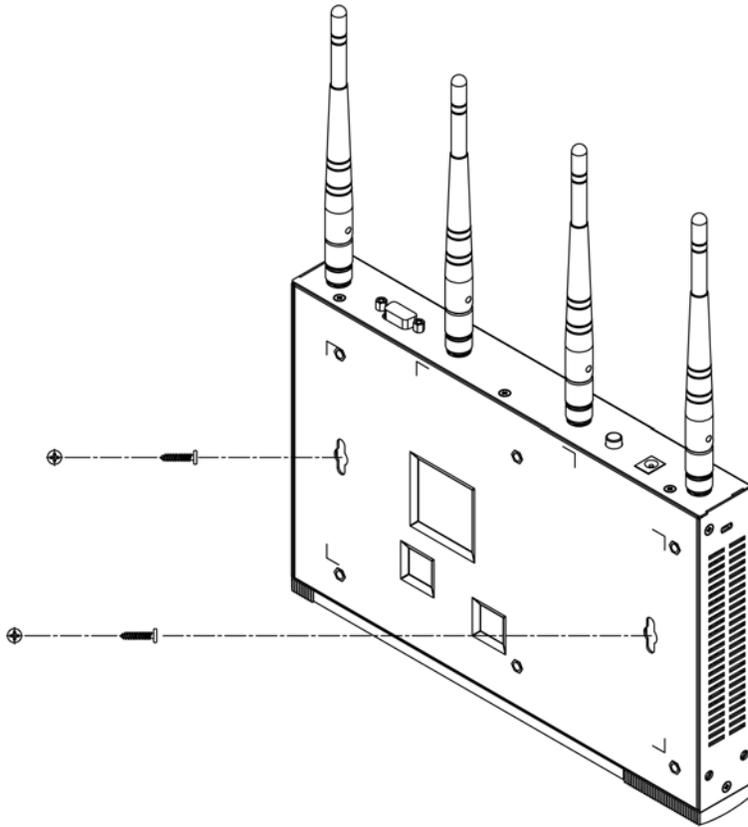
Distance between holes	206 mm
Self-tapping screws (Diameter: 3 mm)	Two
Screw anchors (optional)	Two

- 1 Select a position free of obstructions on a wall strong enough to hold the weight of the device.
- 2 Mark two holes on the wall at the appropriate distance apart for the screws.

Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

- 3 If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do not insert the screws all the way in - leave a small gap of about 0.5 cm.
If not using screw anchors, use a screwdriver to insert the screws into the wall. Do not insert the screws all the way in - leave a gap of about 0.5 cm.
- 4 Make sure the screws are fastened well enough to hold the weight of the UAG with the connection cables.
- 5 Align the holes on the back of the UAG with the screws on the wall. Hang the UAG on the screws.

Figure 16 Wall Mounting Example



2.3 Front Panel

This section introduces the UAG's front panel.

Figure 17 Front Panel: UAG2100 or UAG4100

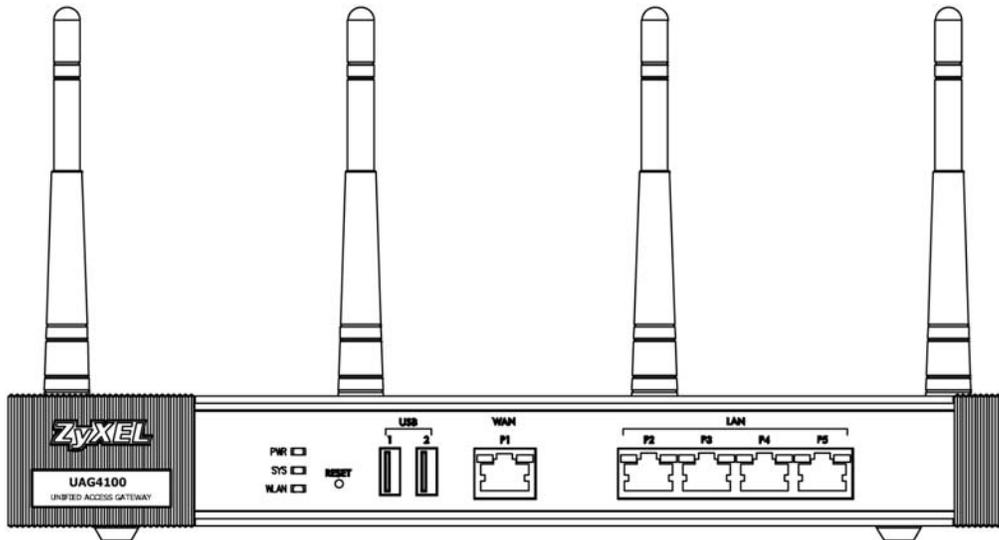
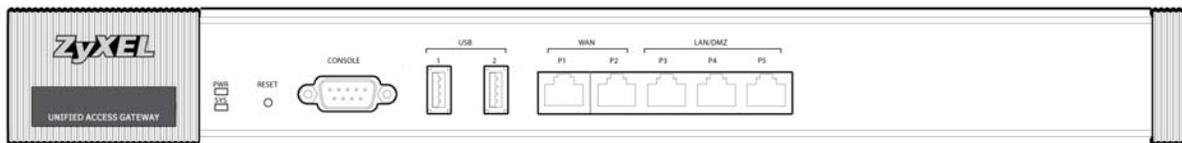


Figure 18 Front Panel: UAG5100

1000Base-T Ports

The 1000Base-T auto-negotiating, auto-crossover Ethernet ports support 10/100/1000 Mbps Gigabit Ethernet so the speed can be 100 Mbps or 1000 Mbps. The duplex mode is full at 1000 Mbps and half or full at 10/100 Mbps. An auto-negotiating port can detect and adjust to the optimum Ethernet speed (10/100/1000 Mbps) and duplex mode (full duplex or half duplex) of the connected device. An auto-crossover (auto-MDI/MDI-X) port automatically works with a straight-through or crossover Ethernet cable. The factory default negotiation settings for the Ethernet ports on the UAG are speed: auto, duplex: auto, and flow control: on (you cannot configure the flow control setting, but the UAG can negotiate with the peer and turn it off if needed).

USB 2.0 Ports

Connect a USB storage device to a USB port on the UAG to archive the UAG system logs or save the UAG operating system kernel to it.

Console Port (UAG5100)

Connect this port to your computer (using an RS-232 cable) if you want to configure the UAG using the command line interface (CLI) via the console port.

For local management, you can use a computer with terminal emulation software configured to the following parameters:

- VT100 terminal emulation
- 115200 bps
- No parity, 8 data bits, 1 stop bit
- No flow control

Connect the male 9-pin end of the RS-232 console cable to the console port of the UAG. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

2.3.1 Front Panel LEDs

The following tables describe the LEDs.

Table 11 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR		Off	The UAG is turned off.
	Green	On	The UAG is turned on.
	Red	On	There is a hardware component failure. Shut down the device, wait for a few minutes and then restart the device (see Section 1.5 on page 35). If the LED turns red again, then please contact your vendor.

Table 11 Front Panel LEDs (continued)

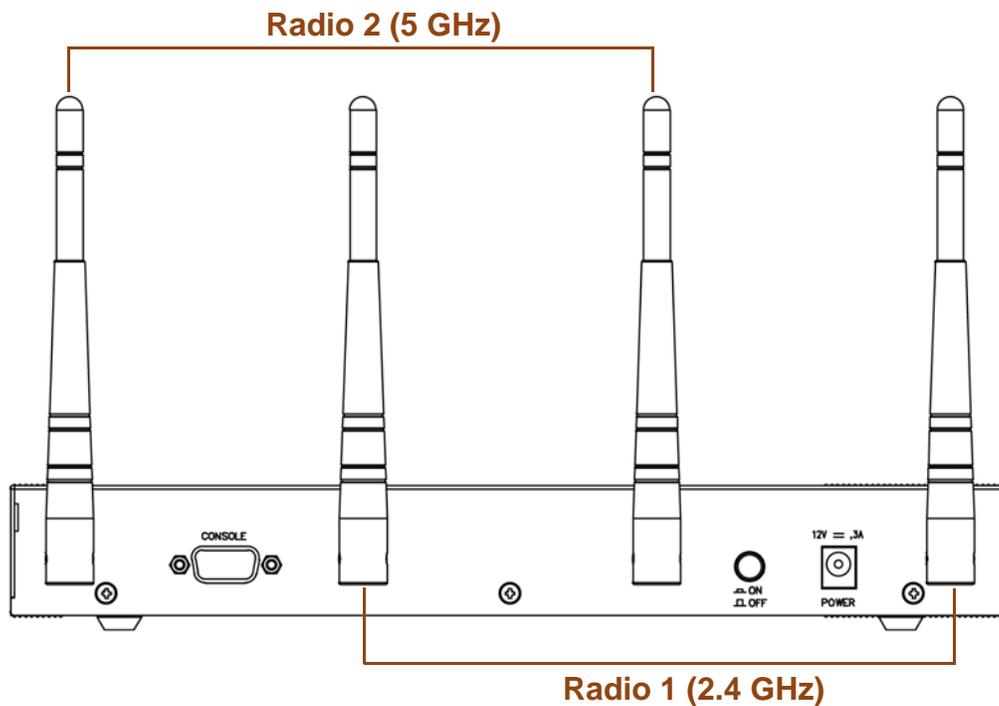
LED	COLOR	STATUS	DESCRIPTION
SYS	Green	Off	The UAG is not ready or has failed.
		On	The UAG is ready and running.
		Blinking	The UAG is booting.
	Red	On	The UAG had an error or has failed.
WLAN (UAG2100 or UAG4100)	Green	On	The wireless network is activated.
		Blinking	The UAG is communicating with other wireless clients.
		Off	The wireless network is not activated.
P1~P5	Green	On	This port has a successful link to a 10/100 Mbps Ethernet network
		Blinking	The UAG is sending or receiving packets to/from a 10/100 Mbps Ethernet network on this port
	Orange	On	This port has a successful link to a 1000 Mbps Ethernet network.
		Blinking	The UAG is sending or receiving packets to/from a 1000 Mbps Ethernet network on this port
		Off	There is no connection on this port.

2.4 Rear Panel

The following figure shows the rear panel of the UAG.

2.4.1 UAG2100 or UAG4100

The rear panel contains a console port, a power switch and a connector for the power receptacle and four antennas.

Figure 19 Rear Panel: UAG2100 or UAG4100

Console Port

Connect this port to your computer (using an RS-232 cable) if you want to configure the UAG using the command line interface (CLI) via the console port.

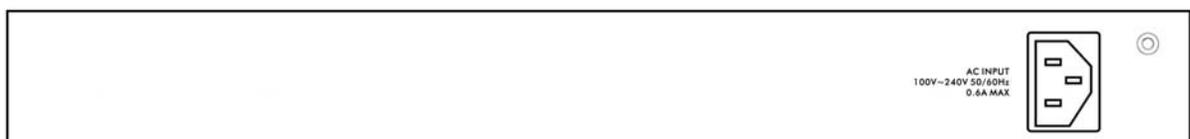
For local management, you can use a computer with terminal emulation software configured to the following parameters:

- VT100 terminal emulation
- 115200 bps
- No parity, 8 data bits, 1 stop bit
- No flow control

Connect the male 9-pin end of the RS-232 console cable to the console port of the UAG. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

2.4.2 UAG5100

The following figure shows the rear panel of the UAG. The rear panel contains a connector for the power receptacle.

Figure 20 Rear Panel: UAG5100

Printer Deployment

3.1 Overview

This chapter shows you how to set up an external statement printer (SP350E for example) and deploy it in your network with the UAG.

In the following examples, you will:

- [Attach the Printer to the UAG.](#)
- [Set up an Internet Connection on the UAG.](#)
- [Allow the UAG to Monitor and Manage the Printer.](#)
- [Turn on Web Authentication on the UAG.](#)
- [Generate a Free Guest Account.](#)

3.2 Attach the Printer to the UAG

This section uses the SP350E as an example. Refer to the printer documentation for detailed information about paper loading.

- 1 Connect the Ethernet port of the printer to one LAN port of the UAG.
- 2 Connect the power socket of the printer to a power outlet. Turn on the printer.

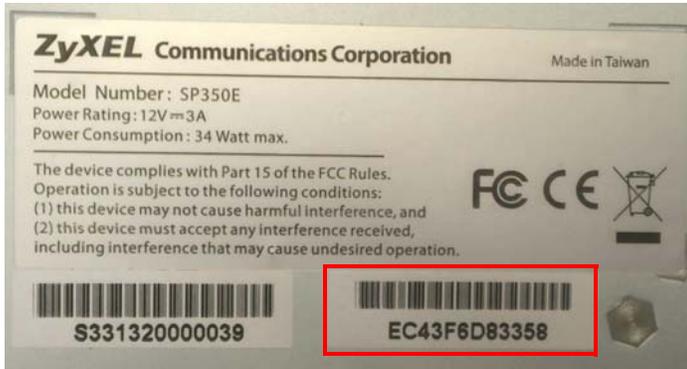
The printer is acting as a DHCP client by default and will obtain an IP address from the connected UAG. Make sure the UAG is turned on already and the DHCP server is enabled on its LAN interface(s).

3.3 Set up an Internet Connection on the UAG

- 1 Connect the WAN port of the UAG to a broadband modem or router.
- 2 Connect your computer to one of the available LAN ports on the UAG.
- 3 Log into the UAG web configurator. See [Section 1.4 on page 22](#) on how to access the web configurator.
- 4 Enter your Internet access information to set up an Internet connection. See [Chapter 4 on page 50](#) for detailed information on how to use the setup wizard.

3.4 Allow the UAG to Monitor and Manage the Printer

Before you add the printer to the UAG's printer list, check the sticker on the printer's rear panel to see its MAC address.



- 1 Go to the **Dashboard** of the UAG web configurator.

#	Status	Name	Version	Expiration	Count
1	Not Licensed	APP Patrol	v3.1.4.0...	N/A	0
2	Not Licensed	Content Filter		N/A	0
3	Default	Managed AP ...		N/A	16
4	Default	Extension User		N/A	500

- 2 Open the **DHCP Table** to find the IP address which is assigned to the printer's MAC address. Make sure the IP address is reserved for the printer. Write down the printer's IP address.

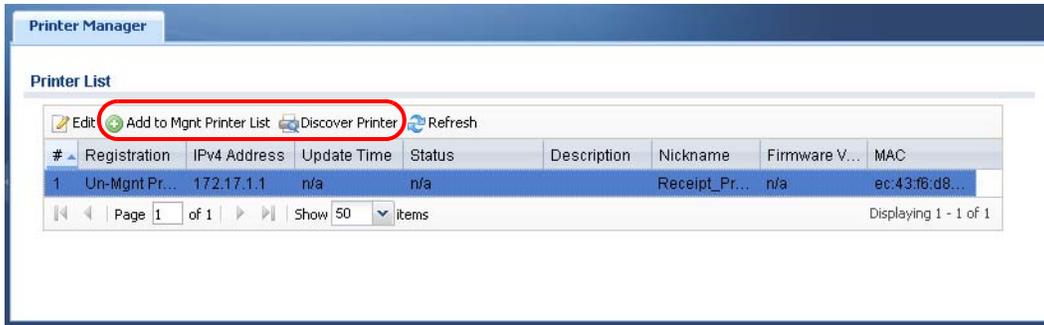
DHCP Table						
#	Interface	IP Address	Host Name	MAC Address	Description	Reserve
3	dmz	172.18.1.1	"nwa5123-nl"	b0:b2:dc:6f:0e:47		<input type="checkbox"/>
2	lan1	172.16.1.1	"twpc"	00:21:85:0c:44:4b		<input type="checkbox"/>
1	lan2	172.17.1.1	none	ec:43:f6:d8:33:55		<input type="checkbox"/>

Refresh Interval: Refresh Now

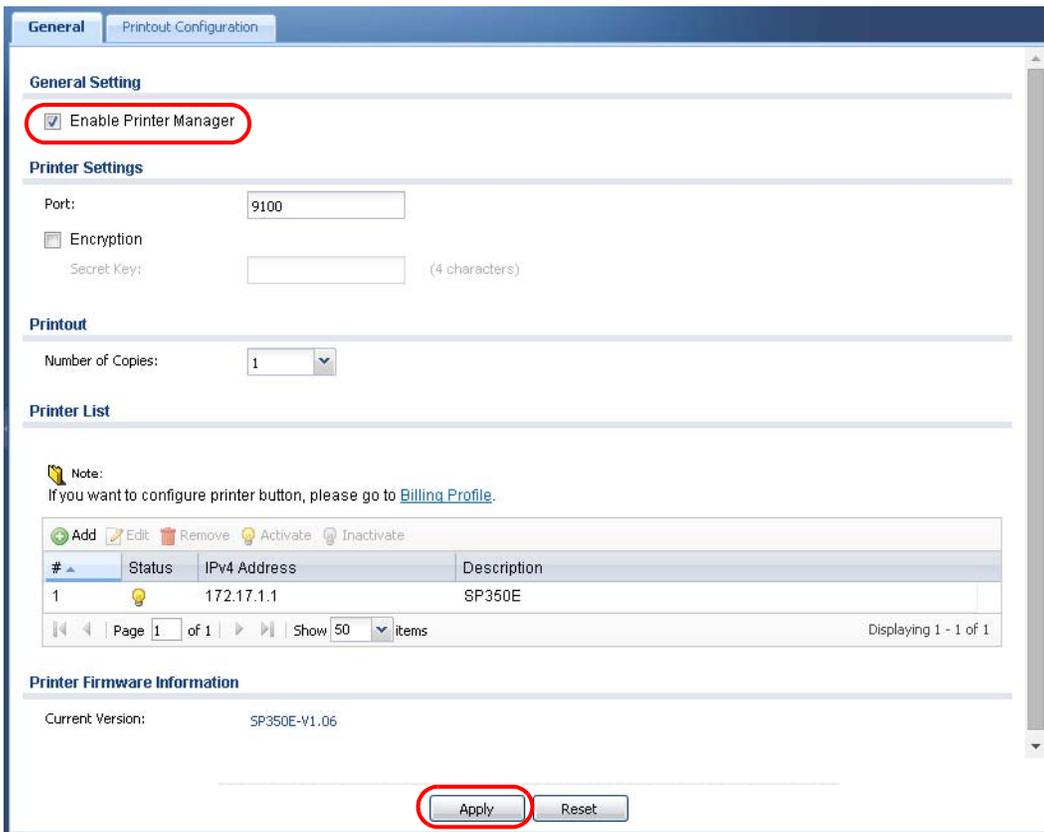
- Go to the **Configuration > Printer > General Setting** screen. Click **Add** in the **Printer List** to create a new entry for your printer.

The screenshot shows the 'General Setting' configuration page for a printer. An 'Add Rule' dialog box is overlaid on the page. In the dialog, the 'Enable Printer Manager' checkbox is checked. The 'IPv4 Address' field contains '172.17.1.1' and the 'Description' field contains 'SP350E'. The 'Add' button in the 'Printer List' section of the background page is circled in red.

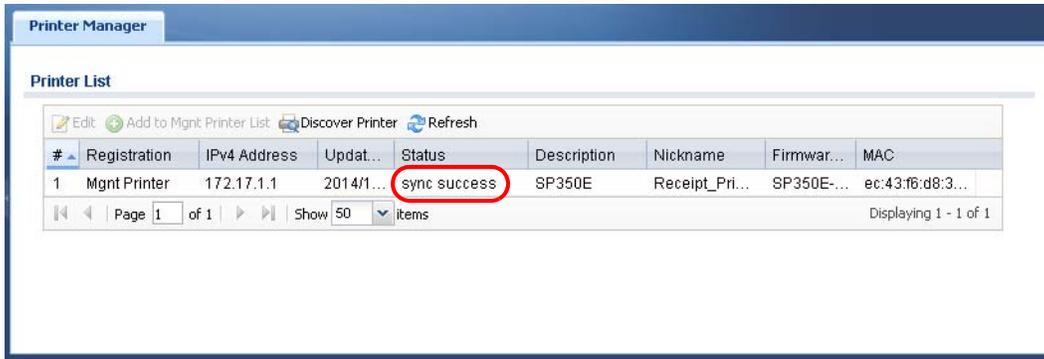
Alternatively, go to the **Configuration > Printer > Printer Manager** screen and click the **Discover Printer** icon. The UAG automatically detects the connected printer(s) and displays the printer information in the list. Select your printer and click **Add to Mgnt Printer List** to let the UAG manage it.



- 4 After the printer's IP address is added to the printer list, select the **Enable Printer Manager** checkbox in the **Configuration > Printer > General Setting** screen and then click **Apply**.



- 5 Go to the **Configuration > Printer > Printer Manager** screen to check if the UAG can connect to the printer (the printer status is **sync success**).

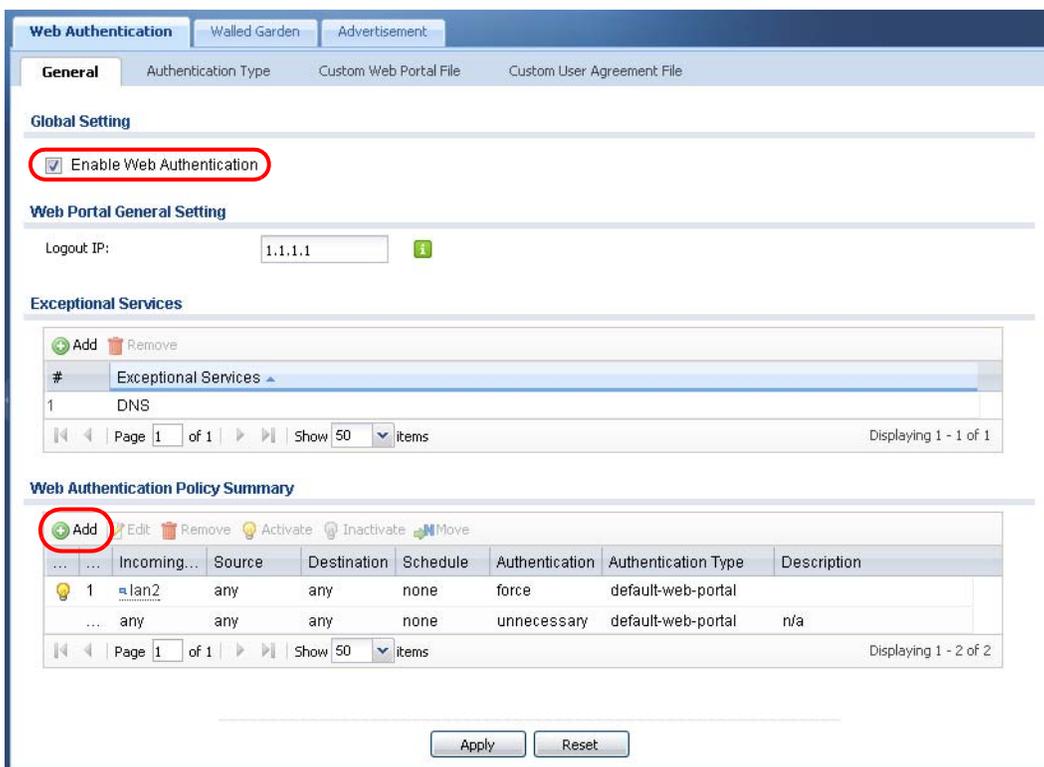


Note: You may need to wait up to 90 seconds for the UAG to synchronize with the printer successfully after you click **Apply** in the the **Configuration > Printer > General Setting** screen.

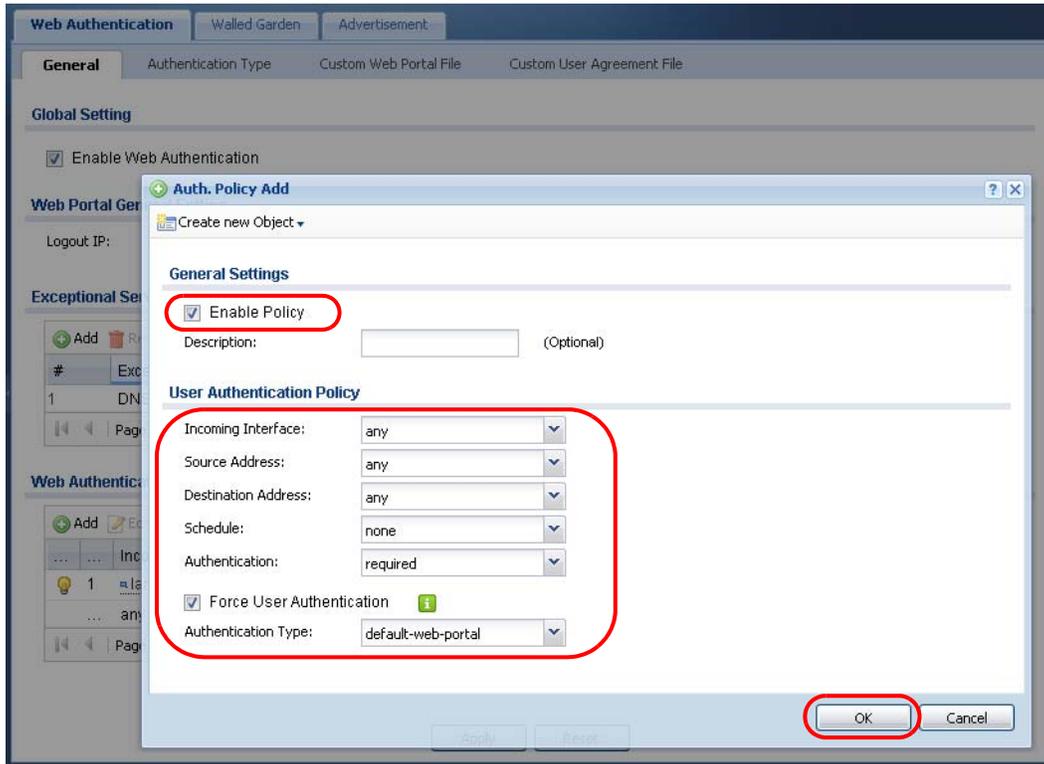
3.5 Turn on Web Authentication on the UAG

With web authentication, users need to log in through a designated web page or agree to the policy of user agreement before they can access the network(s).

- 1 Go to the **Configuration > Web Authentication > General** screen. Select **Enable Web Authentication** to turn on this feature.
- 2 Click **Add** to create a new web authentication policy.



- 3 The **Auth. Policy Add** screen displays. Set **Authentication** to **required** and select **Force User Authentication** to redirect all HTTP traffic to the default login page.
- 4 Select **default-web-portal** from the **Authentication Type** drop-down list box to allow users to authenticate through the default web portal login page.
- 5 Click **OK** to save your changes.



- 6 Click **Apply** in the **Configuration > Web Authentication** screen.

3.6 Generate a Free Guest Account

You can use the buttons on the printer or web-based account generator to create guest accounts based on the pre-defined billing settings (see [Section 26.3 on page 307](#)).

- 1 Go to the **Configuration > Free Time** screen.
- 2 Select the **Enable Free Time** option to turn on this feature. Click **Apply**.

Free Time

General Settings

Enable Free Time

Free Time Period: 30 minute

Reset Time: Daily

Time: 00:00

Maximum Registration Number Before Reset Time: 1 (1-5)

Delivery Method: On-Screen

Note:
If you want to configure ssid profile settings of the account, keep user logged in, please go to [Billing](#).

Apply Reset

3 Whenever a user tries to access a web page, he/she will be redirected to the default login page.

4 Click the link on the login page to get a free guest account.

Enter User Name/Password and click to login.

User Name:

Password:

(max. 63 alphanumeric, printable characters and no spaces)

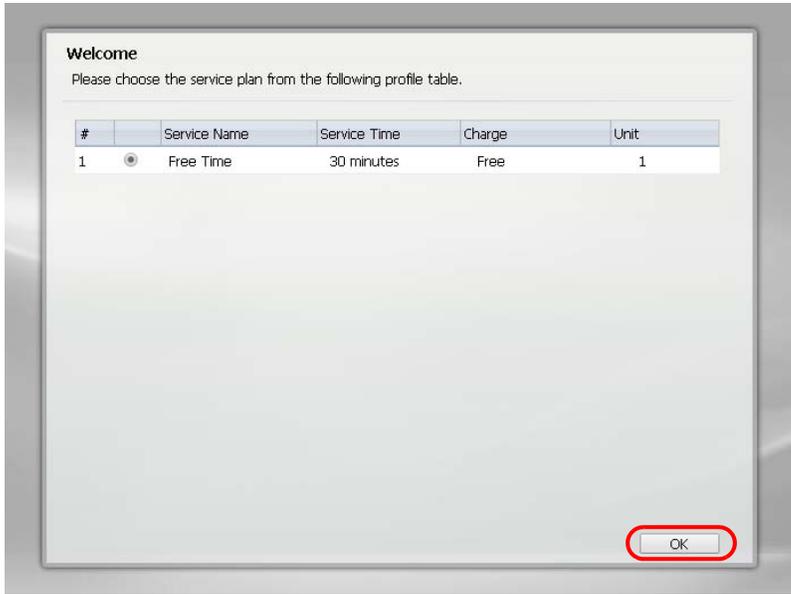
[Without an account? Click here to get a free account.](#)

Login Reset

Note:

1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
4. Allow Gears if you are using Google Chrome.

5 A Welcome screen displays. Select the free time service. Click **OK** to generate and show the account information on the web page.



- 6 Now you can use this account to access the Internet through the UAG for free.

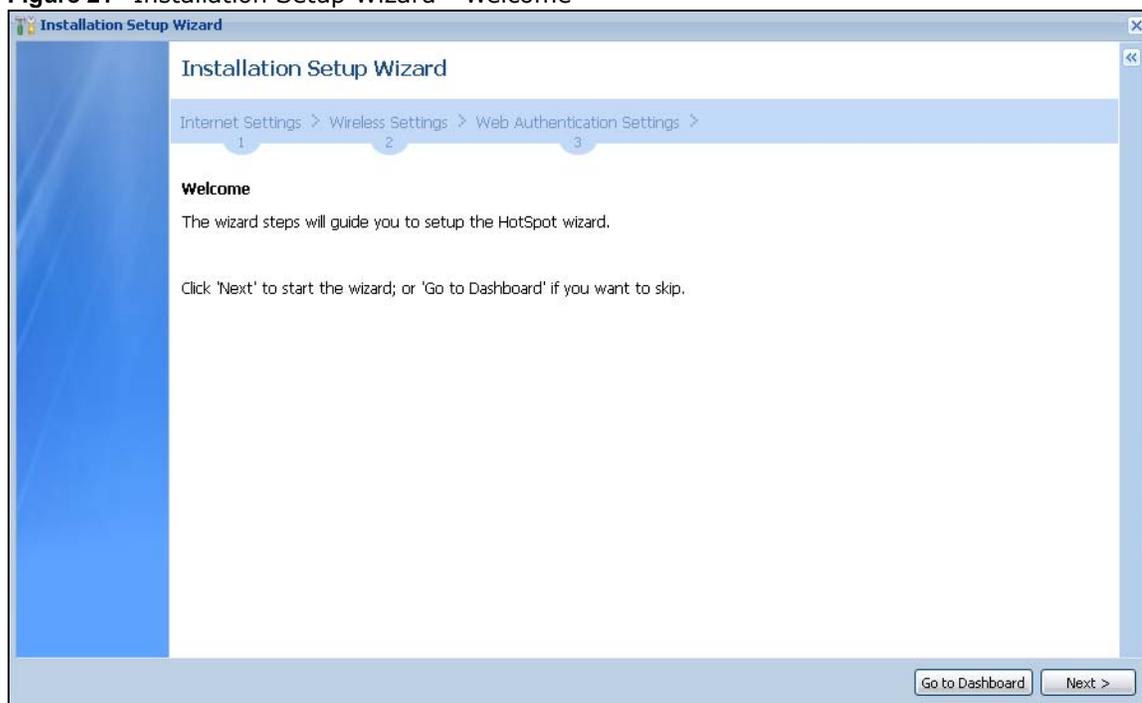


Installation Setup Wizard

4.1 Welcome Screen

When you log into the Web Configurator for the first time or when you reset the UAG to its default configuration, the **Installation Setup Wizard** screen displays. This wizard helps you configure Internet connection settings, wireless security and web authentication settings. This chapter provides information on configuring the Web Configurator's installation setup wizard. See the feature-specific chapters in this User's Guide for background information.

Figure 21 Installation Setup Wizard - Welcome



- Click the double arrow in the upper right corner to display or hide the help.
- Click **Go to Dashboard** to skip the installation setup wizard or click **Next** to start configuring for Internet access.

4.2 Internet Settings

Use this screen to set the WAN interface's type of encapsulation and method of IP address assignment.

Refer to information provided by your ISP to know what to enter in each field. Leave a field blank if you don't have that information.

Note: Enter the Internet access information exactly as your ISP gave it to you.

Figure 22 Internet Access: Step 1 (UAG2100/UAG4100)

The screenshot shows the 'Installation Setup Wizard' window for UAG2100/UAG4100. The title bar reads 'Installation Setup Wizard'. The breadcrumb trail is 'Internet Settings > Wireless Settings > Web Authentication Settings >'. Below the breadcrumb, there are three numbered steps: 1, 2, and 3. Step 1 is highlighted. The main content area is titled 'Internet Access - First WAN Interface'. Under 'ISP Parameters', the 'Encapsulation' dropdown is set to 'Ethernet'. Under 'WAN IP Address Assignments', the 'First WAN Interface' is 'wan1', the 'Zone' is 'WAN', and the 'IP Address Assignment' dropdown is set to 'Auto'. At the bottom right, there are '< Back' and 'Next >' buttons.

Figure 23 Internet Access: Step 1 (UAG5100)

The screenshot shows the 'Installation Setup Wizard' window for UAG5100. The title bar reads 'Installation Setup Wizard'. The breadcrumb trail is 'Internet Settings > Wireless Settings > Web Authentication Settings >'. Below the breadcrumb, there are three numbered steps: 1, 2, and 3. Step 1 is highlighted. The main content area is titled 'Internet Access - First WAN Interface'. Under 'ISP Setting', there is a checkbox labeled 'I have two ISPs' which is unchecked. Under 'ISP Parameters', the 'Encapsulation' dropdown is set to 'Ethernet'. Under 'WAN IP Address Assignments', the 'First WAN Interface' is 'wan1', the 'Zone' dropdown is set to 'WAN', and the 'IP Address Assignment' dropdown is set to 'Auto'. At the bottom right, there are '< Back' and 'Next >' buttons.

- **I have two ISPs:** (Only for the UAG that has multiple WAN interfaces.) Select this option to configure two Internet connections. Leave it cleared to configure just one. This option appears when you are configuring the first WAN interface.
- **Encapsulation:** Choose the **Ethernet** option when the WAN port is used as a regular Ethernet. Otherwise, choose **PPP Over Ethernet** (PPPoE) or **PPTP** for a dial-up connection according to the information from your ISP.
- **First WAN Interface:** This is the interface you are configuring for Internet access.
- **Zone:** Select the security zone to which this interface and Internet connection belong.
- **IP Address Assignment:** Select **Auto** if your ISP did not assign you a fixed IP address. Select **Static** if the ISP assigned a fixed IP address.

4.2.1 Internet Settings: Ethernet

This screen is read-only if you set the previous screen's **IP Address Assignment** field to **Auto** and click **Next**. Use this screen to configure your IP address settings.

Note: Enter the Internet access information exactly as given to you by your ISP.

Figure 24 Internet Access: Ethernet Encapsulation

The screenshot shows the 'Internet Settings' configuration page for 'First WAN Interface'. The breadcrumb trail is 'Internet Settings > Wireless Settings > Web Authentication Settings >'. The page is divided into three numbered sections: 1. Internet Access - First WAN Interface, 2. ISP Parameters, and 3. WAN IP Address Assignments. Under 'ISP Parameters', 'Encapsulation' is set to 'Ethernet'. Under 'WAN IP Address Assignments', 'First WAN Interface' is 'wan1' and 'Zone' is 'WAN'. The 'IP Address' field contains '0.0.0.0', 'IP Subnet Mask' contains '255.255.255.0', and 'Gateway IP Address' contains '0.0.0.0'. Each of these three fields has a red dashed border and a red error icon to its right. The 'First DNS Server' and 'Second DNS Server' fields are empty. At the bottom right, there are '< Back' and 'Next >' buttons.

- **Encapsulation:** This displays the type of Internet connection you are configuring.
- **First WAN Interface:** This is the number of the interface that will connect with your ISP.
- **Zone:** This is the security zone to which this interface and Internet connection will belong.
- **IP Address:** Enter your (static) public IP address. **Auto** displays if you selected **Auto** as the **IP Address Assignment** in the previous screen.

The following fields display if you selected static IP address assignment.

- **IP Subnet Mask:** Enter the subnet mask for this WAN connection's IP address.
- **Gateway IP Address:** Enter the IP address of the router through which this WAN connection will send traffic (the default gateway).

- **First / Second DNS Server:** These fields display if you selected static IP address assignment. The Domain Name System (DNS) maps a domain name to an IP address and vice versa. Enter a DNS server's IP address(es). The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The UAG uses these (in the order you specify here) to resolve domain names for DDNS and the time server. Leave the field as 0.0.0.0 if you do not want to configure DNS servers.

4.2.2 Internet Settings: PPPoE

Note: Enter the Internet access information exactly as given to you by your ISP.

Figure 25 Internet Access: PPPoE Encapsulation

The screenshot shows the 'Internet Settings' configuration page for PPPoE Encapsulation. The page is titled 'Internet Settings' and shows the 'Internet Access - First WAN Interface' configuration. Under 'ISP Parameters', the Encapsulation is set to PPPoE, Authentication Type is Chap/PAP, and Idle timeout is 100 seconds. The User Name, Password, and Retype to Confirm fields are empty and have red error icons. Under 'WAN IP Address Assignments', the First WAN Interface is wan1_ppp, Zone is WAN, and IP Address is 0.0.0.0. The First DNS Server field is empty and has a red error icon. The Second DNS Server field is empty. Navigation buttons for '< Back' and 'Next >' are at the bottom right.

ISP Parameters

- Type the PPPoE **Service Name** from your service provider. PPPoE uses a service name to identify and reach the PPPoE server. You can use alphanumeric and `-_@$./` characters, and it can be up to 64 characters long.
- **Authentication Type** - Select an authentication protocol for outgoing connection requests. Options are:
 - **CHAP/PAP** - Your UAG accepts either CHAP or PAP when requested by the remote node.
 - **CHAP** - Your UAG accepts CHAP only.
 - **PAP** - Your UAG accepts PAP only.
 - **MSCHAP** - Your UAG accepts MSCHAP only.
 - **MSCHAP-V2** - Your UAG accepts MSCHAP-V2 only.
- Type the **User Name** given to you by your ISP. You can use alphanumeric and `-_@$./` characters, and it can be up to 31 characters long.
- Type the **Password** associated with the user name. Use up to 64 ASCII characters except the `[]` and `?`. This field can be blank.

- Select **Nailed-Up** if you do not want the connection to time out. Otherwise, type the **Idle Timeout** in seconds that elapses before the router automatically disconnects from the PPPoE server.

WAN IP Address Assignments

- **First WAN Interface:** This is the name of the interface that will connect with your ISP.
- **Zone:** This is the security zone to which this interface and Internet connection will belong.
- **IP Address:** Enter your (static) public IP address. **Auto** displays if you selected **Auto** as the **IP Address Assignment** in the previous screen.
- **First / Second DNS Server:** These fields display if you selected static IP address assignment. The Domain Name System (DNS) maps a domain name to an IP address and vice versa. Enter a DNS server's IP address(es). The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The UAG uses these (in the order you specify here) to resolve domain names for DDNS and the time server. Leave the field as 0.0.0.0 if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.

4.2.3 Internet Settings: PPTP

Note: Enter the Internet access information exactly as given to you by your ISP.

Figure 26 Internet Access: PPTP Encapsulation

Internet Settings > Wireless Settings > Web Authentication Settings >

1 2 3

Internet Access - First WAN Interface

ISP Parameters

Encapsulation: PPTP

Authentication Type: Chap/PAP

User Name :

Password:

Retype to Confirm:

Nailed-Up

Idle timeout: Seconds

PPTP Configuration

Base Interface: wan1

Base IP Address:

IP Subnet Mask:

Gateway IP Address: (Optional)

Server IP: IP Address

Connection ID: (Optional)

WAN IP Address Assignments

First WAN Interface: wan1_ppp

Zone: WAN

IP Address:

First DNS Server:

Second DNS Server:

< Back Next >

ISP Parameters

- **Authentication Type** - Select an authentication protocol for outgoing calls. Options are:
 - **CHAP/PAP** - Your UAG accepts either CHAP or PAP when requested by the remote node.
 - **CHAP** - Your UAG accepts CHAP only.
 - **PAP** - Your UAG accepts PAP only.
 - **MSCHAP** - Your UAG accepts MSCHAP only.
 - **MSCHAP-V2** - Your UAG accepts MSCHAP-V2 only.
- Type the **User Name** given to you by your ISP. You can use alphanumeric and -_@\$. / characters, and it can be up to 31 characters long.
- Type the **Password** associated with the user name. Use up to 64 ASCII characters except the [] and ?. This field can be blank. Re-type your password in the next field to confirm it.
- Select **Nailed-Up** if you do not want the connection to time out. Otherwise, type the **Idle Timeout** in seconds that elapses before the router automatically disconnects from the PPTP server.

PPTP Configuration

- **Base Interface**: This identifies the Ethernet interface you configure to connect with a modem or router.
- Type a **Base IP Address** (static) assigned to you by your ISP.
- Type the **IP Subnet Mask** assigned to you by your ISP (if given).
- **Gateway IP Address**: Enter the IP address of the gateway if any.
- **Server IP**: Type the IP address of the PPTP server.
- Type a **Connection ID** or connection name. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your broadband modem or router. You can use alphanumeric and -_ : characters, and it can be up to 31 characters long.

WAN IP Address Assignments

- **First WAN Interface**: This is the connection type on the interface you are configuring to connect with your ISP.
- **Zone** This is the security zone to which this interface and Internet connection will belong.
- **IP Address**: Enter your (static) public IP address. **Auto** displays if you selected **Auto** as the **IP Address Assignment** in the previous screen.
- **First / Second DNS Server**: These fields display if you selected static IP address assignment. The Domain Name System (DNS) maps a domain name to an IP address and vice versa. Enter a DNS server's IP address(es). The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The UAG uses these (in the order you specify here) to resolve domain names for DDNS and the time server. Leave the field as 0.0.0.0 if you do not want to configure DNS servers.

4.2.4 Internet Settings - Second WAN Interface

If the UAG has multiple WAN interfaces and you selected **I have two ISPs**, after you configure the **First WAN Interface**, you can configure the **Second WAN Interface**. The screens for configuring the second WAN interface are similar to the first (see [Section 4.2 on page 50](#)).

4.3 Wireless Settings

Use this screen to turn on the controller feature and allow the UAG to manage the connected APs.

Figure 27 Wireless Settings

4.3.1 Wireless and Radio Settings

Use this screen to configure the wireless and wireless security settings when you turn on the local AP.

The screen varies depending on the security mode you selected.

Figure 28 Wireless Settings: Security Mode: WPA2

Wireless Settings

- **SSID** - Enter a descriptive name of up to 32 printable characters for the wireless LAN.
- **Security Mode** - Select **wep**, **wpa2** or **wpa2-mix** to add security on this wireless network. Otherwise, select **none** to allow any wireless client to associate this network without authentication.
- **Key Length and Key** - If you set **Security Mode** to **wep**, select the bit-length of the WEP key and configure the WEP key used to encrypt data.
 - **WEP-64**: Enter 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x11AA22BB33) for each Key used.
or
Enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for each Key used.
 - **WEP-128**: Enter 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x00112233445566778899AABBCC) for each Key used.
or
Enter 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for each Key used.
- **Pre-shared Key** - If you set **Security Mode** to **wpa2** or **wpa2-mix**, enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
- Select the **Hidden SSID** option if you want to hide the SSID in the outgoing beacon frame. A wireless client then cannot obtain the SSID through scanning using a site survey tool.
- Select the **Enable Intra-BSS Traffic Blocking** option if you want to prevent crossover traffic from within the same SSID. Wireless clients can still access the wired network but cannot communicate with each other.

Radio Settings

- **Enable 802.11 2.4G/5G Band** - Select the option to activate the 2.4GHz or 5GHz wireless LAN.
- When using the 2.4 GHz band, select **b/g** in the **Mode** field to let IEEE 802.11b and IEEE 802.11g compliant wireless devices associate with the AP. Otherwise, select **b/g/n** to let IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n compliant wireless devices associate with the AP.
When using the 5 GHz band, select **a** in the **Mode** field to let only IEEE 802.11a compliant wireless devices associate with the AP. Otherwise, select **a/n** to let IEEE 802.11a and IEEE 802.11n compliant wireless devices associate with the AP.
- Select a **Channel** which the UAG local AP will use in the 2.4GHz or 5GHz wireless LAN. The options vary depending on the frequency band and the country you are in. Some 5 GHz channels include the label **indoor use only**. These are for use with an indoor AP only. Do not use them with an outdoor AP.

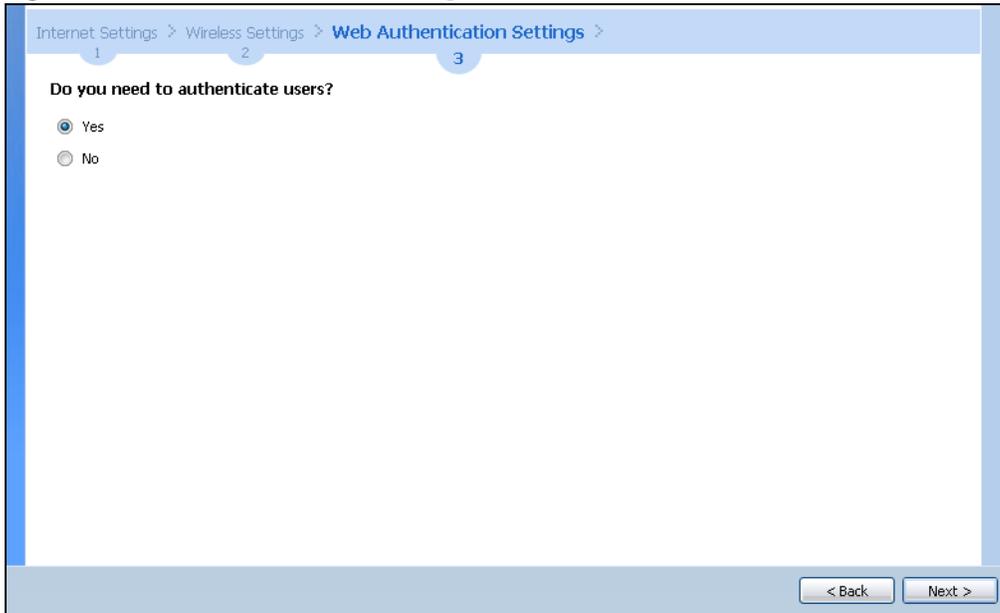
4.4 Web Authentication Settings

Use this screen to turn on the web authentication feature to block LAN2 traffic until a client authenticates with the UAG through the default login page. Otherwise, select **No** and click **Next** to disable web authentication and go to the **Device Registration** screen.

Note: A **View Mobile Version** or **View Desktop Version** link displays on the login page if you enable web authentication.

To block all network traffic or traffic received on a specific interface, use the **Configuration > Web Authentication** screens (Section 23.2 on page 260) to configure a new policy.

Figure 29 Web Authentication Settings

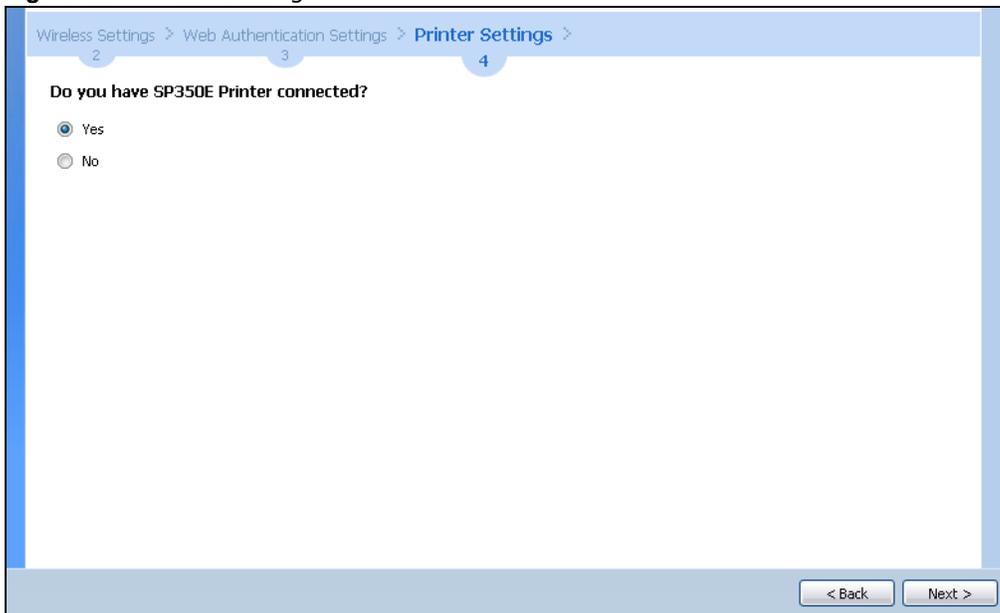


The screenshot shows the 'Web Authentication Settings' screen in the installation wizard. The breadcrumb trail at the top reads: 'Internet Settings > Wireless Settings > Web Authentication Settings >'. Below the breadcrumb, the question 'Do you need to authenticate users?' is displayed. There are two radio button options: 'Yes' (which is selected) and 'No'. At the bottom right of the screen, there are two buttons: '< Back' and 'Next >'. The screen is framed by a light blue border.

4.5 Printer Settings

If you enable the web authentication feature, attach a statement printer and select **Yes** to have the UAG generate dynamic guest accounts. Otherwise, select **No** and click **Next** to go to the **Free Time** screen with which you can allow the UAG to create free guest accounts.

Figure 30 Printer Settings



The screenshot shows the 'Printer Settings' screen in the installation wizard. The breadcrumb trail at the top reads: 'Wireless Settings > Web Authentication Settings > Printer Settings >'. Below the breadcrumb, the question 'Do you have SP350E Printer connected?' is displayed. There are two radio button options: 'Yes' (which is selected) and 'No'. At the bottom right of the screen, there are two buttons: '< Back' and 'Next >'. The screen is framed by a light blue border.

4.5.1 Printer List and Printout Settings

Use this screen to view information about the connected statement printer, such as SP350E.

Figure 31 Printer List and Printout Settings

Wireless Settings > Web Authentication Settings > **Printer Settings** >

Printer Settings

Printer List

Please click "Discover Printer" button to search your printer.

#	Add to Mgmt Printer List	IPv4 Address	MAC

Printout

Number of Copies:

< Back Next >

Printer List

- If there is a statement printer attached to the UAG, click **Discover Printer** to detect the printer that is connected to the UAG and display the printer information.
- **Add to Mgmt Printer List** - Select this to add the printer to the managed printer list.
- **IPv4 Address** - This shows the IP address of the printer.
- **MAC** - This shows the MAC address of the printer.

Printout

- Specify how many copies of subscriber statements you want to print.

4.6 Billing Settings

Use this screen to configure the general billing settings.

Figure 32 Billing Settings

Web Authentication Settings > Printer Settings > **Billing Settings** >

Billing Settings

Accounting Method

Time to Finish

Accumulation

User idle timeout: (1-60 minutes)

Currency

Currency symbol

Currency code

Decimal symbol:

Tax %

< Back Next >

Accounting Method

- Select **Time to Finish** to allow each user a one-time login. Once the user logs in, the system starts counting down the pre-defined usage even if the user stops the Internet access before the time period is finished. If a user disconnects and reconnects before the allocated time expires, the user does not have to enter the user name and password to access the Internet again.
- Select **Accumulation** to allow each user multiple re-login until the time allocated is used up. The UAG accounts the time that the user is logged in for Internet access.

Specify the **User idle timeout** between 1 and 60 minutes. The UAG automatically disconnects a computer from the network after a period of inactivity. The user may need to enter the username and password again before access to the network is allowed.

Currency

- Select the appropriate currency symbol or currency unit. If you set **Currency code** to **User-Define**, enter a three-letter alphabetic code manually.
- **Decimal symbol** - Select whether you would like to use a dot (.) or a comma (,) for the decimal point.
- **Tax** - Select this option to charge sales tax for the account. Enter the tax rate (a 6% sales tax is entered as 6).

4.6.1 Billing Profile

Use this screen to configure the billing profiles that defines the maximum Internet access time and charge per time unit.

Figure 33 Billing Profile

Profile Name	Time Period	Unit	Price
billing_30mins	30	minute	0
billing_1hour	1	hour	0
billing_1day	1	day	0

- **Profile Name** - Enter a name for the billing profile. You can use up to 31 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). Spaces are not allowed. The first character must be a letter.
- **Time Period** - Set the duration of the billing period. When this period expires, the user's access will be stopped.
- **Price** - Set each profile's price, up to 999999.99, per time unit.

4.6.2 Account Generator Settings

Use this screen to select the pre-defined billing profiles that the UAG can use to automatically create dynamic guest accounts. Each button represents a billing profile that defines maximum Internet access time and charge per time unit.

Figure 34 Account Generator Settings

4.7 Free Time Settings

Use this screen to configure the free time settings.

Figure 35 Free Time Settings

- **Free Time Period** - Select the duration of time period for which the free time account is allowed to access the Internet.
- **Reset Time** - Select the time in 24-hour format at which the new free time account is allowed to access the Internet.

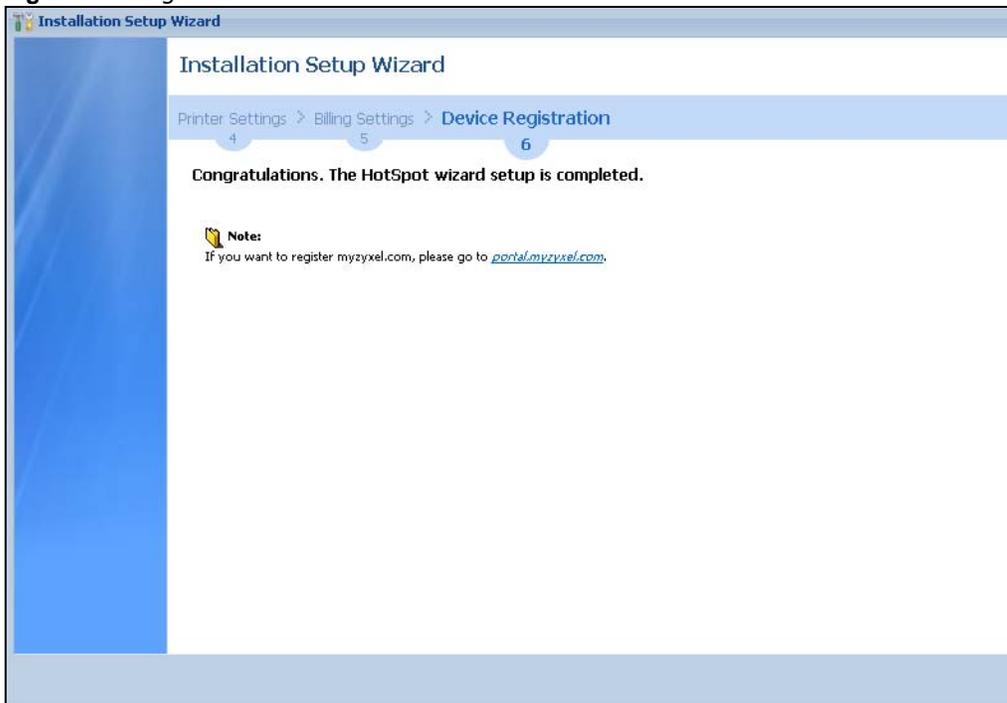
- **Maximum Registration Number Before Reset Time** - Enter the maximum number of the users that are allowed to log in for Internet access with a free guest account before the time specified in the **Reset Time** field. For example, if you set the **Maximum Registration Number Before Reset Time** to 1 and the **Reset Time** to 13:00, even the first free guest account has expired at 11:30, the second account still cannot access the Internet until 13:00.

4.8 Device Registration

Go to <http://portal.myZyXEL.com> with the UAG's serial number and LAN MAC address to register it if you have not already done so.

Note: You must be connected to the Internet to register. Use the **Registration > Service** screen to update your service subscription status.

Figure 36 Registration



Quick Setup Wizards

5.1 Quick Setup Overview

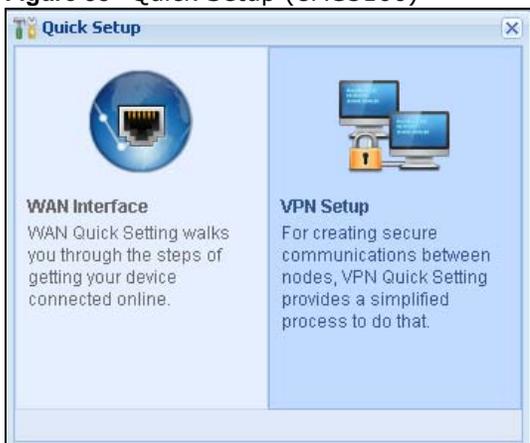
The Web Configurator's quick setup wizards help you configure Internet and VPN connection settings. This chapter provides information on configuring the quick setup screens in the Web Configurator. See the feature-specific chapters in this User's Guide for background information.

In the Web Configurator, click **Configuration > Quick Setup** to open the first **Quick Setup** screen.

Figure 37 Quick Setup (UAG2100/UAG4100)



Figure 38 Quick Setup (UAG5100)



- **WAN Interface**

Click this link to open a wizard to set up a WAN (Internet) connection. This wizard creates matching ISP account settings in the UAG if you use PPPoE or PPTP. See [Section 5.2 on page 65](#).

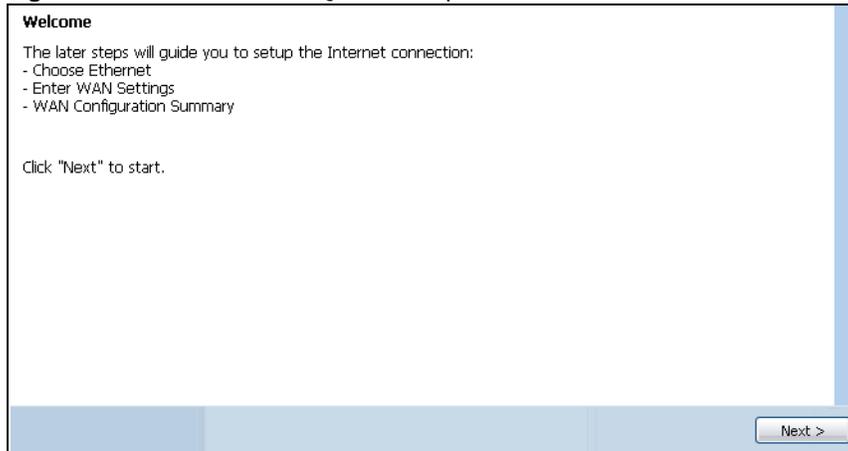
- **VPN Setup**

Use **VPN Setup** to configure a VPN (Virtual Private Network) rule for a secure connection to another computer or network. See [Section 5.3 on page 70](#).

5.2 WAN Interface Quick Setup

Click **WAN Interface** in the main **Quick Setup** screen to open the **WAN Interface Quick Setup Wizard Welcome** screen. Use these screens to configure an interface to connect to the Internet. Click **Next**.

Figure 39 WAN Interface Quick Setup Wizard



5.2.1 Choose an Ethernet Interface

Select the Ethernet interface that you want to configure for a WAN connection and click **Next**.

Figure 40 Choose an Ethernet Interface



5.2.2 Select WAN Type

WAN Type Selection: Select the type of encapsulation this connection is to use. Choose **Ethernet** when the WAN port is used as a regular Ethernet.

Otherwise, choose **PPPoE** or **PPTP** for a dial-up connection according to the information from your ISP.

Figure 41 WAN Interface Setup: Step 2

The screens vary depending on what encapsulation type you use. Refer to information provided by your ISP to know what to enter in each field. Leave a field blank if you don't have that information.

Note: Enter the Internet access information exactly as your ISP gave it to you.

5.2.3 Configure WAN IP Settings

Use this screen to select whether the interface should use a fixed or dynamic IP address.

Figure 42 WAN Interface Setup: Step 2

- **WAN Interface:** This is the interface you are configuring for Internet access.
- **Zone:** This is the security zone to which this interface and Internet connection belong.
- **IP Address Assignment:** Select **Auto** if your ISP did not assign you a fixed IP address. Select **Static** if you have a fixed IP address.

5.2.4 ISP and WAN Connection Settings

Use this screen to configure the ISP and WAN interface settings. This screen is read-only if you select **Ethernet** and set the **IP Address Assignment** to **Auto**. If you set the **IP Address**

Assignment to Static and/or select **PPTP** or **PPPoE**, enter the Internet access information exactly as your ISP gave it to you.

Figure 43 WAN and ISP Connection Settings: (PPTP Shown)

The screenshot shows a configuration window with the following sections and fields:

- ISP Parameters:**
 - Encapsulation: PPTP
 - Authentication Type: Chap/PAP (dropdown)
 - User Name: [Redacted]
 - Password: [Redacted]
 - Retype to Confirm: [Redacted]
 - Nailed-Up
 - Idle timeout: 100 Seconds
- PPTP Configuration:**
 - Base Interface: wan1
 - Base IP Address: 0.0.0.0
 - IP Subnet Mask: 255.255.255.0
 - Gateway IP Address: [Optional]
 - Server IP: 0.0.0.0
 - Connection ID: [Optional]
- IP Address Assignment:**
 - WAN Interface: wan1_ppp
 - Zone: WAN
 - IP Address: 0.0.0.0
 - Gateway IP Address: [Optional]
 - First DNS Server: [Optional]
 - Second DNS Server: [Optional]

At the bottom right, there are buttons for '< Back' and 'Next >'.

The following table describes the labels in this screen.

Table 12 WAN and ISP Connection Settings

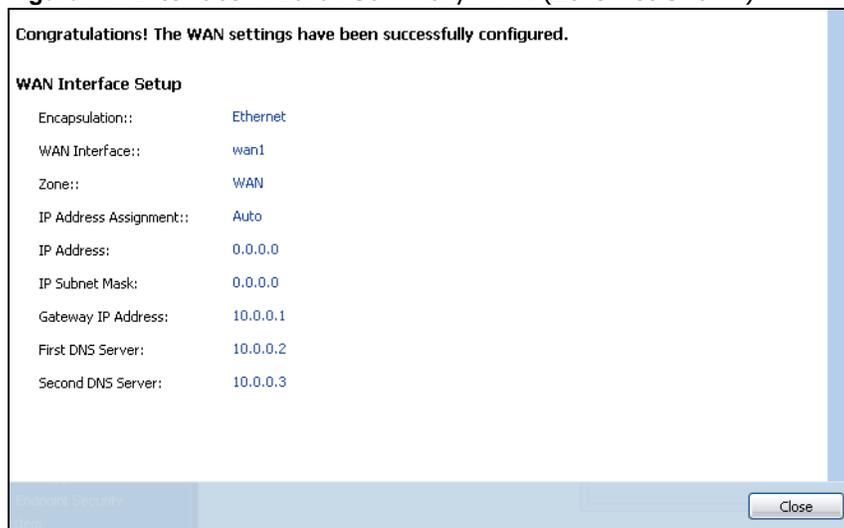
LABEL	DESCRIPTION
ISP Parameter	This section appears if the interface uses a PPPoE or PPTP Internet connection.
Encapsulation	This displays the type of Internet connection you are configuring.
Service Name	Enter the PPPoE service name specified in the ISP account. This field is not available if the ISP account uses PPTP.
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: CHAP/PAP - Your UAG accepts either CHAP or PAP when requested by this remote node. CHAP - Your UAG accepts CHAP only. PAP - Your UAG accepts PAP only. MSCHAP - Your UAG accepts MSCHAP only. MSCHAP-V2 - Your UAG accepts MSCHAP-V2 only.
User Name	Type the user name given to you by your ISP. You can use alphanumeric and -_@\$. / characters, and it can be up to 31 characters long.

Table 12 WAN and ISP Connection Settings (continued)

LABEL	DESCRIPTION
Password	Type the password associated with the user name above. Use up to 64 ASCII characters except the [] and ?. This field can be blank.
Retype to Confirm	Type your password again for confirmation.
Nailed-Up	Select Nailed-Up if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. 0 means no timeout.
PPTP Configuration	This section only appears if the interface uses a PPPoE or PPTP Internet connection.
Base Interface	This displays the identity of the Ethernet interface you configure to connect with a modem or router.
Base IP Address	Type the (static) IP address assigned to you by your ISP.
IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Gateway IP Address	This field only displays for an interface with a static IP address. Enter the IP address of the gateway device.
Server IP	Type the IP address of the PPTP server.
Connection ID	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your DSL modem. You can use alphanumeric and -_ : characters, and it can be up to 31 characters long.
IP Address Assignment	
WAN Interface	This displays the identity of the interface you configure to connect with your ISP.
Zone	This field displays to which security zone this interface and Internet connection will belong.
IP Address	This field is read-only when the WAN interface uses a dynamic IP address. If your WAN interface uses a static IP address, enter it in this field.
Gateway IP Address	This field only displays for an interface with a static IP address. Enter the gateway's IP address.
First DNS Server Second DNS Server	These fields only display for an interface with a static IP address. Enter the DNS server IP address(es) in the field(s) to the right. Leave the field as 0.0.0.0 if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it. DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The UAG uses a system DNS server (in the order you specify here) to resolve domain names for DDNS and the time server.
Back	Click Back to return to the previous screen.
Next	Click Next to continue.

5.2.5 Quick Setup Interface Wizard: Summary

This screen displays the WAN interface's settings.

Figure 44 Interface Wizard: Summary WAN (Ethernet Shown)

The following table describes the labels in this screen.

Table 13 Interface Wizard: Summary WAN

LABEL	DESCRIPTION
Encapsulation	This displays what encapsulation this interface uses to connect to the Internet.
Service Name	This field only appears for a PPPoE interface. It displays the PPPoE service name specified in the ISP account.
Server IP	This field only appears for a PPTP interface. It displays the IP address of the PPTP server.
User Name	This is the user name given to you by your ISP.
Nailed-Up	If No displays the connection will not time out. Yes means the UAG uses the idle timeout.
Idle Timeout	This is how many seconds the connection can be idle before the router automatically disconnects from the PPPoE server. 0 means no timeout.
Connection ID	If you specified a connection ID, it displays here.
WAN Interface	This identifies the interface you configure to connect with your ISP.
Zone	This field displays to which security zone this interface and Internet connection will belong.
IP Address Assignment	This field displays whether the WAN IP address is static or dynamic (Auto).
IP Address	This field displays the WAN IP address.
IP Subnet Mask	This field only appears for an Ethernet interface. It displays the interface's IP subnet mask.
Gateway IP Address	This field only appears for an Ethernet interface. It displays the IP address of the gateway.
First DNS Server Second DNS Server	If the IP Address Assignment is Static , these fields display the DNS server IP address(es).
Close	Click Close to exit the wizard.

5.3 VPN Setup Wizard

On the UAG that supports VPN, click **VPN Setup** in the main **Quick Setup** screen to open the VPN Setup Wizard **Welcome** screen.

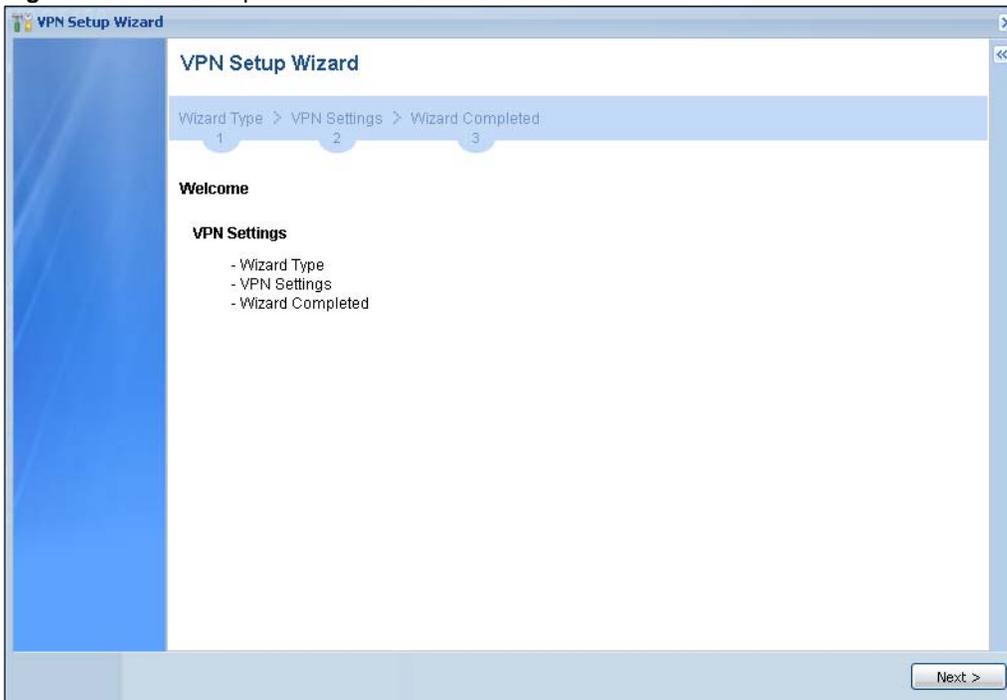
Figure 45 VPN Setup Wizard (UAG5100)



5.3.1 Welcome

Use wizards to create Virtual Private Network (VPN) rules. After you complete the wizard, the Phase 1 rule settings appear in the **VPN > IPsec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPsec VPN > VPN Connection** screen.

Figure 46 VPN Setup Wizard: Welcome

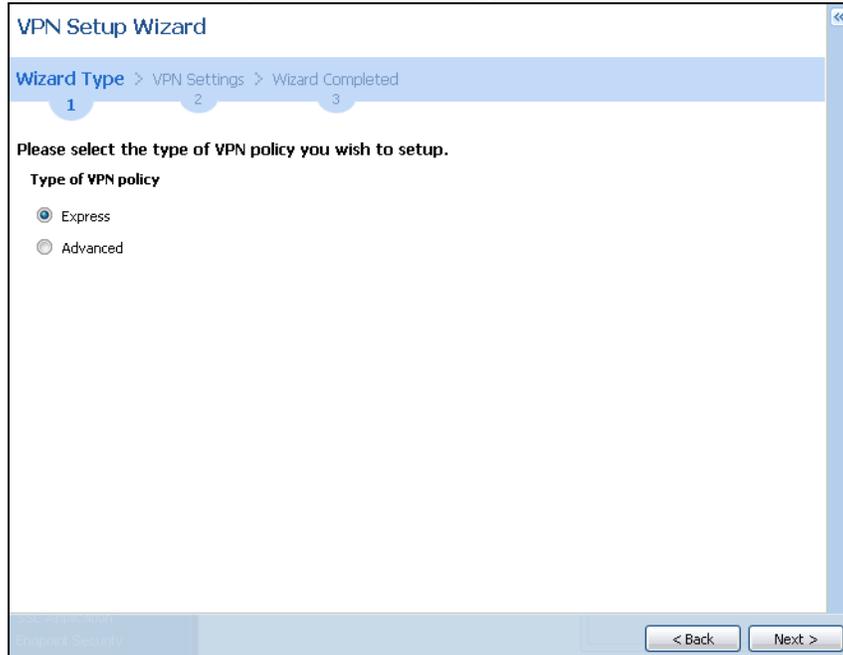


5.3.2 VPN Setup Wizard: Wizard Type

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings to connect to another ZLD-based UAG using a pre-shared key.

Choose **Advanced** to change the default settings and/or use certificates instead of a pre-shared key to create a VPN rule to connect to another IPSec device.

Figure 47 VPN Setup Wizard: Wizard Type



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Please select the type of VPN policy you wish to setup.

Type of VPN policy

Express

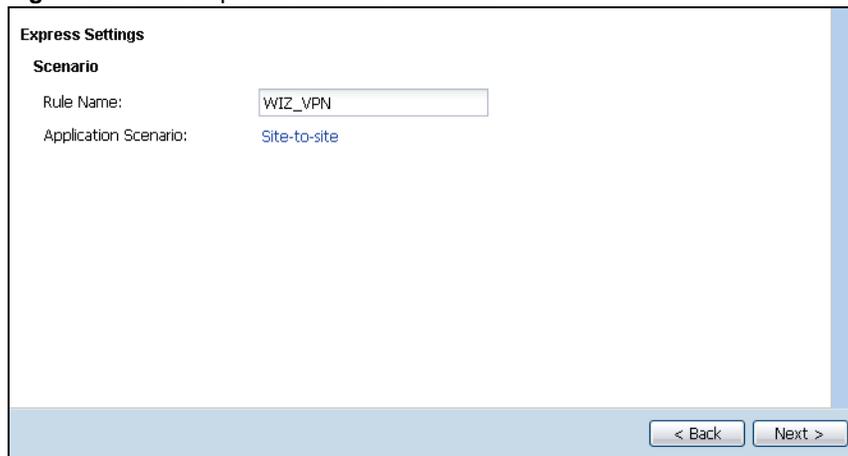
Advanced

< Back Next >

5.3.3 VPN Express Wizard - Scenario

Click the **Express** radio button as shown in [Figure 47 on page 71](#) to display the following screen.

Figure 48 VPN Express Wizard: Scenario



Express Settings

Scenario

Rule Name: WIZ_VPN

Application Scenario: Site-to-site

< Back Next >

Rule Name: Type the name used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

Application Scenario: This shows the scenario that the UAG supports.

- **Site-to-site** - The remote IPsec device has a static IP address or a domain name. This UAG can initiate the VPN tunnel.

5.3.4 VPN Express Wizard - Configuration

Figure 49 VPN Express Wizard: Configuration

- **Secure Gateway:** Enter the WAN IP address or domain name of the remote IPsec device (secure gateway) to identify the remote IPsec router by its IP address or a domain name.
- **Pre-Shared Key:** Type the password. Both ends of the VPN tunnel must use the same password. Use 8 to 31 case-sensitive ASCII characters or 8 to 31 pairs of hexadecimal ("0-9", "A-F") characters. Proceed a hexadecimal key with "0x". You will receive a PYLD_MALFORMED (payload malformed) packet if the same pre-shared key is not used on both ends.
- **Local Policy (IP/Mask):** Type the IP address of a computer on your network that can use the tunnel. You can also specify a subnet. This must match the remote IP address configured on the remote IPsec device.
- **Remote Policy (IP/Mask):** Type the IP address of a computer behind the remote IPsec device. You can also specify a subnet. This must match the local IP address configured on the remote IPsec device.

5.3.5 VPN Express Wizard - Summary

This screen provides a read-only summary of the VPN tunnel's configuration and commands that you can copy and paste into another ZLD-based UAG's command line interface to configure it.

Figure 50 VPN Express Wizard: Summary

Express Settings

Summary

Rule Name:

Secure Gateway:

Pre-Shared Key:

Local Policy (IP/Mask):

Remote Policy (IP/Mask):

Configuration for Secure Gateway

```

## I then remove the # .
# address-object WIZ_VPN_REMOTE 0.0.0.0 255.255.255.0
address-object WIZ_VPN_LOCAL 0.0.0.0 255.255.255.0
crypto map WIZ_VPN
ipsec-isakmp WIZ_VPN
encapsulation tunnel
transform-set esp-des-sha
set security-association lifetime seconds 86400
set pfs none
no nail-up
local-policy WIZ_VPN_LOCAL
remote-policy WIZ_VPN_REMOTE
no replay-detection
no netbios-broadcast
exit

```

Click "Save" button to write the VPN configuration to Device.

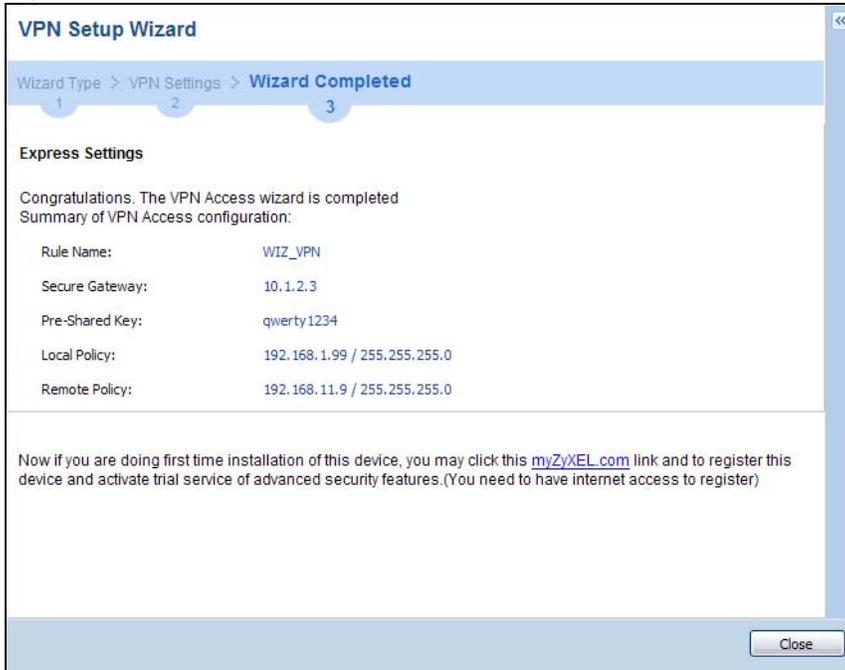
< Back Save

- **Rule Name:** Identifies the VPN gateway policy.
- **Secure Gateway:** IP address or domain name of the remote IPsec device.
- **Pre-Shared Key:** VPN tunnel password. It identifies a communicating party during a phase 1 IKE negotiation.
- **Local Policy:** IP address and subnet mask of the computers on the network behind your UAG that can use the tunnel.
- **Remote Policy:** IP address and subnet mask of the computers on the network behind the remote IPsec device that can use the tunnel.
- Copy and paste the **Configuration for Secure Gateway** commands into another ZLD-based UAG's command line interface to configure it to serve as the other end of this VPN tunnel. You can also use a text editor to save these commands as a shell script file with a ".zysh" filename extension. Use the file manager to run the script in order to configure the VPN connection. See the commands reference guide for details on the commands displayed in this list.

5.3.6 VPN Express Wizard - Finish

Now the rule is configured on the UAG. The Phase 1 rule settings appear in the **VPN > IPsec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPsec VPN > VPN Connection** screen.

Figure 51 VPN Express Wizard: Finish



Click **Close** to exit the wizard.

5.3.7 VPN Advanced Wizard - Scenario

Click the **Advanced** radio button as shown in [Figure 47 on page 71](#) to display the following screen.

Figure 52 VPN Advanced Wizard: Scenario



Rule Name: Type the name used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

Application Scenario: This shows the scenario that the UAG supports.

- **Site-to-site** - The remote IPsec device has a static IP address or a domain name. This UAG can initiate the VPN tunnel.

5.3.8 VPN Advanced Wizard - Phase 1 Settings

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA (Security Association).

Figure 53 VPN Advanced Wizard: Phase 1 Settings

- **Secure Gateway:** **Any** displays in this field if it is not configurable for the chosen scenario. Otherwise, enter the WAN IP address or domain name of the remote IPsec device (secure gateway) to identify the remote IPsec device by its IP address or a domain name. Use 0.0.0.0 if the remote IPsec device has a dynamic WAN IP address.
- **My Address (interface):** Select an interface from the drop-down list box to use on your UAG.
- **Negotiation Mode:** Select **Main** for identity protection. Select **Aggressive** to allow more incoming connections from dynamic IP addresses to use separate passwords.

Note: Multiple SAs connecting through a secure gateway must have the same negotiation mode.

- **Encryption Algorithm:** **3DES** and **AES** use encryption. The longer the key, the higher the security (this may affect throughput). Both sender and receiver must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput. **AES128** uses a 128-bit key and is faster than 3DES. AES192 uses a 192-bit key, and AES256 uses a 256-bit key.
- **Authentication Algorithm:** **MD5** gives minimal security and **SHA512** gives the highest security. MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The stronger the algorithm the slower it is.

- **Key Group: DH5** is more secure than **DH1** or **DH2** (although it may affect throughput). **DH1** (default) refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. **DH5** refers to Diffie-Hellman Group 5 a 1536 bit random number.
- **SA Life Time:** Set how often the UAG renegotiates the IKE SA. A short SA life time increases security, but renegotiation temporarily disconnects the VPN tunnel.
- **NAT Traversal:** Select this if the VPN tunnel must pass through NAT (there is a NAT router between the IPsec devices).

Note: The remote IPsec device must also have NAT traversal enabled. See the help in the main IPsec VPN screens for more information.

- **Dead Peer Detection (DPD)** has the UAG make sure the remote IPsec device is there before transmitting data through the IKE SA. If there has been no traffic for at least 15 seconds, the UAG sends a message to the remote IPsec device. If it responds, the UAG transmits the data. If it does not respond, the UAG shuts down the IKE SA.
- **Authentication Method:** Select **Pre-Shared Key** to use a password or **Certificate** to use one of the UAG's certificates.

5.3.9 VPN Advanced Wizard - Phase 2

Phase 2 in an IKE uses the SA that was established in phase 1 to negotiate SAs for IPsec.

Figure 54 VPN Advanced Wizard: Phase 2 Settings

- **Active Protocol:** **ESP** is compatible with NAT, **AH** is not.
- **Encapsulation:** **Tunnel** is compatible with NAT, **Transport** is not.
- **Encryption Algorithm:** **3DES** and **AES** use encryption. The longer the **AES** key, the higher the security (this may affect throughput). **Null** uses no encryption.
- **Authentication Algorithm:** **MD5** gives minimal security and **SHA512** gives the highest security. MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The stronger the algorithm the slower it is.
- **SA Life Time:** Set how often the UAG renegotiates the IKE SA. A short SA life time increases security, but renegotiation temporarily disconnects the VPN tunnel.

- **Perfect Forward Secrecy (PFS):** Disabling PFS allows faster IPsec setup, but is less secure. Select DH1, DH2 or DH5 to enable PFS. **DH5** is more secure than **DH1** or **DH2** (although it may affect throughput). DH1 refers to Diffie-Hellman Group 1 a 768 bit random number. DH2 refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. DH5 refers to Diffie-Hellman Group 5 a 1536 bit random number (more secure, yet slower).
- **Local Policy (IP/Mask):** Type the IP address of a computer on your network. You can also specify a subnet. This must match the remote IP address configured on the remote IPsec device.
- **Remote Policy (IP/Mask):** Type the IP address of a computer behind the remote IPsec device. You can also specify a subnet. This must match the local IP address configured on the remote IPsec device.
- **Nailed-Up:** This displays for the site-to-site and remote access client role scenarios. Select this to have the UAG automatically renegotiate the IPsec SA when the SA life time expires.

5.3.10 VPN Advanced Wizard - Summary

This is a read-only summary of the VPN tunnel settings.

Figure 55 VPN Advanced Wizard: Summary

Advanced Settings

Summary

Rule Name: WIZ_VPN1

Secure Gateway: 192.168.2.5

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 0.0.0.0 / 255.255.255.0

Remote Policy (IP/Mask): 0.0.0.0 / 255.255.255.0

Phase 1

Negotiation Mode: main

Encryption Algorithm: des

Authentication Algorithm: md5

Key Group: DH1

Phase 2

Active Protocol: esp

Encapsulation: tunnel

Encryption Algorithm: des

Authentication Algorithm: sha

Configuration for Secure Gateway

```

### Edit this shell script according to
### the comments before using it in the remote gateway.
### Check the peer-ip interface.
### Check the local-ip interface.
### Edit the WIZ_VPN1_LOCAL address-object.
### Then remove the following line.
### PLEASE REMOVE THIS LINE
configure terminal
isakmp policy WIZ_VPN1
### If this device's wan1 IP is dynamic,
### consider using DDNS and changing
### the peer-ip listed here to a domain name.
peer-ip 172.23.30.3
### Use the correct interface name in the
### next command line and remove the "#".

```

Click "Save" button to write the VPN configuration to Device.

- **Rule Name:** Identifies the VPN connection (and the VPN gateway).
- **Secure Gateway:** IP address or domain name of the remote IPsec device.

- **Pre-Shared Key:** VPN tunnel password.
- **Certificate:** The certificate the UAG uses to identify itself when setting up the VPN tunnel.
- **Local Policy:** IP address and subnet mask of the computers on the network behind your UAG that can use the tunnel.
- **Remote Policy:** IP address and subnet mask of the computers on the network behind the remote IPSec device that can use the tunnel.
- Copy and paste the **Configuration for Remote Gateway** commands into another ZLD-based UAG's command line interface.
- **Negotiation Mode:** Main mode provides better security, while aggressive mode is faster.
- **Encryption Algorithm:** The key size and encryption algorithm to use in the IPSec SA. **3DES** and **AES** use encryption. The longer the **AES** key, the higher the security (this may affect throughput). **Null** uses no encryption.
- **Authentication Algorithm:** The hash algorithm to use to authenticate packet data in the IPSec SA. **MD5** gives minimal security and **SHA512** gives the highest security.
- **Key Group:** The Diffie-Hellman key group to use for encryption. **DH5** is more secure than **DH1** or **DH2** (although it may affect throughput).
- **Active Protocol:** **ESP** is compatible with NAT, **AH** is not.
- **Encapsulation:** **Tunnel** is compatible with NAT, **Transport** is not.
- Click **Save** to save the VPN rule.

5.3.11 VPN Advanced Wizard - Finish

Now the rule is configured on the UAG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen.

Figure 56 VPN Wizard: Finish

Advanced Settings

Congratulations. The VPN Access wizard is completed
Summary

Rule Name:	WIZ_VPN
Secure Gateway:	10.1.2.5
My Address (interface):	wan1
Pre-Shared Key:	12345789

Phase 1

Negotiation Mode:	aggressive
Encryption Algorithm:	des
Authentication Algorithm:	md5
Key Group:	DH1
SA Life Time:	86400
NAT Traversal:	true
Dead Peer Detection (DPD):	true

Phase 2

Active Protocol:	esp
Encapsulation:	tunnel
Encryption Algorithm:	des
Authentication Algorithm:	sha
SA Life Time:	86400
Perfect Forward Secrecy (PFS):	None

Policy

Local Policy (IP/Mask):	172.17.2.3 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.2.5 / 255.255.255.0
Nailed-Up:	true

Now if you are doing first time installation of this device, you may click this myZyXEL.com link and to register this device and activate trial service of advanced security features.(You need to have internet access to register)

Apply Reset Close

Click **Close** to exit the wizard.

Dashboard

6.1 Overview

Use the **Dashboard** screens to check status information about the UAG.

6.1.1 What You Can Do in this Chapter

Use the **Dashboard** screens for the following.

- Use the main **Dashboard** screen (see [Section 6.2 on page 80](#)) to see the UAG's general device information, system status, system resource usage, licensed service status, and interface status. You can also display other status screens for more information.
- Use the **VPN Status** screen (see [Section 6.2.4 on page 88](#)) to look at the VPN tunnels that are currently established.
- Use the **DHCP Table** screen (see [Section 6.2.5 on page 88](#)) to look at the IP addresses currently assigned to DHCP clients and the IP addresses reserved for specific MAC addresses.
- Use the **Number of Login Users** screen (see [Section 6.2.6 on page 89](#)) to look at a list of the users currently logged into the UAG.

6.2 The Dashboard Screen

The **Dashboard** screen displays when you log into the UAG or click **Dashboard** in the navigation panel. The dashboard displays general device information, system status, system resource usage, licensed service status, and interface status in widgets that you can re-arrange to suit your needs. You can also collapse, refresh, and close individual widgets.

Figure 57 Dashboard



The following table describes the labels in this screen.

Table 14 Dashboard

LABEL	DESCRIPTION
Widget Settings (A)	Use this link to open or close widgets by selecting/clearing the associated checkbox.
Up Arrow (B)	Click this to collapse a widget. It then becomes a down arrow. Click it again to enlarge the widget again.
Refresh Time Setting (C)	Set the interval for refreshing the information displayed in the widget.
Refresh Now (D)	Click this to update the widget's information immediately.

Table 14 Dashboard (continued)

LABEL	DESCRIPTION
Close Widget (E)	Click this to close the widget. Use Widget Setting to re-open it.
Virtual Device	Select to view the front panel or the rear panel. Hover your cursor over a LED, connected slot or Ethernet port to view details about the status of the UAG's front panel LEDs and connections. See Section 2.3.1 on page 39 for LED descriptions. An unconnected interface or slot appears grayed out. You can also see which antennas are for radio 1 (2.4 GHz WLAN) and which antennas are for radio 2 (5 GHz WLAN) on the rear panel.
	The following labels display when you hover your cursor over an Ethernet port or USB port.
Name	This field displays the name of each interface.
Slot	This field displays the name of each extension slot.
Device	This field displays the name of the device connected to the USB port if one is connected.
Status	This field displays the current status of each interface or device installed in a slot. The possible values depend on what type of interface it is. Inactive - The Ethernet interface is disabled. Down - The Ethernet interface does not have any physical ports associated with it or the Ethernet interface is enabled but not connected. Speed / Duplex - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (Full or Half). Ready - The USB port is connected.
Zone	This field displays the zone to which the interface is currently assigned.
IP Address/ Mask	This field displays the current IP address and subnet mask assigned to the interface.
Console speed	This field displays the current console port speed.
Device Information	
System Name	This field displays the name used to identify the UAG on any network. Click the icon to open the screen where you can change it.
Model Name	This field displays the model name of this UAG.
Serial Number	This field displays the serial number of this UAG. The serial number is used for device tracking and control.
MAC Address Range	This field displays the MAC addresses used by the UAG. Each physical port has one MAC address. The first MAC address is assigned to physical port 1, the second MAC address is assigned to physical port 2, and so on.
Firmware Version	This field displays the version number and date of the firmware the UAG is currently running. Click the icon to open the screen where you can upload firmware.
System Status	
System Uptime	This field displays how long the UAG has been running since it last restarted or was turned on.
Current Date/Time	This field displays the current date and time in the UAG. The format is yyyy-mm-dd hh:mm:ss. Click the icon to open the screen where you can configure the UAG's date and time.
VPN Status	This field displays the actual number of VPN tunnels up. Click this to look at the VPN tunnels that are currently established. See Section 6.2.4 on page 88 . This field is available only on the UAG that supports IPsec VPN.
DHCP Table	Click this to look at the IP addresses currently assigned to the UAG's DHCP clients and the IP addresses reserved for specific MAC addresses. See Section 6.2.5 on page 88 .

Table 14 Dashboard (continued)

LABEL	DESCRIPTION
Current Login User	This field displays the user name used to log in to the current session, the amount of reauthentication time remaining, and the amount of lease time remaining.
Number of Login Users	This field displays the number of users currently logged in to the UAG. Click the icon to pop-open a list of the users who are currently logged in to the UAG.
Boot Status	<p>This field displays details about the UAG's startup state.</p> <p>OK - The UAG started up successfully.</p> <p>Firmware update OK - A firmware update was successful.</p> <p>Problematic configuration after firmware update - The application of the configuration failed after a firmware upgrade.</p> <p>System default configuration - The UAG successfully applied the system default configuration. This occurs when the UAG starts for the first time or you intentionally reset the UAG to the system default settings.</p> <p>Fallback to lastgood configuration - The UAG was unable to apply the startup-config.conf configuration file and fell back to the lastgood.conf configuration file.</p> <p>Fallback to system default configuration - The UAG was unable to apply the lastgood.conf configuration file and fell back to the system default configuration file (system-default.conf).</p> <p>Booting in progress - The UAG is still applying the system configuration.</p>
Drop-in Mode Status	<p>This field displays whether the UAG is working in drop-in mode.</p> <p>When the UAG is in drop-in mode, you can deploy it in your existing network without changing the network architecture and use its multiple WAN feature to connect to more than one ISP. See the CLI Reference Guide for how to use commands to set the UAG interfaces to work in drop-in mode.</p> <p>This field is available only on the UAG that supports drop-in mode.</p>
Interface Status Summary	If an Ethernet interface does not have any physical ports associated with it, its entry is displayed in light gray text.
Name	This field displays the name of each interface.
Status	<p>This field displays the current status of each interface. The possible values depend on what type of interface it is.</p> <p>For Ethernet interfaces:</p> <p>Inactive - The Ethernet interface is disabled.</p> <p>Down - The Ethernet interface does not have any physical ports associated with it or the Ethernet interface is enabled but not connected.</p> <p>Up - The Ethernet interface is enabled and connected.</p> <p>For PPP interfaces:</p> <p>Connected - The PPP interface is connected.</p> <p>Disconnected - The PPP interface is not connected.</p> <p>If the PPP interface is disabled, it does not appear in the list.</p>
Zone	This field displays the zone to which the interface is currently assigned.
IP Addr/Netmask	<p>This field displays the current IP address and subnet mask assigned to the interface. If the IP address is 0.0.0.0/0.0.0.0, the interface is disabled or did not receive an IP address and subnet mask via DHCP.</p> <p>If this interface is a member of an active virtual router, this field displays the IP address it is currently using. This is either the static IP address of the interface (if it is the master) or the management IP address (if it is a backup).</p>

Table 14 Dashboard (continued)

LABEL	DESCRIPTION
IP Assignment	This field displays how the interface gets its IP address. Static - This interface has a static IP address. DHCP Client - This Ethernet interface gets its IP address from a DHCP server. Dynamic - This PPP interface gets its IP address from a DHCP server.
Action	Use this field to get or to update the IP address for the interface. Click Renew to send a new DHCP request to a DHCP server. Click the Connect icon to have the UAG try to connect a PPPoE/PPTP interface. If the interface cannot use one of these ways to get or to update its IP address, this field displays n/a . Click the Disconnect icon to stop a PPPoE/PPTP connection.
Extension Slot	This section of the screen displays the status of the USB ports.
#	This field displays how many USB ports there are.
Extension Slot	This field displays the name of each extension slot.
Device	This field displays the name of the device connected to the extension slot (or none if no device is detected).
Status	Ready - A USB storage device connected to the UAG is ready for the UAG to use. none - The UAG is unable to mount a USB storage device connected to the UAG.
Licensed Service Status	
#	This shows how many licensed services there are.
Status	This is the current status of the license.
Name	This identifies the licensed service.
Version	This is the version number of the service.
Expiration	If the service license is valid, this shows when it will expire. n/a displays if the service license does not have a limited period of validity. 0 displays if the service is not licensed or has expired.
Count	This field displays the maximum number of wired and wireless users that may connect to the UAG at the same time or how many managed APs the UAG can support with your current license. 0 displays if the service license does not have a limited period of validity.
System Resources	
CPU Usage	This field displays what percentage of the UAG's processing capability is currently being used. Hover your cursor over this field to display the Show CPU Usage icon that takes you to a chart of the UAG's recent CPU usage.
Memory Usage	This field displays what percentage of the UAG's RAM is currently being used. Hover your cursor over this field to display the Show Memory Usage icon that takes you to a chart of the UAG's recent memory usage.
Flash Usage	This field displays what percentage of the UAG's onboard flash memory is currently being used.
USB Storage Usage	This field shows how much storage in the USB device connected to the UAG is in use.

Table 14 Dashboard (continued)

LABEL	DESCRIPTION
Active Sessions	This field displays how many traffic sessions are currently open on the UAG. These are all sessions, established and non-established, that pass through/from/to/within the UAG. Hover your cursor over this field to display icons. Click the Detail icon to go to the Session Monitor screen to see details about the active sessions. Click the Show Active Sessions icon to display a chart of UAG's recent session usage.
AP Information	This shows a summary of connected wireless Access Points (APs).
All AP	This section displays a summary for all connected wireless APs. Click the link to go to the Monitor > Wireless > AP information > AP List screen.
Online Management AP	This displays the number of currently connected management APs.
Offline Management AP	This displays the number of currently offline managed APs.
Un-Management AP	This displays the number of non-managed APs.
All Station	This section displays a summary of connected stations. Click the link to go to the Monitor > Wireless > Station Info > Station List screen.
Station	This displays the number of stations currently connected to the network.
All Sensed Device	This sections displays a summary of all wireless devices detected by the network. Click the link to go to the Monitor > Wireless > Detected Device screen.
Un-Classified AP	This displays the number of detected unclassified APs.
Rogue AP	This displays the number of detected rogue APs.
Friendly AP	This displays the number of detected friendly APs.
Top 5 Station	Displays the top 5 Access Points (AP) with the highest number of station (aka wireless client) connections.
#	This field displays the rank of the station.
AP MAC	This field displays the MAC address of the AP to which the station belongs.
Max. Station Count	This field displays the maximum number of wireless clients that have connected to this AP.
AP Description	This field displays the AP's description. The default description is "AP-" followed by the AP's MAC address.
Top 5 IPv4 Security Policy Rules that Blocked Traffic	This section displays the most triggered five security policy rules that caused the UAG to block.
#	This is the entry's rank in the list of the most commonly triggered rules.
From	This shows the zone from which packets that triggered the rule came.
To	This shows the zone to which packets that triggered the rule went.
Description	This field displays the descriptive name (if any) of the triggered rule.
Hits	This field displays how many times the rule was triggered.
The Latest Alert Logs	This section of the screen displays recent logs generated by the UAG.
#	This is the entry's rank in the list of alert logs.
Time	This field displays the date and time the log was created.
Priority	This field displays the severity of the log.
Category	This field displays the type of log generated.

Table 14 Dashboard (continued)

LABEL	DESCRIPTION
Message	This field displays the actual log message.
Source	This field displays the source address (if any) in the packet that generated the log.
Destination	This field displays the destination address (if any) in the packet that generated the log.

6.2.1 The CPU Usage Screen

Use this screen to look at a chart of the UAG's recent CPU usage. To access this screen, click **CPU Usage** in the dashboard.

Figure 58 Dashboard > CPU Usage

The following table describes the labels in this screen.

Table 15 Dashboard > CPU Usage

LABEL	DESCRIPTION
	The y-axis represents the percentage of CPU usage.
	The x-axis shows the time period over which the CPU usage occurred
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh Now	Click this to update the information in the window right away.

6.2.2 The Memory Usage Screen

Use this screen to look at a chart of the UAG's recent memory (RAM) usage. To access this screen, click **Memory Usage** in the dashboard.

Figure 59 Dashboard > Memory Usage

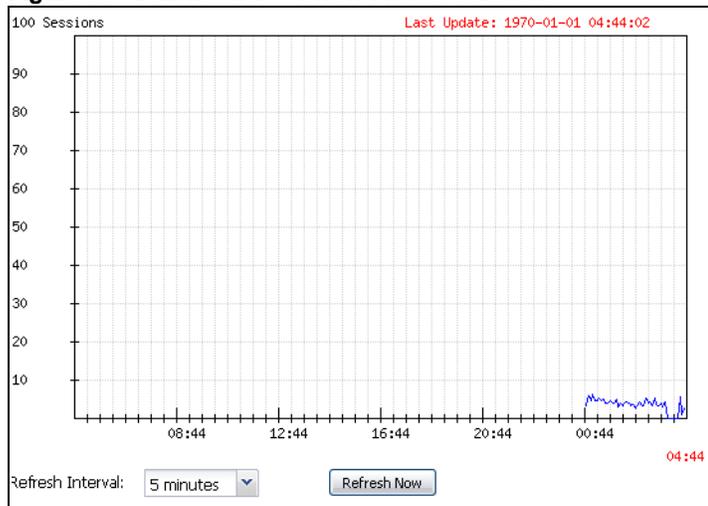
The following table describes the labels in this screen.

Table 16 Dashboard > Memory Usage

LABEL	DESCRIPTION
	The y-axis represents the percentage of RAM usage.
	The x-axis shows the time period over which the RAM usage occurred
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh Now	Click this to update the information in the window right away.

6.2.3 The Active Sessions Screen

Use this screen to look at a chart of the UAG's recent traffic session usage. To access this screen, click **Show Active Sessions** in the dashboard.

Figure 60 Dashboard > Show Active Sessions

The following table describes the labels in this screen.

Table 17 Dashboard > Show Active Sessions

LABEL	DESCRIPTION
Sessions	The y-axis represents the number of session.
	The x-axis shows the time period over which the session usage occurred
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh Now	Click this to update the information in the window right away.

6.2.4 The VPN Status Screen

Use this screen to look at the VPN tunnels that are currently established. To access this screen, click **VPN Status** in **System Status** in the dashboard. This screen is available only on the UAG that supports IPSec VPN.

Figure 61 Dashboard > System Status > VPN Status



The following table describes the labels in this screen.

Table 18 Dashboard > VPN Status

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific SA.
Name	This field displays the name of the IPSec SA.
Encapsulation	This field displays how the IPSec SA is encapsulated.
Algorithm	This field displays the encryption and authentication algorithms used in the SA.
Refresh Interval	Select how often you want this window to be updated automatically.
Refresh Now	Click this to update the information in the window right away.

6.2.5 The DHCP Table Screen

Use this screen to look at the IP addresses currently assigned to DHCP clients and the IP addresses reserved for specific MAC addresses. To access this screen, click **DHCP Table** in **System Status** in the dashboard.

Figure 62 Dashboard > DHCP Table

#	Interface	IP Address	Host Name	MAC Address	Description	Reserve
1	lan1	172.16.1.1	"nwa5123-nl"	b0:b2:dc:6e:7f:24		<input type="checkbox"/>
2	lan1	172.16.2.0	"twpc-01"	00:19:cb:32:be:ac		<input type="checkbox"/>

Refresh Interval: 5 minutes

The following table describes the labels in this screen.

Table 19 Dashboard > DHCP Table

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific entry.
Interface	This field identifies the interface that assigned an IP address to a DHCP client.
IP Address	This field displays the IP address currently assigned to a DHCP client or reserved for a specific MAC address. Click the column's heading cell to sort the table entries by IP address. Click the heading cell again to reverse the sort order.
Host Name	This field displays the name used to identify this device on the network (the computer name). The UAG learns these from the DHCP client requests. "None" shows here for a static DHCP entry.
MAC Address	This field displays the MAC address to which the IP address is currently assigned or for which the IP address is reserved. Click the column's heading cell to sort the table entries by MAC address. Click the heading cell again to reverse the sort order.
Description	For a static DHCP entry, the host name or the description you configured shows here. This field is blank for dynamic DHCP entries.
Reserve	<p>If this field is selected, this entry is a static DHCP entry. The IP address is reserved for the MAC address.</p> <p>If this field is clear, this entry is a dynamic DHCP entry. The IP address is assigned to a DHCP client.</p> <p>To create a static DHCP entry using an existing dynamic DHCP entry, select this field.</p> <p>To remove a static DHCP entry, clear this field.</p>
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh Now	Click this to update the information in the window right away.

6.2.6 The Number of Login Users Screen

Use this screen to look at a list of the users currently logged into the UAG. Users who close their browsers without logging out are still shown as logged in here. To access this screen, click **Number of Login Users** in **System Status** in the dashboard.

Figure 63 Dashboard > Number of Login Users

Number of Login Users									
#	Us...	Reauth/L...	Session ...	Remainin...	Remaining Q...	Type	IP Addr...	Us...	Force L...
0	ad...	unlimited...	unlimited	n/a	- / - / -	console	console	ad...	n/a
1	ad...	unlimited...	unlimited	n/a	- / - / -	http/https	172.17....	ad...	 Logout
2	nz...	n/a / n/a	unlimited	0000day...	unlimited / - / -	http/https	172.17....	dy...	 Logout

The following table describes the labels in this screen.

Table 20 Dashboard > Number of Login Users

LABEL	DESCRIPTION
#	This field is a sequential value and is not associated with any entry.
User ID	This field displays the user name of each user who is currently logged in to the UAG.
Reauth/Lease Time	This field displays the amount of reauthentication time remaining and the amount of lease time remaining for each user. See Chapter 35 on page 399 for more information.
Session Timeout	This field displays the total amount of time the account (authenticated by an external server) can use to log into the UAG or access the Internet through the UAG. This shows unlimited for an administrator account.
Remaining Time	This field displays the amount of Internet access time remaining for each account. This shows n/a for an administrator account.
Remaining Quota (T/U/D)	This field displays the remaining amount of data that can be transmitted or received by each account. You can see the amount of either data in both directions (Total) or upstream data (U pload) and downstream data (D ownload). This shows - / - / - for an administrator account.
Type	This field displays the way the user logged in to the UAG.
IP address	This field displays the IP address of the computer used to log in to the UAG.
User Info	This field displays the types of user accounts the UAG uses. If the user type is ext-user (external user), this field will show its external-group information when you move your mouse over it. If the external user matches two external-group objects, both external-group object names will be shown.
Force Logout	Click this icon to end a user's session.

7.1 Overview

Use the **Monitor** screens to check status and statistics information.

7.1.1 What You Can Do in this Chapter

Use the **Monitor** screens for the following.

- Use the **System Status > Port Statistics** screen (see [Section 7.2 on page 92](#)) to look at packet statistics for each physical port.
- Use the **System Status > Port Statistics > Graph View** screen (see [Section 7.2 on page 92](#)) to look at a line graph of packet statistics for each physical port.
- Use the **System Status > Interface Status** screen (see [Section 7.3 on page 94](#)) to see all of the UAG's interfaces and their packet statistics.
- Use the **System Status > Traffic Statistics** screen (see [Section 7.4 on page 97](#)) to start or stop data collection and view statistics.
- Use the **System Status > Session Monitor** screen (see [Section 7.5 on page 99](#)) to view sessions by user or service.
- Use the **System Status > DDNS Status** screen (see [Section 7.6 on page 101](#)) to view the status of the UAG's DDNS domain names.
- Use the **System Status > IP/MAC Binding** screen (see [Section 7.7 on page 101](#)) to view a list of devices that have received an IP address from UAG interfaces with IP/MAC binding enabled.
- Use the **System Status > Login Users** screen (see [Section 7.8 on page 102](#)) to look at a list of the users currently logged into the UAG.
- Use the **System Status > Dynamic Guest** screen (see [Section 7.9 on page 103](#)) to look at a list of the guest user accounts, which are created automatically and allowed to access the UAG's services for a certain period of time.
- Use the **System Status > UPnP Port Status** screen (see [Section 7.10 on page 105](#)) to look at a list of the NAT port mapping rules that UPnP creates on the UAG.
- Use the **System Status > USB Storage** screen (see [Section 7.11 on page 106](#)) to view information about a connected USB storage device.
- Use the **System Status > Ethernet Neighbor** screen (see [Section 7.12 on page 107](#)) to view and manage the UAG's neighboring devices via Layer Link Discovery Protocol (LLDP).
- Use the **AP Information > AP List** screen (see [Section 7.13 on page 109](#)) to view which APs are currently connected to the UAG.
- Use the **AP Information > Radio List** screen (see [Section 7.14 on page 112](#)) to view statistics about the wireless radio transmitters in each of the APs connected to the UAG.
- Use the **Station Info > Station List** screen (see [Section 7.15 on page 115](#)) to view statistics pertaining to the connected stations (or "wireless clients").

- Use the **Detected Device** screen (Section 7.16 on page 116) to view the wireless devices passively detected by the UAG.
- Use the **Printer Status** screen (see Section 7.17 on page 118) to view information about the connected statement printers.
- Use the **VPN 1-1 Mapping** screen (see Section 7.18 on page 118) to view the status of the active users to which the UAG applied a VPN 1-1 mapping rule.
- Use the **VPN 1-1 Mapping > Statistics** screen (see Section 7.18.1 on page 119) to display statistics for each of the VPN 1-1 mapping rules.
- Use the **VPN Monitor > IPSec** screen (see Section 7.19 on page 120) to display and manage active IPSec SAs.
- Use the **UTM Statistics > App Patrol** screen (see Section 7.20 on page 121) to start or stop data collection and view virus statistics
- Use the **UTM Statistics > Content Filter** screen (see Section 7.21 on page 123) to start or stop data collection and view content filter statistics.
- Use the **Log > View Log** screen (see Section 7.22 on page 125) to view the UAG's current log messages. You can change the way the log is displayed, you can e-mail the log, and you can also clear the log in this screen.
- Use the **Log > View AP Log** screen (see Section 7.22.1 on page 127) to view the UAG's current wireless AP log messages.
- Use the **Log > Dynamic Users Log** screen (see Section 7.22.2 on page 129) to view the UAG's dynamic guest account log messages.

7.2 The Port Statistics Screen

Use this screen to look at packet statistics for each Gigabit Ethernet port. To access this screen, click **Monitor > System Status > Port Statistics**.

Figure 64 Monitor > System Status > Port Statistics

The screenshot shows the 'Port Statistics' screen with the following data:

#	Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
1	1	Down	0	0	0	0	0	00:00:00
2	2	100M/Full	43408	961210	0	57	1758	46:07:52
3	3	Down	0	0	0	0	0	00:00:00
4	4	Down	0	0	0	0	0	00:00:00
5	5	Down	0	0	0	0	0	00:00:00

Additional screen details: Poll Interval: 5 (1-60 seconds), System Up Time: 1 days, 22:03:21, Displaying 1 - 5 of 5.

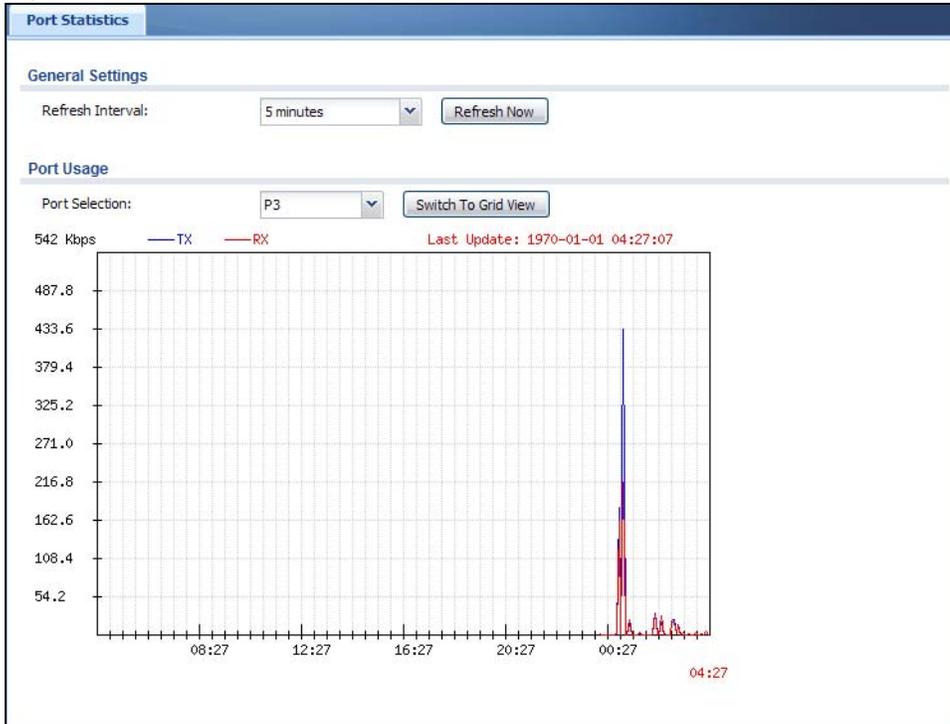
The following table describes the labels in this screen.

Table 21 Monitor > System Status > Port Statistics

LABEL	DESCRIPTION
Poll Interval	Enter how often you want this window to be updated automatically, and click Set Interval .
Set Interval	Click this to set the Poll Interval the screen uses.
Stop	Click this to stop the window from updating automatically. You can start it again by setting the Poll Interval and clicking Set Interval .
Switch to Graphic View	Click this to display the port statistics as a line graph.
#	This field displays the port's number in the list.
Port	This field displays the physical port number.
Status	This field displays the current status of the physical port. Down - The physical port is not connected. Speed / Duplex - The physical port is connected. This field displays the port speed and duplex setting (Full or Half).
TxPkts	This field displays the number of packets transmitted from the UAG on the physical port since it was last connected.
RxPkts	This field displays the number of packets received by the UAG on the physical port since it was last connected.
Collisions	This field displays the number of collisions on the physical port since it was last connected.
Tx B/s	This field displays the transmission speed, in bytes per second, on the physical port in the one-second interval before the screen updated.
Rx B/s	This field displays the reception speed, in bytes per second, on the physical port in the one-second interval before the screen updated.
Up Time	This field displays how long the physical port has been connected.
System Up Time	This field displays how long the UAG has been running since it last restarted or was turned on.

7.2.1 The Port Statistics Graph Screen

Use this screen to look at a line graph of packet statistics for each physical port. To access this screen, click **Port Statistics** in the **Status** screen and then the **Switch to Graphic View** Button.

Figure 65 Monitor > System Status > Port Statistics > Switch to Graphic View

The following table describes the labels in this screen.

Table 22 Monitor > System Status > Port Statistics > Switch to Graphic View

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh Now	Click this to update the information in the window right away.
Port Selection	Select the number of the physical port for which you want to display graphics.
Switch to Grid View	Click this to display the port statistics as a table.
Kbps	The y-axis represents the speed of transmission or reception.
time	The x-axis shows the time period over which the transmission or reception occurred
TX	This line represents traffic transmitted from the UAG on the physical port since it was last connected.
RX	This line represents the traffic received by the UAG on the physical port since it was last connected.
Last Update	This field displays the date and time the information in the window was last updated.

7.3 The Interface Status Screen

This screen lists all of the UAG's interfaces and gives packet statistics for them. Click **Monitor > System Status > Interface Status** to access this screen.

Figure 66 Monitor > System Status > Interface Status

Interface Summary							
Interface Status							
Name	Port	Status	Zone	IP Addr/Netmask	IP Assignm...	Services	Action
wan1	P1	100M/Full	WAN	192.23.30.3 / 255.255.255.0	DHCP client	n/a	Renew
wan1_ppp	P1	Inactive	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
wan2	P2	Down	WAN	0.0.0.0 / 0.0.0.0	DHCP client	n/a	Renew
wan2_ppp	P2	Inactive	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
lan1	P3	100M/Full	LAN1	172.16.0.1 / 255.255.0.0	Static	DHCP server	n/a
lan2	P4	100M/Full	LAN2	172.17.0.1 / 255.255.0.0	Static	DHCP server	n/a
dmz	P5	100M/Full	DMZ	172.18.0.1 / 255.255.0.0	Static	DHCP server	n/a

Interface Statistics						
Refresh						
Name	Status	TxPkts	RxPkts	Tx B/s	Rx B/s	
wan1	100M/Full	738494	1452329	1783	616	
wan2	Down	12	0	0	0	
wan2_ppp	Inactive			0	0	
lan1	100M/Full	982008	740120	2394	1831	
lan2	100M/Full	144788	129967	0	0	
dmz	100M/Full	1755	1778	0	0	

Each field is described in the following table.

Table 23 Monitor > System Status > Interface Status

LABEL	DESCRIPTION
Interface Status	If an Ethernet interface does not have any physical ports associated with it, its entry is displayed in light gray text.
Expand/Close	Click this button to show or hide statistics for all the virtual interfaces on top of the Ethernet interfaces.
Name	This field displays the name of each interface. If there is an Expand icon (plus-sign) next to the name, click this to look at the status of virtual interfaces on top of this interface.
Port	This field displays the physical port number.
Status	<p>This field displays the current status of each interface. The possible values depend on what type of interface it is.</p> <p>For Ethernet interfaces:</p> <ul style="list-style-type: none"> • Inactive - The Ethernet interface is disabled. • Down - The Ethernet interface does not have any physical ports associated with it or the Ethernet interface is enabled but not connected. • Up - The LAN Ethernet interface is enabled and connected. • Speed / Duplex - The WAN Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (Full or Half). <p>For virtual interfaces, this field always displays Up or Down. If the virtual interface is disabled, it displays Inactive.</p> <p>For VLAN and bridge interfaces, this field always displays Up or Down. If the VLAN or bridge interface is disabled, it displays Inactive.</p> <p>For PPP interfaces:</p> <ul style="list-style-type: none"> • Inactive - The PPP interface is disabled. • Connected - The PPP interface is connected. • Disconnected - The PPP interface is not connected.

Table 23 Monitor > System Status > Interface Status (continued)

LABEL	DESCRIPTION
Zone	This field displays the zone to which the interface is assigned.
IP Addr/Netmask	This field displays the current IP address and subnet mask assigned to the interface. If the IP address and subnet mask are 0.0.0.0, the interface is disabled or did not receive an IP address and subnet mask via DHCP.
IP Assignment	<p>This field displays how the interface gets its IP address.</p> <p>Static - This interface has a static IP address.</p> <p>DHCP Client - This interface gets its IP address from a DHCP server.</p>
Services	This field lists which services the interface provides to the network. Examples include DHCP relay , and DHCP server . This field displays n/a if the interface does not provide any services to the network.
Action	Use this field to get or to update the IP address for the interface. Click Renew to send a new DHCP request to a DHCP server. Click Connect to try to connect a PPPoE/PPTP interface. If the interface cannot use one of these ways to get or to update its IP address, this field displays n/a .
Interface Statistics	This table provides packet statistics for each interface.
Refresh	Click this button to update the information in the screen.
Expand/Close	Click this button to show or hide statistics for all the virtual interfaces on top of the Ethernet interfaces.
Name	This field displays the name of each interface. If there is a Expand icon (plus-sign) next to the name, click this to look at the statistics for virtual interfaces on top of this interface.
Status	<p>This field displays the current status of each interface. The possible values depend on what type of interface it is.</p> <p>For Ethernet interfaces:</p> <ul style="list-style-type: none"> • Inactive - The Ethernet interface is disabled. • Down - The Ethernet interface does not have any physical ports associated with it or the Ethernet interface is enabled but not connected. • Up - The LAN Ethernet interface is enabled and connected. • Speed / Duplex - The WAN Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (Full or Half). <p>For virtual interfaces, this field always displays Up or Down. If the virtual interface is disabled, it displays Inactive.</p> <p>For VLAN and bridge interfaces, this field always displays Up or Down. If the VLAN or bridge interface is disabled, it displays Inactive.</p> <p>For PPP interfaces:</p> <ul style="list-style-type: none"> • Inactive - The PPP interface is disabled. • Connected - The PPP interface is connected. • Disconnected - The PPP interface is not connected.
TxPkts	This field displays the number of packets transmitted from the UAG on the interface since it was last connected.
RxPkts	This field displays the number of packets received by the UAG on the interface since it was last connected.
Tx B/s	This field displays the transmission speed, in bytes per second, on the interface in the one-second interval before the screen updated.
Rx B/s	This field displays the reception speed, in bytes per second, on the interface in the one-second interval before the screen updated.

7.4 The Traffic Statistics Screen

Click **Monitor > System Status > Traffic Statistics** to display the **Traffic Statistics** screen. This screen provides basic information about the following for example:

- Most-visited Web sites and the number of times each one was visited. This count may not be accurate in some cases because the UAG counts HTTP GET packets. Please see [Table 24 on page 97](#) for more information.
- Most-used protocols or service ports and the amount of traffic on each one
- LAN IP with heaviest traffic and how much traffic has been sent to and from each one

You use the **Traffic Statistics** screen to tell the UAG when to start and when to stop collecting information for these reports. You cannot schedule data collection; you have to start and stop it manually in the **Traffic Statistics** screen.

Figure 67 Monitor > System Status > Traffic Statistics

There is a limit on the number of records shown in the report. Please see [Table 25 on page 99](#) for more information. The following table describes the labels in this screen.

Table 24 Monitor > System Status > Traffic Statistics

LABEL	DESCRIPTION
Data Collection	
Collect Statistics	Select this to have the UAG collect data for the report. If the UAG has already been collecting data, the collection period displays to the right. The progress is not tracked here real-time, but you can click the Refresh button to update it.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.
Statistics	
Interface	Select the interface from which to collect information. You can collect information from Ethernet, VLAN, bridge and PPPoE/PPTP interfaces.

Table 24 Monitor > System Status > Traffic Statistics (continued)

LABEL	DESCRIPTION
Sort By	Select the type of report to display. Choices are: Host IP Address/User - displays the IP addresses or users with the most traffic and how much traffic has been sent to and from each one. Service/Port - displays the most-used protocols or service ports and the amount of traffic for each one. Web Site Hits - displays the most-visited Web sites and how many times each one has been visited. Each type of report has different information in the report (below).
Refresh	Click this button to update the report display.
Flush Data	Click this button to discard all of the screen's statistics and update the report display.
	These fields are available when the Top is Host IP Address/User .
#	This field is the rank of each record. The IP addresses and users are sorted by the amount of traffic.
Direction	This field indicates whether the IP address or user is sending or receiving traffic. RX From - traffic is coming from the IP address or user to the UAG. Tx To - traffic is going from the UAG to the IP address or user.
IP Address/User	This field displays the IP address or user in this record. The maximum number of IP addresses or users in this report is indicated in Table 25 on page 99 .
Amount	This field displays how much traffic was sent or received from the indicated IP address or user. If the Direction is RX From , a red bar is displayed; if the Direction is Tx To , a blue bar is displayed. The unit of measure is bytes, Kbytes, Mbytes or Gbytes, depending on the amount of traffic for the particular IP address or user. The count starts over at zero if the number of bytes passes the byte count limit. See Table 25 on page 99 .
	These fields are available when the Top is Service/Port .
#	This field is the rank of each record. The protocols and service ports are sorted by the amount of traffic.
Service/Port	This field displays the service and port in this record. The maximum number of services and service ports in this report is indicated in Table 25 on page 99 .
Protocol	This field indicates what protocol the service was using.
Direction	This field indicates whether the indicated protocol or service port is sending or receiving traffic. Ingress - traffic is coming into the router through the interface Egress - traffic is going out from the router through the interface
Amount	This field displays how much traffic was sent or received from the indicated service / port. If the Direction is Ingress , a red bar is displayed; if the Direction is Egress , a blue bar is displayed. The unit of measure is bytes, Kbytes, Mbytes, Gbytes, or Tbytes, depending on the amount of traffic for the particular protocol or service port. The count starts over at zero if the number of bytes passes the byte count limit. See Table 25 on page 99 .
	These fields are available when the Top is Web Site Hits .
#	This field is the rank of each record. The domain names are sorted by the number of hits.
Web Site	This field displays the domain names most often visited. The UAG counts each page viewed on a Web site as another hit. The maximum number of domain names in this report is indicated in Table 25 on page 99 .
Hits	This field displays how many hits the Web site received. The UAG counts hits by counting HTTP GET packets. Many Web sites have HTTP GET references to other Web sites, and the UAG counts these as hits too. The count starts over at zero if the number of hits passes the hit count limit. See Table 25 on page 99 .

The following table displays the maximum number of records shown in the report, the byte count limit, and the hit count limit.

Table 25 Maximum Values for Reports

LABEL	DESCRIPTION
Maximum Number of Records	20
Byte Count Limit	2^{64} bytes; this is just less than 17 million terabytes.
Hit Count Limit	2^{64} hits; this is over 1.8×10^{19} hits.

7.5 The Session Monitor Screen

The **Session Monitor** screen displays information about all established sessions that pass through the UAG for debugging or statistical analysis. It is not possible to manage sessions in this screen. The following information is displayed.

- User who started the session
- Protocol or service port used
- Source address
- Destination address
- Number of bytes received (so far)
- Number of bytes transmitted (so far)
- Duration (so far)

You can look at all the active sessions by user, service, source IP address, or destination IP address. You can also filter the information by user, protocol / service or service group, source address, and/or destination address and view it by user.

Click **Monitor > System Status > Session Monitor** to display the following screen.

Figure 68 Monitor > System Status > Session Monitor

The screenshot shows the Session Monitor interface. At the top, there is a 'Session' section with filters: 'View' set to 'all sessions', a 'Refresh' button, 'User' (empty), 'Service' set to 'any', 'Source Address' (empty), and 'Destination Address' (empty). A 'Search' button is located below the filters. The main area contains a table with the following data:

#	User	Service	Source	Destination	Rx	Tx	Duration
1	admin	HTTP	172.16.2.0:46...	192.13.6.248:...	430 Bytes	882 Bytes	0
2	admin	HTTP	172.16.2.0:46...	192.13.6.248:...	431 Bytes	883 Bytes	0
3	admin	HTTP	172.16.2.0:46...	192.13.6.248:...	3.212 KBytes	1.021 KBytes	0
4	admin	HTTP	172.16.2.0:46...	192.13.6.248:...	805 Bytes	541 Bytes	1
5	admin	HTTP	172.16.2.0:45...	192.13.6.248:...	4.054 KBytes	1.501 KBytes	12

At the bottom of the table, there is a pagination control: 'Page 1 of 1', 'Show 50 items', and 'Displaying 1 - 5 of 5'.

The following table describes the labels in this screen.

Table 26 Monitor > System Status > Session Monitor

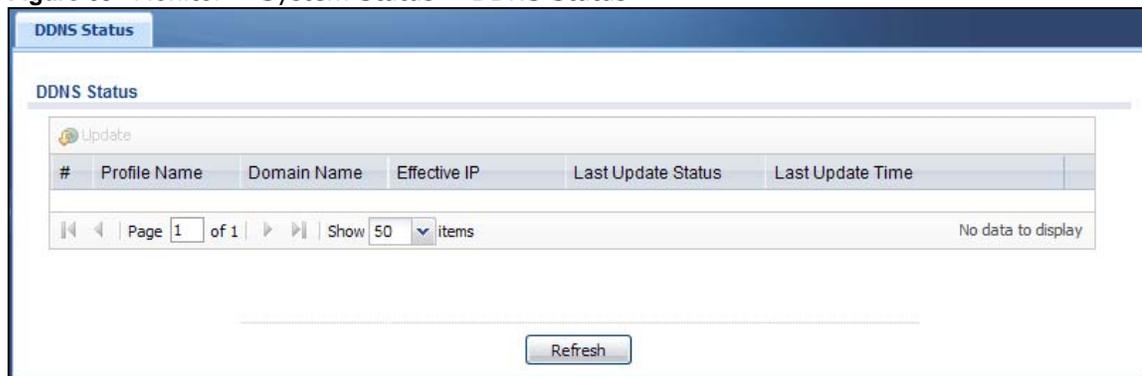
LABEL	DESCRIPTION
View	<p>Select how you want the information to be displayed. Choices are:</p> <p>sessions by users - display all active sessions grouped by user.</p> <p>sessions by services - display all active sessions grouped by service or protocol.</p> <p>sessions by source IP - display all active sessions grouped by source IP address.</p> <p>sessions by destination IP - display all active sessions grouped by destination IP address.</p> <p>all sessions - filter the active sessions by the User, Service, Source Address, and Destination Address, and display each session individually (sorted by user).</p>
Refresh	Click this button to update the information on the screen. The screen also refreshes automatically when you open and close the screen.
	The User , Service , Source Address , and Destination Address fields display if you view all sessions. Select your desired filter criteria and click the Search button to filter the list of sessions.
#	This field is a sequential value and is not associated with any entry.
User	This field displays when View is set to all sessions . Type the user whose sessions you want to view. It is not possible to type part of the user name or use wildcards in this field; you must enter the whole user name.
Service	This field displays when View is set to all sessions . Select the service or service group whose sessions you want to view. The UAG identifies the service by comparing the protocol and destination port of each packet to the protocol and port of each services that is defined. (See Chapter 40 on page 447 for more information about services.)
Source Address	This field displays when View is set to all sessions . Type the source IP address whose sessions you want to view. You cannot include the source port.
Destination Address	This field displays when View is set to all sessions . Type the destination IP address whose sessions you want to view. You cannot include the destination port.
Search	This button displays when View is set to all sessions . Click this button to update the information on the screen using the filter criteria in the User , Service , Source Address , and Destination Address fields.
User	<p>This field displays the user in each active session.</p> <p>If you are looking at the sessions by users (or all sessions) report, click + or - to display or hide details about a user's sessions.</p>
Service	<p>This field displays the protocol used in each active session.</p> <p>If you are looking at the sessions by services report, click + or - to display or hide details about a protocol's sessions.</p>
Source	<p>This field displays the source IP address and port in each active session.</p> <p>If you are looking at the sessions by source IP report, click + or - to display or hide details about a source IP address's sessions.</p>
Destination	<p>This field displays the destination IP address and port in each active session.</p> <p>If you are looking at the sessions by destination IP report, click + or - to display or hide details about a destination IP address's sessions.</p>
Rx	This field displays the amount of information received by the source in the active session.
Tx	This field displays the amount of information transmitted by the source in the active session.
Duration	This field displays the length of the active session in seconds.

Table 26 Monitor > System Status > Session Monitor (continued)

LABEL	DESCRIPTION
Page x of x	This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries.
Show x items	Select how many entries you want to display on each page.

7.6 The DDNS Status Screen

The **DDNS Status** screen shows the status of the UAG's DDNS domain names. Click **Monitor > System Status > DDNS Status** to open the following screen.

Figure 69 Monitor > System Status > DDNS Status

The following table describes the labels in this screen.

Table 27 Monitor > System Status > DDNS Status

LABEL	DESCRIPTION
Update	Click this to have the UAG update the profile to the DDNS server. The UAG attempts to resolve the IP address for the domain name.
#	This field is a sequential value and is not associated with any entry.
Profile Name	This field displays the descriptive profile name for this entry.
Domain Name	This field displays each domain name the UAG can route.
Effective IP	This is the (resolved) IP address of the domain name.
Last Update Status	This shows whether the last attempt to resolve the IP address for the domain name was successful or not. Updating means the UAG is currently attempting to resolve the IP address for the domain name.
Last Update Time	This shows when the last attempt to resolve the IP address for the domain name occurred (in year-month-day hour:minute:second format).

7.7 The IP/MAC Binding Monitor Screen

Click **Monitor > System Status > IP/MAC Binding** to open the **IP/MAC Binding Monitor** screen. This screen lists the devices that have received an IP address from UAG interfaces with IP/MAC binding enabled and have ever established a session with the UAG. Devices that have never established a session with the UAG do not display in the list.

Figure 70 Monitor > System Status > IP/MAC Binding

#	IP Address	Host Name	MAC Address	Last Access	Description
1	172.16.2.0	"twpc-01"	00:19:cb:32:be:ac	Thu May 23 03:21:04...	
2	172.16.1.1	"nwa5123-ni"	b0:b2:dc:6e:7f:24		

The following table describes the labels in this screen.

Table 28 Monitor > System Status > IP/MAC Binding

LABEL	DESCRIPTION
Interface	Select a UAG interface that has IP/MAC binding enabled to show to which devices it has assigned an IP address.
#	This is the index number of an IP/MAC binding entry.
IP Address	This is the IP address that the UAG assigned to a device.
Host Name	This field displays the name used to identify this device on the network (the computer name). The UAG learns these from the DHCP client requests.
MAC Address	This field displays the MAC address to which the IP address is currently assigned.
Last Access	This is when the device last established a session with the UAG through this interface.
Description	This field displays the descriptive name that helps identify the entry.
Refresh	Click this button to update the information in the screen.

7.8 The Login Users Screen

Use this screen to look at a list of the users currently logged into the UAG. To access this screen, click **Monitor > System Status > Login Users**.

Figure 71 Monitor > System Status > Login Users

#	Us...	Reauth/...	Sessio...	Remain...	Remain...	Type	IP Addr...	MAC	User Info	Acct. St...	RADI...
1	ad...	unlimite...	unlimited	n/a	- / -	http/https	172.16....	-	admin(...)	-	N/A

The following table describes the labels in this screen.

Table 29 Monitor > System Status > Login Users

LABEL	DESCRIPTION
Force Logout	Select a user ID and click this icon to end a user's session. Note: You cannot use this button to terminate a user's session when he/she accesses the UAG through the console port.
#	This field is a sequential value and is not associated with any entry.
User ID	This field displays the user name of each user who is currently logged in to the UAG.
Reauth/Lease Time	This field displays the amount of reauthentication time remaining and the amount of lease time remaining for each user. See Chapter 35 on page 399 .
Session Timeout	This field displays the total amount of time the account (authenticated by an external server) can use to log into the UAG or access the Internet through the UAG. This shows unlimited for an administrator account.
Remaining Time	This field displays the amount of Internet access time remaining for each account. This shows n/a for an administrator account.
Remaining Quota (T/U/D)	This field displays the remaining amount of data that can be transmitted or received by each account. You can see the amount of either data in both directions (Total) or upstream data (Upload) and downstream data (Download). This shows -/-/- for an administrator account.
Type	This field displays the way the user logged in to the UAG.
IP Address	This field displays the IP address of the computer used to log in to the UAG.
MAC	For an IEEE 802.1x or MAC authentication login, this field displays the MAC address of the user's computer. A "-" displays for other types of login.
User Info	This field displays the types of user accounts the UAG uses. If the user type is ext-user (external user), this field will show its external-group information when you move your mouse over it. If the external user matches two external-group objects, both external-group object names will be shown.
Acct. Status	For a login through the web authentication page, this field displays the accounting status of the account used to log into the UAG. Accounting-on means accounting is being performed for the user login. Accounting-off means accounting has stopped for this user login. A "-" displays if accounting is not enabled for this login.
RADIUS Profile Name	This field displays the name of the RADIUS profile used to authenticate the login through the web authentication page. N/A displays for logins that do not use the web portal or user agreement page and RADIUS server authentication.
Refresh	Click this button to update the information in the screen.

7.9 The Dynamic Guest Screen

Dynamic guest accounts can be automatically generated for guest users by using a connected statement printer or the web configurator with the guest-manager account (see [Section 26.3.1 on page 308](#) for more information). A dynamic guest account has a dynamically-created user name

and password. Guest users can log in with the dynamic guest accounts when connecting to an SSID for a specified time unit. Use this screen to look at a list of dynamic guest user accounts on the UAG's local database. To access this screen, click **Monitor > System Status > Dynamic Guest**.

Figure 72 Monitor > System Status > Dynamic Guest

#	Us...	Create Ti...	Rem...	Ti...	Expir...	Quot...	Remaini...	Ban...	Ch...	Payment I...	P...	User Role
1	hm...	2014-04...	000...	0...	201...	unli...	unlimite...	unli...	us...	cash	N/A	trial-users
2	oz5...	2014-04...	000...	0...	201...	unli...	unlimite...	unli...	us...	cash	N/A	billing-...

The following table describes the labels in this screen.

Table 30 Monitor > System Status > Dynamic Guest

LABEL	DESCRIPTION
Remove	Select an entry and click this button to remove it from the list. Note: If you delete a valid user account which is in use, the UAG ends the user session.
Refresh	Click this button to update the information in the screen.
#	This is the index number of the dynamic guest account in the list.
Status	This field displays whether an account expires or not.
Username	This field displays the user name of the account.
Create Time	This field displays when the account was created.
Remaining Time	This field displays the amount of Internet access time remaining for each account.
Time Period	This field displays the total amount of time the account can use to access the Internet through the UAG.
Expiration Time	This field displays the date and time the account becomes invalid. Note: Once the time allocated to a dynamic account is used up or a dynamic account remains un-used after the expiration time, the account is deleted from the account list.
Quota (T/U/D)	This field displays how much data in both directions (T otal) or upstream data (U pload) and downstream data (D ownload) can be transmitted through the WAN interface before the account expires.
Remaining Quota (T/U/D)	This field displays the remaining amount of data that can be transmitted or received by each account. You can see the amount of either data in both directions (T otal) or upstream data (U pload) and downstream data (D ownload).
Bandwidth (U/D)	This field displays the maximum upstream (U pload) and downstream (D ownload) bandwidth allowed for the user account in kilobits per second.
Charge	This field displays the total cost of the account.
Payment Info	This field displays the method of payment for each account.
Phone Num	This field displays the mobile phone number for the account.
User Role	This field displays the role of the account.
Refresh	Click this button to update the information in the screen.

The following table describes the icons in this screen.

Table 31 Monitor > System Status > Dynamic Guest Icons

LABEL	DESCRIPTION
	This guest account is un-used.
	This guest account is in use and online.
	This guest account has been used but is offline now.
	This guest account expired.
	This guest account has been deleted.

7.10 The UPnP Port Status Screen

Use this screen to look at the NAT port mapping rules that UPnP creates on the UAG. To access this screen, click **Monitor > System Status > UPnP Port Status**.

Figure 73 Monitor > System Status > UPnP Port Status



The following table describes the labels in this screen.

Table 32 Monitor > System Status > UPnP Port Status

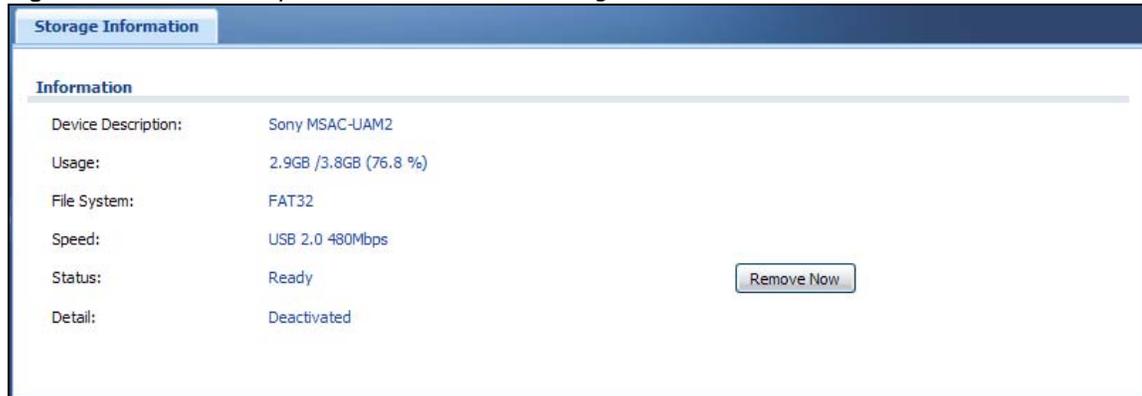
LABEL	DESCRIPTION
Remove	Select an entry and click this button to remove it from the list.
#	This is the index number of the UPnP-created NAT mapping rule entry.
Remote Host	This field displays the source IP address (on the WAN) of inbound IP packets. Since this is often a wildcard, the field may be blank. When the field is blank, the UAG forwards all traffic sent to the External Port on the WAN interface to the Internal Client on the Internal Port . When this field displays an external IP address, the NAT rule has the UAG forward inbound packets to the Internal Client from that IP address only.
External Port	This field displays the port number that the UAG "listens" on (on the WAN port) for connection requests destined for the NAT rule's Internal Port and Internal Client . The UAG forwards incoming packets (from the WAN) with this port number to the Internal Client on the Internal Port (on the LAN). If the field displays "0", the UAG ignores the Internal Port value and forwards requests on all external port numbers (that are otherwise unmapped) to the Internal Client .

Table 32 Monitor > System Status > UPnP Port Status (continued)

LABEL	DESCRIPTION
Protocol	This field displays the protocol of the NAT mapping rule (TCP or UDP).
Internal Port	This field displays the port number on the Internal Client to which the UAG should forward incoming connection requests.
Internal Client	This field displays the DNS host name or IP address of a client on the LAN. Multiple NAT clients can use a single port simultaneously if the internal client field is set to 255.255.255.255 for UDP mappings.
Internal Client Type	This field displays the type of the client application on the LAN.
Description	This field displays a text explanation of the NAT mapping rule.
Delete All	Click this to remove all mapping rules from the NAT table.
Refresh	Click this button to update the information in the screen.

7.11 The USB Storage Screen

This screen displays information about a connected USB storage device. Click **Monitor > System Status > USB Storage** to display this screen.

Figure 74 Monitor > System Status > USB Storage

The following table describes the labels in this screen.

Table 33 Monitor > System Status > USB Storage

LABEL	DESCRIPTION
Device description	This is a basic description of the type of USB device.
Usage	This field displays how much of the USB storage device's capacity is currently being used out of its total capacity and what percentage that makes.
Filesystem	This field displays what file system the USB storage device is formatted with. This field displays Unknown if the file system of the USB storage device is not supported by the UAG, such as NTFS.
Speed	This field displays the connection speed the USB storage device supports.

Table 33 Monitor > System Status > USB Storage (continued)

LABEL	DESCRIPTION
Status	<p>Ready - you can have the UAG use the USB storage device.</p> <p>Click Remove Now to stop the UAG from using the USB storage device so you can remove it.</p> <p>Unused - the connected USB storage device was manually unmounted by using the Remove Now button or for some reason the UAG cannot mount it.</p> <p>Click Use It to have the UAG mount a connected USB storage device. This button is grayed out if the file system is not supported (unknown) by the UAG.</p> <p>none - no USB storage device is connected.</p>
Detail	<p>This field displays any other information the UAG retrieves from the USB storage device.</p> <p>Deactivated - the use of a USB storage device is disabled (turned off) on the UAG.</p> <p>OutOfSpace - the available disk space is less than the disk space full threshold (see Section 46.2 on page 487 for how to configure this threshold).</p> <p>Mounting - the UAG is mounting the USB storage device.</p> <p>Removing - the UAG is unmounting the USB storage device.</p> <p>none - the USB device is operating normally or not connected.</p>

7.12 The Ethernet Neighbor Screen

The **Ethernet Neighbor** screen allows you to view the UAG's neighboring devices in one place.

It uses Smart Connect, that is Link Layer Discovery Protocol (LLDP) for discovering and configuring LLDP-aware devices in the same broadcast domain as the UAG that you're logged into using the web configurator.

LLDP is a layer-2 protocol that allows a network device to advertise its identity and capabilities on the local network. It also allows the device to maintain and store information from adjacent devices which are directly connected to the network device. This helps you discover network changes and perform necessary network reconfiguration and management.

Note: Enable Smart Connect in the **System > ZON** screen.

See also **System > ZON** for more information on the ZyXEL One Network (ZON) utility that uses the ZyXEL Discovery Protocol (ZDP) for discovering and configuring ZDP-aware ZyXEL devices in the same network as the computer on which the ZON utility is installed.

Click **Monitor > System Status > Ethernet Neighbor** to see the following screen.

Figure 75 Monitor > System Status > Ethernet Neighbor

The screenshot shows the 'Ethernet Neighbor' page. At the top, there is a header 'Ethernet Neighbor'. Below it is a table with the following columns: Local Port(Descri..., Model Name, System Name, Firmware Version, Port(Description), IP Address, and MAC. The table is currently empty, with the text 'No data to display' at the bottom right. Below the table is a pagination control showing 'Page 1 of 1' and 'Show 50 items'. At the bottom center, there is a 'Refresh' button.

The following table describes the labels in this screen.

Table 34 Monitor > System Status > Ethernet Neighbor

LABEL	DESCRIPTION
Local Port (Description)	This field displays the port of the UAG, on which the neighboring device is discovered. For UAGs that support Port Role , if ports 3 to 4 are grouped together and there is a connection to P4 only, the UAG will display P3 as the first interface port number (even though there is no connection to that port).
Model Name	This field displays the model name of the discovered device.
System Name	This field displays the system name of the discovered device.
Firmware Version	This field displays the firmware version of the discovered device.
Port (Description)	This field displays the first internal port on the discovered device. Internal is an interface type displayed in the Network > Interface > Ethernet > Edit screen. For example, if P1 and P2 are WAN, P3 to P4 are LAN and P5 is DMZ, then UAG will display P3 as the first internal interface port number. For UAGs that support Port Role , if ports 3 to 4 are grouped together and there is a connection to P4 only, the UAG will display P3 as the first internal interface port number (even though there is no connection to that port).
IP Address	This field displays the IP address of the discovered device.
MAC	This field displays the MAC address of the discovered device.
Refresh	Click this button to update the information in the screen.

7.13 The AP List Screen

Use this screen to view which APs are currently connected to the UAG. To access this screen, click **Monitor > Wireless > AP Information > AP List**.

Figure 76 Monitor > Wireless > AP Information > AP List

The following table describes the labels in this screen.

Table 35 Monitor > Wireless > AP Information > AP List

LABEL	DESCRIPTION
Add to Mgmt AP List	Click this to add the selected AP to the managed AP list.
More Information	Click this to view a daily station count about the selected AP. The count records station activity on the AP over a consecutive 24 hour period.
#	This is the AP's index number in this list.
Status	This visually displays the AP's connection status with icons. For details on the different Status states, see the next table.
Description	This displays the AP's associated description. The default description is "AP-" + the AP's MAC Address.
Registration	This indicates whether the AP is registered with the managed AP list.
CPU Usage	This displays what percentage of the AP's processing capability is currently being used.
IP Address	This displays the AP's IP address.
MAC Address	This displays the AP's MAC address.
Model	This displays the AP's model number.
Mgmt. VLAN ID(AC/AP)	This displays the Access Controller (the UAG) management VLAN ID setting for the AP and the runtime management VLAN ID setting on the AP. VLAN Conflict displays if the AP's management VLAN ID does not match the UAG's management VLAN ID setting for the AP. This field displays n/a if the UAG cannot get VLAN information from the AP.
Station	This displays the number of stations (aka wireless clients) associated with the AP.
Recent On-line Time	This displays the most recent time the AP came on-line. N/A displays if the AP has not come on-line since the UAG last started up.
Last Off-line Time	This displays the most recent time the AP went off-line. N/A displays if the AP has either not come on-line or gone off-line since the UAG last started up.

Table 35 Monitor > Wireless > AP Information > AP List (continued)

LABEL	DESCRIPTION
LED Status	<p>This displays the AP LED status.</p> <p>N/A displays if the AP does not support LED suppression mode and/or have a locator LED to show the actual location of the AP.</p> <p>A gray LED icon signifies that the AP LED suppression mode is enabled. All the LEDs of the AP will turn off after the AP is ready.</p> <p>A green LED icon signifies that the AP LED suppression mode is disabled and the AP LEDs stay lit after the AP is ready.</p> <p>A sun icon signifies that the AP's locator LED is blinking.</p> <p>A circle signifies that the AP's locator LED is extinguished.</p>
Refresh	Click this button to update the information in the screen.

The following table describes the icons in this screen.

Table 36 Monitor > Wireless > AP Information > AP List Icons

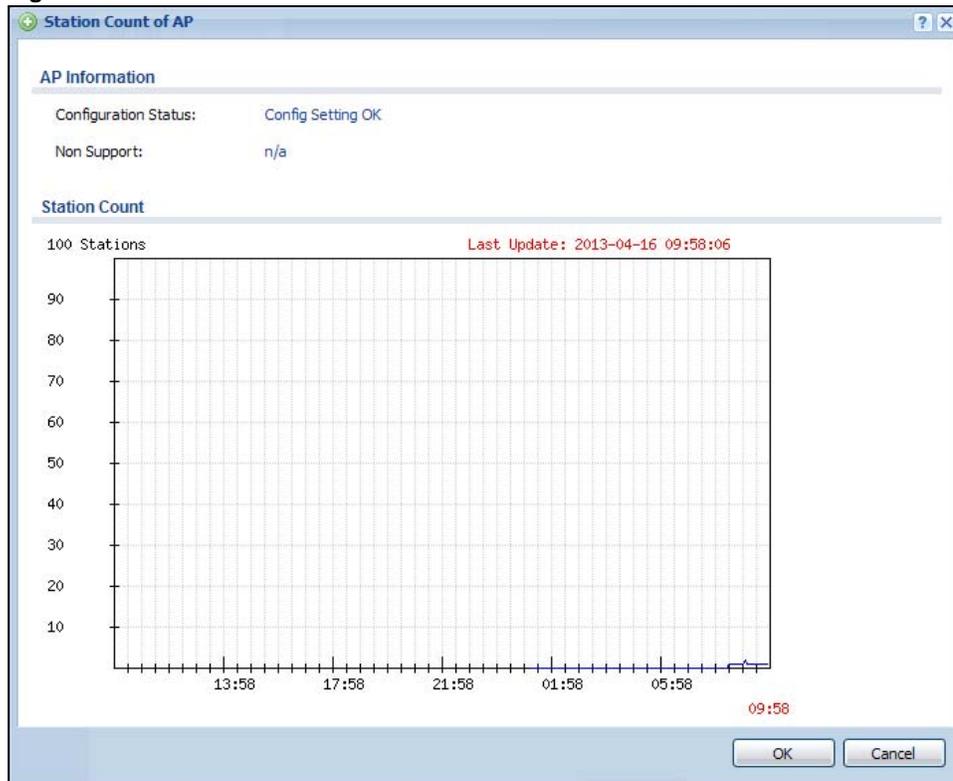
LABEL	DESCRIPTION
	This AP is not on the management list.
	This AP is on the management list and online.
	This AP is in the process of having its firmware updated.
	This AP is on the management list but offline.
	<p>This indicates one of the following cases:</p> <ul style="list-style-type: none"> This AP has a runtime management VLAN ID setting that conflicts with the VLAN ID setting on the Access Controller (the UAG). A setting the UAG assigns to this AP does not match the AP's capability.

7.13.1 Station Count of AP

Use this screen to look at station statistics for the connected AP. To access this screen, select an entry and click the **More Information** button in the **AP List** screen. Use this screen to look at

configuration information, port status and station statistics for the connected AP. To access this screen, select an entry and click the **More Information** button in the **AP List** screen.

Figure 77 Monitor > Wireless > AP Information > AP List > Station Count of AP



The following table describes the labels in this screen.

Table 37 Monitor > Wireless > AP Information > AP List > Station Count of AP

LABEL	DESCRIPTION
Configuration Status	This displays whether or not any of the AP's configuration is in conflict with the UAG's settings for the AP.
Non Support	If any of the AP's configuration conflicts with the UAG's settings for the AP, this field displays which configuration conflicts. It displays n/a if none of the AP's configuration conflicts with the UAG's settings for the AP.
Port Status	
Port	This shows the name of the physical Ethernet port on the UAG.
Status	This field displays the current status of each physical port on the AP. Down - The port is not connected. Speed / Duplex - The port is connected. This field displays the port speed and duplex setting (Full or Half).
PVID	This shows the port's PVID. A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines.
Up Time	This field displays how long the physical port has been connected.
VLAN Configuration	
Name	This shows the name of the VLAN.

Table 37 Monitor > Wireless > AP Information > AP List > Station Count of AP (continued)

LABEL	DESCRIPTION
Status	This displays whether or not the VLAN is activated.
VID	This shows the VLAN ID number.
Member	This field displays the Ethernet port(s) that is a member of this VLAN.
Station Count	
	The y-axis represents the number of connected stations.
	The x-axis shows the time over which a station was connected.
Last Update	This field displays the date and time the information in the window was last updated.

7.14 The Radio List Screen

Use this screen to view statistics about the wireless radio transmitters in each of the APs connected to the UAG. To access this screen, click **Monitor > Wireless > AP Information > Radio List**.

Figure 78 Monitor > Wireless > AP Information > Radio List

#	L...	AP D...	Model	MAC...	R...	O...	Profile	Freq...	Cha...	Tx P...	S...	Rx PKT	Tx PKT	Rx F...	Tx R...
1	-	AP-...	NW...	B0:B...	1	AP	default	2.4G...	6	23 d...	0	1977	77017	189...	472...
2	-	AP-...	NW...	B0:B...	2	AP	defa...	5GHz	36/40	23 d...	1	11326	26082	195...	223...

Page 1 of 1 | Show 50 items | Displaying 1 - 2 of 2

Refresh

The following table describes the labels in this screen.

Table 38 Monitor > Wireless > AP Information > Radio List

LABEL	DESCRIPTION
More Information	Click this to view additional information about the selected radio's SSID(s), wireless traffic and wireless clients. Information spans a 24 hour period.
#	This is the radio's index number in this list.
Loading	This indicates the AP's load balance status (UnderLoad or OverLoad) when load balancing is enabled on the AP. Otherwise, it shows - when load balancing is disabled or the radio is in monitor mode.
AP Description	This displays the description of the AP to which the radio belongs.
Model	This displays the model of the AP to which the radio belongs.
MAC Address	This displays the MAC address of the radio.
Radio	This indicates the radio number on the AP to which it belongs.
OP Mode	This indicates the radio's operating mode, such as AP (access point).
Profile	This indicates the profile name to which the radio belongs.

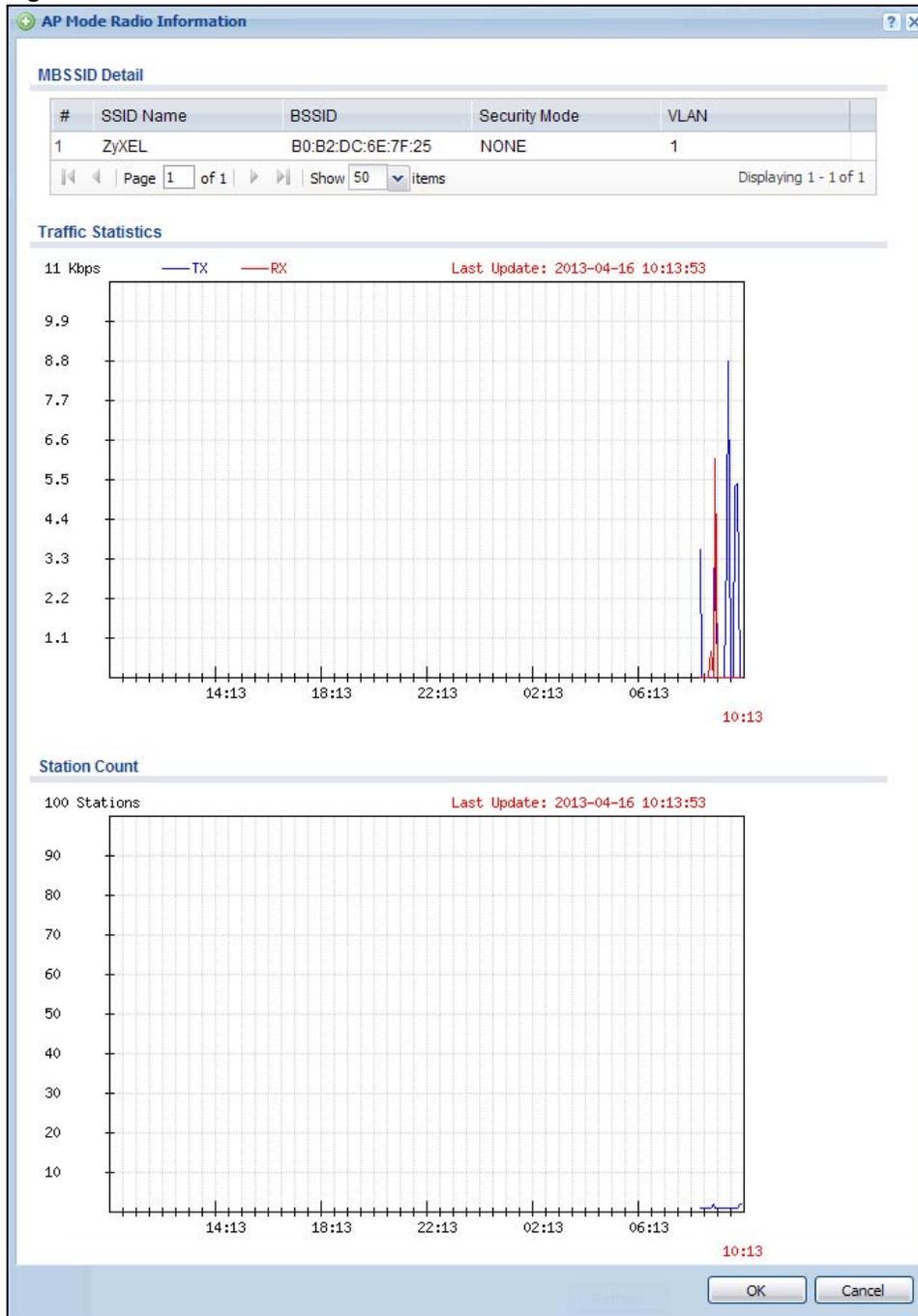
Table 38 Monitor > Wireless > AP Information > Radio List (continued)

LABEL	DESCRIPTION
Frequency Band	This indicates the wireless frequency currently being used by the radio. This shows - when the radio is in monitor mode.
Channel ID	This indicates the radio's channel ID.
Tx Power	This shows the radio's output power (in dBm).
Station	This displays the number of stations (aka wireless clients) associated with the radio.
Rx PKT	This displays the total number of packets received by the radio.
Tx PKT	This displays the total number of packets transmitted by the radio.
Rx FCS Error Count	This indicates the number of received packet errors accrued by the radio.
Tx Retry Count	This indicates the number of times the radio has attempted to re-transmit packets.

7.14.1 AP Mode Radio Information

This screen allows you to view detailed information about a selected radio's SSID(s), wireless traffic and wireless clients for the preceding 24 hours. To access this window, select an entry and click the **More Information** button in the **Radio List** screen.

Figure 79 Monitor > Wireless > AP Information > Radio List > AP Mode Radio Information



The following table describes the labels in this screen.

Table 39 Monitor > Wireless > AP Info > Radio List > AP Mode Radio Information

LABEL	DESCRIPTION
MBSSID Detail	This list shows information about the SSID(s) that is associated with the radio over the preceding 24 hours.
#	This is the items sequential number in the list. It has no bearing on the actual data in this list.
SSID Name	This displays an SSID associated with this radio. There can be up to eight maximum.
BSSID	This displays the MAC address associated with the SSID.
Security Mode	This displays the security mode in which the SSID is operating.
VLAN	This displays the VLAN ID associated with the SSID.
Traffic Statistics	This graph displays the overall traffic information about the radio over the preceding 24 hours.
y-axis	This axis represents the amount of data moved across this radio in megabytes per second.
x-axis	This axis represents the amount of time over which the data moved across this radio.
Station Count	This graph displays information about all the wireless clients that have connected to the radio over the preceding 24 hours.
y-axis	The y-axis represents the number of connected wireless clients.
x-axis	The x-axis shows the time over which a wireless client was connected.
Last Update	This field displays the date and time the information in the window was last updated.
OK	Click this to close this window.
Cancel	Click this to close this window.

7.15 The Station List Screen

Use this screen to view statistics pertaining to the associated stations (or "wireless clients"). Click **Monitor > Wireless > Station Info** to access this screen.

Figure 80 Monitor > Wireless > Station List



The screenshot shows the 'Station List' interface. At the top, there is a tab labeled 'Station List'. Below the tab, the title 'Station List' is displayed. A table lists wireless clients with the following columns: #, MAC Addr..., Asso..., SSID Name, Secur..., Signa..., Cha..., B..., IP Ad..., Tx..., R..., Tx, Rx, and Associati... The table contains one entry for SSID Name: ZyXEL (1 Station). Below the table, there is a 'Refresh' button.

#	MAC Addr...	Asso...	SSID Name	Secur...	Signa...	Cha...	B...	IP Ad...	Tx...	R...	Tx	Rx	Associati...
SSID Name: ZyXEL (1 Station)													
1	40:6F:2A:...	AP-B...	ZyXEL	NONE	-64d...	36	5G	172.1...	47M	42M	1...	1...	2014/10/...

The following table describes the labels in this screen.

Table 40 Monitor > Wireless > Station List

LABEL	DESCRIPTION
SSID Name	This field displays the SSID name with which at least one station is associated. Click + or - to display or hide details about wireless stations that connected to the SSID.
#	This is the station's index number in this list.
MAC Address	This is the station's MAC address.
Associated AP	This indicates the AP through which the station is connected to the network.
SSID Name	This indicates the name of the wireless network to which the station is connected. A single AP can have multiple SSIDs or networks.
Security Mode	This indicates which secure encryption methods is being used by the station to connect to the network.
Signal Strength	This indicates the strength of the signal. The signal strength mainly depends on the antenna output power and the distance between the station and the AP.
Channel	This indicates the number the channel used by the station to connect to the network.
Band	This indicates the frequency band which is currently being used by the station.
IP Address	This is the station's IP address. An 169.x.x.x IP address is a private IP address that means the station didn't get the IP address from a DHCP server.
Tx Rate	This indicates the current data transmission rate of the station.
Rx Rate	This indicates the current data receiving rate of the station.
Tx	This field displays the number of packets transmitted from the station.
Rx	This field displays the number of packets received by the station.
Association Time	This displays the time a wireless station first associated with the AP.
Refresh	Click this to refresh the items displayed on this page.

7.16 Detected Device

Use this screen to view information about wireless devices detected by the AP. Click **Monitor > Wireless > Detected Device** to access this screen.

Note: At least one radio of the APs connected to the UAG must be set to monitor mode (in the **Configuration > Wireless > AP Management** screen) in order to detect other wireless devices in its vicinity.

Figure 81 Monitor > Wireless > Detected Device

#	Stat...	Dev...	Role	MAC Address	SSID Name	Channe...	802...	Sec...	Descrip...	Last Seen
1	💡	infr...		00:13:49:00:00:07	Guest	36	IEE...	None		Tue Oct ...
2	💡	infr...	friendly-ap	00:13:49:01:12:25	ZyXEL	36	IEE...	None		Tue Oct ...
3	💡	infr...		00:13:49:01:23:9A	ZyXEL	36	IEE...	None		Tue Oct ...
4	💡	infr...		00:13:49:43:21:03	ZyXEL	36	IEE...	None		Tue Oct ...
5	💡	infr...		00:1C:28:D3:6D:...	default_extra	40	IEE...	WP...		Tue Oct ...
6	💡	infr...	rogue-ap	02:10:49:01:12:25		36	IEE...	TKI...		Tue Oct ...
7	💡	infr...		02:12:49:01:12:25		36	IEE...	WP...		Tue Oct ...
8	💡	infr...		08:96:D7:75:E9:11	FRIT	36	IEE...	WP...		Tue Oct ...
9	💡	infr...		10:7B:EF:D3:E4:48	ZyXEL	36	IEE...	None		Tue Oct ...
10	💡	infr...		10:7B:EF:D3:E5:...	ZyXEL	36	IEE...	None		Tue Oct ...
11	💡	infr...		28:CF:DA:B6:4A:...	marcom	149	IEE...	WP...		Tue Oct ...
12	💡	infr...		4C:9E:FF:71:09:0E	ZyXEL	36	IEE...	None		Tue Oct ...

The following table describes the labels in this screen.

Table 41 Monitor > Wireless > Rogue AP > Detected Device

LABEL	DESCRIPTION
Mark as Rogue AP	Click this button to mark the selected AP as a rogue AP. A rogue AP can be contained in the Configuration > Wireless > MON Mode screen (Section 9.4 on page 144).
Mark as Friendly AP	Click this button to mark the selected AP as a friendly AP. For more on managing friendly APs, see the Configuration > Wireless > MON Mode screen (Section 9.4 on page 144).
#	This is the station's index number in this list.
Status	This indicates the detected device's status.
Device	This indicates the detected device's network type (such as infrastructure or ad-hoc).
Role	This indicates the detected device's role (such as friendly or rogue).
MAC Address	This indicates the detected device's MAC address.
SSID Name	This indicates the detected device's SSID.
Channel ID	This indicates the detected device's channel ID.
802.11 Mode	This indicates the 802.11 mode (a/b/g/n) transmitted by the detected device.
Security	This indicates the encryption method (if any) used by the detected device.
Description	This displays the detected device's description. For more on managing friendly and rogue APs, see the Configuration > Wireless > MON Mode screen (Section 9.4 on page 144).
Last Seen	This indicates the last time the device was detected by the UAG.
Refresh	Click this to refresh the items displayed on this page.

7.17 The Printer Status Screen

This screen displays information about the connected statement printer, such as SP350E. Click **Monitor > Printer Status** to display this screen.

Figure 82 Monitor > Printer Status

The screenshot shows a web interface titled 'Printer Status'. Below the title is a 'Printer List' section containing a table with the following columns: #, Registration, IPv4 Address, Update Time, Status, Description, Nickname, Firmware V..., and MAC. The table is currently empty, and the text 'No data to display' is visible at the bottom right of the table area. There are also navigation controls for the table, including 'Page 1 of 1' and 'Show 50 items'.

The following table describes the labels in this screen.

Table 42 Monitor > Printer Status

LABEL	DESCRIPTION
#	This is the index number of the printer in the list.
Registration	This field shows that the printer is added to the managed printer list (Mgmt Printer).
IPv4 Address	This field displays the IP address of the printer that you configured in the Configuration > Printer > Printer Manager screen.
Update Time	This field displays the date and time the UAG last synchronized with the printer. This shows n/a when the printer status is sync fail .
Status	This field displays whether the UAG can connect to the printer and update the printer information.
Description	This field displays the descriptive name of the printer that you configured in the Configuration > Printer > Printer Manager screen.
Nickname	This field displays the nickname of the printer that you configured in the Configuration > Printer > Printer Manager screen.
Firmware Version	This field displays the model number and firmware version of the printer. This shows n/a when the printer status is sync fail .
MAC	This field displays the MAC address of the printer.

7.18 The VPN 1-1 Mapping Status Screen

This screen displays the status of the active users to which the UAG applied a VPN 1-1 mapping rule.

Click **Monitor > VPN 1-1 Mapping** to open the following screen.

Figure 83 Monitor > VPN 1-1 Mapping

The following table describes the labels in this screen.

Table 43 Monitor > VPN 1-1 Mapping

LABEL	DESCRIPTION
Force Logout	Select a user ID and click this icon to end a user's session.
#	This field is a sequential value and is not associated with any entry.
User ID	This field displays the user name of each user who is currently logged into the UAG and matches a pre-configured VPN 1-1 mapping rule.
IP Address	This field displays the IP address of the computer used to log in to the UAG.
Mapping IP / Interface	This field displays the public IP address that the UAG assigns to the user according to the matched VPN 1-1 mapping rule. It also displays the interface through which the outgoing traffic is forwarded.
Rule	This field displays the index number of the matched VPN 1-1 mapping rule that you configured in the Configuration > VPN 1-1 Mapping screen.
Pool	This field displays the name of the pool profile that you configured for the VPN 1-1 mapping rule.
Refresh	Click this button to update the information in the screen.

7.18.1 VPN 1-1 Mapping Statistics

This screen shows statistics for each of the VPN 1-1 mapping rules. Click **Monitor > VPN 1-1 Mapping > Statistics** to display this screen.

Figure 84 Monitor > VPN 1-1 Mapping > Statistics

#	Status	User / Group	Pool Profile	Assigned / Failed / Peak Usage
1	🔦	Client-A	POOL-1	0 / 0 / 1
2	🔦	user1	POOL-1	2 / 0 / 2

The following table describes the labels in this screen.

Table 44 Monitor > VPN 1-1 Mapping > Statistics

LABEL	DESCRIPTION
#	This field displays the rule's index number in the list.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
User/Group	This field displays the name of the user or user group object to which the rule is applied.
Pool Profile	This field displays the name of the IP address pool profile to which the rule is applied.
Assigned/Failed/ Peak Usage	This field displays how many times the UAG applied the rule to a user successfully or failed to apply the rule to a user. This also shows the maximum number of times the UAG has applied the rule to a user successfully.

7.19 The IPsec Monitor Screen

You can use this screen to display and to manage active IPsec SAs. To access this screen, click **Monitor > VPN Monitor > IPsec**. The following screen appears. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 85 Monitor > VPN Monitor > IPsec



Each field is described in the following table.

Table 45 Monitor > VPN Monitor > IPsec

LABEL	DESCRIPTION
Name	Enter the name of a IPsec SA here and click Search to find it (if it is associated). You can use a keyword or regular expression. Use up to 30 alphanumeric and <code>_+-.(!\$*^:~ {}[]<>)</code> characters. See Section 7.19.1 on page 121 for more details.
Policy	Enter the IP address(es) or names of the local and remote policies for an IPsec SA and click Search to find it. You can use a keyword or regular expression. Use up to 30 alphanumeric and <code>_+-.(!\$*^:~ {}[]<>)</code> characters. See Section 7.19.1 on page 121 for more details.
Search	Click this button to search for an IPsec SA that matches the information you specified above.
Disconnect	Select an IPsec SA and click this button to disconnect it.

Table 45 Monitor > VPN Monitor > IPSec (continued)

LABEL	DESCRIPTION
Connectivity Check	Select an IPSec SA and click this button to check the connection to the remote IPSec router to make sure it is still available.
Page x of x	This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries.
Show x items	Select how many entries you want to display on each page.
#	This field is a sequential value, and it is not associated with a specific SA.
Name	This field displays the name of the IPSec SA.
Policy	This field displays the content of the local and remote policies for this IPSec SA. The IP addresses, not the address objects, are displayed.
IKE Name	This field displays the Internet Key Exchange (IKE) name.
Cookies	This field displays the cookies information that initiates the IKE.
My Address	This field displays the IP address of local computer.
Secure Gateway	This field displays the secure gateway information.
Up Time	This field displays how many seconds the IPSec SA has been active.
Timeout	This field displays how many seconds remain in the SA life time, before the UAG automatically disconnects the IPSec SA.
Inbound (Bytes)	This field displays the amount of traffic that has gone through the IPSec SA from the remote IPSec router to the UAG since the IPSec SA was established.
Outbound (Bytes)	This field displays the amount of traffic that has gone through the IPSec SA from the UAG to the remote IPSec router since the IPSec SA was established.
Refresh	Click Refresh to update the information in the display.

7.19.1 Regular Expressions in Searching IPSec SAs

A question mark (?) lets a single character in the VPN connection or policy name vary. For example, use "a?c" (without the quotation marks) to specify abc, acc and so on.

Wildcards (*) let multiple VPN connection or policy names match the pattern. For example, use "*abc" (without the quotation marks) to specify any VPN connection or policy name that ends with "abc". A VPN connection named "testabc" would match. There could be any number (of any type) of characters in front of the "abc" at the end and the VPN connection or policy name would still match. A VPN connection or policy name named "testacc" for example would not match.

A * in the middle of a VPN connection or policy name has the UAG check the beginning and end and ignore the middle. For example, with "abc*123", any VPN connection or policy name starting with "abc" and ending in "123" matches, no matter how many characters are in between.

The whole VPN connection or policy name has to match if you do not use a question mark or asterisk.

7.20 The App Patrol Screen

Application patrol provides a convenient way to manage the use of various applications on the network. It manages general protocols (for example, HTTP and FTP) and instant messenger (IM), peer-to-peer (P2P), Voice over IP (VoIP), and streaming (RSTP) applications. You can even control

the use of a particular application's individual features (like text messaging, voice, video conferencing, and file transfers).

Click **Monitor > UTM Statistics > App Patrol** to display the following screen. This screen displays **Application Patrol** statistics based on the **App Patrol** profiles bound to **Security Policy** profiles.

Figure 86 Monitor > UTM Statistics > App Patrol

The following table describes the labels in this screen.

Table 46 Monitor > UTM Statistics > App Patrol

LABEL	DESCRIPTION
Collect Statistics	Select this check box to have the UAG collect app patrol statistics. The collection starting time displays after you click Apply . All of the statistics in this screen are for the time period starting at the time displayed here. The format is year, month, day and hour, minute, second. All of the statistics are erased if you restart the UAG or click Flush Data . Collecting starts over and a new collection start time displays.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.
Refresh	Click this button to update the report display.
Flush Data	Click this button to discard all of the screen's statistics and update the report display.
App Patrol Statistics	
#	This field is a sequential value, and it is not associated with a specific App Patrol session.
Application	This is the protocol.
Forwarded Data (KB)	This is how much of the application's traffic the UAG has sent (in kilobytes).
Dropped Data (KB)	This is how much of the application's traffic the UAG has discarded without notifying the client (in kilobytes). This traffic was dropped because it matched an application policy set to "drop".
Rejected Data (KB)	This is how much of the application's traffic the UAG has discarded and notified the client that the traffic was rejected (in kilobytes). This traffic was rejected because it matched an application policy set to "reject".
Matched Auto Connection	This is how much of the application's traffic the UAG identified by examining the IP payload.

Table 46 Monitor > UTM Statistics > App Patrol

LABEL	DESCRIPTION
Inbound Kbps	This field displays the amount of the application's traffic that has gone to the UAG (in kilo bits per second).
Outbound Kbps	This field displays the amount of the application's traffic that has gone from the UAG (in kilo bits per second).

7.21 The Content Filter Screen

Click **Monitor > UTM Statistics > Content Filter** to display the following screen. This screen displays content filter statistics.

Figure 87 Monitor > UTM Statistics > Content Filter

The screenshot shows a web interface for a 'Report' on 'Content Filter'. It includes sections for 'General Settings', 'Web Request Statistics', 'Category Hit Summary', and 'Block Hit Summary'. All statistics are currently at zero.

General Settings	
<input checked="" type="checkbox"/> Collect Statistics	since 2014-10-08 08:37:21 to 2014-10-08 09:14:05
<input type="button" value="Apply"/>	<input type="button" value="Reset"/>
<input type="button" value="Refresh"/>	<input type="button" value="Flush Data"/>

Web Request Statistics	
Total Web Pages Inspected:	0
Blocked:	0
Warned:	0
Passed:	0

Category Hit Summary	
Security Threat (unsafe):	0
Managed Web Pages:	0

Block Hit Summary	
Web Pages Warned by Category Service:	0
Web Pages Blocked by Custom Service:	0
Restricted Web Features:	0
Forbidden Web Sites:	0
URL Keywords:	0

Visit [Report Server](#) for Detail

The following table describes the labels in this screen.

Table 47 Monitor > UTM Statistics > Content Filter

LABEL	DESCRIPTION
General Settings	
Collect Statistics	Select this check box to have the UAG collect content filtering statistics. The collection starting time displays after you click Apply . All of the statistics in this screen are for the time period starting at the time displayed here. The format is year, month, day and hour, minute, second. All of the statistics are erased if you restart the UAG or click Flush Data . Collecting starts over and a new collection start time displays.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.
Refresh	Click this button to update the report display.
Flush Data	Click this button to discard all of the screen's statistics and update the report display.
Web Request Statistics	
Total Web Pages Inspected	This field displays the number of web pages that the UAG's content filter feature has checked.
Blocked	This is the number of web pages that the UAG blocked access.
Warned	This is the number of web pages for which the UAG displayed a warning message to the access requesters.
Passed	This is the number of web pages to which the UAG allowed access.
Category Hit Summary	
Security Threat (unsafe)	This is the number of requested web pages that the UAG's content filtering service identified as posing a threat to users.
Managed Web Pages	This is the number of requested web pages that the UAG's content filtering service identified as belonging to a category that was selected to be managed.
Block Hit Summary	
Web Pages Warned by Category Service	This is the number of web pages that matched an external database content filtering category selected in the UAG and for which the UAG displayed a warning before allowing users access.
Web Pages Blocked by Custom Service	This is the number of web pages to which the UAG did not allow access due to the content filtering custom service configuration.
Restricted Web Features	This is the number of web pages to which the UAG limited access or removed cookies due to the content filtering custom service's restricted web features configuration.
Forbidden Web Sites	This is the number of web pages to which the UAG did not allow access because they matched the content filtering custom service's forbidden web sites list.
URL Keywords	This is the number of web pages to which the UAG did not allow access because they contained one of the content filtering custom service's list of forbidden keywords.
Report Server	Click this link to go to http://www.myZyXEL.com where you can view content filtering reports after you have activated the category-based content filtering subscription service.

7.22 The Log Screen

Log messages are stored in two separate logs, one for regular log messages and one for debugging messages. In the regular log, you can look at all the log messages by selecting **All Logs**, or you can select a specific category of log messages (for example, Security Policy Control or User). You can also look at the debugging log by selecting **Debug Log**. All debugging messages have the same priority.

To access this screen, click **Monitor > Log**. The log is displayed in the following screen.

Note: When a log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

- The maximum possible number of log messages in the UAG varies by model.

Events that generate an alert (as well as a log message) display in red. Regular logs display in black. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 88 Monitor > Log

The following table describes the labels in this screen.

Table 48 Monitor > Log

LABEL	DESCRIPTION
Show Filter / Hide Filter	Click this button to show or hide the filter settings. If the filter settings are hidden, the Display , Email Log Now , Refresh , and Clear Log fields are available. If the filter settings are shown, the Display , Priority , Source Address , Destination Address , Source Interface , Destination Interface , Service , Keyword , Protocol and Search fields are available.
Display	Select the category of log message(s) you want to view. You can also view All Logs at one time, or you can view the Debug Log .

Table 48 Monitor > Log (continued)

LABEL	DESCRIPTION
Priority	This displays when you show the filter. Select the priority of log messages to display. The log displays the log messages with this priority or higher. Choices are: any , emerg , alert , crit , error , warn , notice , and info , from highest priority to lowest priority. This field is read-only if the Category is Debug Log .
Source Address	This displays when you show the filter. Type the source IP address of the incoming packet that generated the log message. Do not include the port in this filter.
Destination Address	This displays when you show the filter. Type the IP address of the destination of the incoming packet when the log message was generated. Do not include the port in this filter.
Source Interface	This displays when you show the filter. Select the source interface of the packet that generated the log message.
Destination Interface	This displays when you show the filter. Select the destination interface of the packet that generated the log message.
Service	This displays when you show the filter. Select the service whose log messages you would like to see. The Web Configurator uses the protocol and destination port number(s) of the service to select which log messages you see.
Keyword	This displays when you show the filter. Type a keyword to look for in the Message , Source , Destination and Note fields. If a match is found in any field, the log message is displayed. You can use up to 63 alphanumeric characters and the underscore, as well as punctuation marks () ' , ; ? ! + - * / = # \$ % @ ; the period, double quotes, and brackets are not allowed.
Protocol	This displays when you show the filter. Select a service protocol whose log messages you would like to see.
Search	This displays when you show the filter. Click this button to update the log using the current filter settings.
Reset	This displays when you show the filter. Click this button to return the screen to its last-saved settings.
Email Log Now	Click this button to send log message(s) to the Active e-mail address(es) specified in the Send Log To field on the Log Settings page (see Section 47.3.2 on page 538).
Refresh	Click Refresh to update this screen.
Clear Log	Click this button to clear the whole log, regardless of what is currently displayed on the screen.
#	This field is a sequential value, and it is not associated with a specific log message.
Time	This field displays the time the log message was recorded.
Priority	This field displays the priority of the log message. It has the same range of values as the Priority field above.
Category	This field displays the log that generated the log message. It is the same value used in the Display and (other) Category fields.
Message	This field displays the reason the log message was generated. The text "[count=x]", where x is a number, appears at the end of the Message field if log consolidation is turned on (see Log Consolidation in Table 257 on page 540). and multiple entries were aggregated to generate into this one.
Source	This field displays the source IP address and the port number in the event that generated the log message.
Source Interface	This field displays the source interface of the packet that generated the log message.
Destination	This field displays the destination IP address and the port number of the event that generated the log message.
Destination Interface	This field displays the destination interface of the packet that generated the log message.

Table 48 Monitor > Log (continued)

LABEL	DESCRIPTION
Protocol	This field displays the service protocol used by the packet that generated the log message.
Note	This field displays any additional information about the log message.

The Web Configurator saves the filter settings if you leave the **View Log** screen and return to it later.

7.22.1 View AP Log

Use this screen to view the UAG's current wireless AP log messages. Click **Monitor > Log > View AP Log** to access this screen.

Figure 89 Monitor > Log > View AP Log

The screenshot displays the 'View AP Log' interface. At the top, there are three tabs: 'View Log', 'View AP Log' (selected), and 'Dynamic Users Log'. Below the tabs is a 'Hide Filter' button. The 'AP Selection' section includes a dropdown menu for 'Select an AP' with the value 'AP-B0B2DC6E7F24' and a 'Query' button. The 'Log Query Information' section shows 'AP Information: b0:b2:dc:6e:7f:24', 'Log File Status: Exist', and 'Last Log Query Time: 2013-04-17 07:23:43'. The 'Logs' section contains several filter fields: 'Display' (Wireless LAN), 'Source Address', 'Source Interface' (any), 'Service' (any), 'Protocol' (any), 'Priority' (any), 'Destination Address', 'Destination Interface' (any), and 'Keyword'. A 'Search' button is located below the filters. At the bottom, there are links for 'Email Log Now', 'Refresh', and 'Clear Log', followed by a table of log entries with columns for #, Time, Pr..., Ca..., Message, Source, Destination, and Note. The table shows 10 entries with timestamps from 2013-04-17 07:23:43. A pagination bar at the bottom indicates 'Page 1 of 1' and 'Showing 50 items', with a total of 'Displaying 1 - 10 of 10'.

The following table describes the labels in this screen.

Table 49 Monitor > Log > View AP Log

LABEL	DESCRIPTION
Show/Hide Filter	Click this to show or hide the AP log filter.
Select an AP	Select an AP from the list and click Query to view its log messages.
Log Query Status	<p>This indicates the current log query status.</p> <p>init - Indicates the query has not been initialized.</p> <p>querying - Indicates the query is in process.</p> <p>fail - Indicates the query failed.</p> <p>success - Indicates the query succeeded.</p>
AP Information	This displays the MAC address for the selected AP.
Log File Status	This indicates the status of the AP's log messages.
Last Log Query Time	This indicates the last time the AP was queried for its log messages.
Display	Select the log file from the specified AP that you want displayed.
Priority	<p>Select a priority level to use for filtering displayed log messages.</p> <p>Note: This criterion only appears when you Show Filter.</p>
Source Address	<p>Enter a source IP address to display only the log messages that include it.</p> <p>Note: This criterion only appears when you Show Filter.</p>
Destination Address	<p>Enter a destination IP address to display only the log messages that include it.</p> <p>Note: This criterion only appears when you Show Filter.</p>
Source Interface	<p>Enter a source interface to display only the log messages that include it.</p> <p>Note: This criterion only appears when you Show Filter.</p>
Destination Interface	<p>Enter a destination interface to display only the log messages that include it.</p> <p>Note: This criterion only appears when you Show Filter.</p>
Service	<p>Select a service type to display only the log messages related to it.</p> <p>Note: This criterion only appears when you Show Filter.</p>
Keyword	<p>Enter a keyword to display only the log messages that include it.</p> <p>Note: This criterion only appears when you Show Filter.</p>
Protocol	<p>Select a protocol to display only the log messages that include it.</p> <p>Note: This criterion only appears when you Show Filter.</p>
Search	Click this to start the log query based on the selected criteria. If no criteria have been selected, then this displays all log messages for the specified AP regardless.
Email Log Now	Click this open a new e-mail in your default e-mail program with the selected log attached.
Refresh	Click this to refresh the log table.
Clear Log	Click this to clear the log on the specified AP.
#	This field is a sequential value, and it is not associated with a specific log message.
Time	This indicates the time that the log messages was created or recorded on the AP.
Priority	This indicates the selected log message's priority.

Table 49 Monitor > Log > View AP Log (continued)

LABEL	DESCRIPTION
Category	This indicates the selected log message's category.
Message	This displays content of the selected log message.
Source	This displays the source IP address of the selected log message.
Source Interface	This field displays the source interface of the log message.
Destination	This displays the source IP address of the selected log message.
Destination Interface	This field displays the destination interface of the log message.
Protocol	This field displays the service protocol of the log message.
Note	This displays any notes associated with the selected log message.

7.22.2 Dynamic Users Log

Use this screen to view the UAG's dynamic guest account log messages. Click **Monitor > Log > Dynamic Users Log** to access this screen.

Figure 90 Monitor > Log > Dynamic Users Log

The following table describes the labels in this screen.

Table 50 Monitor > Log > Dynamic Users Log

LABEL	DESCRIPTION
Begin/End Date	Select the first and last dates to specify a time period. The UAG displays log messages only for the accounts created during the specified time period after you click Search .
Begin/End Time	Select the begin time of the first date and the end time of the last date to specify a time period. The UAG displays log messages only for the accounts created during the specified time period after you click Search .
Search	Click this button to update the information on the screen using the filter criteria in the date and time fields.
Refresh	Click this button to update the information in the screen.

Table 50 Monitor > Log > Dynamic Users Log (continued)

LABEL	DESCRIPTION
Clear Log	Click this button to delete the log messages for invalid accounts.
#	This is the index number of the dynamic guest account in the list.
Status	This field displays whether an account expires or not.
Username	This field displays the user name of the account.
Create Time	This field displays when the account was created.
Remaining Time	This field displays the amount of Internet access time remaining for each account.
Time Period	This field displays the total account of time the account can use to access the Internet through the UAG.
Expiration Time	This field displays the date and time the account becomes invalid. Note: Once the time allocated to a dynamic account is used up or a dynamic account remains un-used after the expiration time, the account is deleted from the account list.
Quota (T/U/D)	This field displays how much data in both directions (T otal) or upstream data (U pload) and downstream data (D ownload) can be transmitted through the WAN interface before the account expires.
Remaining Quota (T/U/D)	This field displays the remaining amount of data that can be transmitted or received by each account. You can see the amount of either data in both directions (T otal) or upstream data (U pload) and downstream data (D ownload).
Bandwidth (U/D)	This field displays the maximum upstream (U pload) and downstream (D ownload) bandwidth allowed for the user account in kilobits per second.
Charge	This field displays the total cost of the account.
Payment Info	This field displays the method of payment for each account.
Phone Num	This field displays the telephone number for the user account.

Licensing

8.1 Overview

Use the **Configuration > Licensing > Registration** screens to register your UAG and manage its service subscriptions. Use the **Configuration > Licensing > Signature Update** screen to update the UAG's signature packages. Not all screens are available on your UAG.

8.1.1 What You Can Do in this Chapter

- Use the **Registration** screen (see [Section 8.2 on page 132](#)) to register your UAG with myZyXEL.com.
- Use the **Service** screen (see [Section 8.3 on page 132](#)) to display the status of your service registrations and upgrade licenses.
- Use the **Signature Update > AppPatrol** screen (see [Section 8.4 on page 133](#)) to update the signatures used for application patrol.

8.1.2 What you Need to Know

This section introduces the topics covered in this chapter.

myZyXEL.com

myZyXEL.com is ZyXEL's online services center where you can register your UAG and manage subscription services available for the UAG. To use a subscription service, you have to register the UAG and activate the corresponding service at myZyXEL.com (through the UAG).

Note: You need to create a myZyXEL.com account before you can register your device and activate the services at myZyXEL.com.

Go to <http://portal.myZyXEL.com> with the UAG's serial number and LAN MAC address to register it. Refer to the web site's on-line help for details.

Note: To activate a service on a UAG, you need to access myZyXEL.com via that UAG.

Subscription Services Available on the UAG

At the time of writing, the UAG can use the upgrade service to extend the maximum number of the supported managed APs and the LAN/WLAN users that can connect to the UAG at one time.

The UAG2100 can also subscribe to the SMS ticketing service in order to send SMS text messages. The UAG5100 can also use AppPatrol (application patrol), and content filtering subscription services.

The UAG needs a license for UTM (Unified Threat Management) functionality, such as application patrol and content filtering - see [Section 1.1 on page 20](#) for details. You can purchase an iCard and enter the license key from it, at www.myzyxel.com to have the UAG use UTM services. See below the respective chapters in this guide for more information about UTM features.

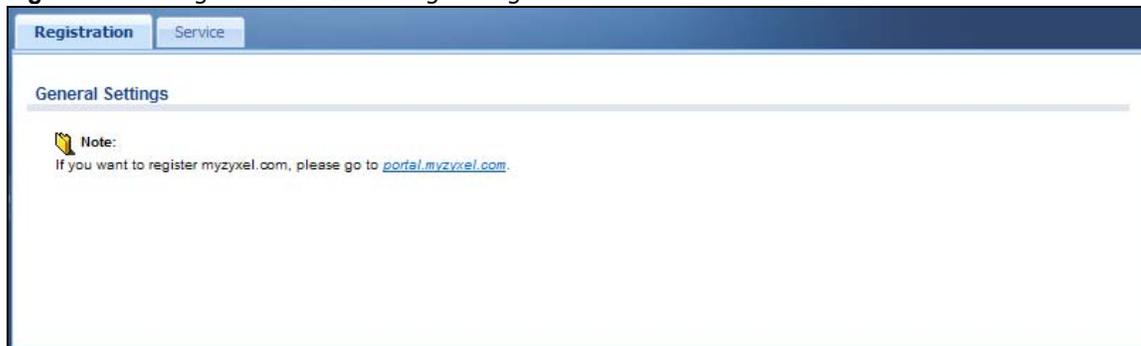
Maximum Number of Managed APs

The UAG is initially configured to support up to one local AP (NOT available on the UAG5100) and 8 remote managed APs (such as the NWA5123-NI). You can increase this by subscribing to additional licenses. As of this writing, each license upgrade allows an additional 8 remote managed APs while the maximum number of remote managed APs a single UAG can support is 8 (UAG2100), 16 (UAG4100) or 32 (UAG5100).

8.2 Registration Screen

Click the link in this screen to register your UAG with myZyXEL.com. The UAG should already have Internet access before you can register it. Click **Configuration > Licensing > Registration** in the navigation panel to open the screen as shown next.

Figure 91 Configuration > Licensing > Registration



8.3 Service Screen

Use this screen to display the status of your service registrations. To activate or extend a standard service subscription, purchase an iCard and enter the iCard's PIN number (license key) at myZyXEL.com. Click **Configuration > Licensing > Registration > Service** to open the screen as shown next.

Figure 92 Configuration > Licensing > Registration > Service

#	Service	Status	Registration Type	Expiration Date	Count
1	APP Patrol	Not Licensed			N/A
2	Content Filter Service	Not Licensed			N/A
3	Managed AP Service	Default	Standard		16
4	Extension User	Default	Standard		500

Page 1 of 1 | Show 50 items | Displaying 1 - 4 of 4

License Refresh

Service License Refresh

Note:
Update device license information from myZyXEL.com server. If you want to activate license, please go to portal.myzyxel.com

The following table describes the labels in this screen.

Table 51 Configuration > Licensing > Registration > Service

LABEL	DESCRIPTION
License Status	
#	This is the entry's position in the list.
Service	This lists the services that are available on the UAG.
Status	This field displays whether this is a default service (Default), or an active license upgrade (Licensed). It also displays Expired (when the service expired) or Not Licensed (if the service is not activated).
Registration Type	This field displays whether you applied for a trial application (Trial) or registered a service with your iCard's PIN number (Standard). This field is blank when a service is not activated. It always displays Standard for a default service.
Expiration Date	This field displays the date your service expires. This field is blank when a service does not expire. You can continue to use AppPatrol after the registration expires, you just won't receive updated signatures
Count	This field displays the maximum number of wired and wireless users that may connect to the UAG at the same time or how many managed APs the UAG can support with your current license. It displays 0 if this field does not apply to a service.
Service License Refresh	Click this button to renew service license information (such as the registration status and expiration day).

8.4 App Patrol Signature Update Screen

The UAG comes with signatures for the application patrol feature. These signatures are continually updated as new attack types evolve. New signatures can be downloaded to the UAG periodically if you have subscribed for the AppPatrol signatures service.

You need to create an account at myZyXEL.com, register your UAG and then subscribe for application patrol service in order to be able to download new packet inspection signatures from myZyXEL.com (see the **Registration** screens). Use the **Signature Update > App Patrol** screen to schedule or immediately download signatures.

- You need a valid service registration to update the App Patrol signatures.
- Schedule signature updates for a day and time when your network is least busy to minimize disruption to your network.
- Your custom signature configurations are not over-written when you download new signatures.

Note: The UAG does not have to reboot when you upload new signatures.

Click **Configuration > Licensing > Signature Update > App Patrol** to display the following screen.

Figure 93 Configuration > Licensing > Signature Update > App Patrol

The following table describes the fields in this screen.

Table 52 Configuration > Licensing > Signature Update > App Patrol

LABEL	DESCRIPTION
Signature Information	The following fields display information on the current signature set that the UAG is using.
Current Version	This field displays the signature and anomaly rule set version number. This number gets larger as the set is enhanced.
Released Date	This field displays the date and time the set was released.
Signature Update	Use these fields to have the UAG check for new signatures at myZyXEL.com. If new signatures are found, they are then downloaded to the UAG.
Update Now	Click this button to have the UAG check for new signatures immediately. If there are new ones, the UAG will then download them.
Auto Update	Select this check box to have the UAG automatically check for new signatures regularly at the time and day specified. You should select a time when your network is not busy for minimal interruption.

Table 52 Configuration > Licensing > Signature Update > App Patrol (continued)

LABEL	DESCRIPTION
Hourly	Select this option to have the UAG check for new signatures every hour.
Daily	Select this option to have the UAG check for new signatures everyday at the specified time. The time format is the 24 hour clock, so '23' means 11 PM for example.
Weekly	Select this option to have the UAG check for new signatures once a week on the day and at the time specified.
Apply	Click this button to save your changes to the UAG.
Reset	Click this button to return the screen to its last-saved settings.

9.1 Overview

Use the **Wireless** screens to configure how the UAG manages the Access Points (APs) that are connected to it.

9.1.1 What You Can Do in this Chapter

- The **Controller** screen ([Section 9.2 on page 137](#)) sets how the UAG allows new APs to connect to the network.
- The **AP Management** screen ([Section 9.3 on page 137](#)) manages all of the APs connected to the UAG.
- The **MON Mode** screen ([Section 9.4 on page 144](#)) allows you to assign APs either to the rogue AP list or the friendly AP list.
- The **Load Balancing** screen ([Section 9.5 on page 146](#)) configures network traffic load balancing between the APs and the UAG.
- The **DCS** screen ([Section 9.6 on page 148](#)) configures dynamic radio channel selection on managed APs.
- The **Auto Healing** screen ([Section 9.7 on page 151](#)) turns on the auto healing feature to extend the wireless service coverage area of the managed APs when one of the APs fails.

9.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

Station / Wireless Client

A station or wireless client is any wireless-capable device that can connect to an AP using a wireless signal.

Dynamic Channel Selection (DCS)

Dynamic Channel Selection (DCS) is a feature that allows an AP to automatically select the radio channel upon which it broadcasts by scanning the area around it and determining what channels are currently being used by other devices.

Load Balancing (Wireless)

Wireless load balancing is the process where you limit the number of connections allowed on an wireless access point (AP) or you limit the amount of wireless traffic transmitted and received on it so the AP does not become overloaded.

9.2 Controller Screen

Use this screen to set how the UAG allows new APs to connect to the network. Click **Configuration > Wireless > Controller** to access this screen.

Figure 94 Configuration > Wireless > Controller

The screenshot shows a web interface for configuring wireless settings. At the top, there is a 'Configuration' tab. Below it, the 'Controller Setting' section is visible. Under 'Registration Type', there are two radio button options: 'Manual' and 'Always Accept'. The 'Always Accept' option is selected. At the bottom of the form, there are 'Apply' and 'Reset' buttons.

Each field is described in the following table.

Table 53 Configuration > Wireless > Controller

LABEL	DESCRIPTION
Registration Type	Select Manual to add each AP to the UAG for management, or Always Accept to automatically add APs to the UAG for management. Note: Select the Manual option for managing a specific set of APs. This is recommended as the registration mechanism cannot automatically differentiate between friendly and rogue APs. For details on how to handle rogue APs, see Section 7.16 on page 116 . APs must be connected to the UAG by a wired connection or network.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

9.3 AP Management Screen

Use this screen to manage all of the APs connected to the UAG. Click **Configuration > Wireless > AP Management** to access this screen.

Figure 95 Configuration > Wireless > AP Management

The screenshot shows the 'Mgmt. AP List' screen. At the top, there are tabs for 'Mgmt. AP List' and 'AP Policy'. Below the tabs, there is a table of APs. The table has columns for '#', 'IP Address', 'MAC Address', 'Model', 'R1 Mode / Pr...', 'R2 Mode / Pr...', 'Mgmt. V...', 'Mgmt. V...', and 'Description'. There is one AP listed with IP 172.17.1.1 and MAC B0:B2:DC:6F:... The table also includes action icons (Edit, Remove, Reboot, LED On, LED Off) and pagination controls (Page 1 of 1, Show 50 items, Displaying 1 - 1 of 1).

#	IP Address	MAC Address	Model	R1 Mode / Pr...	R2 Mode / Pr...	Mgmt. V...	Mgmt. V...	Description
1	172.17.1.1	B0:B2:DC:6F:...	NWA51...	AP / default	MON / default	1	1	AP-B0B2DC6...

Each field is described in the following table.

Table 54 Configuration > Wireless > AP Management

LABEL	DESCRIPTION
Edit	Select an AP and click this button to edit its properties.
Remove	Select one or multiple APs and click this button to remove the AP(s) from the list. Note: If in the Configuration > Wireless > Controller screen you set the Registration Type to Always Accept , then as soon as you remove an AP from this list it reconnects.
Reboot	Select one or multiple APs and click this button to force the AP(s) to restart.
LED On	Select an AP and click this button to disable the AP's LED suppression mode. The AP LEDs stay lit after the AP is ready. This button is not available if the selected AP doesn't support suppression mode.
LED Off	Select an AP and click this button to enable the AP's LED suppression mode. All the LEDs of the AP will turn off after the AP is ready. This button is not available if the selected AP doesn't support suppression mode.
#	This field is a sequential value, and it is not associated with any entry.
IP Address	This field displays the IP address of the AP.
MAC Address	This field displays the MAC address of the AP.
Model	This field displays the AP's hardware model information. It displays N/A (not applicable) only when the AP disconnects from the UAG and the information is unavailable as a result.
R1 Mode / Profile	This field displays the operating mode (AP) and AP profile name for Radio 1. It displays n/a for the profile for a radio not using an AP profile.
R2 Mode / Profile	This field displays the operating mode (AP) and AP profile name for Radio 2. It displays n/a for the profile for a radio not using an AP profile.
Mgmt. VLAN ID(AC)	This displays the Access Controller (the UAG) management VLAN ID setting for the AP.
Mgmt. VLAN ID(AP)	This displays the runtime management VLAN ID setting on the AP. VLAN Conflict displays if the AP's management VLAN ID does not match the Mgmt. VLAN ID(AC) . This field displays n/a if the UAG cannot get VLAN information from the AP.
Description	This field displays the AP's description, which you can configure by selecting the AP's entry and clicking the Edit button.

9.3.1 Edit AP List

Select an AP and click the **Edit** button in the **Configuration > Wireless > AP Management** table to display this screen.

Figure 96 Configuration > Wireless > AP Management > Edit AP List

Each field is described in the following table.

Table 55 Configuration > Wireless > AP Management > Edit AP List

LABEL	DESCRIPTION
Create new Object	Use this menu to create a new Radio Profile or MON Profile object to associate with this AP.
Configuration	
MAC	This displays the MAC address of the selected AP.
Model	This field displays the AP's hardware model information. It displays N/A (not applicable) only when the AP disconnects from the UAG and the information is unavailable as a result.
Description	Enter a description for this AP. You can use up to 31 characters, spaces and underscores allowed.

Table 55 Configuration > Wireless > AP Management > Edit AP List (continued)

LABEL	DESCRIPTION
Radio 1/2 OP Mode	Select the operating mode for radio 1 or radio 2. AP Mode means the AP can receive connections from wireless clients and pass their data traffic through to the UAG to be managed (or subsequently passed on to an upstream gateway for managing). MON Mode means the AP monitors the broadcast area for other APs, then passes their information on to the UAG where it can be determined if those APs are friendly or rogue. If an AP is set to this mode it cannot receive connections from wireless clients. Note: Ensure you restart the managed AP after you change its operating mode.
Radio 1/2 Profile	Select an AP profile or a monitor profile from the list. If no profile exists, you can create a new one through the Create new Object menu.
VLAN Settings	This section is not available when you are editing the local AP's settings.
Force Overwrite VLAN Config	Select this to have the UAG change the AP's management VLAN to match the configuration in this screen.
Management VLAN ID	Enter a VLAN ID for this AP.
As Native VLAN	Select this option to treat this VLAN ID as a VLAN created on the UAG and not one assigned to it from outside the network.
Port Setting	
#	This is the port's index number in this list.
Status	This displays whether or not the port is activated.
Port	This shows the name of the physical Ethernet port on the managed AP.
PVID	This shows the port's PVID. A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines.
VLAN Configuration	
#	This is the VLAN's index number in this list.
Status	This displays whether or not the VLAN is activated.
Name	This shows the name of the VLAN.
VID	This shows the VLAN ID number.
Member	This field displays the Ethernet port(s) that is a member of this VLAN.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to close the window with changes unsaved.

9.3.2 Port Setting Edit

Use this screen to enable or disable a port on the managed AP and configure the port's PVID.

To access this screen, select a port and click the **Edit** button in the **Port Setting** table of the **Configuration > Wireless > AP Management > Edit AP List** screen.

Figure 97 Configuration > Wireless > AP Management > Edit AP List > Edit Port

Each field is described in the following table.

Table 56 Configuration > Wireless > AP Management > Edit AP List > Edit Port

LABEL	DESCRIPTION
Enable	Select this option to activate the port. Otherwise, deselect it.
Name	This shows the name of the port.
Native VID (PVID)	A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines. Enter the PVID from 1 to 4094 for this port.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to close the window with changes unsaved.

9.3.3 VLAN Add/Edit

Use this screen to create a new VLAN or configure an existing VLAN on the UAG.

To access this screen, click **Add** or select a VLAN and click the **Edit** button in the **VLAN Member Configuration** table of the **Configuration > Wireless > AP Management > Edit AP List** screen.

Figure 98 Configuration > Wireless > AP Management > Edit AP List > Edit VLAN

Add Vlan

General Settings

Enable

Port Properties

Name: ⓘ

VID: ⓘ (~4094)

Member Configuration

#	Port Name	Member	Tx Tagging
1	lan1	no	no
2	lan2	no	no
3	lan3	no	no

VLAN Member Configuration

OK Cancel

Each field is described in the following table.

Table 57 Configuration > Wireless > AP Management > Edit AP List > Edit VLAN

LABEL	DESCRIPTION
Enable	Select this option to activate the VLAN. Otherwise, deselect it.
Name	This field is read-only if you are editing an existing VLAN. Enter the number of the VLAN. You can use a number from 1~4094. For example, vlan0, vlan8, and so on.
VID	Enter the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 - 4094. (0 and 4095 are reserved.)
Member Configuration	Use these settings to assign ports to this VLAN as members.
Edit	Click this to edit the selected port's membership values.
#	This is sequential indicator of the port number.
Port Name	This indicates the port name.
Member	This indicates whether the selected port is a member or not of the VLAN which is currently being edited. Click this field to edit the value.
Tx Tagging	This indicates whether the selected port tags outbound traffic with this VLAN's ID . Click this field to edit the value.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to close the window with changes unsaved.

9.3.4 AP Policy

Use this screen to configure the AP controller's IP address on the managed APs and determine the action the managed APs take if the current AP controller fails. Click **Configuration > Wireless > AP Management > AP Policy** to access this screen.

Figure 99 Configuration > Wireless > AP Management > AP Policy

Each field is described in the following table.

Table 58 Configuration > Wireless > AP Management > AP Policy

LABEL	DESCRIPTION
Force Override AC IP Config on AP	Select this to have the UAG change the AP controller's IP address on the managed AP(s) to match the configuration in this screen.
Override Type	Select Auto to have the managed AP(s) automatically send broadcast packets to find any other available AP controllers. Select Manual to replace the AP controller's IP address configured on the managed AP(s) with the one(s) you specified below.
Primary Controller	Specify the IP address of the primary AP controller if you set Override Type to Manual .
Secondary Controller	Specify the IP address of the secondary AP controller if you set Override Type to Manual .
Fall back to Primary Controller when possible	Select this option to have the managed AP(s) change back to associate with the primary AP controller as soon as the primary AP controller is available.
Fall Back Check Interval	Set how often the managed AP(s) check whether the primary AP controller is available.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

9.4 MON Mode

Use this screen to assign APs either to the rogue AP list or the friendly AP list. A rogue AP is a wireless access point operating in a network's coverage area that is not under the control of the network administrator, and which can potentially open up holes in a network's security.

Click **Configuration > Wireless > MON Mode** to access this screen.

Figure 100 Configuration > Wireless > MON Mode

Each field is described in the following table.

Table 59 Configuration > Wireless > MON Mode

LABEL	DESCRIPTION
General Settings	
Enable Rogue AP Containment	Select this to enable rogue AP containment.
Rogue/Friendly AP List	
Add	Click this button to add an AP to the list and assign it either friendly or rogue status.
Edit	Select an AP in the list to edit and reassign its status.
Remove	Select an AP in the list to remove.
Containment	Click this button to quarantine the selected AP. A quarantined AP cannot grant access to any network services. Any stations that attempt to connect to a quarantined AP are disconnected automatically.
Dis-Containment	Click this button to take the selected AP out of quarantine. An unquarantined AP has normal access to the network.
#	This field is a sequential value, and it is not associated with any interface.
Containment	This field indicates the selected AP's containment status.

Table 59 Configuration > Wireless > MON Mode (continued)

LABEL	DESCRIPTION
Role	This field indicates whether the selected AP is a rogue-ap or a friendly-ap . To change the AP's role, click the Edit button.
MAC Address	This field indicates the AP's radio MAC address.
Description	This field displays the AP's description. You can modify this by clicking the Edit button.
Rogue/Friendly AP List Importing/Exporting	These controls allow you to export the current list of rogue and friendly APs or import existing lists.
File Path / Browse / Importing	Enter the file name and path of the list you want to import or click the Browse button to locate it. Once the File Path field has been populated, click Importing to bring the list into the UAG.
Exporting	Click this button to export the current list of either rogue APs or friendly APs.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

9.4.1 Add/Edit Rogue/Friendly List

Select an AP and click the **Edit** button in the **Configuration > Wireless > MON Mode** table to display this screen.

Figure 101 Configuration > Wireless > MON Mode > Add/Edit Rogue/Friendly

Each field is described in the following table.

Table 60 Configuration > Wireless > MON Mode > Add/Edit Rogue/Friendly

LABEL	DESCRIPTION
MAC	Enter the MAC address of the AP you want to add to the list. A MAC address is a unique hardware identifier in the following hexadecimal format: xx:xx:xx:xx:xx:xx where xx is a hexadecimal number separated by colons.
Description	Enter up to 60 characters for the AP's description. Spaces and underscores are allowed.
Role	Select either Rogue AP or Friendly AP for the AP's role.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to close the window with changes unsaved.

9.5 Load Balancing

Use this screen to configure wireless network traffic load balancing between the APs on your network. Click **Configuration > Wireless > Load Balancing** to access this screen.

Figure 102 Configuration > Wireless > Load Balancing

Each field is described in the following table.

Table 61 Configuration > Wireless > Load Balancing

LABEL	DESCRIPTION
Enable Load Balancing	Select this to enable load balancing on the UAG.
Mode	Select a mode by which load balancing is carried out. Select By Station Number to balance network traffic based on the number of specified stations connect to an AP. Select By Traffic Level to balance network traffic based on the volume generated by the stations connected to an AP. Once the threshold is crossed (either the maximum station numbers or with network traffic), then the AP delays association request and authentication request packets from any new station that attempts to make a connection. This allows the station to automatically attempt to connect to another, less burdened AP if one is available.
Max Station Number	Enter the threshold number of stations at which an AP begins load balancing its connections.
Traffic Level	Select the threshold traffic level at which the AP begins load balancing its connections (low, medium, high).
Disassociate station when overloaded	Select this option to disassociate wireless clients connected to the AP when it becomes overloaded. If you do not enable this option, then the AP simply delays the connection until it can afford the bandwidth it requires, or it transfers the connection to another AP within its broadcast radius. The disassociation priority is determined automatically by the UAG and is as follows: <ul style="list-style-type: none"> • Idle Timeout - Devices that have been idle the longest will be disassociated first. If none of the connected devices are idle, then the priority shifts to Signal Strength. • Signal Strength - Devices with the weakest signal strength will be disassociated first. <p>Note: If you enable this function, you should ensure that there are multiple APs within the broadcast radius that can accept any rejected or kicked wireless clients; otherwise, a wireless client attempting to connect to an overloaded AP will be kicked continuously and never be allowed to connect.</p>

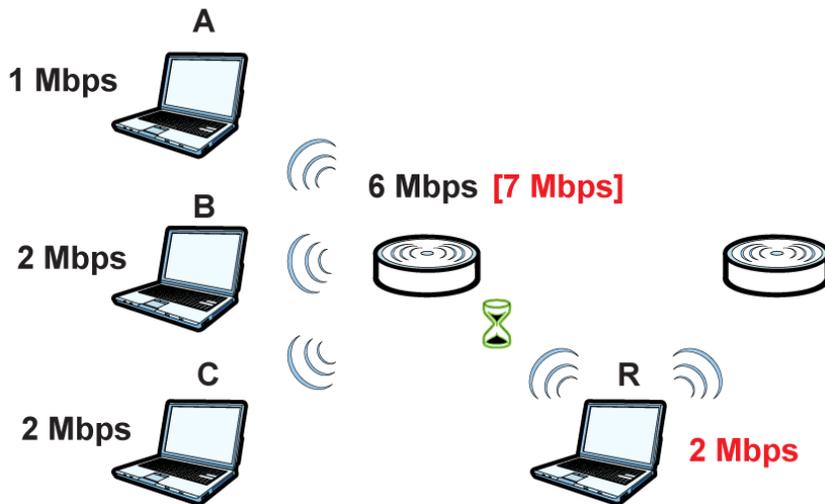
Table 61 Configuration > Wireless > Load Balancing (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

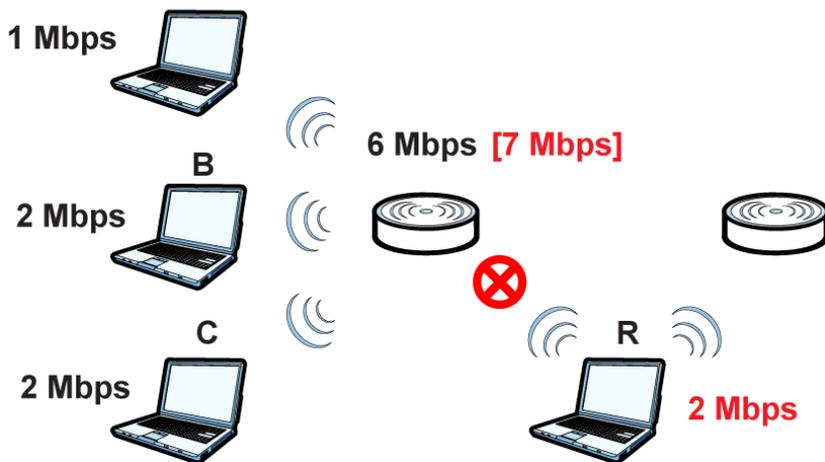
9.5.1 Disassociating and Delaying Connections

When your AP becomes overloaded, there are two basic responses it can take. The first one is to “delay” a client connection. This means that the AP withholds the connection until the data transfer throughput is lowered or the client connection is picked up by another AP. If the client is picked up by another AP then the original AP cannot resume the connection.

For example, here the AP has a balanced bandwidth allotment of 6 Mbps. If laptop **R** connects and it pushes the AP over its allotment, say to 7 Mbps, then the AP delays the red laptop’s connection until it can afford the bandwidth or the laptop is picked up by a different AP with bandwidth to spare.

Figure 103 Delaying a Connection

The second response your AP can take is to kick the connections that are pushing it over its balanced bandwidth allotment.

Figure 104 Kicking a Connection

Connections are kicked based on either **idle timeout** or **signal strength**. The UAG first looks to see which devices have been idle the longest, then starts kicking them in order of highest idle time. If no connections are idle, the next criteria the UAG analyzes is signal strength. Devices with the weakest signal strength are kicked first.

9.6 DCS

Use DCS (Dynamic Channel Selection) in an environment where there are many APs and there may be interference. DCS allows APs to automatically find a less-used channel in such an environment. Use this screen to configure dynamic radio channel selection on managed APs. Click **Configuration > Wireless > DCS** to access this screen.

Figure 105 Configuration > Wireless > DCS

Each field is described in the following table.

Table 62 Configuration > Wireless > DCS

LABEL	DESCRIPTION
General Settings	
Select Now	Click this to have the managed APs scan for and select an available channel immediately.
Enable Dynamic Channel Selection	Select this to turn on dynamic channel selection for the APs that the UAG manages.
DCS Time Interval	Enter a number of minutes. This regulates how often the UAG surveys the other APs within its broadcast radius. If the channel on which it is currently broadcasting suddenly comes into use by another AP, the UAG will then dynamically select the next available clean channel or a channel with lower interference.
Enable DCS Client Aware	Select this to have the AP wait until all connected clients have disconnected before switching channels. If you disable this then the AP switches channels immediately regardless of any client connections. In this instance, clients that are connected to the AP when it switches channels are dropped.
2.4 GHz Settings	
2.4 GHz Channel Selection Method	Select auto to have the AP search for available channels automatically in the 2.4 GHz band. The available channels vary depending on what you select in the 2.4 GHz Channel Deployment field. Select manual and specify the channels the AP uses in the 2.4 GHz band.

Table 62 Configuration > Wireless > DCS (continued)

LABEL	DESCRIPTION
Available channels	This text box lists the channels that are available in the 2.4 GHz band. Select the channels that you want the AP to use, and click the right arrow button to add them.
Channels selected	This text box lists the channels that you allow the AP to use. Select any channels that you want to prevent the AP from using it, and click the left arrow button to remove them.
2.4 GHz Channel Deployment	<p>This field is available only when you set 2.4 GHz Channel Selection Method to auto.</p> <p>Select Three-Channel Deployment to limit channel switching to channels 1,6, and 11, the three channels that are sufficiently attenuated to have almost no impact on one another. In other words, this allows you to minimize channel interference by limiting channel-hopping to these three "safe" channels.</p> <p>Select Four-Channel Deployment to limit channel switching to four channels. Depending on the country domain, if the only allowable channels are 1-11 then the UAG uses channels 1, 4, 7, 11 in this configuration; otherwise, the UAG uses channels 1, 5, 9, 13 in this configuration. Four channel deployment expands your pool of possible channels while keeping the channel interference to a minimum.</p>
5 GHz Settings	
Enable 5 GHz DFS Aware	<p>Select this if your APs are operating in an area known to have RADAR devices. This allows the device to downgrade its frequency to below 5 GHz in the event a RADAR signal is detected, thus preventing it from interfering with that signal.</p> <p>Enabling this forces the AP to select a non-DFS channel.</p>
5 GHz Channel Selection Method	<p>Select auto to have the AP search for available channels automatically in the 5 GHz band.</p> <p>Select manual and specify the channels the AP uses in the 5 GHz band.</p>
Available channels	This text box lists the channels that are available in the 5 GHz band. Select the channels that you want the AP to use, and click the right arrow button to add them.
Channels selected	This text box lists the channels that you allow the AP to use. Select any channels that you want to prevent the AP from using it, and click the left arrow button to remove them.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

9.7 Auto Healing

Use this screen to enable auto healing, which allows you to extend the wireless service coverage area of the managed APs when one of the APs fails. Click **Configuration > Wireless > Auto Healing** to access this screen.

Figure 106 Configuration > Wireless > Auto Healing

Auto Healing Configuration

Enable Auto Healing

Auto Healing Interval: (5~30minutes)

Power Threshold: dBm (-50 ~ -80)

Note:
When deployment is complete/changed, admin should make sure the parameters are ok, all WTP in online status and click Save Current Status button.

Each field is described in the following table.

Table 63 Configuration > Wireless > Auto Healing

LABEL	DESCRIPTION
Enable Auto Healing	Select this option to turn on the auto healing feature.
Save Current State	Click this button to have all managed APs immediately scan their neighborhoods three times in a row and update their neighbor lists to the AP controller (UAG).
Auto Healing Interval	Set the time interval (in minutes) at which the managed APs scan their neighborhoods and report the status of neighbor APs to the AP controller (UAG). An AP is considered "failed" if the AP controller obtains the same scan result that the AP is missing from the neighbor list of other APs three times.
Power Threshold	Set the power level (in dBm) to which the neighbor APs of the failed AP increase their output power in order to extend their wireless service coverage areas. When the failed AP is working again, its neighbor APs return their output power to the original level.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

9.8 Technical Reference

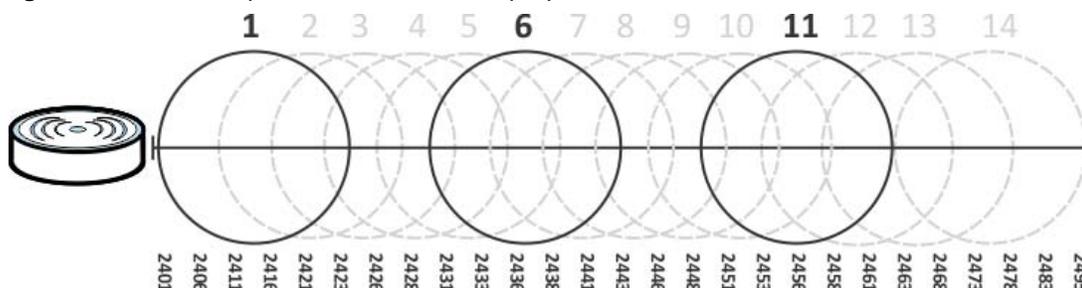
The following section contains additional technical information about the features described in this chapter.

9.8.1 Dynamic Channel Selection

When numerous APs broadcast within a given area, they introduce the possibility of heightened radio interference, especially if some or all of them are broadcasting on the same radio channel. If the interference becomes too great, then the network administrator must open his AP configuration options and manually change the channel to one that no other AP is using (or at least a channel that has a lower level of interference) in order to give the connected stations a minimum degree of interference. Dynamic channel selection frees the network administrator from this task by letting the AP do it automatically. The AP can scan the area around it looking for the channel with the least amount of interference.

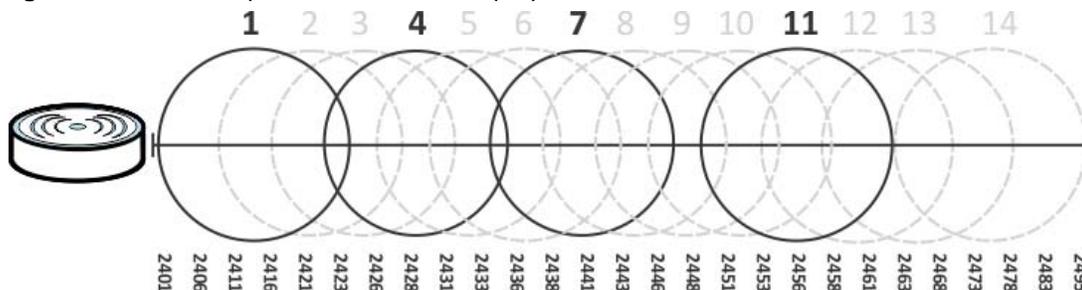
In the 2.4 GHz spectrum, each channel from 1 to 13 is broken up into discrete 22 MHz segments that are spaced 5 MHz apart. Channel 1 is centered on 2.412 GHz while channel 13 is centered on 2.472 GHz.

Figure 107 An Example Three-Channel Deployment



Three channels are situated in such a way as to create almost no interference with one another if used exclusively: 1, 6 and 11. When an AP broadcasts on any of these three channels, it should not interfere with neighboring APs as long as they are also limited to same trio.

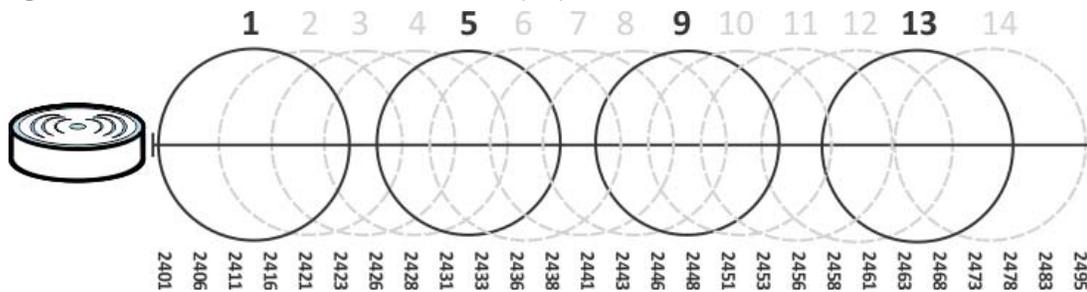
Figure 108 An Example Four-Channel Deployment



However, some regions require the use of other channels and often use a safety scheme with the following four channels: 1, 4, 7 and 11. While they are situated sufficiently close to both each other and the three so-called "safe" channels (1,6 and 11) that interference becomes inevitable, the severity of it is dependent upon other factors: proximity to the affected AP, signal strength, activity, and so on.

Finally, there is an alternative four channel scheme for ETSI, consisting of channels 1, 5, 9, 13. This offers significantly less overlap than the other one.

Figure 109 An Alternative Four-Channel Deployment



9.8.2 Load Balancing

Because there is a hard upper limit on an AP's wireless bandwidth, load balancing can be crucial in areas crowded with wireless users. Rather than let every user connect and subsequently dilute the available bandwidth to the point where each connecting device receives a meager trickle, the load balanced AP instead limits the incoming connections as a means to maintain bandwidth integrity.

There are two kinds of wireless load balancing available on the UAG:

Load balancing by station number limits the number of devices allowed to connect to your AP. If you know exactly how many stations you want to let connect, choose this option.

For example, if your company's graphic design team has their own AP and they have 10 computers, you can load balance for 10. Later, if someone from the sales department visits the graphic design team's offices for a meeting and he tries to access the network, his computer's connection is delayed, giving it the opportunity to connect to a different, neighboring AP. If he still connects to the AP regardless of the delay, then the AP may boot other people who are already connected in order to associate with the new connection.

Load balancing by traffic level limits the number of connections to the AP based on maximum bandwidth available. If you are uncertain as to the exact number of wireless connections you will have then choose this option. By setting a maximum bandwidth cap, you allow any number of devices to connect as long as their total bandwidth usage does not exceed the configured bandwidth cap associated with this setting. Once the cap is hit, any new connections are rejected or delayed provided that there are other APs in range.

Imagine a coffee shop in a crowded business district that offers free wireless connectivity to its customers. The coffee shop owner can't possibly know how many connections his AP will have at any given moment. As such, he decides to put a limit on the bandwidth that is available to his customers but not on the actual number of connections he allows. This means anyone can connect to his wireless network as long as the AP has the bandwidth to spare. If too many people connect and the AP hits its bandwidth cap then all new connections must basically wait for their turn or get shunted to the nearest identical AP.

10.1 Interface Overview

Use the **Interface** screens to configure the UAG's interfaces. You can also create interfaces on top of other interfaces.

- **Ports** are the physical ports to which you connect cables.
- **Interfaces** are used within the system operationally. You use them in configuring various features. An interface also describes a network that is directly connected to the UAG. For example, You connect the LAN network to the LAN interface.
- **Zones** are groups of interfaces used to ease security policy configuration.

10.1.1 What You Can Do in this Chapter

- Use the **Port Role** screen ([Section 10.2 on page 156](#)) to create port groups and to assign physical ports and port groups to Ethernet interfaces.
- Use the **Ethernet** screens ([Section 10.3 on page 157](#)) to configure the Ethernet interfaces. Ethernet interfaces are the foundation for defining other interfaces and network policies.
- Use the **PPP** screens ([Section 10.4 on page 168](#)) for PPPoE or PPTP Internet connections.
- Use the **VLAN** screens ([Section 10.5 on page 174](#)) to divide the physical network into multiple logical networks. VLAN interfaces receive and send tagged frames. The UAG automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- Use the **Bridge** screens ([Section 10.6 on page 181](#)) to combine two or more network segments into a single network.
- Use the **Virtual Interface** screen ([Section 10.7.1 on page 190](#)) to create virtual interfaces on top of Ethernet interfaces to tell the UAG where to route packets. You can create virtual Ethernet interfaces, virtual VLAN interfaces, and virtual bridge interfaces.
- Use the **Trunk** screens ([Chapter 11 on page 195](#)) to configure load balancing.

10.1.2 What You Need to Know

Interface Characteristics

Interfaces generally have the following characteristics (although not all characteristics apply to each type of interface).

- An interface is a logical entity through which (layer-3) packets pass.
- An interface is bound to a physical port or another interface.
- Many interfaces can share the same physical port.
- An interface belongs to at most one zone.
- Many interfaces can belong to the same zone.

- Layer-3 virtualization (IP alias, for example) is a kind of interface.

Types of Interfaces

You can create several types of interfaces in the UAG.

- Setting interfaces to the same port role forms a port group. Port groups create a hardware connection between physical ports at the layer-2 (data link, MAC address) level. Port groups are created when you use the **Interface > Port Roles** screen to set multiple physical ports to be part of the same interface.
- **Ethernet interfaces** are the foundation for defining other interfaces and network policies.
- **VLAN interfaces** receive and send tagged frames. The UAG automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- **Bridge interfaces** create a software connection between Ethernet or VLAN interfaces at the layer-2 (data link, MAC address) level. Unlike port groups, bridge interfaces can take advantage of some security features in the UAG. You can also assign an IP address and subnet mask to the bridge.
- **PPP interfaces** support Point-to-Point Protocols (PPP). ISP accounts are required for PPPoE/PPTP interfaces.
- **Virtual interfaces** provide additional routing information in the UAG. There are three types: **virtual Ethernet interfaces**, **virtual VLAN interfaces**, and **virtual bridge interfaces**.
- **Trunk interfaces** manage load balancing between interfaces.

Port groups and trunks have a lot of characteristics that are specific to each type of interface. See [Section 10.2 on page 156](#) and [Chapter 11 on page 195](#) for details. The other types of interfaces-- Ethernet, PPP, VLAN, bridge, and virtual--have a lot of similar characteristics. These characteristics are listed in the following table and discussed in more detail below.

Table 64 Ethernet, PPP, VLAN, Bridge, and Virtual Interface Characteristics

CHARACTERISTICS	ETHERNET	ETHERNET	PPP	VLAN	BRIDGE	VIRTUAL
Name*	wan1, wan2	lan1, lan2, dmz	pppx	vlanx	brx	**
Configurable Zone	Yes	Yes	Yes	Yes	Yes	No
IP Address Assignment						
Static IP address	Yes	Yes	Yes	Yes	Yes	Yes
DHCP client	Yes	No	Yes	Yes	Yes	No
Routing metric	Yes	Yes	Yes	Yes	Yes	Yes
Interface Parameters						
Bandwidth restrictions	Yes	Yes	Yes	Yes	Yes	Yes
Packet size (MTU)	Yes	Yes	Yes	Yes	Yes	No
DHCP						
DHCP server	No	Yes	No	Yes	Yes	No
DHCP relay	No	Yes	No	Yes	Yes	No
Connectivity Check	Yes	No	Yes	Yes	Yes	No

- * The format of interface names other than the Ethernet and ppp interface names is strict. Each name consists of 2-4 letters (interface type), followed by a number (x). For most interfaces, x is limited by the maximum number of the type of interface. For VLAN interfaces, x is defined by the number you enter in the VLAN name field. For example, Ethernet interface names are wan1, lan1, lan2; VLAN interfaces are vlan0, vlan1, vlan2, ...; and so on.

** - The names of virtual interfaces are derived from the interfaces on which they are created. For example, virtual interfaces created on Ethernet interface wan1 are called wan1:1, wan1:2, and so on. Virtual interfaces created on

VLAN interface vlan2 are called vlan2:1, vlan2:2, and so on. You cannot specify the number after the colon(:) in the Web Configurator; it is a sequential number. You can specify the number after the colon if you use the CLI to set up a virtual interface.

Relationships Between Interfaces

In the UAG, interfaces are usually created on top of other interfaces. Only Ethernet interfaces are created directly on top of the physical ports or port groups. The relationships between interfaces are explained in the following table.

Table 65 Relationships Between Different Types of Interfaces

INTERFACE	REQUIRED PORT / INTERFACE
port group	physical port
Ethernet interface	physical port port group
VLAN interface	Ethernet interface
bridge interface	Ethernet interface* VLAN interface*
PPP interface	Ethernet interface* VLAN interface* bridge interface WAN1, WAN2
virtual interface (virtual Ethernet interface) (virtual VLAN interface) (virtual bridge interface)	Ethernet interface* VLAN interface* bridge interface
trunk	Ethernet interface VLAN interface bridge interface PPP interface

* - You cannot set up a PPP interface, virtual Ethernet interface or virtual VLAN interface if the underlying interface is a member of a bridge. You also cannot add an Ethernet interface or VLAN interface to a bridge if the member interface has a virtual interface or PPP interface on top of it.

Finding Out More

- See [Section 10.8 on page 191](#) for background information on interfaces.
- See [Chapter 11 on page 195](#) to configure load balancing using trunks.

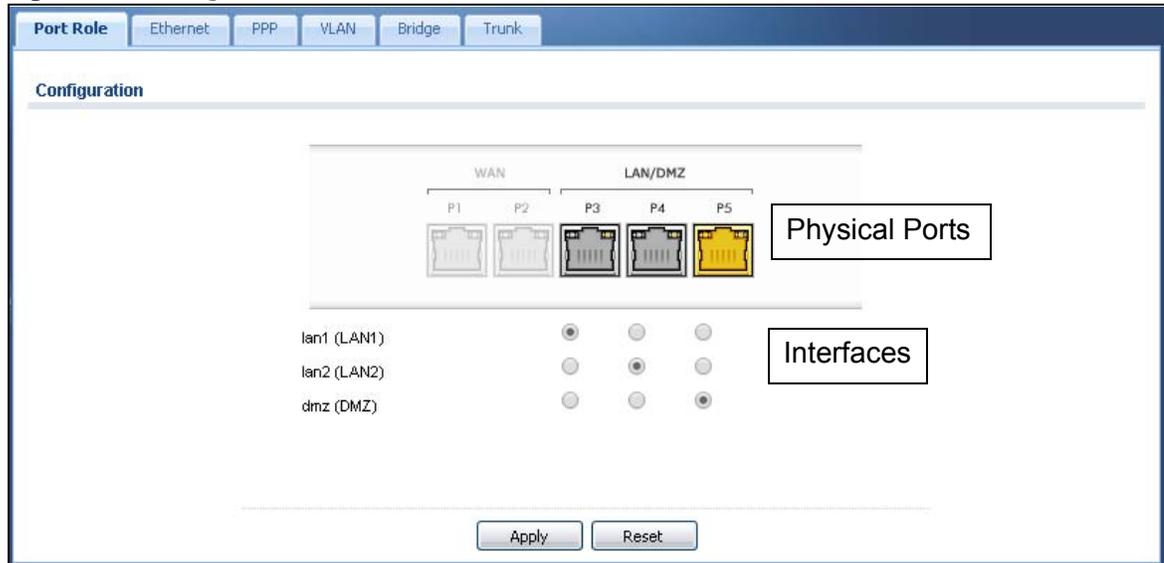
10.2 Port Role Screen

To access this screen, click **Configuration > Network > Interface > Port Role**. Use the **Port Role** screen to set the UAG's flexible ports as part of the **lan1**, **lan2** or **dmz** interfaces. This creates a hardware connection between the physical ports at the layer-2 (data link, MAC address) level. This provides wire-speed throughput but no security.

Note the following if you are configuring from a computer connected to a **lan1**, **lan2** or **dmz** port and change the port's role:

- A port's IP address varies as its role changes, make sure your computer's IP address is in the same subnet as the UAG's **lan1**, **lan2** or **dmz** IP address.
- Use the appropriate **lan1**, **lan2** or **dmz** IP address to access the UAG.

Figure 110 Configuration > Network > Interface > Port Role



The physical Ethernet ports are shown at the top and the Ethernet interfaces and zones are shown at the bottom of the screen. Use the radio buttons to select for which interface (network) you want to use each physical port. For example, select a port's **lan1** radio button to use the port as part of the **lan1** interface. The port will use the UAG's **lan1** IP address and MAC address.

When you assign more than one physical port to a network, you create a port group. Port groups have the following characteristics:

- There is a layer-2 Ethernet switch between physical ports in the port group. This provides wire-speed throughput but no security.
- It can increase the bandwidth between the port group and other interfaces.
- The port group uses a single MAC address.

Click **Apply** to save your changes and apply them to the UAG.

Click **Reset** to change the port groups to their current configuration (last-saved values).

10.3 Ethernet Summary Screen

This screen lists every Ethernet interface and virtual interface created on top of Ethernet interfaces. To access this screen, click **Configuration > Network > Interface > Ethernet**.

Unlike other types of interfaces, you cannot create new Ethernet interfaces nor can you delete any of them. If an Ethernet interface does not have any physical ports assigned to it (see [Section 10.2](#)

on page 156), the Ethernet interface is effectively removed from the UAG, but you can still configure it.

Ethernet interfaces are similar to other types of interfaces in many ways. They have an IP address, subnet mask, and gateway used to make routing decisions. They restrict the amount of bandwidth and packet size. They can provide DHCP services, and they can verify the gateway is available.

Use Ethernet interfaces to control which physical ports exchange routing information with other routers and how much information is exchanged through each one. The more routing information is exchanged, the more efficient the routers should be. However, the routers also generate more network traffic, and some routing protocols require a significant amount of configuration and management.

Figure 111 Configuration > Network > Interface > Ethernet



Each field is described in the following table.

Table 66 Configuration > Network > Interface > Ethernet

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove a virtual interface, select it and click Remove . The UAG confirms you want to remove it before doing so.
Activate	To turn on an interface, select it and click Activate .
Inactivate	To turn off an interface, select it and click Inactivate .
Create Virtual Interface	To open the screen where you can create a virtual Ethernet interface, select an Ethernet interface and click Create Virtual Interface .
Object References	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 10.3.2 on page 165 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the interface.

Table 66 Configuration > Network > Interface > Ethernet (continued)

LABEL	DESCRIPTION
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0 (in the IPv4 network), the interface does not have an IP address yet. In the IPv4 network, this screen also shows whether the IP address is a static IP address (STATIC) or dynamically assigned (DHCP). IP addresses are always static in virtual interfaces.
Mask	This field displays the interface's subnet mask in dot decimal notation.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

10.3.1 Ethernet Edit

The **Ethernet Edit** screen lets you configure IP address assignment, interface parameters, DHCP settings, connectivity check, and MAC address settings. To access this screen, select an entry in the **Ethernet** summary screen and click the **Edit** icon. (See [Section 10.3 on page 157.](#))

Note: If you create IP address objects based on an interface's IP address, subnet, or gateway, the UAG automatically updates every rule or setting that uses the object whenever the interface's IP address settings change. For example, if you change the LAN's IP address, the UAG automatically updates the corresponding interface-based, LAN subnet address object.

Figure 112 Configuration > Network > Interface > Ethernet > Edit (External Type)

Edit Ethernet [?] [X]

Hide Advanced Settings

General Settings

Enable Interface

Interface Properties

Interface Type: external

Interface Name: wan1

Port: P1

Zone: WAN

MAC Address: 00:00:AA:80:31:26

Description: (Optional)

IP Address Assignment

Get Automatically 0.0.0.0

Use Fixed IP Address

IP Address:

Subnet Mask:

Gateway: (Optional)

Metric: 0 (0-15)

Interface Parameters

Egress Bandwidth: 1048576 Kbps ⓘ

Ingress Bandwidth: 1048576 Kbps

MTU: 1500 Bytes

Connectivity Check

Enable Connectivity Check

Check Method: tcp

Check Period: 30 (5-30 seconds)

Check Timeout: 5 (1-10 seconds)

Check Fail Tolerance: 5 (1-10)

Check Default Gateway 0.0.0.0

Check this address (Domain Name or IP Address)

Check Port: 1 (1-65535)

MAC Address Setting

Use Default MAC Address 00:00:AA:80:31:26

Overwrite Default MAC Address

Related Setting

Configure [PPPoE/PPTP](#) ⓘ

Figure 113 Configuration > Network > Interface > Ethernet > Edit (Internal Type)

Edit Ethernet
? X

Hide Advanced Settings

General Settings

Enable Interface

Interface Properties

Interface Type: internal

Interface Name:

Port: P2, P3

Zone: i

MAC Address: 00:00:AA:80:31:27

Description: (Optional)

IP Address Assignment

IP Address:

Subnet Mask:

Interface Parameters

Egress Bandwidth: Kbps i

Ingress Bandwidth: Kbps

MTU: Bytes

DHCP Setting

DHCP:

IP Pool Start Address (Optional): Pool Size:

First DNS Server (Optional):

Second DNS Server (Optional): !

Third DNS Server (Optional): !

First WINS Server (Optional):

Second WINS Server (Optional):

Default Router (Optional):

Lease Time: infinite 2 days 0 hours (Optional) 0 minutes (Optional)

Extended Options

Add Edit Remove

#	Name	Code	Type	Value
No data to display				

Page 1 of 1 Show 50 items

Enable IP/MAC Binding

Enable Logs for IP/MAC Binding Violation

Static DHCP Table

Add Edit Remove

#	IP Address	MAC	Description
No data to display			

Page 1 of 1 Show 50 items

This screen's fields are described in the table below.

Table 67 Configuration > Network > Interface > Ethernet > Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
General Settings	
Enable Interface	Select this to enable this interface. Clear this to disable this interface.
Interface Properties	
Interface Type	<p>Select to which type of network you will connect this interface. When you select internal or external the rest of the screen's options automatically adjust to correspond. The UAG automatically adds default route and SNAT settings for traffic it routes from internal interfaces to external interfaces; for example LAN to WAN traffic.</p> <p>internal is for connecting to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The UAG automatically adds default SNAT settings for traffic flowing from this interface to an external interface.</p> <p>external is for connecting to an external network (like the Internet). The UAG automatically adds this interface to the default WAN trunk.</p> <p>For general, the rest of the screen's options do not automatically adjust and you must manually configure a policy route to add routing and SNAT settings for the interface.</p>
Interface Name	Specify a name for the interface. It can use alphanumeric characters, hyphens, and underscores, and it can be up to 11 characters long.
Port	This is the name of the Ethernet interface's physical port.
Zone	Select the zone to which this interface is to belong. You use zones to apply security settings such as security policy control, and remote management.
MAC Address	This field is read-only. This is the MAC address that the Ethernet interface uses.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and () + / : = ? ! * # @ \$ % _ - characters, and it can be up to 60 characters long.
IP Address Assignment	These IP address fields configure an IPv4 IP address on the interface itself. If you change this IP address on the interface, you may also need to change a related address object for the network connected to the interface. For example, if you use this screen to change the IP address of your LAN interface, you should also change the corresponding LAN subnet address object.
Get Automatically	This option appears when Interface Type is external or general . Select this to make the interface a DHCP client and automatically get the IP address, subnet mask, and gateway address from a DHCP server.
Use Fixed IP Address	This option appears when Interface Type is external or general . Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	This option appears when Interface Type is external or general . Enter the IP address of the gateway. The UAG sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	This option appears when Interface Type is external or general . Enter the priority of the gateway (if any) on this interface. The UAG decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the UAG uses the one that was configured first.
Interface Parameters	

Table 67 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the UAG can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the UAG can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the UAG divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
Connectivity Check	These fields appear when Interface Type is external or general . The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the UAG stops routing to the gateway. The UAG resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select icmp to have the UAG regularly ping the gateway you specify to make sure it is still available. Select tcp to have the UAG regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the UAG stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the Check Method to tcp . Specify the port number to use for a TCP connectivity check.
DHCP Setting	This section appears when Interface Type is internal .
DHCP	Select what type of DHCP service the UAG provides to the network. Choices are: None - the UAG does not provide any DHCP services. There is already a DHCP server on the network. DHCP Relay - the UAG routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. DHCP Server - the UAG assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The UAG is the DHCP server for the network.
	These fields appear if the UAG is a DHCP Relay .
Relay Server 1	Enter the IP address of a DHCP server for the network.
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.
	These fields appear if the UAG is a DHCP Server .

Table 67 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
IP Pool Start Address	<p>Enter the IP address from which the UAG begins allocating IP addresses. If you want to assign a static IP address to a specific computer, use the Static DHCP Table.</p> <p>If this field is blank, the Pool Size must also be blank. In this case, the UAG can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.</p>
Pool Size	<p>Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's Subnet Mask. For example, if the Subnet Mask is 255.255.255.0 and IP Pool Start Address is 10.10.10.10, the UAG can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses.</p> <p>If this field is blank, the IP Pool Start Address must also be blank. In this case, the UAG can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.</p>
First DNS Server, Second DNS Server, Third DNS Server	<p>Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses.</p> <p>Custom Defined - enter a static IP address.</p> <p>From ISP - select the DNS server that another interface received from its DHCP server.</p> <p>Device - the DHCP clients use the IP address of this interface and the UAG works as a DNS relay.</p>
First WINS Server, Second WINS Server	<p>Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.</p>
Default Router	<p>If you set this interface to DHCP Server, you can select to use either the interface's IP address or another IP address as the default router. This default router will become the DHCP clients' default gateway.</p> <p>To use another IP address as the default router, select Custom Defined and enter the IP address.</p>
Lease time	<p>Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are:</p> <p>infinite - select this if IP addresses never expire.</p> <p>days, hours, and minutes - select this to enter how long IP addresses are valid.</p>
Extended Options	<p>This table is available if you selected DHCP server.</p> <p>Configure this table if you want to send more information to DHCP clients through DHCP packets.</p>
Add	<p>Click this to create an entry in this table. See Section 10.3.3 on page 166.</p>
Edit	<p>Select an entry in this table and click this to modify it.</p>
Remove	<p>Select an entry in this table and click this to delete it.</p>
#	<p>This field is a sequential value, and it is not associated with any entry.</p>
Name	<p>This is the name of the DHCP option.</p>
Code	<p>This is the code number of the DHCP option.</p>
Type	<p>This is the type of the set value for the DHCP option.</p>
Value	<p>This is the value set for the DHCP option.</p>
Enable IP/MAC Binding	<p>Select this option to have this interface enforce links between specific IP addresses and specific MAC addresses. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.</p>

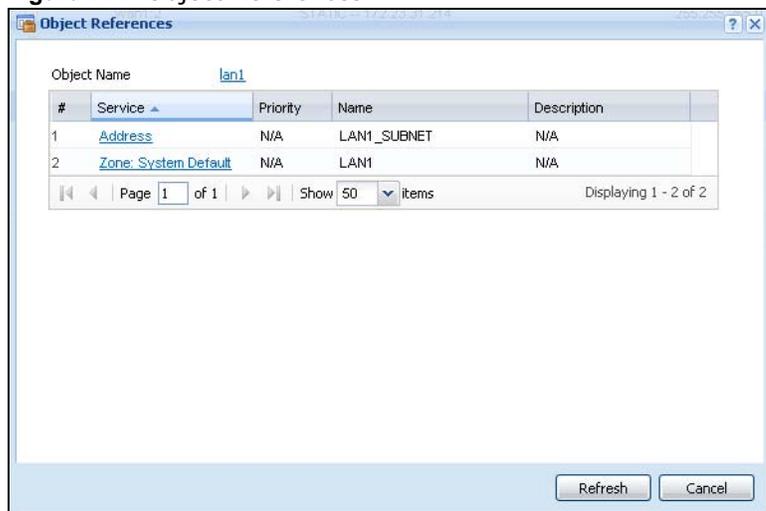
Table 67 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Enable Logs for IP/MAC Binding Violation	Select this option to have the UAG generate a log if a device connected to this interface attempts to use an IP address that is bound to another device's MAC address.
Static DHCP Table	Configure a list of static IP addresses the UAG assigns to computers connected to the interface. Otherwise, the UAG assigns an IP address dynamically using the interface's IP Pool Start Address and Pool Size .
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific entry.
IP Address	Enter the IP address to assign to a device with this entry's MAC address.
MAC	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry. You can use alphanumeric and () +/ :=?!*#@\$_%- characters, and it can be up to 60 characters long.
MAC Address Setting	This section appears when Interface Type is external or general . Have the interface use either the factory assigned default MAC address, a manually specified MAC address, or clone the MAC address of another device or computer.
Use Default MAC Address	Select this option to have the interface use the factory assigned default MAC address. By default, the UAG uses the factory assigned MAC address to identify itself.
Overwrite Default MAC Address	Select this option to have the interface use a different MAC address. Either enter the MAC address in the fields or click Clone by host and enter the IP address of the device or computer whose MAC you are cloning. Once it is successfully configured, the address will be copied to the configuration file. It will not change unless you change the setting or upload a different configuration file.
Related Setting	
Configure PPPoE/PPTP	Click PPPoE/PPTP if this interface's Internet connection uses PPPoE or PPTP.
Configure WAN TRUNK	Click WAN TRUNK to go to a screen where you can set this interface to be part of a WAN trunk for load balancing. This field appears when Interface Type is general .
Configure Policy Route	Click Policy Route to go to the policy route summary screen where you can manually associate traffic with this interface. You must manually configure a policy route to add routing and SNAT settings for an interface with the Interface Type set to general . You can also configure a policy route to override the default routing and SNAT behavior for an interface with an Interface Type of internal or external .
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

10.3.2 Object References

When a configuration screen includes an **Object Reference** icon, select a configuration object and click **Object Reference** to open the **Object Reference** screen. This screen displays which configuration settings reference the selected object. The fields shown vary with the type of object.

Figure 114 Object References



The following table describes labels that can appear in this screen.

Table 68 Object References

LABEL	DESCRIPTION
Object Name	This identifies the object for which the configuration settings that use it are displayed. Click the object's name to display the object's configuration screen in the main window.
#	This field is a sequential value, and it is not associated with any entry.
Service	This is the type of setting that references the selected object. Click a service's name to display the service's configuration screen in the main window.
Priority	If it is applicable, this field lists the referencing configuration item's position in its list, otherwise N/A displays.
Name	This field identifies the configuration item that references the object.
Description	If the referencing configuration item has a description configured, it displays here.
Refresh	Click this to update the information in this screen.
Cancel	Click Cancel to close the screen.

10.3.3 Add/Edit DHCP Extended Options

When you configure an interface as a DHCPv4 server, you can additionally add DHCP extended options which have the UAG to add more information in the DHCP packets. The available fields vary depending on the DHCP option you select in this screen. To open the screen, click **Configuration > Network > Interface > Ethernet > Edit**, select **DHCP Server** in the **DHCP Setting** section, and then click **Add** or **Edit** in the **Extended Options** table.

Figure 115 Configuration > Network > Interface > Ethernet > Edit > Add/Edit Extended Options

The following table describes labels that can appear in this screen.

Table 69 Configuration > Network > Interface > Ethernet > Edit > Add/Edit Extended Options

LABEL	DESCRIPTION
Option	Select which DHCP option that you want to add in the DHCP packets sent through the interface. See Table 70 for more information.
Name	This field displays the name of the selected DHCP option. If you selected User Defined in the Option field, enter a descriptive name to identify the DHCP option. You can enter up to 16 characters ("a-z", "A-Z", "0-9", "-", and "_") with no spaces allowed. The first character must be alphabetical (a-z, A-Z).
Code	This field displays the code number of the selected DHCP option. If you selected User Defined in the Option field, enter a number for the option. This field is mandatory.
Type	This is the type of the selected DHCP option. If you selected User Defined in the Option field, select an appropriate type for the value that you will enter in the next field. Only advanced users should configure User Defined . Misconfiguration could result in interface lockout.
Value	Enter the value for the selected DHCP option. For example, if you selected TFTP Server Name (66) and the type is TEXT , enter the DNS domain name of a TFTP server here. If you selected the Time Offset (2) option, the type is Boolean and you have to enter a Boolean value which should be either 0 or 1, where 1 interpreted as true and 0 is interpreted as false. This field is mandatory.
First IP Address, Second IP Address, Third IP Address	If you selected Time Server (4) , NTP Server (41) , SIP Server (120) , CAPWAP AC (138) , or TFTP Server (150) , you have to enter at least one IP address of the corresponding servers in these fields. The servers should be listed in order of your preference.
First Enterprise ID, Second Enterprise ID	If you selected VIVC (124) or VIVS (125) , you have to enter at least one vendor's 32-bit enterprise number in these fields. An enterprise number is a unique number that identifies a company.
First Class, Second Class	If you selected VIVC (124) , enter the details of the hardware configuration of the host on which the client is running, or of industry consortium compliance.
First Information, Second Information	If you selected VIVS (125) , enter additional information for the corresponding enterprise number in these fields.
First FQDN, Second FQDN, Third FQDN	If the Type is FQDN , you have to enter at least one domain name of the corresponding servers in these fields. The servers should be listed in order of your preference.

Table 69 Configuration > Network > Interface > Ethernet > Edit > Add/Edit Extended Options

LABEL	DESCRIPTION
OK	Click this to close this screen and update the settings to the previous Edit screen.
Cancel	Click Cancel to close the screen.

The following table lists the available DHCP extended options (defined in RFCs) on the UAG. See RFCs for more information.

Table 70 DHCP Extended Options

OPTION NAME	CODE	DESCRIPTION
Time Offset	2	This option specifies the offset of the client's subnet in seconds from Coordinated Universal Time (UTC).
Time Server	4	This option specifies a list of Time servers available to the client.
NTP Server	42	This option specifies a list of the NTP servers available to the client by IP address.
TFTP Server Name	66	This option is used to identify a TFTP server when the "sname" field in the DHCP header has been used for DHCP options. The minimum length of the value is 1.
Bootfile	67	This option is used to identify a bootfile when the "file" field in the DHCP header has been used for DHCP options. The minimum length of the value is 1.
SIP Server	120	This option carries either an IPv4 address or a DNS domain name to be used by the SIP client to locate a SIP server.
VIVC	124	Vendor-Identifying Vendor Class option A DHCP client may use this option to unambiguously identify the vendor that manufactured the hardware on which the client is running, the software in use, or an industry consortium to which the vendor belongs.
VIVS	125	Vendor-Identifying Vendor-Specific option DHCP clients and servers may use this option to exchange vendor-specific information.
CAPWAP AC	138	CAPWAP Access Controller addresses option The Control And Provisioning of Wireless Access Points Protocol allows a Wireless Termination Point (WTP) to use DHCP to discover the Access Controllers to which it is to connect. This option carries a list of IPv4 addresses indicating one or more CAPWAP ACs available to the WTP.
TFTP Server	150	The option contains one or more IPv4 addresses that the client may use. The current use of this option is for downloading configuration from a VoIP server via TFTP; however, the option may be used for purposes other than contacting a VoIP configuration server.

10.4 PPP Interfaces

Use PPPoE/PPTP interfaces to connect to your ISP. This way, you do not have to install or manage PPPoE/PPTP software on each computer in the network.

Figure 116 Example: PPPoE/PPTP Interfaces

PPPoE/PPTP interfaces are similar to other interfaces in some ways. They have an IP address, subnet mask, and gateway used to make routing decisions; they restrict bandwidth and packet size; and they can verify the gateway is available. There are two main differences between PPPoE/PPTP interfaces and other interfaces.

- You must also configure an ISP account object for the PPPoE/PPTP interface to use.
Each ISP account specifies the protocol (PPPoE or PPTP), as well as your ISP account information. If you change ISPs later, you only have to create a new ISP account, not a new PPPoE/PPTP interface. You should not have to change any network policies.
- You do not set up the subnet mask or gateway.
PPPoE/PPTP interfaces are interfaces between the UAG and only one computer. Therefore, the subnet mask is always 255.255.255.255. In addition, the UAG always treats the ISP as a gateway.

10.4.1 PPP Interface Summary

This screen lists every PPPoE/PPTP interface. To access this screen, click **Configuration > Network > Interface > PPP**.

Figure 117 Configuration > Network > Interface > PPP

The screenshot shows the 'PPP' configuration page. At the top, there are tabs for 'Port Role', 'Ethernet', 'PPP', 'VLAN', 'Bridge', and 'Trunk'. Below the tabs is a 'User Configuration' section with a table of PPP interfaces. The table has columns for '#', 'Status', 'Name', 'Base Interface', and 'Account Profile'. Below the table is a 'System Default' section with a table of system default PPP interfaces. The table has columns for '#', 'Status', 'Name', 'Base Interface', and 'Account Profile'. At the bottom of the page are 'Apply' and 'Reset' buttons.

#	Status	Name	Base Interface	Account Profile
1		wan1_ppp	wan1	WAN1_PPPoE_ACCOUNT

Each field is described in the table below.

Table 71 Configuration > Network > Interface > PPP

LABEL	DESCRIPTION
User Configuration / System Default	The UAG comes with the (non-removable) System Default PPP interfaces pre-configured. You can create (and delete) User Configuration PPP interfaces.
Add	Click this to create a new user-configured PPP interface.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove a user-configured PPP interface, select it and click Remove . The UAG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
Connect	To connect an interface, select it and click Connect . You might use this in testing the interface or to manually establish the connection for a Dial-on-Demand PPPoE/PPTP interface.
Disconnect	To disconnect an interface, select it and click Disconnect . You might use this in testing the interface.
Object Reference	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 10.3.2 on page 165 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The connect icon is lit when the interface is connected and dimmed when it is disconnected.
Name	This field displays the name of the interface.
Base Interface	This field displays the interface on the top of which the PPPoE/PPTP interface is.
Account Profile	This field displays the ISP account used by this PPPoE/PPTP interface.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

10.4.2 PPP Interface Add or Edit

Note: You have to set up an ISP account before you create a PPPoE/PPTP interface.

This screen lets you configure a PPPoE or PPTP interface. To access this screen, click the **Add** icon or select an entry in the PPP interface summary screen and click the **Edit** icon.

Figure 118 Configuration > Network > Interface > PPP > Add

Add PPPoE/PPTP [?] [X]

Hide Advanced Settings Create new Object ▾

General Settings

Enable Interface

Interface Properties

Interface Name: ⓘ

Base Interface: ▾

Zone: ▾

Description: (Optional)

Connectivity

Nailed-Up

Dial-on-Demand

ISP Setting

Account Profile: ▾

IP Address Assignment

Get Automatically 0.0.0.0

Use Fixed IP Address

IP Address:

Gateway: (Optional)

Metric: (0-15)

Interface Parameters

Egress Bandwidth: Kbps

Ingress Bandwidth: Kbps

MTU: Bytes

Connectivity Check

Enable Connectivity Check

Check Method: ▾

Check Period: (5-30 seconds)

Check Timeout: (1-10 seconds)

Check Fail Tolerance: (1-10)

Check Default Gateway 0.0.0.0

Check this address (Domain Name or IP Address)

Check Port: (1-65535)

Related Setting

Configure [WAN_TRUNK](#)

Configure [Policy Route](#)

Each field is explained in the following table.

Table 72 Configuration > Network > Interface > PPP > Add

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create new object	Click this button to create an ISP Account that you may use for the ISP settings in this screen.
General Settings	
Enable Interface	Select this to enable this interface. Clear this to disable this interface.
Interface Properties	
Interface Name	Specify a name for the interface. It can use alphanumeric characters, hyphens, and underscores, and it can be up to 11 characters long.
Base Interface	Select the interface upon which this PPP interface is built. Note: Multiple PPP interfaces can use the same base interface.
Zone	Select the zone to which this PPP interface belongs. The zone determines the security settings the UAG uses for the interface.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and () + / : = ? ! * # @ \$ _ % - characters, and it can be up to 60 characters long.
Connectivity	
Nailed-Up	Select this if the PPPoE/PPTP connection should always be up. Clear this to have the UAG establish the PPPoE/PPTP connection only when there is traffic. You might use this option if a lot of traffic needs to go through the interface or it does not cost extra to keep the connection up all the time.
Dial-on-Demand	Select this to have the UAG establish the PPPoE/PPTP connection only when there is traffic. You might use this option if there is little traffic through the interface or if it costs money to keep the connection available.
ISP Setting	
Account Profile	Select the ISP account that this PPPoE/PPTP interface uses. The drop-down box lists ISP accounts by name. Use Create new Object if you need to configure a new ISP account (see Chapter 45 on page 483 for details).
Protocol	This field is read-only. It displays the protocol specified in the ISP account.
User Name	This field is read-only. It displays the user name for the ISP account.
Service Name	This field is read-only. It displays the PPPoE service name specified in the ISP account. This field is not available if the ISP account uses PPTP.
Server IP	This field is read-only. It displays the IP address of the PPTP server specified in the ISP account. This field is not available if the ISP account uses PPPoE.
Connection ID	This field is read-only. It displays the identification name for the PPTP server specified in the ISP account. This field is not available if the ISP account uses PPPoE.
IP Address Assignment	Click Show Advanced Settings to display more settings. Click Hide Advanced Settings to display fewer settings.
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address automatically. The subnet mask and gateway are always defined automatically in PPPoE/PPTP interfaces.
Use Fixed IP Address	Select this if you want to specify the IP address manually.

Table 72 Configuration > Network > Interface > PPP > Add (continued)

LABEL	DESCRIPTION
IP Address	This field is enabled if you select Use Fixed IP Address . Enter the IP address for this interface.
Gateway	This field is enabled if you select Use Fixed IP Address . Enter the IP address of the gateway. The UAG sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (the ISP) on this interface. The UAG decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the UAG uses the one that was configured first.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the UAG can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the UAG can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the UAG divides it into smaller fragments. Allowed values are 576 - 1492. Usually, this value is 1492.
Connectivity Check	The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the UAG stops routing to the gateway. The UAG resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select icmp to have the UAG regularly ping the gateway you specify to make sure it is still available. Select tcp to have the UAG regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the UAG stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the Check Method to tcp . Specify the port number to use for a TCP connectivity check.
Related Setting	
Configure WAN_TRUNK	Click WAN_TRUNK to go to a screen where you can configure the interface as part of a WAN trunk for load balancing.
Policy Route	Click Policy Route to go to the screen where you can manually configure a policy route to associate traffic with this interface.

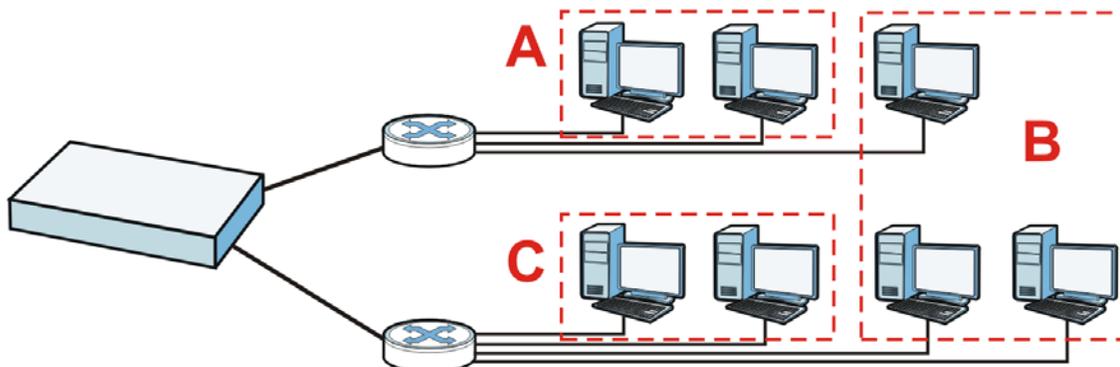
Table 72 Configuration > Network > Interface > PPP > Add (continued)

LABEL	DESCRIPTION
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

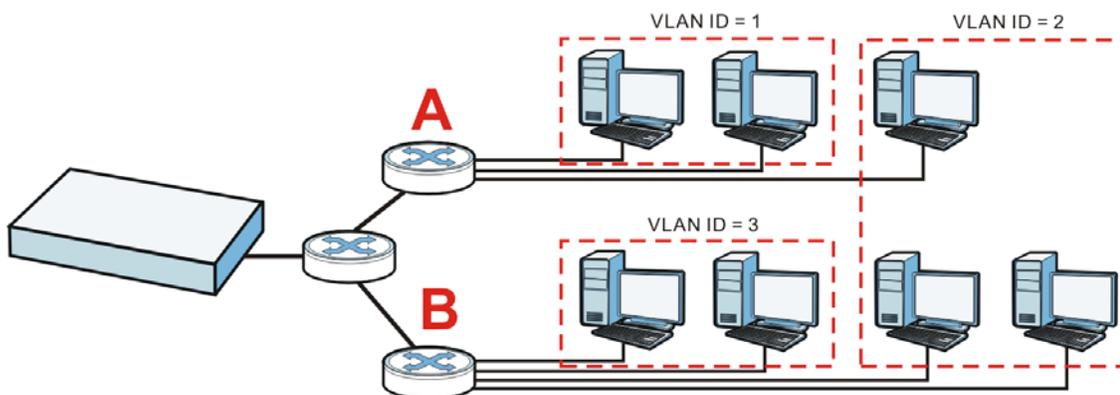
10.5 VLAN Interfaces

A Virtual Local Area Network (VLAN) divides a physical network into multiple logical networks. The standard is defined in IEEE 802.1q.

In this example, there are two physical networks and three departments **A**, **B**, and **C**. The physical networks are connected to hubs, and the hubs are connected to the router.

Figure 119 Example: Before VLAN

Alternatively, you can divide the physical networks into three VLANs.

Figure 120 Example: After VLAN

Each VLAN is a separate network with separate IP addresses, subnet masks, and gateways. Each VLAN also has a unique identification number (ID). The ID is a 12-bit value that is stored in the MAC header. The VLANs are connected to switches, and the switches are connected to the router. (If one switch has enough connections for the entire network, the network does not need switches **A** and **B**.)

- Traffic inside each VLAN is layer-2 communication (data link layer, MAC addresses). It is handled by the switches. As a result, the new switch is required to handle traffic inside VLAN 2. Traffic is only broadcast inside each VLAN, not each physical network.
- Traffic between VLANs (or between a VLAN and another type of network) is layer-3 communication (network layer, IP addresses). It is handled by the router.

This approach provides a few advantages.

- Increased performance - In VLAN 2, the extra switch should route traffic inside the sales department faster than the router does. In addition, broadcasts are limited to smaller, more logical groups of users.
- Higher security - If each computer has a separate physical connection to the switch, then broadcast traffic in each VLAN is never sent to computers in another VLAN.
- Better manageability - You can align network policies more appropriately for users. For example, you can set different bandwidth limits for each VLAN (each department in the example above). These rules are also independent of the physical network, so you can change the physical network without changing policies.

In this example, the new switch handles the following types of traffic:

- Inside VLAN 2.
- Between the router and VLAN 1.
- Between the router and VLAN 2.
- Between the router and VLAN 3.

VLAN Interfaces Overview

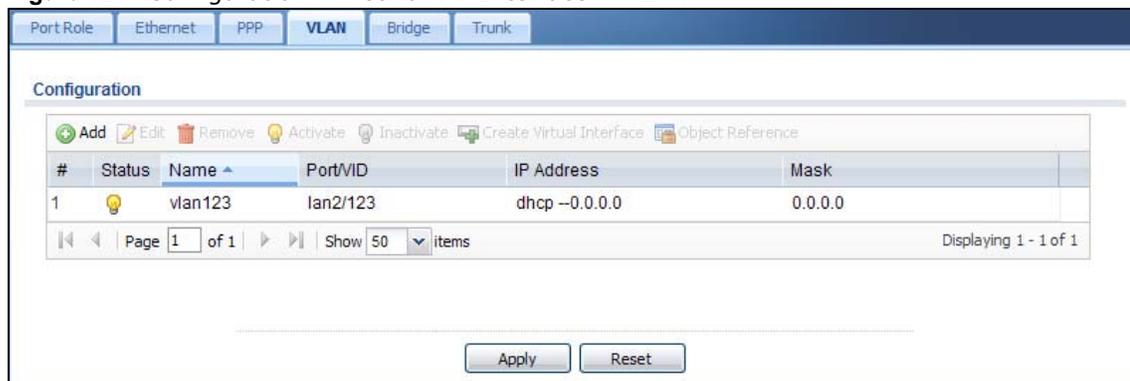
In the UAG, each VLAN is called a VLAN interface. As a router, the UAG routes traffic between VLAN interfaces, but it does not route traffic within a VLAN interface. All traffic for each VLAN interface can go through only one Ethernet interface, though each Ethernet interface can have one or more VLAN interfaces.

Note: Each VLAN interface is created on top of only one Ethernet interface.

Otherwise, VLAN interfaces are similar to other interfaces in many ways. They have an IP address, subnet mask, and gateway used to make routing decisions. They restrict bandwidth and packet size. They can provide DHCP services, and they can verify the gateway is available.

10.5.1 VLAN Interface Summary Screen

This screen lists every VLAN interface and virtual interface created on top of VLAN interfaces. To access this screen, click **Configuration > Network > Interface > VLAN**.

Figure 121 Configuration > Network > Interface > VLAN

Each field is explained in the following table.

Table 73 Configuration > Network > Interface > VLAN

LABEL	DESCRIPTION
Add	Click this to create a new VLAN interface.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
Create Virtual Interface	To open the screen where you can create a virtual interface, select an interface and click Create Virtual Interface .
Object References	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 10.3.2 on page 165 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the interface.
Port/VID	For VLAN interfaces, this field displays <ul style="list-style-type: none"> the Ethernet interface on which the VLAN interface is created the VLAN ID For virtual interfaces, this field is blank.
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet. This screen also shows whether the IP address is a static IP address (static) or dynamically assigned (dhcp). IP addresses are always static in virtual interfaces.
Mask	This field displays the interface's subnet mask in dot decimal notation.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

10.5.2 VLAN Interface Add/Edit

This screen lets you configure IP address assignment, interface bandwidth parameters, DHCP settings, and connectivity check for each VLAN interface. To access this screen, click the **Add** icon

or select an entry in the **VLAN** summary screen and click the **Edit** icon. The following screen appears.

Figure 122 Configuration > Network > Interface > VLAN > Edit

Add VLAN

Hide Advanced Settings

General Settings

Enable Interface

Interface Properties

Interface Type: ⓘ

Interface Name: ⓘ

Zone: ⓘ

Base Port:

VLAN ID: ⓘ

Description: (Optional)

IP Address Assignment

Get Automatically

Use Fixed IP Address

IP Address:

Subnet Mask:

Gateway: (Optional)

Metric: (0-15)

Interface Parameters

Egress Bandwidth: Kbps

Ingress Bandwidth: Kbps

MTU: Bytes

Connectivity Check

Enable Connectivity Check

Check Method:

Check Period: (5-30 seconds)

Check Timeout: (1-10 seconds)

Check Fail Tolerance: (1-10)

Check Default Gateway 0.0.0.0

Check this address (Domain Name or IP Address)

DHCP Setting

DHCP:

IP Pool Start Address (Optional): ⓘ Pool Size: ⓘ

First DNS Server (Optional):

Second DNS Server (Optional):

Third DNS Server (Optional):

First WINS Server (Optional):

Second WINS Server (Optional):

Default Router (Optional):

Lease Time: infinite

days hours (Optional) minutes (Optional)

Extended Options

Enable IP/MAC Binding

Enable Logs for IP/MAC Binding Violation

Static DHCP Table

Enable IP/MAC Binding

Enable Logs for IP/MAC Binding Violation

Related Setting

[Configure WAN TRUNK](#)

[Configure Policy Route](#)

Each field is explained in the following table.

Table 74 Configuration > Network > Interface > VLAN > Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
General Settings	
Enable Interface	Select this to turn this interface on. Clear this to disable this interface.
Interface Properties	
Interface Type	<p>Select one of the following option depending on the type of network to which the UAG is connected or if you want to additionally manually configure some related settings.</p> <p>internal is for connecting to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The UAG automatically adds default SNAT settings for traffic flowing from this interface to an external interface.</p> <p>external is for connecting to an external network (like the Internet). The UAG automatically adds this interface to the default WAN trunk.</p> <p>For general, the rest of the screen's options do not automatically adjust and you must manually configure a policy route to add routing and SNAT settings for the interface.</p>
Interface Name	This field is read-only if you are editing an existing VLAN interface. Enter the number of the VLAN interface. You can use a number from 0~4094. For example, vlan0, vlan8, and so on. The total number of VLANs you can configure on the UAG depends on the model.
Zone	Select the zone to which the VLAN interface belongs.
Base Port	Select the Ethernet interface on which the VLAN interface runs.
VLAN ID	Enter the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 - 4094. (0 and 4095 are reserved.)
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and () + / : = ? ! * # @ \$ _ % - characters, and it can be up to 60 characters long.
IP Address Assignment	
Get Automatically	This option appears when Interface Type is external or general . Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address, subnet mask, and gateway automatically.
Use Fixed IP Address	This option appears when Interface Type is external or general . Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	<p>This field is enabled if you select Use Fixed IP Address.</p> <p>Enter the IP address for this interface.</p>
Subnet Mask	<p>This field is enabled if you select Use Fixed IP Address.</p> <p>Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.</p>
Gateway	<p>This option appears when Interface Type is external or general. This field is enabled if you select Use Fixed IP Address.</p> <p>Enter the IP address of the gateway. The UAG sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.</p>
Metric	This option appears when Interface Type is external or general . Enter the priority of the gateway (if any) on this interface. The UAG decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the UAG uses the one that was configured first.

Table 74 Configuration > Network > Interface > VLAN > Edit (continued)

LABEL	DESCRIPTION
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the UAG can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the UAG can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the UAG divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
Connectivity Check	The UAG can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often to check the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the UAG stops routing to the gateway. The UAG resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select icmp to have the UAG regularly ping the gateway you specify to make sure it is still available. Select tcp to have the UAG regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the UAG stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the Check Method to tcp . Specify the port number to use for a TCP connectivity check.
DHCP Setting	The DHCP settings are available for the LAN interfaces.
DHCP	Select what type of DHCP service the UAG provides to the network. Choices are: None - the UAG does not provide any DHCP services. There is already a DHCP server on the network. DHCP Relay - the UAG routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. DHCP Server - the UAG assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The UAG is the DHCP server for the network.
	These fields appear if the UAG is a DHCP Relay .
Relay Server 1	Enter the IP address of a DHCP server for the network.
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.
	These fields appear if the UAG is a DHCP Server .

Table 74 Configuration > Network > Interface > VLAN > Edit (continued)

LABEL	DESCRIPTION
IP Pool Start Address	<p>Enter the IP address from which the UAG begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click Add Static DHCP.</p> <p>If this field is blank, the Pool Size must also be blank. In this case, the UAG can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.</p>
Pool Size	<p>Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's Subnet Mask. For example, if the Subnet Mask is 255.255.255.0 and IP Pool Start Address is 10.10.10.10, the UAG can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses.</p> <p>If this field is blank, the IP Pool Start Address must also be blank. In this case, the UAG can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.</p>
First DNS Server Second DNS Server Third DNS Server	<p>Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses.</p> <p>Custom Defined - enter a static IP address.</p> <p>From ISP - select the DNS server that another interface received from its DHCP server.</p> <p>Device - the DHCP clients use the IP address of this interface and the UAG works as a DNS relay.</p>
First WINS Server, Second WINS Server	<p>Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.</p>
Default Router	<p>If you set this interface to DHCP Server, you can select to use either the interface's IP address or another IP address as the default router. This default router will become the DHCP clients' default gateway.</p> <p>To use another IP address as the default router, select Custom Defined and enter the IP address.</p>
Lease time	<p>Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are:</p> <p>infinite - select this if IP addresses never expire.</p> <p>days, hours, and minutes - select this to enter how long IP addresses are valid.</p>
Extended Options	<p>This table is available if you selected DHCP server.</p> <p>Configure this table if you want to send more information to DHCP clients through DHCP packets.</p>
Add	Click this to create an entry in this table. See Section 10.3.3 on page 166 .
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
Name	This is the name of the DHCP option.
Code	This is the code number of the DHCP option.
Type	This is the type of the set value for the DHCP option.
Value	This is the value set for the DHCP option.
Enable IP/MAC Binding	<p>Select this option to have the UAG enforce links between specific IP addresses and specific MAC addresses for this VLAN. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.</p>

Table 74 Configuration > Network > Interface > VLAN > Edit (continued)

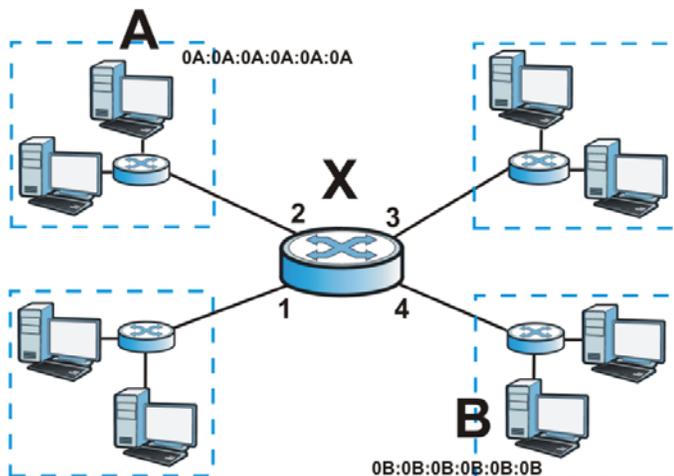
LABEL	DESCRIPTION
Enable Logs for IP/MAC Binding Violation	Select this option to have the UAG generate a log if a device connected to this VLAN attempts to use an IP address that is bound to another device's MAC address.
Static DHCP Table	Configure a list of static IP addresses the UAG assigns to computers connected to the interface. Otherwise, the UAG assigns an IP address dynamically using the interface's IP Pool Start Address and Pool Size .
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific entry.
IP Address	Enter the IP address to assign to a device with this entry's MAC address.
MAC	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry. You can use alphanumeric and ()+/:=?!*#@\$_%- characters, and it can be up to 60 characters long.
MAC Address Setting	This section appears when Interface Type is external or general . Have the interface use either the factory assigned default MAC address, a manually specified MAC address, or clone the MAC address of another device or computer.
Use Default MAC Address	Select this option to have the interface use the factory assigned default MAC address. By default, the UAG uses the factory assigned MAC address to identify itself.
Overwrite Default MAC Address	Select this option to have the interface use a different MAC address. Either enter the MAC address in the fields or click Clone by host and enter the IP address of the device or computer whose MAC you are cloning. Once it is successfully configured, the address will be copied to the configuration file. It will not change unless you change the setting or upload a different configuration file.
Related Setting	This section appears when Interface Type is general .
Configure WAN_TRUNK	Click WAN_TRUNK to go to a screen where you can set this VLAN to be part of a WAN trunk for load balancing.
Configure Policy Route	Click Policy Route to go to the screen where you can manually configure a policy route to associate traffic with this VLAN.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

10.6 Bridge Interfaces

This section introduces bridges and bridge interfaces and then explains the screens for bridge interfaces.

Bridge Overview

A bridge creates a connection between two or more network segments at the layer-2 (MAC address) level. In the following example, bridge **X** connects four network segments.



When the bridge receives a packet, the bridge records the source MAC address and the port on which it was received in a table. It also looks up the destination MAC address in the table. If the bridge knows on which port the destination MAC address is located, it sends the packet to that port. If the destination MAC address is not in the table, the bridge broadcasts the packet on every port (except the one on which it was received).

In the example above, computer A sends a packet to computer B. Bridge X records the source address 0A:0A:0A:0A:0A:0A and port 2 in the table. It also looks up 0B:0B:0B:0B:0B:0B in the table. There is no entry yet, so the bridge broadcasts the packet on ports 1, 3, and 4.

Table 75 Example: Bridge Table After Computer A Sends a Packet to Computer B

MAC ADDRESS	PORT
0A:0A:0A:0A:0A:0A	2

If computer B responds to computer A, bridge X records the source address 0B:0B:0B:0B:0B:0B and port 4 in the table. It also looks up 0A:0A:0A:0A:0A:0A in the table and sends the packet to port 2 accordingly.

Table 76 Example: Bridge Table After Computer B Responds to Computer A

MAC ADDRESS	PORT
0A:0A:0A:0A:0A:0A	2
0B:0B:0B:0B:0B:0B	4

Bridge Interface Overview

A bridge interface creates a software bridge between the members of the bridge interface. It also becomes the UAG's interface for the resulting network.

This UAG can bridge traffic between some interfaces while it routes traffic for other interfaces. The bridge interfaces also support more functions, like interface bandwidth parameters, DHCP settings, and connectivity check. To use the whole UAG as a transparent bridge, add all of the UAG's interfaces to a bridge interface.

A bridge interface may consist of the following members:

- Zero or one VLAN interfaces (and any associated virtual VLAN interfaces)
- Any number of Ethernet interfaces (and any associated virtual Ethernet interfaces)

When you create a bridge interface, the UAG removes the members' entries from the routing table and adds the bridge interface's entries to the routing table. For example, this table shows the routing table before and after you create bridge interface br0 (250.250.250.0/23) between lan1 and vlan1.

Table 77 Example: Routing Table Before and After Bridge Interface br0 Is Created

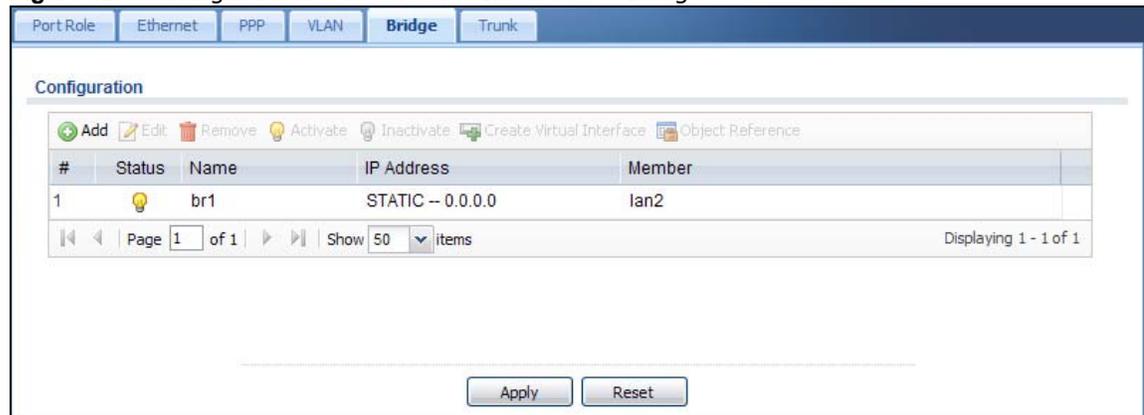
IP ADDRESS(ES)	DESTINATION	IP ADDRESS(ES)	DESTINATION
210.210.210.0/24	lan1	221.221.221.0/24	vlan0
210.211.1.0/24	lan1:1	230.230.230.192/26	wan1
221.221.221.0/24	vlan0	250.250.250.0/23	br0
222.222.222.0/24	vlan1		
230.230.230.192/26	wan1		

In this example, virtual Ethernet interface lan1:1 is also removed from the routing table when lan1 is added to br0. Virtual interfaces are automatically added to or removed from a bridge interface when the underlying interface is added or removed.

10.6.1 Bridge Interface Summary

This screen lists every bridge interface and virtual interface created on top of bridge interfaces. To access this screen, click **Configuration > Network > Interface > Bridge**.

Figure 123 Configuration > Network > Interface > Bridge



Each field is described in the following table.

Table 78 Configuration > Network > Interface > Bridge

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.

Table 78 Configuration > Network > Interface > Bridge (continued)

LABEL	DESCRIPTION
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
Create Virtual Interface	To open the screen where you can create a virtual interface, select an interface and click Create Virtual Interface .
Object Reference	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 10.3.2 on page 165 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the interface.
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet. This screen also shows whether the IP address is a static IP address (STATIC) or dynamically assigned (DHCP). IP addresses are always static in virtual interfaces.
Member	This field displays the Ethernet interfaces and VLAN interfaces in the bridge interface. It is blank for virtual interfaces.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

10.6.2 Bridge Interface Add/Edit

This screen lets you configure IP address assignment, interface bandwidth parameters, DHCP settings, and connectivity check for each bridge interface. To access this screen, click the **Add** icon, or select an entry in the **Bridge** summary screen and click the **Edit** icon. The following screen appears.

Figure 124 Configuration > Network > Interface > Bridge > Add

Add Bridge

Hide Advanced Settings

General Settings

Enable Interface

Interface Properties

Interface Type: ?

Interface Name: !

Zone: ?

Description: (Optional)

Member Configuration

Available

- wan1
- lan1
- lan2
- vlan1

Member

IP Address Assignment

Get Automatically

Use Fixed IP Address

IP Address:

Subnet Mask:

Gateway: (Optional)

Metric: (0-15)

Interface Parameters

Egress Bandwidth: Kbps

Ingress Bandwidth: Kbps

MTU: Bytes

DHCP Setting

DHCP:

IP Pool Start Address (Optional): ! Pool Size: !

First DNS Server (Optional): !

Second DNS Server (Optional): !

Third DNS Server (Optional): !

First WINS Server (Optional):

Second WINS Server (Optional):

Default Router (Optional):

Lease Time: infinite 3 days 0 hours (Optional) 0 minutes (Optional)

Extended Options

Enable IP/MAC Binding

Enable Logs for IP/MAC Binding Violation

Static DHCP Table

#	Name	Code	Type	Value
No data to display				

Connectivity Check

Enable Connectivity Check:

Check Method:

Check Period: (3-30 seconds)

Check Timeout: (1-10 seconds)

Check Fail Tolerance: (1-10)

Check Default Gateway:

Check this address: (Domain Name or IP Address)

Related Setting

[Configure WAN_TRUNKS](#)

[Configure Policy Route](#)

Each field is described in the table below.

Table 79 Configuration > Network > Interface > Bridge > Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
General Settings	
Enable Interface	Select this to enable this interface. Clear this to disable this interface.
Interface Properties	
Interface Type	Select one of the following option depending on the type of network to which the UAG is connected or if you want to additionally manually configure some related settings. internal is for connecting to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The UAG automatically adds default SNAT settings for traffic flowing from this interface to an external interface. external is for connecting to an external network (like the Internet). The UAG automatically adds this interface to the default WAN trunk. For general , the rest of the screen's options do not automatically adjust and you must manually configure a policy route to add routing and SNAT settings for the interface.
Interface Name	This field is read-only if you are editing the interface. Enter the name of the bridge interface. The format is brx, where x is 0 - 11. For example, br0, br3, and so on.
Zone	Select the zone to which the interface is to belong. You use zones to apply security settings such as security policy control, and remote management.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and () + / : = ? ! * # @ \$ _ % - characters, and it can be up to 60 characters long.
Member Configuration	
Available	This field displays Ethernet interfaces and VLAN interfaces that can become part of the bridge interface. An interface is not available in the following situations: <ul style="list-style-type: none"> • There is a virtual interface on top of it • It is already used in a different bridge interface Select one, and click the >> arrow to add it to the bridge interface. Each bridge interface can only have one VLAN interface.
Member	This field displays the interfaces that are part of the bridge interface. Select one, and click the << arrow to remove it from the bridge interface.
IP Address Assignment	
Get Automatically	This option appears when Interface Type is external or general . Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address, subnet mask, and gateway automatically.
Use Fixed IP Address	This option appears when Interface Type is external or general . Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	This field is enabled if you select Use Fixed IP Address . Enter the IP address for this interface.
Subnet Mask	This field is enabled if you select Use Fixed IP Address . Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.

Table 79 Configuration > Network > Interface > Bridge > Edit (continued)

LABEL	DESCRIPTION
Gateway	<p>This option appears when Interface Type is external or general. This field is enabled if you select Use Fixed IP Address.</p> <p>Enter the IP address of the gateway. The UAG sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.</p>
Metric	<p>This option appears when Interface Type is external or general. Enter the priority of the gateway (if any) on this interface. The UAG decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the UAG uses the one that was configured first.</p>
Interface Parameters	
Egress Bandwidth	<p>Enter the maximum amount of traffic, in kilobits per second, the UAG can send through the interface to the network. Allowed values are 0 - 1048576.</p>
Ingress Bandwidth	<p>This is reserved for future use.</p> <p>Enter the maximum amount of traffic, in kilobits per second, the UAG can receive from the network through the interface. Allowed values are 0 - 1048576.</p>
MTU	<p>Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the UAG divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.</p>
DHCP Setting	
DHCP	<p>Select what type of DHCP service the UAG provides to the network. Choices are:</p> <p>None - the UAG does not provide any DHCP services. There is already a DHCP server on the network.</p> <p>DHCP Relay - the UAG routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network.</p> <p>DHCP Server - the UAG assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The UAG is the DHCP server for the network.</p>
	<p>These fields appear if the UAG is a DHCP Relay.</p>
Relay Server 1	<p>Enter the IP address of a DHCP server for the network.</p>
Relay Server 2	<p>This field is optional. Enter the IP address of another DHCP server for the network.</p>
	<p>These fields appear if the UAG is a DHCP Server.</p>
IP Pool Start Address	<p>Enter the IP address from which the UAG begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click Add Static DHCP.</p> <p>If this field is blank, the Pool Size must also be blank. In this case, the UAG can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.</p>
Pool Size	<p>Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's Subnet Mask. For example, if the Subnet Mask is 255.255.255.0 and IP Pool Start Address is 10.10.10.10, the UAG can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses.</p> <p>If this field is blank, the IP Pool Start Address must also be blank. In this case, the UAG can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.</p>

Table 79 Configuration > Network > Interface > Bridge > Edit (continued)

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. Custom Defined - enter a static IP address. From ISP - select the DNS server that another interface received from its DHCP server. Device - the DHCP clients use the IP address of this interface and the UAG works as a DNS relay.
First WINS Server, Second WINS Server	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Default Router	If you set this interface to DHCP Server , you can select to use either the interface's IP address or another IP address as the default router. This default router will become the DHCP clients' default gateway. To use another IP address as the default router, select Custom Defined and enter the IP address.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: infinite - select this if IP addresses never expire days, hours, and minutes - select this to enter how long IP addresses are valid.
Extended Options	This table is available if you selected DHCP server . Configure this table if you want to send more information to DHCP clients through DHCP packets.
Add	Click this to create an entry in this table. See Section 10.3.3 on page 166 .
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
Name	This is the name of the DHCP option.
Code	This is the code number of the DHCP option.
Type	This is the type of the set value for the DHCP option.
Value	This is the value set for the DHCP option.
Enable IP/MAC Binding	Select this option to have this interface enforce links between specific IP addresses and specific MAC addresses. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.
Enable Logs for IP/MAC Binding Violation	Select this option to have the UAG generate a log if a device connected to this interface attempts to use an IP address that is bound to another device's MAC address.
Static DHCP Table	Configure a list of static IP addresses the UAG assigns to computers connected to the interface. Otherwise, the UAG assigns an IP address dynamically using the interface's IP Pool Start Address and Pool Size .
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific entry.
IP Address	Enter the IP address to assign to a device with this entry's MAC address.
MAC Address	Enter the MAC address to which to assign this entry's IP address.

Table 79 Configuration > Network > Interface > Bridge > Edit (continued)

LABEL	DESCRIPTION
Description	Enter a description to help identify this static DHCP entry. You can use alphanumeric and ()+/:=?!*#@\$_%- characters, and it can be up to 60 characters long.
Connectivity Check	The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the UAG stops routing to the gateway. The UAG resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select icmp to have the UAG regularly ping the gateway you specify to make sure it is still available. Select tcp to have the UAG regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the UAG stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the Check Method to tcp . Specify the port number to use for a TCP connectivity check.
Related Setting	
Configure WAN TRUNK	Click WAN TRUNK to go to a screen where you can configure the interface as part of a WAN trunk for load balancing.
Configure Policy Route	Click Policy Route to go to the screen where you can manually configure a policy route to associate traffic with this bridge interface.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

10.7 Virtual Interfaces

Use virtual interfaces to tell the UAG where to route packets.

Virtual interfaces can be created on top of Ethernet interfaces, VLAN interfaces, or bridge interfaces. Virtual VLAN interfaces recognize and use the same VLAN ID. Otherwise, there is no difference between each type of virtual interface. Network policies (for example, security policy control rules) that apply to the underlying interface automatically apply to the virtual interface as well.

Like other interfaces, virtual interfaces have an IP address, subnet mask, and gateway used to make routing decisions. However, you have to manually specify the IP address and subnet mask; virtual interfaces cannot be DHCP clients. Like other interfaces, you can restrict bandwidth through virtual interfaces, but you cannot change the MTU. The virtual interface uses the same MTU that the

underlying interface uses. Unlike other interfaces, virtual interfaces do not provide DHCP services, and they do not verify that the gateway is available.

10.7.1 Virtual Interfaces Add/Edit

This screen lets you configure IP address assignment and interface parameters for virtual interfaces. To access this screen, click the **Create Virtual Interface** icon in the Ethernet, VLAN, or bridge interface summary screen.

Figure 125 Configuration > Network > Interface > Create Virtual Interface

Each field is described in the table below.

Table 80 Configuration > Network > Interface > Create Virtual Interface

LABEL	DESCRIPTION
Interface Properties	
Interface Name	This field is read-only. It displays the name of the virtual interface, which is automatically derived from the underlying Ethernet interface, VLAN interface, or bridge interface.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and () + / : = ? ! * # @ \$ _ % - characters, and it can be up to 60 characters long.
IP Address Assignment	
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	Enter the IP address of the gateway. The UAG sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The UAG decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the UAG uses the one that was configured first.
Interface Parameters	

Table 80 Configuration > Network > Interface > Create Virtual Interface (continued)

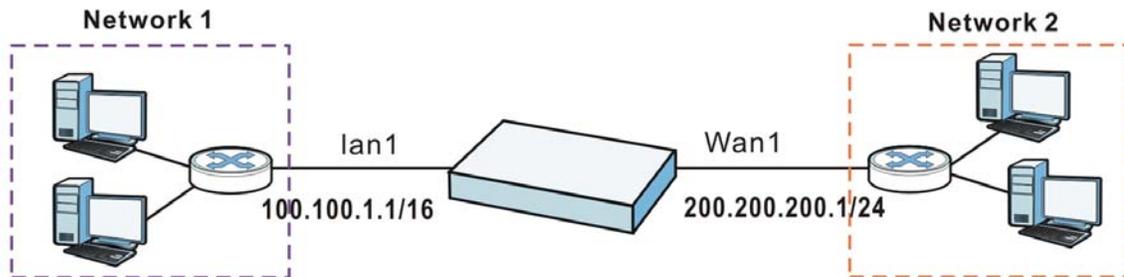
LABEL	DESCRIPTION
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the UAG can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the UAG can receive from the network through the interface. Allowed values are 0 - 1048576.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

10.8 Interface Technical Reference

Here is more detailed information about interfaces on the UAG.

IP Address Assignment

Most interfaces have an IP address and a subnet mask. This information is used to create an entry in the routing table.

Figure 126 Example: Entry in the Routing Table Derived from Interfaces**Table 81** Example: Routing Table Entries for Interfaces

IP ADDRESS(ES)	DESTINATION
100.100.1.1/16	lan1
200.200.200.1/24	wan1

For example, if the UAG gets a packet with a destination address of 100.100.25.25, it routes the packet to interface lan1. If the UAG gets a packet with a destination address of 200.200.200.200, it routes the packet to interface wan1.

In most interfaces, you can enter the IP address and subnet mask manually. In PPPoE/PPTP interfaces, however, the subnet mask is always 255.255.255.255 because it is a point-to-point interface. For these interfaces, you can only enter the IP address.

In many interfaces, you can also let the IP address and subnet mask be assigned by an external DHCP server on the network. In this case, the interface is a DHCP client. Virtual interfaces, however, cannot be DHCP clients. You have to assign the IP address and subnet mask manually.

In general, the IP address and subnet mask of each interface should not overlap, though it is possible for this to happen with DHCP clients.

In the example above, if the UAG gets a packet with a destination address of 5.5.5.5, it might not find any entries in the routing table. In this case, the packet is dropped. However, if there is a default router to which the UAG should send this packet, you can specify it as a gateway in one of the interfaces. For example, if there is a default router at 200.200.200.100, you can create a gateway at 200.200.200.100 on wan1. In this case, the UAG creates the following entry in the routing table.

Table 82 Example: Routing Table Entry for a Gateway

IP ADDRESS(ES)	DESTINATION
0.0.0.0/0	200.200.200.100

The gateway is an optional setting for each interface. If there is more than one gateway, the UAG uses the gateway with the lowest metric, or cost. If two or more gateways have the same metric, the UAG uses the one that was set up first (the first entry in the routing table). In PPPoE/PPTP interfaces, the other computer is the gateway for the interface by default. In this case, you should specify the metric.

If the interface gets its IP address and subnet mask from a DHCP server, the DHCP server also specifies the gateway, if any.

Interface Parameters

The UAG restricts the amount of traffic into and out of the UAG through each interface.

- Egress bandwidth sets the amount of traffic the UAG sends out through the interface to the network.
- Ingress bandwidth sets the amount of traffic the UAG allows in through the interface from the network.¹

If you set the bandwidth restrictions very high, you effectively remove the restrictions.

The UAG also restricts the size of each data packet. The maximum number of bytes in each packet is called the maximum transmission unit (MTU). If a packet is larger than the MTU, the UAG divides it into smaller fragments. Each fragment is sent separately, and the original packet is re-assembled later. The smaller the MTU, the more fragments sent, and the more work required to re-assemble packets correctly. On the other hand, some communication channels, such as Ethernet over ATM, might not be able to handle large data packets.

DHCP Settings

Dynamic Host Configuration Protocol (DHCP, RFC 2131, RFC 2132) provides a way to automatically set up and maintain IP addresses, subnet masks, gateways, and some network information (such as the IP addresses of DNS servers) on computers in the network. This reduces the amount of manual configuration you have to do and usually uses available IP addresses more efficiently.

In DHCP, every network has at least one DHCP server. When a computer (a DHCP client) joins the network, it submits a DHCP request. The DHCP servers get the request; assign an IP address; and provide the IP address, subnet mask, gateway, and available network information to the DHCP client. When the DHCP client leaves the network, the DHCP servers can assign its IP address to another DHCP client.

1. At the time of writing, the UAG does not support ingress bandwidth management.

In the UAG, some interfaces can provide DHCP services to the network. In this case, the interface can be a DHCP relay or a DHCP server.

As a DHCP relay, the interface routes DHCP requests to DHCP servers on different networks. You can specify more than one DHCP server. If you do, the interface routes DHCP requests to all of them. It is possible for an interface to be a DHCP relay and a DHCP client simultaneously.

As a DHCP server, the interface provides the following information to DHCP clients.

- IP address - If the DHCP client's MAC address is in the UAG's static DHCP table, the interface assigns the corresponding IP address. If not, the interface assigns IP addresses from a pool, defined by the starting address of the pool and the pool size.

Table 83 Example: Assigning IP Addresses from a Pool

START IP ADDRESS	POOL SIZE	RANGE OF ASSIGNED IP ADDRESS
50.50.50.33	5	50.50.50.33 - 50.50.50.37
75.75.75.1	200	75.75.75.1 - 75.75.75.200
99.99.1.1	1023	99.99.1.1 - 99.99.4.255
120.120.120.100	100	120.120.120.100 - 120.120.120.199

The UAG cannot assign the first address (network address) or the last address (broadcast address) in the subnet defined by the interface's IP address and subnet mask. For example, in the first entry, if the subnet mask is 255.255.255.0, the UAG cannot assign 50.50.50.0 or 50.50.50.255. If the subnet mask is 255.255.0.0, the UAG cannot assign 50.50.0.0 or 50.50.255.255. Otherwise, it can assign every IP address in the range, except the interface's IP address.

If you do not specify the starting address or the pool size, the interface the maximum range of IP addresses allowed by the interface's IP address and subnet mask. For example, if the interface's IP address is 9.9.9.1 and subnet mask is 255.255.255.0, the starting IP address in the pool is 9.9.9.2, and the pool size is 253.

- Subnet mask - The interface provides the same subnet mask you specify for the interface. See [IP Address Assignment on page 191](#).
- Gateway - The interface provides the same gateway you specify for the interface. See [IP Address Assignment on page 191](#).
- DNS servers - The interface provides IP addresses for up to three DNS servers that provide DNS services for DHCP clients. You can specify each IP address manually (for example, a company's own DNS server), or you can refer to DNS servers that other interfaces received from DHCP servers (for example, a DNS server at an ISP). These other interfaces have to be DHCP clients.

It is not possible for an interface to be the DHCP server and a DHCP client simultaneously.

WINS

WINS (Windows Internet Naming Service) is a Windows implementation of NetBIOS Name Server (NBNS) on Windows. It keeps track of NetBIOS computer names. It stores a mapping table of your network's computer names and IP addresses. The table is dynamically updated for IP addresses assigned by DHCP. This helps reduce broadcast traffic since computers can query the server instead of broadcasting a request for a computer name's IP address. In this way WINS is similar to DNS, although WINS does not use a hierarchy (unlike DNS). A network can have WINS more than one WINS server. Samba can also serve as a WINS server.

PPPoE/PPTP Overview

Point-to-Point Protocol over Ethernet (PPPoE, RFC 2516) and Point-to-Point Tunneling Protocol (PPTP, RFC 2637) are usually used to connect two computers over phone lines or broadband connections. PPPoE is often used with cable modems and DSL connections. It provides the following advantages:

- The access and authentication method works with existing systems, including RADIUS.
- You can access one of several network services. This makes it easier for the service provider to offer the service
- PPPoE does not usually require any special configuration of the modem.

PPTP is used to set up virtual private networks (VPN) in unsecure TCP/IP environments. It sets up two sessions.

- 1 The first one runs on TCP port 1723. It is used to start and manage the second one.
- 2 The second one uses Generic Routing Encapsulation (GRE, RFC 2890) to transfer information between the computers.

PPTP is convenient and easy-to-use, but you have to make sure that security policies support both PPTP sessions.

11.1 Overview

Use trunks for WAN traffic load balancing to increase overall network throughput and reliability. Load balancing divides traffic loads between multiple interfaces. This allows you to improve quality of service and maximize bandwidth utilization for multiple ISP links.

Maybe you have two Internet connections with different bandwidths. You could set up a trunk that uses spillover or weighted round robin load balancing so time-sensitive traffic (like video) usually goes through the higher-bandwidth interface. For other traffic, you might want to use least load first load balancing to even out the distribution of the traffic load.

Suppose ISP A has better connections to Europe while ISP B has better connections to Australia. You could use policy routes and trunks to have traffic for your European branch office primarily use ISP A and traffic for your Australian branch office primarily use ISP B.

Or maybe one of the UAG's interfaces is connected to an ISP that is also your Voice over IP (VoIP) service provider. You can use policy routing to send the VoIP traffic through a trunk with the interface connected to the VoIP service provider set to active and another interface (connected to another ISP) set to passive. This way VoIP traffic goes through the interface connected to the VoIP service provider whenever the interface's connection is up.

11.1.1 What You Can Do in this Chapter

- Use the **Trunk** summary screen ([Section 11.2 on page 198](#)) to configure link sticking and view the list of configured trunks and which load balancing algorithm each trunk uses.
- Use the **Add Trunk** screen ([Section 11.2.1 on page 199](#)) to configure the member interfaces for a trunk and the load balancing algorithm the trunk uses.
- Use the **Add System Default** screen ([Section 11.2.2 on page 201](#)) to configure the load balancing algorithm for the system default trunk.

11.1.2 What You Need to Know

- Add WAN interfaces to trunks to have multiple connections share the traffic load.
- If one WAN interface's connection goes down, the UAG sends traffic through another member of the trunk.
- For example, you connect one WAN interface to one ISP and connect a second WAN interface to a second ISP. The UAG balances the WAN traffic load between the connections. If one interface's connection goes down, the UAG can automatically send its traffic through another interface.

You can also use trunks with policy routing to send specific traffic types through the best WAN interface for that type of traffic.

- If that interface's connection goes down, the UAG can still send its traffic through another interface.
- You can define multiple trunks for the same physical interfaces.

Load Balancing Algorithms

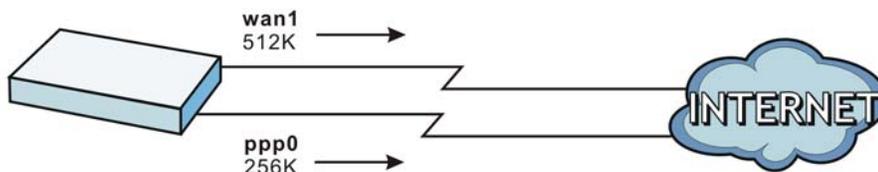
The following sections describe the load balancing algorithms the UAG can use to decide which interface the traffic (from the LAN) should use for a session². The available bandwidth you configure on the UAG refers to the actual bandwidth provided by the ISP and the measured bandwidth refers to the bandwidth an interface is currently using.

Least Load First

The least load first algorithm uses the current (or recent) outbound bandwidth utilization of each trunk member interface as the load balancing index(es) when making decisions about to which interface a new session is to be distributed. The outbound bandwidth utilization is defined as the measured outbound throughput over the available outbound bandwidth.

Here the UAG has two WAN interfaces connected to the Internet. The configured available outbound bandwidths for wan1 and ppp0 are 512K and 256K respectively.

Figure 127 Least Load First Example



The outbound bandwidth utilization is used as the load balancing index. In this example, the measured (current) outbound throughput of wan1 is 412K and ppp0 is 198K. The UAG calculates the load balancing index as shown in the table below.

Since ppp0 has a smaller load balancing index (meaning that it is less utilized than wan1), the UAG will send the subsequent new session traffic through ppp0.

Table 84 Least Load First Example

INTERFACE	OUTBOUND		LOAD BALANCING INDEX (M/A)
	AVAILABLE (A)	MEASURED (M)	
wan1	512 K	412 K	0.8
ppp0	256 K	198 K	0.77

Weighted Round Robin

Round Robin scheduling services queues on a rotating basis and is activated only when an interface has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that interface. This queue then moves to the back of the list. The next queue is

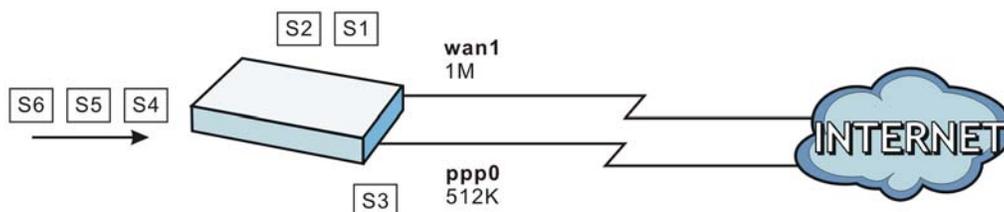
2. In the load balancing section, a session may refer to normal connection-oriented, UDP or SNMP2 traffic.

given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

The Weighted Round Robin (WRR) algorithm is best suited for situations when the bandwidths set for the two WAN interfaces are different. Similar to the Round Robin (RR) algorithm, the Weighted Round Robin (WRR) algorithm sets the UAG to send traffic through each WAN interface in turn. In addition, the WAN interfaces are assigned weights. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight.

For example, in the figure below, the configured available bandwidth of wan1 is 1M and ppp0 is 512K. You can set the UAG to distribute the network traffic between the two interfaces by setting the weight of wan1 and ppp0 to 2 and 1 respectively. The UAG assigns the traffic of two sessions to wan1 and one session's traffic to ppp0 in each round of 3 new sessions.

Figure 128 Weighted Round Robin Algorithm Example



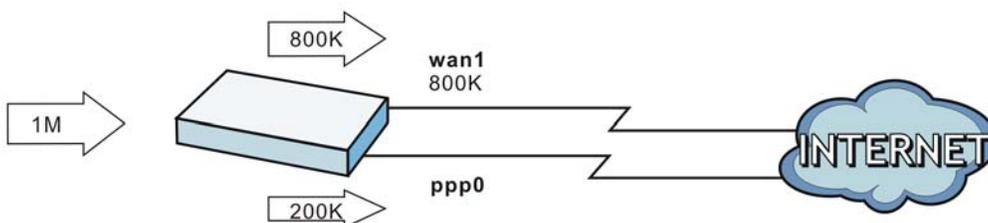
Spillover

The spillover load balancing algorithm sends network traffic to the first interface in the trunk member list until the interface's maximum allowable load is reached, then sends the excess network traffic of new sessions to the next interface in the trunk member list. This continues as long as there are more member interfaces and traffic to be sent through them.

Suppose the first trunk member interface uses an unlimited access Internet connection and the second is billed by usage. Spillover load balancing only uses the second interface when the traffic load exceeds the threshold on the first interface. This fully utilizes the bandwidth of the first interface to reduce Internet usage fees and avoid overloading the interface.

In this example figure, the upper threshold of the first interface is set to 800K. The UAG sends network traffic of new sessions that exceed this limit to the secondary WAN interface.

Figure 129 Spillover Algorithm Example



11.2 The Trunk Summary Screen

Click **Configuration > Network > Interface > Trunk** to open the **Trunk** screen. This screen lists the configured trunks and the load balancing algorithm that each is configured to use.

Figure 130 Configuration > Network > Interface > Trunk

The following table describes the items in this screen.

Table 85 Configuration > Network > Interface > Trunk

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Disconnect Connections Before Falling Back	Select this to terminate existing connections on an interface which is set to passive mode when any interface set to active mode in the same trunk comes back up.
Enable Default SNAT	Select this to have the UAG use the IP address of the outgoing interface as the source IP address of the packets it sends out through its WAN trunks. The UAG automatically adds SNAT settings for traffic it routes from internal interfaces to external interfaces.
Default Trunk Selection	Select whether the UAG is to use the default system WAN trunk or one of the user configured WAN trunks as the default trunk for routing traffic from internal interfaces to external interfaces.

Table 85 Configuration > Network > Interface > Trunk (continued)

LABEL	DESCRIPTION
User Configuration / System Default	The UAG automatically adds all external interfaces into the pre-configured system default SYSTEM_DEFAULT_WAN_TRUNK . You cannot delete it. You can create your own User Configuration trunks and customize the algorithm, member interfaces and the active/passive mode.
Add	Click this to create a new user-configured trunk.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove a user-configured trunk, select it and click Remove . The UAG confirms you want to remove it before doing so.
Object Reference	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 10.3.2 on page 165 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Name	This field displays the label that you specified to identify the trunk.
Algorithm	This field displays the load balancing method the trunk is set to use.
Apply	Click this button to save your changes to the UAG.
Reset	Click this button to return the screen to its last-saved settings.

11.2.1 Configuring a User-Defined Trunk

Click **Configuration > Network > Interface > Trunk**, in the **User Configuration** table click the **Add** (or **Edit**) icon to open the **following** screen. Use this screen to create or edit a WAN trunk entry.

Figure 131 Configuration > Network > Interface > Trunk > Add (or Edit)

The screenshot shows the 'Add Trunk' configuration window. The 'Name' field is empty and has a red error icon. The 'Load Balancing Algorithm' is set to 'Least Load First' and the 'Load Balancing Index(es)' is set to 'Outbound'. Below these are icons for 'Add', 'Edit', 'Remove', and 'Move'. A table with columns '#', 'Member', 'Mode', and 'Egress Bandwidth' is shown, with 'No data to display' below it. The table has a pagination bar showing 'Page 1 of 1' and 'Show 50 items'. At the bottom are 'OK' and 'Cancel' buttons.

Each field is described in the table below.

Table 86 Configuration > Network > Interface > Trunk > Add (or Edit)

LABEL	DESCRIPTION
Name	This is read-only if you are editing an existing trunk. When adding a new trunk, enter a descriptive name for this trunk. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Load Balancing Algorithm	<p>Select a load balancing method to use from the drop-down list box.</p> <p>Select Weighted Round Robin to balance the traffic load between interfaces based on their respective weights. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight. For example, if the weight ratio of wan1 and ppp0 interfaces is 2:1, the UAG chooses wan1 for 2 sessions' traffic and ppp0 for 1 session's traffic in each round of 3 new sessions.</p> <p>Select Least Load First to send new session traffic through the least utilized trunk member.</p> <p>Select Spillover to send network traffic through the first interface in the group member list until there is enough traffic that the second interface needs to be used (and so on).</p>
Load Balancing Index(es)	<p>This field is available if you selected to use the Least Load First or Spillover method.</p> <p>Select Outbound, Inbound, or Outbound + Inbound to set the traffic to which the UAG applies the load balancing method. Outbound means the traffic traveling from an internal interface (ex. LAN) to an external interface (ex. WAN). Inbound means the opposite.</p>
	The table lists the trunk's member interfaces. You can add, edit, remove, or move entries for user configured trunks.
Add	Click this to add a member interface to the trunk. Select an interface and click Add to add a new member interface after the selected member interface.
Edit	Select an entry and click Edit to modify the entry's settings.
Remove	To remove a member interface, select it and click Remove . The UAG confirms you want to remove it before doing so.
Move	To move an interface to a different number in the list, click the Move icon. In the field that appears, specify the number to which you want to move the interface.
#	This column displays the priorities of the group's interfaces. The order of the interfaces in the list is important since they are used in the order they are listed.
Member	Click this table cell and select an interface to be a group member.
Mode	<p>Click this table cell and select Active to have the UAG always attempt to use this connection.</p> <p>Select Passive to have the UAG only use this connection when all of the connections set to active are down. You can only set one of a group's interfaces to passive mode.</p>
Weight	This field displays with the weighted round robin load balancing algorithm. Specify the weight (1~10) for the interface. The weights of the different member interfaces form a ratio. This ratio determines how much traffic the UAG assigns to each member interface. The higher an interface's weight is (relative to the weights of the interfaces), the more sessions that interface should handle.
Ingress Bandwidth	<p>This is reserved for future use.</p> <p>This field displays with the least load first load balancing algorithm. It displays the maximum number of kilobits of data the UAG is to allow to come in through the interface per second.</p> <p>Note: You can configure the bandwidth of an interface in the corresponding interface edit screen.</p>

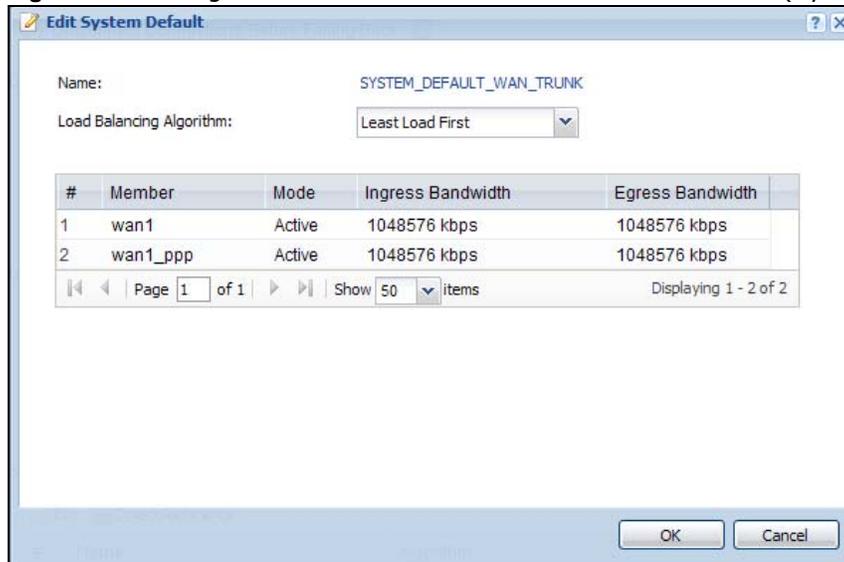
Table 86 Configuration > Network > Interface > Trunk > Add (or Edit) (continued)

LABEL	DESCRIPTION
Egress Bandwidth	This field displays with the least load first or spillover load balancing algorithm. It displays the maximum number of kilobits of data the UAG is to send out through the interface per second. Note: You can configure the bandwidth of an interface in the corresponding interface edit screen.
Total Bandwidth	This field displays with the spillover load balancing algorithm. It displays the maximum number of kilobits of data the UAG is to send out and allow to come in through the interface per second. You can configure the bandwidth of an interface in the corresponding interface edit screen.
Spillover	This field displays with the spillover load balancing algorithm. Specify the maximum bandwidth of traffic in kilobits per second (1~1048576) to send out through the interface before using another interface. When this spillover bandwidth limit is exceeded, the UAG sends new session traffic through the next interface. The traffic of existing sessions still goes through the interface on which they started. The UAG uses the group member interfaces in the order that they are listed.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

11.2.2 Configuring the System Default Trunk

In the **Configuration > Network > Interface > Trunk** screen and the **System Default** section, select the default trunk entry and click **Edit** to open the **following** screen. Use this screen to change the load balancing algorithm and view the bandwidth allocations for each member interface.

Note: The available bandwidth is allocated to each member interface equally and is not allowed to be changed for the default trunk.

Figure 132 Configuration > Network > Interface > Trunk > Edit (System Default)

Each field is described in the table below.

Table 87 Configuration > Network > Interface > Trunk > Edit (System Default)

LABEL	DESCRIPTION
Name	This field displays the name of the selected system default trunk.
Load Balancing Algorithm	<p>Select the load balancing method to use for the trunk.</p> <p>Select Weighted Round Robin to balance the traffic load between interfaces based on their respective weights. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight. For example, if the weight ratio of wan1 and ppp0 interfaces is 2:1, the UAG chooses wan1 for 2 sessions' traffic and ppp0 for 1 session's traffic in each round of 3 new sessions.</p> <p>Select Least Load First to send new session traffic through the least utilized trunk member.</p> <p>Select Spillover to send network traffic through the first interface in the group member list until there is enough traffic that the second interface needs to be used (and so on).</p>
	The table lists the trunk's member interfaces. This table is read-only.
#	This column displays the priorities of the group's interfaces. The order of the interfaces in the list is important since they are used in the order they are listed.
Member	This column displays the name of the member interfaces.
Mode	<p>This field displays Active if the UAG always attempt to use this connection.</p> <p>This field displays Passive if the UAG only use this connection when all of the connections set to active are down. Only one of a group's interfaces can be set to passive mode.</p>
Weight	This field displays with the weighted round robin load balancing algorithm. Specify the weight (1~10) for the interface. The weights of the different member interfaces form a ratio. s
Ingress Bandwidth	<p>This is reserved for future use.</p> <p>This field displays with the least load first load balancing algorithm. It displays the maximum number of kilobits of data the UAG is to allow to come in through the interface per second.</p>
Egress Bandwidth	This field displays with the least load first or spillover load balancing algorithm. It displays the maximum number of kilobits of data the UAG is to send out through the interface per second.
Spillover	<p>This field displays with the spillover load balancing algorithm. Specify the maximum bandwidth of traffic in kilobits per second (1~1048576) to send out through the interface before using another interface. When this spillover bandwidth limit is exceeded, the UAG sends new session traffic through the next interface. The traffic of existing sessions still goes through the interface on which they started.</p> <p>The UAG uses the group member interfaces in the order that they are listed.</p>
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

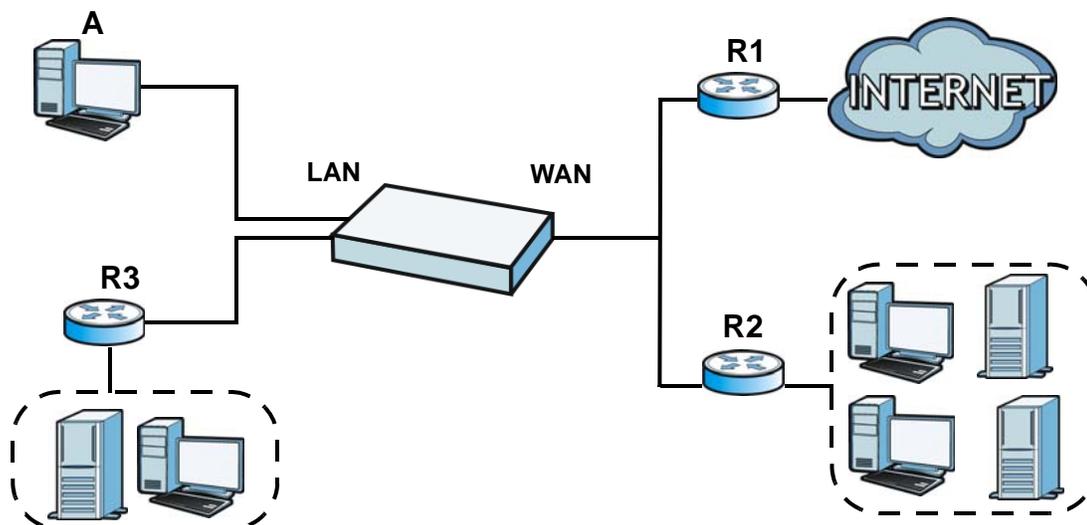
Policy and Static Routes

12.1 Policy and Static Routes Overview

Use policy routes and static routes to override the UAG's default routing behavior in order to send packets through the appropriate interface.

For example, the next figure shows a computer (**A**) connected to the UAG's LAN interface. The UAG routes most traffic from **A** to the Internet through the UAG's default gateway (**R1**). You create one policy route to connect to services offered by your ISP behind router **R2**. You create another policy route to communicate with a separate network behind another router (**R3**) connected to the LAN.

Figure 133 Example of Policy Routing Topology



12.1.1 What You Can Do in this Chapter

- Use the **Policy Route** screens (see [Section 12.2 on page 205](#)) to list and configure policy routes.
- Use the **Static Route** screens (see [Section 12.3 on page 211](#)) to list and configure static routes.

12.1.2 What You Need to Know

Policy Routing

Traditionally, routing is based on the destination address only and the UAG takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator.

Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

How You Can Use Policy Routing

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.
- NAT - The UAG performs NAT by default for traffic going to or from the **WAN** interfaces. A routing policy's SNAT allows network administrators to have traffic received on a specified interface use a specified IP address as the source IP address.

Note: The UAG automatically uses SNAT for traffic it routes from internal interfaces to external interfaces. For example LAN to WAN traffic.

Static Routes

The UAG usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the UAG send data to devices not reachable through the default gateway, use static routes.

Policy Routes Versus Static Routes

- Policy routes are more flexible than static routes. You can select more criteria for the traffic to match and can also use schedules, and NAT.
- Policy routes are only used within the UAG itself.
- Policy routes take priority over static routes. If you need to use a routing policy on the UAG and propagate it to other routers, you could configure a policy route and an equivalent static route.

DiffServ

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP Marking and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.



DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

Finding Out More

- See [Section 12.4 on page 212](#) for more background information on policy routing.

12.2 Policy Route Screen

Click **Configuration > Network > Routing** to open the **Policy Route** screen. Use this screen to see the configured policy routes.

A policy route defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria can include the user name, source address and incoming interface, destination address, schedule, IP protocol (ICMP, UDP, TCP, etc.) and port.

The actions that can be taken include:

- Routing the packet to a different gateway, outgoing interface, or trunk.

IPPR follows the existing packet filtering facility of RAS in style and in implementation.

Figure 134 Configuration > Network > Routing > Policy Route



The following table describes the labels in this screen.

Table 88 Configuration > Network > Routing > Policy Route

LABEL	DESCRIPTION
Use IPv4 Policy Route to Override Direct Route	Select this to have the UAG forward packets that match a policy route according to the policy route instead of sending the packets directly to a connected network.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
Move	To change a rule's position in the numbered list, select the rule and click Move to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
#	This is the number of an individual policy route.
Status	This icon is lit when the entry is active, red when the next hop's connection is down, and dimmed when the entry is inactive.
User	This is the name of the user (group) object from which the packets are sent. any means all users.
Schedule	This is the name of the schedule object. none means the route is active at all times if enabled.
Incoming	This indicates where the packets are coming from. For example, it shows the interface on which the packets are received or the VPN tunnel through which the packets are sent.
Source	This is the name of the source IP address (group) object. any means all IP addresses.
Destination	This is the name of the destination IP address (group) object. any means all IP addresses.
DSCP Code	This is the DSCP value of incoming packets to which this policy route applies. any means all DSCP values or no DSCP marker. default means traffic with a DSCP value of 0. This is usually best effort traffic The " af " entries stand for Assured Forwarding. The number following the " af " identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 212 for more details.
Service	This is the name of the service object. any means all services.
Source Port	This is the name of a service object. The UAG applies the policy route to the packets sent from the corresponding service port. any means all service ports.
Next-Hop	This is the next hop to which packets are directed. It helps forward packets to their destinations and can be a router, outgoing interface or trunk.

Table 88 Configuration > Network > Routing > Policy Route (continued)

LABEL	DESCRIPTION
DSCP Marking	<p>This is how the UAG handles the DSCP value of the outgoing packets that match this route. If this field displays a DSCP value, the UAG applies that DSCP value to the route's outgoing packets.</p> <p>preserve means the UAG does not modify the DSCP value of the route's outgoing packets.</p> <p>default means the UAG sets the DSCP value of the route's outgoing packets to 0.</p> <p>The "af" choices stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 212 for more details.</p>
SNAT	<p>This is the source IP address that the route uses.</p> <p>It displays none if the UAG does not perform NAT for this route.</p>
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

12.2.1 Policy Route Add/Edit Screen

Click **Configuration > Network > Routing** to open the **Policy Route** screen. Then click the **Add** icon or select an entry and click the **Edit** icon. The **Add Policy Route** or **Policy Route Edit** screen opens. Use this screen to configure or edit a policy route.

Figure 135 Configuration > Network > Routing > Policy Route > Add/Edit

Add Policy Route

Hide Advanced Settings Create new Object

Configuration

Enable
Description: (Optional)

Criteria

User: any
Incoming: Tunnel
Please select one member: WIZ_VPN
Source Address: any
Destination Address: any
DSCP Code: any
Schedule: none
Service: any
Source Port: any

Next-Hop

Type: Interface
Interface: dmz

DSCP Marking

DSCP Marking: User Define
User-Defined DSCP Marking: 0 (0-63)

Address Translation

Source Network Address Translation: outgoing-interface

Healthy Check

Disable policy route automatically while Interface link down
 Enable Connectivity Check
Check Method: icmp
Check Period: 5 (5-600 seconds)
Check Timeout: 1 (1-10 seconds)
Check Fail Tolerance: 1 (1-10)
Check this address: (Domain Name or IP Address)

OK Cancel

The following table describes the labels in this screen.

Table 89 Configuration > Network > Routing > Policy Route > Add/Edit

LABEL	DESCRIPTION
Show / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create new Object	Use this to configure any new settings objects that you need to use in this screen.

Table 89 Configuration > Network > Routing > Policy Route > Add/Edit (continued)

LABEL	DESCRIPTION
Configuration	
Enable	Select this to activate the policy.
Description	Enter a descriptive name of up to 31 printable ASCII characters for the policy.
Criteria	
User	Select a user name or user group from which the packets are sent.
Incoming	Select where the packets are coming from; any, an interface, a VPN tunnel, or the UAG itself (Device). For an interface or a VPN tunnel, you also need to select the individual interface or VPN tunnel.
Please select one member	This field displays only when you set Incoming to Interface or Tunnel . Select an interface or VPN tunnel from which the packets are sent.
Source Address	Select a source IP address object from which the packets are sent.
Destination Address	Select a destination IP address object to which the traffic is being sent.
DSCP Code	Select a DSCP code point value of incoming packets to which this policy route applies or select User Define to specify another DSCP code point. The lower the number the higher the priority with the exception of 0 which is usually given only best-effort treatment. any means all DSCP value or no DSCP marker. default means traffic with a DSCP value of 0. This is usually best effort traffic The "af" choices stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 212 for more details.
User-Defined DSCP Code	Use this field to specify a custom DSCP code point.
Schedule	Select a schedule to control when the policy route is active. none means the route is active at all times if enabled.
Service	Select a service or service group to identify the type of traffic to which this policy route applies.
Source Port	Select a service or service group to identify the source port of packets to which the policy route applies.
Next-Hop	
Type	Select Auto to have the UAG use the routing table to find a next-hop and forward the matched packets automatically. Select Gateway to route the matched packets to the next-hop router or switch you specified in the Gateway field. You have to set up the next-hop router or switch as a HOST address object first. Select VPN Tunnel to route the matched packets via the specified VPN tunnel to the remote IPsec router. Select Trunk to route the matched packets through the interfaces in the trunk group based on the load balancing algorithm. Select Interface to route the matched packets through the specified outgoing interface to a gateway (which is connected to the interface).
Gateway	This field displays when you select Gateway in the Type field. Select a HOST address object. The gateway is an immediate neighbor of your UAG that will forward the packet to the destination. The gateway must be a router or switch on the same segment as your UAG's interface(s).
VPN Tunnel	This field displays when you select VPN Tunnel in the Type field. Select a VPN tunnel through which the UAG sends the matched packets to the remote network.

Table 89 Configuration > Network > Routing > Policy Route > Add/Edit (continued)

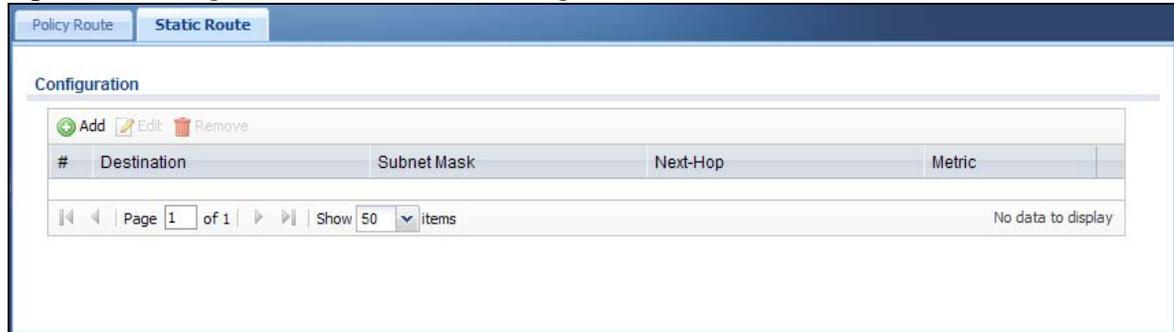
LABEL	DESCRIPTION
Trunk	This field displays when you select Trunk in the Type field. Select a trunk group to have the UAG send the packets via the interfaces in the group.
Interface	This field displays when you select Interface in the Type field. Select an interface to have the UAG send traffic that matches the policy route through the specified interface.
DSCP Marking	
DSCP Marking	<p>Set how the UAG handles the DSCP value of the outgoing packets that match this route.</p> <p>Select one of the pre-defined DSCP values to apply or select User Define to specify another DSCP value. The "af" choices stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 212 for more details.</p> <p>Select preserve to have the UAG keep the packets' original DSCP value.</p> <p>Select default to have the UAG set the DSCP value of the packets to 0.</p>
User-Defined DSCP Marking	Use this field to specify a custom DSCP value.
Address Translation	Use this section to configure NAT for the policy route.
Source Network Address Translation	<p>Select none to not use NAT for the route.</p> <p>Select outgoing-interface to use the IP address of the outgoing interface as the source IP address of the packets that matches this route.</p> <p>To use SNAT for a virtual interface that is in the same WAN trunk as the physical interface to which the virtual interface is bound, the virtual interface and physical interface must be in different subnets.</p> <p>Otherwise, select a pre-defined address (group) to use as the source IP address(es) of the packets that match this route.</p> <p>Use Create new Object if you need to configure a new address (group) to use as the source IP address(es) of the packets that match this route.</p>
Healthy Check	Use this part of the screen to configure a route connectivity check and disable the policy if the interface is down.
Disable policy route automatically while Interface link down	This field displays when you select Interface or Trunk in the Type field. Select this to have the UAG automatically disable this policy route when the interface is down or disabled.
Enable Connectivity Check	<p>This option is available when you select Interface or Gateway in the Type field.</p> <p>Select this to turn on the connection check.</p>
Check Method	<p>Select the method that the gateway allows.</p> <p>Select icmp to have the UAG regularly ping the gateway you specify to make sure it is still available.</p> <p>Select tcp to have the UAG regularly perform a TCP handshake with the gateway you specify to make sure it is still available.</p>
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the UAG stops routing through the gateway.
Check Port	This field only displays when you set the Check Method to tcp . Specify the port number to use for a TCP connectivity check.

Table 89 Configuration > Network > Routing > Policy Route > Add/Edit (continued)

LABEL	DESCRIPTION
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

12.3 IP Static Route Screen

Click **Configuration > Network > Routing > Static Route** to open the **Static Route** screen. This screen displays the configured static routes. Configure static routes to be able to propagate the routing information to other routers.

Figure 136 Configuration > Network > Routing > Static Route

The following table describes the labels in this screen.

Table 90 Configuration > Network > Routing > Static Route

LABEL	DESCRIPTION
Add	Click this to create a new static route.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
#	This is the number of an individual static route.
Destination	This is the destination IP address.
Subnet Mask	This is the IP subnet mask.
Next-Hop	This is the IP address of the next-hop gateway or the interface through which the traffic is routed. The gateway is a router or switch on the same segment as your UAG's interface(s). The gateway helps forward packets to their destinations.
Metric	This is the route's priority among the UAG's routes. The smaller the number, the higher priority the route has.

12.3.1 Static Route Add/Edit Screen

Select a static route index number and click **Add** or **Edit**. The screen shown next appears. Use this screen to configure the required information for a static route.

Figure 137 Configuration > Network > Routing > Static Route > Add

The following table describes the labels in this screen.

Table 91 Configuration > Network > Routing > Static Route > Add

LABEL	DESCRIPTION
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, enter the specific IP address here and use a subnet mask of 255.255.255.255 (for IPv4) in the Subnet Mask field to force the network number to be identical to the host ID.
Subnet Mask	Enter the IP subnet mask here.
Gateway IP	Select the radio button and enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your UAG's interface(s). The gateway helps forward packets to their destinations.
Interface	Select the radio button and a predefined interface through which the traffic is sent.
Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be 0~127. In practice, 2 or 3 is usually a good number.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

12.4 Policy Routing Technical Reference

Here is more detailed information about some of the features you can configure in policy routing.

NAT and SNAT

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address in a packet in one network to a different IP address in another network. Use SNAT (Source NAT) to change the source IP address in one network to a different IP address in another network.

Assured Forwarding (AF) PHB for DiffServ

Assured Forwarding (AF) behavior is defined in RFC 2597. The AF behavior group defines four AF classes. Inside each class, packets are given a high, medium or low drop precedence. The drop

precedence determines the probability that routers in the network will drop packets when congestion occurs. If congestion occurs between classes, the traffic in the higher class (smaller numbered class) is generally given priority. Combining the classes and drop precedence produces the following twelve DSCP encodings from AF11 through AF43. The decimal equivalent is listed in brackets.

Table 92 Assured Forwarding (AF) Behavior Group

	CLASS 1	CLASS 2	CLASS 3	CLASS 4
Low Drop Precedence	AF11 (10)	AF21 (18)	AF31 (26)	AF41 (34)
Medium Drop Precedence	AF12 (12)	AF22 (20)	AF32 (28)	AF42 (36)
High Drop Precedence	AF13 (14)	AF23 (22)	AF33 (30)	AF43 (38)

13.1 DDNS Overview

Dynamic DNS (DDNS) services let you use a domain name with a dynamic IP address.

13.1.1 What You Can Do in this Chapter

- Use the **DDNS** screen (see [Section 13.2 on page 215](#)) to view a list of the configured DDNS domain names and their details.
- Use the **DDNS Add/Edit** screen (see [Section 13.2.1 on page 216](#)) to add a domain name to the UAG or to edit the configuration of an existing domain name.

13.1.2 What You Need to Know

DNS maps a domain name to a corresponding IP address and vice versa. Similarly, dynamic DNS maps a domain name to a dynamic IP address. As a result, anyone can use the domain name to contact you (in NetMeeting, CU-SeeMe, etc.) or to access your FTP server or Web site, regardless of the current IP address.

Note: You must have a public WAN IP address to use Dynamic DNS.

You must set up a dynamic DNS account with a supported DNS service provider before you can use Dynamic DNS services with the UAG. When registration is complete, the DNS service provider gives you a password or key. At the time of writing, the UAG supports the following DNS service providers. See the listed websites for details about the DNS services offered by each.

Table 93 DDNS Service Providers

PROVIDER	SERVICE TYPES SUPPORTED	WEBSITE
DynDNS	Dynamic DNS, Static DNS, and Custom DNS	www.dyndns.com
Dynu	Basic, Premium	www.dynu.com
No-IP	No-IP	www.noip.com
Peanut Hull	Peanut Hull	www.oray.cn
3322	3322 Dynamic DNS, 3322 Static DNS	www.3322.org
Selfhost	Selfhost	selfhost.de

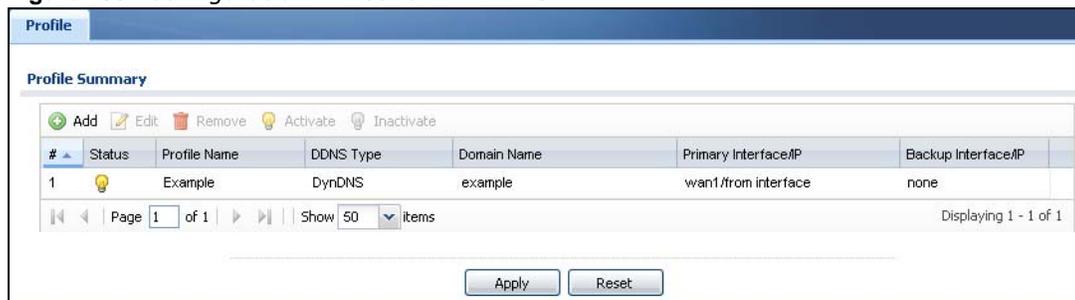
Note: Record your DDNS account's user name, password, and domain name to use to configure the UAG.

After, you configure the UAG, it automatically sends updated IP addresses to the DDNS service provider, which helps redirect traffic accordingly.

13.2 The DDNS Screen

The **DDNS** screen provides a summary of all DDNS domain names and their configuration. In addition, this screen allows you to add new domain names, edit the configuration for existing domain names, and delete domain names. Click **Configuration > Network > DDNS** to open the following screen.

Figure 138 Configuration > Network > DDNS



The following table describes the labels in this screen.

Table 94 Configuration > Network > DDNS

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
#	This is the number of an individual DDNS profile.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Profile Name	This field displays the descriptive profile name for this entry.
DDNS Type	This field displays which DDNS service you are using.
Domain Name	This field displays each domain name the UAG can route.
Primary Interface/IP	This field displays the interface to use for updating the IP address mapped to the domain name followed by how the UAG determines the IP address for the domain name. from interface - The IP address comes from the specified interface. auto detected -The DDNS server checks the source IP address of the packets from the UAG for the IP address to use for the domain name. custom - The IP address is static.
Backup Interface/IP	This field displays the alternate interface to use for updating the IP address mapped to the domain name followed by how the UAG determines the IP address for the domain name. The UAG uses the backup interface and IP address when the primary interface is disabled, its link is down or its connectivity check fails. from interface - The IP address comes from the specified interface. auto detected -The DDNS server checks the source IP address of the packets from the UAG for the IP address to use for the domain name. custom - The IP address is static.

Table 94 Configuration > Network > DDNS (continued)

LABEL	DESCRIPTION
Apply	Click this button to save your changes to the UAG.
Reset	Click this button to return the screen to its last-saved settings.

13.2.1 The Dynamic DNS Add/Edit Screen

The **DDNS Add/Edit** screen allows you to add a domain name to the UAG or to edit the configuration of an existing domain name. Click **Configuration > Network > DDNS** and then an **Add** or **Edit** icon to open this screen.

Figure 139 Configuration > Network > DDNS > Add

The following table describes the labels in this screen.

Table 95 Configuration > Network > DDNS > Add

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Enable DDNS Profile	Select this check box to use this DDNS entry.

Table 95 Configuration > Network > DDNS > Add (continued)

LABEL	DESCRIPTION
Profile Name	<p>When you are adding a DDNS entry, type a descriptive name for this DDNS entry in the UAG. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.</p> <p>This field is read-only when you are editing an entry.</p>
DDNS Type	Select the type of DDNS service you are using.
HTTPS	Select this option to encrypt traffic using SSL (port 443), including traffic with username and password, to the DDNS server. Not all DDNS providers support this option.
DDNS Account	
Username	<p>Type the user name used when you registered your domain name. You can use up to 31 alphanumeric characters and the underscore. Spaces are not allowed.</p> <p>For a Dynu DDNS entry, this user name is the one you use for logging into the service, not the name recorded in your personal information in the Dynu website.</p>
Password	Type the password provided by the DDNS provider. You can use up to 64 alphanumeric characters and the underscore. Spaces are not allowed.
Retype to Confirm	Retype your new password for confirmation.
DDNS Settings	
Domain name	Type the domain name you registered. You can use up to 255 characters.
Primary Binding Address	Use these fields to set how the UAG determines the IP address that is mapped to your domain name in the DDNS server. The UAG uses the Backup Binding Address if the interface specified by these settings is not available.
Interface	Select the interface to use for updating the IP address mapped to the domain name. Select any to let the domain name be used with any interface.
IP Address	<p>The options available in this field vary by DDNS provider.</p> <p>Interface - The UAG uses the IP address of the specified interface. This option appears when you select a specific interface in the Primary Binding Address Interface field.</p> <p>Auto - If the interface has a dynamic IP address, the DDNS server checks the source IP address of the packets from the UAG for the IP address to use for the domain name. You may want to use this if there are one or more NAT routers between the UAG and the DDNS server.</p> <p>Note: The UAG may not determine the proper IP address if there is an HTTP proxy server between the UAG and the DDNS server.</p> <p>Custom - If you have a static IP address, you can select this to use it for the domain name. The UAG still sends the static IP address to the DDNS server.</p>
Custom IP	This field is only available when the IP Address is Custom . Type the IP address to use for the domain name.
Backup Binding Address	Use these fields to set an alternate interface to map the domain name to when the interface specified by the Primary Binding Interface settings is not available.
Interface	Select the interface to use for updating the IP address mapped to the domain name. Select any to let the domain name be used with any interface. Select None to not use a backup address.

Table 95 Configuration > Network > DDNS > Add (continued)

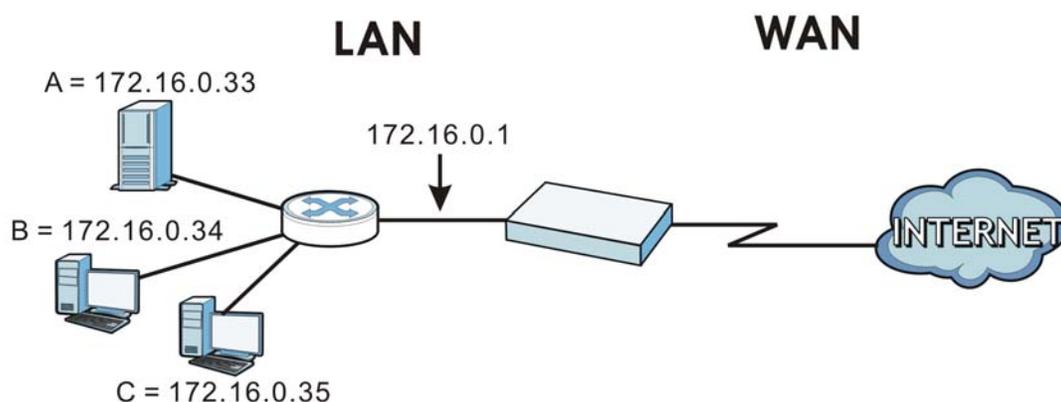
LABEL	DESCRIPTION
IP Address	<p>The options available in this field vary by DDNS provider.</p> <p>Interface -The UAG uses the IP address of the specified interface. This option appears when you select a specific interface in the Backup Binding Address Interface field.</p> <p>Auto -The DDNS server checks the source IP address of the packets from the UAG for the IP address to use for the domain name. You may want to use this if there are one or more NAT routers between the UAG and the DDNS server.</p> <p>Note: The UAG may not determine the proper IP address if there is an HTTP proxy server between the UAG and the DDNS server.</p> <p>Custom - If you have a static IP address, you can select this to use it for the domain name. The UAG still sends the static IP address to the DDNS server.</p>
Custom IP	This field is only available when the IP Address is Custom . Type the IP address to use for the domain name.
Enable Wildcard	<p>This option is only available with a DynDNS account.</p> <p>Enable the wildcard feature to alias subdomains to be aliased to the same IP address as your (dynamic) domain name. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.</p>
Mail Exchanger	<p>This option is only available with a DynDNS account.</p> <p>DynDNS can route e-mail for your domain name to a mail server (called a mail exchanger). For example, DynDNS routes e-mail for john-doe@yourhost.dyndns.org to the host record specified as the mail exchanger.</p> <p>If you are using this service, type the host record of your mail server here. Otherwise leave the field blank.</p> <p>See www.dyndns.org for more information about mail exchangers.</p>
Backup Mail Exchanger	<p>This option is only available with a DynDNS account.</p> <p>Select this check box if you are using DynDNS's backup service for e-mail. With this service, DynDNS holds onto your e-mail if your mail server is not available. Once your mail server is available again, the DynDNS server delivers the mail to you. See www.dyndns.org for more information about this service.</p>
DYNDNS Server:	This field displays when you select User custom from the DDNS Type field above. Type the IP address of the server that will host the DDSN service.
URL	This field displays when you select User custom from the DDNS Type field above. Type the URL that can be used to access the server that will host the DDSN service.
Additional DDNS Options	<p>This field displays when you select User custom from the DDNS Type field above. These are the options supported at the time of writing:</p> <ul style="list-style-type: none"> • <code>dyndns_system</code> to specify the DYNDNS Server type - for example, <code>dyndns@dyndns.org</code> • <code>ip_server_name</code> which should be the URL to get the server's public IP address - for example, <code>http://myip.easylife.tw/</code>
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

14.1 NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network. Use Network Address Translation (NAT) to make computers on a private network behind the UAG available outside the private network. If the UAG has only one public IP address, you can make the computers in the private network available by using ports to forward packets to the appropriate private IP address.

Suppose you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 172.16.0.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 140 Multiple Servers Behind NAT Example



14.1.1 What You Can Do in this Chapter

Use the **NAT** screens (see [Section 14.2 on page 220](#)) to view and manage the list of NAT rules and see their configuration details. You can also create new NAT rules and edit or delete existing ones.

14.1.2 What You Need to Know

NAT is also known as virtual server, port forwarding, or port translation.

Finding Out More

- See [Section 14.3 on page 224](#) for technical background information related to these screens.

14.2 The NAT Screen

The **NAT** summary screen provides a summary of all NAT rules and their configuration. In addition, this screen allows you to create new NAT rules and edit and delete existing NAT rules. To access this screen, login to the Web Configurator and click **Configuration > Network > NAT**. The following screen appears, providing a summary of the existing NAT rules.

Figure 141 Configuration > Network > NAT



The following table describes the labels in this screen.

Table 96 Configuration > Network > NAT

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
Move	To change a rule's position in the numbered list, select the rule and click Move to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Priority	This is the order of the entry in the list.
Name	This field displays the name of the entry.
Mapping Type	This field displays what kind of NAT this entry performs: Virtual Server , 1:1 NAT , or Many 1:1 NAT .
Interface	This field displays the interface on which packets for the NAT entry are received.
Original IP	This field displays the original destination IP address (or address object) of traffic that matches this NAT entry. It displays any if there is no restriction on the original destination IP address.
Mapped IP	This field displays the new destination IP address for the packet.

Table 96 Configuration > Network > NAT (continued)

LABEL	DESCRIPTION
Protocol	This field displays the service used by the packets for this NAT entry. It displays any if there is no restriction on the services.
Original Port	This field displays the original destination port(s) of packets for the NAT entry. This field is blank if there is no restriction on the original destination port.
Mapped Port	This field displays the new destination port(s) for the packet. This field is blank if there is no restriction on the original destination port.
Apply	Click this button to save your changes to the UAG.
Reset	Click this button to return the screen to its last-saved settings.

14.2.1 The NAT Add/Edit Screen

The **NAT Add/Edit** screen lets you create new NAT rules and edit existing ones. To open this window, open the **NAT** summary screen. (See [Section 14.2 on page 220](#).) Then, click on an **Add** icon or **Edit** icon to open the following screen.

Figure 142 Configuration > Network > NAT > Add

The following table describes the labels in this screen.

Table 97 Configuration > Network > NAT > Add

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable Rule	Use this option to turn the NAT rule on or off.

Table 97 Configuration > Network > NAT > Add (continued)

LABEL	DESCRIPTION
Rule Name	Type in the name of the NAT rule. The name is used to refer to the NAT rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Classification	<p>Select what kind of NAT this rule is to perform.</p> <p>Virtual Server - This makes computers on a private network behind the UAG available to a public network outside the UAG (like the Internet).</p> <p>1:1 NAT - If the private network server will initiate sessions to the outside clients, select this to have the UAG translate the source IP address of the server's outgoing traffic to the same public IP address that the outside clients use to access the server.</p> <p>Many 1:1 NAT - If you have a range of private network servers that will initiate sessions to the outside clients and a range of public IP addresses, select this to have the UAG translate the source IP address of each server's outgoing traffic to the same one of the public IP addresses that the outside clients use to access the server. The private and public ranges must have the same number of IP addresses.</p> <p>One many 1:1 NAT rule works like multiple 1:1 NAT rules, but it eases configuration effort since you only create one rule.</p>
Incoming Interface	Select the interface on which packets for the NAT rule must be received. It can be an Ethernet, VLAN, bridge, or PPPoE/PPTP interface.
Original IP	<p>Specify the destination IP address of the packets received by this NAT rule's specified incoming interface.</p> <p>any - Select this to use all of the incoming interface's IP addresses including dynamic addresses or those of any virtual interfaces built upon the selected incoming interface.</p> <p>User Defined - Select this to manually enter an IP address in the User Defined Original IP field. For example, you could enter a static public IP assigned by the ISP without having to create a virtual interface for it.</p> <p>Host address - select a host address object to use the IP address it specifies. The list also includes address objects based on interface IPs. So for example you could select an address object based on a WAN interface even if it has a dynamic IP address.</p>
User-Defined Original IP	This field is available if Original IP is User Defined . Type the destination IP address that this NAT rule supports.
Original IP Subnet/Range	This field displays for Many 1:1 NAT . Select the destination IP address subnet or IP address range that this NAT rule supports. The original and mapped IP address subnets or ranges must have the same number of IP addresses.
Mapped IP	<p>Select to which translated destination IP address this NAT rule forwards packets.</p> <p>User Defined - this NAT rule supports a specific IP address, specified in the User-Defined Mapped IP field.</p>
User-Defined Mapped IP	This field is available if Mapped IP is User Defined . Type the translated destination IP address that this NAT rule supports.
Mapped IP Subnet/Range	This field displays for Many 1:1 NAT . Select to which translated destination IP address subnet or IP address range this NAT rule forwards packets. The original and mapped IP address subnets or ranges must have the same number of IP addresses.

Table 97 Configuration > Network > NAT > Add (continued)

LABEL	DESCRIPTION
Port Mapping Type	<p>Use the drop-down list box to select how many original destination ports this NAT rule supports for the selected destination IP address (Original IP). Choices are:</p> <p>Any - this NAT rule supports all the destination ports.</p> <p>Service - this NAT rule supports the destination port(s) used by the specified service(s).</p> <p>Port - this NAT rule supports one destination port.</p> <p>Ports - this NAT rule supports a range of destination ports. You might use a range of destination ports for unknown services or when one server supports more than one service.</p> <p>This field is read-only and displays any for Many 1:1 NAT.</p>
Original Service	This field is available if Port Mapping Type is Service . Select the original service whose destination port(s) is supported by this NAT rule.
Mapped Service	This field is available if Port Mapping Type is Service . Select the translated service whose destination port(s) is supported if this NAT rule forwards the packet.
Protocol Type	This field is available if Port Mapping Type is Port or Ports . Select the protocol (TCP , UDP , or any) used by the service requesting the connection.
Original Port	This field is available if Port Mapping Type is Port . Enter the original destination port this NAT rule supports.
Mapped Port	This field is available if Port Mapping Type is Port . Enter the translated destination port if this NAT rule forwards the packet.
Original Start Port	This field is available if Port Mapping Type is Ports . Enter the beginning of the range of original destination ports this NAT rule supports.
Original End Port	This field is available if Port Mapping Type is Ports . Enter the end of the range of original destination ports this NAT rule supports.
Mapped Start Port	This field is available if Port Mapping Type is Ports . Enter the beginning of the range of translated destination ports if this NAT rule forwards the packet.
Mapped End Port	This field is available if Port Mapping Type is Ports . Enter the end of the range of translated destination ports if this NAT rule forwards the packet. The original port range and the mapped port range must be the same size.
Enable NAT Loopback	<p>Enable NAT loopback to allow users connected to any interface (instead of just the specified Incoming Interface) to use the NAT rule's specified Original IP address to access the Mapped IP device. For users connected to the same interface as the Mapped IP device, the UAG uses that interface's IP address as the source address for the traffic it sends from the users to the Mapped IP device.</p> <p>For example, if you configure a NAT rule to forward traffic from the WAN to a LAN server, enabling NAT loopback allows users connected to other interfaces to also access the server. For LAN users, the UAG uses the LAN interface's IP address as the source address for the traffic it sends to the LAN server. See NAT Loopback on page 224 for more details.</p> <p>If you do not enable NAT loopback, this NAT rule only applies to packets received on the rule's specified incoming interface.</p>
Security Policy	<p>By default the Security Policy blocks incoming connections from external addresses. After you configure your NAT rule settings, click the Security Policy link to configure a security policy to allow the NAT rule's traffic to come in.</p> <p>The UAG checks NAT rules before it applies To-Device security policies, so To-Device security policies do not apply to traffic that is forwarded by NAT rules. The UAG still checks other security policies according to the source IP address and mapped IP address.</p>
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to return to the NAT summary screen without creating the NAT rule (if it is new) or saving any changes (if it already exists).

14.3 NAT Technical Reference

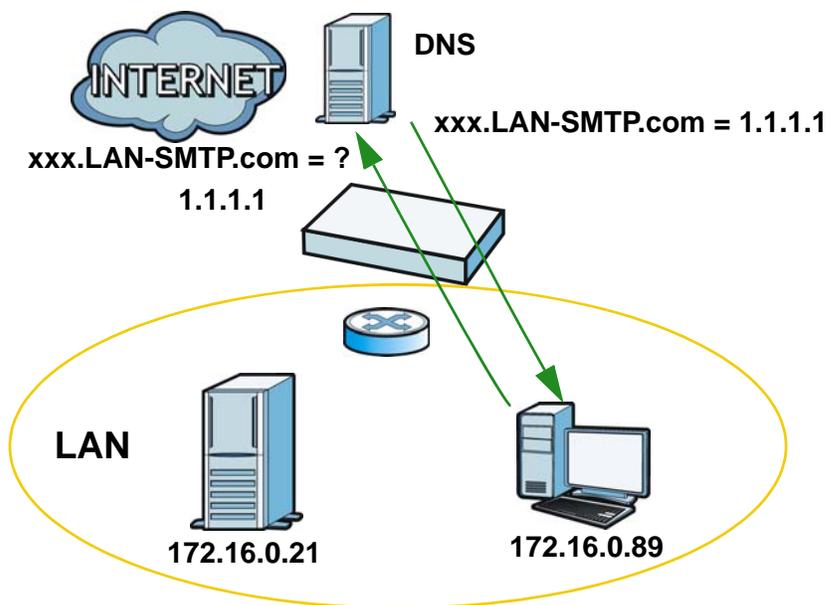
Here is more detailed information about NAT on the UAG.

NAT Loopback

Suppose an NAT 1:1 rule maps a public IP address to the private IP address of a LAN SMTP e-mail server to give WAN users access. NAT loopback allows other users to also use the rule's original IP to access the mail server.

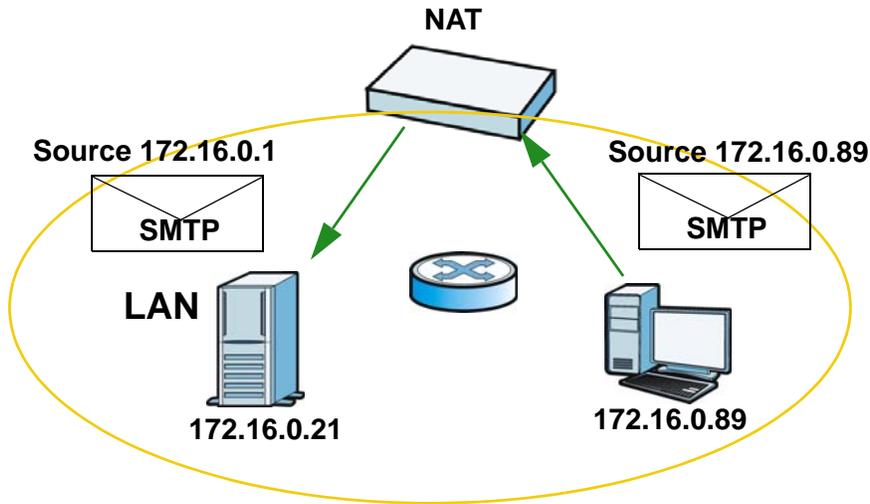
For example, a LAN user's computer at IP address 172.16.0.89 queries a public DNS server to resolve the SMTP server's domain name (xxx.LAN-SMTP.com in this example) and gets the SMTP server's mapped public IP address of 1.1.1.1.

Figure 143 LAN Computer Queries a Public DNS Server



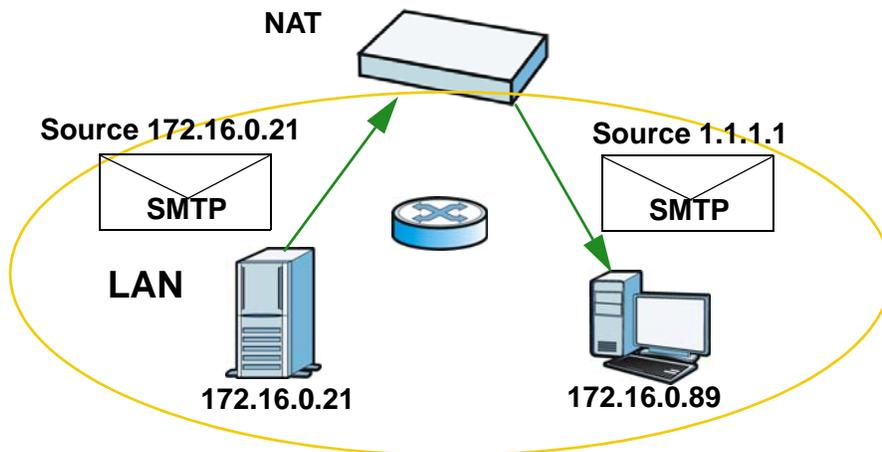
The LAN user's computer then sends traffic to IP address 1.1.1.1. NAT loopback uses the IP address of the UAG's lan1 interface (172.16.0.1) as the source address of the traffic going from the LAN users to the LAN SMTP server.

Figure 144 LAN to LAN Traffic



The LAN SMTP server replies to the UAG's LAN IP address and the UAG changes the source address to 1.1.1.1 before sending it to the LAN user. The return traffic's source matches the original destination address (1.1.1.1). If the SMTP server replied directly to the LAN user without the traffic going through NAT, the source would not match the original destination address which would cause the LAN user's computer to shut down the session.

Figure 145 LAN to LAN Return Traffic



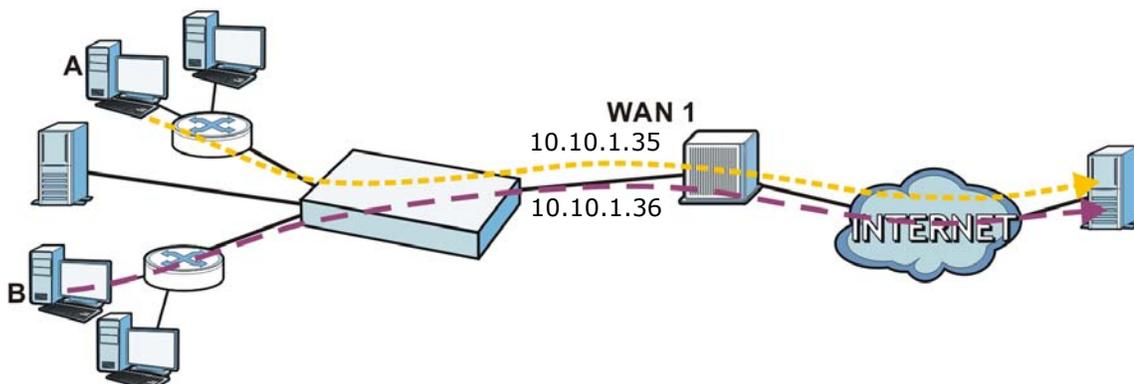
VPN 1-1 Mapping

15.1 VPN 1-1 Mapping Overview

VPN 1-1 mapping allows an authenticated user in your network to access the Internet or an external server using a public IP address different from the one used by the UAG's WAN interface. With VPN 1-1 mapping, each user that logs into the UAG and matches a pre-configured mapping rule can obtain an individual public IP address.

For example, users **A** and **B** are behind the UAG and both want to use a unique WAN IP address to access a public server through the UAG's WAN1 interface. After the user is authenticated by the UAG and meets the criteria in a VPN 1-1 mapping rule, the UAG applies the rule settings and assigns a public IP address to the user. Outgoing traffic from user **A** will then be sent through the WAN1 interface using the mapped public IP address 10.10.1.35. Outgoing traffic from user **B** will be sent through the WAN1 interface using the mapped public IP address 10.10.1.36.

Figure 146 VPN 1-1 Mapping Example



15.1.1 What You Can Do in this Chapter

- Use the **VPN 1-1 Mapping** screens (see [Section 15.2 on page 227](#)) to enable and configure VPN 1-1 mapping to assign a public IP address to each of users that match the rules.
- Use the **VPN 1-1 Mapping > Profile** screen (see [Section 15.3 on page 229](#)) to configure a pool profile which defines the public IP address(es) that the UAG assigns to the matched users and the interface through which the user's traffic is forwarded.

15.1.2 What You Need to Know

VPN 1-1 Mapping, Security Policy and Policy Route

With VPN 1-1 mapping, the relevant packet flow for traffic from the matched user is:

- 1 Security Policy
- 2 Policy Route
- 3 VPN 1-1 Mapping

If you set a policy route to the same user/user group as a VPN 1-1 mapping rule, the UAG checks the policy routing rules first and forwards the traffic to a specified next-hop if matched. You need to make sure there is no security policy(ies) blocking the traffic from the matched user or user group.

To make the example in [Figure 146 on page 226](#) work, make sure you have the following settings. For traffic between **lan1** or **lan2** and **wan1**:

- a from LAN1/LAN2 to WAN security policy (default) to allow any traffic from the user A/B from **lan1** or **lan2** to **wan1**. Responses to this request are allowed automatically.
- a VPN 1-1 mapping rule to forward any traffic from the user A/B through the wan1 interface using a unique public IP address.

15.2 The VPN 1-1 Mapping General Screen

The **VPN 1-1 Mapping** summary screen provides a summary of all VPN 1-1 mapping rules and their configuration. In addition, this screen allows you to create new VPN 1-1 mapping rules and edit and delete existing VPN 1-1 mapping rules. To access this screen, login to the Web Configurator and click **Configuration > Network > VPN 1-1 Mapping**. The following screen appears, providing a summary of the existing VPN 1-1 mapping rules.

Figure 147 Configuration > Network > VPN 1-1 Mapping

#	Status	User / Group	Pool Profile
1	🔦	Client-A	POOL-1
2	🔦	user1	POOL-1

The following table describes the labels in this screen.

Table 98 Configuration > Network > VPN 1-1 Mapping

LABEL	DESCRIPTION
Enable VPN 1-1 Mapping	Select this option to enable VPN 1-1 mapping on the UAG.
Add	Click this to create a new entry.

Table 98 Configuration > Network > VPN 1-1 Mapping (continued)

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
Move	To change a rule's position in the numbered list, select the rule and click Move to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
#	This field is a sequential value, and it is not associated with a specific entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
User / Group	This field displays the name of the user or user group object to which this rule is applied.
Pool Profile	This field displays the name of the pool profile used by this rule.
Apply	Click this button to save your changes to the UAG.
Reset	Click this button to return the screen to its last-saved settings.

15.2.1 The VPN 1-1 Mapping Edit Screen

Click **Network > VPN 1-1 Mapping** to open the **VPN 1-1 Mapping > General** screen. Then click the **Add** or **Edit** icon to open the **VPN 1-1 Mapping Add/Edit Policy** screen where you can configure the rule.

Figure 148 Network > VPN 1-1 Mapping > Add

The screenshot shows the 'Add Policy' configuration window. At the top, there is a title bar with a plus icon, the text 'Add Policy', and standard window controls. Below the title bar is a 'Create new Object' dropdown menu. The main area is divided into three sections by horizontal lines:

- Configuration:** Contains a checkbox labeled 'Enable Policy' which is currently unchecked.
- User / Group:** Contains a label 'User:' followed by a dropdown menu showing 'any'.
- Pool Profile:** Contains two list boxes. The left box is titled 'Selectable Pool Profiles' and contains two entries: 'POOL-1' and '=== Object ==='. The right box is titled 'Selected Pool Profiles' and is currently empty. Between the two boxes are four arrow buttons: a right-pointing arrow, a left-pointing arrow, an up-pointing arrow, and a down-pointing arrow.

At the bottom right of the window are two buttons: 'OK' and 'Cancel'.

The following table describes the labels in this screen.

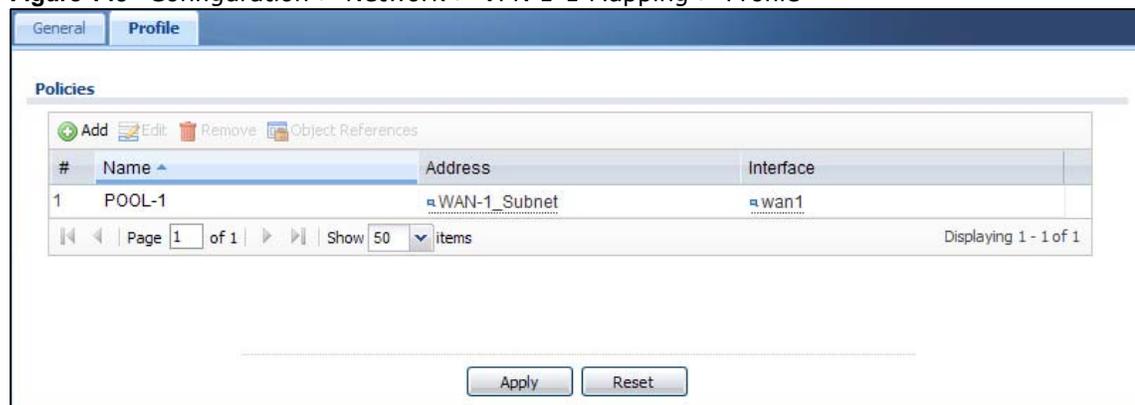
Table 99 Network > VPN 1-1 Mapping > Add

LABEL	DESCRIPTION
Create New Object	Click this button to create any new user/group objects that you need to use in this screen.
Enable Policy	Use this option to turn the VPN 1-1 mapping rule on or off.
User/Group	Use the drop-down list box to select the individual or group for which you want to use this rule. Select any to have the mapping rule apply to all of the traffic that the UAG receives from any user.
Pool Profile	The Selectable Pool Profiles list displays the name(s) of the pool profile(s) you can select for this mapping rule. To associate a pool profile to this mapping rule, you can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and click the right arrow button to add to the Selected Pool Profiles list. To remove a pool profile, select the name(s) in the Selected Pool Profiles list and click the left arrow button. You can also use the up or down arrow button to change the order of members in the Selected Pool Profiles list.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

15.3 The VPN 1-1 Mapping Profile Screen

The **VPN 1-1 Mapping Profile** summary screen provides a summary of all pool profiles for VPN 1-1 mapping and their configuration. In addition, this screen allows you to create new pool profiles and edit and delete existing profiles. A pool profile defines the public IP address(es) that the UAG assigns to the matched users and the interface through which the user's traffic is forwarded. To access this screen, login to the Web Configurator and click **Configuration > Network > VPN 1-1 Mapping > Profile**. The following screen appears, providing a summary of the existing IP address pool profiles.

Figure 149 Configuration > Network > VPN 1-1 Mapping > Profile



The following table describes the labels in this screen.

Table 100 Configuration > Network > VPN 1-1 Mapping > Profile

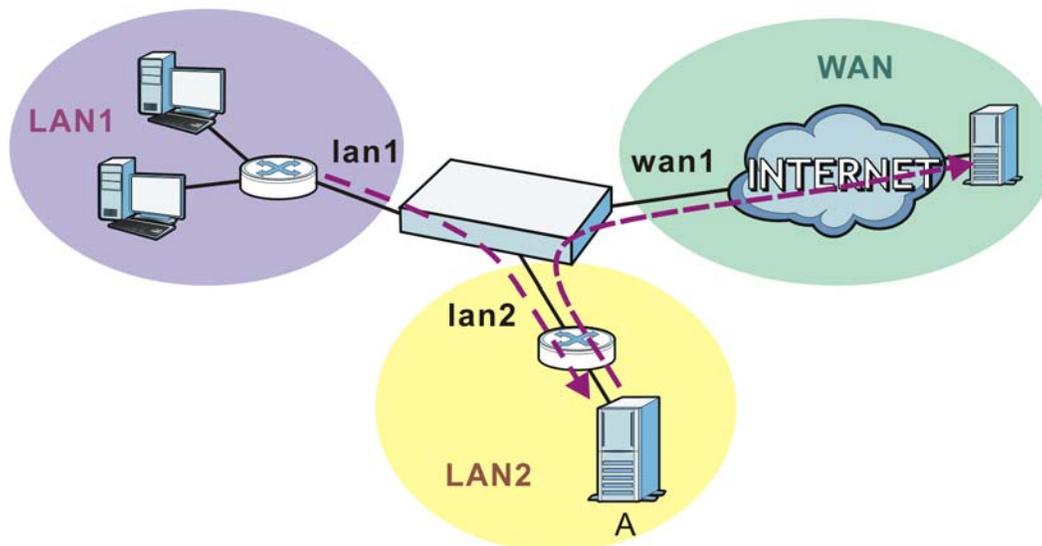
LABEL	DESCRIPTION
Add	Click this to add an entry to the table. If you click Add without selecting an entry in advance then the new entry appears as the first entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Object Reference	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 10.3.2 on page 165 for an example.
#	This field is a sequential value, and it is not associated with a specific entry.
Name	This field displays a descriptive name for the profile. Enter a descriptive name to identify the profile.
Address	This field displays the name of the IP address object the profile is set to use. Select an address object that presents the IP address(es), which can be assigned to the matched users by the UAG. Note: You cannot select an address group object at the time of writing. Note: It's recommended that the IP addresses of the selected address object and the WAN interface are in the same subnet so that the UAG can receive response packets from the remote node.
Interface	This field displays the name of the interface the profile is set to use. Select the interface through which the UAG sends traffic from the matched users.
Apply	Click this button to save your changes to the UAG.
Reset	Click this button to return the screen to its last-saved settings.

HTTP Redirect

16.1 Overview

HTTP redirect forwards the client's HTTP request (except HTTP traffic destined for the UAG) to a web proxy server. In the following example, proxy server **A** is connected to the **lan2** interface in the **LAN2** zone. When a client connected to the **lan1** interface in the **LAN1** zone wants to open a web page, its HTTP request is redirected to proxy server **A** first. If proxy server **A** cannot find the web page in its cache, a policy route allows it to access the Internet to get them from a server. Proxy server **A** then forwards the response to the client.

Figure 150 HTTP Redirect Example



16.1.1 What You Can Do in this Chapter

Use the **HTTP Redirect** screens (see [Section 16.2 on page 232](#)) to display and edit the HTTP redirect rules.

16.1.2 What You Need to Know

Web Proxy Server

A proxy server helps client devices make indirect requests to access the Internet or outside network resources/services. A proxy server can act as a firewall or an ALG (application layer gateway) between the private network and the Internet or other networks. It also keeps hackers from knowing internal IP addresses.

A client connects to a web proxy server each time he/she wants to access the Internet. The web proxy provides caching service to allow quick access and reduce network usage. The proxy checks its local cache for the requested web resource first. If it is not found, the proxy gets it from the specified server and forwards the response to the client.

HTTP Redirect, Security Policy and Policy Route

With HTTP redirect, the relevant packet flow for HTTP traffic is:

- 1 Security Policy
- 2 HTTP Redirect
- 3 Policy Route

Even if you set a policy route to the same incoming interface and service as a HTTP redirect rule, the UAG checks the HTTP redirect rules first and forwards HTTP traffic to a proxy server if matched. You need to make sure there is no security policy(ies) blocking the HTTP requests from the client to the proxy server.

You also need to manually configure a policy route to forward the HTTP traffic from the proxy server to the Internet. To make the example in [Figure 150 on page 231](#) work, make sure you have the following settings.

For HTTP traffic between **lan1** and **lan2**:

- a from LAN1 to LAN2 security policy to allow HTTP requests from **lan1** to **lan2**. Responses to this request are allowed automatically.
- a HTTP redirect rule to forward HTTP traffic from **lan1** to proxy server **A**.

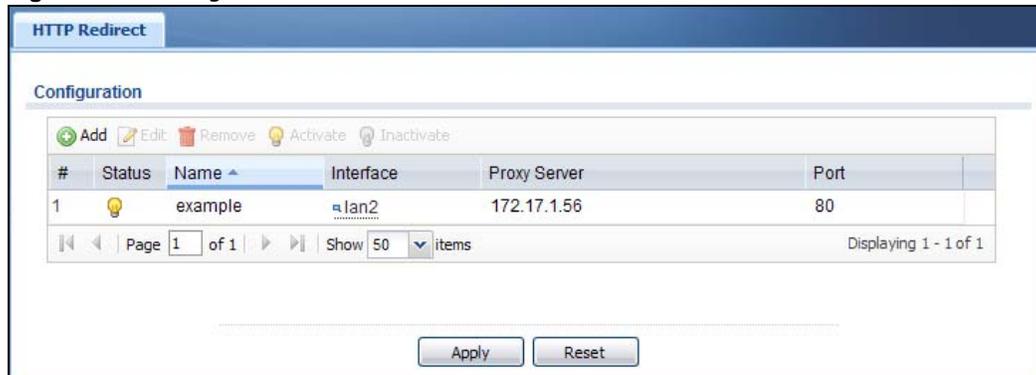
For HTTP traffic between **lan2** and **wan1**:

- a from LAN2 to WAN security policy (default) to allow HTTP requests from **lan2** to **wan1**. Responses to these requests are allowed automatically.
- a policy route to forward HTTP traffic from proxy server **A** to the Internet.

16.2 The HTTP Redirect Screen

To configure redirection of a HTTP request to a proxy server, click **Configuration > Network > HTTP Redirect**. This screen displays the summary of the HTTP redirect rules.

Note: You can configure up to one HTTP redirect rule for each (incoming) interface.

Figure 151 Configuration > Network > HTTP Redirect

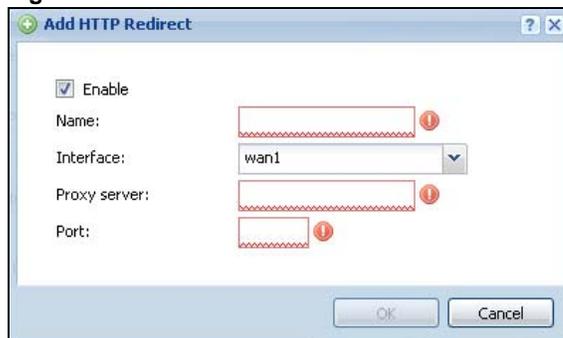
The following table describes the labels in this screen.

Table 101 Configuration > Network > HTTP Redirect

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
#	This field is a sequential value, and it is not associated with a specific entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This is the descriptive name of a rule.
Interface	This is the interface on which the request must be received.
Proxy Server	This is the IP address of the proxy server.
Port	This is the service port number used by the proxy server.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

16.2.1 The HTTP Redirect Edit Screen

Click **Network > HTTP Redirect** to open the **HTTP Redirect** screen. Then click the **Add** or **Edit** icon to open the **HTTP Redirect Edit** screen where you can configure the rule.

Figure 152 Network > HTTP Redirect > Edit

The following table describes the labels in this screen.

Table 102 Network > HTTP Redirect > Edit

LABEL	DESCRIPTION
Enable	Use this option to turn the HTTP redirect rule on or off.
Name	Enter a name to identify this rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Interface	Select the interface on which the HTTP request must be received for the UAG to forward it to the specified proxy server.
Proxy Server	Enter the IP address of the proxy server.
Port	Enter the port number that the proxy server uses.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

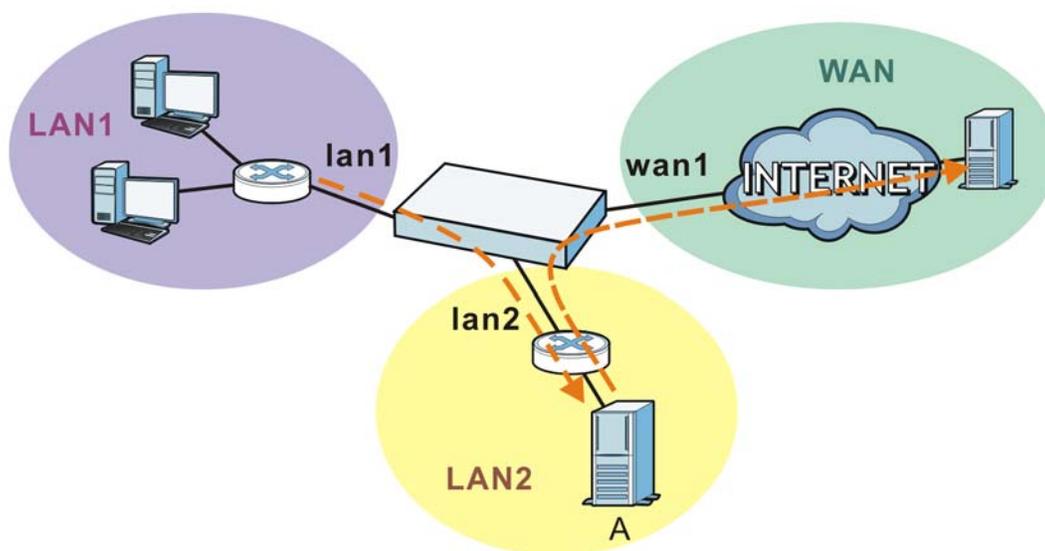
SMTP Redirect

17.1 Overview

SMTP redirect forwards the authenticated client's SMTP message to a SMTP server, that handles all outgoing e-mail messages. In the following example, SMTP server **A** is connected to the **lan2** interface in the **LAN2** zone. When a client connected to the **lan1** interface in the **LAN1** zone logs into the UAG and wants to send an e-mail, its SMTP message is redirected to SMTP server **A**. SMTP server **A** then sends it to a mail server, where the message will be delivered to the recipient.

The UAG forwards SMTP traffic using TCP port 25.

Figure 153 SMTP Redirect Example



17.1.1 What You Can Do in this Chapter

Use the **SMTP Redirect** screens (see [Section 17.2 on page 236](#)) to display and edit the SMTP redirect rules.

17.1.2 What You Need to Know

SMTP

Simple Mail Transfer Protocol (SMTP) is the Internet's message transport standard. It controls the sending of e-mail messages between servers. E-mail clients (also called e-mail applications) then use mail server protocols such as POP (Post Office Protocol) or IMAP (Internet Message Access Protocol) to retrieve e-mail. E-mail clients also generally use SMTP to send messages to a mail

server. The older POP2 requires SMTP for sending messages while the newer POP3 can be used with or without it. This is why many e-mail applications require you to specify both the SMTP server and the POP or IMAP server (even though they may actually be the same server).

SMTP Redirect, Security Policy and Policy Route

With SMTP redirect, the relevant packet flow for SMTP traffic is:

- 1 Security Policy
- 2 SMTP Redirect
- 3 Policy Route

Even if you set a policy route to the same incoming interface and service as a SMTP redirect rule, the UAG checks the SMTP redirect rules first and forwards SMTP traffic to a SMTP server if matched. You need to make sure there is no security policy(ies) blocking the SMTP traffic from the client to the SMTP server.

You also need to manually configure a policy route to forward the SMTP traffic from the SMTP server to the Internet. To make the example in [Figure 153 on page 235](#) work, make sure you have the following settings.

For SMTP traffic between **lan1** and **lan2**:

- a from LAN1 to LAN2 security policy to allow SMTP messages from **lan1** to **lan2**. Responses to this request are allowed automatically.
- a SMTP redirect rule to forward SMTP traffic from **lan1** to SMTP server **A**.

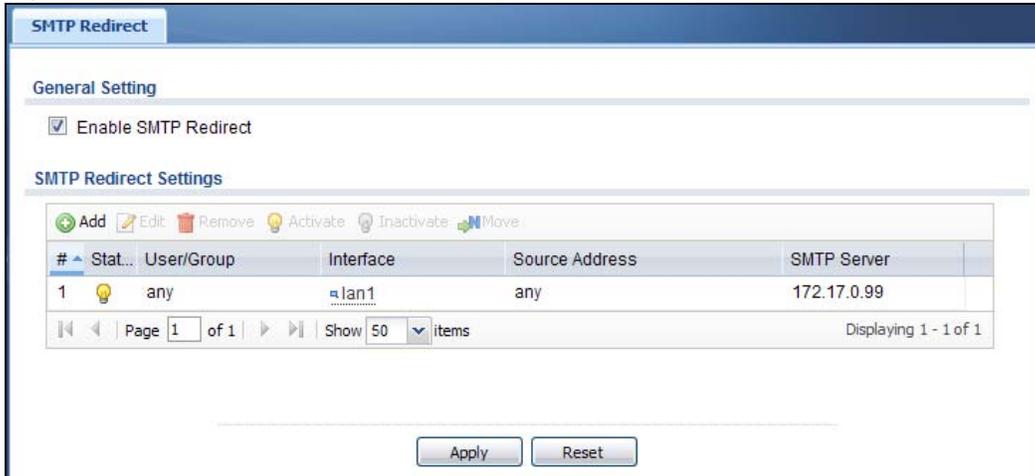
For SMTP traffic between **lan2** and **wan1**:

- a from LAN2 to WAN security policy (default) to allow SMTP messages from **lan2** to **wan1**. Responses to these requests are allowed automatically.
- a policy route to forward SMTP messages from SMTP server **A** to the Internet.

17.2 The SMTP Redirect Screen

To configure redirection of a SMTP message to a SMTP server, click **Configuration > Network > SMTP Redirect**. This screen displays the summary of the SMTP redirect rules.

Note: You can configure up to one SMTP redirect rule for each (incoming) interface.

Figure 154 Configuration > Network > SMTP Redirect

The following table describes the labels in this screen.

Table 103 Configuration > Network > SMTP Redirect

LABEL	DESCRIPTION
Enable SMTP Redirect	Select this option to turn on the SMTP redirect feature on the UAG.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
Move	To change a rule's position in the numbered list, select the rule and click Move to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
#	This field is a sequential value, and it is not associated with a specific entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
User/Group	This is the user account or user group name to whose SMTP traffic this rule is applied.
Interface	This is the name of the interface on which the SMTP traffic must be received.
Source Address	This is the name of the source IP address object from which the SMTP traffic should be sent. If any displays, the rule is effective for every source.
SMTP Server	This is the IP address or Fully-Qualified Domain Name (FQDN) of the SMTP server to which the matched SMTP traffic is forwarded.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

17.2.1 The SMTP Redirect Edit Screen

Click **Network > SMTP Redirect** to open the **SMTP Redirect** screen. Then click the **Add** or **Edit** icon to open the **SMTP Redirect Edit** screen where you can configure the rule.

Figure 155 Network > SMTP Redirect > Edit

The following table describes the labels in this screen.

Table 104 Network > SMTP Redirect > Edit

LABEL	DESCRIPTION
Enable	Use this option to turn the SMTP redirect rule on or off.
User	Use the drop-down list box to select the individual user or user group for which you want to use this rule. Select any to have the SMTP redirect rule apply to all of the SMTP messages that the UAG receives from any user.
Interface	Select the interface on which the SMTP traffic must be received for the UAG to forward it to the specified SMTP server.
Source Address	Select the source address or address group for whom this rule applies. Use Create new Object if you need to configure a new one. Select any if the rule is effective for every source.
SMTP Server	Enter the IP address or Fully-Qualified Domain Name (FQDN) of the SMTP server.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

18.1 ALG Overview

Application Layer Gateway (ALG) allows the following application to operate properly through the UAG's NAT.

- FTP - File Transfer Protocol - an Internet file transfer service.

The ALG feature is only needed for traffic that goes through the UAG's NAT.

18.1.1 What You Can Do in this Chapter

Use the **ALG** screen ([Section 18.2 on page 240](#)) to set up the FTP ALG settings.

18.1.2 What You Need to Know

Application Layer Gateway (ALG), NAT and Security Policy

The UAG can function as an Application Layer Gateway (ALG) to allow certain NAT un-friendly applications to operate properly through the UAG's NAT and security policies. The UAG dynamically creates an implicit NAT session and security policy session for the application's traffic from the WAN to the LAN. The ALG on the UAG supports all of the UAG's NAT mapping types.

FTP ALG

The FTP ALG allows TCP packets with a specified port destination to pass through. If the FTP server is located on the LAN, you must also configure NAT (port forwarding) and security policies if you want to allow access to the server from the WAN.

ALG and Trunks

If you send your ALG-managed traffic through an interface trunk and all of the interfaces are set to active, you can configure routing policies to specify which interface the ALG-managed traffic uses.

You could also have a trunk with one interface set to active and a second interface set to passive. The UAG does not automatically change ALG-managed connections to the second (passive) interface when the active interface's connection goes down. When the active interface's connection fails, the client needs to re-initialize the connection through the second interface (that was set to passive) in order to have the connection go through the second interface.

18.1.3 Before You Begin

You must also configure the security policies and enable NAT in the UAG to allow sessions initiated from the WAN.

18.2 The ALG Screen

Click **Configuration > Network > ALG** to open the **ALG** screen. Use this screen to turn the ALG off or on, configure the port numbers to which it applies.

Figure 156 Configuration > Network > ALG

The following table describes the labels in this screen.

Table 105 Configuration > Network > ALG

LABEL	DESCRIPTION
Enable FTP ALG	Turn on the FTP ALG to detect FTP (File Transfer Program) traffic and help build FTP sessions through the UAG's NAT.
Enable FTP Transformations	Select this option to have the UAG modify IP addresses and port numbers embedded in the FTP data payload to match the UAG's NAT environment. Clear this option if you have an FTP device or server that will modify IP addresses and port numbers embedded in the FTP data payload to match the UAG's NAT environment.
FTP Signaling Port	If you are using a custom TCP port number (not 21) for FTP traffic, enter it here.
Additional FTP Signaling Port for Transformations	If you are also using FTP on an additional TCP port number, enter it here.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

19.1 Overview

The UAG supports both UPnP and NAT-PMP to permit networking devices to discover each other and connect seamlessly.

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use. A gateway that supports UPnP is called Internet Gateway Device (IGD). The standardized Device Control Protocol (DCP) is defined by the UPnP Forum for IGDs to configure port mapping automatically.

NAT Port Mapping Protocol (NAT-PMP), introduced by Apple and implemented in current Apple products, is used as an alternative NAT traversal solution to the UPnP IGD protocol. NAT-PMP runs over UDP port 5351. NAT-PMP is much simpler than UPnP IGD and mainly designed for small home networks. It allows a client behind a NAT router to retrieve the router's public IP address and port number and make them known to the peer device with which it wants to communicate. The client can automatically configure the NAT router to create a port mapping to allow the peer to contact it.

19.2 What You Need to Know

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

19.2.1 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

19.2.2 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening security policy ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the UAG allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

19.3 UPnP Screen

Use this screen to enable UPnP and NAT-PMP on your UAG.

Click **Configuration > Network > UPnP** to display the screen shown next.

Figure 157 Configuration > Network > UPnP

The screenshot displays the UPnP configuration interface. At the top, there is a blue header with the text "UPnP". Below this, the "General Setting" section contains three checked checkboxes: "Enable UPnP", "Enable NAT-PMP", and "Allow UPnP or NAT-PMP to pass through Firewall". Below these checkboxes is a label "Outgoing WAN Interface:" followed by a dropdown menu currently set to "ALL".

The "Support LAN List" section is divided into two columns: "Available" and "Member". The "Available" column lists "lan2" and "vlan0". The "Member" column lists "lan1". Between the two columns are two arrow buttons: a right-pointing arrow (→) and a left-pointing arrow (←).

At the bottom of the screen, there are two buttons: "Apply" and "Reset".

The following table describes the fields in this screen.

Table 106 Configuration > Network > UPnP

LABEL	DESCRIPTION
Enable UPnP	Select this check box to activate UPnP on the UAG. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the UAG's IP address (although you must still enter the password to access the web configurator).
Enable NAT-PMP	Select this check box to activate NAT-PMP on the UAG. Be aware that anyone could use a NAT-PMP application to open the web configurator's login screen without entering the UAG's IP address (although you must still enter the password to access the web configurator).
Allow UPnP or NAT-PMP to pass through Firewall	Select this check box to allow traffic from UPnP-enabled or NAT-PMP-enabled applications to bypass the security policies. Clear this check box to have the security policies block all UPnP or NAT-PMP application packets (for example, MSN packets).
Outgoing WAN Interface	Select through which WAN interface(s) you want to send out traffic from UPnP-enabled or NAT-PMP-enabled applications. If the WAN interface you select loses its connection, the UAG attempts to use the other WAN interface. If the other WAN interface also does not work, the UAG drops outgoing packets from UPnP-enabled or NAT-PMP-enabled applications.
Support LAN List	The Available list displays the name(s) of the internal interface(s) on which the UAG supports UPnP and/or NAT-PMP. To enable UPnP and/or NAT-PMP on an interface, you can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and click the right arrow button to add to the Member list. To remove an interface, select the name(s) in the Member list and click the left arrow button.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

19.4 Technical Reference

The sections show examples of using UPnP.

19.4.1 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the UAG.

Make sure the computer is connected to a LAN port of the UAG. Turn on your computer and the UAG.

19.4.1.1 Auto-discover Your UPnP-enabled Network Device

- 1 Click **start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
- 2 Right-click the icon and select **Properties**.

Figure 158 Network Connections



- 3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Figure 159 Internet Connection Properties



- 4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 160 Internet Connection Properties: Advanced Settings

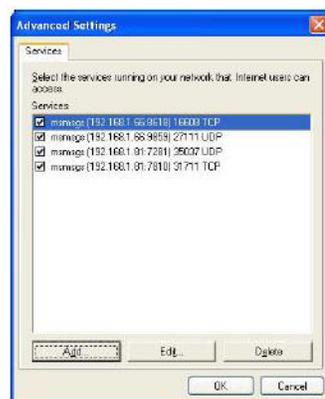
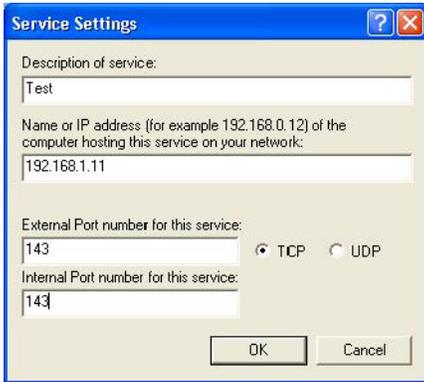


Figure 161 Internet Connection Properties: Advanced Settings: Add

Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

- 5 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

Figure 162 System Tray Icon

- 6 Double-click on the icon to display your current Internet connection status.

Figure 163 Internet Connection Status

19.4.2 Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the UAG without finding out the IP address of the UAG first. This comes helpful if you do not know the IP address of the UAG.

Follow the steps below to access the web configurator.

- 1 Click **Start** and then **Control Panel**.
- 2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

Figure 164 Network Connections



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click on the icon for your UAG and select **Invoke**. The web configurator login screen displays.

Figure 165 Network Connections: My Network Places



6 Right-click on the icon for your UAG and select **Properties**. A properties window displays with basic information about the UAG.

Figure 166 Network Connections: My Network Places: Properties: Example



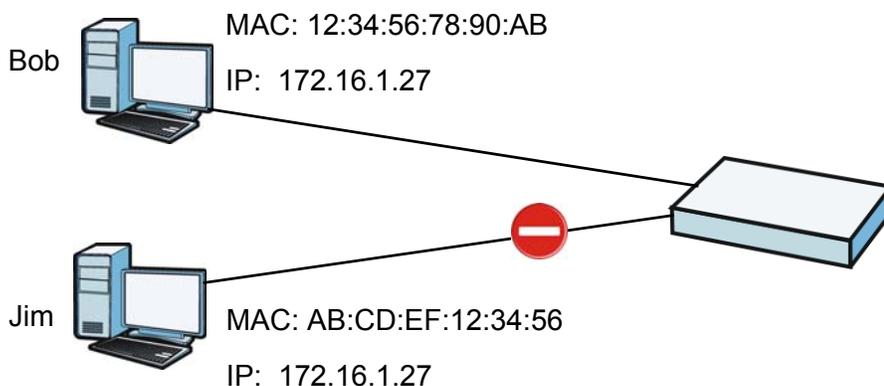
IP/MAC Binding

20.1 IP/MAC Binding Overview

IP address to MAC address binding helps ensure that only the intended devices get to use privileged IP addresses. The UAG uses DHCP to assign IP addresses and records to MAC address it assigned each IP address. The UAG then checks incoming connection attempts against this list. A user cannot manually assign another IP to his computer and use it to connect to the UAG.

Suppose you configure access privileges for IP address 172.16.1.27 and use static DHCP to assign it to Bob's computer's MAC address of 12:34:56:78:90:AB. IP/MAC binding drops traffic from any computer trying to use IP address 172.16.1.27 with another MAC address.

Figure 167 IP/MAC Binding Example



20.1.1 What You Can Do in this Chapter

- Use the **Summary** and **Edit** screens ([Section 20.2 on page 249](#)) to bind IP addresses to MAC addresses.
- Use the **Exempt List** screen ([Section 20.3 on page 251](#)) to configure ranges of IP addresses to which the UAG does not apply IP/MAC binding.

20.1.2 What You Need to Know

DHCP

IP/MAC address bindings are based on the UAG's dynamic and static DHCP entries.

Interfaces Used With IP/MAC Binding

IP/MAC address bindings are grouped by interface. You can use IP/MAC binding with Ethernet, bridge, VLAN interfaces. You can also enable or disable IP/MAC binding and logging in an interface's configuration screen.

20.2 IP/MAC Binding Summary

Click **Configuration > Network > IP/MAC Binding** to open the **IP/MAC Binding Summary** screen. This screen lists the total number of IP to MAC address bindings for devices connected to each supported interface.

Figure 168 Configuration > Network > IP/MAC Binding > Summary

#	Status	Interface	Number of Binding
1		dmz	1
2		lan1	1
3		lan2	7
4		wan1	0
5		wan2	0

The following table describes the labels in this screen.

Table 107 Configuration > Network > IP/MAC Binding > Summary

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
#	This field is a sequential value, and it is not associated with a specific entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Interface	This is the name of an interface that supports IP/MAC binding.
Number of Binding	This field displays the interface's total number of IP/MAC bindings and IP addresses that the interface has assigned by DHCP.
Apply	Click Apply to save your changes back to the UAG.

20.2.1 IP/MAC Binding Edit

Click **Configuration > Network > IP/MAC Binding > Edit** to open the **IP/MAC Binding Edit** screen. Use this screen to configure an interface's IP to MAC address binding settings.

Figure 169 Configuration > Network > IP/MAC Binding > Edit

The following table describes the labels in this screen.

Table 108 Configuration > Network > IP/MAC Binding > Edit

LABEL	DESCRIPTION
IP/MAC Binding Settings	
Interface Name	This field displays the name of the interface within the UAG and the interface's IP address and subnet mask.
Enable IP/MAC Binding	Select this option to have this interface enforce links between specific IP addresses and specific MAC addresses. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.
Enable Logs for IP/MAC Binding Violation	Select this option to have the UAG generate a log if a device connected to this interface attempts to use an IP address not assigned by the UAG.
Static DHCP Bindings	This table lists the bound IP and MAC addresses. The UAG checks this table when it assigns IP addresses. If the computer's MAC address is in the table, the UAG assigns the corresponding IP address. You can also access this table from the interface's edit screen.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
#	This is the index number of the static DHCP entry.
IP Address	This is the IP address that the UAG assigns to a device with the entry's MAC address.
MAC Address	This is the MAC address of the device to which the UAG assigns the entry's IP address.

Table 108 Configuration > Network > IP/MAC Binding > Edit (continued)

LABEL	DESCRIPTION
Description	This helps identify the entry.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

20.2.2 Static DHCP Edit

Click **Configuration > Network > IP/MAC Binding > Edit** to open the **IP/MAC Binding Edit** screen. Click the **Add** or **Edit** icon to open the following screen. Use this screen to add or configure a static DHCP entry.

Figure 170 Configuration > Network > IP/MAC Binding > Edit > Add

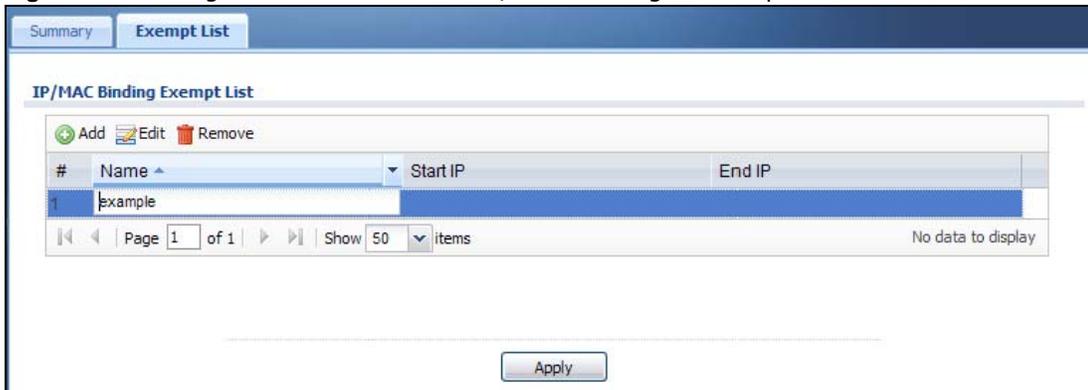
The following table describes the labels in this screen.

Table 109 Configuration > Network > IP/MAC Binding > Edit > Add

LABEL	DESCRIPTION
Interface Name	This field displays the name of the interface within the UAG and the interface's IP address and subnet mask.
IP Address	Enter the IP address that the UAG is to assign to a device with the entry's MAC address.
MAC Address	Enter the MAC address of the device to which the UAG assigns the entry's IP address.
Description	Enter up to 64 printable ASCII characters to help identify the entry. For example, you may want to list the computer's owner.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

20.3 IP/MAC Binding Exempt List

Click **Configuration > Network > IP/MAC Binding > Exempt List** to open the **IP/MAC Binding Exempt List** screen. Use this screen to configure ranges of IP addresses to which the UAG does not apply IP/MAC binding.

Figure 171 Configuration > Network > IP/MAC Binding > Exempt List

The following table describes the labels in this screen.

Table 110 Configuration > Network > IP/MAC Binding > Exempt List

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Click an entry or select it and click Edit to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
#	This is the index number of the IP/MAC binding list entry.
Name	Enter a name to help identify this entry.
Start IP	Enter the first IP address in a range of IP addresses for which the UAG does not apply IP/MAC binding.
End IP	Enter the last IP address in a range of IP addresses for which the UAG does not apply IP/MAC binding.
Apply	Click Apply to save your changes back to the UAG.

Layer 2 Isolation

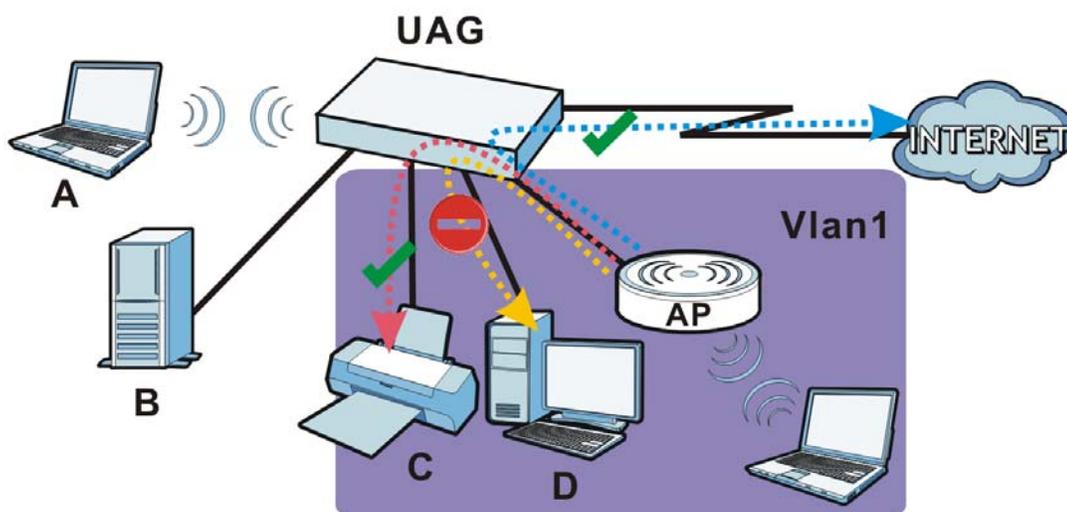
21.1 Overview

Layer-2 isolation is used to prevent connected devices from communicating with each other in the UAG's local network(s), except for the devices in the white list, when layer-2 isolation is enabled on the UAG and the local interface(s).

Note: The security policy control must be enabled before you can use layer-2 isolation.

In the following example, layer-2 isolation is enabled on the UAG's interface Vlan1. A printer, PC and AP are in the Vlan1. The IP address of network printer (C) is added to the white list. With this setting, the connected AP then cannot communicate with the PC (D), but can access the network printer (C), server (B), wireless client (A) and the Internet.

Figure 172 Layer-2 Isolation Application



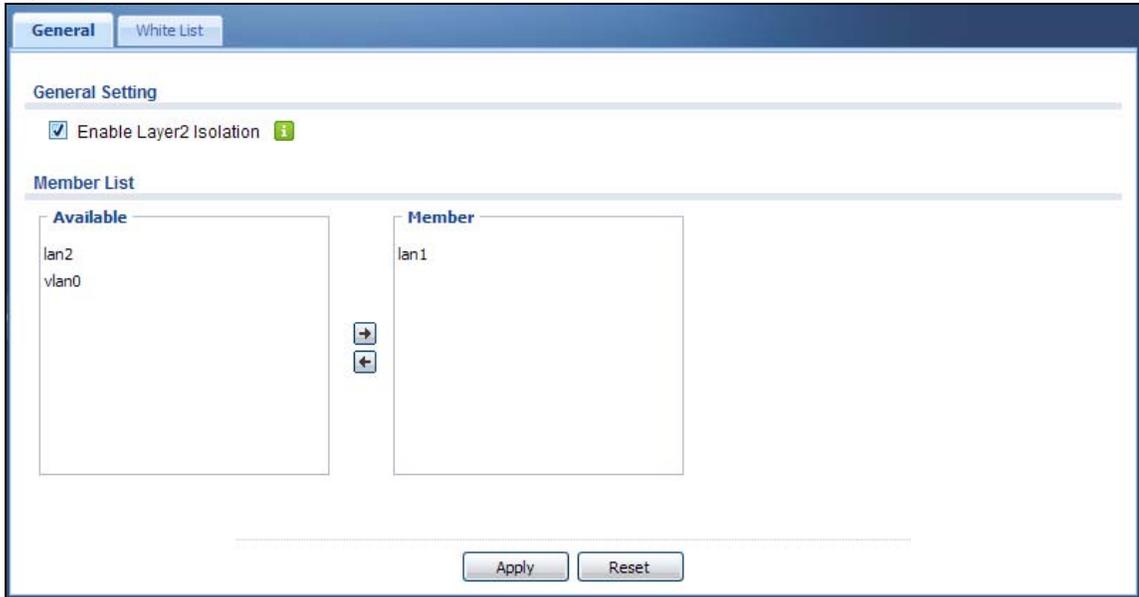
21.1.1 What You Can Do in this Chapter

- Use the **General** screen ([Section 21.2 on page 254](#)) to enable layer-2 isolation on the UAG and the internal interface(s).
- Use the **White List** screen ([Section 21.3 on page 254](#)) to enable and configures the white list.

21.2 Layer-2 Isolation General Screen

This screen allows you to enable Layer-2 isolation on the UAG and specific internal interface(s). To access this screen click **Configuration > Network > Layer 2 Isolation**.

Figure 173 Configuration > Network > Layer 2 Isolation



The following table describes the labels in this screen.

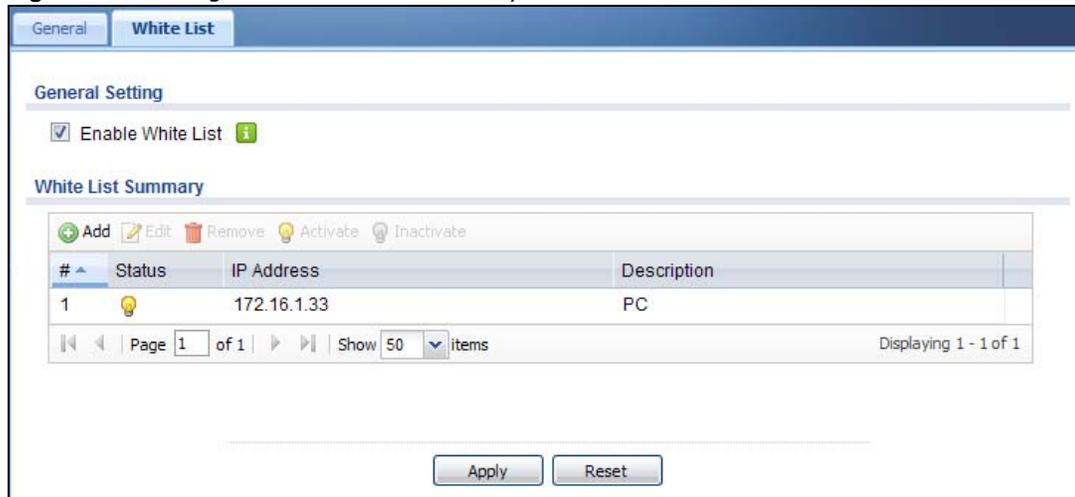
Table 111 Configuration > Network > Layer 2 Isolation

LABEL	DESCRIPTION
Enable Layer2 Isolation	Select this option to turn on the layer-2 isolation feature on the UAG. Note: You can enable this feature only when the security policy is enabled.
Member List	The Available list displays the name(s) of the internal interface(s) on which you can enable layer-2 isolation. To enable layer-2 isolation on an interface, you can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and click the right arrow button to add to the Member list. To remove an interface, select the name(s) in the Member list and click the left arrow button.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

21.3 White List Screen

IP addresses that are not listed in the white list are blocked from communicating with other devices in the layer-2-isolation-enabled internal interface(s) except for broadcast packets.

To access this screen click **Configuration > Network > Layer 2 Isolation > White List**.

Figure 174 Configuration > Network > Layer 2 Isolation > White List

The following table describes the labels in this screen.

Table 112 Configuration > Network > Layer 2 Isolation > White List

LABEL	DESCRIPTION
Enable White List	Select this option to turn on the white list on the UAG. Note: You can enable this feature only when the security policy is enabled.
Add	Click this to add a new rule.
Edit	Click this to edit the selected rule.
Remove	Click this to remove the selected rule.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
#	This field is a sequential value, and it is not associated with a specific rule.
Status	This icon is lit when the rule is active and dimmed when the rule is inactive.
IP Address	This field displays the IP address of device that can be accessed by the devices connected to an internal interface on which layer-2 isolation is enabled.
Description	This field displays the description for the IP address in this rule.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

21.3.1 Add/Edit White List Rule

This screen allows you to create a new rule in the white list or edit an existing one. To access this screen, click the **Add** button or select an entry from the list and click the **Edit** button.

Note: You can configure up to 100 white list rules on the UAG.

Note: You need to know the IP address of each connected device that you want to allow to be accessed by other devices when layer-2 isolation is enabled.

Figure 175 Configuration > Network > Layer 2 Isolation > White List > Add/Edit

The following table describes the labels in this screen.

Table 113 Configuration > Network > Layer 2 Isolation > White List > Add/Edit

LABEL	DESCRIPTION
Enable	Select this option to turn on the rule.
Host IP Address	Enter an IPv4 address associated with this rule.
Description	Specify a description for the IP address associated with this rule. Enter up to 60 characters, spaces and underscores allowed.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving your changes.

22.1 Overview

IP Plug and Play (IPnP) allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, even when the IP addresses of the computer and the UAG are not in the same subnet.

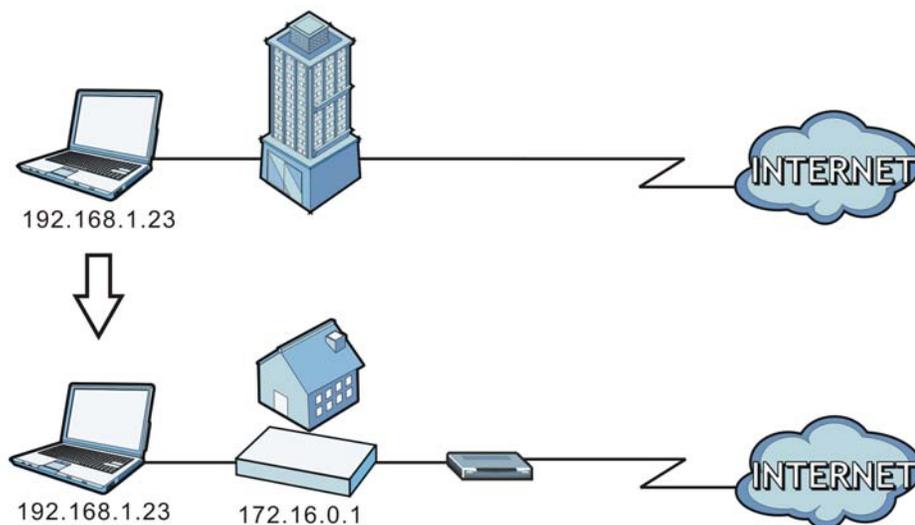
When you disable the IPnP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the UAG's LAN IP address can connect to the UAG or access the Internet through the UAG.

The IPnP feature does not apply to a computer using either a dynamic IP address or a static IP address that is in the same subnet as the UAG's IP address.

Note: You must enable NAT to use the IPnP feature.

The following figure depicts a scenario where a computer is set to use a static private IP address in the corporate environment. In a residential house where a UAG is installed, you can still use the computer to access the Internet without changing the network settings, even when the IP addresses of the computer and the UAG are not in the same subnet.

Figure 176 IPnP Application



22.1.1 What You Can Do in this Chapter

Use the **IP** screen ([Section 22.2 on page 258](#)) to enable IPnP on the UAG and the internal interface(s).

22.2 IPnP Screen

This screen allows you to enable IPnP on the UAG and specific internal interface(s). To access this screen click **Configuration > Network > IPnP**.

Figure 177 Configuration > Network > IPnP

The following table describes the labels in this screen.

Table 114 Configuration > Network > IPnP

LABEL	DESCRIPTION
Enable IPnP	Select this option to turn on the IPnP feature on the UAG. Note: You can enable this feature only when the security policy is enabled.
Member List	The Available list displays the name(s) of the internal interface(s) on which you can enable IPnP. To enable IPnP on an interface, you can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and click the right arrow button to add to the Member list. To remove an interface, select the name(s) in the Member list and click the left arrow button.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

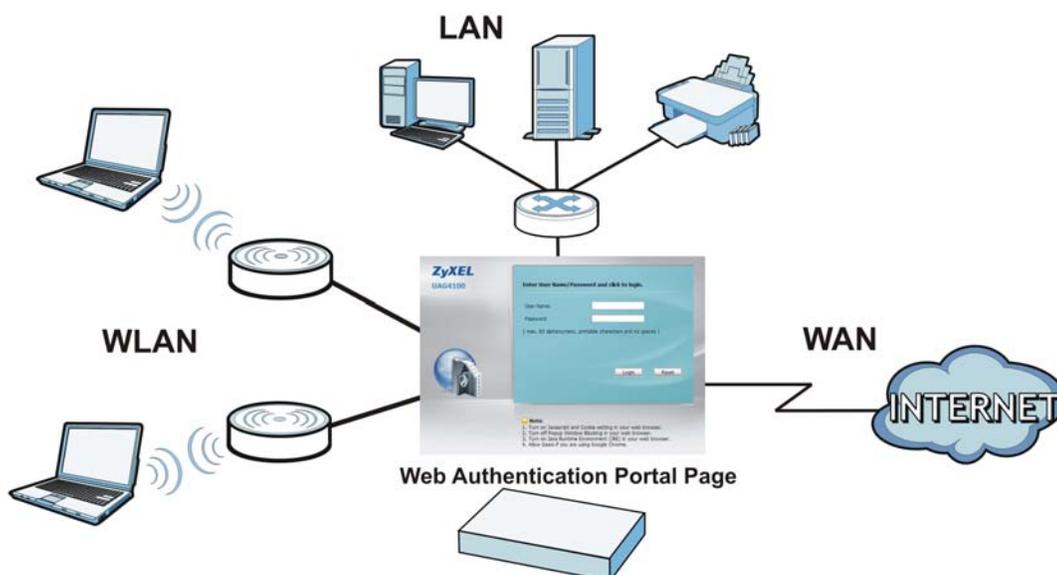
Web Authentication

23.1 Overview

Web authentication can intercepts network traffic, according to the authentication policies, until the user authenticates his or her connection, usually through a specifically designated login web page or user agreement page. This means all web page requests can initially be redirected to a special web page that requires users to authenticate their sessions. Once authentication is successful, they can then connect to the rest of the network or Internet.

As soon as a user attempt to open a web page, the UAG reroutes his/her browser to a web portal page that prompts he/she to log in or agree to the policy of user agreement.

Figure 178 Web Authentication Example



The web authentication page only appears once per authentication session. Unless a user session times out or he/she closes the connection, he or she generally will not see it again during the same session.

23.1.1 What You Can Do in this Chapter

- Use the **Configuration > Web Authentication** screens ([Section 23.2 on page 260](#)) to enable web authentication, set the logout IP, create and manage web authentication policies, configure authentication type profiles and upload or download custom files.
- Use the **Configuration > Web Authentication > Walled Garden** screens ([Section 23.3 on page 277](#)) to enable and create walled garden links that display in the login screen.

- Use the **Configuration > Web Authentication > Advertisement** screens ([Section 23.4 on page 283](#)) to enable and set advertisement links.

23.1.2 What You Need to Know

Forced User Authentication

Instead of making users for which user-aware policies have been configured go to the UAG **Login** screen manually, you can configure the UAG to display the **Login** screen automatically whenever it routes HTTP traffic for anyone who has not logged in yet.

Note: This works with HTTP traffic only. The UAG does not display the **Login** screen when users attempt to send other kinds of traffic.

The UAG does not automatically route the request that prompted the login, however, so users have to make this request again.

Finding Out More

See [Section 23.2.2 on page 264](#) for an example of using an authentication policy for user-aware access control.

23.2 Web Authentication

Click **Configuration > Web Authentication** to display the screen.

23.2.1 General Screen

The **Web Authentication General** screen displays the general web portal settings and web authentication policies you have configured on the UAG. Use this screen to enable web authentication on the UAG.

Figure 179 Configuration > Web Authentication: General

Web Authentication | Walled Garden | Advertisement

General | Authentication Type | Custom Web Portal File | Custom User Agreement File

Global Setting

Enable Web Authentication

Web Portal General Setting

Logout IP: ⓘ

Exceptional Services

➕ Add 🗑️ Remove

#	Exceptional Services
1	DNS

⏪ ⏩ Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

Web Authentication Policy Summary

➕ Add ✎ Edit 🗑️ Remove 💡 Activate ⏻ Inactivate 📦 Move

S...	P...	Incoming I...	Source	Destination	Schedule	Authentication	Authentica...	Description
💡	1	lan2	any	any	none	force	default-we...	
	D...	any	any	any	none	unnecessary	n/a	n/a

⏪ ⏩ Page 1 of 1 Show 50 items Displaying 1 - 2 of 2

Apply Reset

The following table gives an overview of the objects you can configure.

Table 115 Configuration > Web Authentication: General

LABEL	DESCRIPTION
Global Setting	
Enable Web Authentication	Select the check box to turn on the web authentication feature. Otherwise, clear the check box to turn it off. Once enabled, all network traffic is blocked until a client authenticates with the UAG through the specifically designated web portal or user agreement page.
Web Portal General Setting	
Logout IP	Specify an IP address that users can use to terminate their sessions manually by entering the IP address in the address bar of the web browser.

Table 115 Configuration > Web Authentication: General (continued)

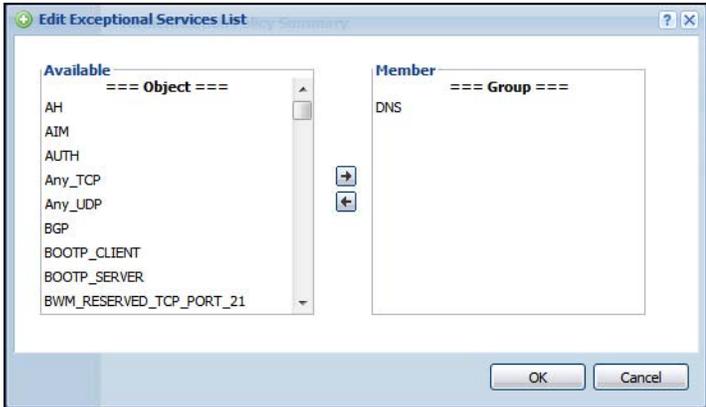
LABEL	DESCRIPTION
Exceptional Services	<p>Use this table to list services that users can access without logging in.</p> <p>Click Add to change the list's membership. A screen appears. Available services appear on the left. Select any services you want users to be able to access without logging in and click the right arrow button to add them. The member services are on the right. Select any service that you want to remove from the member list, and click the left arrow button to remove them.</p> <p>Keeping DNS as a member allows users' computers to resolve domain names into IP addresses.</p> <p>Figure 180 Configuration > Web Authentication > Add Exceptional Service</p>  <p>In the table, select one or more entries and click Remove to delete it or them.</p>
Web Authentication Policy Summary	Use this table to manage the UAG's list of web authentication policies.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
Move	To move an entry to a different number in the list, click the Move icon. In the field that appears, specify the number to which you want to move the interface.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Priority	This is the position of the authentication policy in the list. The priority is important as the policies are applied in order of priority. Default displays for the default authentication policy that the UAG uses on traffic that does not match any exceptional service or other authentication policy. You can edit the default rule but not delete it.
Incoming Interface	This field displays the interface on which packets for this policy are received.
Source	This displays the source address object to which this policy applies.
Destination	This displays the destination address object to which this policy applies.
Schedule	This field displays the schedule object that dictates when the policy applies. none means the policy is active at all times if enabled.

Table 115 Configuration > Web Authentication: General (continued)

LABEL	DESCRIPTION
Authentication	This field displays the authentication requirement for users when their traffic matches this policy. unnecessary - Users do not need to be authenticated. required - Users need to be authenticated. They must manually go to the login screen or user agreement page. The UAG will not redirect them to the login screen. force - Users need to be authenticated. The UAG automatically displays the login screen or user agreement page whenever it routes HTTP traffic for users who have not logged in yet.
Authentication Type	This field displays the name of the authentication type profile used in this policy to define how users authenticate their sessions. It shows n/a if Authentication is set to unnecessary .
Description	If the entry has a description configured, it displays here. This is n/a for the default policy.
Apply	Click this button to save your changes to the UAG.
Reset	Click this button to return the screen to its last-saved settings.

Creating/Editing an Authentication Policy

Open the **Configuration > Web Authentication > General** screen, then click the **Add** icon or select an entry and click the **Edit** icon in the **Web Authentication Policy Summary** section to open the **Auth. Policy Add/Edit** screen. Use this screen to configure an authentication policy.

Figure 181 Configuration > Web Authentication > Add

Auth. Policy Add

Create new Object ▾

General Settings

Enable Policy

Description: (Optional)

User Authentication Policy

Incoming Interface: ▾

Source Address: ▾

Destination Address: ▾

Schedule: ▾

Authentication: ▾

Force User Authentication +

Authentication Type: ▾

OK Cancel

The following table gives an overview of the objects you can configure.

Table 116 Configuration > Web Authentication > Add

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable Policy	Select this check box to activate the authentication policy. This field is available for user-configured policies.
Description	Enter a descriptive name of up to 60 printable ASCII characters for the policy. Spaces are allowed. This field is available for user-configured policies.
User Authentication Policy	Use this section of the screen to determine which traffic requires (or does not require) the senders to be authenticated in order to be routed.
Incoming Interface	Select an interface on which packets for the policy must be received. Select any if the policy is effective for every interface.
Source Address	Select a source address or address group for whom this policy applies. Select any if the policy is effective for every source. This is any and not configurable for the default policy.
Destination Address	Select a destination address or address group for whom this policy applies. Select any if the policy is effective for every destination. This is any and not configurable for the default policy.
Schedule	Select a schedule that defines when the policy applies. Otherwise, select none and the rule is always effective. This is none and not configurable for the default policy.
Authentication	Select the authentication requirement for users when their traffic matches this policy. unnecessary - Users do not need to be authenticated. required - Users need to be authenticated. If Force User Authentication is selected, all HTTP traffic from unauthenticated users is redirected to a default or user-defined login page. Otherwise, they must manually go to the login screen. The UAG will not redirect them to the login screen.
Log	This field is available for the default policy. Select whether to have the UAG generate a log (log), log and alert (log alert) or not (no) for packets that match the default policy. See Chapter 47 on page 534 for more on logs.
Force User Authentication	This field is available for user-configured policies that require authentication. Select this to have the UAG automatically display the login screen when users who have not logged in yet try to send HTTP traffic.
Authentication Type	Select the authentication type profile you want to use in this policy. You can configure the profile using the Web Authentication > Authentication Type screen.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

23.2.2 User-aware Access Control Example

You can configure many policies and security settings for specific users or groups of users. Users can be authenticated locally by the UAG or by an external (RADIUS) authentication server.

In this example the users are authenticated by an external RADIUS server at 172.16.1.200. First, set up the user accounts and user groups in the UAG. Then, set up user authentication using the RADIUS server. Finally, set up the policies in the table above.

23.2.2.1 Set Up User Accounts

Set up user accounts in the RADIUS server. This example uses the Web Configurator. If you can export user names from the RADIUS server to a text file, then you might configure a script to create the user accounts instead.

- 1 Click **Configuration > Object > User/Group > User**. Click the **Add** icon.
- 2 Enter the same user name that is used in the RADIUS server, and set the **User Type** to **ext-user** because this user account is authenticated by an external server. Click **OK**.

Figure 182 Configuration > Object > User/Group > User > Add

The screenshot shows a window titled "Add A User" with a "User Configuration" section. The fields are as follows:

User Name:	Leo
User Type:	ext-user
Description:	Leo
User Settings:	<input checked="" type="radio"/> Use Default Settings <input type="radio"/> Use Manual Settings
Lease Time:	1440 minutes
Reauthentication Time:	1440 minutes

Buttons: OK, Cancel

- 3 Repeat this process to set up the remaining user accounts.

23.2.2.2 Set Up User Groups

Set up the user groups and assign the users to the user groups.

- 1 Click **Configuration > Object > User/Group > Group**. Click the **Add** icon.
- 2 Enter the name of the group. In this example, it is "Finance". Then, select **Object/Leo** and click the right arrow to move him to the **Member** list. This example only has one member in this group, so click **OK**. Of course you could add more members later.

Figure 183 Configuration > Object > User/Group > Group > Add

- 3 Repeat this process to set up the remaining user groups.

23.2.2.3 Set Up User Authentication Using the RADIUS Server

This step sets up user authentication using the RADIUS server. First, configure the settings for the RADIUS server. Then, set up the authentication method, and configure the UAG to use the authentication method. Finally, force users to log into the UAG before it routes traffic for them.

- 1 Click **Configuration > Object > AAA Server > RADIUS**. Double-click the **radius** entry. Configure the RADIUS server's address, authentication port (1812 if you were not told otherwise), and key. Click **OK**.

Figure 184 Configuration > Object > AAA Server > RADIUS > Add

Add RADIUS

General Settings

Name: radius

Description: (Optional)

Authentication Server Settings

Server Address: 172.16.1.200 (IP or FQDN)

Authentication Port: 1812 (1-65535)

Backup Server Address: (IP or FQDN) Optional

Backup Authentication Port: (1-65535) Optional

Key: *****

Accounting Server Settings

Server Address: (IP or FQDN) (Optional)

Accounting Port: (1-65535) (Optional)

Backup Server Address: (IP or FQDN) (Optional)

Backup Accounting Port: (1-65535) (Optional)

Key:

Maximum retry count: 3 (1~10)

Enable Accounting Interim update

Interim Interval: 10 (1-1440 minutes)

General Server Settings

Timeout: 5 (1-300 seconds)

NAS IP Address: 127.0.0.1 (IP Address)

OK Cancel

- 2 Click **Configuration > Object > Auth. Method**. Double-click the **default** entry. Click the **Add** icon. Select **group radius** because the UAG should use the specified RADIUS server for authentication. Click **OK**.

Figure 185 Configuration > Object > Auth. method > Edit

Edit Authentication Method default

General Settings

Name: default

#	Method List
1	group radius
2	local

OK Cancel

- 3 Click **Configuration > Web Authentication**. In the **Web Authentication > General** screen, select **Enable Web Authentication** to turn on the web authentication feature and click **Apply**.

Figure 186 Configuration > Web Authentication

Web Authentication | Walled Garden | Advertisement

General | Authentication Type | Custom Web Portal File | Custom User Agreement File

Global Setting

Enable Web Authentication

Web Portal General Setting

Logout IP: ⓘ

Exceptional Services

➕ Add ⚡ Remove

#	Exceptional Services
1	DNS

Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

Web Authentication Policy Summary

➕ Add ✎ Edit ⚡ Remove ⏻ Inactivate ⏻ Inactivate 📁 Move

S...	P...	Incoming I...	Source	Destination	Schedule	Authentication	Authentica...	Description
1		lan2	any	any	none	force	default-we...	
D...		any	any	any	none	unnecessary	n/a	n/a

Page 1 of 1 | Show 50 items | Displaying 1 - 2 of 2

Apply Reset

- 4 In the **Web Authentication Policy Summary** section, click the **Add** icon to set up a default policy that has priority over other policies and forces every user to log into the UAG before the UAG routes traffic for them.
- 5 Select **Enable Policy**. Enter a descriptive name, "default_policy" for example. Set the **Authentication** field to **required**, and make sure **Force User Authentication** is selected. Select an authentication type profile ("default-web-portal" in this example). Keep the rest of the default settings, and click **OK**.

Note: The users must log in at the Web Configurator login screen before they can use HTTP or MSN.

Figure 187 Configuration > Web Authentication: General: Add

The screenshot shows the 'Auth. Policy Add' configuration window. The 'General Settings' section includes a checked 'Enable Policy' checkbox and a 'Description' field with the value 'default_policy'. The 'User Authentication Policy' section includes dropdown menus for 'Incoming Interface' (any), 'Source Address' (any), 'Destination Address' (any), and 'Schedule' (none). The 'Authentication' dropdown is set to 'required', and the 'Force User Authentication' checkbox is checked. The 'Authentication Type' dropdown is set to 'default-web-portal'. The window has 'OK' and 'Cancel' buttons at the bottom right.

When the users try to browse the web (or use any HTTP application), the login screen appears. They have to log in using the user name and password in the RADIUS server.

23.2.2.4 User Group Authentication Using the RADIUS Server

The previous example showed how to have a RADIUS server authenticate individual user accounts. If the RADIUS server has different user groups distinguished by the value of a specific attribute, you can make a couple of slight changes in the configuration to have the RADIUS server authenticate groups of user accounts defined in the RADIUS server.

- 1 Click **Configuration > Object > AAA Server > RADIUS**. Double-click the **radius** entry. Besides configuring the RADIUS server's address, authentication port, and key; set the **Group Membership Attribute** field to the attribute that the UAG is to check to determine to which group a user belongs. This example uses **Class**. This attribute's value is called a group identifier; it determines to which group a user belongs. In this example the values are Finance, Engineer, Sales, and Boss.

Figure 188 Configuration > Object > AAA Server > RADIUS > Add

Add RADIUS

General Settings

Name: radius

Description: (Optional)

Authentication Server Settings

Server Address: 172.16.1.200 (IP or FQDN)

Authentication Port: 1812 (1-65535)

Backup Server Address: (IP or FQDN)Optional

Backup Authentication Port: (1-65535)Optional

Key:

Accounting Server Settings

Server Address: (IP or FQDN) (Optional)

Accounting Port: (1-65535) (Optional)

Backup Server Address: (IP or FQDN) (Optional)

Backup Accounting Port: (1-65535) (Optional)

Key:

Maximum retry count: 3 (1~10)

Enable Accounting Interim update

Interim Interval: 10 (1-1440 minutes)

General Server Settings

Timeout: 5 (1-300 seconds)

NAS IP Address: 127.0.0.1 (IP Address)

NAS Identifier:

Case-sensitive User Names i

User Login Settings

Group Membership Attribute: Class(25) 25

OK Cancel

- Now you add ext-group-user user objects to identify groups based on the group identifier values. Set up one user account for each group of user accounts in the RADIUS server. Click **Configuration > Object > User/Group > User**. Click the **Add** icon.

Enter a user name and set the **User Type** to **ext-group-user**. In the **Group Identifier** field, enter Finance, Engineer, Sales, or Boss and set the **Associated AAA Server Object** to **radius**.

Figure 189 Configuration > Object > User/Group > User > Add

- Repeat this process to set up the remaining groups of user accounts.

23.2.3 Authentication Type Screen

Use this screen to view, create and manage the authentication type profiles on the UAG. An authentication type profile decides which type of web authentication pages to be used for user authentication. Go to **Configuration > Web Authentication** and then select the **Authentication Type** tab to display the screen.

Figure 190 Configuration > Web Authentication: Authentication Type

#	Name	Type	Web Page
1	default-web-portal	web-portal	System Default Page
2	default-user-agreement	user-agreement	System Default Page

The following table describes the labels in this screen.

Table 117 Configuration > Web Authentication: Authentication Type

LABEL	DESCRIPTION
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Name	<p>This field displays the name of the profile.</p> <p>default-web-portal: the default login page built into the UAG.</p> <p>Note: You can also customize the default login page built into the UAG in the System > WWW > Login Page screen.</p> <p>default-web-portal: the default user agreement page built into the UAG.</p>
Type	This field displays the type of the web authentication page used by this profile.
Web Page	This field displays whether this profile uses the default web authentication page built into the UAG (System Default Page) or custom web authentication pages from an external web server (External Page).
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

Add/Edit an Authentication Type Profile

Click the **Add** icon or select an entry in the **Web Authentication > Authentication Type** screen and click the **Edit** icon to display the screen. The screen differs depending on what you select in the **Type** field.

Figure 191 Configuration > Web Authentication: Authentication Type: Add/Edit (Web Portal)

The screenshot shows a configuration window titled "Add Authentication Type" with a close button in the top right corner. The window is divided into sections:

- Web Authentication Type:** Contains two radio buttons: "Web Portal" (selected) and "User Agreement".
- General Settings:**
 - Profile Name:** A text input field with a red dashed border and a red exclamation mark icon to its right, indicating a validation error.
 - Internal Web Portal (User Upload Page):** Selected radio button. Below it is a "Preview" dropdown menu with the text "Please select one ...".
 - Note:** A yellow notepad icon followed by the text: "If you want to configure customize file, please go to Web portal customize file".
 - Customize file:** A dropdown menu with "default_wp.zip" selected.
 - External Web Portal:** Unselected radio button. Below it are five text input fields for "Login URL:", "Logout URL:", "Welcome URL:", "Session URL:", and "Error URL:". Each field has "(Optional)" to its right.
 - Below the URL fields is a link: [Download](#) the external web portal example.

At the bottom right of the window are "OK" and "Cancel" buttons.

Figure 192 Configuration > Web Authentication: Authentication Type: Add/Edit (User Agreement)

The following table describes the labels in this screen.

Table 118 Configuration > Web Authentication: Authentication Type: Add/Edit

LABEL	DESCRIPTION
Type	Select the type of the web authentication page through which users authenticate their connections. If you select User Agreement , by agreeing to the policy of user agreement, users can access the Internet without a guest account.
Profile Name	Enter a name for the profile. You can use up to 31 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). Spaces are not allowed. The first character must be a letter.
The following fields are available if you set Type to Web Portal .	
Internal Web Portal	Select this to use the web portal pages uploaded to the UAG. The login page appears whenever the web portal intercepts network traffic, preventing unauthorized users from gaining access to the network.
Preview	Select to display the page you uploaded to the UAG in a new frame. Note: You must select a custom file uploaded to the UAG before you can preview the pages.
Customize file	Select the file name of the web portal file in the UAG. Note: You can upload zipped custom web portal files to the UAG using the Configuration > Web Authentication > Web Portal Customize File screen.

Table 118 Configuration > Web Authentication: Authentication Type: Add/Edit (continued)

LABEL	DESCRIPTION
External Web Portal	Select this to use a custom login page from an external web portal instead of the one uploaded to the UAG. You can configure the look and feel of the web portal page.
Login URL	Specify the login page's URL; for example, http://IIS server IP Address/login.html. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Logout URL	Specify the logout page's URL; for example, http://IIS server IP Address/logout.html. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Welcome URL	Specify the welcome page's URL; for example, http://IIS server IP Address/welcome.html. Users will be redirected to the welcome page after authentication. This field is optional. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Session URL	Specify the session page's URL; for example, http://IIS server IP Address/session.html. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Error URL	Specify the error page's URL; for example, http://IIS server IP Address/error.html. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Download	Click this to download an example external web portal file for your reference.
The following fields are available if you set Type to User Agreement .	
Enable Idle Detection	This is applicable for access users. Select this check box if you want the UAG to monitor how long each access user is logged in and idle (in other words, there is no traffic for this access user). The UAG automatically logs out the access user once the Idle timeout has been reached.
Idle timeout	This is applicable for access users. This field is effective when Enable Idle Detection is checked. Type the number of minutes each access user can be logged in and idle before the UAG automatically logs out the access user.
Reauthentication Time	Enter the number of minutes the user can be logged into the UAG in one session before having to log in again.
Internal User Agreement	Select this to use the user agreement pages in the UAG. The user agreement page appears whenever the UAG intercepts network traffic, preventing unauthorized users from gaining access to the network.
Preview	Select to display the page you uploaded to the UAG in a new frame. Note: You must select a custom file uploaded to the UAG before you can preview the pages.
Customize file	Select the file name of the user agreement file in the UAG. Note: You can upload zipped custom user agreement files to the UAG using the Configuration > Web Authentication > User Agreement Customize File screen.
External User Agreement	Select this to use custom user agreement pages from an external web server instead of the default one built into the UAG. You can configure the look and feel of the user agreement page.
Agreement URL	Specify the user agreement page's URL; for example, http://IIS server IP Address/logout.html. The Internet Information Server (IIS) is the web server on which the user agreement files are installed.

Table 118 Configuration > Web Authentication: Authentication Type: Add/Edit (continued)

LABEL	DESCRIPTION
Welcome URL	Specify the welcome page's URL; for example, http://IIS server IP Address/welcome.html. The Internet Information Server (IIS) is the web server on which the user agreement files are installed. If you leave this field blank, the UAG will use the welcome page of internal user agreement file.
Download	Click this to download an example external user agreement file for your reference.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

23.2.4 Custom Web Portal / User Agreement File Screen

Use this screen to upload the zipped custom web portal or user agreement files to the UAG. You can also download the custom files to your computer.

Click **Configuration > Web Authentication** and then select the **Custom Web Portal File** or **Custom User Agreement File** tab to display the screen.

Figure 193 Configuration > Web Authentication: Custom Web Portal File

The screenshot displays the 'Custom Web Portal File' configuration interface. At the top, there are tabs for 'Web Authentication', 'Walled Garden', and 'Advertisement'. Below these are sub-tabs for 'General', 'Authentication Type', 'Custom Web Portal File', and 'Custom User Agreement File'. The 'Custom Web Portal File' tab is active.

Internal Web Portal Customize File

Remove Download

#	File Name	Size	Last Modified
1	default_wp.zip	842706	2014-10-21 20:59:00
2	wp1.zip	832893	2014-10-22 03:30:12

Page 1 of 1 Show 50 items Displaying 1 - 2 of 2

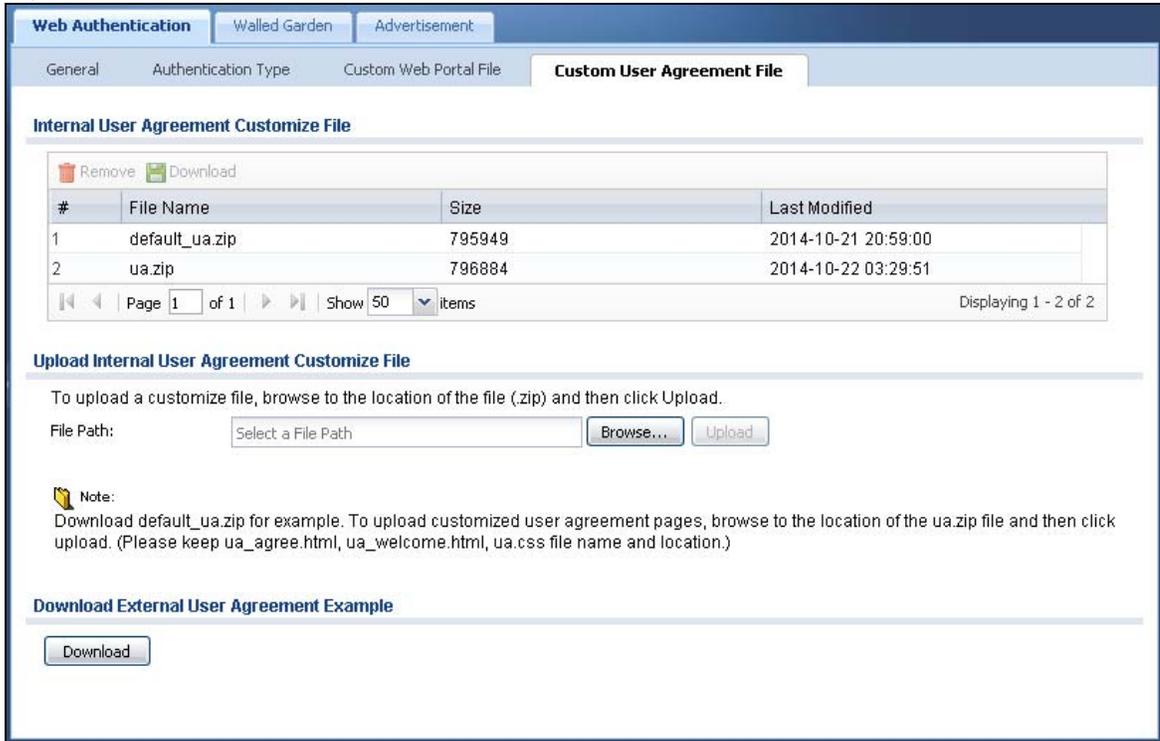
Upload Internal Web Portal Customize File

To upload a customize file, browse to the location of the file (.zip) and then click Upload.

File Path:

Note:
Download default_wp.zip for example. To upload customized web portal pages, browse to the location of the wp.zip file and then click upload. (Please keep welcome.html login.html logout.html session.html error.html file name and location.)

Download External Web Portal Example

Figure 194 Configuration > Web Authentication: Custom User Agreement File

The following table describes the labels in this screen.

Table 119 Configuration > Web Authentication: Custom Web Portal / User Agreement File

LABEL	DESCRIPTION
Remove	Click a file's row to select it and and click Remove to delete it from the UAG.
Download	Click a file's row to select it and and click Download to save the zipped file to your computer.
#	This column displays the index number for each file entry. This field is a sequential value, and it is not associated with a specific entry.
File Name	This column displays the label that identifies a web portal or user agreement file.
Size	This column displays the size (in KB) of a file.
Last Modified	This column displays the date and time that the individual files were last changed or saved.
Browse / Upload	Click Browse... to find the zipped file you want to upload, then click the Upload button to put it on the UAG.
Download	Click this to download an example external web portal or user agreement file for your reference.

23.3 Walled Garden

A user must log in before the UAG allows the user's access to the Internet. However, with a walled garden, you can define one or more web site addresses that all users can access without logging in. These can be used for advertisements for example.

23.3.1 General Screen

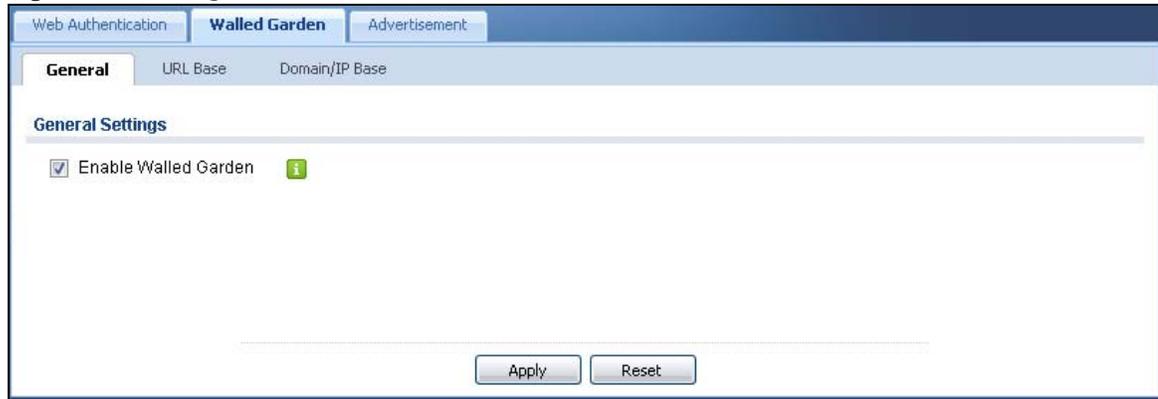
Use this screen to turn on the walled garden feature.

Note: You must enable web authentication before you can access the **Walled Garden** screens.

Note: You can configure up to 20 walled garden web site links.

Click **Configuration > Web Authentication > Walled Garden** to display the screen.

Figure 195 Configuration > Web Authentication > Walled Garden: General



The following table describes the labels in this screen.

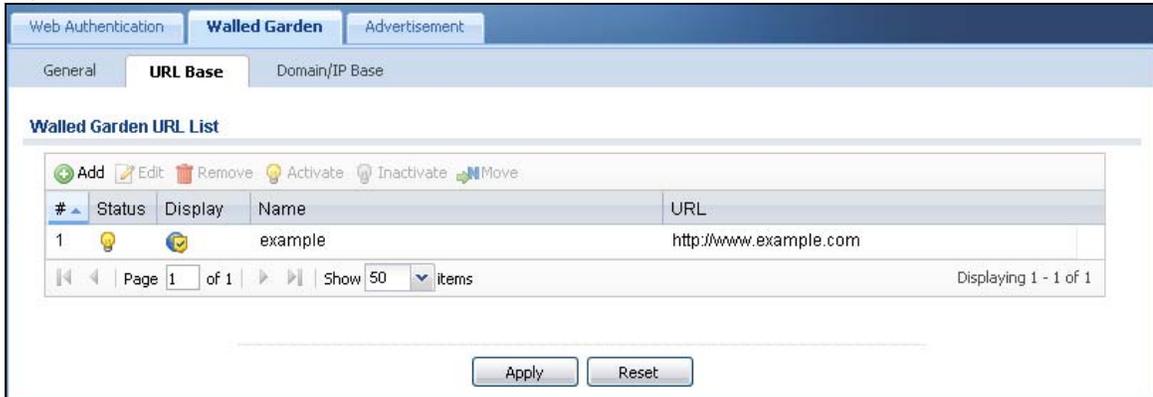
Table 120 Configuration > Web Authentication > Walled Garden: General

LABEL	DESCRIPTION
Enable Walled Garden	Select this to turn on the walled garden feature. Note: This feature works only with the web portal authentication type.
Apply	Click this button to save your changes to the UAG.
Reset	Click this button to return the screen to its last-saved settings.

23.3.2 URL Base Screen

Use this screen to configure the walled garden web addresses (URLs that use the HTTP or HTTPS protocol) for web sites that all users are allowed to access without logging in. The web site link(s) displays in the user login screen by default.

Click **Configuration > Web Authentication > Walled Garden** and then select the **URL Base** tab to display the screen.

Figure 196 Configuration > Web Authentication > Walled Garden: URL Base

The following table describes the labels in this screen.

Table 121 Configuration > Web Authentication > Walled Garden: URL Based

LABEL	DESCRIPTION
Walled Garden URL List	Use this table to manage the list of walled garden web site links.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
Move	To move an entry to a different number in the list, click the Move icon. In the field that appears, specify the number to which you want to move the interface.
#	This field is a sequential value, and it is not associated with any entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Display	This icon is lit when the web site link is set to display in the user login screen.
Name	This field displays the descriptive name of the web site.
URL	This field displays the URL of the web site.
Apply	Click this button to save your changes to the UAG.
Reset	Click this button to return the screen to its last-saved settings.

Adding/Editing a Walled Garden URL

Go to the **Configuration > Web Authentication > Walled Garden > URL Base** screen. Click **Add** or select an entry and click the **Edit** to open the **Add/Edit Walled Garden URL** screen. Use this screen to configure a walled garden web site URL entry.

Figure 197 Configuration > Web Authentication > Walled Garden: URL Base: Add/Edit

The following table describes the labels in this screen.

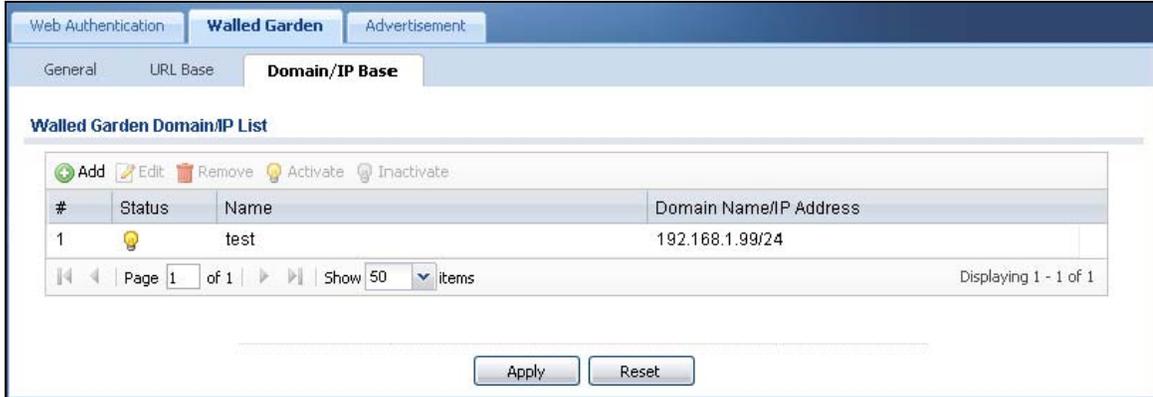
Table 122 Configuration > Web Authentication > Walled Garden: URL Base: Add/Edit

LABEL	DESCRIPTION
Enable	Select this to activate the entry.
Hide in login page	Select this to not display the web site link in the user login screen. This is helpful if a user's access to a specific web site is required to stay connected but he or she doesn't need to visit that web site.
Name	Enter a descriptive name for the walled garden link to be displayed in the login screen. You can use up to 31 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). Spaces are also allowed. The first character must be a letter.
URL	Enter the URL of the web site. Use "http://" or "https://" followed by up to 262 characters (0-9a-zA-Z;/?:@&=+\$\._!~*()*%). For example, http://www.example.com or http://172.16.1.35.
Preview	Click this button to open the specified web site in a new frame.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

23.3.3 Domain/IP Base Screen

Use this screen to configure walled garden web site links, which use a (wildcard) domain name or an IP address. These links will not display in the login page.

Click **Configuration > Web Authentication > Walled Garden** and then select the **Domain/IP Base** tab to display the screen.

Figure 198 Configuration > Web Authentication > Walled Garden: Domain/IP Base

The following table describes the labels in this screen.

Table 123 Configuration > Web Authentication > Walled Garden: Domain/IP Based

LABEL	DESCRIPTION
Walled Garden Domain/IP List	Use this table to manage the list of walled garden web site links.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
#	This field is a sequential value, and it is not associated with any entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the descriptive name of the web site.
Domain Name/IP Address	This field displays the domain name or IP address and subnet mask of the web site.
Apply	Click this button to save your changes to the UAG.
Reset	Click this button to return the screen to its last-saved settings.

Adding/Editing a Walled Garden Domain or IP

Go to the **Configuration > Web Authentication > Walled Garden > Domain/IP Base** screen. Click **Add** or select an entry and click the **Edit** to open the **Add/Edit Walled Garden Domain/IP** screen. Use this screen to configure the domain name or IP address entry for a walled garden web site.

Figure 199 Configuration > Web Authentication > Walled Garden: Domain/IP Base: Add/Edit

The following table describes the labels in this screen.

Table 124 Configuration > Web Authentication > Walled Garden: Domain/IP Base: Add/Edit

LABEL	DESCRIPTION
Enable	Select this to activate the entry.
Name	Enter a descriptive name for the walled garden link. You can use up to 31 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). Spaces are also allowed. The first character must be a letter.
Type	Select whether you want to create the link by entering a domain name or an IP address.
Domain Name / IP Address	If you select Domain , type a Fully-Qualified Domain Name (FQDN) of a web site. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain. Underscores are not allowed. Use "*" as a prefix in the FQDN for a wildcard domain name (for example, *.example.com). If you select IP , enter the IP address and subnet mask of the web site.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

23.3.4 Walled Garden Login Example

The following figure shows the user login screen with two walled garden links. The links are named **WalledGardenLink1** through **2** for demonstration purposes.

Figure 200 Walled Garden Login Example

WalledGardenLink2
WalledGardenLink1

Enter User Name/Password and click to login.

User Name:

Password:

(max. 63 alphanumeric, printable characters and no spaces)

Login Reset

Note:

1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
4. Allow Gears if you are using Google Chrome.

23.4 Advertisement Screen

Use this screen to set the UAG to display an advertisement web page as the first web page whenever the user connects to the Internet.

Click **Configuration > Web Authentication > Advertisement** to display the screen.

Figure 201 Configuration > Web Authentication > Advertisement

Web Authentication Walled Garden **Advertisement**

General Settings

Enable Advertisement

Advertisement Summary

+ Add Edit Remove

#	Name	URL
1	example	http://www.zyxel.com

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

Apply Reset

The following table gives an overview of the objects you can configure.

Table 125 Configuration > Web Authentication > Advertisement

LABEL	DESCRIPTION
Enable Advertisement	Select this to turn on the advertisement feature. Note: This feature works only when you enable web authentication.
Advertisement Summary	Use this table to manage the list of advertisement web pages.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with any entry.
Name	This field displays the descriptive name of web site.
URL	This field displays the address of web site.
Apply	Click this button to save your changes to the UAG.
Reset	Click this button to return the screen to its last-saved settings.

23.4.1 Adding/Editing an Advertisement URL

Click **Configuration > Web Authentication > Advertisement** and then the **Add** (or **Edit**) icon in the **Advertisement Summary** section to open the **Add/Edit Advertisement URL** screen. Use this screen to configure an advertisement address entry.

Note: You can create up to 20 advertisement URL entries. The UAG randomly picks one and open the specified web site in a new frame when an authenticated user is attempts to access the Internet.

Figure 202 Configuration > Web Authentication > Advertisement > Add/Edit

The following table gives an overview of the objects you can configure.

Table 126 Configuration > Web Authentication > Advertisement > Add/Edit

LABEL	DESCRIPTION
Name	Enter a descriptive name for the advertisement web site. You can use up to 31 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). Spaces are not allowed. The first character must be a letter.
URL	Enter the URL or IP address of the web site. Use "http://" followed by up to 262 characters (0-9a-zA-Z;/?:@&=+\$\._!~*'(%)%). For example, http://www.example.com or http://172.16.1.35.
Preview	Click this button to open the specified web site in a new frame.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

24.1 Overview

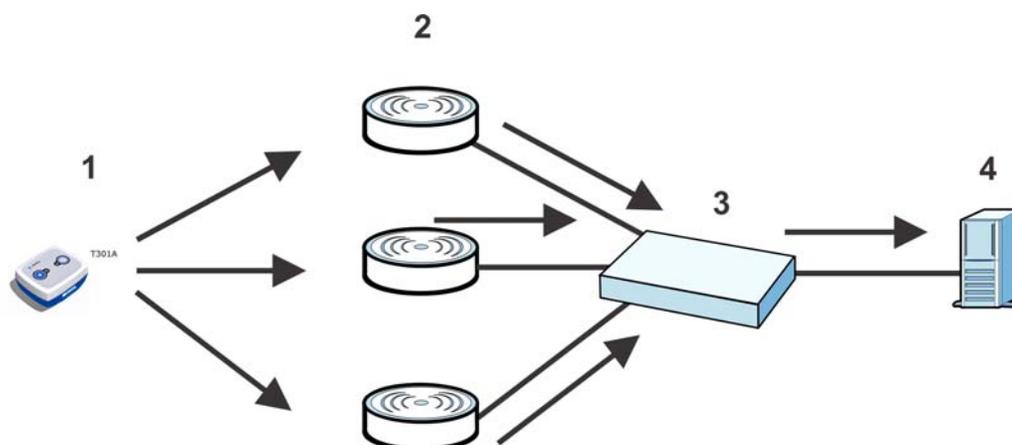
Ekahau RTLS (Real Time Location Service) tracks battery-powered Wi-Fi tags attached to APs managed by the UAG to create maps, alerts, and reports.

The Ekahau RTLS Controller is the centerpiece of the RTLS system. This server software runs on a Windows computer to track and locate Ekahau tags from Wi-Fi signal strength measurements. Use the UAG with the Ekahau RTLS system to take signal strength measurements at the APs (Integrated Approach / Blink Mode).

The following example shows the Ekahau RTLS Integrated Approach (Blink Mode).

- 1 The Wi-Fi tag sends blink packets at specified intervals (or triggered by something like motion or button presses).
- 2 The APs pick up the blink packets, measure the signal strength, and send it to the UAG.
- 3 The UAG forwards the signal measurements to the Ekahau RTLS Controller.
- 4 The Ekahau RTLS Controller calculates the tag positions.

Figure 203 RTLS Example



24.1.1 What You Can Do in this Chapter

Use the **RTLS** screen ([Section 24.3 on page 287](#)) to use the managed APs as part of an Ekahau RTLS to track the location of Ekahau Wi-Fi tags.

24.2 Before You Begin

You need:

- At least three APs managed by the UAG (the more APs the better since it increases the amount of information the Ekahau RTLS Controller has for calculating the location of the tags)
- IP addresses for the Ekahau Wi-Fi tags
- A dedicated RTLS SSID is recommended
- Ekahau RTLS Controller in blink mode with TZSP Updater enabled
- Security policies to allow RTLS traffic if the UAG security policy control is enabled or the Ekahau RTLS Controller is behind a firewall.

For example, if the Ekahau RTLS Controller is behind a firewall, open ports 8550, 8553, and 8569 to allow traffic the APs send to reach the Ekahau RTLS Controller.

The following table lists default port numbers and types of packets RTLS uses.

Table 127 RTLS Traffic Port Numbers

PORT NUMBER	TYPE	DESCRIPTION
8548	TCP	Ekahau T201 location update.
8549	UDP	Ekahau T201 location update.
8550	TCP	Ekahau T201 tag maintenance protocol and Ekahau RTLS Controller user interface.
8552	UDP	Ekahau Location Protocol
8553	UDP	Ekahau Maintenance Protocol
8554	UDP	Ekahau T301 firmware update.
8560	TCP	Ekahau Vision web interface
8562	UDP	Ekahau T301W firmware update.
8569	UDP	Ekahau TZSP Listener Port

24.3 Configuring RTLS

Click **Configuration > RTLS** to open this screen. Use this screen to turn RTLS (Real Time Location System) on or off and specify the IP address and server port of the Ekahau RTLS Controller.

Figure 204 Configuration > RTLS

The following table describes the labels in this screen.

Table 128 Configuration > RTLS

LABEL	DESCRIPTION
Enable	Select this to use Wi-Fi to track the location of Ekahau Wi-Fi tags.
IP Address	Specify the IP address of the Ekahau RTLS Controller.
Server Port	Specify the server port number of the Ekahau RTLS Controller.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

Security Policy

25.1 Overview

A security policy is a template of security settings that can be applied to specific traffic at specific times. The policy can be applied:

- to a specific direction of travel of packets (from / to)
- to a specific source and destination address objects
- to a specific type of traffic (services)
- to a specific user or group of users
- at a specific schedule

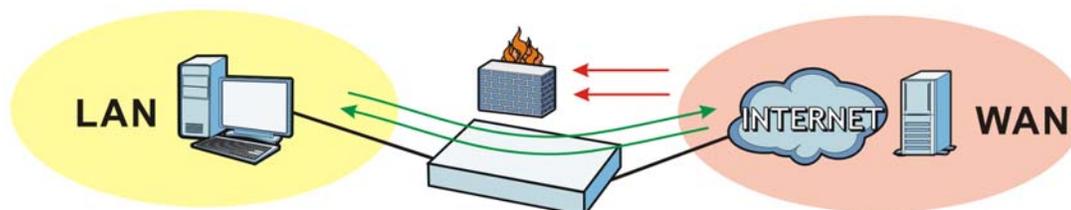
The policy can be configured:

- to allow or deny traffic that matches the criteria above
- send a log or alert for traffic that matches the criteria above
- to apply the actions configured in the UTM profiles (application patrol, content filter) to traffic that matches the criteria above

The security policies can also limit the number of user sessions.

The following example shows the UAG's default security policy behavior for WAN to LAN traffic and how stateful inspection works. A LAN user can initiate a Telnet session from within the LAN zone and the UAG allows the response. However, the UAG blocks Telnet traffic initiated from the WAN zone and destined for the LAN zone.

Figure 205 Default Security Policy Action



25.1.1 What You Can Do in this Chapter

- Use the **Security Policy Control** screens ([Section 25.2 on page 291](#)) to enable or disable policy control and asymmetrical routes, and manage and configure policies.
- Use the **Session Control** screens (see [Section 25.3 on page 296](#)) to limit the number of concurrent NAT/security policies sessions a client can use.

25.1.2 What You Need to Know

Stateful Inspection

The UAG uses stateful inspection in its security policies. The UAG restricts access by screening data packets against defined access rules. It also inspects sessions. For example, traffic from one zone is not allowed unless it is initiated by a computer in another zone first.

Zones

A zone is a group of interfaces. Group the UAG's interfaces into different zones based on your needs. You can configure security policies for data passing between zones or even between interfaces.

Default Security Policy Behavior

Security policies are grouped based on the direction of travel of packets to which they apply. Here is the default security policy behavior for traffic going through the UAG in various directions.

Note: Intra-zone traffic (such as LAN to LAN traffic or WAN to WAN traffic) can also be blocked by the zone configuration. See [Section 34.2.1 on page 397](#) for details.

Table 129 Default Security Policy Behavior

FROM ZONE TO ZONE	BEHAVIOR
From any to Device	DHCP traffic from any interface to the UAG is allowed.
From LAN1 to any (other than the UAG)	Traffic from the LAN1 to any of the networks connected to the UAG is allowed.
From LAN2 to any (other than the UAG)	Traffic from the LAN2 to any of the networks connected to the UAG is allowed.
From LAN1 to Device	Traffic from the LAN1 to the UAG itself is allowed.
From LAN2 to Device	Traffic from the LAN2 to the UAG itself is allowed.
From WAN to Device	The default services listed in To-Device Rules on page 290 are allowed from the WAN to the UAG itself. All other WAN to UAG traffic is dropped.
From any to any	Traffic that does not match any security policy is dropped. This includes traffic from the WAN to any of the networks behind the UAG. This also includes traffic to or from interfaces that are not assigned to a zone (extra-zone traffic).

To-Device Rules

Rules with **Device** as the **To Zone** apply to traffic going to the UAG itself. By default:

- The security policy allows only LAN, or WAN computers to access or manage the UAG.
- The UAG allows DHCP traffic from any interface to the UAG.
- The UAG drops most packets from the WAN zone to the UAG itself and generates a log except for AH, ESP, GRE, HTTPS, IKE, NATT.

When you configure a security policy for packets destined for the UAG itself, make sure it does not conflict with your service control rule. See [Chapter 46 on page 486](#) for more information about

service control (remote management). The UAG checks the security policies before the service control rules for traffic destined for the UAG.

A **From Any To Device** direction rule applies to traffic from an interface which is not in a zone.

Global Security Policies

Security policies with **from any** and/or **to any** as the packet direction are called global security policies. The global security policies are the only security policies that apply to an interface that is not included in a zone. The **from any** rules apply to traffic coming from the interface and the **to any** rules apply to traffic going to the interface.

Security Policy Rule Criteria

The UAG checks the schedule, user name (user's login name on the UAG), source IP address, destination IP address and IP protocol type of network traffic against the policy control rules (in the order you list them). When the traffic matches a rule, the UAG takes the action specified in the rule.

User Specific Security Policies

You can specify users or user groups in security policies. For example, to allow a specific user from any computer to access a zone by logging in to the UAG, you can set up a policy based on the user name only. If you also apply a schedule to the security policy, the user can only access the network at the scheduled time. A user-aware security policy is activated whenever the user logs in to the UAG and will be disabled after the user logs out of the UAG.

Session Limits

Accessing the UAG or network resources through the UAG requires a NAT session and corresponding security policy session. Peer to peer applications, such as file sharing applications, may use a large number of NAT sessions. A single client could use all of the available NAT sessions and prevent others from connecting to or through the UAG. The UAG lets you limit the number of concurrent NAT/security policy sessions a client can use.

Finding Out More

- See [Section 25.4 on page 299](#) for an example of creating security policies as part of configuring user-aware access control.

25.2 Security Policy Control Screen

Asymmetrical Routes

If an alternate gateway on the LAN has an IP address in the same subnet as the UAG's LAN IP address, return traffic may not go through the UAG. This is called an asymmetrical or "triangle" route. This causes the UAG to reset the connection, as the connection has not been acknowledged.

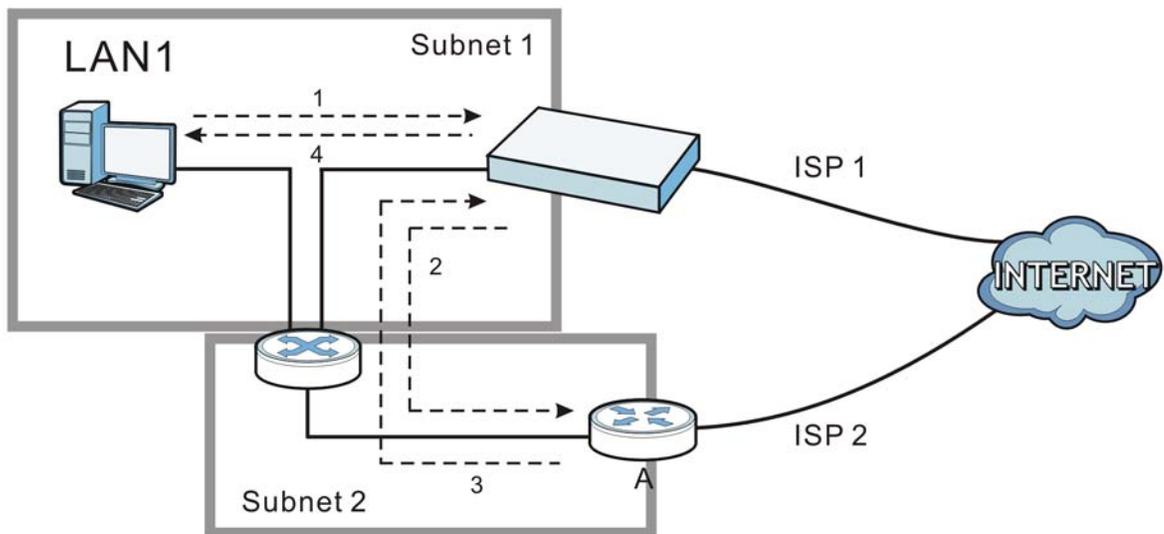
You can have the UAG permit the use of asymmetrical route topology on the network (not reset the connection). However, allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the UAG. A better solution is to use virtual interfaces to put the UAG

and the backup gateway on separate subnets. Virtual interfaces allow you to partition your network into logical sections over the same interface. See the chapter about interfaces for more information.

By putting LAN 1 and the alternate gateway (**A** in the figure) in different subnets, all returning network traffic must pass through the UAG to the LAN. The following steps and figure describe such a scenario.

- 1 A computer on the LAN1 initiates a connection by sending a SYN packet to a receiving server on the WAN.
- 2 The UAG reroutes the packet to gateway **A**, which is in **Subnet 2**.
- 3 The reply from the WAN goes to the UAG.
- 4 The UAG then sends it to the computer on the LAN1 in **Subnet 1**.

Figure 206 Using Virtual Interfaces to Avoid Asymmetrical Routes

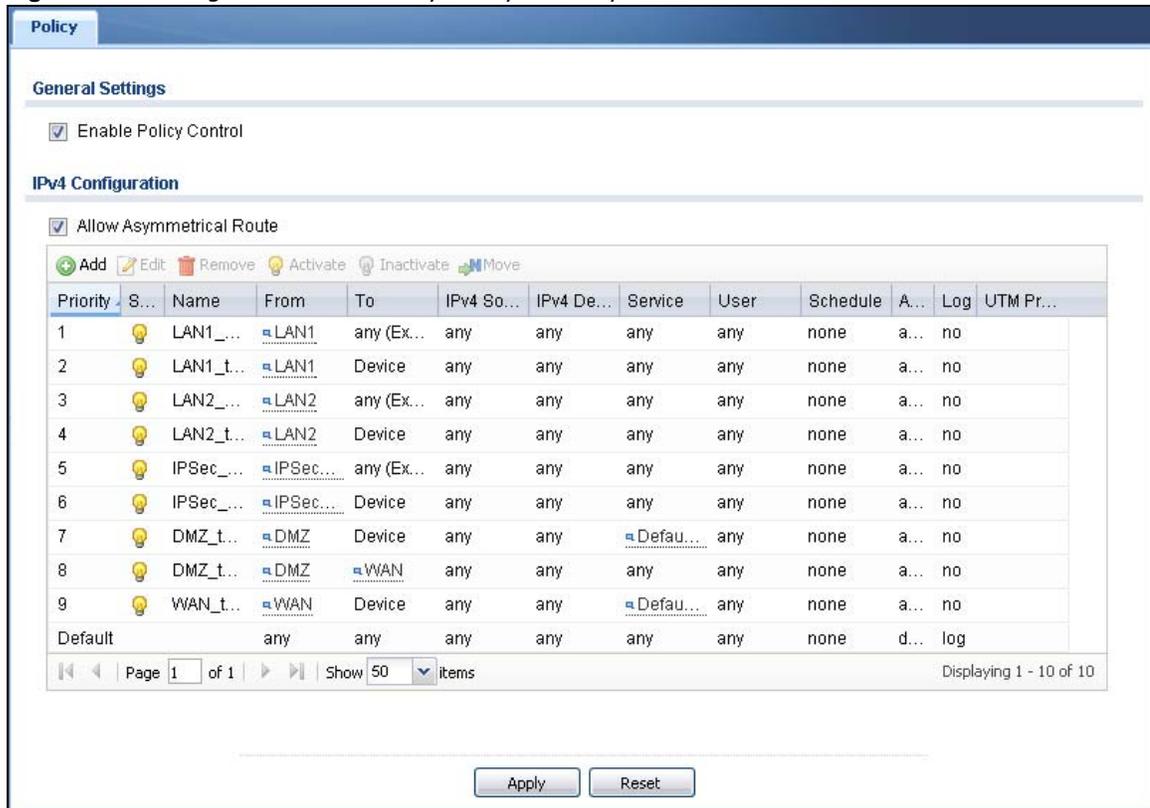


25.2.1 Configuring the Security Policy Control Screen

Click **Configuration > Security Policy > Policy Control** to open the **Policy** screen. Use this screen to enable or disable policy control and asymmetrical routes, set a maximum number of sessions per host, and display the configured policy control rules. Specify from which zone packets come and to which zone packets travel to display only the rules specific to the selected direction. Note the following.

- Besides configuring policy control, you also need to configure NAT rules to allow computers on the WAN to access LAN devices. See [Chapter 14 on page 219](#) for more information.
- The UAG applies NAT (Destination NAT) settings before applying the policy control rules. So for example, if you configure a NAT entry that sends WAN traffic to a LAN IP address, when you configure a corresponding policy control rule to allow the traffic, you need to set the LAN IP address as the destination.
- The ordering of your rules is very important as rules are applied in sequence.

Figure 207 Configuration > Security Policy > Policy Control



The following table describes the labels in this screen.

Table 130 Configuration > Security Policy > Policy Control

LABEL	DESCRIPTION
General Settings	
Enable Policy Control	Select this check box to activate security policy control. The UAG performs access control when this is activated.
IPv4 Configuration	
Allow Asymmetrical Route	<p>If an alternate gateway on the LAN has an IP address in the same subnet as the UAG’s LAN IP address, return traffic may not go through the UAG. This is called an asymmetrical or “triangle” route. This causes the UAG to reset the connection, as the connection has not been acknowledged.</p> <p>Select this check box to have the UAG permit the use of asymmetrical route topology on the network (not reset the connection).</p> <p>Note: Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the UAG. A better solution is to use virtual interfaces to put the UAG and the backup gateway on separate subnets.</p>
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry’s settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate .

Table 130 Configuration > Security Policy > Policy Control (continued)

LABEL	DESCRIPTION
Inactivate	To turn off an entry, select it and click Inactivate .
Move	To change a rule's position in the numbered list, select the rule and click Move to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
The following read-only fields summarize the policies you have created that apply to traffic traveling in the selected packet direction.	
Priority	This is the position of your security policy in the global policy list (including all through-UAG and to-UAG policies). The ordering of your policies is important as policies are applied in sequence. Default displays for the default security policy behavior that the UAG performs on traffic that does not match any other security policy.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This is the name of the security policy.
From To	This is the direction of travel of packets to which the security policy applies. Policy control rules are grouped based on the direction of travel of packets to which they apply. For example, from LAN to LAN means packets traveling from a computer or subnet on the LAN to either another computer or subnet on the LAN. From any displays all the policy control rules for traffic going to the selected To Zone . To any displays all the policy control rules for traffic coming from the selected From Zone . From any to any displays all of the policy control rules. To Device rules are for traffic that is destined for the UAG and control which computers can manage the UAG.
IPv4 Source	This displays the IPv4 source address object to which this security policy applies.
IPv4 Destination	This displays the IPv4 destination address object to which this security policy applies.
Service	This displays the service object to which this security policy applies.
User	This is the user name or user group name to which this security policy applies.
Schedule	This field tells you the schedule object that the policy uses. none means the policy is active at all times if enabled.
Action	This field displays whether security policy silently discards packets (deny), or permits the passage of packets (allow).
Log	This field shows you whether a log (and alert) is created when packets match this policy or not.
UTM Profile	This field shows which UTM profiles (application patrol, content filter) apply to this policy.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

25.2.2 Add/Edit Policy Control Rule

In the **Policy Control** screen, click the **Add** icon or select a rule and click **Edit** to display this screen.

Figure 208 Configuration > Security Policy > Policy Control > Add

The following table describes the labels in this screen.

Table 131 Configuration > Security Policy > Policy Control > Add/Edit

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable	Select this check box to activate the security policy.
Name	Type a name to identify the policy. You can use up to 31 alphanumeric characters (A-Z, a-z, 0-9), hyphens (-) and underscores (_). Spaces are not allowed. The first character must be a letter.
Description	Enter a descriptive name of up to 60 printable ASCII characters for the security policy. Spaces are allowed.
From To	For through-UAG rules, select the direction of travel of packets to which the policy applies. any means all interfaces. Device means packets destined for the UAG itself.
Source	Select an IPv4 address or address group to apply an IPv4 rule to traffic coming from it. Select any to apply an IPv4 rule to all traffic coming from IPv4 addresses.
Destination	Select an IPv4 address or address group to apply an IPv4 rule to traffic going to it. Select any to apply an IPv4 rule to all traffic going to IPv4 addresses.
Service	Select a service or service group from the drop-down list box.

Table 131 Configuration > Security Policy > Policy Control > Add/Edit (continued)

LABEL	DESCRIPTION
User	<p>This field is not available when you are configuring a to-UAG policy.</p> <p>Select a user name or user group to which to apply the policy. The security policy is activated only when the specified user logs into the system and the policy will be disabled when the user logs out.</p> <p>Otherwise, select any and there is no need for user logging.</p> <p>Note: If you specified a source IP address (group) instead of any in the field below, the user's IP address should be within the IP address range.</p>
Schedule	Select a schedule that defines when the policy applies. Otherwise, select none and the policy is always effective.
Action	<p>Use the drop-down list box to select what the security policy is to do with packets that match this rule.</p> <p>Select deny to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.</p> <p>Select allow to permit the passage of the packets.</p>
Log matched traffic	Select whether to have the UAG generate a log (log), log and alert (log alert) or not (no) when the policy is matched. See Chapter 47 on page 534 for more on logs.
UTM Profile	<p>Use this section to apply UTM profiles (created in the Configuration > UTM Profile screens) to traffic that matches the criteria above. You must have created a profile first; otherwise none displays.</p> <p>Select by profile to decide whether a log will be generated based on the UTM profile's settings. Otherwise, select no to not generate a log for all traffic that matches criteria in the profile.</p>
Application Patrol	Select an Application Patrol profile from the list box; none displays if no profiles have been created in the Configuration > UTM Profile > App Patrol screen.
Content Filter	Select a Content Filter profile from the list box; none displays if no profiles have been created in the Configuration > UTM Profile > Content Filter screen.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

25.3 Session Control Screen

Click **Configuration > Security Policy > Session Control** to display the **Security Policy Session Control** screen. Use this screen to limit the number of concurrent NAT/security policy sessions a client can use. You can apply a default limit for all users and individual limits for specific users, addresses, or both. The individual limit takes priority if you apply both.

Figure 209 Configuration > Security Policy > Session Control

Session Control

General Settings

UDP Session Time Out: (1-300 seconds)

Session Limit Settings

Enable Session Limit

IPv4 Configuration

Default Session per Host: (0-8192, 0 is unlimited)

Status	#	User	IPv4 Address	Description	Limit
No data to display					

The following table describes the labels in this screen.

Table 132 Configuration > Security Policy > Session Control

LABEL	DESCRIPTION
General Settings	
UDP Session Time Out	Set how many seconds (from 1 to 300) the UAG will allow a UDP session to remain idle (without UDP traffic) before closing it.
Session Limit Settings	
Enable Session limit	Select this check box to control the number of concurrent sessions hosts can have.
IPv4 Configuration	This table lists the rules for limiting the number of concurrent sessions hosts can have.
Default Session per Host	<p>This field is configurable only when you enable session limit.</p> <p>Use this field to set a common limit to the number of concurrent NAT/security policy sessions each client computer can have.</p> <p>If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions.</p> <p>Create rules below to apply other limits for specific users or addresses.</p>
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .

Table 132 Configuration > Security Policy > Session Control (continued)

LABEL	DESCRIPTION
Move	To change a rule's position in the numbered list, select the rule and click Move to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
#	This is the index number of a session limit rule. It is not associated with a specific rule.
User	This is the user name or user group name to which this session limit rule applies.
IPv4 Address	This is the IPv4 address object to which this session limit rule applies.
Description	This is the information configured to help you identify the rule.
Limit	This is how many concurrent sessions this user or address is allowed to have.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

25.3.1 Add/Edit a Session Limit Rule

In the **Configuration > Security Policy > Session Control** screen, click the **Add** icon or select an entry and click the **Edit** icon to display the **Add/Edit Session Limit** screen. Use this screen to configure rules that define a session limit for specific users or addresses.

Figure 210 Configuration > Security Policy > Session Control > Add/Edit

The following table describes the labels in this screen.

Table 133 Configuration > Security Policy > Session Control > Add/Edit

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable Rule	Select this check box to turn on this session limit rule.
Description	Enter information to help you identify this rule. Use up to 60 printable ASCII characters. Spaces are allowed.

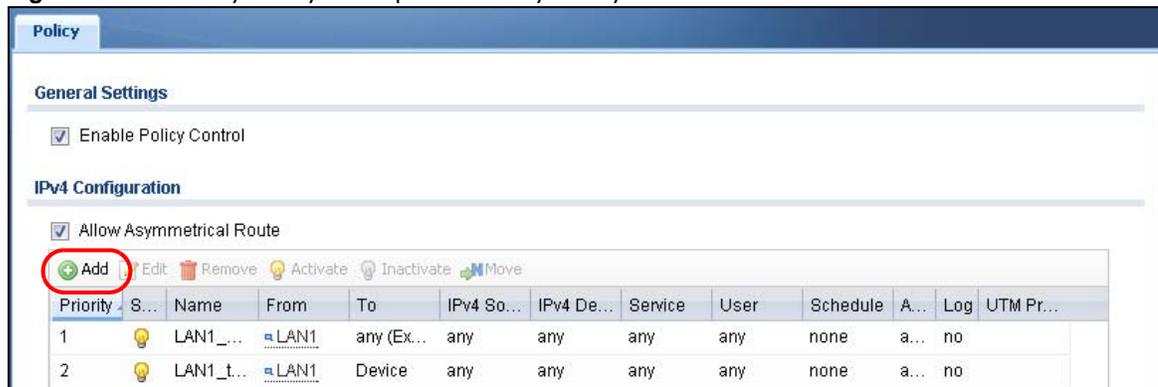
Table 133 Configuration > Security Policy > Session Control > Add/Edit (continued)

LABEL	DESCRIPTION
User	Select a user name or user group to which to apply the rule. The rule is activated only when the specified user logs into the system and the rule will be disabled when the user logs out. Otherwise, select any and there is no need for user logging. Note: If you specified an IP address (or address group) instead of any in the field below, the user's IP address should be within the IP address range.
Address	Select the IPv4 source address or address group to which this rule applies. Select any to apply the rule to all IPv4 source addresses.
Session Limit per Host	Use this field to set a limit to the number of concurrent NAT/security policy sessions this rule's users or addresses can have. For this rule's users and addresses, this setting overrides the Default Session per Host setting in the general Security Policy > Session Control screen.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

25.4 Security Policy Configuration Example

The following Internet security policy example allows Doom players from the WAN to IP addresses 172.16.1.10 through 172.16.1.15 (Dest_1) on the LAN.

- 1 Click **Configuration > Security Policy > Policy Control**. In the summary of security policies click **Add** to configure a new first entry. The sequence (priority) of the policies is important since they are applied in order.

Figure 211 Security Policy Example: Security Policy Control Screen

- 2 At the top of the screen, click **Create new Object > Address** to configure an address object. Configure it as follows and click **OK**.

Figure 212 Security Policy Example: Create an Address Object

The 'Create Address' dialog box contains the following fields:

- Name: Dest_1
- Address Type: RANGE
- Starting IP Address: 172.16.1.10
- End IP Address: 172.16.1.15

Buttons: OK, Cancel

- 3 Click **Create new Object > Service** to configure a service object for Doom (UDP port 666). Configure it as follows and click **OK**.

Figure 213 Security Policy Example: Create a Service Object

The 'Create Service Object' dialog box contains the following fields:

- Name: Doom
- IP Protocol: UDP
- Starting Port: 666 (1..65535)
- Ending Port: 666 (1..65535)

Buttons: OK, Cancel

- 4 Select **From WAN** and **To LAN** and enter a name for the security policy. Select **Dest_1** for the **Destination** and **Doom** as the **Service**. Enter a name and configure the rest of the screen as follows. Click **OK** when you are done.

Figure 214 Security Policy Example: Edit a Security Policy

The 'Add corresponding' dialog box contains the following fields:

- Enable
- Name: Doom-example
- Description: (Optional)
- From: WAN
- To: LAN1
- Source: any
- Destination: Dest_1
- Service: Doom
- User: any
- Schedule: none
- Action: allow
- Log matched traffic: no

UTM Profile

- Application Patrol: none
- Content Filter: none
- Log: by profile
- Log: by profile

Buttons: OK, Cancel

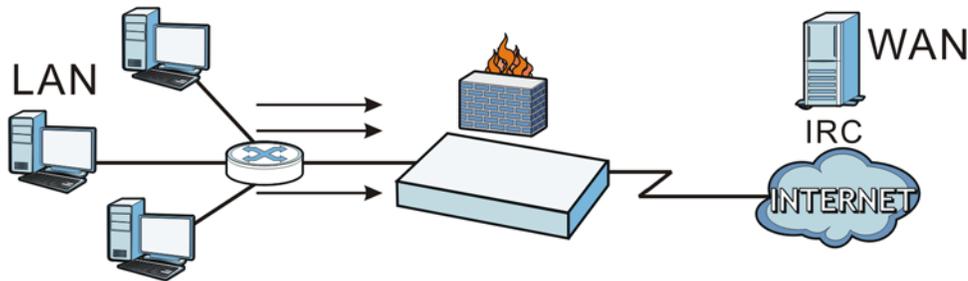
- 5 The security policy appears in the Security Policy summary.

Figure 215 Security Policy Example: Doom Rule in Summary

Prior...	Name	From	To	IPv4 So...	IPv4 De...	Service	User	Schedule	UTM Pr...
1	Doom-e...	WAN	LAN1	any	Dest_1	Doom	any	none	...	no	
2	LAN1_O...	LAN1	any (Ex...	any	any	any	any	none	...	no	
3	LAN1_to...	LAN1	Device	any	any	any	any	none	...	no	
4	LAN2_O...	LAN2	any (Ex...	any	any	any	any	none	...	no	
5	LAN2_to...	LAN2	Device	any	any	any	any	none	...	no	

25.5 Security Policy Example Applications

Suppose you decide to block LAN users from using IRC (Internet Relay Chat) through the Internet. To do this, you would configure a LAN to WAN security policy that blocks IRC traffic from any source IP address from going to any destination address. You do not need to specify a schedule since you need the security policy to always be in effect. The following figure shows the results of this rule.

Figure 216 Blocking All LAN to WAN IRC Traffic Example

Your security policy would have the following settings.

Table 134 Blocking All LAN to WAN IRC Traffic Example

#	USER	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	Any	Any	Any	Any	IRC	Deny
2	Any	Any	Any	Any	Any	Allow

- The first row blocks LAN access to the IRC service on the WAN.
- The second row is the security policy's default policy that allows all LAN1 to WAN traffic.

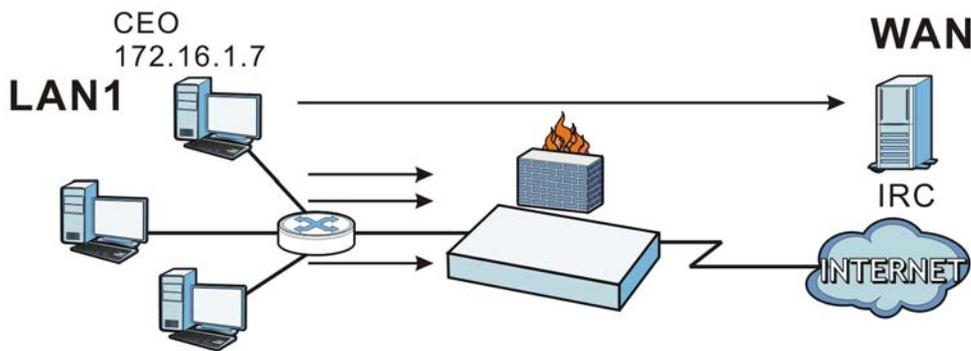
The UAG applies the security policies in order. So for this example, when the UAG receives traffic from the LAN, it checks it against the first rule. If the traffic matches (if it is IRC traffic) the security policy takes the action in the rule (drop) and stops checking the subsequent security policies. Any traffic that does not match the first security policy will match the second policy and the UAG forwards it.

Now suppose you need to let the CEO use IRC. You configure a LAN1 to WAN security policy that allows IRC traffic from the IP address of the CEO's computer. You can also configure a LAN to WAN policy that allows IRC traffic from any computer through which the CEO logs into the UAG with his/her user name. In order to make sure that the CEO's computer always uses the same IP address, make sure it either:

- Has a static IP address,
- or
- You configure a static DHCP entry for it so the UAG always assigns it the same IP address (see [DHCP Settings on page 192](#) for information on DHCP).

Now you configure a LAN1 to WAN security policy that allows IRC traffic from the IP address of the CEO's computer (172.16.1.7 for example) to go to any destination address. You do not need to specify a schedule since you want the security policy to always be in effect. The following figure shows the results of your two custom rules.

Figure 217 Limited LAN to WAN IRC Traffic Example



Your security policy would have the following configuration.

Table 135 Limited LAN1 to WAN IRC Traffic Example 1

#	USER	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	Any	172.16.1.7	Any	Any	IRC	Allow
2	Any	Any	Any	Any	IRC	Deny
3	Any	Any	Any	Any	Any	Allow

- The first row allows the LAN1 computer at IP address 172.16.1.7 to access the IRC service on the WAN.
- The second row blocks LAN1 access to the IRC service on the WAN.
- The third row is the security policy's default policy of allowing all traffic from the LAN1 to go to the WAN.

Alternatively, you configure a LAN1 to WAN security policy with the CEO's user name (say CEO) to allow IRC traffic from any source IP address to go to any destination address.

Your security policy would have the following configuration.

Table 136 Limited LAN1 to WAN IRC Traffic Example 2

#	USER	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	CEO	Any	Any	Any	IRC	Allow
2	Any	Any	Any	Any	IRC	Deny
3	Any	Any	Any	Any	Any	Allow

- The first row allows any LAN1 computer to access the IRC service on the WAN by logging into the UAG with the CEO's user name.
- The second row blocks LAN1 access to the IRC service on the WAN.
- The third row is the security policy's default policy of allowing all traffic from the LAN1 to go to the WAN.

The policy for the CEO must come before the policy that blocks all LAN1 to WAN IRC traffic. If the policy that blocks all LAN1 to WAN IRC traffic came first, the CEO's IRC traffic would match that policy and the UAG would drop it and not check any other security policies.

26.1 Overview

You can use the built-in billing function to setup billing profiles. A billing profile describes how to charge users. This chapter also shows you how to select an accounting method, configure a discount price plan or use an online payment service by credit card.

26.1.1 What You Can Do in this Chapter

- Use the **General** screen (see [Section 26.2 on page 305](#)) to configure the general billing settings, such as the accounting method, currency unit and the SSID profiles to which the settings are applied.
- Use the **Billing Profile** screen (see [Section 26.3 on page 307](#)) to configure the billing profiles for the web-based account generator and each button on the connected statement printer.
- Use the **Discount** screen (see [Section 26.4 on page 314](#)) to enable and configure discount price plans.
- Use the **Payment Service** screen (see [Section 26.5 on page 316](#)) to enable online payment service and configure the service pages.

26.1.2 What You Need to Know

Accumulation Accounting Method

The accumulation accounting method allows multiple re-logins until the allocated time period or until the user account is expired. The UAG accounts the time that the user is logged in for Internet access.

Time-to-finish Accounting Method

The time-to-finish accounting method is good for one-time logins. Once a user logs in, the UAG stores the IP address of the user's computer for the duration of the time allocated. Thus the user does not have to enter the user name and password again for re-login within the allocated time. Once activated, the user account is valid until the allocated time is reached even if the user disconnects Internet access for a certain period within the allocated time. For example, Joe purchases a one-hour time-to-finish account. He starts using the Internet for the first 20 minutes and then disconnects his Internet access to go to a 20-minute meeting. After the meeting, he only has 20 minutes left on his account.

26.2 The General Screen

Use this screen to configure the general billing settings, such as the accounting method, currency unit and the SSID profiles to which the settings are applied. Click **Configuration > Billing > General** to open the following screen.

Figure 218 Configuration > Billing > General

The screenshot shows the 'Configuration > Billing > General' screen. It has a navigation bar with tabs: General, Billing Profile, Discount, and Payment Service. The 'General' tab is active. The screen is organized into sections:

- General Settings:**
 - Unused account will be deleted after the time: 24 hour
 - Accounting Method:
 - Time to Finish
 - Accumulation
 - User idle timeout: 3 (1-60 minutes)
 - Accumulation account will be deleted after the time: 90 day
- Billing User Logon Settings:**
 - Maximum number per billing account: 1 (1-10)
 - Reach maximum number per billing account:
 - Block
 - Remove previous user and login
 - Username & Password length: 6
 - Keep user logged in
- Currency:**
 - Currency symbol: €
 - Currency code: User-Define
 - Number of decimals places: 2
 - Decimal symbol: comma
 - Tax: 0 %
- SSID Profile Settings:**
 - Selectable SSID Profiles: (empty)
 - Selected SSID Profiles:
 - === Object ===
 - default

At the bottom, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 137 Configuration > Billing > General

LABEL	DESCRIPTION
General Settings	
Unused account will be deleted after the time:	Enter the number and select a time unit from the drop-down list box to specify how long to wait before the UAG deletes an account that has not been used.

Table 137 Configuration > Billing > General (continued)

LABEL	DESCRIPTION
Accounting Method	<p>Select Time to Finish to allow each user a one-time login. Once the user logs in, the system starts counting down the pre-defined usage even if the user stops the Internet access before the time period is finished. If a user disconnects and reconnects before the allocated time expires, the user does not have to enter the user name and password to access the Internet again.</p> <p>Select Accumulation to allow each user multiple re-login until the time allocated is used up. The UAG accounts the time that the user is logged in for Internet access.</p>
User idle timeout	<p>The UAG automatically disconnects a computer from the network after a period of inactivity. The user may need to enter the username and password again before access to the network is allowed.</p> <p>If you select Accumulation, specify the idle timeout between 1 and 60 minutes.</p>
Accumulation account will be deleted after the time:	<p>Enter the number and select a time unit from the drop-down list box to specify how long to wait before the UAG deletes an idle account.</p> <p>This is for use with accumulation accounting.</p>
Billing User Logon Settings	
Maximum number per billing account	Enter the maximum number of the users that are allowed to log in with the same account.
Reach maximum number per billing account	<p>Select Block to stop new users from logging in when the Maximum number per billing account is reached.</p> <p>Select Remove previous user and login to disassociate the first user that logged in and allow new user to log in when the Maximum number per billing account is reached.</p>
Username & Password length	Select to specify how many characters the username and password of a newly-created dynamic guest account will have after you click Apply .
Keep user logged in	<p>Select to let the users automatically log in without entering their user name and password if the UAG restarts.</p> <p>Note: This works only for free guest accounts or when the accounting method is Time to Finish.</p>
Currency	<p>Select the appropriate currency symbol or currency unit.</p> <p>If you set Currency code to User-Define, enter a three-letter alphabetic code manually.</p>
Number of decimals places	This shows the number of decimal places to be used for billing.
Decimal symbol	Select whether you would like to use a dot (.) or a comma (,) for the decimal point.
Tax	Select this option to charge sales tax for the account. Enter the tax rate (a 6% sales tax is entered as 6).
SSID Profile Settings	<p>The Selectable SSID Profiles list displays the name(s) of the SSID profile(s) to which you can apply the general billing settings.</p> <p>To apply settings to an SSID profile, you can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and click the right arrow button to add to the Selected SSID Profiles list. To remove an SSID profile, select the name(s) in the Selected SSID Profiles list and click the left arrow button.</p>
Apply	Click this button to save your changes to the UAG.
Reset	Click this button to return the screen to its last-saved settings.

26.3 The Billing Profile Screen

Use this screen to configure the billing profiles that defines the maximum Internet access time and charge per time unit. Click **Configuration > Billing > Billing Profile** to open the following screen.

Figure 219 Configuration > Billing > Billing Profile

The following table describes the labels in this screen.

Table 138 Configuration > Billing > Billing Profile

LABEL	DESCRIPTION
Account Generator Settings	
Button A ~ C	Select a billing profile for each button of the web-based account generator. The buttons correspond to the buttons on a connected statement printer.
Preview	Click this button to open the Account Generator screen, where you can generate a dynamic guest account and print the account information using a statement printer connected to the UAG (see Section 26.3.1 on page 308 for more information).
Billing Profile	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
#	This field is a sequential value, and it is not associated with a specific entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the descriptive profile name for this entry.

Table 138 Configuration > Billing > Billing Profile (continued)

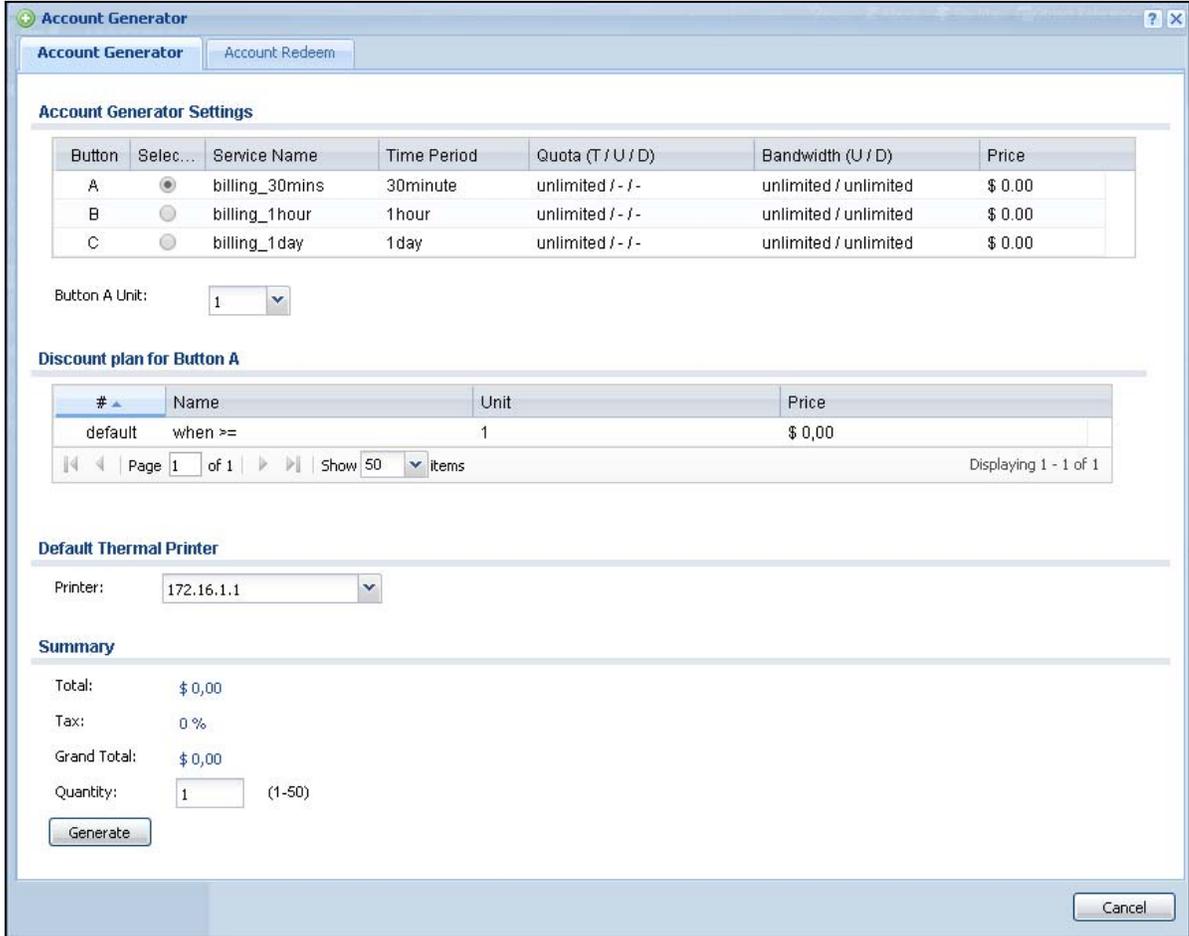
LABEL	DESCRIPTION
Time Period	This field displays the duration of the billing period.
Quota (T/U/D)	This field displays how much data in both directions (T otal) or upstream data (U pload) and downstream data (D ownload) can be transmitted through the WAN interface before the account expires.
Bandwidth (U/D)	This field displays the maximum upstream (U pload) and downstream (D ownload) bandwidth allowed for the user account in kilobits per second.
Price	This field displays each profile's price per time unit.
Apply	Click this button to save your changes to the UAG.
Reset	Click this button to return the screen to its last-saved settings.

26.3.1 The Account Generator Screen

The **Account Generator** screen allows you to automatically create dynamic guest accounts (see [Section 7.9 on page 103](#) and [Dynamic-Guest Accounts on page 400](#) for more information on dynamic guest accounts).

Click **Configuration > Billing > Billing Profile** and then the **Preview** button to open this screen. You can also open this screen by logging into the Web Configurator with the guest-manager account.

Figure 220 Account Generator



The following table describes the labels in this screen.

Table 139 Account Generator

LABEL	DESCRIPTION
Account Generator Settings	Select a button and specify how many units of billing period to be charged for new account in the Button x Unit field.
Discount plan for Button x	This section displays only when you enable the discount price plan in the Billing > Discount screen.
#	This is the number of each discount level. The default (first) level cannot be edited or deleted. It is created automatically according to the billing profile of the button you select.
Name	This field displays the conditions of each discount level.
Unit	This field displays the duration of the billing period that should be reached before the UAG charges users at this level.
Price	This field displays the price per time unit for each level.
Default Thermal Printer	Select a statement printer that is attached to the UAG. It displays n/a if there is no printer attached.
Summary	
Total	This shows the total price for the account before sales tax is added.

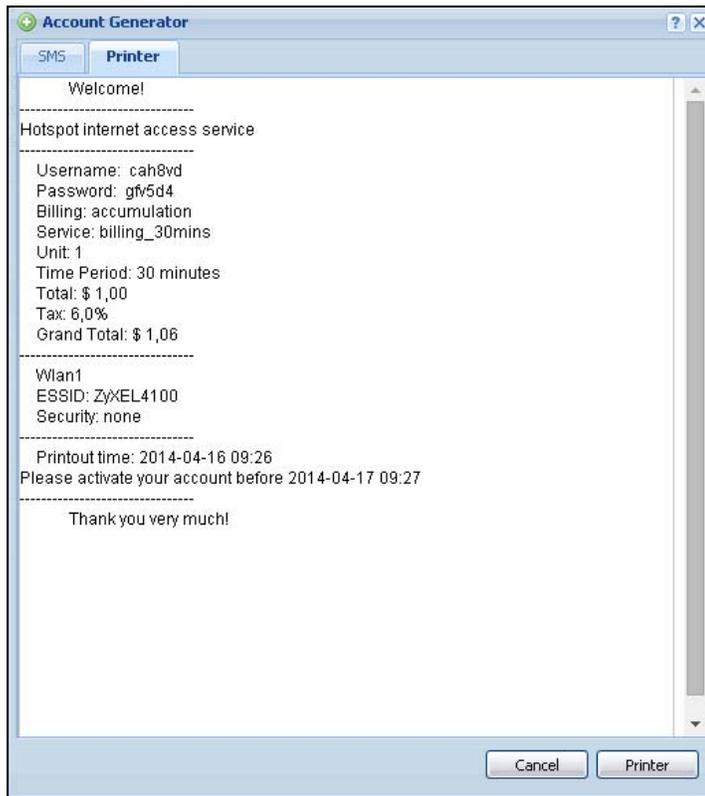
Table 139 Account Generator (continued)

LABEL	DESCRIPTION
Tax	This shows the tax rate.
Grand Total	This shows the total price including tax.
Quantity	Specify the number of account to be created.
Generate	Click Generate to generate an account based on the billing settings you configure for the selected button in the Billing Profile screen. A window displays showing the SMS message and/or a printout preview of the account generated.
Cancel	Click Cancel to exit this screen without saving.
Logout	Click Logout to log out of the web configurator. This button is available only when you open this screen by logging in with the guest-manager account.

The following figure shows an example SMS message with account information. The **SMS** screen displays only when you enable SMS in the **Configuration > SMS** screen. You can enter the user's mobile phone number and click **Send SMS** to send the account information in an SMS text message to the user's mobile phone. Click **Cancel** to close this window when you are finished viewing it.

The screenshot shows a web browser window titled "Account Generator" with a sub-tab "SMS". The main content area is titled "SMS Content" and displays a message box with the following text: "Username:g7kqua Password:nhj7mr Activate account before 2014-04-17 09:24". Below this, there is a "Send SMS" section with input fields for "Country Code" (886) and "Mobile Number" (0912345678). An example number "[886][091 01 23456] (for Taiwan)" is provided. A "Send SMS" button is located below the input fields. At the bottom of the window, there are "Cancel" and "Printer" buttons.

The **Printer** screen shows a printout preview example. Click **Printer** to print this subscriber statement. Click **Cancel** to close this window when you are finished viewing it.



26.3.2 The Account Redeem Screen

The **Account Redeem** screen allows you to send SMS messages for certain accounts. Click the **Account Redeem** tab in the **Account Generator** screen to open this screen.

Figure 221 Account Redeem

The following table describes the labels in this screen.

Table 140 Account Redeem

LABEL	DESCRIPTION
Query Account Information	
Phone Number	Enter the country code and mobile phone number and click Query to display only the account(S) that has the specified phone number.
SMS	Click this button to send text messages for the accounts in the list below. You can use this button only when SMS is enabled and there is at least one account in the list.
#	This is the index number of the dynamic guest account in the list.
Status	This field displays whether an account expires or not.
Username	This field displays the user name of the account.
Create Time	This field displays when the account was created.
Remaining Time	This field displays the amount of Internet access time remaining for each account.
Time Period	This field displays the total account of time the account can use to access the Internet through the UAG.
Expiration Time	This field displays the date and time the account becomes invalid. Note: Once the time allocated to a dynamic account is used up or a dynamic account remains un-used after the expiration time, the account is deleted from the account list.
Charge	This field displays the total cost of the account.
Payment Info	This field displays the method of payment for each account.
Phone Num	This field displays the mobile phone number for the account.

Table 140 Account Redeem (continued)

LABEL	DESCRIPTION
Cancel	Click Cancel to exit this screen without saving.
Logout	Click Logout to log out of the web configurator. This button is available only when you open this screen by logging in with the guest-manager account.

26.3.3 The Billing Profile Add/Edit Screen

The **Billing Profile Add/Edit** screen allows you to create a new billing profile or edit an existing one. Click **Configuration > Billing > Billing Profile** and then an **Add** or **Edit** icon to open this screen.

Figure 222 Configuration > Billing > Billing Profile > Add/Edit

The screenshot shows the 'Billing Profile' configuration window. It is divided into four main sections:

- General Settings:** Includes a checked checkbox for 'Enable billing profile'. Below it are 'Name' and 'Price' text input fields, both highlighted with red dashed boxes and a red exclamation mark icon.
- Time Period Setting:** Features a 'Time Period' text input field (red dashed box, exclamation mark), a dropdown menu set to 'minute', and a note '(0 is unlimited)'.
- Quota Settings:** Shows 'Quota Type' with radio buttons for 'Total' and 'Upload / Download' (selected). Below are 'Upload Quota' and 'Download Quota' text input fields (red dashed boxes, exclamation marks), each followed by a unit dropdown menu set to 'MB' and a note '(0-1023 MB, 0 is unlimited)'.
- Bandwidth Settings:** Includes a checked checkbox for 'Enable Bandwidth'. Below are 'Upload' and 'Download' text input fields (both set to '0'), each followed by 'kbps (0 is unlimited)' and a 'Priority' dropdown menu set to '4'.

At the bottom right, there are 'OK' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 141 Configuration > Billing > Billing Profile > Add/Edit

LABEL	DESCRIPTION
Enable billing profile	Select this option to activate the profile.
Name	Enter a name for the billing profile. You can use up to 31 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). Spaces are not allowed. The first character must be a letter.
Price	Define each profile's price, up to 999999.99, per time unit.
Time Period	Set the duration of the billing period (minute , hour , or day). When this period expires, the user's access will be stopped.

Table 141 Configuration > Billing > Billing Profile > Add/Edit (continued)

LABEL	DESCRIPTION
Quota Type	<p>The quota settings section is NOT available when you set Accounting Method to Time to Finish in the Billing > General screen.</p> <p>Set a limit for the user accounts. This only applies to user's traffic that is received or transmitted through the WAN interface.</p> <p>Note: When the limit is exceeded, the user is not allowed to access the Internet through the UAG.</p> <p>Select Total to set a limit on the total traffic in both directions.</p> <p>Select Upload/Download to set a limit on the upstream traffic and downstream traffic respectively.</p>
Total Quota	<p>If you select Total, specify how much downstream and/or upstream data (in MB (Megabytes) or GB (Gigabytes)) can be transmitted through the WAN interface before the account expires. 0 means there is no data limit for the user account.</p>
Upload Quota	<p>If you select Upload/Download, specify how much upstream data (in MB (Megabytes) or GB (Gigabytes)) can be transmitted through the WAN interface before the account expires.</p> <p>0 means there is no data limit for the user account.</p>
Download Quota	<p>If you select Upload/Download, specify how much downstream data (in MB (Megabytes) or GB (Gigabytes)) can be transmitted through the WAN interface before the account expires.</p> <p>0 means there is no data limit for the user account.</p>
Enable Bandwidth	<p>Select this option to turn on bandwidth management for the user accounts.</p>
Upload	<p>Specify the maximum outgoing bandwidth allowed for the user account in kilobits per second. Upload refers to the traffic the UAG sends out from a user.</p>
Download	<p>Specify the maximum incoming bandwidth allowed for the user account in kilobits per second. Download refers to the traffic the UAG sends to a user.</p>
Priority	<p>Enter a number between 1 and 7 to set the priority for the user's traffic. The smaller the number, the higher the priority.</p> <p>Traffic with a higher priority is given bandwidth before traffic with a lower priority.</p> <p>Note: The priority setting here has priority over the priority setting in a bandwidth management rule.</p>
OK	<p>Click OK to save your changes back to the UAG.</p>
Cancel	<p>Click Cancel to exit this screen without saving.</p>

26.4 The Discount Screen

Use this screen to configure a custom discount pricing plan. This is useful for providing reduced rates for purchases of longer periods of time. You can charge higher rates per unit at lower levels (fewer units purchased) and lower rates per unit at higher levels (more units purchased). Click **Configuration > Billing > Discount** to open the following screen.

Note: The discount price plan does not apply to users who purchase access time online with a credit card.

Figure 223 Configuration > Billing > Discount

The following table describes the labels in this screen.

Table 142 Configuration > Billing > Discount

LABEL	DESCRIPTION
Discount Settings	
Enable Discount	Select the check box to activate the discount price plan.
Button Select	Select a button from the drop-down list box to assign the base charge.
Charge by levels	Select this to charge the rate at each successive level from the first level (most expensive per unit) to the highest level (least expensive per unit) that the total purchase reaches. Otherwise, deselect this to charge all of the user's time units only at the highest level (least expensive) that their total purchase reaches.
Discount Price Plan	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
#	This is the number of each discount level. The default (first) level cannot be edited or deleted. It is created automatically according to the billing profile of the button you select.
Name	This field displays the conditions of each discount level.
Unit	This field displays the duration of the billing period that should be reached before the UAG charges users at this level.
Price	This field displays the price per time unit for each level.
Apply	Click this button to save your changes to the UAG.
Reset	Click this button to return the screen to its last-saved settings.

26.4.1 The Discount Add/Edit Screen

The **Discount Add/Edit** screen allows you to create a new discount level or edit an existing one. Click **Configuration > Billing > Discount** and then an **Add** or **Edit** icon to open this screen.

Figure 224 Configuration > Billing > Discount > Add/Edit

The following table describes the labels in this screen.

Table 143 Configuration > Billing > Discount > Add/Edit

LABEL	DESCRIPTION
Name	This field displays the conditions of each discount level.
Unit	Set the duration of the billing period that should be reached before the UAG charges users at this level.
Price	Define this level's charge per time unit.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

26.5 The Payment Service General Screen

Use this screen to use a credit card service to authorize, process, and manage credit card transactions directly through the Internet. You must register with the supported credit card service before you can configure the UAG to handle credit card transactions. Click **Configuration > Billing > Payment Service** to open the following screen.

Figure 225 Configuration > Billing > Payment Service > General

The following table describes the labels in this screen.

Table 144 Configuration > Billing > payment Service > General

LABEL	DESCRIPTION
General Setting	
Enable Payment Service	Select the check box to use PayPal to authorize credit card payments. Note: After you set up web authentication policies and enable the online payment service on the UAG, a link displays in the login screen when users try to access the Internet. The link redirects users to a screen where they can make online payments by credit card to purchase access time and get dynamic guest account information.
Payment Provider Selection	
Account	You should already have a PayPal account to receive credit card payments. Enter your PayPal account name.
Currency	Select the currency in which payments are made. The available options depend on currencies that PayPal supports.
Identity Token	Enter the ID token provided to you by PayPal after successfully applying for your PayPal account.
Payment Gateway	Enter the address of the PayPal gateway provided to you by PayPal after applying for your PayPal account.
Account Delivery Method	

Table 144 Configuration > Billing > payment Service > General (continued)

LABEL	DESCRIPTION
Delivery Method	<p>Specify how the UAG provides dynamic guest account information after the user's online payment is done.</p> <p>Select On-Screen to display the user account information in the web screen.</p> <p>Select SMS to use Short Message Service (SMS) to send account information in a text message to the user's mobile device.</p> <p>Select On-Screen and SMS to provide the account information both in the web screen and via SMS text messages.</p> <p>Note: You should have enabled SMS in the Configuration > SMS screen to send text messages to the user's mobile device.</p>
Apply	Click this button to save your changes to the UAG.
Reset	Click this button to return the screen to its last-saved settings.

26.5.1 The Payment Service Desktop View / Mobile View Screen

Use this screen to customize the online payment service pages that displays after an unauthorized user click the link in the Web Configurator login screen to purchase access time. You can configure both the desktop and mobile versions of the the service pages. Users click a link in the pages to switch between the two versions.

Click **Configuration > Billing > Payment Service > Desktop View** or **Mobile View** to open the following screen.

Figure 226 Configuration > Billing > Payment Service > Desktop View

Select Type

Use Default Page
 Use Customized Page

Customized Profile Selection Page

Selection Message:

#	Service Name	Time Period	Charge	Quantity
1	AAA	2 hour	\$ 23	1 ▼
2	AAA	2 hour	\$ 23	1 ▼
3	AAA	2 hour	\$ 23	1 ▼
4	AAA	2 hour	\$ 23	1 ▼
5	AAA	2 hour	\$ 23	1 ▼
6	AAA	2 hour	\$ 23	1 ▼

OK

Customized Successfully Page

Successful Message:
 Activation Message:
 Activation Code:
 Account Message:
 Exp. Time:

Customized Fail Page

Fail Message:

Customized SMS Page

Information Message:

Apply Reset

Welcome
Please choose from the following service selection

Welcome
You may now use the internet.
IMPORTANT! Please Make a note of your username and password for logging in later. This will be your only opportunity to do so. Note upper and lowercase letters.
This is your account information, please keep this for your internet service.

Your username is XXX
Your password is XXX
Your time period is 0 day, 00 hour 30 minutes

Please activate your account before 28/03/2012, 23:00:00

Welcome
Sorry! We can't handle your payment transaction at this time.

Go to [Payment](#) and check your account.

Welcome
Please check your mobile phone for the account information.

Figure 227 Configuration > Billing > Payment Service > Mobile View

The screenshot displays the ZyXEL configuration interface for the Payment Service in Mobile View. The interface is divided into several sections for configuring different user-facing pages:

- Select Type:** Options include "Use Default Page" and "Use Customized Page" (selected).
- Customized Profile Selection Page:**
 - Selection Message: "Please choose the service plan from the following profile table"
 - Preview shows a table with columns: Time, Quota, and Charge.

Time	Quota	Charge
50min	100MB / 1000D	€1.00
24hr	unlimited	€3.00
- Customized Successfully Page:**
 - Successfully Message: "you may now use the internet."
 - Notification Message: "IMPORTANT! MAKE a note for your case-sensitive"
 - Notification Color: "red"
 - Preview shows a success message with a warning icon, followed by fields for "Your username" (13qxs3), "Your password" (ze10mk), "Your time period" (30 minutes), and an expiration date "26/04/2014, 23:00:00". A "Login Now" button is present.
- Customized Fail Page:**
 - Failed Message: "Sorry! We can't handle your payment transaction at this time"
 - Preview shows a failure message with a warning icon, a "Reason: Invalid operation" message, and buttons for "OK" and "Go to PayPal".
- Customized SMS Page:**
 - Information Message: "Please check your mobile phone for the account inform."
 - Preview shows an SMS message with an "OK" button.

At the bottom of the configuration area, there are "Apply" and "Reset" buttons.

The following table describes the labels in this screen.

Table 145 Configuration > Billing > payment Service > Desktop View or Mobile View

LABEL	DESCRIPTION
Select Type	
Use Default Page	Select this to use the default online payment service page built into the device. If you later create a custom online payment service page, you can still return to the UAG's default page as it is saved indefinitely.
Use Customized Page	Select this to use a custom online payment service page instead of the default one built into the UAG. Once this option is selected, the custom page controls below become active.
Customized Profile Selection Page	
Selection Message	Enter a note to display in the first welcome page that allows users to choose a billing period they want. Use up to 256 printable ASCII characters. Spaces are allowed.
Customized Successfully Page	
Successfully Message	Enter a note to display in the second page after the user's online payment is made successfully. Use up to 256 printable ASCII characters. Spaces are allowed.
Notification Message	Enter the important information you want to display. Use up to 256 printable ASCII characters. Spaces are allowed.
Notification Color	Specify the font color of the important information. You can use the color palette chooser, or enter a color value of your own.
Account Message	Enter a note to display above the user account information. Use up to 256 printable ASCII characters. Spaces are allowed.
Day Time	Select the format in which you want to display the date and how long an account is allowed to stay un-used before it expires.
Customized Fail Page	
Failed Message	Enter a note to display when the user's online payment failed. Use up to 256 printable ASCII characters. Spaces are allowed.
Customized SMS Page	
Information Message	Enter a note to display when you set the UAG to send account information via SMS text messages. Use up to 256 printable ASCII characters. Spaces are allowed.
Apply	Click this button to save your changes to the UAG.
Reset	Click this button to return the screen to its last-saved settings.

27.1 Overview

You can create dynamic guest accounts and print guest account information by pressing the button on an external statement printer, such as SP350E.

Make sure that the printer is connected to the appropriate power and the UAG, and that there is printing paper in the printer. Refer to the printer's documentation for details.

27.1.1 What You Can Do in this Chapter

- Use the **General Setting > General** screen (see [Section 27.2 on page 322](#)) to configure the printer list and enable printer management.
- Use the **General Setting > Printout Configuration** screen (see [Section 27.3 on page 325](#)) to customize the account printout.
- Use the **Printer Manager** screen (see [Section 27.4 on page 326](#)) to manage and view information about the connected statement printer.

27.2 The General Setting Screen

Use this screen to configure a printer list and allow the UAG to monitor the printer status. Click **Configuration > Printer > General > General Setting** to open the following screen.

Figure 228 Configuration > Printer > General Setting > General

General Setting

Enable Printer Manager

Printer Settings

Port:

Encryption

Secret Key: (4 characters)

Printout

Number of Copies:

Printer List

Note:
If you want to configure printer button, please go to [Billing Profile](#).

#	Status	IPv4 Address	Description
1		172.17.0.23	4F
2		172.16.1.1	SP350E

Page 1 of 1 | Show 50 items | Displaying 1 - 2 of 2

Printer Firmware Information

Current Version: SP350E-V1.03

Apply Reset

The following table describes the labels in this screen.

Table 146 Configuration > Printer > General Setting > General

LABEL	DESCRIPTION
General Setting	
Enable Printer Manager	Select the check box to allow the UAG to manage and monitor the printer status.
Printer Settings	
Port	Enter the number of port on which the UAG sends data to the printer for it to print.
Encryption	Select the check box to turn on data encryption. Data transmitted between the UAG and the printer will be encrypted with a secret key
Secret Key	Enter four alphanumeric characters (A-Z, a-z, 0-9) to specify a key for data encryption.
Printout	
Number of Copies	Select how many copies of subscriber statements you want to print (1 is the default).
Printer List	Use this section to add the printer(s) that can be managed by the UAG.
Add	Click this to create a new entry.

Table 146 Configuration > Printer > General Setting > General (continued)

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
#	This field is a sequential value, and it is not associated with any entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
IPv4 Address	This field displays the IP address of the printer.
Description	This field displays the descriptive name for the printer.
Printer Firmware Information	
Current Version	This is the version of the printer firmware currently uploaded to the UAG. The UAG automatically installs it in the connected printers to make sure the printers are upgraded to the same version.
Apply	Click this button to save your changes to the UAG.
Reset	Click this button to return the screen to its last-saved settings.

27.2.1 Add/Edit Printer Rule

Click the **Add** icon or select an entry in the **Printer > General Setting > General** screen and click the **Edit** icon to open the following screen. Use this screen to add a new printer or modify the printer's settings.

Figure 229 Configuration > Printer > General Setting > General: Add/Edit

The following table describes the labels in this screen.

Table 147 Configuration > Printer > General Setting > General: Add/Edit

LABEL	DESCRIPTION
Enable Printer Manager	Select this option to turn on this entry in order to allow the UAG to manage this printer.
IPv4 Address	Enter an IPv4 address for the printer. This field is read-only if you are editing an existing entry.
Description	Enter a description of this printer. You can use alphanumeric and () + , / : = ? ! * # @ \$ _ % - " characters, and it can be up to 60 characters long.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

27.3 The Printout Configuration Screen

Use this screen to customize the account printout. Click **Configuration > Printer > General Setting > Printout Configuration** to open the following screen.

Figure 230 Configuration > Printer > General Setting > Printout Configuration

The following table describes the labels in this screen.

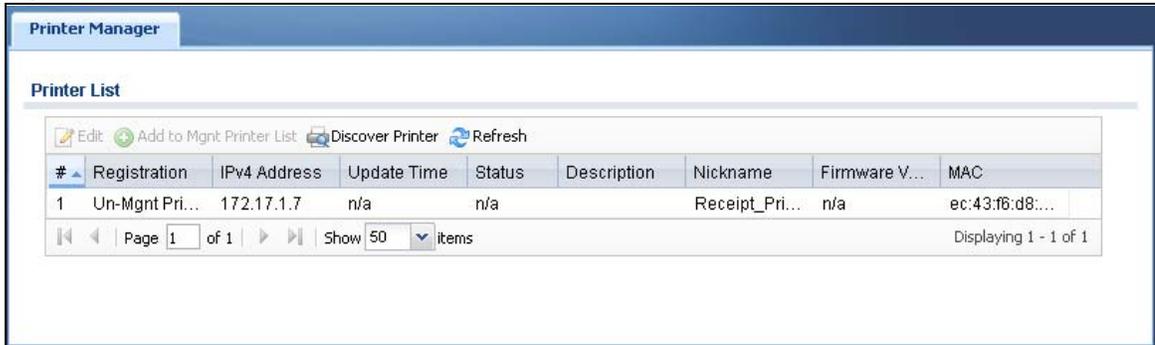
Table 148 Configuration > Printer > General Setting > Printout Configuration

LABEL	DESCRIPTION
Use Default Printout Configuration	Select this to use the default account printout format built into the device. If you later create a custom account printout format, you can still return to the UAG's default format as it is saved indefinitely.
Use Customized Printout Configuration	Select this to use a custom account printout format instead of the default one built into the UAG. Once this option is selected, the custom format controls below become active.
Preview	Click the button to display a preview of account printout format you uploaded to the UAG.
File Name	This shows the file name of account printout format file in the UAG. Click Download to download the account printout format file from the UAG to your computer.
File Path / Browse / Upload	Browse for the account printout format file or enter the file path in the available input box, then click the Upload button to put it on the UAG.
Restore Customized File to Default	Click Restore to set the UAG back to use the default built-in account printout format.
Download	Click this to download an example account printout format file from the UAG for your reference.
Apply	Click this button to save your changes to the UAG.
Reset	Click this button to return the screen to its last-saved settings.

27.4 The Printer Manager Screen

Use this screen to manage and view information about the connected statement printer, such as SP350E. Click **Configuration > Printer > Printer Manager** to display this screen.

Figure 231 Configuration > Printer > Printer Manager



The following table describes the labels in this screen.

Table 149 Configuration > Printer > Printer Manager

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings. Note: You cannot edit an entry's settings when the printer status is sync fail or sync progressing .
Add to Mgmt Printer List	Click this to add the selected printer to the managed printer list.
Discover Printer	Click this to detect the printer(s) that is connected to the UAG and display the printer information in the list below. Note: Use the Printer > General > General Setting to manually configure a printer's IP address and add it to the managed printer list when the printer is not detected or connected to the UAG.
Refresh	Click this button to update the information in the screen.
#	This is the index number of the printer in the list.
Registration	This field displays whether the printer is added to the managed printer list (Mgmt Printer) or not (Un-Mgmt Printer).
IPv4 Address	This field displays the IP address of the printer that you configured in the Configuration > Printer > Printer Manager screen.
Update Time	This field displays the date and time the UAG last synchronized with the printer. This shows n/a when the printer is not in the managed printer list or the printer status is sync fail or sync progressing .
Status	This field displays whether the UAG can connect to the printer and update the printer information. This shows n/a when the printer is not in the managed printer list.
Description	This field displays the descriptive name of the printer that you configured.
Nickname	This field displays the nickname of the printer that you configured.

Table 149 Configuration > Printer > Printer Manager (continued)

LABEL	DESCRIPTION
Firmware Version	This field displays the model number and firmware version of the printer. This shows n/a when the printer is not in the managed printer list or the printer status is sync fail .
MAC	This field displays the MAC address of the printer.

27.4.1 Edit Printer Manager

Select an entry in the **Printer > Printer Manager** screen and click the **Edit** icon to open the following screen. Use this screen to modify the printer's nickname and IP address.

Figure 232 Configuration > Printer > Printer Manager: Edit

The following table describes the labels in this screen.

Table 150 Configuration > Printer > Printer Manager: Edit

LABEL	DESCRIPTION
General Settings	
Nickname	Enter a nickname for the printer.
IP Address Assignment	
Get Automatically	Select this to make the printer a DHCP client and automatically get the IP address, subnet mask, and gateway address from a DHCP server.
Use Fixed IP Address	Select this if you want to specify the printer's IP address, subnet mask, and gateway manually.
IP Address	Enter the IP address for this printer.
Subnet Mask	Enter the subnet mask of this printer in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	Enter the IP address of the gateway. The UAG sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the printer.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving.

27.4.2 Reports Overview

The SP350E allows you to print status reports about the guest accounts and general UAG system information. Simply press a key combination on the SP350E to print a report instantly without accessing the web configurator.

The following lists the reports that you can print using the SP300E.

- Daily account summary
- Monthly account summary
- Last month account summary
- System status

27.4.3 Key Combinations

The following table lists the key combination to print each report.

Note: You must press the key combination on the SP350E within five seconds to print.

Table 151 Report Printing Key Combinations

REPORT TYPE	KEY COMBINATION
Daily Account Summary	A B C A A
Monthly Account Summary	A B C B A
Last Month Account Summary	A B C B B
System Status	A B C C A

The following sections describe each report printout in detail.

27.4.4 Daily Account Summary

The daily account report lists the accounts printed during the current day, the current day's total number of accounts and the total charge. It covers the accounts that have been printed during the current day starting from midnight (not the past 24 hours). For example, if you press the daily account key combination on 2013/05/10 at 20:00:00, the daily account report includes the accounts created on 2013/05/10 between 00:00:01 and 19:59:59.

Key combination: A B C A A

The following figure shows an example.

Figure 233 Daily Account Example

```

Daily Account
-----
      2013/05/10

Username  Price
-----
p2m6pf52 1.00
s4pcms28 2.00
-----
TOTAL ACCOUNTS: 2
TOTAL PRICE: $ 3.00
-----
2013/05/10 20:00:00
      ---End---

```

27.4.5 Monthly Account Summary

The monthly account report lists the accounts printed during the current month, the current month's total number of accounts and the total charge. It covers the accounts that have been printed during the current month starting from midnight of the first day of the current month (not the past one month period). For example, if you press the monthly account key combination on 2013/05/17 at 20:00:00, the monthly account report includes the accounts created from 2013/05/01 at 00:00:01 to 2013/05/17 at 19:59:59.

Key combination: A B C B A

The following figure shows an example.

Figure 234 Monthly Account Example

```

Monthly Account
-----
      2013/05

Username  Price
-----
p2m6pf52 1.00
s4pcms28 2.00
7ufm7z22 2.00
qm5fxn95 6.00
-----
TOTAL ACCOUNTS: 4
TOTAL PRICE: $ 11.00
-----
2013/05/17 20:00:11
      ---End---

```

27.4.6 Account Report Notes

The daily, monthly or last month account report holds up to 2000 entries. If there are more than 2000 accounts created in the same month or same day, the account report's calculations only include the latest 2000.

For example, if 2030 accounts (each priced at \$1) have been created from 2013/05/01 00:00:00 to 2013/05/31 19:59:59, the monthly account report includes the latest 2000 accounts, so the total would be \$2,000 instead of \$2,030.

Use the **Monitor > System Status > Dynamic Guest** screen to see the accounts generated on another day or month (up to 2000 entries total).

27.4.7 System Status

This report shows the current system information such as the host name and WAN IP address.

Key combination: A B C C A

The following figure shows an example.

Figure 235 System Status Example

```

System Status
-----
Item   Description
-----
SYST   02:02:35
WAST   Link up
WLST   Activate
FWVR   2.50 (AACG.0)
BTVR   1.22
WAMA   00-90-0E-00-4A-29
LAMA   00-90-0E-00-4A-30
WAIP   10.21.2.267
LAIP   172.16.0.1
WLIP   10.59.1.1
DHSP   10.59.1.33
DHEP   10.59.1.254
-----
CPUS   5%
MEMS   40%
DKST   5%
-----
2012/04/12 17:10:22
---End---

```

The following table describes the labels in this report.

Table 152 System Status

LABEL	DESCRIPTION
SYST	This field displays the time since the system was last restarted.
WAST	This field displays the WAN connection status.

Table 152 System Status (continued)

LABEL	DESCRIPTION
WLST	This field displays the status of the UAG's wireless LAN.
FWVR	This field displays the version of the firmware on the UAG.
BTVR	This field displays the version of the bootrom.
WAMA	This field displays the MAC address of the UAG on the WAN.
LAMA	This field displays the MAC address of the UAG on the LAN.
WAIP	This field displays the IP address of the WAN port on the UAG.
LAIP	This field displays the IP address of the LAN port on the UAG.
WLIP	This field displays the IP address of the wireless LAN interface on the UAG.
DHSP	This field displays the first of the continuous addresses in the IP address pool.
DHEP	This field displays the end of the continuous addresses in the IP address pool.
CPUS	This field displays the UAG's recent CPU usage.
MEMS	This field displays the UAG's recent memory usage.
DKST	This field displays what percentage of the UAG's onboard flash memory is currently being used.

Free Time

28.1 Overview

With Free Time, the UAG can create dynamic guest accounts that allow users to browse the Internet free of charge for a specified period of time.

28.1.1 What You Can Do in this Chapter

Use the **Free Time** screen (see [Section 28.2 on page 332](#)) to turn on this feature to allow users to get a free account for Internet surfing during the specified time period.

28.2 The Free Time Screen

Use this screen to enable and configure the free time settings. Click **Configuration > Free Time** to open the following screen.

Figure 236 Configuration > Free Time

Free Time

General Settings

Enable Free Time

Free Time Period: 30 minute

Reset Time: Daily

Time: 00:00

Maximum Registration Number Before Reset Time: 1 (1-5)

Delivery Method: On-Screen

Note:
If you want to configure ssid profile settings of the account, keep user logged in, please go to [Billing](#).

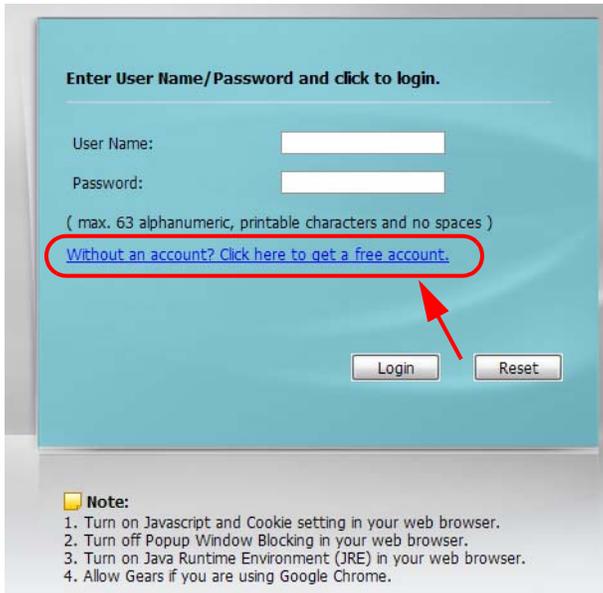
Apply Reset

The following table describes the labels in this screen.

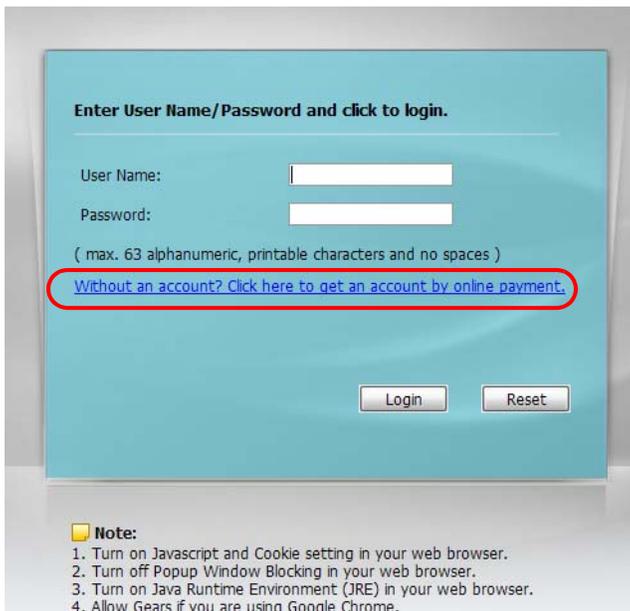
Table 153 Configuration > Free Time

LABEL	DESCRIPTION
Enable Free Time	<p>Select the check box to turn on the free time feature.</p> <p>Note: After you set up web authentication policies and enable the free time feature on the UAG, a link displays in the login screen when users try to access the Internet. The link redirects users to a screen where they can get a free account.</p>
Free Time Period	<p>Select the duration of time period for which the free time account is allowed to access the Internet.</p>
Reset Time	<p>Select Daily to have the UAG allow free account access every day at the specified time.</p> <p>Select Weekly to have the UAG allow free account access once a week on the day you select.</p> <p>Select Monthly to have the UAG allow free account access once a month on a set date.</p>
Time	<p>If you select Daily, select the time in 24-hour format at which the new free time account is allowed to access the Internet.</p>
Day	<p>If you select Weekly, select the day on which the new free time account is allowed to access the Internet.</p> <p>If you select Monthly, enter the date on which the new free time account is allowed to access the Internet. If the date you selected is not available in a month, such as 30th or 31th, the UAG allows the free account access on the last day of the month.</p>
Maximum Registration Number Before Reset Time	<p>Enter the maximum number of the users that are allowed to log in for Internet access with a free guest account before the time specified in the Reset Time field. This also sets how many free guest accounts a user can get.</p> <p>For example, if you set the Maximum Registration Number Before Reset Time to 1, the Reset Time to Daily and the Reset Time to 13:00, even the first free guest account has expired at 11:30, the user cannot get a second account and/or access the Internet until 13:00.</p>
Delivery Method	<p>Specify how the UAG provides dynamic guest account information.</p> <p>Select On-Screen to display the user account information in the web screen.</p> <p>Select SMS to use Short Message Service (SMS) to send account information in a text message to the user's mobile device.</p> <p>Select On-Screen and SMS to provide the account information both in the web screen and via SMS text messages.</p> <p>Note: You should have enabled SMS in the Configuration > SMS screen to send text messages to the user's mobile device.</p>
Apply	<p>Click this button to save your changes to the UAG.</p>
Reset	<p>Click this button to return the screen to its last-saved settings.</p>

The following figure shows an example login screen with a link to create a free guest account.



If you enable both online payment service and free time feature on the UAG, the link description in the login screen will be mainly for online payment service. You can still click the link to get a free account.



If SMS is enabled on the UAG, you have to enter your mobile phone number before clicking **OK** to get a free guest account.

Welcome
Please choose the service plan from the following profile table.

#	Service Name	Service Time	Charge	Unit
1	Free Time	30 minutes	Free	1

Country Code:
Mobile Number:
Example: [886][0910123456](for Taiwan)

The guest account information then displays in the screen and/or is sent to the configured mobile phone number.

Welcome

You may now use the internet.

IMPORTANT! MAKE a note for your case-sensitive username and password for logging later. This will be your only opportunity to do so.

This is your account information, please keep this for your internet service.

Your username is **uz39**
Your password is **4wmdm**
Your time period is **30 minutes**

EXAMPLE

29.1 Overview

The UAG supports Short Message Service (SMS) to send short text messages to mobile phone devices. At the time of writing, the UAG uses ViaNett as the SMS gateway to help forward SMS messages. You must already have a Vianett account in order to use the SMS service.

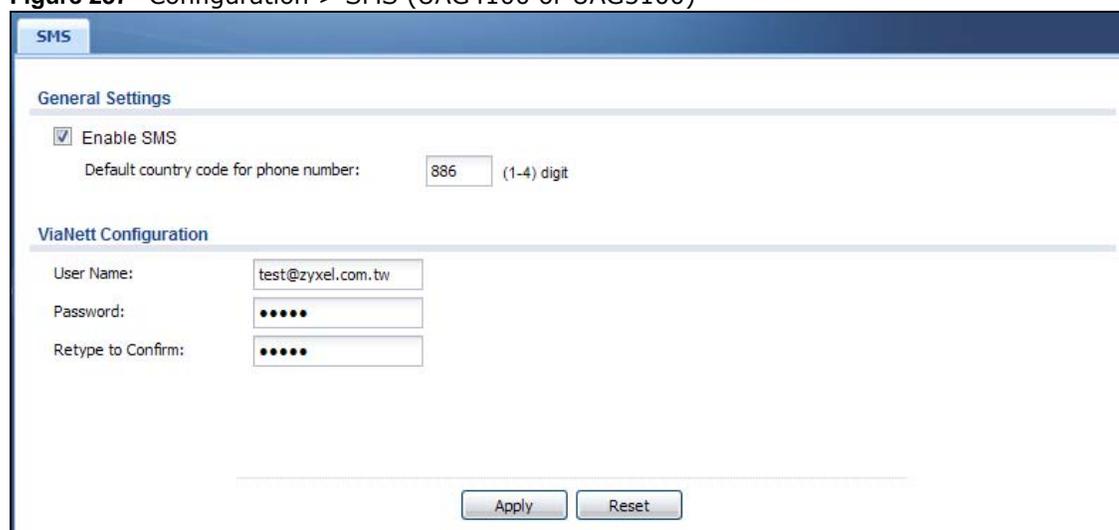
29.1.1 What You Can Do in this Chapter

Use the **SMS** screen (see [Section 29.2 on page 336](#)) to turn on the SMS service on the UAG.

29.2 The SMS Screen

Use this screen to enable SMS in order to send dynamic guest account information in text messages. Click **Configuration > SMS** to open the following screen.

Figure 237 Configuration > SMS (UAG4100 or UAG5100)



The screenshot displays the 'SMS' configuration interface. It is divided into two main sections: 'General Settings' and 'ViaNett Configuration'. In the 'General Settings' section, there is a checked checkbox for 'Enable SMS' and a text input field for 'Default country code for phone number' containing the value '886', with a note '(1-4) digit' to its right. The 'ViaNett Configuration' section includes three input fields: 'User Name' with the value 'test@zyxel.com.tw', 'Password' with five dots, and 'Retype to Confirm' with five dots. At the bottom of the form, there are two buttons: 'Apply' and 'Reset'.

Figure 238 Configuration > SMS (UAG2100)

The following table describes the labels in this screen.

Table 154 Configuration > SMS

LABEL	DESCRIPTION
General Settings	
Enable SMS	Select the check box to turn on the SMS service.
Default country code for phone number	Enter the default country code for the mobile phone number to which you want to send SMS messages.
ViaNett Configuration	
User Name	Enter the user name for your ViaNett account.
Password	Type the Password associated with the user name.
Retype to Confirm	Type your password again for confirmation.
License	This section is available only on the UAG that requires SMS service subscription, the UAG2100 for example.
Licensed Service Status	This field displays whether the service is activated (Licensed) or not (Not Licensed). Note: You must subscribe to the SMS service before you can use the service to send a text message.
License Type	This field displays Standard when the service is activated. Otherwise, it displays None .
Register Now	Click the link to go to myZyXEL.com where you can register your UAG and activate the service. This link is available only when the service is not activated yet.
Apply	Click this button to save your changes to the UAG.
Reset	Click this button to return the screen to its last-saved settings.

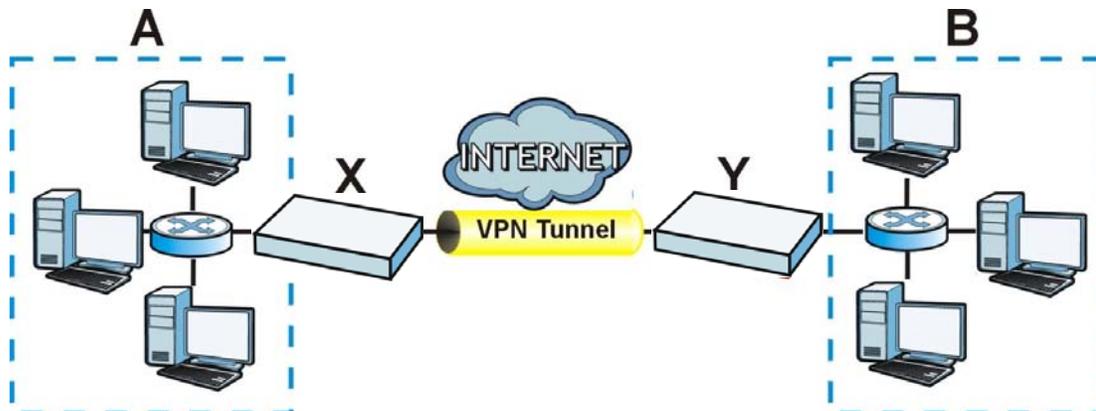
30.1 Virtual Private Networks (VPN) Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

IPSec VPN

Internet Protocol Security (IPSec) VPN connects IPSec routers or remote users using IPSec client software. This standards-based VPN offers flexible solutions for secure data communications across a public network. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer. The UAG can also combine multiple IPSec VPN connections into one secure network. Here local UAG **X** uses an IPSec VPN tunnel to remote (peer) UAG **Y** to connect the local (**A**) and remote (**B**) networks.

Figure 239 IPSec VPN Example



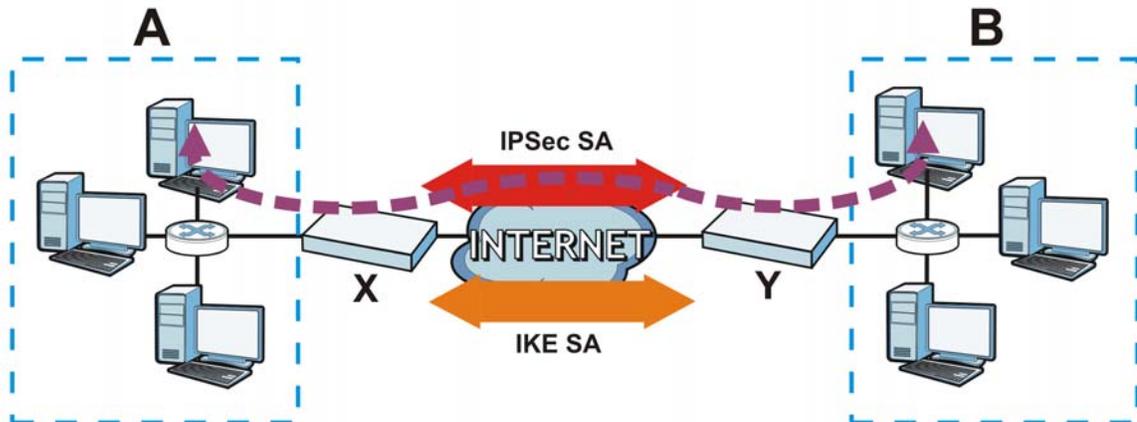
30.1.1 What You Can Do in this Chapter

- Use the **VPN Connection** screens (see [Section 30.2 on page 340](#)) to specify which IPSec VPN gateway an IPSec VPN connection policy uses, which devices behind the IPSec routers can use the VPN tunnel, and the IPSec SA settings (phase 2 settings). You can also activate or deactivate and connect or disconnect each VPN connection (each IPSec SA).
- Use the **VPN Gateway** screens (see [Section 30.3 on page 347](#)) to manage the UAG's VPN gateways. A VPN gateway specifies the IPSec routers at either end of a VPN tunnel and the IKE SA settings (phase 1 settings). You can also activate and deactivate each VPN gateway.

30.1.2 What You Need to Know

An IPsec VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the UAG and the remote IPsec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the UAG and remote IPsec router. The second phase uses the IKE SA to securely establish an IPsec SA through which the UAG and remote IPsec router can send data between computers on the local network and remote network. This is illustrated in the following figure.

Figure 240 VPN: IKE SA and IPsec SA



In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPsec SA. The IPsec SA is secure because routers **X** and **Y** established the IKE SA first.

Finding Out More

- See [Section 30.4 on page 354](#) for IPsec VPN background information.
- See the help in the IPsec VPN quick setup wizard screens.

30.1.3 Before You Begin

This section briefly explains the relationship between VPN tunnels and other features. It also gives some basic suggestions for troubleshooting.

You should set up the following features before you set up the VPN tunnel.

- In any VPN connection, you have to select address objects to specify the local policy and remote policy. You should set up the address objects first.
- In a VPN gateway, you can select an Ethernet interface, virtual Ethernet interface, VLAN interface, or virtual VLAN interface to specify what address the UAG uses as its IP address when it establishes the IKE SA. You should set up the interface first. See [Chapter 10 on page 154](#).
- In a VPN gateway, you can enable extended authentication. If the UAG is in server mode, you should set up the authentication method (AAA server) first. The authentication method specifies how the UAG authenticates the remote IPsec router. See [Chapter 42 on page 459](#).

- In a VPN gateway, the UAG and remote IPsec router can use certificates to authenticate each other. Make sure the UAG and the remote IPsec router will trust each other's certificates. See [Chapter 44 on page 467](#).

30.2 The VPN Connection Screen

Click **Configuration > VPN > IPsec VPN** to open the **VPN Connection** screen. The **VPN Connection** screen lists the VPN connection policies and their associated VPN gateway(s), and various settings. In addition, it also lets you activate or deactivate and connect or disconnect each VPN connection (each IPsec SA). Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 241 Configuration > VPN > IPsec VPN > VPN Connection



Each field is discussed in the following table. See [Section 30.2.1 on page 341](#) for more information.

Table 155 Configuration > VPN > IPsec VPN > VPN Connection

LABEL	DESCRIPTION
Ignore "Don't Fragment" setting in IPv4 header	Select this to fragment packets larger than the MTU (Maximum Transmission Unit) that have the "don't fragment" bit in the IP header turned on. When you clear this the UAG drops packets larger than the MTU that have the "don't fragment" bit in the header turned on.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
Connect	To connect an IPsec SA, select it and click Connect .
Disconnect	To disconnect an IPsec SA, select it and click Disconnect .
Object Reference	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 10.3.2 on page 165 for an example.

Table 155 Configuration > VPN > IPsec VPN > VPN Connection (continued)

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific connection.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The connect icon is lit when the interface is connected and dimmed when it is disconnected.
Name	This field displays the name of the IPsec SA.
VPN Gateway	This field displays the associated VPN gateway(s).
Policy	This field displays the local policy and the remote policy, respectively.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

30.2.1 The VPN Connection Add/Edit Screen

The **Add/Edit VPN Connection** screen allows you to create a new VPN connection policy or edit an existing one. To access this screen, go to the **Configuration > VPN > IPsec VPN > VPN Connection** screen (see [Section 30.2 on page 340](#)), and either click the **Add** icon or select an entry and click the **Edit** icon.

Figure 242 Configuration > VPN > IPSec VPN > VPN Connection > Add/Edit

Add VPN Connection

Hide Advanced Settings Create new Object

General Settings

Enable
 Connection Name:
 Nailed-Up
 Enable Replay Detection
 Enable NetBIOS broadcast over IPSec
 MSS Adjustment
 Custom Size (200 - 1460 Bytes)
 Auto

VPN Gateway

Application Scenario: Site-to-site
 VPN Gateway:

Policy

Local policy:
 Remote policy:
 Policy Enforcement

Phase 2 Setting

SA Life Time: (180 - 3000000 Seconds)
 Active Protocol:
 Encapsulation:
 Proposal

#	Encryption	Authentication
1	DES	SHA1

 Perfect Forward Security (PFS):

Related Settings

Zone:

Connectivity Check

Enable Connectivity Check
 Check Method:
 Check Port:
 Check Period: (5-30 Seconds)
 Check Timeout: (1-10 Seconds)
 Check Fail Tolerance:
 Check This Address (Domain Name or IP Address)
 Check the First and Last IP Address in the Remote Policy
 Log

Inbound/Outbound traffic NAT

Outbound Traffic

Source NAT
 Source:
 Destination:
 SNAT:

Inbound Traffic

Source NAT
 Source:
 Destination:
 SNAT:
 Destination NAT

#	Original IP	Mapped IP	Protocol	Original Port S...	Original Port E...	Mapped Port ...	Mapped Port ...
No data to display							

Page 1 of 1 Show 50 items

OK Cancel

Each field is described in the following table.

Table 156 Configuration > VPN > IPsec VPN > VPN Connection > Add/Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create new Object	Use to configure any new settings objects that you need to use in this screen.
General Settings	
Enable	Select this check box to activate this VPN connection.
Connection Name	Type the name used to identify this IPsec SA. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Nailed-Up	Select this if you want the UAG to automatically renegotiate the IPsec SA when the SA life time expires.
Enable Replay Detection	Select this check box to detect and reject old or duplicate packets to protect against Denial-of-Service attacks.
Enable NetBIOS Broadcast over IPsec	<p>Select this check box if you the UAG to send NetBIOS (Network Basic Input/Output System) packets through the IPsec SA.</p> <p>NetBIOS packets are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. It may sometimes be necessary to allow NetBIOS packets to pass through IPsec SAs in order to allow local computers to find computers on the remote network and vice versa.</p>
MSS Adjustment	<p>Select Custom Size to set a specific number of bytes for the Maximum Segment Size (MSS) meaning the largest amount of data in a single TCP segment or IP datagram for this VPN connection.</p> <p>Select Auto to have the UAG automatically set the MSS for this VPN connection.</p>
VPN Gateway	
Application Scenario	<p>This field is read-only and shows the scenario that the UAG supports.</p> <p>Site-to-site - The remote IPsec router needs to have a static IP address or a domain name. This UAG can initiate the VPN tunnel.</p>
VPN Gateway	Select the VPN gateway this VPN connection is to use or select Create new Object to add another VPN gateway for this VPN connection to use.
Policy	
Local Policy	Select the address corresponding to the local network. Use Create new Object if you need to configure a new one.
Remote Policy	Select the address corresponding to the remote network. Use Create new Object if you need to configure a new one.
Policy Enforcement	<p>Clear this to allow traffic with source and destination IP addresses that do not match the local and remote policy to use the VPN tunnel. Leave this cleared for free access between the local and remote networks.</p> <p>Selecting this restricts who can use the VPN tunnel. The UAG drops traffic with source and destination IP addresses that do not match the local and remote policy.</p>
Phase 2 Settings	
SA Life Time	Type the maximum number of seconds the IPsec SA can last. Shorter life times provide better security. The UAG automatically negotiates a new IPsec SA before the current one expires, if there are users who are accessing remote resources.

Table 156 Configuration > VPN > IPsec VPN > VPN Connection > Add/Edit (continued)

LABEL	DESCRIPTION
Active Protocol	<p>Select which protocol you want to use in the IPsec SA. Choices are:</p> <p>AH (RFC 2402) - provides integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not encryption. If you select AH, you must select an Authentication algorithm.</p> <p>ESP (RFC 2406) - provides encryption and the same services offered by AH, but its authentication is weaker. If you select ESP, you must select an Encryption algorithm and Authentication algorithm.</p> <p>Both AH and ESP increase processing requirements and latency (delay).</p> <p>The UAG and remote IPsec router must use the same active protocol.</p>
Encapsulation	<p>Select which type of encapsulation the IPsec SA uses. Choices are</p> <p>Tunnel - this mode encrypts the IP header information and the data.</p> <p>Transport - this mode only encrypts the data.</p> <p>The UAG and remote IPsec router must use the same encapsulation.</p>
Proposal	Use this section to manage the encryption algorithm and authentication algorithm pairs the UAG accepts from the remote IPsec router for negotiating the IPsec SA.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific proposal. The sequence of proposals should not affect performance significantly.
Encryption	<p>This field is applicable when the Active Protocol is ESP. Select which key size and encryption algorithm to use in the IPsec SA. Choices are:</p> <p>NULL - no encryption key or algorithm</p> <p>DES - a 56-bit key with the DES encryption algorithm</p> <p>3DES - a 168-bit key with the DES encryption algorithm</p> <p>AES128 - a 128-bit key with the AES encryption algorithm</p> <p>AES192 - a 192-bit key with the AES encryption algorithm</p> <p>AES256 - a 256-bit key with the AES encryption algorithm</p> <p>The UAG and the remote IPsec router must both have at least one proposal that uses use the same encryption and the same key.</p> <p>Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput.</p>
Authentication	<p>Select which hash algorithm to use to authenticate packet data in the IPsec SA. Choices are SHA1, SHA256, SHA512 and MD5. SHA is generally considered stronger than MD5, but it is also slower.</p> <p>The UAG and the remote IPsec router must both have a proposal that uses the same authentication algorithm.</p>

Table 156 Configuration > VPN > IPsec VPN > VPN Connection > Add/Edit (continued)

LABEL	DESCRIPTION
Perfect Forward Secrecy (PFS)	<p>Select whether or not you want to enable Perfect Forward Secrecy (PFS) and, if you do, which Diffie-Hellman key group to use for encryption. Choices are:</p> <p>none - disable PFS</p> <p>DH1 - enable PFS and use a 768-bit random number</p> <p>DH2 - enable PFS and use a 1024-bit random number</p> <p>DH5 - enable PFS and use a 1536-bit random number</p> <p>PFS changes the root key that is used to generate encryption keys for each IPsec SA. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.</p>
Related Settings	
Zone	Select the security zone into which to add this VPN connection policy. Any security rules or settings configured for the selected zone apply to this VPN connection policy.
Connectivity Check	The UAG can regularly check the VPN connection to the gateway you specified to make sure it is still available.
Enable Connectivity Check	Select this to turn on the VPN connection check.
Check Method	<p>Select how the UAG checks the connection. The peer must be configured to respond to the method you select.</p> <p>Select icmp to have the UAG regularly ping the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to respond to pings.</p> <p>Select tcp to have the UAG regularly perform a TCP handshake with the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to accept the TCP connection.</p>
Check Port	This field displays when you set the Check Method to tcp . Specify the port number to use for a TCP connectivity check.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures allowed before the UAG disconnects the VPN tunnel. The UAG resumes using the first peer gateway address when the VPN connection passes the connectivity check.
Check this Address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check the First and Last IP Address in the Remote Policy	Select this to have the UAG check the connection to the first and last IP addresses in the connection's remote policy. Make sure one of these is the peer gateway's LAN IP address.
Log	Select this to have the UAG generate a log every time it checks this VPN connection.
Inbound/Outbound traffic NAT	
Outbound Traffic	
Source NAT	This translation hides the source address of computers in the local network. It may also be necessary if you want the UAG to route packets from computers outside the local network through the IPsec SA.
Source	Select the address object that represents the original source address (or select Create new Object to configure a new one). This is the address object for the computer or network outside the local network. The size of the original source address range (Source) must be equal to the size of the translated source address range (SNAT).

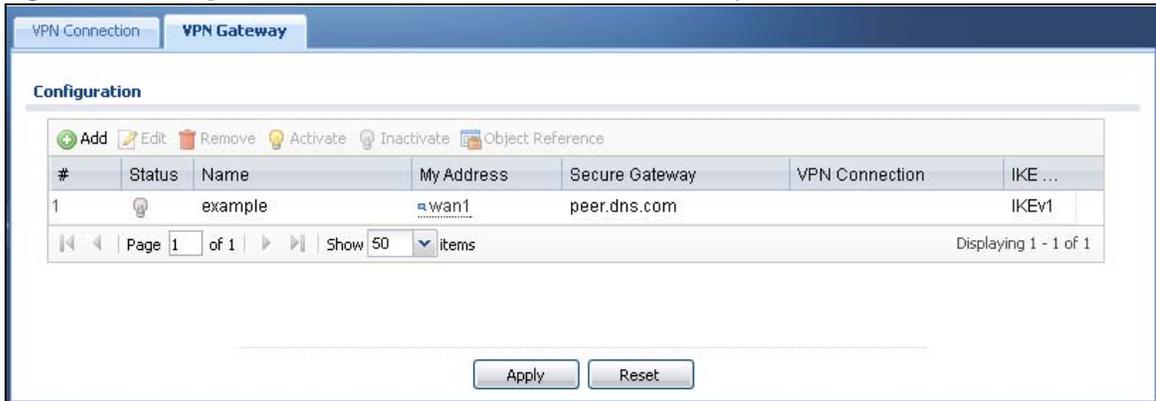
Table 156 Configuration > VPN > IPsec VPN > VPN Connection > Add/Edit (continued)

LABEL	DESCRIPTION
Destination	Select the address object that represents the original destination address (or select Create new Object to configure a new one). This is the address object for the remote network.
SNAT	Select the address object that represents the translated source address (or select Create new Object to configure a new one). This is the address object for the local network. The size of the original source address range (Source) must be equal to the size of the translated source address range (SNAT).
Inbound Traffic	
Source NAT	This translation hides the source address of computers in the remote network.
Source	Select the address object that represents the original source address (or select Create new Object to configure a new one). This is the address object for the remote network. The size of the original source address range (Source) must be equal to the size of the translated source address range (SNAT).
Destination	Select the address object that represents the original destination address (or select Create new Object to configure a new one). This is the address object for the local network.
SNAT	Select the address object that represents the translated source address (or select Create new Object to configure a new one). This is the address that hides the original source address. The size of the original source address range (Source) must be equal to the size of the translated source address range (SNAT).
Destination NAT	This translation forwards packets (for example, mail) from the remote network to a specific computer (for example, the mail server) in the local network.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Move	To change an entry's position in the numbered list, select it and click Move to display a field to type a number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed.
#	This field is a sequential value, and it is not associated with a specific NAT record. However, the order of records is the sequence in which conditions are checked and executed.
Original IP	Select the address object that represents the original destination address. This is the address object for the remote network.
Mapped IP	Select the address object that represents the desired destination address. For example, this is the address object for the mail server.
Protocol	Select the protocol required to use this translation. Choices are: TCP , UDP , or All .
Original Port Start / Original Port End	These fields are available if the protocol is TCP or UDP . Enter the original destination port or range of original destination ports. The size of the original port range must be the same size as the size of the mapped port range.
Mapped Port Start / Mapped Port End	These fields are available if the protocol is TCP or UDP . Enter the translated destination port or range of translated destination ports. The size of the original port range must be the same size as the size of the mapped port range.
OK	Click OK to save the changes.
Cancel	Click Cancel to discard all changes and return to the main VPN screen.

30.3 The VPN Gateway Screen

The **VPN Gateway** summary screen displays the IPsec VPN gateway policies in the UAG, as well as the UAG's address, remote IPsec router's address, and associated VPN connections for each one. In addition, it also lets you activate and deactivate each VPN gateway. To access this screen, click **Configuration > VPN > IPsec VPN > VPN Gateway**. The following screen appears.

Figure 243 Configuration > VPN > IPsec VPN > VPN Gateway



Each field is discussed in the following table. See [Section 30.3.1 on page 348](#) for more information.

Table 157 Configuration > VPN > IPsec VPN > VPN Gateway

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
Object Reference	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 10.3.2 on page 165 for an example.
#	This field is a sequential value, and it is not associated with a specific VPN gateway.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the VPN gateway
My Address	This field displays the interface or a domain name the UAG uses for the VPN gateway.
Secure Gateway	This field displays the IP address(es) of the remote IPsec routers.
VPN Connection	This field displays VPN connections that use this VPN gateway.
IKE Version	This field displays what IKE version the associated VPN gateway(s) is using.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

30.3.1 The VPN Gateway Add/Edit Screen

The **VPN Gateway Add/Edit** screen allows you to create a new VPN gateway policy or edit an existing one. To access this screen, go to the **VPN Gateway summary** screen (see [Section 30.3 on page 347](#)), and either click the **Add** icon or select an entry and click the **Edit** icon.

Figure 244 Configuration > VPN > IPsec VPN > VPN Gateway > Add/Edit

Add VPN Gateway
? X

Hide Advanced Settings
Create new Object ▾

General Settings

Enable

VPN Gateway Name: !

Gateway Settings

My Address

Interface wan1 ▾ DHCP client -- 0.0.0.0/0.0.0.0

Domain Name / IPv4

Peer Gateway Address

Static Address:

Primary

Secondary

Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: (60-86400 seconds)

Authentication

Pre-Shared Key

unmasked

Certificate default ▾ (See [My Certificates](#))

User Based PSK admin ▾ !

Local ID Type: EMAIL

Content: uag5100_CC5D4E63D454

Peer ID Type: Any ▾

Content:

Phase 1 Settings

SA Life Time: (180 - 3000000 Seconds)

Negotiation Mode: Aggressive ▾

Proposal

+ Add
🔍 Edit
🗑 Remove

#	Encryption ▾	Authenticat...
1	DES	MD5

Key Group: DH1 ▾

NAT Traversal

Dead Peer Detection (DPD)

X-Auth

Enable Extended Authentication

Server Mode default ▾

Client Mode

User Name : !

Password: !

Retype to Confirm: !

Apply
Reset
OK
Cancel

Each field is described in the following table.

Table 158 Configuration > VPN > IPsec VPN > VPN Gateway > Add/Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
General Settings	
Enable	Select this check box to activate this VPN gateway policy.
VPN Gateway Name	Type the name used to identify this VPN gateway. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Gateway Settings	
My Address	<p>Select how the IP address of the UAG in the IKE SA is defined.</p> <p>If you select Interface, select the Ethernet interface, VLAN interface, virtual Ethernet interface, virtual VLAN interface or PPPoE/PPTP interface. The IP address of the UAG in the IKE SA is the IP address of the interface.</p> <p>If you select Domain Name / IPv4, enter the domain name or the IP address of the UAG. The IP address of the UAG in the IKE SA is the specified IP address or the IP address corresponding to the domain name. 0.0.0.0 is not generally recommended as it has the UAG accept IPsec requests destined for any interface address on the UAG.</p>
Peer Gateway Address	<p>Select how the IP address of the remote IPsec router in the IKE SA is defined.</p> <p>Select Static Address to enter the domain name or the IP address of the remote IPsec router. You can provide a second IP address or domain name for the UAG to try if it cannot establish an IKE SA with the first one.</p> <p>Fall back to Primary Peer Gateway when possible: When you select this, if the connection to the primary address goes down and the UAG changes to using the secondary connection, the UAG will reconnect to the primary address when it becomes available again and stop using the secondary connection. Users will lose their VPN connection briefly while the UAG changes back to the primary connection. To use this, the peer device at the secondary address cannot be set to use a nailed-up VPN connection. In the Fall Back Check Interval field, set how often to check if the primary address is available.</p>
Authentication	<p>Note: The UAG and remote IPsec router must use the same authentication method to establish the IKE SA.</p>
Pre-Shared Key	<p>Select this to have the UAG and remote IPsec router use a pre-shared key (password) to identify each other when they negotiate the IKE SA. Type the pre-shared key in the field to the right. The pre-shared key can be:</p> <ul style="list-style-type: none"> • alphanumeric characters or , ; . ` ~ ! @ # \$ % ^ & * () _ + \ { } ' : . / < > = - " • pairs of hexadecimal (0-9, A-F) characters, preceded by "0x". <p>Type "0x" at the beginning of a hexadecimal key. For example, "0x0123456789ABCDEF" is in hexadecimal format; "0123456789ABCDEF" is in ASCII format. If you use hexadecimal, you must enter twice as many characters since you need to enter pairs.</p> <p>The UAG and remote IPsec router must use the same pre-shared key.</p>
unmasked	<p>Select this option to see the pre-shared key in readable plain text.</p> <p>De-select this option to not display the real key (password) and instead show a sequence of dots.</p>

Table 158 Configuration > VPN > IPsec VPN > VPN Gateway > Add/Edit (continued)

LABEL	DESCRIPTION
Certificate	<p>Select this to have the UAG and remote IPsec router use certificates to authenticate each other when they negotiate the IKE SA. Then select the certificate the UAG uses to identify itself to the remote IPsec router.</p> <p>This certificate is one of the certificates in My Certificates. If this certificate is self-signed, import it into the remote IPsec router. If this certificate is signed by a CA, the remote IPsec router must trust that CA.</p> <p>Note: The IPsec routers must trust each other's certificates.</p> <p>The UAG uses one of its Trusted Certificates to authenticate the remote IPsec router's certificate. The trusted certificate can be a self-signed certificate or that of a trusted CA that signed the remote IPsec router's certificate.</p>
User Based PSK	<p>User-based PSK (IKEv1 only) generates and manages separate pre-shared keys for every user. This enables multiple users, each with a unique key, to access the same VPN gateway policy with one-to-one authentication and strong encryption. Access can be denied on a per-user basis thus allowing VPN SA user-based policies. Click User Based PSK then select a user or group object who is allowed VPN SA access using this VPN gateway policy. This is for IKEv1 only.</p>
Local ID Type	<p>This field is read-only if the UAG and remote IPsec router use certificates to identify each other. Select which type of identification is used to identify the UAG during authentication. Choices are:</p> <p>IPv4 - the UAG is identified by an IP address</p> <p>DNS - the UAG is identified by a domain name</p> <p>E-mail - the UAG is identified by the string specified in this field</p>
Content	<p>This field is read-only if the UAG and remote IPsec router use certificates to identify each other. Type the identity of the UAG during authentication. The identity depends on the Local ID Type.</p> <p>IPv4 - type an IP address; if you type 0.0.0.0, the UAG uses the IP address specified in the My Address field. This is not recommended in the following situations:</p> <ul style="list-style-type: none"> • There is a NAT router between the UAG and remote IPsec router. • You want the remote IPsec router to be able to distinguish between IPsec SA requests that come from IPsec routers with dynamic WAN IP addresses. <p>In these situations, use a different IP address, or use a different Local ID Type.</p> <p>DNS - type the domain name; you can use up to 63 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string.</p> <p>E-mail - the UAG is identified by the string you specify here; you can use up to 63 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string.</p>
Peer ID Type	<p>Select which type of identification is used to identify the remote IPsec router during authentication. Choices are:</p> <p>IPv4 - the remote IPsec router is identified by an IP address</p> <p>DNS - the remote IPsec router is identified by a domain name</p> <p>E-mail - the remote IPsec router is identified by the string specified in this field</p> <p>Any - the UAG does not check the identity of the remote IPsec router</p> <p>If the UAG and remote IPsec router use certificates, there is one more choice.</p> <p>Subject Name - the remote IPsec router is identified by the subject name in the certificate</p>

Table 158 Configuration > VPN > IPsec VPN > VPN Gateway > Add/Edit (continued)

LABEL	DESCRIPTION
Content	<p>This field is disabled if the Peer ID Type is Any. Type the identity of the remote IPsec router during authentication. The identity depends on the Peer ID Type.</p> <p>If the UAG and remote IPsec router do not use certificates,</p> <p>IPv4 - type an IP address; see the note at the end of this description.</p> <p>DNS - type the domain name; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string.</p> <p>E-mail - the remote IPsec router is identified by the string you specify here; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string.</p> <p>If the UAG and remote IPsec router use certificates, type the following fields from the certificate used by the remote IPsec router.</p> <p>IPv4 - subject alternative name field; see the note at the end of this description.</p> <p>DNS - subject alternative name field</p> <p>E-mail - subject alternative name field</p> <p>Subject Name - subject name (maximum 255 ASCII characters, including spaces)</p> <p>Note: If Peer ID Type is IPv4, please read the rest of this section.</p> <p>If you type 0.0.0.0, the UAG uses the IP address specified in the Secure Gateway Address field. This is not recommended in the following situations:</p> <ul style="list-style-type: none"> • There is a NAT router between the UAG and remote IPsec router. • You want the remote IPsec router to be able to distinguish between IPsec SA requests that come from IPsec routers with dynamic WAN IP addresses. <p>In these situations, use a different IP address, or use a different Peer ID Type.</p>
Phase 1 Settings	
SA Life Time (Seconds)	Type the maximum number of seconds the IKE SA can last. When this time has passed, the UAG and remote IPsec router have to update the encryption and authentication keys and re-negotiate the IKE SA. This does not affect any existing IPsec SAs, however.
Negotiation Mode	<p>Select the negotiation mode to use to negotiate the IKE SA. Choices are</p> <p>Main - this encrypts the UAG's and remote IPsec router's identities but takes more time to establish the IKE SA</p> <p>Aggressive - this is faster but does not encrypt the identities</p> <p>The UAG and the remote IPsec router must use the same negotiation mode.</p>
Proposal	Use this section to manage the encryption algorithm and authentication algorithm pairs the UAG accepts from the remote IPsec router for negotiating the IKE SA.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific proposal. The sequence of proposals should not affect performance significantly.

Table 158 Configuration > VPN > IPsec VPN > VPN Gateway > Add/Edit (continued)

LABEL	DESCRIPTION
Encryption	<p>Select which key size and encryption algorithm to use in the IKE SA. Choices are:</p> <p>DES - a 56-bit key with the DES encryption algorithm</p> <p>3DES - a 168-bit key with the DES encryption algorithm</p> <p>AES128 - a 128-bit key with the AES encryption algorithm</p> <p>AES192 - a 192-bit key with the AES encryption algorithm</p> <p>AES256 - a 256-bit key with the AES encryption algorithm</p> <p>The UAG and the remote IPsec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput.</p>
Authentication	<p>Select which hash algorithm to use to authenticate packet data in the IPsec SA. Choices are SHA1, SHA256, SHA512 and MD5. SHA is generally considered stronger than MD5, but it is also slower.</p> <p>The remote IPsec router must use the same authentication algorithm.</p>
Key Group	<p>Select which Diffie-Hellman key group (DHx) you want to use for encryption keys. Choices are:</p> <p>DH1 - use a 768-bit random number</p> <p>DH2 - use a 1024-bit random number</p> <p>DH5 - use a 1536-bit random number</p> <p>The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.</p>
NAT Traversal	<p>Select this if any of these conditions are satisfied.</p> <ul style="list-style-type: none"> • This IKE SA might be used to negotiate IPsec SAs that use ESP as the active protocol. • There are one or more NAT routers between the UAG and remote IPsec router, and these routers do not support IPsec pass-thru or a similar feature. <p>The remote IPsec router must also enable NAT traversal, and the NAT routers have to forward packets with UDP port 500 and UDP 4500 headers unchanged.</p>
Dead Peer Detection (DPD)	<p>Select this check box if you want the UAG to make sure the remote IPsec router is there before it transmits data through the IKE SA. The remote IPsec router must support DPD. If there has been no traffic for at least 15 seconds, the UAG sends a message to the remote IPsec router. If the remote IPsec router responds, the UAG transmits the data. If the remote IPsec router does not respond, the UAG shuts down the IKE SA.</p> <p>If the remote IPsec router does not support DPD, see if you can use the VPN connection connectivity check (see Section 30.2.1 on page 341).</p>
X-Auth	<p>When multiple IPsec routers use the same VPN tunnel to connect to a single VPN tunnel (telecommuters sharing a tunnel for example), use extended authentication to enforce a user name and password check. This way even though they all know the VPN tunnel's security settings, each still has to provide a unique user name and password.</p>
Enable Extended Authentication	<p>Select this if one of the routers (the UAG or the remote IPsec router) verifies a user name and password from the other router using the local user database and/or an external server.</p>
Server Mode	<p>Select this if the UAG authenticates the user name and password from the remote IPsec router. You also have to select the authentication method, which specifies how the UAG authenticates this information.</p>
Client Mode	<p>Select this radio button if the UAG provides a username and password to the remote IPsec router for authentication. You also have to provide the User Name and the Password.</p>

Table 158 Configuration > VPN > IPsec VPN > VPN Gateway > Add/Edit (continued)

LABEL	DESCRIPTION
User Name	This field is required if the UAG is in Client Mode for extended authentication. Type the user name the UAG sends to the remote IPsec router. The user name can be 1-31 ASCII characters. It is case-sensitive, but spaces are not allowed.
Password	This field is required if the UAG is in Client Mode for extended authentication. Type the password the UAG sends to the remote IPsec router. The password can be 1-31 ASCII characters. It is case-sensitive, but spaces are not allowed.
Retype to Confirm	Type the password again here to confirm it.
OK	Click OK to save your settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

30.4 IPsec VPN Background Information

Here is some more detailed IPsec VPN background information.

IKE SA Overview

The IKE SA provides a secure connection between the UAG and remote IPsec router.

It takes several steps to establish an IKE SA. The negotiation mode determines how many. There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Note: Both routers must use the same negotiation mode.

These modes are discussed in more detail in [Negotiation Mode on page 357](#). Main mode is used in various examples in the rest of this section.

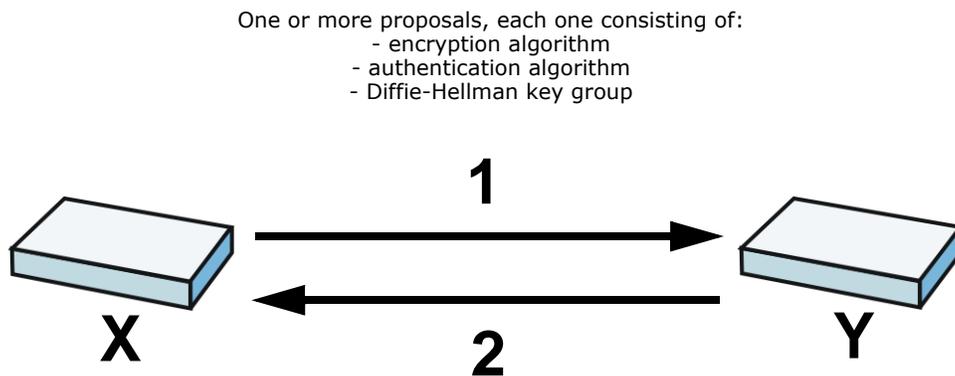
IP Addresses of the UAG and Remote IPsec Router

To set up an IKE SA, you have to specify the IP addresses of the UAG and remote IPsec router. You can usually enter a static IP address or a domain name for either or both IP addresses. Sometimes, your UAG might offer another alternative, such as using the IP address of a port or interface, as well.

You can also specify the IP address of the remote IPsec router as 0.0.0.0. This means that the remote IPsec router can have any IP address. In this case, only the remote IPsec router can initiate an IKE SA because the UAG does not know the IP address of the remote IPsec router. This is often used for telecommuters.

IKE SA Proposal

The IKE SA proposal is used to identify the encryption algorithm, authentication algorithm, and Diffie-Hellman (DH) key group that the UAG and remote IPsec router use in the IKE SA. In main mode, this is done in steps 1 and 2, as illustrated next.

Figure 245 IKE SA: Main Negotiation Mode, Steps 1 - 2: IKE SA Proposal

The UAG sends one or more proposals to the remote IPsec router. (In some devices, you can only set up one proposal.) Each proposal consists of an encryption algorithm, authentication algorithm, and DH key group that the UAG wants to use in the IKE SA. The remote IPsec router selects an acceptable proposal and sends the accepted proposal back to the UAG. If the remote IPsec router rejects all of the proposals, the UAG and remote IPsec router cannot establish an IKE SA.

Note: Both routers must use the same encryption algorithm, authentication algorithm, and DH key group.

In most UAGs, you can select one of the following encryption algorithms for each proposal. The algorithms are listed in order from weakest to strongest.

- Data Encryption Standard (DES) is a widely used method of data encryption. It applies a 56-bit key to each 64-bit block of data.
- Triple DES (3DES) is a variant of DES. It iterates three times with three separate keys, effectively tripling the strength of DES.
- Advanced Encryption Standard (AES) is a newer method of data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data. It is faster than 3DES.

Some UAGs also offer stronger forms of AES that apply 192-bit or 256-bit keys to 128-bit blocks of data.

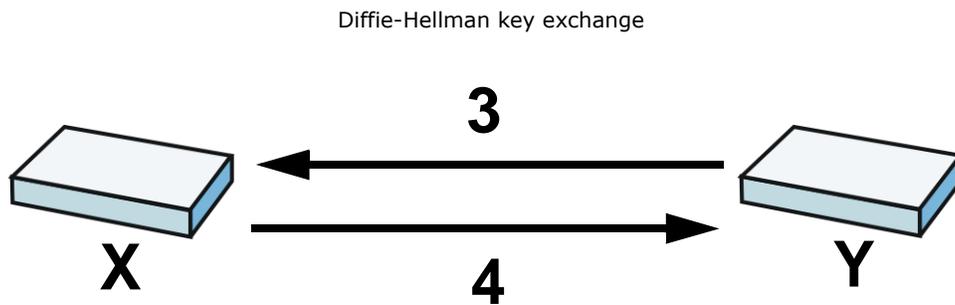
In most UAGs, you can select one of the following authentication algorithms for each proposal. The algorithms are listed in order from weakest to strongest.

- MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
- SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
- SHA256 (Secure Hash Algorithm) produces a 256-bit digest to authenticate packet data.
- SHA512 (Secure Hash Algorithm) produces a 512-bit digest to authenticate packet data.

See [Diffie-Hellman \(DH\) Key Exchange on page 355](#) for more information about DH key groups.

Diffie-Hellman (DH) Key Exchange

The UAG and the remote IPsec router use DH public-key cryptography to establish a shared secret. The shared secret is then used to generate encryption keys for the IKE SA and IPsec SA. In main mode, this is done in steps 3 and 4, as illustrated next.

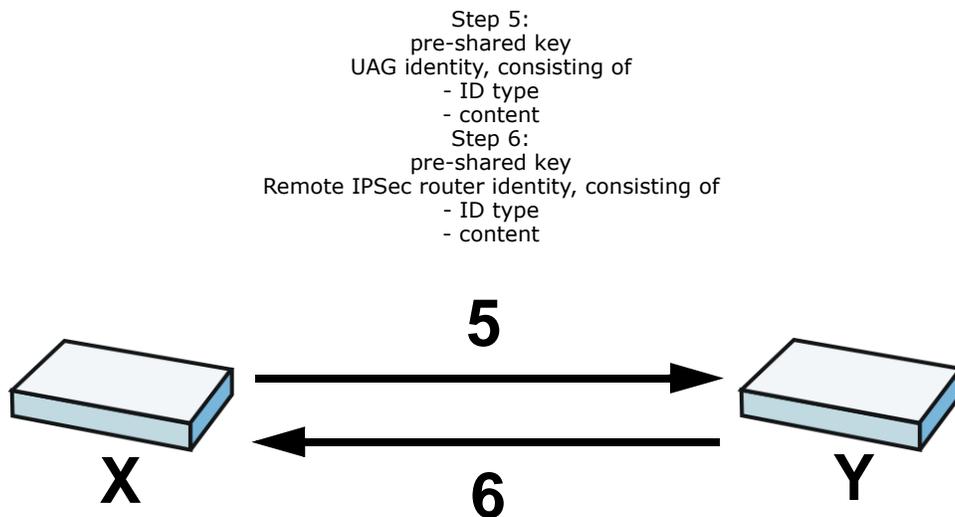
Figure 246 IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange

DH public-key cryptography is based on DH key groups. Each key group is a fixed number of bits long. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. For example, DH2 keys (1024 bits) are more secure than DH1 keys (768 bits), but DH2 keys take longer to encrypt and decrypt.

Authentication

Before the UAG and remote IPsec router establish an IKE SA, they have to verify each other's identity. This process is based on pre-shared keys and router identities.

In main mode, the UAG and remote IPsec router authenticate each other in steps 5 and 6, as illustrated below. The identities are also encrypted using the encryption algorithm and encryption key the UAG and remote IPsec router selected in previous steps.

Figure 247 IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication (continued)

You have to create (and distribute) a pre-shared key. The UAG and remote IPsec router use it in the authentication process, though it is not actually transmitted or exchanged.

Note: The UAG and the remote IPsec router must use the same pre-shared key.

Router identity consists of ID type and content. The ID type can be domain name, IP address, or e-mail address, and the content is a (properly-formatted) domain name, IP address, or e-mail address. The content is only used for identification. Any domain name or e-mail address that you

enter does not have to actually exist. Similarly, any domain name or IP address that you enter does not have to correspond to the UAG's or remote IPsec router's properties.

The UAG and the remote IPsec router have their own identities, so both of them must store two sets of information, one for themselves and one for the other router. Local ID type and content refers to the ID type and content that applies to the router itself, and peer ID type and content refers to the ID type and content that applies to the other router.

Note: The UAG's local and peer ID type and content must match the remote IPsec router's peer and local ID type and content, respectively.

For example, in [Table 159 on page 357](#), the UAG and the remote IPsec router authenticate each other successfully. In contrast, in [Table 160 on page 357](#), the UAG and the remote IPsec router cannot authenticate each other and, therefore, cannot establish an IKE SA.

Table 159 VPN Example: Matching ID Type and Content

UAG	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

Table 160 VPN Example: Mismatching ID Type and Content

UAG	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.20	Peer ID content: tom@yourcompany.com

It is also possible to configure the UAG to ignore the identity of the remote IPsec router. In this case, you usually set the peer ID type to **Any**. This is less secure, so you should only use this if your UAG provides another way to check the identity of the remote IPsec router (for example, extended authentication) or if you are troubleshooting a VPN tunnel.

Additional Topics for IKE SA

This section provides more information about IKE SA.

Negotiation Mode

There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Main mode takes six steps to establish an IKE SA.

Steps 1 - 2: The UAG sends its proposals to the remote IPsec router. The remote IPsec router selects an acceptable proposal and sends it back to the UAG.

Steps 3 - 4: The UAG and the remote IPsec router exchange pre-shared keys for authentication and participate in a Diffie-Hellman key exchange, based on the accepted DH key group, to establish a shared secret.

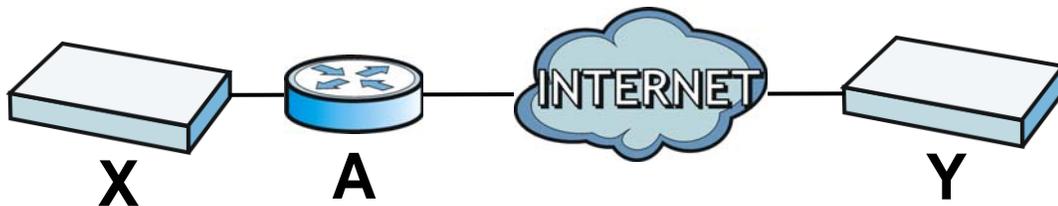
Steps 5 - 6: Finally, the UAG and the remote IPSec router generate an encryption key (from the shared secret), encrypt their identities, and exchange their encrypted identity information for authentication.

In contrast, aggressive mode only takes three steps to establish an IKE SA. Aggressive mode does not provide as much security because the identity of the UAG and the identity of the remote IPSec router are not encrypted. It is usually used in remote-access situations, where the address of the initiator is not known by the responder and both parties want to use pre-shared keys for authentication. For example, the remote IPSec router may be a telecommuter who does not have a static IP address.

VPN, NAT, and NAT Traversal

In the following example, there is another router (**A**) between router **X** and router **Y**.

Figure 248 VPN/NAT Example



If router **A** does NAT, it might change the IP addresses, port numbers, or both. If router **X** and router **Y** try to establish a VPN tunnel, the authentication fails because it depends on this information. The routers cannot establish a VPN tunnel.

Most routers like router **A** now have an IPSec pass-thru feature. This feature helps router **A** recognize VPN packets and route them appropriately. If router **A** has this feature, router **X** and router **Y** can establish a VPN tunnel as long as the active protocol is ESP. (See [Active Protocol on page 359](#) for more information about active protocols.)

If router **A** does not have an IPSec pass-thru or if the active protocol is AH, you can solve this problem by enabling NAT traversal. In NAT traversal, router **X** and router **Y** add an extra header to the IKE SA and IPSec SA packets. If you configure router **A** to forward these packets unchanged, router **X** and router **Y** can establish a VPN tunnel.

You have to do the following things to set up NAT traversal.

- Enable NAT traversal on the UAG and remote IPSec router.
- Configure the NAT router to forward packets with the extra header unchanged. (See the field description for detailed information about the extra header.)

The extra header may be UDP port 500 or UDP port 4500, depending on the standard(s) the UAG and remote IPSec router support.

Extended Authentication

Extended authentication is often used when multiple IPSec routers use the same VPN tunnel to connect to a single IPSec router. For example, this might be used with telecommuters.

In extended authentication, one of the routers (the UAG or the remote IPSec router) provides a user name and password to the other router, which uses a local user database and/or an external server to verify the user name and password. If the user name or password is wrong, the routers do not establish an IKE SA.

You can set up the UAG to provide a user name and password to the remote IPSec router, or you can set up the UAG to check a user name and password that is provided by the remote IPSec router.

If you use extended authentication, it takes four more steps to establish an IKE SA. These steps occur at the end, regardless of the negotiation mode (steps 7-10 in main mode, steps 4-7 in aggressive mode).

Certificates

It is possible for the UAG and remote IPSec router to authenticate each other with certificates. In this case, you do not have to set up the pre-shared key, local identity, or remote identity because the certificates provide this information instead.

- Instead of using the pre-shared key, the UAG and remote IPSec router check the signatures on each other's certificates. Unlike pre-shared keys, the signatures do not have to match.
- The local and peer ID type and content come from the certificates.

Note: You must set up the certificates for the UAG and remote IPSec router first.

IPSec SA Overview

Once the UAG and remote IPSec router have established the IKE SA, they can securely negotiate an IPSec SA through which to send data between computers on the networks.

Note: The IPSec SA stays connected even if the underlying IKE SA is not available anymore.

This section introduces the key components of an IPSec SA.

Local Network and Remote Network

In an IPSec SA, the local network, the one(s) connected to the UAG, may be called the local policy. Similarly, the remote network, the one(s) connected to the remote IPSec router, may be called the remote policy.

Active Protocol

The active protocol controls the format of each packet. It also specifies how much of each packet is protected by the encryption and authentication algorithms. IPSec VPN includes two active protocols, AH (Authentication Header, RFC 2402) and ESP (Encapsulating Security Payload, RFC 2406).

Note: The UAG and remote IPSec router must use the same active protocol.

Usually, you should select ESP. AH does not support encryption, and ESP is more suitable with NAT.

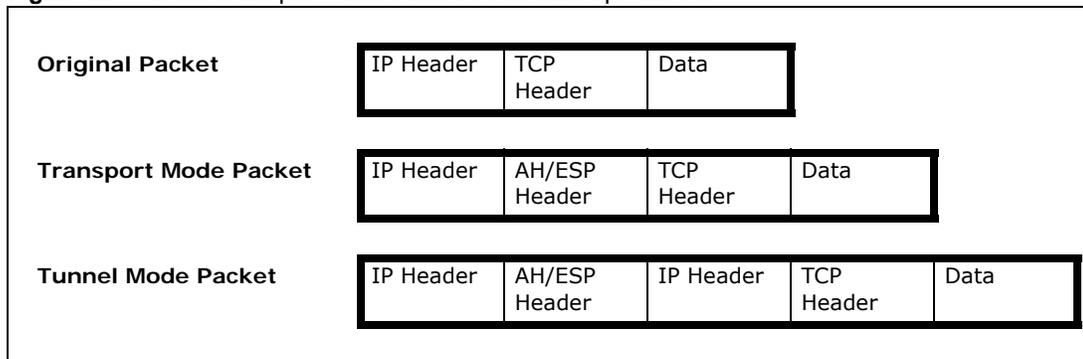
Encapsulation

There are two ways to encapsulate packets. Usually, you should use tunnel mode because it is more secure. Transport mode is only used when the IPSec SA is used for communication between the UAG and remote IPSec router (for example, for remote management), not between computers on the local and remote networks.

Note: The UAG and remote IPSec router must use the same encapsulation.

These modes are illustrated below.

Figure 249 VPN: Transport and Tunnel Mode Encapsulation



In tunnel mode, the UAG uses the active protocol to encapsulate the entire IP packet. As a result, there are two IP headers:

- **Outside header:** The outside IP header contains the IP address of the UAG or remote IPSec router, whichever is the destination.
- **Inside header:** The inside IP header contains the IP address of the computer behind the UAG or remote IPSec router. The header for the active protocol (AH or ESP) appears between the IP headers.

In transport mode, the encapsulation depends on the active protocol. With AH, the UAG includes part of the original IP header when it encapsulates the packet. With ESP, however, the UAG does not include the IP header when it encapsulates the packet, so it is not possible to verify the integrity of the source IP address.

IPSec SA Proposal and Perfect Forward Secrecy

An IPSec SA proposal is similar to an IKE SA proposal (see [IKE SA Proposal on page 354](#)), except that you also have the choice whether or not the UAG and remote IPSec router perform a new DH key exchange every time an IPSec SA is established. This is called Perfect Forward Secrecy (PFS).

If you enable PFS, the UAG and remote IPSec router perform a DH key exchange every time an IPSec SA is established, changing the root key from which encryption keys are generated. As a result, if one encryption key is compromised, other encryption keys remain secure.

If you do not enable PFS, the UAG and remote IPSec router use the same root key that was generated when the IKE SA was established to generate encryption keys.

The DH key exchange is time-consuming and may be unnecessary for data that does not require such security.

Additional Topics for IPsec SA

This section provides more information about IPsec SA in your UAG.

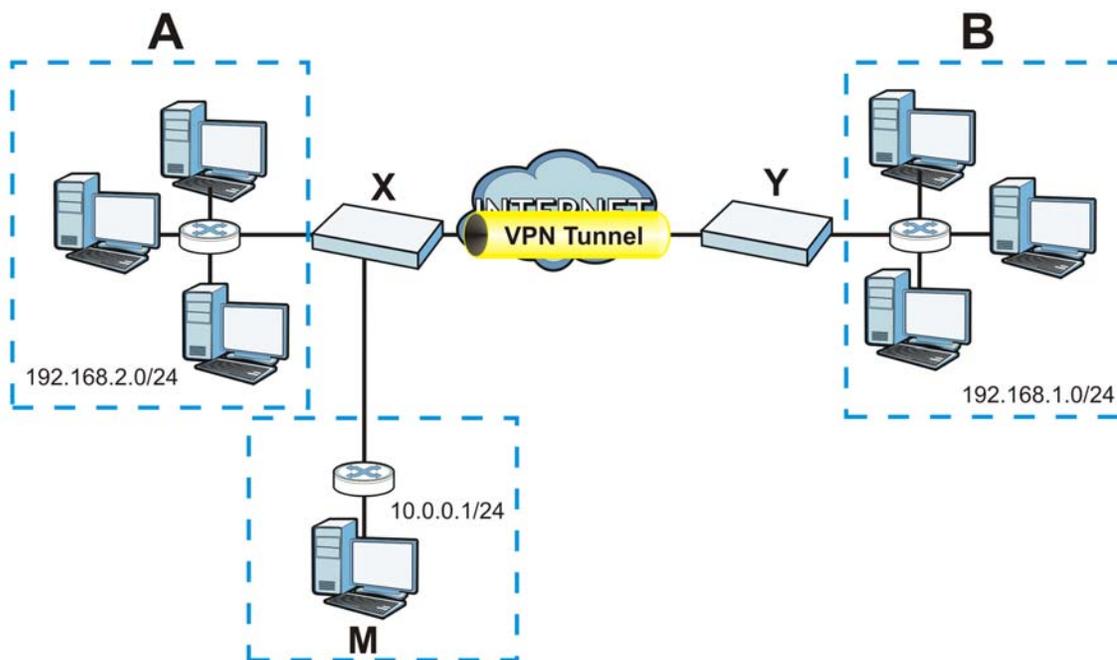
NAT for Inbound and Outbound Traffic

The UAG can translate the following types of network addresses in IPsec SA.

- Source address in outbound packets - this translation is necessary if you want the UAG to route packets from computers outside the local network through the IPsec SA.
- Source address in inbound packets - this translation hides the source address of computers in the remote network.
- Destination address in inbound packets - this translation is used if you want to forward packets (for example, mail) from the remote network to a specific computer (like the mail server) in the local network.

Each kind of translation is explained below. The following example is used to help explain each one.

Figure 250 VPN Example: NAT for Inbound and Outbound Traffic



Source Address in Outbound Packets (Outbound Traffic, Source NAT)

This translation lets the UAG route packets from computers that are not part of the specified local network (local policy) through the IPsec SA. For example, in [Figure 250 on page 361](#), you have to configure this kind of translation if you want computer **M** to establish a connection with any computer in the remote network (**B**). If you do not configure it, the remote IPsec router may not route messages for computer **M** through the IPsec SA because computer **M**'s IP address is not part of its local policy.

To set up this NAT, you have to specify the following information:

- Source - the original source address; most likely, computer **M**'s network.

- Destination - the original destination address; the remote network (**B**).
- SNAT - the translated source address; the local network (**A**).

Source Address in Inbound Packets (Inbound Traffic, Source NAT)

You can set up this translation if you want to change the source address of computers in the remote network. To set up this NAT, you have to specify the following information:

- Source - the original source address; the remote network (**B**).
- Destination - the original destination address; the local network (**A**).
- SNAT - the translated source address; a different IP address (range of addresses) to hide the original source address.

Destination Address in Inbound Packets (Inbound Traffic, Destination NAT)

You can set up this translation if you want the UAG to forward some packets from the remote network to a specific computer in the local network. For example, in [Figure 250 on page 361](#), you can configure this kind of translation if you want to forward mail from the remote network to the mail server in the local network (**A**).

You have to specify one or more rules when you set up this kind of NAT. The UAG checks these rules similar to the way it checks security policies. The first part of these rules define the conditions in which the rule apply.

- Original IP - the original destination address; the remote network (**B**).
- Protocol - the protocol [TCP, UDP, or both] used by the service requesting the connection.
- Original Port - the original destination port or range of destination ports; in [Figure 250 on page 361](#), it might be port 25 for SMTP.

The second part of these rules controls the translation when the condition is satisfied.

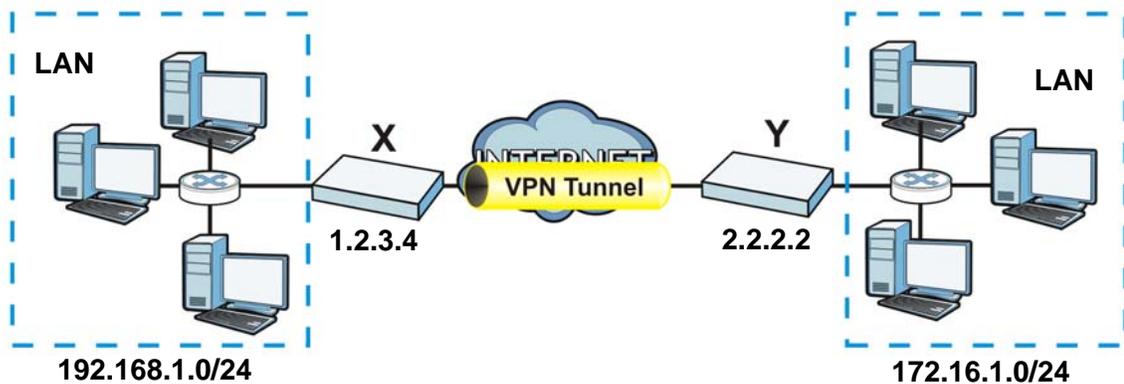
- Mapped IP - the translated destination address; in [Figure 250 on page 361](#), the IP address of the mail server in the local network (**A**).
- Mapped Port - the translated destination port or range of destination ports.

The original port range and the mapped port range must be the same size.

IPsec VPN Example

Here is an example of configuring a site-to-site IPsec VPN.

Figure 251 IPsec VPN Example



UAG X uses 1.2.3.4 as its public address, and remote IPsec router Y uses 2.2.2.2. Create the VPN tunnel between the UAG's LAN subnet (192.168.1.0/24) and the LAN subnet behind the peer IPsec router (172.16.1.0/24).

Set Up the VPN Gateway that Manages the IKE SA

In **Configuration > VPN > IPsec VPN > VPN Gateway > Add**, enable the VPN gateway and name it (VPN_GW_EXAMPLE here). Set **My Address** to **Interface** and select a WAN interface. Set **Peer Gateway Address** to **Static Address** and enter the remote IPsec router's public IP address (2.2.2.2 here) as the **Primary**. Set **Authentication** to **Pre-Shared Key** and enter 12345678. Click **OK**.

Add VPN Gateway

Show Advanced Settings

General Settings

Enable

VPN Gateway Name:

Gateway Settings

My Address

Interface Static -- 1.2.3.4/255.255.0.0

Domain Name / IP

Peer Gateway Address

Static Address

Primary

Secondary

Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: (60-86400 seconds)

Dynamic Address

Authentication

Pre-Shared Key

Certificate (See My Certificates)

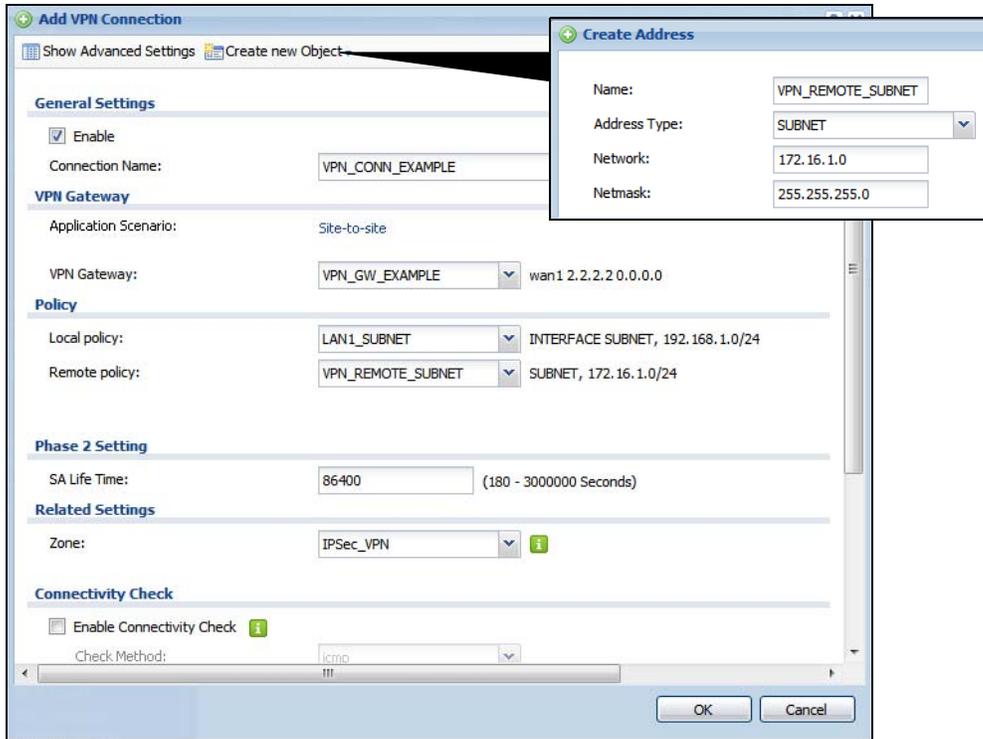
Phase 1 Settings

SA Life Time: (180 - 3000000 Seconds)

OK Cancel

Set Up the VPN Connection that Manages the IPsec SA

- 1 In **Configuration > VPN > IPsec VPN > VPN Connection > Add**, click **Create New Object > Address** to create an address object for the remote network. Set the **Address Type** to **SUBNET**, the **Network** field to 172.16.1.0, and the **Netmask** to 255.255.255.0.
- 2 Enable the VPN connection and name it ("VPN_CONN_EXAMPLE"). Set **VPN Gateway** to **Site-to-site** and select the VPN gateway you configured (**VPN_GW_EXAMPLE**). Set **Local Policy** to **LAN1_SUBNET** and **Remote Policy** to **VPN_REMOTE_SUBNET** for the remote. Click **OK**.



Bandwidth Management

31.1 Overview

Bandwidth management provides a convenient way to manage the use of various services on the network. It manages general protocols (for example, HTTP and FTP) and applies traffic prioritization to enhance the performance of delay-sensitive applications like voice and video.

31.1.1 What You Can Do in this Chapter

Use the **BWM** screens (see [Section 31.2 on page 370](#)) to control bandwidth for services passing through the UAG, and it identifies the conditions that refine this.

31.1.2 What You Need to Know

When you allow a service, you can restrict the bandwidth it uses. It controls TCP and UDP traffic. Use policy routes to manage other types of traffic (like ICMP).

Note: Bandwidth management in policy routes has priority over TCP and UDP traffic policies.

If you want to use a service, make sure both the security policy allow the service's packets to go through the UAG.

Note: The UAG checks security policies before it checks bandwidth management rules for traffic going through the UAG.

Bandwidth management examines every TCP and UDP connection passing through the UAG. Then, you can specify, by port, whether or not the UAG continues to route the connection.

BWM Type

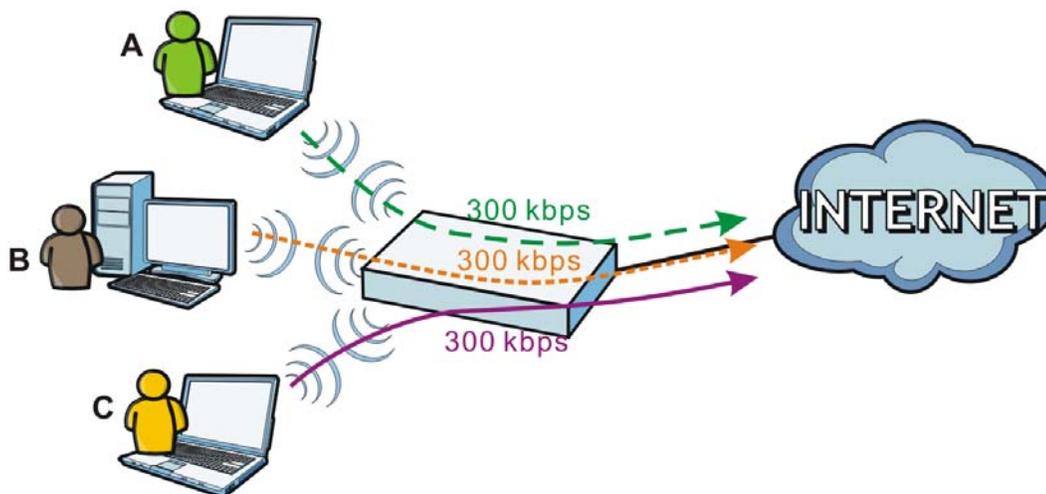
The UAG supports three types of bandwidth management: **Shared**, **Per user** and **Per-Source-IP**.

The **Shared** BWM type is selected by default in a bandwidth management rule. All matched traffic shares the bandwidth configured in the rule.

If the BWM type is set to **Per user** in a rule, each user that matches the rule can use up to the configured bandwidth by his/her own.

Select the **Per-Source-IP** type when you want to set the maximum bandwidth for traffic from an individual source IP address.

In the following example, you configure a **Per user** bandwidth management rule for billing-users to limit outgoing traffic to 300 kbs. Then all billing-users (**A**, **B** and **C**) can send 300 kbps of traffic.



DiffServ and DSCP Marking

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application specific types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

Connection and Packet Directions

Bandwidth management looks at the connection direction, that is from which interface the connection was initiated and to which interface the connection is going.

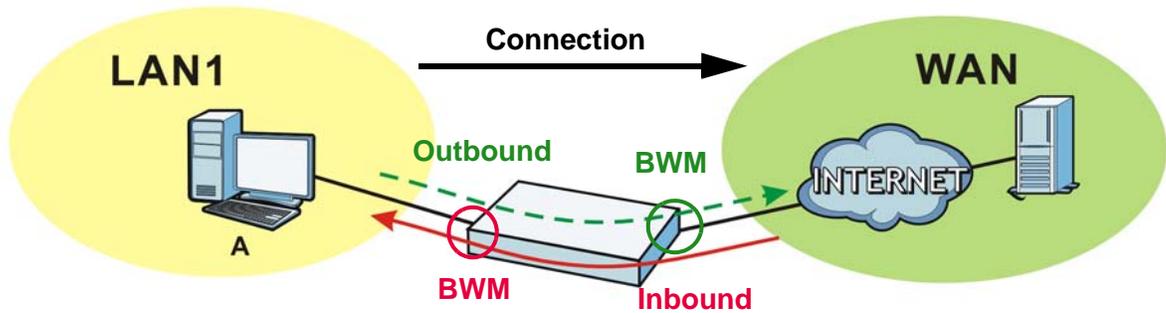
A connection has outbound and inbound packet flows. The UAG controls the bandwidth of traffic of each flow as it is going out through an interface.

- The outbound traffic flows from the connection initiator to the connection responder.
- The inbound traffic flows from the connection responder to the connection initiator.

For example, a LAN1 to WAN connection is initiated from LAN1 and goes to the WAN.

- Outbound traffic goes from a LAN1 device to a WAN device. Bandwidth management is applied before sending the packets out a WAN interface on the UAG.
- Inbound traffic comes back from the WAN device to the LAN1 device. Bandwidth management is applied before sending the traffic out a LAN1 interface.

Figure 252 LAN1 to WAN Connection and Packet Directions

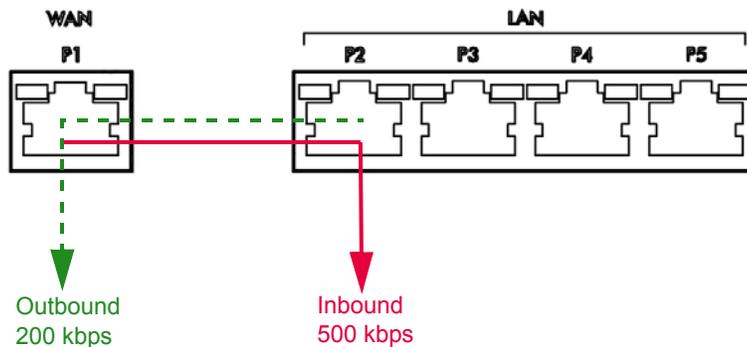


Outbound and Inbound Bandwidth Limits

You can limit an application's outbound or inbound bandwidth. This limit keeps the traffic from using up too much of the out-going interface's bandwidth. This way you can make sure there is bandwidth for other applications. When you apply a bandwidth limit to outbound or inbound traffic, each member of the out-going zone can send up to the limit. Take a LAN1 to WAN policy for example.

- Outbound traffic is limited to 200 kbps. The connection initiator is on the LAN1 so outbound means the traffic traveling from the LAN1 to the WAN. Each of the WAN zone's two interfaces can send the limit of 200 kbps of traffic.
- Inbound traffic is limited to 500 kbps. The connection initiator is on the LAN1 so inbound means the traffic traveling from the WAN to the LAN1.

Figure 253 LAN1 to WAN, Outbound 200 kbps, Inbound 500 kbps



Bandwidth Management Priority

- The UAG gives bandwidth to higher-priority traffic first, until it reaches its configured bandwidth rate.
- Then lower-priority traffic gets bandwidth.
- The UAG uses a fairness-based (round-robin) scheduler to divide bandwidth among traffic flows with the same priority.
- The UAG automatically treats traffic with bandwidth management disabled as priority 7 (the lowest priority).

Maximize Bandwidth Usage

Maximize bandwidth usage allows applications with maximize bandwidth usage enabled to “borrow” any unused bandwidth on the out-going interface.

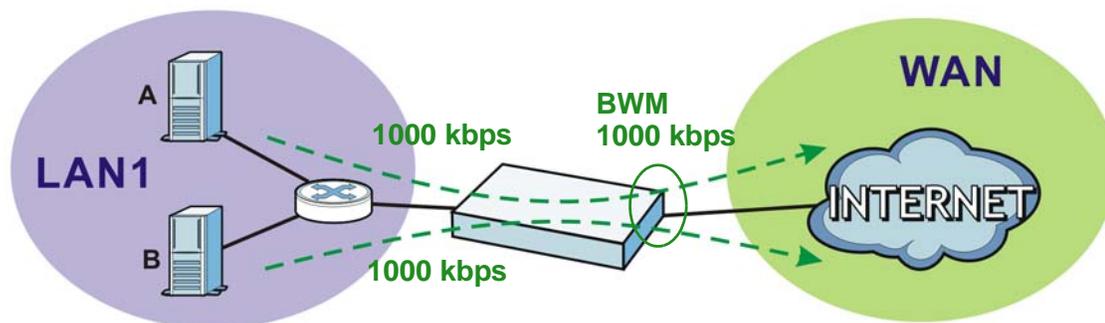
After each application gets its configured bandwidth rate, the UAG uses the fairness- based scheduler to divide any unused bandwidth on the out-going interface amongst applications that need more bandwidth and have maximize bandwidth usage enabled.

Unused bandwidth is divided equally. Higher priority traffic does not get a larger portion of the unused bandwidth.

Bandwidth Management Behavior

The following sections show how bandwidth management behaves with various settings. For example, you configure LAN1 to WAN policies for FTP servers **A** and **B**. Each server tries to send 1000 kbps, but the WAN is set to a maximum outgoing speed of 1000 kbps. You configure policy A for server **A**'s traffic and policy B for server **B**'s traffic.

Figure 254 Bandwidth Management Behavior



Configured Rate Effect

In the following table the configured rates total less than the available bandwidth and maximize bandwidth usage is disabled, both servers get their configured rate.

Table 161 Configured Rate Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	300 kbps	No	1	300 kbps
B	200 kbps	No	1	200 kbps

Priority Effect

Here the configured rates total more than the available bandwidth. Because server **A** has higher priority, it gets up to it's configured rate (800 kbps), leaving only 200 kbps for server **B**.

Table 162 Priority Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	800 kbps	Yes	1	800 kbps
B	1000 kbps	Yes	2	200 kbps

Maximize Bandwidth Usage Effect

With maximize bandwidth usage enabled, after each server gets its configured rate, the rest of the available bandwidth is divided equally between the two. So server **A** gets its configured rate of 300 kbps and server **B** gets its configured rate of 200 kbps. Then the UAG divides the remaining bandwidth ($1000 - 500 = 500$) equally between the two ($500 / 2 = 250$ kbps for each). The priority has no effect on how much of the unused bandwidth each server gets.

So server **A** gets its configured rate of 300 kbps plus 250 kbps for a total of 550 kbps. Server **B** gets its configured rate of 200 kbps plus 250 kbps for a total of 450 kbps.

Table 163 Maximize Bandwidth Usage Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	300 kbps	Yes	1	550 kbps
B	200 kbps	Yes	2	450 kbps

Priority and Over Allotment of Bandwidth Effect

Server **A** has a configured rate that equals the total amount of available bandwidth and a higher priority. You should regard extreme over allotment of traffic with different priorities (as shown here) as a configuration error. Even though the UAG still attempts to let all traffic get through and not be lost, regardless of its priority, server **B** gets almost no bandwidth with this configuration.

Table 164 Priority and Over Allotment of Bandwidth Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	1000 kbps	Yes	1	999 kbps
B	1000 kbps	Yes	2	1 kbps

Finding Out More

- See [DSCP Marking and Per-Hop Behavior on page 205](#) for a description of DSCP marking.

31.2 The Bandwidth Management Screen

The Bandwidth management screens control the bandwidth allocation for TCP and UDP traffic. You can use source interface, destination interface, destination port, schedule, user, source, destination information, DSCP code and service type as criteria to create a sequence of specific conditions, similar to the sequence of security policies, to specify how the UAG handles the DSCP value and allocate bandwidth for the matching packets.

Click **Configuration > BWM** to open the following screen. This screen allows you to enable/disable bandwidth management and add, edit, and remove user-defined bandwidth management policies.

The default bandwidth management policy is the one with the priority of "default". It is the last policy the UAG checks if traffic does not match any other bandwidth management policies you have configured. You cannot remove, activate, deactivate or move the default bandwidth management policy.

Figure 255 Configuration > BWM

The following table describes the labels in this screen. See [Section 31.2.1 on page 372](#) for more information as well.

Table 165 Configuration > BWM

LABEL	DESCRIPTION
Enable BWM	Select this check box to activate management bandwidth.
Enable Highest Bandwidth Priority for SIP Traffic	Select this to maximize the throughput of SIP traffic to improve SIP-based VoIP call sound quality. This has the UAG immediately send SIP traffic upon identifying it. When this option is enabled the UAG ignores any other application patrol rules for SIP traffic (so there is no bandwidth control for SIP traffic) and does not record SIP traffic bandwidth usage statistics.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
Move	To change an entry's position in the numbered list, select it and click Move to display a field to type a number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The status icon is not available for the default bandwidth management policy.
Priority	This is the position of your bandwidth management policy in the list. The ordering of your rules is important as rules are applied in sequence. This field displays default for the default bandwidth management policy that the UAG performs on traffic that does not match any other bandwidth management policy.
Description	This is the descriptive name of the policy.
BWM Type	This is the bandwidth management type of the policy.
User	This is the user name or user group to which the policy applies. If any displays, the policy applies to all users.
Schedule	This is the schedule that defines when the policy applies. none means the policy always applies.

Table 165 Configuration > BWM (continued)

LABEL	DESCRIPTION
Incoming Interface	This is the source interface of the traffic to which this policy applies.
Outgoing Interface	This is the destination interface of the traffic to which this policy applies.
Source	This is the source address or address group for whom this policy applies. If any displays, the policy is effective for every source.
Destination	This is the destination address or address group for whom this policy applies. If any displays, the policy is effective for every destination.
DSCP Code	This is the DSCP value of the incoming or outgoing packets to which this policy applies. any means all DSCP values or no DSCP marker. default means traffic with a DSCP value of 0. This is usually best effort traffic.
Service	This is the service object to which this policy applies. If any displays, the policy is effective for every service.
BWM In/Pri/Out/ Pri	This field shows the amount of bandwidth the traffic can use. In - This is how much inbound bandwidth, in kilobits per second, this policy allows the matching traffic to use. Inbound refers to the traffic the UAG sends to a connection's initiator. If no displays here, this policy does not apply bandwidth management for the inbound traffic. Out - This is how much outgoing bandwidth, in kilobits per second, this policy allows the matching traffic to use. Outbound refers to the traffic the UAG sends out from a connection's initiator. If no displays here, this policy does not apply bandwidth management for the outbound traffic. Pri - This is the priority for the incoming (the first Pri value) or outgoing (the second Pri value) traffic that matches this policy. The smaller the number, the higher the priority. Traffic with a higher priority is given bandwidth before traffic with a lower priority. The UAG ignores this number if the incoming and outgoing limits are both set to 0. In this case the traffic is automatically treated as being set to the lowest priority (7) regardless of this field's configuration.
DSCP Marking	This is how the UAG handles the DSCP value of the incoming and outgoing packets that match this policy. preserve means the UAG does not modify the DSCP value of the route's packets. default means the UAG sets the DSCP value of the route's packets to 0. If this field displays a DSCP value, the UAG applies that DSCP value to the route's packets. The "af" choices stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Section 12.4 on page 212 for more details.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

31.2.1 The Bandwidth Management Add/Edit Screen

The **Configuration > BWM Add/Edit** screen allows you to create a new condition or edit an existing one. To access this screen, go to the **Configuration > BWM** screen (see [Section 31.2 on page 370](#)), and click either the **Add** icon or an **Edit** icon.

Figure 256 Configuration > BWM > Edit (For the Default Policy)

Add Policy

Create new Object ▾

Bandwidth Shaping

Guaranteed Bandwidth

Inbound Priority:

Outbound Priority:

OK Cancel

Figure 257 Configuration > BWM > Add/Edit

Add Policy

Create new Object ▾

Configuration

Enable

Description: (Optional)

BWM Type: Shared Per user Per-Source-IP ⓘ

Criteria

User: ▾

Schedule: ▾

Incoming Interface: ▾

Outgoing Interface: ▾

Source: ▾

Destination: ▾

DSCP Code: ▾

Service Type: Service Object Application Object

Application Object: ▾

DSCP Marking

DSCP Marking

Inbound Marking: ▾

Outbound Marking: ▾

Bandwidth Shaping

Guaranteed Bandwidth

Inbound: kbps (0 : disabled) Priority:

Maximize Bandwidth Usage Maximum: kbps

Outbound: kbps (0 : disabled) Priority:

Maximize Bandwidth Usage Maximum: kbps

Related Setting

Log ▾

Apply Revert OK Cancel

The following table describes the labels in this screen.

Table 166 Configuration > BWM > Add/Edit

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable	Select this check box to turn on this policy.
Description	Enter a description of this policy. You can use alphanumeric and ()+/:=?!*#@\$_%-characters, and it can be up to 60 characters long.
BWM Type	Select Shared when the policy is set for all matched traffic. Select Per user when the policy is set for an individual user. Select Per-Source-IP when the policy is set for an individual source IP.
User	Select a type of the user account to which to apply the policy. Use Create new Object if you need to configure a new user account. Select any to apply the policy for every user.
Schedule	Select a schedule that defines when the policy applies or select Create new Object to configure a new one (see Chapter 41 on page 453 for details). Otherwise, select none to make the policy always effective.
Incoming Interface	Select the source interface of the traffic to which this policy applies.
Outgoing Interface	Select the destination interface of the traffic to which this policy applies.
Source	Select a source address or address group for whom this policy applies. Use Create new Object if you need to configure a new one. Select any if the policy is effective for every source. If you set BWM Type to Per-Source-IP , you can only select a source address (group) that contains no more than 256 IP addresses.
Destination	Select a destination address or address group for whom this policy applies. Use Create new Object if you need to configure a new one. Select any if the policy is effective for every destination.
DSCP Code	Select a DSCP code point value of incoming or outgoing packets to which this policy applies or select User Define to specify another DSCP code point. The lower the number the higher the priority with the exception of 0 which is usually given only best-effort treatment. any means all DSCP value or no DSCP marker. default means traffic with a DSCP value of 0. This is usually best effort traffic. The "af" choices stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Section 12.4 on page 212 for more details.
User-Defined DSCP Code	Use this field to specify a custom DSCP code point.
Service Type	Select Service Object or Application Object if you want a specific service (defined in a service object) or application patrol service to which the policy applies.
Service Object	This field is available if you selected Service Object as the service type. Select a service or service group to identify the type of traffic to which this policy applies. any means all services.
Application Object	This field is available if you selected Application Object as the service type. Select an application patrol service to identify the specific traffic to which this policy applies.
DSCP Marking	Set how the UAG handles the DSCP value of the incoming and outgoing packets that match this policy.

Table 166 Configuration > BWM > Add/Edit

LABEL	DESCRIPTION
Inbound Marking Outbound Marking	<p>Inbound refers to the traffic the UAG sends to a connection's initiator. Outbound refers to the traffic the UAG sends out from a connection's initiator.</p> <p>Select one of the pre-defined DSCP values to apply or select User Defined to specify another DSCP value. The "af" choices stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Section 12.4 on page 212 for more details.</p> <p>Select preserve to have the UAG keep the packets' original DSCP value.</p> <p>Select default to have the UAG set the DSCP value of the packets to 0.</p>
Bandwidth Shaping	Configure these fields to set the amount of bandwidth the matching traffic can use.
Inbound kbps	<p>Type how much inbound bandwidth, in kilobits per second, this policy allows the traffic to use. Inbound refers to the traffic the UAG sends to a connection's initiator.</p> <p>If you enter 0 here, this policy does not apply bandwidth management for the matching traffic that the UAG sends to the initiator. Traffic with bandwidth management disabled (inbound and outbound are both set to 0) is automatically treated as the lowest priority (7).</p> <p>If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.</p>
Outbound kbps	<p>Type how much outbound bandwidth, in kilobits per second, this policy allows the traffic to use. Outbound refers to the traffic the UAG sends out from a connection's initiator.</p> <p>If you enter 0 here, this policy does not apply bandwidth management for the matching traffic that the UAG sends out from the initiator. Traffic with bandwidth management disabled (inbound and outbound are both set to 0) is automatically treated as the lowest priority (7).</p> <p>If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.</p>
Priority	<p>Enter a number between 1 and 7 to set the priority for traffic that matches this policy. The smaller the number, the higher the priority.</p> <p>Traffic with a higher priority is given bandwidth before traffic with a lower priority.</p> <p>The UAG uses a fairness-based (round-robin) scheduler to divide bandwidth between traffic flows with the same priority.</p> <p>The number in this field is ignored if the incoming and outgoing limits are both set to 0. In this case the traffic is automatically treated as being set to the lowest priority (7) regardless of this field's configuration.</p>
Maximize Bandwidth Usage	<p>This field displays when the inbound or outbound bandwidth management is not set to 0. Enable maximize bandwidth usage to let the traffic matching this policy "borrow" any unused bandwidth on the out-going interface.</p> <p>After each application or type of traffic gets its configured bandwidth rate, the UAG uses the fairness-based scheduler to divide any unused bandwidth on the out-going interface amongst applications and traffic types that need more bandwidth and have maximize bandwidth usage enabled.</p>
Related Setting	
Log	Select whether to have the UAG generate a log (log), log and alert (log alert) or not (no) for packets that match the policy.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving your changes.

Application Patrol

32.1 Overview

Application patrol provides a convenient way to manage the use of various applications on the network. It manages general protocols (for example, HTTP and FTP) and instant messenger (IM), peer-to-peer (P2P), Voice over IP (VoIP), and streaming (RSTP) applications. You can even control the use of a particular application's individual features (like text messaging, voice, video conferencing, and file transfers). You can also configure bandwidth management with application patrol in the **Configuration > BWM** screen for traffic prioritization to enhance the performance of delay-sensitive applications like voice and video.

32.1.1 What You Can Do in this Chapter

- Use the **Profile** summary screen (see [Section 32.2 on page 377](#)) to view application patrol profiles configured on the UAG.
- Use the **Profile Add/Edit** screens (see [Section 32.2.1 on page 378](#)) to set actions for application categories and for specific applications within the category.

32.1.2 What You Need to Know

If you want to use a service, make sure both the Security Policy and application patrol allow the service's packets to go through the UAG.

Note: The UAG checks secure policies before it checks application patrol rules for traffic going through the UAG.

Application patrol examines every TCP and UDP connection passing through the UAG and identifies what application is using the connection. Then, you can specify whether or not the UAG continues to route the connection. Traffic not recognized by the application patrol signatures is ignored.

Application Profiles & Policies

An application patrol profile is a group of categories of application patrol signatures. For each profile, you can specify the default action the UAG takes once a packet matches a signature (forward, drop, or reject a service's connections and/or create a log alert).

Use policies to link profiles to traffic flows based on criteria such as source zone, destination zone, source address, destination address, schedule, user.

Classification of Applications

There are two ways the UAG can identify the application. The first is called auto. The UAG looks at the IP payload (OSI level-7 inspection) and attempts to match it with known patterns for specific

applications. Usually, this occurs at the beginning of a connection, when the payload is more consistent across connections, and the UAG examines several packets to make sure the match is correct. Before confirmation, packets are forwarded by App Patrol with no action taken. The number of packets inspected before confirmation varies by signature.

Note: The UAG allows the first eight packets to go through the security policy, regardless of the application patrol policy for the application. The UAG examines these first eight packets to identify the application.

The second approach is called service ports. The UAG uses only OSI level-4 information, such as ports, to identify what application is using the connection. This approach is available in case the UAG identifies a lot of “false positives” for a particular application.

Custom Ports for SIP and the SIP ALG

Configuring application patrol to use custom port numbers for SIP traffic also configures the SIP ALG to use the same port numbers for SIP traffic. Likewise, configuring the SIP ALG to use custom port numbers for SIP traffic also configures application patrol to use the same port numbers for SIP traffic.

Finding Out More

- You must configure services in **Objects > Application**.
- See **Configuration > BWM** chapter for detailed information on bandwidth management.

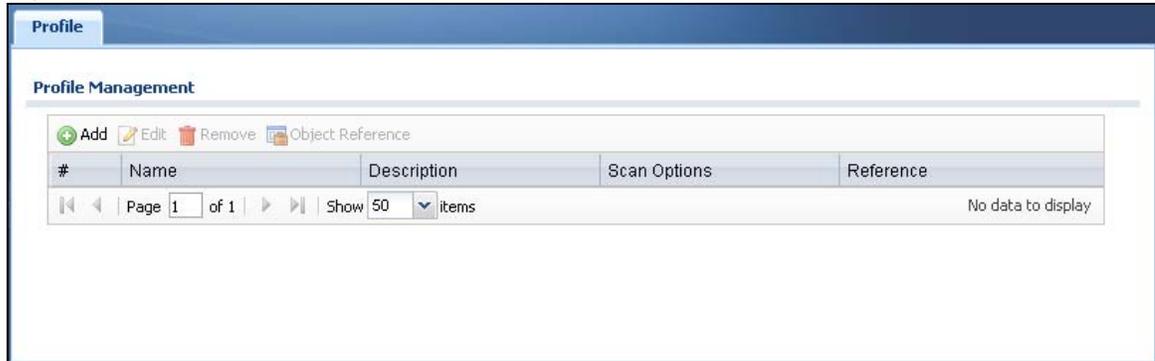
32.2 Application Patrol Profile

Use the application patrol **Profile** screens to customize action and log settings for a group of application patrol signatures. You then link a profile to a security policy (see [Section 25.2 on page 291](#)).

Note: You must register for the AppPatrol signature service (at least the trial) before you can use it.

A profile is an application object(s) or application group(s) that has customized action and log settings.

Click **Configuration > UTM Profile > App Patrol > Profile** to open the following screen.

Figure 258 Configuration > UTM Profile > App Patrol > Profile

The following table describes the labels in this screen.

Table 167 Configuration > UTM Profile > App Patrol > Profile

LABEL	DESCRIPTION
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	Select an entry and click Remove to delete the selected entry.
Object Reference	Select an entry and click Object References to open a screen that shows which settings use the entry. Click Refresh to update information on this screen.
#	This field is a sequential value showing the number of the profile. The profile order is not important.
Name	This displays the name of the profile created.
Description	This displays the description of the App Patrol Profile.
Scan Options	This field displays the scan options from the App Patrol profile.
Reference	This displays the number of times an object reference is used in a profile.

32.2.1 Add/Edit Application Patrol Profile

Use this screen to configure profile settings. Click **Configuration > UTM Profile > App Patrol > Profile**, then click **Add** to create a new profile rule or click an existing profile and click **Edit** (or double-click it) to open the following screen.

Figure 259 Configuration > UTM Profile > App Patrol > Profile > Add/Edit

The following table describes the labels in this screen.

Table 168 Configuration > UTM Profile > App Patrol > Profile > Add/Edit

LABEL	DESCRIPTION
General Settings	
Name	Type the name of the profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. These are valid, unique profile names: <ul style="list-style-type: none"> • MyProfile • mYProfile • Mymy12_3-4 These are invalid profile names: <ul style="list-style-type: none"> • 1mYProfile • My Profile • MyProfile? • Whatalongprofilename123456789012
Description	Enter a description of this profile. You can use alphanumeric and () + , / : = ? ! * # @ \$ % - " characters, and it can be up to 60 characters long.
Profile Management	
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Remove	Select an entry and click Remove to delete the selected entry.
#	This field is a sequential value showing the number of the profile. The profile order is not important.
Application	This field displays the application name of the policy.
Action	Select the default action for all signatures in this category. <p>forward - the UAG routes packets that matches these signatures.</p> <p>Drop - the UAG silently drops packets that matches these signatures without notification.</p> <p>Reject - the UAG drops packets that matches these signatures and sends notification.</p>

Table 168 Configuration > UTM Profile > App Patrol > Profile > Add/Edit (continued)

LABEL	DESCRIPTION
Log	Select whether to have the UAG generate a log (log), log and alert (log alert) or neither (no) by default when traffic matches a signature in this category.
OK	Click OK to save your settings to the UAG, complete the profile and return to the profile summary page.
Cancel	Click Cancel to return to the profile summary page without saving any changes.

32.2.2 Add/Edit Application Patrol Profile Rule Application

Click **Add** or **Edit** under **Profile Management** in the previous screen to display the following screen.

Figure 260 Configuration > UTM Profile > App Patrol > Profile > Add/Edit Rule > Add/Edit Application

The following table describes the labels in this screen.

Table 169 Configuration > UTM Profile > App Patrol > Profile > Add/Edit Rule > Add/Edit Application

LABEL	DESCRIPTION
General Settings	
Application	Select an application to apply the policy. You must have configured an application object in the Configuration > Object > Application screen.
Action	Select the default action for all signatures in this category. forward - the UAG routes packets that matches these signatures. Drop - the UAG silently drops packets that matches these signatures without notification. Reject - the UAG drops packets that matches these signatures and sends notification.
Log	Select whether to have the UAG generate a log (log), log and alert (log alert) or neither (no) by default when traffic matches a signature in this category.
OK	Click OK to save your settings to the UAG.
Cancel	Click Cancel to return to the profile summary page without saving any changes.

Content Filtering

33.1 Overview

Use the content filtering feature to control access to specific web sites or web content.

33.1.1 What You Can Do in this Chapter

- Use the **Profile** screens ([Section 33.2 on page 383](#)) to set up content filtering profiles.
- Use the **Trusted Web Sites** screens ([Section 33.3 on page 391](#)) to create a common list of good (allowed) web site addresses.
- Use the **Forbidden Web Sites** screens ([Section 33.4 on page 392](#)) to create a common list of bad (blocked) web site addresses.

33.1.2 What You Need to Know

Content Filtering

Content filtering allows you to block certain web features, such as cookies, and/or block access to specific web sites. It can also block access to specific categories of web site content. You can create different content filter policies for different addresses, schedules, users or groups and content filter profiles. For example, you can configure one policy that blocks John Doe's access to arts and entertainment web pages during the workday and another policy that lets him access them after work.

Content Filtering Policies

A content filtering policy allows you to do the following.

- Use schedule objects to define when to apply a content filter profile.
- Use address and/or user/group objects to define to whose web access to apply the content filter profile.
- Apply a content filter profile that you have custom-tailored.

Content Filtering Profiles

A content filtering profile conveniently stores your custom settings for the following features.

- **Category-based Blocking**
The UAG can block access to particular categories of web site content, such as pornography or racial intolerance.

- Restrict Web Features

The UAG can disable web proxies and block web features such as ActiveX controls, Java applets and cookies.

- Customize Web Site Access

You can specify URLs to which the UAG blocks access. You can alternatively block access to all URLs except ones that you specify. You can also have the UAG block access to URLs that contain particular keywords.

Content Filtering Configuration Guidelines

When the UAG receives an HTTP request, the content filter searches for a policy that matches the source address and time (schedule). The content filter checks the policies in order (based on the policy numbers). When a matching policy is found, the content filter allows or blocks the request depending on the settings of the filtering profile specified by the policy. Some requests may not match any policy. The UAG allows the request if the default policy is not set to block. The UAG blocks the request if the default policy is set to block.

External Web Filtering Service

When you register for and enable the external web filtering service, your UAG accesses an external database that has millions of web sites categorized based on content. You can have the UAG block, block and/or log access to web sites based on these categories.

Keyword Blocking URL Checking

The UAG checks the URL's domain name (or IP address) and file path separately when performing keyword blocking.

The URL's domain name or IP address is the characters that come before the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the domain name is www.zyxel.com.tw.

The file path is the characters that come after the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the file path is news/pressroom.php.

Since the UAG checks the URL's domain name (or IP address) and file path separately, it will not find items that go across the two. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the UAG would find "tw" in the domain name (www.zyxel.com.tw). It would also find "news" in the file path (news/pressroom.php) but it would not find "tw/news".

Finding Out More

- See [Section 33.5 on page 393](#) for content filtering background/technical information.

33.1.3 Before You Begin

- You must configure an address object, a schedule object and a filtering profile before you can set up a content security policy.
- You must have Content Filtering license in order to use the function.subscribe to use the external database content filtering (see the **Licensing > Registration** screens).

33.2 Content Filter Profile Screen

Click **Configuration > UTM Profile > Content Filter > Profile** to open the **Content Filter Profile** screen. Use this screen to enable content filtering, view and order your list of content filter policies, create a denial of access message or specify a redirect URL and check your external web filtering service registration status.

Figure 261 Configuration > UTM Profile > Content Filter > Profile

The following table describes the labels in this screen.

Table 170 Configuration > UTM Profile > Content Filter > Profile

LABEL	DESCRIPTION
General Settings	
Enable Content Filter Report Service	Select this check box to have the UAG collect category-based content filtering statistics.
Report Server	Click this link to choose where your UAG is registered: myZyXEL.com or myZyXEL.com 2.0. Choose myZyXEL.com 2.0 for a model in this series.
Content Filter Category Service Timeout	Specify the allowable time period in seconds for accessing the external web filtering service's server.
Message to display when a site is blocked	

Table 170 Configuration > UTM Profile > Content Filter > Profile (continued)

LABEL	DESCRIPTION
Denied Access Message	<p>Enter a message to be displayed when content filter blocks access to a web page. Use up to 127 characters (0-9a-zA-Z;/?:@&=+\$\._!~*'(%)"). For example, "Access to this web page is not allowed. Please contact the network administrator".</p> <p>It is also possible to leave this field blank if you have a URL specified in the Redirect URL field. In this case if the content filter blocks access to a web page, the UAG just opens the web page you specified without showing a denied access message.</p>
Redirect URL	<p>Enter the URL of the web page to which you want to send users when their web access is blocked by content filter. The web page you specify here opens in a new frame below the denied access message.</p> <p>Use "http://" or "https://" followed by up to 262 characters (0-9a-zA-Z;/?:@&=+\$\._!~*'(%)"). For example, http://192.168.1.17/blocked access.</p>
Profile Management	
Add	Click Add to create a new content filter rule.
Edit	Click Edit to make changes to a content filter rule.
Remove	Click Remove to delete a content filter rule.
Object Reference	Select an entry and click Object References to open a screen that shows which settings use the entry. Click Refresh to update information on this screen.
#	This column lists the index numbers of the content filter profile.
Name	This column lists the names of the content filter profile rule.
Description	This column lists the description of the content filter profile rule.
Reference	This displays the number of times an Object Reference is used in a rule.
Content Filter Category Service License Status	
License Status	<p>This read-only field displays the status of your content-filtering database service registration.</p> <p>Not Licensed displays if you have not successfully registered and activated the service.</p> <p>Expired displays if your subscription to the service has expired.</p> <p>Licensed displays if you have successfully registered the UAG and activated the service.</p> <p>You can view content filter reports after you register the UAG and activate the subscription service in the Registration screen.</p>
License Type	<p>This read-only field displays what kind of service registration you have for the content-filtering database.</p> <p>None displays if you have not successfully registered and activated the service.</p> <p>Standard displays if you have successfully registered the UAG and activated the service.</p> <p>Trial displays if you have successfully registered the UAG and activated the trial service subscription.</p>
Expiration Date	This field displays the date your service license expires.
Register Now	This link appears if you have not registered for the service or the service has expired. Click this link to go to the screen where you can register for the service.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

33.2.1 Add/Edit Content Filter Profile

Click **Configuration > UTM > Content Filter > Profile > Add/Edit** to open the **Add Filter Profile** screen. Configure **Category Service** and **Custom Service** tabs.

33.2.1.1 Category Service

Click the **Category Service** tab.

Figure 262 Configuration > UTM Profile > Content Filter > Profile > Add/Edit Filter Profile > Category Service

Add Filter Profile

Category Service | Custom Service

General Settings

License Status: **Not Licensed**

License Type: **None**

Name: ⓘ

Description: (Optional)

Enable Content Filter Category Service

Action for Unsafe Web Pages: Warn Log

Action for Managed Web Pages: Block Log

Action for Unrated Web Pages: Warn Log

Action When Category Server Is Unavailable: Warn Log

Select Categories

Select All Categories Clear All Categories

Security Threat (unsafe)

Anonymizers Botnets Compromised

Malware Network Errors Parked Domains

Phishing & Fraud Spam Sites

Managed Categories

Advertisements & Pop-Ups Alcohol/Tobacco Arts

Business Transportation Chat

Forums & Newsgroups Computers & Technology Criminal Activity

Dating & Personals Download Sites Education

Apply Reset OK Cancel

The following table describes the labels in this screen.

Table 171 Configuration > UTM Profile > Content Filter > Profile > Add/Edit Filter Profile > Category Service

LABEL	DESCRIPTION
License Status	<p>This read-only field displays the status of your content-filtering database service registration.</p> <p>Not Licensed displays if you have not successfully registered and activated the service.</p> <p>Expired displays if your subscription to the service has expired.</p> <p>Licensed displays if you have successfully registered the UAG and activated the service.</p> <p>You can view content filter reports after you register the UAG and activate the subscription service in the Registration screen.</p>
License Type	<p>This read-only field displays what kind of service registration you have for the content-filtering database.</p> <p>None displays if you have not successfully registered and activated the service.</p> <p>Standard displays if you have successfully registered the UAG and activated the standard content filtering service.</p> <p>Trial displays if you have successfully registered the UAG and activated the trial service subscription.</p>
Name	<p>Enter a descriptive name for this content filtering profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.</p>
Description	<p>Enter a description for the content filtering profile rule to help identify the purpose of rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.</p> <p>This field is optional.</p>
Enable Content Filter Category Service	<p>Enable external database content filtering to have the UAG check an external database to find to which category a requested web page belongs. The UAG then blocks or forwards access to the web page depending on the configuration of the rest of this page.</p>
Action for Unsafe Web Pages	<p>Select Pass to allow users to access web pages that match the unsafe categories that you select below.</p> <p>Select Block to prevent users from accessing web pages that match the unsafe categories that you select below. When external database content filtering blocks access to a web page, it displays the denied access message that you configured in the Content Filter General screen along with the category of the blocked web page.</p> <p>Select Warn to display a warning message before allowing users to access web pages that match the unsafe categories that you select below.</p> <p>Select Log to record attempts to access web pages that match the unsafe categories that you select below.</p>

Table 171 Configuration > UTM Profile > Content Filter > Profile > Add/Edit Filter Profile > Category Service (continued)

LABEL	DESCRIPTION
Action for Managed Web Pages	<p>Select Pass to allow users to access web pages that match the other categories that you select below.</p> <p>Select Block to prevent users from accessing web pages that match the other categories that you select below. When external database content filtering blocks access to a web page, it displays the denied access message that you configured in the Content Filter General screen along with the category of the blocked web page.</p> <p>Select Log to record attempts to access web pages that match the other categories that you select below.</p>
Action for Unrated Web Pages	<p>Select Pass to allow users to access web pages that the external web filtering service has not categorized.</p> <p>Select Block to prevent users from accessing web pages that the external web filtering service has not categorized. When the external database content filtering blocks access to a web page, it displays the denied access message that you configured in the Content Filter General screen along with the category of the blocked web page.</p> <p>Select Warn to display a warning message before allowing users to access web pages that the external web filtering service has not categorized.</p> <p>Select Log to record attempts to access web pages that are not categorized.</p>
Action When Category Server Is Unavailable	<p>Select Pass to allow users to access any requested web page if the external content filtering database is unavailable.</p> <p>Select Block to block access to any requested web page if the external content filtering database is unavailable.</p> <p>Select Warn to display a warning message before allowing users to access any requested web page if the external content filtering database is unavailable.</p> <p>The following are possible causes for the external content filtering server not being available:</p> <ul style="list-style-type: none"> • There is no response from the external content filtering server within the time period specified in the Content Filter Server Unavailable Timeout field. • The UAG is not able to resolve the domain name of the external content filtering database. • There is an error response from the external content filtering database. This can be caused by an expired content filtering registration (External content filtering's license key is invalid"). <p>Select Log to record attempts to access web pages that occur when the external content filtering database is unavailable.</p>
Select Categories	
Select All Categories	Select this check box to restrict access to all site categories listed below.
Clear All Categories	Select this check box to clear the selected categories below.
Security Threat (unsafe)	<p>The categories of web pages that are known to pose a threat to users or their computers are:</p> <ul style="list-style-type: none"> • Anonymizers • Botnets • Compromised • Malware • Network Errors • Parked Domains • Phishing & Fraud • Spam Sites

Table 171 Configuration > UTM Profile > Content Filter > Profile > Add/Edit Filter Profile > Category Service (continued)

LABEL	DESCRIPTION
Managed Categories	These are categories of web pages based on their content. Select categories in this section to control access to specific types of Internet content. You must have the Category Service content filtering license to filter these categories.
Test Web Site Category	
URL to test	You can check which category a web page belongs to. Enter a web site URL in the text box. When the content filter is active, you should see the web page's category. The query fails if the content filter is not active.
Test Against Content Filter Category Server	Click this button to see the category recorded in the external content filter server's database for the web page you specified.
If you think the category is incorrect	Click this link to see the category recorded in the UAG's content filtering database for the web page you specified (if the database has an entry for it).
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving your changes.

33.2.1.2 Custom Service

Click **Configuration > UTM Profile > Content Filter > Filter Profile > Add/Edit > Custom Service** to open the **Custom Service** screen. You can create a list of good (allowed) web site addresses and a list of bad (blocked) web site addresses. You can also block web sites based on whether the web site's address contains a keyword. Use this screen to add or remove specific sites or keywords from the filter list.

Figure 263 Configuration > UTM Profile > Content Filter > Profile > Add/Edit Filter Profile > Custom Service

Add Filter Profile

Category Service **Custom Service**

General Settings

Name: !

Description: (Optional)

Enable Custom Service

Allow web traffic for trusted web sites only

Check Common Trusted/Forbidden List

Restricted Web Features

Block: ActiveX Java Cookies Web Proxy

Allow Java/ActiveX/Cookies/Web proxy to trusted web sites

Trusted Web Sites

#	Trusted Web Sites
No data to display	

Page 1 of 1 | Show 50 items

Forbidden Web Sites

#	Forbidden Web Sites
No data to display	

Page 1 of 1 | Show 50 items

Blocked URL Keywords

#	Blocked URL Keywords
No data to display	

Page 1 of 1 | Show 50 items

The following table describes the labels in this screen.

Table 172 Configuration > UTM Profile > Content Filter > Profile > Add/Edit Filter Profile > Custom Service

LABEL	DESCRIPTION
Name	Enter a descriptive name for this content filtering profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description for the content filtering profile rule to help identify the purpose of rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. This field is optional.
Enable Custom Service	Select this check box to allow trusted web sites and block forbidden web sites. Content filter list customization may be enabled and disabled without re-entering these site names.
Allow Web traffic for trusted web sites only	When this box is selected, the UAG blocks Web access to sites that are not on the Trusted Web Sites list. If they are chosen carefully, this is the most effective way to block objectionable material.

Table 172 Configuration > UTM Profile > Content Filter > Profile > Add/Edit Filter Profile > Custom Service (continued)

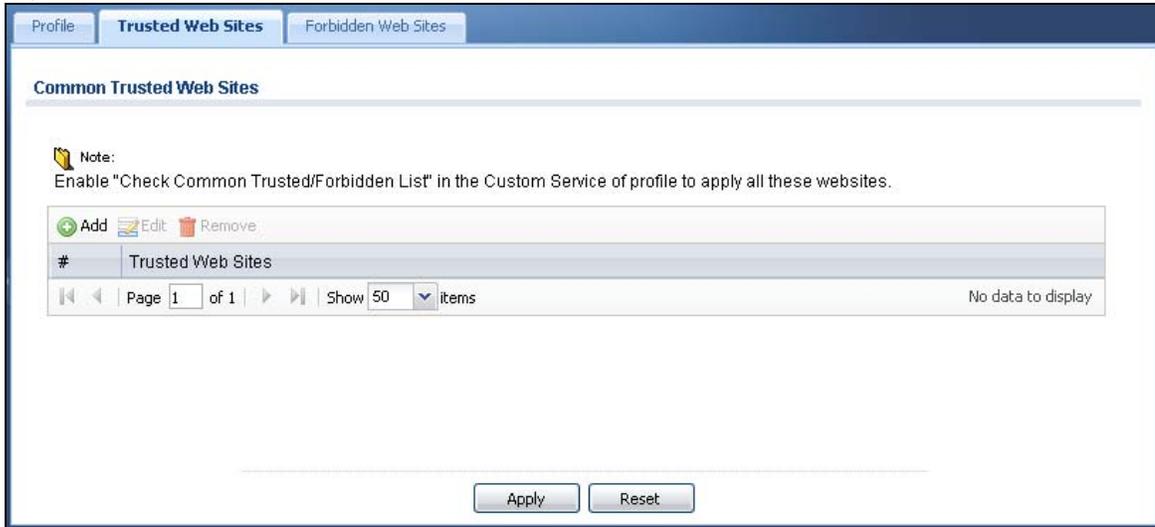
LABEL	DESCRIPTION
Check Common Trusted/ Forbidden List	Select this check box to check the common trusted and forbidden web sites lists. See Section 33.3 on page 391 and Section 33.4 on page 392 for information on configuring these lists.
Restricted Web Features	<p>Select the check box(es) to restrict a feature. Select the check box(es) to restrict a feature.</p> <ul style="list-style-type: none"> When you download a page containing ActiveX or Java, that part of the web page will be blocked with an X. When you download a page coming from a Web Proxy, the whole web page will be blocked. When you download a page containing cookies, the cookies will be removed, but the page will not be blocked.
Block ActiveX	ActiveX is a tool for building dynamic and active web pages and distributed object applications. When you visit an ActiveX web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	Java is a programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Cookies are files stored on a computer's hard drive. Some web servers use them to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Allow Java/ActiveX/Cookies/ Web proxy to trusted web sites	When this box is selected, the UAG will permit Java, ActiveX and Cookies from sites on the Trusted Web Sites list to the LAN. In certain cases, it may be desirable to allow Java, ActiveX or Cookies from sites that are known and trusted.
Trusted Web Sites	These are sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This displays the index number of the trusted web sites.
Trusted Web Site	<p>This column displays the trusted web sites already added.</p> <p>Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are allowed. For example, entering "*zyxel.com" also allows "www.zyxel.com", "partner.zyxel.com", "press.zyxel.com", and so on. You can also enter just a top level domain. For example, enter "*.com" to allow all .com domains.</p> <p>Use up to 127 characters (0-9a-z-). The casing does not matter. "*" can be used as a wildcard to match any string. The entry must contain at least one "." or it will be invalid.</p>
Forbidden Web Site List	Sites that you want to block access to, regardless of their content rating, can be allowed by adding them to this list.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This displays the index number of the forbidden web sites.

Table 172 Configuration > UTM Profile > Content Filter > Profile > Add/Edit Filter Profile > Custom Service (continued)

LABEL	DESCRIPTION
Forbidden Web Sites	<p>This list displays the forbidden web sites already added.</p> <p>Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are also blocked. For example, entering "*bad-site.com" also blocks "www.bad-site.com", "partner.bad-site.com", "press.bad-site.com", and do on. You can also enter just a top level domain. For example, enter "*.com" to block all .com domains.</p> <p>Use up to 127 characters (0-9a-z-). The casing does not matter. "*" can be used as a wildcard to match any string. The entry must contain at least one "." or it will be invalid.</p>
Blocked URL Keywords	<p>This section allows you to block Web sites with URLs that contain certain keywords in the domain name or IP address.</p>
Add	<p>Click this to create a new entry.</p>
Edit	<p>Select an entry and click this to be able to modify it.</p>
Remove	<p>Select an entry and click this to delete it.</p>
#	<p>This displays the index number of the blocked URL keywords.</p>
Blocked URL Keywords	<p>This list displays the keywords already added.</p> <p>Enter a keyword or a numerical IP address to block. You can also enter a numerical IP address.</p> <p>Use up to 127 case-insensitive characters (0-9a-zA-Z;/?:@&=+\$\._!~*()%). "*" can be used as a wildcard to match any string. Use " " to indicate a single wildcard character.</p> <p>For example enter *Bad_Site* to block access to any web page that includes the exact phrase Bad_Site. This does not block access to web pages that only include part of the phrase (such as Bad for example).</p>
OK	<p>Click OK to save your changes back to the UAG.</p>
Cancel	<p>Click Cancel to exit this screen without saving your changes.</p>

33.3 Content Filter Trusted Web Sites Screen

Click **Configuration > UTM Profile > Content Filter > Trusted Web Sites** to open the **Trusted Web Sites** screen. You can create a common list of good (allowed) web site addresses. When you configure **Filter Profiles**, you can select the option to check the **Common Trusted Web Sites** list. Use this screen to add or remove specific sites from the filter list.

Figure 264 Configuration > UTM Profile > Content Filter > Trusted Web Sites

The following table describes the labels in this screen.

Table 173 Configuration > UTM Profile > Content Filter > Trusted Web Sites

LABEL	DESCRIPTION
Common Trusted Web Sites	These are sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This displays the index number of the trusted web sites.
Trusted Web Site	This column displays the trusted web sites already added. Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are allowed. For example, entering "zyxel.com" also allows "www.zyxel.com", "partner.zyxel.com", "press.zyxel.com", and so on. You can also enter just a top level domain. For example, enter .com to allow all .com domains. Use up to 127 characters (0-9a-z-). The casing does not matter.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

33.4 Content Filter Forbidden Web Sites Screen

Click **Configuration > UTM Profile > Content Filter > Forbidden Web Sites** to open the **Forbidden Web Sites** screen. You can create a common list of bad (blocked) web site addresses. When you configure **Filter Profiles**, you can select the option to check the **Common Forbidden Web Sites** list. Use this screen to add or remove specific sites from the filter list.

Figure 265 Configuration > UTM Profile > Content Filter > Forbidden Web Sites

The following table describes the labels in this screen.

Table 174 Configuration > UTM Profile > Content Filter > Forbidden Web Sites

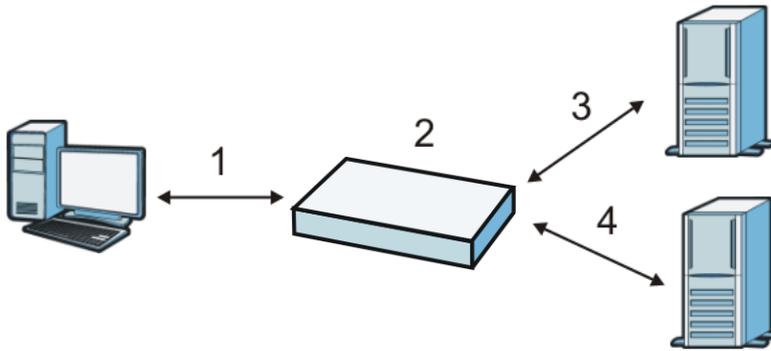
LABEL	DESCRIPTION
Forbidden Web Site List	Sites that you want to block access to, regardless of their content rating, can be allowed by adding them to this list.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This displays the index number of the forbidden web sites.
Forbidden Web Sites	This list displays the forbidden web sites already added. Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are also blocked. For example, entering "bad-site.com" also blocks "www.bad-site.com", "partner.bad-site.com", "press.bad-site.com", and do on. You can also enter just a top level domain. For example, enter .com to block all .com domains. Use up to 127 characters (0-9a-z-). The casing does not matter.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

33.5 Content Filter Technical Reference

This section provides content filtering background information.

External Content Filter Server Lookup Procedure

The content filter lookup process is described below.

Figure 266 Content Filter Lookup Procedure

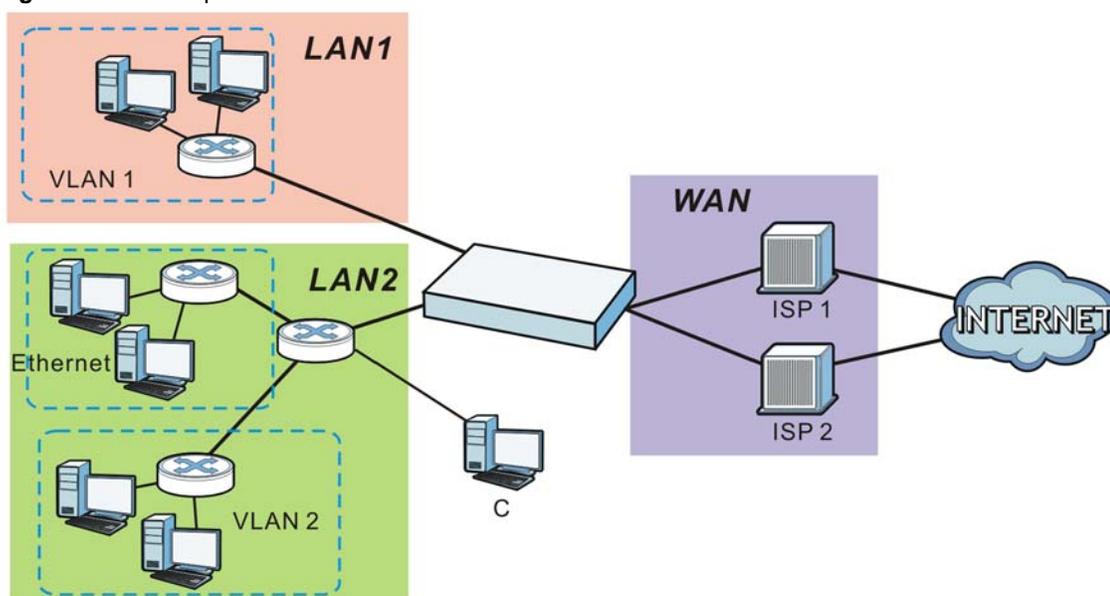
- 1 A computer behind the UAG tries to access a web site.
- 2 The UAG looks up the web site in its cache. If an attempt to access the web site was made in the past, a record of that web site's category will be in the UAG's cache. The UAG blocks, blocks and logs or just logs the request based on your configuration.
- 3 If the UAG has no record of the web site, it queries the external content filter database and simultaneously sends the request to the web server.
- 4 The external content filter server sends the category information back to the UAG, which then blocks and/or logs access to the web site based on the settings in the content filter profile. The web site's address and category are then stored in the UAG's content filter cache.

34.1 Zones Overview

Set up zones to configure network security and network policies in the UAG. A zone is a group of interfaces. The UAG uses zones instead of interfaces in many security and policy settings, such as security policies and remote management.

Zones cannot overlap. Each Ethernet interface, VLAN interface, bridge interface, and PPPoE/PPTP interface can be assigned to at most one zone. Virtual interfaces are automatically assigned to the same zone as the interface on which they run.

Figure 267 Example: Zones



34.1.1 What You Can Do in this Chapter

Use the **Zone** screens (see [Section 34.2 on page 396](#)) to manage the UAG's zones.

34.1.2 What You Need to Know

Effects of Zones on Different Types of Traffic

Zones effectively divide traffic into three types--intra-zone traffic, inter-zone traffic, and extra-zone traffic--which are affected differently by zone-based security and policy settings.

Intra-zone Traffic

- Intra-zone traffic is traffic between interfaces in the same zone. For example, in [Figure 267 on page 395](#), traffic between **VLAN1** and the Ethernet is intra-zone traffic.
- You can also set up security policies to control intra-zone traffic (for example, LAN1-to-LAN1), but many other types of zone-based security and policy settings do not affect intra-zone traffic.

Inter-zone Traffic

Inter-zone traffic is traffic between interfaces in different zones. For example, in [Figure 267 on page 395](#), traffic between **VLAN1** and the Internet is inter-zone traffic. This is the normal case when zone-based security and policy settings apply.

Extra-zone Traffic

- Extra-zone traffic is traffic to or from any interface that is not assigned to a zone. For example, in [Figure 267 on page 395](#), traffic to or from computer **C** is extra-zone traffic.
- Some zone-based security and policy settings may apply to extra-zone traffic, especially if you can set the zone attribute in them to **Any** or **All**. See the specific feature for more information.

34.2 The Zone Screen

The **Zone** screen provides a summary of all zones. In addition, this screen allows you to add, edit, and remove zones. To access this screen, click **Configuration > Object > Zone**.

Figure 268 Configuration > Object > Zone

The screenshot shows the 'Zone' configuration screen. It is divided into two main sections: 'User Configuration' and 'System Default'.

User Configuration: This section is currently empty, showing 'No data to display'. It includes buttons for 'Add', 'Edit', 'Remove', and 'Object Reference'. The table headers are '#', 'Name', 'Member', and 'Refere...'. Navigation controls show 'Page 1 of 1' and 'Show 50 items'.

System Default: This section contains a table with 5 rows of zone configurations. It includes buttons for 'Edit' and 'Object Reference'. The table headers are '#', 'Name', 'Member', and 'Refere...'. Navigation controls show 'Page 1 of 1' and 'Show 50 items', with a status 'Displaying 1 - 5 of 5'.

#	Name	Member	Refere...
1	LAN1	lan1	3
2	LAN2	lan2	2
3	WAN	wan1,wan1_ppp,wan2,wan2_ppp	3
4	DMZ	dmz	2
5	IPSec_VPN		2

The following table describes the labels in this screen.

Table 175 Configuration > Object > Zone

LABEL	DESCRIPTION
User Configuration / System Default	The UAG comes with pre-configured System Default zones that you cannot delete. You can create your own User Configuration zones
Add	Click this to create a new, user-configured zone.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove a user-configured trunk, select it and click Remove . The UAG confirms you want to remove it before doing so.
Object Reference	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 10.3.2 on page 165 for an example.
#	This field is a sequential value, and it is not associated with any entry.
Name	This field displays the name of the zone.
Member	This field displays the names of the interfaces that belong to each zone.
Reference	This field displays the number of times an Object Reference is used in a policy.

34.2.1 Add/Edit Zone

The **Zone Edit** screen allows you to add or edit a zone. To access this screen, go to the **Zone** screen (see [Section 34.2 on page 396](#)), and click the **Add** icon or an **Edit** icon.

Figure 269 Configuration > Object > Zone Add

The following table describes the labels in this screen.

Table 176 Configuration > Object > Zone > Add/Edit

LABEL	DESCRIPTION
Name	For a system default zone, the name is read only. For a user-configured zone, type the name used to refer to the zone. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Member List	Available lists the interfaces that do not belong to any zone. Select the interfaces that you want to add to the zone you are editing, and click the right arrow button to add them. Member lists the interfaces that belong to the zone. Select any interfaces that you want to remove from the zone, and click the left arrow button to remove them.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

User/Group

35.1 Overview

This chapter describes how to set up user accounts, user groups, and user settings for the UAG. You can also set up rules that control when users have to log in to the UAG before the UAG routes traffic for them.

35.1.1 What You Can Do in this Chapter

- The **User** screen (see [Section 35.2 on page 401](#)) provides a summary of all user accounts.
- The **Group** screen (see [Section 35.3 on page 405](#)) provides a summary of all user groups. In addition, this screen allows you to add, edit, and remove user groups. User groups may consist of access users and other user groups. You cannot put admin users in user groups
- The **Setting** screen (see [Section 35.4 on page 406](#)) controls default settings, login settings, lockout settings, and other user settings for the UAG. You can also use this screen to specify when users must log in to the UAG before it routes traffic for them.
- The **MAC Address** screen (see [Section 35.5 on page 411](#)) allows you to configure the MAC addresses of wireless clients for MAC authentication using the local user database.

35.1.2 What You Need To Know

User Account

A user account defines the privileges of a user logged into the UAG. User accounts are used in security policies and application patrol, in addition to controlling access to configuration and services in the UAG.

User Types

These are the types of user accounts the UAG uses.

Table 177 Types of User Accounts

TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
admin	Change UAG configuration (web, CLI)	WWW, TELNET, SSH, FTP, Console
limited-admin	Look at UAG configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, TELNET, SSH, Console
Access Users		
ext-user	External user account	WWW
ext-group-user	External group user account	WWW

Table 177 Types of User Accounts (continued)

TYPE	ABILITIES	LOGIN METHOD(S)
guest-manager	Create dynamic guest accounts	WWW
pre-subscriber	Access network services	Web Authentication Portal
dynamic-guest	Access network services	Web Authentication Portal

Note: The default **admin** account is always authenticated locally, regardless of the authentication method setting. (See [Chapter 43 on page 464](#) for more information about authentication methods.)

Ext-User Accounts

Set up an **ext-user** account if the user is authenticated by an external server and you want to set up specific policies for this user in the UAG. If you do not want to set up policies for this user, you do not have to set up an **ext-user** account.

All **ext-user** users should be authenticated by an external server, such as RADIUS. If the UAG tries to use the local database to authenticate an **ext-user**, the authentication attempt always fails. (This is related to AAA servers and authentication methods, which are discussed in [Chapter 42 on page 459](#) and [Chapter 43 on page 464](#), respectively.)

Note: If the UAG tries to authenticate an **ext-user** using the local database, the attempt always fails.

Once an **ext-user** user has been authenticated, the UAG tries to get the user type (see [Table 177 on page 399](#)) from the external server. If the external server does not have the information, the UAG sets the user type for this session to **User**.

For the rest of the user attributes, such as reauthentication time, the UAG checks the following places, in order.

- 1 User account in the remote server.
- 2 User account (Ext-User) in the UAG.
- 3 Default user account for RADIUS users (**radius-users**) in the UAG.

See [Setting up User Attributes in an External Server on page 413](#) for a list of attributes and how to set up the attributes in an external server.

Ext-Group-User Accounts

Ext-Group-User accounts are similar to ext-user accounts but allow you to group users by the value of the group membership attribute configured for the RADIUS server. See [Section 42.2.1 on page 460](#) for more on the group membership attribute.

Dynamic-Guest Accounts

Dynamic guest accounts are guest accounts, but are created dynamically and stored in the UAG's local user database. A dynamic guest account has a dynamically-created user name and password. A dynamic guest account user can access the UAG's services only within a given period of time and will become invalid after the expiration date/time.

There are three types of dynamic guest accounts depending on how they are created or authenticated: **billing-users**, **ua-users** and **trial-users**.

billing-users are guest account created with the guest manager account or an external printer and paid by cash or created and paid via the on-line payment service. **ua-users** are users that log in from the user agreement page. **trial-users** are free guest accounts that are created with the Free Time function.

Pre-Subscriber Accounts

Use the pre-subscriber account to test the Internet connection between the UAG and the ISP. The UAG does not impose time limitations or charges on this account. Thus, anyone who logs in with this account is able to gain Internet access for free.

User Groups

User groups may consist of user accounts or other user groups. Use user groups when you want to create the same rule for several user accounts, instead of creating separate rules for each one.

Note: You cannot put access users and admin users in the same user group.

Note: You cannot put the default **admin** account into any user group.

The sequence of members in a user group is not important.

User Awareness

By default, users do not have to log into the UAG to use the network services it provides. The UAG automatically routes packets for everyone. If you want to restrict network services that certain users can use via the UAG, you can require them to log in to the UAG first. The UAG is then 'aware' of the user who is logged in and you can create 'user-aware policies' that define what services they can use. See [Section 35.4.2 on page 410](#) for a user-aware login example.

Finding Out More

- See [Section 35.6 on page 413](#) for some information on users who use an external authentication server in order to log in.

35.2 User Summary Screen

The **User** screen provides a summary of all user accounts. To access this screen, login to the Web Configurator, and click **Configuration > Object > User/Group > User**.

Figure 270 Configuration > Object > User/Group > User

#	User Name	User Type	Description	Reference
1	admin	admin	Administration account	0
2	radius-users	ext-user	External RADIUS Users	0
3	billing-users	dynamic-guest	Billing Account Users	0
4	ua-users	dynamic-guest	User Agreement Users	0
5	trial-users	dynamic-guest	Free Time Users	0

The following table describes the labels in this screen.

Table 178 Configuration > Object > User/Group > User

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Object Reference	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 10.3.2 on page 165 for an example.
#	This field is a sequential value, and it is not associated with a specific user.
User Name	This field displays the user name of each user.
User Type	This field displays the kind of account of each user. These are the kinds of user account the UAG supports. <ul style="list-style-type: none"> • admin - this user can look at and change the configuration of the UAG • limited-admin - this user can look at the configuration of the UAG but not to change it • dynamic-guest - this user has access to the UAG's services but cannot look at the configuration. • ext-user - this user account is maintained in a remote server, such as RADIUS. • ext-group-user - this user account is maintained in a remote server, such as RADIUS. • guest-manager - this user can log in via the web configurator login screen and create dynamic guest accounts using the Account Generator screen that pops up. See Section 26.3.1 on page 308 for detailed information about the Account Generator screen. • pre-subscriber - this user has access to the UAG's services but cannot look at the configuration.
Description	This field displays the description for each user.
Reference	This displays the number of times an object reference is used in a profile.

35.2.1 User Add/Edit Screen

The **User Add/Edit** screen allows you to create a new user account or edit an existing one.

35.2.1.1 Rules for User Names

Enter a user name from 1 to 31 characters.

The user name can only contain the following characters:

- Alphanumeric A-z 0-9 (there is no unicode support)
- _ [underscores]
- - [dashes]

The first character must be alphabetical (A-Z a-z), an underscore (_), or a dash (-). Other limitations on user names are:

- User names are case-sensitive. If you enter a user 'bob' but use 'BOB' when connecting via CIFS or FTP, it will use the account settings used for 'BOB' not 'bob'.
- User names have to be different than user group names.
- Here are the reserved user names:
 - adm
 - admin
 - any
 - bin
 - daemon
 - debug
 - devicehaecived
 - ftp
 - games
 - halt
 - ldap-users
 - lp
 - mail
 - news
 - nobody
 - operator
 - radius-users
 - root
 - shutdown
 - sshd
 - sync
 - uucp
 - zyxel

To access this screen, go to the **User** screen (see [Section 35.2 on page 401](#)), and click either the **Add** icon or an **Edit** icon.

Figure 271 Configuration > Object > User/Group > User > Add/Edit

The screenshot shows a 'User Configuration' dialog box with the following fields and settings:

- User Name :** [Empty field with red error icon]
- User Type:** admin (dropdown menu)
- Password:** [Empty field with red error icon]
- Retype:** [Empty field]
- Description:** External User
- Authentication Timeout Settings:**
 - Use Default Settings
 - Use Manual Settings
- Lease Time:** 1440 minutes
- Reauthentication Time:** 1440 minutes

Buttons: OK, Cancel

The following table describes the labels in this screen.

Table 179 Configuration > Object > User/Group > User > Add/Edit

LABEL	DESCRIPTION
User Name	Type the user name for this user account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User names have to be different than user group names, and some words are reserved. See Section 35.2.1.1 on page 402 .
User Type	<p>This field displays the types of user accounts the UAG uses:</p> <ul style="list-style-type: none"> • admin - this user can look at and change the configuration of the UAG • limited-admin - this user can look at the configuration of the UAG but not to change it • ext-user - this user account is maintained in a remote server, such as RADIUS. See Ext-User Accounts on page 400 for more information about this type. • ext-group-user - this user account is maintained in a remote server, such as RADIUS. See Ext-Group-User Accounts on page 400 for more information about this type. • guest-manager - this user can log in via the web configurator login screen and create dynamic guest accounts using the Account Generator screen that pops up. See Section 26.3.1 on page 308 for detailed information about the Account Generator screen. • pre-subscriber - this user has access to the UAG's services but cannot look at the configuration.
Password	<p>This field is not available if you select the ext-user or ext-group-user type.</p> <p>Enter the password of this user account. It can consist of 4 - 31 alphanumeric characters.</p>
Retype	This field is not available if you select the ext-user or ext-group-user type.
Group Identifier	<p>This field is available for a ext-group-user type user account.</p> <p>Specify the value of the RADIUS server's Group Membership Attribute that identifies the group to which this user belongs.</p>
Associated AAA Server Object	This field is available for a ext-group-user type user account. Select the AAA server to use to authenticate this account's users.
Description	Enter the description of each user, if any. You can use up to 60 printable ASCII characters. Default descriptions are provided.
Authentication Timeout Settings	If you want the system to use default settings, select Use Default Settings . If you want to set authentication timeout to a value other than the default settings, select Use Manual Settings then fill your preferred values in the fields that follow.
Lease Time	<p>If you select Use Default Settings in the User Settings field, the default lease time is shown.</p> <p>If you select Use Manual Settings, you need to enter the number of minutes this user has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the Renew button on their screen. If you allow access users to renew time automatically (see Section 35.4 on page 406), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.</p>
Reauthentication Time	<p>If you select Use Default Settings in the User Settings field, the default lease time is shown.</p> <p>If you select Use Manual Settings, you need to type the number of minutes this user can be logged into the UAG in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike Lease Time, the user has no opportunity to renew the session without logging out.</p>

Table 179 Configuration > Object > User/Group > User > Add/Edit (continued)

LABEL	DESCRIPTION
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving your changes.

35.3 User Group Summary Screen

User groups consist of access users and other user groups. You cannot put admin users in user groups. The **Group** screen provides a summary of all user groups. In addition, this screen allows you to add, edit, and remove user groups. To access this screen, login to the Web Configurator, and click **Configuration > Object > User/Group > Group**.

Figure 272 Configuration > Object > User/Group > Group

The following table describes the labels in this screen. See [Section 35.3.1 on page 405](#) for more information as well.

Table 180 Configuration > Object > User/Group > Group

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so. Removing a group does not remove the user accounts in the group.
Object Reference	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 10.3.2 on page 165 for an example.
#	This field is a sequential value, and it is not associated with a specific user group.
Group Name	This field displays the name of each user group.
Description	This field displays the description for each user group.
Member	This field lists the members in the user group. Each member is separated by a comma.
Reference	This displays the number of times an object reference is used in a profile.

35.3.1 Group Add/Edit Screen

The **Group Add/Edit** screen allows you to create a new user group or edit an existing one. To access this screen, go to the **Group** screen (see [Section 35.3 on page 405](#)), and click either the **Add** icon or an **Edit** icon.

Figure 273 Configuration > User/Group > Group > Add

The following table describes the labels in this screen.

Table 181 Configuration > User/Group > Group > Add

LABEL	DESCRIPTION
Name	Type the name for this user group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User group names have to be different than user names.
Description	Enter the description of the user group, if any. You can use up to 60 characters, punctuation marks, and spaces.
Member List	The Member list displays the names of the users and user groups that have been added to the user group. The order of members is not important. Select users and groups from the Available list that you want to be members of this group and move them to the Member list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Move any members you do not want included to the Available list.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving your changes.

35.4 User/Group Setting Screen

The **Setting** screen controls default settings, login settings, lockout settings, and other user settings for the UAG. You can also use this screen to specify when users must log in to the UAG before it routes traffic for them.

To access this screen, log into the Web Configurator, and click **Configuration > Object > User/Group > Setting**.

Figure 274 Configuration > Object > User/Group > Setting

User Default Setting

Default Authentication Timeout Settings

[Edit](#)

#	User Type	Lease Time	Reauthentication Time
1	admin	1440	1440
2	limited-admin	1440	1440
3	ext-user	1440	1440
4	ext-group-user	1440	1440
5	guest-manager	1440	1440
6	pre-subscriber	1440	1440

Page 1 of 1 | Show 50 items | Displaying 1 - 6 of 6

Miscellaneous Settings

Allow renewing lease time automatically

Enable user idle detection

User idle timeout: (1-60 minutes)

User Logon Settings

Limit the number of simultaneous logons for administration account

Maximum number per administration account: (1-500)

Limit the number of simultaneous logons for access account

Maximum number per access account: (1-500)

Reach maximum number per account: Block Remove previous user and login

User Lockout Settings

Enable logon retry limit

Maximum retry count: (1-99)

Lockout period: (1-65535 minutes)

The following table describes the labels in this screen.

Table 182 Configuration > Object > User/Group > Setting

LABEL	DESCRIPTION
User Default Setting	
Default Authentication Timeout Settings	These authentication timeout settings are used by default when you create a new user account. They also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentication timeout settings.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
#	This field is a sequential value, and it is not associated with a specific entry.

Table 182 Configuration > Object > User/Group > Setting (continued)

LABEL	DESCRIPTION
User Type	<p>These are the kinds of user account the UAG supports.</p> <ul style="list-style-type: none"> • admin - this user can look at and change the configuration of the UAG • limited-admin - this user can look at the configuration of the UAG but not to change it • ext-user - this user account is maintained in a remote server, such as RADIUS. See Ext-User Accounts on page 400 for more information about this type. • ext-group-user - this user account is maintained in a remote server, such as RADIUS. See Ext-Group-User Accounts on page 400 for more information about this type. • guest-manager - this user can log in via the web configurator login screen and create dynamic guest accounts using the Account Generator screen that pops up. • pre-subscriber - this user has access to the UAG's services but cannot look at the configuration.
Lease Time	<p>This is the default lease time in minutes for each type of user account. It defines the number of minutes the user has to renew the current session before the user is logged out.</p> <p>Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the Renew button on their screen. If you allow access users to renew time automatically (see Section 35.4 on page 406), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.</p>
Reauthentication Time	<p>This is the default reauthentication time in minutes for each type of user account. It defines the number of minutes the user can be logged into the UAG in one session before having to log in again. Unlike Lease Time, the user has no opportunity to renew the session without logging out.</p>
Miscellaneous Settings	
Allow renewing lease time automatically	<p>Select this check box if access users can renew lease time automatically, as well as manually, simply by selecting the Updating lease time automatically check box on their screen.</p>
Enable user idle detection	<p>This is applicable for access users.</p> <p>Select this check box if you want the UAG to monitor how long each access user is logged in and idle (in other words, there is no traffic for this access user). The UAG automatically logs out the access user once the User idle timeout has been reached.</p>
User idle timeout	<p>This is applicable for access users.</p> <p>This field is effective when Enable user idle detection is checked. Type the number of minutes each access user can be logged in and idle before the UAG automatically logs out the access user.</p>
User Logon Settings	
Limit number of simultaneous logons for administration account	<p>Select this check box if you want to set a limit on the number of simultaneous logins by admin users. If you do not select this, admin users can log in as many times as they want at the same time using the same or different IP addresses.</p>
Maximum number per administration account	<p>This field is effective when Limit number of simultaneous logons for administration account is checked. Type the maximum number of simultaneous logins by each admin user.</p>
Limit number of simultaneous logons for access account	<p>Select this check box if you want to set a limit on the number of simultaneous logins by non-admin users. If you do not select this, access users can log in as many times as they want as long as they use different IP addresses.</p>
Maximum number per access account	<p>This field is effective when Limit number of simultaneous logons for access account is checked. Type the maximum number of simultaneous logins by each access user.</p>

Table 182 Configuration > Object > User/Group > Setting (continued)

LABEL	DESCRIPTION
Reach maximum number per account	Select Block to stop new users from logging in when the Maximum number per access account is reached. Select Remove previous user and login to disassociate the first user that logged in and allow new user to log in when the Maximum number per access account is reached.
User Lockout Settings	
Enable logon retry limit	Select this check box to set a limit on the number of times each user can login unsuccessfully (for example, wrong password) before the IP address is locked out for a specified amount of time.
Maximum retry count	This field is effective when Enable logon retry limit is checked. Type the maximum number of times each user can login unsuccessfully before the IP address is locked out for the specified Lockout period . The number must be between 1 and 99.
Lockout period	This field is effective when Enable logon retry limit is checked. Type the number of minutes the user must wait to try to login again, if logon retry limit is enabled and the Maximum retry count is reached. This number must be between 1 and 65,535 (about 45.5 days).
Apply	Click Apply to save the changes.
Reset	Click Reset to return the screen to its last-saved settings.

35.4.1 Default User Settings Edit Screens

The **Edit User Default Settings** screen allows you to set the default authentication timeout settings for the selected type of user account. These default authentication timeout settings also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentication timeout settings.

To access this screen, go to the **Configuration > Object > User/Group > Setting** screen (see [Section 35.4 on page 406](#)), and select one of the **Default Settings** section's entry and click the **Edit** icons.

Figure 275 Configuration > Object > User/Group > Setting > Edit

The screenshot shows a dialog box titled "Edit User Auth Settings". It contains the following fields and values:

- User Type: admin
- Lease Time: 1440 (0-1440 minutes, 0 is unlimited)
- Reauthentication Time: 1440 (0-1440 minutes, 0 is unlimited)

At the bottom right of the dialog are "OK" and "Cancel" buttons.

The following table describes the labels in this screen.

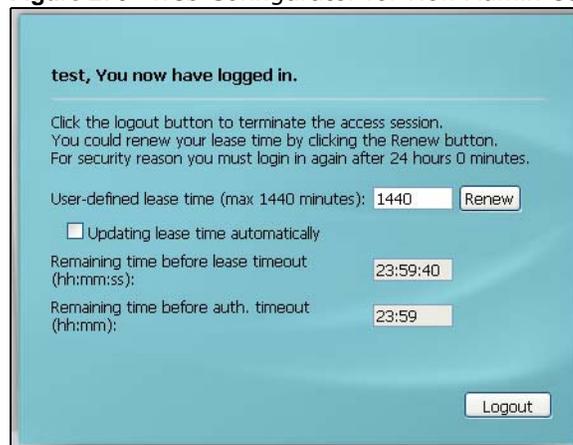
Table 183 Configuration > Object > User/Group > Setting > Edit

LABEL	DESCRIPTION
User Type	<p>This read-only field identifies the type of user account for which you are configuring the default settings.</p> <ul style="list-style-type: none"> • admin - this user can look at and change the configuration of the UAG • limited-admin - this user can look at the configuration of the UAG but not to change it. • ext-user - this user account is maintained in a remote server, such as RADIUS. See Ext-User Accounts on page 400 for more information about this type. • ext-group-user - this user account is maintained in a remote server, such as RADIUS. See Ext-Group-User Accounts on page 400 for more information about this type. • guest-manager - this user can log in via the web configurator login screen and create dynamic guest accounts using the Account Generator screen that pops up. • pre-subscriber - this user has access to the UAG's services but cannot look at the configuration.
Lease Time	<p>Enter the number of minutes this type of user account has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited.</p> <p>Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the Renew button on their screen. If you allow access users to renew time automatically (see Section 35.4 on page 406), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.</p>
Reauthentication Time	<p>Select this option and type the number of minutes this type of user account can be logged into the UAG in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike Lease Time, the user has no opportunity to renew the session without logging out.</p>
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving your changes.

35.4.2 User Aware Login Example

Access users cannot use the Web Configurator to browse the configuration of the UAG. Instead, after access users log into the UAG, the following status screen appears.

Figure 276 Web Configurator for Non-Admin Users



The following table describes the labels in this screen.

Table 184 Web Configurator for Non-Admin Users

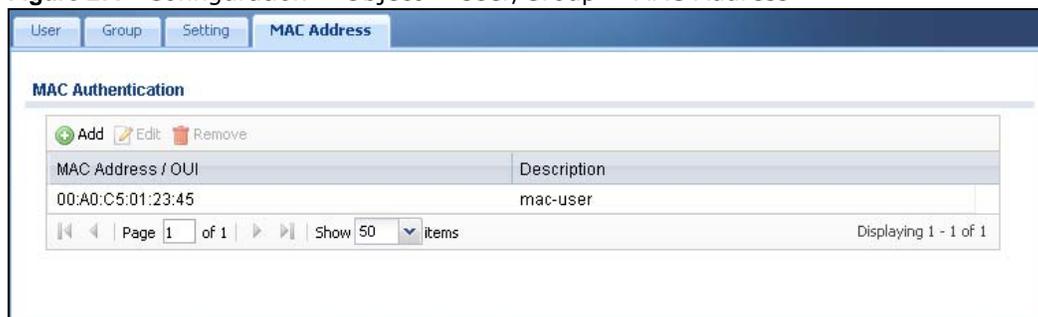
LABEL	DESCRIPTION
User-defined lease time (max ... minutes)	Access users can specify a lease time shorter than or equal to the one that you specified. The default value is the lease time that you specified.
Renew	Access users can click this button to reset the lease time, the amount of time remaining before the UAG automatically logs them out. The UAG sets this amount of time according to the <ul style="list-style-type: none"> • User-defined lease time field in this screen • Lease time field in the User Add/Edit screen (see Section 35.2.1 on page 402) • Lease time field in the Setting > Edit screen (see Section 35.4 on page 406)
Updating lease time automatically	This box appears if you checked the Allow renewing lease time automatically box in the Setting screen. (See Section 35.4 on page 406 .) Access users can select this check box to reset the lease time automatically 30 seconds before it expires. Otherwise, access users have to click the Renew button to reset the lease time.
Remaining time before lease timeout	This field displays the amount of lease time that remains, though the user might be able to reset it.
Remaining time before auth. timeout	This field displays the amount of time that remains before the UAG automatically logs the access user out, regardless of the lease time.

35.5 MAC Address Screen

This screen shows the MAC addresses of wireless clients, which can be authenticated by their MAC addresses using the local user database. Click **Configuration > Object > User/Group > MAC Address** to open this screen.

Note: You need to configure an SSID security profile's MAC authentication settings to have the AP use the UAG's local database to authenticate wireless clients by their MAC addresses.

Figure 277 Configuration > Object > User/Group > MAC Address



The following table describes the labels in this screen.

Table 185 Configuration > Object > User/Group > MAC Address

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
MAC Address/OUI	The wireless client MAC address or OUI (Organizationally Unique Identifier). The OUI is the first three octets in a MAC address and uniquely identifies the manufacturer of a network device.
Description	This field displays the description for each entry.

35.5.1 Add/Edit MAC Address

Use this screen to configure the wireless client's MAC address and save it into the UAG's local user database for MAC authentication.

Figure 278 Configuration > Object > User/Group > MAC Address > Add

The following table describes the labels in this screen.

Table 186 Configuration > Object > User/Group > MAC Address > Add/Edit

LABEL	DESCRIPTION
MAC Address/OUI	Specify the wireless client's MAC address or OUI (Organizationally Unique Identifier). The OUI is the first three octets in a MAC address and uniquely identifies the manufacturer of a network device. This field is read-only if you are editing an existing entry.
Description	Enter the description of the entry.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving your changes.

35.6 User /Group Technical Reference

This section provides some information on users who use an external authentication server in order to log in.

Setting up User Attributes in an External Server

To set up user attributes, such as reauthentication time, in RADIUS servers, use the following keywords in the user configuration file.

Table 187 RADIUS: Keywords for User Attributes

KEYWORD	CORRESPONDING ATTRIBUTE IN WEB CONFIGURATOR
type	User Type. Possible Values: admin, limited-admin, pre-subscriber, dynamic-guest.
leaseTime	Lease Time. Possible Values: 1-1440 (minutes).
reauthTime	Reauthentication Time. Possible Values: 1-1440 (minutes).

The following example shows you how you might set up user attributes in RADIUS servers.

Figure 279 RADIUS Example: Keywords for User Attributes

```
type=user;leaseTime=222;reauthTime=222
```

Creating a Large Number of Ext-User Accounts

If you plan to create a large number of **Ext-User** accounts, you might use CLI commands, instead of the Web Configurator, to create the accounts. Extract the user names from the RADIUS server, and create a shell script that creates the user accounts. See [Chapter 48 on page 549](#) for more information about shell scripts.

36.1 Overview

This chapter shows you how to configure preset profiles for the Access Points (APs) connected to your UAG's wireless network.

36.1.1 What You Can Do in this Chapter

- The **Radio** screen ([Section 36.2 on page 415](#)) creates radio configurations that can be used by the APs.
- The **SSID** screen ([Section 36.3 on page 420](#)) configures three different types of profiles for your networked APs.

36.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

Wireless Profiles

At the heart of all wireless AP configurations on the UAG are profiles. A profile represents a group of saved settings that you can use across any number of connected APs. You can set up the following wireless profile types:

- **Radio** - This profile type defines the properties of an AP's radio transmitter. You can have a maximum of 32 radio profiles on the UAG2100 and the UAG4100, or 64 radio profiles on the UAG5100.
- **SSID** - This profile type defines the properties of a single wireless network signal broadcast by an AP. Each radio on a single AP can broadcast up to 8 SSIDs. You can have a maximum of 32 SSID profiles on the UAG2100 and the UAG4100, or 64 SSID profiles on the UAG5100.
- **Security** - This profile type defines the security settings used by a single SSID. It controls the encryption method required for a wireless client to associate itself with the SSID. You can have a maximum of 32 security profiles on the UAG2100 and the UAG4100, or 64 security profiles on the UAG5100.
- **MAC Filtering** - This profile provides an additional layer of security for an SSID, allowing you to block access or allow access to that SSID based on wireless client MAC addresses. If a client's MAC address is on the list, then it is either allowed or denied, depending on how you set up the MAC Filter profile. You can have a maximum of 32 MAC filtering profiles on the UAG2100 and the UAG4100, or 64 MAC filtering profiles on the UAG5100.

SSID

The SSID (Service Set Identifier) is the name that identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. In other words, it is the name of the wireless network that clients use to connect to it.

WEP

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the AP and the wireless stations associated with it in order to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. Key differences between WPA(2) and WEP are improved data encryption and user authentication.

IEEE 802.1x

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication is done using an external RADIUS server.

36.2 Radio Screen

This screen allows you to create radio profiles for the APs on your network. A radio profile is a list of settings that a supported managed AP (NWA5121-N for example) can use to configure either one of its two radio transmitters. To access this screen click **Configuration > Object > AP Profile**.

Figure 280 Configuration > Object > AP Profile > Radio

The screenshot shows the 'Radio' configuration screen. At the top, there are tabs for 'Radio' and 'SSID'. Below the tabs is a 'Radio Summary' section. This section contains a toolbar with icons for 'Add', 'Edit', 'Remove', 'Activate', 'Inactivate', and 'Object Reference'. Below the toolbar is a table with the following data:

#	Status	Profile Name	Frequency Band	Channel ID	Schedule
1		default	2.4G	6	none
2		default2	5G	36	none

Below the table, there is a pagination control showing 'Page 1 of 1' and 'Show 50 items'. At the bottom right of the table area, it says 'Displaying 1 - 2 of 2'. At the bottom of the screen, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 188 Configuration > Object > AP Profile > Radio

LABEL	DESCRIPTION
Add	Click this to add a new radio profile.
Edit	Click this to edit the selected radio profile.
Remove	Click this to remove the selected radio profile.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
Object Reference	Click this to view which other objects are linked to the selected radio profile.
#	This field is a sequential value, and it is not associated with a specific profile.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Profile Name	This field indicates the name assigned to the radio profile.
Frequency Band	This field indicates the frequency band which this radio profile is configured to use.
Channel ID	This field indicates the broadcast channel which this radio profile is configured to use.
Schedule	This field indicates the name of the schedule object used in this radio profile. none means the WLAN of the managed AP (to which the radio profile is applied) is active at all times if the profile is enabled.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

36.2.1 Add/Edit Radio Profile

This screen allows you to create a new radio profile or edit an existing one. To access this screen, click the **Add** button or select a radio profile from the list and click the **Edit** button.

Figure 281 Configuration > Object > AP Profile > Add/Edit Radio Profile

Add Radio Profile

Hide Advanced Settings Create new Object

General Settings

Activate

Profile Name:

802.11 Band: 2.4G

Mode: b/g/n

Channel: 6

Schedule: none

Advanced Settings

Channel Width: Auto 20 MHz

Guard Interval: Short Long

Enable A-MPDU Aggregation

A-MPDU Limit: 50000 (100~65535)

A-MPDU Subframe: 32 (2~64)

Enable A-MSDU Aggregation

A-MSDU Limit: 4096 (2290~4096)

RTS/CTS Threshold: 2347 (0~2347)

Beacon Interval: 100 (40ms~1000ms)

DTIM: 1 (1~255)

Output Power: Max

Enable Signal Threshold

Station Signal Threshold: -76 dBm (-20 ~ -76)

Disassociate Station Threshold: -90 dbm (-20 ~ -90)

Allow Station Connection after Multiple Retries

Station Retry Count: 6 (1 ~ 100)

Rate Configuration

Basic Rate (Mbps): 1 2 5.5 11 6 9 12 18 24 36 48 54

Support Rate (Mbps): 1 2 5.5 11 6 9 12 18 24 36 48 54

MCS Rate: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Multicast Settings

Transmission Mode: Multicast to Unicast Fixed Multicast Rate

Multicast Rate (Mbps): 1 2 5.5 11 6 9 12 18 24 36 48 54

MBSSID Settings

Edit

#	SSID Profile
1	default
2	disable
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable

Apply Reset OK Cancel

The following table describes the labels in this screen.

Table 189 Configuration > Object > AP Profile > Add/Edit Radio Profile

LABEL	DESCRIPTION
Hide / Show Advanced Settings	Click this to hide or show the Advanced Settings in this window.
Create New Object	Select an item from this menu to create a new object of that type. Any objects created in this way are automatically linked to this radio profile.
General Settings	
Activate	Select this option to make this profile active.
Profile Name	Enter up to 31 alphanumeric characters to be used as this profile's name. Underscores are allowed.
802.11 Band	Select the wireless band which this radio profile should use. 2.4 GHz is the frequency used by IEEE 802.11b/g/n wireless clients. 5 GHz is the frequency used by IEEE 802.11a/n wireless clients.
Mode	Select how to let wireless clients connect to the AP. When using the 2.4 GHz band, select b/g to let IEEE 802.11b and IEEE 802.11g compliant WLAN devices associate with the AP. When using the 2.4 GHz band, select b/g/n to let IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n compliant WLAN devices associate with the AP. When using the 5 GHz band, select a to let only IEEE 802.11a compliant WLAN devices associate with the AP. When using the 5 GHz band, select a/n to let IEEE 802.11a and IEEE 802.11n compliant WLAN devices associate with the AP.
Channel	Select the wireless channel which this radio profile should use. It is recommended that you choose the channel least in use by other APs in the region where this profile will be implemented. This will reduce the amount of interference between wireless clients and the AP to which this profile is assigned. Some 5 GHz channels include the label indoor use only . These are for use with an indoor AP only. Do not use them with an outdoor AP.
Schedule	Select a schedule to control when the WLAN of the managed AP (to which this radio profile is applied) is turned on. Otherwise, select none and the managed AP's WLAN is always enabled.
Advanced Settings	
Channel Width	Select the channel bandwidth you want to use for your wireless network. Select Auto to allow the UAG to adjust the channel bandwidth to 40 MHz or 20 MHz depending on network conditions. Select 20 MHz if you want to lessen radio interference with other wireless devices in your neighborhood.
Guard Interval	Set the guard interval for this radio profile to either short or long . The guard interval is the gap introduced between data transmission from users in order to reduce interference. Reducing the interval increases data transfer rates but also increases interference. Increasing the interval reduces data transfer rates but also reduces interference.
Enable A-MPDU Aggregation	Select this to enable A-MPDU aggregation. Message Protocol Data Unit (MPDU) aggregation collects Ethernet frames along with their 802.11n headers and wraps them in a 802.11n MAC header. This method is useful for increasing bandwidth throughput in environments that are prone to high error rates.

Table 189 Configuration > Object > AP Profile > Add/Edit Radio Profile (continued)

LABEL	DESCRIPTION
A-MPDU Limit	Enter the maximum frame size to be aggregated.
A-MPDU Subframe	Enter the maximum number of frames to be aggregated each time.
Enable A-MSDU Aggregation	Select this to enable A-MSDU aggregation. Mac Service Data Unit (MSDU) aggregation collects Ethernet frames without any of their 802.11n headers and wraps the header-less payload in a single 802.11n MAC header. This method is useful for increasing bandwidth throughput. It is also more efficient than A-MPDU except in environments that are prone to high error rates.
A-MSDU Limit	Enter the maximum frame size to be aggregated.
RTS/CTS Threshold	Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions). A wireless client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS/CTS equal to or higher than the fragmentation threshold to turn RTS/CTS off.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. A high value helps save current consumption of the access point.
DTIM	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255.
Output Power	Set the output power of the AP in this field. If there is a high density of APs in an area, decrease the output power of the NWA5160N to reduce interference with other APs. Select one of the following Max , -3dB (50%) , -6dB (25%) , -9dB (12.5%) , or Min . See the product specifications for more information on your UAG's output power. Note: Reducing the output power also reduces the UAG's effective broadcast radius.
Enable Signal Threshold	Select the check box to use the signal threshold to ensure wireless clients receive good throughput. This allows only wireless clients with a strong signal to connect to the AP. Clear the check box to not require wireless clients to have a minimum signal strength to connect to the AP.
Station Signal Threshold	Set a minimum client signal strength. A wireless client is allowed to connect to the AP only when its signal strength is stronger than the specified threshold. -20 dBm is the strongest signal you can require and -76 is the weakest.
Disassociate Station Threshold	Set a minimum kick-off signal strength. When a wireless client's signal strength is lower than the specified threshold, the UAG disconnects the wireless client from the AP. -20 dBm is the strongest signal you can require and -90 is the weakest.
Allow Station Connection after Multiple Retries	Select this option to allow a wireless client to try to associate with the AP again after it is disconnected due to weak signal strength.
Station Retry Count	Set the maximum number of times a wireless client can attempt to re-connect to the AP

Table 189 Configuration > Object > AP Profile > Add/Edit Radio Profile (continued)

LABEL	DESCRIPTION
Rate Configuration	<p>This section controls the data rates permitted for clients.</p> <p>For each Rate, select a rate option from its list. The rates are:</p> <ul style="list-style-type: none"> • Basic Rate (Mbps) - Set the basic rate configuration in Mbps. • Support Rate (Mbps) - Set the support rate configuration in Mbps. • MCS Rate - Set the MCS rate configuration. IEEE 802.11n supports many different data rates which are called MCS rates. MCS stands for Modulation and Coding Scheme. This is an 802.11n feature that increases the wireless network performance in terms of throughput.
Multicast Settings	Use this section to set a transmission mode and maximum rate for multicast traffic.
Transmission Mode	<p>Set how the AP handles multicast traffic.</p> <p>Select Multicast to Unicast to broadcast wireless multicast traffic to all of the wireless clients as unicast traffic. Unicast traffic dynamically changes the data rate based on the application's bandwidth requirements. The retransmit mechanism of unicast traffic provides more reliable transmission of the multicast traffic, although it also produces duplicate packets.</p> <p>Select Fixed Multicast Rate to send wireless multicast traffic at a single data rate. You must know the multicast application's bandwidth requirements and set it in the following field.</p>
Multicast Rate (Mbps)	If you set the multicast transmission mode to fixed multicast rate, set the data rate for multicast traffic here. For example, to deploy 4 Mbps video, select a fixed multicast rate higher than 4 Mbps.
MBSSID Settings	This section allows you to associate an SSID profile with the radio profile.
Edit	Select an SSID and click this button to reassign it. The selected SSID becomes editable immediately upon clicking.
#	This field is a sequential value, and it is not associated with a specific profile.
SSID Profile	Indicates which SSID profile is associated with this radio profile.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving your changes.

36.3 SSID Screen

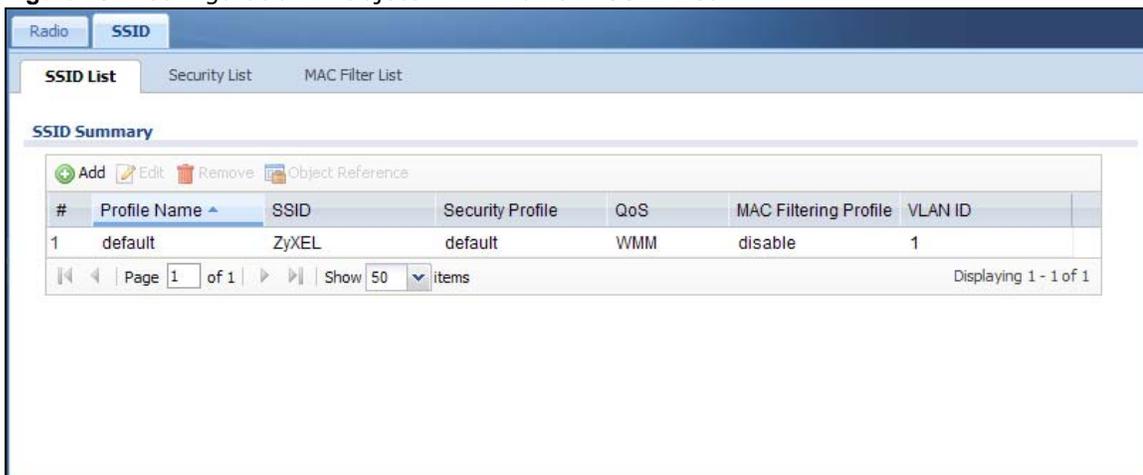
The SSID screens allow you to configure three different types of profiles for your networked APs: an SSID list, which can assign specific SSID configurations to your APs; a security list, which can assign specific encryption methods to the APs when allowing wireless clients to connect to them; and a MAC filter list, which can limit connections to an AP based on wireless clients MAC addresses.

36.3.1 SSID List

This screen allows you to create and manage SSID configurations that can be used by the APs. An SSID, or Service Set Identifier, is basically the name of the wireless network to which a wireless client can connect. The SSID appears as readable text to any device capable of scanning for wireless frequencies (such as the WiFi adapter in a laptop), and is displayed as the wireless network name when a person makes a connection to it.

To access this screen click **Configuration > Object > AP Profile > SSID**.

Figure 282 Configuration > Object > AP Profile > SSID List



The following table describes the labels in this screen.

Table 190 Configuration > Object > AP Profile > SSID List

LABEL	DESCRIPTION
Add	Click this to add a new SSID profile.
Edit	Click this to edit the selected SSID profile.
Remove	Click this to remove the selected SSID profile.
Object Reference	Click this to view which other objects are linked to the selected SSID profile (for example, radio profile).
#	This field is a sequential value, and it is not associated with a specific profile.
Profile Name	This field indicates the name assigned to the SSID profile.
SSID	This field indicates the SSID name as it appears to wireless clients.
Security Profile	This field indicates which (if any) security profile is associated with the SSID profile.
QoS	This field indicates the QoS type associated with the SSID profile.
MAC Filtering Profile	This field indicates which (if any) MAC Filter Profile is associated with the SSID profile.
VLAN ID	This field indicates the VLAN ID associated with the SSID profile.

36.3.2 Add/Edit SSID Profile

This screen allows you to create a new SSID profile or edit an existing one. To access this screen, click the **Add** button or select an SSID profile from the list and click the **Edit** button.

Figure 283 Configuration > Object > AP Profile > SSID List: Add/Edit SSID Profile

The following table describes the labels in this screen.

Table 191 Configuration > Object > AP Profile > SSID List: Add/Edit SSID Profile

LABEL	DESCRIPTION
Create new Object	Select an object type from the list to create a new one associated with this SSID profile.
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Underscores are allowed.
SSID	Enter the SSID name for this profile. This is the name visible on the network to wireless clients. Enter up to 32 characters, spaces and underscores are allowed.
Security Profile	Select a security profile from this list to associate with this SSID. If none exist, you can use the Create new Object menu to create one. Note: It is highly recommended that you create security profiles for all of your SSIDs to enhance your network security.
MAC Filtering Profile	Select a MAC filtering profile from the list to associate with this SSID. If none exist, you can use the Create new Object menu to create one. MAC filtering allows you to limit the wireless clients connecting to your network through a particular SSID by wireless client MAC addresses. Any clients that have MAC addresses not in the MAC filtering profile of allowed addresses are denied connections. The disable setting means no MAC filtering is used.

Table 191 Configuration > Object > AP Profile > SSID List: Add/Edit SSID Profile (continued)

LABEL	DESCRIPTION
QoS	<p>Select a Quality of Service (QoS) access category to associate with this SSID. Access categories minimize the delay of data packets across a wireless network. Certain categories, such as video or voice, are given a higher priority due to the time sensitive nature of their data packets.</p> <p>QoS access categories are as follows:</p> <p>disable: Turns off QoS for this SSID. All data packets are treated equally and not tagged with access categories.</p> <p>WMM: Enables automatic tagging of data packets. The UAG assigns access categories to the SSID by examining data as it passes through it and making a best guess effort. If something looks like video traffic, for instance, it is tagged as such.</p> <p>WMM_VOICE: All wireless traffic to the SSID is tagged as voice data. This is recommended if an SSID is used for activities like placing and receiving VoIP phone calls.</p> <p>WMM_VIDEO: All wireless traffic to the SSID is tagged as video data. This is recommended for activities like video conferencing.</p> <p>WMM_BEST_EFFORT: All wireless traffic to the SSID is tagged as "best effort," meaning the data travels the best route it can without displacing higher priority traffic. This is good for activities that do not require the best bandwidth throughput, such as surfing the Internet.</p> <p>WMM_BACKGROUND: All wireless traffic to the SSID is tagged as low priority or "background traffic", meaning all other access categories take precedence over this one. If traffic from an SSID does not have strict throughput requirements, then this access category is recommended. For example, an SSID that only has network printers connected to it.</p>
Rate Limiting	
Downlink	Define the maximum incoming transmission data rate (either in mbps or kbps) on a per-station basis.
Uplink	Define the maximum outgoing transmission data rate (either in mbps or kbps) on a per-station basis.
Band Select	<p>To improve network performance and avoid interference in the 2.4 GHz frequency band, you can enable this feature to use the 5 GHz band first. You should set 2.4GHz and 5 GHz radio profiles to use the same SSID and security settings.</p> <p>Select standard to have the AP try to connect the wireless clients to the same SSID using the 5 GHz band. Connections to an SSID using the 2.4GHz band are still allowed.</p> <p>Otherwise, select disable to turn off this feature.</p>
VLAN ID	Enter the VLAN ID that will be used to tag all traffic originating from this SSID if the VLAN is different from the native VLAN.
Hidden SSID	<p>Select this if you want to "hide" your SSID from wireless clients. This tells any wireless clients in the vicinity of the AP using this SSID profile not to display its SSID name as a potential connection. Not all wireless clients respect this flag and display it anyway.</p> <p>When an SSID is "hidden" and a wireless client cannot see it, the only way you can connect to the SSID is by manually entering the SSID name in your wireless connection setup screen(s) (these vary by client, client connectivity software, and operating system).</p>
Enable Intra-BSS Traffic Blocking	Select this option to prevent crossover traffic from within the same SSID.
Local VAP Setting	This section is available only on the UAG that supports a local AP.
VLAN Support	Select ON to tag traffic from the local Virtual AP (VAP) with the VLAN ID specified in this SSID profile. Otherwise, select Off .

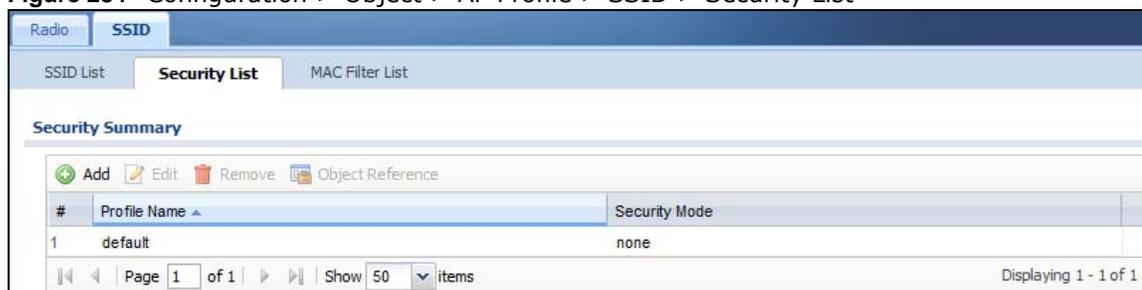
Table 191 Configuration > Object > AP Profile > SSID List: Add/Edit SSID Profile (continued)

LABEL	DESCRIPTION
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving your changes.

36.3.3 Security List

This screen allows you to manage wireless security configurations that can be used by your SSIDs. Wireless security is implemented strictly between the AP broadcasting the SSID and the stations that are connected to it.

To access this screen click **Configuration > Object > AP Profile > SSID > Security List**.

Figure 284 Configuration > Object > AP Profile > SSID > Security List

The following table describes the labels in this screen.

Table 192 Configuration > Object > AP Profile > SSID > Security List

LABEL	DESCRIPTION
Add	Click this to add a new security profile.
Edit	Click this to edit the selected security profile.
Remove	Click this to remove the selected security profile.
Object Reference	Click this to view which other objects are linked to the selected security profile (for example, SSID profile).
#	This field is a sequential value, and it is not associated with a specific profile.
Profile Name	This field indicates the name assigned to the security profile.
Security Mode	This field indicates this profile's security mode (if any).

36.3.4 Add/Edit Security Profile

This screen allows you to create a new security profile or edit an existing one. To access this screen, click the **Add** button or select a security profile from the list and click the **Edit** button.

Note: This screen's options change based on the **Security Mode** selected. Only the default screen is displayed here.

Figure 285 Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile

The following table describes the labels in this screen.

Table 193 Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile

LABEL	DESCRIPTION
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Underscores are allowed.
Security Mode	Select a security mode from the list: none , wep , wpa2 , or wpa2-mix .

Table 193 Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile

LABEL	DESCRIPTION
Radius Server Type	Select Internal to use the UAG's internal authentication database, or External to use an external RADIUS server for authentication.
Primary / Secondary Radius Server Activate	Select this to have the UAG use the specified RADIUS server.
Radius Server IP Address	Enter the IP address of the RADIUS server to be used for authentication.
Radius Server Port	Enter the port number of the RADIUS server to be used for authentication.
Radius Server Secret	Enter the shared secret password of the RADIUS server to be used for authentication.
MAC Authentication	Select this to use an external server or the UAG's local database to authenticate wireless clients by their MAC addresses. Users cannot get an IP address if the MAC authentication fails. An external server can use the wireless client's account (username/password) or Calling Station ID for MAC authentication. Configure the ones the external server uses.
Auth. Method	This field is available only when you set the RADIUS server type to Internal . Select an authentication method if you have created any in the Configuration > Object > Auth. Method screen.
Delimiter (Account)	Select the separator the external server uses for the two-character pairs within account MAC addresses.
Case (Account)	Select the case (upper or lower) the external server requires for letters in the account MAC addresses.
Delimiter (Calling Station ID)	RADIUS servers can require the MAC address in the Calling Station ID RADIUS attribute. Select the separator the external server uses for the pairs in calling station MAC addresses.
Case (Calling Station ID)	Select the case (upper or lower) the external server requires for letters in the calling station MAC addresses.
802.1X	Select this to enable 802.1x secure authentication.
Auth. Method	This field is available only when you set the RADIUS server type to Internal . Select an authentication method if you have created any in the Configuration > Object > Auth. Method screen.
Reauthentication Timer	Enter the interval (in seconds) between authentication requests. Enter a 0 for unlimited requests.
The following fields are available if you set Security Mode to wep .	
Idle Timeout	Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued.
Authentication Type	Select a WEP authentication method. Choices are Open or Share key.

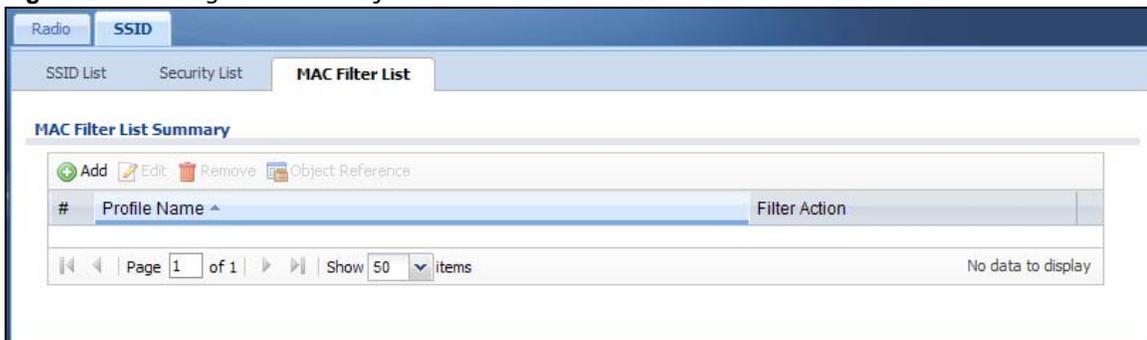
Table 193 Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile

LABEL	DESCRIPTION
Key Length	<p>Select the bit-length of the encryption key to be used in WEP connections.</p> <p>If you select WEP-64:</p> <ul style="list-style-type: none"> Enter 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x11AA22BB33) for each Key used. <p>or</p> <ul style="list-style-type: none"> Enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for each Key used. <p>If you select WEP-128:</p> <ul style="list-style-type: none"> Enter 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x00112233445566778899AABBCC) for each Key used. <p>or</p> <ul style="list-style-type: none"> Enter 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for each Key used.
Key 1~4	Based on your Key Length selection, enter the appropriate length hexadecimal or ASCII key.
The following fields are available if you set Security Mode to wpa2 or wpa2-mix .	
PSK	Select this option to use a Pre-Shared Key with WPA encryption.
Pre-Shared Key	Enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
Cipher Type	<p>Select an encryption cipher type from the list.</p> <ul style="list-style-type: none"> auto - This automatically chooses the best available cipher based on the cipher in use by the wireless client that is attempting to make a connection. tkip - This is the Temporal Key Integrity Protocol encryption method added later to the WEP encryption protocol to further secure. Not all wireless clients may support this. aes - This is the Advanced Encryption Standard encryption method. It is a more recent development over TKIP and considerably more robust. Not all wireless clients may support this.
Idle Timeout	Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued.
Group Key Update Timer	Enter the interval (in seconds) at which the AP updates the group WPA encryption key.
Pre-Authentication	<p>This field is available only when you set Security Mode to wpa2 or wpa2-mix and enable 802.1x authentication.</p> <p>Enable or Disable pre-authentication to allow the AP to send authentication information to other APs on the network, allowing connected wireless clients to switch APs without having to re-authenticate their network connection.</p>
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving your changes.

36.3.5 MAC Filter List

This screen allows you to create and manage security configurations that can be used by your SSIDs. To access this screen click **Configuration > Object > AP Profile > SSID > MAC Filter List**.

Figure 286 Configuration > Object > AP Profile > SSID > MAC Filter List



The following table describes the labels in this screen.

Table 194 Configuration > Object > AP Profile > SSID > MAC Filter List

LABEL	DESCRIPTION
Add	Click this to add a new MAC filtering profile.
Edit	Click this to edit the selected MAC filtering profile.
Remove	Click this to remove the selected MAC filtering profile.
Object Reference	Click this to view which other objects are linked to the selected MAC filtering profile (for example, SSID profile).
#	This field is a sequential value, and it is not associated with a specific profile.
Profile Name	This field indicates the name assigned to the MAC filtering profile.
Filter Action	This field indicates this profile's filter action (if any).

36.3.6 Add/Edit MAC Filter Profile

This screen allows you to create a new MAC filtering profile or edit an existing one. To access this screen, click the **Add** button or select a MAC filter profile from the list and click the **Edit** button.

Figure 287 SSID > MAC Filter List > Add/Edit MAC Filter Profile

The following table describes the labels in this screen.

Table 195 SSID > MAC Filter List > Add/Edit MAC Filter Profile

LABEL	DESCRIPTION
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Underscores are allowed.
Filter Action	Select allow to permit the wireless client with the MAC addresses in this profile to connect to the network through the associated SSID; select deny to block the wireless clients with the specified MAC addresses.
Add	Click this to add a MAC address to the profile's list.
Edit	Click this to edit the selected MAC address in the profile's list.
Remove	Click this to remove the selected MAC address from the profile's list.
#	This field is a sequential value, and it is not associated with a specific profile.
MAC	This field specifies a MAC address associated with this profile.
Description	This field displays a description for the MAC address associated with this profile. You can click the description to make it editable. Enter up to 60 characters, spaces and underscores allowed.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving your changes.

MON Profile

37.1 Overview

This screen allows you to set up monitor mode configurations that allow your connected APs to scan for other wireless devices in the vicinity. Once detected, you can use the **MON Mode** screen ([Section 9.4 on page 144](#)) to classify them as either rogue or friendly and then manage them accordingly.

37.1.1 What You Can Do in this Chapter

The **MON Profile** screen ([Section 37.2 on page 430](#)) creates preset monitor mode configurations that can be used by the APs.

37.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

Active Scan

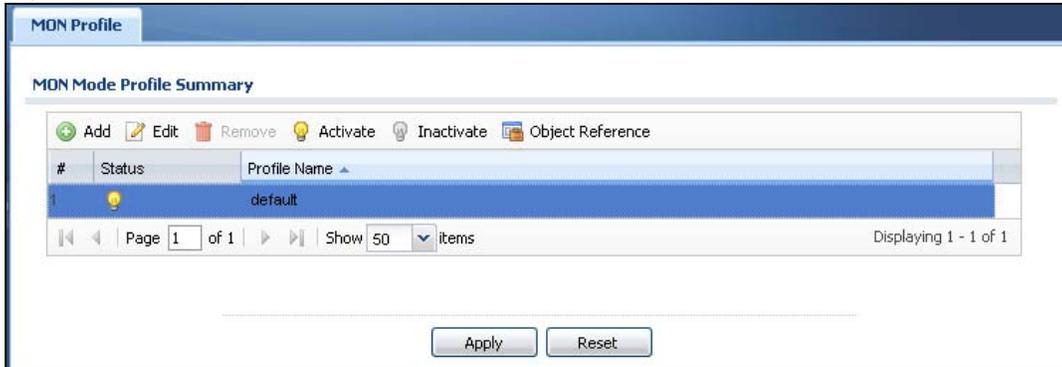
An active scan is performed when an 802.11-compatible wireless monitoring device is explicitly triggered to scan a specified channel or number of channels for other wireless devices broadcasting on the 802.11 frequencies by sending probe request frames.

Passive Scan

A passive scan is performed when an 802.11-compatible monitoring device is set to periodically listen to a specified channel or number of channels for other wireless devices broadcasting on the 802.11 frequencies.

37.2 MON Profile

This screen allows you to create monitor mode configurations that can be used by the APs. To access this screen, login to the Web Configurator, and click **Configuration > Object > MON Profile**.

Figure 288 Configuration > Object > MON Profile

The following table describes the labels in this screen.

Table 196 Configuration > Object > MON Profile

LABEL	DESCRIPTION
Add	Click this to add a new monitor mode profile.
Edit	Click this to edit the selected monitor mode profile.
Remove	Click this to remove the selected monitor mode profile.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
Object Reference	Click this to view which other objects are linked to the selected monitor mode profile (for example, an AP management profile).
#	This field is a sequential value, and it is not associated with a specific user.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Profile Name	This field indicates the name assigned to the monitor profile.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

37.2.1 Add/Edit MON Profile

This screen allows you to create a new monitor mode profile or edit an existing one. To access this screen, click the **Add** button or select an existing monitor mode profile and click the **Edit** button.

Figure 289 Configuration > Object > MON Profile > Add/Edit MON Profile

The following table describes the labels in this screen.

Table 197 Configuration > Object > MON Profile > Add/Edit MON Profile

LABEL	DESCRIPTION
Activate	Select this to activate this monitor mode profile.
Profile Name	This field indicates the name assigned to the monitor mode profile.
Channel dwell time	Enter the interval (in milliseconds) before the AP switches to another channel for monitoring.
Scan Channel Mode	Select auto to have the AP switch to the next sequential channel once the Channel dwell time expires. Select manual to set specific channels through which to cycle sequentially when the Channel dwell time expires. Selecting this options makes the Scan Channel List options available.
Set Scan Channel List (2.4 GHz)	Move a channel from the Available channels column to the Channels selected column to have the APs using this profile scan that channel when Scan Channel Mode is set to manual. These channels are limited to the 2 GHz range (802.11 b/g/n).

Table 197 Configuration > Object > MON Profile > Add/Edit MON Profile (continued)

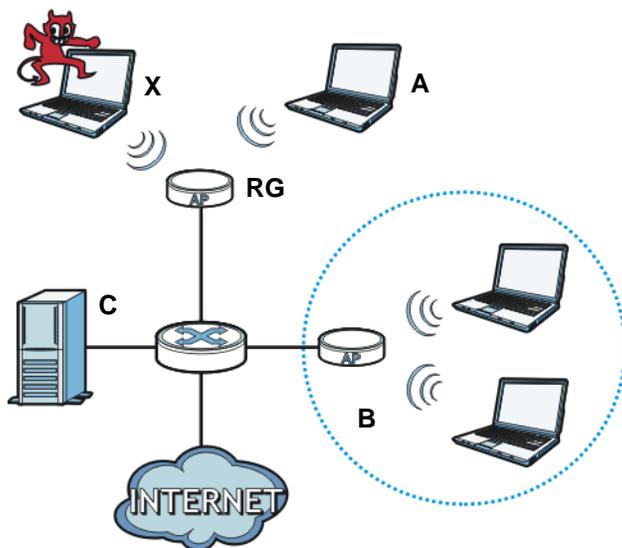
LABEL	DESCRIPTION
Set Scan Channel List (5 GHz)	Move a channel from the Available channels column to the Channels selected column to have the APs using this profile scan that channel when Scan Channel Mode is set to manual. These channels are limited to the 5 GHz range (802.11 a/n).
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving your changes.

37.3 Technical Reference

The following section contains additional technical information about the features described in this chapter.

Rogue APs

Rogue APs are wireless access points operating in a network's coverage area that are not under the control of the network's administrators, and can open up holes in a network's security. Attackers can take advantage of a rogue AP's weaker (or non-existent) security to gain access to the network, or set up their own rogue APs in order to capture information from wireless clients. If a scan reveals a rogue AP, you can use commercially-available software to physically locate it.

Figure 290 Rogue AP Example

In the example above, a corporate network's security is compromised by a rogue AP (**RG**) set up by an employee at his workstation in order to allow him to connect his notebook computer wirelessly (**A**). The company's legitimate wireless network (the dashed ellipse **B**) is well-secured, but the rogue AP uses inferior security that is easily broken by an attacker (**X**) running readily available encryption-cracking software. In this example, the attacker now has access to the company network, including sensitive data stored on the file server (**C**).

Friendly APs

If you have more than one AP in your wireless network, you should also configure a list of “friendly” APs. Friendly APs are other wireless access points that are detected in your network, as well as any others that you know are not a threat (those from recognized networks, for example). It is recommended that you export (save) your list of friendly APs often, especially if you have a network with a large number of access points.

Application

38.1 Overview

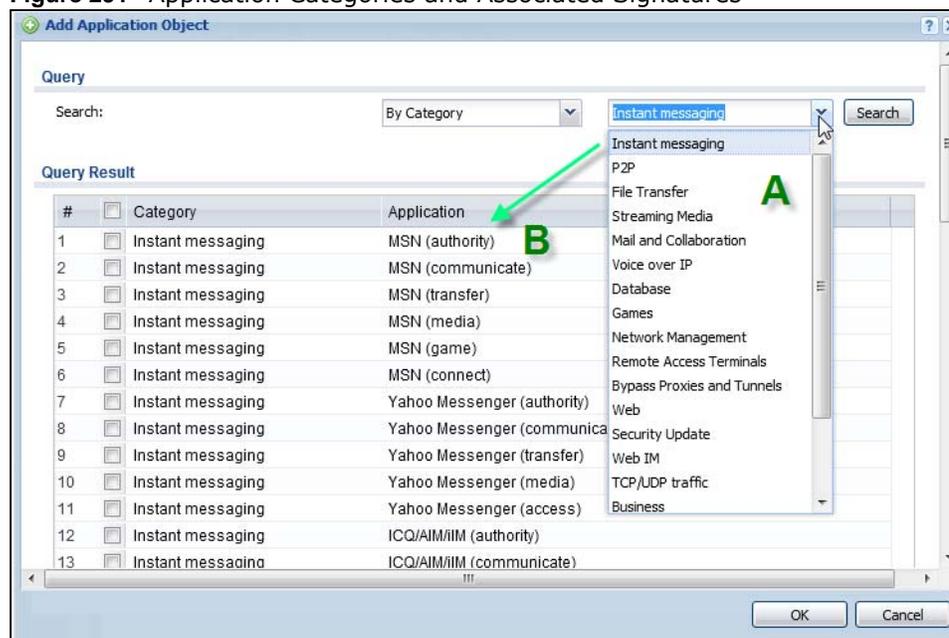
The UAG identifies applications by either their port or signature. Go to **Configuration > Licensing > Signature Update > AppPatrol** to check that you have the latest App Patrol signatures. These signatures are available to create application objects in **Configuration > Object > Application > Application**. Categories of applications include (at the time of writing):

Table 198 Categories of Applications

• Instant Messaging	• P2P	• File Transfer
• Streaming Media	• Mail and Collaboration	• Voice over IP
• Database	• Games	• Network Management
• Remote Access Terminals	• Bypass Proxies and Tunnels	• Web
• Security Update	• Web IM	• TCP/UDP traffic
• Business	• Network Protocols	• Mobile
• Private Protocol	• Social Network	•

The following table shows the types of categories currently supported (A) and the associated signatures for each category (B).

Figure 291 Application Categories and Associated Signatures



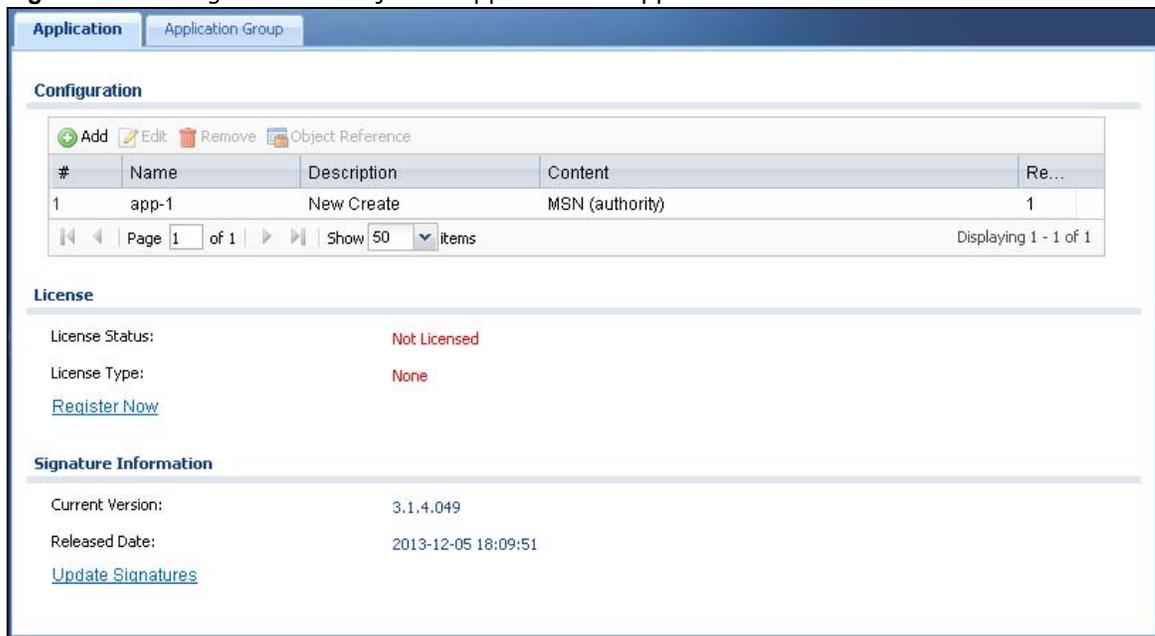
38.1.1 What You Can Do in this Chapter

- Use the **Application** screen ([Section 38.2 on page 436](#)) to create application objects that can be used in App Patrol profiles.
- Use the **Application Group** screen ([Section 38.3 on page 440](#)) to group application objects as an individual object that can be used in App Patrol profiles.

38.2 Application Screen

This screen allows you to create application objects consisting of service signatures as well as view license and signature information. To access this screen click **Configuration > Object > Application > Application**.

Figure 292 Configuration > Object > Application > Application



The following table describes the labels in this screen.

Table 199 Configuration > Object > Application > Application

LABEL	DESCRIPTION
Add	Click this to add a new application object.
Edit	Click this to edit the selected application object.
Remove	Click this to remove the selected application object.
Object Reference	Click this to view which other objects are linked to the selected application object.
#	This field is a sequential value associated with an application object.
Name	This field indicates the name assigned to the application object.
Description	This field shows some extra information on the application object.
Content	This field shows the application signature(s) in this application object.
Reference	This displays the number of times an object reference is used in a profile.

Table 199 Configuration > Object > Application > Application (continued)

LABEL	DESCRIPTION
License	You need to buy a license or use a trial license in order to use AppPatrol signatures. These fields show license-related information.
License Status	This field shows whether you have activated an AppPatrol signatures license
License Type	This field shows the type of AppPatrol signatures license you have activated
Signature Information	An activated license allows you to download signatures to the UAG from myZyXEL.com. These fields show details on the signatures downloaded.
Current Version	The version number increments when signatures are updated at myZyXEL.com. This field shows the current version downloaded to the UAG.
Released Date	This field shows the date (YYYY-MM-DD) and time the current signature version was released.
Update Signatures	If your signature set is not the most recent, click this to go to Configuration > Licensing > Signature Update > IDP / AppPatrol to update your signatures.

38.2.1 Add Application Rule

Click **Add** in **Configuration > Object > Application > Application** to create a new application rule. In the first screen you type a name to identify this application object and write an optional brief description of it.

You then click **Add** again to choose the signatures that should go into this object.

Figure 293 Configuration > Object > Application > Application > Add Application Rule

The screenshot shows the 'Add Application Rule' dialog box. It features a title bar with a plus icon and the text 'Add Application Rule'. The main area contains a 'Name:' field with a red dashed border and a red error icon, and a 'Description:' field with the text 'New Create' and '(Optional)'. Below these is a table with columns '#', 'Category', and 'Application'. The table is currently empty, showing 'Page 1 of 1' and 'Show 50 items'. At the bottom are 'OK' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 200 Configuration > Object > Application > Application > Add Application Rule

LABEL	DESCRIPTION
Name	Type a name to identify this application rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	You may type some extra information on the application object here.
Add	Click this to create a new application rule.
Remove	Click this to remove the selected application rule.
#	This field is a sequential value associated with this application rule..
Category	This field shows the category to which the signature belongs in this application rule.
Application	This displays the name of the application signature used in this application rule.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving your changes.

38.2.1.1 Add Application Object by Category or Service

Click **Add** in **Configuration > Object > Application > Application > Add Application Rule**. Use this screen to choose the signatures that should go into this object.

Figure 294 Configuration > Object > Application > Application > Add Application Rule > Add By Category

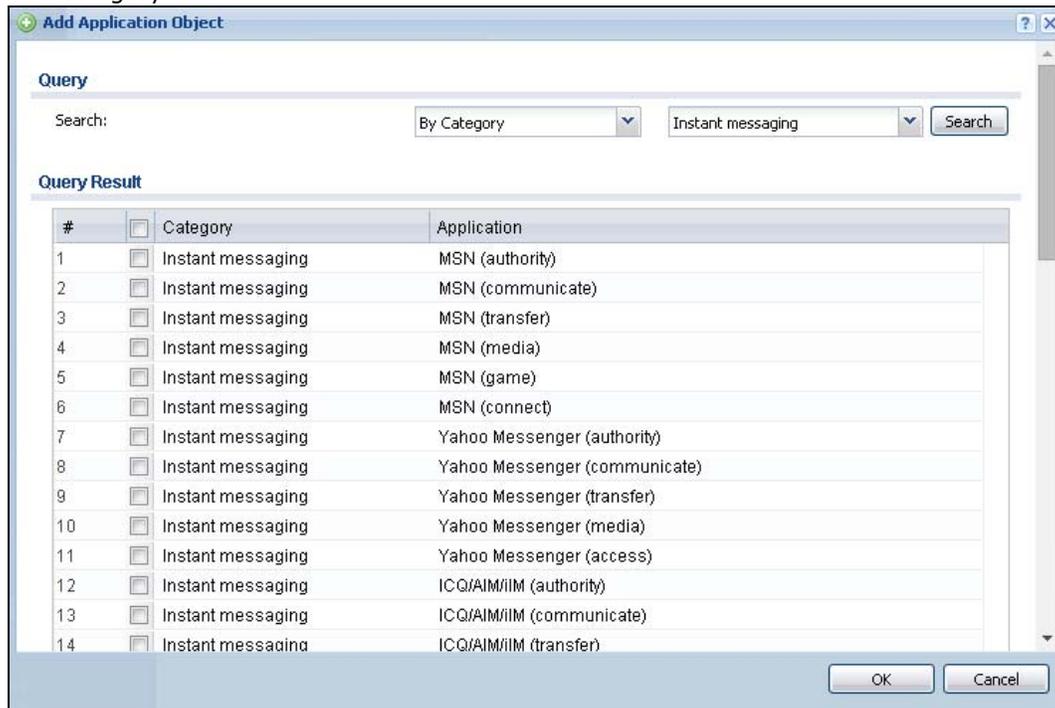


Figure 295 Configuration > Object > Application > Application > Add Application Rule > Add By Service

The screenshot shows a dialog box titled "Add Application Object". Under the "Query" section, there is a "Search:" label, a dropdown menu set to "By Service", a text input field containing "service", and a "Search" button. Below this is the "Query Result" section, which contains a table with the following data:

#	<input type="checkbox"/>	Category	Application
1	<input type="checkbox"/>	Instant messaging	MSN (authority)
2	<input type="checkbox"/>	Instant messaging	MSN (communicate)
3	<input type="checkbox"/>	Instant messaging	MSN (transfer)
4	<input type="checkbox"/>	Instant messaging	MSN (media)
5	<input type="checkbox"/>	Instant messaging	MSN (game)
6	<input type="checkbox"/>	Instant messaging	MSN (connect)
7	<input type="checkbox"/>	Instant messaging	Yahoo Messenger (authority)
8	<input type="checkbox"/>	Instant messaging	Yahoo Messenger (communicate)
9	<input type="checkbox"/>	Instant messaging	Yahoo Messenger (transfer)
10	<input type="checkbox"/>	Instant messaging	Yahoo Messenger (media)
11	<input type="checkbox"/>	Instant messaging	Yahoo Messenger (access)
12	<input type="checkbox"/>	Instant messaging	ICQ/AIM/iIM (authority)
13	<input type="checkbox"/>	Instant messaging	ICQ/AIM/iIM (communicate)
14	<input type="checkbox"/>	Instant messaging	ICQ/AIM/iIM (transfer)

At the bottom right of the dialog are "OK" and "Cancel" buttons.

The following table describes the labels in this screen.

Table 201 Configuration > Object > Application > Application > Add Application Rule > Add Application Object

LABEL	DESCRIPTION
Query	
Search	Choose signatures in one of the following ways: <ul style="list-style-type: none"> • Select By Category then select a category in the adjacent drop-down list box to display all signatures of that category • Select By Service, type a keyword and click Search to display all signatures containing that keyword.
Query Result	The results of the search are displayed here.
#	This field is a sequential value associated with this signature
Category	This field shows the category to which the signature belongs. Select the checkbox to add this signature to the application object.
Application	This displays the name of the application signature.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving your changes.

38.3 Application Group Screen

This screen allows you to group individual application objects to be treated as a single application object. To access this screen click **Configuration > Object > Application > Application Group**.

Figure 296 Configuration > Object > Application > Application Group

The following table describes the labels in this screen.

Table 202 Configuration > Object > Application > Application Group

LABEL	DESCRIPTION
Add	Click this to add a new application group.
Edit	Click this to edit the selected application group.
Remove	Click this to remove the selected application group.
Object Reference	Click this to view which other objects are linked to the selected application group.
#	This field is a sequential value associated with an application group..
Name	This field indicates the name assigned to the application group.
Description	You may type some extra information on the application group here.
Member	This field shows the application objects in this application group.
Reference	This displays the number of times an object reference is used in a profile.
License	You need to buy a license or use a trial license in order to use IDP/AppPatrol signatures. These fields show license-related information.
License Status	This field shows whether you have activated an IDP/AppPatrol signatures license
License Type	This field shows the type of IDP/AppPatrol signatures license you have activated
Signature Information	An activated license allows you to download signatures to the UAG from myZyXEL.com. These fields show details on the signatures downloaded.
Current Version	The version number increments when signatures are updated at myZyXEL.com. This field shows the current version downloaded to the UAG.

Table 202 Configuration > Object > Application > Application Group (continued)

LABEL	DESCRIPTION
Released Date	This field shows the date (YYYY-MM-DD) and time the current signature version was released.
Update Signatures	If your signature set is not the most recent, click this to go to Configuration > Licensing > Signature Update > IDP / AppPatrol to update your signatures.

38.3.1 Add Application Group Rule

Click **Add** in **Configuration > Object > Application > Application Group**. Use this screen to select already created application rules and combine them as a single new rule.

Figure 297 Configuration > Object > Application > Application > Add Application Group Rule

The following table describes the labels in this screen.

Table 203 Configuration > Object > Application > Application > Add Application Group Rule

LABEL	DESCRIPTION
Name	Enter a name for the group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	This field displays the description of each group, if any. You can use up to 60 characters, punctuation marks, and spaces.
Member List	<p>The Member list displays the names of the application and application group objects that have been added to the application group. The order of members is not important.</p> <p>Select items from the Available list that you want to be members and move them to the Member list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them.</p> <p>Move any members you do not want included to the Available list.</p>
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving your changes.

Addresses

39.1 Overview

Address objects can represent a single IP address or a range of IP addresses. Address groups are composed of address objects and other address groups.

39.1.1 What You Can Do in this Chapter

- The **Address** screen ([Section 39.2 on page 442](#)) provides a summary of all addresses in the UAG. Use the **Address Add/Edit** screen to create a new address or edit an existing one.
- Use the **Address Group** summary screen ([Section 39.3 on page 444](#)) and the **Address Group Add/Edit** screen, to maintain address groups in the UAG.

39.1.2 What You Need To Know

Address objects and address groups are used in security policies, and VPN 1-1 mapping profiles. Please see the respective sections for more information about how address objects and address groups are used in each one.

Address groups are composed of address objects and address groups. The sequence of members in the address group is not important.

39.2 Address Summary Screen

The address screens are used to create, maintain, and remove addresses. There are the types of address objects.

- **HOST** - a host address is defined by an **IP Address**.
- **RANGE** - a range address is defined by a **Starting IP Address** and an **Ending IP Address**.
- **SUBNET** - a network address is defined by a **Network** IP address and **Netmask** subnet mask.

The **Address** screen provides a summary of all addresses in the UAG. To access this screen, click **Configuration > Object > Address > Address**. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 298 Configuration > Object > Address > Address

#	Name	Type	IPv4 Address	Reference
1	DMZ_SUBNET	INTERFACE SUBNET	dmz-172.18.0.0/16	1
2	Dest_1	RANGE	172.16.1.10-172.16.1.15	2
3	LAN1_SUBNET	INTERFACE SUBNET	lan1-172.16.0.0/16	0
4	LAN2_SUBNET	INTERFACE SUBNET	lan2-172.17.0.0/16	0

The following table describes the labels in this screen. See [Section 39.2.1 on page 443](#) for more information as well.

Table 204 Configuration > Object > Address > Address

LABEL	DESCRIPTION
Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Object Reference	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 10.3.2 on page 165 for an example.
#	This field is a sequential value, and it is not associated with a specific address.
Name	This field displays the configured name of each address object.
Type	This field displays the type of each address object. " INTERFACE " means the object uses the settings of one of the UAG's interfaces.
IPv4 Address	This field displays the IPv4 addresses represented by each address object. If the object's settings are based on one of the UAG's interfaces, the name of the interface displays first followed by the object's current address settings.
Reference	This displays the number of times an object reference is used in a profile.

39.2.1 Address Add/Edit Screen

The **Configuration > Object > Address Add/Edit** screen allows you to create a new address or edit an existing one. To access this screen, go to the **Address** screen (see [Section 39.2 on page 442](#)), and click either the **Add** icon or an **Edit** icon in the **Configuration** section.

Figure 299 IPv4 Address Configuration > Add/Edit

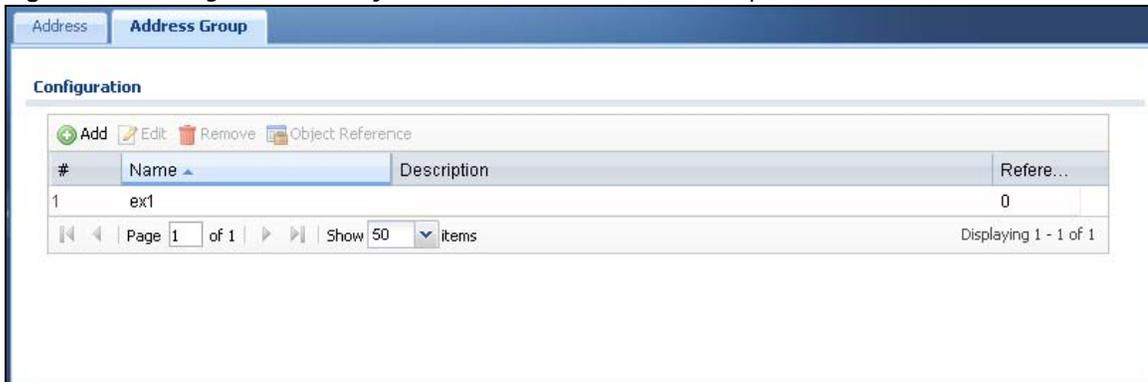
The following table describes the labels in this screen.

Table 205 IPv4 Address Configuration > Add/Edit

LABEL	DESCRIPTION
Name	Type the name used to refer to the address. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Address Type	Select the type of address you want to create. Choices are: HOST , RANGE , SUBNET , INTERFACE IP , INTERFACE SUBNET , and INTERFACE GATEWAY . Note: The UAG automatically updates address objects that are based on an interface's IP address, subnet, or gateway if the interface's IP address settings change. For example, if you change lan1's IP address, the UAG automatically updates the corresponding interface-based, LAN subnet address object.
IP Address	This field is only available if the Address Type is HOST . This field cannot be blank. Enter the IP address that this address object represents.
Starting IP Address	This field is only available if the Address Type is RANGE . This field cannot be blank. Enter the beginning of the range of IP addresses that this address object represents.
Ending IP Address	This field is only available if the Address Type is RANGE . This field cannot be blank. Enter the end of the range of IP address that this address object represents.
Network	This field is only available if the Address Type is SUBNET , in which case this field cannot be blank. Enter the IP address of the network that this address object represents.
Netmask	This field is only available if the Address Type is SUBNET , in which case this field cannot be blank. Enter the subnet mask of the network that this address object represents. Use dotted decimal format.
Interface	If you selected INTERFACE IP , INTERFACE SUBNET , or INTERFACE GATEWAY as the Address Type , use this field to select the interface of the network that this address object represents.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving your changes.

39.3 Address Group Summary Screen

The **Address Group** screen provides a summary of all address groups. To access this screen, click **Configuration > Object > Address > Address Group**. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 300 Configuration > Object > Address > Address Group

The following table describes the labels in this screen. See [Section 39.3.1 on page 445](#) for more information as well.

Table 206 Configuration > Object > Address > Address Group

LABEL	DESCRIPTION
Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Object Reference	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 10.3.2 on page 165 for an example.
#	This field is a sequential value, and it is not associated with a specific address group.
Name	This field displays the name of each address group.
Description	This field displays the description of each address group, if any.
Reference	This displays the number of times an object reference is used in a profile.

39.3.1 Address Group Add/Edit Screen

The **Address Group Add/Edit** screen allows you to create a new address group or edit an existing one. To access this screen, go to the **Address Group** screen (see [Section 39.3 on page 444](#)), and click either the **Add** icon or an **Edit** icon in the **Configuration** section.

Figure 301 Address Group Configuration > Add

The following table describes the labels in this screen.

Table 207 Address Group Configuration > Add

LABEL	DESCRIPTION
Name	Enter a name for the address group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	This field displays the description of each address group, if any. You can use up to 60 characters, punctuation marks, and spaces.
Member List	<p>The Member list displays the names of the address and address group objects that have been added to the address group. The order of members is not important.</p> <p>Select items from the Available list that you want to be members and move them to the Member list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them.</p> <p>Move any members you do not want included to the Available list.</p>
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving your changes.

40.1 Overview

Use service objects to define TCP applications, UDP applications, and ICMP messages. You can also create service groups to refer to multiple service objects in other features.

40.1.1 What You Can Do in this Chapter

- Use the **Service** screens ([Section 40.2 on page 448](#)) to view and configure the UAG's list of services and their definitions.
- Use the **Service Group** screens ([Section 40.2 on page 448](#)) to view and configure the UAG's list of service groups.

40.1.2 What You Need to Know

IP Protocols

IP protocols are based on the eight-bit protocol field in the IP header. This field represents the next-level protocol that is sent in this packet. This section discusses three of the most common IP protocols.

Computers use Transmission Control Protocol (TCP, IP protocol 6) and User Datagram Protocol (UDP, IP protocol 17) to exchange data with each other. TCP guarantees reliable delivery but is slower and more complex. Some uses are FTP, HTTP, SMTP, and TELNET. UDP is simpler and faster but is less reliable. Some uses are DHCP, DNS, RIP, and SNMP.

TCP creates connections between computers to exchange data. Once the connection is established, the computers exchange data. If data arrives out of sequence or is missing, TCP puts it in sequence or waits for the data to be re-transmitted. Then, the connection is terminated.

In contrast, computers use UDP to send short messages to each other. There is no guarantee that the messages arrive in sequence or that the messages arrive at all.

Both TCP and UDP use ports to identify the source and destination. Each port is a 16-bit number. Some port numbers have been standardized and are used by low-level system processes; many others have no particular meaning.

Unlike TCP and UDP, Internet Control Message Protocol (ICMP, IP protocol 1) is mainly used to send error messages or to investigate problems. For example, ICMP is used to send the response if a computer cannot be reached. Another use is ping. ICMP does not guarantee delivery, but networks often treat ICMP messages differently, sometimes looking at the message itself to decide where to send it.

Service Objects and Service Groups

Use service objects to define IP protocols.

- TCP applications
- UDP applications
- ICMP messages
- user-defined services (for other types of IP protocols)

These objects are used in policy routes, and security policies.

Use service groups when you want to create the same rule for several services, instead of creating separate rules for each service. Service groups may consist of services and other service groups. The sequence of members in the service group is not important.

40.2 The Service Summary Screen

The **Service** summary screen provides a summary of all services and their definitions. In addition, this screen allows you to add, edit, and remove services.

To access this screen, log in to the Web Configurator, and click **Configuration > Object > Service > Service**. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 302 Configuration > Object > Service > Service

#	Name	Content	Refere...
1	AH	Protocol=51	1
2	AIM	TCP=5190	0
3	AUTH	TCP=113	0
4	Any_TCP	TCP/1-65535	0
5	Any_UDP	UDP/1-65535	0
6	BGP	TCP=179	0
7	BONJOUR	UDP=5353	0
8	BOOTP_CLIENT	UDP=68	0
9	BOOTP_SERVER	UDP=67	0
10	CAPWAP-CONTROL	UDP=5246	0
11	CAPWAP-DATA	UDP=5247	0
12	CU_SEEME_TCP1	TCP=7648	1
13	CU_SEEME_TCP2	TCP=24032	1
14	CU_SEEME_UDP1	UDP=7648	1
15	CU_SEEME_UDP2	UDP=24032	1
16	DNS_TCP	TCP=53	1
17	DNS_UDP	UDP=53	1
18	Doom	UDP=666	1
19	ESP	Protocol=50	1
20	FINGER	TCP=79	0

The following table describes the labels in this screen.

Table 208 Configuration > Object > Service > Service

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Object Reference	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 10.3.2 on page 165 for an example.
#	This field is a sequential value, and it is not associated with a specific service.
Name	This field displays the name of each service.
Content	This field displays a description of each service.
Reference	This displays the number of times an object reference is used in a profile.

40.2.1 The Service Add/Edit Screen

The **Service Add/Edit** screen allows you to create a new service or edit an existing one. To access this screen, go to the **Service** screen (see [Section 40.2 on page 448](#)), and click either the **Add** icon or an **Edit** icon.

Figure 303 Configuration > Object > Service > Service > Edit

The following table describes the labels in this screen.

Table 209 Configuration > Object > Service > Service > Edit

LABEL	DESCRIPTION
Name	Type the name used to refer to the service. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
IP Protocol	Select the protocol the service uses. Choices are: TCP , UDP , ICMP , and User Defined .
Starting Port Ending Port	This field appears if the IP Protocol is TCP or UDP . Specify the port number(s) used by this service. If you fill in one of these fields, the service uses that port. If you fill in both fields, the service uses the range of ports.
ICMP Type	This field appears if the IP Protocol is ICMP . Select the ICMP message used by this service. This field displays the message text, not the message number.
IP Protocol Number	This field appears if the IP Protocol is User Defined . Enter the number of the next-level protocol (IP protocol). Allowed values are 1 - 255.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving your changes.

40.3 The Service Group Summary Screen

The **Service Group** summary screen provides a summary of all service groups. In addition, this screen allows you to add, edit, and remove service groups.

To access this screen, log into the Web Configurator, and click **Configuration > Object > Service > Service Group**.

Figure 304 Configuration > Object > Service > Service Group

The screenshot shows the 'Service Group' configuration screen. At the top, there are tabs for 'Service' and 'Service Group'. Below the tabs is a 'Configuration' section with a toolbar containing 'Add', 'Edit', 'Remove', and 'Object Reference' icons. The main area is a table with columns: '#', 'Name', 'Description', and 'Refere...'. The table contains 11 rows of service groups. At the bottom, there is a pagination control showing 'Page 1 of 1', 'Show 50 items', and 'Displaying 1 - 11 of 11'.

#	Name	Description	Refere...
1	CU-SEEME		0
2	DNS		2
3	Default_Allow_DMZ_To_Device	System Default Allow From DMZ To Device	1
4	Default_Allow_WAN_To_Device	System Default Allow From WAN To Device	1
5	IRC		0
6	NetBIOS		1
7	ROADRUNNER		0
8	RTSP		0
9	SNMP		0
10	SNMP-TRAPS		0
11	SSH		0

The following table describes the labels in this screen. See [Section 40.3.1 on page 451](#) for more information as well.

Table 210 Configuration > Object > Service > Service Group

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Object Reference	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 10.3.2 on page 165 for an example.
#	This field is a sequential value, and it is not associated with a specific service group.
Name	This field displays the name of each service group. By default, the UAG uses services starting with "Default_Allow_" in the security policies to allow certain services to connect to the UAG.
Description	This field displays the description of each service group, if any.
Reference	This displays the number of times an object reference is used in a profile.

40.3.1 The Service Group Add/Edit Screen

The **Service Group Add/Edit** screen allows you to create a new service group or edit an existing one. To access this screen, go to the **Service Group** screen (see [Section 40.3 on page 450](#)), and click either the **Add** icon or an **Edit** icon.

Figure 305 Configuration > Object > Service > Service Group > Edit

The following table describes the labels in this screen.

Table 211 Configuration > Object > Service > Service Group > Edit

LABEL	DESCRIPTION
Name	Enter the name of the service group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description of the service group, if any. You can use up to 60 printable ASCII characters.
Member List	<p>The Member list displays the names of the service and service group objects that have been added to the service group. The order of members is not important.</p> <p>Select items from the Available list that you want to be members and move them to the Member list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them.</p> <p>Move any members you do not want included to the Available list.</p>
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving your changes.

Schedules

41.1 Overview

Use schedules to set up one-time and recurring schedules for policy routes, and security policies. The UAG supports one-time and recurring schedules. One-time schedules are effective only once, while recurring schedules usually repeat. Both types of schedules are based on the current date and time in the UAG.

Note: Schedules are based on the UAG's current date and time.

41.1.1 What You Can Do in this Chapter

- Use the **Schedule** summary screen ([Section 41.2 on page 454](#)) to see a list of all schedules in the UAG.
- Use the **One-Time Schedule Add/Edit** screen ([Section 41.2.1 on page 455](#)) to create or edit a one-time schedule.
- Use the **Recurring Schedule Add/Edit** screen ([Section 41.2.2 on page 456](#)) to create or edit a recurring schedule.
- Use the **Schedule Group** screen ([Section 41.3 on page 457](#)) to merge individual schedule objects as one object.

41.1.2 What You Need to Know

One-time Schedules

One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods.

Recurring Schedules

Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring schedules always begin and end in the same day. Recurring schedules are useful for defining the workday and off-work hours.

Finding Out More

- See [Section 46.4 on page 488](#) for information about the UAG's current date and time.

41.2 The Schedule Summary Screen

The **Schedule** summary screen provides a summary of all schedules in the UAG. To access this screen, click **Configuration > Object > Schedule**.

Figure 306 Configuration > Object > Schedule

The screenshot shows the 'Schedule' configuration screen. It is divided into two sections: 'One Time' and 'Recurring'. Each section has a toolbar with 'Add', 'Edit', 'Remove', and 'Object References' icons. Below the toolbars are data tables. The 'One Time' table is currently empty, showing 'No data to display'. The 'Recurring' table contains one entry with the following details:

#	Name	Start Time	Stop Time
1	workday	09:00	17:00

Both tables include pagination controls showing 'Page 1 of 1' and 'Show 50 items'.

The following table describes the labels in this screen. See [Section 41.2.1 on page 455](#) and [Section 41.2.2 on page 456](#) for more information as well.

Table 212 Configuration > Object > Schedule

LABEL	DESCRIPTION
One Time	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Object Reference	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 10.3.2 on page 165 for an example.
#	This field is a sequential value, and it is not associated with a specific schedule.
Name	This field displays the name of the schedule, which is used to refer to the schedule.
Start Day / Time	This field displays the date and time at which the schedule begins.
Stop Day / Time	This field displays the date and time at which the schedule ends.
Recurring	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Object Reference	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 10.3.2 on page 165 for an example.
#	This field is a sequential value, and it is not associated with a specific schedule.
Name	This field displays the name of the schedule, which is used to refer to the schedule.
Start Time	This field displays the time at which the schedule begins.
Stop Time	This field displays the time at which the schedule ends.

41.2.1 The One-Time Schedule Add/Edit Screen

The **One-Time Schedule Add/Edit** screen allows you to define a one-time schedule or edit an existing one. To access this screen, go to the **Schedule** screen (see [Section 41.2 on page 454](#)), and click either the **Add** icon or an **Edit** icon in the **One Time** section.

Figure 307 Configuration > Object > Schedule > Edit (One Time)

The following table describes the labels in this screen.

Table 213 Configuration > Object > Schedule > Edit (One Time)

LABEL	DESCRIPTION
Configuration	
Name	Type the name used to refer to the one-time schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Date Time	
StartDate	Specify the year, month, and day when the schedule begins. <ul style="list-style-type: none"> • Year - 1900 - 2999 • Month - 1 - 12 • Day - 1 - 31 (it is not possible to specify illegal dates, such as February 31.)
StartTime	Specify the hour and minute when the schedule begins. <ul style="list-style-type: none"> • Hour - 0 - 23 • Minute - 0 - 59
StopDate	Specify the year, month, and day when the schedule ends. <ul style="list-style-type: none"> • Year - 1900 - 2999 • Month - 1 - 12 • Day - 1 - 31 (it is not possible to specify illegal dates, such as February 31.)
StopTime	Specify the hour and minute when the schedule ends. <ul style="list-style-type: none"> • Hour - 0 - 23 • Minute - 0 - 59
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving your changes.

41.2.2 The Recurring Schedule Add/Edit Screen

The **Recurring Schedule Add/Edit** screen allows you to define a recurring schedule or edit an existing one. To access this screen, go to the **Schedule** screen (see [Section 41.2 on page 454](#)), and click either the **Add** icon or an **Edit** icon in the **Recurring** section.

Figure 308 Configuration > Object > Schedule > Edit (Recurring)

The **Year**, **Month**, and **Day** columns are not used in recurring schedules and are disabled in this screen. The following table describes the remaining labels in this screen.

Table 214 Configuration > Object > Schedule > Edit (Recurring)

LABEL	DESCRIPTION
Configuration	
Name	Type the name used to refer to the recurring schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Date Time	
StartTime	Specify the hour and minute when the schedule begins each day. <ul style="list-style-type: none"> • Hour - 0 - 23 • Minute - 0 - 59
StopTime	Specify the hour and minute when the schedule ends each day. <ul style="list-style-type: none"> • Hour - 0 - 23 • Minute - 0 - 59
Weekly	
Week Days	Select each day of the week the recurring schedule is effective.
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving your changes.

41.3 The Schedule Group Summary Screen

The **Schedule Group** summary screen provides a summary of all groups of schedules in the UAG. To access this screen, click **Configuration > Object > Schedule > Group**.

Figure 309 Configuration > Object > Schedule > Schedule Group



The following table describes the fields in the above screen.

Table 215 Configuration > Object > Schedule > Schedule Group

LABEL	DESCRIPTION
Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Object Reference	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific schedule.
Name	This field displays the name of the schedule group, which is used to refer to the schedule.
Description	This field displays the description of the schedule group.
Members	This field lists the members in the schedule group. Each member is separated by a comma.
Reference	This displays the number of times an object reference is used in a profile.

41.3.1 The Schedule Group Add/Edit Screen

The **Schedule Group Add/Edit** screen allows you to define a schedule group or edit an existing one. To access this screen, go to the **Schedule** screen (see), and click either the **Add** icon or an **Edit** icon in the **Schedule Group** section.

Figure 310 Configuration > Schedule > Schedule Group > Add

The following table describes the fields in the above screen.

Table 216 Configuration > Schedule > Schedule Group > Add

LABEL	DESCRIPTION
Group Members	
Name	Type the name used to refer to the recurring schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description of the service group, if any. You can use up to 60 printable ASCII characters.
Member List	<p>The Member list displays the names of the service and service group objects that have been added to the service group. The order of members is not important.</p> <p>Select items from the Available list that you want to be members and move them to the Member list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them.</p> <p>Move any members you do not want included to the Available list.</p>
OK	Click OK to save your changes back to the UAG.
Cancel	Click Cancel to exit this screen without saving your changes.

AAA Server

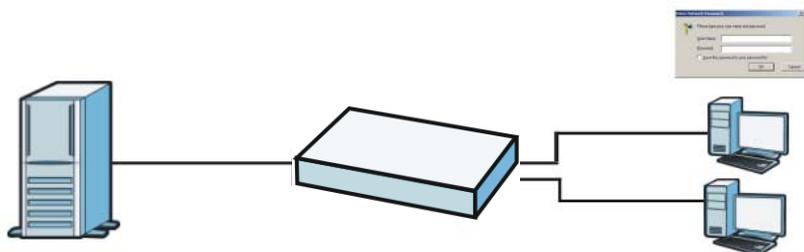
42.1 Overview

You can use a AAA (Authentication, Authorization, Accounting) server to provide access control to your network. The AAA server can be a RADIUS server. Use the **AAA Server** screens to create and manage objects that contain settings for using AAA servers. You use AAA server objects in configuring ext-group-user user objects and authentication method objects (see [Chapter 43 on page 464](#)).

42.1.1 RADIUS Server

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate a large number of users from a central location.

Figure 311 RADIUS Server Network Example



42.1.2 What You Can Do in this Chapter

Use the **Configuration > Object > AAA Server > RADIUS** screen ([Section 42.2 on page 460](#)) to configure the default external RADIUS server to use for user authentication.

42.1.3 What You Need To Know

AAA Servers Supported by the UAG

The following lists the types of authentication server the UAG supports.

- Local user database

The UAG uses the built-in local user database to authenticate administrative users logging into the UAG's Web Configurator or network access users logging into the network through the UAG.

- RADIUS

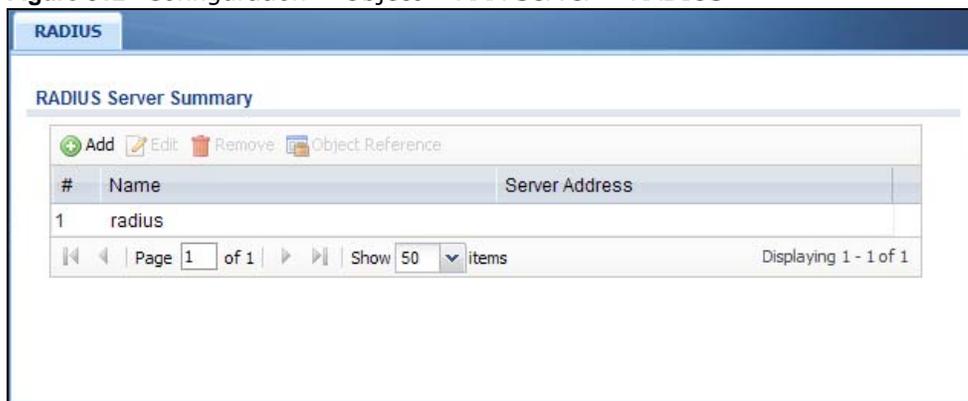
RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external or built-in RADIUS server. RADIUS authentication allows you to validate a large number of users from a central location.

42.2 RADIUS Server Summary

Use the **RADIUS** screen to manage the list of RADIUS servers the UAG can use in authenticating users.

Click **Configuration > Object > AAA Server > RADIUS** to display the **RADIUS** screen.

Figure 312 Configuration > Object > AAA Server > RADIUS



The following table describes the labels in this screen.

Table 217 Configuration > Object > AAA Server > RADIUS

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Object Reference	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 10.3.2 on page 165 for an example.
#	This field displays the index number.
Name	This is the name of the RADIUS server entry.
Server Address	This is the address of the RADIUS server.

42.2.1 Adding/Editing a RADIUS Server

Click **Configuration > Object > AAA Server > RADIUS** to display the **RADIUS** screen. Click the **Add** icon or an **Edit** icon to display the following screen. Use this screen to create a new RADIUS entry or edit an existing one.

Figure 313 Configuration > Object > AAA Server > RADIUS > Add

Add RADIUS

General Settings

Name:

Description: (Optional)

Authentication Server Settings

Server Address: ⓘ or FQDN

Authentication Port: (1-65535)

Backup Server Address: (IP or FQDN) (Optional)

Backup Authentication Port: (1-65535) (Optional)

Key: ⓘ

Accounting Server Settings

Server Address: (IP or FQDN) (Optional)

Accounting Port: (1-65535) (Optional)

Backup Server Address: (IP or FQDN) (Optional)

Backup Accounting Port: (1-65535) (Optional)

Key:

Maximum Retry Count: (1~10)

Enable Accounting Interim update

Interim Interval: (1-1440 minutes)

General Server Settings

Timeout: (1-300 seconds)

NAS IP Address: (IP Address)

NAS Identifier:

Case-sensitive User Names ⓘ

User Login Settings

Group Membership Attribute: (1-255)

OK Cancel

The following table describes the labels in this screen.

Table 218 Configuration > Object > AAA Server > RADIUS > Add/Edit

LABEL	DESCRIPTION
General Settings	
Name	Enter a descriptive name (up to 63 alphanumeric characters) for identification purposes.
Description	Enter the description of each server, if any. You can use up to 60 printable ASCII characters.
Authentication Server Settings	
Server Address	Enter the address of the RADIUS authentication server.
Authentication Port	Specify the port number on the RADIUS server to which the UAG sends authentication requests. Enter a number between 1 and 65535.

Table 218 Configuration > Object > AAA Server > RADIUS > Add/Edit (continued)

LABEL	DESCRIPTION
Backup Server Address	If the RADIUS server has a backup authentication server, enter its address here.
Backup Authentication Port	Specify the port number on the RADIUS server to which the UAG sends authentication requests. Enter a number between 1 and 65535.
Key	<p>Enter a password (up to 15 alphanumeric characters) as the key to be shared between the external authentication server and the UAG.</p> <p>The key is not sent over the network. This key must be the same on the external authentication server and the UAG.</p>
Accounting Server Settings	
Server Address	Enter the IP address or Fully-Qualified Domain Name (FQDN) of the RADIUS accounting server.
Accounting Port	Specify the port number on the RADIUS server to which the UAG sends accounting information. Enter a number between 1 and 65535.
Backup Server Address	If the RADIUS server has a backup accounting server, enter its address here.
Backup Accounting Port	Specify the port number on the RADIUS server to which the UAG sends accounting information. Enter a number between 1 and 65535.
Key	<p>Enter a password (up to 15 alphanumeric characters) as the key to be shared between the external accounting server and the UAG.</p> <p>The key is not sent over the network. This key must be the same on the external accounting server and the UAG.</p>
Maximum Retry Count	<p>At times the UAG may not be able to use the primary RADIUS accounting server. Specify the number of times the UAG should reattempt to use the primary RADIUS server before attempting to use the secondary RADIUS server. This also sets how many times the UAG will attempt to use the secondary RADIUS server.</p> <p>For example, you set this field to 3. If the UAG does not get a response from the primary RADIUS server, it tries again up to three times. If there is no response, the UAG tries the secondary RADIUS server up to three times.</p> <p>If there is also no response from the secondary RADIUS server, the UAG stops attempting to authenticate the subscriber. The subscriber will see a message that says the RADIUS server was not found.</p>
Enable Accounting Interim update	Select this to have the UAG send subscriber status updates to the RADIUS server at the interval you specify.
Interim Interval	Specify the time interval for how often the UAG is to send a subscriber status update to the RADIUS server.
General Server Settings	
Timeout	<p>Specify the timeout period (between 1 and 300 seconds) before the UAG disconnects from the RADIUS server. In this case, user authentication fails.</p> <p>Search timeout occurs when either the user information is not in the RADIUS server or the RADIUS server is down.</p>
NAS IP Address	If the RADIUS server requires the UAG to provide the Network Access Server IP address attribute with a specific value, enter it here.
NAS Identifier	If the RADIUS server requires the UAG to provide the Network Access Server identifier attribute with a specific value, enter it here.
Case-sensitive User Names	Select this if the server checks the case of the usernames.

Table 218 Configuration > Object > AAA Server > RADIUS > Add/Edit (continued)

LABEL	DESCRIPTION
User Login Settings	
Group Membership Attribute	<p>A RADIUS server defines attributes for its accounts. Select the name and number of the attribute that the UAG is to check to determine to which group a user belongs. If it does not display, select User Defined and specify the attribute's number.</p> <p>This attribute's value is called a group identifier; it determines to which group a user belongs. You can add ext-group-user user objects to identify groups based on these group identifier values.</p> <p>For example you could have an attribute named "memberOf" with values like "sales", "RD", and "management". Then you could also create a ext-group-user user object for each group. One with "sales" as the group identifier, another for "RD" and a third for "management".</p>
OK	Click OK to save the changes.
Cancel	Click Cancel to discard the changes.

Authentication Method

43.1 Overview

Authentication method objects set how the UAG authenticates wireless, HTTP/HTTPS clients, and peer IPsec routers (extended authentication) clients. Configure authentication method objects to have the UAG use the local user database, and/or the authentication servers and authentication server groups specified by AAA server objects. By default, user accounts created and stored on the UAG are authenticated locally.

43.1.1 What You Can Do in this Chapter

- Use the **Configuration > Object > Auth. Method** screens ([Section 43.2 on page 464](#)) to create and manage authentication method objects.

43.1.2 Before You Begin

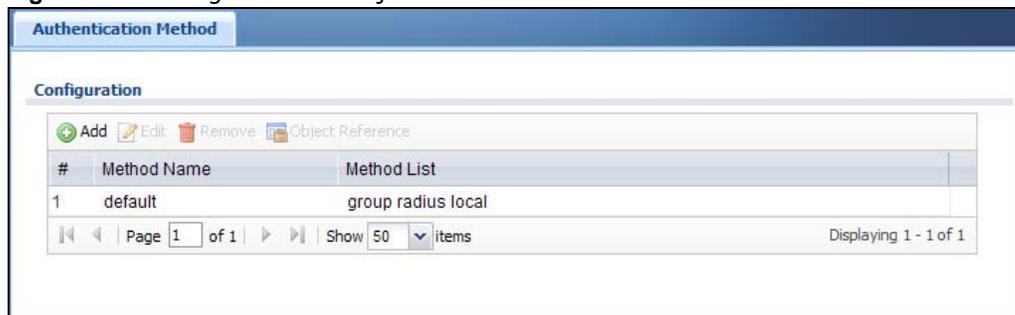
Configure AAA server objects (see [Chapter 42 on page 459](#)) before you configure authentication method objects.

43.2 Authentication Method Objects

Click **Configuration > Object > Auth. Method** to display the screen as shown.

Note: You can create up to four authentication method objects.

Figure 314 Configuration > Object > Auth. Method



The following table describes the labels in this screen.

Table 219 Configuration > Object > Auth. Method

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Object Reference	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 10.3.2 on page 165 for an example.
#	This field displays the index number.
Method Name	This field displays a descriptive name for identification purposes.
Method List	This field displays the authentication method(s) for this entry.

43.2.1 Creating an Authentication Method Object

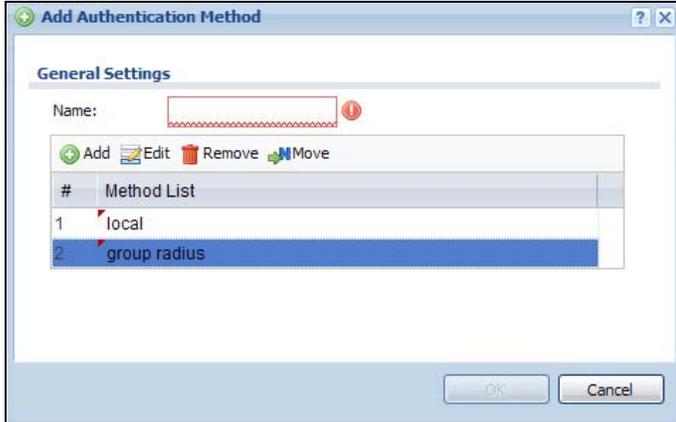
Follow the steps below to create an authentication method object.

- 1 Click **Configuration > Object > Auth. Method**.
- 2 Click **Add**.
- 3 Specify a descriptive name for identification purposes in the **Name** field. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. For example, "My_Device".
- 4 Click **Add** to insert an authentication method in the table.
- 5 Select a server object from the **Method List** drop-down list box.
- 6 You can add up to four server objects to the table. The ordering of the **Method List** column is important. The UAG authenticates the users using the databases (in the local user database or the external authentication server) in the order they appear in this screen.

If two accounts with the same username exist on two authentication servers you specify, the UAG does not continue the search on the second authentication server when you enter the username and password that doesn't match the one on the first authentication server.

Note: You can NOT select two server objects of the same type.

- 7 Click **OK** to save the settings or click **Cancel** to discard all changes and return to the previous screen.

Figure 315 Configuration > Object > Auth. Method > Add

The following table describes the labels in this screen.

Table 220 Configuration > Object > Auth. Method > Add

LABEL	DESCRIPTION
Name	Specify a descriptive name for identification purposes. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. For example, "My_Device".
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Move	To change a method's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed. The ordering of your methods is important as UAG authenticates the users using the authentication methods in the order they appear in this screen.
#	This field displays the index number.
Method List	Select a server object from the drop-down list box. You can create a server object in the AAA Server screen (see Chapter 42 on page 459 for more information). The UAG authenticates the users using the databases (in the local user database or the external authentication server) in the order they appear in this screen. If two accounts with the same username exist on two authentication servers you specify, the UAG does not continue the search on the second authentication server when you enter the username and password that doesn't match the one on the first authentication server.
OK	Click OK to save the changes.
Cancel	Click Cancel to discard the changes.

Certificates

44.1 Overview

The UAG can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

44.1.1 What You Can Do in this Chapter

- Use the **My Certificates** screens (see [Section 44.2 on page 470](#) to [Section 44.2.3 on page 476](#)) to generate and export self-signed certificates or certification requests and import the CA-signed certificates.
- Use the **Trusted Certificates** screens (see [Section 44.3 on page 477](#) to [Section 44.3.2 on page 481](#)) to save CA certificates and trusted remote host certificates to the UAG. The UAG trusts any valid certificate that you have imported as a trusted certificate. It also trusts any valid certificate signed by any of the certificates that you have imported as a trusted certificate.

44.1.2 What You Need to Know

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available. The other key is private and must be kept secure.

These keys work like a handwritten signature (in fact, certificates are often referred to as "digital signatures"). Only you can write your signature exactly as it should look. When people know what your signature looks like, they can verify whether something was signed by you, or by someone else. In the same way, your private key "writes" your digital signature and your public key allows people to verify whether data was signed by you, or by someone else. This process works as follows.

- 1 Tim wants to send a message to Jenny. He needs her to be sure that it comes from him, and that the message content has not been altered by anyone else along the way. Tim generates a public key pair (one public key and one private key).
- 2 Tim keeps the private key and makes the public key openly available. This means that anyone who receives a message seeming to come from Tim can read it and verify whether it is really from him or not.
- 3 Tim uses his private key to sign the message and sends it to Jenny.
- 4 Jenny receives the message and uses Tim's public key to verify it. Jenny knows that the message is from Tim, and that although other people may have been able to read the message, no-one can have altered it (because they cannot re-sign the message with Tim's private key).

- 5 Additionally, Jenny uses her own private key to sign a message and Tim uses Jenny's public key to verify the message.

The UAG uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The UAG does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The UAG can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

Advantages of Certificates

Certificates offer the following benefits.

- The UAG only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

Self-signed Certificates

You can have the UAG act as a certification authority and sign its own certificates.

Factory Default Certificate

The UAG generates its own unique self-signed certificate when you first turn it on. This certificate is referred to in the GUI as the factory default certificate.

Certificate File Formats

Any certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The UAG currently allows the importation of a PKCS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.

- Binary PKCS#12: This is a format for transferring public key and private key certificates. The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the UAG.

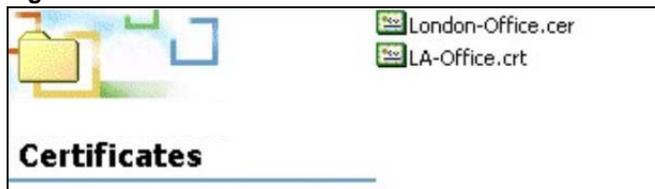
Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

44.1.3 Verifying a Certificate

Before you import a trusted certificate into the UAG, you should verify that you have the correct certificate. You can do this using the certificate's fingerprint. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithm. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

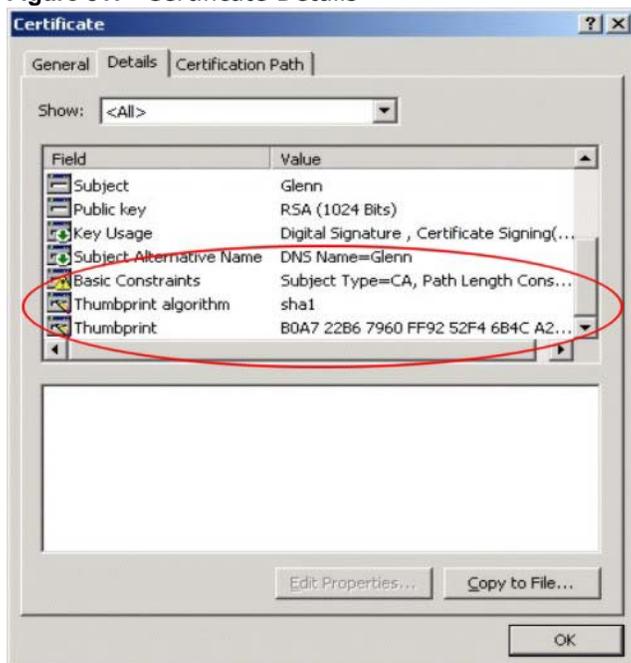
- 1 Browse to where you have the certificate saved on your computer.
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 316 Remote Host Certificates



- 3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 317 Certificate Details

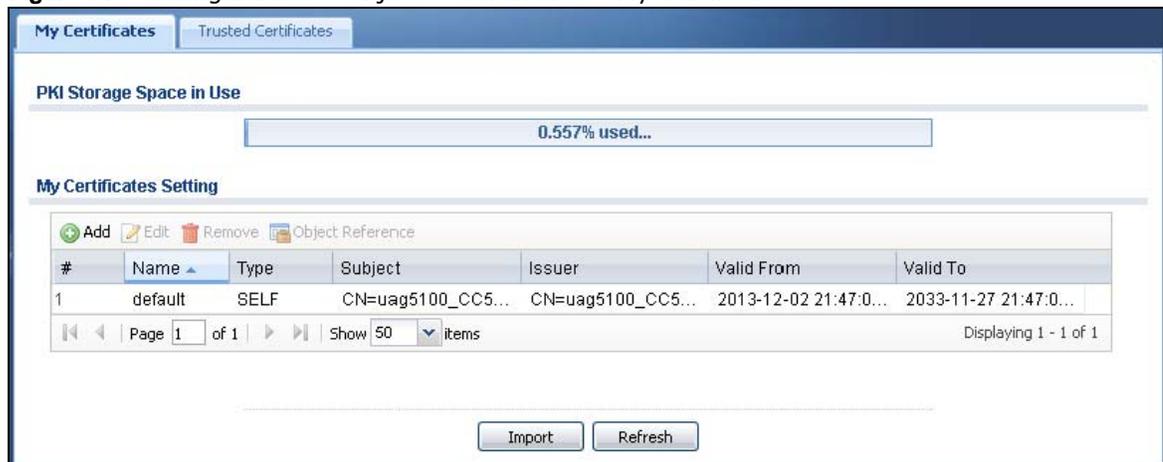


- Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may vary based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

44.2 The My Certificates Screen

Click **Configuration > Object > Certificate > My Certificates** to open the **My Certificates** screen. This is the UAG's summary list of certificates and certification requests.

Figure 318 Configuration > Object > Certificate > My Certificates



The following table describes the labels in this screen.

Table 221 Configuration > Object > Certificate > My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the UAG's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Add	Click this to go to the screen where you can have the UAG generate a certificate or a certification request.
Edit	Double-click an entry or select it and click Edit to open a screen with an in-depth list of information about the certificate.
Remove	The UAG keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so. Subsequent certificates move up by one when you take this action.
Object Reference	You cannot delete certificates that any of the UAG's features are configured to use. Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 10.3.2 on page 165 for an example.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.

Table 221 Configuration > Object > Certificate > My Certificates (continued)

LABEL	DESCRIPTION
Type	<p>This field displays what kind of certificate this is.</p> <p>REQ represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the My Certificate Import screen to import the certificate and replace the request.</p> <p>SELF represents a self-signed certificate.</p> <p>CERT represents a certificate issued by a certification authority.</p>
Subject	<p>This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.</p>
Issuer	<p>This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field.</p>
Valid From	<p>This field displays the date that the certificate becomes applicable.</p>
Valid To	<p>This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.</p>
Import	<p>Click Import to open a screen where you can save a certificate to the UAG.</p>
Refresh	<p>Click Refresh to display the current validity status of the certificates.</p>

44.2.1 The My Certificates Add Screen

Click **Configuration > Object > Certificate > My Certificates** and then the **Add** icon to open the **My Certificates Add** screen. Use this screen to have the UAG create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request.

Figure 319 Configuration > Object > Certificate > My Certificates > Add

The following table describes the labels in this screen.

Table 222 Configuration > Object > Certificate > My Certificates > Add

LABEL	DESCRIPTION
Name	Type a name to identify this certificate. You can use up to 31 alphanumeric and ;'~!@#\$%^&()_+[]{}',.- characters.
Subject Information	<p>Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although you must specify a Host IP Address, Host Domain Name, or E-Mail. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.</p> <p>Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address is for identification purposes only and can be any string.</p> <p>A domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods.</p> <p>An e-mail address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore.</p>

Table 222 Configuration > Object > Certificate > My Certificates > Add (continued)

LABEL	DESCRIPTION
Organizational Unit	Identify the organizational unit or department to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Organization	Identify the company or group to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Town (City)	Identify the town or city where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
State (Province)	Identify the state or province where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Country	Identify the nation where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Key Type	Select RSA to use the Rivest, Shamir and Adleman public-key algorithm. Select DSA to use the Digital Signature Algorithm public-key algorithm.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Extended Key Usage	Select Server Authentication to allow a web server to send clients the certificate to authenticate itself. Select Client Authentication to use the certificate's key to authenticate clients to the secure gateway. Select IKE Intermediate to have the certificate contain the IP Security IKE Intermediate Object Identifier (OID).
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select this to have the UAG generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select this to have the UAG generate and store a request for a certificate. Use the My Certificate Details screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the My Certificate Details screen (see Section 44.2.2 on page 473) and then send it to the certification authority.
OK	Click OK to begin certificate or certification request generation.
Cancel	Click Cancel to quit and return to the My Certificates screen.

44.2.2 The My Certificates Edit Screen

Click **Configuration > Object > Certificate > My Certificates** and then the **Edit** icon to open the **My Certificate Edit** screen. You can use this screen to view in-depth certificate information and change the certificate's name.

Figure 320 Configuration > Object > Certificate > My Certificates > Edit

The following table describes the labels in this screen.

Table 223 Configuration > Object > Certificate > My Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can use up to 31 alphanumeric and ;'~!@#%\$%^&()_+[]{}',.= - characters.
Certification Path	This field displays for a certificate, not a certification request. Click the Refresh button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The UAG does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click Refresh to display the certification path.

Table 223 Configuration > Object > Certificate > My Certificates > Edit (continued)

LABEL	DESCRIPTION
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the UAG.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O), State (ST), and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the Subject Name field. "none" displays for a certification request.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The UAG uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. "none" displays for a certification request.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired. "none" displays for a certification request.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the UAG uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Extended Key Usage	This field displays for what EKU (Extended Key Usage) functions the certificate's key can be used.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path. This field does not display for a certification request.
MD5 Fingerprint	This is the certificate's message digest that the UAG calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the UAG calculated using the SHA1 algorithm.

Table 223 Configuration > Object > Certificate > My Certificates > Edit (continued)

LABEL	DESCRIPTION
Certificate in PEM (Base-64) Encoded Format	<p>This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form.</p> <p>You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment.</p> <p>You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).</p>
Export Certificate Only	Use this button to save a copy of the certificate without its private key. Click this button and then Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save .
Password	If you want to export the certificate with its private key, create a password and type it here. Make sure you keep this password in a safe place. You will need to use it if you import the certificate to another device.
Export Certificate with Private Key	Use this button to save a copy of the certificate with its private key. Type the certificate's password and click this button. Click Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save .
OK	Click OK to save your changes back to the UAG. You can only change the name.
Cancel	Click Cancel to quit and return to the My Certificates screen.

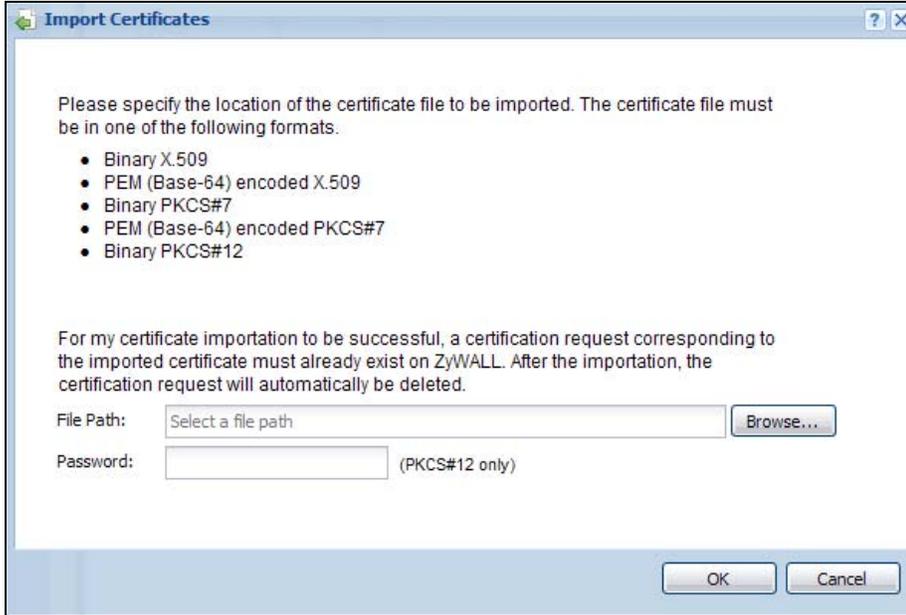
44.2.3 The My Certificates Import Screen

Click **Configuration > Object > Certificate > My Certificates > Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the UAG.

Note: You can import a certificate that matches a corresponding certification request that was generated by the UAG. You can also import a certificate in PKCS#12 format, including the certificate's public and private keys.

The certificate you import replaces the corresponding request in the **My Certificates** screen.

You must remove any spaces from the certificate's filename before you can import it.

Figure 321 Configuration > Object > Certificate > My Certificates > Import

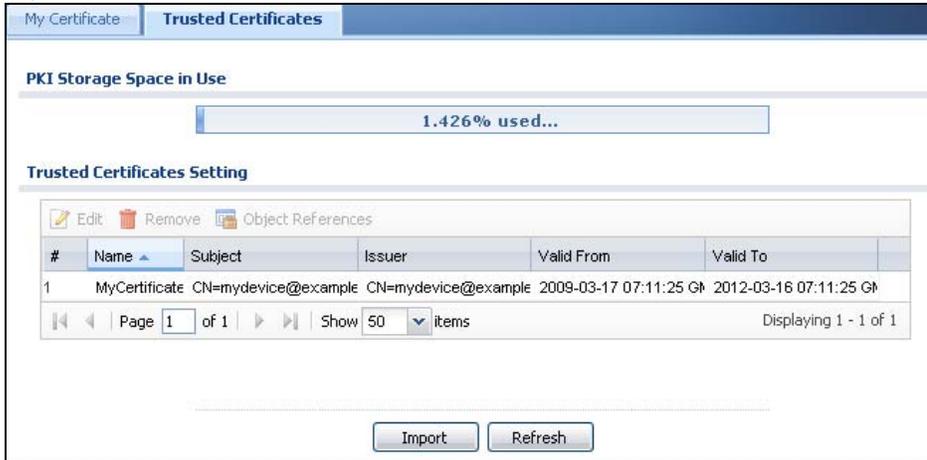
The following table describes the labels in this screen.

Table 224 Configuration > Object > Certificate > My Certificates > Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it. You cannot import a certificate with the same name as a certificate that is already in the UAG.
Browse	Click Browse to find the certificate file you want to upload.
Password	This field only applies when you import a binary PKCS#12 format file. Type the file's password that was created when the PKCS #12 file was exported.
OK	Click OK to save the certificate on the UAG.
Cancel	Click Cancel to quit and return to the My Certificates screen.

44.3 The Trusted Certificates Screen

Click **Configuration > Object > Certificate > Trusted Certificates** to open the **Trusted Certificates** screen. This screen displays a summary list of certificates that you have set the UAG to accept as trusted. The UAG also accepts any valid certificate signed by a certificate on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certificates.

Figure 322 Configuration > Object > Certificate > Trusted Certificates

The following table describes the labels in this screen.

Table 225 Configuration > Object > Certificate > Trusted Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the UAG's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Edit	Double-click an entry or select it and click Edit to open a screen with an in-depth list of information about the certificate.
Remove	The UAG keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so. Subsequent certificates move up by one when you take this action.
Object Reference	You cannot delete certificates that any of the UAG's features are configured to use. Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 10.3.2 on page 165 for an example.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Import	Click Import to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the UAG.
Refresh	Click this button to display the current validity status of the certificates.

44.3.1 The Trusted Certificates Edit Screen

Click **Configuration > Object > Certificate > Trusted Certificates** and then a certificate's **Edit** icon to open the **Trusted Certificates Edit** screen. Use this screen to view in-depth information about the certificate, change the certificate's name and set whether or not you want the UAG to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Figure 323 Configuration > Object > Certificate > Trusted Certificates > Edit

Edit Trusted Certificates

Configuration

Name:

Certification Path

Certificate Validation

LDAP Server

Address:

ID:

Password:

Port:

Certificate Information

Type: Self-signed X.509 Certificate

Version: V1

Serial Number: 14639633616644582581

Subject: C=TW, ST=TW, O=Zyxel, CN=www.zyxel.com.tw

Issuer: C=TW, ST=TW, O=Zyxel, CN=www.zyxel.com.tw

Signature Algorithm: rsa-pkcs1-sha1

Valid From: 2009-07-07 02:17:10 GMT

Valid To: 2029-07-07 02:17:10 GMT

Key Algorithm: rsaEncryption (1024 bits)

Subject Alternative Name:

Key Usage:

Basic Constraint:

MD5 Fingerprint: f5:86:93:08:57:ee:01:19:68:48:c9:e4:f1:bf:3d:1f

SHA1 Fingerprint: 6b:60:0a:6d:c1:d3:7d:59:cb:bf:8c:0a:fa:49:76:08:ab:20:95:77

Certificate in PEM (Base-64) Encoded Format

-----BEGIN X509 CERTIFICATE-----
 MIICATCCAwoCCQDLKm010festTANBgqhkiG9w0BAQUFADBFMRkwFwYDVQQDExB3
 d3cuenl4ZWwY29tLnR3MQ4wDAYDVQQKEwVaeXhlbDELMakGA1UECBMCFcxzAJ
 BgNVBAYTAiR3MB4XDTA5MDcwNzAyMTcxMFoXDTE1MDcwNzAyMTcxMFowRTEZMBCG

The following table describes the labels in this screen.

Table 226 Configuration > Object > Certificate > Trusted Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can change the name. You can use up to 31 alphanumeric and ;`~!@#\$%^&()_+[]{}',.- characters.
Certification Path	Click the Refresh button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certificate, it may be the only certification authority in the list (along with the end entity's own certificate). The UAG does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click Refresh to display the certification path.
LDAP Server	Select this check box if the directory server uses LDAP (Lightweight Directory Access Protocol). LDAP is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates.
Address	Type the IP address (in dotted decimal notation) of the directory server.
Port	Use this field to specify the LDAP server port number. You must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.
ID	The UAG may need to authenticate itself in order to assess the CRL directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the CRL directory server (usually a certification authority).
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the Subject Name field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the UAG uses RSA encryption) and the length of the key set in bits (1024 bits for example).

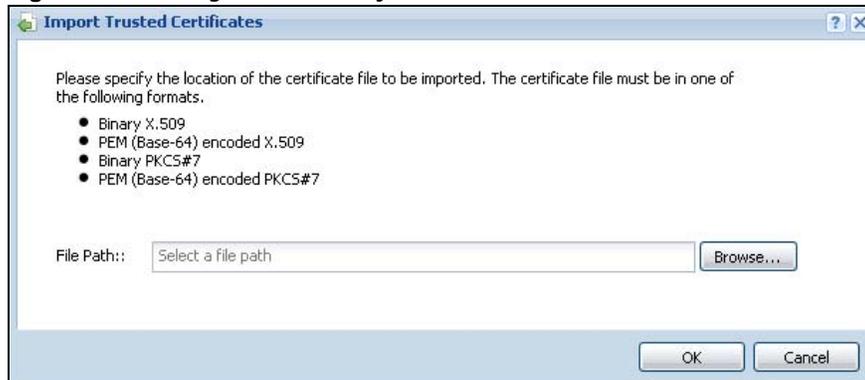
Table 226 Configuration > Object > Certificate > Trusted Certificates > Edit (continued)

LABEL	DESCRIPTION
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the UAG calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the UAG calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export Certificate	Click this button and then Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save .
OK	Click OK to save your changes back to the UAG. You can only change the name.
Cancel	Click Cancel to quit and return to the Trusted Certificates screen.

44.3.2 The Trusted Certificates Import Screen

Click **Configuration > Object > Certificate > Trusted Certificates > Import** to open the **Trusted Certificates Import** screen. Follow the instructions in this screen to save a trusted certificate to the UAG.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 324 Configuration > Object > Certificate > Trusted Certificates > Import

The following table describes the labels in this screen.

Table 227 Configuration > Object > Certificate > Trusted Certificates > Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it. You cannot import a certificate with the same name as a certificate that is already in the UAG.
Browse	Click Browse to find the certificate file you want to upload.
OK	Click OK to save the certificate on the UAG.
Cancel	Click Cancel to quit and return to the previous screen.

ISP Accounts

45.1 Overview

Use ISP accounts to manage Internet Service Provider (ISP) account information for PPPoE/PPTP interfaces. An ISP account is a profile of settings for Internet access using PPPoE or PPTP.

Finding Out More

- See [Section 10.4 on page 168](#) for information about PPPoE/PPTP interfaces.

45.1.1 What You Can Do in this Chapter

Use the **Object > ISP Account** screens ([Section 45.2 on page 483](#)) to create and manage ISP accounts in the UAG.

45.2 ISP Account Summary

This screen provides a summary of ISP accounts in the UAG. To access this screen, click **Configuration > Object > ISP Account**.

Figure 325 Configuration > Object > ISP Account

#	Profile Name	Protocol	Authentication Type	User Name
1	some-ISP	pppoe	chap-pap	test

The following table describes the labels in this screen. See [the ISP Account Edit section](#) below for more information as well.

Table 228 Configuration > Object > ISP Account

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so.
Object Reference	Select an entry and click Object Reference to open a screen that shows which settings use the entry. See Section 10.3.2 on page 165 for an example.

Table 228 Configuration > Object > ISP Account (continued)

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific entry.
Profile Name	This field displays the profile name of the ISP account. This name is used to identify the ISP account.
Protocol	This field displays the protocol used by the ISP account.
Authentication Type	This field displays the authentication type used by the ISP account.
User Name	This field displays the user name of the ISP account.

45.2.1 ISP Account Edit

The **ISP Account Edit** screen lets you add information about new accounts and edit information about existing accounts. To open this window, open the **ISP Account** screen. (See [Section 45.2 on page 483](#).) Then, click on an **Add** icon or **Edit** icon to open the **ISP Account Edit** screen below.

Figure 326 Configuration > Object > ISP Account > Edit

The following table describes the labels in this screen.

Table 229 Configuration > Object > ISP Account > Edit

LABEL	DESCRIPTION
Profile Name	This field is read-only if you are editing an existing account. Type in the profile name of the ISP account. The profile name is used to refer to the ISP account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Protocol	This field is read-only if you are editing an existing account. Select the protocol used by the ISP account. Options are: pppoe - This ISP account uses the PPPoE protocol. pptp - This ISP account uses the PPTP protocol.

Table 229 Configuration > Object > ISP Account > Edit (continued)

LABEL	DESCRIPTION
Authentication Type	<p>Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:</p> <p>CHAP/PAP - Your UAG accepts either CHAP or PAP when requested by this remote node.</p> <p>Chap - Your UAG accepts CHAP only.</p> <p>PAP - Your UAG accepts PAP only.</p> <p>MSCHAP - Your UAG accepts MSCHAP only.</p> <p>MSCHAP-V2 - Your UAG accepts MSCHAP-V2 only.</p>
Encryption Method	<p>This field is available if this ISP account uses the PPTP protocol. Use the drop-down list box to select the type of Microsoft Point-to-Point Encryption (MPPE). Options are:</p> <p>nomppe - This ISP account does not use MPPE.</p> <p>mppe-40 - This ISP account uses 40-bit MPPE.</p> <p>mppe-128 - This ISP account uses 128-bit MMPE.</p>
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above. The password can only consist of alphanumeric characters (A-Z, a-z, 0-9). This field can be blank.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
IP Address/ FQDN	<p>If this ISP account uses the PPPoE protocol, this field is not displayed.</p> <p>If this ISP account uses the PPTP protocol, type the IP address or domain name of the PPTP server.</p>
Connection ID	This field is available if this ISP account uses the PPTP protocol. Type your identification name for the PPTP server. This field can be blank.
Service Name	<p>If this ISP account uses the PPPoE protocol, type the PPPoE service name to access. PPPoE uses the specified service name to identify and reach the PPPoE server. This field can be blank.</p> <p>If this ISP account uses the PPTP protocol, this field is not displayed.</p>
Compression	Select On button to turn on stac compression, and select Off to turn off stac compression. Stac compression is a data compression technique capable of compressing data by a factor of about four.
Idle Timeout	This value specifies the number of seconds that must elapse without outbound traffic before the UAG automatically disconnects from the PPPoE/PPTP server. This value must be an integer between 0 and 360. If this value is zero, this timeout is disabled.
OK	Click OK to save your changes back to the UAG. If there are no errors, the program returns to the ISP Account screen. If there are errors, a message box explains the error, and the program stays in the ISP Account Edit screen.
Cancel	Click Cancel to return to the ISP Account screen without creating the profile (if it is new) or saving any changes to the profile (if it already exists).

46.1 Overview

Use the system screens to configure general UAG settings.

46.1.1 What You Can Do in this Chapter

- Use the **System > Host Name** screen (see [Section 46.2 on page 487](#)) to configure a unique name for the UAG in your network.
- Use the **System > USB Storage** screen (see [Section 46.3 on page 487](#)) to configure the settings for the connected USB devices.
- Use the **System > Date/Time** screen (see [Section 46.4 on page 488](#)) to configure the date and time for the UAG.
- Use the **System > Console Speed** screen (see [Section 46.5 on page 492](#)) to configure the console port speed when you connect to the UAG via the console port using a terminal emulation program.
- Use the **System > DNS** screen (see [Section 46.6 on page 493](#)) to configure the DNS (Domain Name System) server used for mapping a domain name to its corresponding IP address and vice versa.
- Use the **System > WWW** screens (see [Section 46.7 on page 501](#)) to configure settings for HTTP or HTTPS access to the UAG and how the login and access user screens look.
- Use the **System > SSH** screen (see [Section 46.8 on page 518](#)) to configure SSH (Secure SHell) used to securely access the UAG's command line interface. You can specify which zones allow SSH access and from which IP address the access can come.
- Use the **System > TELNET** screen (see [Section 46.9 on page 523](#)) to configure Telnet to access the UAG's command line interface. Specify which zones allow Telnet access and from which IP address the access can come.
- Use the **System > FTP** screen (see [Section 46.10 on page 524](#)) to specify from which zones FTP can be used to access the UAG. You can also specify from which IP addresses the access can come. You can upload and download the UAG's firmware and configuration files using FTP. Please also see [Chapter 48 on page 549](#) for more information about firmware and configuration files.
- Your UAG can act as an SNMP agent, which allows a manager station to manage and monitor the UAG through the network. Use the **System > SNMP** screen (see [Section 46.11 on page 525](#)) to configure SNMP settings, including from which zones SNMP can be used to access the UAG. You can also specify from which IP addresses the access can come.
- Use the **Auth. Server** screen ([Section 46.12 on page 528](#)) to configure the UAG to operate as a RADIUS server.
- Use the **Language** screen ([Section 46.13 on page 531](#)) to set the user interface language for the UAG's Web Configurator screens.
- Use the **ZON** screen ([Section 46.14 on page 531](#)) to enable or disable ZDP discovery and LLDP discovery on the UAG.

Note: See each section for related background information and term definitions.

46.2 Host Name

A host name is the unique name by which a device is known on a network. Click **Configuration > System > Host Name** to open the **Host Name** screen.

Figure 327 Configuration > System > Host Name

The following table describes the labels in this screen.

Table 230 Configuration > System > Host Name

LABEL	DESCRIPTION
System Name	Enter a descriptive name to identify your UAG device. This name can be up to 64 alphanumeric characters long. Spaces are not allowed, but dashes (-) underscores (_) and periods (.) are accepted.
Domain Name	Enter the domain name (if you know it) here. This name is propagated to DHCP clients connected to interfaces with the DHCP server enabled. This name can be up to 254 alphanumeric characters long. Spaces are not allowed, but dashes "-" are accepted.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

46.3 USB Storage

The UAG can use a connected USB device to store the system log and other diagnostic information. Use this screen to turn on this feature and set a disk full warning limit.

Note: Only connect one USB device. It must allow writing (it cannot be read-only) and use the FAT16, FAT32, EXT2, or EXT3 file system.

Click **Configuration > System > USB Storage** to open the screen as shown next.

Figure 328 Configuration > System > USB Storage

The following table describes the labels in this screen.

Table 231 Configuration > System > USB Storage

LABEL	DESCRIPTION
Activate USB storage service	Select this if you want to use the connected USB device(s).
Disk full warning when remaining space is less than	Set a number and select a unit (MB or %) to have the UAG send a warning message when the remaining USB storage space is less than the value you set here.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

46.4 Date and Time

For effective scheduling and logging, the UAG system time must be accurate. The UAG's Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server.

To change your UAG's time based on your local time zone and date, click **Configuration > System > Date/Time**. The screen displays as shown. You can manually set the UAG's time and date or have the UAG get the date and time from a time server.

Figure 329 Configuration > System > Date and Time

The following table describes the labels in this screen.

Table 232 Configuration > System > Date and Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the present time of your UAG.
Current Date	This field displays the present date of your UAG.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, time zone and daylight saving at the same time, the time zone and daylight saving will affect the new time and date you entered. When you enter the time settings manually, the UAG uses the new setting once you click Apply .
New Time (hh-mm-ss)	This field displays the last updated time from the time server or the last time configured manually. When you set Time and Date Setup to Manual , enter the new time in this field and then click Apply .
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server or the last date configured manually. When you set Time and Date Setup to Manual , enter the new date in this field and then click Apply .

Table 232 Configuration > System > Date and Time (continued)

LABEL	DESCRIPTION
Get from Time Server	<p>Select this radio button to have the UAG get the time and date from the time server you specify below. The UAG requests time and date settings from the time server under the following circumstances.</p> <ul style="list-style-type: none"> • When the UAG starts up. • When you click Apply or Sync. Now in this screen. • 24-hour intervals after starting up.
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Sync. Now	Click this button to have the UAG get the time and date from a time server (see the Time Server Address field). This also saves your changes (except the daylight saving settings).
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Enable Daylight Saving	<p>Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.</p> <p>Select this option if you use Daylight Saving Time.</p>
Start Date	<p>Configure the day and time when Daylight Saving Time starts if you selected Enable Daylight Saving. The at field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Second, Sunday, March and type 2 in the at field.</p> <p>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, March. The time you type in the at field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
End Date	<p>Configure the day and time when Daylight Saving Time ends if you selected Enable Daylight Saving. The at field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select First, Sunday, November and type 2 in the at field.</p> <p>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, October. The time you type in the at field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
Offset	<p>Specify how much the clock changes when daylight saving begins and ends.</p> <p>Enter a number from 1 to 5.5 (by 0.5 increments).</p> <p>For example, if you set this field to 3.5, a log occurred at 6 P.M. in local official time will appear as if it had occurred at 10:30 P.M.</p>
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

46.4.1 Pre-defined NTP Time Servers List

When you turn on the UAG for the first time, the date and time start at 2003-01-01 00:00:00. The UAG then attempts to synchronize with one of the following pre-defined list of Network Time Protocol (NTP) time servers.

The UAG continues to use the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

Table 233 Default Time Servers

0.pool.ntp.org
1.pool.ntp.org
2.pool.ntp.org

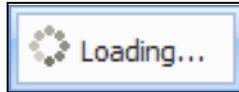
When the UAG uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the UAG goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

46.4.2 Time Server Synchronization

Click the **Synchronize Now** button to get the time and date from the time server you specified in the **Time Server Address** field.

When the **Loading...** screen appears, you may have to wait up to one minute.

Figure 330 Synchronization in Process



The **Current Time** and **Current Date** fields will display the appropriate settings if the synchronization is successful.

If the synchronization was not successful, a log displays in the **View Log** screen. Try re-configuring the **Date/Time** screen.

To manually set the UAG date and time.

- 1 Click **System > Date/Time**.
- 2 Select **Manual** under **Time and Date Setup**.
- 3 Enter the UAG's time in the **New Time** field.
- 4 Enter the UAG's date in the **New Date** field.
- 5 Under **Time Zone Setup**, select your **Time Zone** from the list.
- 6 As an option you can select the **Enable Daylight Saving** check box to adjust the UAG clock for daylight savings.
- 7 Click **Apply**.

To get the UAG date and time from a time server

- 1 Click **System > Date/Time**.
- 2 Select **Get from Time Server** under **Time and Date Setup**.
- 3 Under **Time Zone Setup**, select your **Time Zone** from the list.
- 4 As an option you can select the **Enable Daylight Saving** check box to adjust the UAG clock for daylight savings.
- 5 Under **Time and Date Setup**, enter a **Time Server Address** ([Table 233 on page 491](#)).
- 6 Click **Apply**.

46.5 Console Port Speed

This section shows you how to set the console port speed when you connect to the UAG via the console port using a terminal emulation program. See [Table 2 on page 22](#) for default console port settings.

Click **Configuration > System > Console Speed** to open the **Console Speed** screen.

Figure 331 Configuration > System > Console Speed

The following table describes the labels in this screen.

Table 234 Configuration > System > Console Speed

LABEL	DESCRIPTION
Console Port Speed	Use the drop-down list box to change the speed of the console port. Your UAG supports 9600, 19200, 38400, 57600, and 115200 bps (default) for the console port. The Console Port Speed applies to a console port connection using terminal emulation software and NOT the Console in the UAG Web Configurator Status screen.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

46.6 DNS Overview

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

46.6.1 DNS Server Address Assignment

The UAG can get the DNS server addresses in the following ways.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
- If your ISP dynamically assigns the DNS server IP addresses (along with the UAG's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.
- You can manually enter the IP addresses of other DNS servers.

46.6.2 Configuring the DNS Screen

Click **Configuration > System > DNS** to change your UAG's DNS settings. Use the **DNS** screen to configure the UAG to use a DNS server to resolve domain names for UAG system features like DDNS and the time server. You can also configure the UAG to accept or discard DNS queries. Use the **Network > Interface** screens to configure the DNS server information that the UAG sends to the specified DHCP client devices.

Figure 332 Configuration > System > DNS

DNS

Address/PTR Record

+ Add
 ✎ Edit
 ✖ Remove

#	FQDN	IP Address
No data to display		

⏪ ⏩ Page 1 of 1 ⏪ ⏩ Show 50 items

CNAME Record

+ Add
 ✎ Edit
 ✖ Remove

#	Alias Name	FQDN
No data to display		

⏪ ⏩ Page 1 of 1 ⏪ ⏩ Show 50 items

Domain Zone Forwarder

+ Add
 ✎ Edit
 ✖ Remove
 ↔ Move

#	Domain Zone	Type	DNS Server	Query via
-	*	Default	172.13.1.2 172.13.1.1	wan1 wan1

⏪ ⏩ Page 1 of 1 ⏪ ⏩ Show 50 items Displaying 1 - 1 of 1

MX Record (for My FQDN)

+ Add
 ✎ Edit
 ✖ Remove

#	Domain Name	IP/FQDN
No data to display		

⏪ ⏩ Page 1 of 1 ⏪ ⏩ Show 50 items

Service Control

+ Add
 ✎ Edit
 ✖ Remove
 ↔ Move

#	Zone	Address	Action
-	ALL	ALL	Accept

⏪ ⏩ Page 1 of 1 ⏪ ⏩ Show 50 items Displaying 1 - 1 of 1

The following table describes the labels in this screen.

Table 235 Configuration > System > DNS

LABEL	DESCRIPTION
Address/PTR Record	This record specifies the mapping of a Fully-Qualified Domain Name (FQDN) to an IP address. An FQDN consists of a host and domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
#	This is the index number of the address/PTR record.
FQDN	This is a host's fully qualified domain name.
IP Address	This is the IP address of a host.

Table 235 Configuration > System > DNS (continued)

LABEL	DESCRIPTION
CNAME Record	This record specifies an alias for a FQDN. Use this record to bind all subdomains with the same IP address as the FQDN without having to update each one individually, which increases chance for errors. See CNAME Record (Section 46.6.6 on page 497) for more details.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The UAG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
#	This is the index number of the domain zone forwarder record. The ordering of your rules is important as rules are applied in sequence. A hyphen (-) displays for the default domain zone forwarder record. The default record is not configurable. The UAG uses this default record if the domain zone that needs to be resolved does not match any of the other domain zone forwarder records.
Alias Name	Enter an Alias name. Use "*" as prefix for a wildcard domain name. For example, *.example.com.
FQDN	Enter the Fully Qualified Domain Name (FQDN).
Domain Zone Forwarder	This specifies a DNS server's IP address. The UAG can query the DNS server to resolve domain zones for features like DDNS and the time server. When the UAG needs to resolve a domain zone, it checks it against the domain zone forwarder entries in the order that they appear in this list.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This is the index number of the domain zone forwarder record. The ordering of your rules is important as rules are applied in sequence. A hyphen (-) displays for the default domain zone forwarder record. The default record is not configurable. The UAG uses this default record if the domain zone that needs to be resolved does not match any of the other domain zone forwarder records.
Domain Zone	A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. A "*" means all domain zones.
Type	This displays whether the DNS server IP address is assigned by the ISP dynamically through a specified interface or configured manually (User-Defined).
DNS Server	This is the IP address of a DNS server. This field displays N/A if you have the UAG get a DNS server IP address from the ISP dynamically but the specified interface is not active.
Query Via	This is the interface through which the UAG sends DNS queries to the entry's DNS server.
MX Record (for My FQDN)	A MX (Mail eXchange) record identifies a mail server that handles the mail for a particular domain.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
#	This is the index number of the MX record.

Table 235 Configuration > System > DNS (continued)

LABEL	DESCRIPTION
Domain Name	This is the domain name where the mail is destined for.
IP/FQDN	This is the IP address or Fully-Qualified Domain Name (FQDN) of a mail server that handles the mail for the domain specified in the field above.
Service Control	This specifies from which computers and zones you can send DNS queries to the UAG.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule. The ordering of your rules is important as rules are applied in sequence. The entry with a hyphen (-) instead of a number is the UAG's (non-configurable) default policy. The UAG applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the UAG will not have to use the default policy.
Zone	This is the zone on the UAG the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to send DNS queries.
Action	This displays whether the UAG accepts DNS queries from the computer with the IP address specified above through the specified zone (Accept) or discards them (Deny).

46.6.3 Address Record

An address record contains the mapping of a Fully-Qualified Domain Name (FQDN) to an IP address. An FQDN consists of a host and domain name. For example, `www.zyxel.com` is a fully qualified domain name, where "www" is the host, "zyxel" is the second-level domain, and "com" is the top level domain. `mail.myZyXEL.com.tw` is also a FQDN, where "mail" is the host, "myZyXEL" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain.

The UAG allows you to configure address records about the UAG itself or another device. This way you can keep a record of DNS names and addresses that people on your network may use frequently. If the UAG receives a DNS query for an FQDN for which the UAG has an address record, the UAG can send the IP address in a DNS response without having to query a DNS name server.

46.6.4 PTR Record

A PTR (pointer) record is also called a reverse record or a reverse lookup record. It is a mapping of an IP address to a domain name.

46.6.5 Adding an Address/PTR Record

Click the **Add** icon in the **Address/PTR Record** table to add an address/PTR record.

Figure 333 Configuration > System > DNS > Address/PTR Record Add

The following table describes the labels in this screen.

Table 236 Configuration > System > DNS > Address/PTR Record Add

LABEL	DESCRIPTION
FQDN	Type a Fully-Qualified Domain Name (FQDN) of a server. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain. Underscores are not allowed. Use ".*." as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).
IP Address	Enter the IP address of the host in dotted decimal notation.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving

46.6.6 CNAME Record

A Canonical Name Record or CNAME record is a type of resource record in the Domain Name System (DNS) that specifies that the domain name is an alias of another, canonical domain name. This allows users to set up a record for a domain name which translates to an IP address, in other words, the domain name is an alias of another. This record also binds all the subdomains to the same IP address without having to create a record for each, so when the IP address is changed, all subdomain's IP address is updated as well, with one edit to the record.

For example, the domain name zyxel.com is hooked up to a record named **A** which translates it to 11.22.33.44. You also have several subdomains, like mail.zyxel.com, ftp.zyxel.com and you want this subdomain to point to your main domain zyxel.com. Edit the IP address in record **A** and all subdomains will follow automatically. This eliminates chances for errors and increases efficiency in DNS management.

46.6.7 Adding a CNAME Record

Click the **Add** icon in the CNAME Record table to add a record. Use ".*." as a prefix for a wildcard domain name. For example *.zyxel.com.

Figure 334 Configuration > System > DNS > CNAME Record > Add

The following table describes the labels in this screen.

Table 237 Configuration > System > DNS > CNAME Record > Add

LABEL	DESCRIPTION
Alias name	Enter an Alias Name. Use ".*." as a prefix in the Alias name for a wildcard domain name (for example, *.example.com).
FQDN	Type a Fully-Qualified Domain Name (FQDN) of a server. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain. Underscores are not allowed. Use ".*." as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving

46.6.8 Domain Zone Forwarder

A domain zone forwarder contains a DNS server's IP address. The UAG can query the DNS server to resolve domain zones for features like DDNS and the time server. A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.

46.6.9 Adding a Domain Zone Forwarder

Click the **Add** icon in the **Domain Zone Forwarder** table to add a domain zone forwarder record.

Figure 335 Configuration > System > DNS > Domain Zone Forwarder Add

The following table describes the labels in this screen.

Table 238 Configuration > System > DNS > Domain Zone Forwarder Add

LABEL	DESCRIPTION
Domain Zone	<p>A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. For example, whenever the UAG receives needs to resolve a zyxel.com.tw domain name, it can send a query to the recorded name server IP address.</p> <p>Enter * if all domain zones are served by the specified DNS server(s).</p>
DNS Server	<p>Select DNS Server(s) from ISP if your ISP dynamically assigns DNS server information. You also need to select an interface through which the ISP provides the DNS server IP address(es). The interface should be activated and set to be a DHCP client. The fields below display the (read-only) DNS server IP address(es) that the ISP assigns. N/A displays for any DNS server IP address fields for which the ISP does not assign an IP address.</p> <p>Select Public DNS Server if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. The DNS server could be on the Internet or one of the UAG's local networks. You cannot use 0.0.0.0. Use the Query via field to select the interface through which the UAG sends DNS queries to a DNS server.</p> <p>Select Private DNS Server if you have the IP address of a DNS server to which the UAG connects through a VPN tunnel. Enter the DNS server's IP address in the field to the right. You cannot use 0.0.0.0.</p>
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving

46.6.10 MX Record

A MX (Mail eXchange) record indicates which host is responsible for the mail for a particular domain, that is, controls where mail is sent for that domain. If you do not configure proper MX records for your domain or other domain, external e-mail from other mail servers will not be able to be delivered to your mail server and vice versa. Each host or domain can have only one MX record, that is, one domain is mapping to one host.

46.6.11 Adding a MX Record

Click the **Add** icon in the **MX Record** table to add a MX record.

Figure 336 Configuration > System > DNS > MX Record Add

The following table describes the labels in this screen.

Table 239 Configuration > System > DNS > MX Record Add

LABEL	DESCRIPTION
Domain Name	Enter the domain name where the mail is destined for.
IP Address/FQDN	Enter the IP address or Fully-Qualified Domain Name (FQDN) of a mail server that handles the mail for the domain specified in the field above.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving

46.6.12 Adding a DNS Service Control Rule

Click the **Add** icon in the **Service Control** table to add a service control rule.

Figure 337 Configuration > System > DNS > Service Control Rule Add

The following table describes the labels in this screen.

Table 240 Configuration > System > DNS > Service Control Rule Add

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Address Object	Select ALL to allow or deny any computer to send DNS queries to the UAG. Select a predefined address object to just allow or deny the computer with the IP address that you specified to send DNS queries to the UAG.
Zone	Select ALL to allow or prevent DNS queries through any zones. Select a predefined zone on which a DNS query to the UAG is allowed or denied.

Table 240 Configuration > System > DNS > Service Control Rule Add (continued)

LABEL	DESCRIPTION
Action	Select Accept to have the UAG allow the DNS queries from the specified computer. Select Deny to have the UAG reject the DNS queries from the specified computer.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving

46.7 WWW Overview

The following figure shows secure and insecure management of the UAG coming in from the WAN. HTTPS and SSH access are secure. HTTP and Telnet access are not secure.

Note: To allow the UAG to be accessed from a specified computer using a service, make sure you do not have a service control rule or to-Device security policy to block that traffic.

- See [To-Device Rules on page 290](#) for more on To-Device security policies.

To stop a service from accessing the UAG, clear **Enable** in the corresponding service screen.

46.7.1 Service Access Limitations

A service cannot be used to access the UAG when:

- 1 You have disabled that service in the corresponding screen.
- 2 The allowed IP address (address object) in the **Service Control** table does not match the client IP address (the UAG disallows the session).
- 3 The IP address (address object) in the **Service Control** table is not in the allowed zone or the action is set to **Deny**.
- 4 There is a security policy that blocks it.

46.7.2 System Timeout

There is a lease timeout for administrators. The UAG automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

Each user is also forced to log in the UAG for authentication again when the reauthentication time expires.

You can change the timeout settings in the **User/Group** screens.

46.7.3 HTTPS

You can set the UAG to use HTTP or HTTPS (HTTPS adds security) for Web Configurator sessions. Specify which zones allow Web Configurator access and from which IP address the access can come.

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

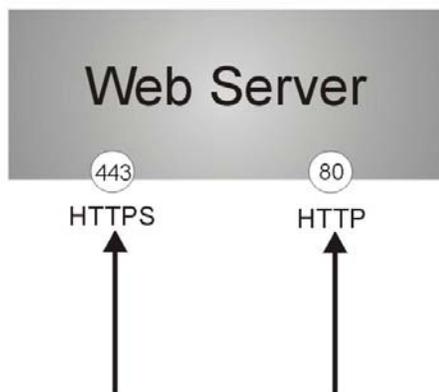
It relies upon certificates, public keys, and private keys (see [Chapter 44 on page 467](#) for more information).

HTTPS on the UAG is used so that you can securely access the UAG using the Web Configurator. The SSL protocol specifies that the HTTPS server (the UAG) must always authenticate itself to the HTTPS client (the computer which requests the HTTPS connection with the UAG), whereas the HTTPS client only should authenticate itself when the HTTPS server requires it to do so (select **Authenticate Client Certificates** in the **WWW** screen). **Authenticate Client Certificates** is optional and if selected means the HTTPS client must send the UAG a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the UAG.

Please refer to the following figure.

- 1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the UAG's web server.
- 2 HTTP connection requests from a web browser go to port 80 (by default) on the UAG's web server.

Figure 338 HTTP/HTTPS Implementation



Note: If you disable **HTTP** in the **WWW** screen, then the UAG blocks all HTTP connection attempts.

46.7.4 Configuring WWW Service Control

Click **Configuration > System > WWW** to open the **WWW** screen. Use this screen to specify from which zones you can access the UAG using HTTP or HTTPS. You can also specify which IP addresses the access can come from.

Note: **Admin Service Control** deals with management access (to the Web Configurator). **User Service Control** deals with user access to the UAG (logging into a web portal to access the Internet for example).

Figure 339 Configuration > System > WWW > Service Control

The screenshot shows the 'Service Control' configuration page. It is organized into several sections:

- HTTPS:** Includes an 'Enable' checkbox (checked), a 'Server Port' field (443), an 'Authenticate Client Certificates' checkbox (unchecked), a 'Server Certificate' dropdown (default), and a 'Redirect HTTP to HTTPS' checkbox (unchecked).
- Admin Service Control:** A table with columns '#', 'Zone', 'Address', and 'Action'. It contains one row: Zone: ALL, Address: ALL, Action: accept. Below the table are navigation controls: Page 1 of 1, Show 50 items, and Displaying 1 - 1 of 1.
- User Service Control:** A table with columns '#', 'Zone', 'Address', and 'Action'. It contains one row: Zone: ALL, Address: ALL, Action: accept. Below the table are navigation controls: Page 1 of 1, Show 50 items, and Displaying 1 - 1 of 1.
- HTTP:** Includes an 'Enable' checkbox (checked), a 'Server Port' field (80).
- Admin Service Control (HTTP):** A table with columns '#', 'Zone', 'Address', and 'Action'. It contains one row: Zone: ALL, Address: ALL, Action: accept. Below the table are navigation controls: Page 1 of 1, Show 50 items, and Displaying 1 - 1 of 1.
- User Service Control (HTTP):** A table with columns '#', 'Zone', 'Address', and 'Action'. It contains one row: Zone: ALL, Address: ALL, Action: accept. Below the table are navigation controls: Page 1 of 1, Show 50 items, and Displaying 1 - 1 of 1.
- Authentication:** Includes a 'Client Authentication Method' dropdown (default).

At the bottom of the page are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 241 Configuration > System > WWW > Service Control

LABEL	DESCRIPTION
HTTPS	
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the UAG Web Configurator using secure HTTPs connections.

Table 241 Configuration > System > WWW > Service Control (continued)

LABEL	DESCRIPTION
Server Port	The HTTPS server listens on port 443 by default. If you change the HTTPS server port to a different number on the UAG, for example 8443, then you must notify people who need to access the UAG Web Configurator to use "https://UAG IP Address: 8443 " as the URL.
Authenticate Client Certificates	Select Authenticate Client Certificates (optional) to require the SSL client to authenticate itself to the UAG by sending the UAG a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the UAG (see Section 46.7.7.5 on page 513 on importing certificates for details).
Server Certificate	Select a certificate the HTTPS server (the UAG) uses to authenticate itself to the HTTPS client. You must have certificates already configured in the My Certificates screen.
Redirect HTTP to HTTPS	To allow only secure Web Configurator access, select this to redirect all HTTP connection requests to the HTTPS server.
Admin/User Service Control	Admin Service Control specifies from which zones an administrator can use HTTPS to manage the UAG (using the Web Configurator). You can also specify the IP addresses from which the administrators can manage the UAG. User Service Control specifies from which zones a user can use HTTPS to log into the UAG (to log into a web portal to access the Internet for example). You can also specify the IP addresses from which the users can access the UAG.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This is the index number of the service control rule. The entry with a hyphen (-) instead of a number is the UAG's (non-configurable) default policy. The UAG applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the UAG will not have to use the default policy.
Zone	This is the zone on the UAG the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the UAG zone(s) configured in the Zone field (Accept) or not (Deny).
HTTP	
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the UAG Web Configurator using HTTP connections.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service to access the UAG.

Table 241 Configuration > System > WWW > Service Control (continued)

LABEL	DESCRIPTION
Admin/User Service Control	Admin Service Control specifies from which zones an administrator can use HTTP to manage the UAG (using the Web Configurator). You can also specify the IP addresses from which the administrators can manage the UAG. User Service Control specifies from which zones a user can use HTTP to log into the UAG (to log into a web portal to access the Internet for example). You can also specify the IP addresses from which the users can access the UAG.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This is the index number of the service control rule. The entry with a hyphen (-) instead of a number is the UAG's (non-configurable) default policy. The UAG applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the UAG will not have to use the default policy.
Zone	This is the zone on the UAG the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the UAG zone(s) configured in the Zone field (Accept) or not (Deny).
Authentication	
Client Authentication Method	Select a method the HTTPS or HTTP server uses to authenticate a client. You must have configured the authentication methods in the Auth. method screen.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

46.7.5 Service Control Rules

Click **Add** or **Edit** in the **Service Control** table in a **WWW**, **SSH**, **Telnet**, **FTP** or **SNMP** screen to add a service control rule.

Figure 340 Configuration > System > Service Control Rule > Edit

The screenshot shows a dialog box titled "Create new Object" with a dropdown arrow. It contains three rows of configuration options, each with a label and a dropdown menu:

- Address Object: ALL
- Zone: ALL
- Action: Accept

At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

The following table describes the labels in this screen.

Table 242 Configuration > System > Service Control Rule > Edit

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Address Object	Select ALL to allow or deny any computer to communicate with the UAG using this service. Select a predefined address object to just allow or deny the computer with the IP address that you specified to access the UAG using this service.
Zone	Select ALL to allow or prevent any UAG zones from being accessed using this service. Select a predefined UAG zone on which a incoming service is allowed or denied.
Action	Select Accept to allow the user to access the UAG from the specified computers. Select Deny to block the user's access to the UAG from the specified computers.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving

46.7.6 Customizing the WWW Login Page

Click **Configuration > System > WWW > Login Page** to open the **Login Page** screen. Use this screen to customize the Web Configurator login screen. You can also customize the page that displays after an access user logs into the Web Configurator to access network services like the Internet. See [Chapter 35 on page 399](#) for more on access user accounts. You can configure both the desktop and mobile versions of the the service pages. Users click a link in the pages to switch between the two versions.

Figure 341 Configuration > System > WWW > Login Page (Desktop View)

Service Control | **Login Page**

Desktop View | Mobile View

Select Type

Use Default Login Page

Use Customized Login Page

Logo File

To upload a logo file (*.gif/png/jpg), browse to the location of the file and then click Upload.
(support format: *.gif/png/jpg, maximum size: 100K, suggest pixel size: 103*29)

File Path:

Customized Login Page

Title:

Titlecolor: (CSS color code)

Message Color: (CSS color code)

Note Message:

Background (support format: *.gif/png/jpg, maximum size: 100K)

Picture

Color (CSS color code)

Customized Access Page

Title:

Message Color: (CSS color code)

Note Message:

Background (support format: *.gif/png/jpg, maximum size: 100K)

Picture

Color (CSS color code)

My Device

Enter User Name/Password and click to login.

User Name:

Password:

(max. 63 alphanumeric, printable characters and no spaces)

Error Message

Note:

1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.

You now have logged in.

Click the logout button to terminate the access session.
You could renew your lease time by clicking the Renew button.
For security reason you must login in again after

User-defined lease time (max

Remaining time before lease

timeout (hh:mm:ss):

Remaining time before auth. timeout (hh:mm):

none

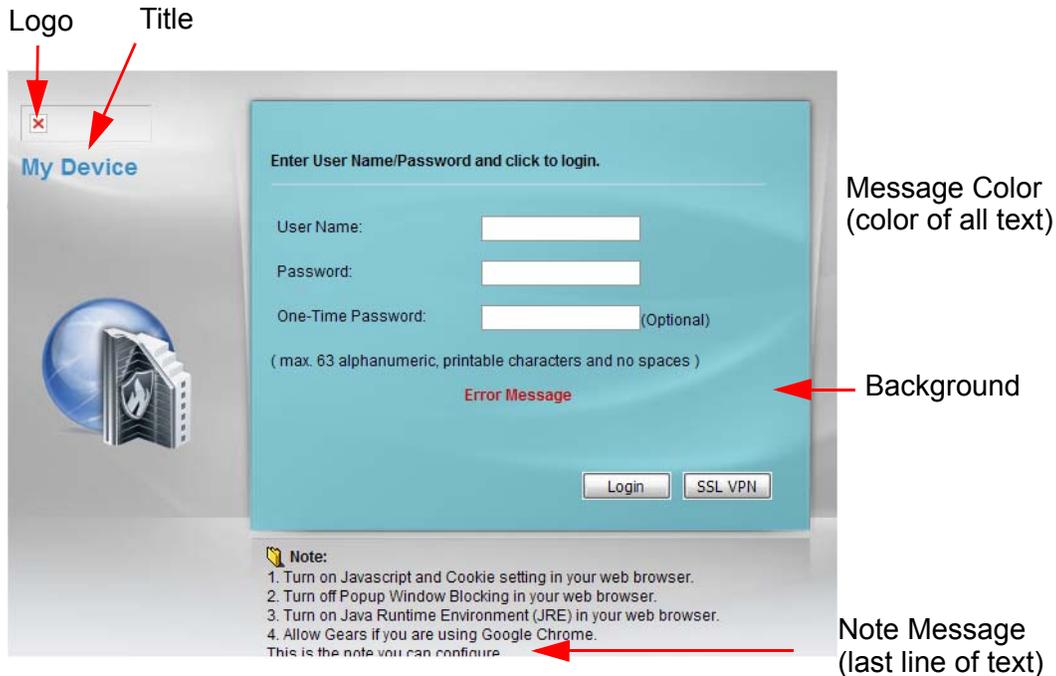
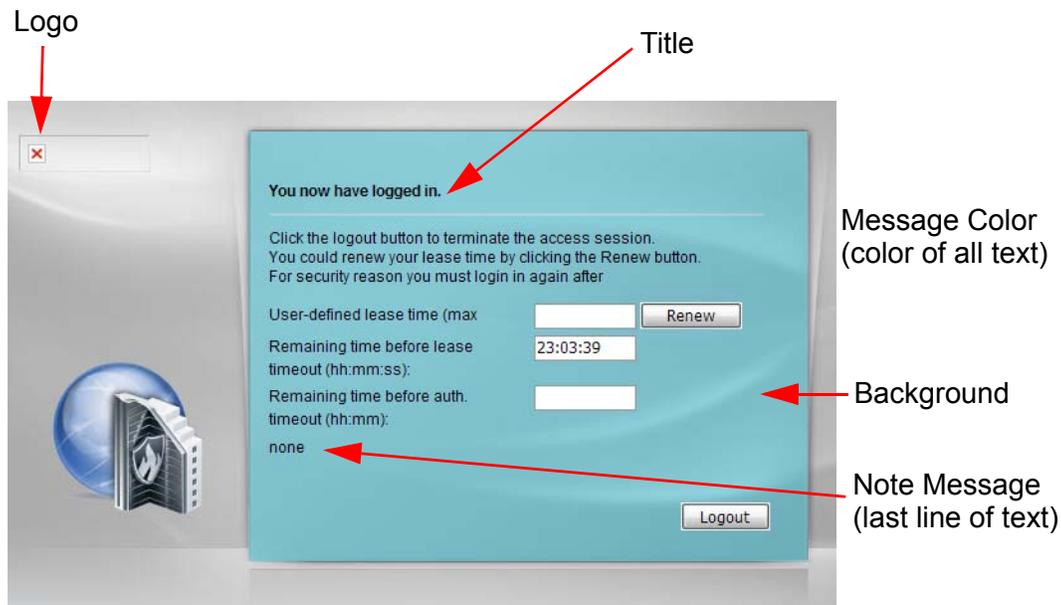
Figure 342 Configuration > System > WWW > Login Page (Mobile View)

The configuration interface for the mobile login page is shown in the screenshot. It includes the following sections and fields:

- Service Control:** Login Page
- View:** Desktop View, Mobile View
- Select Type:**
 - Use Default Login Page
 - Use Customized Login Page
- General:**
 - Logo File:** To upload a logo file (*.gif/png/jpg), browse to the location of the file and then click Upload. (support format: *.gif/png/jpg, maximum size: 100K, suggest pixel size: 70*20)
 - File Path:** Select a File Path, Browse..., Upload
 - Banner Color:** #0c5698, Color, (CSS color code)
- Customized Login Page:**
 - Title:** Login
 - Titlecolor:** #666666, Color, (CSS color code)
- Customized Access Page:**
 - Title:** you now have logged in.
 - Message Color:** #666666, Color, (CSS color code)

At the bottom of the configuration area are **Apply** and **Reset** buttons.

The following figures identify the parts you can customize in the login and access pages.

Figure 343 Login Page Customization**Figure 344** Access Page Customization

You can specify colors in one of the following ways:

- Click **Color** to display a screen of web-safe colors from which to choose.
- Enter the name of the desired color.
- Enter a pound sign (#) followed by the six-digit hexadecimal number that represents the desired color. For example, use "#000000" for black.

- Enter "rgb" followed by red, green, and blue values in parenthesis and separate by commas. For example, use "rgb(0,0,0)" for black.

Your desired color should display in the preview screen on the right after you click in another field, click **Apply**, or press [ENTER]. If your desired color does not display, your browser may not support it. Try selecting another color.

The following table describes the labels in the screen.

Table 243 Configuration > System > WWW > Login Page

LABEL	DESCRIPTION
Select Type	Select whether the Web Configurator uses the default login screen or the one that you customize in the rest of this screen.
Logo File	You can upload a graphic logo to be displayed on the upper left corner of the Web Configurator login screen and access page. Specify the location and file name of the logo graphic or click Browse to locate it. Note: Use a GIF, JPG, or PNG of 100 kilobytes or less. Click Upload to transfer the specified graphic file from your computer to the UAG.
Banner Color	Specify the color of the banner on the top of the screen for the mobile version.
Customized Login Page	Use this section to set how the Web Configurator login screen looks.
Title	Enter the title for the top of the screen. Use up to 64 printable ASCII characters. Spaces are allowed.
Title Color	Specify the color of the screen's title text.
Message Color	Specify the color of the screen's text.
Note Message	Enter a note to display at the bottom of the screen. Use up to 64 printable ASCII characters. Spaces are allowed. This field is not applicable to the mobile version.
Background	Set how the screen background looks. To use a graphic, select Picture and upload a graphic. Specify the location and file name of the logo graphic or click Browse to locate it. The picture's size cannot be over 438 x 337 pixels. Note: Use a GIF, JPG, or PNG of 100 kilobytes or less. To use a color, select Color and specify the color. This field is not applicable to the mobile version.
Customized Access Page	Use this section to customize the page that displays after an access user logs into the Web Configurator to access network services like the Internet.
Title	Enter the title for the top of the screen. Use up to 64 printable ASCII characters. Spaces are allowed.
Message Color	Specify the color of the screen's text.
Note Message	Enter a note to display below the title. Use up to 64 printable ASCII characters. Spaces are allowed. This field is not applicable to the mobile version.

Table 243 Configuration > System > WWW > Login Page

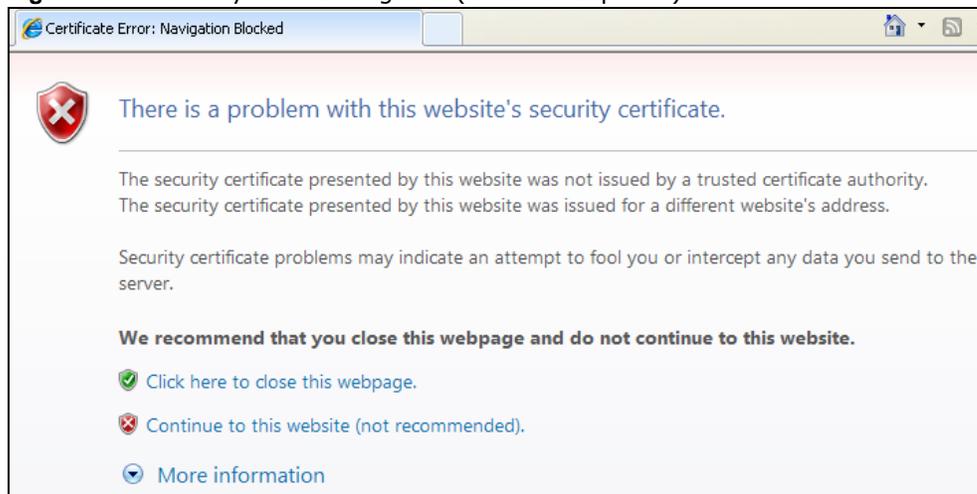
LABEL	DESCRIPTION
Background	<p>Set how the window's background looks.</p> <p>To use a graphic, select Picture and upload a graphic. Specify the location and file name of the logo graphic or click Browse to locate it. The picture's size cannot be over 438 x 337 pixels.</p> <p>Note: Use a GIF, JPG, or PNG of 100 kilobytes or less.</p> <p>To use a color, select Color and specify the color.</p> <p>This field is not applicable to the mobile version.</p>
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

46.7.7 HTTPS Example

If you haven't changed the default HTTPS port on the UAG, then in your browser enter "https://UAG IP Address/" as the web site address where "UAG IP Address" is the IP address or domain name of the UAG you wish to access.

46.7.7.1 Internet Explorer Warning Messages

When you attempt to access the UAG HTTPS server, you will see the error message shown in the following screen.

Figure 345 Security Alert Dialog Box (Internet Explorer)

Select **Continue to this website** to proceed to the Web Configurator login screen. Otherwise, select **Click here to close this webpage** to block the access.

46.7.7.2 Mozilla Firefox Warning Messages

When you attempt to access the UAG HTTPS server, a **The Connection is Untrusted** screen appears as shown in the following screen. Click **Technical Details** if you want to verify more information about the certificate from the UAG.

Select **I Understand the Risks** and then click **Add Exception** to add the UAG to the security exception list. Click **Confirm Security Exception**.

Figure 346 Security Certificate 1 (Firefox)

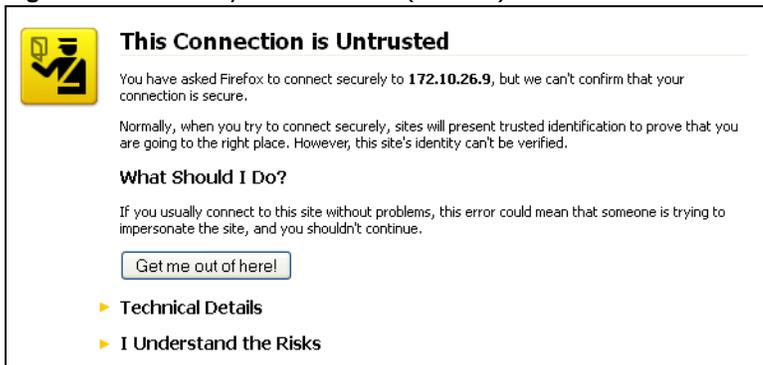
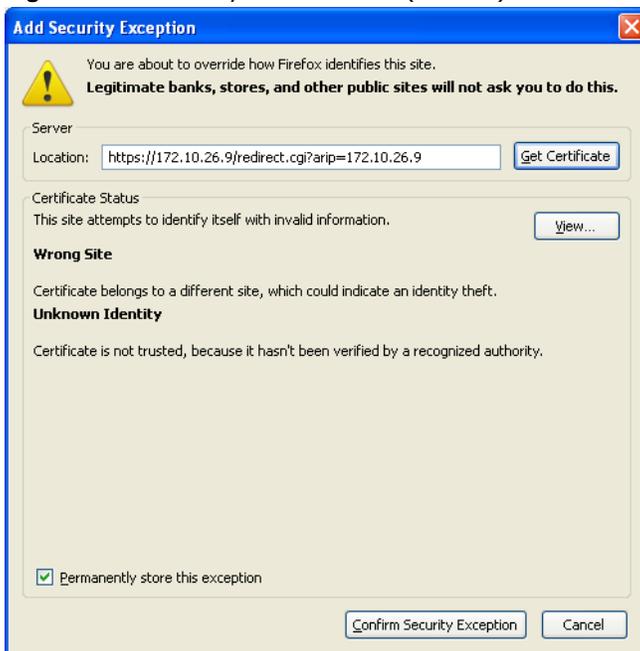


Figure 347 Security Certificate 2 (Firefox)



46.7.7.3 Avoiding Browser Warning Messages

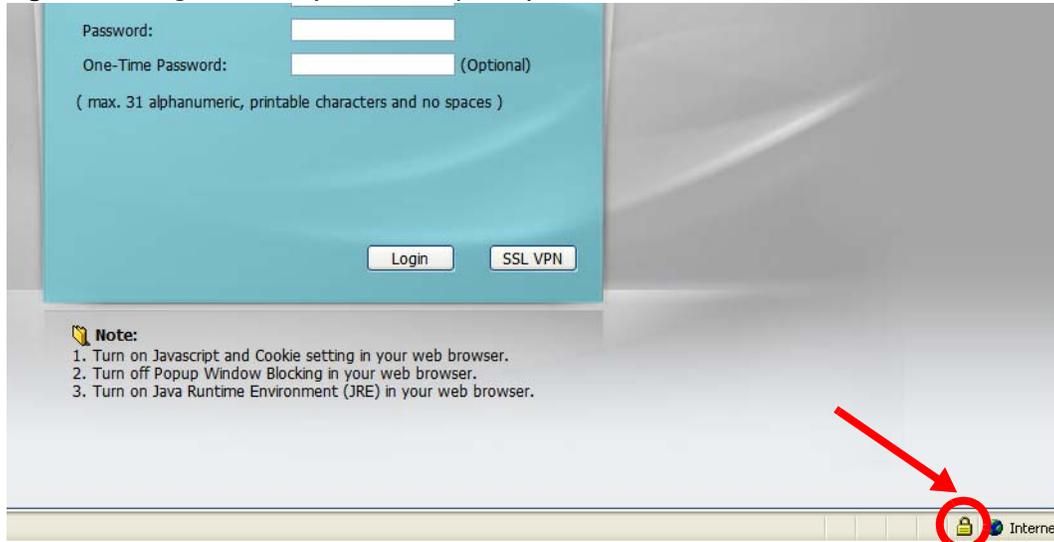
Here are the main reasons your browser displays warnings about the UAG's HTTPS server certificate and what you can do to avoid seeing the warnings:

- The issuing certificate authority of the UAG's HTTPS server certificate is not one of the browser's trusted certificate authorities. The issuing certificate authority of the UAG's factory default certificate is the UAG itself since the certificate is a self-signed certificate.
- For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.
- To have the browser trust the certificates issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certificate.

46.7.7.4 Login Screen

After you accept the certificate, the UAG login screen appears. The lock displayed in the bottom of the browser status bar denotes a secure connection.

Figure 348 Login Screen (Internet Explorer)



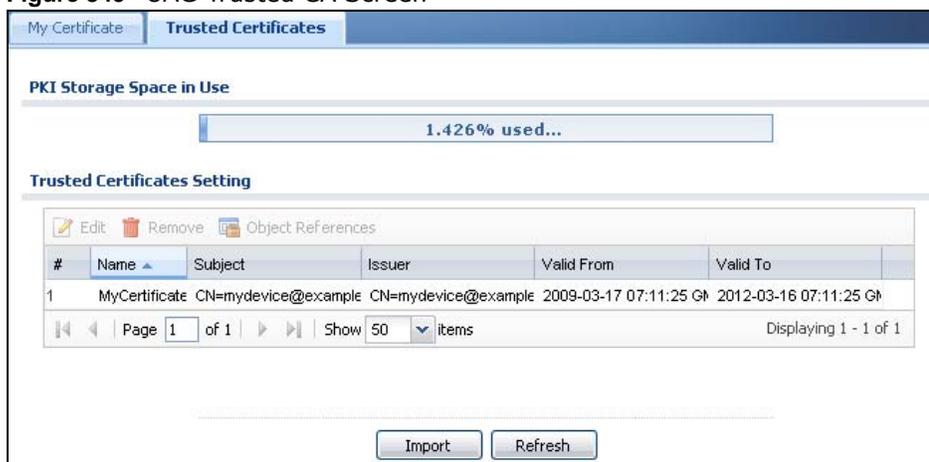
46.7.7.5 Enrolling and Importing SSL Client Certificates

The SSL client needs a certificate if **Authenticate Client Certificates** is selected on the UAG.

You must have imported at least one trusted CA to the UAG in order for the **Authenticate Client Certificates** to be active (see the Certificates chapter for details).

Apply for a certificate from a Certification Authority (CA) that is trusted by the UAG (see the UAG's **Trusted CA Web Configurator** screen).

Figure 349 UAG Trusted CA Screen



The CA sends you a package containing the CA's trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

46.7.7.5.1 Installing the CA's Certificate

- 1 Double click the CA's trusted certificate to produce a screen similar to the one shown next.

Figure 350 CA Certificate Example



- 2 Click **Install Certificate** and follow the wizard as shown earlier in this appendix.

46.7.7.5.2 Installing Your Personal Certificate(s)

You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next

- 1 Click **Next** to begin the wizard.

Figure 351 Personal Certificate Import Wizard 1

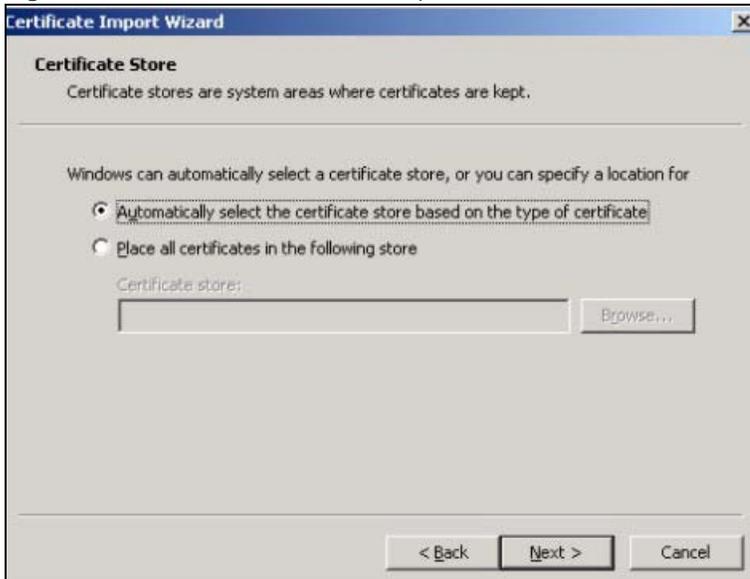
- 2 The file name and path of the certificate you double-clicked should automatically appear in the **File name** text box. Click **Browse** if you wish to import a different certificate.

Figure 352 Personal Certificate Import Wizard 2

- 3 Enter the password given to you by the CA.

Figure 353 Personal Certificate Import Wizard 3

- 4 Have the wizard determine where the certificate should be saved on your computer or select **Place all certificates in the following store** and choose a different location.

Figure 354 Personal Certificate Import Wizard 4

- 5 Click **Finish** to complete the wizard and begin the import process.

Figure 355 Personal Certificate Import Wizard 5

- 6 You should see the following screen when the certificate is correctly installed on your computer.

Figure 356 Personal Certificate Import Wizard 6

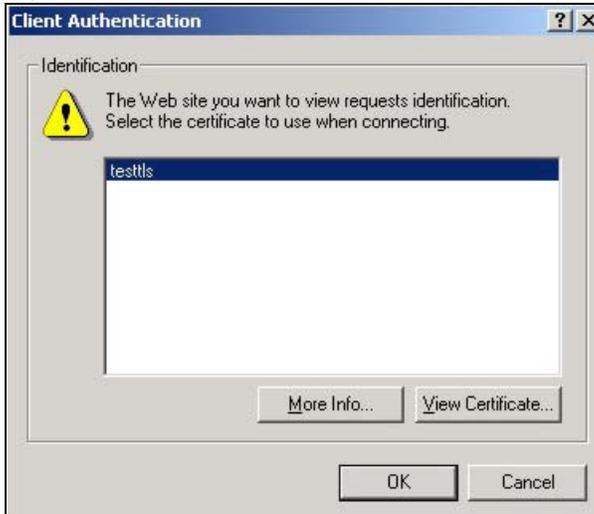
46.7.7.6 Using a Certificate When Accessing the UAG Example

Use the following procedure to access the UAG via HTTPS.

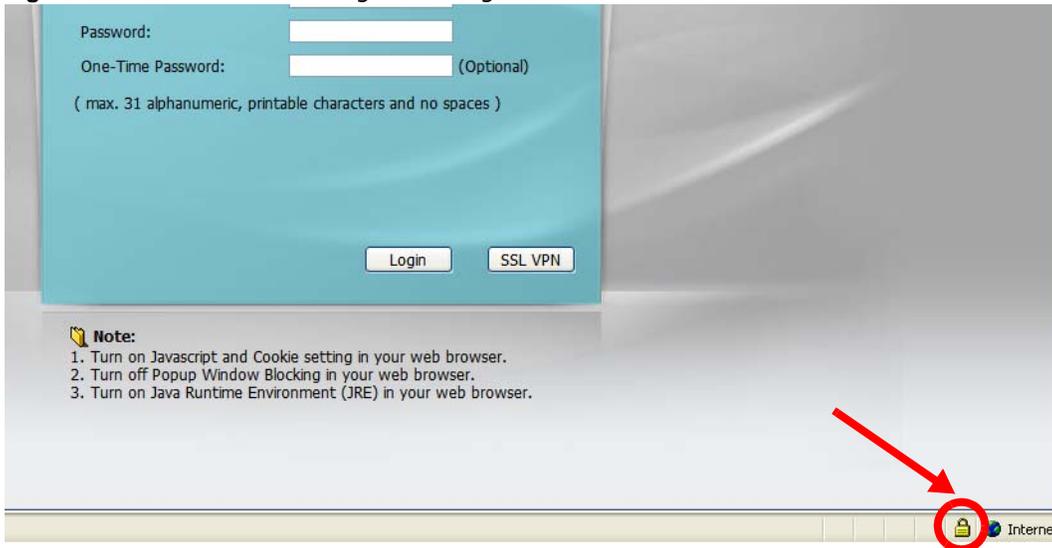
- 1 Enter 'https://UAG IP Address/' in your browser's web address field.

Figure 357 Access the UAG Via HTTPS

- 2 When **Authenticate Client Certificates** is selected on the UAG, the following screen asks you to select a personal certificate to send to the UAG. This screen displays even if you only have a single certificate as in the example.

Figure 358 SSL Client Authentication

- 3 You next see the Web Configurator login screen.

Figure 359 Secure Web Configurator Login Screen

46.8 SSH

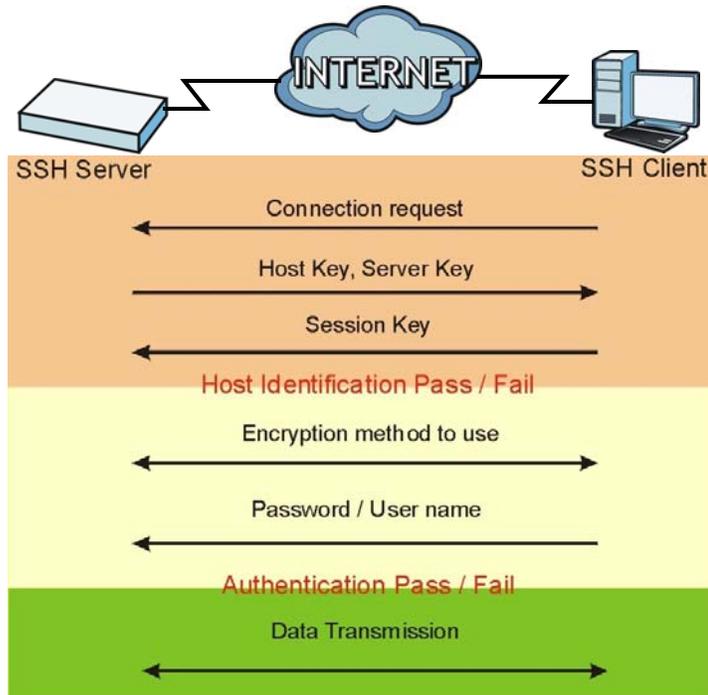
You can use SSH (Secure SHell) to securely access the UAG's command line interface. Specify which zones allow SSH access and from which IP address the access can come.

SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. In the following figure, computer A on the Internet uses SSH to securely connect to the WAN port of the UAG for a management session.

Figure 360 SSH Communication Over the WAN Example

46.8.1 How SSH Works

The following figure is an example of how a secure connection is established between two remote hosts using SSH v1.

Figure 361 How SSH v1 Works Example

1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

46.8.2 SSH Implementation on the UAG

Your UAG supports SSH versions 1 and 2 using RSA authentication and four encryption methods (AES, 3DES, Archfour, and Blowfish). The SSH server is implemented on the UAG for management using port 22 (by default).

46.8.3 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the UAG over SSH.

46.8.4 Configuring SSH

Click **Configuration > System > SSH** to change your UAG's Secure Shell settings. Use this screen to specify from which zones SSH can be used to manage the UAG. You can also specify from which IP addresses the access can come.

Figure 362 Configuration > System > SSH

The following table describes the labels in this screen.

Table 244 Configuration > System > SSH

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the UAG CLI using this service.
Version 1	Select the check box to have the UAG use both SSH version 1 and version 2 protocols. If you clear the check box, the UAG uses only SSH version 2 protocol.

Table 244 Configuration > System > SSH (continued)

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the UAG for SSH connections. You must have certificates already configured in the My Certificates screen (See Chapter 44 on page 467 for details).
Service Control	This specifies from which computers you can access which UAG zones.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry. Refer to Table 242 on page 506 for details on the screen that opens.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule.
Zone	This is the zone on the UAG the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the UAG zone(s) configured in the Zone field (Accept) or not (Deny).
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

46.8.5 Secure Telnet Using SSH Examples

This section shows two examples using a command interface and a graphical interface SSH client program to remotely access the UAG. The configuration and connection steps are similar for most SSH client programs. Refer to your SSH client program user's guide.

46.8.5.1 Example 1: Microsoft Windows

This section describes how to access the UAG using the Secure Shell Client program.

- 1 Launch the SSH client and specify the connection information (IP address, port number) for the UAG.
- 2 Configure the SSH client to accept connection using SSH version 1.
- 3 A window displays prompting you to store the host key in you computer. Click **Yes** to continue.

Figure 363 SSH Example 1: Store Host Key

Enter the password to log in to the UAG. The CLI screen displays next.

46.8.5.2 Example 2: Linux

This section describes how to access the UAG using the OpenSSH client program that comes with most Linux distributions.

- 1 Test whether the SSH service is available on the UAG.

Enter "telnet 172.16.0.1 22" at a terminal prompt and press [ENTER]. The computer attempts to connect to port 22 on the UAG (using the default IP address of 172.16.0.1).

A message displays indicating the SSH protocol version supported by the UAG.

Figure 364 SSH Example 2: Test

```
$ telnet 172.16.0.1 22
Trying 172.16.0.1...
Connected to 172.16.0.1.
Escape character is '^]'.
SSH-1.5-1.0.0
```

- 2 Enter "ssh -1 172.16.0.1". This command forces your computer to connect to the UAG using SSH version 1. If this is the first time you are connecting to the UAG using SSH, a message displays prompting you to save the host information of the UAG. Type "yes" and press [ENTER].

Then enter the password to log in to the UAG.

Figure 365 SSH Example 2: Log in

```
$ ssh -1 172.16.0.1
The authenticity of host '172.16.0.1 (172.16.0.1)' can't be established.
RSA1 key fingerprint is 21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.0.1' (RSA1) to the list of known hosts.
Administrator@172.16.0.1's password:
```

- 3 The CLI screen displays next.

46.9 Telnet

You can use Telnet to access the UAG's command line interface. Specify which zones allow Telnet access and from which IP address the access can come.

46.9.1 Configuring Telnet

Click **Configuration > System > TELNET** to configure your UAG for remote Telnet access. Use this screen to specify from which zones Telnet can be used to manage the UAG. You can also specify from which IP addresses the access can come.

Figure 366 Configuration > System > TELNET

The following table describes the labels in this screen.

Table 245 Configuration > System > TELNET

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the UAG CLI using this service.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Service Control	This specifies from which computers you can access which UAG zones.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry. Refer to Table 242 on page 506 for details on the screen that opens.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.

Table 245 Configuration > System > TELNET (continued)

LABEL	DESCRIPTION
#	This is the index number of the service control rule. The entry with a hyphen (-) instead of a number is the UAG's (non-configurable) default policy. The UAG applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the UAG will not have to use the default policy.
Zone	This is the zone on the UAG the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the UAG zone(s) configured in the Zone field (Accept) or not (Deny).
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

46.10 FTP

You can upload and download the UAG's firmware and configuration files using FTP. To use this feature, your computer must have an FTP client. Please see [Chapter 48 on page 549](#) for more information about firmware and configuration files.

46.10.1 Configuring FTP

To change your UAG's FTP settings, click **Configuration > System > FTP** tab. The screen appears as shown. Use this screen to specify from which zones FTP can be used to access the UAG. You can also specify from which IP addresses the access can come.

Figure 367 Configuration > System > FTP

The screenshot shows the 'FTP' configuration page. Under 'General Settings', the 'Enable' checkbox is checked, 'TLS required' is unchecked, 'Server Port' is 21, and 'Server Certificate' is 'default'. The 'Service Control' section contains a table with one entry: # '-', Zone ALL, Address ALL, and Action Accept. The table has 'Add', 'Edit', 'Remove', and 'Move' icons above it. At the bottom are 'Apply' and 'Reset' buttons.

#	Zone	Address	Action
-	ALL	ALL	Accept

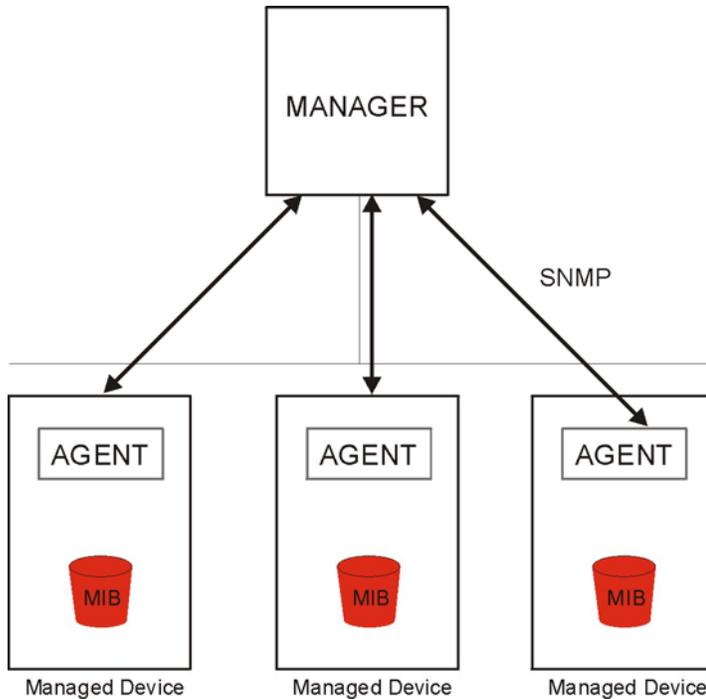
The following table describes the labels in this screen.

Table 246 Configuration > System > FTP

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the UAG using this service.
TLS required	Select the check box to use FTP over TLS (Transport Layer Security) to encrypt communication. This implements TLS as a security mechanism to secure FTP clients and/or servers.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the UAG for FTP connections. You must have certificates already configured in the My Certificates screen (See Chapter 44 on page 467 for details).
Service Control	This specifies from which computers you can access which UAG zones.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry. Refer to Table 242 on page 506 for details on the screen that opens.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule. The entry with a hyphen (-) instead of a number is the UAG's (non-configurable) default policy. The UAG applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the UAG will not have to use the default policy.
Zone	This is the zone on the UAG the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the UAG zone(s) configured in the Zone field (Accept) or not (Deny).
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

46.11 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your UAG supports SNMP agent functionality, which allows a manager station to manage and monitor the UAG through the network. The UAG supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation.

Figure 368 SNMP Management Model

An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the UAG). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

46.11.1 Supported MIBs

The UAG supports MIB II that is defined in RFC-1213 and RFC-1215. The UAG also supports private MIBs (private.mib and enterprise.mib) to collect information about CPU and memory usage. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance. You can download the UAG's MIBs from www.zyxel.com.

46.11.2 SNMP Traps

The UAG will send traps to the SNMP manager when any one of the following events occurs.

Table 247 SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the UAG is turned on or an agent restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.

46.11.3 Configuring SNMP

To change your UAG's SNMP settings, click **Configuration > System > SNMP** tab. The screen appears as shown. Use this screen to configure your SNMP settings, including from which zones SNMP can be used to access the UAG. You can also specify from which IP addresses the access can come.

Figure 369 Configuration > System > SNMP

SNMP

General Settings

Enable

Server Port:

Trap:

Community: (Optional)

Destination: (Optional)

Trap CAPWAP Event

Get Community:

Set Community:

Service Control

#	Zone	Address	Action
-	ALL	ALL	Accept

Displaying 1 - 1 of 1

The following table describes the labels in this screen.

Table 248 Configuration > System > SNMP

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the UAG using this service.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the SNMP manager to which your SNMP traps are sent.
Trap CAPWAP Event	Select this option to have the UAG send a trap to the SNMP manager when a managed AP is connected to or disconnected from the UAG.
Get Community	Enter the Get Community , which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the Set community , which is the password for incoming Set requests from the management station. The default is private and allows all requests.
Service Control	This specifies from which computers you can access which UAG zones.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry. Refer to Table 242 on page 506 for details on the screen that opens.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule. The entry with a hyphen (-) instead of a number is the UAG's (non-configurable) default policy. The UAG applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the UAG will not have to use the default policy.
Zone	This is the zone on the UAG the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the UAG zone(s) configured in the Zone field (Accept) or not (Deny).
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

46.12 Authentication Server

You can set the UAG to work as a RADIUS server to exchange messages with a RADIUS client, such as an AP for user authentication and authorization. Click **Configuration > System > Auth. Server** tab. The screen appears as shown. Use this screen to enable the authentication server feature of the UAG and specify the RADIUS client's IP address.

Figure 370 Configuration > System > Auth. Server

Auth. Server

General Settings

Enable Authentication Server

Authentication Server Certificate: default

Authentication Method: default

Trusted Client

Add Edit Remove Activate Inactivate

#	Status	Profile Name	IP Address	Mask	Description
1		test	172.16.1.11	255.255.255.0	

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

Apply Reset

The following table describes the labels in this screen.

Table 249 Configuration > System > Auth. Server

LABEL	DESCRIPTION
Enable Authentication Server	Select the check box to have the UAG act as a RADIUS server.
Authentication Server Certificate	Select the certificate whose corresponding private key is to be used to identify the UAG to the RADIUS client. You must have certificates already configured in the My Certificates screen.
Authentication Method	Select an authentication method if you have created any in the Configuration > Object > Auth. Method screen.
Trusted Client	Use this section to configure trusted clients in the UAG RADIUS server database.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The UAG confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
#	This is the index number of the entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Profile Name	This field indicates the name assigned to the profile.
IP Address	This is the IP address of the RADIUS client that is allowed to exchange messages with the UAG.
Mask	This is the subnet mask of the RADIUS client.
Description	This is the description of the RADIUS client.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

46.12.1 Add/Edit Trusted RADIUS Client

Click **Configuration > System > Auth. Server** to display the **Auth. Server** screen. Click the **Add** icon or an **Edit** icon to display the following screen. Use this screen to create a new entry or edit an existing one.

Figure 371 Configuration > System > Auth. Server > Add/Edit

The following table describes the labels in this screen.

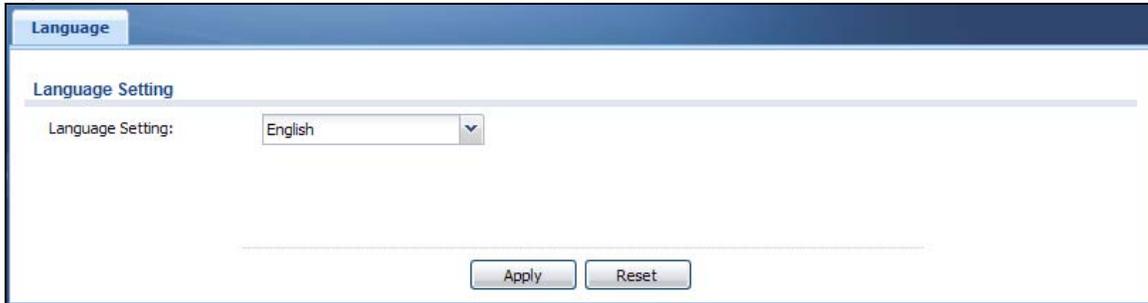
Table 250 Configuration > System > Auth. Server > Add/Edit

LABEL	DESCRIPTION
Activate	Select this check box to make this profile active.
Profile Name	Enter a descriptive name (up to 31 alphanumeric characters) for identification purposes.
IP Address	Enter the IP address of the RADIUS client that is allowed to exchange messages with the UAG.
Netmask	Enter the subnet mask of the RADIUS client.
Secret	Enter a password (up to 64 alphanumeric characters) as the key to be shared between the UAG and the RADIUS client. The key is not sent over the network. This key must be the same on the external authentication server and the UAG.
Description	Enter the description of each server, if any. You can use up to 60 printable ASCII characters.
OK	Click OK to save the changes.
Cancel	Click Cancel to discard the changes.

46.13 Language

Click **Configuration > System > Language** to open this screen. Use this screen to select a display language for the UAG's Web Configurator screens.

Figure 372 Configuration > System > Language



The following table describes the labels in this screen.

Table 251 Configuration > System > Language

LABEL	DESCRIPTION
Language Setting	Select a display language for the UAG's Web Configurator screens. You also need to open a new browser session to display the screens in the new language.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

46.14 ZyXEL One Network (ZON) Utility

The ZyXEL One Network (ZON) utility uses the ZyXEL Discovery Protocol (ZDP) for discovering and configuring ZDP-aware ZyXEL devices in the same broadcast domain as the computer on which ZON is installed.

The ZON Utility issues requests via ZDP and in response to the query, the ZyXEL device responds with basic information including IP address, firmware version, location, system and model name. The information is then displayed in the ZON Utility screen and you can perform tasks like basic configuration of the devices and batch firmware upgrade in it. You can download the ZON Utility at www.zyxel.com and install it on a computer.

The following figure shows the ZON Utility screen.

Figure 373 ZON Utility Screen



In the ZON Utility, select a device and then use the icons to perform actions. The following table describes the icons numbered from left to right in the ZON Utility screen.

Table 252 ZON Utility Icons

ICON	DESCRIPTION
1 IP configuration	Change the selected device's IP address. This is not supported by the UAG at the time of writing.
2 Renew IP	Update a DHCP-assigned dynamic IP address. This is not supported by the UAG at the time of writing.
3 Reboot Device	Use this icon to restart the selected device(s). This may be useful when troubleshooting or upgrading new firmware.
4 Flash Locator LED	Use this icon to locate the selected device by causing its Locator LED to blink. This is not available on the UAG at the time of writing.
5 Web GUI	Use this to access the selected device web configurator from your browser. You will need a username and password to log in.
6 Firmware Upgrade	Use this icon to upgrade new firmware to selected device(s) of the same model. Make sure you have downloaded the firmware from the ZyXEL website to your computer and unzipped it in advance.
7 Change Admin Password	Use this icon to change the admin password of the selected device. You must know the current admin password before changing to a new one.
8 ZAC	Use this icon to run the ZyXEL AP Configurator of the selected AP. This is not supported by the UAG at the time of writing.
9 Discovery	You should use this icon first to display all connected devices in the same network as your computer.
10 Save Configuration	Use this icon to save configuration changes to permanent memory on a selected device. This is not needed by the UAG at the time of writing.
11 Settings	Use this icon to select a network adaptor for the computer on which the ZON utility is installed, and the utility language.

The following table describes the fields in the ZON Utility main screen.

Table 253 ZON Utility Fields

LABEL	DESCRIPTION
Type	This field displays an icon of the kind of device discovered.
Model	This field displays the model name of the discovered device.
Firmware Version	This field displays the firmware version of the discovered device.
MAC Address	This field displays the MAC address of the discovered device.
IP Address	This field displays the IP address of an internal interface on the discovered device that first received an ZDP discovery request from the ZON utility.
System Name	This field displays the system name of the discovered device.
Location	This field displays where the discovered device is.
Status	This field displays whether changes to the discovered device have been done successfully. As the UAG does not support IP Configuration , Renew IP address and Flash Locator LED , this field displays "Update failed", "Not support Renew IP address" and "Not support Flash Locator LED" respectively.

46.14.1 ZyXEL One Network (ZON) System Screen

Use this screen to enable **ZDP** and **Smart Connect**.

See **Monitor > System Status > Ethernet Neighbor** for information on using **Smart Connect** (Link Layer Discovery Protocol (LLDP)) for discovering and configuring LLDP-aware devices in the same broadcast domain as the UAG that you're logged into using the web configurator.

Click **Configuration > System > ZON** to open this screen.

Figure 374 Configuration > System > ZON

The following table describes the labels in this screen.

Table 254 Configuration > System > ZON

LABEL	DESCRIPTION
ZDP	ZyXEL Discovery Protocol (ZDP) is the protocol that the ZyXEL One Network (ZON) utility uses for discovering and configuring ZDP-aware ZyXEL devices in the same broadcast domain as the computer on which ZON is installed.
Enable	Select to activate ZDP discovery on the UAG.
Smart Connect	Smart Connect uses Link Layer Discovery Protocol (LLDP) for discovering and configuring LLDP-aware devices in the same broadcast domain as the UAG that you're logged into using the web configurator.
Enable	Select to activate LLDP discovery on the UAG. See also Monitor > System Status > Ethernet Discovery .
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

Log and Report

47.1 Overview

Use these screens to configure daily reporting and log settings.

47.1.1 What You Can Do In this Chapter

- Use the **Email Daily Report** screen ([Section 47.2 on page 534](#)) to configure where and how to send daily reports and what reports to send.
- Use the **Log Settings** screens ([Section 47.3 on page 536](#)) to specify settings for recording log messages and alerts, e-mailing them, storing them on a connected USB storage device, and sending them to remote syslog servers.

47.2 Email Daily Report

Use the **Email Daily Report** screen to start or stop data collection and view various statistics about traffic passing through your UAG.

Note: Data collection may decrease the UAG's traffic throughput rate.

Click **Configuration > Log & Report > Email Daily Report** to display the following screen. Configure this screen to have the UAG e-mail you system statistics every day.

Figure 375 Configuration > Log & Report > Email Daily Report

Email Daily Report

General Settings

Enable Email Daily Report

Email Settings

Mail Server: (Outgoing SMTP Server Name or IP Address)

Mail Server Port: TLS Security Authenticate Server

Mail Subject:

Append system name Append date time

Mail From: (Email Address)

Mail To: (Email Address)

(Email Address)

(Email Address)

(Email Address)

(Email Address)

SMTP Authentication

User Name :

Password:

Retype to Confirm:

Schedule

Time For Sending Report: (hours) (minutes)

Report Items

System Resource Usage

CPU Usage

Memory Usage

Session Usage

Port Usage

Wireless Report

Station Count

TX Statistics

RX Statistics

Threat Report

Content Filter

Interface Traffic Statistics

Reset counters after sending report successfully

The following table describes the labels in this screen.

Table 255 Configuration > Log & Report > Email Daily Report

LABEL	DESCRIPTION
Enable Email Daily Report	Select this to send reports by e-mail every day.
Mail Server	Type the name or IP address of the outgoing SMTP server.
Mail Server Port	Enter the same port number here as is on the mail server for mail traffic.
TLS Security	Select this option to use Transport Layer Security (TLS) if you want encrypted communications between the mail server and the UAG.
Authenticate Server	If you choose TLS Security , you may also select this to have the UAG authenticate the mail server in the TLS handshake.
Mail Subject	Type the subject line for the outgoing e-mail. Select Append system name to add the UAG's system name to the subject. Select Append date time to add the UAG's system date and time to the subject.
Append system name	Select Append system name to add the UAG's system name to the subject.
Append date time	Select Append date time to add the UAG's system date and time to the subject.
Mail From	Type the e-mail address from which the outgoing e-mail is delivered. This address is used in replies.
Mail To	Type the e-mail address (or addresses) to which the outgoing e-mail is delivered.
SMTP Authentication	Select this check box if it is necessary to provide a user name and password to the SMTP server.
User Name	This box is effective when you select the SMTP Authentication check box. Type the user name to provide to the SMTP server when the log is e-mailed.
Password	This box is effective when you select the SMTP Authentication check box. Type the password to provide to the SMTP server when the log is e-mailed.
Retype to Confirm	Retype your new password for confirmation.
Send Report Now	Click this button to have the UAG send the daily e-mail report immediately.
Schedule	
Time For Sending Report	Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation.
Report Items	Select the information to include in the report. Select Reset counters after sending report successfully if you only want to see statistics for a 24 hour period.
Reset All Counters	Click this to discard all report data and start all of the counters over at zero.
Apply	Click Apply to save your changes back to the UAG.
Reset	Click Reset to return the screen to its last-saved settings.

47.3 Log Settings Screens

The **Log Settings** screens control log messages and alerts. A log message stores the information for viewing or regular e-mailing later, and an alert is e-mailed immediately. Usually, alerts are used for events that require more serious attention, such as system errors and attacks.

The UAG provides a system log and supports e-mail profiles and remote syslog servers. View the system log in the **MONITOR > Log** screen. Use the e-mail profiles to mail log messages to the specific destinations. You can also have the UAG store system logs on a connected USB storage device. The other four logs are stored on specified syslog servers.

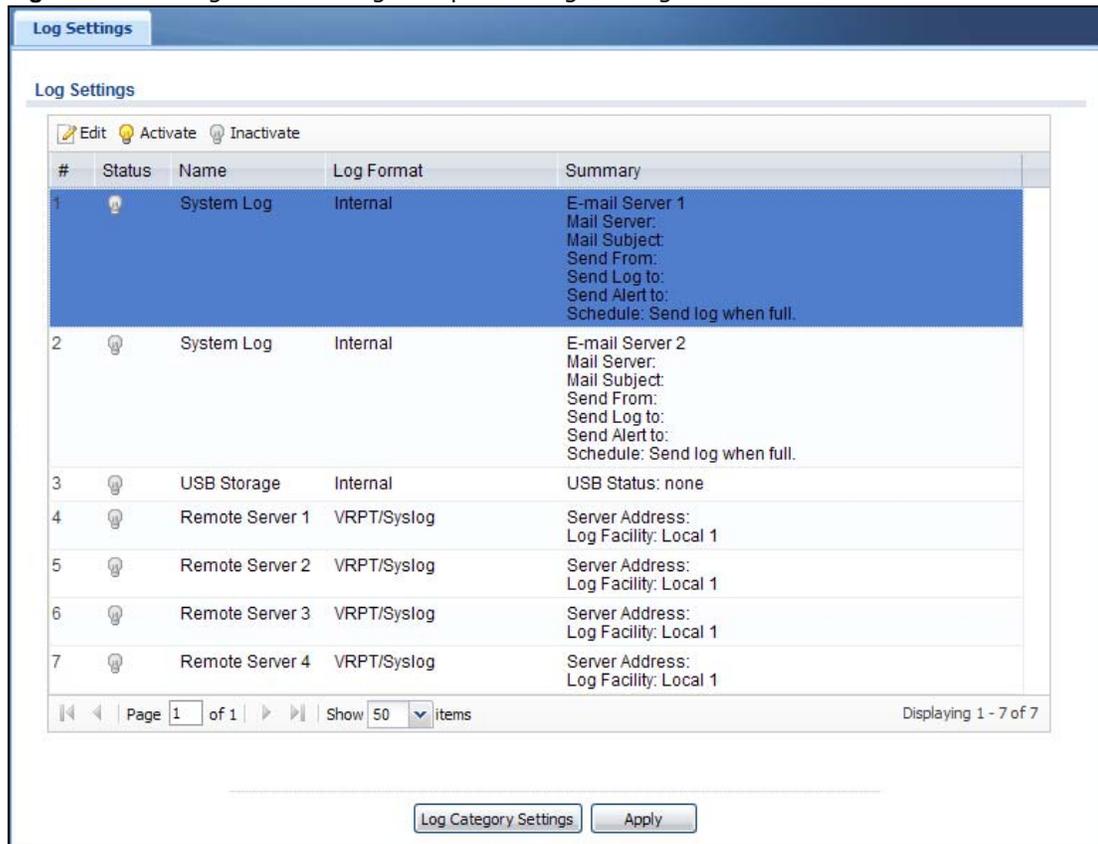
The **Log Settings** screens control what information the UAG saves in each log. You can also specify which log messages to e-mail for the system log, and where and how often to e-mail them. These screens also set for which events to generate alerts and where to email the alerts.

The first **Log Settings** screen provides a settings summary. Use the **Edit** screens to configure settings such as log categories, e-mail addresses, and server names for any log. Use the **Log Category Settings** screen to edit what information is included in the system log, USB storage, e-mail profiles, and remote servers.

47.3.1 Log Settings Summary

To access this screen, click **Configuration > Log & Report > Log Settings**.

Figure 376 Configuration > Log & Report > Log Settings



The following table describes the labels in this screen.

Table 256 Configuration > Log & Report > Log Settings

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify it.
Activate	To turn on an entry, select it and click Activate .

Table 256 Configuration > Log & Report > Log Settings (continued)

LABEL	DESCRIPTION
Inactivate	To turn off an entry, select it and click Inactivate .
#	This field is a sequential value, and it is not associated with a specific log.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the type of log setting entry (system log, logs stored on a USB storage device connected to the UAG, or one of the remote servers).
Log Format	This field displays the format of the log. Internal - system log; you can view the log on the View Log tab. VRPT/Syslog - ZyXEL's Vantage Report, syslog-compatible format. CEF/Syslog - Common Event Format, syslog-compatible format.
Summary	This field is a summary of the settings for each log. Please see Section 47.3.2 on page 538 for more information.
Log Category Settings	Click this button to open the Log Category Settings screen.
Apply	Click this button to save your changes (activate and deactivate logs) and make them take effect.

47.3.2 Edit System Log Settings

The **Log Settings Edit** screen controls the detailed settings for each log in the system log (which includes the e-mail profiles). Go to the **Log Settings Summary** screen (see [Section 47.3.1 on page 537](#)), and click the system log **Edit** icon.

Figure 377 Configuration > Log & Report > Log Settings > Edit (System Log)

Edit Log Setting

E-mail Server 1

Active

Mail Server: (Outgoing SMTP Server Name or IP Address)

Mail Server Port: TLS Security Authenticate Server

Mail Server: (Outgoing SMTP Server Name or IP Address)

Mail Subject:

Send From: (E-Mail Address)

Send Log to: (E-Mail Address)

Send Alerts to: (E-Mail Address)

Sending Log:

Day for Sending Log:

Time for Sending Log:

SMTP Authentication

User Name:

Password:

Retype to Confirm:

E-mail Server 2

Active

Active Log and Alert (AC)

System Log E-mail Server 1 E-mail Server 2

#	Log Category	System Log	E-mail Server 1	E-mail Server 2
1	Account	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
2	Advertisement	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
3	Auth. Policy	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
4	Authentication Server	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
5	Built-in Service	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
6	BWM	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
7	CAPWAP	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
8	Connectivity Check	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
9	Daily Report	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Page 1 of 1 | Show 50 items | Displaying 1 - 30 of 30

Active Log and Alert (AP)

System Log E-mail Server 1 E-mail Server 2

#	Log Category	System Log	E-mail Server 1	E-mail Server 2
1	Account	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
2	Built-in Service	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
3	CAPWAP	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
4	Daily Report	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
5	Default	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
6	DHCP	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
7	File Manager	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
8	Force Authentication	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
9	Interface	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Page 1 of 1 | Show 50 items | Displaying 1 - 20 of 20

Log Consolidation

Active

Log Consolidation Interval (seconds): (10 - 600)

OK Cancel

The following table describes the labels in this screen.

Table 257 Configuration > Log & Report > Log Settings > Edit (System Log)

LABEL	DESCRIPTION
E-Mail Server 1/2	
Active	Select this to send log messages and alerts according to the information in this section. You specify what kinds of log messages are included in log information and what kinds of log messages are included in alerts in the Active Log and Alert section.
Mail Server	Type the name or IP address of the outgoing SMTP server.
Mail Server Port	Enter the same port number here as is on the mail server for mail traffic.
TLS Security	Select this option to use Transport Layer Security (TLS) if you want encrypted communications between the mail server and the UAG.
Authenticate Server	If you choose TLS Security , you may also select this to have the UAG authenticate the mail server in the TLS handshake.
Mail Subject	Type the subject line for the outgoing e-mail.
Send From	Type the e-mail address from which the outgoing e-mail is delivered. This address is used in replies.
Send Log To	Type the e-mail address to which the outgoing e-mail is delivered.
Send Alerts To	Type the e-mail address to which alerts are delivered.
Sending Log	Select how often log information is e-mailed. Choices are: When Full, Hourly and When Full, Daily and When Full , and Weekly and When Full .
Day for Sending Log	This field is available if the log is e-mailed weekly. Select the day of the week the log is e-mailed.
Time for Sending Log	This field is available if the log is e-mailed weekly or daily. Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation.
SMTP Authentication	Select this check box if it is necessary to provide a user name and password to the SMTP server.
User Name	This box is effective when you select the SMTP Authentication check box. Type the user name to provide to the SMTP server when the log is e-mailed.
Password	This box is effective when you select the SMTP Authentication check box. Type the password to provide to the SMTP server when the log is e-mailed.
Retype to Confirm	Retype your new password for confirmation.
Active Log and Alert	
System Log	<p>Use the System Log drop-down list to change the log settings for all of the log categories.</p> <p>disable all logs (red X) - do not log any information for any category for the system log or e-mail any logs to e-mail server 1 or 2.</p> <p>enable normal logs (green check mark) - create log messages and alerts for all categories for the system log. If e-mail server 1 or 2 also has normal logs enabled, the UAG will e-mail logs to them.</p> <p>enable normal logs and debug logs (yellow check mark) - create log messages, alerts, and debugging information for all categories. The UAG does not e-mail debugging information, even if this setting is selected.</p>

Table 257 Configuration > Log & Report > Log Settings > Edit (System Log) (continued)

LABEL	DESCRIPTION
E-mail Server 1	<p>Use the E-Mail Server 1 drop-down list to change the settings for e-mailing logs to e-mail server 1 for all log categories.</p> <p>Using the System Log drop-down list to disable all logs overrides your e-mail server 1 settings.</p> <p>enable normal logs (green check mark) - e-mail log messages for all categories to e-mail server 1.</p> <p>enable alert logs (red exclamation point) - e-mail alerts for all categories to e-mail server 1.</p>
E-mail Server 2	<p>Use the E-Mail Server 2 drop-down list to change the settings for e-mailing logs to e-mail server 2 for all log categories.</p> <p>Using the System Log drop-down list to disable all logs overrides your e-mail server 2 settings.</p> <p>enable normal logs (green check mark) - e-mail log messages for all categories to e-mail server 2.</p> <p>enable alert logs (red exclamation point) - e-mail alerts for all categories to e-mail server 2.</p>
#	This field is a sequential value, and it is not associated with a specific entry.
Log Category	This field displays each category of messages. It is the same value used in the Display and Category fields in the View Log tab. The Default category includes debugging messages generated by open source software.
System log	<p>Select which events you want to log by Log Category. There are three choices:</p> <p>disable all logs (red X) - do not log any information from this category</p> <p>enable normal logs (green check mark) - create log messages and alerts from this category</p> <p>enable normal logs and debug logs (yellow check mark) - create log messages, alerts, and debugging information from this category; the UAG does not e-mail debugging information, however, even if this setting is selected.</p>
E-mail Server 1	Select whether each category of events should be included in the log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in E-Mail Server 1 . The UAG does not e-mail debugging information, even if it is recorded in the System log .
E-mail Server 2	Select whether each category of events should be included in log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in E-Mail Server 2 . The UAG does not e-mail debugging information, even if it is recorded in the System log .
Log Consolidation	
Active	Select this to activate log consolidation. Log consolidation aggregates multiple log messages that arrive within the specified Log Consolidation Interval . In the View Log tab, the text "[count=x]", where <i>x</i> is the number of original log messages, is appended at the end of the Message field, when multiple log messages were aggregated.
Log Consolidation Interval	Type how often, in seconds, to consolidate log information. If the same log message appears multiple times, it is aggregated into one log message with the text "[count=x]", where <i>x</i> is the number of original log messages, appended at the end of the Message field.
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

47.3.3 Edit Log on USB Storage Setting

The **Edit Log on USB Storage Setting** screen controls the detailed settings for saving logs to a connected USB storage device. Go to the **Log Setting Summary** screen (see [Section 47.3.1 on page 537](#)), and click the USB storage **Edit** icon.

Figure 378 Configuration > Log & Report > Log Settings > Edit (USB Storage)

The following table describes the labels in this screen.

Table 258 Configuration > Log & Report > Log Settings > Edit (USB Storage)

LABEL	DESCRIPTION
Duplicate logs to USB storage (if ready)	Select this to have the UAG save a copy of its system logs to a connected USB storage device. Use the Active Log section to specify what kinds of messages to include.
Enable log keep duration	Select this option to have the UAG save a copy of its system logs to a connected USB storage device on a daily basis.
Keep duration	Specify how long the UAG is to keep the copy of system logs in the connected USB storage device before discarding it.
Active Log	

Table 258 Configuration > Log & Report > Log Settings > Edit (USB Storage) (continued)

LABEL	DESCRIPTION
Selection	Use the Selection drop-down list to change the log settings for all of the log categories. disable all logs (red X) - do not send the remote server logs for any log category. enable normal logs (green check mark) - send the remote server log messages and alerts for all log categories. enable normal logs and debug logs (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
#	This field is a sequential value, and it is not associated with a specific entry.
Log Category	This field displays each category of messages. The Default category includes debugging messages generated by open source software.
Selection	Select what information you want to log from each Log Category (except All Logs ; see below). Choices are: disable all logs (red X) - do not log any information from this category enable normal logs (green check mark) - log regular information and alerts from this category enable normal logs and debug logs (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

47.3.4 Edit Remote Server Log Settings

The **Log Settings Edit** screen controls the detailed settings for each log in the remote server (syslog). Go to the **Log Settings Summary** screen (see [Section 47.3.1 on page 537](#)), and click a remote server **Edit** icon.

Figure 379 Configuration > Log & Report > Log Settings > Edit (Remote Server)

Log Settings for Remote Server

Active

Log Format: VRPT/Syslog

Server Address: (Server Name or IP Address)

Log Facility: Local 1

Active Log (AC)

#	Log Category	Selection
1	Account	<input type="radio"/> <input checked="" type="radio"/> <input checked="" type="radio"/>
2	Advertisement	<input type="radio"/> <input type="radio"/> <input type="radio"/>
3	Auth. Policy	<input type="radio"/> <input type="radio"/> <input type="radio"/>
4	Authentication Server	<input type="radio"/> <input type="radio"/> <input type="radio"/>
5	Built-in Service	<input type="radio"/> <input type="radio"/> <input type="radio"/>
6	BWM	<input type="radio"/> <input type="radio"/> <input type="radio"/>
7	CAPWAP	<input type="radio"/> <input type="radio"/> <input type="radio"/>
8	Connectivity Check	<input type="radio"/> <input type="radio"/> <input type="radio"/>
9	Daily Report	<input type="radio"/> <input type="radio"/> <input type="radio"/>
10	Default	<input type="radio"/> <input type="radio"/> <input type="radio"/>

Page 1 of 1 | Show 50 items | Displaying 1 - 33 of 33

Active Log (AP)

#	Log Category	Selection
1	Account	<input type="radio"/> <input checked="" type="radio"/> <input checked="" type="radio"/>
2	Built-in Service	<input type="radio"/> <input type="radio"/> <input type="radio"/>
3	CAPWAP	<input type="radio"/> <input type="radio"/> <input type="radio"/>
4	Daily Report	<input type="radio"/> <input type="radio"/> <input type="radio"/>
5	Default	<input type="radio"/> <input type="radio"/> <input type="radio"/>
6	DHCP	<input type="radio"/> <input type="radio"/> <input type="radio"/>
7	File Manager	<input type="radio"/> <input type="radio"/> <input type="radio"/>
8	Force Authentication	<input type="radio"/> <input type="radio"/> <input type="radio"/>
9	Interface	<input type="radio"/> <input type="radio"/> <input type="radio"/>
10	Interface Statistics	<input type="radio"/> <input type="radio"/> <input type="radio"/>
11	PKI	<input type="radio"/> <input type="radio"/> <input type="radio"/>
23	ZySH	<input type="radio"/> <input type="radio"/> <input type="radio"/>

Page 1 of 1 | Show 50 items | Displaying 1 - 23 of 23

OK Cancel

The following table describes the labels in this screen.

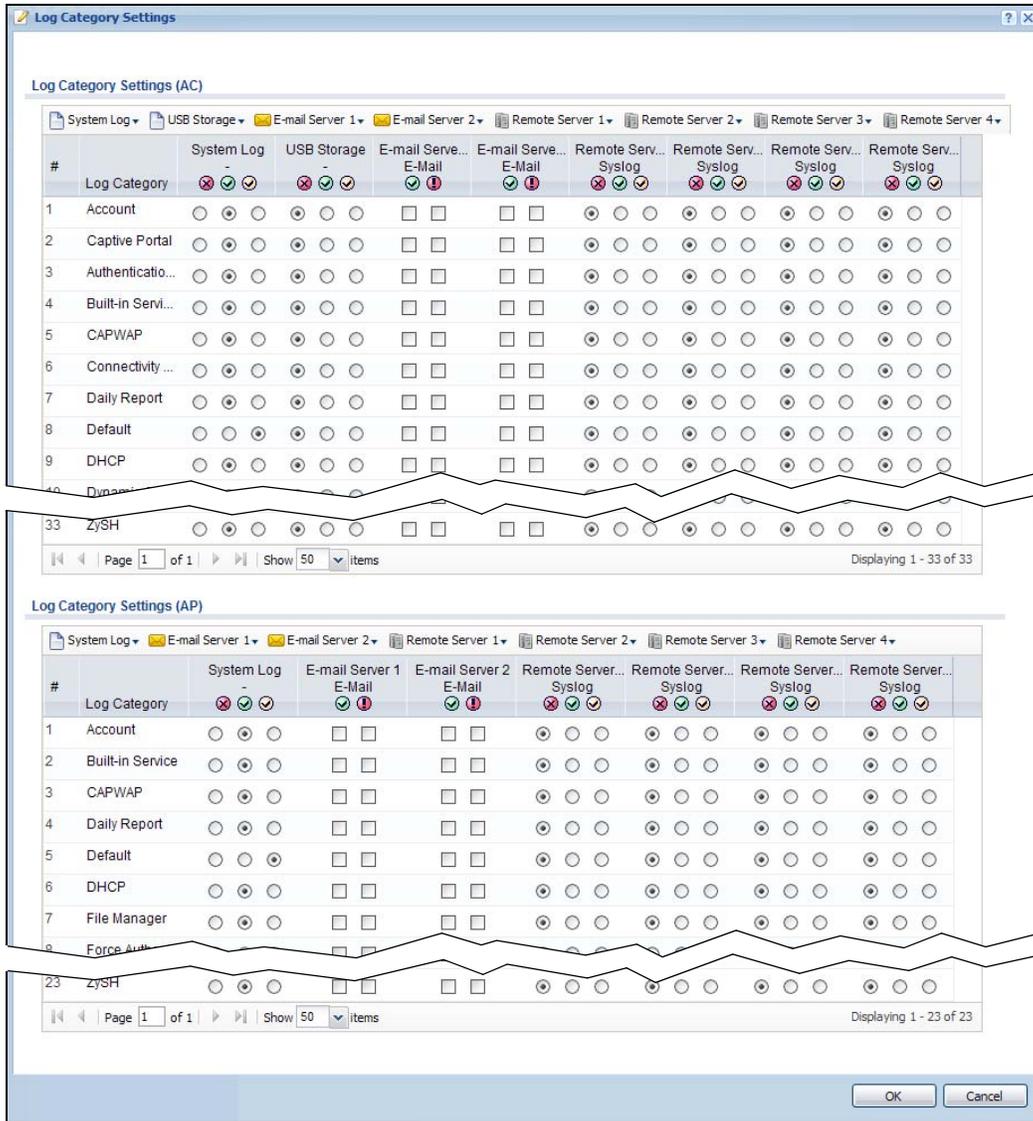
Table 259 Configuration > Log & Report > Log Setting > Edit (Remote Server)

LABEL	DESCRIPTION
Log Settings for Remote Server	
Active	Select this check box to send log information according to the information in this section. You specify what kinds of messages are included in log information in the Active Log section.
Log Format	This field displays the format of the log information. VRPT/Syslog - ZyXEL's Vantage Report, syslog-compatible format. CEF/Syslog - Common Event Format, syslog-compatible format.
Server Address	Type the server name or the IP address of the syslog server to which to send log information.
Log Facility	Select a log facility. The log facility allows you to log the messages to different files in the syslog server. Please see the documentation for your syslog program for more information.
Active Log	
Selection	Use the Selection drop-down list to change the log settings for all of the log categories. disable all logs (red X) - do not send the remote server logs for any log category. enable normal logs (green check mark) - send the remote server log messages and alerts for all log categories. enable normal logs and debug logs (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
#	This field is a sequential value, and it is not associated with a specific entry.
Log Category	This field displays each category of messages. It is the same value used in the Display and Category fields in the View Log tab. The Default category includes debugging messages generated by open source software.
Selection	Select what information you want to log from each Log Category (except All Logs ; see below). Choices are: disable all logs (red X) - do not log any information from this category enable normal logs (green check mark) - log regular information and alerts from this category enable normal logs and debug logs (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

47.3.5 Log Category Settings Screen

This screen allows you to view and to edit what information is included in the system log, USB storage, e-mail profiles, and remote servers at the same time. It does not let you change other log settings (for example, where and how often log information is e-mailed or remote server names). To access this screen, go to the **Log Settings Summary** screen (see [Section 47.3.1 on page 537](#)), and click the **Log Category Settings** button.

Figure 380 Configuration > Log & Report > Log Setting > Log Category Settings



This screen provides a different view and a different way of indicating which messages are included in each log and each alert. Please see [Section 47.3.2 on page 538](#), where this process is discussed. (The **Default** category includes debugging messages generated by open source software.)

The following table describes the fields in this screen.

Table 260 Configuration > Log & Report > Log Setting > Log Category Settings

LABEL	DESCRIPTION
System Log	<p>Use the System Log drop-down list to change the log settings for all of the log categories.</p> <p>disable all logs (red X) - do not log any information for any category for the system log or e-mail any logs to e-mail server 1 or 2.</p> <p>enable normal logs (green check mark) - create log messages and alerts for all categories for the system log. If e-mail server 1 or 2 also has normal logs enabled, the UAG will e-mail logs to them.</p> <p>enable normal logs and debug logs (yellow check mark) - create log messages, alerts, and debugging information for all categories. The UAG does not e-mail debugging information, even if this setting is selected.</p>
USB Storage	<p>Use the USB Storage drop-down list to change the log settings for saving logs to a connected USB storage device.</p> <p>disable all logs (red X) - do not log any information for any category to a connected USB storage device.</p> <p>enable normal logs (green check mark) - create log messages and alerts for all categories and save them to a connected USB storage device.</p> <p>enable normal logs and debug logs (yellow check mark) - create log messages, alerts, and debugging information for all categories and save them to a connected USB storage device.</p>
E-mail Server 1	<p>Use the E-Mail Server 1 drop-down list to change the settings for e-mailing logs to e-mail server 1 for all log categories.</p> <p>Using the System Log drop-down list to disable all logs overrides your e-mail server 1 settings.</p> <p>enable normal logs (green check mark) - e-mail log messages for all categories to e-mail server 1.</p> <p>enable alert logs (red exclamation point) - e-mail alerts for all categories to e-mail server 1.</p>
E-mail Server 2	<p>Use the E-Mail Server 2 drop-down list to change the settings for e-mailing logs to e-mail server 2 for all log categories.</p> <p>Using the System Log drop-down list to disable all logs overrides your e-mail server 2 settings.</p> <p>enable normal logs (green check mark) - e-mail log messages for all categories to e-mail server 2.</p> <p>enable alert logs (red exclamation point) - e-mail alerts for all categories to e-mail server 2.</p>
Remote Server 1~4	<p>For each remote server, use the Selection drop-down list to change the log settings for all of the log categories.</p> <p>disable all logs (red X) - do not send the remote server logs for any log category.</p> <p>enable normal logs (green check mark) - send the remote server log messages and alerts for all log categories.</p> <p>enable normal logs and debug logs (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.</p>
#	<p>This field is a sequential value, and it is not associated with a specific entry.</p>
Log Category	<p>This field displays each category of messages. It is the same value used in the Display and Category fields in the View Log tab. The Default category includes debugging messages generated by open source software.</p>

Table 260 Configuration > Log & Report > Log Setting > Log Category Settings (continued)

LABEL	DESCRIPTION
System Log	<p>Select which events you want to log by Log Category. There are three choices:</p> <p>disable all logs (red X) - do not log any information from this category</p> <p>enable normal logs (green check mark) - create log messages and alerts from this category</p> <p>enable normal logs and debug logs (yellow check mark) - create log messages, alerts, and debugging information from this category; the UAG does not e-mail debugging information, however, even if this setting is selected.</p>
USB Storage	<p>Select which event log categories to save to a connected USB storage device. There are three choices:</p> <p>disable all logs (red X) - do not log any information from this category</p> <p>enable normal logs (green check mark) - save log messages and alerts from this category</p> <p>enable normal logs and debug logs (yellow check mark) - save log messages, alerts, and debugging information from this category.</p>
E-mail Server 1 E-mail	<p>Select whether each category of events should be included in the log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in E-Mail Server 1. The UAG does not e-mail debugging information, even if it is recorded in the System log.</p>
E-mail Server 2 E-mail	<p>Select whether each category of events should be included in log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in E-Mail Server 2. The UAG does not e-mail debugging information, even if it is recorded in the System log.</p>
Remote Server 1~4 Syslog	<p>For each remote server, select what information you want to log from each Log Category (except All Logs; see below). Choices are:</p> <p>disable all logs (red X) - do not log any information from this category</p> <p>enable normal logs (green check mark) - log regular information and alerts from this category</p> <p>enable normal logs and debug logs (yellow check mark) - log regular information, alerts, and debugging information from this category</p>
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

File Manager

48.1 Overview

Configuration files define the UAG's settings. Shell scripts are files of commands that you can store on the UAG and run when you need them. You can apply a configuration file or run a shell script without the UAG restarting. You can store multiple configuration files and shell script files on the UAG. You can edit configuration files or shell scripts in a text editor and upload them to the UAG. Configuration files use a .conf extension and shell scripts use a .zysh extension.

48.1.1 What You Can Do in this Chapter

- Use the **Configuration File** screen (see [Section 48.2 on page 551](#)) to store and name configuration files. You can also download configuration files from the UAG to your computer and upload configuration files from your computer to the UAG.
- Use the **Firmware Package** screen (see [Section 48.3 on page 555](#)) to check your current firmware version and upload firmware to the UAG.
- Use the **Shell Script** screen (see [Section 48.4 on page 557](#)) to store, name, download, upload and run shell script files.

48.1.2 What you Need to Know

Configuration Files and Shell Scripts

When you apply a configuration file, the UAG uses the factory default settings for any features that the configuration file does not include. When you run a shell script, the UAG only applies the commands that it contains. Other settings do not change.

These files have the same syntax, which is also identical to the way you run CLI commands manually. An example is shown below.

Figure 381 Configuration File / Shell Script: Example

```
# enter configuration mode
configure terminal
# change administrator password
username admin password 4321 user-type admin
# configure wan1
interface wan1
ip address 10.16.17.240 255.255.255.0
ip gateway 10.16.17.254 metric 1
exit
# create address objects for remote management / to-Device security policies
# use the address group in case we want to open up remote management later
address-object TW_SUBNET 10.16.37.0/24
object-group address TW_TEAM
address-object TW_SUBNET
exit
# enable Telnet access (not enabled by default, unlike other services)
ip telnet server
# open WAN-to-Device firewall for TW_TEAM for remote management
firewall WAN Device insert 4
sourceip TW_TEAM
service TELNET
action allow
exit
write
```

While configuration files and shell scripts have the same syntax, the UAG applies configuration files differently than it runs shell scripts. This is explained below.

Table 261 Configuration Files and Shell Scripts in the UAG

Configuration Files (.conf)	Shell Scripts (.zysh)
<ul style="list-style-type: none"> Resets to default configuration. Goes into CLI Configuration mode. Runs the commands in the configuration file. 	<ul style="list-style-type: none"> Goes into CLI Privilege mode. Runs the commands in the shell script.

You have to run the example in [Figure 381 on page 550](#) as a shell script because the first command is run in **Privilege** mode. If you remove the first command, you have to run the example as a configuration file because the rest of the commands are executed in **Configuration** mode.

Comments in Configuration Files or Shell Scripts

In a configuration file or shell script, use “#” or “!” as the first character of a command line to have the UAG treat the line as a comment.

Your configuration files or shell scripts can use “exit” or a command line consisting of a single “!” to have the UAG exit sub command mode.

Note: “exit” or “!” must follow sub commands if it is to make the UAG exit sub command mode.

Line 3 in the following example exits sub command mode.

```
interface lan1
ip address dhcp
!
```

Lines 1 and 3 in the following example are comments and line 4 exits sub command mode.

```
!
interface lan1
# this interface is a DHCP client
!
```

Lines 1 and 2 are comments. Line 5 exits sub command mode.

```
! this is from Joe
# on 2008/04/05
interface lan1
ip address dhcp
!
```

Errors in Configuration Files or Shell Scripts

When you apply a configuration file or run a shell script, the UAG processes the file line-by-line. The UAG checks the first line and applies the line if no errors are detected. Then it continues with the next line. If the UAG finds an error, it stops applying the configuration file or shell script and generates a log.

You can change the way a configuration file or shell script is applied. Include `setenv stop-on-error off` in the configuration file or shell script. The UAG ignores any errors in the configuration file or shell script and applies all of the valid commands. The UAG still generates a log for any errors.

48.2 The Configuration File Screen

Click **Maintenance > File Manager > Configuration File** to open the **Configuration File** screen. Use the **Configuration File** screen to store, run, and name configuration files. You can also download configuration files from the UAG to your computer and upload configuration files from your computer to the UAG.

Once your UAG is configured and functioning properly, it is highly recommended that you back up your configuration file before making further configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Configuration File Flow at Restart

- If there is not a **startup-config.conf** when you restart the UAG (whether through a management interface or by physically turning the power off and back on), the UAG uses the **system-default.conf** configuration file with the UAG's default settings.
- If there is a **startup-config.conf**, the UAG checks it for errors and applies it. If there are no errors, the UAG uses it and copies it to the **lastgood.conf** configuration file as a back up file. If there is an error, the UAG generates a log and copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file. If there isn't a **lastgood.conf** configuration file or it also has an error, the UAG applies the **system-default.conf** configuration file.
- You can change the way the **startup-config.conf** file is applied. Include the `setenv-startup stop-on-error off` command. The UAG ignores any errors in the **startup-config.conf** file and applies all of the valid commands. The UAG still generates a log for any errors.

Figure 382 Maintenance > File Manager > Configuration File

The screenshot shows the 'Configuration File' tab in a file manager. It features a table of files with columns for '#', 'File Name', 'Size', and 'Last Modified'. Below the table is a pagination control showing 'Page 1 of 1' and 'Show 50 items'. At the bottom, there is an 'Upload Configuration File' section with a text input for 'File Path', a 'Browse...' button, and an 'Upload' button.

#	File Name	Size	Last Modified
1	startup-config-back.conf	17756	1970-01-01 00:00:13
2	htm-default.conf	20	2012-03-15 02:20:33
3	system-default.conf	7753	1970-01-01 00:00:13
4	startup-config.conf	15020	1970-01-01 05:48:04
5	lastgood.conf	14945	1970-01-01 02:31:22
6	120224608_1.conf	9084	1970-01-01 01:22:30
7	VPN.conf	8235	2012-04-10 03:28:30

Page 1 of 1 | Show 50 items | Displaying 1 - 7 of 7

Upload Configuration File

To upload a configuration file, browse to the location of the file (.conf) and then click Upload.

File Path:

Do not turn off the UAG while configuration file upload is in progress.

The following table describes the labels in this screen.

Table 262 Maintenance > File Manager > Configuration File

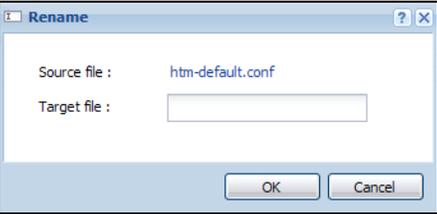
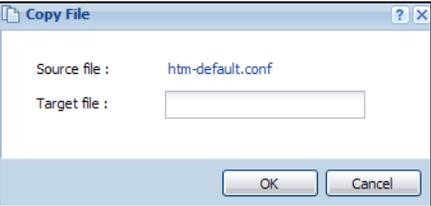
LABEL	DESCRIPTION
Rename	<p>Use this button to change the label of a configuration file on the UAG. You can only rename manually saved configuration files. You cannot rename the lastgood.conf, system-default.conf and startup-config.conf files.</p> <p>You cannot rename a configuration file to the name of another configuration file in the UAG.</p> <p>Click a configuration file's row to select it and click Rename to open the Rename File screen.</p> <p>Figure 383 Maintenance > File Manager > Configuration File > Rename</p>  <p>Specify the new name for the configuration file. Use up to 25 characters (including a-zA-Z0-9;~!@#\$%^&()_+[]{}',=-).</p> <p>Click OK to save the duplicate or click Cancel to close the screen without saving a duplicate of the configuration file.</p>
Remove	<p>Click a configuration file's row to select it and click Remove to delete it from the UAG. You can only delete manually saved configuration files. You cannot delete the system-default.conf, startup-config.conf and lastgood.conf files.</p> <p>A pop-up window asks you to confirm that you want to delete the configuration file. Click OK to delete the configuration file or click Cancel to close the screen without deleting the configuration file.</p>
Download	<p>Click a configuration file's row to select it and click Download to save the configuration to your computer.</p>
Copy	<p>Use this button to save a duplicate of a configuration file on the UAG.</p> <p>Click a configuration file's row to select it and click Copy to open the Copy File screen.</p> <p>Figure 384 Maintenance > File Manager > Configuration File > Copy</p>  <p>Specify a name for the duplicate configuration file. Use up to 25 characters (including a-zA-Z0-9;~!@#\$%^&()_+[]{}',=-).</p> <p>Click OK to save the duplicate or click Cancel to close the screen without saving a duplicate of the configuration file.</p>

Table 262 Maintenance > File Manager > Configuration File (continued)

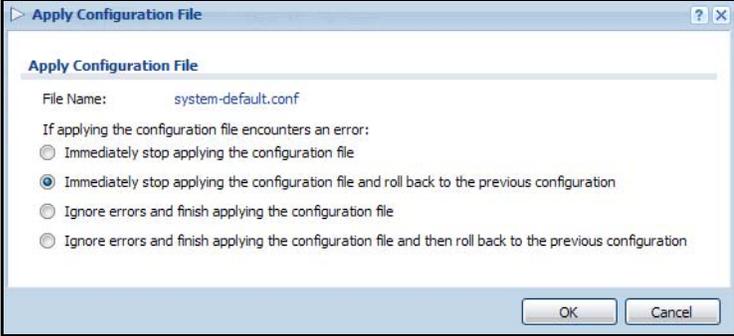
LABEL	DESCRIPTION
Apply	<p>Use this button to have the UAG use a specific configuration file.</p> <p>Click a configuration file's row to select it and click Apply to have the UAG use that configuration file. The UAG does not have to restart in order to use a different configuration file, although you will need to wait for a few minutes while the system reconfigures.</p> <p>The following screen gives you options for what the UAG is to do if it encounters an error in the configuration file.</p> <p>Figure 385 Maintenance > File Manager > Configuration File > Apply</p>  <p>Immediately stop applying the configuration file - this is not recommended because it would leave the rest of the configuration blank. If the interfaces were not configured before the first error, the console port may be the only way to access the device.</p> <p>Immediately stop applying the configuration file and roll back to the previous configuration - this gets the UAG started with a fully valid configuration file as quickly as possible.</p> <p>Ignore errors and finish applying the configuration file - this applies the valid parts of the configuration file and generates error logs for all of the configuration file's errors. This lets the UAG apply most of your configuration and you can refer to the logs for what to fix.</p> <p>Ignore errors and finish applying the configuration file and then roll back to the previous configuration - this applies the valid parts of the configuration file, generates error logs for all of the configuration file's errors, and starts the UAG with a fully valid configuration file.</p> <p>Click OK to have the UAG start applying the configuration file or click Cancel to close the screen</p>
#	<p>This column displays the number for each configuration file entry. This field is a sequential value, and it is not associated with a specific entry. The total number of configuration files that you can save depends on the sizes of the configuration files and the available flash storage space.</p>

Table 262 Maintenance > File Manager > Configuration File (continued)

LABEL	DESCRIPTION
File Name	<p>This column displays the label that identifies a configuration file.</p> <p>You cannot delete the following configuration files or change their file names.</p> <p>The system-default.conf file contains the UAG's default settings. Select this file and click Apply to reset all of the UAG settings to the factory defaults. This configuration file is included when you upload a firmware package.</p> <p>The startup-config.conf file is the configuration file that the UAG is currently using. If you make and save changes during your management session, the changes are applied to this configuration file. The UAG applies configuration changes made in the Web Configurator to the configuration file when you click Apply or OK. It applies configuration changes made via commands when you use the <code>write</code> command.</p> <p>The lastgood.conf is the most recently used (valid) configuration file that was saved when the device last restarted. If you upload and apply a configuration file with an error, you can apply lastgood.conf to return to a valid configuration.</p>
Size	This column displays the size (in KB) of a configuration file.
Last Modified	This column displays the date and time that the individual configuration files were last changed or saved.
Upload Configuration File	<p>The bottom part of the screen allows you to upload a new or previously saved configuration file from your computer to your UAG</p> <p>You cannot upload a configuration file named system-default.conf or lastgood.conf.</p> <p>If you upload startup-config.conf, it will replace the current configuration and immediately apply the new settings.</p>
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click Browse... to find the .conf file you want to upload. The configuration file must use a ".conf" filename extension. You will receive an error message if you try to upload a file of a different format. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click Upload to begin the upload process. This process may take up to two minutes.

48.3 The Firmware Package Screen

Click **Maintenance > File Manager > Firmware Package** to open the **Firmware Package** screen. Use the **Firmware Package** screen to check your current firmware version and upload firmware to the UAG.

Note: The Web Configurator is the recommended method for uploading firmware. You only need to use the command line interface if you need to recover the firmware. See the CLI Reference Guide for how to determine if you need to recover the firmware and how to recover it.

Find the firmware package at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, "UAG.bin".

The firmware update can take up to five minutes. Do not turn off or reset the UAG while the firmware update is in progress!

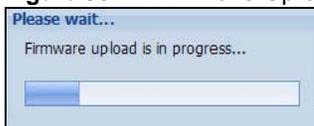
Figure 386 Maintenance > File Manager > Firmware Package

The following table describes the labels in this screen.

Table 263 Maintenance > File Manager > Firmware Package

LABEL	DESCRIPTION
Boot Module	This is the version of the boot module that is currently on the UAG.
Current Version	This is the firmware version and the date created.
Released Date	This is the date that the version of the firmware was created.
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click Browse... to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click Upload to begin the upload process. This process may take up to two minutes.

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the UAG again.

Figure 387 Firmware Upload In Process

Note: The UAG automatically reboots after a successful upload.

The UAG automatically restarts causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 388 Network Temporarily Disconnected

After five minutes, log in again and check your new firmware version in the **Dashboard** screen.

If the upload was not successful, the following message appears in the status bar at the bottom of the screen.

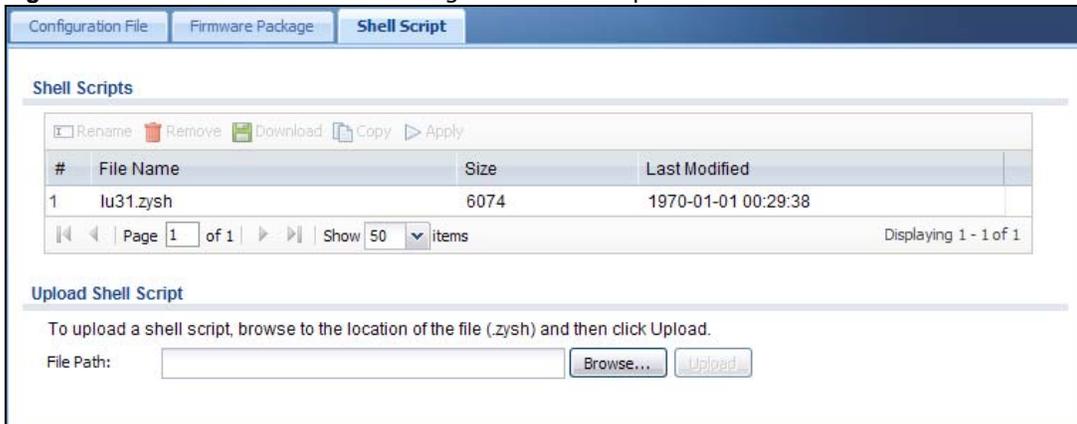
Figure 389 Firmware Upload Error

48.4 The Shell Script Screen

Use shell script files to have the UAG use commands that you specify. Use a text editor to create the shell script files. They must use a “.zysh” filename extension.

Click **Maintenance > File Manager > Shell Script** to open the **Shell Script** screen. Use the **Shell Script** screen to store, name, download, upload and run shell script files. You can store multiple shell script files on the UAG at the same time.

Note: You should include `write` commands in your scripts. If you do not use the `write` command, the changes will be lost when the UAG restarts. You could use multiple `write` commands in a long script.

Figure 390 Maintenance > File Manager > Shell Script

Each field is described in the following table.

Table 264 Maintenance > File Manager > Shell Script

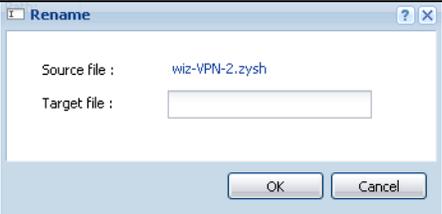
LABEL	DESCRIPTION
Rename	<p>Use this button to change the label of a shell script file on the UAG.</p> <p>You cannot rename a shell script to the name of another shell script in the UAG.</p> <p>Click a shell script's row to select it and click Rename to open the Rename File screen.</p> <p>Figure 391 Maintenance > File Manager > Shell Script > Rename</p>  <p>Specify the new name for the shell script file. Use up to 25 characters (including a-zA-Z0-9;~!@#\$\$%^&()_+[]{}',.-).</p> <p>Click OK to save the duplicate or click Cancel to close the screen without saving a duplicate of the configuration file.</p>
Remove	<p>Click a shell script file's row to select it and click Remove to delete the shell script file from the UAG.</p> <p>A pop-up window asks you to confirm that you want to delete the shell script file. Click OK to delete the shell script file or click Cancel to close the screen without deleting the shell script file.</p>
Download	<p>Click a shell script file's row to select it and click Download to save the configuration to your computer.</p>
Copy	<p>Use this button to save a duplicate of a shell script file on the UAG.</p> <p>Click a shell script file's row to select it and click Copy to open the Copy File screen.</p> <p>Figure 392 Maintenance > File Manager > Shell Script > Copy</p>  <p>Specify a name for the duplicate file. Use up to 25 characters (including a-zA-Z0-9;~!@#\$\$%^&()_+[]{}',.-).</p> <p>Click OK to save the duplicate or click Cancel to close the screen without saving a duplicate of the configuration file.</p>
Apply	<p>Use this button to have the UAG use a specific shell script file.</p> <p>Click a shell script file's row to select it and click Apply to have the UAG use that shell script file. You may need to wait awhile for the UAG to finish applying the commands.</p>
#	<p>This column displays the number for each shell script file entry.</p>
File Name	<p>This column displays the label that identifies a shell script file.</p>
Size	<p>This column displays the size (in KB) of a shell script file.</p>
Last Modified	<p>This column displays the date and time that the individual shell script files were last changed or saved.</p>

Table 264 Maintenance > File Manager > Shell Script (continued)

LABEL	DESCRIPTION
Upload Shell Script	The bottom part of the screen allows you to upload a new or previously saved shell script file from your computer to your UAG.
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click Browse... to find the .zysh file you want to upload.
Upload	Click Upload to begin the upload process. This process may take up to several minutes.

Diagnostics

49.1 Overview

Use the diagnostics screens for troubleshooting.

49.1.1 What You Can Do in this Chapter

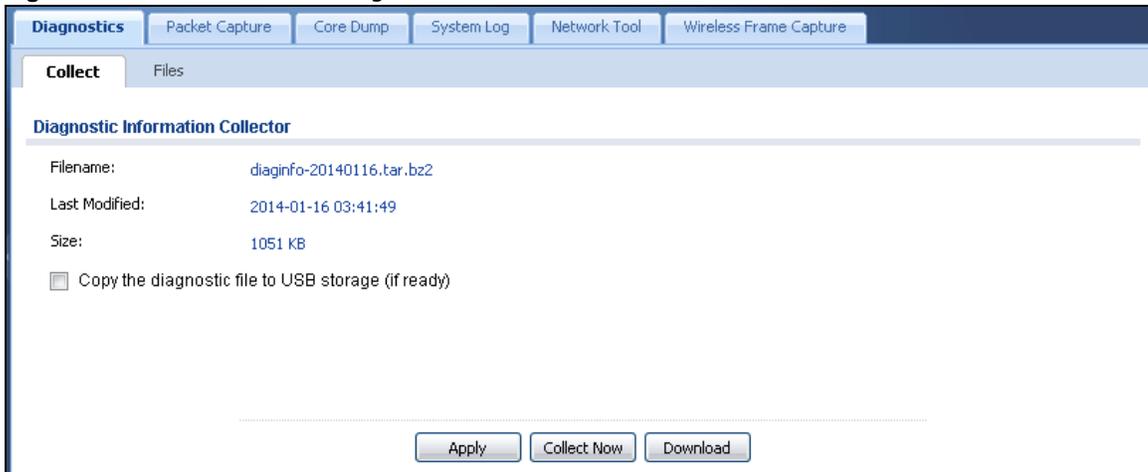
- Use the **Diagnostics** screen (see [Section 49.2 on page 560](#)) to generate a file containing the UAG's configuration and diagnostic information if you need to provide it to customer support during troubleshooting.
- Use the **Packet Capture** screens (see [Section 49.3 on page 562](#)) to capture packets going through the UAG.
- Use the **Core Dump** screens (see [Section 49.4 on page 566](#)) to have the UAG save a process's core dump to an attached USB storage device if the process terminates abnormally (crashes) so you can send the file to customer support for troubleshooting.
- Use the **System Log** screens (see [Section 49.5 on page 567](#)) to download files of system logs from a connected USB storage device to your computer.
- Use the **Network Tool** screen (see [Section 49.6 on page 568](#)) to ping an IP address or trace the route packets take to a host.
- Use the **Wireless Frame Capture** screens (see [Section 49.7 on page 569](#)) to capture network traffic going through the AP interfaces connected to your UAG.

49.2 The Diagnostics Screen

The **Diagnostic** screen provides an easy way for you to generate a file containing the UAG's configuration and diagnostic information. You may need to send this file to customer support for troubleshooting.

Click **Maintenance > Diagnostics** to open the **Diagnostic** screen.

Figure 393 Maintenance > Diagnostics



The following table describes the labels in this screen.

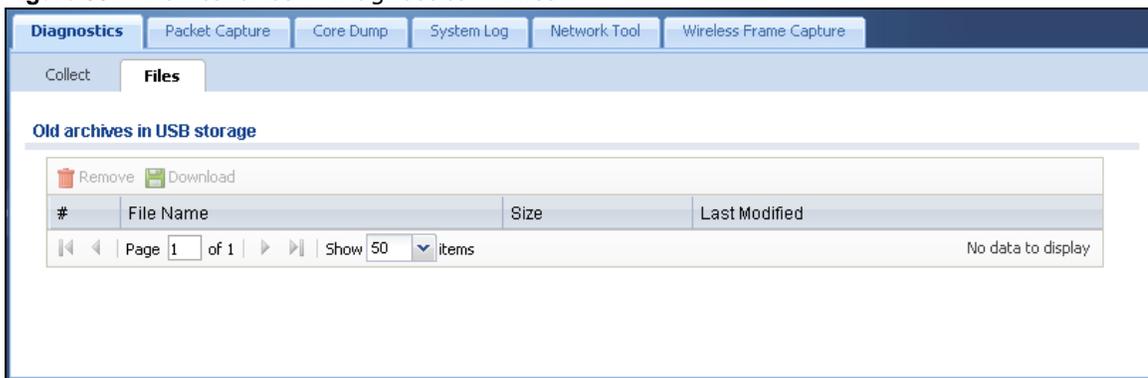
Table 265 Maintenance > Diagnostics

LABEL	DESCRIPTION
Filename	This is the name of the most recently created diagnostic file.
Last modified	This is the date and time that the last diagnostic file was created. The format is yyyy-mm-dd hh:mm:ss.
Size	This is the size of the most recently created diagnostic file.
Copy the diagnostic file to USB storage (if ready)	Select this to have the UAG create an extra copy of the diagnostic file to a connected USB storage device.
Apply	Click Apply to save your changes.
Collect Now	Click this to have the UAG create a new diagnostic file.
Download	Click this to save the most recent diagnostic file to a computer.

49.2.1 The Diagnostics Files Screen

Click **Maintenance > Diagnostics > Files** to open the diagnostic files screen. This screen lists the files of diagnostic information the UAG has collected and stored in a connected USB storage device. You may need to send these files to customer support for troubleshooting.

Figure 394 Maintenance > Diagnostics > Files



The following table describes the labels in this screen.

Table 266 Maintenance > Diagnostics > Files

LABEL	DESCRIPTION
Remove	Select files and click Remove to delete them from the UAG. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click Download to save it to your computer.
#	This column displays the number for each file entry. The total number of files that you can save depends on the file sizes and the available storage space.
File Name	This column displays the label that identifies the file.
Size	This column displays the size (in bytes) of a file.
Last Modified	This column displays the date and time that the individual files were saved.

49.3 The Packet Capture Screen

Use this screen to capture network traffic going through the UAG's interfaces. Studying these packet captures may help you identify network problems. Click **Maintenance > Diagnostics > Packet Capture** to open the packet capture screen.

Note: New capture files overwrite existing files of the same name. Change the **File Suffix** field's setting to avoid this.

Figure 395 Maintenance > Diagnostics > Packet Capture

The following table describes the labels in this screen.

Table 267 Maintenance > Diagnostics > Packet Capture

LABEL	DESCRIPTION
Interfaces	Enabled interfaces (except for virtual interfaces) appear under Available Interfaces . Select interfaces for which to capture packets and click the right arrow button to move them to the Capture Interfaces list. Use the [Shift] and/or [Ctrl] key to select multiple objects.
IP Version	Select the version of the Internet Protocol (IP) by which traffic is routed across the networks and Internet. Select any to capture packets for traffic sent by either IP version.
Protocol Type	Select the protocol type of traffic for which to capture packets. Select any to capture packets for all types of traffic.
Host IP	Select a host IP address object for which to capture packets. Select any to capture packets for all hosts. Select User Defined to be able to enter an IP address.
Host Port	This field is configurable when you set the Protocol Type to any , tcp , or udp . Specify the port number of traffic to capture.
Continuously capture and overwrite old ones	Select this to have the UAG keep capturing traffic and overwriting old packet capture entries when the available storage space runs out.

Table 267 Maintenance > Diagnostics > Packet Capture (continued)

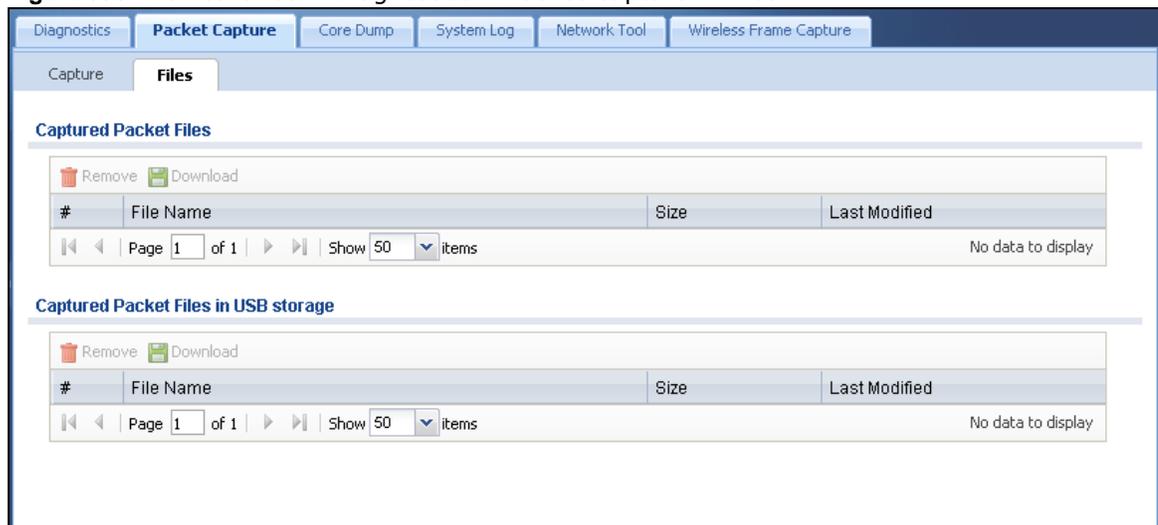
LABEL	DESCRIPTION
Save data to onboard storage only	<p>Select this to have the UAG only store packet capture entries on the UAG. The available storage size is displayed as well.</p> <p>Note: The UAG reserves some onboard storage space as a buffer.</p>
Save data to USB storage	<p>Select this to have the UAG store packet capture entries only on a USB storage device connected to the UAG.</p> <p>Status:</p> <p>Unused - the connected USB storage device was manually unmounted by using the Remove Now button or for some reason the UAG cannot mount it.</p> <p>none - no USB storage device is connected.</p> <p>available - you can have the UAG use the USB storage device. The available storage capacity also displays.</p> <p>service deactivated - the USB storage feature is disabled and the UAG cannot use a connected USB device to store the system log and other diagnostic information.</p> <p>Note: The UAG reserves some USB storage space as a buffer.</p>
Captured Packet Files	<p>When saving packet captures only to the UAG's onboard storage, specify a maximum limit in megabytes for the total combined size of all the capture files on the UAG.</p> <p>When saving packet captures to a connected USB storage device, specify a maximum limit in megabytes for each capture file.</p> <p>Note: If you have existing capture files and have not selected the Continuously capture and overwrite old ones option, you may need to set this size larger or delete existing capture files.</p> <p>The valid range depends on the available onboard/USB storage size. The UAG stops the capture and generates the capture file when either the file reaches this size or the time period specified in the Duration field expires.</p>
Split threshold	Specify a maximum size limit in megabytes for individual packet capture files. After a packet capture file reaches this size, the UAG starts another packet capture file.
Duration	Set a time limit in seconds for the capture. The UAG stops the capture and generates the capture file when either this period of time has passed or the file reaches the size specified in the File Size field. 0 means there is no time limit.
File Suffix	<p>Specify text to add to the end of the file name (before the dot and filename extension) to help you identify the packet capture files. Modifying the file suffix also avoids making new capture files that overwrite existing files of the same name.</p> <p>The file name format is "interface name-file suffix.cap", for example "vlan2-packet-capture.cap".</p>
Number Of Bytes To Capture (Per Packet)	Specify the maximum number of bytes to capture per packet. The UAG automatically truncates packets that exceed this size. As a result, when you view the packet capture files in a packet analyzer, the actual size of the packets may be larger than the size of captured packets.

Table 267 Maintenance > Diagnostics > Packet Capture (continued)

LABEL	DESCRIPTION
Capture	<p>Click this button to have the UAG capture packets according to the settings configured in this screen.</p> <p>You can configure the UAG while a packet capture is in progress although you cannot modify the packet capture settings.</p> <p>The UAG's throughput or performance may be affected while a packet capture is in progress.</p> <p>After the UAG finishes the capture it saves a separate capture file for each selected interface. The total number of packet capture files that you can save depends on the file sizes and the available flash storage space. Once the flash storage space is full, adding more packet captures will fail.</p>
Stop	Click this button to stop a currently running packet capture and generate a separate capture file for each selected interface.
Reset	Click this button to return the screen to its last-saved settings.

49.3.1 The Packet Capture Files Screen

Click **Maintenance > Diagnostics > Packet Capture > Files** to open the packet capture files screen. This screen lists the files of packet captures stored on the UAG or a connected USB storage device. You can download the files to your computer where you can study them using a packet analyzer (also known as a network or protocol analyzer) such as Wireshark.

Figure 396 Maintenance > Diagnostics > Packet Capture > Files

The following table describes the labels in this screen.

Table 268 Maintenance > Diagnostics > Packet Capture > Files

LABEL	DESCRIPTION
Remove	Select files and click Remove to delete them from the UAG or the connected USB storage device. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click Download to save it to your computer.

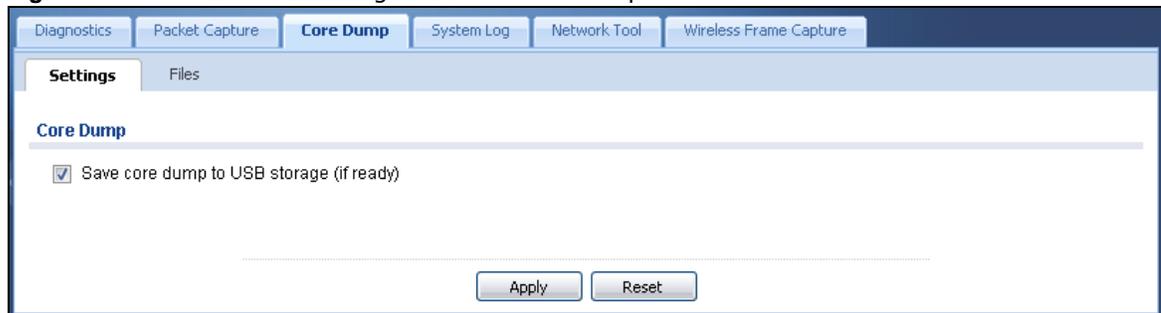
Table 268 Maintenance > Diagnostics > Packet Capture > Files (continued)

LABEL	DESCRIPTION
#	This column displays the number for each packet capture file entry. The total number of packet capture files that you can save depends on the file sizes and the available flash storage space.
File Name	This column displays the label that identifies the file. The file name format is interface name-file suffix.cap.
Size	This column displays the size (in bytes) of a configuration file.
Last Modified	This column displays the date and time that the individual files were saved.

49.4 The Core Dump Screen

Use the **Core Dump** screen to have the UAG save a process's core dump to an attached USB storage device if the process terminates abnormally (crashes). You may need to send this file to customer support for troubleshooting.

Click **Maintenance > Diagnostics > Core Dump** to open the following screen.

Figure 397 Maintenance > Diagnostics > Core Dump

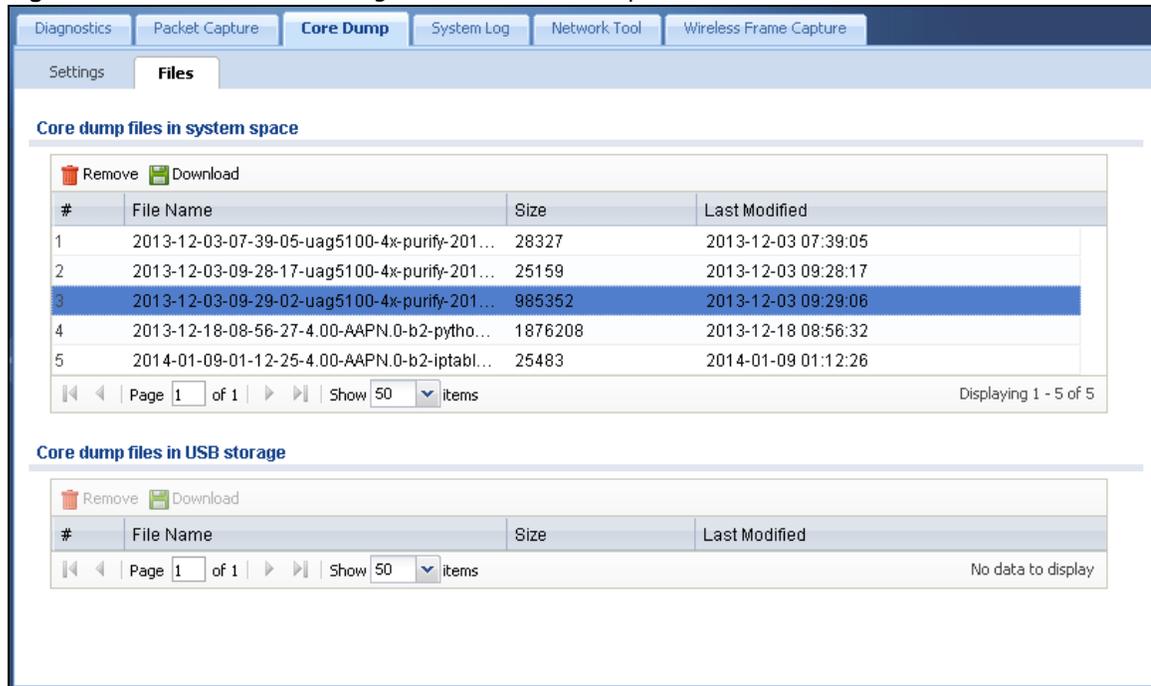
The following table describes the labels in this screen.

Table 269 Maintenance > Diagnostics > Core Dump

LABEL	DESCRIPTION
Save core dump to USB storage (if ready)	Select this to have the UAG save a process's core dump to an attached USB storage device if the process terminates abnormally (crashes). If you clear this option the UAG only saves to flash memory. Once the flash is full, the UAG stops generating the core dump file.
Apply	Click Apply to save the changes.
Reset	Click Reset to return the screen to its last-saved settings.

49.4.1 The Core Dump Files Screen

Click **Maintenance > Diagnostics > Core Dump > Files** to open the core dump files screen. This screen lists the core dump files stored on the UAG or a connected USB storage device. You may need to send these files to customer support for troubleshooting.

Figure 398 Maintenance > Diagnostics > Core Dump > Files

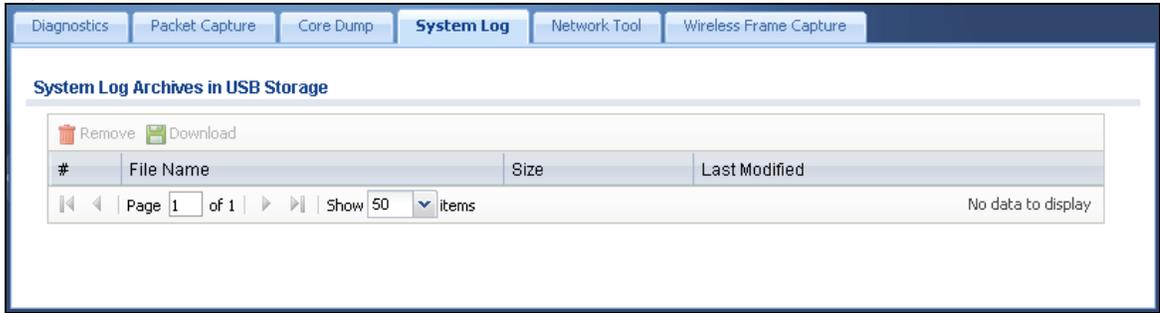
The following table describes the labels in this screen.

Table 270 Maintenance > Diagnostics > Core Dump > Files

LABEL	DESCRIPTION
Remove	Select files and click Remove to delete them from the UAG. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click Download to save it to your computer.
#	This column displays the number for each packet capture file entry. The total number of packet capture files that you can save depends on the file sizes and the available flash storage space.
File Name	This column displays the label that identifies the file.
Size	This column displays the size (in bytes) of a file.
Last Modified	This column displays the date and time that the individual files were saved.

49.5 The System Log Screen

Click **Maintenance > Diagnostics > System Log** to open the system log files screen. This screen lists the files of system logs stored on a connected USB storage device. The files are in comma separated value (csv) format. You can download them to your computer and open them in a tool like Microsoft's Excel.

Figure 399 Maintenance > Diagnostics > System Log

The following table describes the labels in this screen.

Table 271 Maintenance > Diagnostics > System Log

LABEL	DESCRIPTION
Remove	Select files and click Remove to delete them from the UAG. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click Download to save it to your computer.
#	This column displays the number for each file entry. The total number of files that you can save depends on the file sizes and the available storage space.
File Name	This column displays the label that identifies the file.
Size	This column displays the size (in bytes) of a file.
Last Modified	This column displays the date and time that the individual files were saved.

49.6 The Network Tool Screen

Use this screen to ping or traceroute an IP address.

Click **Maintenance > Diagnostics > Network Tool** to display this screen.

Figure 400 Maintenance > Diagnostics > Network Tool

Diagnosics Packet Capture Core Dump System Log **Network Tool** Wireless Frame Capture

Show Advanced Settings

Network Tool

Network Tool: PING IPv4

Domain Name or IP Address: 172.16.0.99

Test Stop Reset

```
# ping 172.16.0.99 -n -c 3
PING 172.16.0.99 (172.16.0.99) 56(84) bytes of data.
From 172.16.0.1 icmp_seq=1 Destination Host Unreachable
From 172.16.0.1 icmp_seq=2 Destination Host Unreachable
From 172.16.0.1 icmp_seq=3 Destination Host Unreachable

--- 172.16.0.99 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2006ms
, pipe 3
```

The following table describes the labels in this screen.

Table 272 Maintenance > Diagnostics > Network Tool

LABEL	DESCRIPTION
Network Tool	Select PING IPv4 to ping the IP address that you entered. Select TRACEROUTE IPv4 to perform the traceroute function. This determines the path a packet takes to the specified computer.
Domain Name or IP Address	Type the IPv4 address of a computer that you want to perform ping or traceroute in order to test a connection.
Test	Click this button to start to ping or run a traceroute.
Stop	Click this button to terminate the current ping operation or traceroute.
Reset	Click this button to return the screen to its last-saved settings.

49.7 The Wireless Frame Capture Screen

Use this screen to capture wireless network traffic going through the AP interfaces connected to your UAG. Studying these frame captures may help you identify network problems.

Click **Maintenance > Diagnostics > Wireless Frame Capture** to display this screen.

Note: New capture files overwrite existing files of the same name. Change the **File Prefix** field's setting to avoid this.

Figure 401 Maintenance > Diagnostics > Wireless Frame Capture > Capture

The following table describes the labels in this screen.

Table 273 Maintenance > Diagnostics > Wireless Frame Capture > Capture

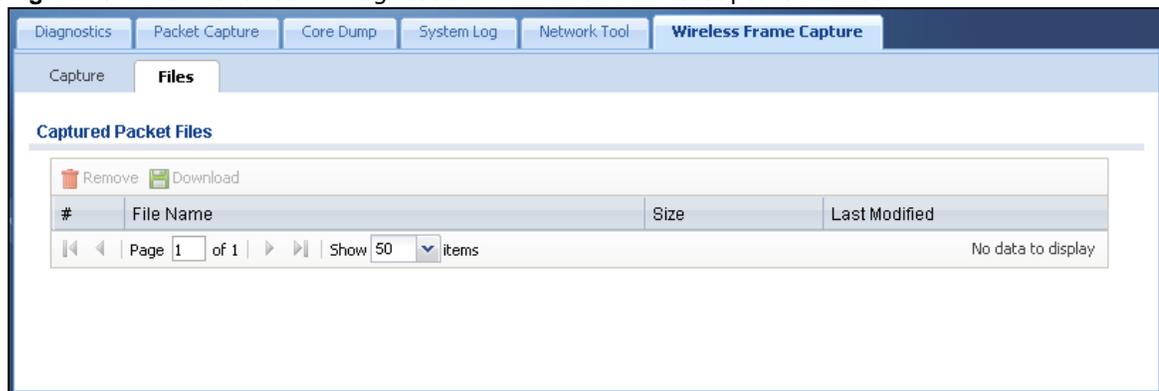
LABEL	DESCRIPTION
MON Mode APs	
Configure AP to MON Mode	Click this to go the Configuration > Wireless > AP Management screen, where you can set one or more APs to monitor mode.
Available MON Mode APs	This column displays which APs on your wireless network are currently configured for monitor mode. Use the arrow buttons to move APs off this list and onto the Captured MON Mode APs list.
Capture MON Mode APs	This column displays the monitor-mode configured APs selected for wireless frame capture.
Misc Setting	
File Size	Specify a maximum size limit in kilobytes for the total combined size of all the capture files on the UAG, including any existing capture files and any new capture files you generate. Note: If you have existing capture files you may need to set this size larger or delete existing capture files. The valid range is 1 to 50000. The UAG stops the capture and generates the capture file when either the file reaches this size.
File Prefix	Specify text to add to the front of the file name in order to help you identify frame capture files. You can modify the prefix to also create new frame capture files each time you perform a frame capture operation. Doing this does no overwrite existing frame capture files. The file format is: [file prefix].cap. For example, "monitor.cap".

Table 273 Maintenance > Diagnostics > Wireless Frame Capture > Capture (continued)

LABEL	DESCRIPTION
Capture	<p>Click this button to have the UAG capture frames according to the settings configured in this screen.</p> <p>You can configure the UAG while a frame capture is in progress although you cannot modify the frame capture settings.</p> <p>The UAG's throughput or performance may be affected while a frame capture is in progress.</p> <p>After the UAG finishes the capture it saves a combined capture file for all APs. The total number of frame capture files that you can save depends on the file sizes and the available flash storage space. Once the flash storage space is full, adding more frame captures will fail.</p>
Stop	Click this button to stop a currently running frame capture and generate a combined capture file for all APs.
Reset	Click this button to return the screen to its last-saved settings.

49.7.1 The Wireless Frame Capture Files Screen

Click **Maintenance > Diagnostics > Wireless Frame Capture > Files** to open this screen. This screen lists the files of wireless frame captures the UAG has performed. You can download the files to your computer where you can study them using a packet analyzer (also known as a network or protocol analyzer) such as Wireshark.

Figure 402 Maintenance > Diagnostics > Wireless Frame Capture > Files

The following table describes the labels in this screen.

Table 274 Maintenance > Diagnostics > Wireless Frame Capture > Files

LABEL	DESCRIPTION
Remove	Select files and click Remove to delete them from the UAG. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click Download to save it to your computer.
#	This column displays the number for each packet capture file entry. The total number of packet capture files that you can save depends on the file sizes and the available flash storage space.
File Name	This column displays the label that identifies the file. The file name format is interface name-file suffix.cap.
Size	This column displays the size (in bytes) of a configuration file.
Last Modified	This column displays the date and time that the individual files were saved.

Packet Flow Explore

50.1 Overview

Use this to get a clear picture on how the UAG determines where to forward a packet and how to change the source IP address of the packet according to your current settings. This function provides you a summary of all your routing and SNAT settings and helps troubleshoot any related problems.

50.1.1 What You Can Do in this Chapter

- Use the **Routing Status** screen (see [Section 50.2 on page 572](#)) to view the overall routing flow and each routing function's settings.
- Use the **SNAT Status** screen (see [Section 50.3 on page 578](#)) to view the overall source IP address conversion (SNAT) flow and each SNAT function's settings.

50.2 The Routing Status Screen

The **Routing Status** screen allows you to view the current routing flow and quickly link to specific routing settings. Click a function box in the **Routing Flow** section, the related routes (activated) will display in the **Routing Table** section. To access this screen, click **Maintenance > Packet Flow Explore**.

The order of the routing flow may vary depending on whether you:

- select **use policy route to override direct route** in the **CONFIGURATION > Network > Routing > Policy Route** screen.
- use policy routes to control 1-1 NAT by using the `policy control-virtual-server-rules activate` command.
- select **use policy routes to control dynamic IPSec rules** in the **CONFIGURATION > VPN > IPSec VPN > VPN Connection** screen.

Note: Once a packet matches the criteria of a routing rule, the UAG takes the corresponding action and does not perform any further flow checking.

Figure 403 Maintenance > Packet Flow Explore > Routing Status (Direct Route)

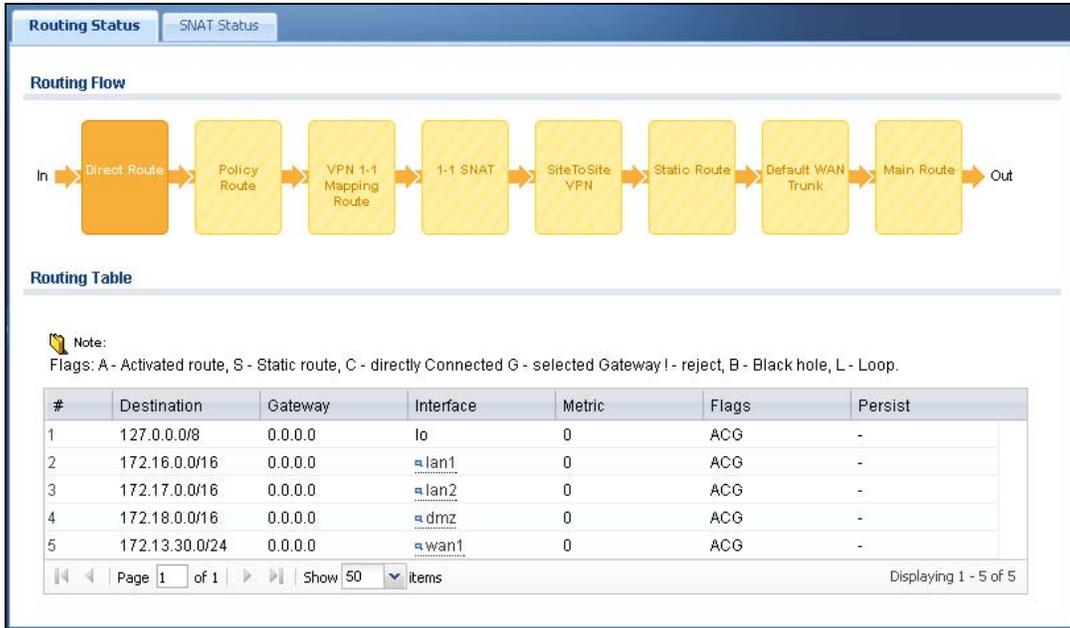


Figure 404 Maintenance > Packet Flow Explore > Routing Status (Policy Route)

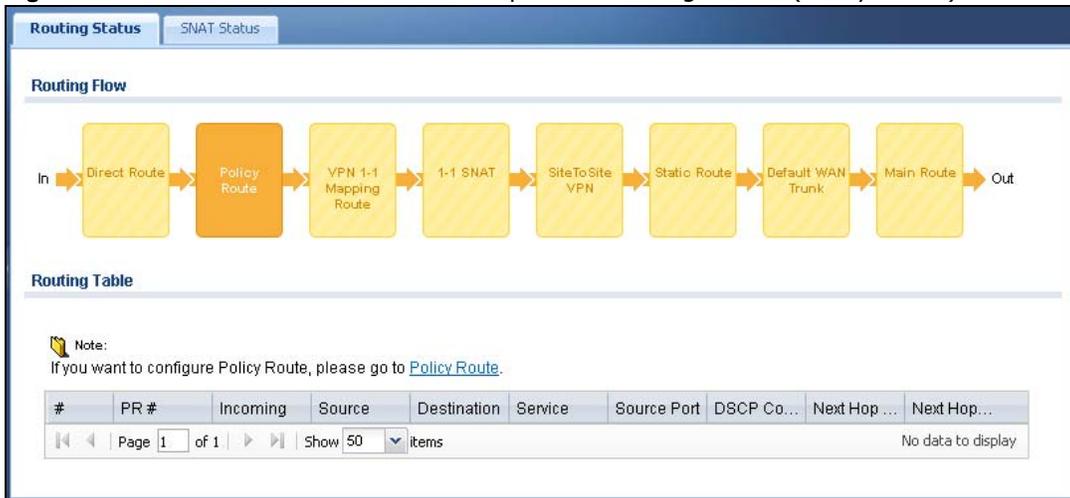


Figure 405 Maintenance > Packet Flow Explore > Routing Status (VPN 1-1 Mapping Route)

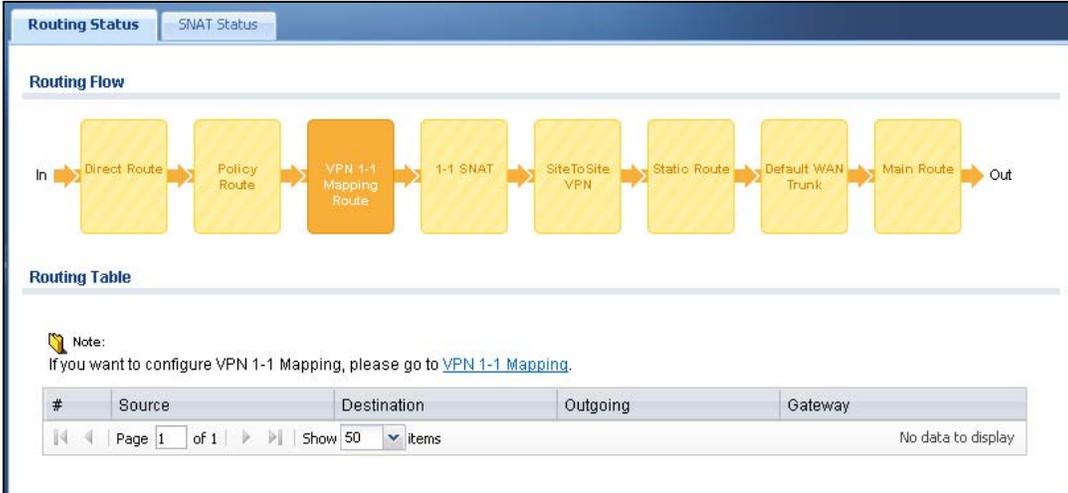


Figure 406 Maintenance > Packet Flow Explore > Routing Status (1-1 SNAT)

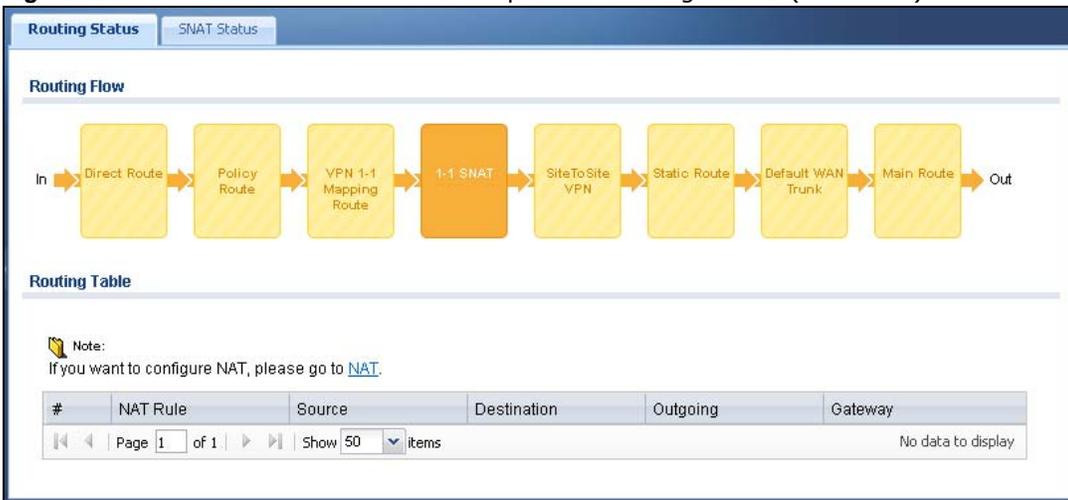


Figure 407 Maintenance > Packet Flow Explore > Routing Status (SiteToSite VPN)

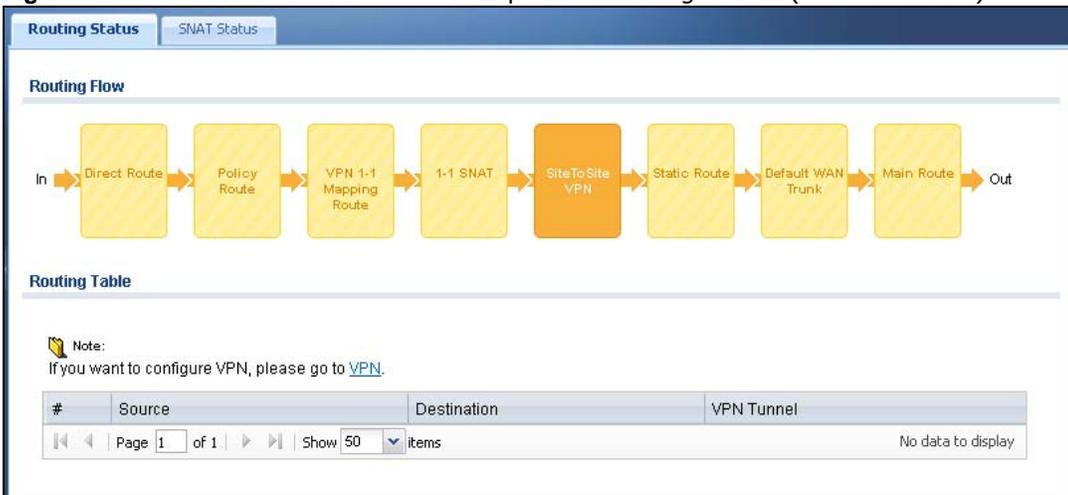


Figure 408 Maintenance > Packet Flow Explore > Routing Status (Static Route)

The screenshot shows the 'Routing Status' page for a 'Static Route'. The 'Routing Flow' diagram consists of a sequence of steps: In → Direct Route → Policy Route → VPN 1-1 Mapping Route → 1-1 SNAT → SiteToSite VPN → **Static Route** → Default WAN Trunk → Main Route → Out. The 'Static Route' step is highlighted in orange. Below the diagram is a 'Routing Table' section with a note: 'Note: If you want to configure Static Route, please go to [Static Route](#). Flags: A - Activated route, S - Static route, C - directly Connected G - selected Gateway ! - reject, B - Black hole, L - Loop.' The table below has columns for #, Destination, Gateway, Interface, Metric, Flags, and Persist, but it is currently empty, displaying 'No data to display'.

Figure 409 Maintenance > Packet Flow Explore > Routing Status (Default WAN Trunk)

The screenshot shows the 'Routing Status' page for a 'Default WAN Trunk'. The 'Routing Flow' diagram is identical to Figure 408, but the 'Default WAN Trunk' step is highlighted in orange. Below the diagram is a 'Routing Table' section with a note: 'Note: If you want to configure Default WAN Trunk, please go to [Trunk](#).' The table below has columns for #, Source, Destination, and Trunk. It contains one entry: # 1, Source any, Destination any, Trunk SYSTEM_DEFAULT_WAN_TRUNK. The table footer indicates 'Displaying 1 - 1 of 1'.

#	Source	Destination	Trunk
1	any	any	SYSTEM_DEFAULT_WAN_TRUNK

Figure 410 Maintenance > Packet Flow Explore > Routing Status (Main Route)

The screenshot displays the 'Routing Status' page for the 'Main Route'. It features two main sections: 'Routing Flow' and 'Routing Table'.

Routing Flow: A sequence of steps from 'In' to 'Out': Direct Route → Policy Route → VPN 1-1 Mapping Route → 1-1 SNAT → SiteToSite VPN → Static Route → Default WAN Trunk → Main Route → Out.

Routing Table: A table with 7 columns: #, Destination, Gateway, Interface, Metric, Flags, and Persist. It lists 6 routes. A note explains the flags: A - Activated route, S - Static route, C - directly Connected, G - selected Gateway, ! - reject, B - Black hole, L - Loop.

#	Destination	Gateway	Interface	Metric	Flags	Persist
1	0.0.0.0/0	172.13.30.254	wan1	0	ASG	-
2	127.0.0.0/8	0.0.0.0	lo	0	ACG	-
3	172.16.0.0/16	0.0.0.0	lan1	0	ACG	-
4	172.17.0.0/16	0.0.0.0	lan2	0	ACG	-
5	172.18.0.0/16	0.0.0.0	dmz	0	ACG	-
6	172.13.30.0/24	0.0.0.0	wan1	0	ACG	-

Page 1 of 1 | Show 50 items | Displaying 1 - 6 of 6

The following table describes the labels in this screen.

Table 275 Maintenance > Packet Flow Explore > Routing Status

LABEL	DESCRIPTION
Routing Flow	This section shows you the flow of how the UAG determines where to route a packet. Click a function box to display the related settings in the Routing Table section.
Routing Table	This section shows the corresponding settings according to the function box you click in the Routing Flow section.
The following fields are available if you click Direct Route , Static Route , or Main Route in the Routing Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
Destination	This is the destination IP address of a route.
Gateway	This is the IP address of the next-hop gateway or the interface through which the traffic is routed.
Interface	This is the name of an interface associated with the route.
Metric	This is the route's priority among the displayed routes.
Flags	This indicates additional information for the route. The possible flags are: <ul style="list-style-type: none"> • A - this route is currently activated. • S - this is a static route. • C - this is a direct connected route. • G - the route is to a gateway (router) in the same network. • ! - this is a route which forces a route lookup to fail. • B - this is a route which discards packets. • L - this is a recursive route.
Persist	This is the remaining time of a dynamically learned route. The UAG removes the route after this time period is counted down to zero.
The following fields are available if you click SiteToSite VPN in the Routing Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
Source	This is the IP address(es) of the local VPN network.

Table 275 Maintenance > Packet Flow Explore > Routing Status (continued)

LABEL	DESCRIPTION
Destination	This is the IP address(es) for the remote VPN network.
VPN Tunnel	This is the name of the VPN tunnel.
The following fields are available if you click Policy Route in the Routing Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
PR #	This is the number of an activated policy route. If you have configured a schedule for the route, this screen only displays the route at the scheduled time.
Incoming	This is the interface on which the packets are received.
Source	This is the source IP address(es) from which the packets are sent.
Destination	This is the destination IP address(es) to which the packets are transmitted.
Service	This is the name of the service object. any means all services.
Source Port	This is the name of a service object. The UAG applies the policy route to the packets sent from the corresponding service port. any means all service ports.
DSCP Code	This is the DSCP value of incoming packets to which this policy route applies. See Section 12.2 on page 205 for more information.
Next Hop Type	This is the type of the next hop to which packets are directed.
Next Hop Info	<ul style="list-style-type: none"> This is the main route if the next hop type is Auto. This is the interface name and gateway IP address if the next hop type is Interface / GW. This is the trunk name if the next hop type is Trunk.
The following fields are available if you click VPN 1-1 Mapping Route in the Routing Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
Source	This is the original source IP address(es). any means any IP address.
Destination	This is the original destination IP address(es). any means any IP address.
Outgoing	This is the name of an interface which transmits packets out of the UAG.
Gateway	This is the IP address of the gateway in the same network of the outgoing interface.
The following fields are available if you click 1-1 SNAT in the Routing Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
NAT Rule	This is the name of an activated 1:1 or Many 1:1 NAT rule in the NAT table.
Source	This is the original source IP address(es). any means any IP address.
Destination	This is the original destination IP address(es). any means any IP address.
Outgoing	This is the name of an interface which transmits packets out of the UAG.
Gateway	This is the IP address of the gateway in the same network of the outgoing interface.
The following fields are available if you click Default WAN Trunk in the Routing Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
Source	This is the source IP address(es) from which the packets are sent. any means any IP address.
Destination	This is the destination IP address(es) to which the packets are transmitted. any means any IP address.
Trunk	This is the name of the WAN trunk through which the matched packets are transmitted.

50.3 The SNAT Status Screen

The **SNAT Status** screen allows you to view and quickly link to specific source NAT (SNAT) settings. Click a function box in the **SNAT Flow** section, the related SNAT rules (activated) will display in the **SNAT Table** section. To access this screen, click **Maintenance > Packet Flow Explore > SNAT Status**.

The order of the SNAT flow may vary depending on whether you:

- select **use default SNAT** in the **Configuration > Network > Interface > Trunk** screen.
- use policy routes to control 1-1 NAT by using the `policy control-virtual-server-rules activate` command.

Note: Once a packet matches the criteria of an SNAT rule, the UAG takes the corresponding action and does not perform any further flow checking.

Figure 411 Maintenance > Packet Flow Explore > SNAT Status (Policy Route SNAT)

The screenshot shows the SNAT Status screen for Policy Route SNAT. The interface includes a 'Routing Status' tab and a 'SNAT Status' sub-tab. The 'SNAT Flow' section displays a sequence of five steps: 'In', 'Policy Route SNAT', 'VPN 1-1 Mapping SNAT', '1-1 SNAT', 'Loopback SNAT', 'Default SNAT', and 'Out'. The 'SNAT Table' section is empty, with a note: 'Note: If you want to configure Policy Route SNAT, please go to [Policy Route](#).' The table has columns for '#', 'PR #', 'Outgoing', and 'SNAT'. The page shows 'Page 1 of 1' and 'Show 50 items'.

Figure 412 Maintenance > Packet Flow Explore > SNAT Status (VPN 1-1 Mapping Route)

The screenshot shows the SNAT Status screen for VPN 1-1 Mapping Route. The interface includes a 'Routing Status' tab and a 'SNAT Status' sub-tab. The 'SNAT Flow' section displays a sequence of five steps: 'In', 'Policy Route SNAT', 'VPN 1-1 Mapping SNAT', '1-1 SNAT', 'Loopback SNAT', 'Default SNAT', and 'Out'. The 'SNAT Table' section is empty, with a note: 'Note: If you want to configure VPN 1-1 Mapping SNAT, please go to [VPN 1-1 Mapping](#).' The table has columns for '#', 'Source', 'Destination', 'Outgoing', and 'SNAT'. The page shows 'Page 1 of 1' and 'Show 50 items'.

Figure 413 Maintenance > Packet Flow Explore > SNAT Status (1-1 SNAT)

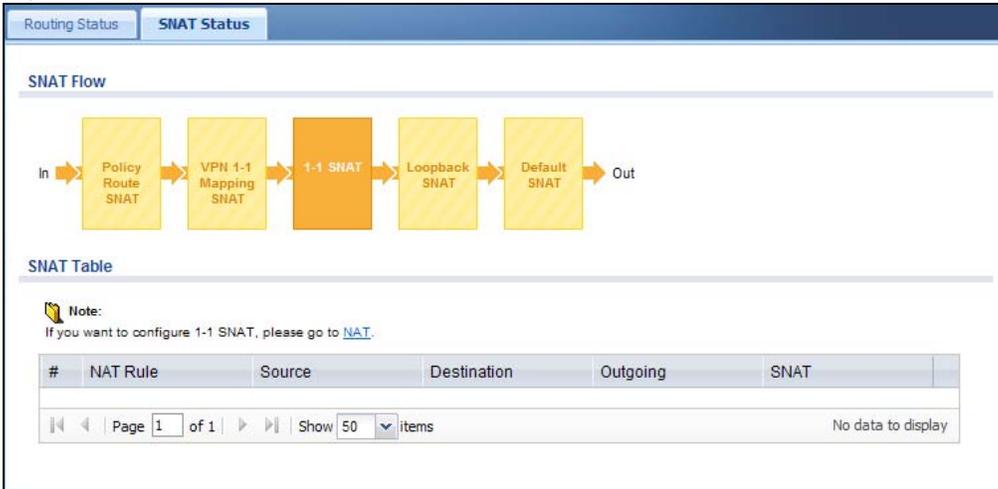


Figure 414 Maintenance > Packet Flow Explore > SNAT Status (Loopback SNAT)

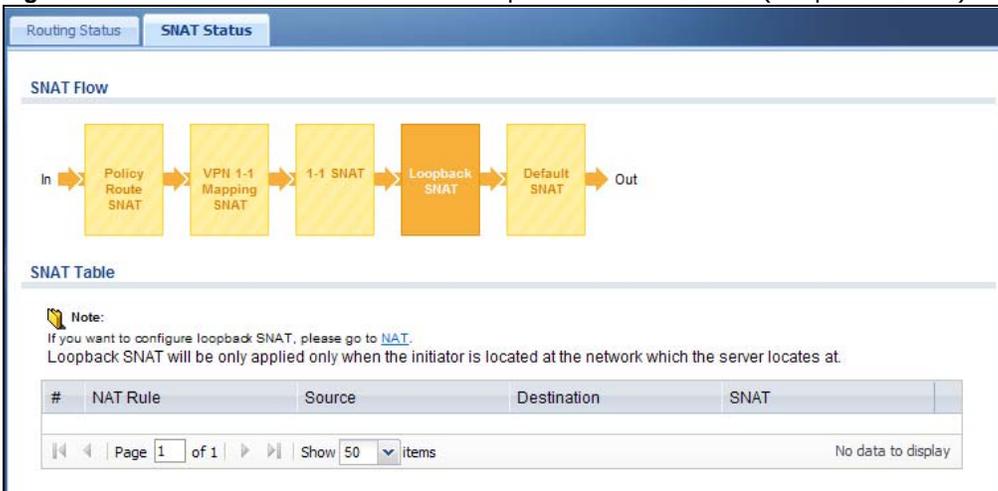
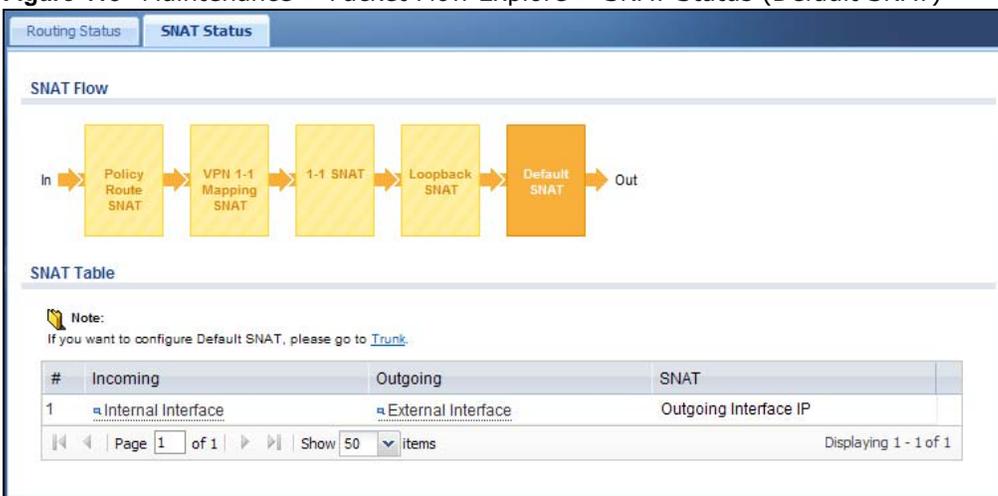


Figure 415 Maintenance > Packet Flow Explore > SNAT Status (Default SNAT)



The following table describes the labels in this screen.

Table 276 Maintenance > Packet Flow Explore > SNAT Status

LABEL	DESCRIPTION
SNAT Flow	This section shows you the flow of how the UAG changes the source IP address for a packet according to the rules you have configured in the UAG. Click a function box to display the related settings in the SNAT Table section.
SNAT Table	The table fields in this section vary depending on the function box you select in the SNAT Flow section.
The following fields are available if you click Policy Route SNAT in the SNAT Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
PR #	This is the number of an activated policy route which uses SNAT.
Outgoing	This is the outgoing interface that the route uses to transmit packets.
SNAT	This is the source IP address(es) that the SNAT rule uses finally.
The following fields are available if you click VPN 1-1 Mapping SNAT in the SNAT Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
Source	This is the original source IP address(es).
Destination	This is the original destination IP address(es).
Outgoing	This is the outgoing interface that the SNAT rule uses to transmit packets.
SNAT	This is the source IP address(es) that the SNAT rule uses finally.
The following fields are available if you click 1-1 SNAT in the SNAT Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
NAT Rule	This is the name of an activated NAT rule which uses SNAT.
Source	This is the original source IP address(es).
Destination	This is the original destination IP address(es).
Outgoing	This is the outgoing interface that the SNAT rule uses to transmit packets.
SNAT	This is the source IP address(es) that the SNAT rule uses finally.
The following fields are available if you click Loopback SNAT in the SNAT Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
NAT Rule	This is the name of an activated NAT rule which uses SNAT and enables NAT loopback.
Source	This is the original source IP address(es). any means any IP address.
Destination	This is the original destination IP address(es). any means any IP address.
SNAT	This indicates which source IP address the SNAT rule uses finally. For example, Outgoing Interface IP means that the UAG uses the IP address of the outgoing interface as the source IP address for the matched packets it sends out through this rule.
The following fields are available if you click Default SNAT in the SNAT Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
Incoming	This indicates internal interface(s) on which the packets are received.
Outgoing	This indicates external interface(s) from which the packets are transmitted.
SNAT	This indicates which source IP address the SNAT rule uses finally. For example, Outgoing Interface IP means that the UAG uses the IP address of the outgoing interface as the source IP address for the matched packets it sends out through this rule.

51.1 Overview

Use this to restart the device (for example, if the device begins behaving erratically). See also [Section 1.5 on page 35](#) for information on different ways to start and stop the UAG.

51.1.1 What You Need To Know

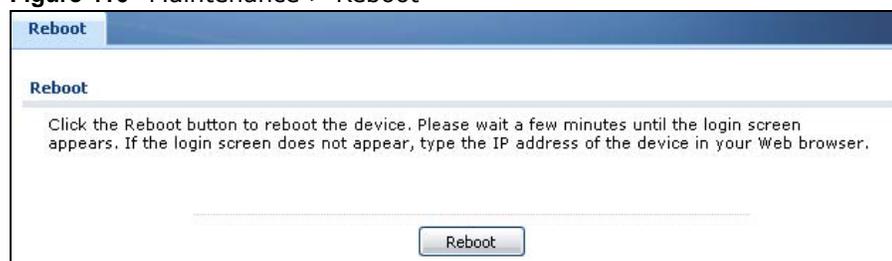
If you applied changes in the Web configurator, these were saved automatically and do not change when you reboot. If you made changes in the CLI, however, you have to use the `write` command to save the configuration before you reboot. Otherwise, the changes are lost when you reboot.

Reboot is different to reset; (see [Section 53.1 on page 589](#)) reset returns the device to its default configuration.

51.2 The Reboot Screen

The **Reboot** screen allows remote users to restart the device. To access this screen, click **Maintenance > Reboot**.

Figure 416 Maintenance > Reboot



Click the **Reboot** button to restart the UAG. Wait a few minutes until the login screen appears. If the login screen does not appear, type the IP address of the device in your Web browser.

You can also use the CLI command `reboot` to restart the UAG.

Shutdown

52.1 Overview

Use this to shutdown the device in preparation for disconnecting the power. See also [Section 1.5 on page 35](#) for information on different ways to start and stop the UAG.

Always use the Maintenance > Shutdown > Shutdown screen or the “shutdown” command before you turn off the UAG or remove the power. Not doing so can cause the firmware to become corrupt.

52.1.1 What You Need To Know

Shutdown writes all cached data to the local storage and stops the system processes.

52.2 The Shutdown Screen

To access this screen, click **Maintenance > Shutdown**.

Figure 417 Maintenance > Shutdown



Click the **Shutdown** button to shut down the UAG. Wait for the device to shut down before you manually turn off or remove the power. It does not turn off the power.

You can also use the CLI command `shutdown` to shutdown the UAG.

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter.

- You can also refer to the logs (see [Chapter 7 on page 125](#)).
- For the order in which the UAG applies its features and checks, see [Chapter 50 on page 572](#).

None of the LEDs turn on.

Make sure that you have the power cord connected to the UAG and plugged in to an appropriate power source. Make sure you have the UAG turned on. Check all cable connections.

If the LEDs still do not turn on, you may have a hardware problem. In this case, you should contact your local vendor.

Cannot access the UAG from the LAN.

- Check the cable connection between the UAG and your computer or switch.
- Ping the UAG from a LAN computer. Make sure your computer's Ethernet card is installed and functioning properly. Also make sure that its IP address is in the same subnet as the UAG's.
- In the computer, click **Start, (All) Programs, Accessories** and then **Command Prompt**. In the **Command Prompt** window, type "ping" followed by the UAG's LAN IP address (172.16.0.1 or 172.17.0.1 is the default) and then press [ENTER]. The UAG should reply.
- If you've forgotten the UAG's password, use the **RESET** button. Press the button in for about 5 seconds (or until the **PWR** LED starts to blink), then release it. It returns the UAG to the factory defaults (password is 1234, LAN IP address 172.16.0.1 or 172.17.0.1 etc.; see your User's Guide for details).
- If you've forgotten the UAG's IP address, you can use the commands through the console port to check it. Connect your computer to the **CONSOLE** port using a console cable. Your computer should have a terminal emulation communications program (such as HyperTerminal) set to VT100 terminal emulation, no parity, 8 data bits, 1 stop bit, no flow control and 115200 bps port speed.

I cannot access the Internet.

- Check the UAG's connection to the Ethernet jack with Internet access. Make sure the Internet gateway device (such as a DSL modem) is working properly.

- Check the WAN interface's status in the **Dashboard**. Use the installation setup wizard again and make sure that you enter the correct settings. Use the same case as provided by your ISP.

I configured security settings but the UAG is not applying them for certain interfaces.

Many security settings are usually applied to zones. Make sure you assign the interfaces to the appropriate zones. When you create an interface, there is no security applied on it until you assign it to a zone.

The UAG is not applying the custom policy route I configured.

The UAG checks the policy routes in the order that they are listed. So make sure that your custom policy route comes before any other routes that the traffic would also match.

The UAG is not applying the custom security policy I configured.

The UAG checks the security policies in the order that they are listed. So make sure that your custom security policy comes before any other rules that the traffic would also match.

I cannot enter the interface name I want.

- The format of interface names other than the Ethernet interface names is very strict. Each name consists of 2-4 letters (interface type), followed by a number (x, limited by the maximum number of each type of interface). For example, VLAN interfaces are vlan0, vlan1, vlan2, ...; and so on.
- The names of virtual interfaces are derived from the interfaces on which they are created. For example, virtual interfaces created on Ethernet interface wan1 are called wan1:1, wan1:2, and so on. Virtual interfaces created on VLAN interface vlan2 are called vlan2:1, vlan2:2, and so on. You cannot specify the number after the colon(:) in the Web Configurator; it is a sequential number. You can specify the number after the colon if you use the CLI to set up a virtual interface.

I cannot set up a PPP interface, virtual Ethernet interface or virtual VLAN interface on an Ethernet interface.

You cannot set up a PPP interface, virtual Ethernet interface or virtual VLAN interface if the underlying interface is a member of a bridge. You also cannot add an Ethernet interface or VLAN interface to a bridge if the member interface has a virtual interface or PPP interface on top of it.

My rules and settings that apply to a particular interface no longer work.

The interface's IP address may have changed. To avoid this create an IP address object based on the interface. This way the UAG automatically updates every rule or setting that uses the object whenever the interface's IP address settings change. For example, if you change LAN1's IP address, the UAG automatically updates the corresponding interface-based, LAN1 subnet address object.

I cannot set up a PPP interface.

You have to set up an ISP account before you create a PPPoE or PPTP interface.

I cannot configure a particular VLAN interface on top of an Ethernet interface even though I have it configured it on top of another Ethernet interface.

Each VLAN interface is created on top of only one Ethernet interface.

The UAG is not applying an interface's configured ingress bandwidth limit.

At the time of writing, the UAG does not support ingress bandwidth management.

The UAG routes and applies SNAT for traffic from some interfaces but not from others.

The UAG automatically uses SNAT for traffic it routes from internal interfaces to external interfaces. For example LAN to WAN traffic. You must manually configure a policy route to add routing and SNAT settings for an interface with the **Interface Type** set to **General**. You can also configure a policy route to override the default routing and SNAT behavior for an interface with the **Interface Type** set to **Internal** or **External**.

I cannot get Dynamic DNS to work.

- You must have a public WAN IP address to use Dynamic DNS.
- Make sure you recorded your DDNS account's user name, password, and domain name and have entered them properly in the UAG.
- You may need to configure the DDNS entry's IP Address setting to **Auto** if the interface has a dynamic IP address or there are one or more NAT routers between the UAG and the DDNS server.

- The UAG may not determine the proper IP address if there is an HTTP proxy server between the UAG and the DDNS server.

I cannot create a second HTTP redirect rule for an incoming interface.

You can configure up to one HTTP redirect rule for each (incoming) interface.

The UAG keeps resetting the connection.

If an alternate gateway on the LAN has an IP address in the same subnet as the UAG's LAN IP address, return traffic may not go through the UAG. This is called an asymmetrical or "triangle" route. This causes the UAG to reset the connection, as the connection has not been acknowledged.

You can set the UAG's security policies to permit the use of asymmetrical route topology on the network (so it does not reset the connection) although this is not recommended since allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the UAG. A better solution is to use virtual interfaces to put the UAG and the backup gateway on separate subnets. See [Asymmetrical Routes on page 291](#) and the chapter about interfaces for more information.

I changed the LAN IP address and can no longer access the Internet.

The UAG automatically updates address objects based on an interface's IP address, subnet, or gateway if the interface's IP address settings change. However, you need to manually edit any address objects for your LAN that are not based on the interface.

I cannot get the RADIUS server to authenticate the UAG's default admin account.

The default **admin** account is always authenticated locally, regardless of the authentication method setting. (See [Chapter 42 on page 459](#) for more information about authentication methods.)

The UAG fails to authentication the ext-user user accounts I configured.

An external server such as RADIUS must authenticate the ext-user accounts. If the UAG tries to use the local database to authenticate an **ext-user**, the authentication attempt will always fail. (This is related to AAA servers and authentication methods, which are discussed in [Chapter 42 on page 459](#) and [Chapter 43 on page 464](#), respectively.)

I cannot add the admin users to a user group with access users.

You cannot put access users and admin users in the same user group.

I cannot add the default admin account to a user group.

You cannot put the default **admin** account into any user group.

The schedule I configured is not being applied at the configured times.

Make sure the UAG's current date and time are correct.

I cannot get a certificate to import into the UAG.

- 1 For **My Certificates**, you can import a certificate that matches a corresponding certification request that was generated by the UAG. You can also import a certificate in PKCS#12 format, including the certificate's public and private keys.
- 2 You must remove any spaces from the certificate's filename before you can import the certificate.
- 3 Any certificate that you want to import has to be in one of these file formats:
 - Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
 - PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
 - Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The UAG currently allows the importation of a PKCS#7 file that contains a single certificate.
 - PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.
 - Binary PKCS#12: This is a format for transferring public key and private key certificates. The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the UAG.

Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

I cannot access the UAG from a computer connected to the Internet.

Check the service control rules and to-UAG security policies.

I uploaded a logo to display on the upper left corner of the Web Configurator login screen and access page but it does not display properly.

Make sure the logo file is a GIF, JPG, or PNG of 100 kilobytes or less.

I uploaded a logo to use as the screen or window background but it does not display properly.

Make sure the logo file is a GIF, JPG, or PNG of 100 kilobytes or less.

The UAG's traffic throughput rate decreased after I started collecting traffic statistics.

Data collection may decrease the UAG's traffic throughput rate.

I can only see newer logs. Older logs are missing.

When a log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

The commands in my configuration file or shell script are not working properly.

- In a configuration file or shell script, use “#” or “!” as the first character of a command line to have the UAG treat the line as a comment.
- Your configuration files or shell scripts can use “exit” or a command line consisting of a single “!” to have the UAG exit sub command mode.
- Include `write` commands in your scripts. Otherwise the changes will be lost when the UAG restarts. You could use multiple `write` commands in a long script.

Note: “exit” or “!” must follow sub commands if it is to make the UAG exit sub command mode.

See [Chapter 48 on page 549](#) for more on configuration files and shell scripts.

I cannot get the firmware uploaded using the commands.

The Web Configurator is the recommended method for uploading firmware. You only need to use the command line interface if you need to recover the firmware. See the CLI Reference Guide for how to determine if you need to recover the firmware and how to recover it.

My packet capture captured less than I wanted or failed.

The packet capture screen's **File Size** sets a maximum size limit for the total combined size of all the capture files on the UAG, including any existing capture files and any new capture files you generate. If you have existing capture files you may need to set this size larger or delete existing capture files.

The UAG stops the capture and generates the capture file when either the capture files reach the **File Size** or the time period specified in the **Duration** field expires.

My earlier packet capture files are missing.

New capture files overwrite existing files of the same name. Change the **File Suffix** field's setting to avoid this.

53.1 Resetting the UAG

If you cannot access the UAG by any method, try restarting it by turning the power off and then on again. If you still cannot access the UAG by any method or you forget the administrator password(s), you can reset the UAG to its factory-default settings. Any configuration files or shell scripts that you saved on the UAG should still be available afterwards.

Use the following procedure to reset the UAG to its factory-default settings. This overwrites the settings in the startup-config.conf file with the settings in the system-default.conf file.

Note: This procedure removes the current configuration.

If you want to reboot the device without changing the current configuration, see [Chapter 51 on page 581](#).

- 1 Make sure the **SYS** LED is on and not blinking.
- 2 Press the **RESET** button and hold it until the **SYS** LED begins to blink. (This usually takes about five seconds.)
- 3 Release the **RESET** button, and wait for the UAG to restart.

You should be able to access the UAG using the default settings.

53.2 Getting More Troubleshooting Help

Search for support information for your model at www.zyxel.com for more troubleshooting suggestions.

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. Regional websites are listed below.

See also http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml

Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- ZyXEL Communications Corporation
- <http://www.zyxel.com>

Asia

China

- ZyXEL Communications (Shanghai) Corp.
- ZyXEL Communications (Beijing) Corp.
- ZyXEL Communications (Tianjin) Corp.
- <http://www.zyxel.cn>

India

- ZyXEL Technology India Pvt Ltd
- <http://www.zyxel.in>

Kazakhstan

- ZyXEL Kazakhstan
- <http://www.zyxel.kz>

Korea

- ZyXEL Korea Corp.
- <http://www.zyxel.kr>

Malaysia

- ZyXEL Malaysia Sdn Bhd.
- <http://www.zyxel.com.my>

Pakistan

- ZyXEL Pakistan (Pvt.) Ltd.
- <http://www.zyxel.com.pk>

Philippines

- ZyXEL Philippines
- <http://www.zyxel.com.ph>

Singapore

- ZyXEL Singapore Pte Ltd.
- <http://www.zyxel.com.sg>

Taiwan

- ZyXEL Communications Corporation
- <http://www.zyxel.com>

Thailand

- ZyXEL Thailand Co., Ltd
- <http://www.zyxel.co.th>

Vietnam

- ZyXEL Communications Corporation-Vietnam Office
- <http://www.zyxel.com/vn/vi>

Europe

Austria

- ZyXEL Deutschland GmbH
- <http://www.zyxel.de>

Belarus

- ZyXEL BY
- <http://www.zyxel.by>

Belgium

- ZyXEL Communications B.V.
- <http://www.zyxel.com/be/nl/>

Bulgaria

- ZyXEL България
- <http://www.zyxel.com/bg/bg/>

Czech

- ZyXEL Communications Czech s.r.o
- <http://www.zyxel.cz>

Denmark

- ZyXEL Communications A/S
- <http://www.zyxel.dk>

Estonia

- ZyXEL Estonia
- <http://www.zyxel.com/ee/et/>

Finland

- ZyXEL Communications
- <http://www.zyxel.fi>

France

- ZyXEL France
- <http://www.zyxel.fr>

Germany

- ZyXEL Deutschland GmbH
- <http://www.zyxel.de>

Hungary

- ZyXEL Hungary & SEE
- <http://www.zyxel.hu>

Latvia

- ZyXEL Latvia

- <http://www.zyxel.com/lv/lv/homepage.shtml>

Lithuania

- ZyXEL Lithuania
- <http://www.zyxel.com/lt/lt/homepage.shtml>

Netherlands

- ZyXEL Benelux
- <http://www.zyxel.nl>

Norway

- ZyXEL Communications
- <http://www.zyxel.no>

Poland

- ZyXEL Communications Poland
- <http://www.zyxel.pl>

Romania

- ZyXEL Romania
- <http://www.zyxel.com/ro/ro>

Russia

- ZyXEL Russia
- <http://www.zyxel.ru>

Slovakia

- ZyXEL Communications Czech s.r.o. organizacna zlozka
- <http://www.zyxel.sk>

Spain

- ZyXEL Spain
- <http://www.zyxel.es>

Sweden

- ZyXEL Communications
- <http://www.zyxel.se>

Switzerland

- Studerus AG

- <http://www.zyxel.ch/>

Turkey

- ZyXEL Turkey A.S.
- <http://www.zyxel.com.tr>

UK

- ZyXEL Communications UK Ltd.
- <http://www.zyxel.co.uk>

Ukraine

- ZyXEL Ukraine
- <http://www.ua.zyxel.com>

Latin America

Argentina

- ZyXEL Communication Corporation
- <http://www.zyxel.com/ec/es/>

Ecuador

- ZyXEL Communication Corporation
- <http://www.zyxel.com/ec/es/>

Middle East

Egypt

- ZyXEL Communication Corporation
- <http://www.zyxel.com/homepage.shtml>

Middle East

- ZyXEL Communication Corporation
- <http://www.zyxel.com/homepage.shtml>

North America

USA

- ZyXEL Communications, Inc. - North America Headquarters
- <http://www.us.zyxel.com/>

Oceania

Australia

- ZyXEL Communications Corporation
- <http://www.zyxel.com/au/en/>

Africa

South Africa

- Nology (Pty) Ltd.
- <http://www.zyxel.co.za>

Legal Information

Copyright

Copyright © 2015 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimers

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Your use of the UAG is subject to the terms and conditions of any related service providers.

Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Regulatory Notice and Statement

UNITED STATE AMERICA



The following information applies if you use the product within USA area.

FCC EMC Statement

• This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- 1 This device may not cause harmful interference, and
 - 2 this device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
 - This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
 - If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
 - 1 Reorient or relocate the receiving antenna.
 - 2 Increase the separation between the equipment or devices.
 - 3 Connect the equipment to an outlet other than the receiver's.
 - 4 Consult a dealer or an experienced radio/TV technician for assistance.

FCC Radiation Exposure Statement

- This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.

CANADA

The following information applies if you use the product within Canada area.

Industry Canada ICES statement

CAN ICES-3 (B)/NMB-3(B)

Industry Canada RSS-GEN & RSS-210 statement

- This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.
- Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.
- This radio transmitter (2468C-Z2FPM9582, 2468C-Z5SPM9382) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.
- Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.
- Le présent émetteur radio (2468C-Z2FPM9582, 2468C-Z5SPM9382) de modèle s'il fait partie du matériel de catégorie I a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Industry Canada radiation exposure statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

EUROPEAN UNION



The following information applies if you use the product within the European Union.

Declaration of Conformity with Regard to EU Directive 1999/5/EC (R&TTE Directive)

Compliance information for 2.4GHz and/or 5GHz wireless products relevant to the EU and other Countries following the EU Directive 1999/5/EC (R&TTE).

Български (Bulgarian)	С настоящото ZyXEL декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/EC.
Español (Spanish)	Por medio de la presente ZyXEL declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Čeština (Czech)	ZyXEL tímto prohlašuje, že tento zařizení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC.
Dansk (Danish)	Undertegnede ZyXEL erklærer herved, at følgende udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch (German)	Hiermit erkläre ZyXEL, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab ZyXEL seadme seadmed vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ΖyxEL ΔΗΛΩΝΕΙ ΟΤΙ ΕΞΟΠΛΙΣΜΟΣ ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕC.
English	Hereby, ZyXEL declares that this equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Français (French)	Par la présente ZyXEL déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/EC.
Hrvatski (Croatian)	ZyXEL ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 1999/5/EC.
Íslenska (Icelandic)	Hér með lýsir, ZyXEL því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 1999/5/EC.

Italiano (Italian)	Con la presente ZyXEL dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviešu valoda (Latvian)	Ar šo ZyXEL deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių kalba (Lithuanian)	Šiuo ZyXEL deklaruoją, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, ZyXEL nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EK irányelv egyéb előírásainak.
Malti (Maltese)	Hawnhekk, ZyXEL, jiddikjara li dan taghmir jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Dirrettiva 1999/5/EC.
Nederlands (Dutch)	Hierbij verklaart ZyXEL dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC.
Polski (Polish)	Niniejszym ZyXEL oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português (Portuguese)	ZyXEL declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/EC.
Română (Romanian)	Prin prezenta, ZyXEL declară că acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 1999/5/EC.
Slovenčina (Slovak)	ZyXEL týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EC.
Slovenščina (Slovene)	ZyXEL izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/EC.
Suomi (Finnish)	ZyXEL vakuuttaa täten että laitteet tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar ZyXEL att denna utrustning står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EC.
Norsk (Norwegian)	Erklærer herved ZyXEL at dette utstyret er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 1999/5/EF.

National Restrictions

This product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 2014/53/UE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttiva 2014/53/UE) senza nessuna limitazione, eccetto per i paesi menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der Richtlinie 2014/53/EU folgen) mit Ausnahme der folgenden aufgeführten Staaten:

In the majority of the EU and other European countries, the 2.4GHz and 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable.

The requirements for any country may evolve. ZyXEL recommends that you check with the local authorities for the latest status of their national regulations for both the 2.4GHz and 5GHz wireless LANs.

The following countries have restrictions and/or requirements in addition to those given in the table labeled "Overview of Regulatory Requirements for Wireless LANs":.

Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check <http://www.bipt.be> for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie <http://www.bipt.be> voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez <http://www.ibpt.be> pour de plus amples détails.

Denmark

In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.

I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check <http://www.sviluppoeconomico.gov.it/> for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare <http://www.sviluppoeconomico.gov.it/> per maggiori dettagli.

Latvia

The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check <http://www.esd.lv> for more details.

2.4 GHz frekvenču joslas izmantošanai ārpus telpām nepieciešama atļauja no Elektronisko sakaru direkcijas. Vairāk informācijas: <http://www.esd.lv>.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 2014/53/EU has also been implemented in those countries.
2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CR	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Sweden	SE
Ireland	IE	Switzerland	CH
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.
- The PoE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.
- This product is for indoor use only (utilisation intérieure exclusivement).
- FOR COUNTRY CODE SELECTION USAGE (WLAN DEVICES)
Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all Wi-Fi product marketed in US must fixed to US operation channels only.

Environment statement

ErP (Energy-related Products)

ZyXEL products put on the EU market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

Network standby power consumption < 12W, and/or

Off mode power consumption < 0.5W, and/or

Standby mode power consumption < 0.5W.

Wireless setting, please refer to "Wireless" chapter for more detail.

WEEE Directive



Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

"INFORMAZIONI AGLI UTENTI"

Ai sensi della Direttiva 2012/19/UE del Parlamento europeo e del Consiglio, del 4 luglio 2012, sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE)

Il simbolo del cassonetto barrato riportato sull'apparecchiatura o sulla sua confezione indica che il prodotto alla fine della propria vita utile deve essere raccolto separatamente dagli altri rifiuti.

La raccolta differenziata della presente apparecchiatura giunta a fine vita e organizzata e gestita dal produttore. L'utente che vorrà disfarsi della presente apparecchiatura dovrà quindi contattare il produttore e seguire il sistema che questo ha adottato per consentire la raccolta separata dell'apparecchiatura giunta a fine vita.

L'adeguata raccolta differenziata per l'avvio successivo dell'apparecchiatura dismessa al riciclaggio, al trattamento e allo smaltimento ambientalmente compatibile contribuisce ad evitare possibili effetti negativi sull'ambiente e sulla salute e favorisce il reimpiego e/o riciclo dei materiali di cui è composta l'apparecchiatura.

Lo smaltimento abusivo del prodotto da parte del detentore comporta l'applicazione delle sanzioni amministrative previste dalla normativa vigente."

Environmental Product Declaration

Български (Bulgarian)	Čeština (Czech)	Dansk (Danish)	Deutsch (German)
<p>Екологична продуктова декларация</p> <p>RoHS Директива 2011/65/ЕО WEEE Директива 2012/19/ЕО PPW Директива 94/62/ЕО REACH РЕГЛАМЕНТ (ЕО) № 1907/2006 ErP Директива 2009/125/ЕО</p> <p>Име/титул: Richard Hsu / Quality Management Division Senior Manager Подпис: <i>Richard Hsu</i> Дата (dd/mm/yyyy): 01/10/2014</p>  	<p>Environmentální prohlášení o produktu</p> <p>RoHS Směrnice 2011/65/EU WEEE Směrnice 2012/19/EU PPW Směrnice 94/62/ES REACH Nařízení (ES) č. 1907/2006 ErP Směrnice 2009/125/ES</p> <p>Jméno/ titul: Richard Hsu / Quality Management Division Senior Manager Podpis: <i>Richard Hsu</i> Datum (dd/mm/yyyy): 01/10/2014</p>  	<p>Miljøvaredeklaration</p> <p>RoHS Direktiv 2011/65/EU WEEE Direktiv 2012/19/EU PPW Direktiv 94/62/EF REACH Forordning (EF) nr. 1907/2006 ErP Direktiv 2009/125/EF</p> <p>Navn/ titel: Richard Hsu / Quality Management Division Senior Manager Underskrift: <i>Richard Hsu</i> Dato (dd/mm/åååå): 01/10/2014</p>  	<p>Produkt-Umweltdeklaration</p> <p>RoHS Richtlinie 2011/65/EU WEEE Richtlinie 2012/19/EU PPW Richtlinie 94/62/EG REACH VERORDNUNG (EG) Nr. 1907/2006 ErP Richtlinie 2009/125/EG</p> <p>Name/ titel: Richard Hsu / Quality Management Division Senior Manager Unterschrift: <i>Richard Hsu</i> Datum (dd/mm/yyyy): 2014/10/01</p>  
<p>Toote keskkonnadeklaratsioon</p> <p>RoHS Direktiiv 2011/65/EL WEEE Direktiiv 2012/19/EL PPW Direktiiv 94/62/EÜ REACH MAARLUS (EÜ) nr 1907/2006 ErP Direktiiv 2009/125/EÜ</p> <p>Nimi/ pealkiri: Richard Hsu / Quality Management Division Senior Manager Allkiri: <i>Richard Hsu</i> Kuupäev (pp/kk/aaaa): 01/10/2014</p>  	<p>Environmental product declaration</p> <p>RoHS Directive 2011/65/EU WEEE Directive 2012/19/EU PPW Directive 94/62/EC REACH Regulation (EC) No 1907/2006 ErP Directive 2009/125/EC</p> <p>Name/ title: Richard Hsu / Quality Management Division Senior Manager Signature: <i>Richard Hsu</i> Date (dd/mm/yyyy): 01/10/2014</p>  	<p>Declaraciones Ambientales de Producto</p> <p>RoHS Directiva 2011/65/UE WEEE Directiva 2012/19/UE PPW Directiva 94/62/CE REACH REGLAMENTO (CE) n.º 1907/2006 ErP Directiva 2009/125/CE</p> <p>Nombre/ título: Richard Hsu / Quality Management Division Senior Manager Firma: <i>Richard Hsu</i> Fecha (aaaa/mm/dd): 2014/10/01</p>  	<p>Profil environnemental de produit</p> <p>RoHS Directive 2011/65/UE WEEE Directive 2012/19/UE PPW Directive 94/62/CE REACH RÈGLEMENT (CE) N° 1907/2006 ErP Directive 2009/125/CE</p> <p>Nom/ titre: Richard Hsu / Quality Management Division Senior Manager Signature: <i>Richard Hsu</i> Date (aaaa/mm/jj): 2014/10/01</p>  
<p>Deklaraciju o zbirjanju proizvoda</p> <p>RoHS Direktiva 2011/65/EU WEEE Direktiva 2012/19/EU PPW Direktiva 94/62/EZ REACH Uredba (EZ) br. 1907/2006 ErP Direktiva 2009/125/EZ</p> <p>Ime/ naslov: Richard Hsu / Quality Management Division Senior Manager Podpis: <i>Richard Hsu</i> Datum (dd/mm/yyyy): 01/10/2014</p>  	<p>Dichiarazione ambientale di prodotto</p> <p>RoHS Direttiva 2011/65/UE WEEE Direttiva 2012/19/UE PPW Direttiva 94/62/CE REACH REGOLAMENTO (CE) n. 1907/2006 ErP Direttiva 2009/125/CE</p> <p>Nome/ titolo: Richard Hsu / Quality Management Division Senior Manager Firma: <i>Richard Hsu</i> Data (aaaa/mm/gg): 2014/10/01</p>  	<p>Produkta vides ietekmējuma deklarācija</p> <p>RoHS Direktīva 2011/65/ES WEEE Direktīva 2012/19/ES PPW Direktīva 94/62/EK REACH Regula (EK) Nr. 1907/2006 ErP Direktīva 2009/125/EK</p> <p>Nosaukums/ tūls: Richard Hsu / Quality Management Division Senior Manager Paraksts: <i>Richard Hsu</i> Datums (dd/mm/gggg): 01/10/2014</p>  	<p>Aplinkosauginis gaminio deklaracija</p> <p>RoHS Direktyva 2011/65/ES WEEE Direktyva 2012/19/ES PPW Direktyva 94/62/EB REACH REGULIAMENTAS (ES) Nr. 1907/2006 ErP Direktyva 2009/125/EB</p> <p>Vardas/ titulas: Richard Hsu / Quality Management Division Senior Manager Parašas: <i>Richard Hsu</i> Data (dd/mm/mmmmm): 01/10/2014</p>  
<p>Köznyelvetudományi terméknyilatkozatot</p> <p>RoHS 2011/65/EU irányelv WEEE 2012/19/EU irányelv PPW 94/62/EK irányelv REACH 1907/2006/EK Rendelet ErP 2009/125/EK irányelv</p> <p>Név/ cím: Richard Hsu / Quality Management Division Senior Manager Aláírás: <i>Richard Hsu</i> Dátum (dd/mm/yyyy): 2014/10/01</p>  	<p>Dikjarazzjoni Ambientali dwar il-Prodott</p> <p>RoHS Direttiva 2011/65/UE WEEE Direttiva 2012/19/UE PPW Direttiva 94/62/KE REACH REGOLAMENTO (KE) NR 1907/2006 ErP Direttiva 2009/125/CE</p> <p>Isem/ titolu: Richard Hsu / Quality Management Division Senior Manager Firma: <i>Richard Hsu</i> Data (aaaa/mm/jgg): 2014/10/01</p>  	<p>Miljøproductveklaring</p> <p>RoHS Richtlijn 2011/65/EU WEEE Richtlijn 2012/19/EU PPW Richtlijn 94/62/EG REACH Verordening (EG) nr. 1907/2006 ErP Richtlijn 2009/125/EK</p> <p>Handtekening: Richard Hsu / Quality Management Division Senior Manager Datum (dd/mm/jaar): 01/10/2014</p>  	<p>Deklarację środowiskową produktu</p> <p>RoHS Dyrektywa 2011/65/UE WEEE Dyrektywa 2012/19/UE PPW Dyrektywa 94/62/WE REACH Rozporządzenie (WE) nr 1907/2006 ErP Dyrektywa 2009/125/WE</p> <p>Nazwisko/ tytuł: Richard Hsu / Quality Management Division Senior Manager Podpis: <i>Richard Hsu</i> Data (dd/mm/rrrr): 2014/10/01</p>  
<p>Declaração ambiental do produto</p> <p>RoHS Diretiva 2011/65/UE WEEE Diretiva 2012/19/UE PPW Diretiva 94/62/CE REACH Regulamento (CE) n.º 1907/2006 ErP Diretiva 2009/125/CE</p> <p>Nome/ título: Richard Hsu / Quality Management Division Senior Manager Assinatura: <i>Richard Hsu</i> Data (dd/mm/aaaa): 01/10/2014</p>  	<p>Declarație de mediu privind produsele</p> <p>RoHS Directiva 2011/65/UE WEEE Directiva 2012/19/UE PPW Directiva 94/62/CE REACH REGULAMENTUL (CE) NR. 1907/2006 ErP Directiva 2009/125/CE</p> <p>Nume/ titlu: Richard Hsu / Quality Management Division Senior Manager Semnatura: <i>Richard Hsu</i> Data (zz/mm/aaaa): 01/10/2014</p>  	<p>Vyhlasenie o environmentálnom výrobku</p> <p>RoHS Smernica 2011/65/EU WEEE Smernica 2012/19/EU PPW Smernica 94/62/ES REACH Naariadenie (ES) č. 1907/2006 ErP Smernica 2009/125/ES</p> <p>Menlo/ titul: Richard Hsu / Quality Management Division Senior Manager Podpis: <i>Richard Hsu</i> Datum (dd/mm/yyyy): 01/10/2014</p>  	<p>Okološko deklaracija izdelka</p> <p>RoHS Direktiva 2011/65/UE WEEE Direktiva 2012/19/UE PPW Direktiva 94/62/ES REACH Uredba (ES) br. 1907/2006 ErP Direktiva 2009/125/ES</p> <p>Ime/ naziv: Richard Hsu / Quality Management Division Senior Manager Podpis: <i>Richard Hsu</i> Datum (dd/mm/yyyy): 01/10/2014</p>  
<p>Standardin perustava ympäristötietustieto</p> <p>RoHS Direktiiv 2011/65/EU WEEE Direktiiv 2012/19/EU PPW Direktiiv 94/62/EY REACH ASETUS (EY) N:o 1907/2006 ErP Direktiiv 2009/125/EY</p> <p>Nimi/ titteli: Richard Hsu / Quality Management Division Senior Manager Alkajatus: <i>Richard Hsu</i> Päivämäärä (pp/kk/vvvv): 01/10/2014</p>  	<p>Miljöproduktdeklaration</p> <p>RoHS Direktiv 2011/65/EU WEEE Direktiv 2012/19/EU PPW Direktiv 94/62/EG REACH Förordning (EG) nr 1907/2006 ErP Direktiv 2009/125/EG</p> <p>Namn/ titel: Richard Hsu / Quality Management Division Senior Manager Namnteckning: <i>Richard Hsu</i> Datum (dd/mm/yyyy): 01/10/2014</p>  	<p>Περιβαλλοντική δήλωση προϊόντος</p> <p>RoHS Οδηγία 2011/65/ΕΕ WEEE Οδηγία 2012/19/ΕΕ PPW Οδηγία 94/62/ΕΚ REACH Κανονισμός (ΕΚ) αριθ. 1907/2006 ErP Οδηγία 2009/125/ΕΚ</p> <p>Όνομα/ τίτλος: Richard Hsu / Quality Management Division Senior Manager Υπογραφή: <i>Richard Hsu</i> Ημερομηνία (gg/mm/yyyy): 01/10/2014</p>  	<p>Miljødeklarasjon</p> <p>RoHS Direktiv 2011/65/EU WEEE Direktiv 2012/19/EU PPW Direktiv 94/62/EF REACH Forordning (EF) nr. 1907/2006 ErP Direktiv 2009/125/EF</p> <p>Navn/ tittel: Richard Hsu / Quality Management Division Senior Manager Signatur: <i>Richard Hsu</i> Dato (dd/mm/åååå): 01/10/2014</p>  

台灣



以下訊息僅適用於產品銷售至台灣地區

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Viewing Certifications

Go to <http://www.zyxel.com> to view this product's documentation and certifications.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. If you cannot find it there, contact your vendor or ZyXEL Technical Support at support@zyxel.com.tw.

To obtain the source code covered under those Licenses, please contact your vendor or ZyXEL Technical Support at support@zyxel.com.tw.

Symbols

Numbers

3322 Dynamic DNS [214](#)

3DES [355](#)

A

AAA

port [461, 462](#)

AAA server [459](#)

and users [400](#)

local user database [459](#)

RADIUS [459, 460](#)

RADIUS group [460](#)

see also RADIUS

access [23](#)

access users [399, 401](#)

custom page [506](#)

forcing login [260](#)

idle timeout [408](#)

logging in [260](#)

multiple logins [408](#)

see also users [399](#)

Web Configurator [410](#)

access users, see also force user authentication policies

account

user [399](#)

accounting server [459](#)

active protocol [359](#)

AH [359](#)

and encapsulation [360](#)

ESP [359](#)

active sessions [85, 87, 99](#)

ActiveX [390](#)

AD

port [461, 462](#)

address groups [442](#)

and content filtering [381, 382](#)

and FTP [525](#)

and SNMP [528](#)

and SSH [521](#)

and Telnet [524](#)

and WWW [506](#)

address objects [442](#)

and content filtering [381, 382](#)

and FTP [525](#)

and NAT [210, 222](#)

and policy routes [209](#)

and SNMP [528](#)

and SSH [521](#)

and Telnet [524](#)

and VPN connections [339](#)

and WWW [506](#)

HOST [442](#)

RANGE [442](#)

SUBNET [442](#)

types of [442](#)

address record [496](#)

admin user

troubleshooting [587](#)

admin users [399](#)

multiple logins [408](#)

see also users [399](#)

Advanced Encryption Standard, see AES

AES [355](#)

AF [212](#)

AH [344, 359](#)

and transport mode [360](#)

alerts [540, 541, 543, 545, 546, 547](#)

ALG [239](#)

and NAT [239](#)

and policy routes [239](#)

and security policy [239](#)

and trunks [239](#)

FTP [239](#)

H.323 [239](#)

- see also VoIP pass through [239](#)
 - SIP [239](#)
 - Application Layer Gateway, see ALG
 - application patrol [376](#)
 - actions [376](#)
 - and security policy [376](#)
 - classification [376](#)
 - exceptions [376](#)
 - port-less [376](#)
 - ports [377](#)
 - service ports [377](#)
 - vs security policy [289](#)
 - asymmetrical routes [291](#)
 - allowing through the security policy [293](#)
 - vs virtual interfaces [291](#)
 - attacks
 - Denial of Service (DoS) [343](#)
 - authentication
 - in IPSec [344](#)
 - server [459](#)
 - authentication algorithms [354, 355](#)
 - and active protocol [355](#)
 - MD5 [355](#)
 - SHA1 [355](#)
 - Authentication Header, see AH
 - authentication method objects [464](#)
 - and users [400](#)
 - and WWW [505](#)
 - create [465](#)
 - authentication policy
 - exceptional services [262](#)
 - Authentication server
 - RADIUS client [530](#)
 - authentication server [528](#)
 - authentication type [67, 485](#)
 - Authentication, Authorization, Accounting servers,
 - see AAA server
 - authorization server [459](#)
- B**
- backing up configuration files [551](#)
 - bandwidth limit
 - troubleshooting [585](#)
 - bandwidth management [366, 376](#)
 - and schedules [371, 374](#)
 - and user groups [371, 374](#)
 - and users [371, 374](#)
 - maximize bandwidth usage [370](#)
 - see also application patrol [376](#)
 - boot module [556](#)
 - bridge interfaces [155, 182](#)
 - and virtual interfaces of members [183](#)
 - basic characteristics [155](#)
 - effect on routing table [183](#)
 - member interfaces [183](#)
 - virtual [189](#)
 - bridges [182](#)
- C**
- CA
 - and certificates [468](#)
 - CA (Certificate Authority), see certificates
 - Calling Station ID [426](#)
 - capturing packets [562](#)
 - CEF (Common Event Format) [538, 545](#)
 - certificate
 - troubleshooting [587](#)
 - Certificate Authority (CA)
 - see certificates
 - Certificate Revocation List (CRL) [468](#)
 - certificates [467](#)
 - advantages of [468](#)
 - and CA [468](#)
 - and FTP [525](#)
 - and HTTPS [502](#)
 - and IKE SA [359](#)
 - and SSH [521](#)
 - and VPN gateways [340](#)
 - and WWW [504](#)
 - certification path [468, 474, 480](#)
 - expired [468](#)
 - factory-default [468](#)
 - file formats [468](#)
 - fingerprints [475, 481](#)
 - importing [471](#)
 - in IPSec [351](#)
 - not used for encryption [468](#)
 - revoked [468](#)
 - self-signed [468, 473](#)
 - serial number [475, 480](#)

- storage space [470, 478](#)
 - thumbprint algorithms [469](#)
 - thumbprints [469](#)
 - used for authentication [468](#)
 - verifying fingerprints [469](#)
 - certification requests [473](#)
 - certifications
 - viewing [603](#)
 - Challenge Handshake Authentication Protocol (CHAP) [485](#)
 - CHAP (Challenge Handshake Authentication Protocol) [485](#)
 - CHAP/PAP [485](#)
 - CLI [22, 26](#)
 - button [26](#)
 - messages [26](#)
 - popup window [26](#)
 - Reference Guide [2](#)
 - commands [22](#)
 - sent by Web Configurator [26](#)
 - Common Event Format (CEF) [538, 545](#)
 - comparison table [20](#)
 - compression (stac) [485](#)
 - computer names [164, 180, 188, 193](#)
 - configuration
 - information [560, 566](#)
 - configuration file
 - troubleshooting [588](#)
 - configuration files [549](#)
 - at restart [552](#)
 - backing up [551](#)
 - downloading [553, 571](#)
 - downloading with FTP [524](#)
 - editing [549](#)
 - how applied [550](#)
 - lastgood.conf [552, 555](#)
 - managing [551](#)
 - startup-config.conf [555](#)
 - startup-config-bad.conf [552](#)
 - syntax [550](#)
 - system-default.conf [555](#)
 - uploading [555](#)
 - uploading with FTP [524](#)
 - use without restart [549](#)
 - connection
 - troubleshooting [586](#)
 - connectivity check [163, 173, 179, 189, 345](#)
 - console port
 - speed [492](#)
 - contact information [591](#)
 - content filtering [381, 382](#)
 - and address groups [381, 382](#)
 - and address objects [381, 382](#)
 - and registration [384, 386](#)
 - and schedules [381, 382](#)
 - and user groups [381](#)
 - and users [381](#)
 - by category [381, 382, 387](#)
 - by keyword (in URL) [382, 391](#)
 - by URL [382, 390, 392, 393](#)
 - by web feature [382, 390](#)
 - categories [387](#)
 - category service [386](#)
 - default policy [382](#)
 - external web filtering service [386, 394](#)
 - filter list [382](#)
 - managed web pages [387](#)
 - policies [381, 382](#)
 - registration status [384, 386](#)
 - statistics [123](#)
 - testing [388](#)
 - uncategorized pages [387](#)
 - unsafe web pages [386](#)
 - URL for blocked access [384](#)
 - cookies [22, 390](#)
 - copyright [597](#)
 - CPU usage [84, 86](#)
 - current date/time [82, 488](#)
 - and schedules [453](#)
 - daylight savings [490](#)
 - setting manually [491](#)
 - time server [492](#)
 - custom
 - access user page [506](#)
 - login page [506](#)
 - customer support [591](#)
- ## D
- Data Encryption Standard, see DES
 - date [488](#)
 - daylight savings [490](#)
 - DDNS [214](#)

- backup mail exchanger [218](#)
 - mail exchanger [218](#)
 - service providers [214](#)
 - troubleshooting [585](#)
 - Dead Peer Detection, see DPD
 - default
 - security policy behavior [290](#)
 - Denial of Service (Dos) attacks [343](#)
 - DES [355](#)
 - device access
 - troubleshooting [583](#)
 - DHCP [192, 487](#)
 - and DNS servers [193](#)
 - and domain name [487](#)
 - and interfaces [193](#)
 - client list [88](#)
 - pool [193](#)
 - static DHCP [193](#)
 - diagnostics [560, 566](#)
 - Diffie-Hellman key group [356](#)
 - DiffServ [212](#)
 - Digital Signature Algorithm public-key algorithm, see DSA
 - direct routes [206](#)
 - disclaimer [597](#)
 - DNS [493](#)
 - address records [496](#)
 - domain name forwarders [498](#)
 - domain name to IP address [496](#)
 - IP address to domain name [496](#)
 - Mail eXchange (MX) records [499](#)
 - pointer (PTR) records [496](#)
 - DNS servers [68, 493, 498](#)
 - and interfaces [193](#)
 - documentation
 - related [2](#)
 - domain name [487](#)
 - Domain Name System, see DNS
 - DPD [353](#)
 - DSA [473](#)
 - DSCP [206, 209, 372, 374, 577](#)
 - Dynamic Domain Name System, see DDNS
 - dynamic guest [103](#)
 - dynamic guest account [103, 400](#)
 - Dynamic Host Configuration Protocol, see DHCP.
 - DynDNS [214](#)
 - DynDNS see also DDNS [214](#)
 - Dynu [214](#)
- ## E
- Ekahau RTLS [286](#)
 - e-mail
 - daily statistics report [534](#)
 - Encapsulating Security Payload, see ESP
 - encapsulation
 - and active protocol [360](#)
 - IPSec [344](#)
 - transport mode [360](#)
 - tunnel mode [360](#)
 - VPN [360](#)
 - encryption
 - IPSec [344](#)
 - RSA [475](#)
 - encryption algorithms [355](#)
 - 3DES [355](#)
 - AES [355](#)
 - and active protocol [355](#)
 - DES [355](#)
 - encryption method [485](#)
 - enforcing policies in IPSec [343](#)
 - ESP [344, 359](#)
 - and transport mode [360](#)
 - Ethernet interfaces [155](#)
 - and routing protocols [158](#)
 - basic characteristics [155](#)
 - virtual [189](#)
 - exceptional services [262](#)
 - extended authentication
 - and VPN gateways [339](#)
 - IKE SA [358](#)
 - Extended Service Set IDentification [415](#)
 - ext-user
 - troubleshooting [586](#)
- ## F
- FCC interference statement [597](#)
 - file extensions
 - configuration files [549](#)

- shell scripts [549](#)
- file manager [549](#)
- Firefox [22](#)
- firmware
 - and restart [555](#)
 - boot module, see boot module
 - current version [82](#), [556](#)
 - getting updated [555](#)
 - uploading [555](#), [556](#)
 - uploading with FTP [524](#)
- firmware upload
 - troubleshooting [589](#)
- flash usage [84](#)
- forcing login [260](#)
- FQDN [496](#)
- free guest account [332](#)
- free time [332](#)
 - configuration [332](#)
 - enable [332](#)
- FTP [524](#)
 - additional signaling port [240](#)
 - ALG [239](#)
 - and address groups [525](#)
 - and address objects [525](#)
 - and certificates [525](#)
 - and zones [525](#)
 - signaling port [240](#)
 - with Transport Layer Security (TLS) [525](#)
- Fully-Qualified Domain Name, see FQDN

G

- Generic Routing Encapsulation, see GRE.
- GRE [194](#)
- Guide
 - CLI Reference [2](#)
 - Quick Start [2](#)

H

- HTTP
 - over SSL, see HTTPS
 - redirect to HTTPS [504](#)
 - vs HTTPS [502](#)

- HTTP redirect [231](#)
 - and interfaces [234](#)
 - and policy routes [232](#)
 - and security policy [232](#)
 - packet flow [232](#)
 - troubleshooting [586](#)
- HTTPS [502](#)
 - and certificates [502](#)
 - authenticating clients [502](#)
 - avoiding warning messages [512](#)
 - example [511](#)
 - vs HTTP [502](#)
 - with Internet Explorer [511](#)
 - with Netscape Navigator [511](#)
- HyperText Transfer Protocol over Secure Socket Layer, see HTTPS

I

- ICMP [447](#)
- IEEE 802.1q VLAN
- IEEE 802.1x [415](#)
- IKE SA
 - aggressive mode [354](#), [357](#), [358](#)
 - and certificates [359](#)
 - and RADIUS [359](#)
 - authentication algorithms [354](#), [355](#)
 - content [356](#)
 - Dead Peer Detection (DPD) [353](#)
 - Diffie-Hellman key group [356](#)
 - encryption algorithms [355](#)
 - extended authentication [358](#)
 - ID type [356](#)
 - IP address, remote IPsec router [354](#)
 - IP address, ZyXEL device [354](#)
 - local identity [357](#)
 - main mode [354](#), [357](#)
 - NAT traversal [358](#)
 - negotiation mode [354](#)
 - password [359](#)
 - peer identity [357](#)
 - pre-shared key [356](#)
 - proposal [354](#)
 - see also VPN
 - user name [359](#)
- Instant Messenger (IM) [376](#)
 - managing [376](#)

- interface
 - status [83, 95](#)
 - troubleshooting [584](#)
- interfaces [154](#)
 - and DNS servers [193](#)
 - and HTTP redirect [234](#)
 - and layer-3 virtualization [155](#)
 - and NAT [222](#)
 - and physical ports [154](#)
 - and policy routes [210](#)
 - and SMTP redirect [238](#)
 - and static routes [212](#)
 - and VPN gateways [339](#)
 - and zones [154](#)
 - as DHCP relays [193](#)
 - as DHCP servers [193, 487](#)
 - backup, see trunks
 - bandwidth management [192, 200, 202](#)
 - bridge, see also bridge interfaces.
 - DHCP clients [191](#)
 - Ethernet, see also Ethernet interfaces.
 - gateway [192](#)
 - general characteristics [154](#)
 - IP address [191](#)
 - metric [192](#)
 - MTU [192](#)
 - overlapping IP address and subnet mask [191](#)
 - port groups, see also port groups.
 - PPPoE/PPTP, see also PPPoE/PPTP interfaces.
 - prerequisites [156](#)
 - relationships between [156](#)
 - static DHCP [193](#)
 - subnet mask [191](#)
 - trunks, see also trunks.
 - types [155](#)
 - virtual, see also virtual interfaces.
 - VLAN, see also VLAN interfaces.
- Internet access
 - troubleshooting [583, 586](#)
- Internet Control Message Protocol, see ICMP
- Internet Explorer [22](#)
- Internet Protocol Security, see IPSec
- IP policy routing, see policy routes
- IP protocols [447](#)
 - and service objects [448](#)
 - ICMP, see ICMP
 - TCP, see TCP
 - UDP, see UDP
- IP static routes, see static routes
- IP/MAC binding
 - example [248](#)
 - exempt list [251](#)
 - monitor [101](#)
 - overview [248](#)
 - static DHCP [251](#)
- IPSec [338](#)
 - active protocol [344](#)
 - AH [344](#)
 - and certificates [340](#)
 - authentication [344](#)
 - certificates [351](#)
 - connections [339](#)
 - connectivity check [345](#)
 - encapsulation [344](#)
 - encryption [344](#)
 - ESP [344](#)
 - established in two phases [339](#)
 - local network [338](#)
 - local policy [343](#)
 - NetBIOS [343](#)
 - peer [338](#)
 - Perfect Forward Secrecy [345](#)
 - PFS [345](#)
 - phase 2 settings [343](#)
 - policy enforcement [343](#)
 - remote IPSec router [338](#)
 - remote network [338](#)
 - remote policy [343](#)
 - replay detection [343](#)
 - SA life time [343](#)
 - SA monitor [120](#)
 - SA see also IPSec SA [359](#)
 - see also VPN
 - static site-to-site [343](#)
 - transport encapsulation [344](#)
 - tunnel encapsulation [344](#)
 - VPN gateway [339](#)
- IPSec SA
 - active protocol [359](#)
 - authentication algorithms [354, 355](#)
 - destination NAT for inbound traffic [362](#)
 - encapsulation [360](#)
 - encryption algorithms [355](#)
 - local policy [359](#)
 - NAT for inbound traffic [361](#)
 - NAT for outbound traffic [361](#)
 - Perfect Forward Secrecy (PFS) [360](#)

- proposal [360](#)
 - remote policy [359](#)
 - search by name [120](#)
 - search by policy [120](#)
 - see also IPsec
 - see also VPN
 - source NAT for inbound traffic [362](#)
 - source NAT for outbound traffic [361](#)
 - status [120](#)
 - transport mode [360](#)
 - tunnel mode [360](#)
 - when IKE SA is disconnected [359](#)
 - ISP account
 - CHAP [485](#)
 - CHAP/PAP [485](#)
 - MPPE [485](#)
 - MSCHAP [485](#)
 - MSCHAP-V2 [485](#)
 - PAP [485](#)
 - ISP accounts [483](#)
 - and PPPoE/PPTP interfaces [169, 483](#)
 - authentication type [485](#)
 - encryption method [485](#)
 - stac compression [485](#)
- ## J
- Java [390](#)
 - permissions [22](#)
 - JavaScripts [22](#)
- ## K
- key pairs [467](#)
- ## L
- lastgood.conf [552, 555](#)
 - layer-2 isolation [253](#)
 - example [253](#)
 - IP [254](#)
 - LDAP
 - and users [400](#)
 - port [461, 462](#)
 - least load first load balancing [196](#)
 - LED suppression mode [138](#)
 - LED troubleshooting [583](#)
 - level-4 inspection [377](#)
 - level-7 inspection [376](#)
 - licensing [131](#)
 - Link Layer Discovery Protocol (LLDP) [107](#)
 - LLDP (Link Layer Discovery Protocol) [107](#)
 - load balancing [195](#)
 - algorithms [196, 200, 202](#)
 - least load first [196](#)
 - round robin [196](#)
 - see also trunks [195](#)
 - session-oriented [196](#)
 - spillover [197](#)
 - weighted round robin [197](#)
 - local user database [459](#)
 - log
 - troubleshooting [588](#)
 - log messages
 - categories [541, 543, 545, 546, 547](#)
 - debugging [125](#)
 - regular [125](#)
 - types of [125](#)
 - logged in users [89](#)
 - login
 - custom page [506](#)
 - logo
 - troubleshooting [588](#)
 - logout
 - Web Configurator [24](#)
 - logs
 - and security policy [296](#)
 - e-mail profiles [537](#)
 - e-mailing log messages [126, 540](#)
 - formats [538](#)
 - log consolidation [541](#)
 - settings [536](#)
 - syslog servers [537](#)
 - system [537](#)
 - types of [537](#)

M

MAC address [411](#)
 and VLAN [174](#)
 Ethernet interface [162](#)
 range [82](#)

MAC authentication [426](#)
 Calling Station ID [426](#)
 case [426](#)
 delimiter [426](#)

mac role [411](#)

managed web pages [387](#)

management access
 troubleshooting [588](#)

Management Information Base (MIB) [526](#)

MD5 [355](#)

memory usage [84](#), [86](#)

Message Digest 5, see MD5

messages
 CLI [26](#)

metrics, see reports

Microsoft
 Challenge-Handshake Authentication Protocol (MSCHAP) [485](#)
 Challenge-Handshake Authentication Protocol Version 2 (MSCHAP-V2) [485](#)
 Point-to-Point Encryption (MPPE) [485](#)

model name [82](#)

monitor
 SA [120](#)

MPPE (Microsoft Point-to-Point Encryption) [485](#)

MSCHAP (Microsoft Challenge-Handshake Authentication Protocol) [485](#)

MSCHAP-V2 (Microsoft Challenge-Handshake Authentication Protocol Version 2) [485](#)

multicast [420](#)

multicast rate [420](#)

My Certificates, see also certificates [470](#)

myZyXEL.com [131](#), [134](#)
 accounts, creating [131](#)

N

NAT [212](#), [219](#)
 ALG, see ALG

and address objects [210](#)
 and address objects (HOST) [222](#)
 and ALG [239](#)
 and interfaces [222](#)
 and policy routes [204](#), [210](#)
 and security policy [292](#)
 and to-Device security policy [223](#)
 and VPN [358](#)
 loopback [224](#)
 port forwarding, see NAT
 port translation, see NAT
 traversal [358](#)

NAT Port Mapping Protocol [241](#)

NAT Traversal [241](#)

NAT-PMP [241](#)

NBNS [164](#), [180](#), [188](#), [193](#)

NetBIOS
 Broadcast over IPSec [343](#)
 Name Server, see NBNS.

Netscape Navigator [22](#)

Network Address Translation, see NAT

Network Time Protocol (NTP) [491](#)

No-IP [214](#)

O

objects
 AAA server [459](#)
 addresses and address groups [442](#)
 authentication method [464](#)
 certificates [467](#)
 schedules [453](#)
 services and service groups [447](#)
 users, user groups [399](#)

OSI level-4 [377](#)

OSI level-7 [376](#)

other documentation [2](#)

OUI [412](#)

P

packet
 statistics [92](#), [93](#), [110](#)

packet capture [562](#)

- files [561](#), [565](#), [566](#), [567](#)
 - troubleshooting [589](#)
 - packet captures
 - downloading files [562](#), [565](#), [567](#), [568](#)
 - PAP (Password Authentication Protocol) [485](#)
 - Password Authentication Protocol (PAP) [485](#)
 - Peanut Hull [214](#)
 - Peer-to-peer (P2P)
 - managing [376](#)
 - Perfect Forward Secrecy (PFS) [345](#)
 - Diffie-Hellman key group [360](#)
 - PFS (Perfect Forward Secrecy) [345](#), [360](#)
 - physical ports
 - packet statistics [92](#), [93](#), [110](#)
 - pointer record [496](#)
 - Point-to-Point Protocol over Ethernet, see PPPoE.
 - Point-to-Point Tunneling Protocol, see PPTP
 - policy enforcement in IPsec [343](#)
 - policy route
 - troubleshooting [584](#)
 - policy routes [203](#)
 - actions [205](#)
 - and address objects [209](#)
 - and ALG [239](#)
 - and HTTP redirect [232](#)
 - and interfaces [210](#)
 - and NAT [204](#)
 - and schedules [209](#)
 - and service objects [448](#)
 - and SMTP redirect [236](#)
 - and trunks [195](#), [210](#)
 - and user groups [209](#)
 - and users [209](#)
 - and VPN 1-1 mapping [227](#)
 - benefits [204](#)
 - criteria [205](#)
 - overriding direct routes [206](#)
 - pop-up windows [22](#)
 - port forwarding, see NAT
 - port groups [155](#), [157](#)
 - port roles [156](#)
 - and Ethernet interfaces [156](#)
 - and physical ports [156](#)
 - port translation, see NAT
 - power off [582](#)
 - PPP [194](#)
 - troubleshooting [585](#)
 - PPP interfaces
 - subnet mask [191](#)
 - PPPoE [194](#)
 - and RADIUS [194](#)
 - TCP port 1723 [194](#)
 - PPPoE/PPTP interfaces [155](#), [168](#)
 - and ISP accounts [169](#), [483](#)
 - basic characteristics [155](#)
 - gateway [169](#)
 - subnet mask [169](#)
 - PPTP [194](#)
 - and GRE [194](#)
 - as VPN [194](#)
 - pre-subscriber account [401](#)
 - printer
 - status [118](#)
 - printer firmware [322](#)
 - printer list [322](#)
 - printer management [322](#)
 - problems [583](#)
 - product registration [603](#)
 - proxy servers [231](#)
 - web, see web proxy servers
 - PTR record [496](#)
 - Public-Key Infrastructure (PKI) [468](#)
 - public-private key pairs [467](#)
- ## Q
- QoS [204](#), [367](#)
 - Quick Start Guide [2](#)
- ## R
- RADIUS [459](#), [460](#)
 - advantages [459](#)
 - and IKE SA [359](#)
 - and PPPoE [194](#)
 - and users [400](#)
 - user attributes [413](#)
 - RADIUS server [528](#)
 - troubleshooting [586](#)

- reboot [581](#)
 - vs reset [581](#)
 - Reference Guide, CLI [2](#)
 - registration [131](#)
 - and content filtering [384, 386](#)
 - product [603](#)
 - related documentation [2](#)
 - Remote Authentication Dial-In User Service, see RADIUS
 - remote management
 - FTP, see FTP
 - see also service control [501](#)
 - Telnet [523](#)
 - to-Device security policy [290](#)
 - WWW, see WWW
 - remote network [338](#)
 - replay detection [343](#)
 - reports
 - collecting data [97](#)
 - content filtering [123](#)
 - daily [534](#)
 - daily e-mail [534](#)
 - specifications [99](#)
 - traffic statistics [97](#)
 - reset [589](#)
 - vs reboot [581](#)
 - RESET button [589](#)
 - RFC
 - 1631 (NAT) [212](#)
 - 2131 (DHCP) [192](#)
 - 2132 (DHCP) [192](#)
 - 2402 (AH) [344, 359](#)
 - 2406 (ESP) [344, 359](#)
 - 2516 (PPPoE) [194](#)
 - 2637 (PPTP) [194](#)
 - 2890 (GRE) [194](#)
 - Rivest, Shamir and Adleman public-key algorithm (RSA) [473](#)
 - round robin [196](#)
 - routing
 - troubleshooting [585](#)
 - routing protocols
 - and Ethernet interfaces [158](#)
 - RSA [473, 475, 480](#)
 - RSSI threshold [419](#)
 - RTLS [286](#)
- ## S
- schedule
 - troubleshooting [587](#)
 - schedules [453](#)
 - and bandwidth management [371, 374](#)
 - and content filtering [381, 382](#)
 - and current date/time [453](#)
 - and policy routes [209](#)
 - and security policy [296](#)
 - one-time [453](#)
 - recurring [453](#)
 - types of [453](#)
 - screen resolution [22](#)
 - Secure Hash Algorithm, see SHA1
 - Secure Socket Layer, see SSL
 - security associations, see IPsec
 - security policy [289](#)
 - actions [296](#)
 - and ALG [239](#)
 - and application patrol [376](#)
 - and HTTP redirect [232](#)
 - and logs [296](#)
 - and NAT [292](#)
 - and schedules [296](#)
 - and service groups [295](#)
 - and service objects [448](#)
 - and services [295](#)
 - and SMTP redirect [236](#)
 - and user groups [296, 299](#)
 - and users [296, 299](#)
 - and VPN 1-1 mapping [227](#)
 - and zones [290, 294](#)
 - asymmetrical routes [291, 293](#)
 - global rules [291](#)
 - priority [294](#)
 - rule criteria [291](#)
 - session control [296](#)
 - session limits [291](#)
 - stateful inspection [290](#)
 - to-Device, see to-Device security policy
 - triangle routes [291, 293](#)
 - troubleshooting [584](#)
 - vs application patrol [289](#)
 - security settings
 - troubleshooting [584](#)
 - serial number [82](#)
 - service control [501](#)

- and to-Device security policy [501](#)
- and users [501](#)
- limitations [501](#)
- timeouts [501](#)
- service groups [448](#)
 - and security policy [295](#)
- service objects [447](#)
 - and IP protocols [448](#)
 - and policy routes [448](#)
 - and security policy [448](#)
- Service Set [415](#)
- service subscription status [133](#)
- services [447](#)
 - and security policy [295](#)
- session control [296](#)
- session limits [291](#)
- sessions [99](#)
- sessions usage [85, 87](#)
- SHA1 [355](#)
- shell script
 - troubleshooting [588](#)
- shell scripts [549](#)
 - and users [413](#)
 - downloading [558](#)
 - editing [557](#)
 - how applied [550](#)
 - managing [557](#)
 - syntax [550](#)
 - uploading [559](#)
- Short Message Service [336](#)
- shutdown [582](#)
- signatures
 - updating [134](#)
- Simple Network Management Protocol, see [SNMP](#)
- SMS [336](#)
 - configuration [336](#)
 - send account information [336](#)
 - ViaNett account [336](#)
- SMS gateway [336](#)
- SMTP redirect
 - and interfaces [238](#)
 - and policy routes [236](#)
 - and security policy [236](#)
 - packet flow [236](#)
- SNAT [212](#)
 - troubleshooting [585](#)
- SNMP [525, 526](#)
 - agents [526](#)
 - and address groups [528](#)
 - and address objects [528](#)
 - and zones [528](#)
 - Get [526](#)
 - GetNext [526](#)
 - Manager [526](#)
 - managers [526](#)
 - MIB [526](#)
 - network components [526](#)
 - Set [526](#)
 - Trap [526](#)
 - traps [527](#)
 - versions [525](#)
- Source Network Address Translation, see [SNAT](#)
- spillover (for load balancing) [197](#)
- SSH [518](#)
 - and address groups [521](#)
 - and address objects [521](#)
 - and certificates [521](#)
 - and zones [521](#)
 - client requirements [520](#)
 - encryption methods [520](#)
 - for secure Telnet [521](#)
 - how connection is established [519](#)
 - versions [520](#)
 - with Linux [522](#)
 - with Microsoft Windows [521](#)
- SSL [502](#)
- stac compression [485](#)
- startup-config.conf [555](#)
 - if errors [552](#)
 - missing at restart [552](#)
 - present at restart [552](#)
- startup-config-bad.conf [552](#)
- stateful inspection [290](#)
- static DHCP [251](#)
- static routes [204](#)
 - and interfaces [212](#)
 - metric [212](#)
- statistics
 - content filtering [123](#)
 - daily e-mail report [534](#)
 - traffic [97](#)
- status [80](#)
- streaming protocols management [376](#)
- subscription services

- status [133](#)
- supported browsers [22](#)
- syslog [545](#)
- syslog servers, see also logs
- system log, see logs
- system name [82, 487](#)
- system reports, see reports
- system uptime [82](#)
- system-default.conf [555](#)

T

- TCP [447](#)
 - connections [447](#)
 - port numbers [447](#)
- Telnet [523](#)
 - and address groups [524](#)
 - and address objects [524](#)
 - and zones [524](#)
 - with SSH [521](#)
- throughput rate
 - troubleshooting [588](#)
- time [488](#)
- time servers (default) [491](#)
- to-Device security policy [290](#)
 - and NAT [223](#)
 - and remote management [290](#)
 - and service control [501](#)
 - global rules [290](#)
- trademarks [597](#)
- traffic statistics [97](#)
- Transmission Control Protocol, see TCP
- transport encapsulation [344](#)
- Transport Layer Security (TLS) [525](#)
- triangle routes [291](#)
 - allowing through the security policy [293](#)
 - vs virtual interfaces [291](#)
- Triple Data Encryption Standard, see 3DES
- troubleshooting [560, 566, 583](#)
 - admin user [587](#)
 - bandwidth limit [585](#)
 - certificate [587](#)
 - configuration file [588](#)
 - connection resets [586](#)
 - DDNS [585](#)

- device access [583](#)
- ext-user [586](#)
- firmware upload [589](#)
- HTTP redirect [586](#)
- interface [584](#)
- Internet access [583, 586](#)
- LEDs [583](#)
- logo [588](#)
- logs [588](#)
- management access [588](#)
- packet capture [589](#)
- policy route [584](#)
- PPP [585](#)
- RADIUS server [586](#)
- routing [585](#)
- schedules [587](#)
- security policy [584](#)
- security settings [584](#)
- shell scripts [588](#)
- SNAT [585](#)
- throughput rate [588](#)
- VLAN [585](#)
- trunks [155, 195](#)
 - and ALG [239](#)
 - and policy routes [195, 210](#)
 - member interface mode [200, 202](#)
 - member interfaces [200, 202](#)
 - see also load balancing [195](#)
- Trusted Certificates, see also certificates [477](#)
- tunnel encapsulation [344](#)

U

- UDP [447](#)
 - messages [447](#)
 - port numbers [447](#)
- Universal Plug and Play [241](#)
 - Application [241](#)
 - security issues [242](#)
- unsafe web pages [386](#)
- updating
 - signatures [134](#)
- upgrading
 - firmware [555](#)
- uploading
 - configuration files [555](#)
 - firmware [555](#)

- shell scripts [557](#)
- UPnP [241](#)
- usage
 - CPU [84, 86](#)
 - flash [84](#)
 - memory [84, 86](#)
 - onboard flash [84](#)
 - sessions [85, 87](#)
- USB storage
 - status [106](#)
- user authentication [399](#)
 - external [400](#)
 - local user database [459](#)
- user awareness [401](#)
- User Datagram Protocol, see UDP
- user group objects [399](#)
- user groups [399, 401](#)
 - and bandwidth management [371, 374](#)
 - and content filtering [381](#)
 - and policy routes [209](#)
 - and security policy [296, 299](#)
- user name
 - rules [402](#)
- user objects [399](#)
- user sessions, see sessions
- user-aware [264](#)
- users [399](#)
 - access, see also access users
 - admin (type) [399](#)
 - admin, see also admin users
 - and AAA servers [400](#)
 - and authentication method objects [400](#)
 - and bandwidth management [371, 374](#)
 - and content filtering [381](#)
 - and LDAP [400](#)
 - and policy routes [209](#)
 - and RADIUS [400](#)
 - and security policy [296, 299](#)
 - and service control [501](#)
 - and shell scripts [413](#)
 - attributes for Ext-User [400](#)
 - attributes for RADIUS [413](#)
 - attributes in AAA servers [413](#)
 - currently logged in [83, 89](#)
 - default lease time [408, 410](#)
 - default reauthentication time [408, 410](#)
 - default type for Ext-User [400](#)
 - ext-group-user (type) [399](#)

- Ext-User (type) [400](#)
- ext-user (type) [399](#)
- groups, see user groups
- guest-manager (type) [400](#)
- lease time [404](#)
- limited-admin (type) [399](#)
- lockout [409](#)
- reauthentication time [404](#)
- types of [399](#)
- user names [402](#)

V

- Vantage Report (VRPT) [545](#)
- virtual interfaces [155, 189](#)
 - basic characteristics [155](#)
 - not DHCP clients [191](#)
 - types of [189](#)
 - vs asymmetrical routes [291](#)
 - vs triangle routes [291](#)
- Virtual Local Area Network, see VLAN.
- Virtual Private Network, see VPN
- VLAN [174](#)
 - advantages [175](#)
 - and MAC address [174](#)
 - ID [174](#)
 - troubleshooting [585](#)
- VLAN interfaces [155, 175](#)
 - and Ethernet interfaces [175, 585](#)
 - basic characteristics [155](#)
 - virtual [189](#)
- VoIP pass through
 - see also ALG [239](#)
- VPN [338](#)
 - active protocol [359](#)
 - and NAT [358](#)
 - IKE SA, see IKE SA
 - IPSec [338](#)
 - IPSec SA
 - proposal [355](#)
 - security associations (SA) [339](#)
 - see also IKE SA
 - see also IPSec [338](#)
 - see also IPSec SA
 - status [88](#)
- VPN 1-1 mapping [226](#)
 - and policy routes [227](#)

- and security policy [227](#)
 - example [226](#)
 - introduction [226](#)
 - packet flow [226](#)
 - pool profile [229](#)
- VPN connections
- and address objects [339](#)
- VPN gateways
- and certificates [340](#)
 - and extended authentication [339](#)
 - and interfaces [339](#)
- VRPT (Vantage Report) [545](#)
- ## W
- warranty [603](#)
- note [603](#)
- Web Configurator [21](#)
- access [23](#)
 - access users [410](#)
 - requirements [22](#)
 - supported browsers [22](#)
- web features
- ActiveX [390](#)
 - cookies [390](#)
 - Java [390](#)
 - web proxy servers [390](#)
- web proxy servers [232](#), [390](#)
- see also HTTP redirect
- weighted round robin (for load balancing) [197](#)
- WEP (Wired Equivalent Privacy) [415](#)
- Wi-Fi Protected Access [415](#)
- Windows Internet Naming Service, see WINS
- Windows Internet Naming Service, see WINS.
- WINS [164](#), [180](#), [188](#), [193](#)
- WINS server [164](#)
- Wizard Setup [50](#), [64](#)
- WPA [415](#)
- WPA2 [415](#)
- WWW [502](#)
- and address groups [506](#)
 - and address objects [506](#)
 - and authentication method objects [505](#)
 - and certificates [504](#)
 - and zones [506](#)
- see also HTTP, HTTPS [502](#)
- ## Z
- ZON Utility [531](#)
- zones [395](#)
- and FTP [525](#)
 - and interfaces [395](#)
 - and security policy [290](#), [294](#)
 - and SNMP [528](#)
 - and SSH [521](#)
 - and Telnet [524](#)
 - and WWW [506](#)
 - extra-zone traffic [396](#)
 - inter-zone traffic [396](#)
 - intra-zone traffic [396](#)
 - types of traffic [395](#)