ZYXEL
Your Networking Ally

# User's Guide

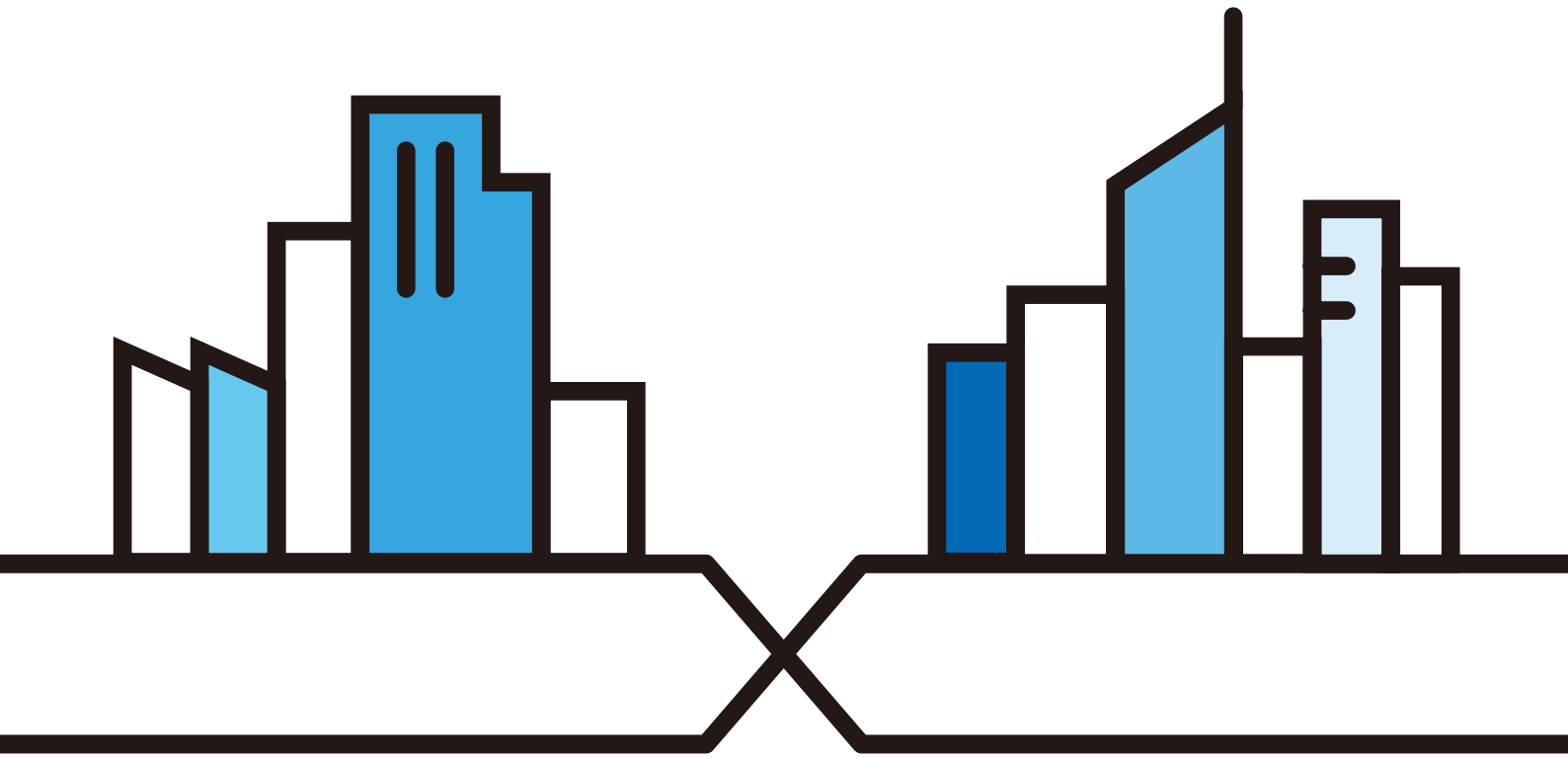
# UAG Series

## UAG2100 / UAG4100 / UAG5100

## Unified Access Gateway

| Default Login Details | |
|---|---|
| LAN IP Address 1 | http://172.16.0.1 |
| LAN IP Address 2 | http://172.17.0.1 |
| User Name | admin |
| Password | 1234 |

Version 4.15 Edition 1, 12/2016



Copyright © 2016 Zyxel Communications Corporation

**IMPORTANT!**

**READ CAREFULLY BEFORE USE.**

**KEEP THIS GUIDE FOR FUTURE REFERENCE.**

This is a User's Guide for a series of products. Not all products support all firmware features. 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.

- Web Configurator Online Help

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

- More Information

  Go to **support.zyxel.com** to find other information on the UAG.

# Contents Overview

Introduction ..... 20
Hardware Installation and Connection ..... 36
Printer Deployment ..... 42
Installation Setup Wizard ..... 50
Quick Setup Wizards ..... 64
Dashboard ..... 80
Monitor ..... 92
Licensing ..... 136
Wireless ..... 141
Interfaces ..... 169
Trunks ..... 210
Policy and Static Routes ..... 218
DDNS ..... 229
NAT ..... 234
VPN 1-1 Mapping ..... 241
HTTP Redirect ..... 246
SMTP Redirect ..... 250
ALG ..... 254
UPnP ..... 256
IP/MAC Binding ..... 263
Layer 2 Isolation ..... 268
IPnP ..... 272
Web Authentication ..... 274
Security Policy ..... 300
Billing ..... 314
Printer ..... 332
Free Time ..... 342
SMS ..... 346
IPSec VPN ..... 348
Bandwidth Management ..... 375
Application Patrol ..... 385
Content Filtering ..... 390
Zones ..... 404
User/Group ..... 408
AP Profile ..... 423
MON Profile ..... 439
Application ..... 444
Addresses ..... 451
Service ..... 456

Schedules ..... 462
AAA Server ..... 468
Authentication Method ..... 473
Certificates ..... 476
ISP Accounts ..... 492
System ..... 495
Log and Report ..... 543
File Manager ..... 558
Diagnostics ..... 568
Packet Flow Explore ..... 581
Reboot ..... 590
Shutdown ..... 591
Troubleshooting ..... 592

# 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 ..... 27
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 ..... 87

6.2.3 The Active Sessions Screen ..... 87
6.2.4 The VPN Status Screen ..... 88
6.2.5 The DHCP Table Screen ..... 89
6.2.6 The Number of Login Users Screen ..... 90

**Chapter 7**
**Monitor ..... 92**

7.1 Overview ..... 92
7.1.1 What You Can Do in this Chapter ..... 92
7.2 The Port Statistics Screen ..... 93
7.2.1 The Port Statistics Graph Screen ..... 94
7.3 The Interface Status Screen ..... 95
7.4 The Traffic Statistics Screen ..... 98
7.5 The Session Monitor Screen ..... 100
7.6 The DDNS Status Screen ..... 102
7.7 The IP/MAC Binding Monitor Screen ..... 102
7.8 The Login Users Screen ..... 103
7.9 The Dynamic Guest Screen ..... 104
7.10 The UPnP Port Status Screen ..... 106
7.11 The USB Storage Screen ..... 107
7.12 The Ethernet Neighbor Screen ..... 108
7.13 The AP List Screen ..... 110
7.13.1 Station Count of AP More Information ..... 111
7.13.2 Config AP ..... 113
7.14 The Radio List Screen ..... 117
7.14.1 AP Mode Radio Information ..... 119
7.15 The Station List Screen ..... 120
7.16 Detected Device ..... 121
7.17 The Printer Status Screen ..... 123
7.18 The VPN 1-1 Mapping Status Screen ..... 123
7.18.1 VPN 1-1 Mapping Statistics ..... 124
7.19 The IPSec Monitor Screen ..... 125
7.19.1 Regular Expressions in Searching IPSec SAs ..... 126
7.20 TheApp Patrol Screen ..... 126
7.21 TheContent Filter Screen ..... 128
7.22 The Log Screen ..... 129
7.22.1 View AP Log ..... 132
7.22.2 Dynamic Users Log ..... 134

**Chapter 8**
**Licensing ..... 136**

8.1 Overview ..... 136
8.1.1 What You Can Do in this Chapter ..... 136

8.1.2 What you Need to Know ..... 136
8.2 Registration Screen ..... 137
8.3 Service Screen ..... 137
8.4 App Patrol Signature Update Screen ..... 138

**Chapter 9**
**Wireless ..... 141**

9.1 Overview ..... 141
9.1.1 What You Can Do in this Chapter ..... 141
9.1.2 What You Need to Know ..... 141
9.2 Controller Screen ..... 142
9.3 AP Management Screen ..... 143
9.3.1 Add/Edit AP List ..... 145
9.3.2 Port Setting Edit ..... 148
9.3.3 VLAN Add/Edit ..... 148
9.3.4 AP Policy ..... 150
9.3.5 AP Group ..... 151
9.3.6 AP Group Add/Edit ..... 152
9.3.7 Firmware ..... 158
9.4 MON Mode ..... 160
9.4.1 Add/Edit Rogue/Friendly List ..... 161
9.5 Auto Healing ..... 162
9.6 RTLS ..... 163
9.6.1 Before You Begin ..... 164
9.7 Technical Reference ..... 165
9.7.1 Dynamic Channel Selection ..... 165
9.7.2 Disassociating and Delaying Connections ..... 166
9.7.3 Load Balancing ..... 167

**Chapter 10**
**Interfaces ..... 169**

10.1 Interface Overview ..... 169
10.1.1 What You Can Do in this Chapter ..... 169
10.1.2 What You Need to Know ..... 169
10.2 Port Role Screen ..... 171
10.3 Ethernet Screen ..... 172
10.3.1 Ethernet Edit ..... 174
10.3.2 Object References ..... 180
10.3.3 Add/Edit DHCP Extended Options ..... 181
10.4 PPP Interfaces ..... 183
10.4.1 PPP Interface Summary ..... 184
10.4.2 PPP Interface Add or Edit ..... 185
10.5 VLAN Interfaces ..... 189

10.5.1 VLAN Interface Summary Screen ..... 190
10.5.2 VLAN Interface Add/Edit ..... 191
10.6 Bridge Interfaces ..... 196
10.6.1 Bridge Interface Summary ..... 198
10.6.2 Bridge Interface Add/Edit ..... 199
10.7 Virtual Interfaces ..... 204
10.7.1 Virtual Interfaces Add/Edit ..... 204
10.8 Interface Technical Reference ..... 206

**Chapter 11**
**Trunks ..... 210**

11.1 Overview ..... 210
11.1.1 What You Can Do in this Chapter ..... 210
11.1.2 What You Need to Know ..... 210
11.2 The Trunk Screen ..... 213
11.2.1 Configuring a User-Defined Trunk ..... 214
11.2.2 Configuring the System Default Trunk ..... 216

**Chapter 12**
**Policy and Static Routes ..... 218**

12.1 Policy and Static Routes Overview ..... 218
12.1.1 What You Can Do in this Chapter ..... 218
12.1.2 What You Need to Know ..... 218
12.2 Policy Route Screen ..... 220
12.2.1 Policy Route Add/Edit Screen ..... 222
12.3 IP Static Route Screen ..... 226
12.3.1 Static Route Add/Edit Screen ..... 226
12.4 Policy Routing Technical Reference ..... 227

**Chapter 13**
**DDNS ..... 229**

13.1 DDNS Overview ..... 229
13.1.1 What You Can Do in this Chapter ..... 229
13.1.2 What You Need to Know ..... 229
13.2 The DDNS Screen ..... 230
13.2.1 The Dynamic DNS Add/Edit Screen ..... 231

**Chapter 14**
**NAT ..... 234**

14.1 NAT Overview ..... 234
14.1.1 What You Can Do in this Chapter ..... 234
14.1.2 What You Need to Know ..... 234
14.2 The NAT Screen ..... 235

14.2.1 The NAT Add/Edit Screen ..... 236
14.3 NAT Technical Reference ..... 239

**Chapter 15**
**VPN 1-1 Mapping ..... 241**

15.1 VPN 1-1 Mapping Overview ..... 241
15.1.1 What You Can Do in this Chapter ..... 241
15.1.2 What You Need to Know ..... 242
15.2 The VPN 1-1 Mapping General Screen ..... 242
15.2.1 The VPN 1-1 Mapping Edit Screen ..... 243
15.3 The VPN 1-1 Mapping Profile Screen ..... 244

**Chapter 16**
**HTTP Redirect ..... 246**

16.1 Overview ..... 246
16.1.1 What You Can Do in this Chapter ..... 246
16.1.2 What You Need to Know ..... 246
16.2 The HTTP Redirect Screen ..... 247
16.2.1 The HTTP Redirect Add/Edit Screen ..... 248

**Chapter 17**
**SMTP Redirect ..... 250**

17.1 Overview ..... 250
17.1.1 What You Can Do in this Chapter ..... 250
17.1.2 What You Need to Know ..... 250
17.2 The SMTP Redirect Screen ..... 251
17.2.1 The SMTP Redirect Edit Screen ..... 252

**Chapter 18**
**ALG ..... 254**

18.1 ALG Overview ..... 254
18.1.1 What You Can Do in this Chapter ..... 254
18.1.2 What You Need to Know ..... 254
18.1.3 Before You Begin ..... 255
18.2 The ALG Screen ..... 255

**Chapter 19**
**UPnP ..... 256**

19.1 Overview ..... 256
19.2 What You Need to Know ..... 256
19.2.1 NAT Traversal ..... 256
19.2.2 Cautions with UPnP ..... 257
19.3 UPnP Screen ..... 257

19.4 Technical Reference ..... 258
19.4.1 Using UPnP in Windows XP Example ..... 258
19.4.2 Web Configurator Easy Access ..... 260

**Chapter 20**
**IP/MAC Binding ..... 263**

20.1 IP/MAC Binding Overview ..... 263
20.1.1 What You Can Do in this Chapter ..... 263
20.1.2 What You Need to Know ..... 263
20.2 IP/MAC Binding Summary Screen ..... 264
20.2.1 IP/MAC Binding Edit ..... 265
20.2.2 Static DHCP Edit ..... 266
20.3 IP/MAC Binding Exempt List ..... 266

**Chapter 21**
**Layer 2 Isolation ..... 268**

21.1 Overview ..... 268
21.1.1 What You Can Do in this Chapter ..... 268
21.2 Layer-2 Isolation General Screen ..... 269
21.3 White List Screen ..... 269
21.3.1 Add/Edit White List Rule ..... 270

**Chapter 22**
**IPnP ..... 272**

22.1 Overview ..... 272
22.1.1 What You Can Do in this Chapter ..... 272
22.2 IPnP Screen ..... 273

**Chapter 23**
**Web Authentication ..... 274**

23.1 Overview ..... 274
23.1.1 What You Can Do in this Chapter ..... 274
23.1.2 What You Need to Know ..... 275
23.2 Web Authentication ..... 275
23.2.1 General Screen ..... 275
23.2.2 User-aware Access Control Example ..... 279
23.2.3 Authentication Type Screen ..... 285
23.2.4 Custom Web Portal / User Agreement File Screen ..... 290
23.3 Walled Garden ..... 291
23.3.1 General Screen ..... 292
23.3.2 URL Base Screen ..... 292
23.3.3 Domain/IP Base Screen ..... 294
23.3.4 Walled Garden Login Example ..... 296

23.4 Advertisement Screen ..... 297
23.4.1 Adding/Editing an Advertisement URL ..... 298

**Chapter 24**
**Security Policy ..... 300**

24.1 Overview ..... 300
24.1.1 What You Can Do in this Chapter ..... 300
24.1.2 What You Need to Know ..... 301
24.2 Security Policy Control Screen ..... 302
24.2.1 Configuring the Security Policy Control Screen ..... 303
24.2.2 Add/Edit Policy Control Rule ..... 305
24.3 Session Control Screen ..... 307
24.3.1 Add/Edit a Session Limit Rule ..... 309
24.4 Security Policy Configuration Example ..... 310
24.5 Security Policy Example Applications ..... 312

**Chapter 25**
**Billing ..... 314**

25.1 Overview ..... 314
25.1.1 What You Can Do in this Chapter ..... 314
25.1.2 What You Need to Know ..... 314
25.2 The General Screen ..... 314
25.3 The Billing Profile Screen ..... 316
25.3.1 The Account Generator Screen ..... 318
25.3.2 The Account Redeem Screen ..... 321
25.3.3 The Billing Profile Add/Edit Screen ..... 323
25.4 The Discount Screen ..... 324
25.4.1 The Discount Add/Edit Screen ..... 326
25.5 The Payment Service General Screen ..... 326
25.5.1 The Payment Service Desktop View / Mobile View Screen ..... 328

**Chapter 26**
**Printer ..... 332**

26.1 Overview ..... 332
26.1.1 What You Can Do in this Chapter ..... 332
26.2 The General Setting Screen ..... 332
26.2.1 Add/Edit Printer Rule ..... 334
26.3 The Printout Configuration Screen ..... 335
26.4 The Printer Manager Screen ..... 336
26.4.1 Edit Printer Manager ..... 337
26.4.2 Reports Overview ..... 338
26.4.3 Key Combinations ..... 338
26.4.4 Daily Account Summary ..... 338

26.4.5 Monthly Account Summary ..... 339
26.4.6 Account Report Notes ..... 340
26.4.7 System Status ..... 340

**Chapter 27**
**Free Time ..... 342**

27.1 Overview ..... 342
27.1.1 What You Can Do in this Chapter ..... 342
27.2 The Free Time Screen ..... 342

**Chapter 28**
**SMS ..... 346**

28.1 Overview ..... 346
28.1.1 What You Can Do in this Chapter ..... 346
28.2 The SMS Screen ..... 346

**Chapter 29**
**IPSec VPN ..... 348**

29.1 Virtual Private Networks (VPN) Overview ..... 348
29.1.1 What You Can Do in this Chapter ..... 348
29.1.2 What You Need to Know ..... 349
29.1.3 Before You Begin ..... 349
29.2 The VPN Connection Screen ..... 350
29.2.1 The VPN Connection Add/Edit Screen ..... 351
29.3 The VPN Gateway Screen ..... 357
29.3.1 The VPN Gateway Add/Edit Screen ..... 358
29.4 IPSec VPN Background Information ..... 364

**Chapter 30**
**Bandwidth Management ..... 375**

30.1 Overview ..... 375
30.1.1 What You Can Do in this Chapter ..... 375
30.1.2 What You Need to Know ..... 375
30.2 The Bandwidth Management Screen ..... 379
30.2.1 The Bandwidth Management Add/Edit Screen ..... 381

**Chapter 31**
**Application Patrol ..... 385**

31.1 Overview ..... 385
31.1.1 What You Can Do in this Chapter ..... 385
31.1.2 What You Need to Know ..... 385
31.2 Application Patrol Profile ..... 386
31.2.1 Add/Edit Application Patrol Profile ..... 387

31.2.2 Add/Edit Application Patrol Profile Rule Application ..... 388

**Chapter 32**
**Content Filtering ..... 390**

32.1 Overview ..... 390
32.1.1 What You Can Do in this Chapter ..... 390
32.1.2 What You Need to Know ..... 390
32.1.3 Before You Begin ..... 391
32.2 Content Filter Profile Screen ..... 392
32.2.1 Add/Edit Content Filter Profile ..... 394
32.3 Content Filter Trusted Web Sites Screen ..... 400
32.4 Content Filter Forbidden Web Sites Screen ..... 401
32.5 Content Filter Technical Reference ..... 402

**Chapter 33**
**Zones ..... 404**

33.1 Zones Overview ..... 404
33.1.1 What You Can Do in this Chapter ..... 404
33.1.2 What You Need to Know ..... 405
33.2 The Zone Screen ..... 405
33.2.1 Add/Edit Zone ..... 406

**Chapter 34**
**User/Group ..... 408**

34.1 Overview ..... 408
34.1.1 What You Can Do in this Chapter ..... 408
34.1.2 What You Need To Know ..... 408
34.2 User Summary Screen ..... 410
34.2.1 User Add/Edit Screen ..... 411
34.3 User Group Summary Screen ..... 414
34.3.1 Group Add/Edit Screen ..... 414
34.4 User/Group Setting Screen ..... 415
34.4.1 Default User Settings Edit Screens ..... 418
34.4.2 User Aware Login Example ..... 419
34.5 MAC Address Screen ..... 420
34.5.1 Add/Edit MAC Address ..... 421
34.6 User /Group Technical Reference ..... 421

**Chapter 35**
**AP Profile ..... 423**

35.1 Overview ..... 423
35.1.1 What You Can Do in this Chapter ..... 423
35.1.2 What You Need To Know ..... 423

35.2 Radio Screen ..... 424
35.2.1 Add/Edit Radio Profile ..... 426
35.3 SSID Screen ..... 430
35.3.1 SSID List ..... 430
35.3.2 Add/Edit SSID Profile ..... 431
35.3.3 Security List ..... 433
35.3.4 Add/Edit Security Profile ..... 434
35.3.5 MAC Filter List ..... 437
35.3.6 Add/Edit MAC Filter Profile ..... 437

**Chapter 36**
**MON Profile ..... 439**

36.1 Overview ..... 439
36.1.1 What You Can Do in this Chapter ..... 439
36.1.2 What You Need To Know ..... 439
36.2 MON Profile ..... 439
36.2.1 Add/Edit MON Profile ..... 440
36.3 Technical Reference ..... 442

**Chapter 37**
**Application ..... 444**

37.1 Overview ..... 444
37.1.1 What You Can Do in this Chapter ..... 445
37.2 Application Screen ..... 445
37.2.1 Add Application Rule ..... 446
37.3 Application Group Screen ..... 449
37.3.1 Add Application Group Rule ..... 450

**Chapter 38**
**Addresses ..... 451**

38.1 Overview ..... 451
38.1.1 What You Can Do in this Chapter ..... 451
38.1.2 What You Need To Know ..... 451
38.2 Address Summary Screen ..... 451
38.2.1 Address Add/Edit Screen ..... 452
38.3 Address Group Summary Screen ..... 453
38.3.1 Address Group Add/Edit Screen ..... 454

**Chapter 39**
**Service ..... 456**

39.1 Overview ..... 456
39.1.1 What You Can Do in this Chapter ..... 456
39.1.2 What You Need to Know ..... 456

39.2 The Service Summary Screen ..... 457
39.2.1 The Service Add/Edit Screen ..... 458
39.3 The Service Group Summary Screen ..... 459
39.3.1 The Service Group Add/Edit Screen ..... 460

**Chapter 40**
**Schedules ..... 462**

40.1 Overview ..... 462
40.1.1 What You Can Do in this Chapter ..... 462
40.1.2 What You Need to Know ..... 462
40.2 The Schedule Summary Screen ..... 463
40.2.1 The One-Time Schedule Add/Edit Screen ..... 464
40.2.2 The Recurring Schedule Add/Edit Screen ..... 465
40.3 The Schedule Group Summary Screen ..... 466
40.3.1 The Schedule Group Add/Edit Screen ..... 466

**Chapter 41**
**AAA Server ..... 468**

41.1 Overview ..... 468
41.1.1 RADIUS Server ..... 468
41.1.2 What You Can Do in this Chapter ..... 468
41.1.3 What You Need To Know ..... 468
41.2 RADIUS Server Summary ..... 469
41.2.1 Adding/Editing a RADIUS Server ..... 470

**Chapter 42**
**Authentication Method ..... 473**

42.1 Overview ..... 473
42.1.1 What You Can Do in this Chapter ..... 473
42.1.2 Before You Begin ..... 473
42.2 Authentication Method Objects ..... 473
42.2.1 Creating an Authentication Method Object ..... 474

**Chapter 43**
**Certificates ..... 476**

43.1 Overview ..... 476
43.1.1 What You Can Do in this Chapter ..... 476
43.1.2 What You Need to Know ..... 476
43.1.3 Verifying a Certificate ..... 478
43.2 The My Certificates Screen ..... 479
43.2.1 The My Certificates Add Screen ..... 480
43.2.2 The My Certificates Edit Screen ..... 482
43.2.3 The My Certificates Import Screen ..... 485

43.3 The Trusted Certificates Screen ..... 486
43.3.1 The Trusted Certificates Edit Screen ..... 487
43.3.2 The Trusted Certificates Import Screen ..... 490

**Chapter 44**
**ISP Accounts ..... 492**

44.1 Overview ..... 492
44.1.1 What You Can Do in this Chapter ..... 492
44.2 ISP Account Summary ..... 492
44.2.1 ISP Account Add/Edit ..... 493

**Chapter 45**
**System ..... 495**

45.1 Overview ..... 495
45.1.1 What You Can Do in this Chapter ..... 495
45.2 Host Name ..... 496
45.3 USB Storage ..... 496
45.4 Date and Time ..... 497
45.4.1 Pre-defined NTP Time Servers List ..... 500
45.4.2 Time Server Synchronization ..... 500
45.5 Console Port Speed ..... 501
45.6 DNS Overview ..... 502
45.6.1 DNS Server Address Assignment ..... 502
45.6.2 Configuring the DNS Screen ..... 502
45.6.3 Address Record ..... 505
45.6.4 PTR Record ..... 505
45.6.5 Adding an Address/PTR Record ..... 505
45.6.6 CNAME Record ..... 506
45.6.7 Adding a CNAME Record ..... 506
45.6.8 Domain Zone Forwarder ..... 507
45.6.9 Adding a Domain Zone Forwarder ..... 507
45.6.10 MX Record ..... 508
45.6.11 Adding a MX Record ..... 508
45.6.12 Adding a DNS Service Control Rule ..... 509
45.7 WWW Overview ..... 510
45.7.1 Service Access Limitations ..... 510
45.7.2 System Timeout ..... 510
45.7.3 HTTPS ..... 510
45.7.4 Configuring WWW Service Control ..... 511
45.7.5 Service Control Rules ..... 514
45.7.6 Customizing the WWW Login Page ..... 515
45.7.7 HTTPS Example ..... 520
45.8 SSH ..... 527

45.8.1 How SSH Works ..... 528
45.8.2 SSH Implementation on the UAG ..... 529
45.8.3 Requirements for Using SSH ..... 529
45.8.4 Configuring SSH ..... 529
45.8.5 Secure Telnet Using SSH Examples ..... 530
45.9 Telnet ..... 532
45.9.1 Configuring Telnet ..... 532
45.10 FTP ..... 533
45.10.1 Configuring FTP ..... 533
45.11 SNMP ..... 534
45.11.1 Supported MIBs ..... 535
45.11.2 SNMP Traps ..... 536
45.11.3 Configuring SNMP ..... 536
45.12 Authentication Server ..... 537
45.12.1 Add/Edit Trusted RADIUS Client ..... 539
45.13 Language ..... 540
45.14 Zyxel One Network (ZON) Utility ..... 540
45.14.1 Zyxel One Network (ZON) System Screen ..... 541

**Chapter 46**
**Log and Report ..... 543**

46.1 Overview ..... 543
46.1.1 What You Can Do In this Chapter ..... 543
46.2 Email Daily Report ..... 543
46.3 Log Settings Screens ..... 545
46.3.1 Log Settings Summary ..... 546
46.3.2 Edit System Log Settings ..... 547
46.3.3 Edit Log on USB Storage Setting ..... 551
46.3.4 Edit Remote Server Log Settings ..... 552
46.3.5 Log Category Settings Screen ..... 554

**Chapter 47**
**File Manager ..... 558**

47.1 Overview ..... 558
47.1.1 What You Can Do in this Chapter ..... 558
47.1.2 What you Need to Know ..... 558
47.2 The Configuration File Screen ..... 560
47.3 The Firmware Package Screen ..... 564
47.4 The Shell Script Screen ..... 565

**Chapter 48**
**Diagnostics ..... 568**

48.1 Overview ..... 568

48.1.1 What You Can Do in this Chapter ..... 568
48.2 The Diagnostics Screen ..... 568
48.2.1 The Diagnostic Collect on AP Screen ..... 569
48.2.2 The Diagnostics Files Screen ..... 570
48.3 The Packet Capture Screen ..... 571
48.3.1 The Packet Capture Files Screen ..... 574
48.4 The Core Dump Screen ..... 575
48.4.1 The Core Dump Files Screen ..... 575
48.5 The System Log Screen ..... 576
48.6 The Network Tool Screen ..... 577
48.7 The Wireless Frame Capture Screen ..... 578
48.7.1 The Wireless Frame Capture Files Screen ..... 580

**Chapter 49**
**Packet Flow Explore ..... 581**

49.1 Overview ..... 581
49.1.1 What You Can Do in this Chapter ..... 581
49.2 The Routing Status Screen ..... 581
49.3 The SNAT Status Screen ..... 586

**Chapter 50**
**Reboot ..... 590**

50.1 Overview ..... 590
50.1.1 What You Need To Know ..... 590
50.2 The Reboot Screen ..... 590

**Chapter 51**
**Shutdown ..... 591**

51.1 Overview ..... 591
51.1.1 What You Need To Know ..... 591
51.2 The Shutdown Screen ..... 591

**Chapter 52**
**Troubleshooting ..... 592**

52.1 Resetting the UAG ..... 598
52.2 Getting More Troubleshooting Help ..... 598

Appendix A Customer Support ..... 599

Appendix B Legal Information ..... 605

**Index ..... 618**

# CHAPTER 1
# Introduction

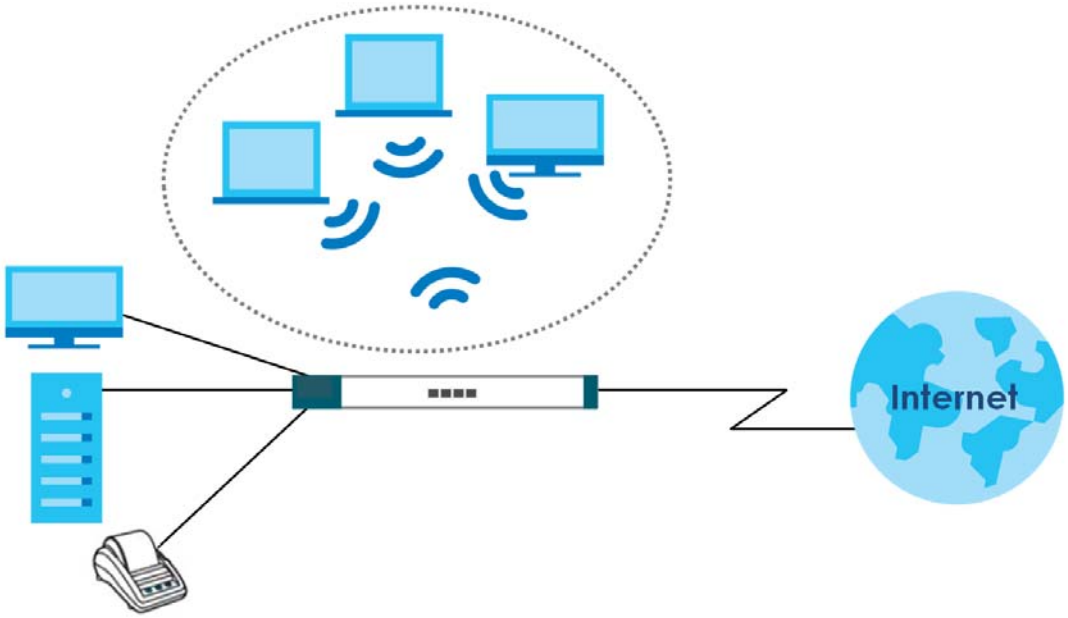
## 1.1 Overview

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 | V | | |
| IPSec VPN (Site-to-Site) | | | V |
| Content Filtering | | | V |
| Application Patrol | | | V |
| Local AP (Built-in Wireless LAN Module) | V | V | |
| Drop-in Mode | | | V |

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.

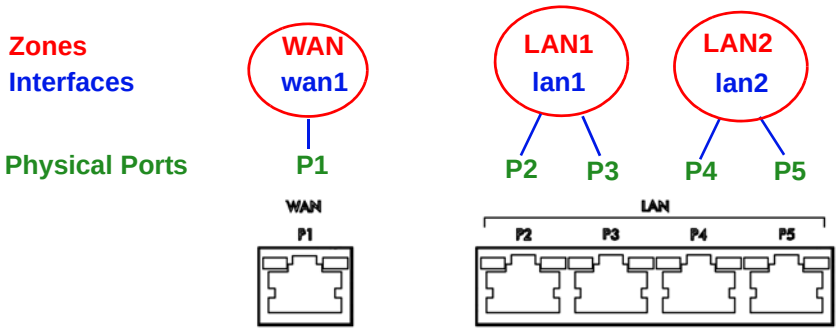
The UAG lets you set up multiple networks for your company. The UAG also provides two separate LAN networks. You can set ports to be part of the LAN1 or LAN2.

# 1.2 Default Zones, Interfaces, and Ports

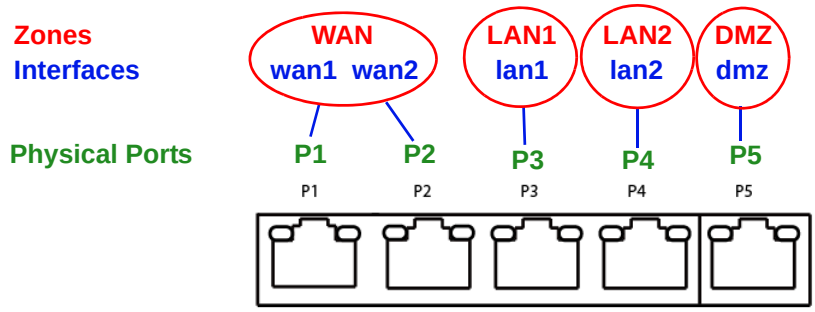
The default configurations for zones, interfaces, and ports are as follows. References to interfaces may be generic rather than the specific name used in your model. For example, this guide may use "the WAN interface" rather than "P1".

**Figure 1** Zones, Interfaces, and Physical Ethernet Ports

**UAG2100 / UAG4100**




**UAG5100**



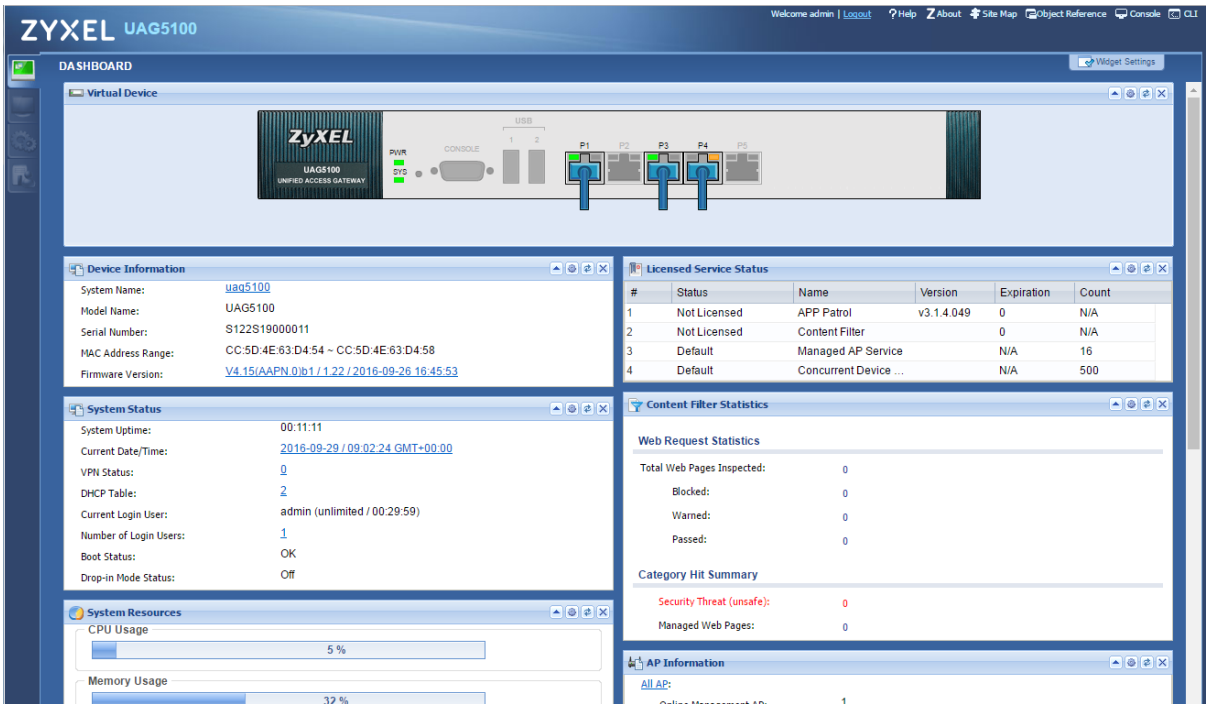

# 1.3 Management Overview

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:

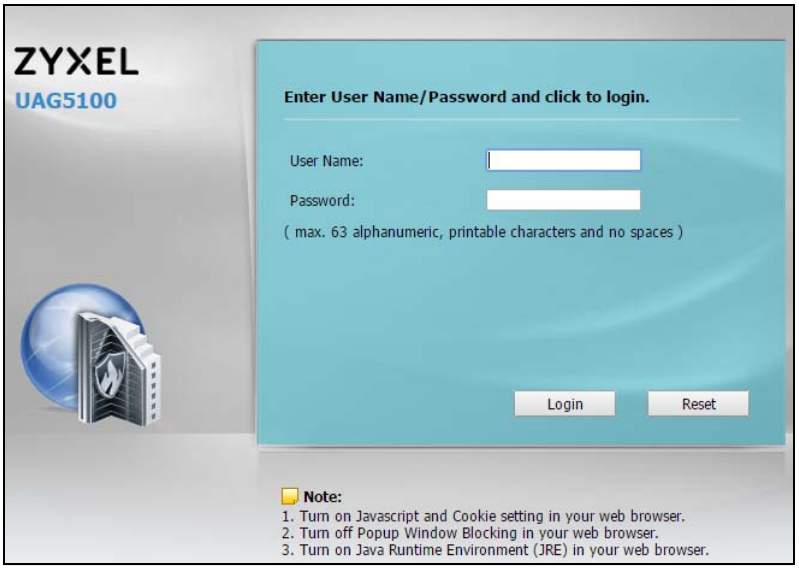
- Use one of the following web browser versions or later: Internet Explorer 6.0, Firefox 8.0, Chrome 14.0, Safari 4.0
- Allow pop-up windows (blocked by default in Windows XP Service Pack 2)
- Enable JavaScripts, Java permissions, and cookies

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.

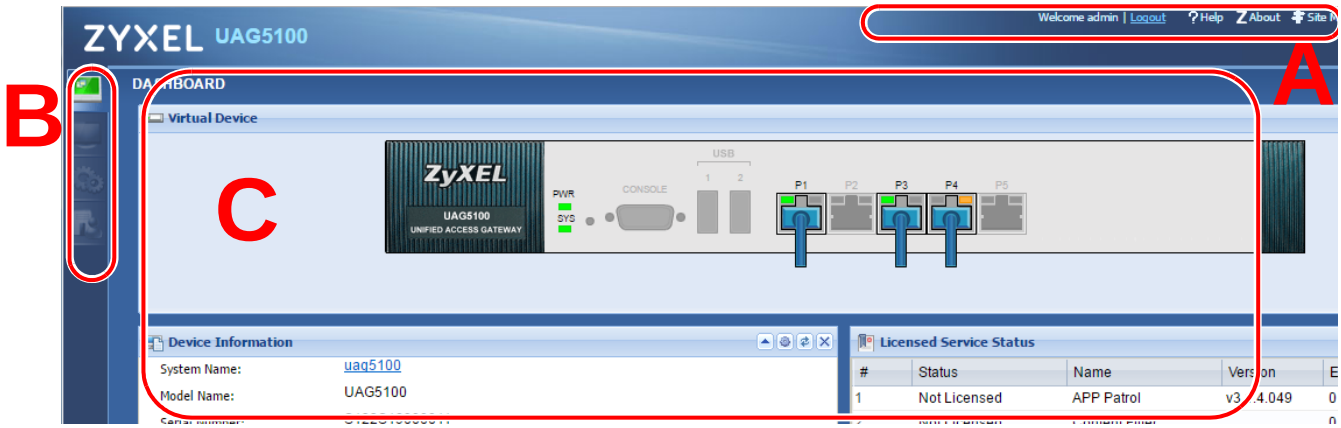
2 In your browser go to http://172.16.0.1 or http://172.17.0.1. The **Login** screen appears.




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.

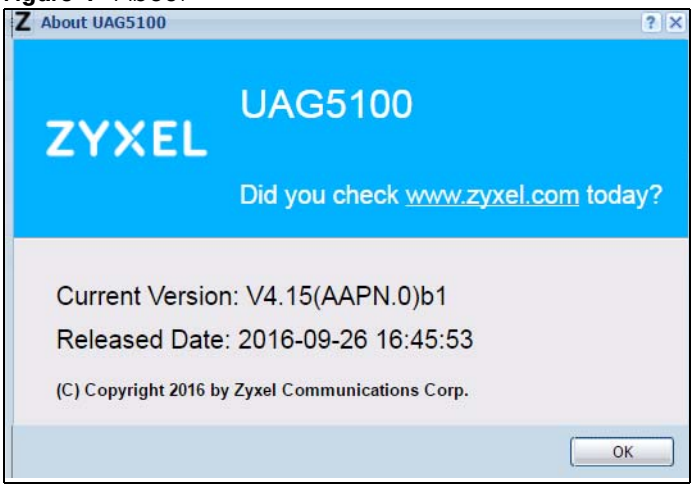
Table 3 Title Bar: Web Configurator Icons

| 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 |
|---|---|
| Current Version | This shows the firmware version of the UAG. |

Table 4 About (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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

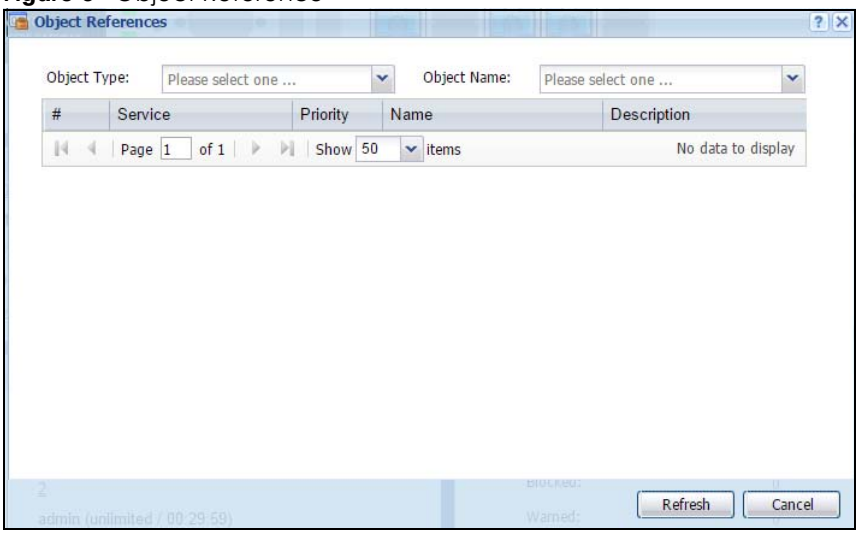
Click **Site MAP** to see an overview of links to the Web Configurator screens. Click a screen's link to go to that screen.

**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.

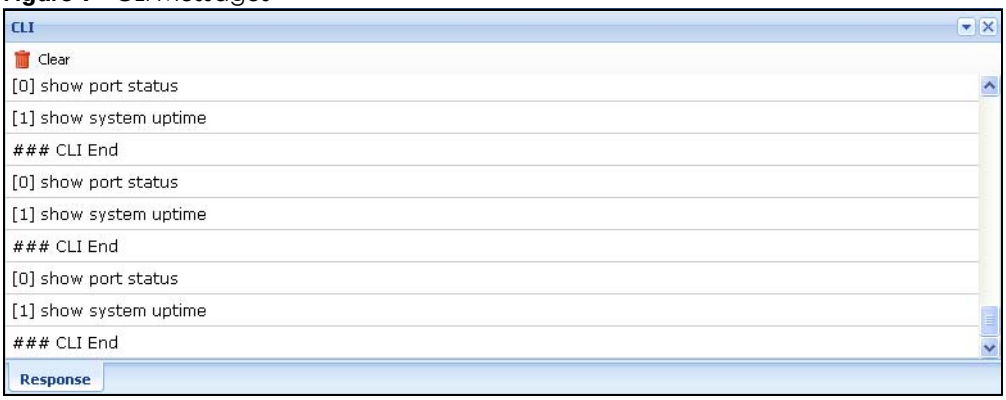
Table 5 Object References

| 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



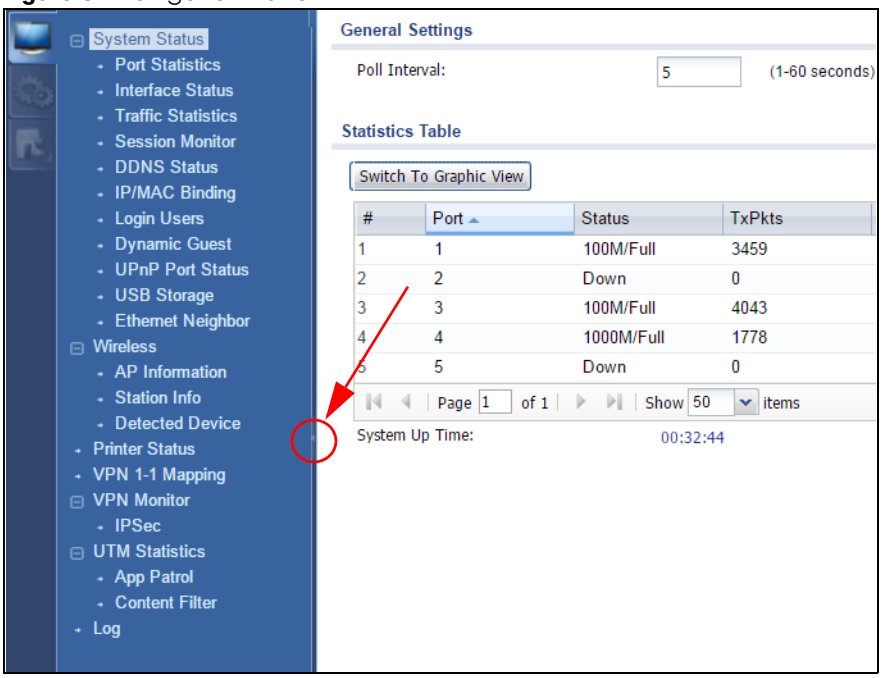

Click **Clear** to remove the currently displayed information.

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. |
| 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 | Mgnt. 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. |
| | AP Group | Create groups of APs, define their radio, VLAN, port and load balancing settings. |
| | Firmware | Update the firmware on APs connected to your UAG. |
| MON Mode | Rogue/Friendly AP List | Configure how the UAG monitors rogue APs. |
| Auto Healing | | Use this screen for the UAG to automatically detect failures and compensate by increasing the wireless coverage of nearby APs. |
| RTLS | Real Time Location System | Use the managed APs as part of an Ekahau RTLS to track the location of Ekahau Wi-Fi tags. |
| 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. |

Table 7 Configuration Menu Screens Summary (continued)

| FOLDER OR LINK | TAB | FUNCTION |
|---|---|---|
| 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. |
| 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. |
| 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 | | Allow users to get a free account for Internet surfing during the specified time period. |
| 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 | | 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. |

Table 7 Configuration Menu Screens Summary (continued)

| FOLDER OR LINK | TAB | FUNCTION |
|---|---|---|
| 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. |
| 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 | | 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

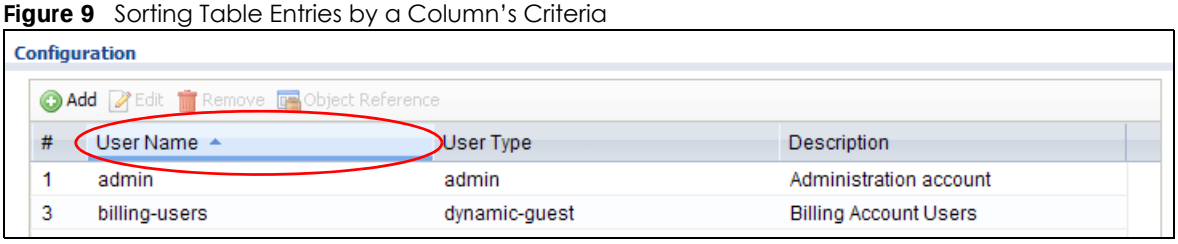
| FOLDER OR LINK | TAB | FUNCTION |
|---|---|---|
| File Manager | Configuration File | Manage and upload configuration files for the UAG. |
| | Firmware Package | View the current firmware version and to upload firmware. |
| | Shell Script | Manage and run shell script files for the UAG. |
| Diagnostics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

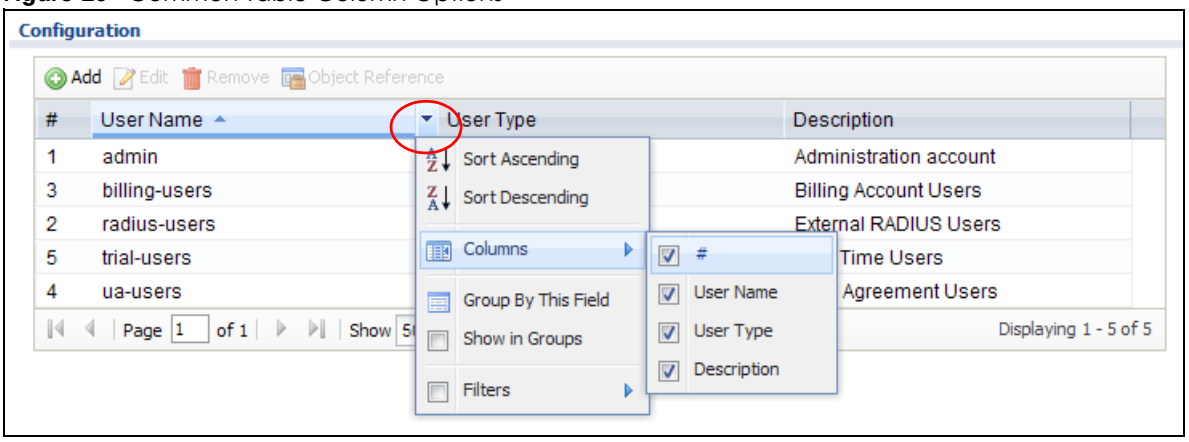



Click the down arrow next to a column heading for more options about how to display the entries. The options available vary depending on the type of fields in the column. Here are some examples of what you can do:

- Sort in ascending or descending (reverse) alphabetical order
- Select which columns to display
- Group entries by field
- Show entries in groups

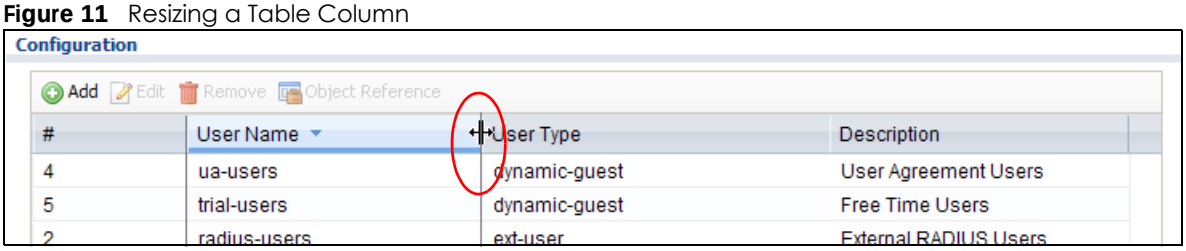
- Filter by mathematical operators (<, >, or =) or searching for text

**Figure 10** Common Table Column Options



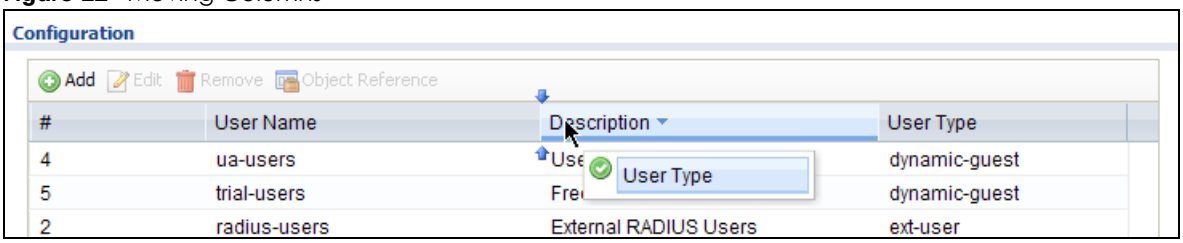

Select a column heading cell's right border and drag to re-size the column.

**Figure 11** Resizing a Table Column



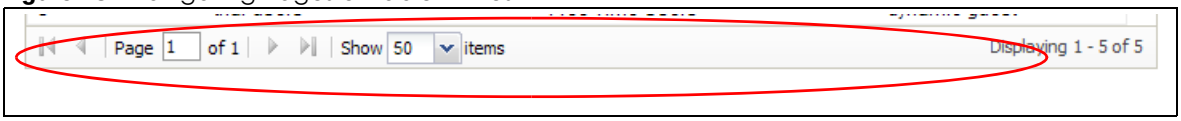

Select a column heading and drag and drop it to change the column order. A green check mark displays next to the column's title when you drag the column to a valid new location.

**Figure 12** Moving Columns



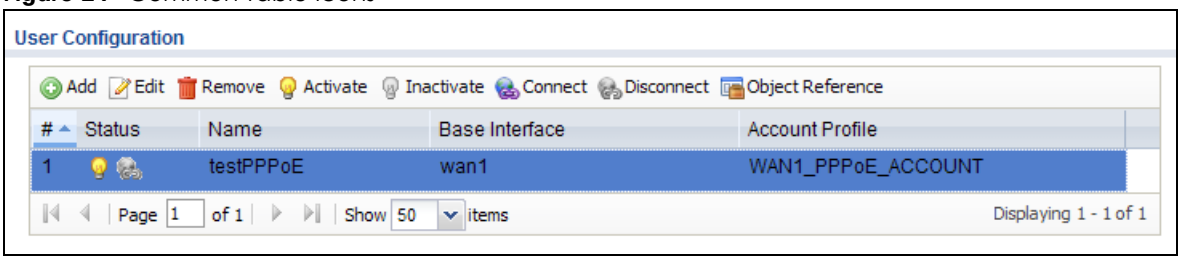

Use the icons and fields at the bottom of the table to navigate to different pages of entries and control how many entries display at a time.

**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.

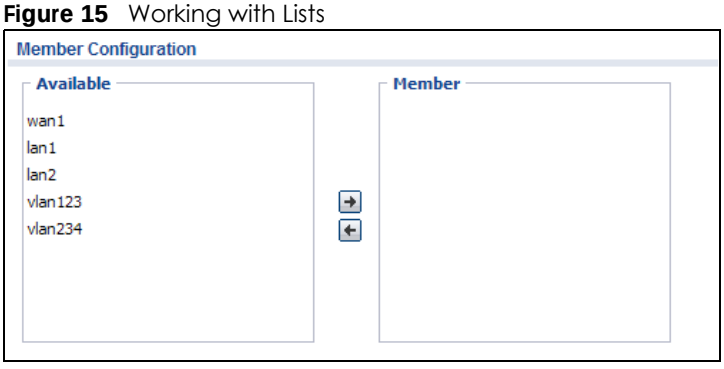
Table 9 Common Table Icons

| 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.

# CHAPTER 2
# 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.

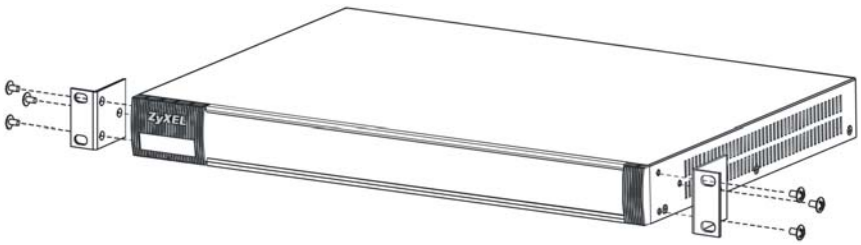
Note: Leave 10 cm of clearance at the sides and 20 cm in the rear.

Use a #2 Phillips screwdriver to install the screws.

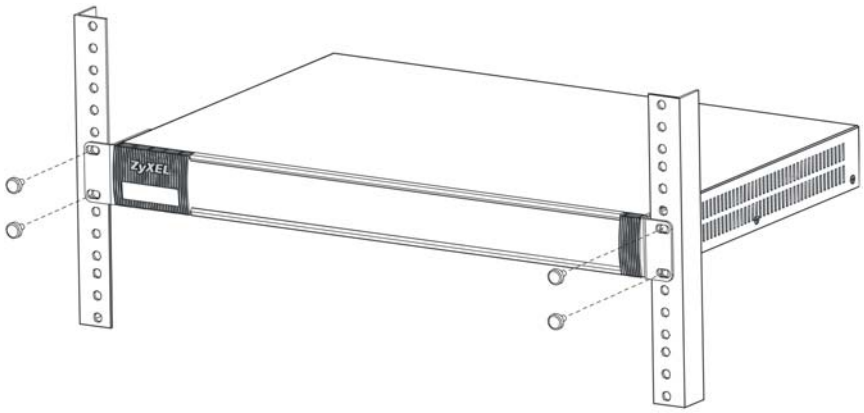
Note: Failure to use the proper screws may damage the unit.

**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.**

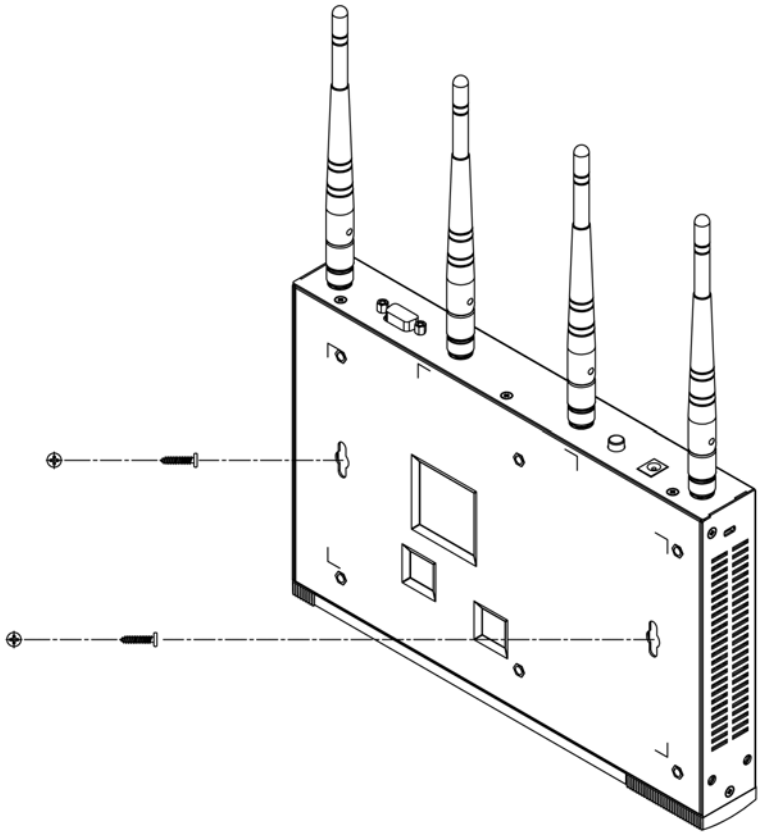
3 If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do not insert the screws all the way in - leave a small gap of about 0.5 cm.

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

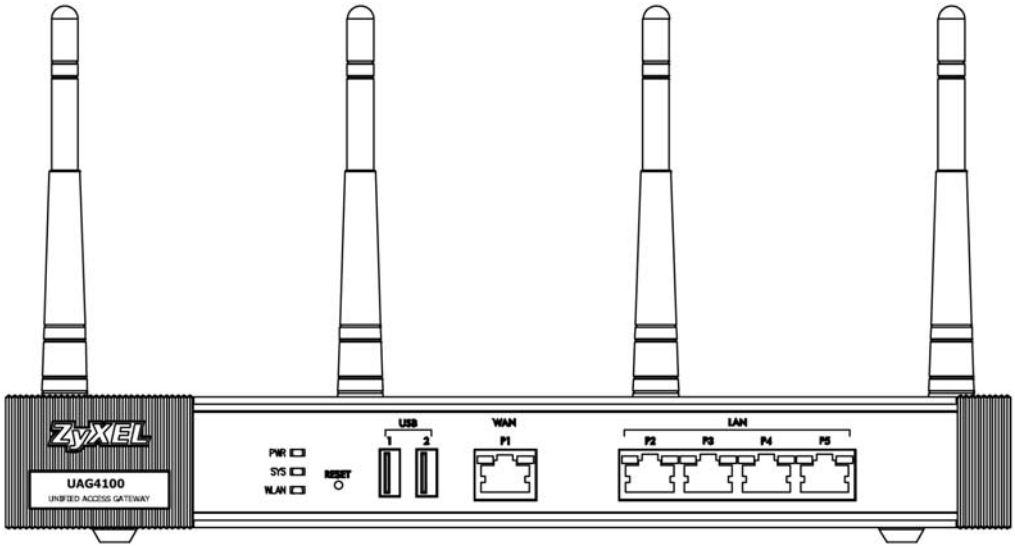
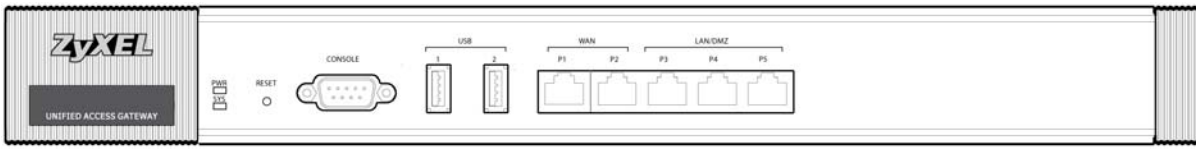


**Figure 18** Front Panel: UAG5100




### 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. |

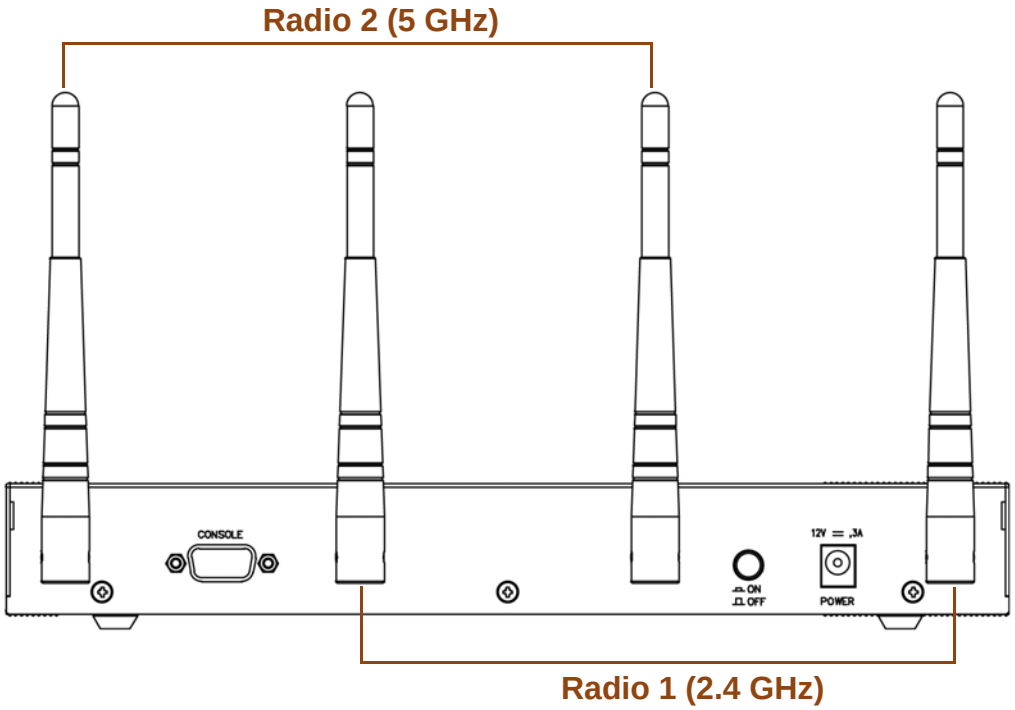
# 2.4 Rear Panel

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

# CHAPTER 3
# 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.

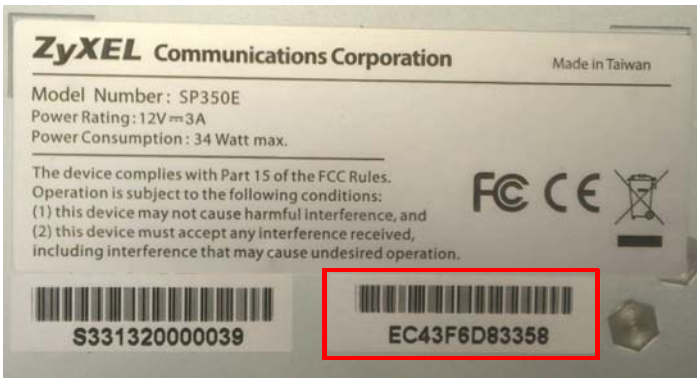
2 Connect your computer to one of the available LAN port on the UAG.

3 Log into the UAG web configurator. See Section 1.4 on page 22 on how to access the web configurator.

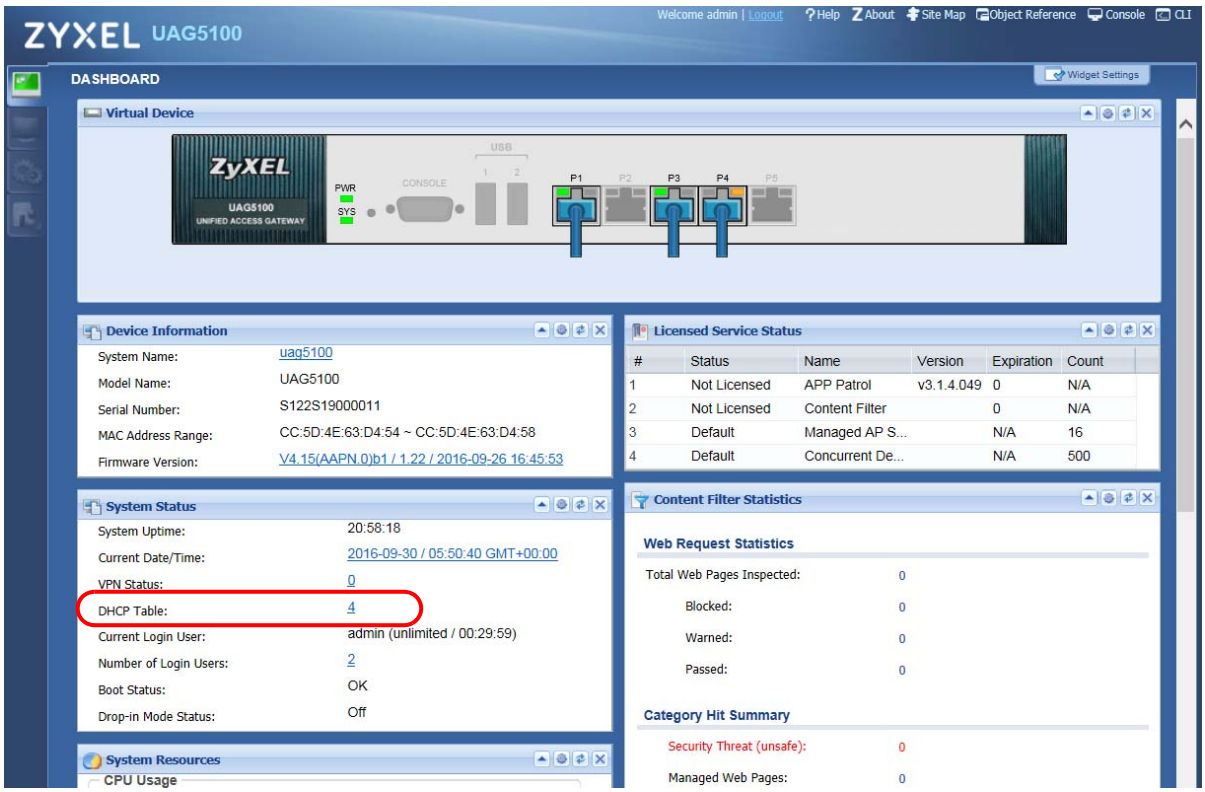
4 Enter your Internet access information to set up a Internet connection. See Chapter 4 on page 50 for detailed information on how to use the setup wizard.

# 3.4 Allow the UAG to Monitor and Manage the Printer

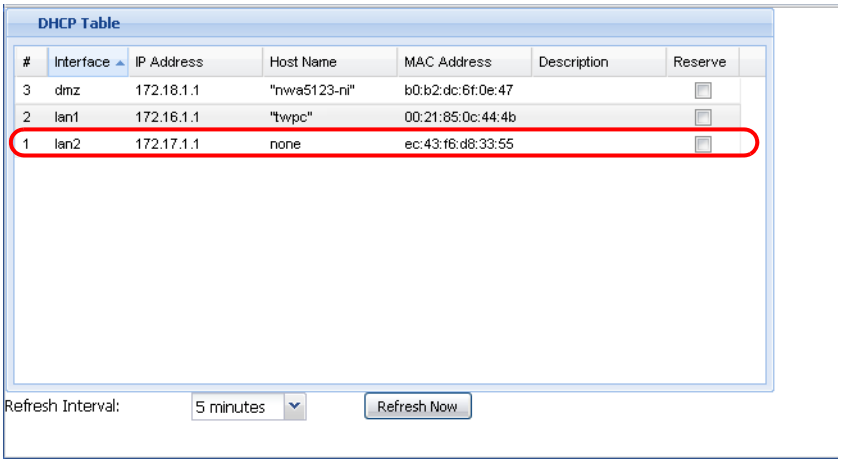
Before you add the printer to the UAG's printer list, check the sticker on the printer's rear panel to see its MAC address.



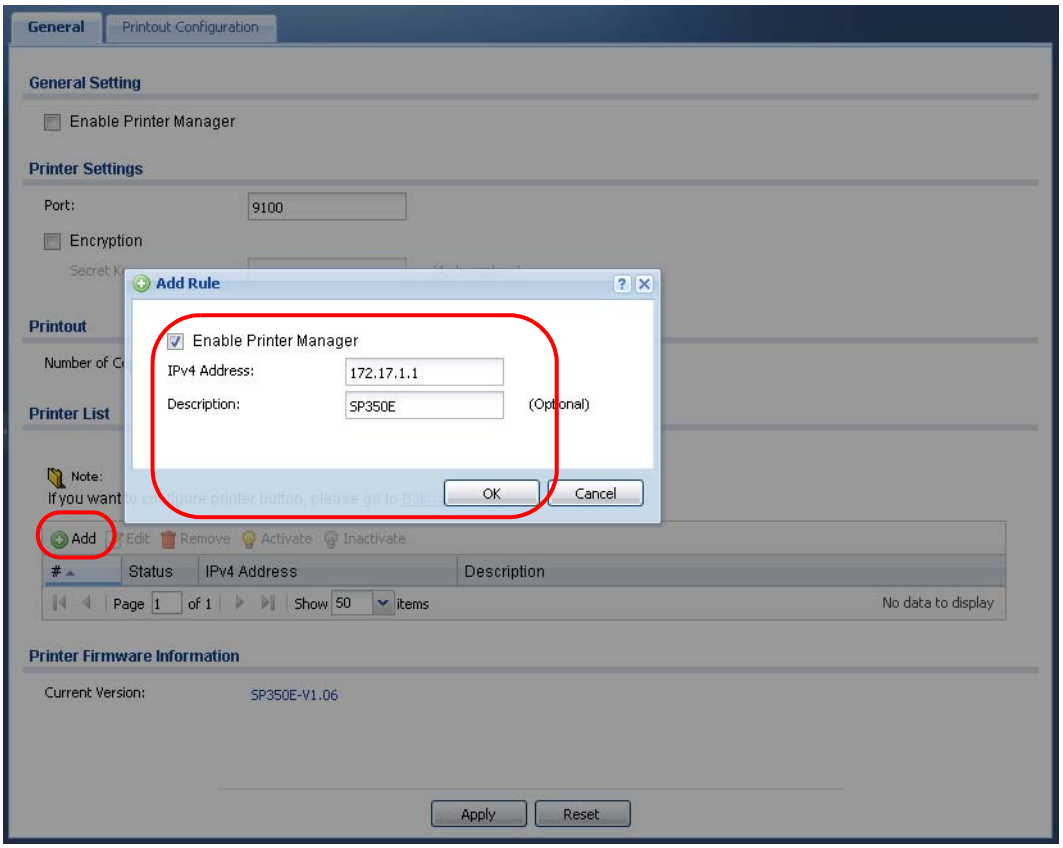

1 Go to the **Dashboard** of the UAG web configurator.



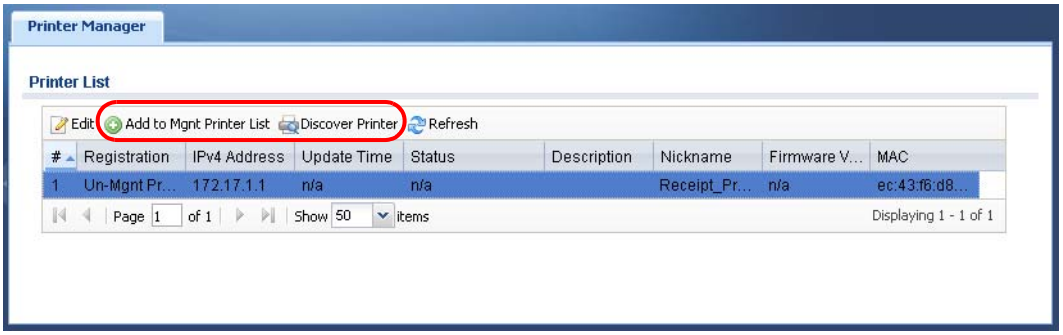

2 Open the **DHCP Table** to find the IP address which is assigned to the printer's MAC address. Make sure the IP address is reserved for the printer. Write down the printer's IP address.



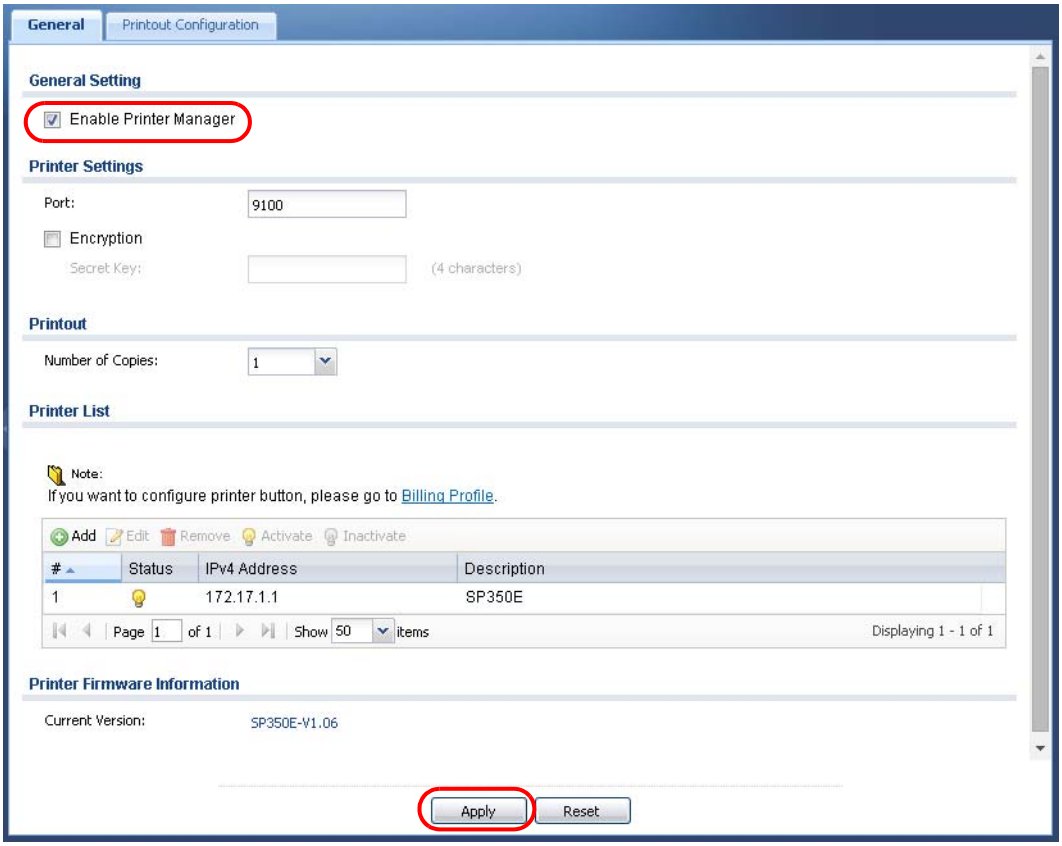

3 Go to the **Configuration > Printer > General Setting** screen. Click **Add** in the **Printer List** to create a new entry for your printer.



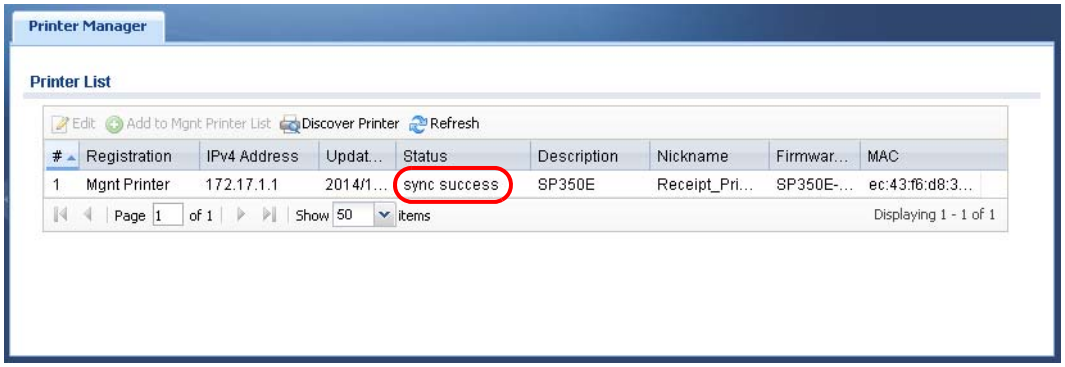

Alternatively, go to the **Configuration > Printer > Printer Manager** screen and click the **Discover Printer** icon. The UAG automatically detects the connected printer(s) and displays the printer information in the list. Select your printer and click **Add to Mgnt Printer List** to let the UAG manage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



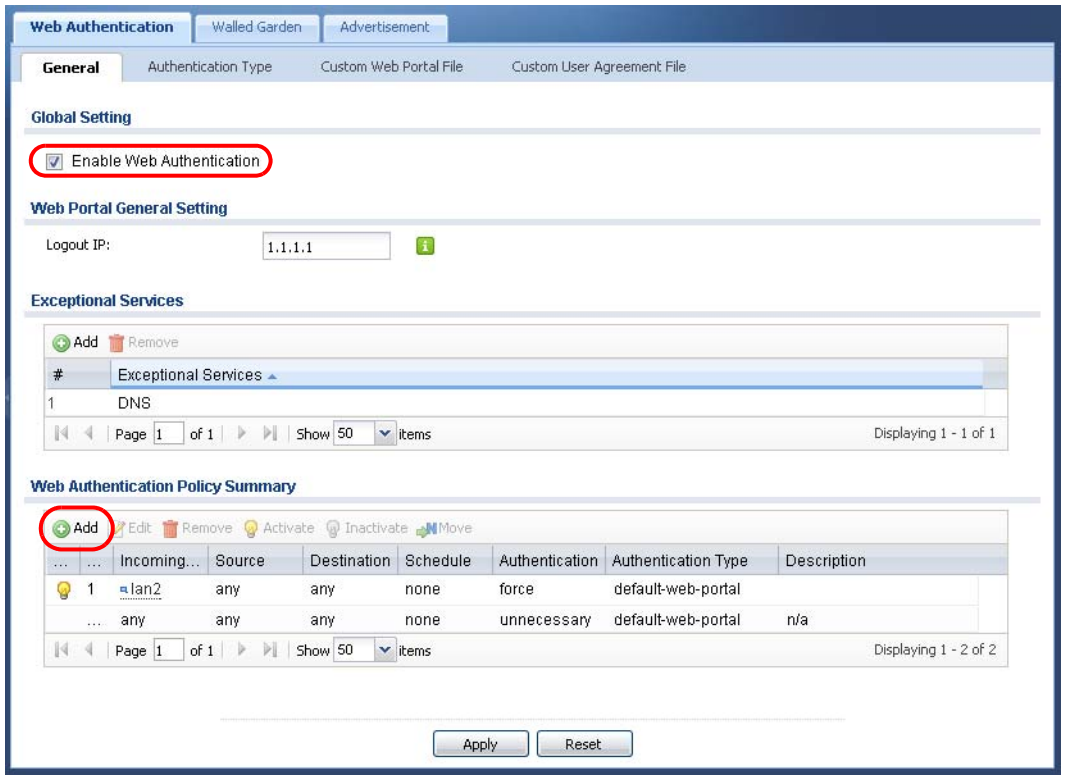

Note: You may need to wait up to 90 seconds for the UAG to synchronize with the printer successfully after you click **Apply** in the **Configuration > Printer > General Setting** screen.

# 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.

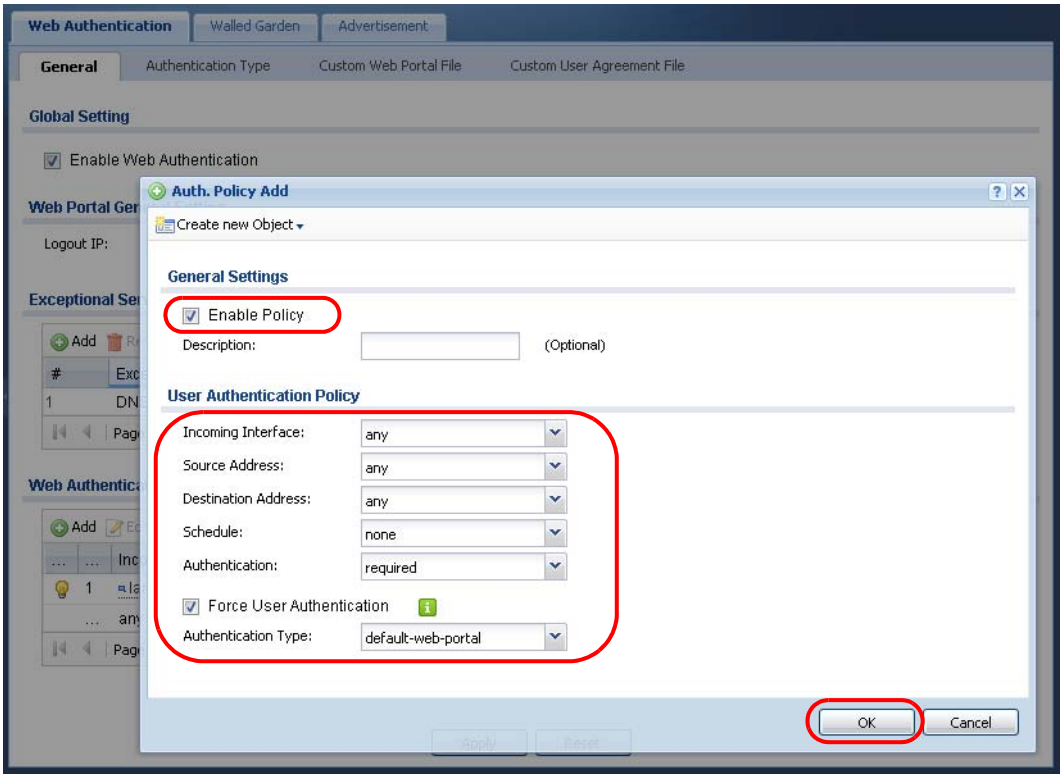
2 Click **Add** to create a new web authentication policy.



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.



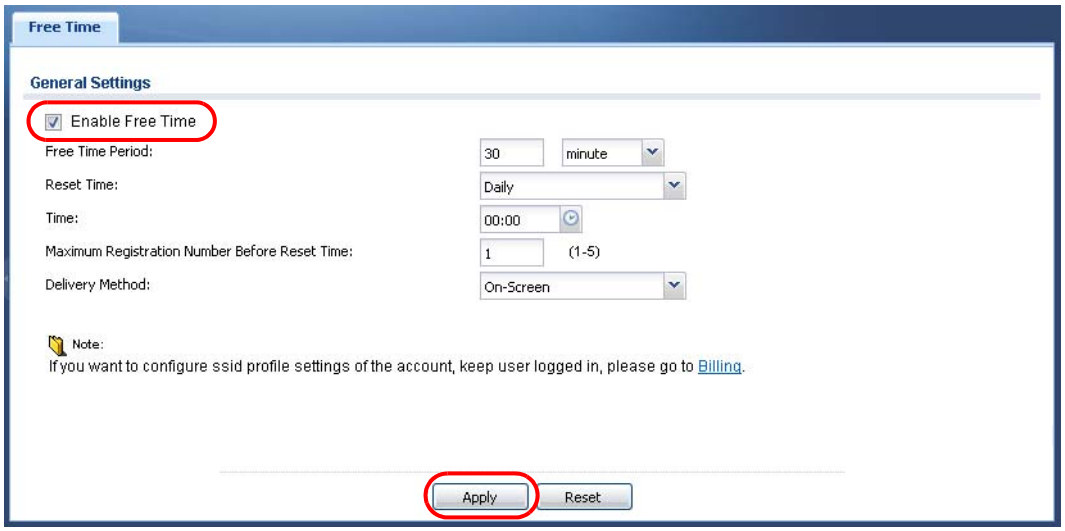

6 Click **Apply** in the **Configuration > Web Authentication** screen.

# 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 25.3 on page 316).

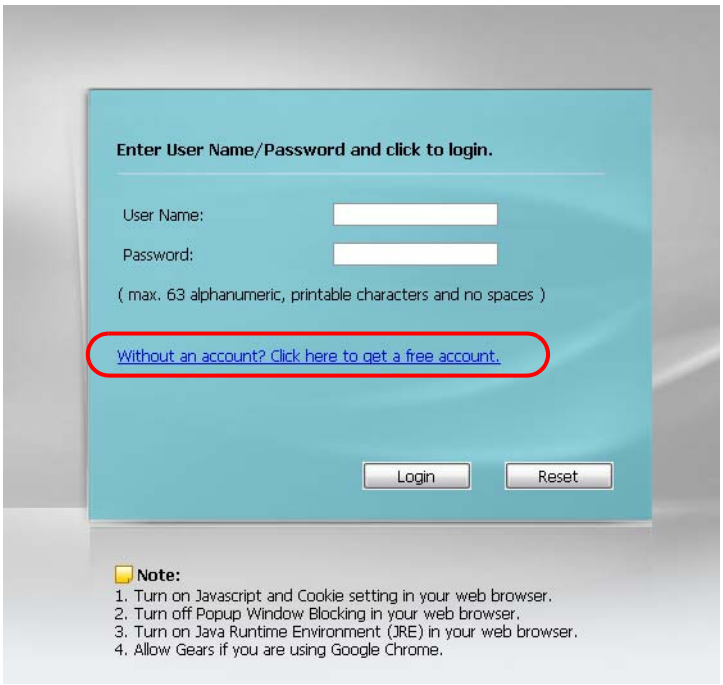
1 Go to the **Configuration > Free Time** screen.

2 Select the **Enable Free Time** option to turn on this feature. Click **Apply**.

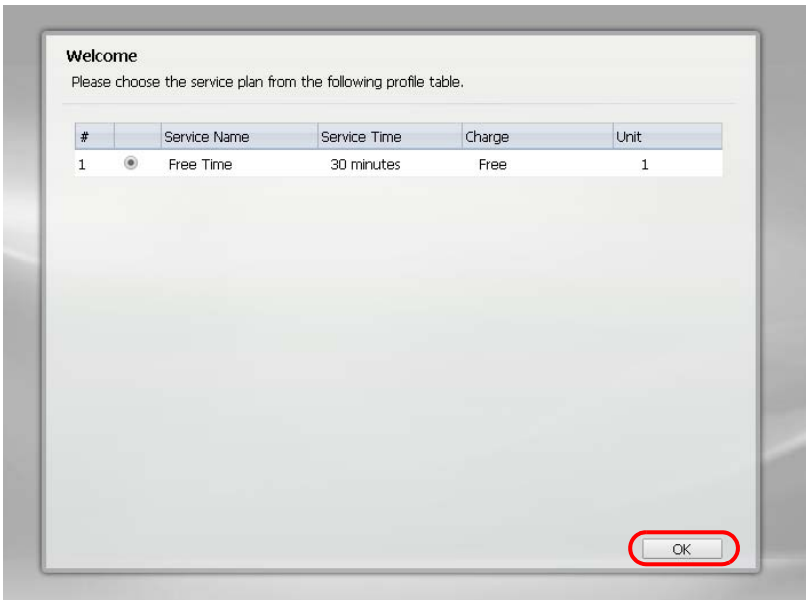



3 Whenever a user tries to access a web page, he/she will be redirected to the default login page.

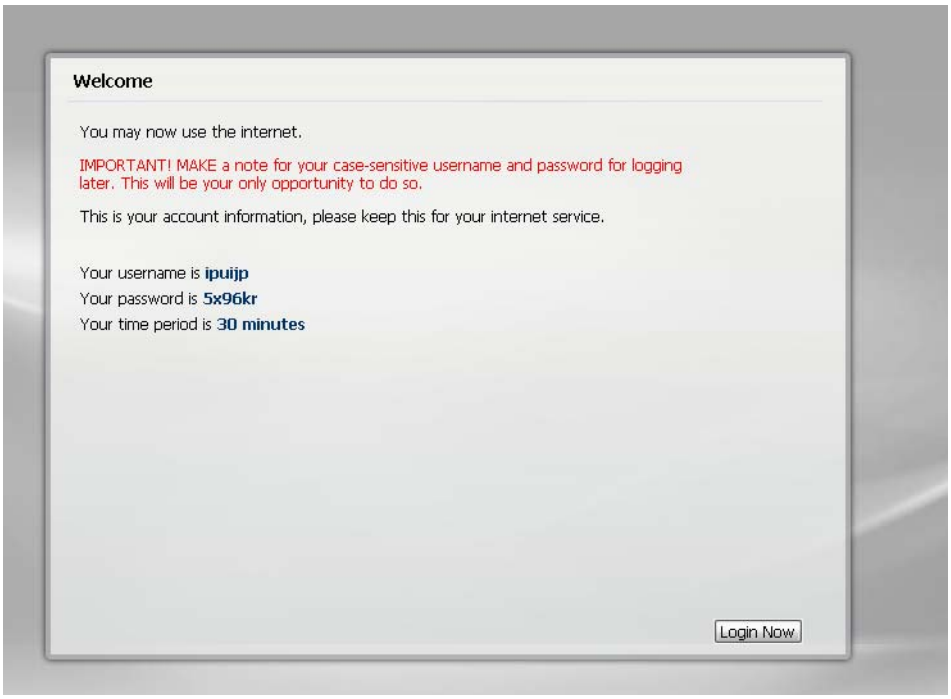
4 Click the link on the login page to get a free guest account.




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.

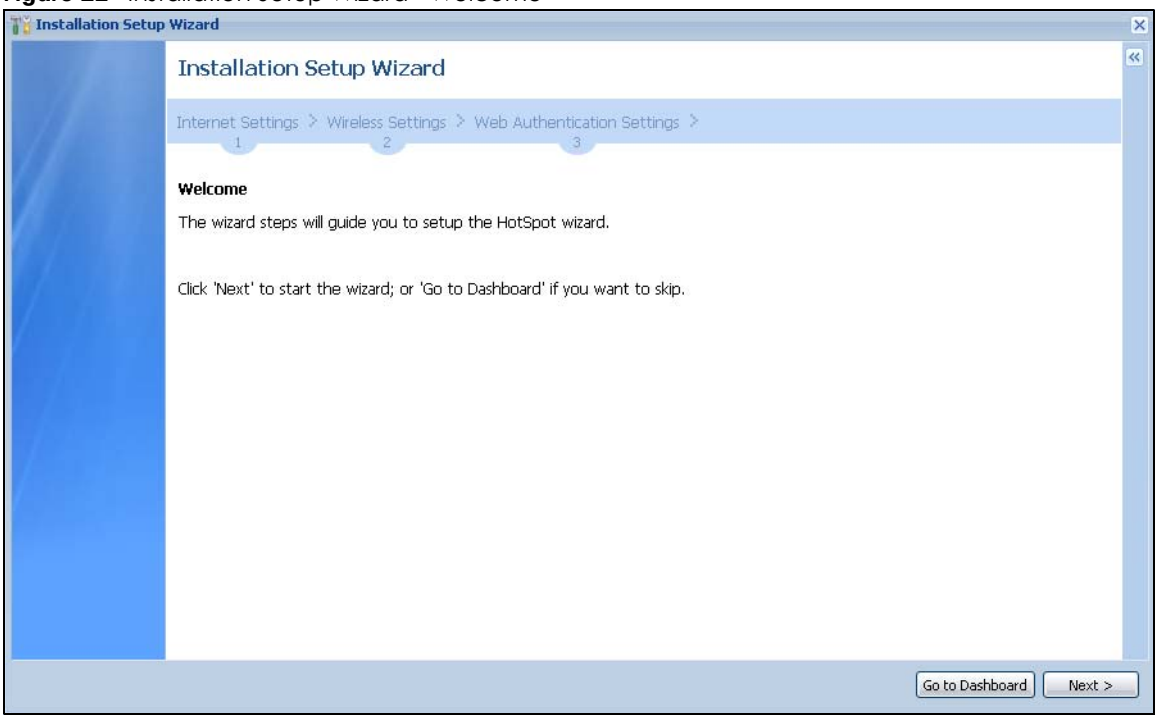


# CHAPTER 4
# Installation Setup Wizard

## 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)

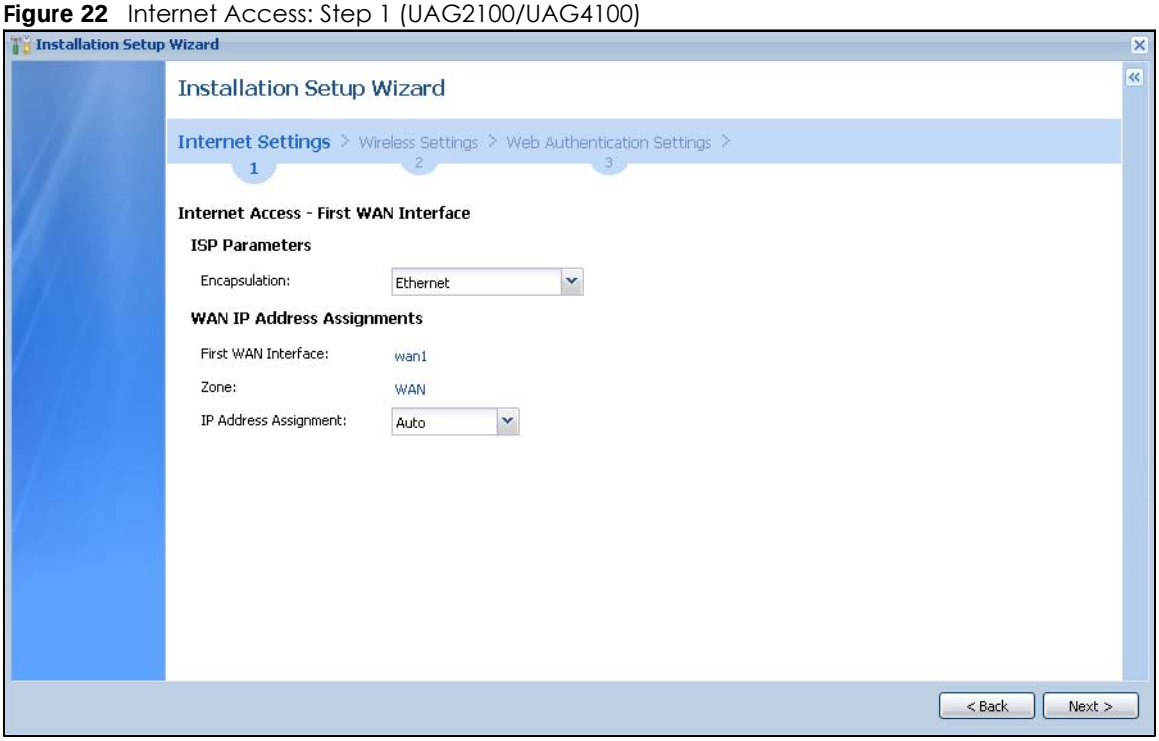
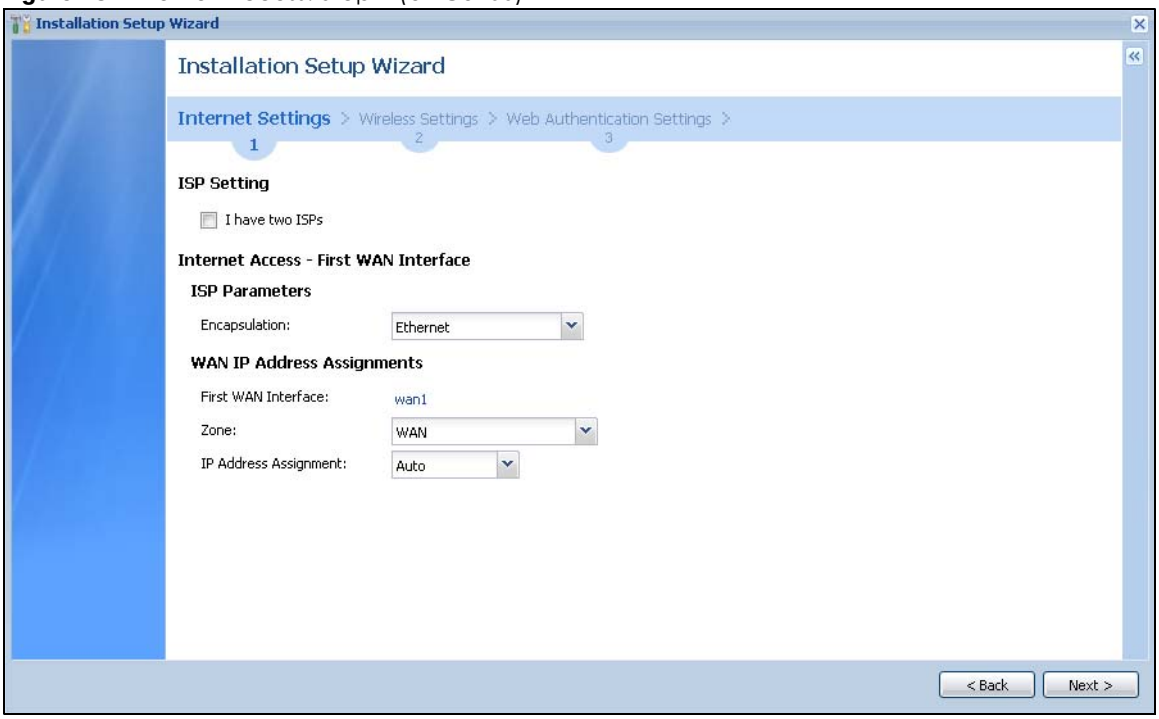



**Figure 23** Internet Access: Step 1 (UAG5100)




- **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.

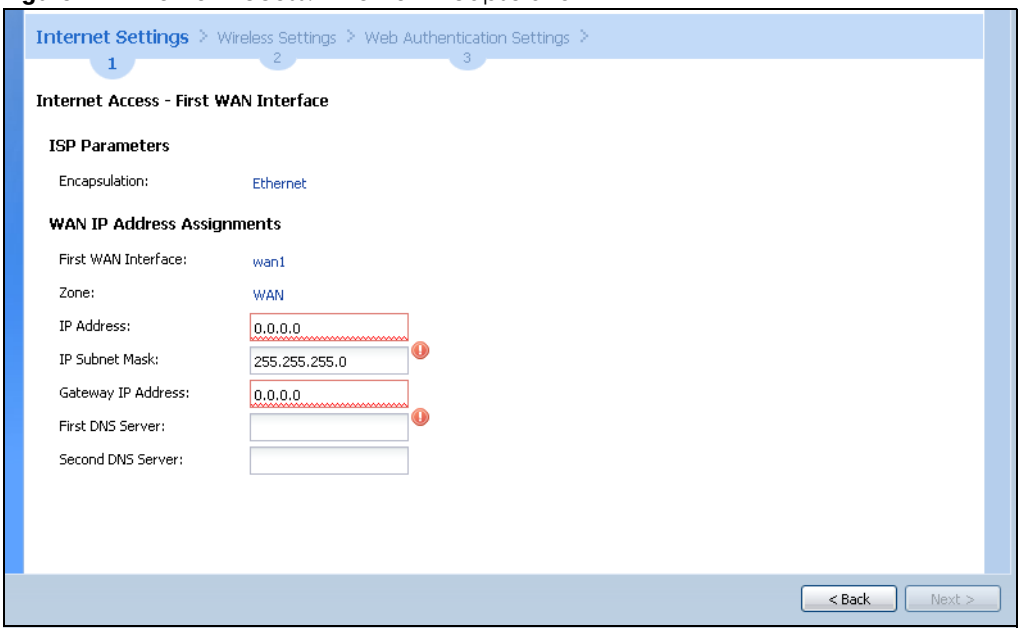
- **Encapsulation**: Choose the **Ethernet** option when the WAN port is used as a regular Ethernet. Otherwise, choose **PPP Over Ethernet** (PPPoE) or **PPTP** for a dial-up connection according to the information from your ISP.
- **First WAN Interface**: This is the interface you are configuring for 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




- **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.

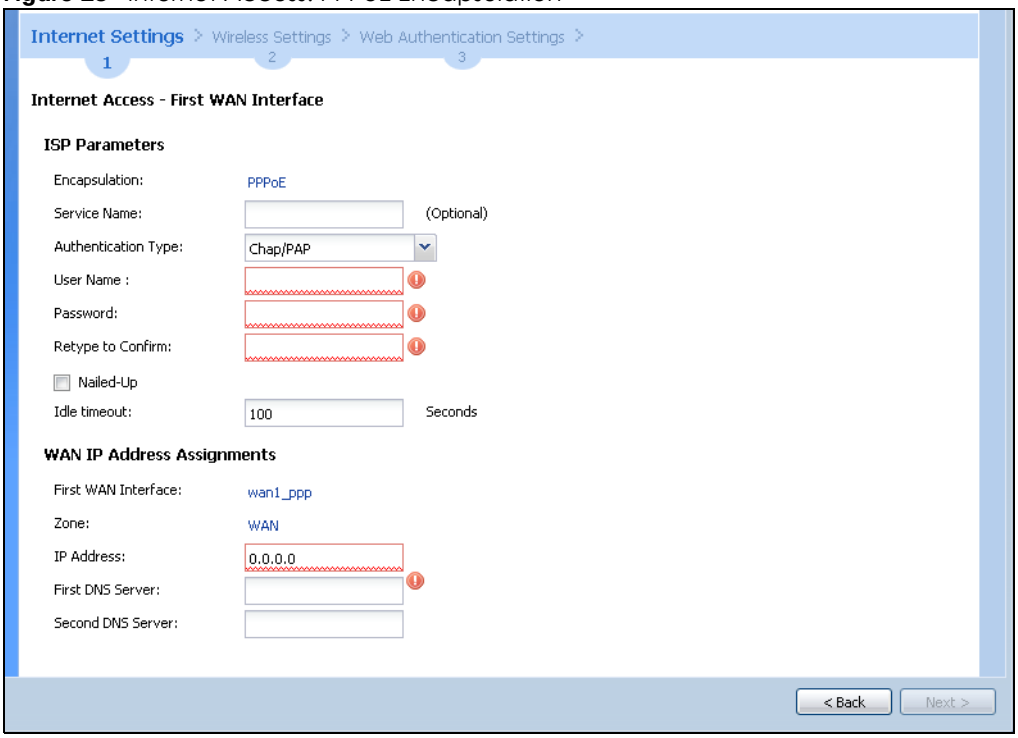
- **IP Subnet Mask**: Enter the subnet mask for this WAN connection's IP address.
- **Gateway IP Address**: Enter the IP address of the router through which this WAN connection will send traffic (the default gateway).

- **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




### 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.

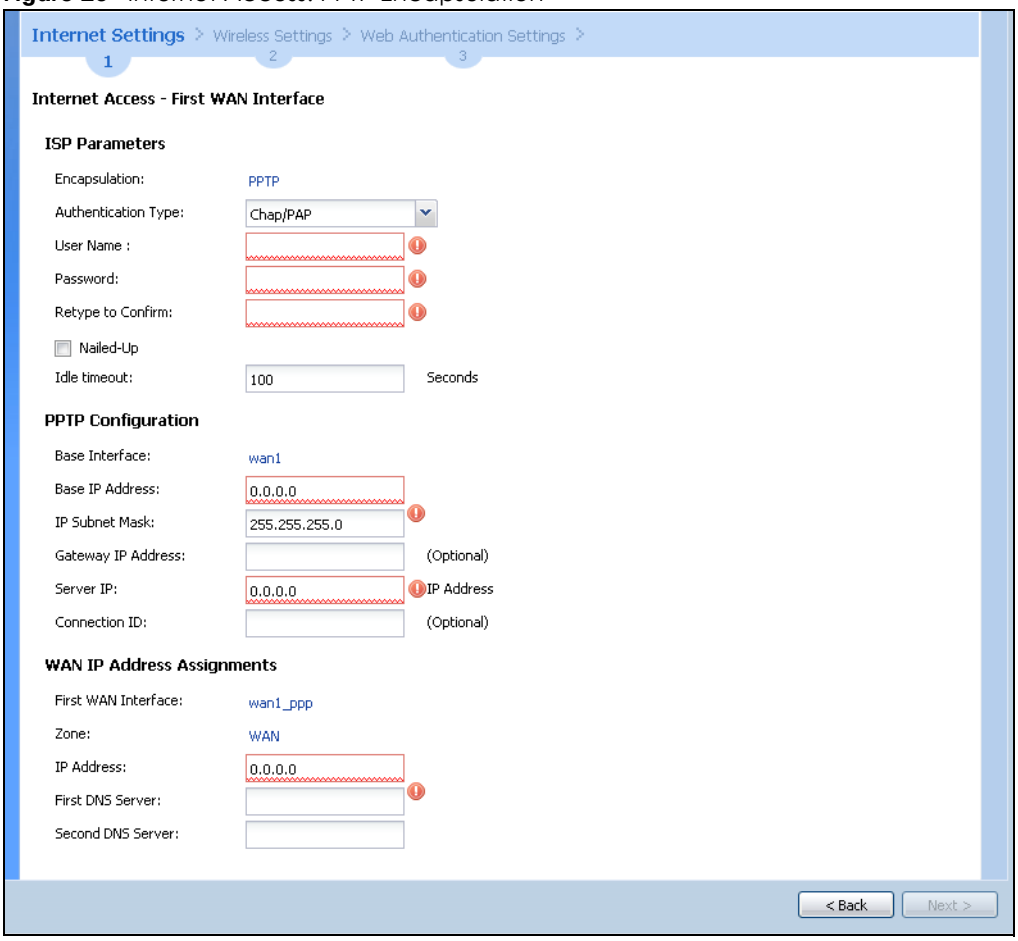
### WAN IP Address Assignments

- **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



### 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.

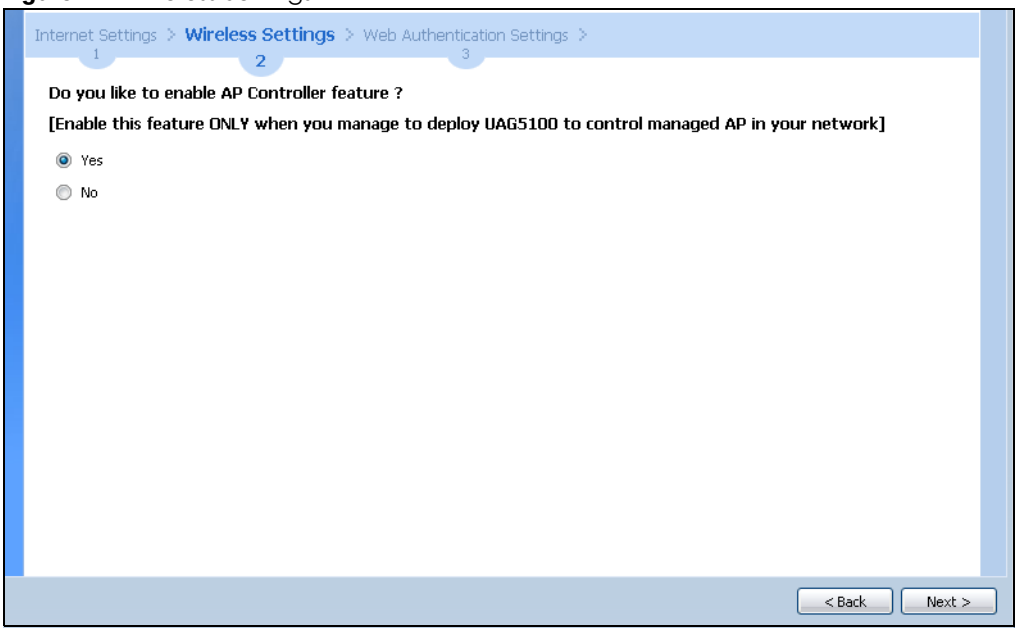
## 4.2.4 Internet Settings - Second WAN Interface

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

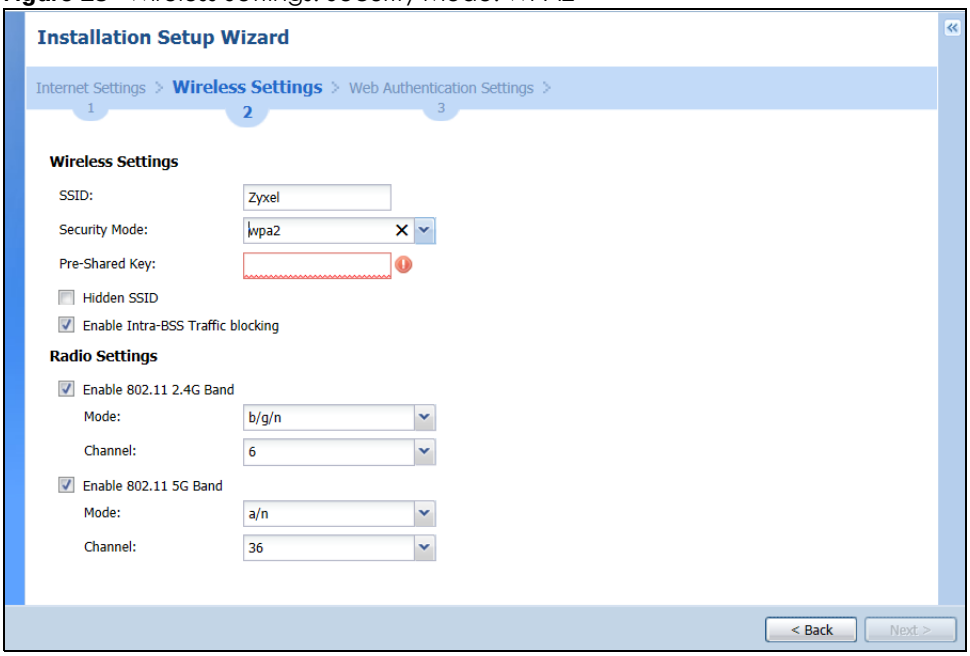



## 4.3.1 Wireless and Radio Settings

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.

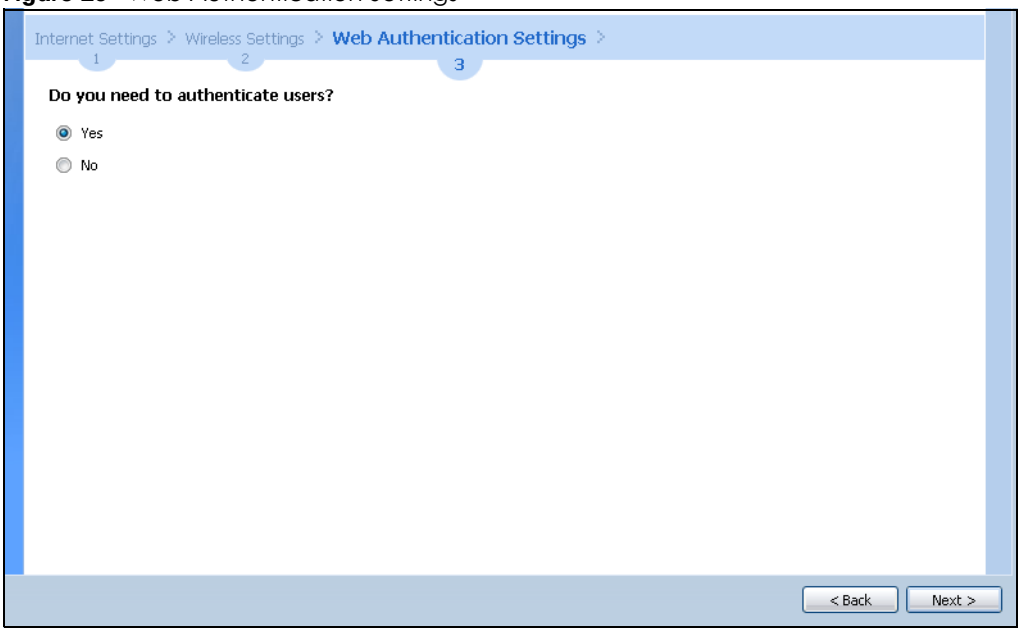
# 4.4 Web Authentication Settings

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 275) to configure a new policy.

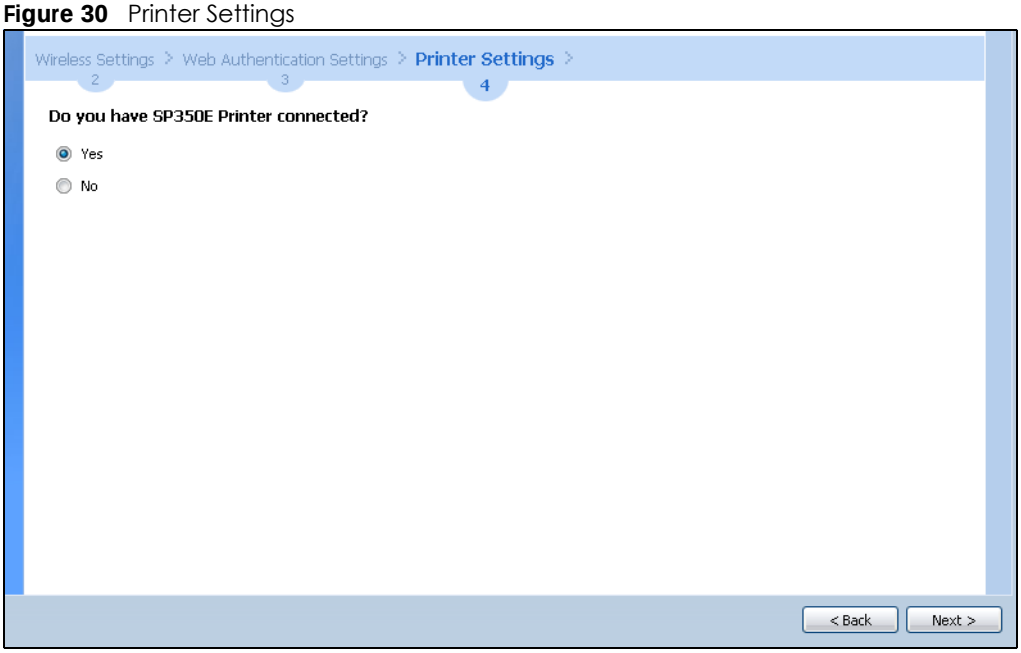
**Figure 29** Web Authentication Settings




# 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.

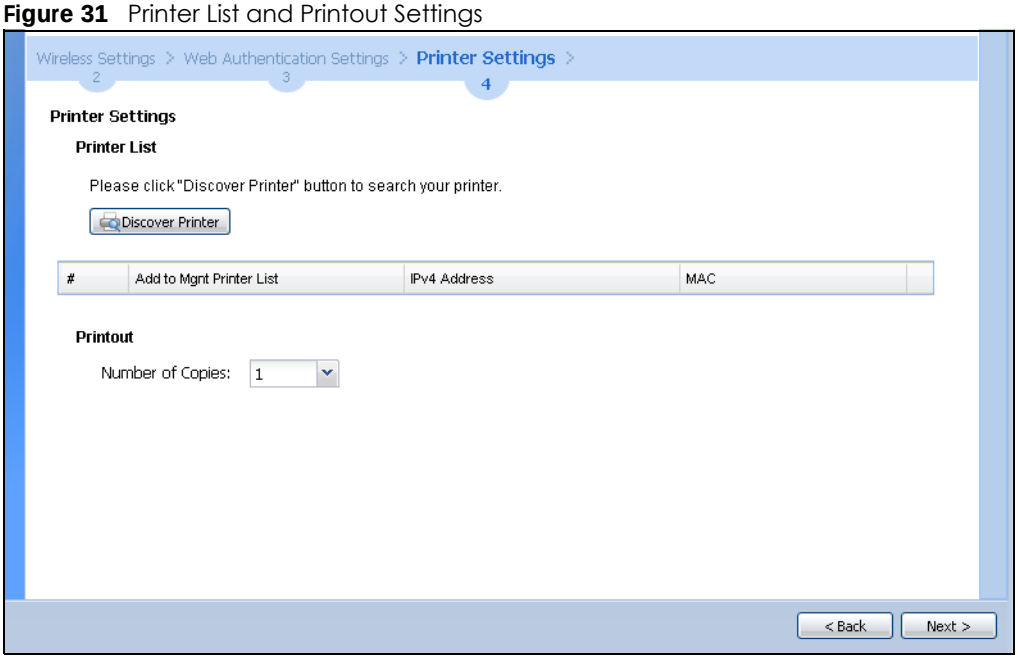
**Figure 30** Printer Settings



### 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




#### 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 Mgnt 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.

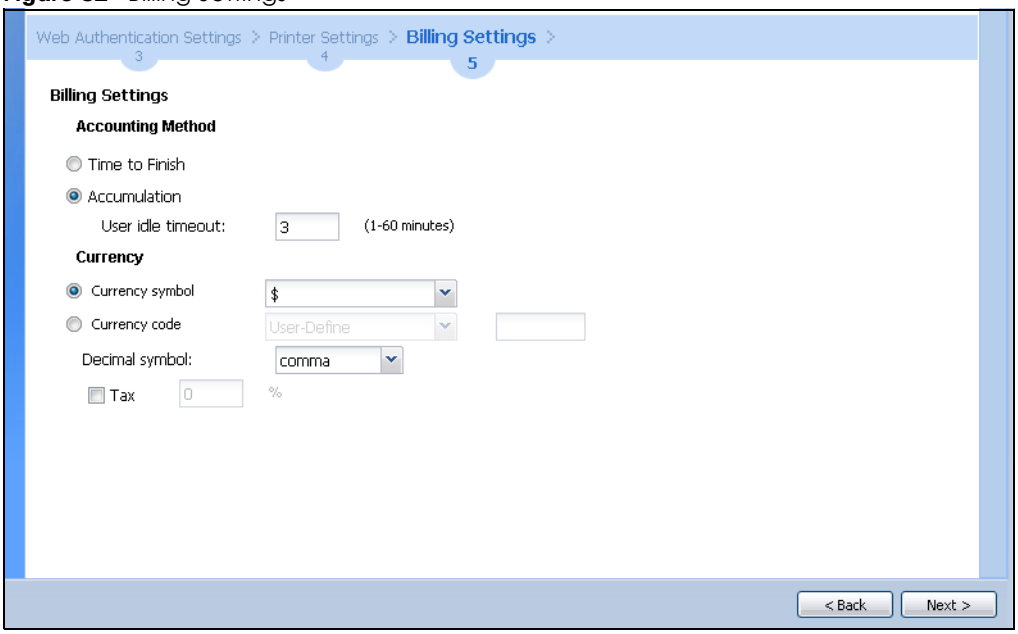
#### Printout

- 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




### 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.

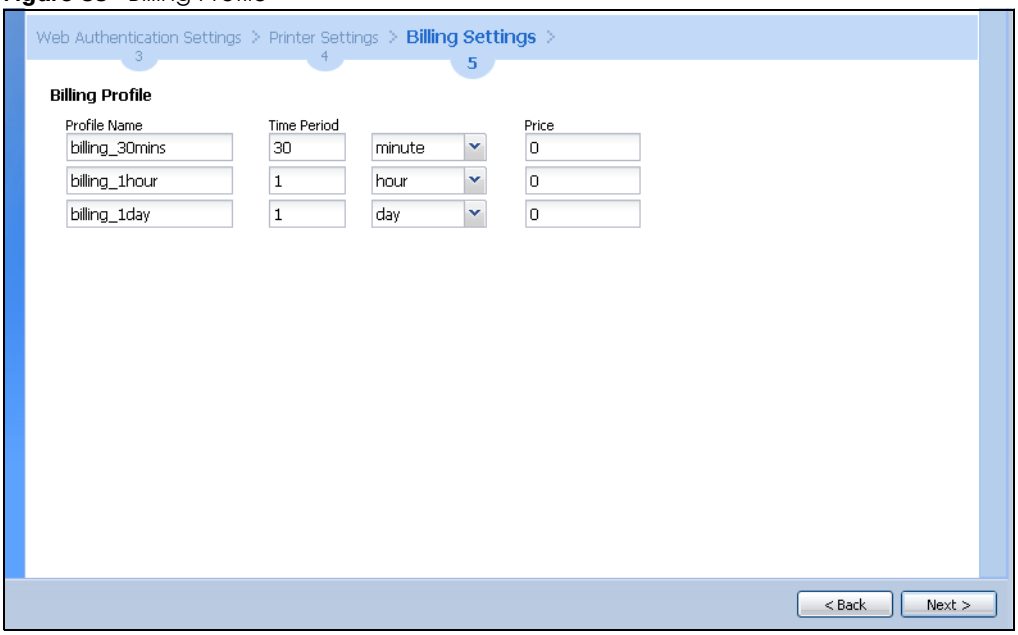
### Currency

- 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

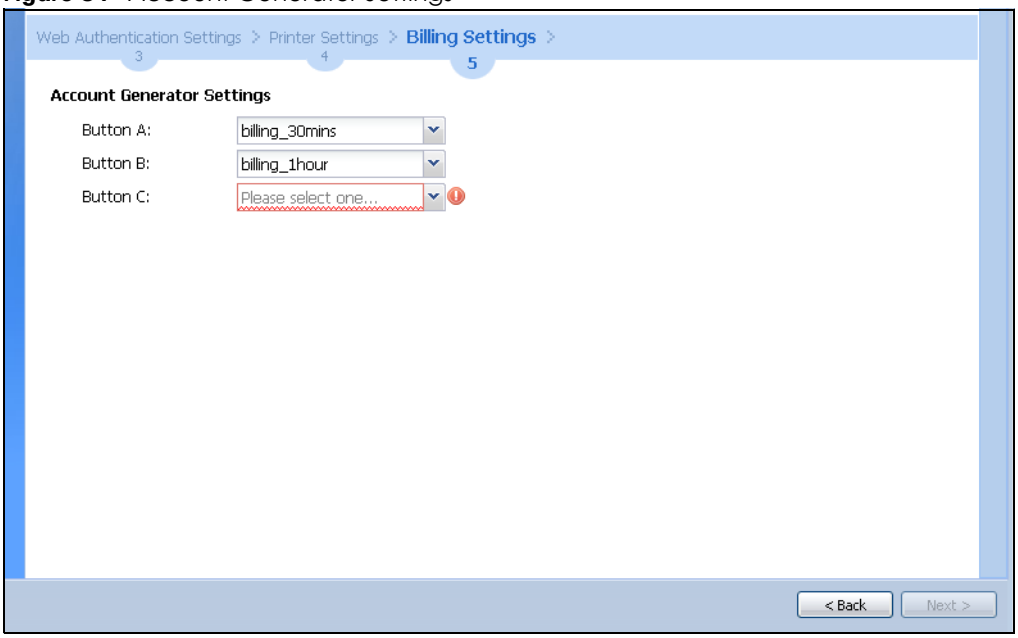



- **Profile Name** - Enter a name for the billing profile. You can use up to 31 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). Spaces are not allowed. The first character must be a letter.
- **Time Period** - Set the duration of the billing period. When this period expires, the user's access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

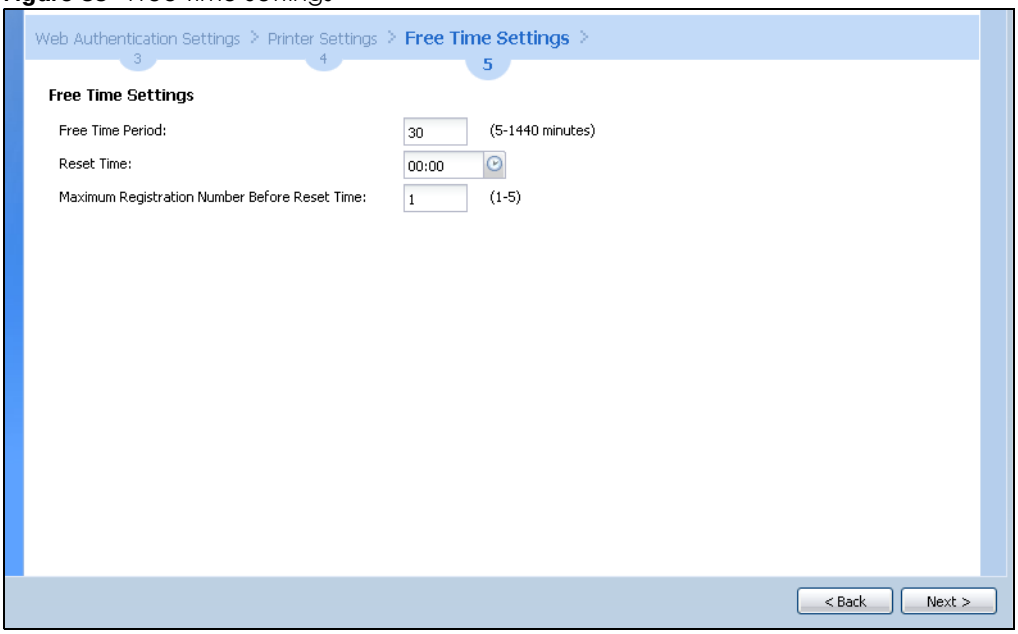
**Figure 34** Account Generator Settings




# 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.

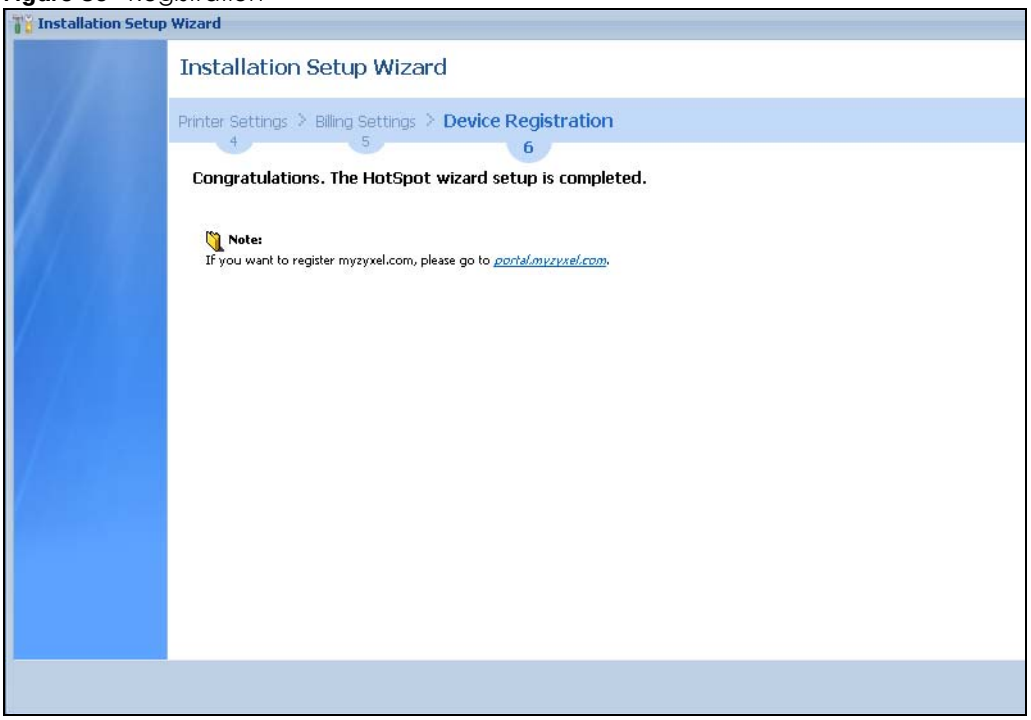
- **Maximum Registration Number Before Reset Time** - Enter the maximum number of the users that are allowed to log in for Internet access with a free guest account before the time specified in the **Reset Time** field. For example, if you set the **Maximum Registration Number Before Reset Time** to 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



# CHAPTER 5
# Quick Setup Wizards

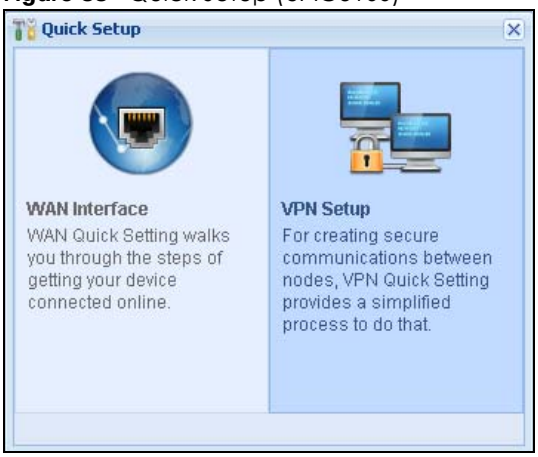
## 5.1 Quick Setup Overview

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.

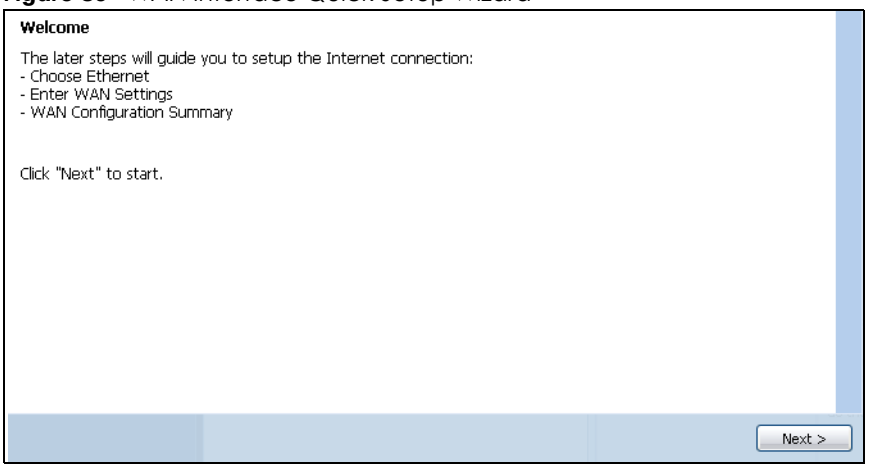
- **VPN Setup**

  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**.

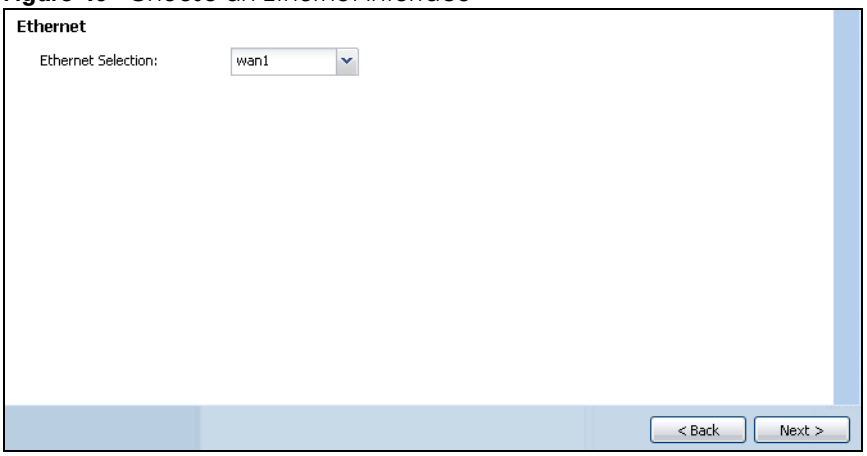
**Figure 39** WAN Interface Quick Setup Wizard




## 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

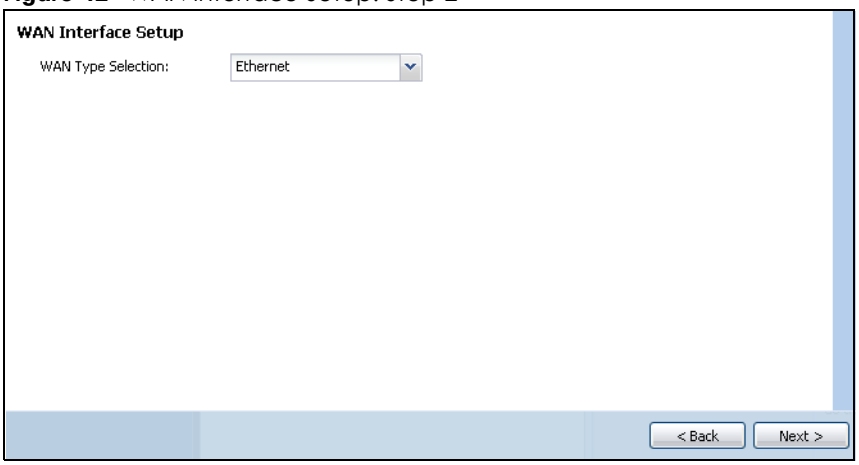



## 5.2.2 Select WAN Type

**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



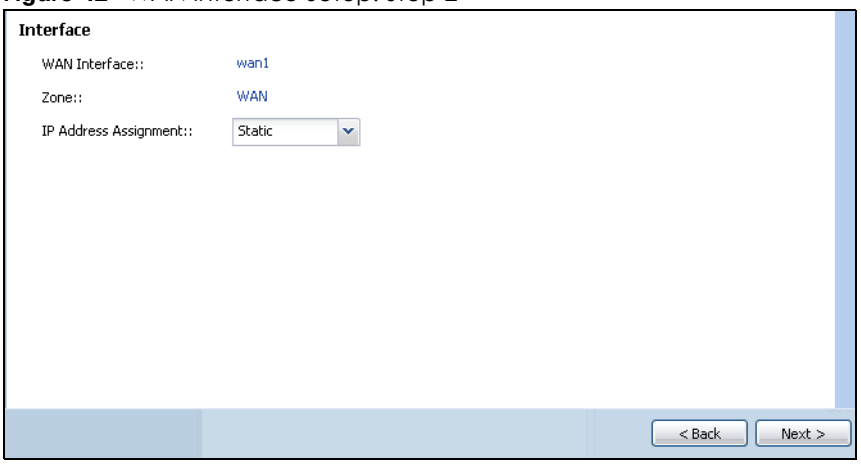

The screens vary depending on what encapsulation type you use. Refer to information provided by your ISP to know what to enter in each field. Leave a field blank if you don't have that information.

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

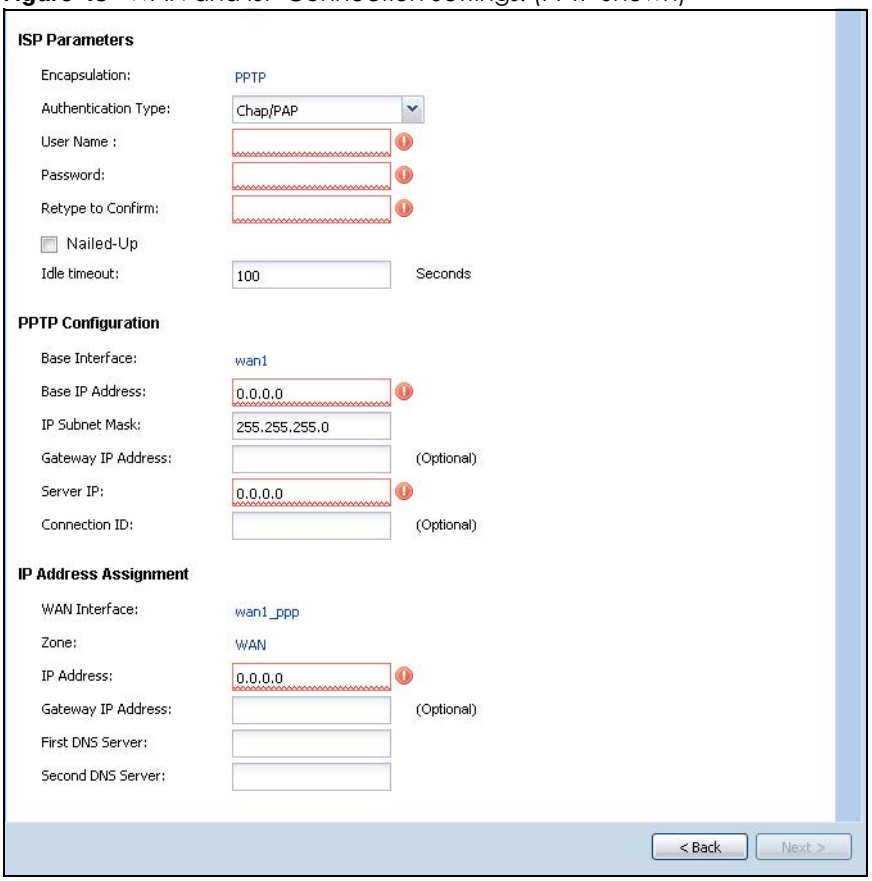



- **WAN Interface**: This is the interface you are configuring for Internet access.
- **Zone**: This is the security zone to which this interface and Internet connection belong.
- **IP Address Assignment**: Select **Auto** If your ISP did not assign you a fixed IP address. Select **Static** if you have 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 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:<br>**CHAP/PAP** - Your UAG accepts either CHAP or PAP when requested by this remote node.<br>**CHAP** - Your UAG accepts CHAP only.<br>**PAP** - Your UAG accepts PAP only.<br>**MSCHAP** - Your UAG accepts MSCHAP only.<br>**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. |
| 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. |

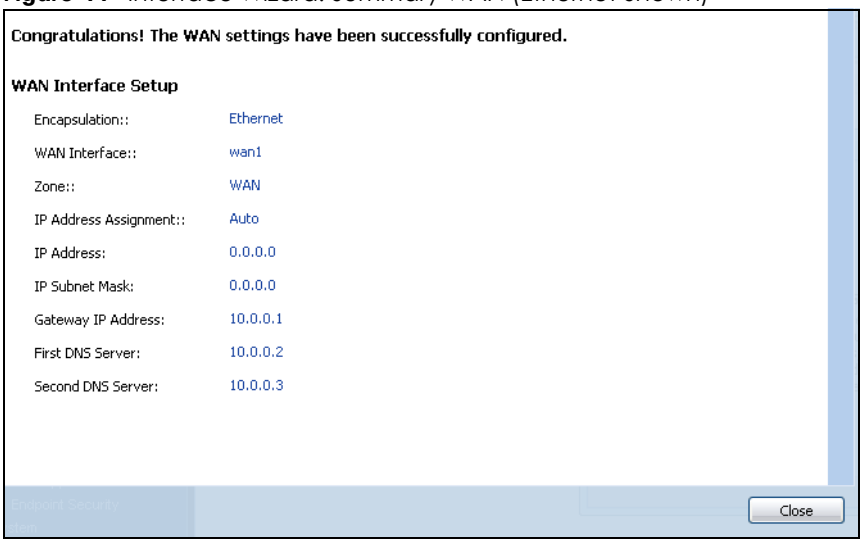
Table 12 WAN and ISP Connection Settings (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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.<br>This field is optional and depends on the requirements of your DSL modem.<br>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<br>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.<br>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.<br>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.

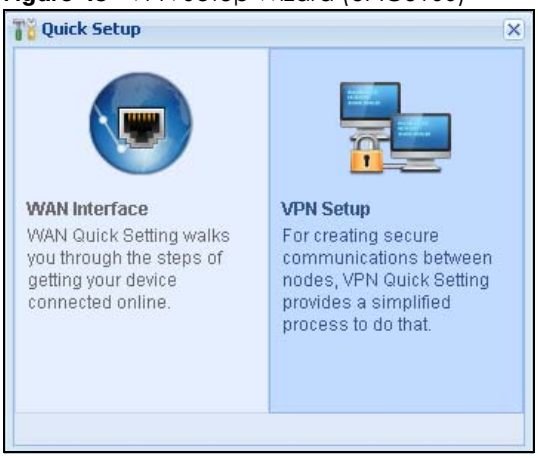
Table 13 Interface Wizard: Summary WAN

| 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<br><br>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.

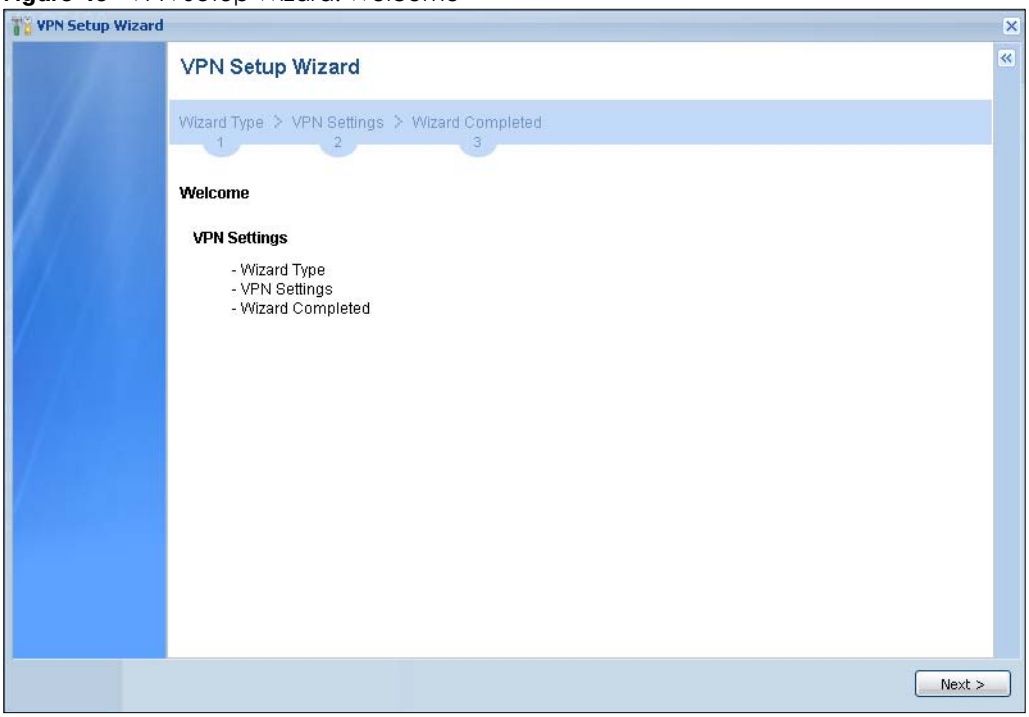
**Figure 45** VPN Setup Wizard (UAG5100)




## 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

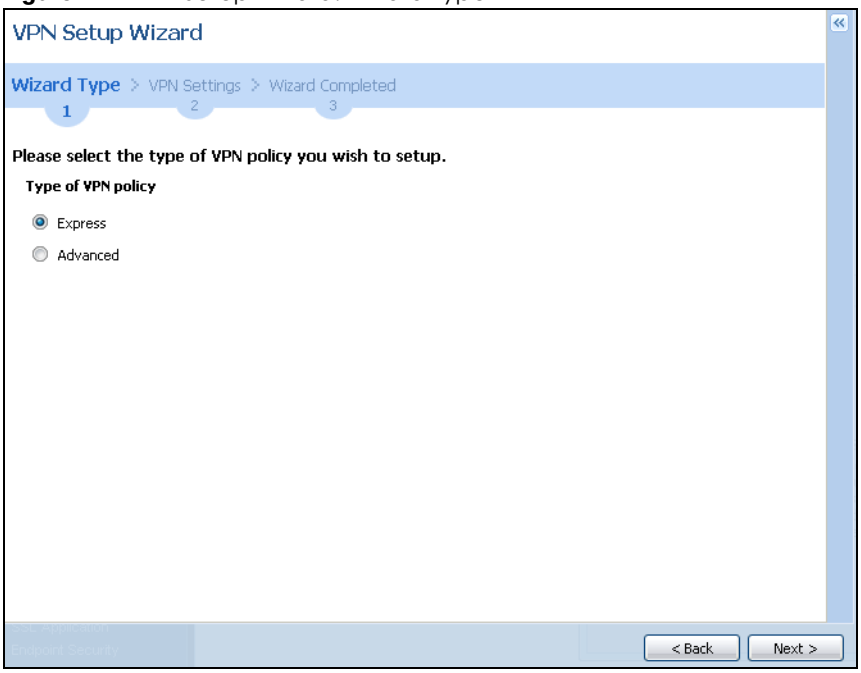


## 5.3.2 VPN Setup Wizard: Wizard Type

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.

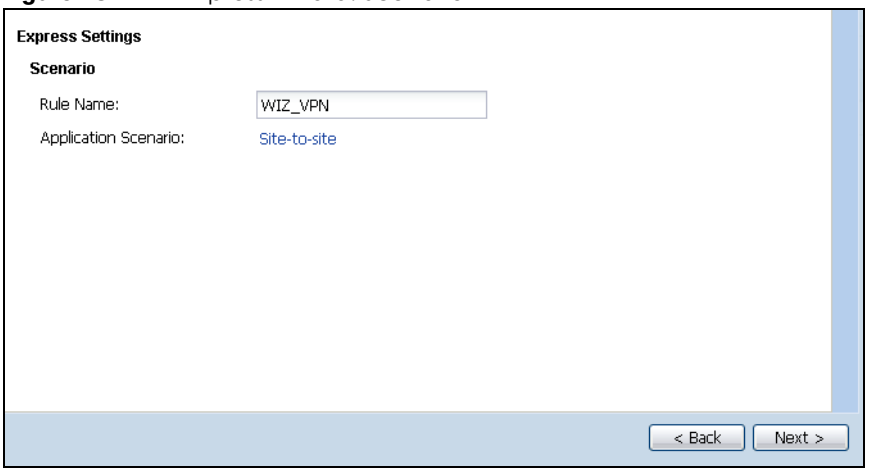
**Figure 47** VPN Setup Wizard: Wizard Type




## 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



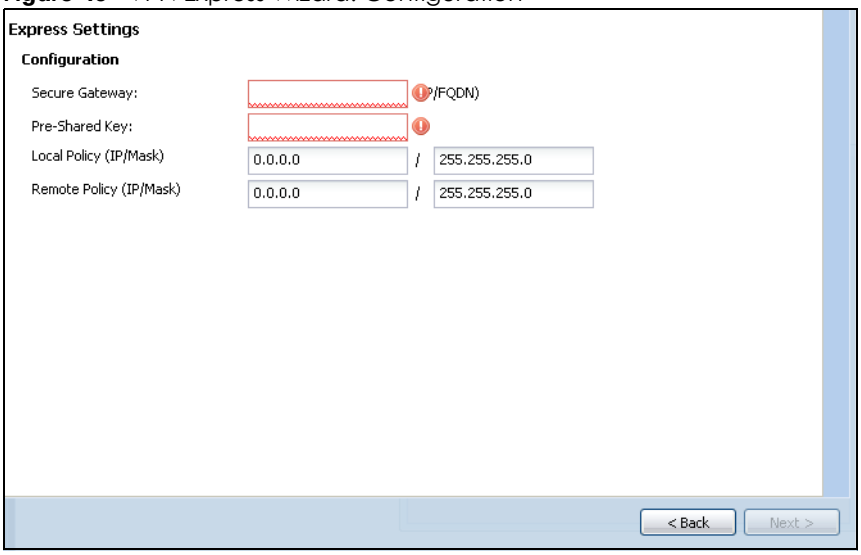
**Rule Name**: Type the name used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

**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

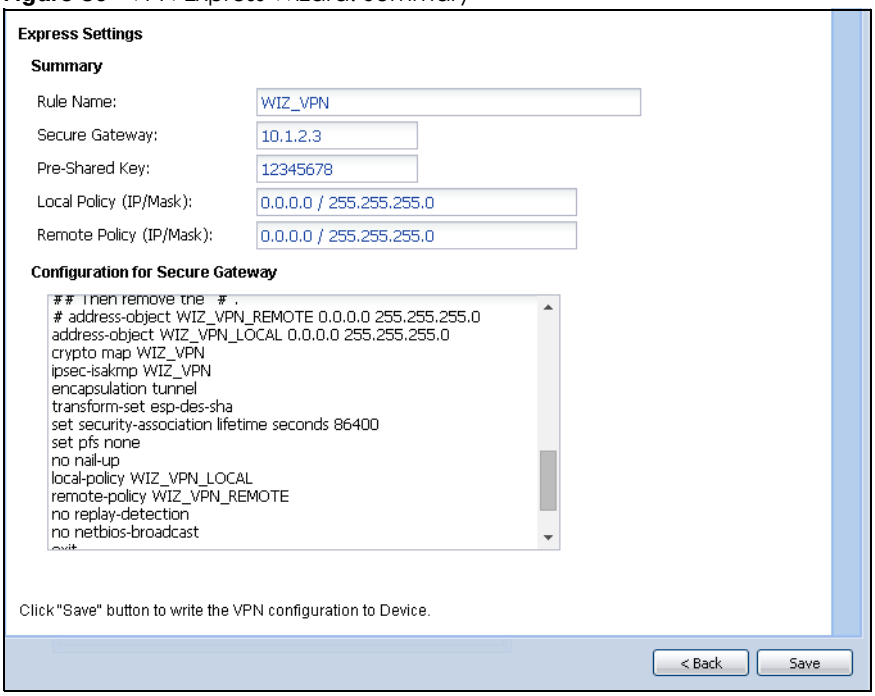



- **Secure Gateway**: Enter the WAN IP address or domain name of the remote IPSec device (secure gateway) to identify the remote IPSec router by its IP address or a domain name.
- **Pre-Shared Key**: Type the password. Both ends of the VPN tunnel must use the same password. Use 8 to 31 case-sensitive 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

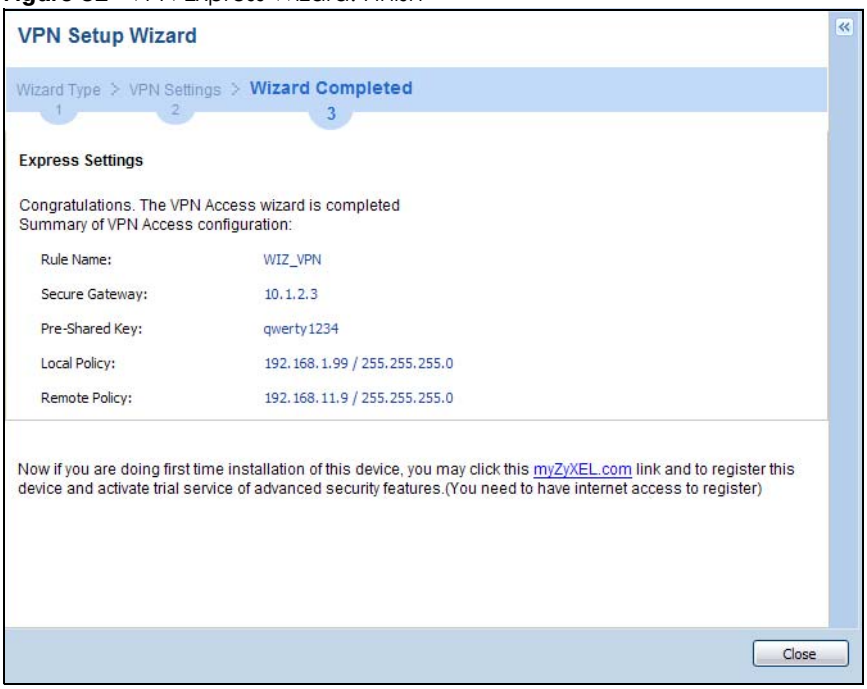



- **Rule Name**: Identifies the VPN gateway policy.
- **Secure Gateway**: IP address or domain name of the remote IPSec device.
- **Pre-Shared Key**: VPN tunnel password. It identifies a communicating party during a phase 1 IKE negotiation.
- **Local Policy**: IP address and subnet mask of the computers 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

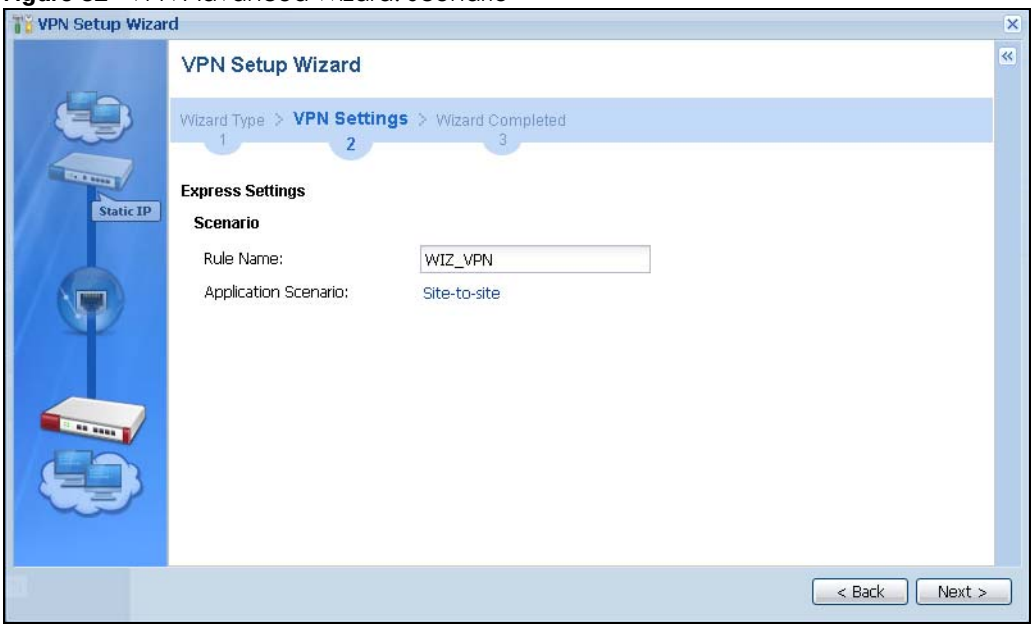



Click **Close** to exit the wizard.

## 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.

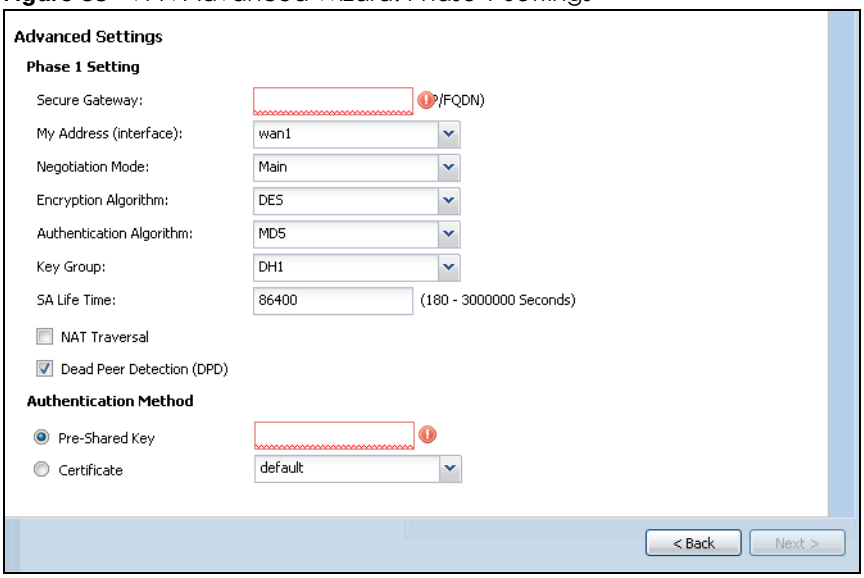
**Application Scenario**: This shows the scenario that the UAG supports.

- **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).

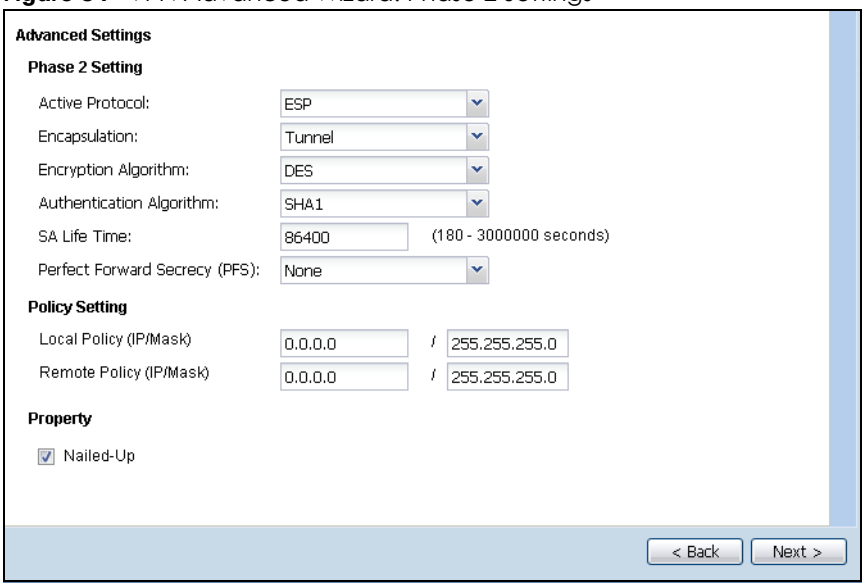
Note: The remote IPSec device must also have NAT traversal enabled. See the help in the main IPSec VPN screens for more information.

- **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



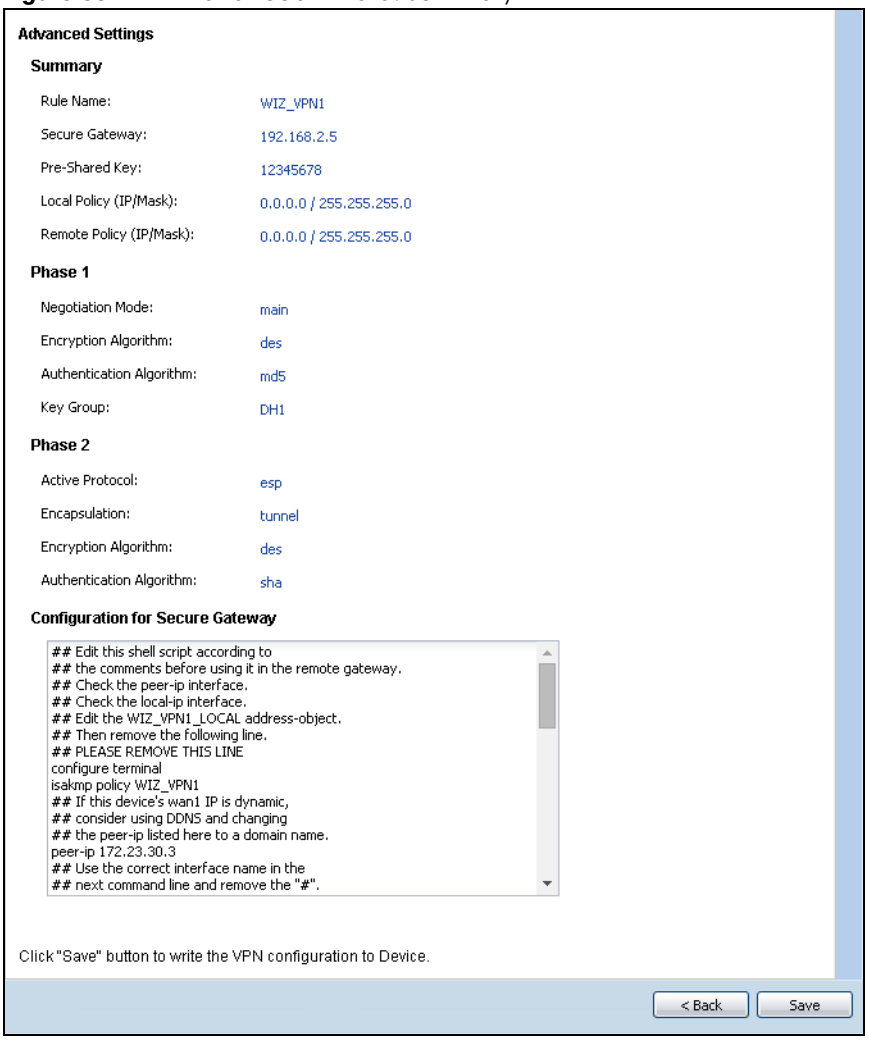

- **Active Protocol**: **ESP** is compatible with NAT, **AH** is not.
- **Encapsulation**: **Tunnel** is compatible with NAT, **Transport** is not.
- **Encryption Algorithm**: **3DES** and **AES** use encryption. The longer the **AES** key, the higher the security (this may affect throughput). **Null** 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



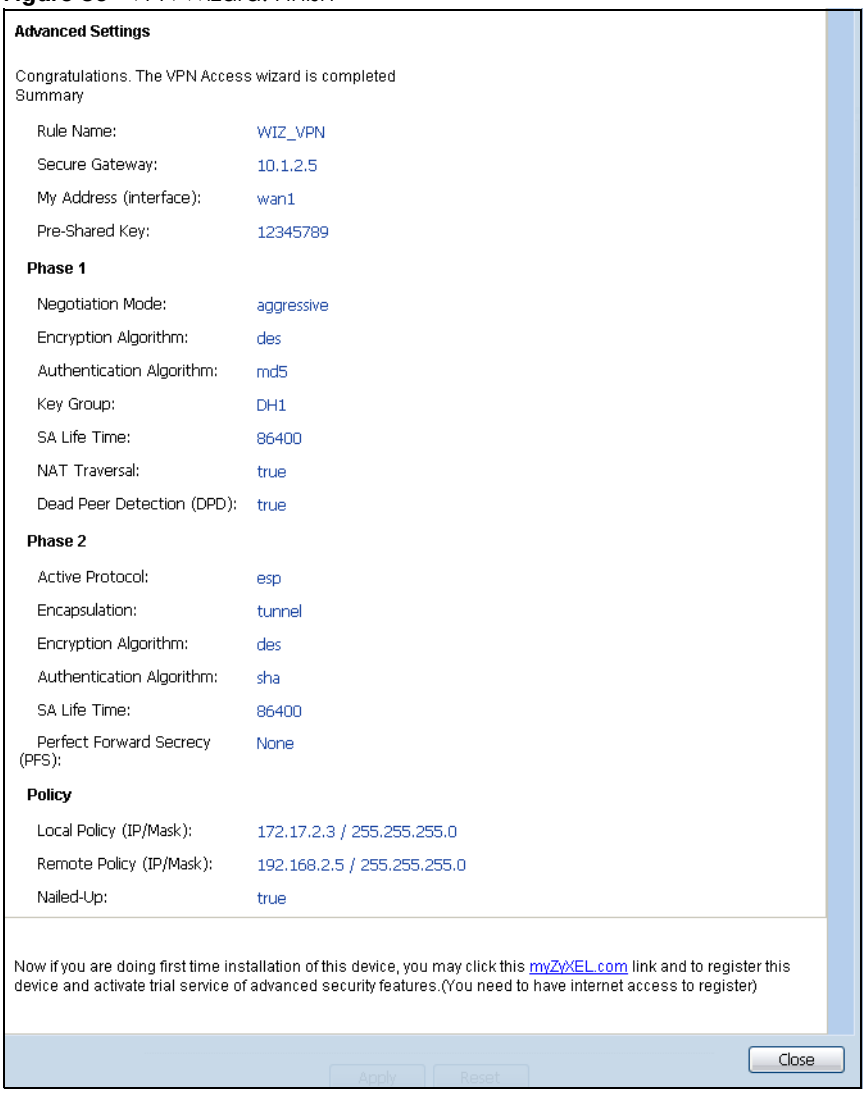

- **Rule Name**: Identifies the VPN connection (and the VPN gateway).
- **Secure Gateway**: IP address or domain name of the remote IPSec device.
- **Pre-Shared Key**: VPN tunnel password.
- **Certificate**: The certificate the UAG uses to identify itself when setting up the VPN tunnel.
- **Local Policy**: 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




Click **Close** to exit the wizard.

# CHAPTER 6
# 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 89) 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 90) 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. |
| 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.<br>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.<br>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.<br>**Inactive** - The Ethernet interface is disabled.<br>**Down** - The Ethernet interface does not have any physical ports associated with it or the Ethernet interface is enabled but not connected.<br>**Speed / Duplex** - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (**Full** or **Half**).<br>**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. |

Table 14 Dashboard (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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.<br><br>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 89. |
| 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 | This field displays details about the UAG's startup state.<br><br>**OK** - The UAG started up successfully.<br><br>**Firmware update OK** - A firmware update was successful.<br><br>**Problematic configuration after firmware update** - The application of the configuration failed after a firmware upgrade.<br><br>**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.<br><br>**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.<br><br>**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).<br><br>**Booting in progress** - The UAG is still applying the system configuration. |
| Drop-in Mode Status | This field displays whether the UAG is working in drop-in mode.<br><br>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.<br><br>This field is available only on the UAG that supports drop-in mode. |
| 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. |
| 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. |
| Interface Status Summary | If an Ethernet interface does not have any physical ports associated with it, its entry is displayed in light gray text. |

Table 14 Dashboard (continued)

| LABEL | DESCRIPTION |
|---|---|
| Name | This field displays the name of each interface. |
| Status | This field displays the current status of each interface. The possible values depend on what type of interface it is.<br>For Ethernet interfaces:<br>**Inactive** - The Ethernet interface is disabled.<br>**Down** - The Ethernet interface does not have any physical ports associated with it or the Ethernet interface is enabled but not connected.<br>**Up** - The Ethernet interface is enabled and connected.<br>For PPP interfaces:<br>**Connected** - The PPP interface is connected.<br>**Disconnected** - The PPP interface is not connected.<br>If the PPP interface is disabled, it does not appear in the list. |
| Zone | This field displays the zone to which the interface is currently assigned. |
| IP Addr/ Netmask | 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.<br>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). |
| IP Assignment | This field displays how the interface gets its IP address.<br>**Static** - This interface has a static IP address.<br>**DHCP Client** - This Ethernet interface gets its IP address from a DHCP server.<br>**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.<br>Click **Renew** to send a new DHCP request to a DHCP server.<br>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**.<br>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.<br>**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. |

Table 14 Dashboard (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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.<br><br>**0** displays if the service license does not have a limited period of validity. |
| Content Filter Statistics | |
| Total Web Pages Inspected | This displays the number of web pages the UAG's content filter feature has checked. |
| Blocked | This displays the number of web pages that the UAG blocked access. |
| Warned | This displays the number of web pages for which the UAG displayed a warning message to access requesters. |
| Passed | This displays 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. |
| 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. |

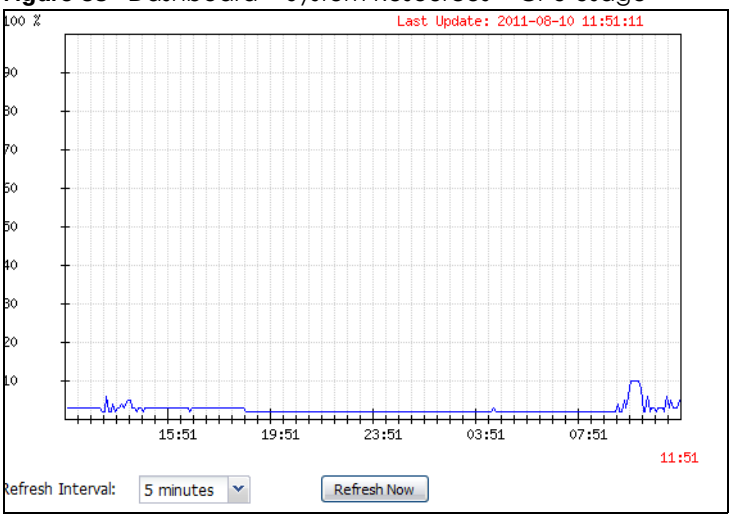
Table 14 Dashboard (continued)

| LABEL | DESCRIPTION |
|---|---|
| # | 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. |
| 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 the in the **System Resources > CPU Usage** in the dashboard.

**Figure 58** Dashboard > System Resources > CPU Usage




The following table describes the labels in this screen.

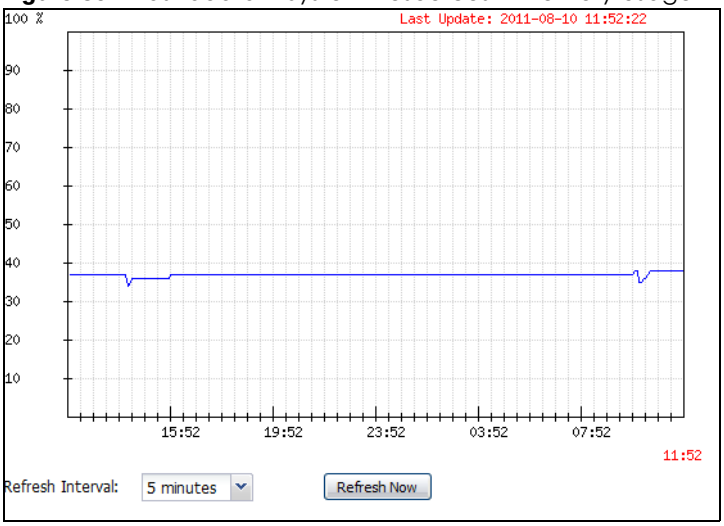
Table 15 Dashboard > System Resources > CPU Usage

| 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 the in the **System Resources > Memory Usage** in the dashboard.

**Figure 59** Dashboard > System Resources > Memory Usage




The following table describes the labels in this screen.

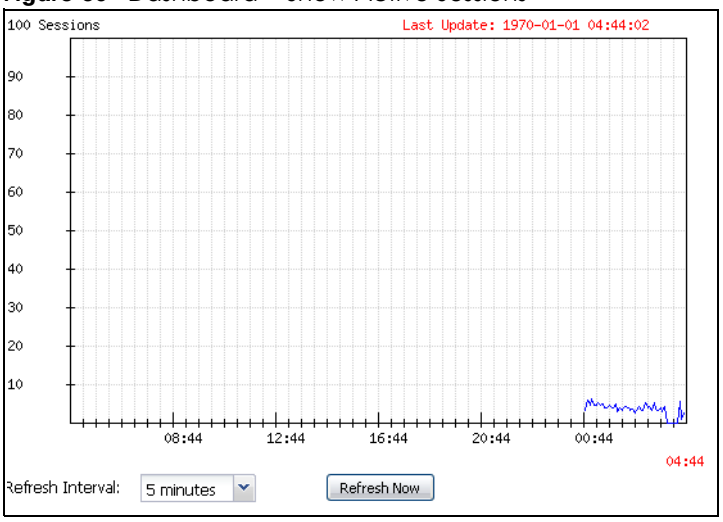
Table 16 Dashboard > System Resources > Memory Usage

| 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 the in the **System Resources > Active Sessions** in the dashboard.

**Figure 60** Dashboard > Show Active Sessions




The following table describes the labels in this screen.

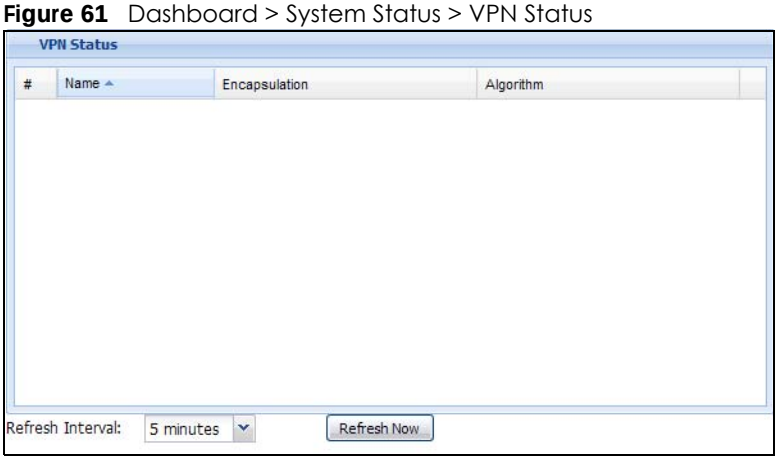
Table 17 Dashboard > Show Active Sessions

| 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.

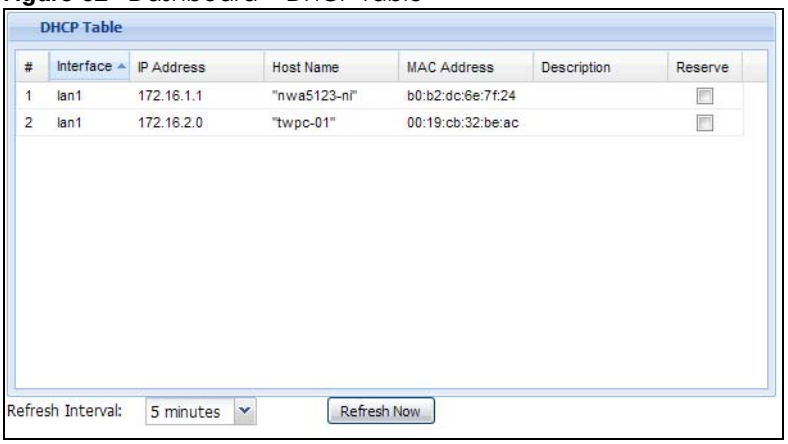
Table 18 Dashboard > VPN Status

| 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




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. |

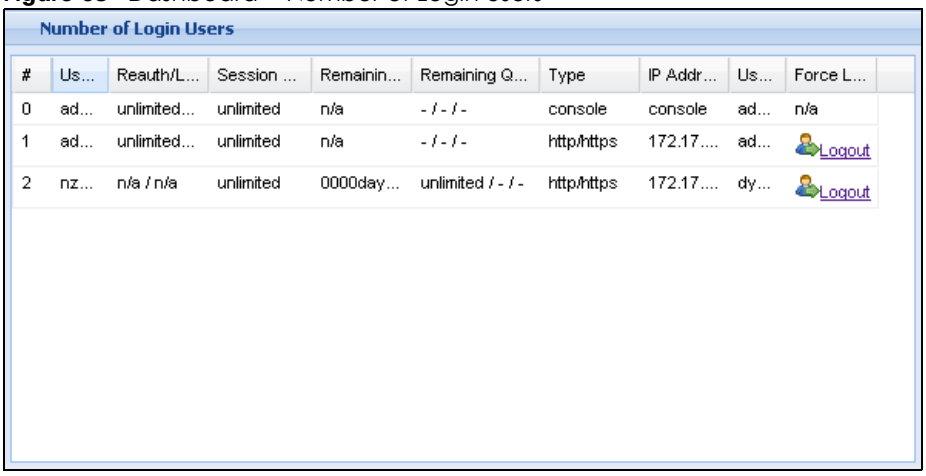
Table 19 Dashboard > DHCP Table (continued)

| LABEL | DESCRIPTION |
|---|---|
| Reserve | If this field is selected, this entry is a static DHCP entry. The IP address is reserved for the MAC address.<br>If this field is clear, this entry is a dynamic DHCP entry. The IP address is assigned to a DHCP client.<br>To create a static DHCP entry using an existing dynamic DHCP entry, select this field.<br>To remove a static DHCP entry, clear this field. |
| 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




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 34 on page 408 for more information. |
| Session Timeout | This field displays the total account of time the account (authenticated by an external server) can use to log into the UAG or access the Internet through the UAG.<br>This shows **unlimited** for an administrator account. |
| Remaining Time | This field displays the amount of Internet access time remaining for each account.<br>This shows **n/a** for an administrator account. |

Table 20 Dashboard > Number of Login Users (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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).<br><br>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.<br><br>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. |

# CHAPTER 7
# Monitor

## 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.

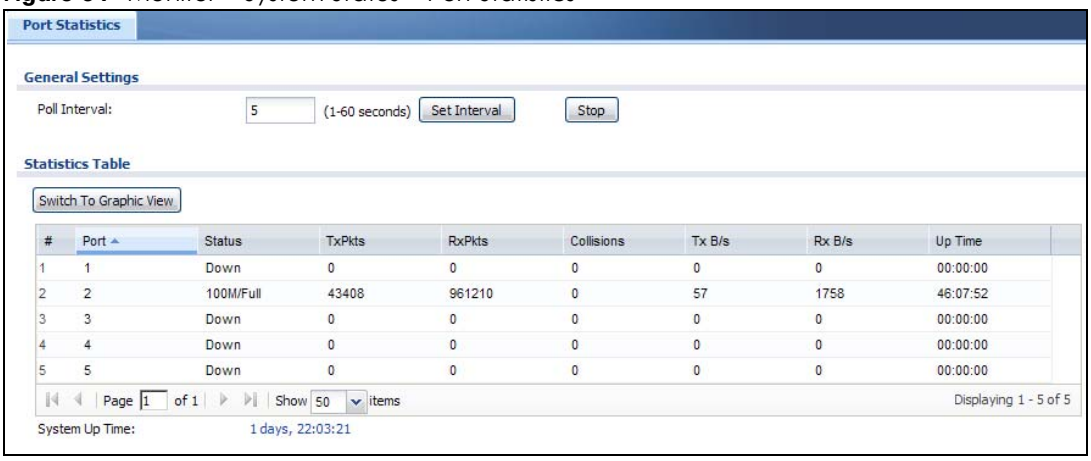
- Use the **System Status > Port Statistics** screen (see Section 7.2 on page 93) to look at packet statistics for each physical port.
- Use the **System Status > Port Statistics > Graph View** screen (see Section 7.2 on page 93) to look at a line graph of packet statistics for each physical port.
- Use the **System Status > Interface Status** screen (see Section 7.3 on page 95) 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 98) to start or stop data collection and view statistics.
- Use the **System Status > Session Monitor** screen (see Section 7.5 on page 100) to view sessions by user or service.
- Use the **System Status > DDNS Status** screen (see Section 7.6 on page 102) 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 102) 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 103) 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 104) 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 106) 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 107) to view information about a connected USB storage device.
- Use the **System Status > Ethernet Neighbor** screen (see Section 7.12 on page 108) to view and manage the UAG's neighboring devices via Layer Link Discovery Protocol (LLDP).
- Use the **Wireless > AP Information > AP List** screen (see Section 7.13 on page 110) to view which APs are currently connected to the UAG.
- Use the **Wireless > AP Information > Radio List** screen (see Section 7.14 on page 117) to view statistics about the wireless radio transmitters in each of the APs connected to the UAG.
- Use the **Wireless > Station Info > Station List** screen (see Section 7.15 on page 120) to view statistics pertaining to the connected stations (or "wireless clients").

- Use the **Wireless > Detected Device** screen (Section 7.16 on page 121) to view the wireless devices passively detected by the UAG.
- Use the **Printer Status** screen (see Section 7.17 on page 123) to view information about the connected statement printers.
- Use the **VPN 1-1 Mapping** screen (see Section 7.18 on page 123) 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 124) to display statistics for each of the VPN 1-1 mapping rules.
- Use the **VPN Monitor > IPSec** screen (see Section 7.19 on page 125) to display and manage active IPSec SAs.
- Use the **UTM Statistics > App Patrol** screen (see Section 7.20 on page 126) to start or stop data collection and view virus statistics
- Use the **UTM Statistics > Content Filter** screen (see Section 7.21 on page 128) to start or stop data collection and view content filter statistics.
- Use the **Log > View Log** screen (see Section 7.22 on page 129) 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 132) to view the UAG's current wireless AP log messages.
- Use the **Log > Dynamic Users Log** screen (see Section 7.22.2 on page 134) 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 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. |

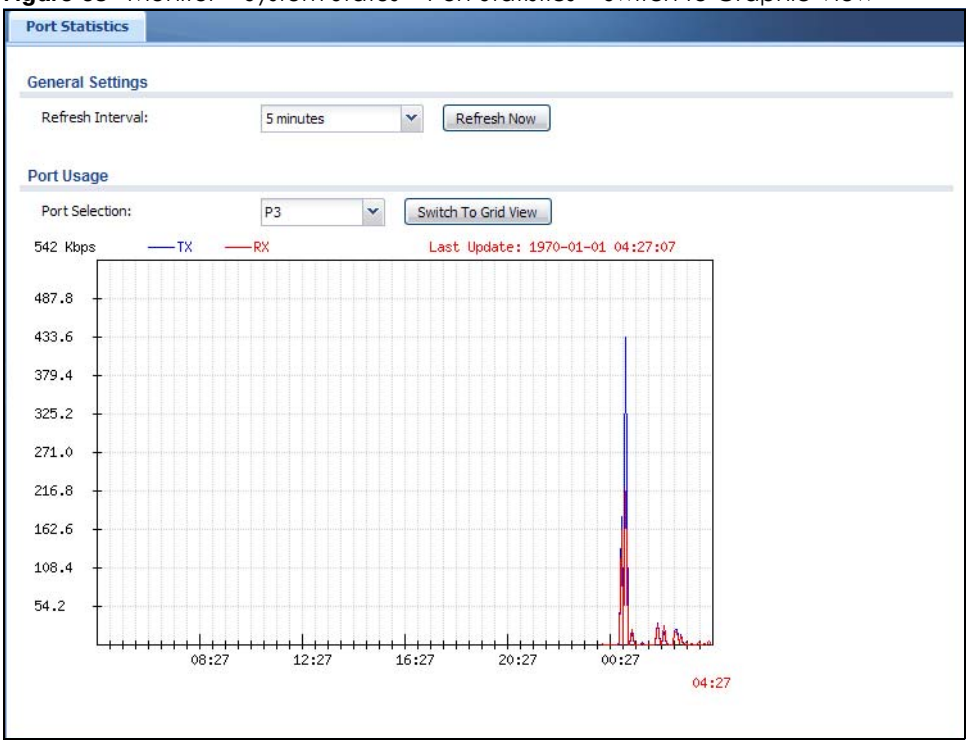
Table 21 Monitor > System Status > Port Statistics (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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.<br>**Down** - The physical port is not connected.<br>**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.

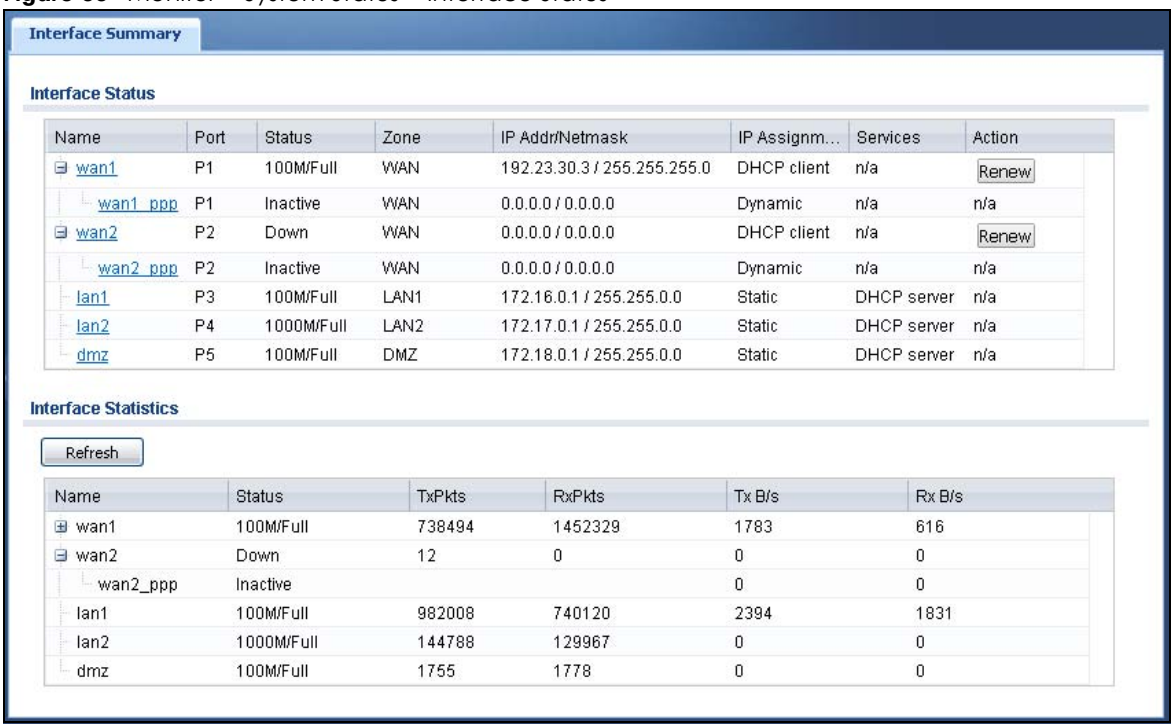
Table 22 Monitor > System Status > Port Statistics > Switch to Graphic View

| 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




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 | This field displays the current status of each interface. The possible values depend on what type of interface it is.<br><br>For Ethernet interfaces:<br><br>• **Inactive** - The Ethernet interface is disabled.<br>• **Down** - The Ethernet interface does not have any physical ports associated with it or the Ethernet interface is enabled but not connected.<br>• **Up** - The LAN Ethernet interface is enabled and connected.<br>• **Speed / Duplex** - The WAN Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (**Full** or **Half**).<br><br>For virtual interfaces, this field always displays **Up** or **Down**. If the virtual interface is disabled, it displays **Inactive**.<br><br>For VLAN and bridge interfaces, this field always displays **Up** or **Down**. If the VLAN or bridge interface is disabled, it displays **Inactive**.<br><br>For PPP interfaces:<br><br>• **Inactive** - The PPP interface is disabled.<br>• **Connected** - The PPP interface is connected.<br>• **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 | This field displays how the interface gets its IP address.<br>**Static** - This interface has a static IP address.<br>**DHCP Client** - This interface gets its IP address from a DHCP server. |
| 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 | This field displays the current status of each interface. The possible values depend on what type of interface it is.<br>For Ethernet interfaces:<br>• **Inactive** - The Ethernet interface is disabled.<br>• **Down** - The Ethernet interface does not have any physical ports associated with it or the Ethernet interface is enabled but not connected.<br>• **Up** - The LAN Ethernet interface is enabled and connected.<br>• **Speed / Duplex** - The WAN Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (**Full** or **Half**).<br>For virtual interfaces, this field always displays **Up** or **Down**. If the virtual interface is disabled, it displays **Inactive**.<br>For VLAN and bridge interfaces, this field always displays **Up** or **Down**. If the VLAN or bridge interface is disabled, it displays **Inactive**.<br>For PPP interfaces:<br>• **Inactive** - The PPP interface is disabled.<br>• **Connected** - The PPP interface is connected.<br>• **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. |

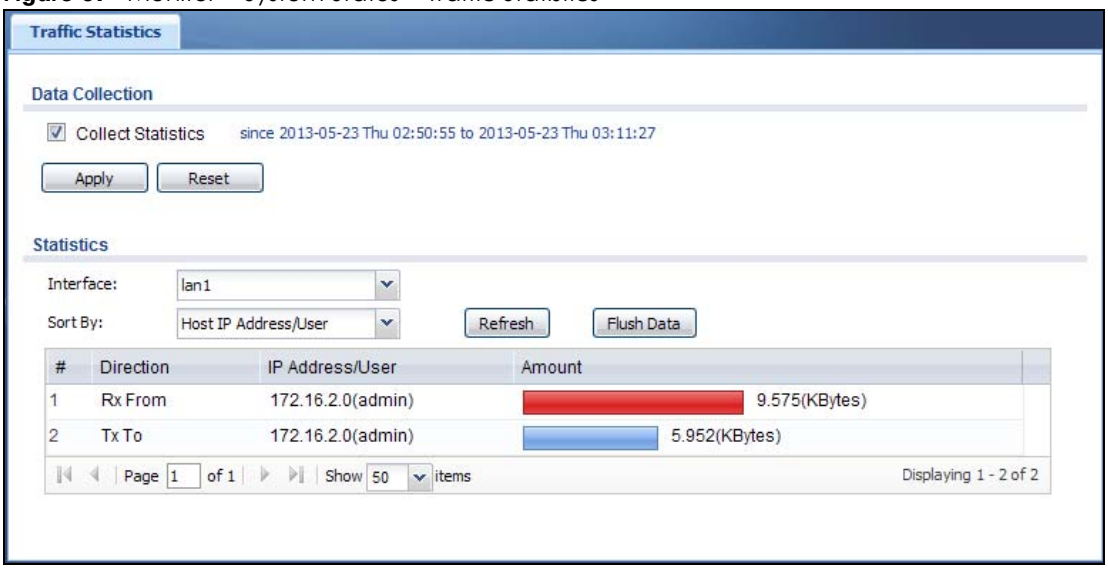
# 7.4 The Traffic Statistics Screen

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 98 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 100 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:<br>**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.<br>**Service/Port** - displays the most-used protocols or service ports and the amount of traffic for each one.<br>**Web Site Hits** - displays the most-visited Web sites and how many times each one has been visited.<br>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.<br>**RX From**- traffic is coming from the IP address or user to the UAG.<br>**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 100the next table. |
| 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 100. |
| | 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 100the next table. |
| 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.<br>**Ingress** - traffic is coming into the router through the interface<br>**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 100. |
| | 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 100the next table. |
| 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 100. |

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 x $10^{19}$ hits. |

# 7.5 The Session Monitor Screen

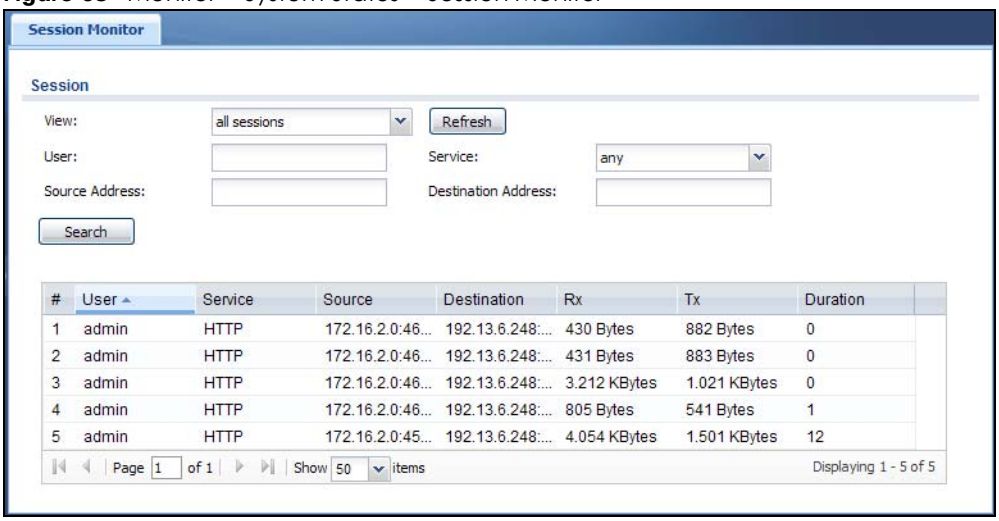
The **Session Monitor** screen displays information about all established sessions that pass through the UAG for debugging or statistical analysis. It is not possible to manage sessions in this screen. The following information is displayed.

- 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 following table describes the labels in this screen.

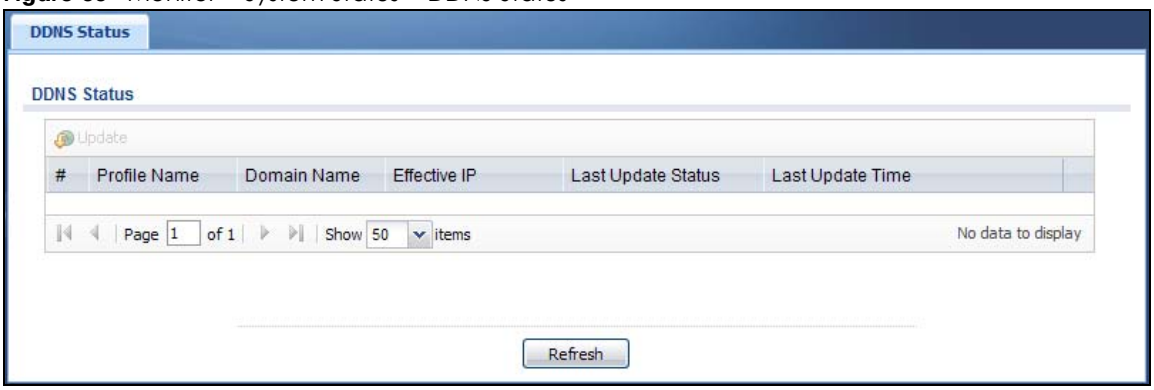
Table 26 Monitor > System Status > Session Monitor

| LABEL | DESCRIPTION |
|---|---|
| View | Select how you want the information to be displayed. Choices are:<br>**sessions by users** - display all active sessions grouped by user.<br>**sessions by services** - display all active sessions grouped by service or protocol.<br>**sessions by source IP** - display all active sessions grouped by source IP address.<br>**sessions by destination IP** - display all active sessions grouped by destination IP address.<br>**all sessions** - filter the active sessions by the **User**, **Service**, **Source Address**, and **Destination Address**, and display each session individually (sorted by user). |
| 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 39 on page 456 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 | This field displays the user in each active session.<br>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. |
| Service | This field displays the protocol used in each active session.<br>If you are looking at the **sessions by services** report, click **+** or **-** to display or hide details about a protocol's sessions. |
| Source | This field displays the source IP address and port in each active session.<br>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. |
| Destination | This field displays the destination IP address and port in each active session.<br>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. |
| 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. |
| 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.

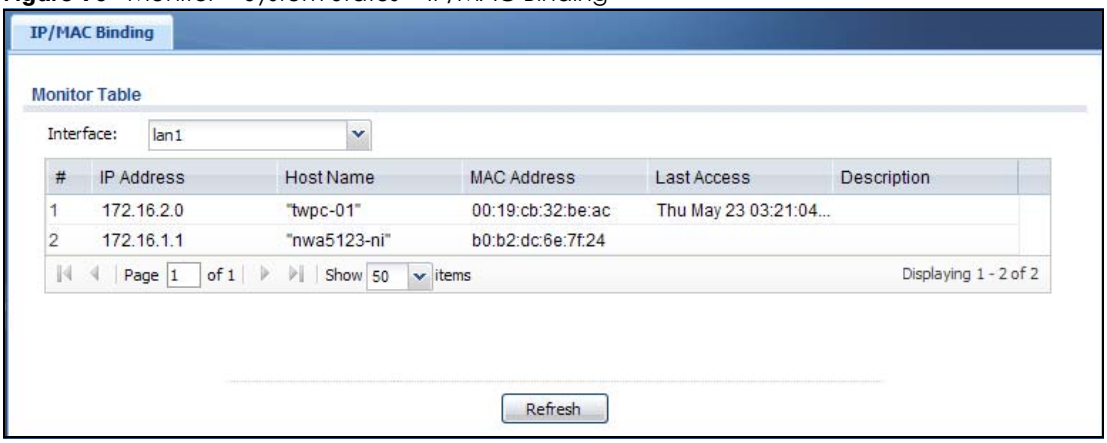
Table 27 Monitor > System Status > DDNS Status

| 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




The following table describes the labels in this screen.

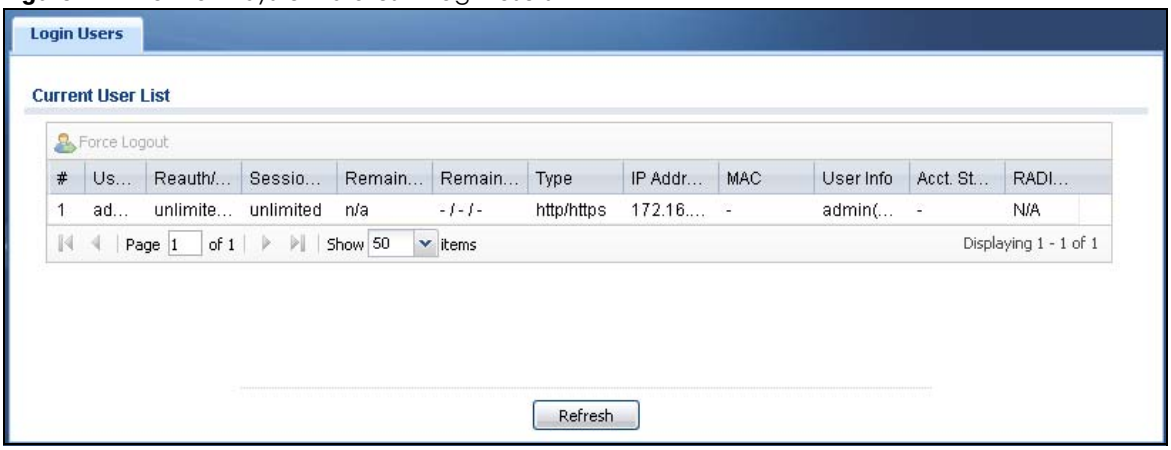
Table 28 Monitor > System Status > IP/MAC Binding

| 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



The following table describes the labels in this screen.

Table 29 Monitor > System Status > Login Users

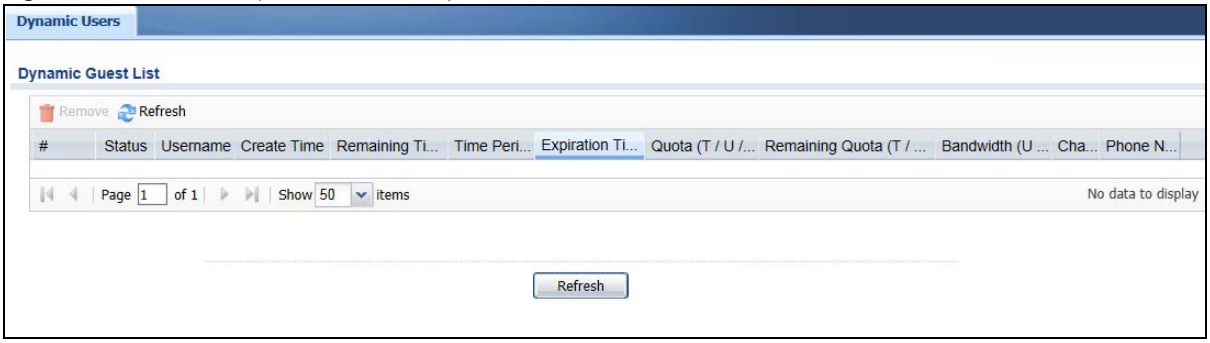
| LABEL | DESCRIPTION |
|---|---|
| Force Logout | Select a user ID and click this icon to end a user's session.<br><br>Note: You cannot use this button to terminate a user's session when he/she accesses the UAG through the console port. |
| # | This field is a sequential value and is not associated 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 34 on page 408. |
| Session Timeout | This field displays the total account of time the account (authenticated by an external server) can use to log into the UAG or access the Internet through the UAG.<br><br>This shows **unlimited** for an administrator account. |
| Remaining Time | This field displays the amount of Internet access time remaining for each account.<br><br>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 (**T**otal) or upstream data (**U**pload) and downstream data (**D**ownload).<br><br>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.<br><br>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.<br><br>**Accounting-on** means accounting is being performed for the user login.<br><br>**Accounting-off** means accounting has stopped for this user login.<br><br>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.<br><br>**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 25.3.1 on page 318 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




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.<br><br>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 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.<br><br>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.

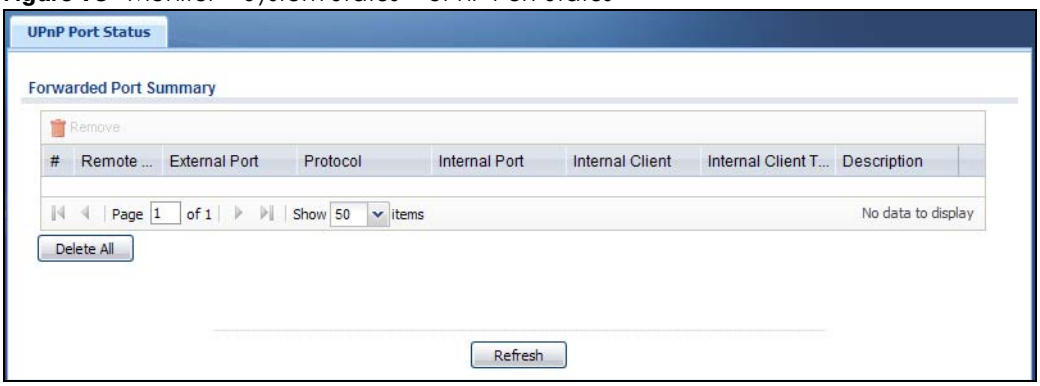
Table 31 Monitor > System Status > Dynamic Guest Icons

| 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.<br>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**.<br>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**. |
| Protocol | This field displays the protocol of the NAT mapping rule (TCP or UDP). |

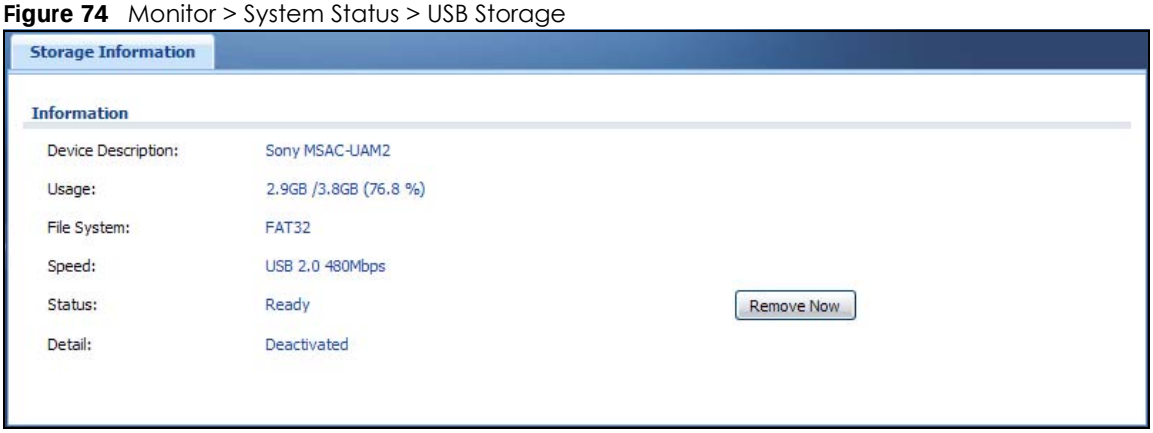
Table 32 Monitor > System Status > UPnP Port Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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 | **Ready** - you can have the UAG use the USB storage device.<br>Click **Remove Now** to stop the UAG from using the USB storage device so you can remove it.<br>**Unused** - the connected USB storage device was manually unmounted by using the **Remove Now** button or for some reason the UAG cannot mount it.<br>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.<br>**none** - no USB storage device is connected. |
| Detail | This field displays any other information the UAG retrieves from the USB storage device.<br>**Deactivated** - the use of a USB storage device is disabled (turned off) on the UAG.<br>**OutofSpace** - the available disk space is less than the disk space full threshold (see Section 45.2 on page 496 for how to configure this threshold).<br>**Mounting** - the UAG is mounting the USB storage device.<br>**Removing** - the UAG is unmounting the USB storage device.<br>**none** - the USB device is operating normally or not connected. |

# 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.

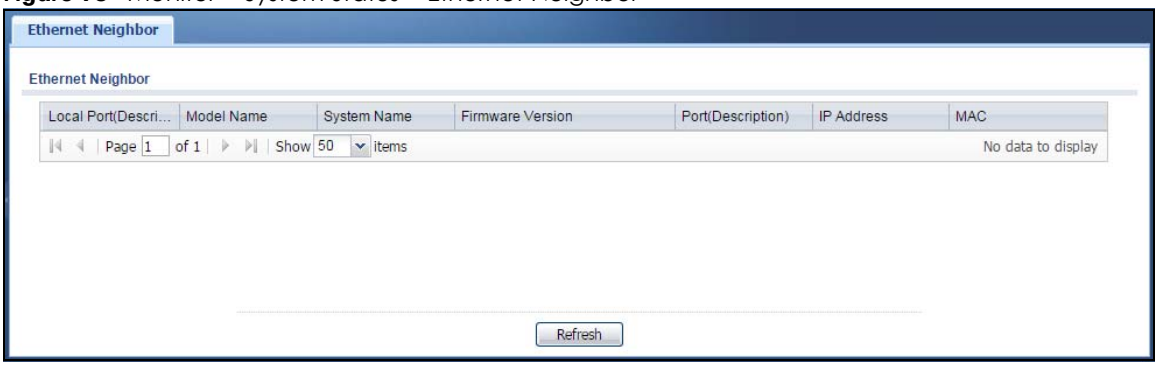
LLDP is a layer-2 protocol that allows a network device to advertise its identity and capabilities on the local network. It also allows the device to maintain and store information from adjacent devices which are directly connected to the network device. This helps you discover network changes and perform 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 following table describes the labels in this screen.

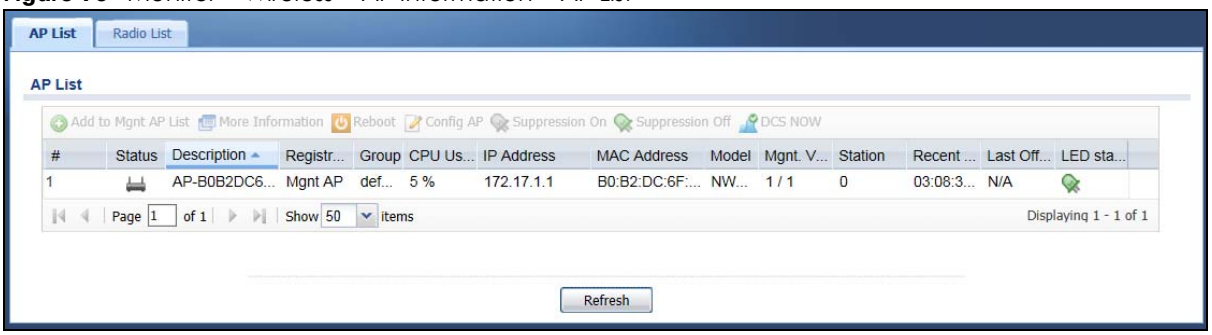
Table 34 Monitor > System Status > Ethernet Neighbor

| LABEL | DESCRIPTION |
|---|---|
| Local Port (Description) | This field displays the port of the UAG, on which the neighboring device is discovered.<br>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.<br>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.<br>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 Mgnt 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. |
| Reboot | Click this to reboot the selected AP. |
| Config AP | Click this to configure the selected AP's group, radio, port and VLAN settings. |
| Suppression On | Click this to enable the selected AP's LED suppression mode. The AP LED stays lit after the AP is ready. This button is not available if the select AP does not support suppression mode. |
| Suppression Off | Click this to disable the selected 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 select AP does not support suppression mode. |
| DCS NOW | Click this to enable DCS (Dynamic Channel Selection) on the selected AP. DCS allows the AP to automatically find a less-used channel. |
| # | 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. |
| Mgnt. 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.<br><br>**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. |

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

| LABEL | DESCRIPTION |
|---|---|
| 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. |
| LED Status | This displays the AP LED status.<br>**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.<br>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.<br>A green LED icon signifies that the AP LED suppression mode is disabled and the AP LEDs stay lit after the AP is ready.<br>A sun icon signifies that the AP's locator LED is blinking.<br>A circle signifies that the AP's locator LED is extinguished. |
| 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

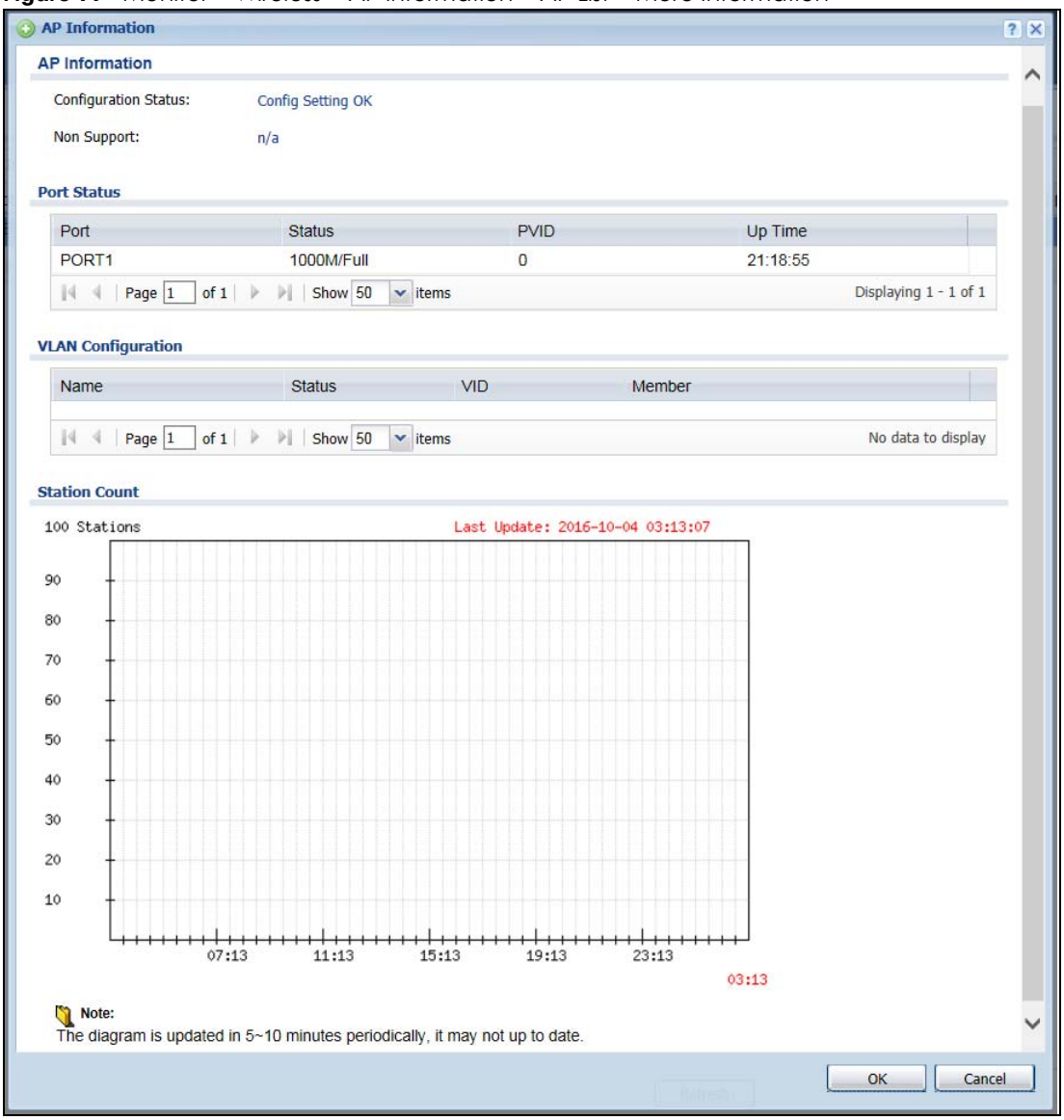
| LABEL | DESCRIPTION |
|---|---|
| | This AP is not on the management list. |
| | This AP is on the management list and online. |
| | This AP is in the process of having its firmware updated. |
| | This AP is on the management list but offline. |
| | This indicates one of the following cases:<br>• This AP has a runtime management VLAN ID setting that conflicts with the VLAN ID setting on the Access Controller (the UAG).<br>• A setting the UAG assigns to this AP does not match the AP's capability. |
| | This AP is offline and in the process of having its firmware updated. |

## 7.13.1 Station Count of AP More Information

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 > More Information




The following table describes the labels in this screen.

Table 37 Monitor > Wireless > AP Information > AP List > More Information

| LABEL | DESCRIPTION |
|---|---|
| AP Information | |
| 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. |

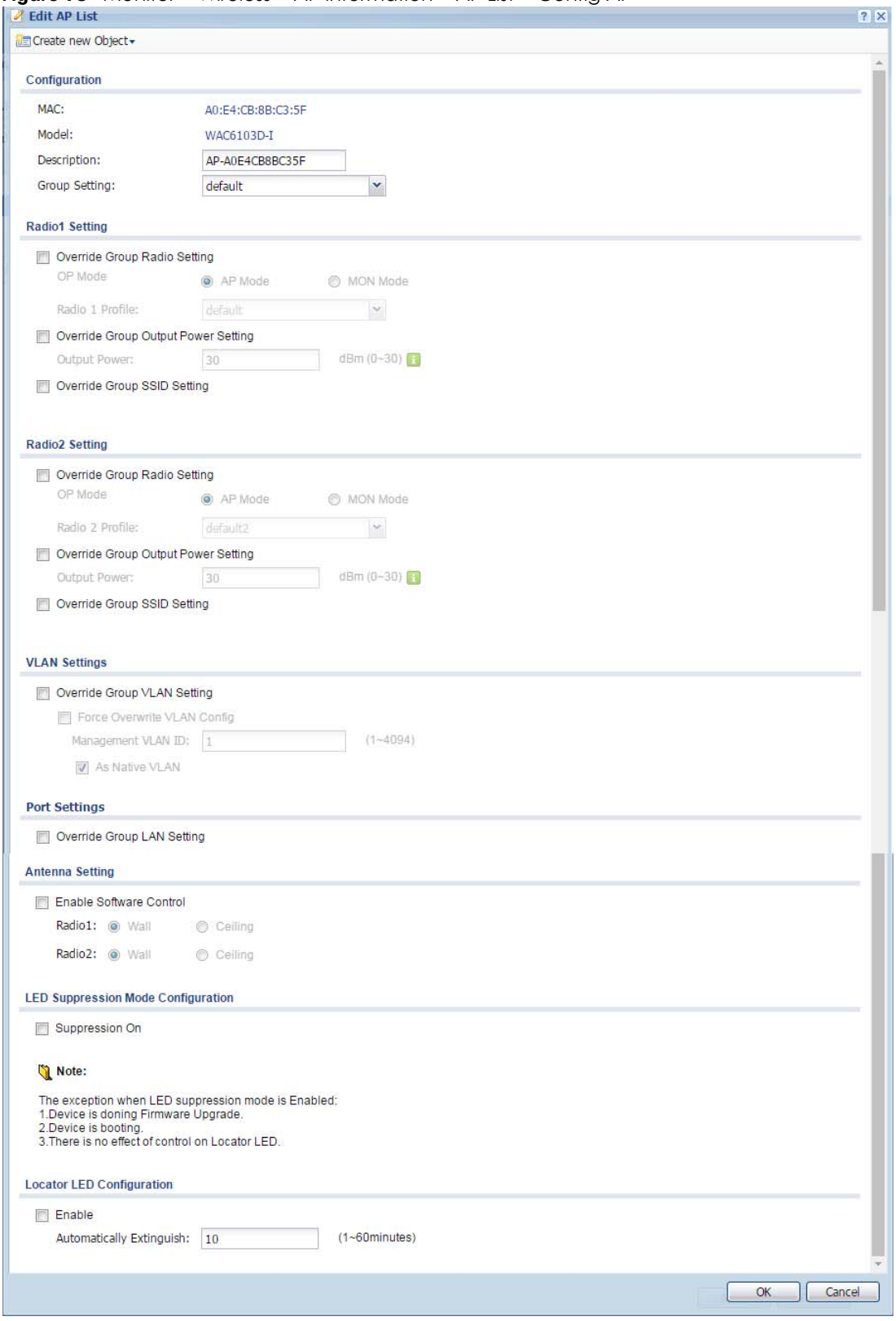
Table 37 Monitor > Wireless > AP Information > AP List > More Information (continued)

| LABEL | DESCRIPTION |
|---|---|
| Status | This field displays the current status of each physical port on the AP.<br>**Down** - The port is not connected.<br>**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.<br>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. |
| 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. |
| OK | Click **OK** to save your changes back to the UAG. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 7.13.2 Config AP

Select an AP and click the **Config AP** button in the **Monitor > Wireless > AP List** table to display this screen.

**Figure 78** Monitor > Wireless > AP Information > AP List > Config AP



Each field is described in the following table.

Table 38 Monitor > Wireless > AP Information > AP List > Config AP

| 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. |
| Group Setting | Select the group to which this AP belongs. |
| Radio1/2 Setting | |
| Override Group Radio Setting | Select this option to overwrite the AP radio settings with the settings you configure. |
| OP Mode | Select the operating mode for radio 1 or radio 2.<br>**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).<br>**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.<br>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. |
| Override Group Output Power Setting | Select this option to overwrite the AP output power setting with the setting you configure here. |
| Output Power | Set the maximum output power of the AP.<br>If there is a high density of APs in an area, decrease the output power of the managed AP to reduce interference with other APs.<br>Note: Reducing the output power also reduces the UAG's effective broadcast radius. |
| Override Group SSID Setting | Select this option to overwrite the AP SSID profile setting with the setting you configure here.<br>This section allows you to associate an SSID profile with the radio. |
| Edit | Select an SSID and click this button to reassign it. The selected SSID becomes editable immediately upon clicking. |
| # | This is the index number of the SSID profile. You can associate up to eight SSID profiles with an AP radio. |
| SSID Profile | Indicates which SSID profile is associated with this radio profile. |
| VLAN Settings | This section is not available when you are editing the local AP's settings. |
| Override Group VLAN Setting | Click on this to modify VLAN Settings of the selected AP. |
| Force Override 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. |

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

| LABEL | DESCRIPTION |
|---|---|
| Port Settings | |
| Override Group LAN Setting | Click on this to modify the selected AP's LAN settings. |
| 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 a port, select it and click **Activate**. |
| Inactivate | To turn off a port, select it and click **Inactivate**. |
| # | 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.<br>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 | |
| 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 erase it from the VLAN configuration list. |
| Activate | To turn on a VLAN, select it and click **Activate**. |
| Inactivate | To turn off a VLAN, select it and click **Inactivate**. |
| # | 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. |
| Antenna Setting | |
| Enable Software Control | Click on this to allow the AP's software control.<br>Note: This criterion only appears for APs with an antenna switch. |
| Radio 1/2 | Select the antenna orientation of the radio (**Wall** or **Ceiling**). |
| LED Suppression Mode Configuration | |
| Suppression On | Click this button to enable the selected 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. |
| Locator LED Configuration<br>Note: This section is available only when the AP has a locator LED. | |
| Turn On/Turn Off | When the locator LED is off, click the **Turn On** button to activate the locator function. It will show the actual location of the AP between several devices in the network.<br>If the locator LED is blinking, click the **Turn Off** button to stop the locator LED from blinking immediately. |
| Automatically Extinguish After | Enter a time interval between 1 and 60 minutes to stop the locator LED from blinking. The locator LED will start to blink for the number of minutes set here.<br>If you make changes to the time default setting, it will be stored as the default when the AP restarts. |

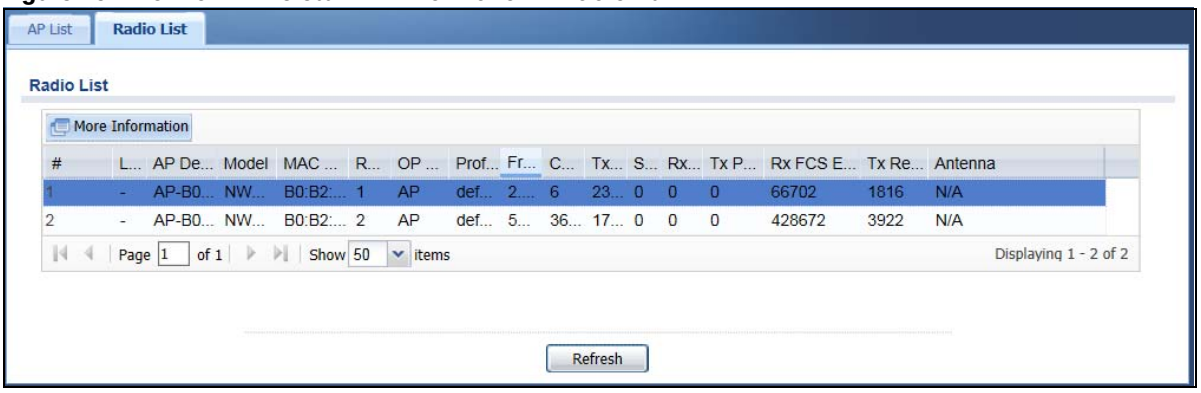
Table 38 Monitor > Wireless > AP Information > AP List > Config AP (continued)

| LABEL | DESCRIPTION |
|---|---|
| OK | Click **OK** to save your changes back to the UAG. |
| Cancel | Click **Cancel** to close the window with changes unsaved. |

# 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 79** Monitor > Wireless > AP Information > Radio List




The following table describes the labels in this screen.

Table 39 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. |
| Frequency Band | This indicates the wireless frequency currently being used by the radio.<br>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. |

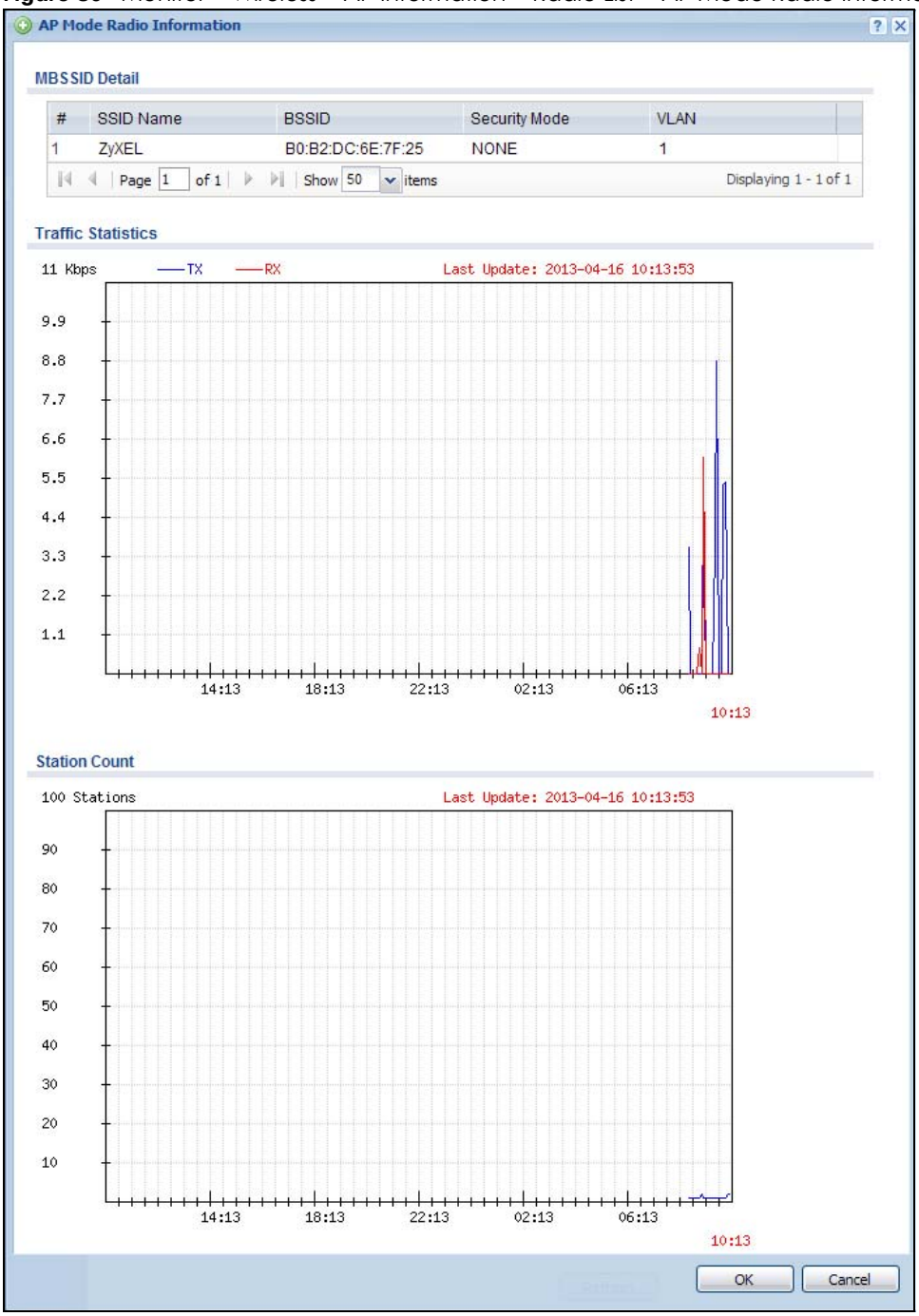
Table 39 Monitor > Wireless > AP Information > Radio List (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. |
| Antenna | This indicates the antenna orientation for the radio (**Wall** or **Ceiling**).<br>This shows **N/A** if the AP does not allow you to adjust coverage depending on the orientation of the antenna for each radio using the web configurator or a physical switch. |

## 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 80** Monitor > Wireless > AP Information > Radio List > AP Mode Radio Information



The following table describes the labels in this screen.

Table 40 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 81** Monitor > Wireless > Station List

The following table describes the labels in this screen.

Table 41 Monitor > Wireless > Station List

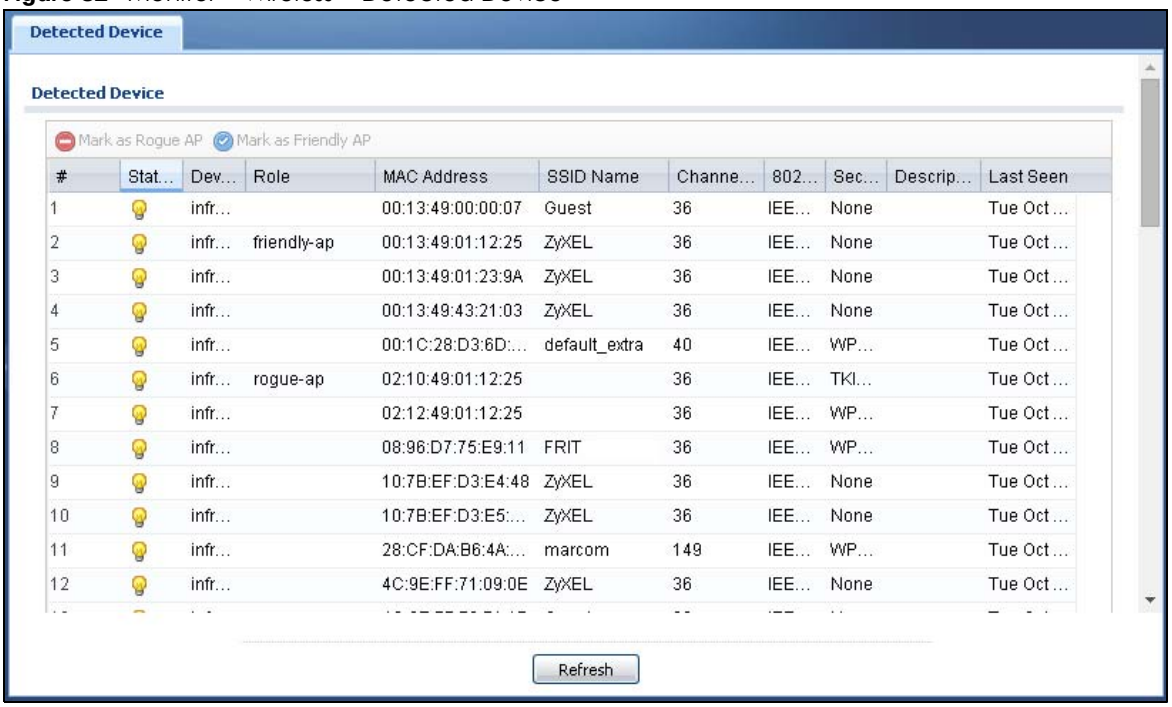
| LABEL | DESCRIPTION |
|---|---|
| SSID Name | This field displays the SSID name with which at least one station is associated.<br>Click + or - to display or hide details about wireless stations that connected to the SSID. |
| # | This is the station's index number in this list. |
| MAC Address | This 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 82** Monitor > Wireless > Detected Device




The following table describes the labels in this screen.

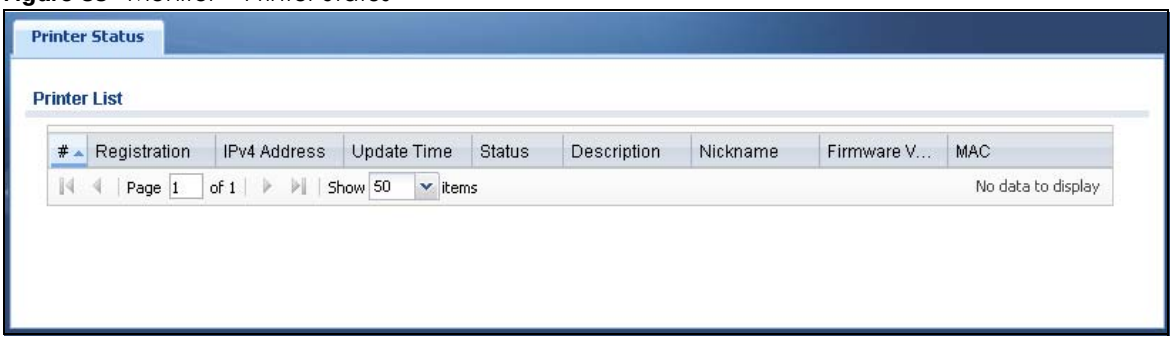
Table 42 Monitor > Wireless > Rogue AP > Detected Device

| 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 160). |
| 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 160). |
| # | 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 160). |
| 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 83** Monitor > Printer Status




The following table describes the labels in this screen.

Table 43 Monitor > Printer Status

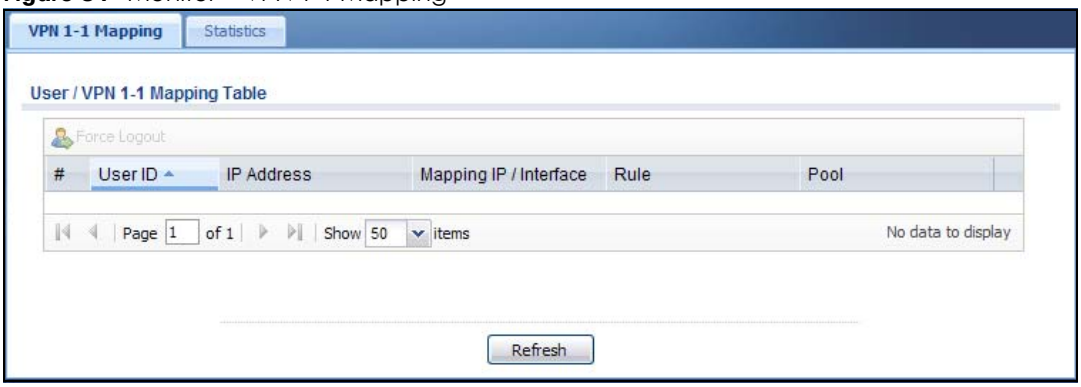
| LABEL | DESCRIPTION |
|---|---|
| Printer List | |
| # | This is the index number of the printer in the list. |
| Registration | This field shows that the printer is added to the managed printer list (**Mgnt Printer**). |
| IPv4 Address | This field displays the IP address of the printer that you configured in the **Configuration > Printer > Printer Manager** screen. |
| Update Time | This field displays the date and time the UAG last synchronized with the printer.<br>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.<br>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 84** Monitor > VPN 1-1 Mapping




The following table describes the labels in this screen.

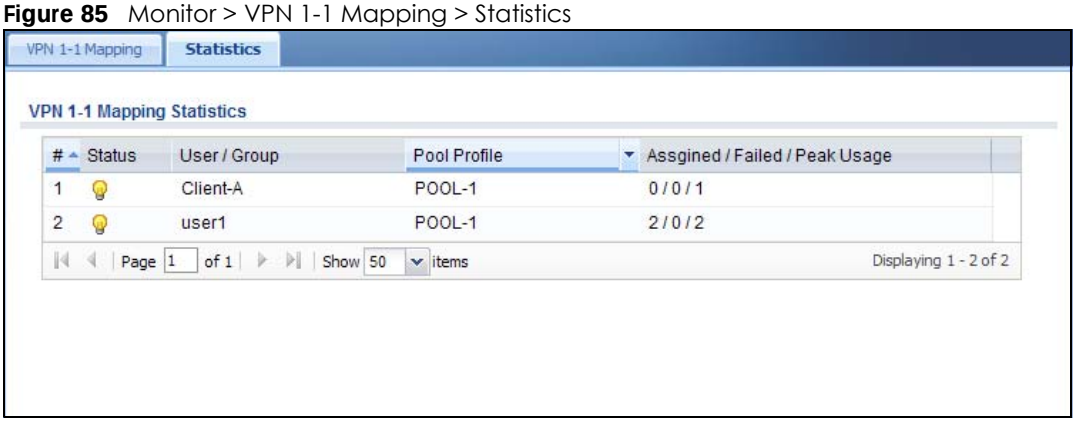
Table 44 Monitor > VPN 1-1 Mapping

| LABEL | DESCRIPTION |
|---|---|
| User / VPN 1-1 Mapping Table | |
| 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 85** Monitor > VPN 1-1 Mapping > Statistics



The following table describes the labels in this screen.

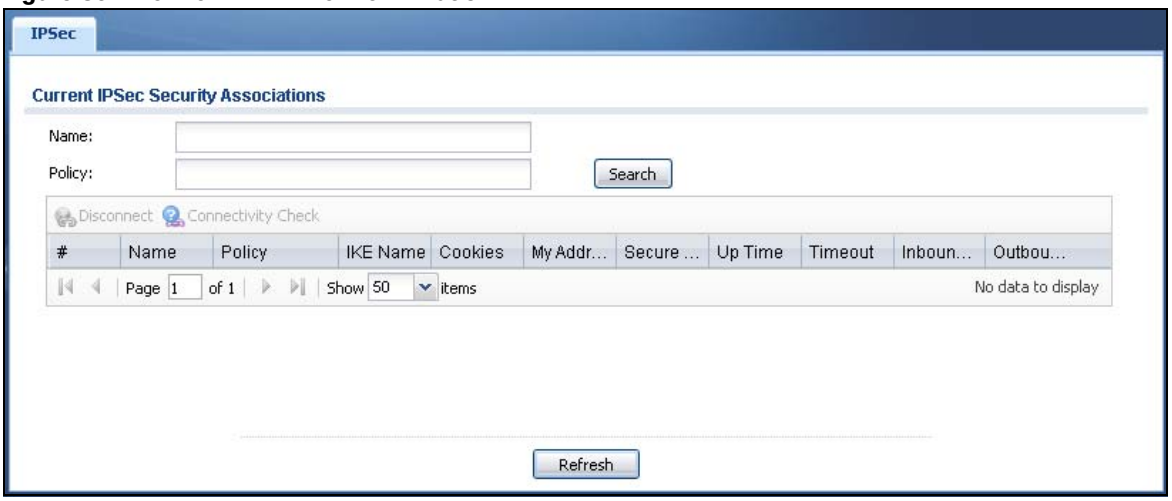
Table 45 Monitor > VPN 1-1 Mapping > Statistics

| LABEL | DESCRIPTION |
|---|---|
| APN 1-1 Mapping Statistics | |
| # | 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 86** Monitor > VPN Monitor > IPSec




Each field is described in the following table.

Table 46 Monitor > VPN Monitor > IPSec

| LABEL | DESCRIPTION |
|---|---|
| Current IPSec Security Associations | |
| 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 _+-.()!$*^:? \| {}[]<>/ characters. See Section 7.19.1 on page 126 for more details. |
| Policy | Enter the IP address(es) or names of the local and remote policies for an IPSec SA and click **Search** to find it. You can use a keyword or regular expression. Use up to 30 alphanumeric and _+-.()!$*^:? \| {}[]<>/ characters. See Section 7.19.1 on page 126 for more details. |
| Search | Click this button to search for an IPSec SA that matches the information you specified above. |

Table 46 Monitor > VPN Monitor > IPSec (continued)

| LABEL | DESCRIPTION |
|---|---|
| Disconnect | Select an IPSec SA and click this button to disconnect it. |
| 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. |
| # | 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.

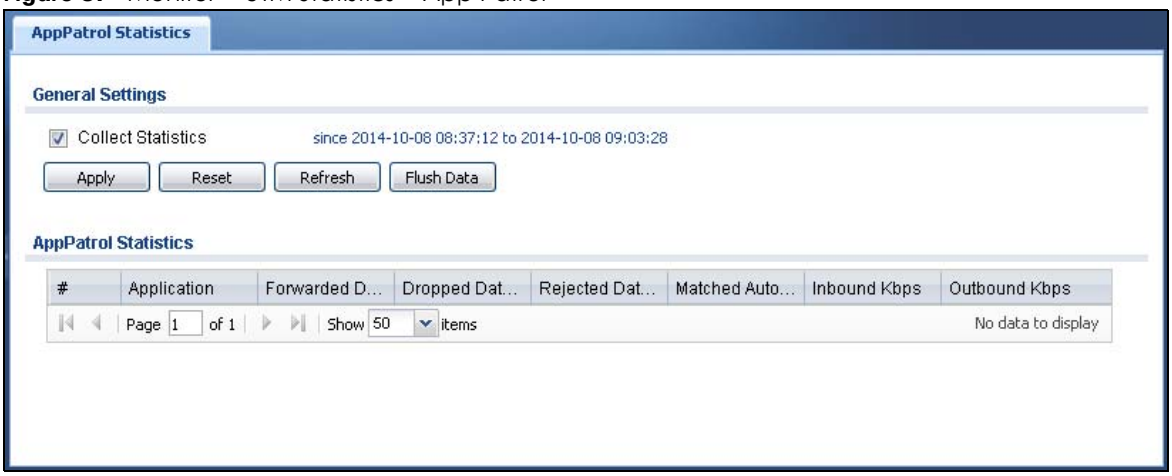
The whole VPN connection or policy name has to match if you do not use a question mark or asterisk.

## 7.20 TheApp 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 87** Monitor > UTM Statistics > App Patrol




The following table describes the labels in this screen.

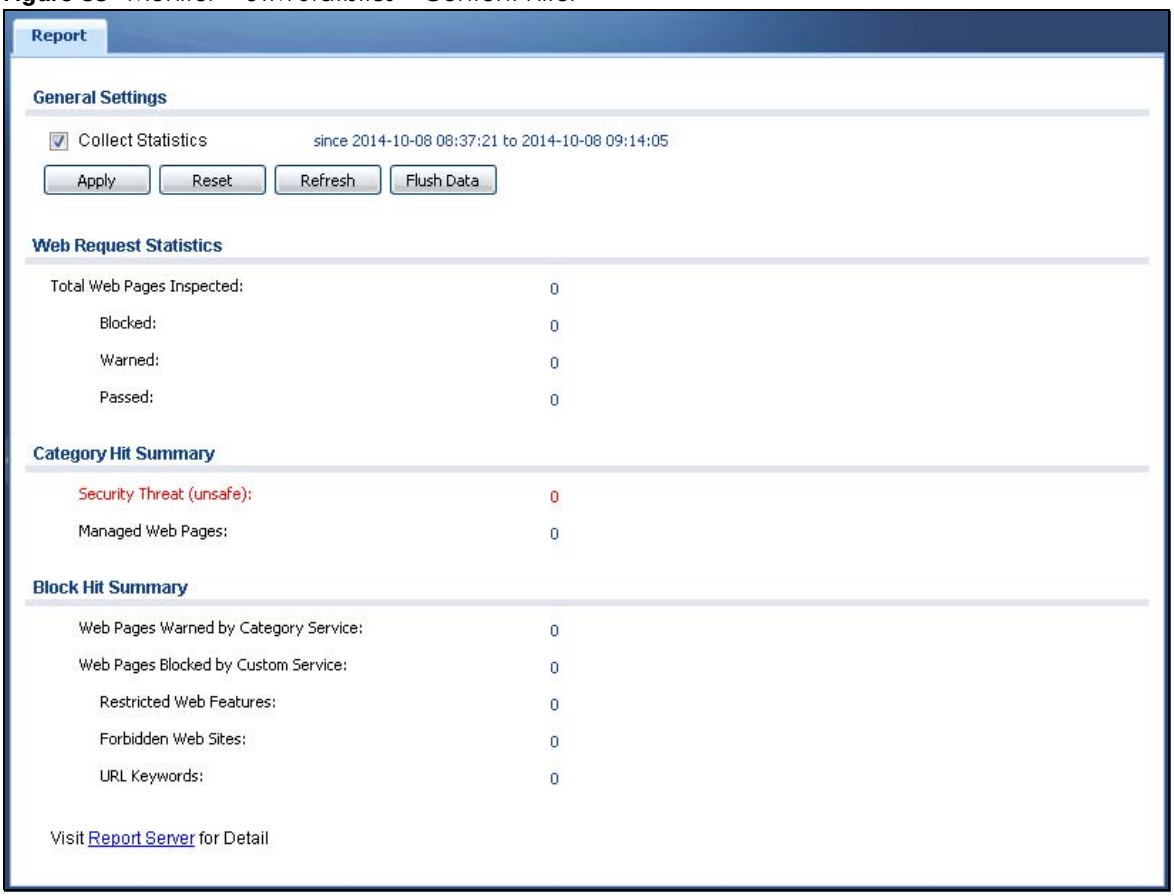
Table 47 Monitor > UTM Statistics > App Patrol

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Collect Statistics | Select this check box to have the UAG collect app patrol statistics.<br>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. |
| 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 TheContent Filter Screen

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

**Figure 88** Monitor > UTM Statistics > Content Filter




The following table describes the labels in this screen.

Table 48 Monitor > UTM Statistics > Content Filter

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Collect Statistics | Select this check box to have the UAG collect content filtering statistics.<br>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. |

Table 48 Monitor > UTM Statistics > Content Filter (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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.

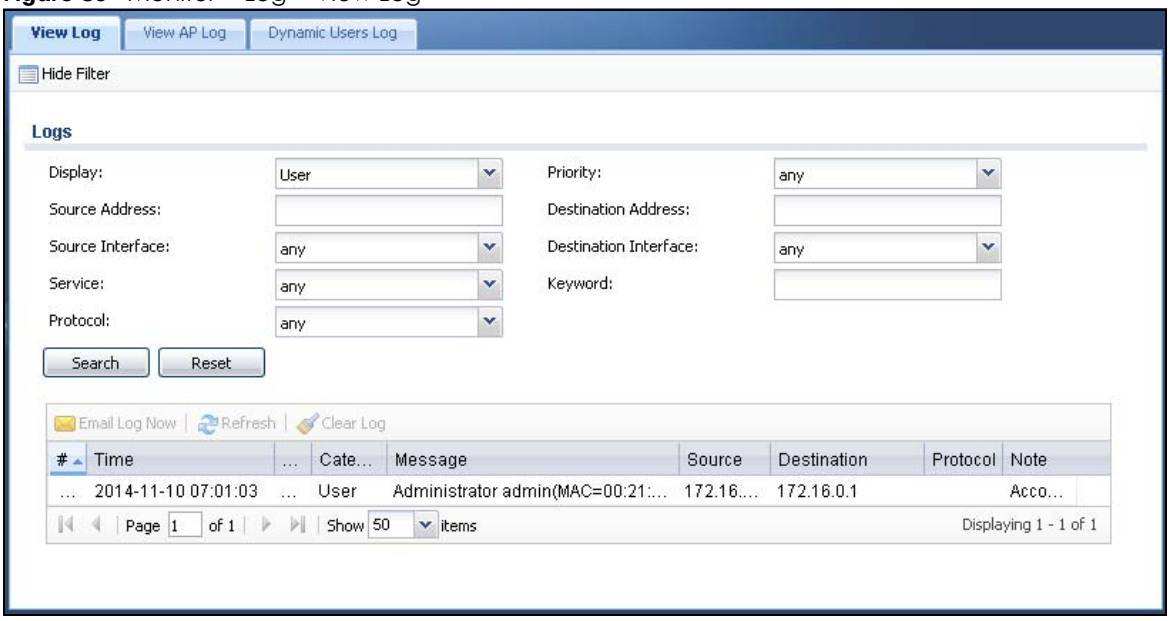
To access this screen, click **Monitor > Log > View Log**. The log is displayed in the following screen.

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 89** Monitor > Log > View Log




The following table describes the labels in this screen.

Table 49 Monitor > Log > View Log

| LABEL | DESCRIPTION |
|---|---|
| Show Filter / Hide Filter | Click this button to show or hide the filter settings.<br>If the filter settings are hidden, the **Display**, **Email Log Now**, **Refresh**, and **Clear Log** fields are available.<br>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. |
| Logs | |
| 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**. |
| 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. |

Table 49 Monitor > Log > View Log (continued)

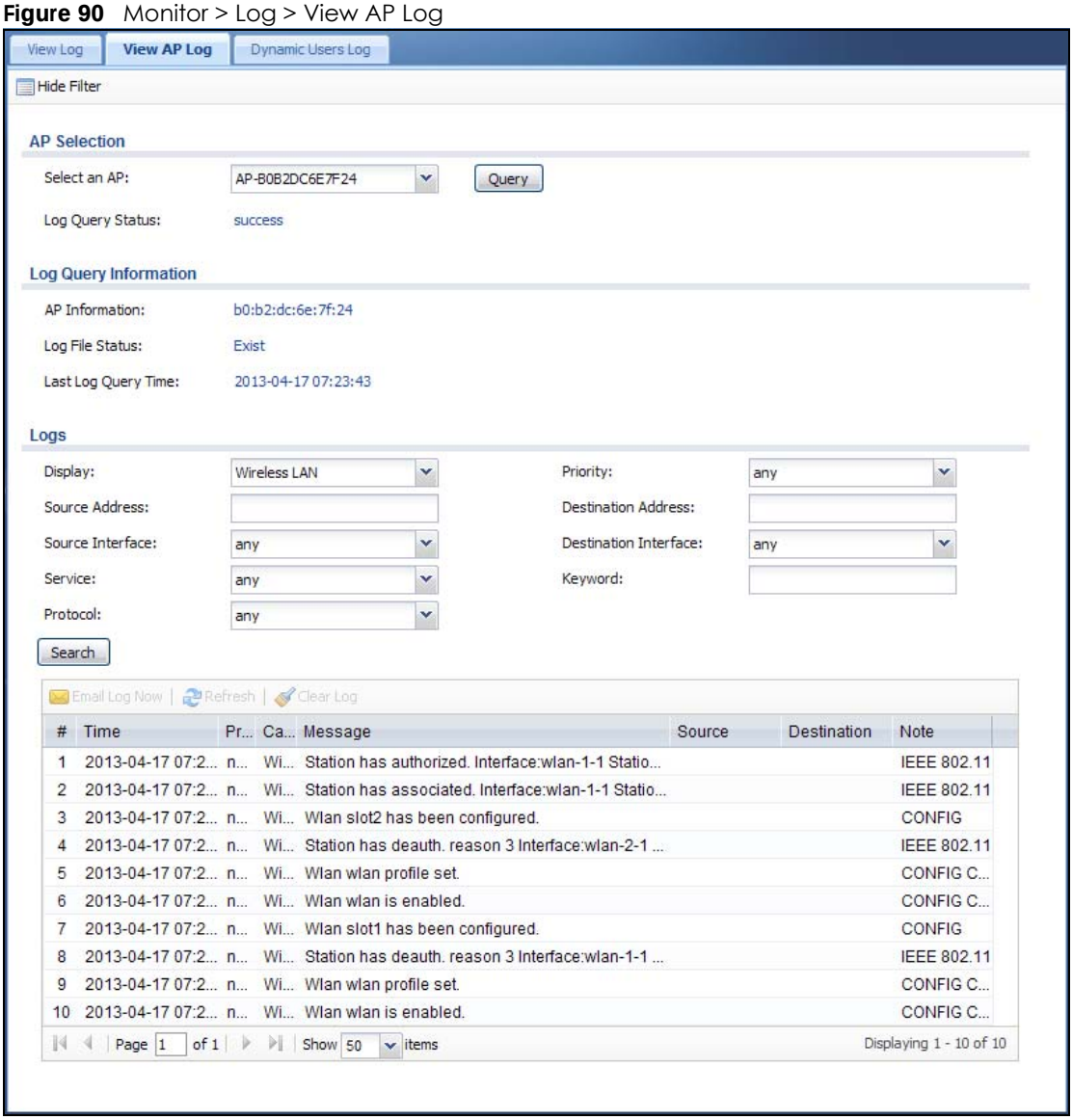
| LABEL | DESCRIPTION |
|---|---|
| Protocol | This displays when you show the filter. Select a service protocol whose log messages you would like to see. |
| Search | This displays when you show the filter. Click this button to update the log using the current filter settings. |
| Reset | This displays 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 46.3.2 on page 547). |
| 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 261 on page 549). 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. |
| Destination | This field displays the destination IP address and the port number of the event 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 90** Monitor > Log > View AP Log




The following table describes the labels in this screen.

Table 50 Monitor > Log > View AP Log

| LABEL | DESCRIPTION |
|---|---|
| Show/Hide Filter | Click this to show or hide the AP log filter. |
| AP Selection | |
| Select an AP | Select an AP from the list and click **Query** to view its log messages. |

Table 50 Monitor > Log > View AP Log (continued)

| LABEL | DESCRIPTION |
|---|---|
| Log Query Status | This indicates the current log query status.<br>**init** - Indicates the query has not been initialized.<br>**querying** - Indicates the query is in process.<br>**fail** - Indicates the query failed.<br>**success** - Indicates the query succeeded. |
| Log Query Information | |
| 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. |
| Logs | |
| Display | Select the log file from the specified AP that you want displayed. |
| Priority | Select a priority level to use for filtering displayed log messages.<br>Note: This criterion only appears when you **Show Filter**. |
| Source Address | Enter a source IP address to display only the log messages that include it.<br>Note: This criterion only appears when you **Show Filter**. |
| Destination Address | Enter a destination IP address to display only the log messages that include it.<br>Note: This criterion only appears when you **Show Filter**. |
| Source Interface | Enter a source interface to display only the log messages that include it.<br>Note: This criterion only appears when you **Show Filter**. |
| Destination Interface | Enter a destination interface to display only the log messages that include it.<br>Note: This criterion only appears when you **Show Filter**. |
| Service | Select a service type to display only the log messages related to it.<br>Note: This criterion only appears when you **Show Filter**. |
| Keyword | Enter a keyword to display only the log messages that include it.<br>Note: This criterion only appears when you **Show Filter**. |
| Protocol | Select a protocol to display only the log messages that include it.<br>Note: This criterion only appears when you **Show Filter**. |
| 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. |
| Category | This indicates the selected log message's category. |

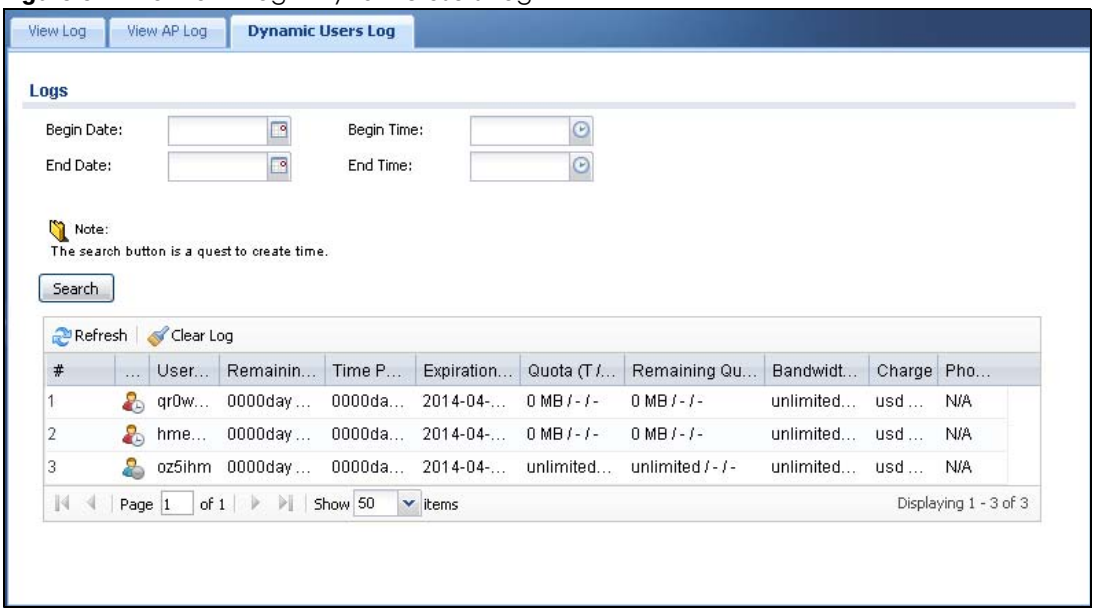
Table 50 Monitor > Log > View AP Log (continued)

| LABEL | DESCRIPTION |
|---|---|
| Message | This displays content of the selected log message. |
| Source | This displays the source IP address of the selected log message. |
| Destination | This displays the source IP address of the selected 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 91** Monitor > Log > Dynamic Users Log




The following table describes the labels in this screen.

Table 51 Monitor > Log > Dynamic Users Log

| LABEL | DESCRIPTION |
|---|---|
| Logs | |
| 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. |
| 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. |

Table 51 Monitor > Log > Dynamic Users Log (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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.<br>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. |

# CHAPTER 8
# 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 137) to register your UAG with myZyxel.com.
- Use the **Service** screen (see Section 8.3 on page 137) to display the status of your service registrations and upgrade licenses.
- Use the **Signature Update > AppPatrol** screen (see Section 8.4 on page 138) 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 92** 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 93** Configuration > Licensing > Registration > Service

The following table describes the labels in this screen.

Table 52 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.<br>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.<br>It displays **0** if this field does not apply to a service. |
| License Refresh | |
| 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.

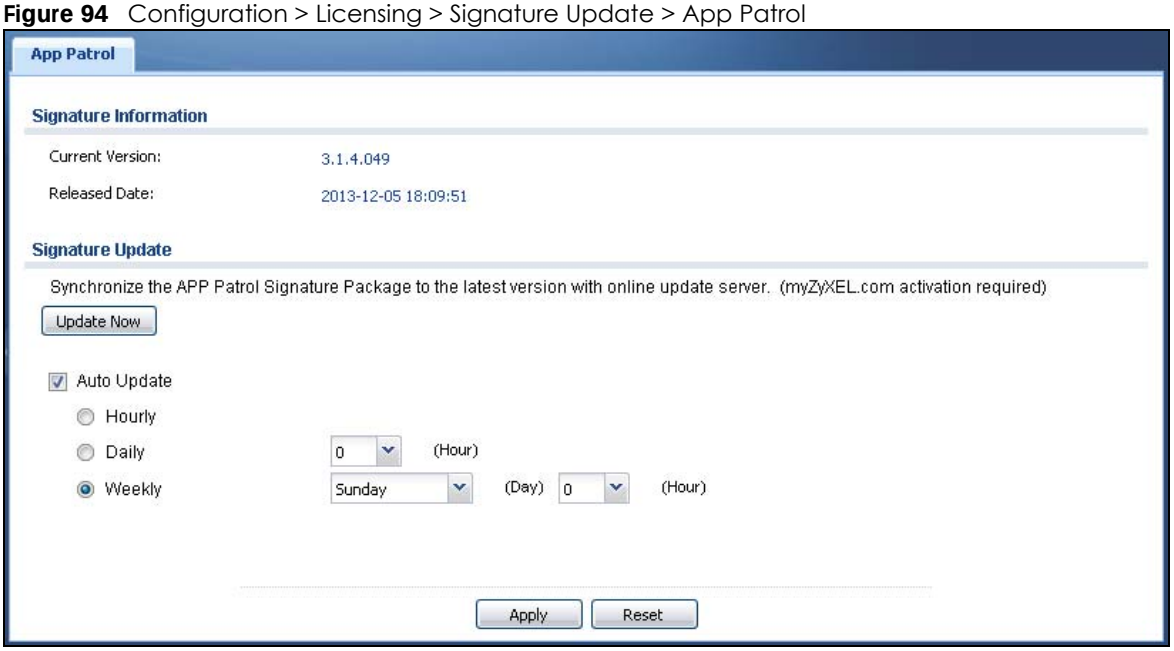
You need to create an account at myZyxel.com, register your UAG and then subscribe for application patrol service in order to be able to download new packet inspection signatures from myZyxel.com (see the **Registration** screens). Use the **Signature Update > App Patrol** screen to schedule or immediately 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 94** Configuration > Licensing > Signature Update > App Patrol




The following table describes the fields in this screen.

Table 53 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.<br>You should select a time when your network is not busy for minimal interruption. |
| Hourly | Select this option to have the UAG check for new signatures every hour. |

Table 53 Configuration > Licensing > Signature Update > App Patrol (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. |

# CHAPTER 9
# Wireless

## 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 142) sets how the UAG allows new APs to connect to the network.
- The **AP Management** screen (Section 9.3 on page 143) manages all of the APs connected to the UAG.
- The **MON Mode** screen (Section 9.4 on page 160) allows you to assign APs either to the rogue AP list or the friendly AP list.
- The **Auto Healing** screen (Section 9.5 on page 162) turns on the auto healing feature to extend the wireless service coverage area of the managed APs when one of the APs fails.
- The **RTLS** screen (Section 9.6 on page 163) to allow the UAG to track battery-powered Wi-Fi tags attached to APs.

### 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.

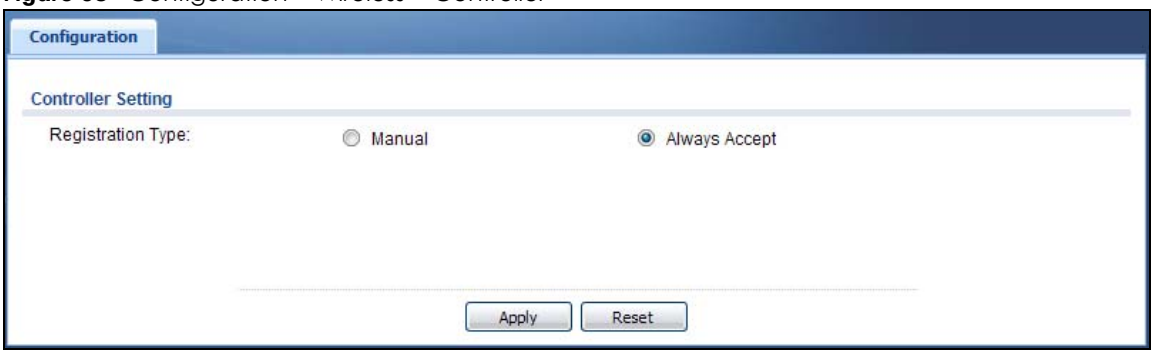
#### Load Balancing (Wireless)

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 95** Configuration > Wireless > Controller




Each field is described in the following table.

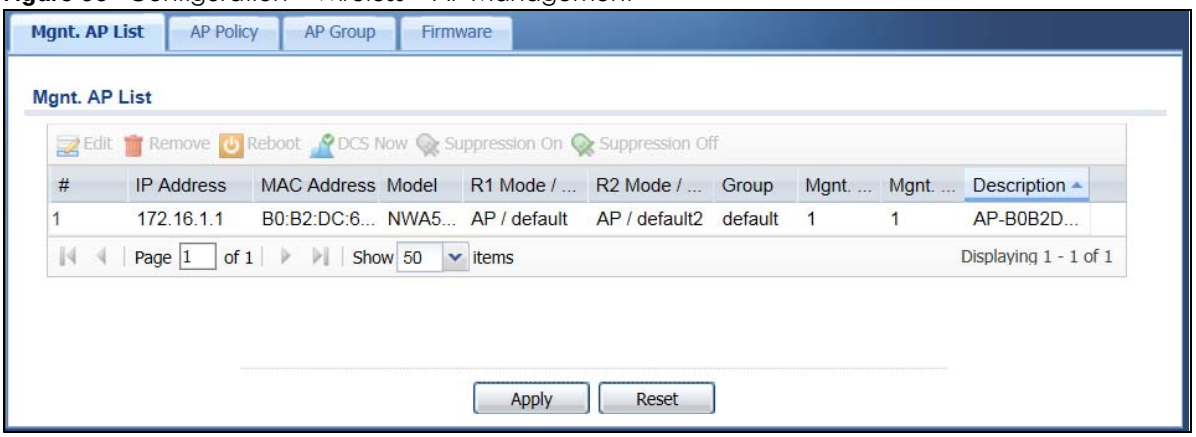
Table 54 Configuration > Wireless > Controller

| 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.<br><br>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 121.<br><br>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 96** Configuration > Wireless > AP Management




Each field is described in the following table.

Table 55 Configuration > Wireless > AP Management

| LABEL | DESCRIPTION |
|---|---|
| Mgnt. AP List | |
| 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.<br><br>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. |
| DCS Now | Select one or multiple APs and click this button to use DCS (Dynamic Channel Selection) to allow the AP to automatically find a less-used channel in an environment where there are many APs and there may be interference.<br><br>Note: You should have enabled DCS in the applied AP radio profile before the APs can use DCS. |
| Suppression 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. |
| Suppression 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. |

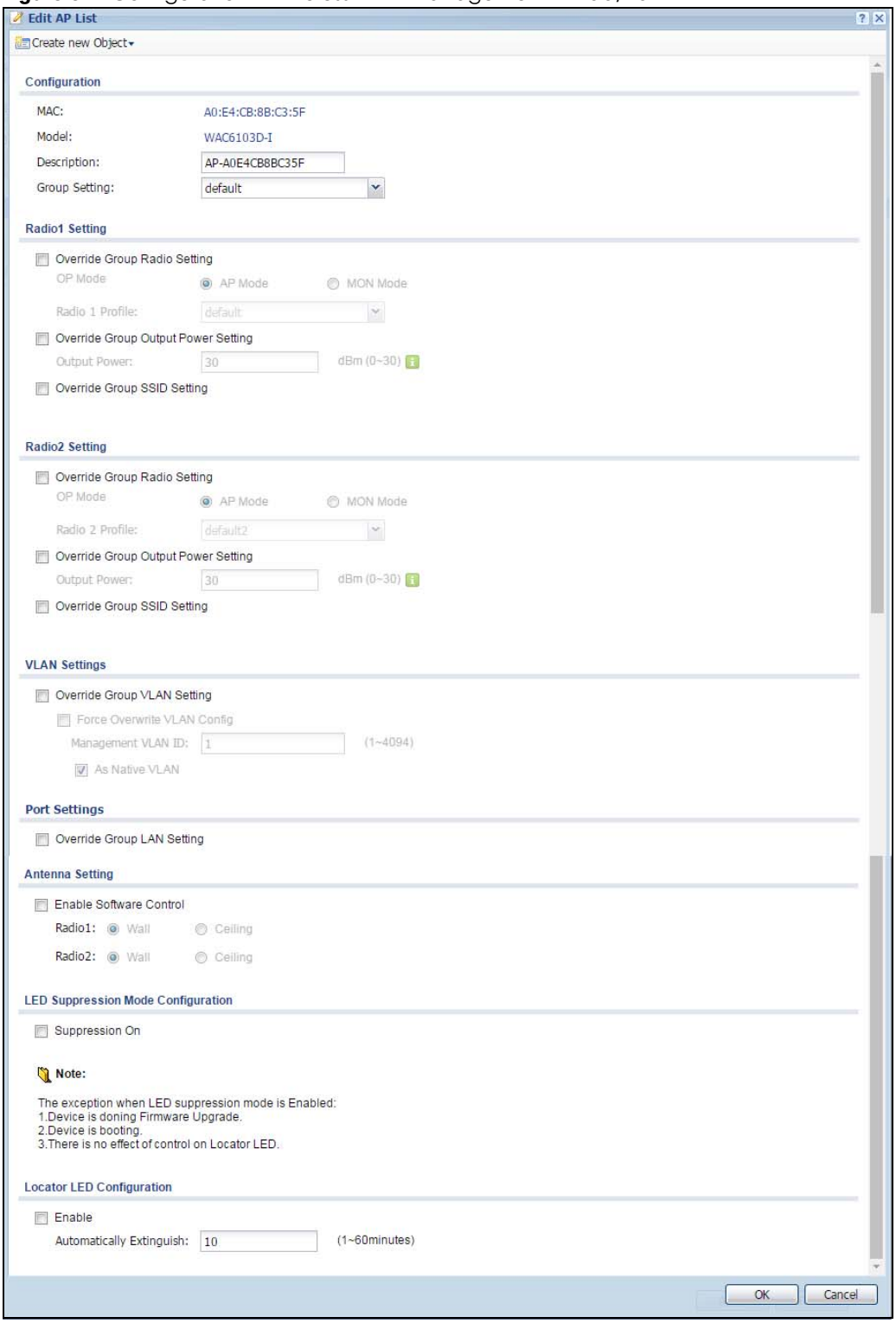
Table 55 Configuration > Wireless > AP Management (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. |
| Group | This displays the group name to which the selected AP belongs. |
| Mgnt. VLAN ID(AC) | This displays the Access Controller (the UAG) management VLAN ID setting for the AP. |
| Mgnt. 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 **Mgnt. 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 Add/Edit AP List

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

**Figure 97** Configuration > Wireless > AP Management > Add/Edit



Each field is described in the following table.

Table 56 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. |
| Group Setting | Select the group to which this AP belongs. |
| Radio1/2 Setting | |
| Override Group Radio Setting | Select this option to overwrite the AP radio settings with the settings you configure. |
| OP Mode | Select the operating mode for radio 1 or radio 2.<br>**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).<br>**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.<br>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. |
| Override Group Output Power Setting | Select this option to overwrite the AP output power setting with the setting you configure here. |
| Output Power | Set the maximum output power of the AP.<br>If there is a high density of APs in an area, decrease the output power of the managed AP to reduce interference with other APs.<br>Note: Reducing the output power also reduces the UAG's effective broadcast radius. |
| Override Group SSID Setting | Select this option to overwrite the AP SSID profile setting with the setting you configure here.<br>This section allows you to associate an SSID profile with the radio. |
| Edit | Select an SSID and click this button to reassign it. The selected SSID becomes editable immediately upon clicking. |
| # | This is the index number of the SSID profile. You can associate up to eight SSID profiles with an AP radio. |
| SSID Profile | Indicates which SSID profile is associated with this radio profile. |
| VLAN Settings | This section is not available when you are editing the local AP's settings. |
| Override Group VLAN Setting | Click on this to modify VLAN Settings of the selected AP. |
| Force Override 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. |

Table 56 Configuration > Wireless > AP Management > Edit AP List (continued)

| LABEL | DESCRIPTION |
|---|---|
| Port Settings | |
| Override Group LAN Setting | Click on this to modify the selected AP's LAN settings. |
| 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 a port, select it and click **Activate**. |
| Inactivate | To turn off a port, select it and click **Inactivate**. |
| # | 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.<br>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 | |
| 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 erase it from the VLAN configuration list. |
| Activate | To turn on a VLAN, select it and click **Activate**. |
| Inactivate | To turn off a VLAN, select it and click **Inactivate**. |
| # | 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. |
| Antenna Setting | |
| Enable Software Control | Click on this to allow the AP's software control.<br>Note: This criterion only appears for APs with an antenna switch. |
| Radio 1/2 | Select the antenna orientation of the radio (**Wall** or **Ceiling**). |
| LED Suppression Mode Configuration | |
| Suppression On | Click this button to enable the selected 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. |
| Locator LED Configuration<br>Note: This section is available only when the AP has a locator LED. | |
| Turn On/Turn Off | When the locator LED is off, click the **Turn On** button to activate the locator function. It will show the actual location of the AP between several devices in the network.<br>If the locator LED is blinking, click the **Turn Off** button to stop the locator LED from blinking immediately. |
| Automatically Extinguish After | Enter a time interval between 1 and 60 minutes to stop the locator LED from blinking. The locator LED will start to blink for the number of minutes set here.<br>If you make changes to the time default setting, it will be stored as the default when the AP restarts. |

Table 56 Configuration > Wireless > AP Management > Edit AP List (continued)

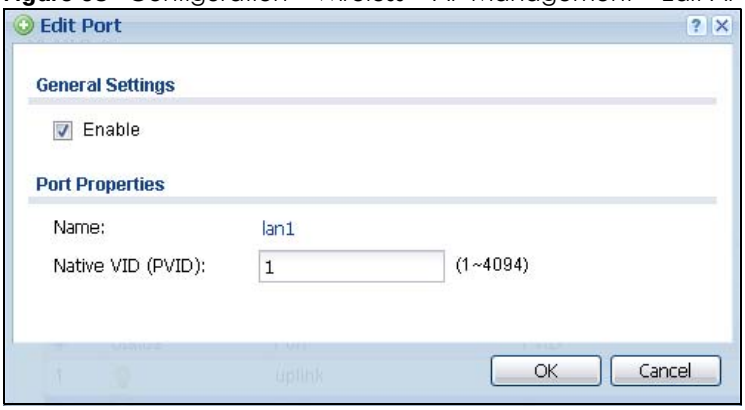
| LABEL | DESCRIPTION |
|---|---|
| OK | Click **OK** to save your changes back to the UAG. |
| Cancel | Click **Cancel** to close the window with changes unsaved. |

## 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 98** Configuration > Wireless > AP Management > Edit AP List > Edit Port




Each field is described in the following table.

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

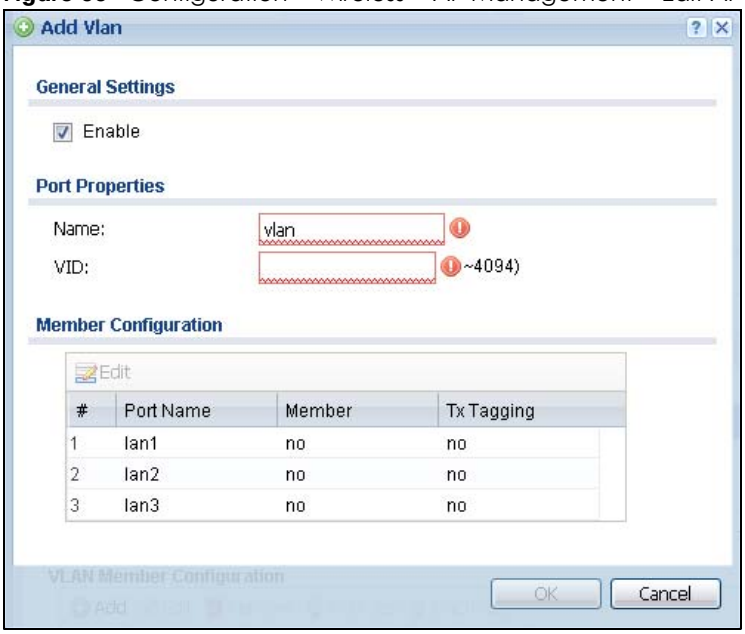
| LABEL | DESCRIPTION |
|---|---|
| Enable | Select this option to activate the port. Otherwise, deselect it. |
| Name | This shows the name of the port. |
| Native VID (PVID) | A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines.<br>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 99** Configuration > Wireless > AP Management > Edit AP List > Edit VLAN




Each field is described in the following table.

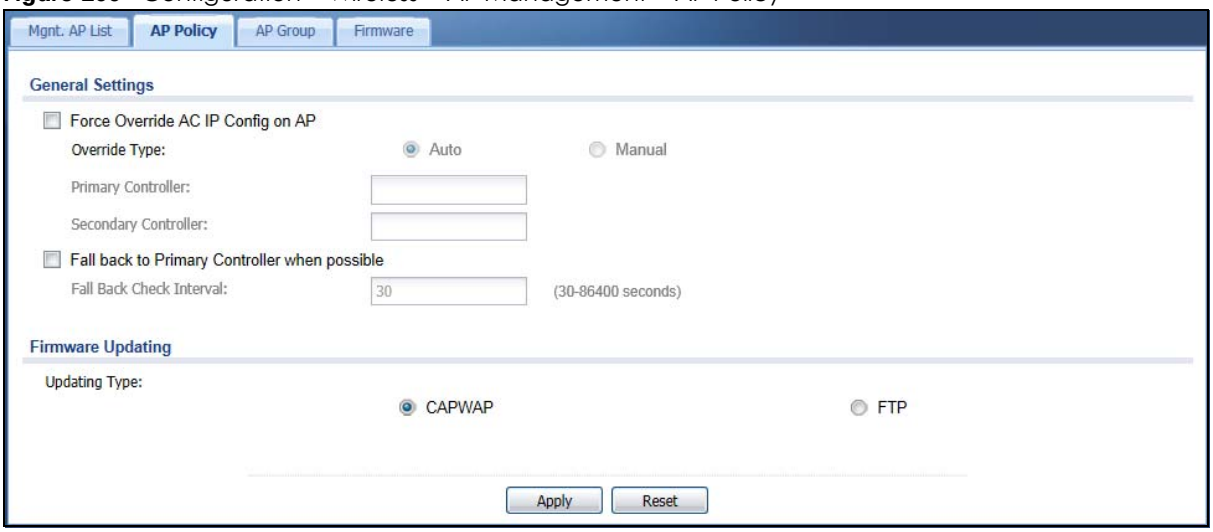
Table 58 Configuration > Wireless > AP Management > Edit AP List > Edit VLAN

| 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.<br>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.<br>Click this field to edit the value. |
| Tx Tagging | This indicates whether the selected port tags outbound traffic with this VLAN's ID.<br>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 100** Configuration > Wireless > AP Management > AP Policy




Each field is described in the following table.

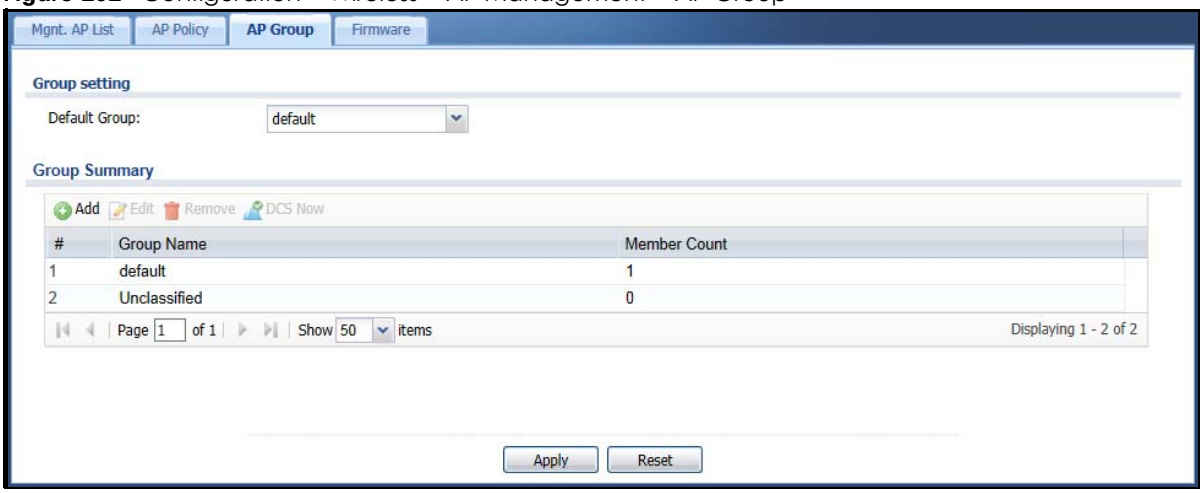
Table 59 Configuration > Wireless > AP Management > AP Policy

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| 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.<br>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. |
| Firmware Updating | |
| Updating Type | Select the type of protocol used to update the firmware. |
| Apply | Click **Apply** to save your changes back to the UAG. |
| Reset | Click **Reset** to return the screen to its last-saved settings. |

## 9.3.5 AP Group

Use this screen to create and manage your existing groups and create new ones. An AP group function reduces repetitive AP configuration and eases AP provision. Click **Configuration > Wireless > AP Management > AP Group**.

**Figure 101** Configuration > Wireless > AP Management > AP Group




Each field is described in the following table.

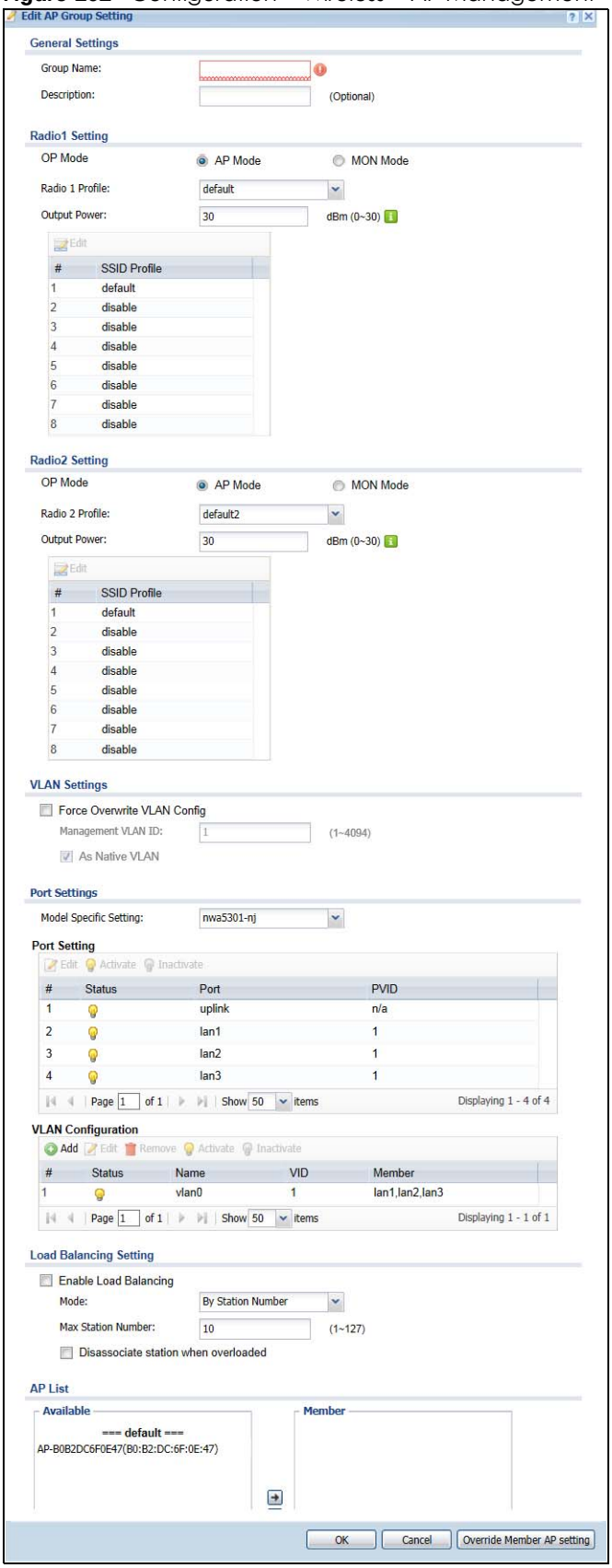
Table 60 Configuration > Wireless > AP Management > AP Group

| LABEL | DESCRIPTION |
|---|---|
| Group Setting | |
| Default Group | Choose which AP group from your group summary is your default group. |
| Group Summary | |
| Add | Click **Add** to open a new screen to create a new AP group. |
| Edit | Double click an entry or select it and click **Edit** to open a screen where you can modify the AP group settings. |
| Remove | Select an entry and click **Remove** to delete it from the Group Summary. |
| DCS Now | Click this to enable DCS (Dynamic Channel Selection) on the selected AP group. DCS allows the AP group to automatically find a less-used channel.<br><br>Note: You should have enabled DCS in the applied AP radio profile before the APs can use DCS.<br><br>Note: DCS is not supported on the radio which is working in repeater AP mode. |
| # | This field is a sequential value, and it is not associated with a specific entry. |
| Group Name | This field displays the name of the each AP group. |
| Member Count | This field displays the number of APs that are part of this group. |
| Apply | Click **Apply** to save the changes to your UAG. |
| Reset | Click **Reset** to return the screen to its last-saved settings. |

## 9.3.6 AP Group Add/Edit

Use this screen to create a new AP group or configure an existing group on the UAG. To access this screen, click **Add** or select an AP group and click the **Edit** button in the **Group Summary** table of the **Configuration > Wireless > AP Management > AP Group** screen.

**Figure 102** Configuration > Wireless > AP Management > AP Group > Add/Edit



Each field is described in the following table.

Table 61 Configuration > Wireless > AP Management > AP Group > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Group Name | Enter a name for this group. You can use up to 31 alphanumeric characters. Dashes and underscores are also allowed. The name should start with a letter. |
| Description | Enter a description for this group. You can use up to 31 characters, spaces and underscores allowed. |
| Radio 1/2 Setting | |
| OP Mode | Select the operating mode for radio 1 or radio 2.<br>**AP Mode** means the AP group 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).<br>**MON Mode** means the AP group 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.<br>Note: Ensure you restart the managed AP Group after you change its operating mode. |
| Radio 1/2 Profile | Select an AP group profile or a monitor profile from the list. If no profile exists, you can create a new one through the Create new Object menu. |
| Output Power | Set the maximum output power of the AP.<br>If there is a high density of APs in an area, decrease the output power of the managed AP to reduce interference with other APs.<br>Note: Reducing the output power also reduces the UAG's effective broadcast radius. |
| Edit | Select an SSID and select **Edit**. The selected SSID becomes editable immediately upon clicking. |
| # | This is the index number of the SSID profile. You can associate up to eight SSID profiles with an AP radio. |
| SSID Profile | This field indicates which SSID profile is associated with this radio profile. |
| VLAN 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 group. |
| As Native LAN | 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 Settings | |
| Model Specific Setting | Select the model of the managed AP to display the model-specific port and VLAN settings in the tables below. |
| Edit | Select an entry and click **Edit** to modify this port's settings. |
| Activate | Select an entry and click **Activate** to enable this port. |
| Inactivate | Select an entry and click **Inactivate** to disable this port. |
| # | This is the port's index number in this list. |
| Status | This field displays whether or not the port is activated. |
| Port | This shows the name of the physical Ethernet port on the managed AP group. |

Table 61 Configuration > Wireless > AP Management > AP Group > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| PVID | This shows the port's PVID.<br>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 | Use **Add** to create a new VLAN Configuration. Select a VLAN Configuration first to use the **Edit**, **Remove**, **Activate** and **Inactivate** buttons. |
| # | 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. |
| Load Balancing Setting | |
| Enable Load Balancing | Click this to enable Load Balancing on the UAG.<br>Use this section to configure wireless network traffic load balancing between the managed APs in this group. |
| Mode | Select a mode by which load balancing is carried out.<br>Select **By Station Number** to balance network traffic based on the number of specified stations connected to an AP.<br>Select **By Traffic Level** to balance network traffic based on the volume generated by the stations connected to an AP.<br>Select **By Smart Classroom** to balance network traffic based on the number of specified stations connected to an AP. The AP ignores association request and authentication request packets from any new station when the maximum number of stations is reached.<br>If you select **By Station Number** or **By Traffic Level**, once the threshold is crossed (either the maximum station numbers or with network traffic), 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 group begins load balancing its connections. |
| Traffic Level | Select the threshold traffic level at which the AP begins load balancing its connections (**Low, Medium, High**).<br>The maximum bandwidth allowed for each level is:<br>• **Low** - 11 Mbps<br>• **Medium** - 23 Mbps<br>• **High** - 35M bps |

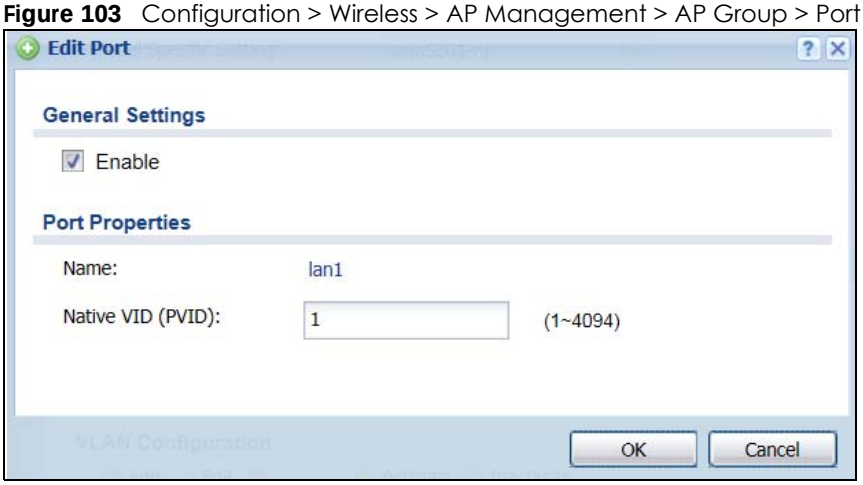
Table 61 Configuration > Wireless > AP Management > AP Group > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Disassociate station when overloaded | Select this option to disassociate wireless clients connected to the AP group when it becomes overloaded. If you do not enable this option, then the AP group simply delays the connection until it can afford the bandwidth it requires, or it transfers the connection to another AP group within its broadcast radius.<br>The disassociation priority is determined automatically by the UAG and is as follows:<br>• **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.<br>• **Signal Strength** - Devices with the weakest signal strength will be disassociated first.<br>Note: If you enable this function, you should ensure that there are multiple AP groups 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. |
| AP List | |
| Available | This lists the APs that do not belong to this group. Select the APs that you want to add to the group you are editing, and click the right arrow button to add them. |
| Member | This lists the APs that belong to this group. Select any APs that you want to remove from the group, and click the left arrow button to remove them. |
| OK | Click **OK** to save your changes back to the UAG. |
| Cancel | Click **Cancel** to close the window with changes unsaved. |
| Override Member AP Setting | Click this button to overwrite the settings of all managed APs in this group with the settings you configure here. All Override Group check boxes on the **AP Management > Mgnt. AP List > Edit AP List** screen for the APs in this group will be deselected. |

### 9.3.6.1 Edit Port

Use this screen to modify a port's settings. Click **Configuration > Wireless > AP Management > AP Group > Port Settings > Edit** to open the following screen.

**Figure 103** Configuration > Wireless > AP Management > AP Group > Port Setting > Edit



Each field is described in the following table.

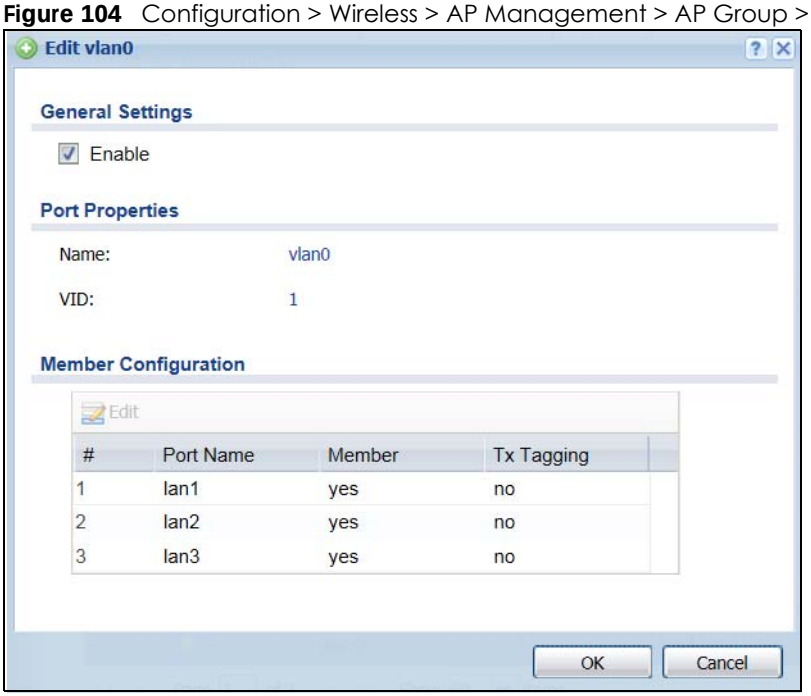
Table 62 Configuration > Wireless > AP Management > AP Group > Port Setting > Edit

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Enable | Click this to enable this port. |
| Port Properties | |
| Name | This field displays the name assigned to this 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. |

### 9.3.6.2 Edit VLAN

Use this screen to modify a port's settings. Click **Configuration > Wireless > AP Management > AP Group > VLAN Configuration > Edit** to open the following screen.

**Figure 104** Configuration > Wireless > AP Management > AP Group > VLAN Configuration > Edit




Each field is described in the following table.

Table 63 Configuration > Wireless > AP Management > AP Group > VLAN Configuration > Edit

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Enable | Click this to enable this VLAN configuration. |
| Port Properties | |
| Name | This field is read-only if you are editing an existing VLAN.<br>Enter the number of the VLAN. You can use a number from 1~4094. For example, vlan0, vlan8, and so on. |
| VID | This field displays the VLAN ID number. |
| Member Configuration | |

Table 63 Configuration > Wireless > AP Management > AP Group > VLAN Configuration > Edit

| LABEL | DESCRIPTION |
|---|---|
| Edit | Select a port and click **Edit** to modify the port settings. |
| # | This is the member's index number in this list. |
| Port Name | This field displays the name assigned to this port. |
| Member | This indicates whether the selected port is a member or not of the VLAN which is currently being edited. |
| Tx Tagging | This indicates whether the selected port tags outbound traffic with this VLAN's ID . |

## 9.3.7 Firmware

The UAG stores an AP firmware in order to manage supported APs. This screen allows the UAG to check for and download new AP firmware when it becomes available on the firmware server. All APs managed by the UAG must have the same firmware version as the AP firmware on the UAG.

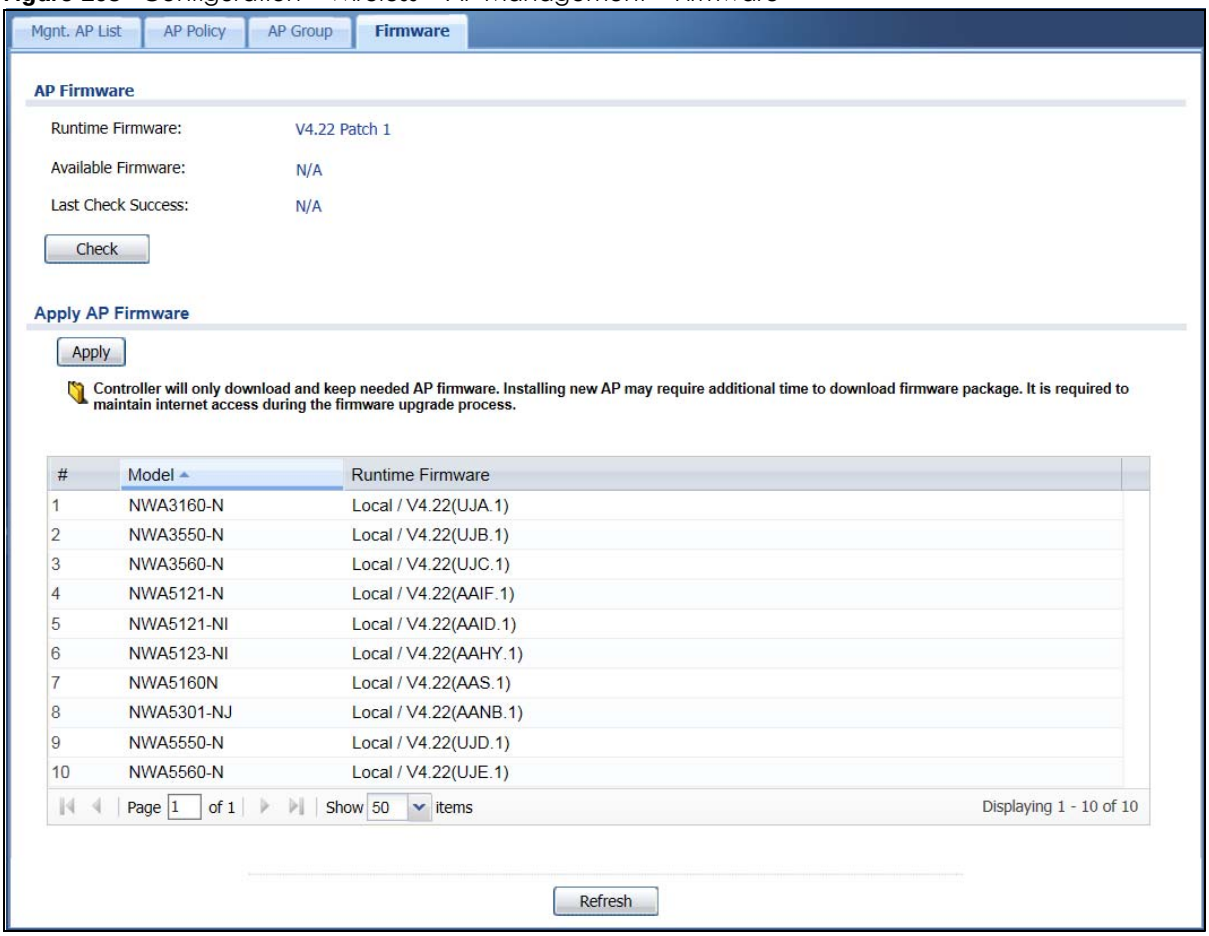
When an AP connects to the UAG wireless controller, the UAG will check if the AP has the same firmware version as the AP firmware on the UAG. If yes, then the UAG can manage it. If no, then the AP must upgrade (or downgrade) its firmware to be the same version as the AP firmware on the UAG (and reboot).

The UAG should always have the latest AP firmware so that:

- APs don't have to downgrade firmware in order to be managed.
- All new APs are supported.

Use **Check** to see if the UAG has the latest AP firmware. Use **Apply** to have the UAG download the latest AP firmware from the firmware server. If the UAG does not have enough space for the latest AP firmware, then the UAG will delete an existing firmware that no AP is using before downloading the new AP firmware. To access this screen, click **Configuration > Wireless > AP Management > Firmware** screen.

**Figure 105** Configuration > Wireless > AP Management > Firmware




Each field is described in the following table.

Table 64 Configuration > Wireless > AP Management > Firmware

| LABEL | DESCRIPTION |
|---|---|
| AP Firmware | |
| Runtime Firmware | This displays the current AP firmware version on the UAG. The UAG must have the latest AP firmware to manage all supported APs. |
| Available Firmware | This field displays if there is a later AP firmware version available on the firmware server. It displays **N/A** if the UAG cannot connect with the firmware server. Check that the UAG has Internet access if **N/A** displays and then click the **Check** button below.<br>If a newer UAG AP firmware is available, its version number and a **More Details** icon displays here.<br>Available Firmware: V4.20 Patch 0 More Details |
| Last Check Success | This displays the date and time the last check for new firmware was made and whether the check is in progress (**checking**), was successful (**success**), or has failed (**fail**). |
| Check | Click this button to have the UAG display the latest AP firmware version available on the firmware server. |

Table 64 Configuration > Wireless > AP Management > Firmware

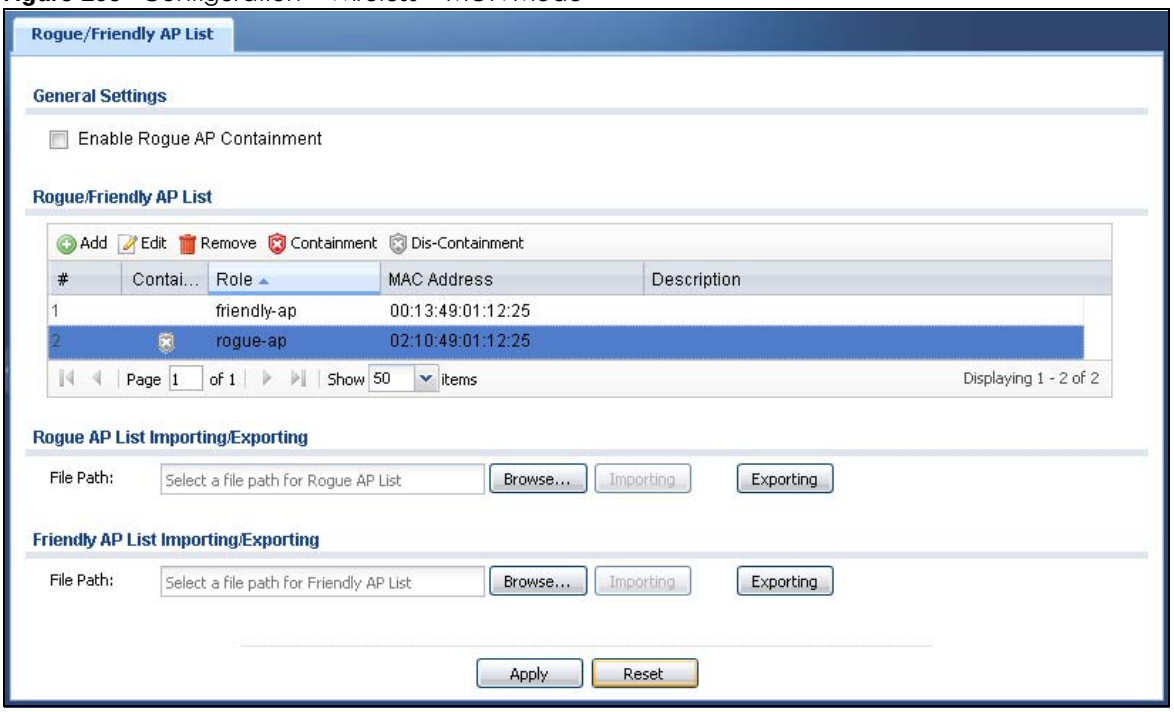
| LABEL | DESCRIPTION |
|---|---|
| Apply AP Firmware | Due to space limitations, the UAG only downloads and keeps AP firmware for APs it is currently managing. If you connect a new AP to the UAG, the UAG may need to download a new AP firmware. Please wait while downloading new firmware as the speed depends on your Internet connection speed. Make sure to maintain the Internet connection while downloading new firmware. |
| Apply | Click this to download newer Available Firmware from the firmware server and update the Runtime Firmware version. |
| # | This is an index number of a managed AP. |
| Model | This displays the name of all manageable AP models. |
| Runtime Firmware | This displays the firmware version that the managed AP must have in order to be managed by the UAG. Firmware for APs that the UAG already has displays in bold; firmware that the UAG doesn't have or is still downloading is grayed out. Firmware that is in the download queue will show **To be downloaded**. |
| Refresh | Click this to update the model firmware table. |

# 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 106** Configuration > Wireless > MON Mode



Each field is described in the following table.

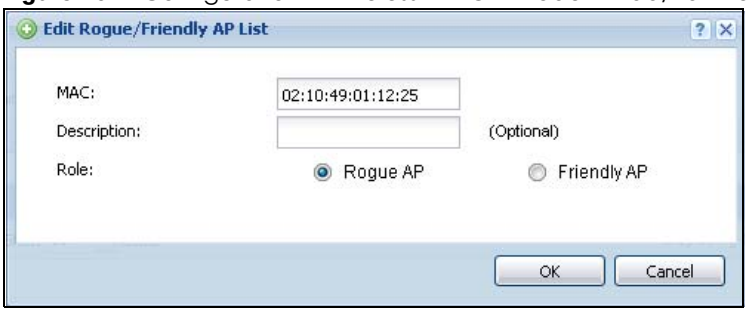
Table 65 Configuration > Wireless > MON Mode

| 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.<br>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.<br>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. |
| 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 107** Configuration > Wireless > MON Mode > Add/Edit Rogue/Friendly



Each field is described in the following table.

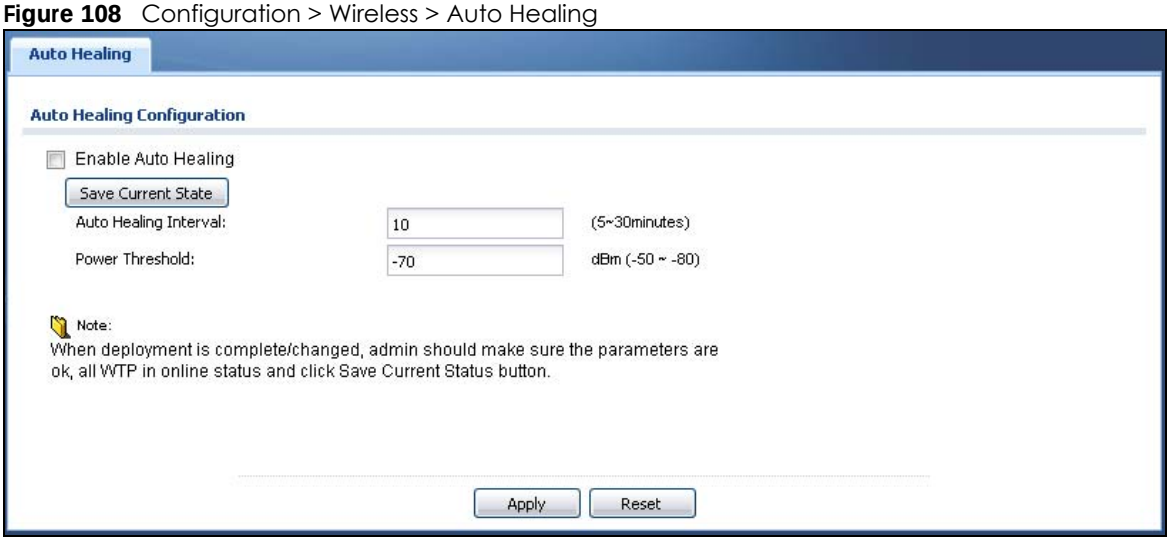
Table 66 Configuration > Wireless > MON Mode > Add/Edit Rogue/Friendly

| 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 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 108** Configuration > Wireless > Auto Healing




Each field is described in the following table.

Table 67 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).<br>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. |

Table 67 Configuration > Wireless > Auto Healing (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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.<br>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. |

# 9.6 RTLS

Use this screen to configure RTLS (Real Time Location System) on or off and specify the IP address and server port of the Ekahau RTLS Controller.

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).

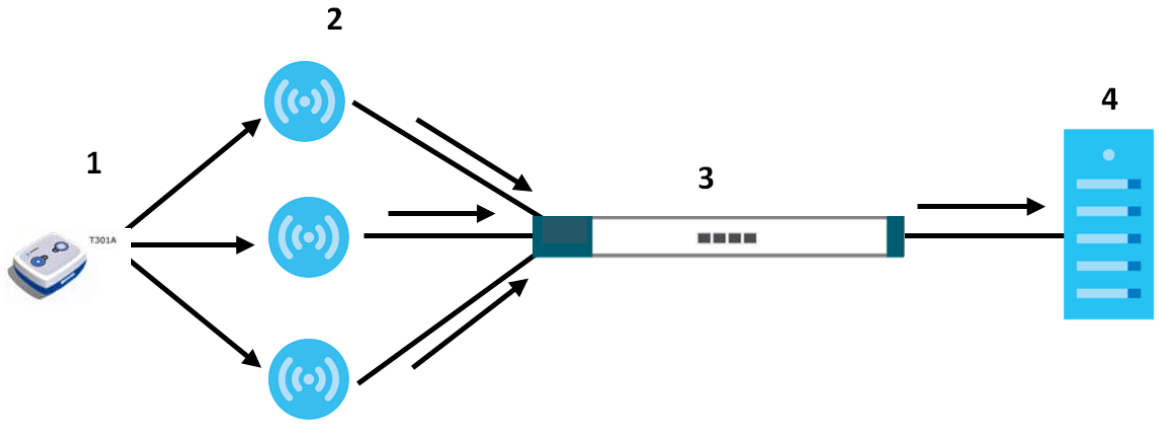
1 The Wi-Fi tag sends blink packets at specified intervals (or triggered by something like motion or button presses).

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 109** RTLS Example



## 9.6.1 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.

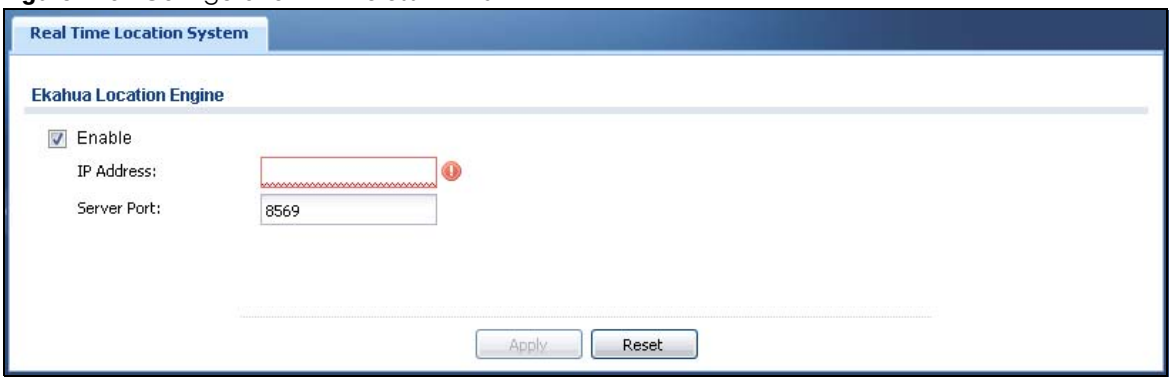
The following table lists default port numbers and types of packets RTLS uses.

Table 68 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 |

Click **Configuration > Wireless > RTLS** to access this screen.

**Figure 110** Configuration > Wireless > RTLS



The following table describes the labels in this screen.

Table 69 Configuration > Wireless > 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. |

# 9.7 Technical Reference

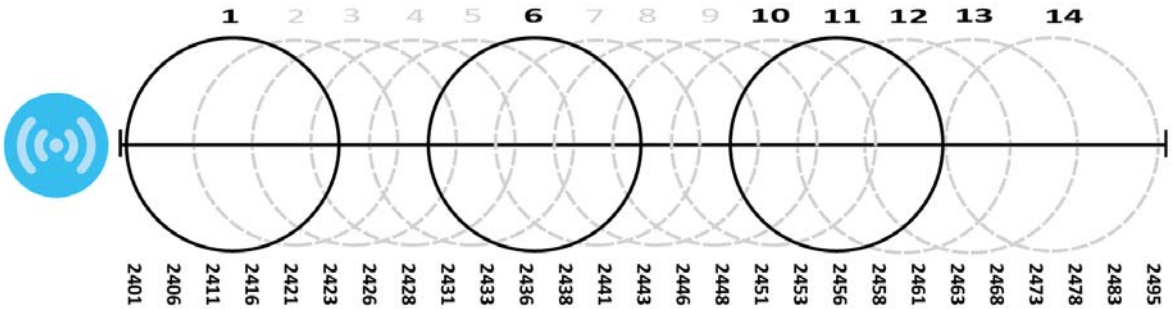
The following section contains additional technical information about the features described in this chapter.

## 9.7.1 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.

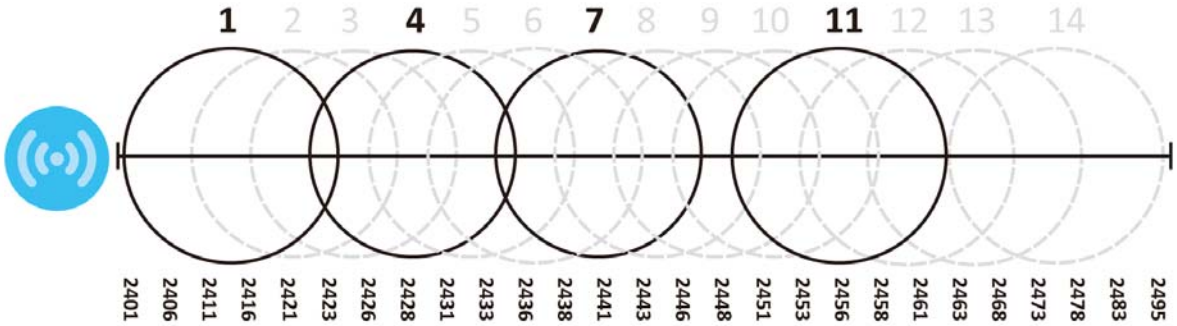
In the 2.4 GHz spectrum, each channel from 1 to 13 is broken up into discrete 22 MHz segments that are spaced 5 MHz apart. Channel 1 is centered on 2.412 GHz while channel 13 is centered on 2.472 GHz.

**Figure 111** 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.

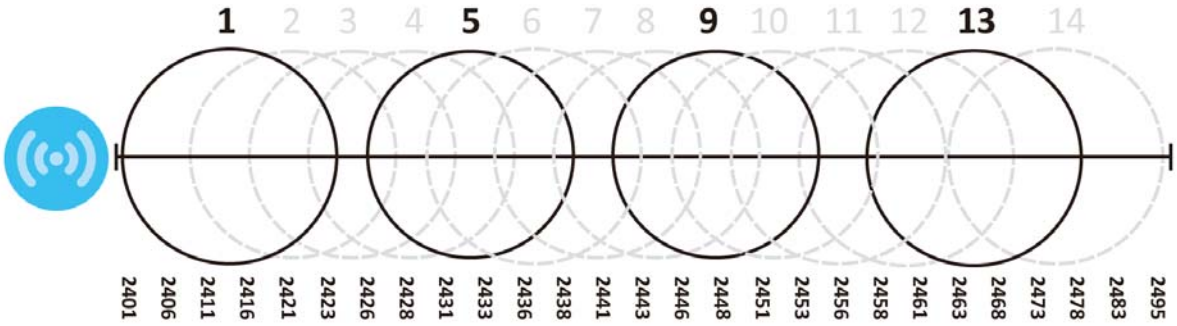
**Figure 112** An Example Four-Channel Deployment




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 that the other one.

**Figure 113** An Alternative Four-Channel Deployment

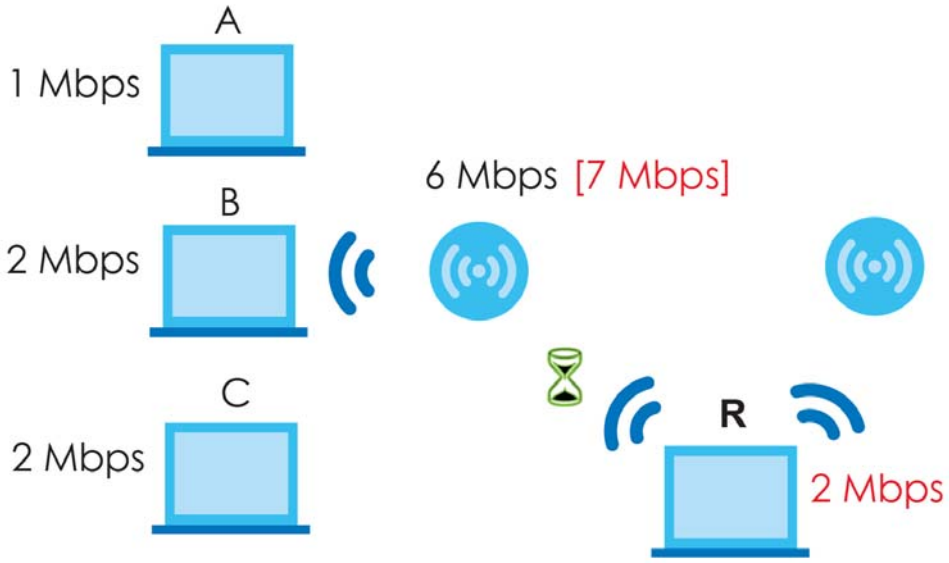



## 9.7.2 Disassociating and Delaying Connections

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.

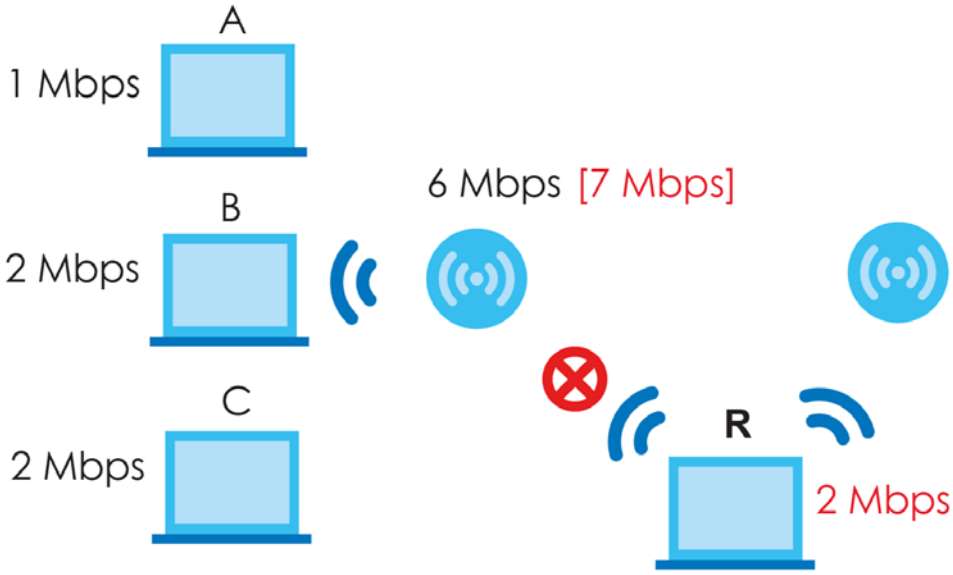
For example, here the AP has a balanced bandwidth allotment of 6 Mbps. If laptop **R** connects and it pushes the AP over its allotment, say to 7 Mbps, then the AP delays the red laptop's connection until it can afford the bandwidth or the laptop is picked up by a different AP with bandwidth to spare.

**Figure 114** 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 115** 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.

## 9.7.3 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.

# CHAPTER 10
# Interfaces

## 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 171) to create port groups and to assign physical ports and port groups to Ethernet interfaces.
- Use the **Ethernet** screens (Section 10.3 on page 172) 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 183) for PPPoE or PPTP Internet connections.
- Use the **VLAN** screens (Section 10.5 on page 189) 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 196) to combine two or more network segments into a single network.
- Use the **Virtual Interface** screen (Section 10.7.1 on page 204) 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 210) 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 171 and Chapter 11 on page 210 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 70 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 71 Relationships Between Different Types of Interfaces

| INTERFACE | REQUIRED PORT / INTERFACE |
|---|---|
| port group | physical port |
| Ethernet interface | physical port<br>port group |
| VLAN interface | Ethernet interface |
| bridge interface | Ethernet interface*<br>VLAN interface* |
| PPP interface | Ethernet interface*<br>VLAN interface*<br>bridge interface<br>WAN1, WAN2 |
| virtual interface<br>(virtual Ethernet interface)<br>(virtual VLAN interface)<br>(virtual bridge interface) | <br>Ethernet interface*<br>VLAN interface*<br>bridge interface |
| trunk | Ethernet interface<br>VLAN interface<br>bridge interface<br>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 206 for background information on interfaces.
- See Chapter 11 on page 210 to configure load balancing using trunks.

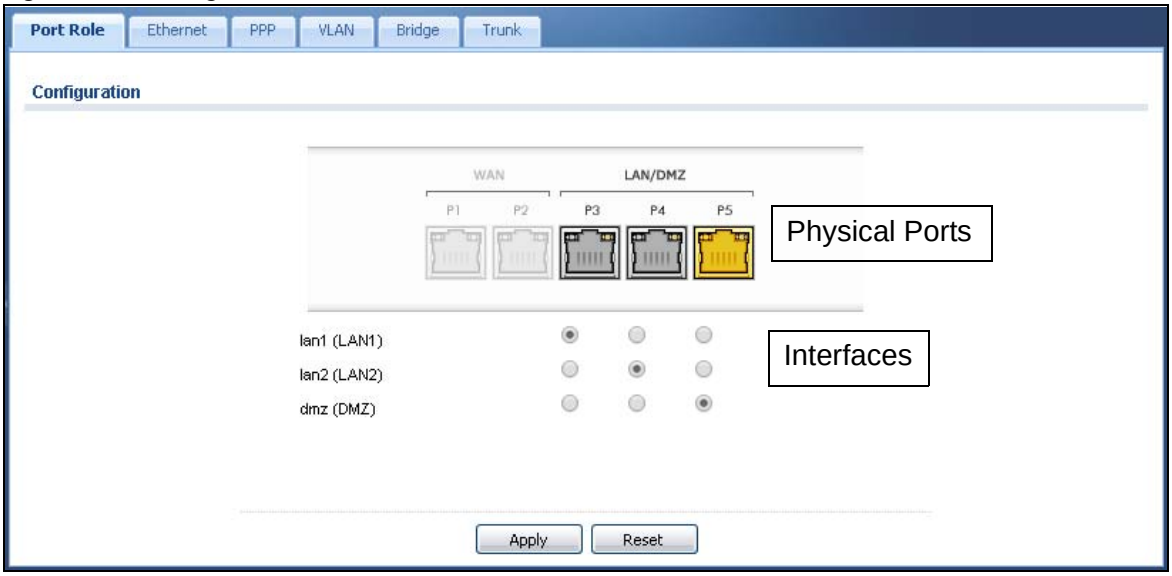
## 10.2 Port Role Screen

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 116** 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 Screen

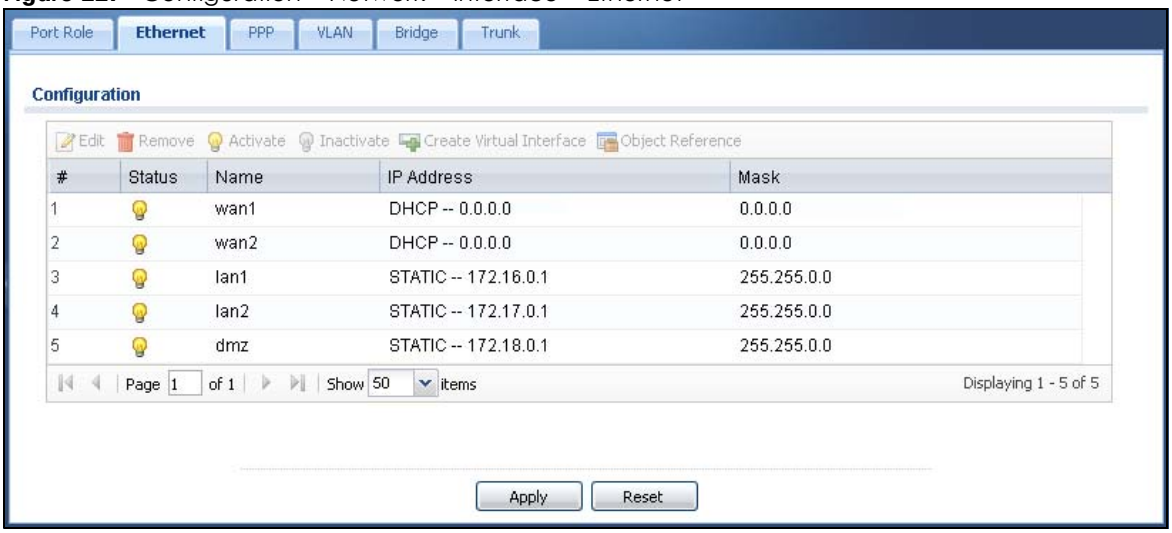
This screen lists every Ethernet interface and virtual interface created on top of Ethernet interfaces. To access this screen, click **Configuration > Network** > **Interface > Ethernet**.

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 171), 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 117** Configuration > Network > Interface > Ethernet




Each field is described in the following table.

Table 72 Configuration > Network > Interface > Ethernet

| LABEL | DESCRIPTION |
|---|---|
| Configuration | |
| 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 180 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 (in the IPv4 network), the interface does not have an IP address yet.<br>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. |

Table 72 Configuration > Network > Interface > Ethernet (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. |

## 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 172.)

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 118** Configuration > Network > Interface > Ethernet > Edit (External Type)

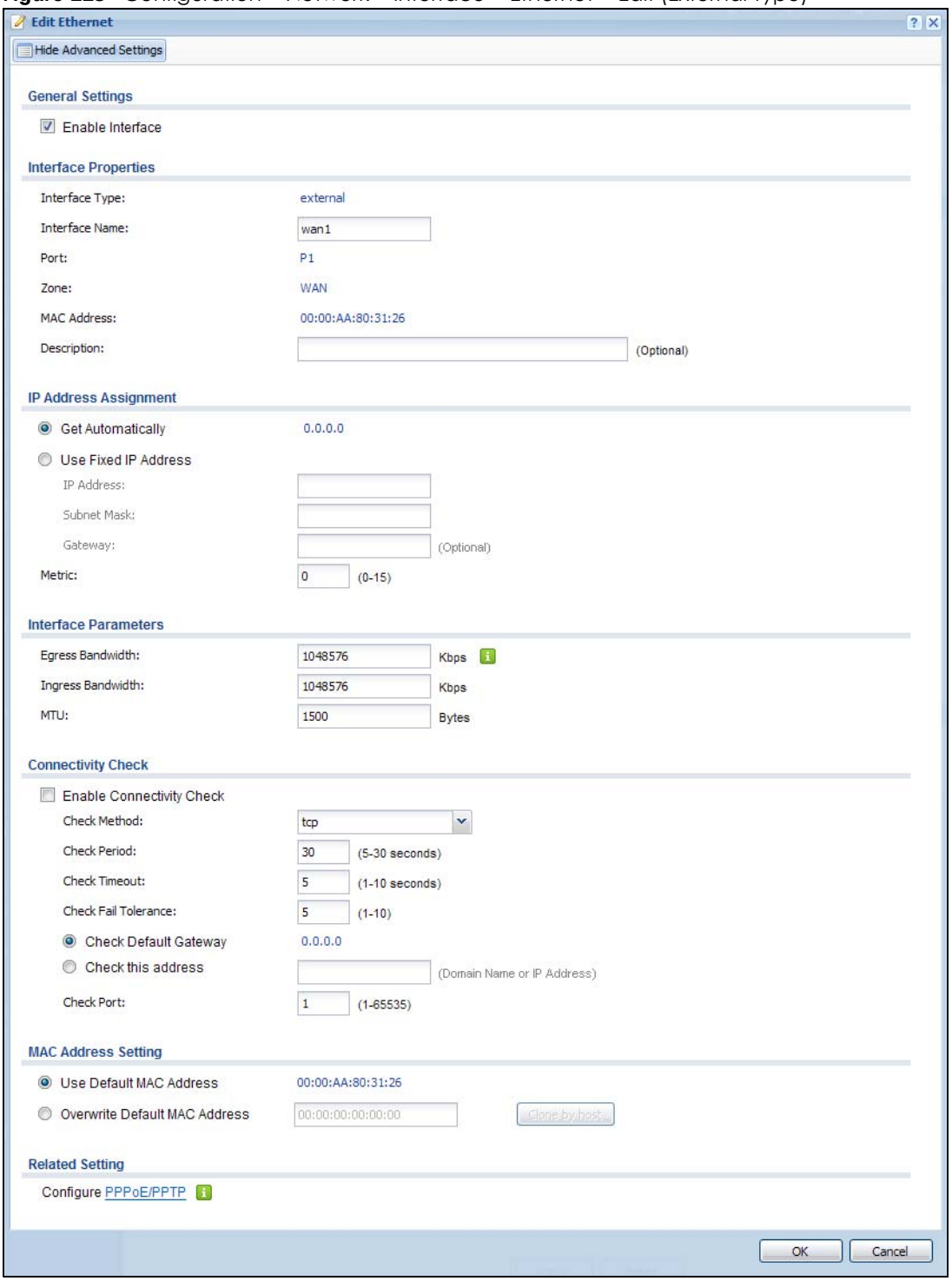
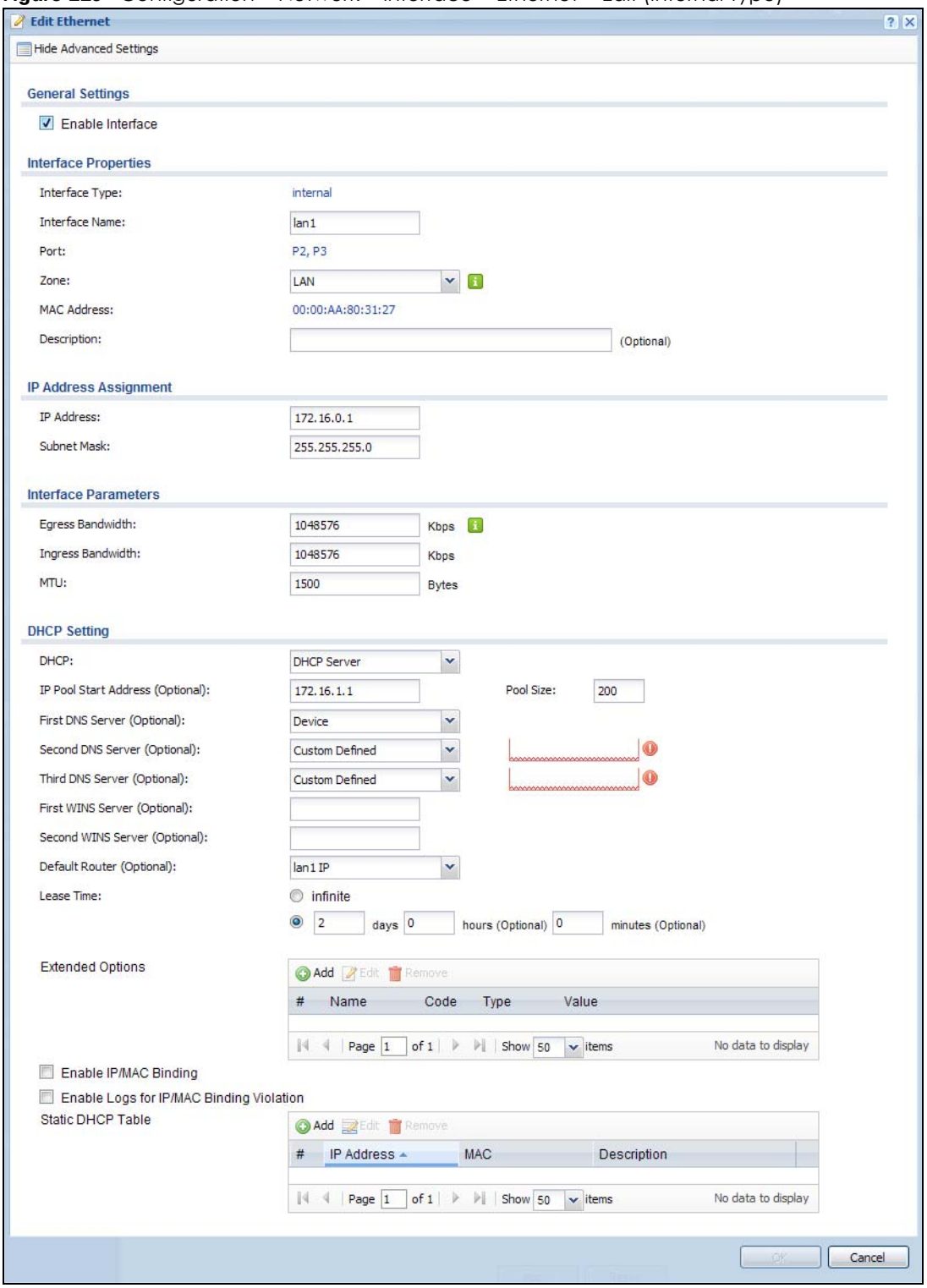


**Figure 119** Configuration > Network > Interface > Ethernet > Edit (Internal Type)



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

Table 73 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 | 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.<br>**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.<br>**external** is for connecting to an external network (like the Internet). The UAG automatically adds this interface to the default WAN trunk.<br>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 | 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 | |
| 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. |

Table 73 Configuration > Network > Interface > Ethernet > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Ingress Bandwidth | This is reserved for future use.<br>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**.<br>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.<br>Select **icmp** to have the UAG regularly ping the gateway you specify to make sure it is still available.<br>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:<br>**None** - the UAG does not provide any DHCP services. There is already a DHCP server on the network.<br>**DHCP Relay** - the UAG routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network.<br>**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**. |
| IP Pool Start Address | 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**.<br>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. |

Table 73 Configuration > Network > Interface > Ethernet > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Pool Size | 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.<br><br>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. |
| 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.<br><br>**Custom Defined** - enter a static IP address.<br><br>**From ISP** - select the DNS server that another interface received from its DHCP server.<br><br>**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.<br><br>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:<br><br>**infinite** - select this if IP addresses never expire.<br><br>**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**.<br><br>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 181. |
| 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**. |

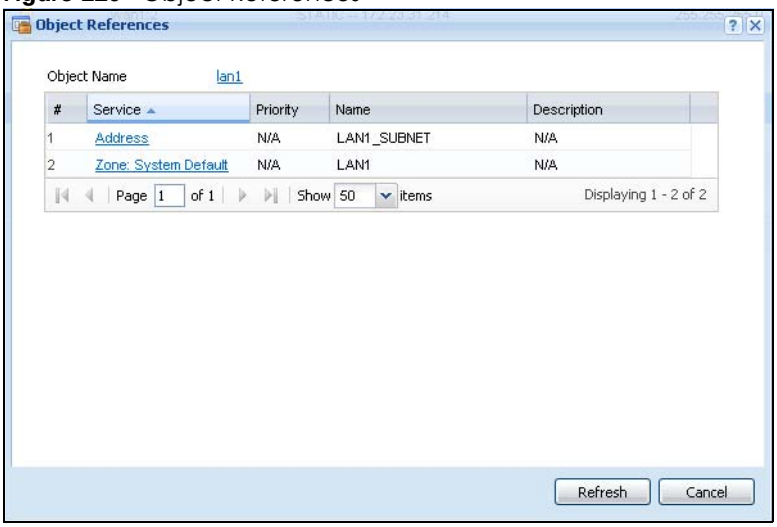
Table 73 Configuration > Network > Interface > Ethernet > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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.<br>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.<br>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 120** Object References




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

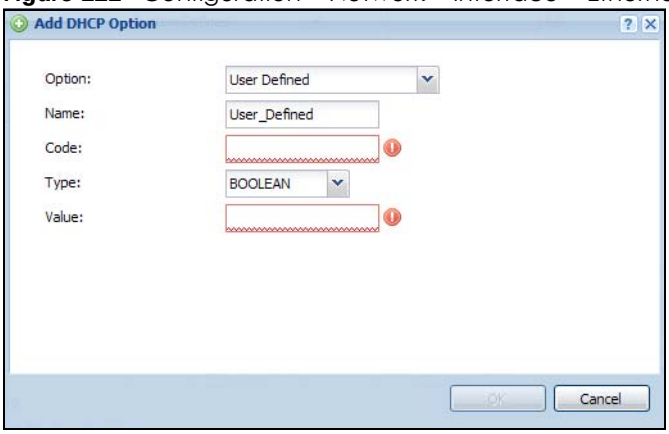
Table 74 Object References

| 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 121** Configuration > Network > Interface > Ethernet > Edit > Add/Edit Extended Options




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

Table 75 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 76 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.<br><br>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. |
| 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.

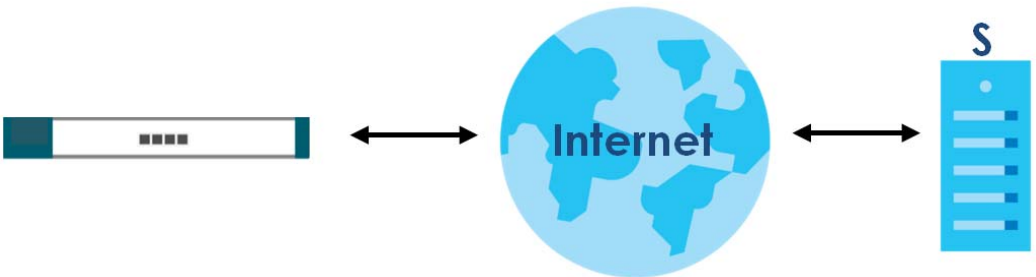
Table 76 DHCP Extended Options

| 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<br>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<br>DHCP clients and servers may use this option to exchange vendor-specific information. |
| CAPWAP AC | 138 | CAPWAP Access Controller addresses option<br>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 PPPoE/PPTP server (S). This way, you do not have to install or manage PPPoE/PPTP software on each computer in the network.

**Figure 122** 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.

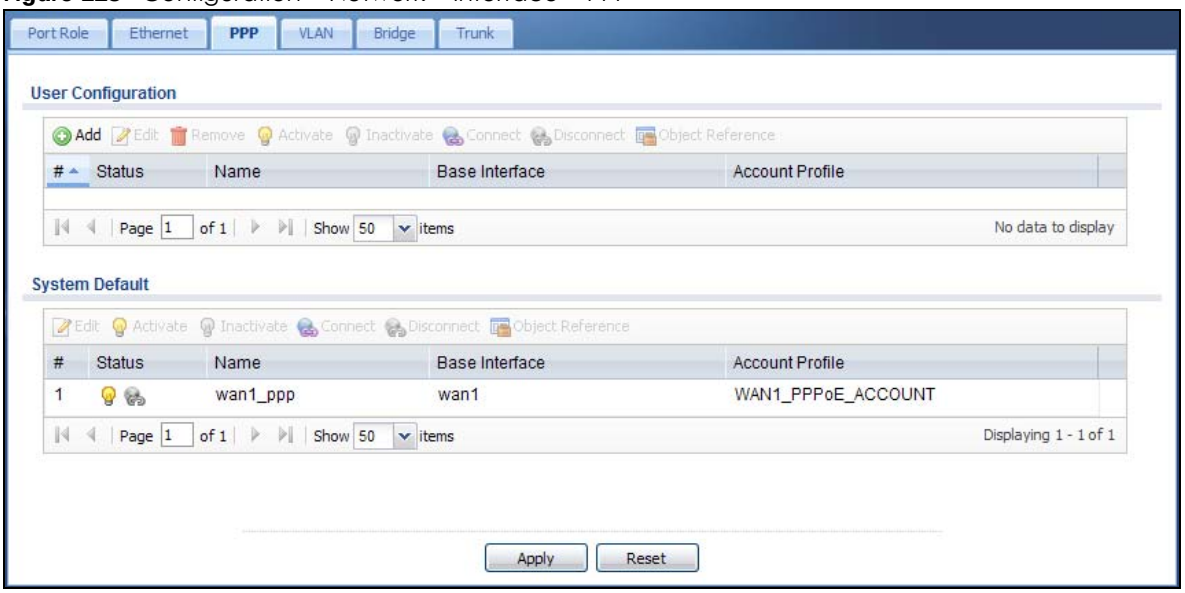
- You do not set up the subnet mask or gateway.

  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 123** Configuration > Network > Interface > PPP




Each field is described in the table below.

Table 77 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**. |

Table 77 Configuration > Network > Interface > PPP (continued)

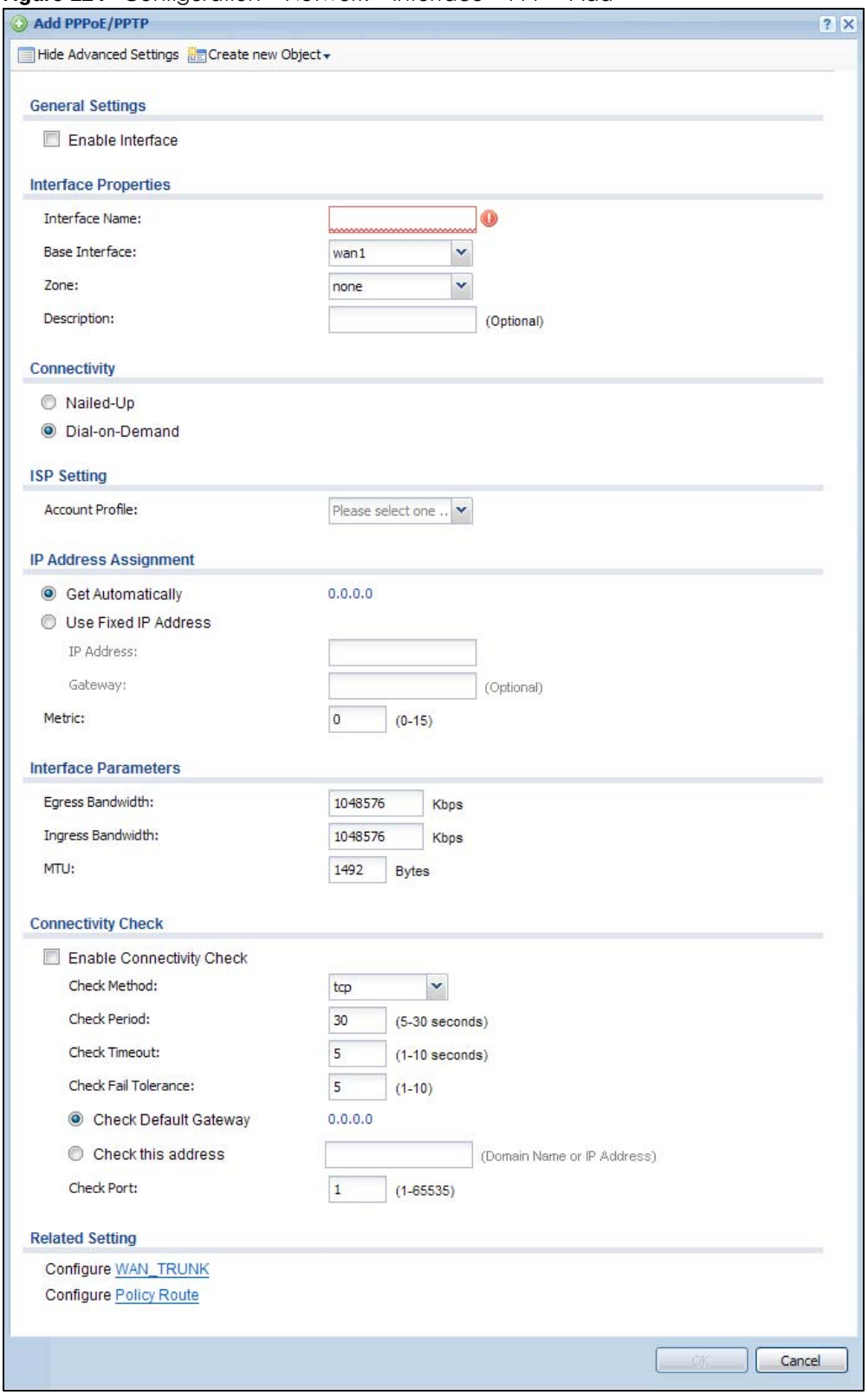
| LABEL | DESCRIPTION |
|---|---|
| Connect | To connect an interface, select it and click **Connect**. You might use this in testing the interface or to manually establish the connection for a **Dial-on-Demand** PPPoE/PPTP interface. |
| Disconnect | To disconnect an interface, select it and click **Disconnect**. 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 180 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.<br>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 124** Configuration > Network > Interface > PPP > Add



Each field is explained in the following table.

Table 78 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.<br><br>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 44 on page 492 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.<br><br>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.<br><br>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 78 Configuration > Network > Interface > PPP > Add (continued)

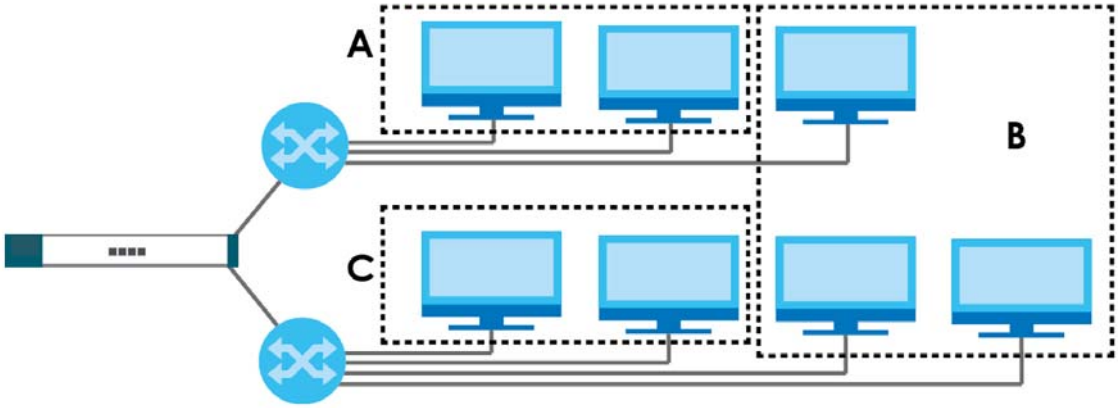
| LABEL | DESCRIPTION |
|---|---|
| IP Address | This field is enabled if you select **Use Fixed IP Address**.<br>Enter the IP address for this interface. |
| Gateway | This field is enabled if you select **Use Fixed IP Address**.<br>Enter the IP address of the gateway. The UAG sends packets to the gateway 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.<br>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.<br>Select **icmp** to have the UAG regularly ping the gateway you specify to make sure it is still available.<br>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. |
| 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.

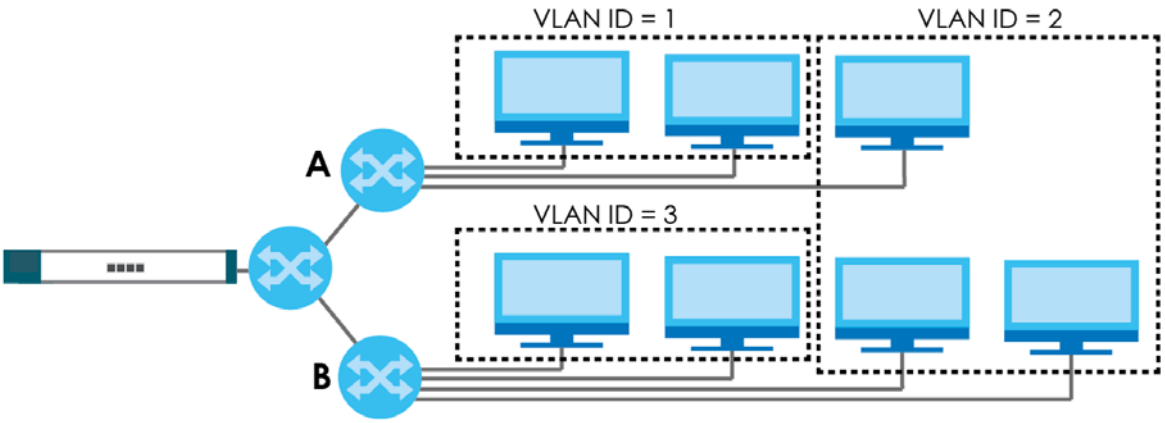
In this example, there are two physical networks and three departments **A**, **B**, and **C**. The physical networks are connected to hubs, and the hubs are connected to the router.

**Figure 125** Example: Before VLAN




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

**Figure 126** 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.

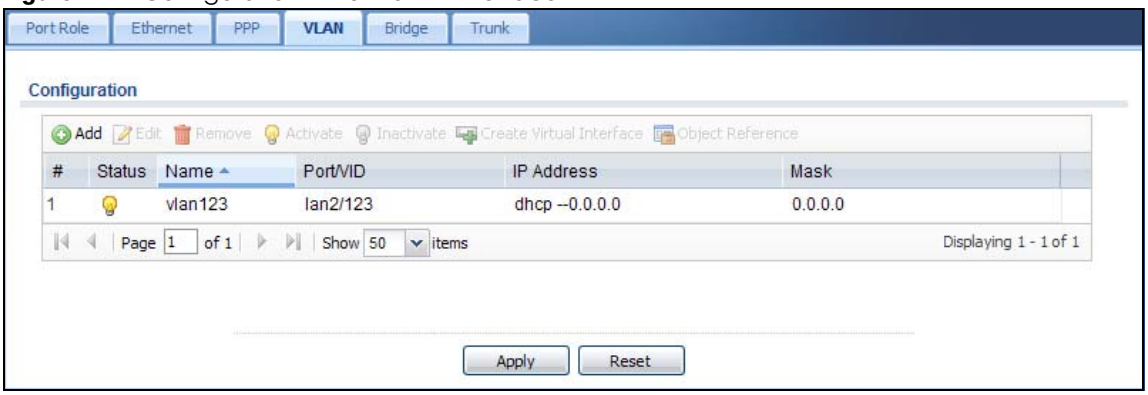
Note: Each VLAN interface is created on top of only one Ethernet interface.

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 127** Configuration > Network > Interface > VLAN



Each field is explained in the following table.

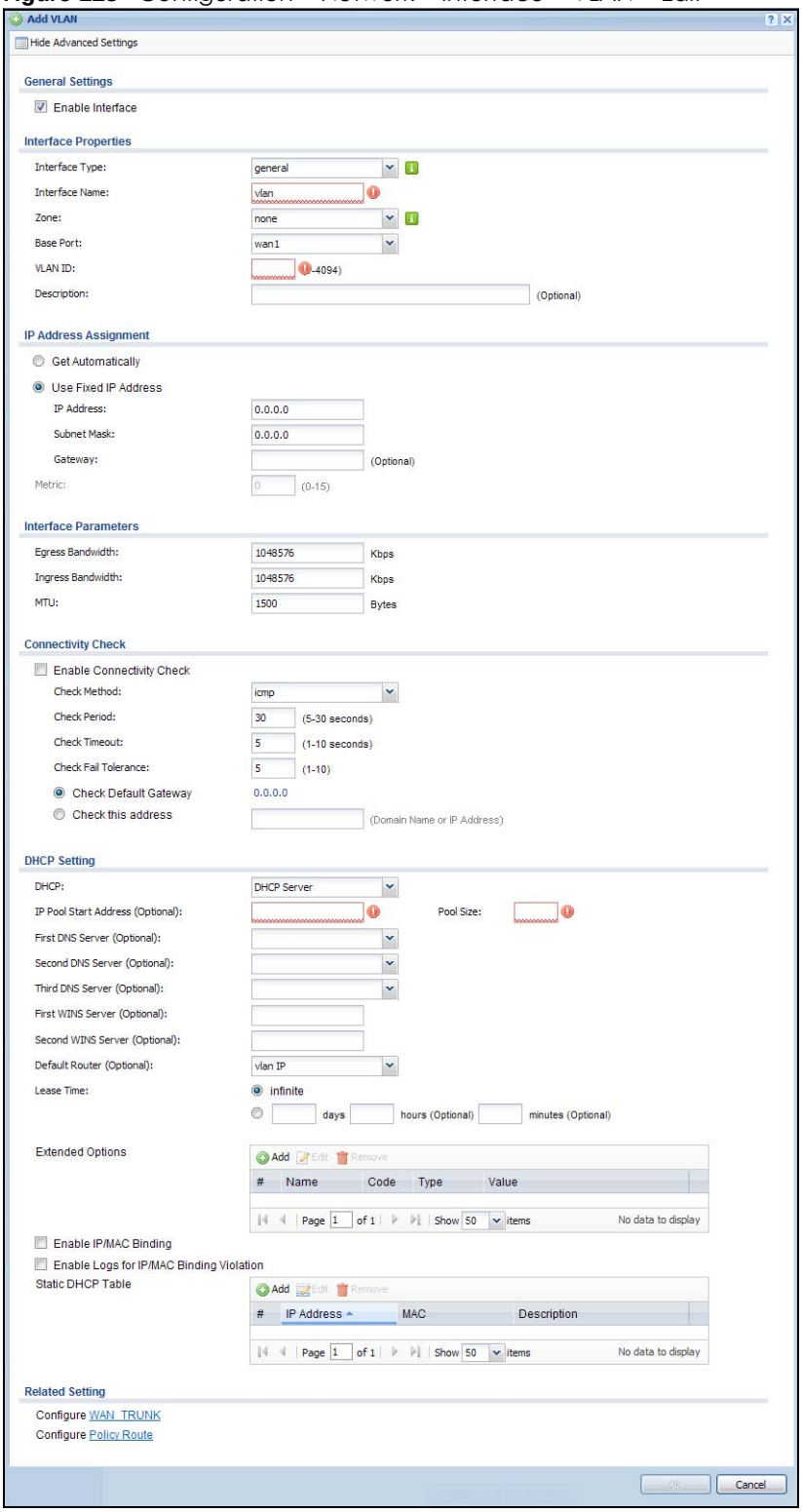
Table 79 Configuration > Network > Interface > VLAN

| LABEL | DESCRIPTION |
|---|---|
| Configuration | |
| 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 180 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<br>• the Ethernet interface on which the VLAN interface is created<br>• the VLAN ID<br>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.<br>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 128** Configuration > Network > Interface > VLAN > Edit



Each field is explained in the following table.

Table 80 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 | 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.<br><br>**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.<br><br>**external** is for connecting to an external network (like the Internet). The UAG automatically adds this interface to the default WAN trunk.<br><br>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 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 | This field is enabled if you select **Use Fixed IP Address**.<br><br>Enter the IP address for this interface. |
| Subnet Mask | This field is enabled if you select **Use Fixed IP Address**.<br><br>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**. This field is enabled if you select **Use Fixed IP Address**.<br><br>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 80 Configuration > Network > Interface > VLAN > 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.<br>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.<br>Select **icmp** to have the UAG regularly ping the gateway you specify to make sure it is still available.<br>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:<br>**None** - the UAG does not provide any DHCP services. There is already a DHCP server on the network.<br>**DHCP Relay** - the UAG routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network.<br>**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**. |
| IP Pool Start Address | 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**.<br>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. |

Table 80 Configuration > Network > Interface > VLAN > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Pool Size | 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.<br><br>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. |
| First DNS Server<br>Second DNS Server<br>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.<br><br>**Custom Defined** - enter a static IP address.<br><br>**From ISP** - select the DNS server that another interface received from its DHCP server.<br><br>**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.<br><br>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:<br><br>**infinite** - select this if IP addresses never expire.<br><br>**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**.<br><br>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 181. |
| 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 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. |
| 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**. |

Table 80 Configuration > Network > Interface > VLAN > Edit (continued)

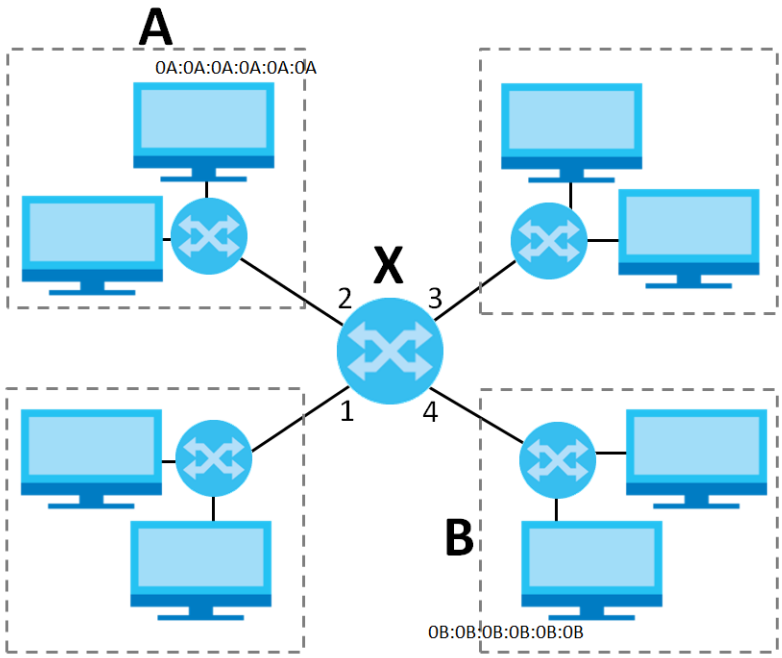
| LABEL | DESCRIPTION |
|---|---|
| Add | Click this to create a new entry. |
| Edit | Select an entry and click this to be able to modify it. |
| Remove | Select an entry and click this to delete it. |
| # | This field is a sequential value, and it is not associated with a specific entry. |
| IP Address | 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 81 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 82 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 83 Example: Routing Table Before and After Bridge Interface br0 Is Created

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

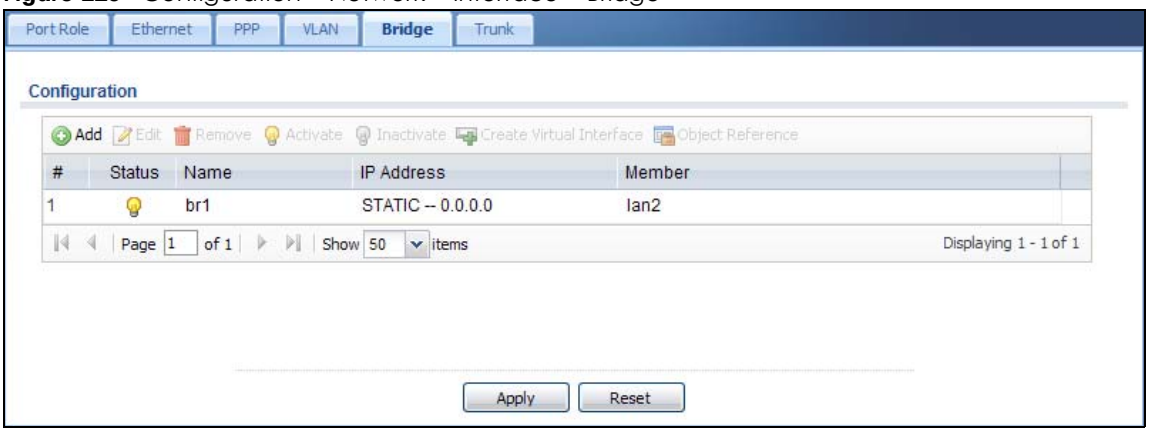
| IP ADDRESS(ES) | DESTINATION |
|---|---|
| 221.221.221.0/24 | vlan0 |
| 230.230.230.192/26 | wan1 |
| 250.250.250.0/23 | br0 |

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 remove 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 129** Configuration > Network > Interface > Bridge



Each field is described in the following table.

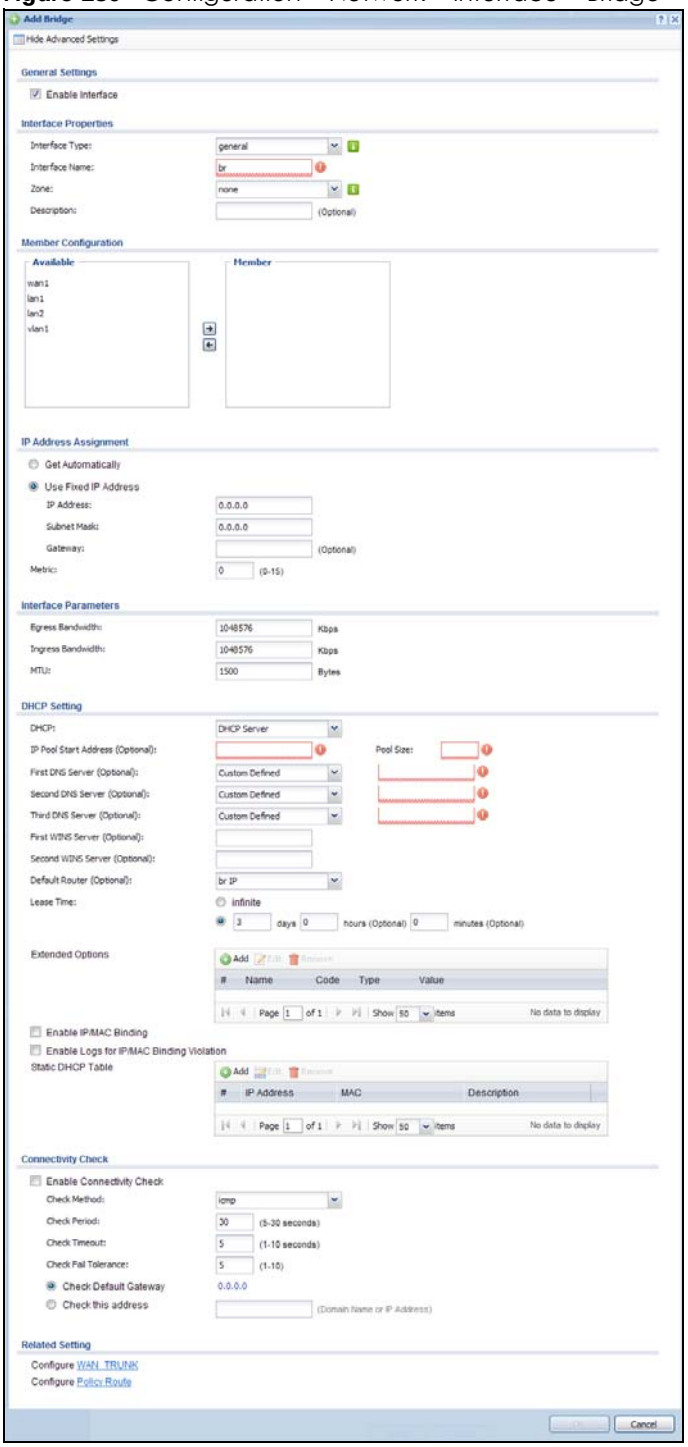
Table 84 Configuration > Network > Interface > Bridge

| 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. |
| 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 180 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.<br>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 130** Configuration > Network > Interface > Bridge > Add



Each field is described in the table below.

Table 85 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.<br><br>**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.<br><br>**external** is for connecting to an external network (like the Internet). The UAG automatically adds this interface to the default WAN trunk.<br><br>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 br*x*, 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:<br><br>• There is a virtual interface on top of it<br>• It is already used in a different bridge interface<br><br>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**.<br><br>Enter the IP address for this interface. |
| Subnet Mask | This field is enabled if you select **Use Fixed IP Address**.<br><br>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**. This field is enabled if you select **Use Fixed IP Address**.<br><br>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. |

Table 85 Configuration > Network > Interface > Bridge > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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 | |
| 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.<br>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. |
| DHCP Setting | |
| DHCP | Select what type of DHCP service the UAG provides to the network. Choices are:<br>**None** - the UAG does not provide any DHCP services. There is already a DHCP server on the network.<br>**DHCP Relay** - the UAG routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network.<br>**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**. |
| IP Pool Start Address | 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**.<br>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. |
| Pool Size | 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.<br>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. |
| First DNS Server<br>Second DNS Server<br>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.<br>**Custom Defined** - enter a static IP address.<br>**From ISP** - select the DNS server that another interface received from its DHCP server.<br>**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. |

Table 85 Configuration > Network > Interface > Bridge > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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.<br>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:<br>**infinite** - select this if IP addresses never expire<br>**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**.<br>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 181. |
| 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. |
| 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. |

Table 85 Configuration > Network > Interface > Bridge > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Check Method | Select the method that the gateway allows.<br>Select **icmp** to have the UAG regularly ping the gateway you specify to make sure it is still available.<br>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.

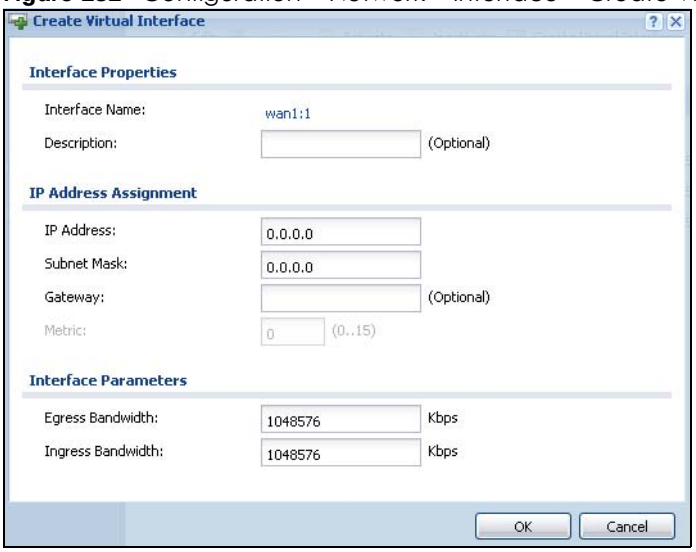
Virtual interfaces can be created on top of Ethernet interfaces, VLAN interfaces, or bridge interfaces. Virtual VLAN interfaces recognize and use the same VLAN ID. Otherwise, there is no difference between each type of virtual interface. Network policies (for example, security policy control rules) that 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 131** Configuration > Network > Interface > Create Virtual Interface




Each field is described in the table below.

Table 86 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 | |
| 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.<br><br>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 132** Example: Entry in the Routing Table Derived from Interfaces

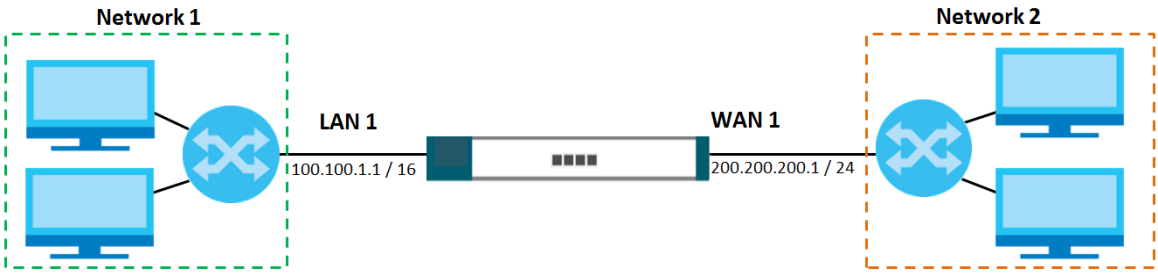



Table 87 Example: Routing Table Entries for Interfaces

| 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 88 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.

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.

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

- 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 89 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 206.
- Gateway - The interface provides the same gateway you specify for the interface. See IP Address Assignment on page 206.
- 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 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.

# CHAPTER 11
# Trunks

## 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 213) 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 214) 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 216) 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

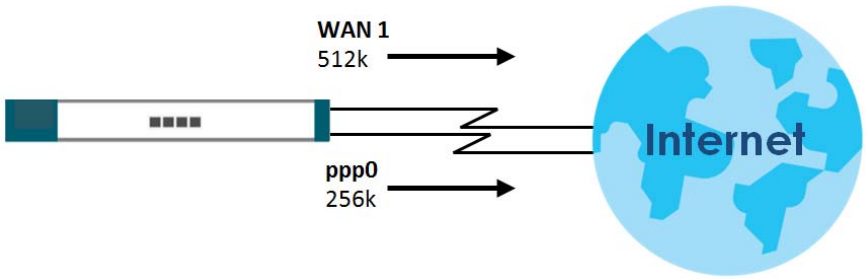
The following sections describe the load balancing algorithms the UAG can use to decide which interface the traffic (from the LAN) should use for a session[2]. The available bandwidth you configure on the UAG refers to the actual bandwidth provided by the ISP and the measured bandwidth refers to the 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 133** 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 90 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 given an equal

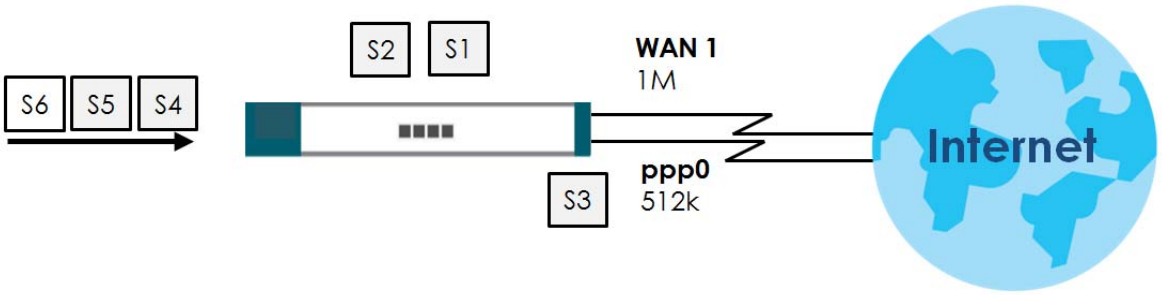
2. In the load balancing section, a session may refer to normal connection-oriented, UDP or SNMP2 traffic.

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 134** Weighted Round Robin Algorithm Example



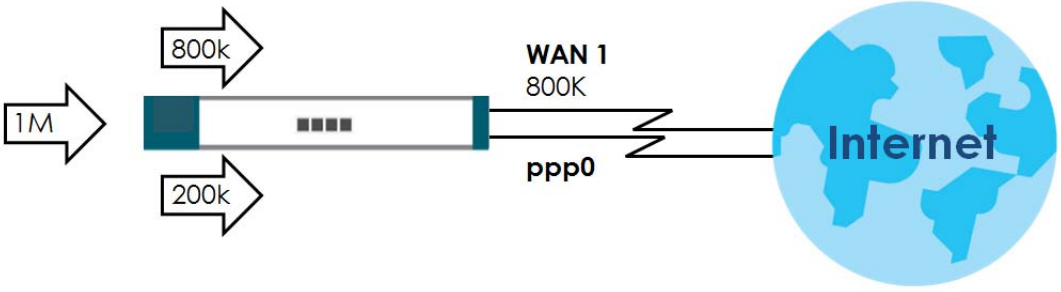

## Spillover

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.

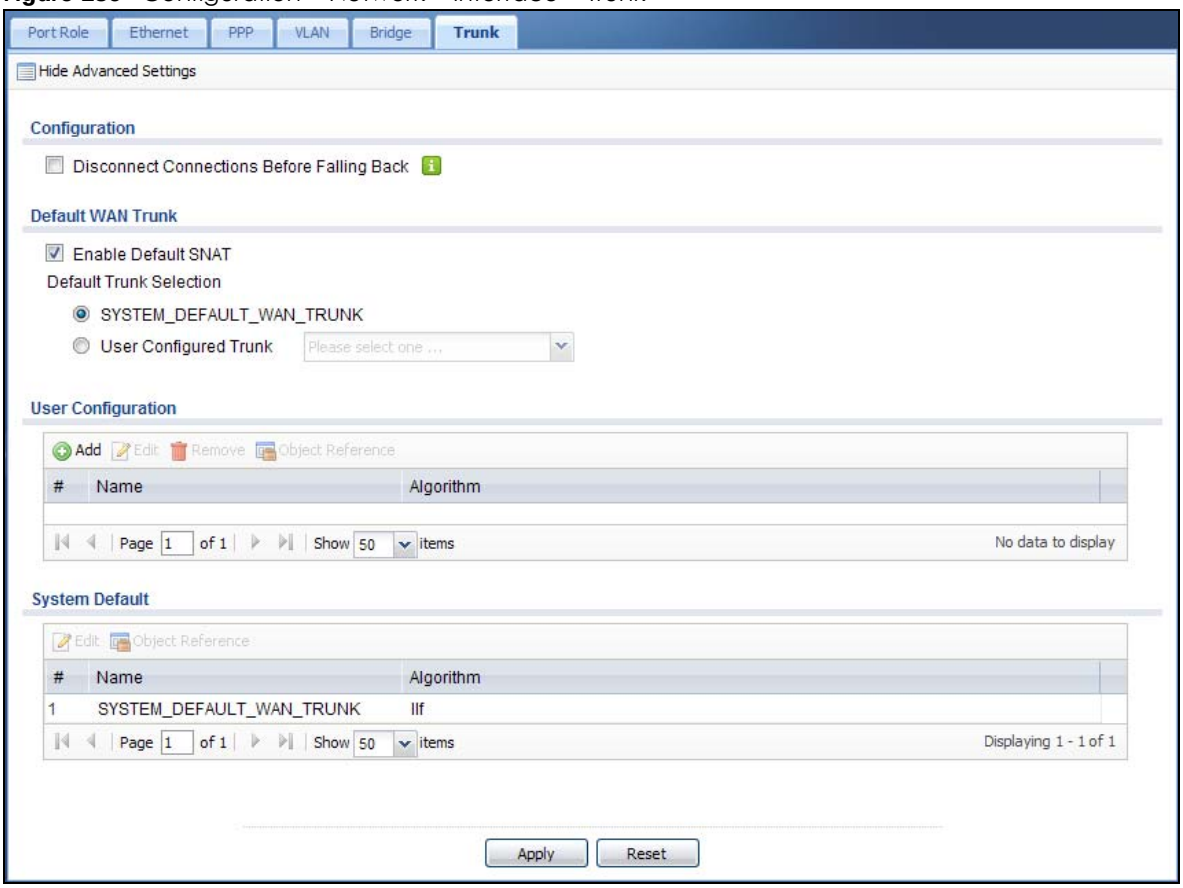
**Figure 135** Spillover Algorithm Example



# 11.2 The Trunk 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 136** Configuration > Network > Interface > Trunk




The following table describes the items in this screen.

Table 91 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. |

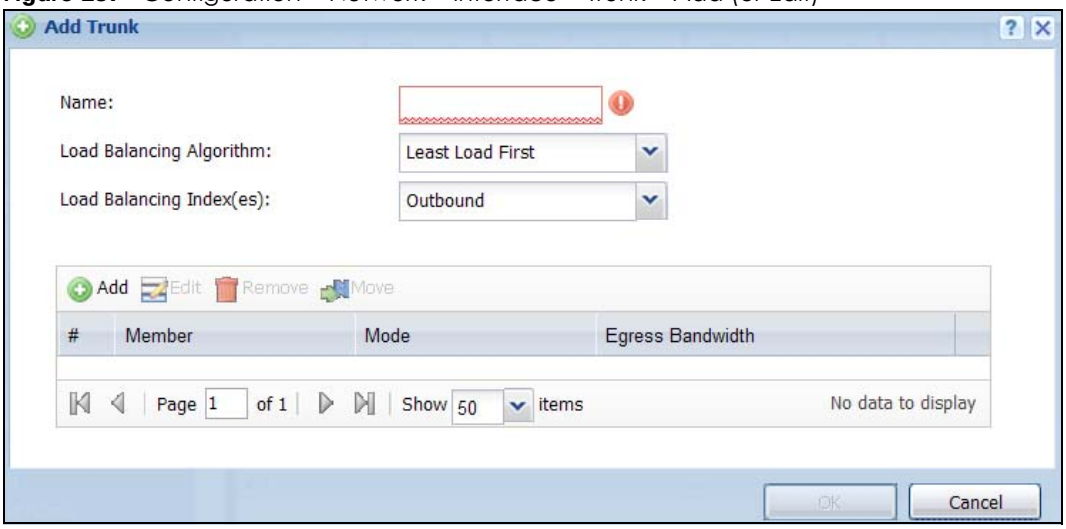
Table 91 Configuration > Network > Interface > Trunk (continued)

| 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 180 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 137** Configuration > Network > Interface > Trunk > Add (or Edit)



Each field is described in the table below.

Table 92 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 | Select a load balancing method to use from the drop-down list box.<br>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.<br>Select **Least Load First** to send new session traffic through the least utilized trunk member.<br>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). |
| Load Balancing Index(es) | This field is available if you selected to use the **Least Load First** or **Spillover** method.<br>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. |
| | 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 | Click this table cell and select **Active** to have the UAG always attempt to use this connection.<br>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. |
| 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 | This is reserved for future use.<br>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.<br>Note: You can configure the bandwidth of an interface in the corresponding interface edit screen. |
| 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.<br>Note: You can configure the bandwidth of an interface in the corresponding interface edit screen. |

Table 92 Configuration > Network > Interface > Trunk > Add (or Edit) (continued)

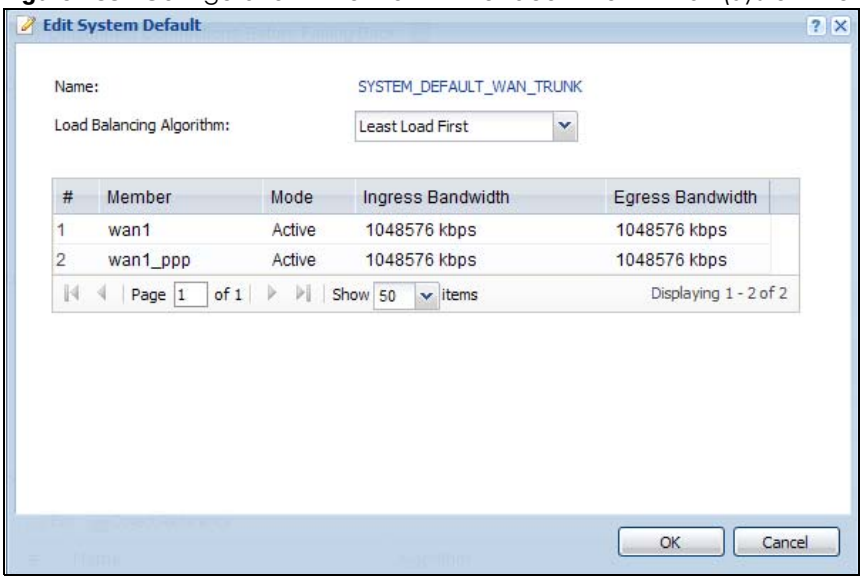
| LABEL | DESCRIPTION |
|---|---|
| Total Bandwidth | This field displays with the spillover load balancing algorithm. It displays the maximum number of kilobits of data the UAG is to send out and allow to come in through the interface per second.<br><br>You can configure the bandwidth of an interface 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.<br><br>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 138** Configuration > Network > Interface > Trunk > Edit (System Default)



Each field is described in the table below.

Table 93 Configuration > Network > Interface > Trunk > Edit (System Default)

| LABEL | DESCRIPTION |
|---|---|
| Name | This field displays the name of the selected system default trunk. |
| Load Balancing Algorithm | Select the load balancing method to use for the trunk.<br>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.<br>Select **Least Load First** to send new session traffic through the least utilized trunk member.<br>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). |
| | 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 | This field displays **Active** if the UAG always attempt to use this connection.<br>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. |
| 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 | This is reserved for future use.<br>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. |
| 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 | 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.<br>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. |

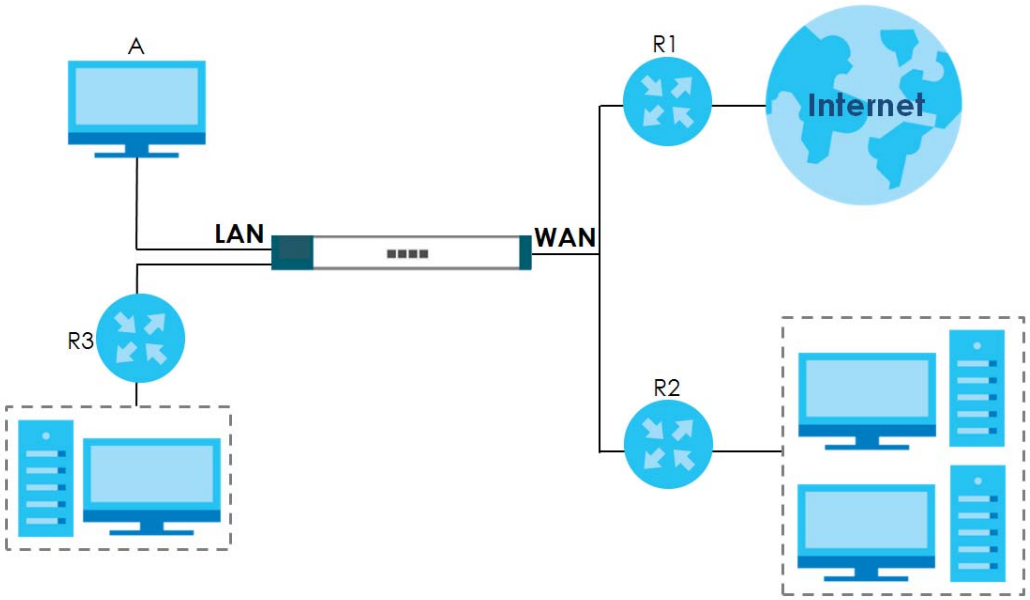
# CHAPTER 12
# Policy and Static Routes

## 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 139** 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 220) to list and configure policy routes.
- Use the **Static Route** screens (see Section 12.3 on page 226) 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 (6 bits) | Unused (2 bits) |
|---|---|

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 227 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 140** Configuration > Network > Routing > Policy Route

The following table describes the labels in this screen.

Table 94 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.<br>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.<br>**any** means all DSCP values or no DSCP marker.<br>**default** means traffic with a DSCP value of 0. This is usually best effort traffic<br>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 227 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. |
| DSCP Marking | 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.<br>**preserve** means the UAG does not modify the DSCP value of the route's outgoing packets.<br>**default** means the UAG sets the DSCP value of the route's outgoing packets to 0.<br>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 227 for more details. |

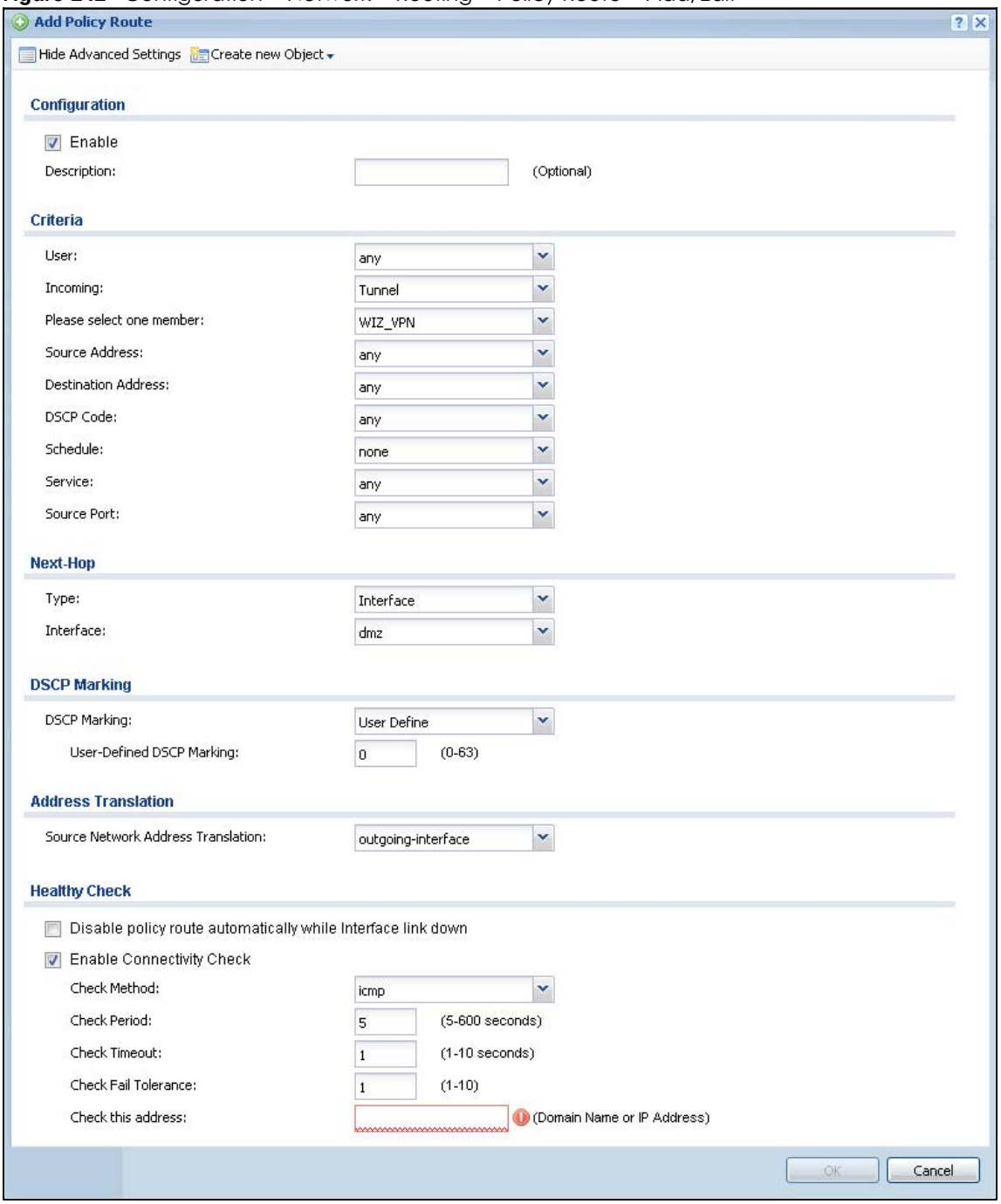
Table 94 Configuration > Network > Routing > Policy Route (continued)

| LABEL | DESCRIPTION |
|---|---|
| SNAT | This is the source IP address that the route uses.<br>It displays **none** if the UAG does not perform NAT for this route. |
| 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 141** Configuration > Network > Routing > Policy Route > Add/Edit




The following table describes the labels in this screen.

Table 95 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 95 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.<br>**any** means all DSCP value or no DSCP marker.<br>**default** means traffic with a DSCP value of 0. This is usually best effort traffic<br>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 227 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.<br>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.<br>Select **VPN Tunnel** to route the matched packets via the specified VPN tunnel to the remote IPSec router.<br>Select **Trunk** to route the matched packets through the interfaces in the trunk group based on the load balancing algorithm.<br>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 95 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 | Set how the UAG handles the DSCP value of the outgoing packets that match this route.<br>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 227 for more details.<br>Select **preserve** to have the UAG keep the packets' original DSCP value.<br>Select **default** to have the UAG set the DSCP value of the packets to 0. |
| 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 | Select **none** to not use NAT for the route.<br>Select **outgoing-interface** to use the IP address of the outgoing interface as the source IP address of the packets that matches this route.<br>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.<br>Otherwise, select a pre-defined address (group) to use as the source IP address(es) of the packets that match this route.<br>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. |
| 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 | This option is available when you select **Interface** or **Gateway** in the **Type** field.<br>Select this to turn on the connection check. |
| Check Method | Select the method that the gateway allows.<br>Select **icmp** to have the UAG regularly ping the gateway you specify to make sure it is still available.<br>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 Port | This field only displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check. |

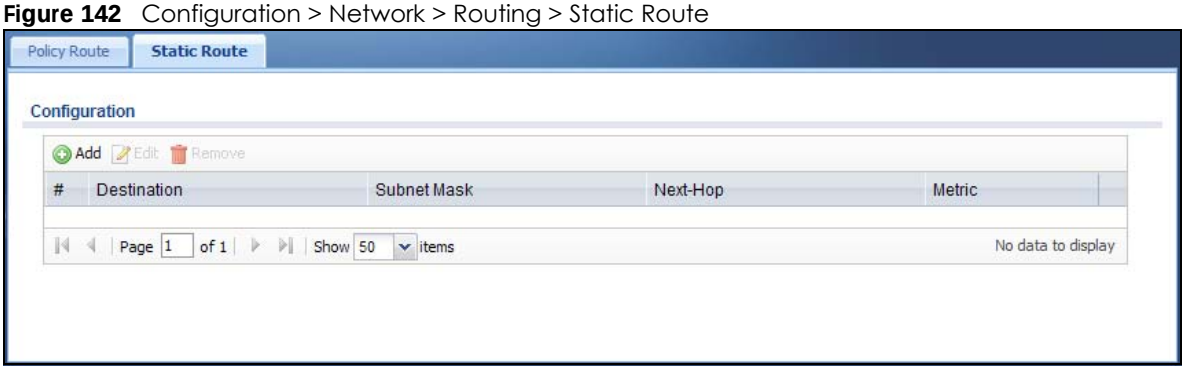
Table 95 Configuration > Network > Routing > Policy Route > Add/Edit (continued)

| 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 142** Configuration > Network > Routing > Static Route




The following table describes the labels in this screen.

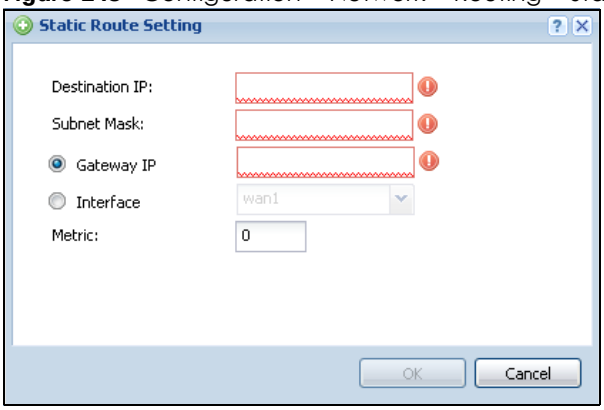
Table 96 Configuration > Network > Routing > Static Route

| 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 143** Configuration > Network > Routing > Static Route > Add




The following table describes the labels in this screen.

Table 97 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.<br>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 98 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) |

# CHAPTER 13
# DDNS

## 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 230) 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 231) 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 99 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 144** Configuration > Network > DDNS

The following table describes the labels in this screen.

Table 100 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.<br>**from interface** - The IP address comes from the specified interface.<br>**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.<br>**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.<br>**from interface** - The IP address comes from the specified interface.<br>**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.<br>**custom** - The IP address is static. |

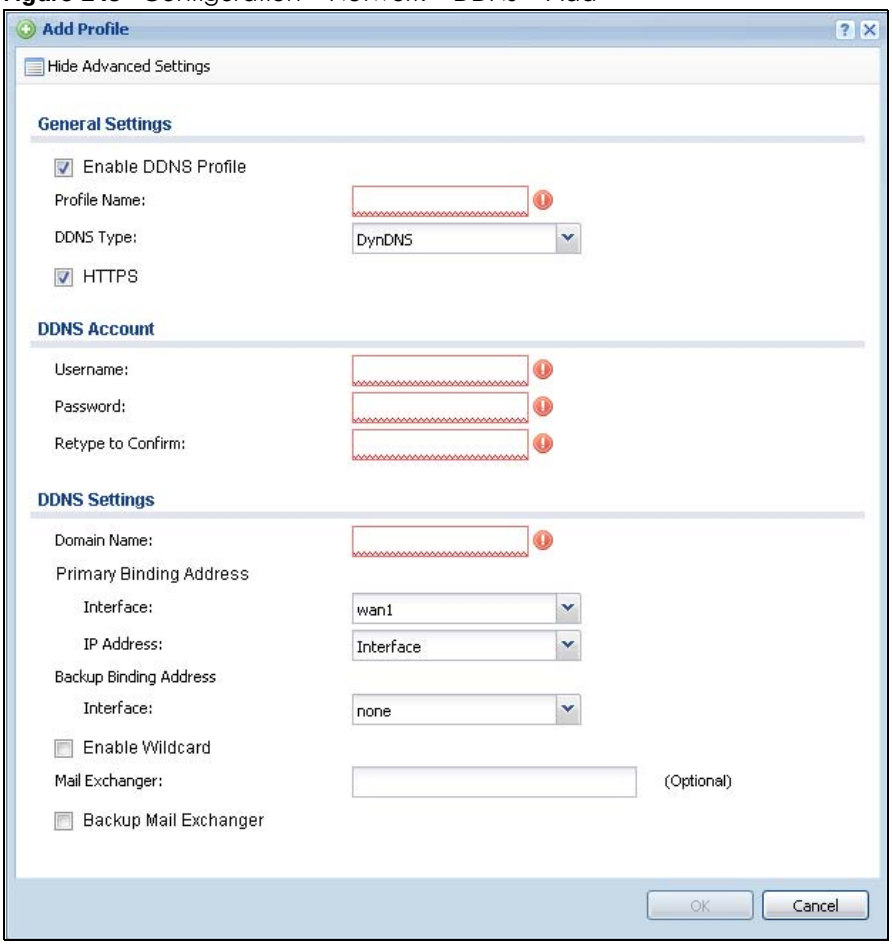
Table 100 Configuration > Network > DDNS (continued)

| 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 145** Configuration > Network > DDNS > Add




The following table describes the labels in this screen.

Table 101 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 101 Configuration > Network > DDNS > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Show/Hide Advanced Settings | Click this button to display a greater or lesser number of configuration fields. |
| General Settings | |
| Enable DDNS Profile | Select this to enable DDNS. Clear this to disable it. |
| Profile Name | 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.<br>This field is read-only when you are editing an entry. |
| 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 | 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.<br>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. |
| 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 | The options available in this field vary by DDNS provider.<br>**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.<br>**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.<br>Note: The UAG may not determine the proper IP address if there is an HTTP proxy server between the UAG and the DDNS server.<br>**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. |
| 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 101 Configuration > Network > DDNS > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| IP Address | The options available in this field vary by DDNS provider.<br><br>**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.<br><br>**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.<br><br>Note: The UAG may not determine the proper IP address if there is an HTTP proxy server between the UAG and the DDNS server.<br><br>**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. |
| 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 | This option is only available with a DynDNS account.<br><br>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. |
| Mail Exchanger | This option is only available with a DynDNS account.<br><br>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.<br><br>If you are using this service, type the host record of your mail server here. Otherwise leave the field blank.<br><br>See www.dyndns.org for more information about mail exchangers. |
| Backup Mail Exchanger | This option is only available with a DynDNS account.<br><br>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. |
| 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 | This field displays when you select **User custom** from the **DDNS Type** field above. These are the options supported at the time of writing:<br><br>• dyndns_system to specify the DYNDNS Server type - for example, dyndns@dyndns.org<br>• ip_server_name which should be the URL to get the server's public IP address - for example, http://myip.easylife.tw/ |
| OK | Click **OK** to save your changes back to the UAG. |
| Cancel | Click **Cancel** to exit this screen without saving. |

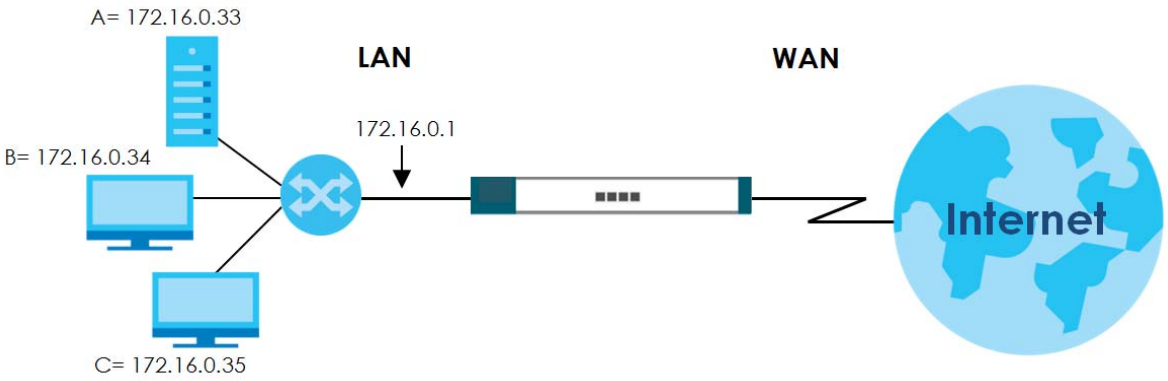
# CHAPTER 14
# NAT

## 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 146** 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 235) 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.

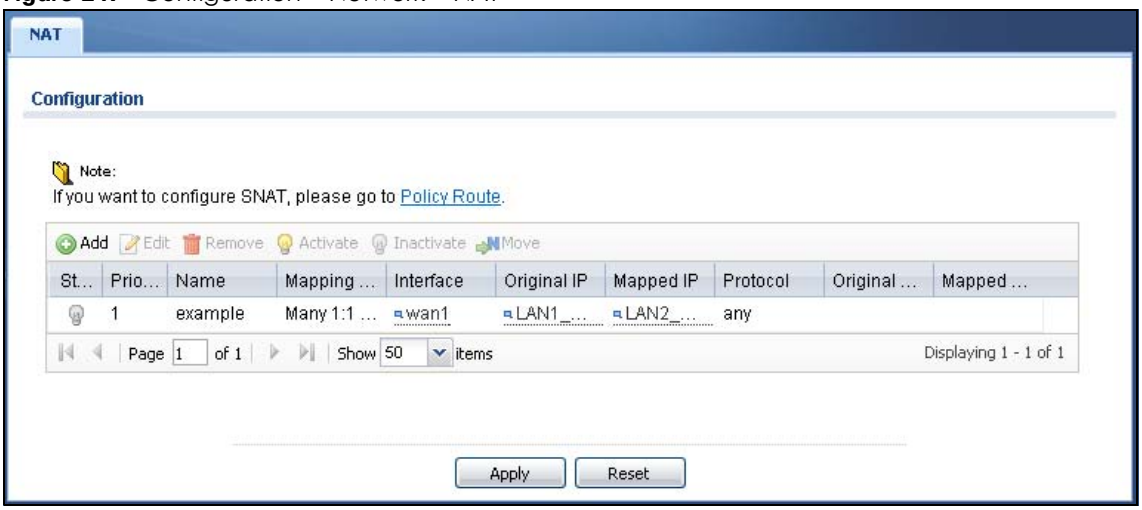
#### Finding Out More

- See Section 14.3 on page 239 for technical background information related to these screens.

# 14.2 The NAT Screen

The **NAT** 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 147** Configuration > Network > NAT




The following table describes the labels in this screen.

Table 102 Configuration > Network > NAT

| LABEL | DESCRIPTION |
|---|---|
| Configuration | |
| 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.<br>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. |

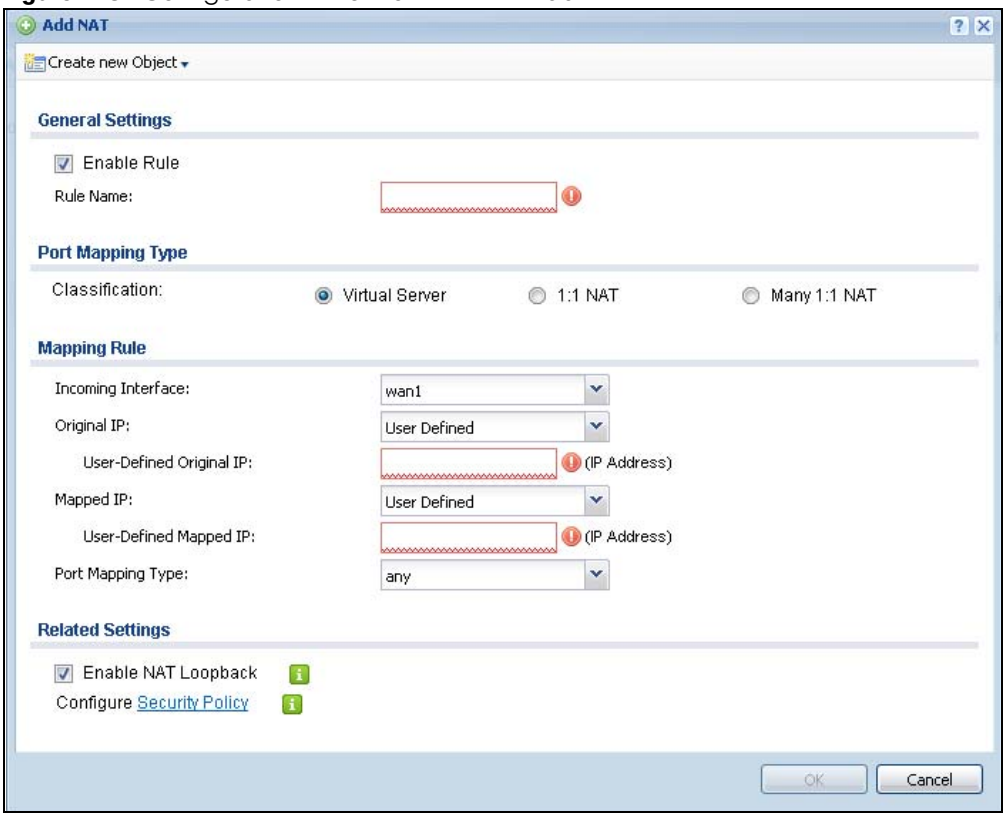
Table 102 Configuration > Network > NAT (continued)

| 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 235.) Then, click on an **Add** icon or **Edit** icon to open the following screen.

**Figure 148** Configuration > Network > NAT > Add




The following table describes the labels in this screen.

Table 103 Configuration > Network > NAT > Add

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

Table 103 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. |
| Port Mapping Type | |
| Classification | Select what kind of NAT this rule is to perform.<br>**Virtual Server** - This makes computers on a private network behind the UAG available to a public network outside the UAG (like the Internet).<br>**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.<br>**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.<br>One many 1:1 NAT rule works like multiple 1:1 NAT rules, but it eases configuration effort since you only create one rule. |
| Mapping Rule | |
| 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 | Specify the destination IP address of the packets received by this NAT rule's specified incoming interface.<br>**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.<br>**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.<br>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. |
| 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 | Select to which translated destination IP address this NAT rule forwards packets.<br>**User Defined** - this NAT rule supports a specific IP address, specified in the **User-Defined Mapped IP** field. |
| 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 103 Configuration > Network > NAT > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Port Mapping Type | 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:<br>**Any** - this NAT rule supports all the destination ports.<br>**Service** - this NAT rule supports the destination port(s) used by the specified service(s).<br>**Port** - this NAT rule supports one destination port.<br>**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.<br>This field is read-only and displays **any** for **Many 1:1 NAT**. |
| 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. |
| Related Settings | |
| Enable NAT Loopback | 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.<br>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 239 for more details.<br>If you do not enable NAT loopback, this NAT rule only applies to packets received on the rule's specified incoming interface. |
| Security Policy | 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.<br>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. |
| 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

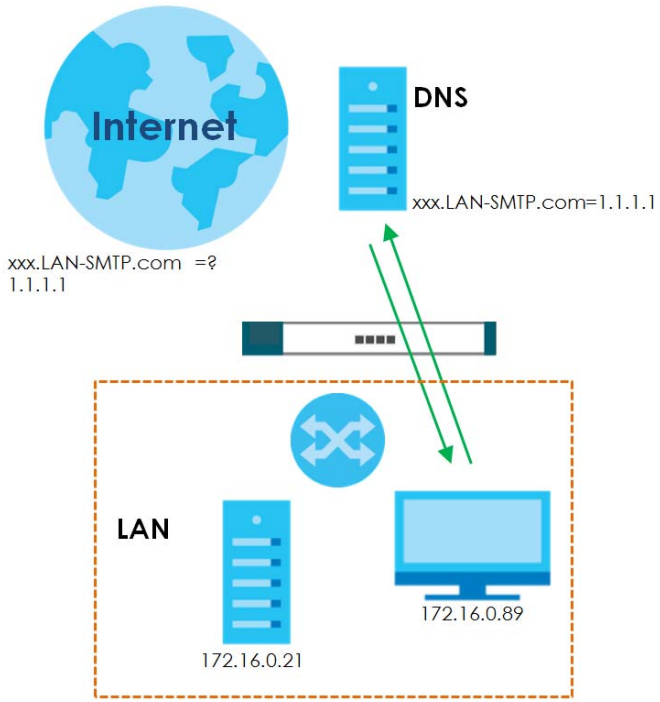
Here is more detailed information about NAT on the UAG.

## 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.

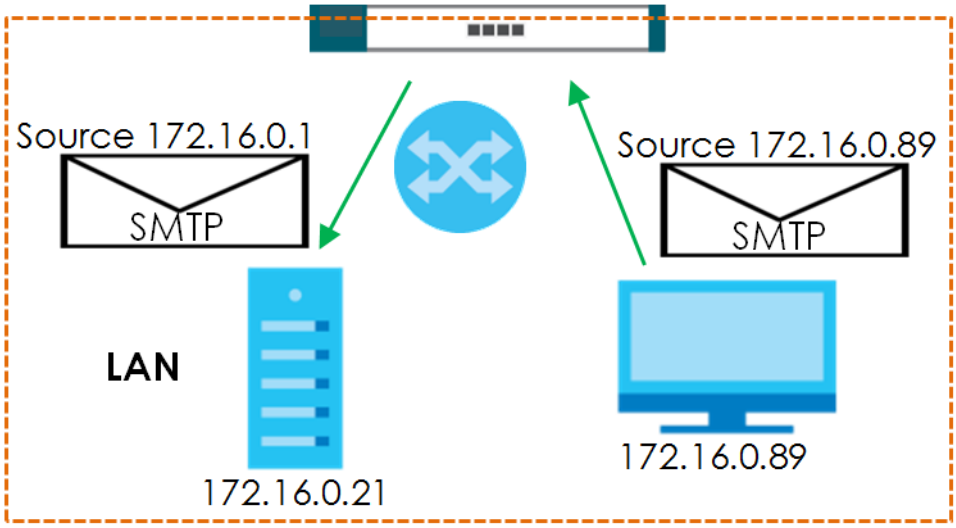
For example, a LAN user's computer at IP address 172.16.0.89 queries a public DNS server to resolve the SMTP server's domain name (xxx.LAN-SMTP.com in this example) and gets the SMTP server's mapped public IP address of 1.1.1.1.

**Figure 149** LAN Computer Queries a Public DNS Server



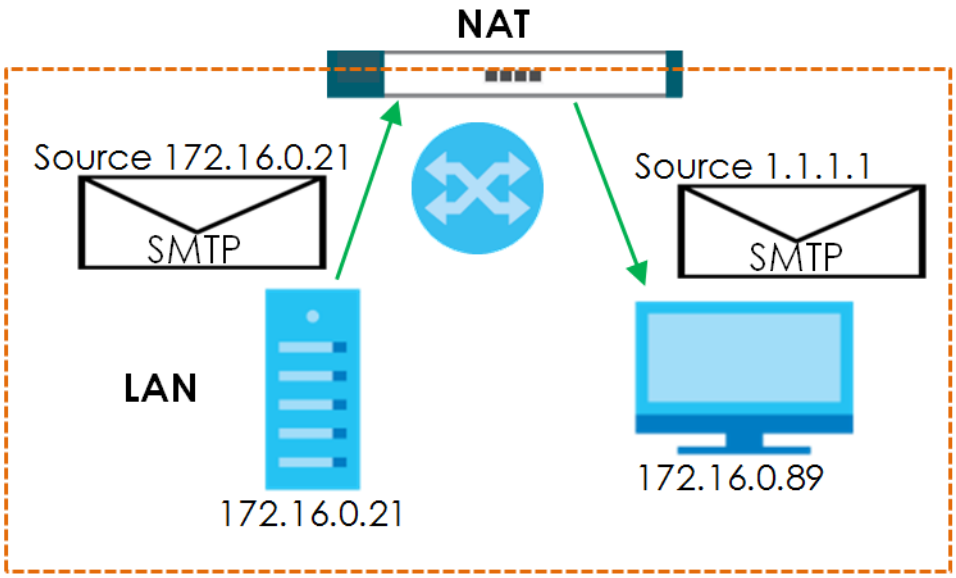

The LAN user's computer then sends traffic to IP address 1.1.1.1. NAT loopback uses the IP address of the UAG's lan1 interface (172.16.0.1) as the source address of the traffic going from the LAN users to the LAN SMTP server.

**Figure 150** 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 151** LAN to LAN Return Traffic



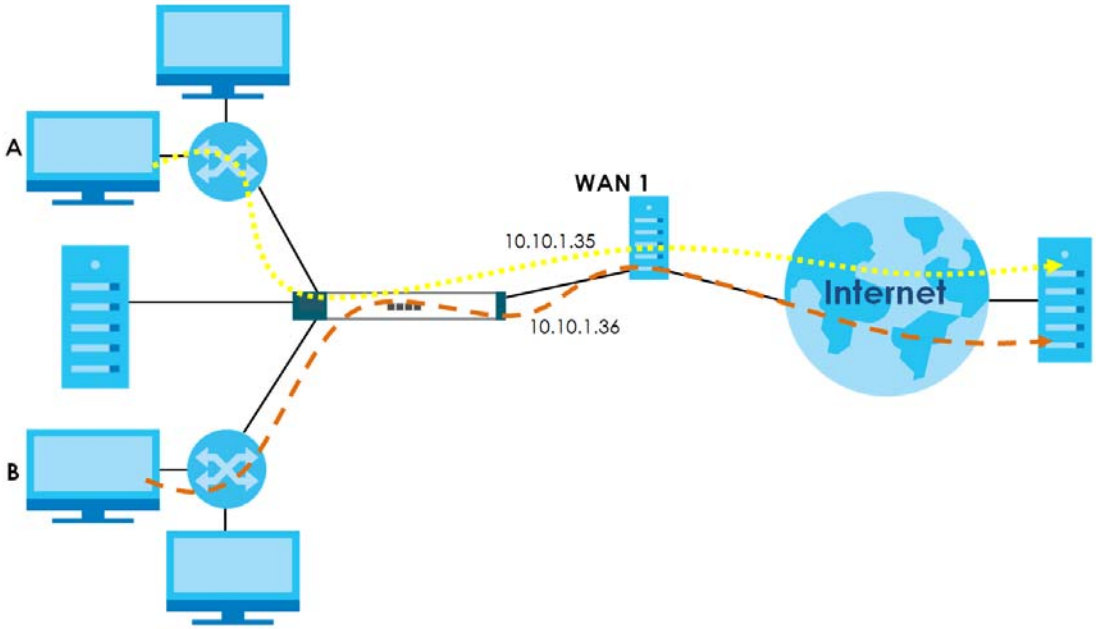
# CHAPTER 15
# VPN 1-1 Mapping

## 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 152** 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 242) 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 244) 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.

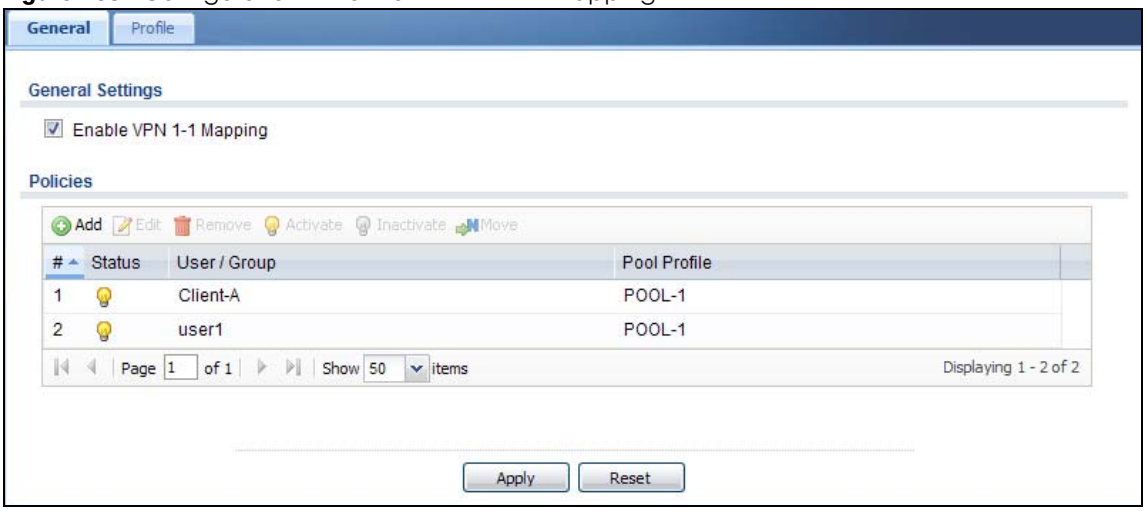
To make the example in Figure 152 on page 241 work, make sure you have the following settings. For traffic between **lan1** or **lan2** and **wan1**:

- 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 153** Configuration > Network > VPN 1-1 Mapping



The following table describes the labels in this screen.

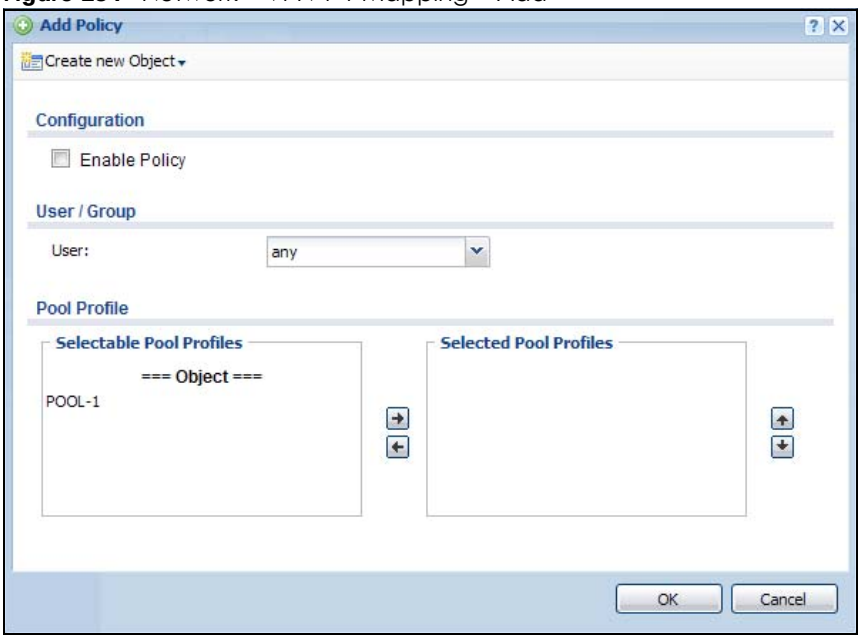
Table 104 Configuration > Network > VPN 1-1 Mapping

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Enable VPN 1-1 Mapping | Select this option to enable VPN 1-1 mapping on the UAG. |
| Policies | |
| 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.<br>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 154** Network > VPN 1-1 Mapping > Add




The following table describes the labels in this screen.

Table 105 Network > VPN 1-1 Mapping > Add

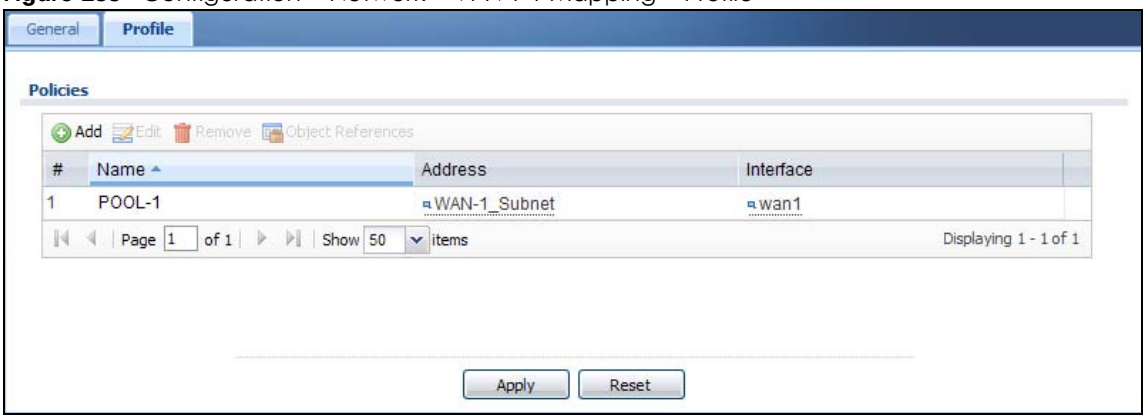
| LABEL | DESCRIPTION |
|---|---|
| Create New Object | Click this button to create any new user/group objects that you need to use in this screen. |
| Configuration | |
| Enable Policy | Use this option to turn the VPN 1-1 mapping rule on or off. |
| User/Group | Use the drop-down list box to select the individual or group for which you want to use this rule.<br>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.<br>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.<br>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 155** Configuration > Network > VPN 1-1 Mapping > Profile




The following table describes the labels in this screen.

Table 106 Configuration > Network > VPN 1-1 Mapping > Profile

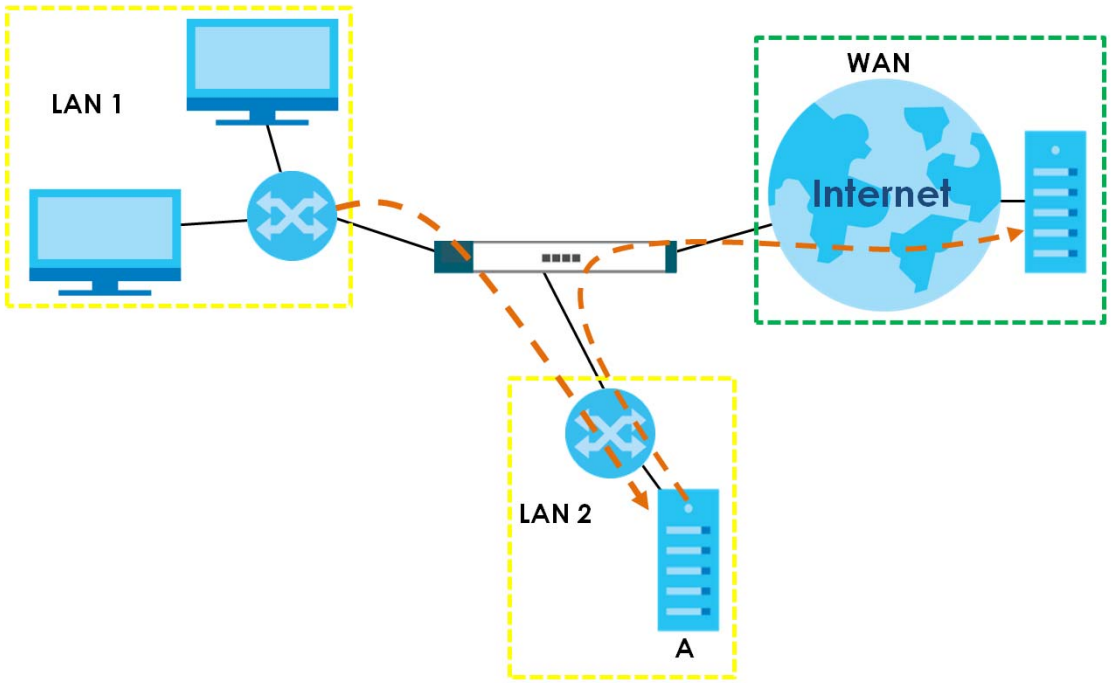
| LABEL | DESCRIPTION |
|---|---|
| Policies | |
| Add | Click this to add an entry to the table.<br>If you click **Add** without selecting an entry in advance then the new entry appears as the first entry. |
| Edit | Double-click an entry or select it and click **Edit** to be able to modify the entry's 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 180 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.<br>Note: You cannot select an address group object at the time of writing.<br>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. |

# CHAPTER 16
# 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 156** HTTP Redirect Example




### 16.1.1 What You Can Do in this Chapter

Use the **HTTP Redirect** screens (see Section 16.2 on page 247) 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 156 on page 246 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**:

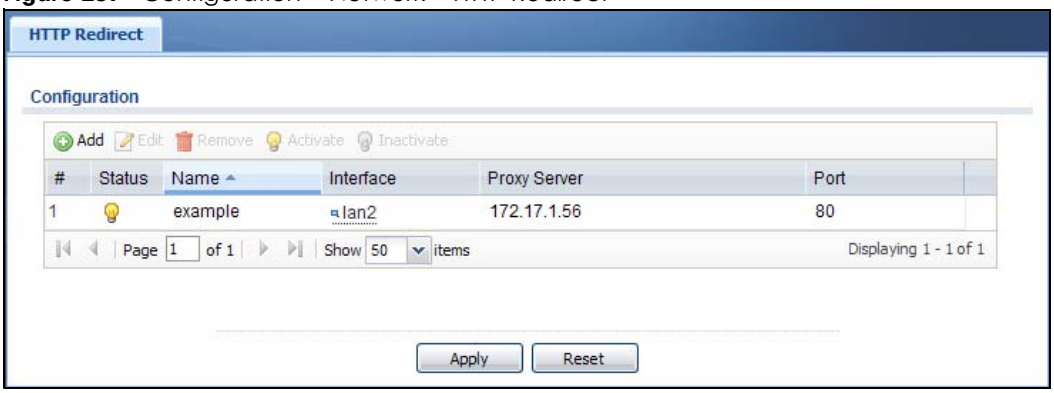
- a from LAN2 to WAN security policy (default) to allow HTTP requests from **lan2** to **wan1**. Responses to these requests are allowed automatically.
- a policy route to forward HTTP traffic from proxy server **A** to the Internet.

## 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 157** Configuration > Network > HTTP Redirect




The following table describes the labels in this screen.

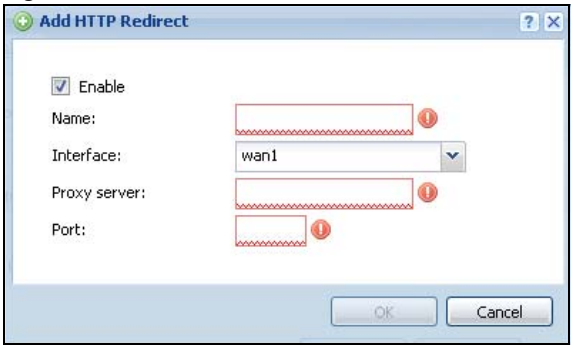
Table 107 Configuration > Network > HTTP Redirect

| 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 Add/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 158** Network > HTTP Redirect > Edit



The following table describes the labels in this screen.

Table 108 Network > HTTP Redirect > Add/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. |

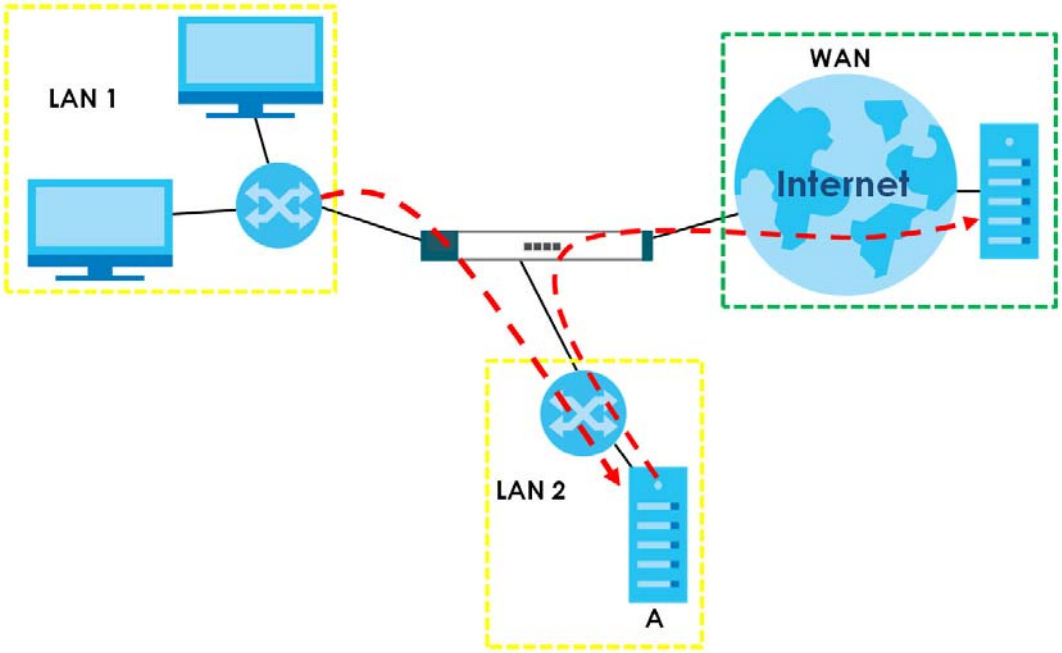
# CHAPTER 17
# SMTP Redirect

## 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 159** SMTP Redirect Example




### 17.1.1 What You Can Do in this Chapter

Use the **SMTP Redirect** screens (see Section 17.2 on page 251) 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 159 on page 250 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**:

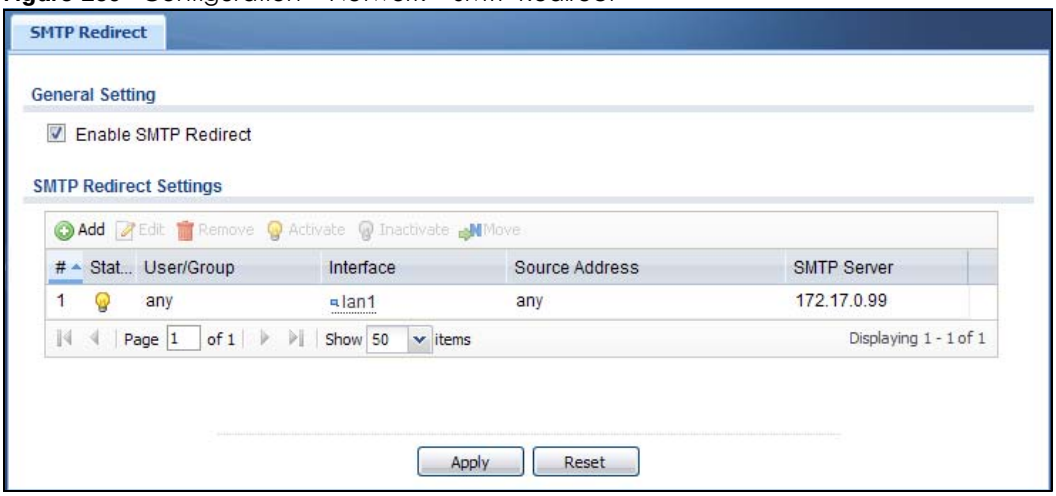
- a from LAN2 to WAN security policy (default) to allow SMTP messages from **lan2** to **wan1**. Responses to these requests are allowed automatically.
- a policy route to forward SMTP messages from SMTP server **A** to the Internet.

## 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 160** Configuration > Network > SMTP Redirect




The following table describes the labels in this screen.

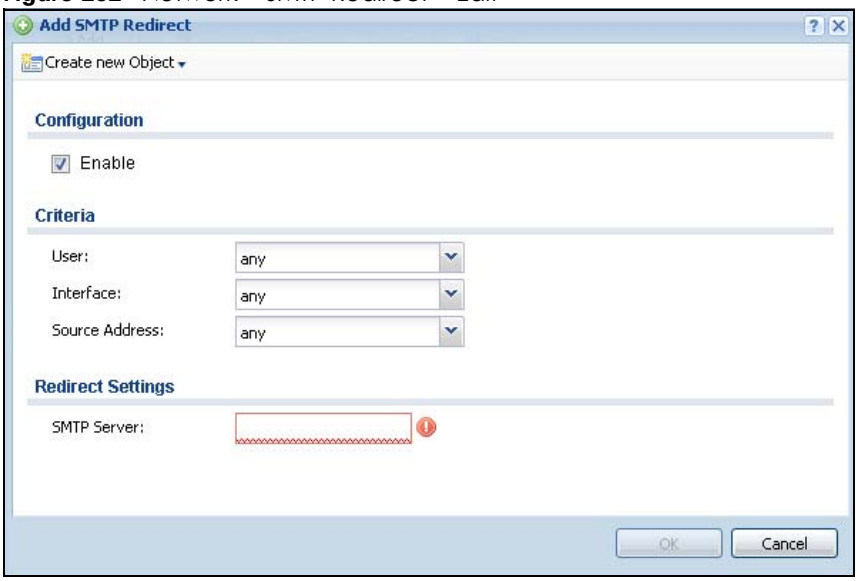
Table 109 Configuration > Network > SMTP Redirect

| LABEL | DESCRIPTION |
|---|---|
| General Setting | |
| 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.<br>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 161** Network > SMTP Redirect > Edit




The following table describes the labels in this screen.

Table 110 Network > SMTP Redirect > Edit

| LABEL | DESCRIPTION |
|---|---|
| Configuration | |
| Enable | Use this option to turn the SMTP redirect rule on or off. |
| Criteria | |
| User | Use the drop-down list box to select the individual user or user group for which you want to use this rule.<br>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. |
| Redirect Settings | |
| 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. |

# CHAPTER 18
# ALG

## 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 255) 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.

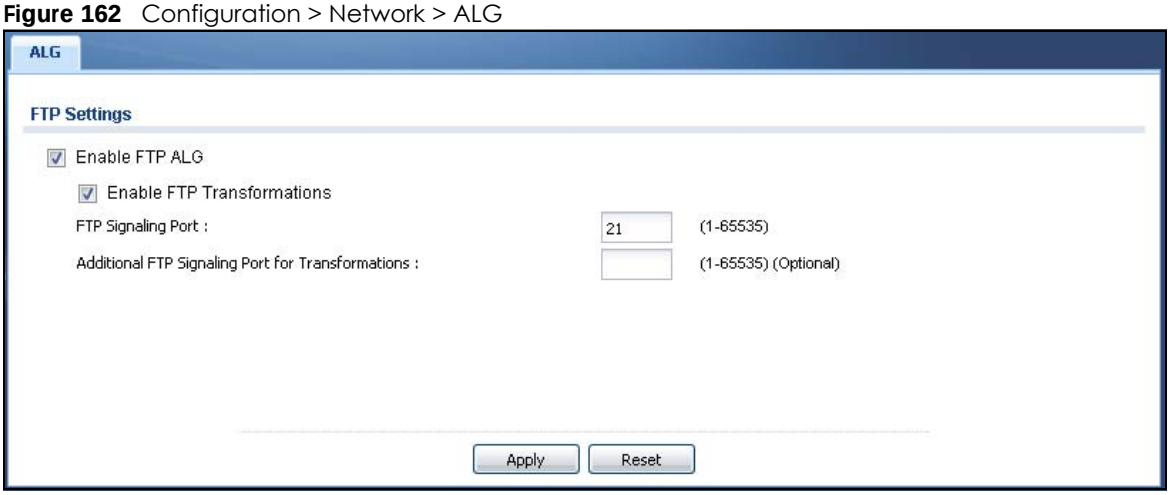
### 18.1.3 Before You Begin

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 162** Configuration > Network > ALG




The following table describes the labels in this screen.

Table 111 Configuration > Network > ALG

| LABEL | DESCRIPTION |
|---|---|
| FTP Settings | |
| 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.<br>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. |

# CHAPTER 19
# UPnP

## 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.

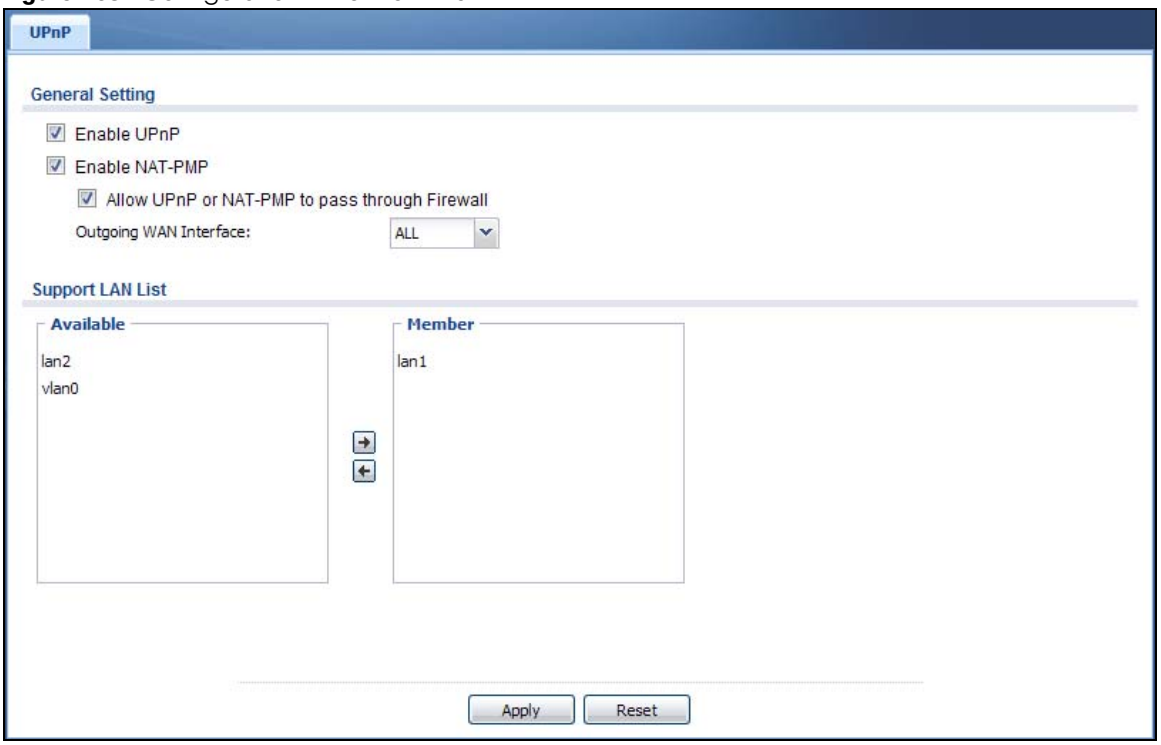
All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

## 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 163** Configuration > Network > UPnP




The following table describes the fields in this screen.

Table 112 Configuration > Network > UPnP

| LABEL | DESCRIPTION |
|---|---|
| General Setting | |
| 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). |

Table 112 Configuration > Network > UPnP (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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.<br>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.<br>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

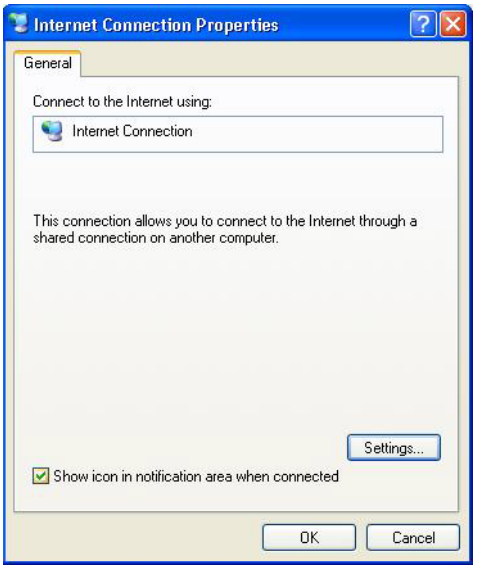
1 Click **start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

2 Right-click the icon and select **Properties**.

**Figure 164** Network Connections

3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

**Figure 165** Internet Connection Properties




4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

**Figure 166** Internet Connection Properties: Advanced Settings

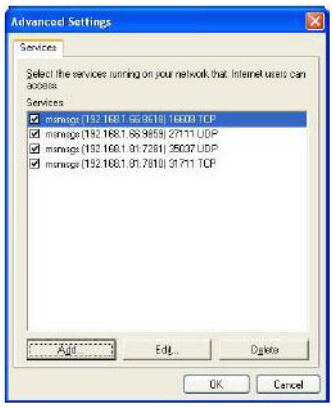
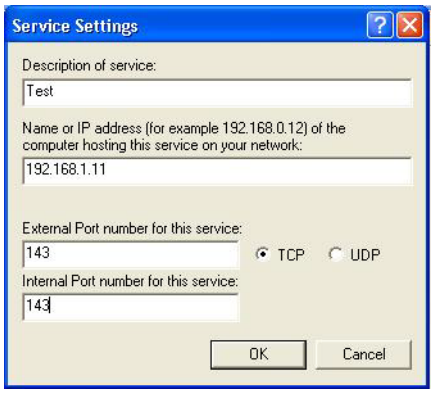


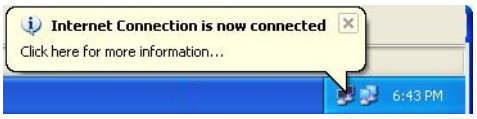
**Figure 167** Internet Connection Properties: Advanced Settings: Add




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 168** System Tray Icon




6 Double-click on the icon to display your current Internet connection status.

**Figure 169** 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.

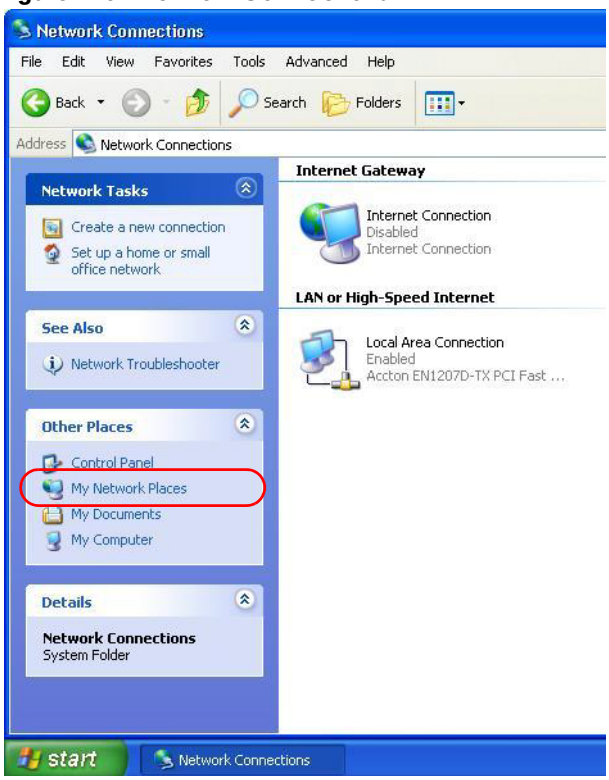
Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

**Figure 170** 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 171** 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 172** Network Connections: My Network Places: Properties: Example

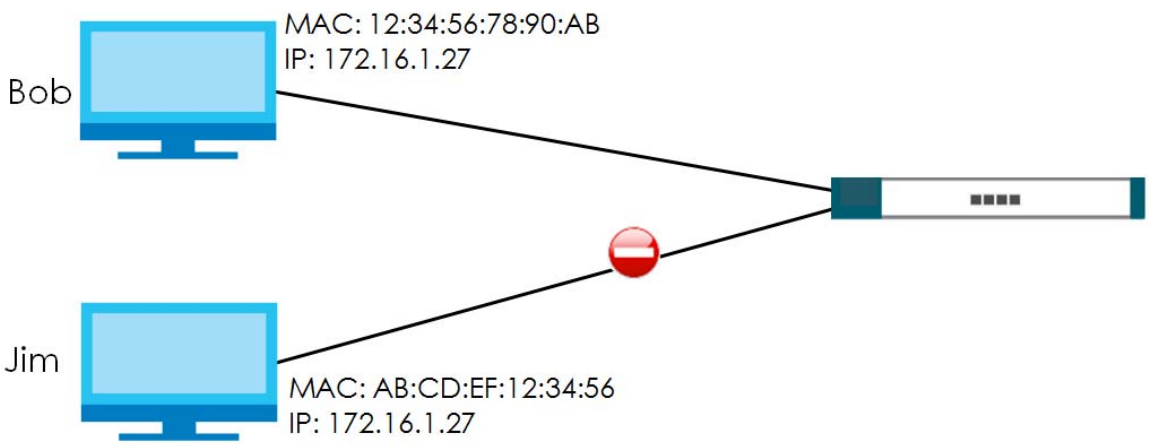
# CHAPTER 20
# IP/MAC Binding

## 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 173** 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 264) to bind IP addresses to MAC addresses.
- Use the **Exempt List** screen (Section 20.3 on page 266) 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.

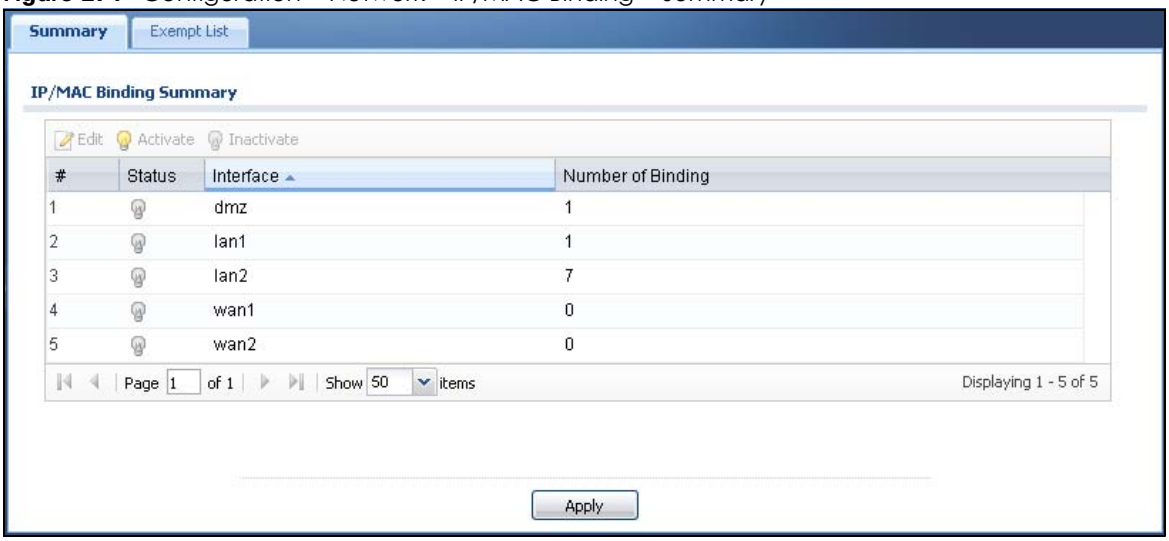
### Interfaces Used With IP/MAC Binding

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 Screen

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 174** Configuration > Network > IP/MAC Binding > Summary




The following table describes the labels in this screen.

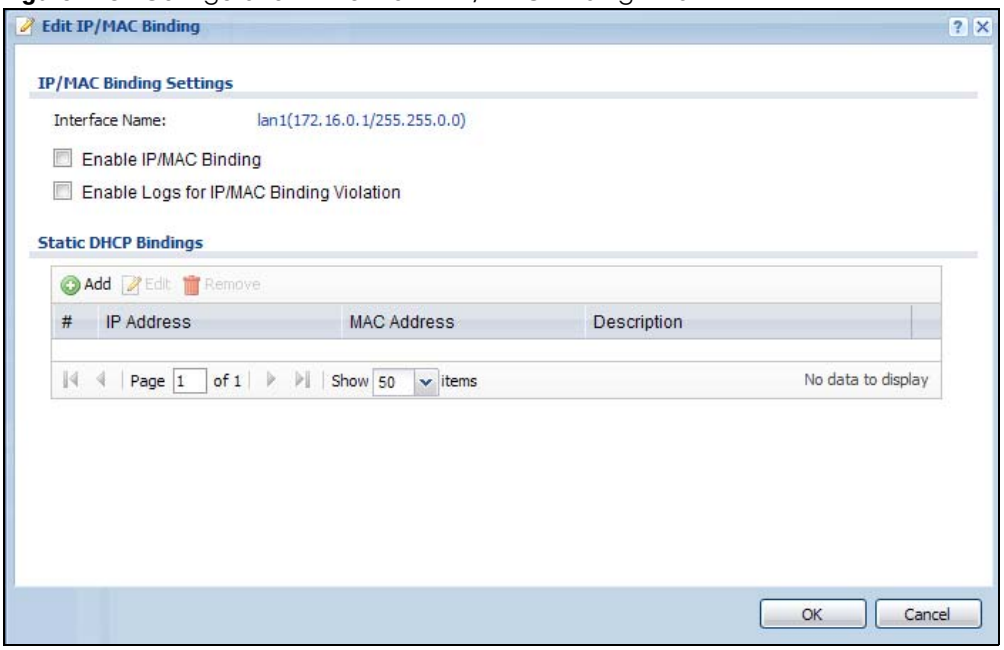
Table 113 Configuration > Network > IP/MAC Binding > Summary

| 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 175** Configuration > Network > IP/MAC Binding > Edit




The following table describes the labels in this screen.

Table 114 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. |

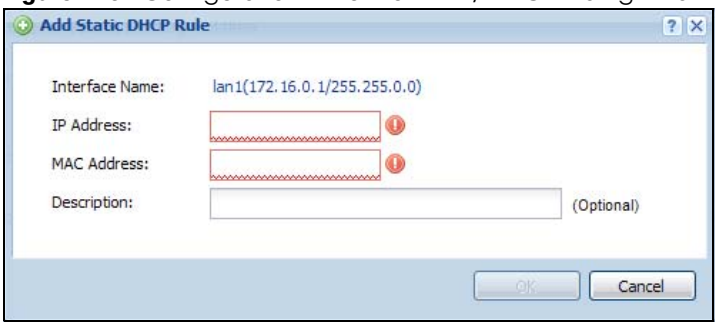
Table 114 Configuration > Network > IP/MAC Binding > Edit (continued)

| 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 176** Configuration > Network > IP/MAC Binding > Edit > Add




The following table describes the labels in this screen.

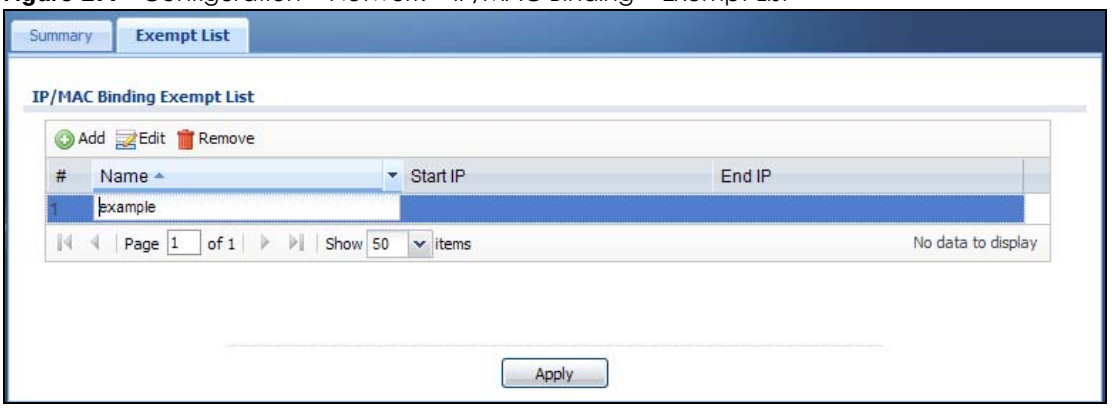
Table 115 Configuration > Network > IP/MAC Binding > Edit > Add

| 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 177** Configuration > Network > IP/MAC Binding > Exempt List




The following table describes the labels in this screen.

Table 116 Configuration > Network > IP/MAC Binding > Exempt List

| LABEL | DESCRIPTION |
|---|---|
| IP/MAC Binding Exempt List | |
| 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. |

# CHAPTER 21
# Layer 2 Isolation

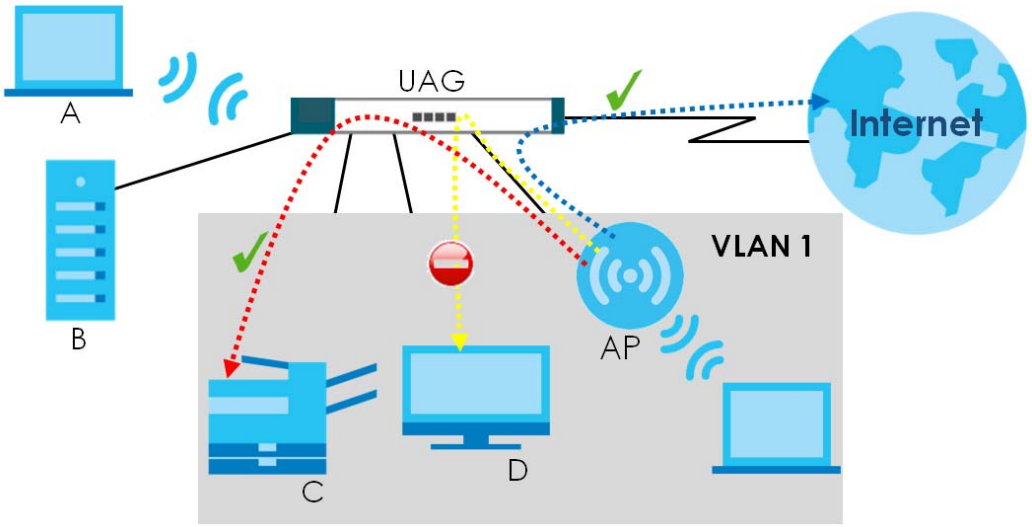
## 21.1 Overview

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 178** Layer-2 Isolation Application



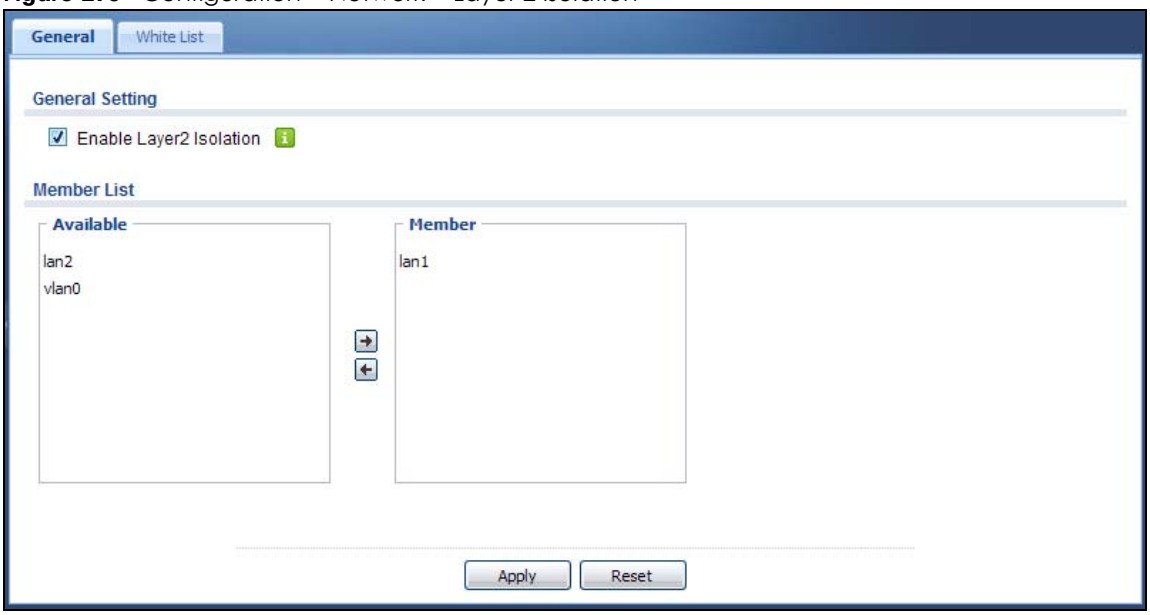

### 21.1.1 What You Can Do in this Chapter

- Use the **General** screen (Section 21.2 on page 269) to enable layer-2 isolation on the UAG and the internal interface(s).
- Use the **White List** screen (Section 21.3 on page 269) 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 179** Configuration > Network > Layer 2 Isolation




The following table describes the labels in this screen.

Table 117 Configuration > Network > Layer 2 Isolation

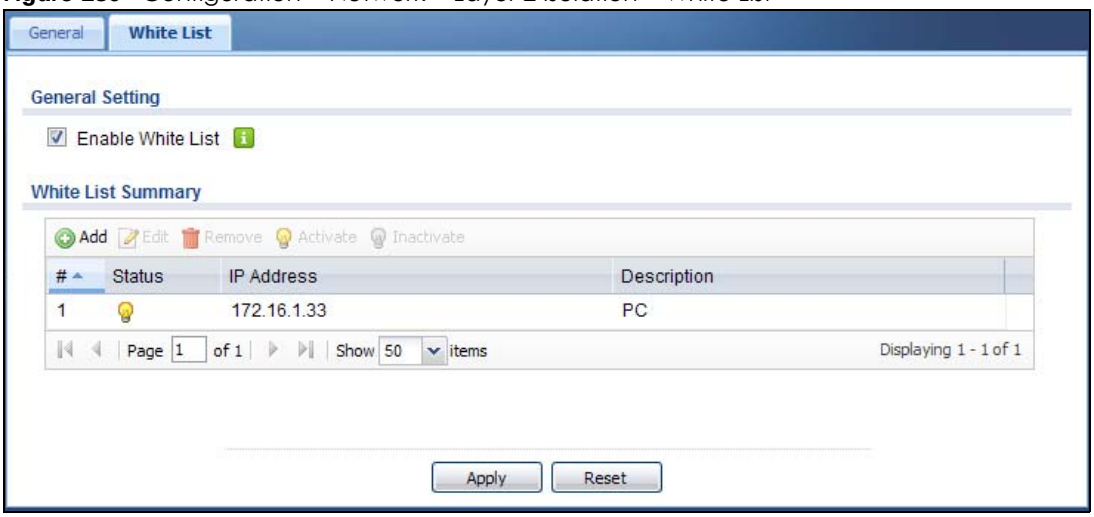
| LABEL | DESCRIPTION |
|---|---|
| General Setting | |
| Enable Layer2 Isolation | Select this option to turn on the layer-2 isolation feature on the UAG.<br>Note: You can enable this feature only when the security policy is enabled. |
| Member List | The **Available** list displays the name(s) of the internal interface(s) on which you can enable layer-2 isolation.<br>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 180** Configuration > Network > Layer 2 Isolation > White List




The following table describes the labels in this screen.

Table 118 Configuration > Network > Layer 2 Isolation > White List

| LABEL | DESCRIPTION |
|---|---|
| General Setting | |
| Enable White List | Select this option to turn on the white list on the UAG.<br><br>Note: You can enable this feature only when the security policy is enabled. |
| White List Summary | |
| 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. |

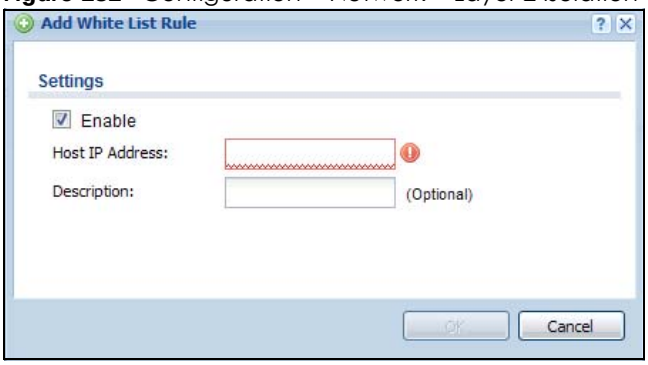
## 21.3.1 Add/Edit White List Rule

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 181** Configuration > Network > Layer 2 Isolation > White List > Add/Edit




The following table describes the labels in this screen.

Table 119 Configuration > Network > Layer 2 Isolation > White List > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Settings | |
| 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. |

# CHAPTER 22
# IPnP

## 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.

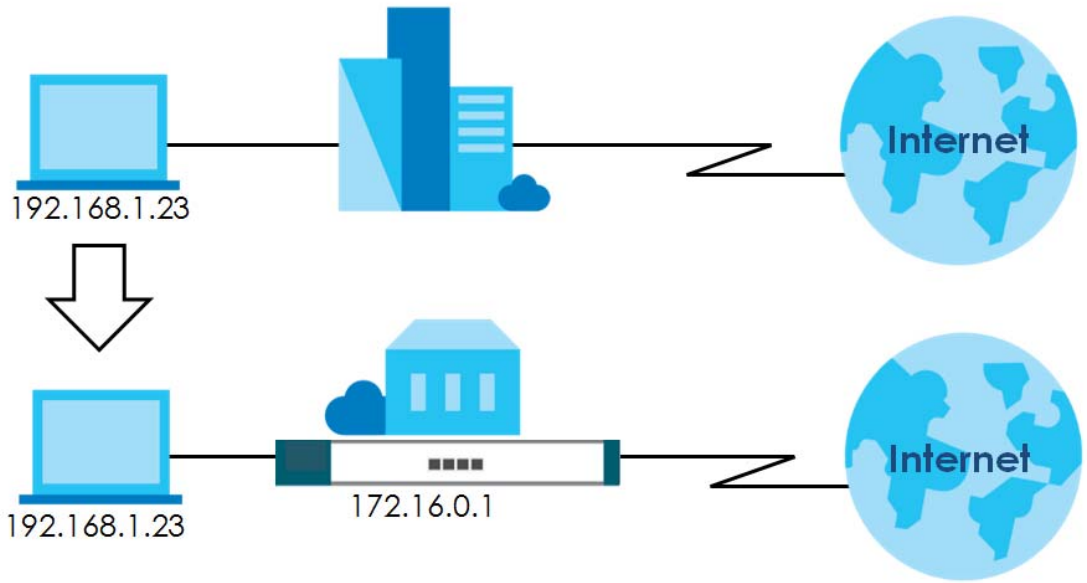
When you disable the IPnP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the UAG's LAN IP address can connect to the UAG or access the Internet through the UAG.

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 182** IPnP Application



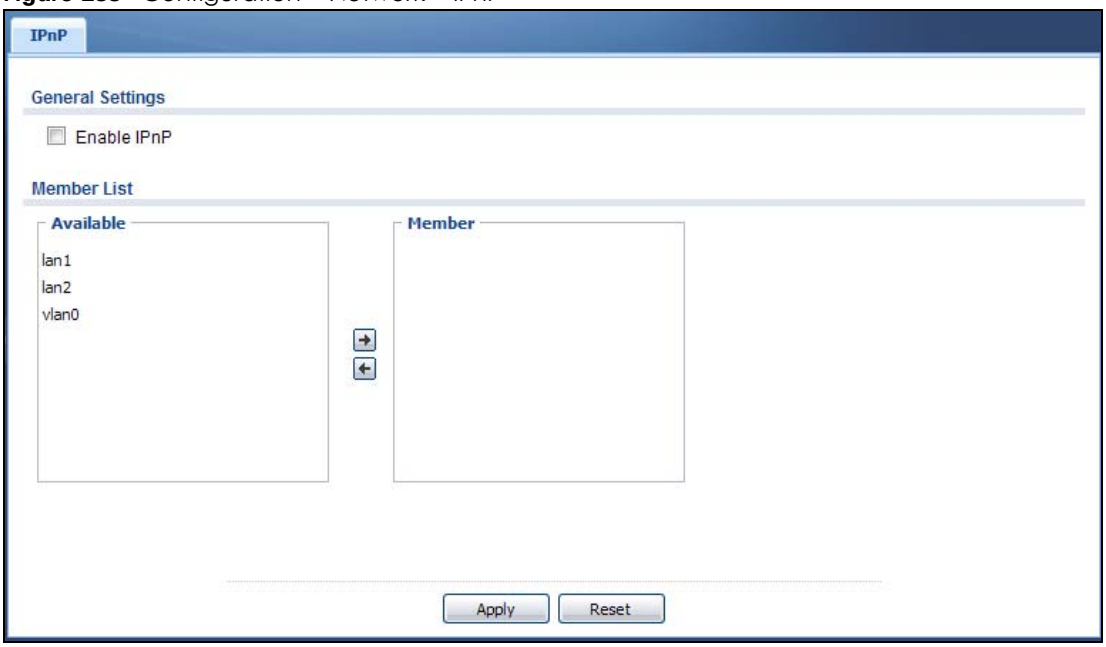

### 22.1.1 What You Can Do in this Chapter

Use the **IP** screen (Section 22.2 on page 273) 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 183** Configuration > Network > IPnP




The following table describes the labels in this screen.

Table 120 Configuration > Network > IPnP

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Enable IPnP | Select this option to turn on the IPnP feature on the UAG.<br><br>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.<br><br>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. |

# CHAPTER 23
# 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 184** 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 275) 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 291) 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 297) 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 279 for an example of using an authentication policy for user-aware access control.

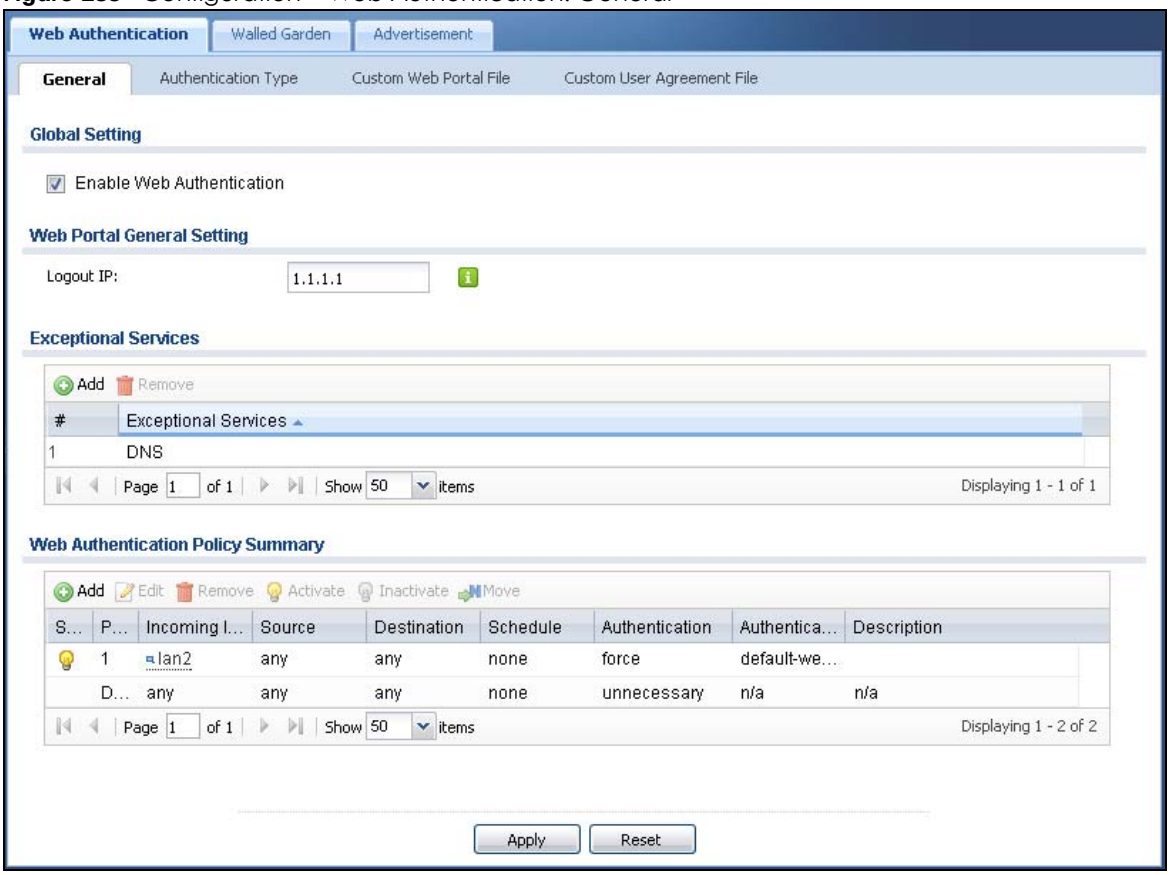
## 23.2 Web Authentication

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 185** Configuration > Web Authentication: General




The following table gives an overview of the objects you can configure.

Table 121 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.<br>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 121 Configuration > Web Authentication: General (continued)

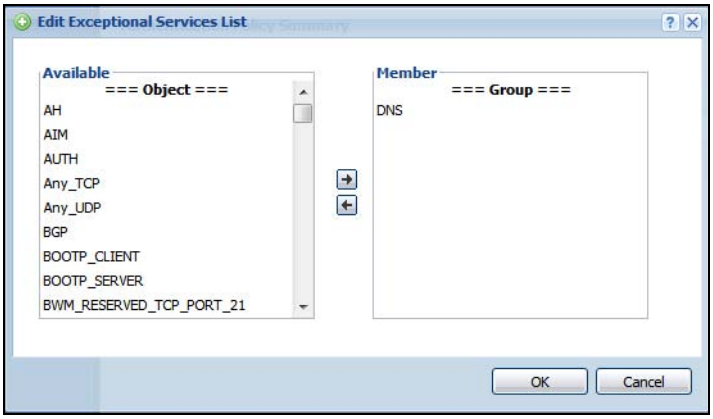
| LABEL | DESCRIPTION |
|---|---|
| Exceptional Services | Use this table to list services that users can access without logging in.<br><br>Click **Add** to change the list's membership. A screen appears. Available services appear on the left. Select any services you want users to be able to access without 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.<br><br>Keeping DNS as a member allows users' computers to resolve domain names into IP addresses.<br><br>**Figure 186** Configuration > Web Authentication > Add Exceptional Service<br><br>  <br><br>In the table, select one or more entries and click **Remove** to delete it or them. |
| 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. |

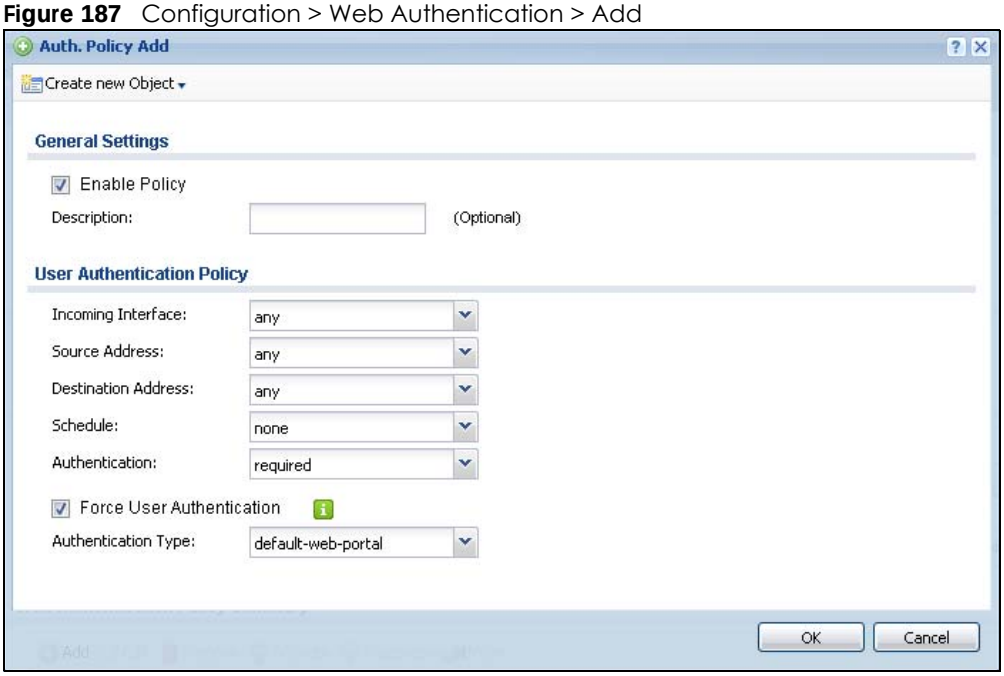
Table 121 Configuration > Web Authentication: General (continued)

| LABEL | DESCRIPTION |
|---|---|
| Authentication | This field displays the authentication requirement for users when their traffic matches this policy.<br>**unnecessary** - Users do not need to be authenticated.<br>**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.<br>**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 187** Configuration > Web Authentication > Add




The following table gives an overview of the objects you can configure.

Table 122 Configuration > Web Authentication > Add

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| 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. |

Table 122 Configuration > Web Authentication > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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.<br>**unnecessary** - Users do not need to be authenticated.<br>**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 46 on page 543 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.<br>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.

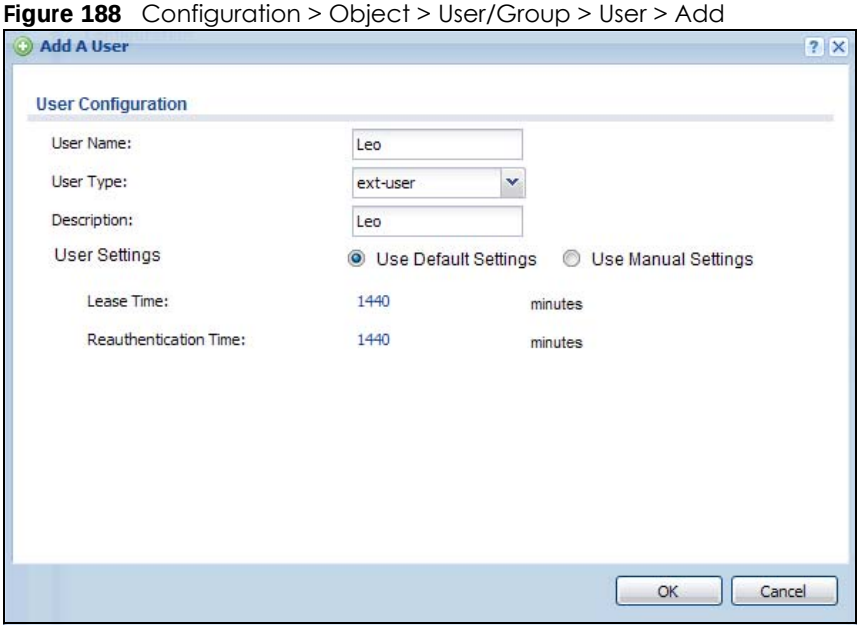
### 23.2.2.1 Set Up User Accounts

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 188** Configuration > Object > User/Group > User > Add




3 Repeat this process to set up the remaining user accounts.

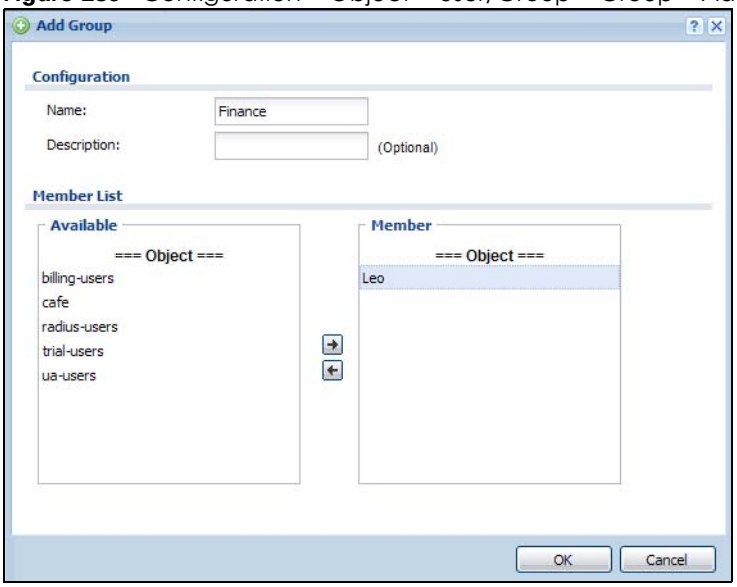
### 23.2.2.2 Set Up User Groups

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 189** Configuration > Object > User/Group > Group > Add



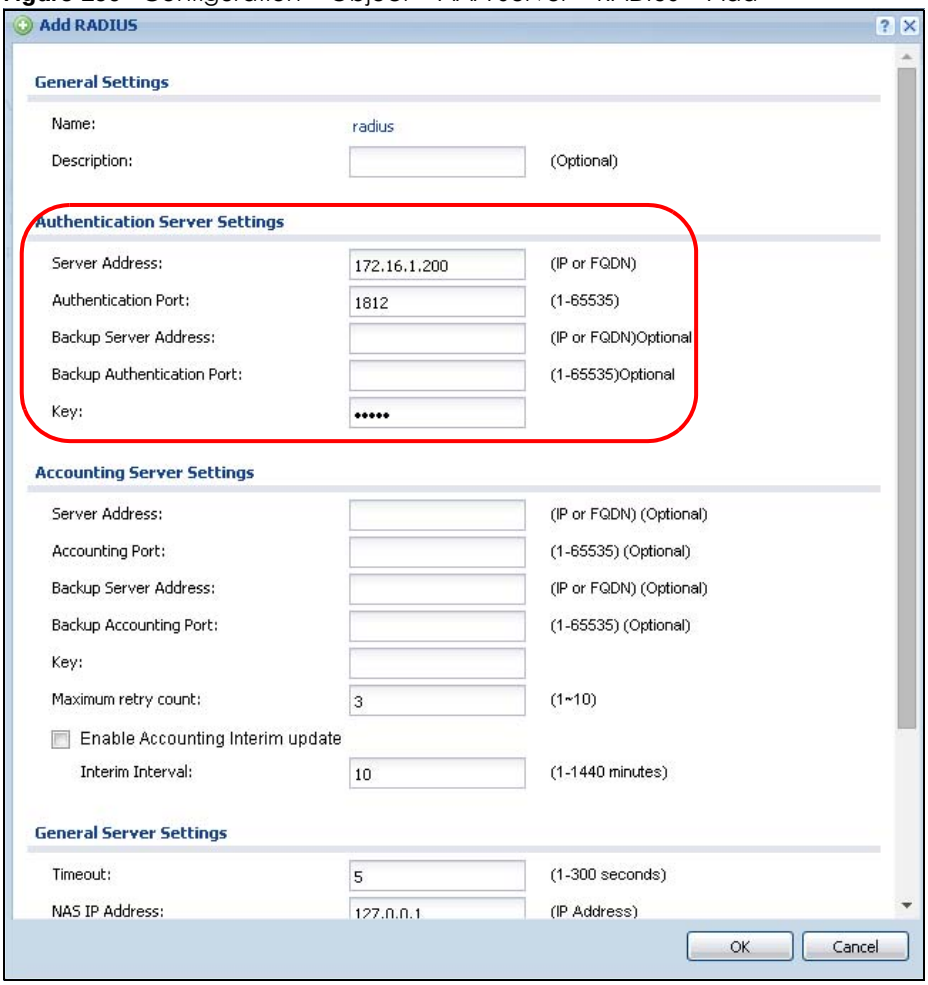
3 Repeat this process to set up the remaining user groups.

### 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.

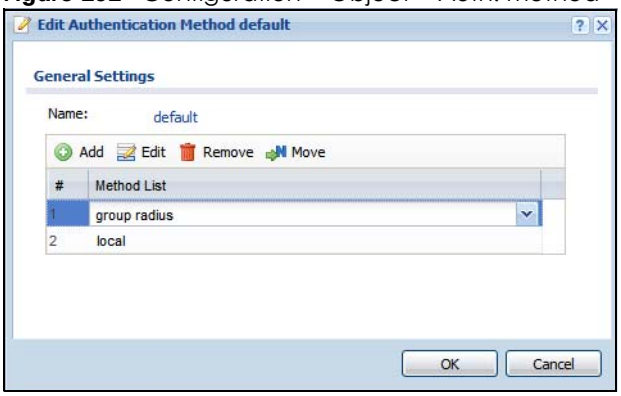
1 Click **Configuration > Object > AAA Server > RADIUS**. Double-click the **radius** entry. Configure the RADIUS server's address, authentication port (1812 if you were not told otherwise), and key. Click **OK**.

**Figure 190** Configuration > Object > AAA Server > RADIUS > Add



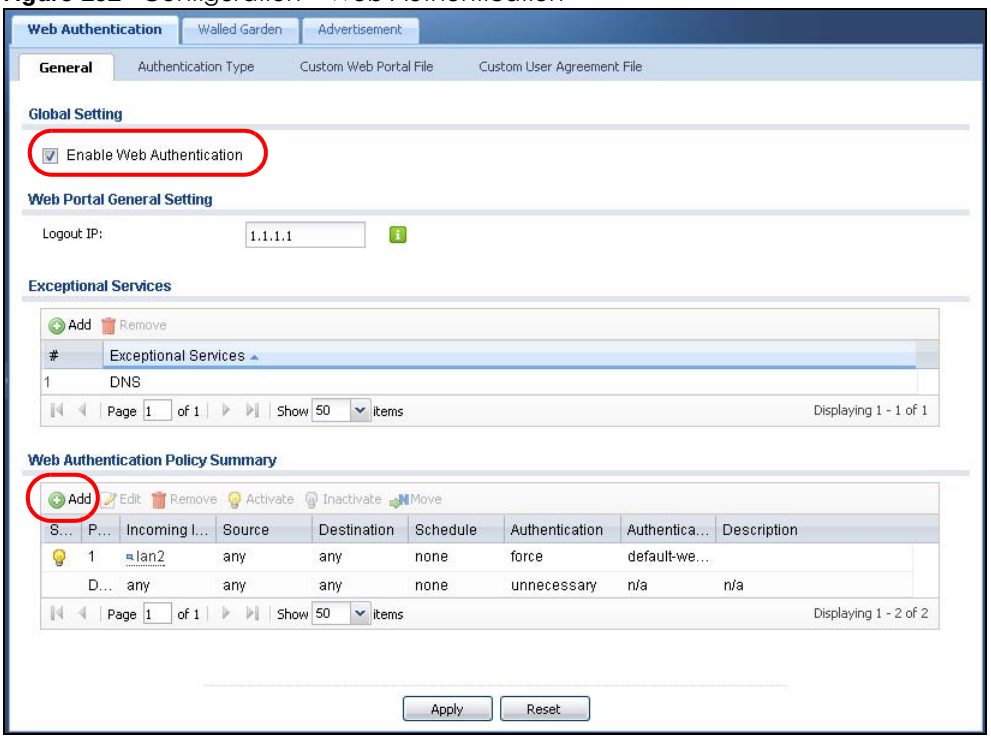

2 Click **Configuration > Object > Auth. Method**. Double-click the **default** entry. Click the **Add** icon. Select **group radius** because the UAG should use the specified RADIUS server for authentication. Click **OK**.

**Figure 191** Configuration > Object > Auth. method > Edit




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 192** Configuration > Web Authentication

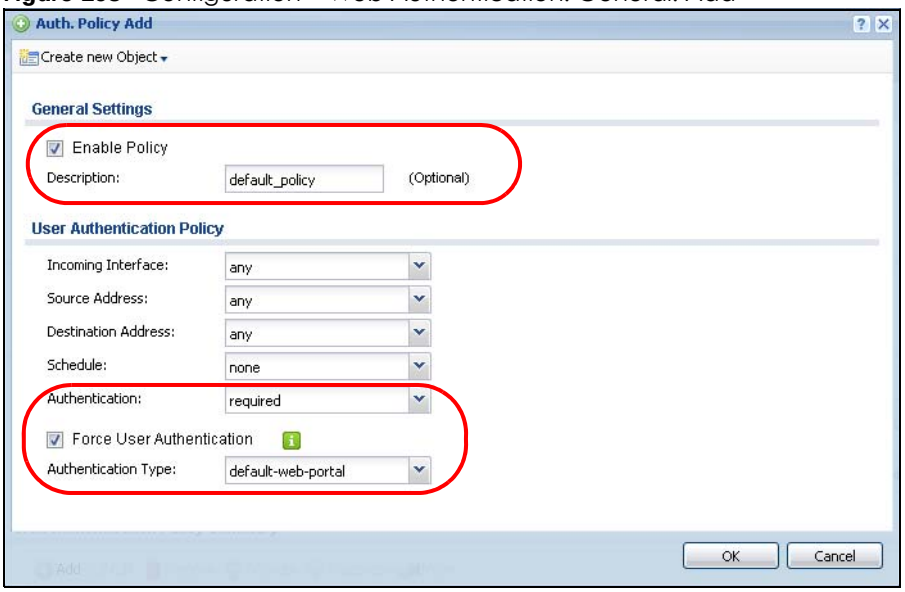



4 In the **Web Authentication Policy Summary** section, click the **Add** icon to set up a default policy that has priority over other policies and forces every user to log into the UAG before the UAG routes traffic for them.

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 193** Configuration > Web Authentication: General: Add



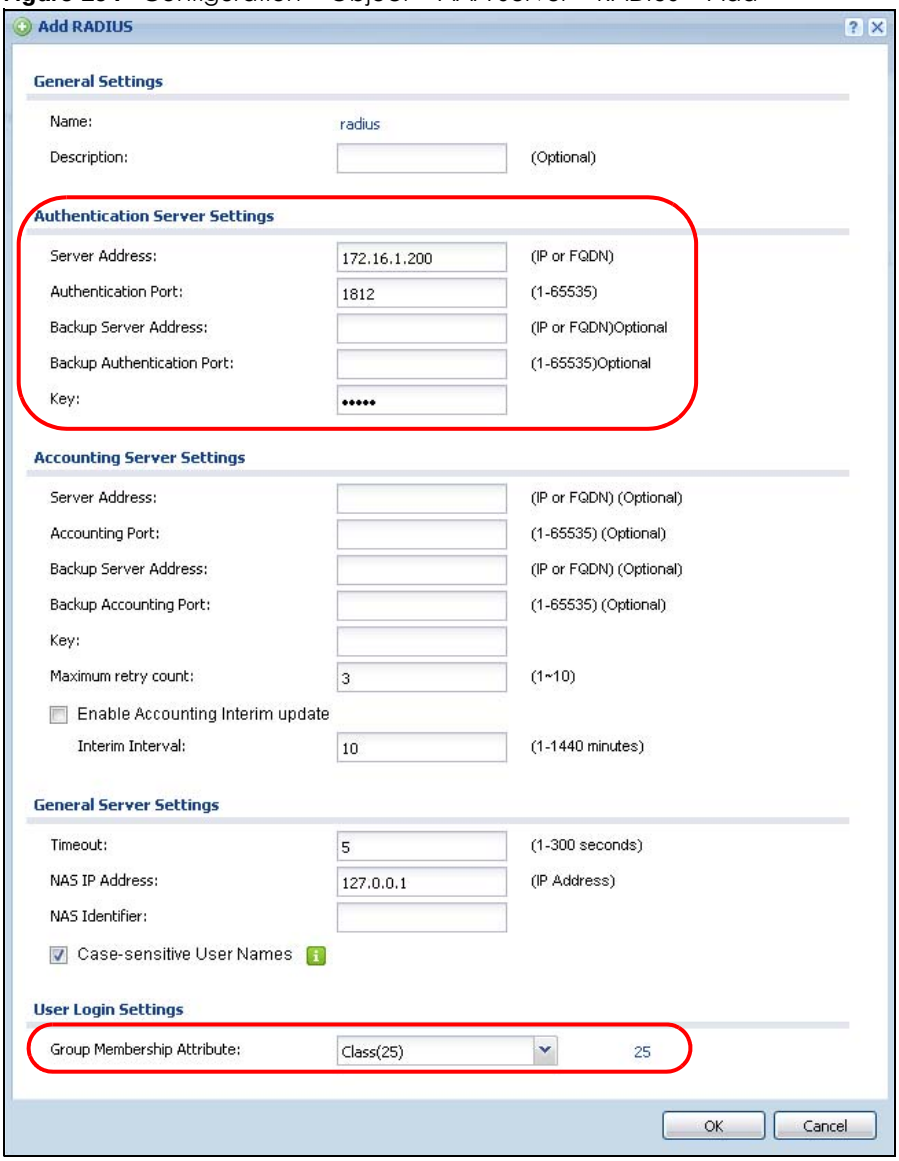

When the users try to browse the web (or use any HTTP application), the login screen appears. They have to log in using the user name and password in the RADIUS server.

### 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.

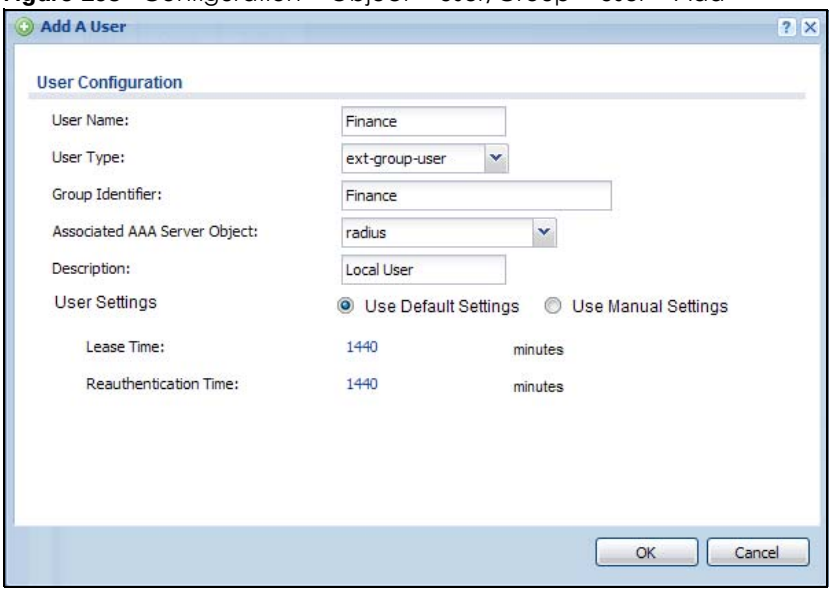
**Figure 194** Configuration > Object > AAA Server > RADIUS > Add




2 Now you add ext-group-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 195** Configuration > Object > User/Group > User > Add

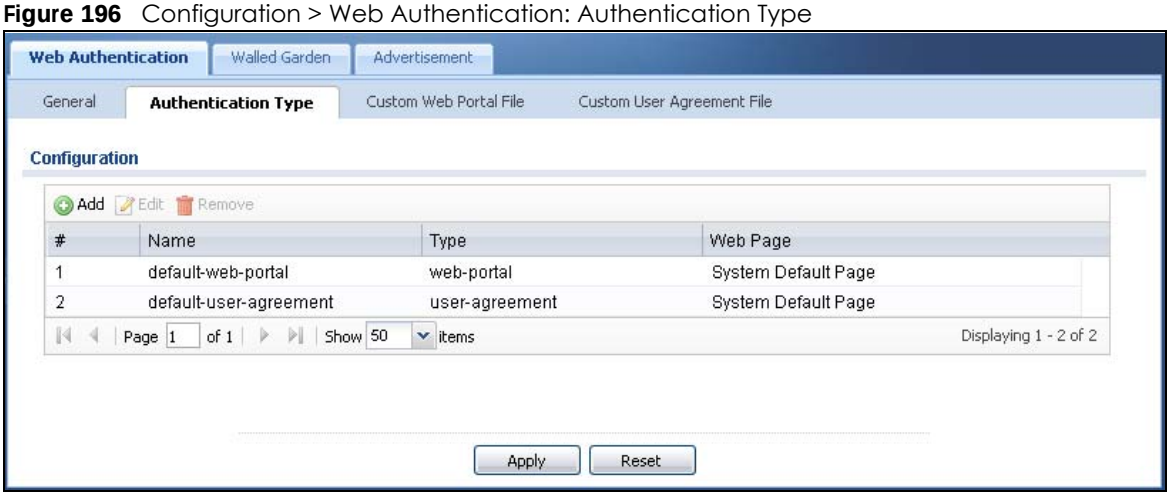



3 Repeat this process to set up the remaining groups of user accounts.

## 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 196** Configuration > Web Authentication: Authentication Type




The following table describes the labels in this screen.

Table 123 Configuration > Web Authentication: Authentication Type

| LABEL | DESCRIPTION |
|---|---|
| Configuration | |
| Add | Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry. |

Table 123 Configuration > Web Authentication: Authentication Type (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. |
| # | This field is a sequential value, and it is not associated with a specific entry. |
| Name | This field displays the name of the profile.<br>default-web-portal: the default login page built into the UAG.<br>Note: You can also customize the default login page built into the UAG in the **System > WWW > Login Page** screen.<br>default-web-portal: the default user agreement page built into the UAG. |
| 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 197** Configuration > Web Authentication: Authentication Type: Add/Edit (Web Portal)

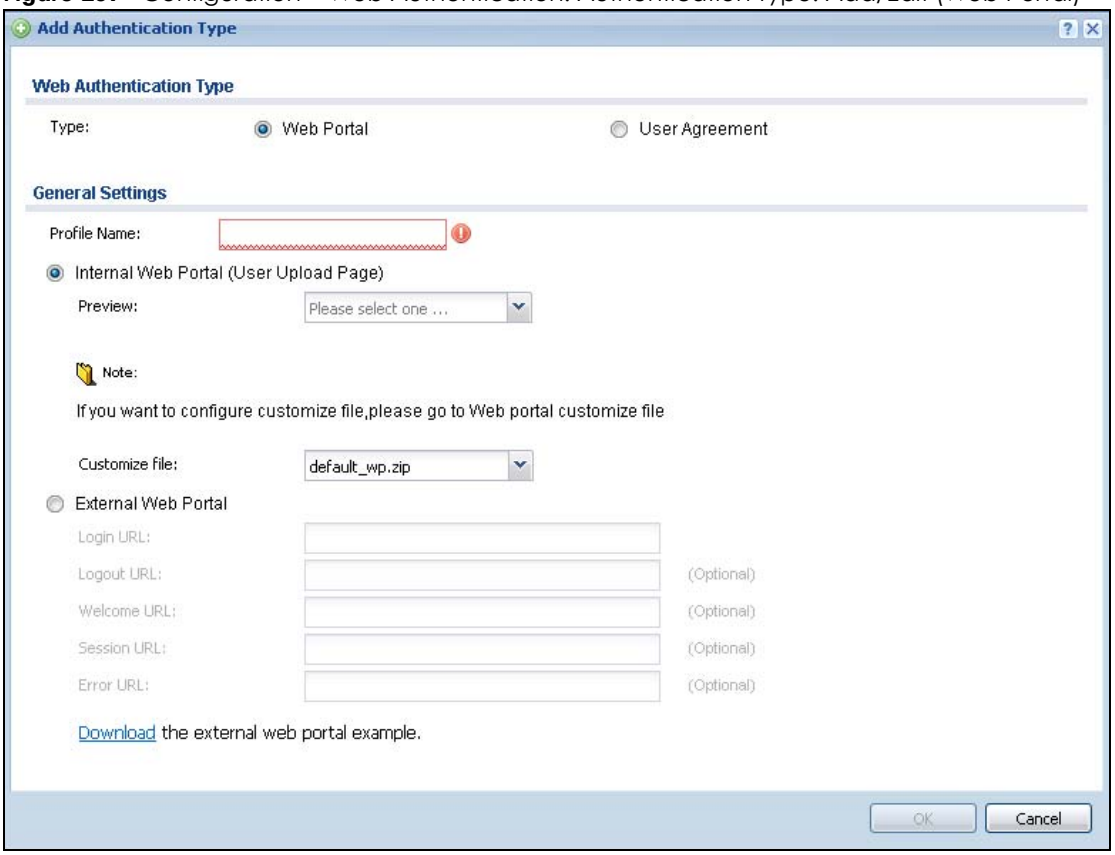
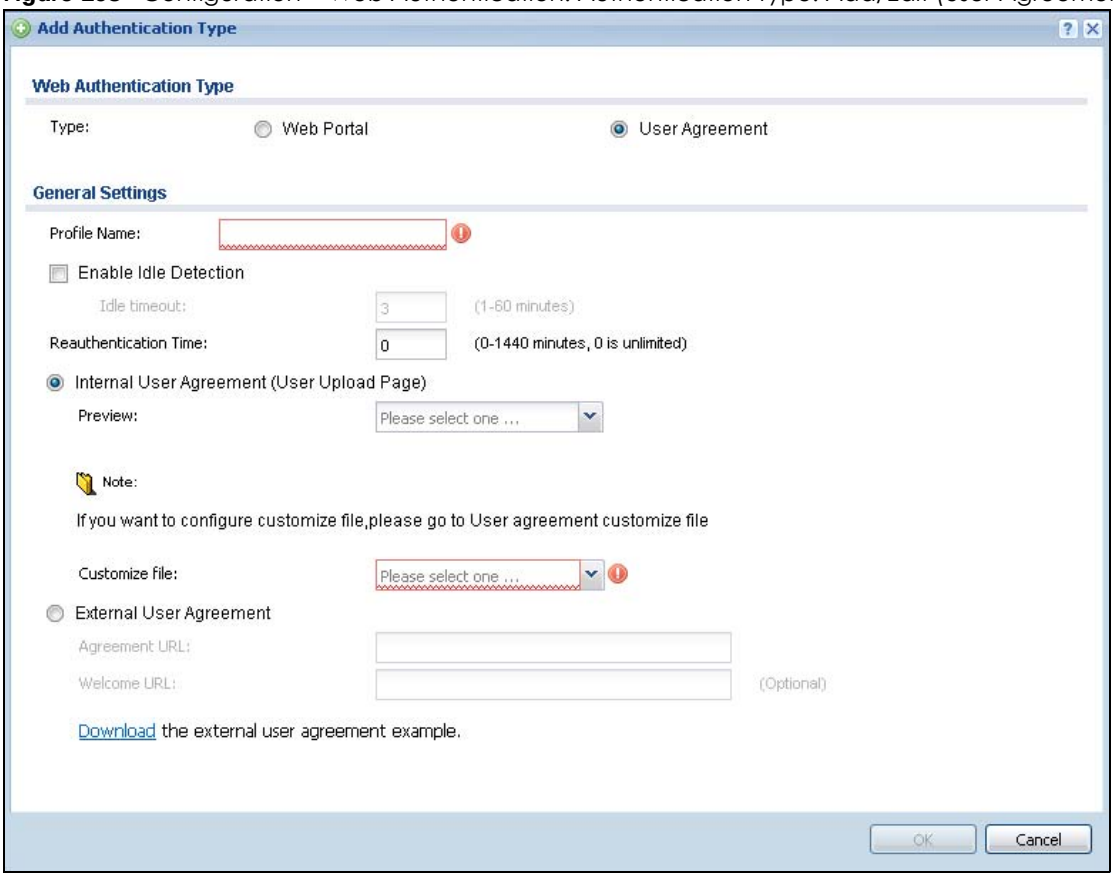


**Figure 198** Configuration > Web Authentication: Authentication Type: Add/Edit (User Agreement)




The following table describes the labels in this screen.

Table 124 Configuration > Web Authentication: Authentication Type: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Web Authentication Type | |
| Type | Select the type of the web authentication page through which users authenticate their connections.<br><br>If you select **User Agreement**, by agreeing to the policy of user agreement, users can access the Internet without a guest account. |
| General Settings | |
| Profile Name | Enter a name for the profile.<br><br>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.<br><br>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.<br><br>Note: You must select a custom file uploaded to the UAG before you can preview the pages. |

Table 124 Configuration > Web Authentication: Authentication Type: Add/Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Customize file | Select the file name of the web portal file in the UAG.<br><br>Note: You can upload zipped custom web portal files to the UAG using the **Configuration > Web Authentication > Web Portal Customize File** screen. |
| 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.<br><br>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.<br><br>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.<br><br>Users will be redirected to the welcome page after authentication. This field is optional.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>The Internet Information Server (IIS) is the web server on which the user agreement files are installed. |

Table 124 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.<br>The Internet Information Server (IIS) is the web server on which the user agreement files are installed.<br>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 199** Configuration > Web Authentication: Custom Web Portal File

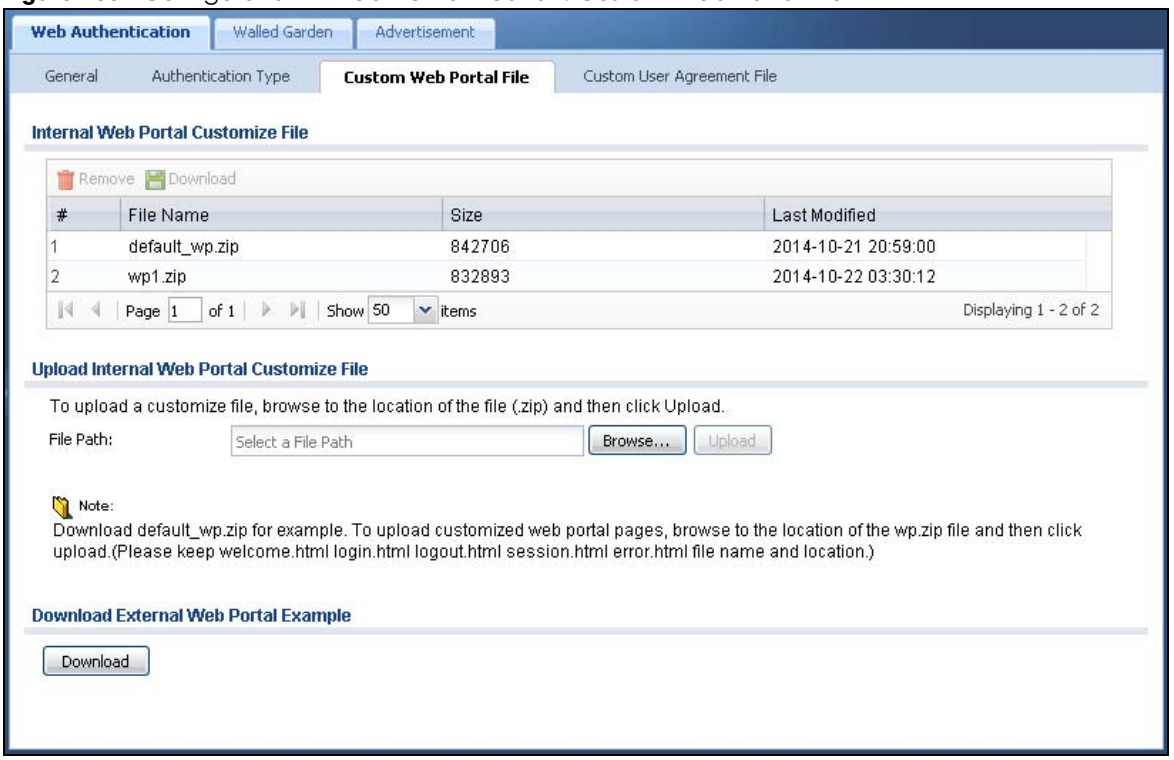
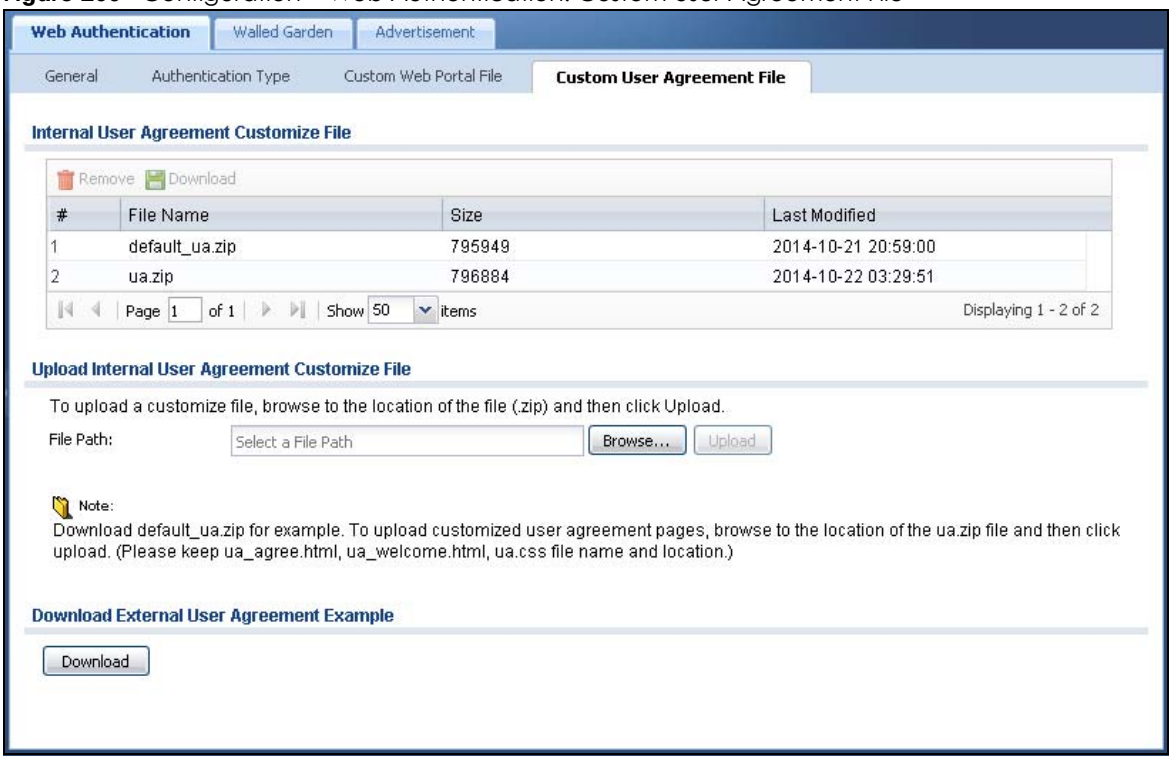


**Figure 200** Configuration > Web Authentication: Custom User Agreement File




The following table describes the labels in this screen.

Table 125 Configuration > Web Authentication: Custom Web Portal / User Agreement File

| LABEL | DESCRIPTION |
|---|---|
| Internal User Agreement Customize File | |
| Remove | Click a file's row to select it and click **Remove** to delete it from the UAG. |
| Download | Click a file's row to select it 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. |
| Upload Internal User Agreement Customize File | |
| 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 External User Agreement Example | |
| 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 201** Configuration > Web Authentication > Walled Garden: General

The following table describes the labels in this screen.

Table 126 Configuration > Web Authentication > Walled Garden: General

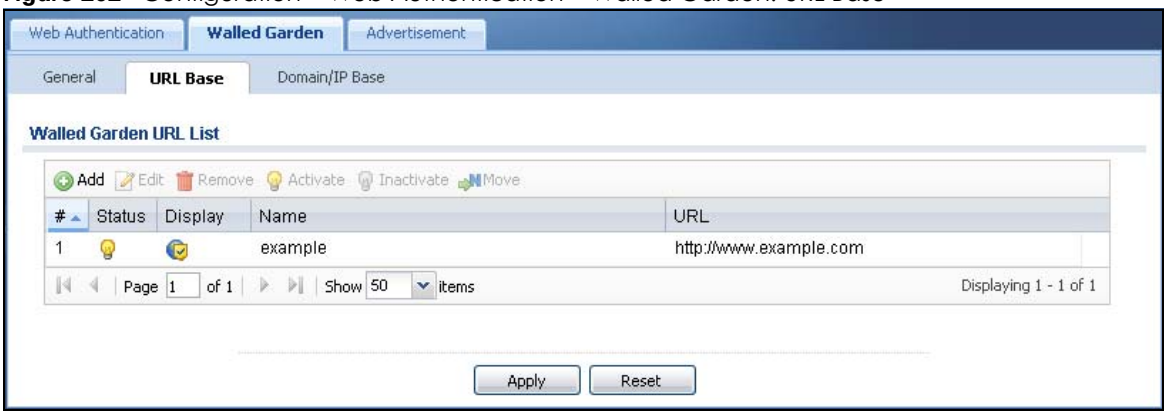
| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Enable Walled Garden | Select this to turn on the walled garden feature.<br><br>Note: This feature works only with the web portal authentication type. |
| Apply | Click this button to save your changes to the UAG. |
| Reset | Click this button 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 202** Configuration > Web Authentication > Walled Garden: URL Base




The following table describes the labels in this screen.

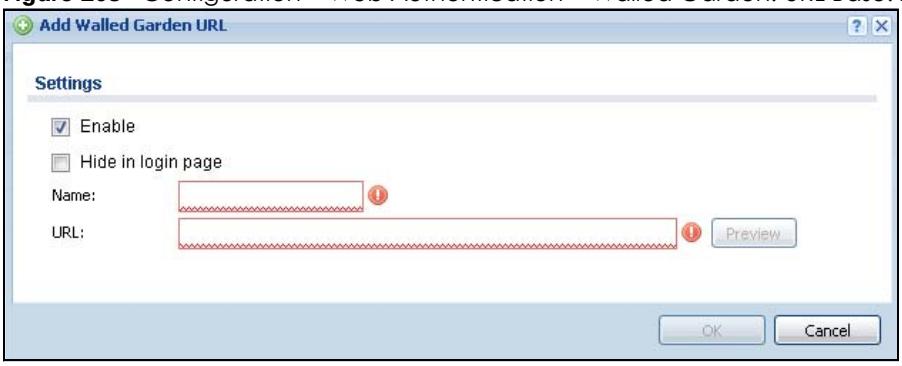
Table 127 Configuration > Web Authentication > Walled Garden: URL Based

| 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 203** Configuration > Web Authentication > Walled Garden: URL Base: Add/Edit




The following table describes the labels in this screen.

Table 128 Configuration > Web Authentication > Walled Garden: URL Base: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Settings | |
| Enable Walled Garden | Select this to turn on the walled garden feature.<br>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. |
| 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.<br>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.<br>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.<br>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 204** Configuration > Web Authentication > Walled Garden: Domain/IP Base

The following table describes the labels in this screen.

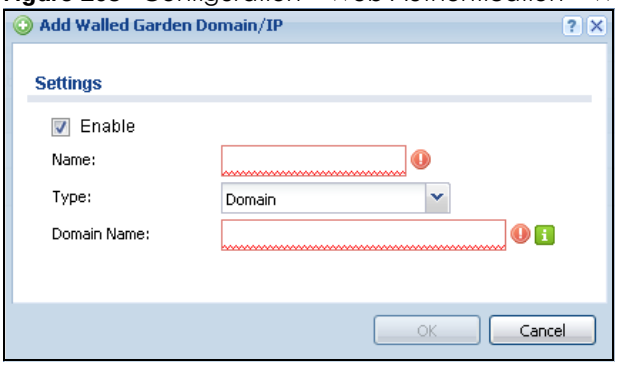
Table 129 Configuration > Web Authentication > Walled Garden: Domain/IP Based

| 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 205** Configuration > Web Authentication > Walled Garden: Domain/IP Base: Add/Edit




The following table describes the labels in this screen.

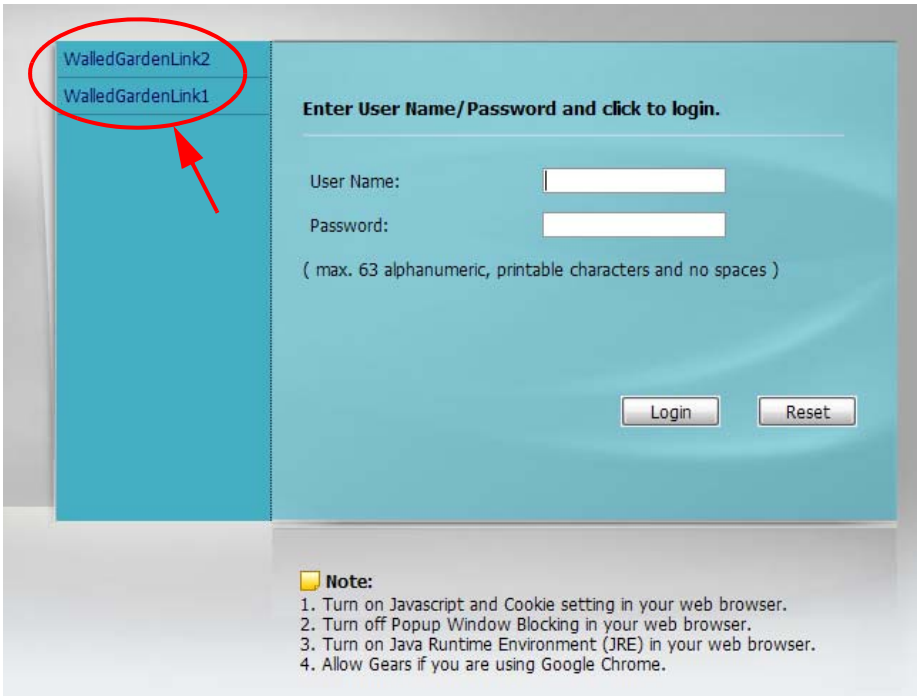
Table 130 Configuration > Web Authentication > Walled Garden: Domain/IP Base: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Settings | |
| Enable | Select this to activate the entry. |
| Name | Enter a descriptive name for the walled garden link.<br><br>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).<br><br>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 206** Walled Garden Login Example

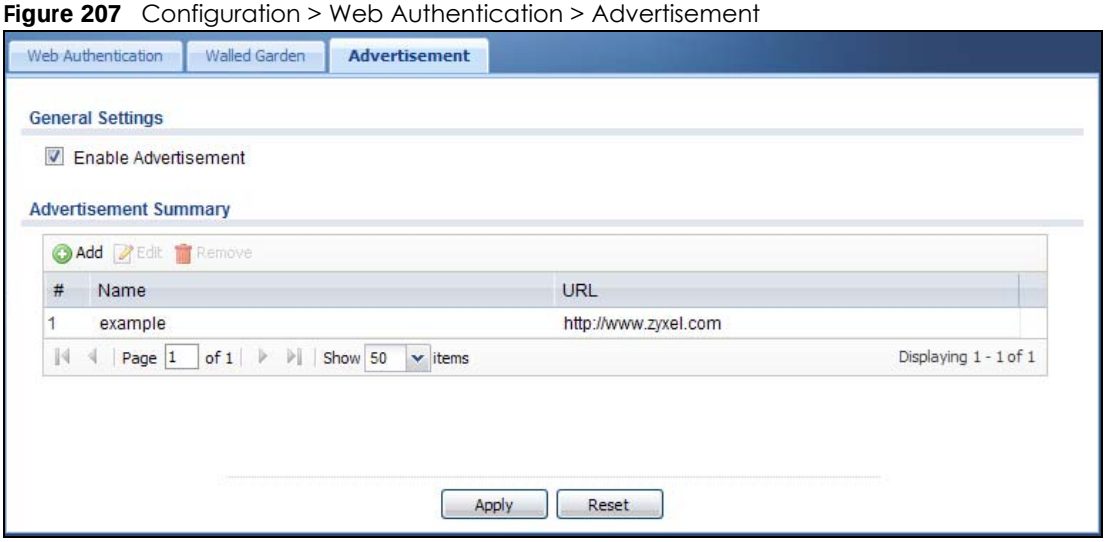



# 23.4 Advertisement Screen

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 207** Configuration > Web Authentication > Advertisement



The following table gives an overview of the objects you can configure.

Table 131 Configuration > Web Authentication > Advertisement

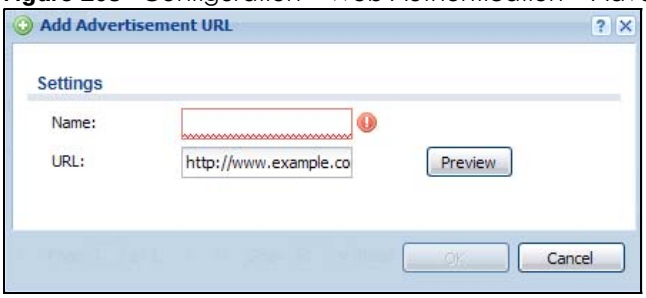
| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Enable Advertisement | Select this to turn on the advertisement feature.<br><br>Note: This feature works only when you enable web authentication. |
| Advertisement Summary | Use this table to manage the list of advertisement web pages. |
| Add | 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 208** Configuration > Web Authentication > Advertisement > Add/Edit



The following table gives an overview of the objects you can configure.

Table 132 Configuration > Web Authentication > Advertisement > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Settings | |
| Name | Enter a descriptive name for the advertisement web site.<br>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.<br>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. |

# CHAPTER 24
# Security Policy

## 24.1 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

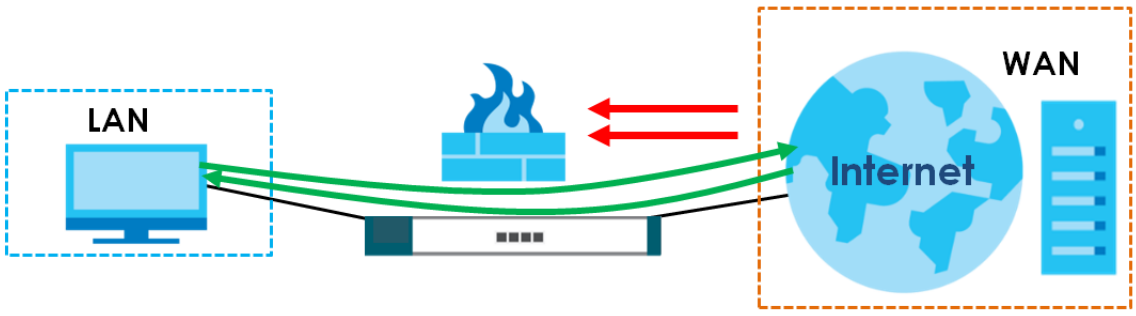
The policy can be configured:

- 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 209** Default Security Policy Action




### 24.1.1 What You Can Do in this Chapter

- Use the Security **Policy Control** screens (Section 24.2 on page 302) to enable or disable policy control and asymmetrical routes, and manage and configure policies.
- Use the **Session Control** screens (see Section 24.3 on page 307) to limit the number of concurrent NAT/ security policies sessions a client can use.

## 24.1.2 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 33.1.2 on page 405 for details.

Table 133 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 301are 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.<br>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 45 on page 495 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 24.4 on page 310 for an example of creating security policies as part of configuring user-aware access control.

## 24.2 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.

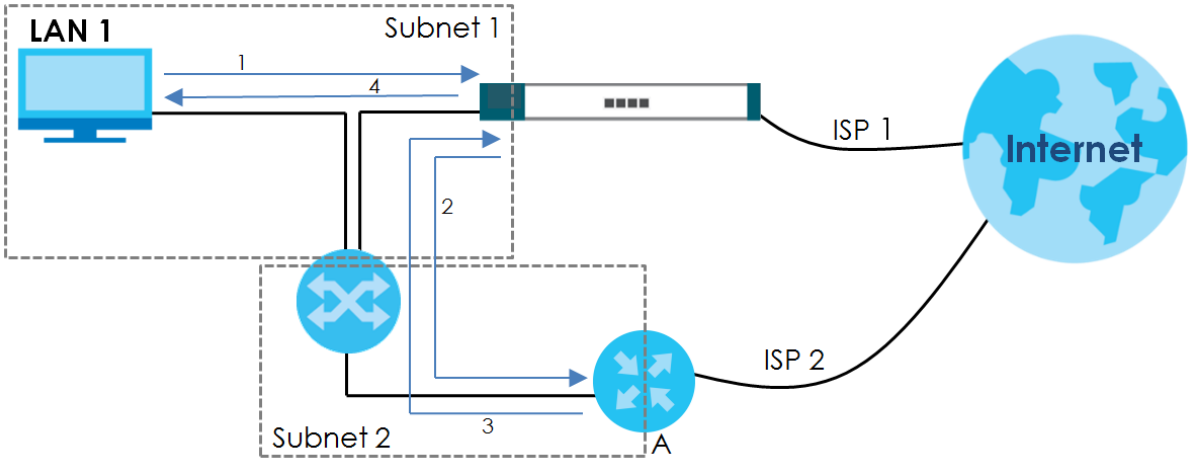
1 A computer on the LAN1 initiates a connection by sending a SYN packet to a receiving server on the WAN.

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 210** Using Virtual Interfaces to Avoid Asymmetrical Routes

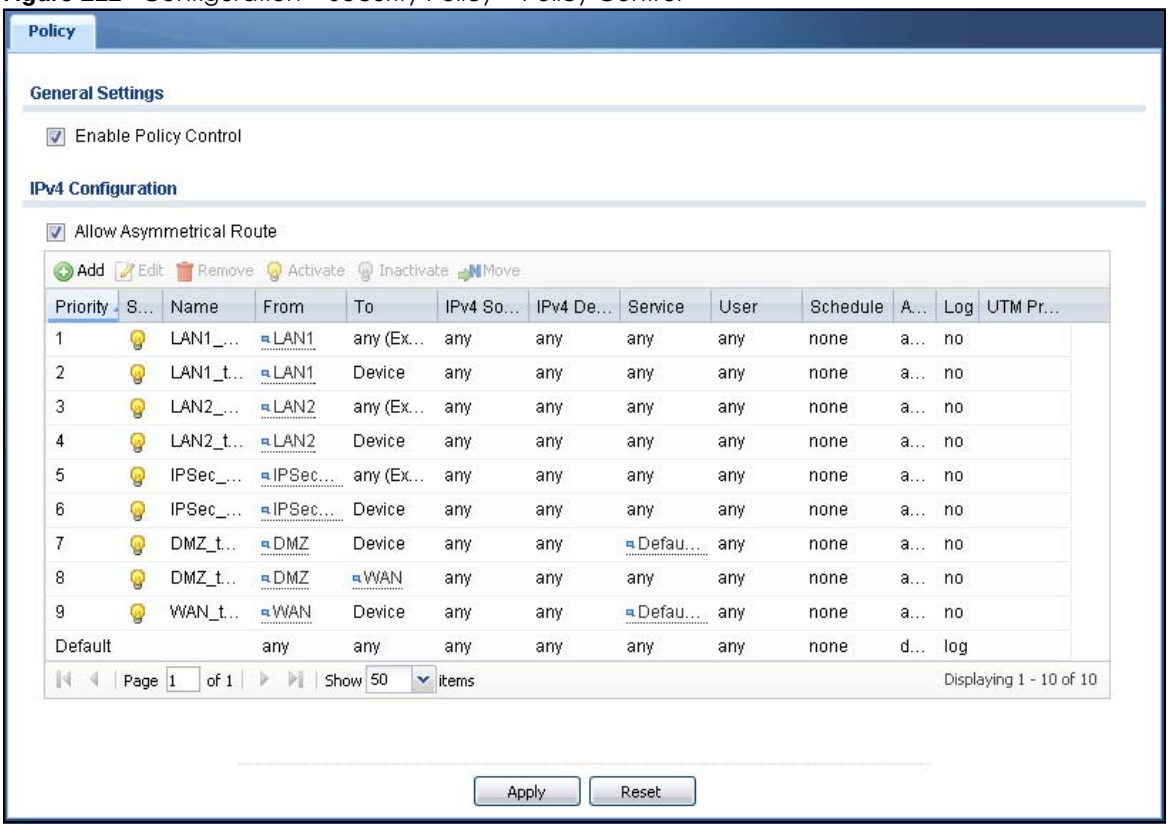



## 24.2.1 Configuring the Security Policy Control Screen

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 234 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 211** Configuration > Security Policy > Policy Control




The following table describes the labels in this screen.

Table 134 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 | 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.<br>Select this check box to have the UAG permit the use of asymmetrical route topology on the network (not reset the connection).<br>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. |
| 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**. |

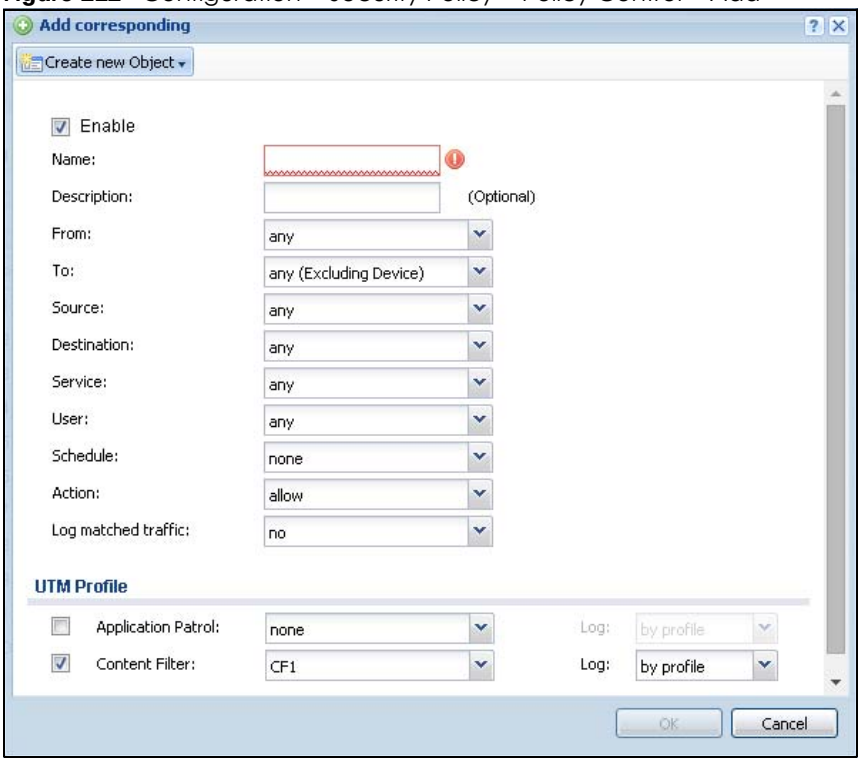
Table 134 Configuration > Security Policy > Policy Control (continued)

| 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.<br>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<br>To | This is the direction of travel of packets to which the security policy applies.<br>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.<br>From **any** displays all the policy control rules for traffic going to the selected **To Zone**.<br>To **any** displays all the policy control rules for traffic coming from the selected **From Zone**.<br>From **any** to **any** displays all of the policy control rules.<br>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. |

## 24.2.2 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 212** Configuration > Security Policy > Policy Control > Add




The following table describes the labels in this screen.

Table 135 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.<br>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<br>To | For through-UAG rules, select the direction of travel of packets to which the policy applies.<br>**any** means all interfaces.<br>**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. |

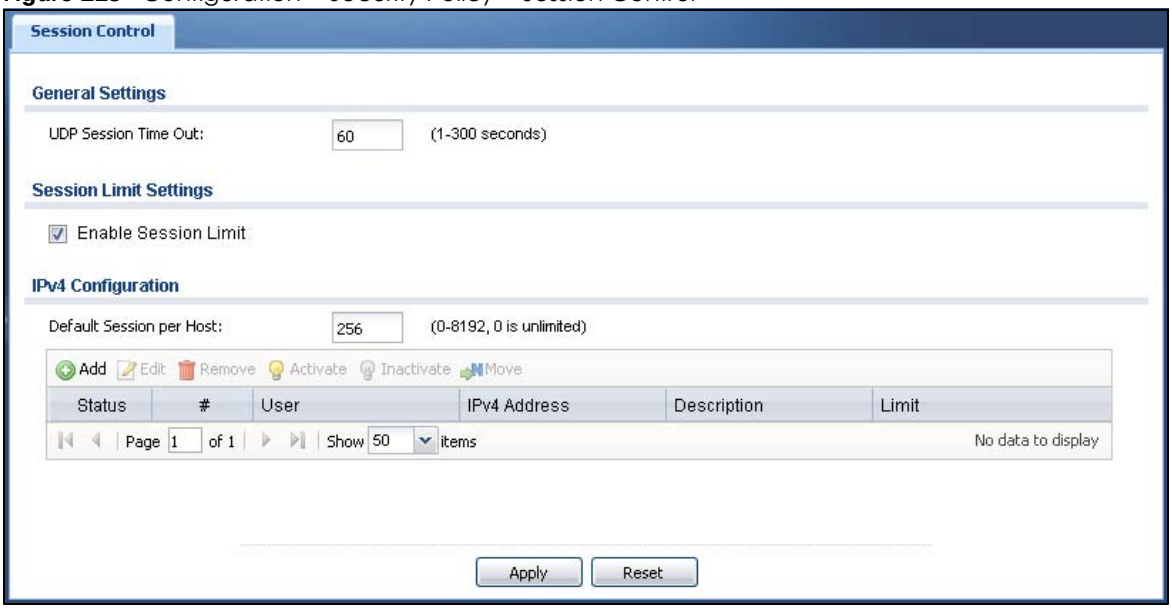
Table 135 Configuration > Security Policy > Policy Control > Add/Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| User | This field is not available when you are configuring a to-UAG policy.<br>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.<br>Otherwise, select **any** and there is no need for user logging.<br>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. |
| Schedule | Select a schedule that defines when the policy applies. Otherwise, select **none** and the policy is always effective. |
| Action | Use the drop-down list box to select what the security policy is to do with packets that match this rule.<br>Select **deny** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.<br>Select **allow** to permit the passage of the packets. |
| 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 46 on page 543 for more on logs. |
| UTM Profile | 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.<br>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. |
| 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. |

# 24.3 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 213** Configuration > Security Policy > Session Control




The following table describes the labels in this screen.

Table 136 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 | This field is configurable only when you enable session limit.<br>Use this field to set a common limit to the number of concurrent NAT/security policy sessions each client computer can have.<br>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.<br>Create rules below to apply other limits for specific users or addresses. |
| 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.<br>The ordering of your rules is important as they are applied in order of their numbering. |

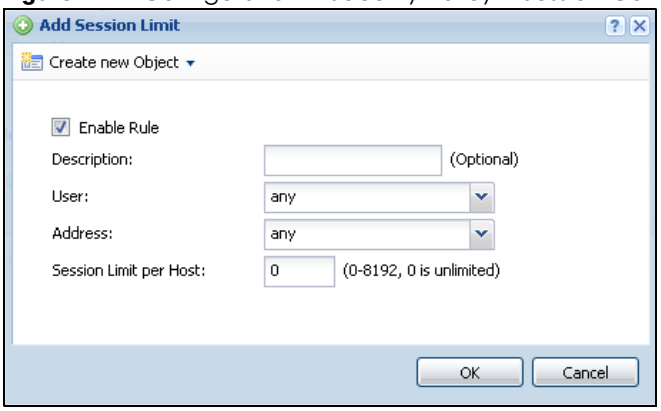
Table 136 Configuration > Security Policy > Session Control (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. |

## 24.3.1 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 214** Configuration > Security Policy > Session Control > Add/Edit




The following table describes the labels in this screen.

Table 137 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. |
| 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.<br>Otherwise, select **any** and there is no need for user logging.<br>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. |

Table 137 Configuration > Security Policy > Session Control > Add/Edit (continued)

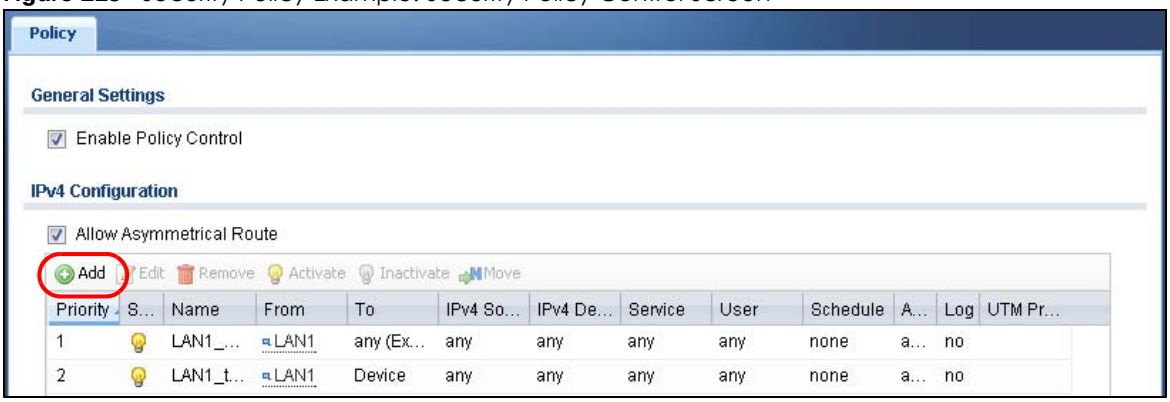
| LABEL | DESCRIPTION |
|---|---|
| Session Limit per Host | Use this field to set a limit to the number of concurrent NAT/security policy sessions this rule's users or addresses can have.<br>For this rule's users and addresses, this setting overrides the **Default Session per Host** setting in the general **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. |

# 24.4 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.

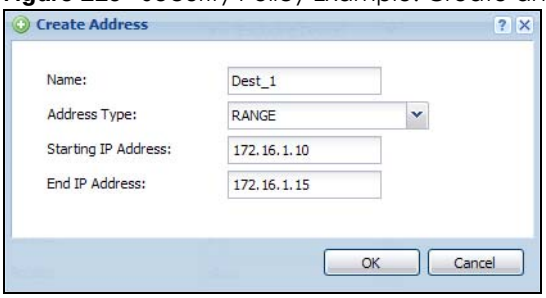
1 Click **Configuration > Security Policy > Policy Control**. In the summary of security policies click **Add** to configure a new first entry. The sequence (priority) of the policies is important since they are applied in order.

**Figure 215** Security Policy Example: Security Policy Control Screen



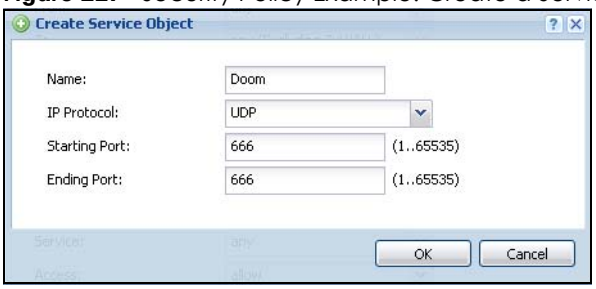

2 At the top of the screen, click **Create new Object > Address** to configure an address object. Configure it as follows and click **OK**.

**Figure 216** Security Policy Example: Create an Address Object




3 Click **Create new Object > Service** to configure a service object for Doom (UDP port 666). Configure it as follows and click **OK**.

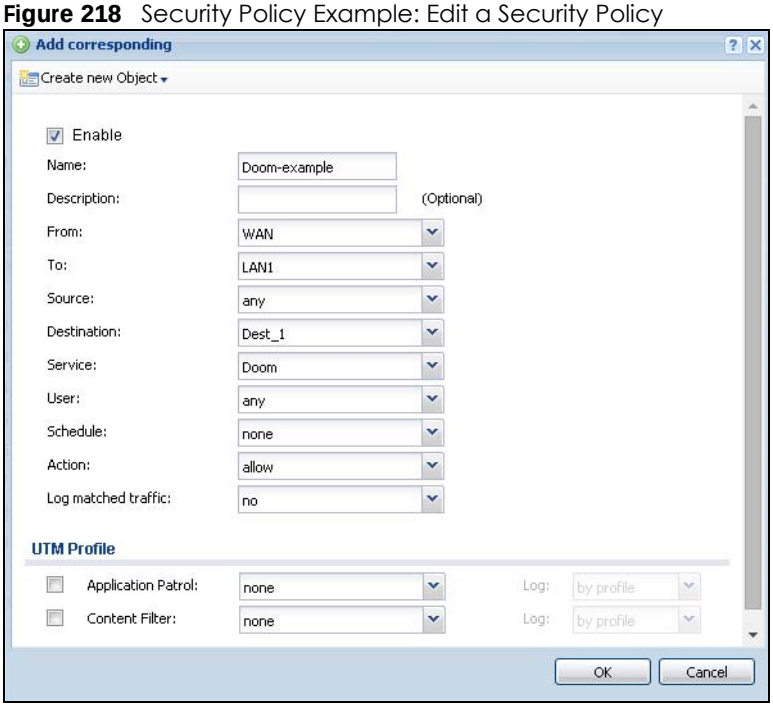
**Figure 217** Security Policy Example: Create a Service Object




4 Select **From WAN** and **To LAN** and enter a name for the security policy.

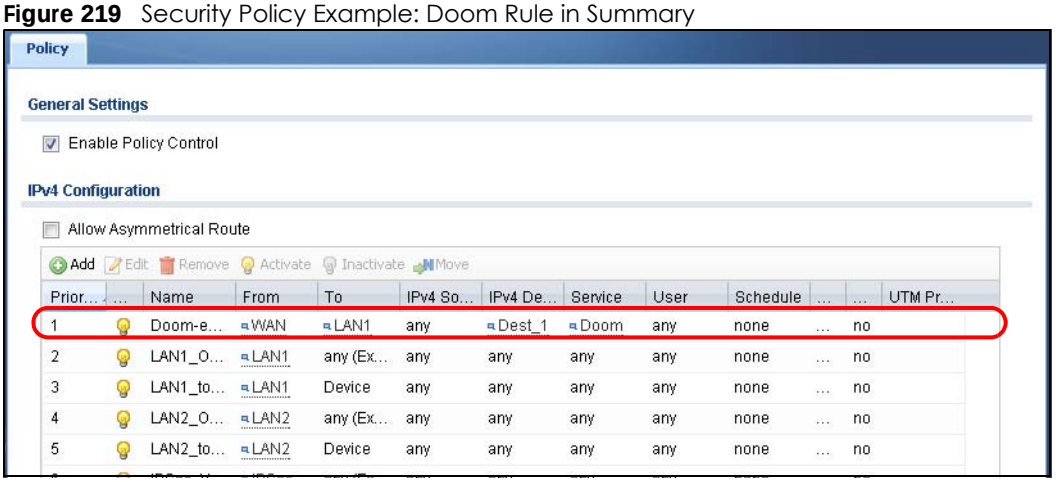
Select **Dest_1** for the **Destination** and **Doom** as the **Service**. Enter a name and configure the rest of the screen as follows. Click **OK** when you are done.

**Figure 218** Security Policy Example: Edit a Security Policy




5 The security policy appears in the Security Policy summary.

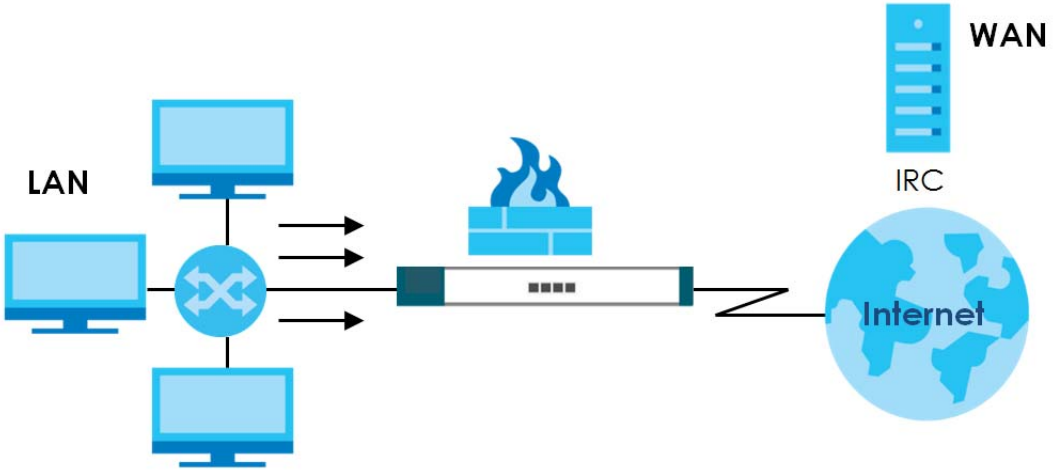
**Figure 219** Security Policy Example: Doom Rule in Summary



# 24.5 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 220** Blocking All LAN to WAN IRC Traffic Example




Your security policy would have the following settings.

Table 138 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,

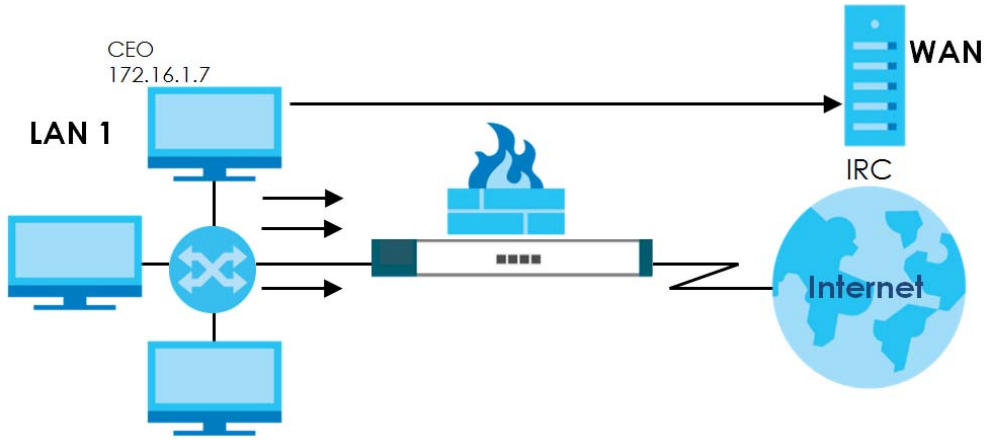
  or

- You configure a static DHCP entry for it so the UAG always assigns it the same IP address (see DHCP Settings on page 207 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 221** Limited LAN to WAN IRC Traffic Example




Your security policy would have the following configuration.

Table 139 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 140 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.

# CHAPTER 25
# Billing

## 25.1 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.

### 25.1.1 What You Can Do in this Chapter

- Use the **General** screen (see Section 25.2 on page 314) 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 25.3 on page 316) 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 25.4 on page 324) to enable and configure discount price plans.
- Use the **Payment Service** screen (see Section 25.5 on page 326) to enable online payment service and configure the service pages.

### 25.1.2 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.

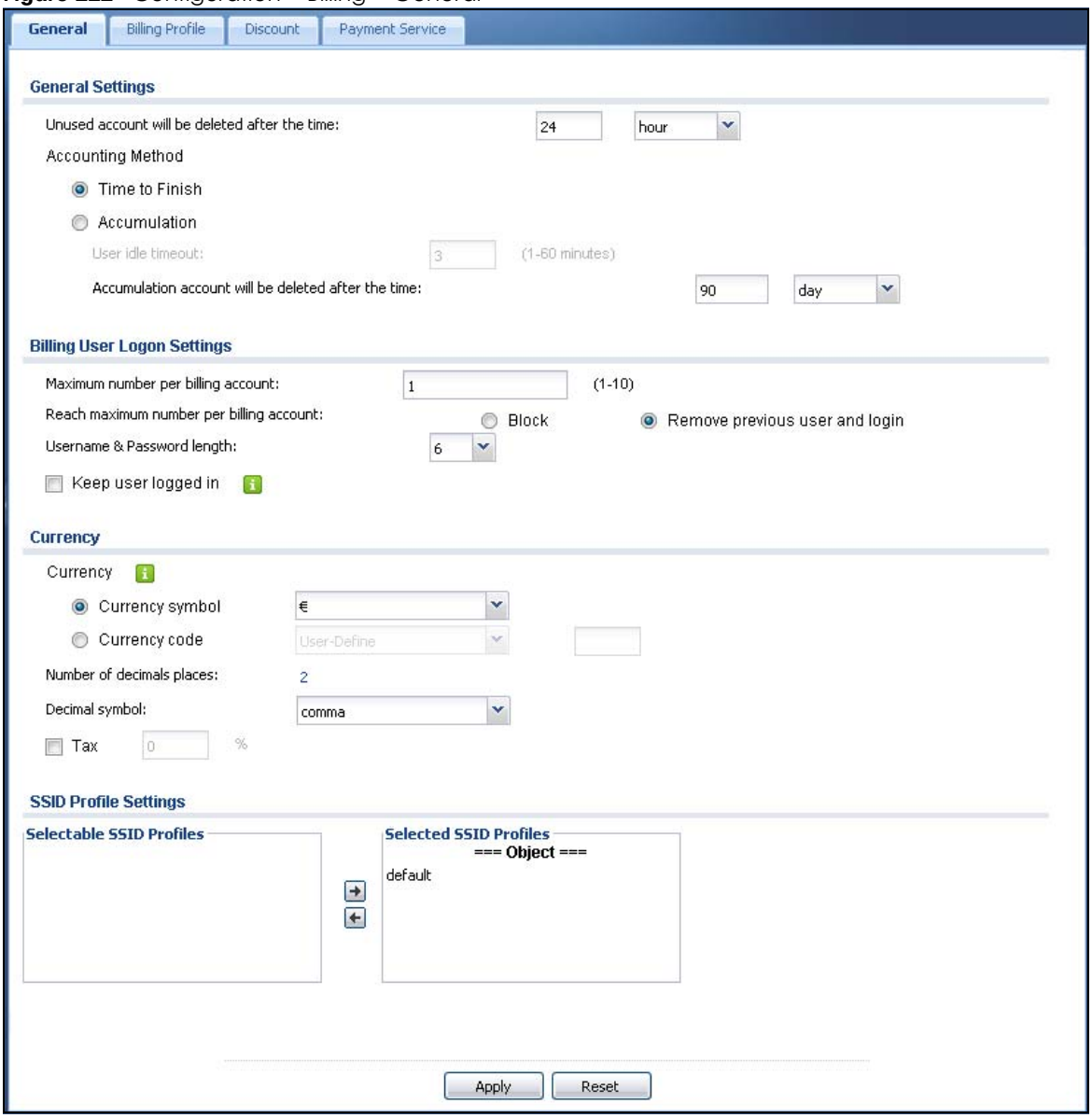
#### Time-to-finish Accounting Method

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.

## 25.2 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 222** Configuration > Billing > General




The following table describes the labels in this screen.

Table 141 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. The maximum unused account can be 365. |
| 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.<br><br>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. |

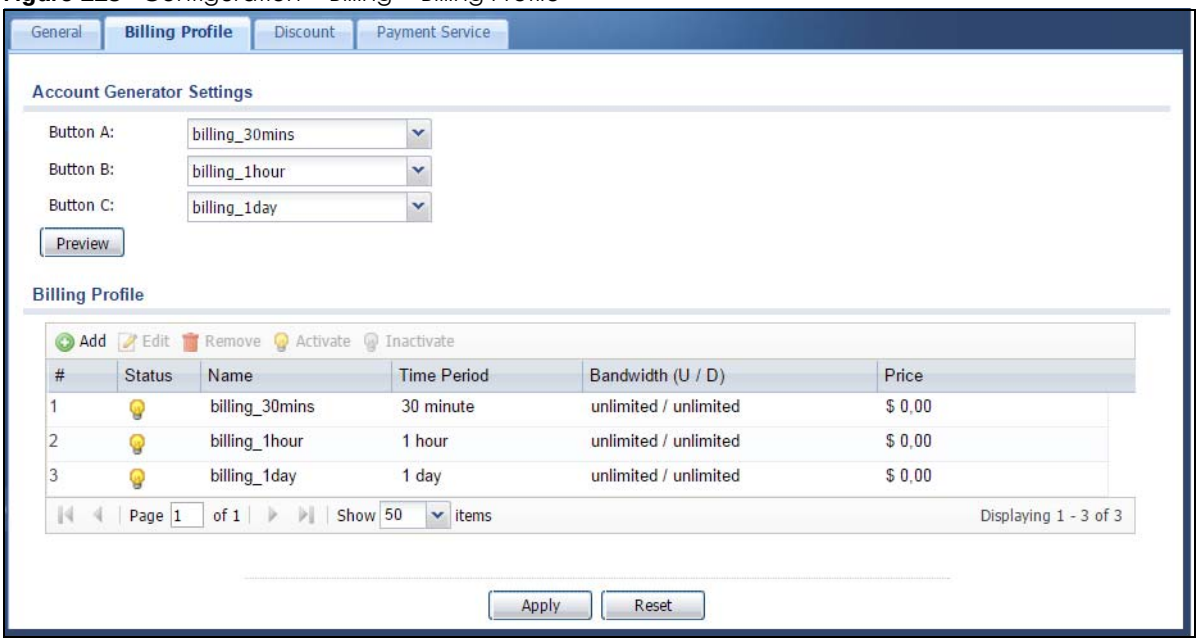
Table 141 Configuration > Billing > General (continued)

| LABEL | DESCRIPTION |
|---|---|
| User idle timeout | 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.<br>If you select **Accumulation**, specify the idle timeout between 1 and 60 minutes. |
| Accumulation 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.<br>This is for use with accumulation accounting. |
| 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 | Select **Block** to stop new users from logging in when the **Maximum number per billing account** is reached.<br>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. |
| 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 | Select to let the users automatically log in without entering their user name and password if the UAG restarts.<br>Note: This works only for free guest accounts or when the accounting method is **Time to Finish**. |
| Currency | Select the appropriate currency symbol or currency unit.<br>If you set **Currency code** to **User-Define**, enter a three-letter alphabetic code manually. |
| 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 | The **Selectable SSID Profiles** list displays the name(s) of the SSID profile(s) to which you can apply the general billing settings.<br>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. |
| Apply | Click this button to save your changes to the UAG. |
| Reset | Click this button to return the screen to its last-saved settings. |

# 25.3 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 223** Configuration > Billing > Billing Profile




The following table describes the labels in this screen.

Table 142 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 25.3.1 on page 318 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. |
| 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. |

Table 142 Configuration > Billing > Billing Profile (continued)

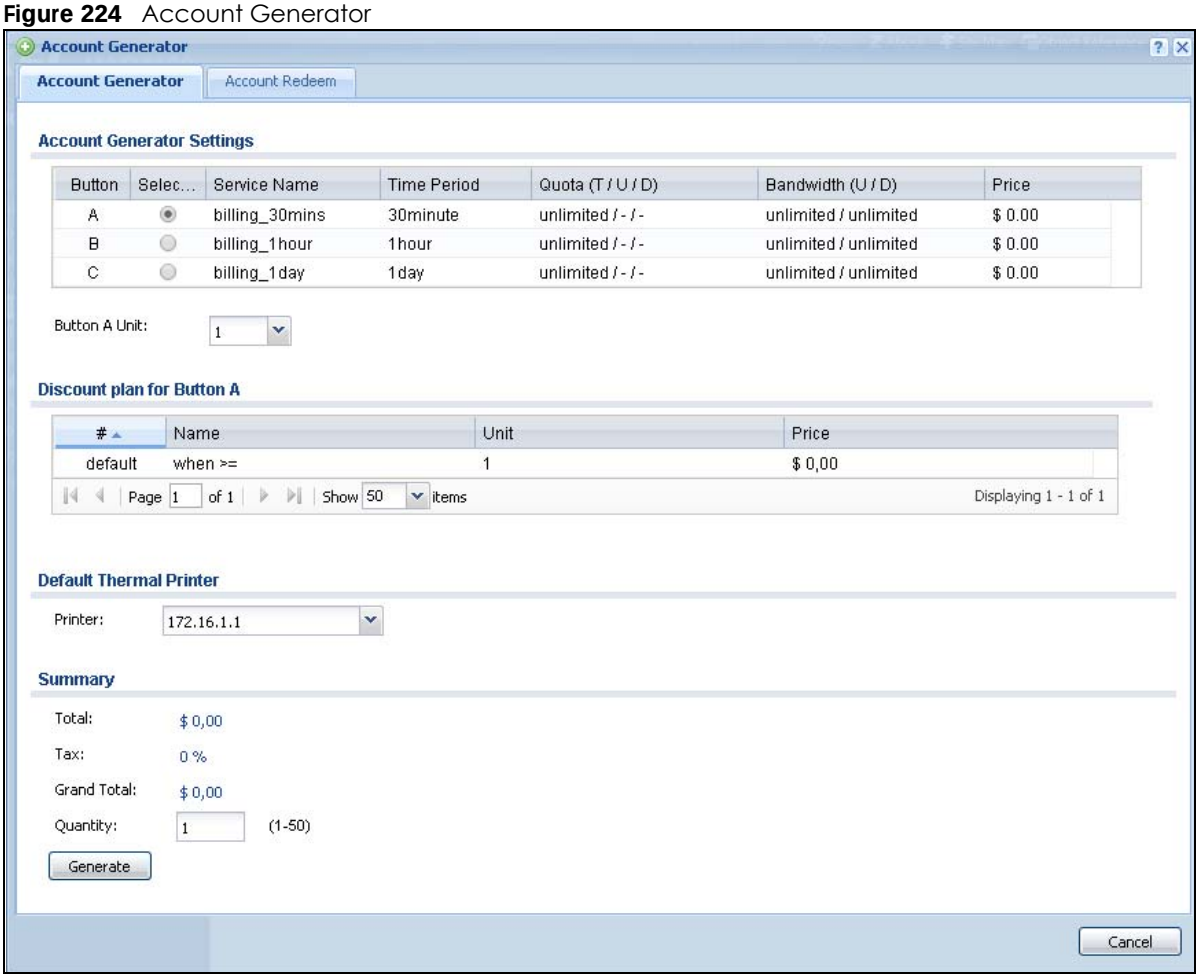
| LABEL | DESCRIPTION |
|---|---|
| Apply | Click this button to save your changes to the UAG. |
| Reset | Click this button to return the screen to its last-saved settings. |

## 25.3.1 The Account Generator Screen

The **Account Generator** screen allows you to automatically create dynamic guest accounts (see Section 7.9 on page 104 and Dynamic-Guest Accounts on page 409 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 224** Account Generator



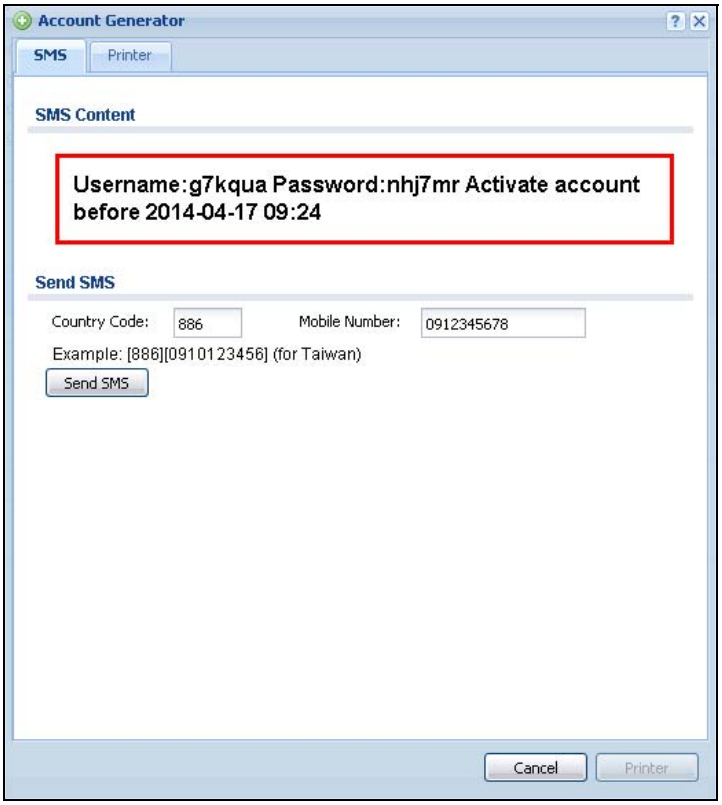
The following table describes the labels in this screen.

Table 143 Account Generator

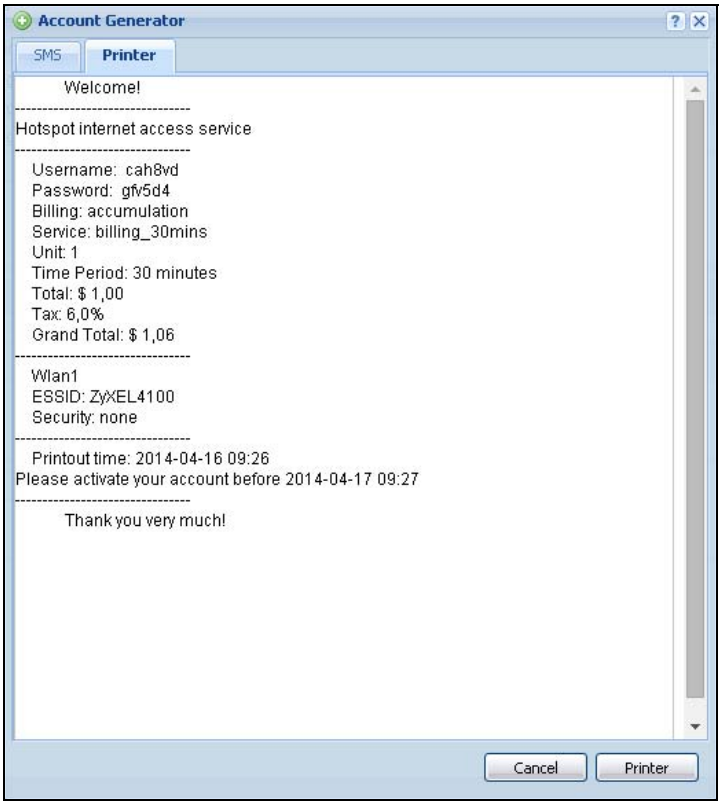
| LABEL | DESCRIPTION |
|---|---|
| Account Generator Settings | Select a button and specify how many units of billing period to be charged for new account in the **Button x Unit** field. |
| Discount plan for Button x | This section displays only when you enable the discount price plan in the **Billing > Discount** screen. |
| # | This is the number of each discount level.<br>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 | |
| 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. |
| 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.



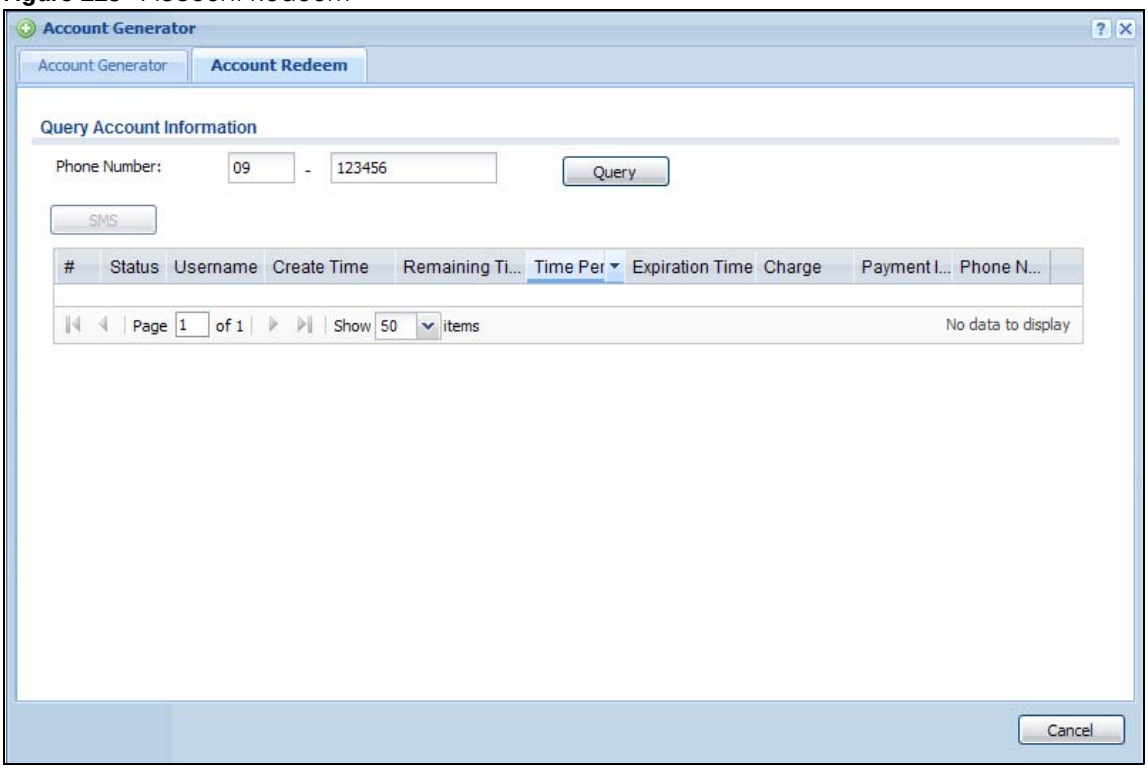
The **Printer** screen shows a printout preview example. Click **Printer** to print this subscriber statement. Click **Cancel** to close this window when you are finished viewing it.




## 25.3.2 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 225** Account Redeem




The following table describes the labels in this screen.

Table 144 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.<br>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.<br>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. |

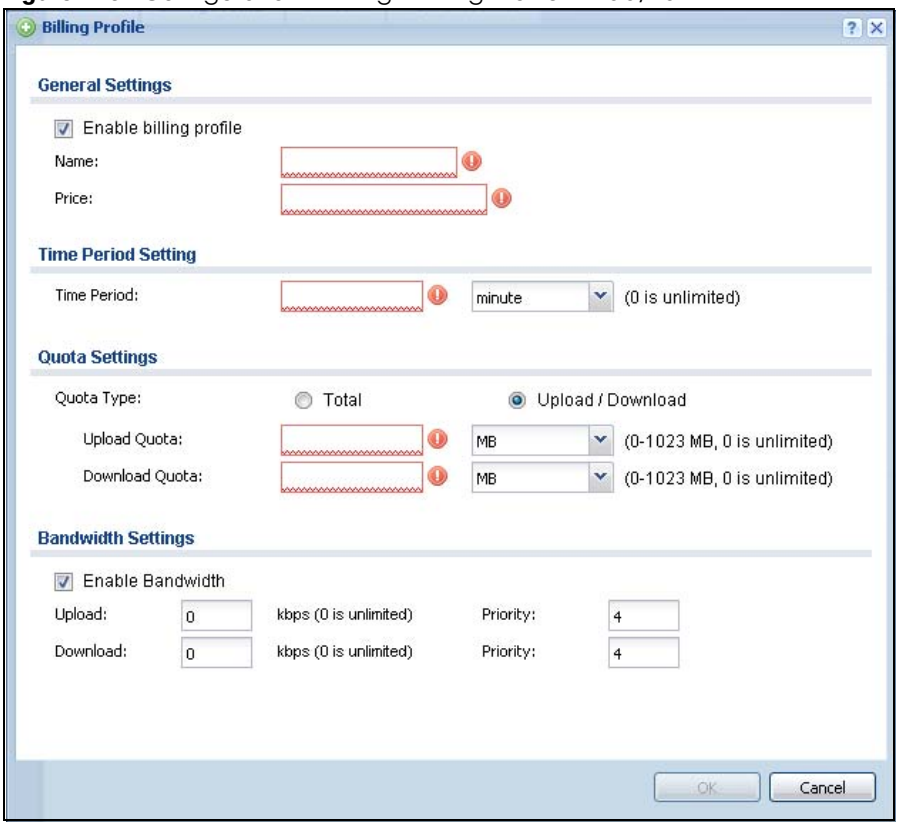
Table 144 Account Redeem (continued)

| 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. |

## 25.3.3 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 226** Configuration > Billing > Billing Profile > Add/Edit




The following table describes the labels in this screen.

Table 145 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.<br>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 145 Configuration > Billing > Billing Profile > Add/Edit (continued)

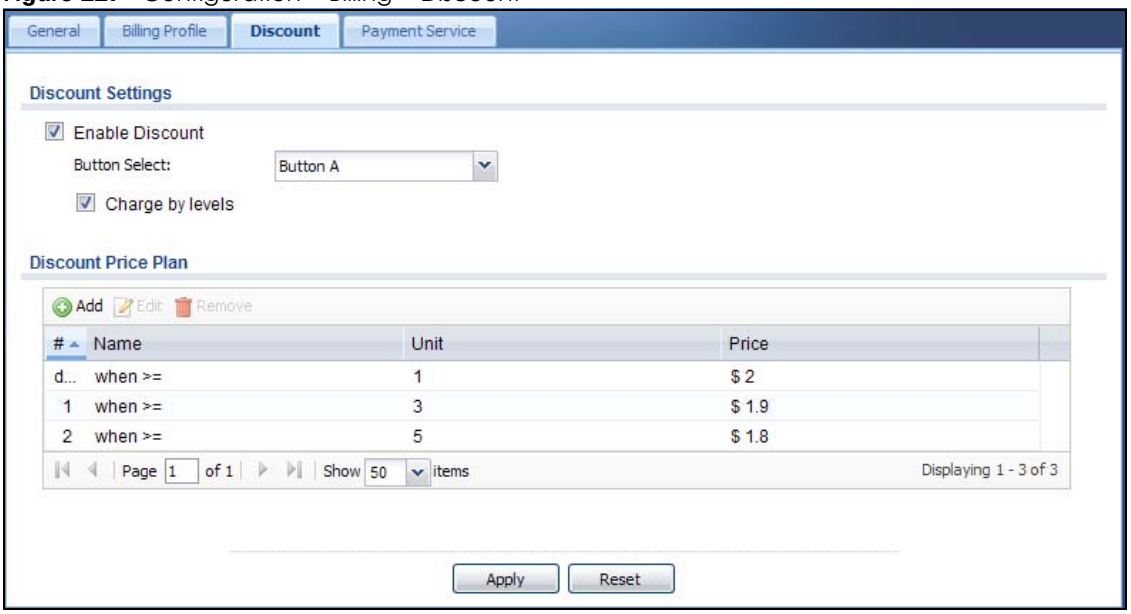
| LABEL | DESCRIPTION |
|---|---|
| Quota Type | The quota settings section is NOT available when you set **Accounting Method** to **Time to Finish** in the **Billing > General** screen.<br>Set a limit for the user accounts. This only applies to user's traffic that is received or transmitted through the WAN interface.<br>Note: When the limit is exceeded, the user is not allowed to access the Internet through the UAG.<br>Select **Total** to set a limit on the total traffic in both directions.<br>Select **Upload/Download** to set a limit on the upstream traffic and downstream traffic respectively. |
| Total Quota | 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. |
| Upload Quota | 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.<br>**0** means there is no data limit for the user account. |
| Download Quota | 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.<br>**0** means there is no data limit for the user account. |
| Enable Bandwidth | Select this option to turn on bandwidth management for the user accounts. |
| Upload | 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. |
| Download | 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. |
| Priority | Enter a number between 1 and 7 to set the priority for the user's traffic. The smaller the number, the higher the priority.<br>Traffic with a higher priority is given bandwidth before traffic with a lower priority.<br>Note: The priority setting here has priority over the priority setting in a bandwidth management rule. |
| OK | Click **OK** to save your changes back to the UAG. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 25.4 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 227** Configuration > Billing > Discount




The following table describes the labels in this screen.

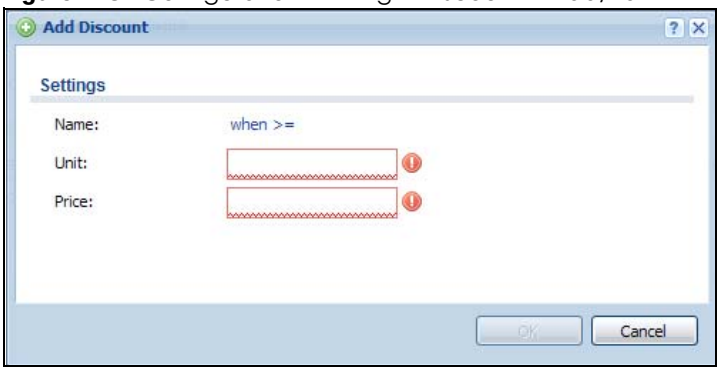
Table 146 Configuration > Billing > Discount

| 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.<br>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.<br>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. |

### 25.4.1 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 228** Configuration > Billing > Discount > Add/Edit




The following table describes the labels in this screen.

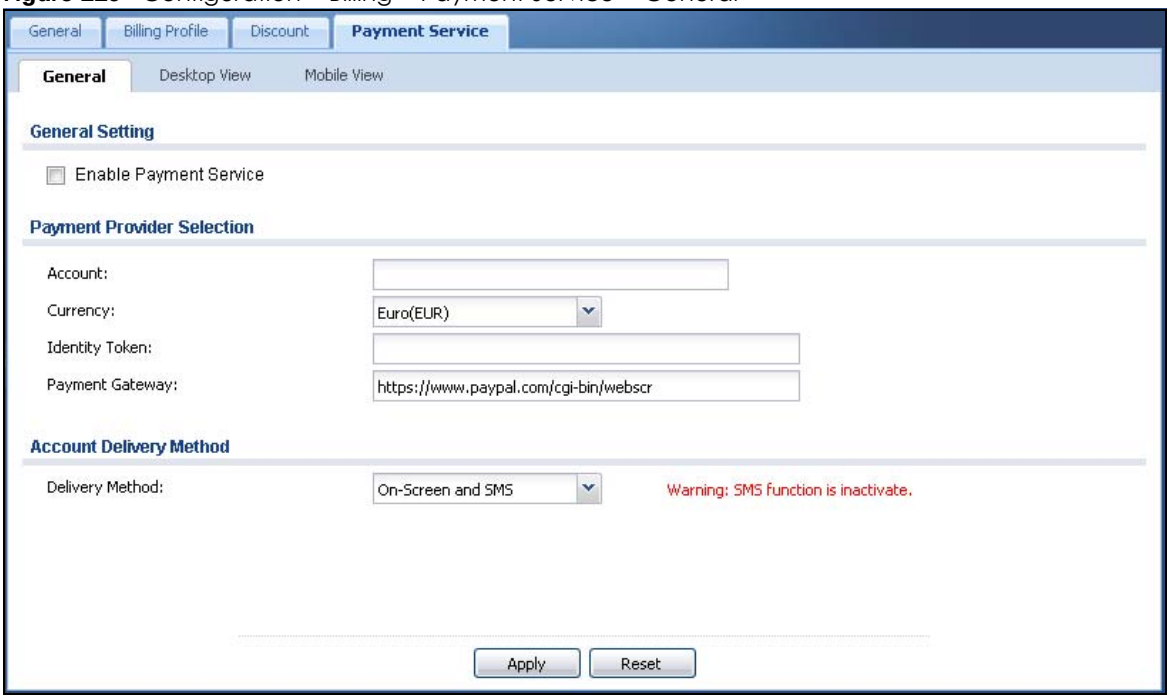
Table 147 Configuration > Billing > Discount > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Settings | |
| 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. |

## 25.5 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 229** Configuration > Billing > Payment Service > General




The following table describes the labels in this screen.

Table 148 Configuration > Billing > payment Service > General

| LABEL | DESCRIPTION |
|---|---|
| General Setting | |
| Enable Payment Service | Select the check box to use PayPal to authorize credit card payments.<br><br>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.<br><br>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 148 Configuration > Billing > payment Service > General (continued)

| LABEL | DESCRIPTION |
|---|---|
| Delivery Method | Specify how the UAG provides dynamic guest account information after the user's online payment is done.<br>Select **On-Screen** to display the user account information in the web screen.<br>Select **SMS** to use Short Message Service (SMS) to send account information in a text message to the user's mobile device.<br>Select **On-Screen and SMS** to provide the account information both in the web screen and via SMS text messages.<br>Note: You should have enabled SMS in the **Configuration > SMS** screen to send text messages to the user's mobile device. |
| Apply | Click this button to save your changes to the UAG. |
| Reset | Click this button to return the screen to its last-saved settings. |

## 25.5.1 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 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 230** Configuration > Billing > Payment Service > Desktop View

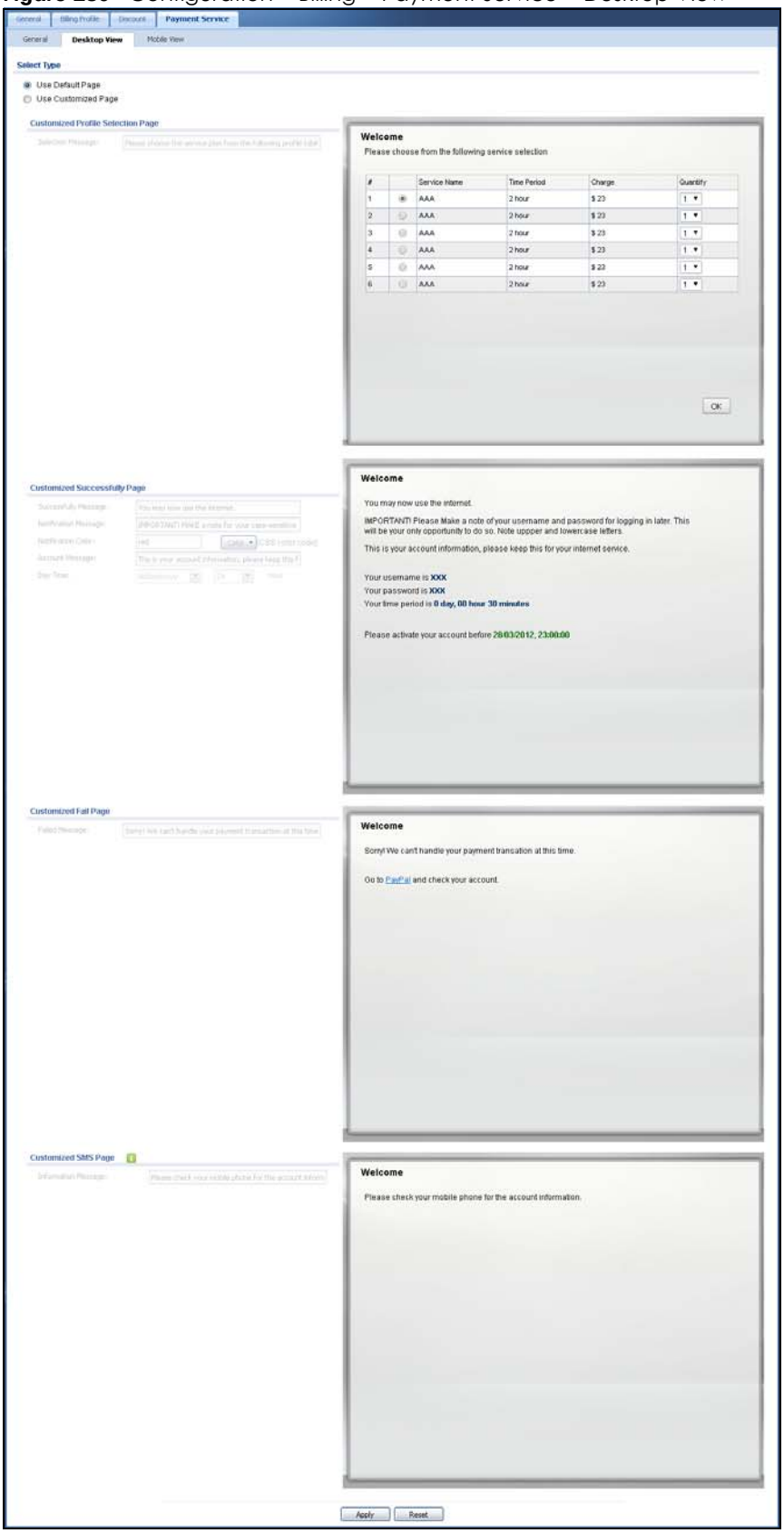
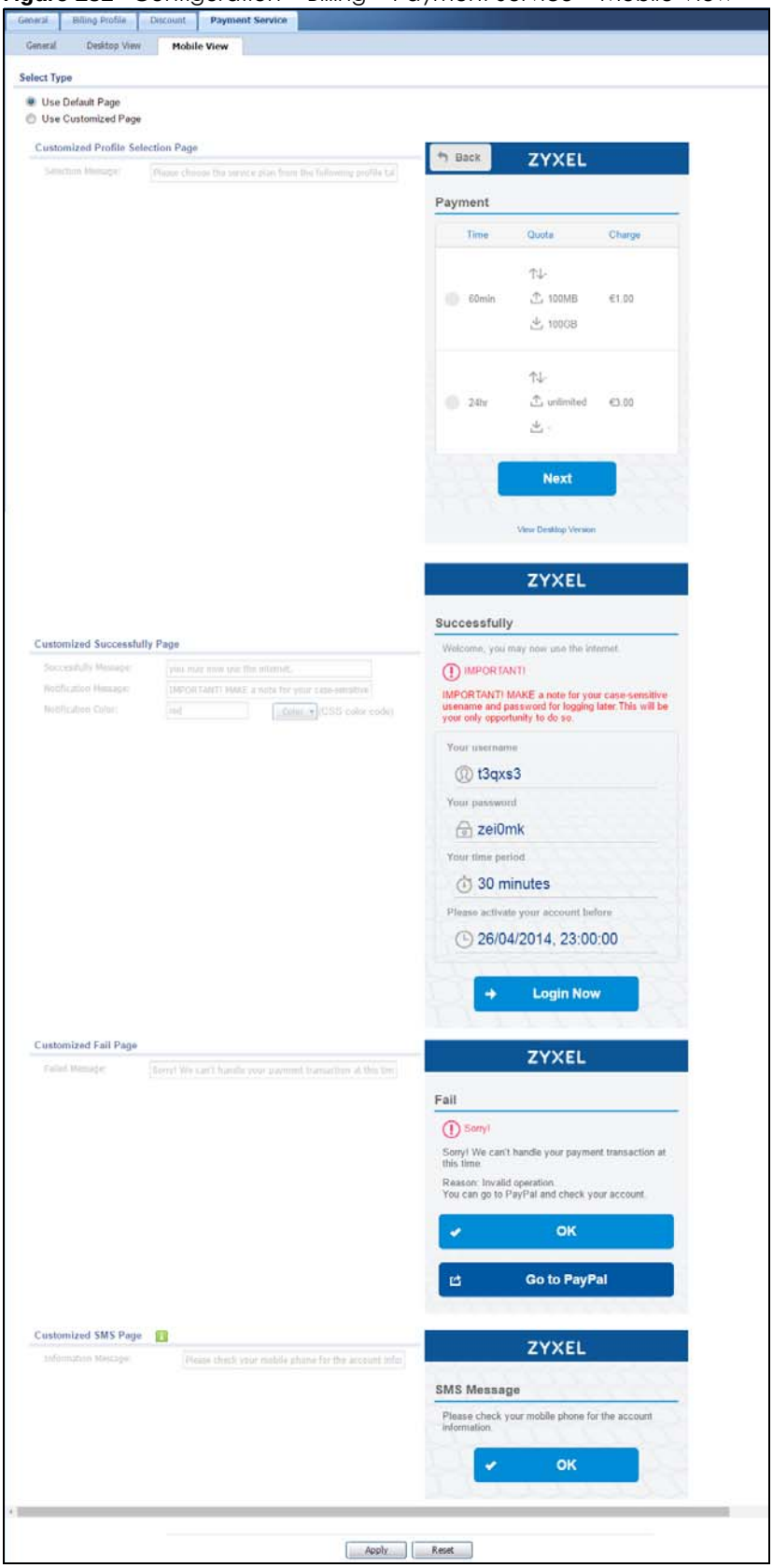


**Figure 231** Configuration > Billing > Payment Service > Mobile View



The following table describes the labels in this screen.

Table 149 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. |

# CHAPTER 26
# Printer

## 26.1 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.

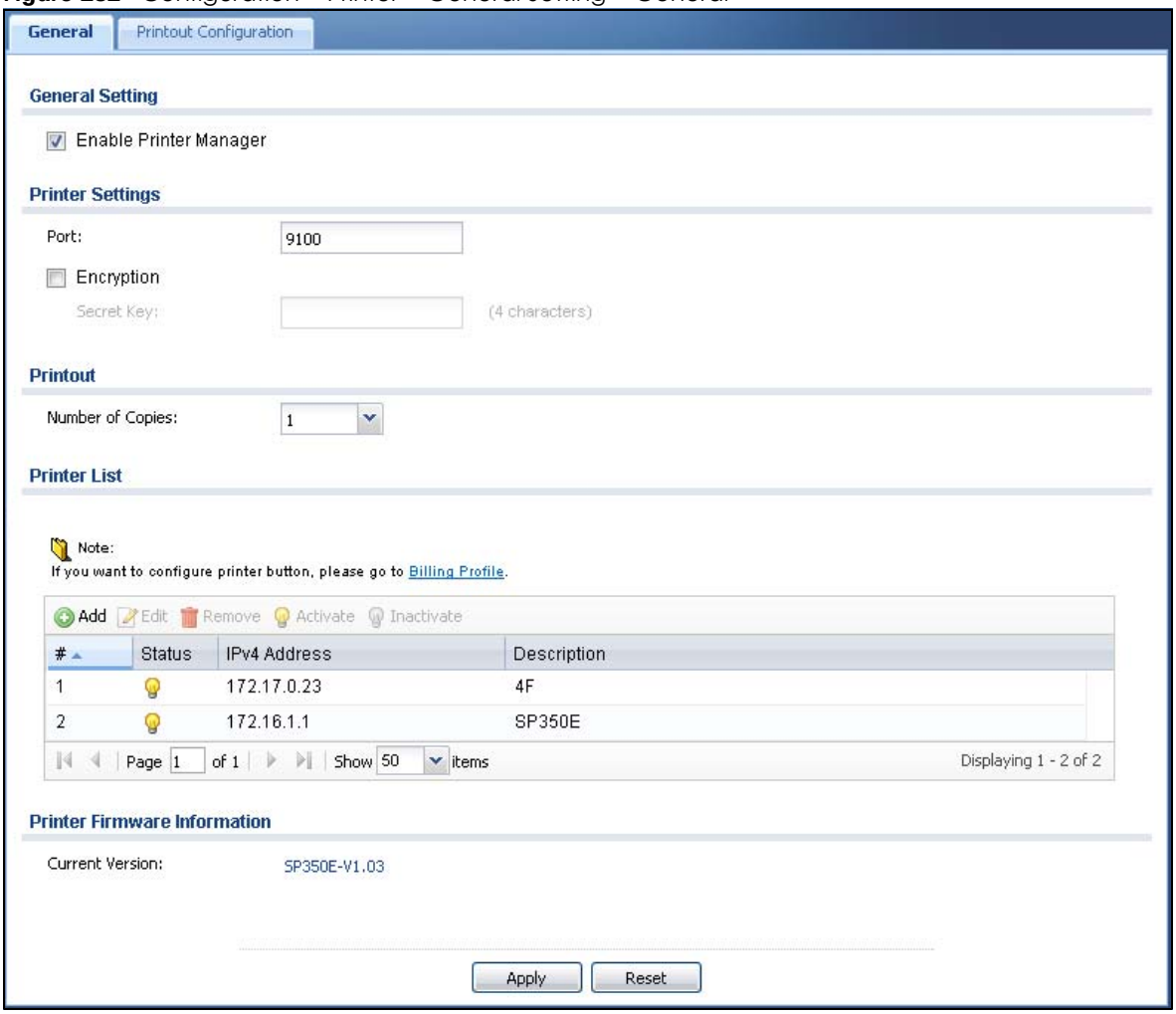
### 26.1.1 What You Can Do in this Chapter

- Use the **General Setting > General** screen (see Section 26.2 on page 332) to configure the printer list and enable printer management.
- Use the **General Setting > Printout Configuration** screen (see Section 26.3 on page 335) to customize the account printout.
- Use the **Printer Manager** screen (see Section 26.4 on page 336) to manage and view information about the connected statement printer.

## 26.2 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 232** Configuration > Printer > General Setting > General




The following table describes the labels in this screen.

Table 150 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 150 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. |

## 26.2.1 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 233** Configuration > Printer > General Setting > General: Add/Edit

The following table describes the labels in this screen.

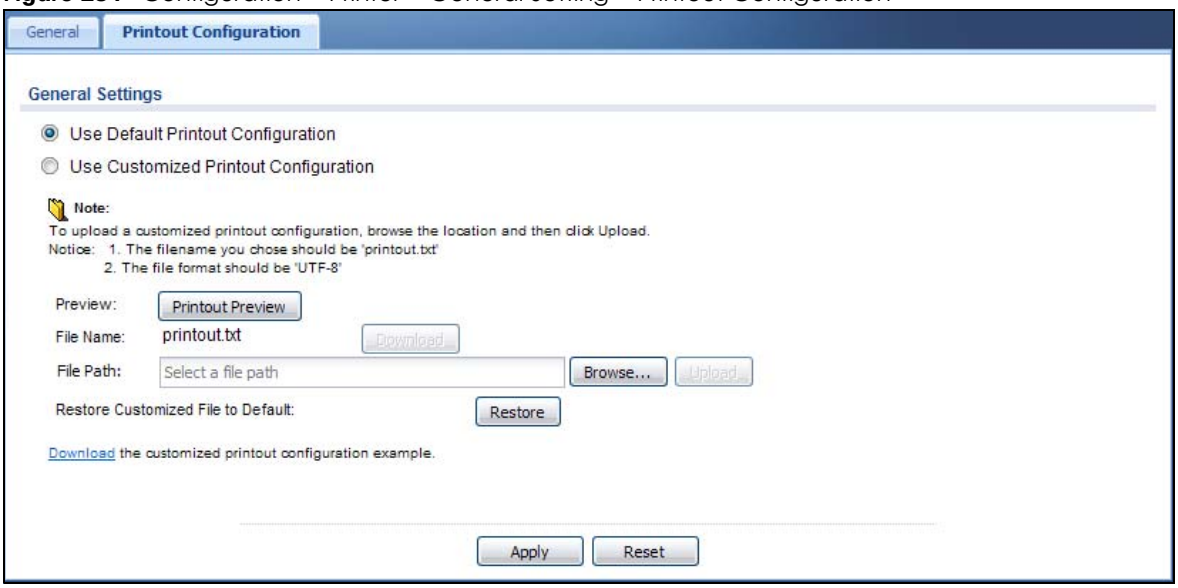
Table 151 Configuration > Printer > General Setting > General: Add/Edit

| 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.<br>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. |

# 26.3 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 234** Configuration > Printer > General Setting > Printout Configuration




The following table describes the labels in this screen.

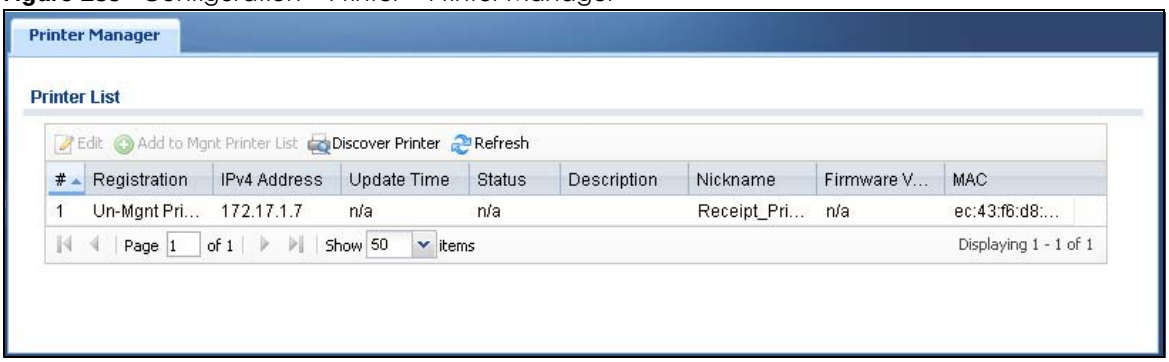
Table 152 Configuration > Printer > General Setting > Printout Configuration

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| 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.<br>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. |

# 26.4 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 235** Configuration > Printer > Printer Manager




The following table describes the labels in this screen.

Table 153 Configuration > Printer > Printer Manager

| LABEL | DESCRIPTION |
|---|---|
| Printer List | |
| Edit | Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.<br><br>Note: You cannot edit an entry's settings when the printer status is **sync fail** or **sync progressing**. |
| Add to Mgnt 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.<br><br>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 (**Mgnt Printer**) or not (**Un-Mgnt 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.<br><br>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.<br><br>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. |

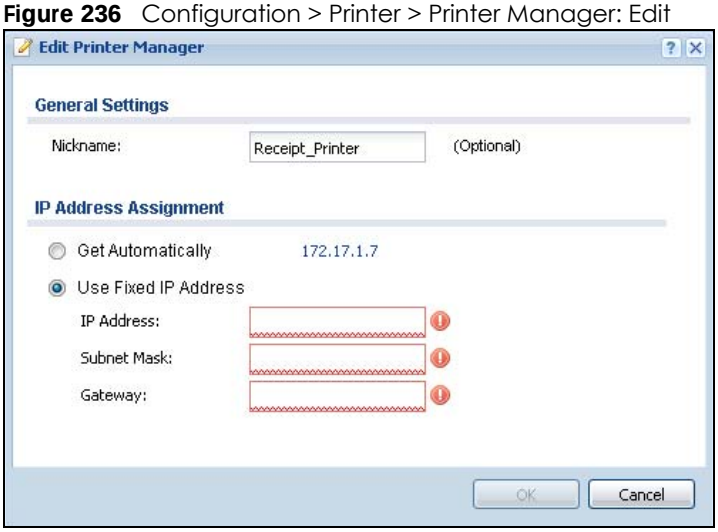
Table 153 Configuration > Printer > Printer Manager (continued)

| LABEL | DESCRIPTION |
|---|---|
| Firmware Version | This field displays the model number and firmware version of the printer.<br>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. |

## 26.4.1 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 236** Configuration > Printer > Printer Manager: Edit




The following table describes the labels in this screen.

Table 154 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. |

## 26.4.2 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

## 26.4.3 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 155 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.

## 26.4.4 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 237** 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---
```

## 26.4.5 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 238** 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---
```

## 26.4.6 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).

## 26.4.7 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 239** 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 156 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 156 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. |

# CHAPTER 27
# Free Time

## 27.1 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.

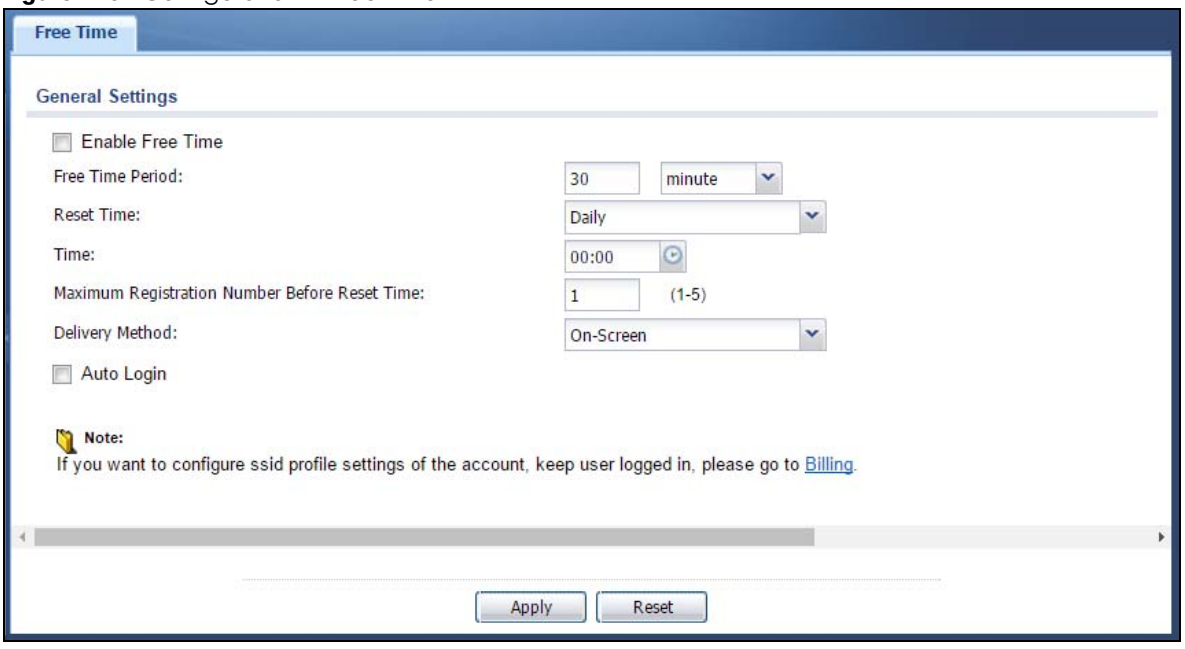
### 27.1.1 What You Can Do in this Chapter

Use the **Free Time** screen (see Section 27.2 on page 342) to turn on this feature to allow users to get a free account for Internet surfing during the specified time period.

## 27.2 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 240** Configuration > Free Time



The following table describes the labels in this screen.

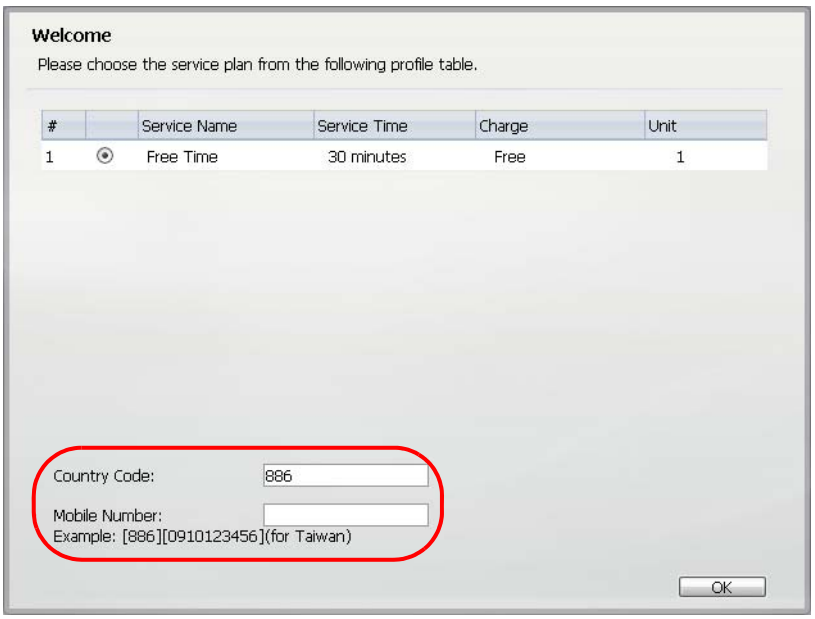
Table 157 Configuration > Free Time

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Enable Free Time | Select the check box to turn on the free time feature.<br>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. |
| Free Time Period | Select the duration of time period for which the free time account is allowed to access the Internet. |
| Reset Time | Select **Daily** to have the UAG allow free account access every day at the specified time.<br>Select **Weekly** to have the UAG allow free account access once a week on the day you select.<br>Select **Monthly** to have the UAG allow free account access once a month on a set date. |
| Time | If you select **Daily**, select the time in 24-hour format at which the new free time account is allowed to access the Internet. |
| Day | If you select **Weekly**, select the day on which the new free time account is allowed to access the Internet.<br>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. |
| 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. This also sets how many free guest accounts a user can get.<br>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. |
| Delivery Method | Specify how the UAG provides dynamic guest account information.<br>Select **On-Screen** to display the user account information in the web screen.<br>Select **SMS** to use Short Message Service (SMS) to send account information in a text message to the user's mobile device.<br>Select **On-Screen and SMS** to provide the account information both in the web screen and via SMS text messages.<br>Note: You should have enabled SMS in the **Configuration > SMS** screen to send text messages to the user's mobile device. |
| Auto Login | Select the check box to allow users to log in automatically when using Free Time. |
| Apply | Click this button to save your changes to the UAG. |
| Reset | Click this button to return the screen to its last-saved settings. |

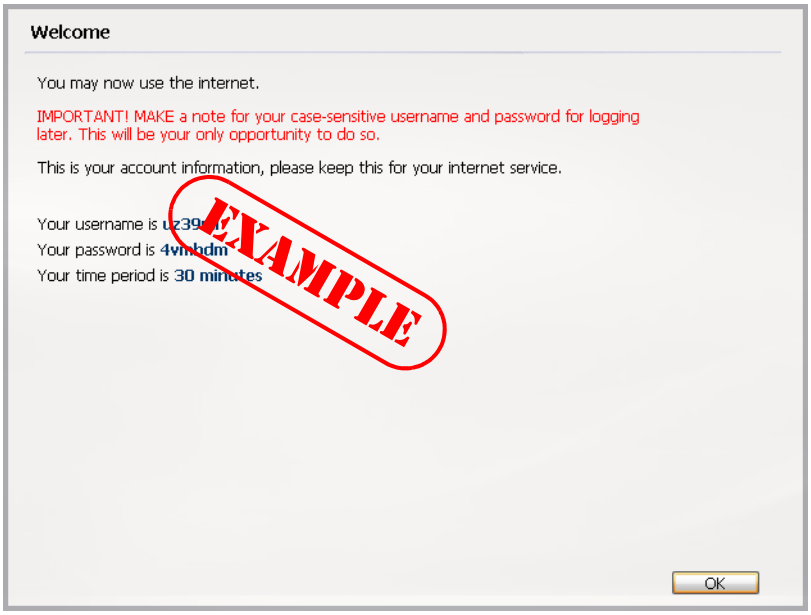
The following figure shows an example login screen with a link to create a free guest account.

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.




The guest account information then displays in the screen and/or is sent to the configured mobile phone number.



# CHAPTER 28
# SMS

## 28.1 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.

### 28.1.1 What You Can Do in this Chapter

Use the **SMS** screen (see Section 28.2 on page 346) to turn on the SMS service on the UAG.

## 28.2 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 241** Configuration > SMS (UAG4100 or UAG5100)

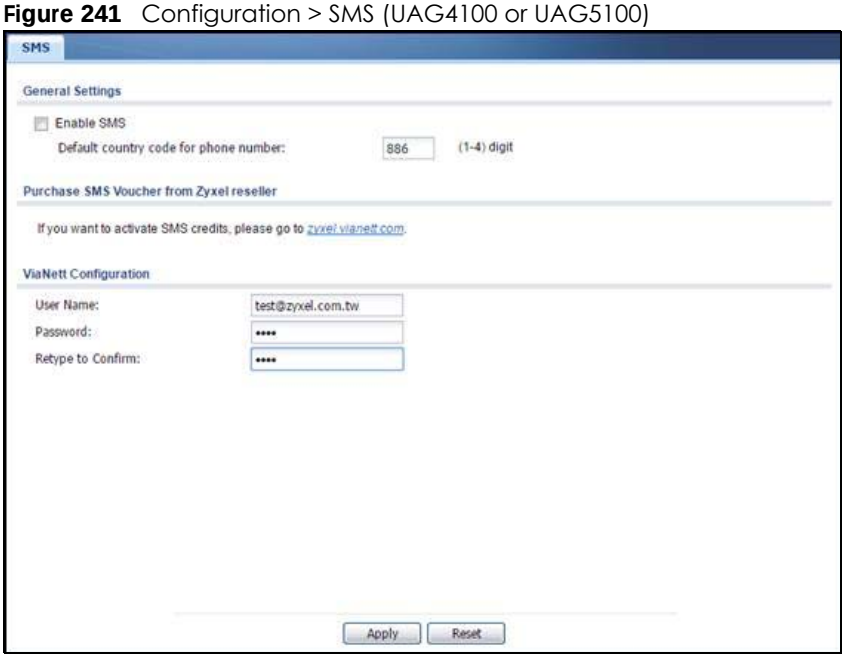
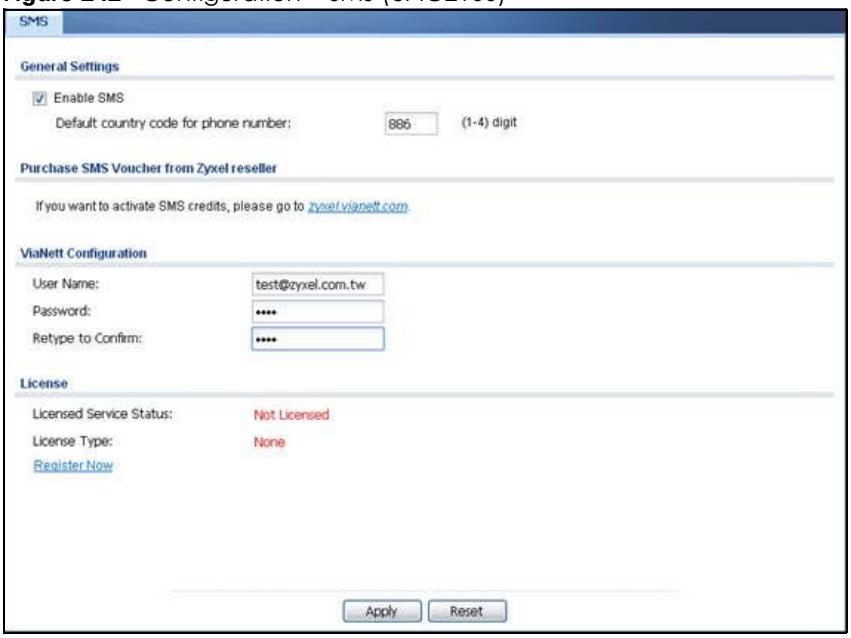


**Figure 242** Configuration > SMS (UAG2100)




The following table describes the labels in this screen.

Table 158 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. |
| Purchase SMS Voucher from Zyxel Reseller | Use this link to access Zyxel portal and activate the SMS credits. |
| 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**).<br>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.<br>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. |

# CHAPTER 29
# IPSec VPN

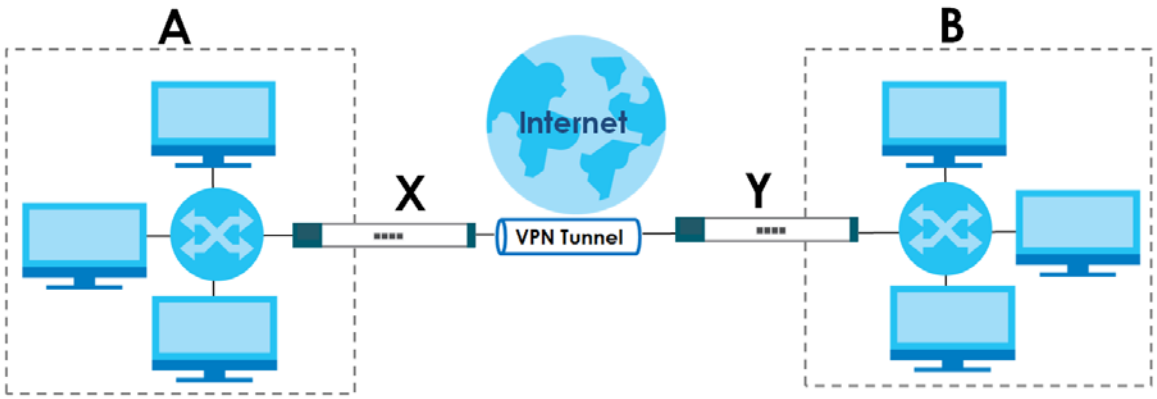
## 29.1 Virtual Private Networks (VPN) Overview

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 243** IPSec VPN Example



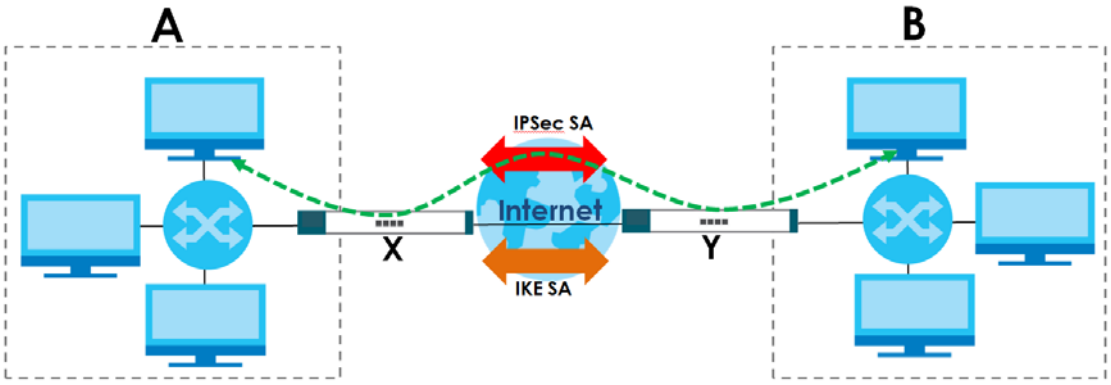

### 29.1.1 What You Can Do in this Chapter

- Use the **VPN Connection** screens (see Section 29.2 on page 350) 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 29.3 on page 357) 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.

## 29.1.2 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 244** 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 29.4 on page 364 for IPSec VPN background information.
- See the help in the IPSec VPN quick setup wizard screens.

## 29.1.3 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 169.
- 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 41 on page 468.
- 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 43 on page 476.

# 29.2 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 245** Configuration > VPN > IPSec VPN > VPN Connection

Each field is discussed in the following table. See Section 29.2.1 on page 351 for more information.

Table 159 Configuration > VPN > IPSec VPN > VPN Connection

| LABEL | DESCRIPTION |
|---|---|
| Global Setting | |
| 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. |
| Configuration | |
| 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 180 for an example. |
| # | This field is a sequential value, and it is not associated with a specific connection. |

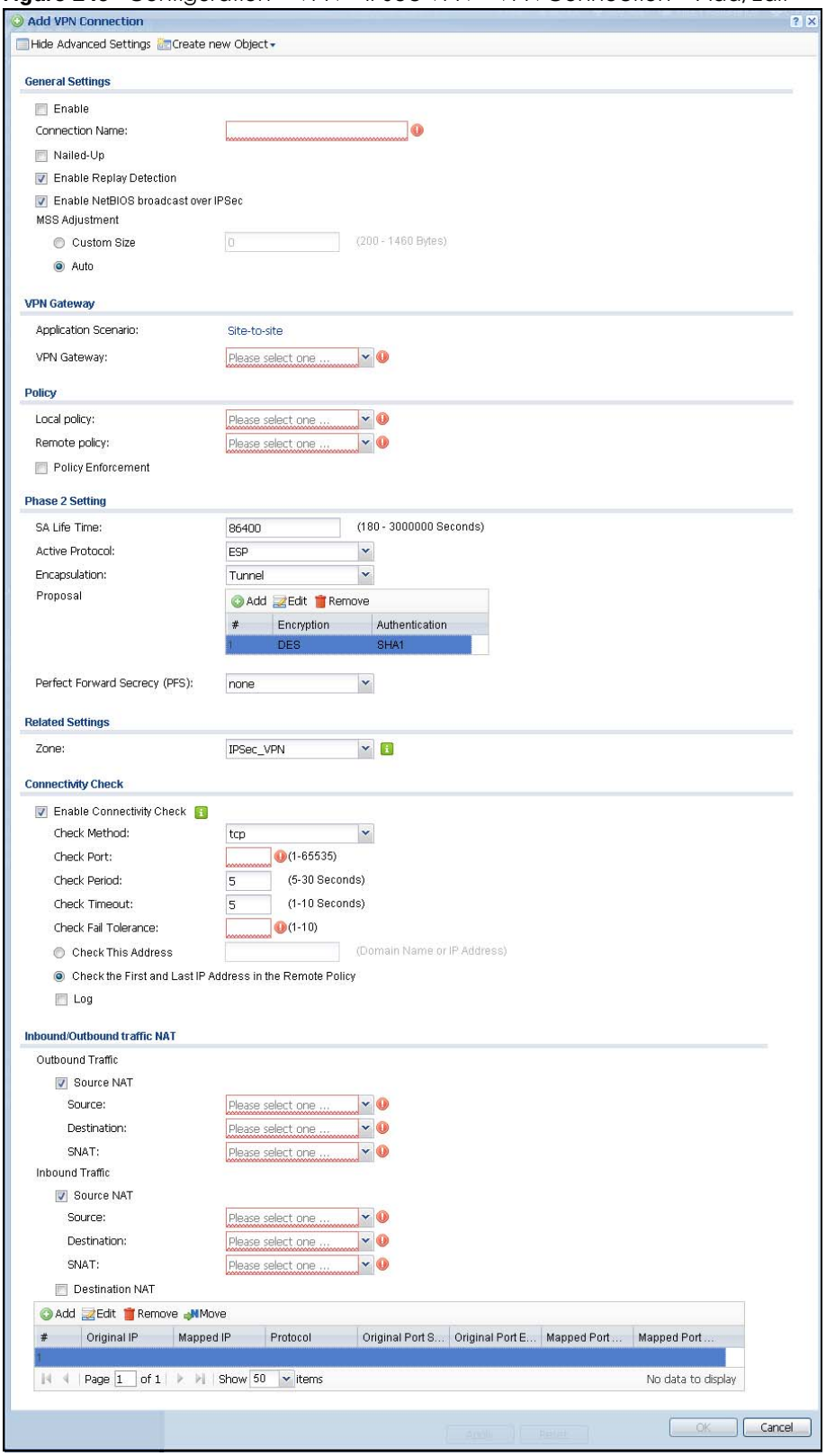
Table 159 Configuration > VPN > IPSec VPN > VPN Connection (continued)

| LABEL | DESCRIPTION |
|---|---|
| Status | The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.<br>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. |

## 29.2.1 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 29.2 on page 350), and either click the **Add** icon or select an entry and click the **Edit** icon.

**Figure 246** Configuration > VPN > IPSec VPN > VPN Connection > Add/Edit



Each field is described in the following table.

Table 160 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 | Select this check box if you the UAG to send NetBIOS (Network Basic Input/Output System) packets through the IPSec SA.<br>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. |
| MSS Adjustment | 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.<br>Select **Auto** to have the UAG automatically set the MSS for this VPN connection. |
| VPN Gateway | |
| Application Scenario | This field is read-only and shows the scenario that the UAG supports.<br>**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. |
| 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 | 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.<br>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. |
| 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 160 Configuration > VPN > IPSec VPN > VPN Connection > Add/Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Active Protocol | Select which protocol you want to use in the IPSec SA. Choices are:<br>**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.<br>**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.<br>Both **AH** and **ESP** increase processing requirements and latency (delay).<br>The UAG and remote IPSec router must use the same active protocol. |
| Encapsulation | Select which type of encapsulation the IPSec SA uses. Choices are<br>**Tunnel** - this mode encrypts the IP header information and the data.<br>**Transport** - this mode only encrypts the data.<br>The UAG and remote IPSec router must use the same encapsulation. |
| 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 | 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:<br>**NULL** - no encryption key or algorithm<br>**DES** - a 56-bit key with the DES encryption algorithm<br>**3DES** - a 168-bit key with the DES encryption algorithm<br>**AES128** - a 128-bit key with the AES encryption algorithm<br>**AES192** - a 192-bit key with the AES encryption algorithm<br>**AES256** - a 256-bit key with the AES encryption algorithm<br>The UAG and the remote IPSec router must both have at least one proposal that uses use the same encryption and the same key.<br>Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput. |
| Authentication | 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.<br>The UAG and the remote IPSec router must both have a proposal that uses the same authentication algorithm. |

Table 160 Configuration > VPN > IPSec VPN > VPN Connection > Add/Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Perfect Forward Secrecy (PFS) | 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:<br>**none** - disable PFS<br>**DH1** - enable PFS and use a 768-bit random number<br>**DH2** - enable PFS and use a 1024-bit random number<br>**DH5** - enable PFS and use a 1536-bit random number<br>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. |
| 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 | Select how the UAG checks the connection. The peer must be configured to respond to the method you select.<br>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.<br>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. |
| 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**). |

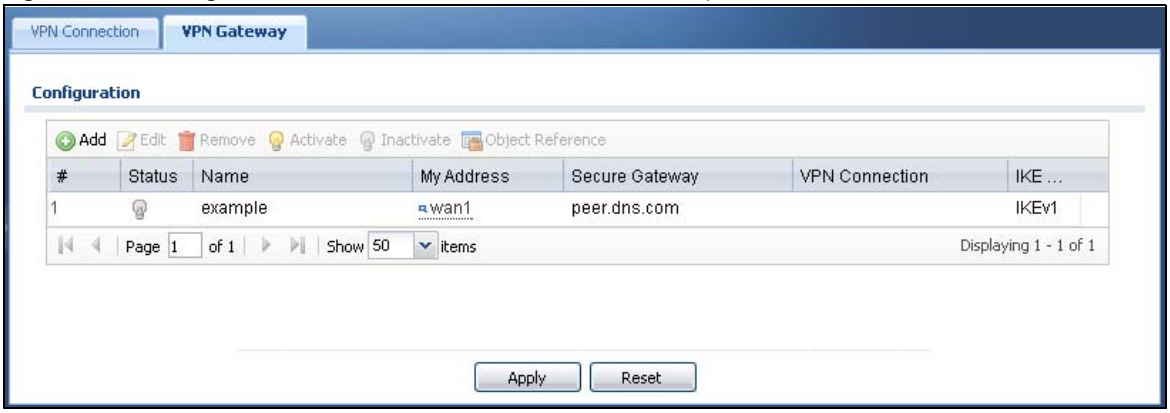
Table 160 Configuration > VPN > IPSec VPN > VPN Connection > Add/Edit (continued)

| 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. |

# 29.3 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 247** Configuration > VPN > IPSec VPN > VPN Gateway




Each field is discussed in the following table. See Section 29.3.1 on page 358 for more information.

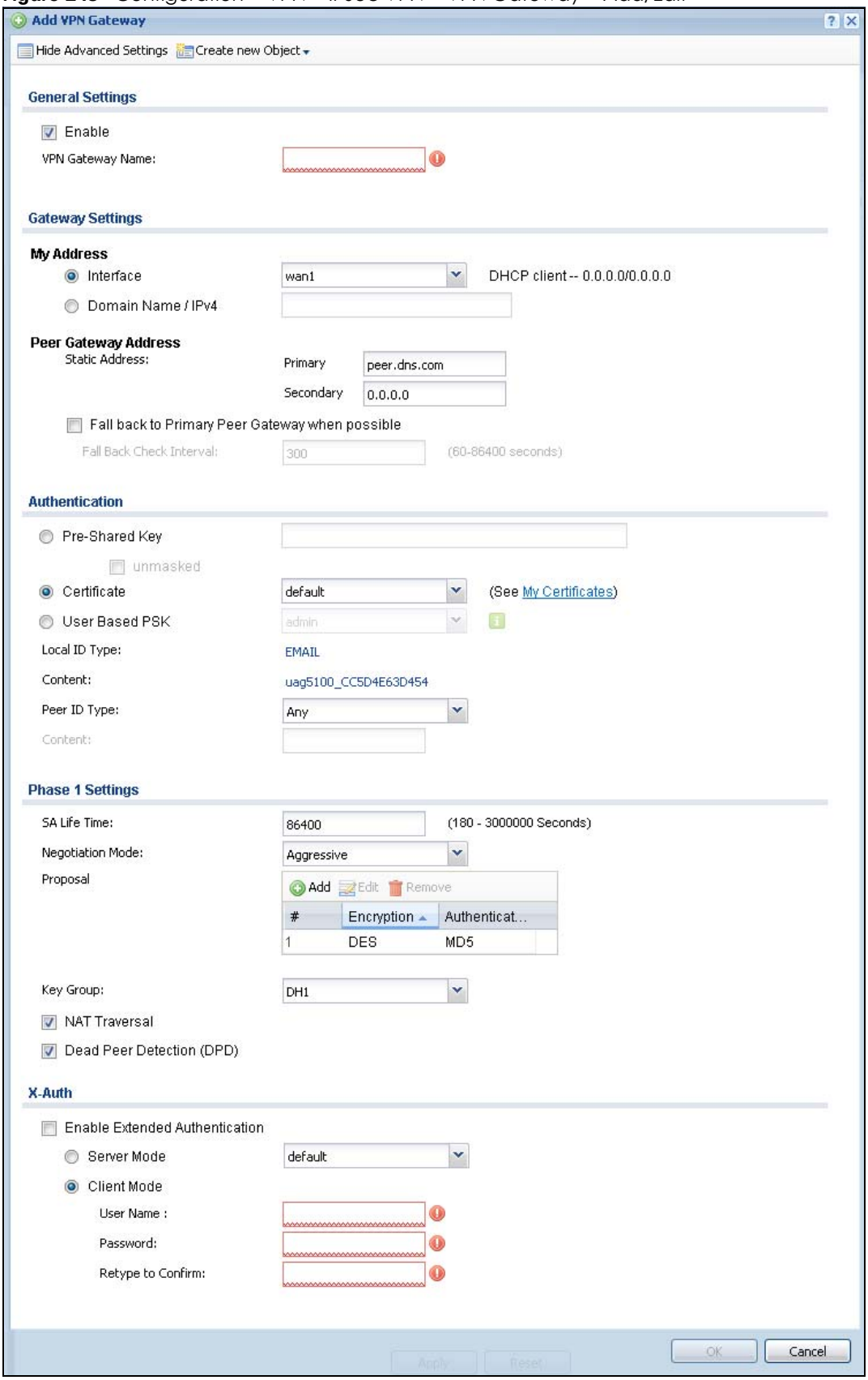
Table 161 Configuration > VPN > IPSec VPN > VPN Gateway

| LABEL | DESCRIPTION |
|---|---|
| Configuration | |
| 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 180 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. |

### 29.3.1 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 29.3 on page 357), and either click the **Add** icon or select an entry and click the **Edit** icon.

**Figure 248** Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit



Each field is described in the following table.

Table 162 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 | Select how the IP address of the UAG in the IKE SA is defined.<br>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.<br>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. |
| Peer Gateway Address | Select how the IP address of the remote IPSec router in the IKE SA is defined.<br>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.<br>**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. |
| Authentication | Note: The UAG and remote IPSec router must use the same authentication method to establish the IKE SA. |
| Pre-Shared Key | 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:<br>• alphanumeric characters or ,;. \| `~!@#$%^&*()_+\{}':./<>=-"<br>• pairs of hexadecimal (0-9, A-F) characters, preceded by "0x".<br>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.<br>The UAG and remote IPSec router must use the same pre-shared key. |
| unmasked | Select this option to see the pre-shared key in readable plain text.<br>De-select this option to not display the real key (password) and instead show a sequence of dots. |

Table 162 Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Certificate | 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.<br><br>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.<br><br>Note: The IPSec routers must trust each other's certificates.<br><br>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. |
| User Based PSK | 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. |
| Local ID Type | 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:<br><br>**IPv4** - the UAG is identified by an IP address<br><br>**DNS** - the UAG is identified by a domain name<br><br>**E-mail** - the UAG is identified by the string specified in this field |
| Content | 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**.<br><br>**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:<br><br>• There is a NAT router between the UAG and remote IPSec router.<br>• 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.<br><br>In these situations, use a different IP address, or use a different **Local ID Type**.<br><br>**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.<br><br>**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. |
| Peer ID Type | Select which type of identification is used to identify the remote IPSec router during authentication. Choices are:<br><br>**IPv4** - the remote IPSec router is identified by an IP address<br><br>**DNS** - the remote IPSec router is identified by a domain name<br><br>**E-mail** - the remote IPSec router is identified by the string specified in this field<br><br>**Any** - the UAG does not check the identity of the remote IPSec router<br><br>If the UAG and remote IPSec router use certificates, there is one more choice.<br><br>**Subject Name** - the remote IPSec router is identified by the subject name in the certificate |

Table 162 Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Content | 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**.<br><br>If the UAG and remote IPSec router do not use certificates,<br><br>**IPv4** - type an IP address; see the note at the end of this description.<br><br>**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.<br><br>**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.<br><br>If the UAG and remote IPSec router use certificates, type the following fields from the certificate used by the remote IPSec router.<br><br>**IPv4** - subject alternative name field; see the note at the end of this description.<br><br>**DNS** - subject alternative name field<br><br>**E-mail** - subject alternative name field<br><br>**Subject Name** - subject name (maximum 255 ASCII characters, including spaces)<br><br>Note: If **Peer ID Type** is **IPv4**, please read the rest of this section.<br><br>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:<br><br>• There is a NAT router between the UAG and remote IPSec router.<br>• 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.<br><br>In these situations, use a different IP address, or use a different **Peer ID Type**. |
| 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 | Select the negotiation mode to use to negotiate the IKE SA. Choices are<br><br>**Main** - this encrypts the UAG's and remote IPSec router's identities but takes more time to establish the IKE SA<br><br>**Aggressive** - this is faster but does not encrypt the identities<br><br>The UAG and the remote IPSec router must use the same negotiation mode. |
| 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 162 Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Encryption | Select which key size and encryption algorithm to use in the IKE SA. Choices are:<br>**DES** - a 56-bit key with the DES encryption algorithm<br>**3DES** - a 168-bit key with the DES encryption algorithm<br>**AES128** - a 128-bit key with the AES encryption algorithm<br>**AES192** - a 192-bit key with the AES encryption algorithm<br>**AES256** - a 256-bit key with the AES encryption algorithm<br>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. |
| Authentication | 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.<br>The remote IPSec router must use the same authentication algorithm. |
| Key Group | Select which Diffie-Hellman key group (DH*x*) you want to use for encryption keys. Choices are:<br>**DH1** - use a 768-bit random number<br>**DH2** - use a 1024-bit random number<br>**DH5** - use a 1536-bit random number<br>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. |
| NAT Traversal | Select this if any of these conditions are satisfied.<br>• This IKE SA might be used to negotiate IPSec SAs that use ESP as the active protocol.<br>• 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.<br>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. |
| Dead Peer Detection (DPD) | 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.<br>If the remote IPSec router does not support DPD, see if you can use the VPN connection connectivity check (see Section 29.2.1 on page 351). |
| X-Auth | 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. |
| Enable Extended Authentication | 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. |
| Server Mode | 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. |
| Client Mode | 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**. |

Table 162 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. |

# 29.4 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 367. Main mode is used in various examples in the rest of this section.

## IP Addresses of the UAG and Remote IPSec Router

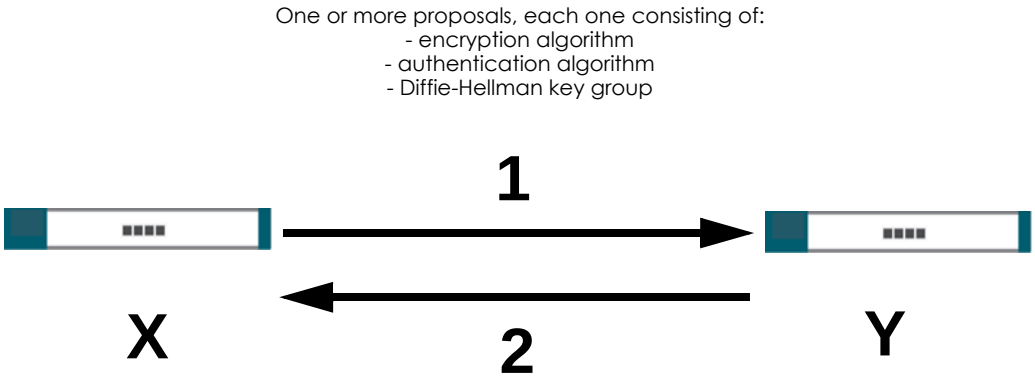
To set up an IKE SA, you have to specify the IP addresses of the UAG and remote IPSec router. You can usually enter a static IP address or a domain name for either or both IP addresses. Sometimes, your UAG might offer another alternative, such as using the IP address of a port or interface, as well.

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 249** 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.

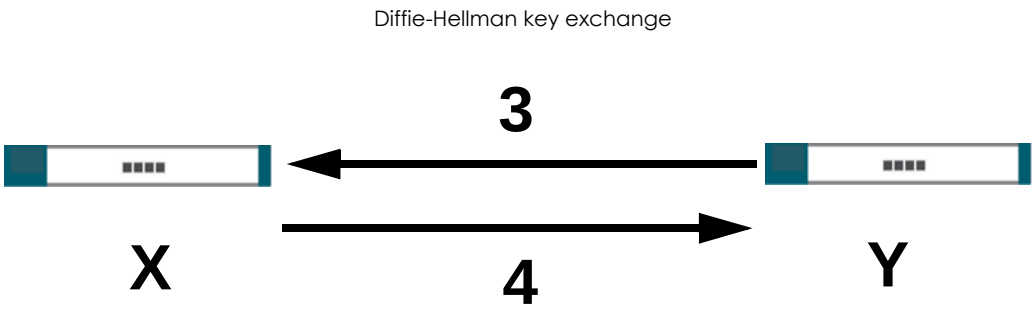
- MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
- SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
- SHA256 (Secure Hash Algorithm) produces a 256-bit digest to authenticate packet data.
- SHA512 (Secure Hash Algorithm) produces a 512-bit digest to authenticate packet data.

See Diffie-Hellman (DH) Key Exchange on page 365 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 250** IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange



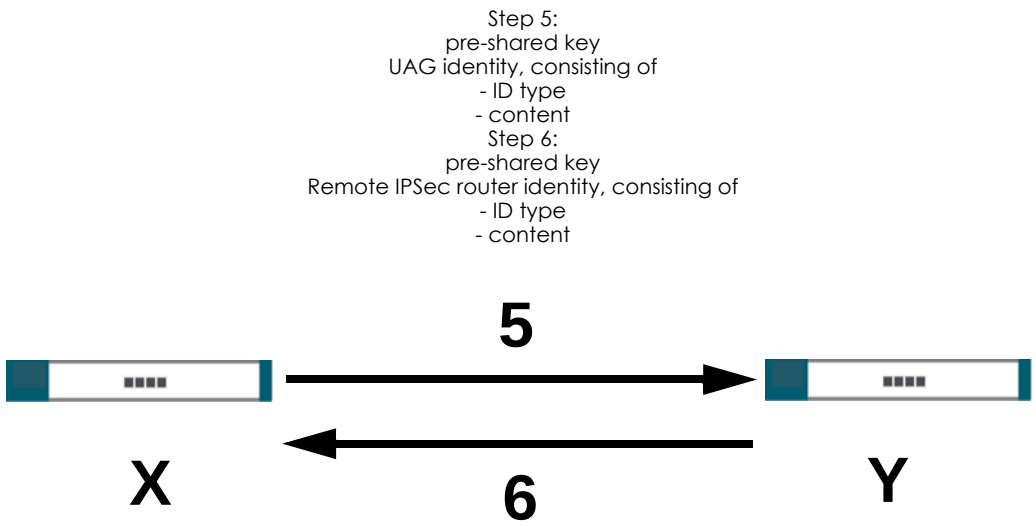

DH public-key cryptography is based on DH key groups. Each key group is a fixed number of bits long. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. For example, DH2 keys (1024 bits) are more secure than DH1 keys (768 bits), but DH2 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 251** 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 163 on page 367, the UAG and the remote IPSec router authenticate each other successfully. In contrast, in Table 164 on page 367, the UAG and the remote IPSec router cannot authenticate each other and, therefore, cannot establish an IKE SA.

Table 163 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 164 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.

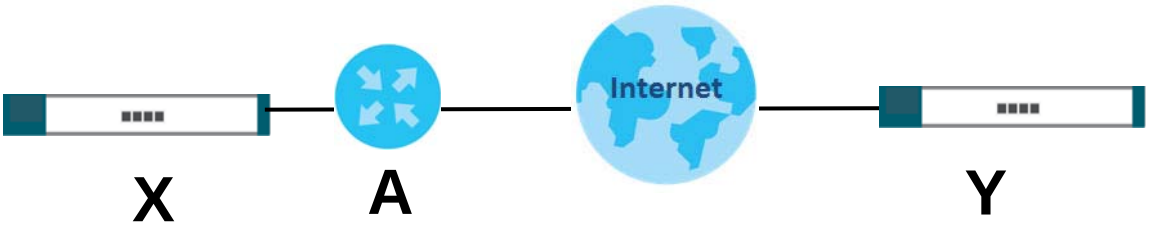
Steps 5 - 6: Finally, the UAG and the remote IPSec router generate an encryption key (from the shared secret), encrypt their identities, and exchange their encrypted identity information for authentication.

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 252** 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 369 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.

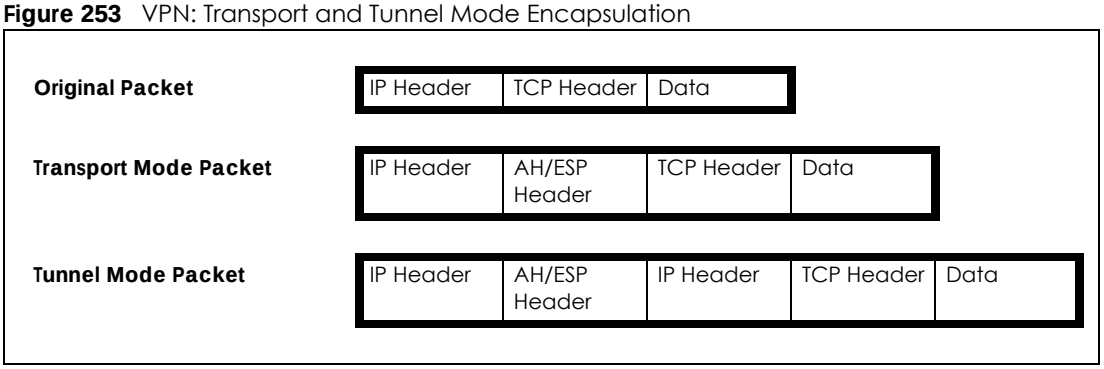
## Encapsulation

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 253** 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 364), 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.

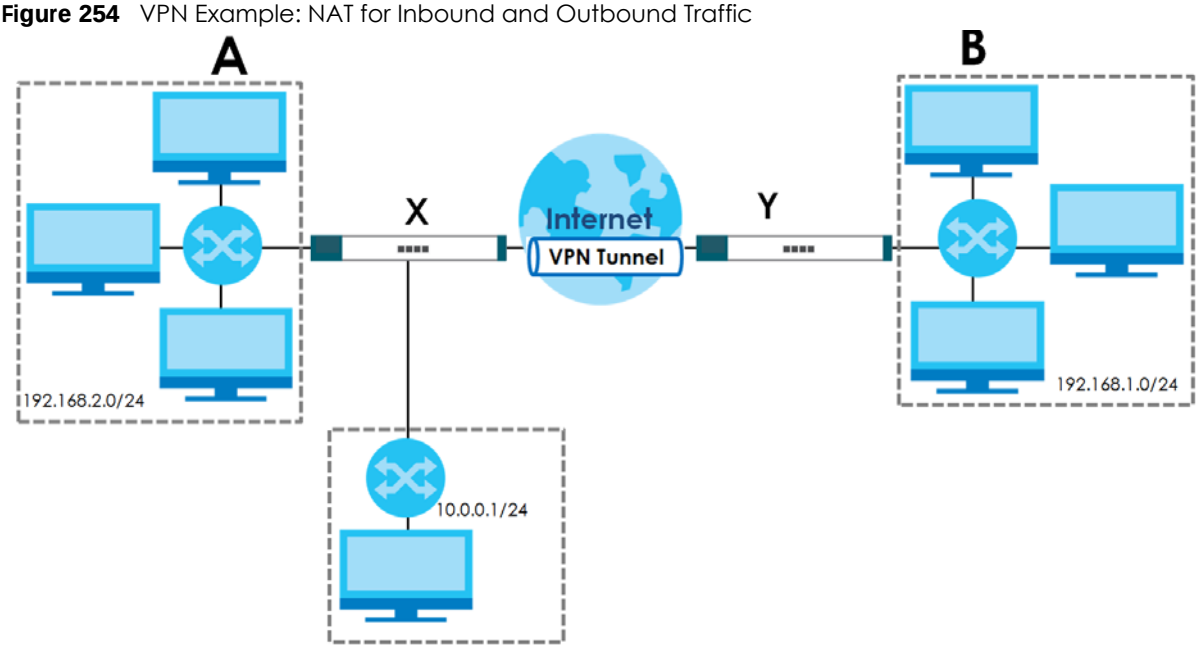
### NAT for Inbound and Outbound Traffic

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 254** 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 254 on page 371, 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 254 on page 371, 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 254 on page 371, it might be port 25 for SMTP.

The second part of these rules controls the translation when the condition is satisfied.

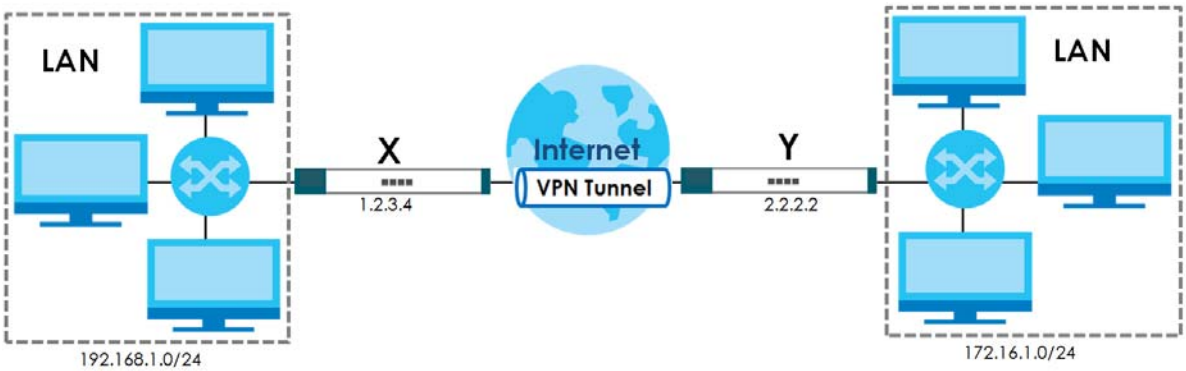
- Mapped IP - the translated destination address; in Figure 254 on page 371, the IP address of the mail server in the local network (**A**).
- Mapped Port - the translated destination port or range of destination ports.

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.

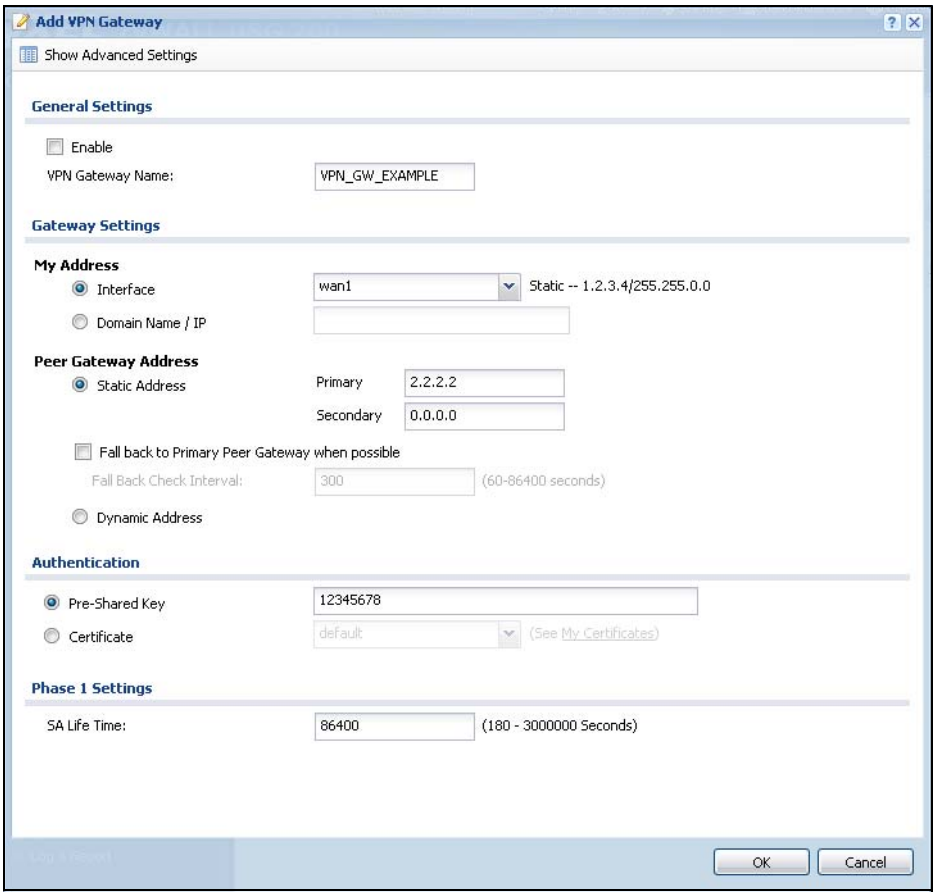
**Figure 255** IPSec VPN Example




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

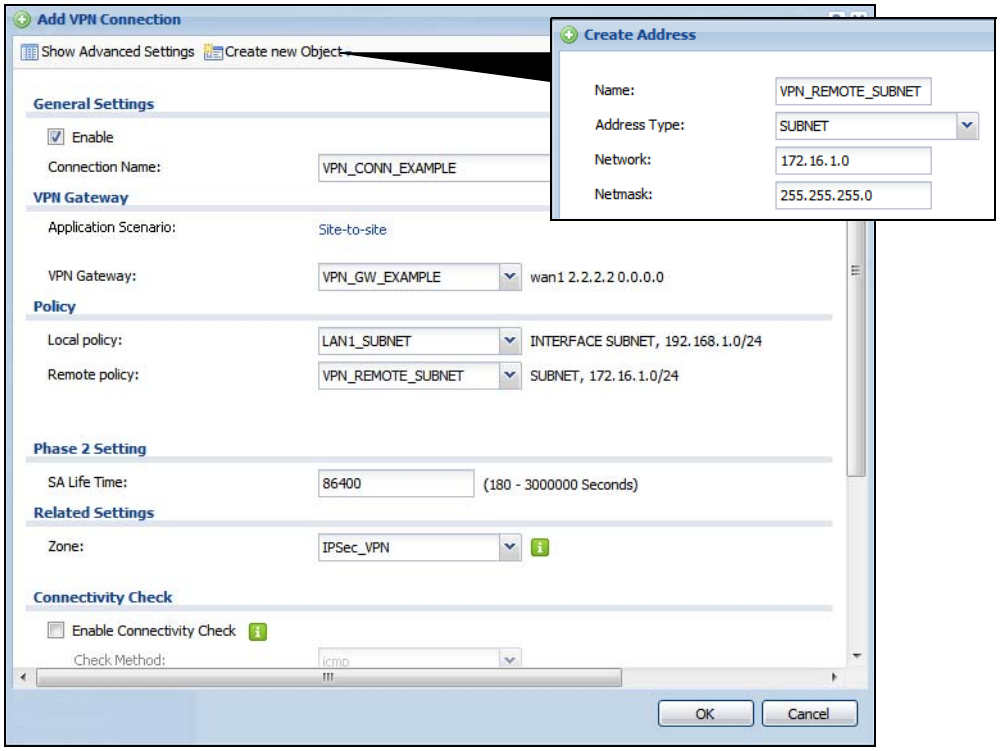
In **Configuration > VPN > IPSec VPN > VPN Gateway > Add**, enable the VPN gateway and name it (VPN_GW_EXAMPLE here). Set **My Address** to **Interface** and select a WAN interface. Set **Peer Gateway Address** to **Static Address** and enter the remote IPSec router's public IP address (2.2.2.2 here) as the **Primary**. Set **Authentication** to **Pre-Shared Key** and enter 12345678. Click **OK**.




## 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**.


Add VPN Connection
Show Advanced Settings
Create new Object
General Settings
Enable
Connection Name:
VPN_CONN_EXAMPLE
VPN Gateway
Application Scenario:
Site-to-site
VPN Gateway:
VPN_GW_EXAMPLE
wan1 2.2.2.2 0.0.0.0
Policy
Local policy:
LAN1_SUBNET
INTERFACE SUBNET, 192.168.1.0/24
Remote policy:
VPN_REMOTE_SUBNET
SUBNET, 172.16.1.0/24
Phase 2 Setting
SA Life Time:
86400
(180 - 3000000 Seconds)
Related Settings
Zone:
IPSec_VPN
Connectivity Check
Enable Connectivity Check
Check Method:
icmp
OK
Cancel
Create Address
Name:
VPN_REMOTE_SUBNET
Address Type:
SUBNET
Network:
172.16.1.0
Netmask:
255.255.255.0

# CHAPTER 30
# Bandwidth Management

## 30.1 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.

### 30.1.1 What You Can Do in this Chapter

Use the **BWM** screens (see Section 30.2 on page 379) to control bandwidth for services passing through the UAG, and it identifies the conditions that refine this.

### 30.1.2 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**.

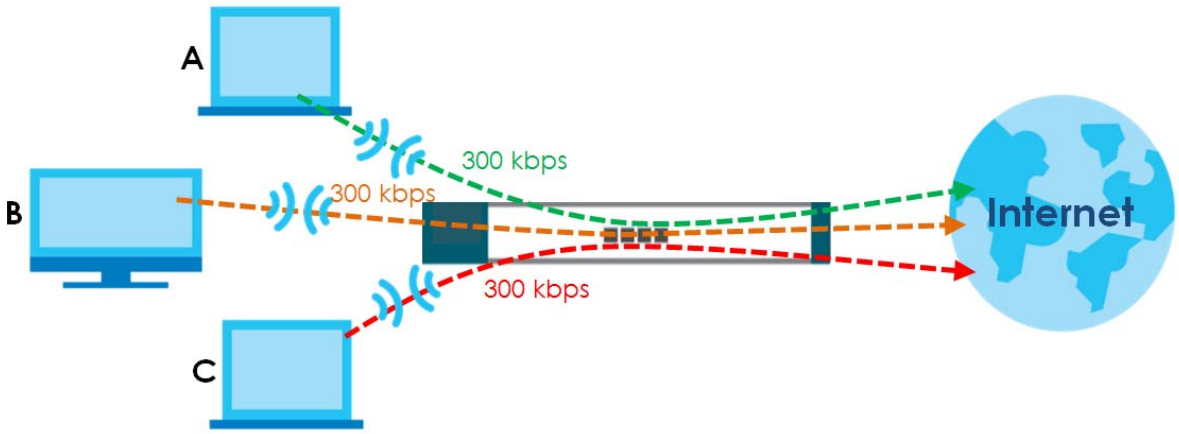
The **Shared** BWM type is selected by default in a bandwidth management rule. All matched traffic shares the bandwidth configured in the rule.

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.

**Figure 256** Bandwidth Management Example




## 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 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.

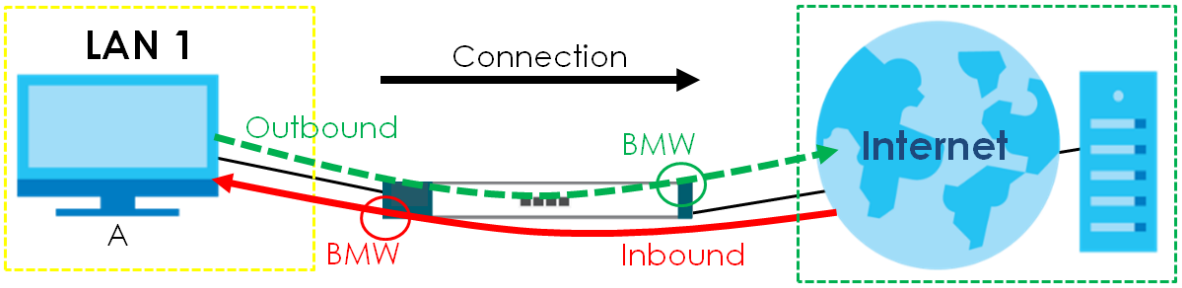
A connection has outbound and inbound packet flows. The UAG controls the bandwidth of traffic of each flow as it is going out through an interface.

- 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 257** LAN1 to WAN Connection and Packet Directions

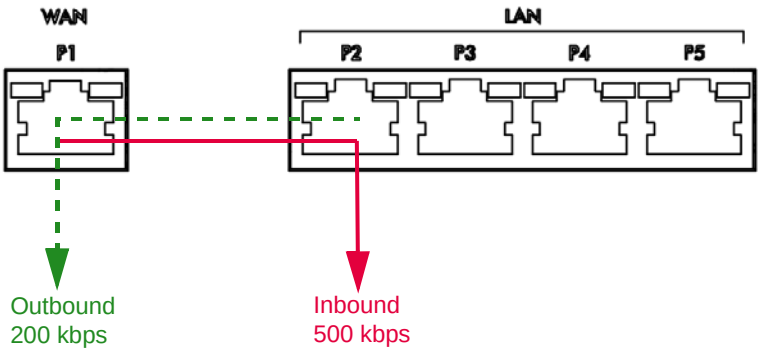



## Outbound and Inbound Bandwidth Limits

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 kbs. The connection initiator is on the LAN1 so inbound means the traffic traveling from the WAN to the LAN1.

**Figure 258** 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.

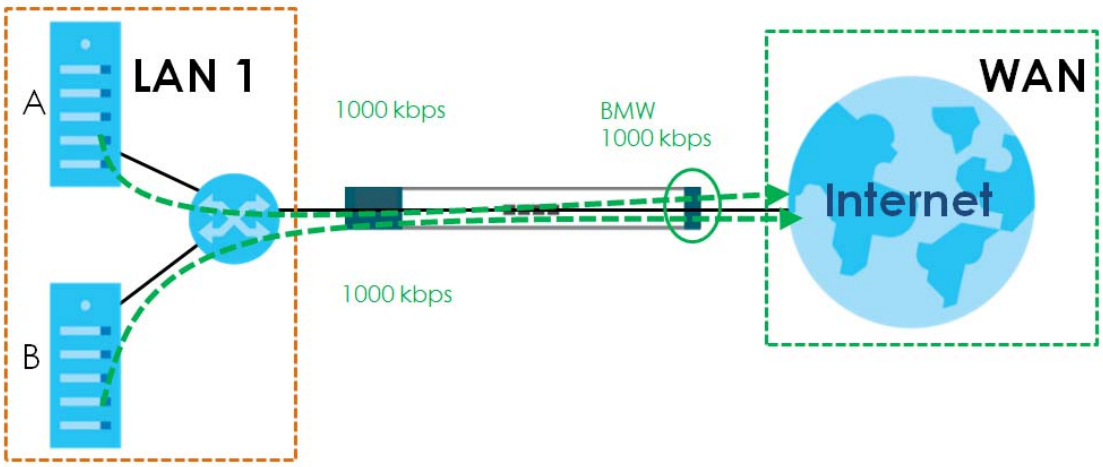
After each application gets its configured bandwidth rate, the UAG uses the fairness- based scheduler to divide any unused bandwidth on the out-going interface amongst applications that need more bandwidth and have maximize bandwidth usage enabled.

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 259** 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 165 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 166 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 167 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 168 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 220 for a description of DSCP marking.

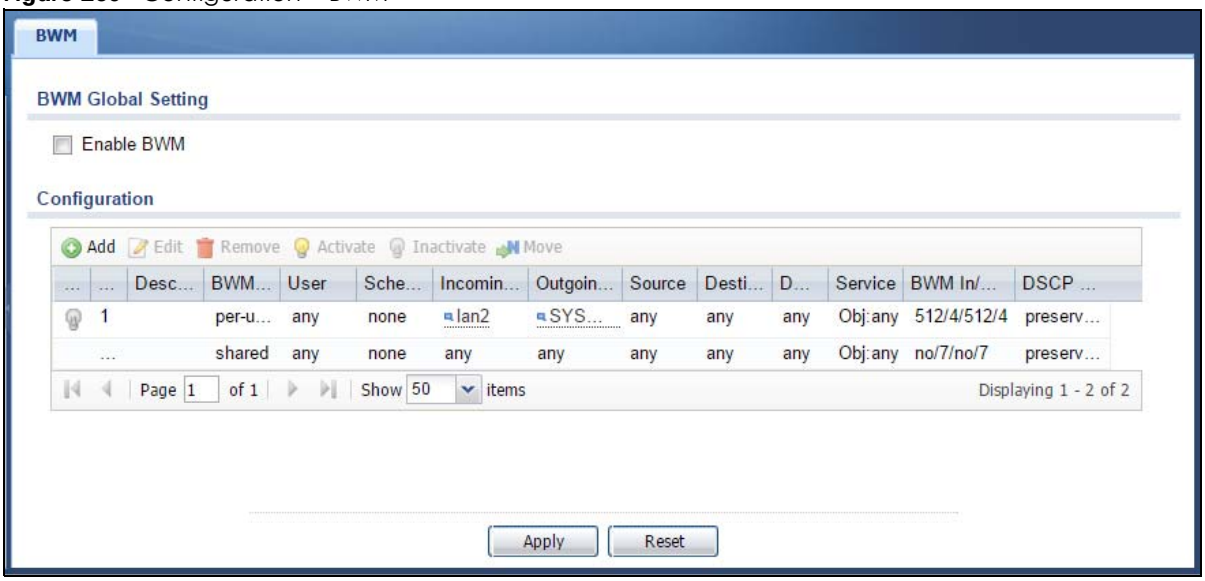
## 30.2 The Bandwidth Management Screen

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 260** Configuration > BWM




The following table describes the labels in this screen. See Section 30.2.1 on page 381 for more information as well.

Table 169 Configuration > BWM

| LABEL | DESCRIPTION |
|---|---|
| Enable BWM | Select this check box to activate management bandwidth. |
| 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.<br>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. |
| 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. |

Table 169 Configuration > BWM (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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.<br>**any** means all DSCP values or no DSCP marker.<br>**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.<br>**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.<br>**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.<br>**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.<br>**preserve** means the UAG does not modify the DSCP value of the route's packets.<br>**default** means the UAG sets the DSCP value of the route's packets to 0.<br>If this field displays a DSCP value, the UAG applies that DSCP value to the route's packets.<br>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 227 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. |

## 30.2.1 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 30.2 on page 379), and click either the **Add** icon or an **Edit** icon.

**Figure 261** Configuration > BWM > Edit (For the Default Policy)

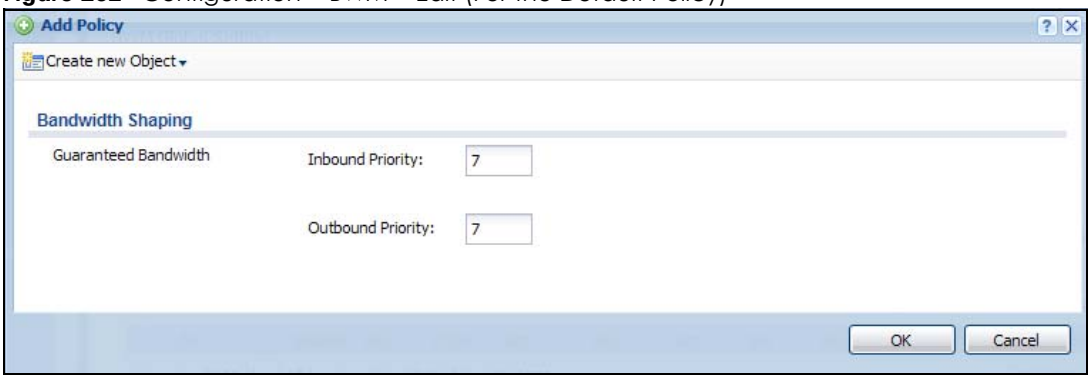
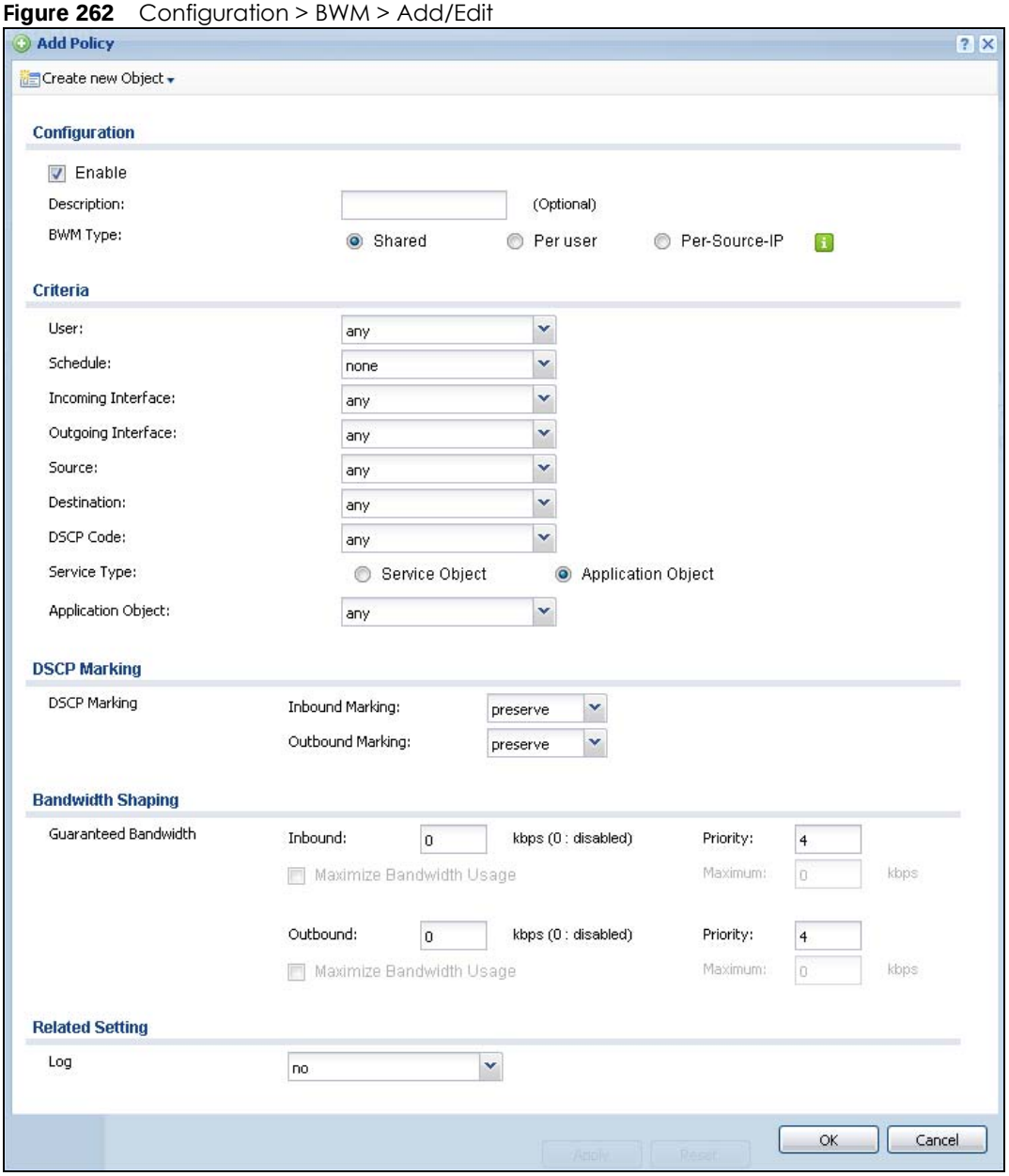



**Figure 262** Configuration > BWM > Add/Edit



The following table describes the labels in this screen.

Table 170 Configuration > BWM > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Create new Object | Use to configure any new settings objects that you need to use in this screen. |
| Configuration | |
| 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.<br>Select **Per user** when the policy is set for an individual user.<br>Select **Per-Source-IP** when the policy is set for an individual source IP. |
| Criteria | |
| 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 40 on page 462 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.<br>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.<br>**any** means all DSCP value or no DSCP marker.<br>**default** means traffic with a DSCP value of 0. This is usually best effort traffic.<br>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 227 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.<br>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.<br>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 170 Configuration > BWM > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Inbound Marking<br><br>Outbound Marking | 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.<br><br>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 227 for more details.<br><br>Select **preserve** to have the UAG keep the packets' original DSCP value.<br><br>Select **default** to have the UAG set the DSCP value of the packets to 0. |
| Bandwidth Shaping | Configure these fields to set the amount of bandwidth the matching traffic can use. |
| Inbound kbps | 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.<br><br>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).<br><br>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. |
| Outbound kbps | 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.<br><br>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).<br><br>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. |
| Priority | 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.<br><br>Traffic with a higher priority is given bandwidth before traffic with a lower priority.<br><br>The UAG uses a fairness-based (round-robin) scheduler to divide bandwidth between traffic flows with the same priority.<br><br>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. |
| Maximize Bandwidth Usage | 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.<br><br>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. |
| 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. |

# CHAPTER 31
# Application Patrol

## 31.1 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.

### 31.1.1 What You Can Do in this Chapter

- Use the **Profile** summary screen (see Section 31.2 on page 386) to view application patrol profiles configured on the UAG.
- Use the **Profile Add/Edit** screens (see Section 31.2.1 on page 387) to set actions for application categories and for specific applications within the category.

### 31.1.2 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.

## 31.2 Application Patrol Profile

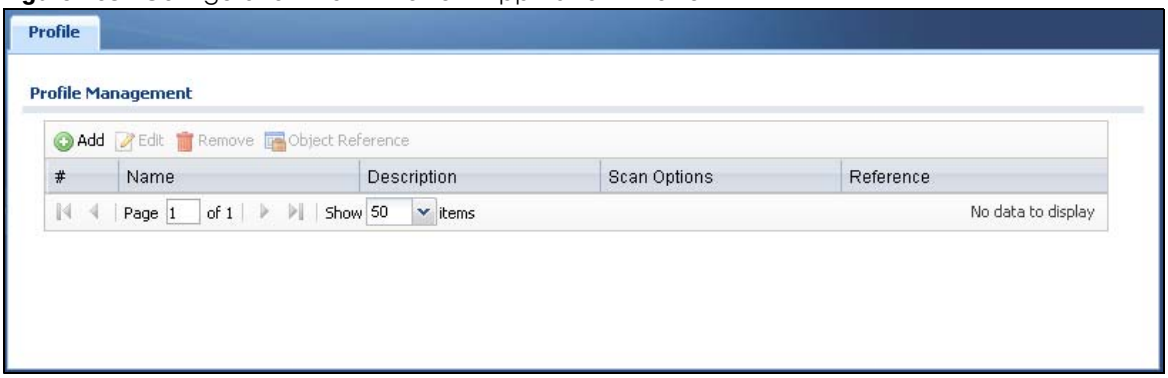
Use the application patrol **Profile** screens to customize action and log settings for a group of application patrol signatures. You then link a profile to a security policy (see Section 24.2 on page 302).

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 263** Configuration > UTM Profile > App Patrol > Profile



The following table describes the labels in this screen.

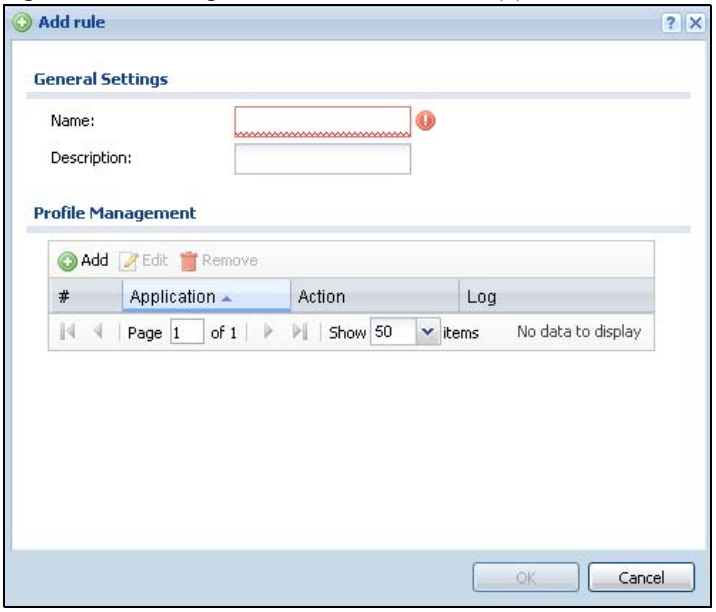
Table 171 Configuration > UTM Profile > App Patrol > Profile

| LABEL | DESCRIPTION |
|---|---|
| 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. |
| 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 Reference**s 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. |

## 31.2.1 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 264** Configuration > UTM Profile > App Patrol > Profile > Add/Edit



The following table describes the labels in this screen.

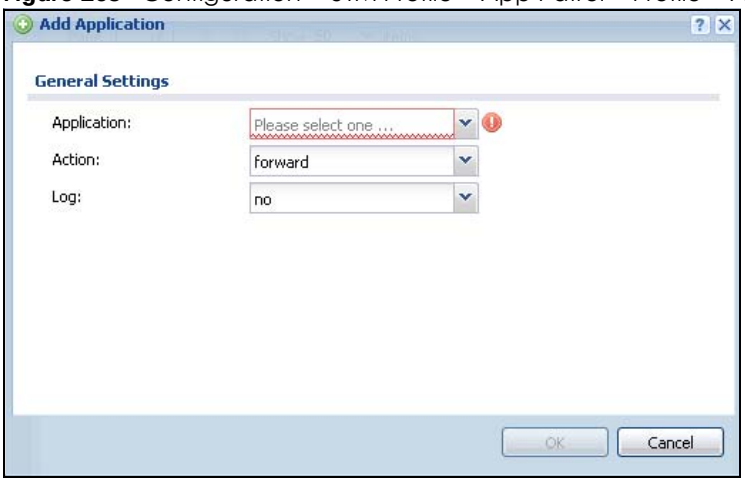
Table 172 Configuration > UTM Profile > App Patrol > Profile > Add/Edit

| 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:<br>• MyProfile<br>• mYProfile<br>• Mymy12_3-4<br>These are invalid profile names:<br>• 1mYProfile<br>• My Profile<br>• MyProfile?<br>• 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. |
| Edit | Select an entry and click **Edit** to change any of the entry's settings. |
| 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.<br>**forward** - the UAG routes packets that matches these signatures.<br>**Drop** - the UAG silently drops packets that matches these signatures without notification.<br>**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, complete the profile and return to the profile summary page. |
| Cancel | Click **Cancel** to return to the profile summary page without saving any changes. |

## 31.2.2 Add/Edit Application Patrol Profile Rule Application

Click **Add** or **Edit** under **Profile Management** in the previous screen to display the following screen.

**Figure 265** Configuration > UTM Profile > App Patrol > Profile > Add/Edit Rule > Add/Edit Application




The following table describes the labels in this screen.

Table 173 Configuration > UTM Profile > App Patrol > Profile > Add/Edit Rule > Add/Edit Application

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Application | Select an application to apply the policy.<br>You must have configured an application object in the **Configuration > Object > Application** screen. |
| Action | Select the default action for all signatures in this category.<br>**forward** - the UAG routes packets that matches these signatures.<br>**Drop** - the UAG silently drops packets that matches these signatures without notification.<br>**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. |

# CHAPTER 32
# Content Filtering

## 32.1 Overview

Use the content filtering feature to control access to specific web sites or web content.

### 32.1.1 What You Can Do in this Chapter

- Use the **Profile** screens (Section 32.2 on page 392) to set up content filtering profiles.
- Use the **Trusted Web Sites** screens (Section 32.3 on page 400) to create a common list of good (allowed) web site addresses.
- Use the **Forbidden Web Sites** screens (Section 32.4 on page 401) to create a common list of bad (blocked) web site addresses.

### 32.1.2 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 32.5 on page 402 for content filtering background/technical information.

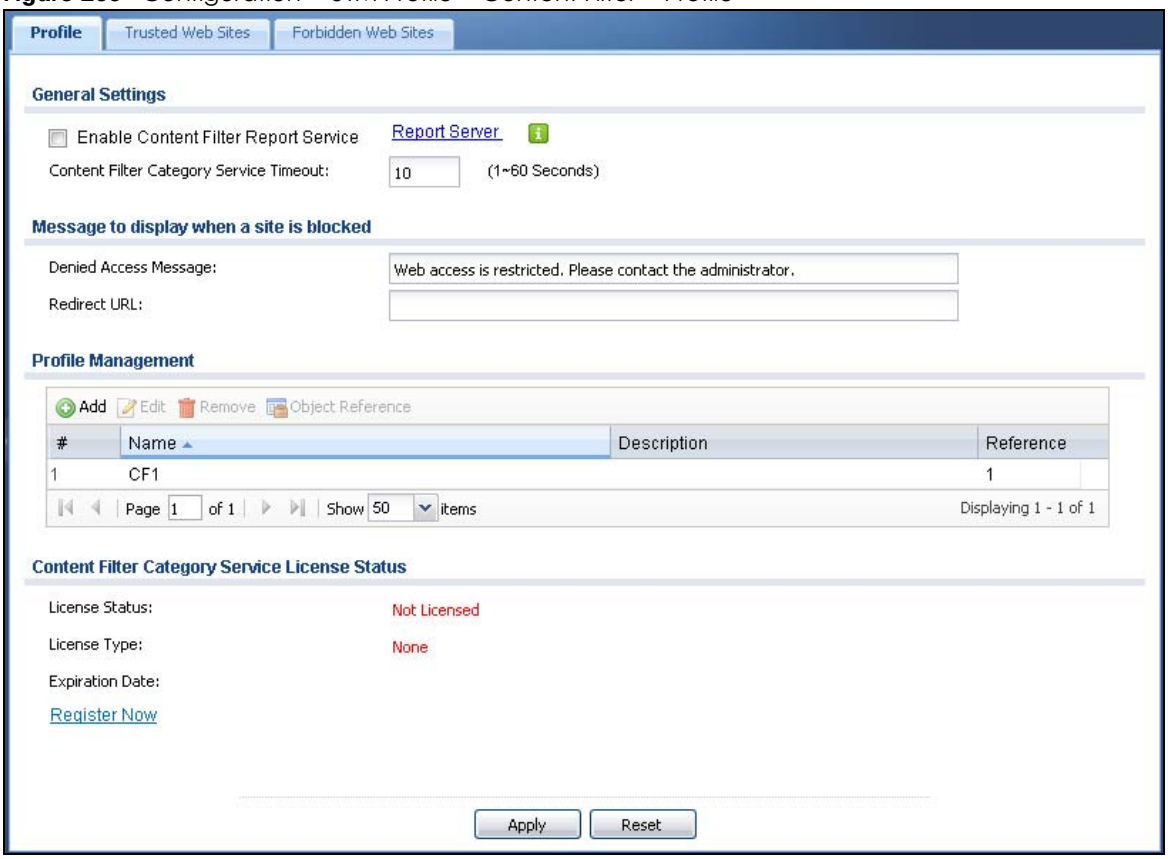
## 32.1.3 Before You Begin

- 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).

# 32.2 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 266** Configuration > UTM Profile > Content Filter > Profile




The following table describes the labels in this screen.

Table 174 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 174 Configuration > UTM Profile > Content Filter > Profile (continued)

| LABEL | DESCRIPTION |
|---|---|
| Denied Access Message | Enter a message to be displayed when content filter blocks access to a web page. Use up to 127 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator".<br><br>It is also possible to leave this field blank if you have a URL specified in the **Redirect URL** field. In this case if the content filter blocks access to a web page, the UAG just opens the web page you specified without showing a denied access message. |
| Redirect URL | Enter the URL of the web page to which you want to send users when their web access is blocked by content filter. The web page you specify here opens in a new frame below the denied access message.<br><br>Use "http://" or "https://" followed by up to 262 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%). For example, http://192.168.1.17/blocked access. |
| 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 the delete a content filter rule. |
| Object Reference | Select an entry and click **Object Reference**s 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 | This read-only field displays the status of your content-filtering database service registration.<br><br>**Not Licensed** displays if you have not successfully registered and activated the service.<br><br>**Expired** displays if your subscription to the service has expired.<br><br>**Licensed** displays if you have successfully registered the UAG and activated the service.<br><br>You can view content filter reports after you register the UAG and activate the subscription service in the **Registration** screen. |
| License Type | This read-only field displays what kind of service registration you have for the content-filtering database.<br><br>**None** displays if you have not successfully registered and activated the service.<br><br>**Standard** displays if you have successfully registered the UAG and activated the service.<br><br>**Trial** displays if you have successfully registered the UAG and activated the trial service subscription. |
| 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. |

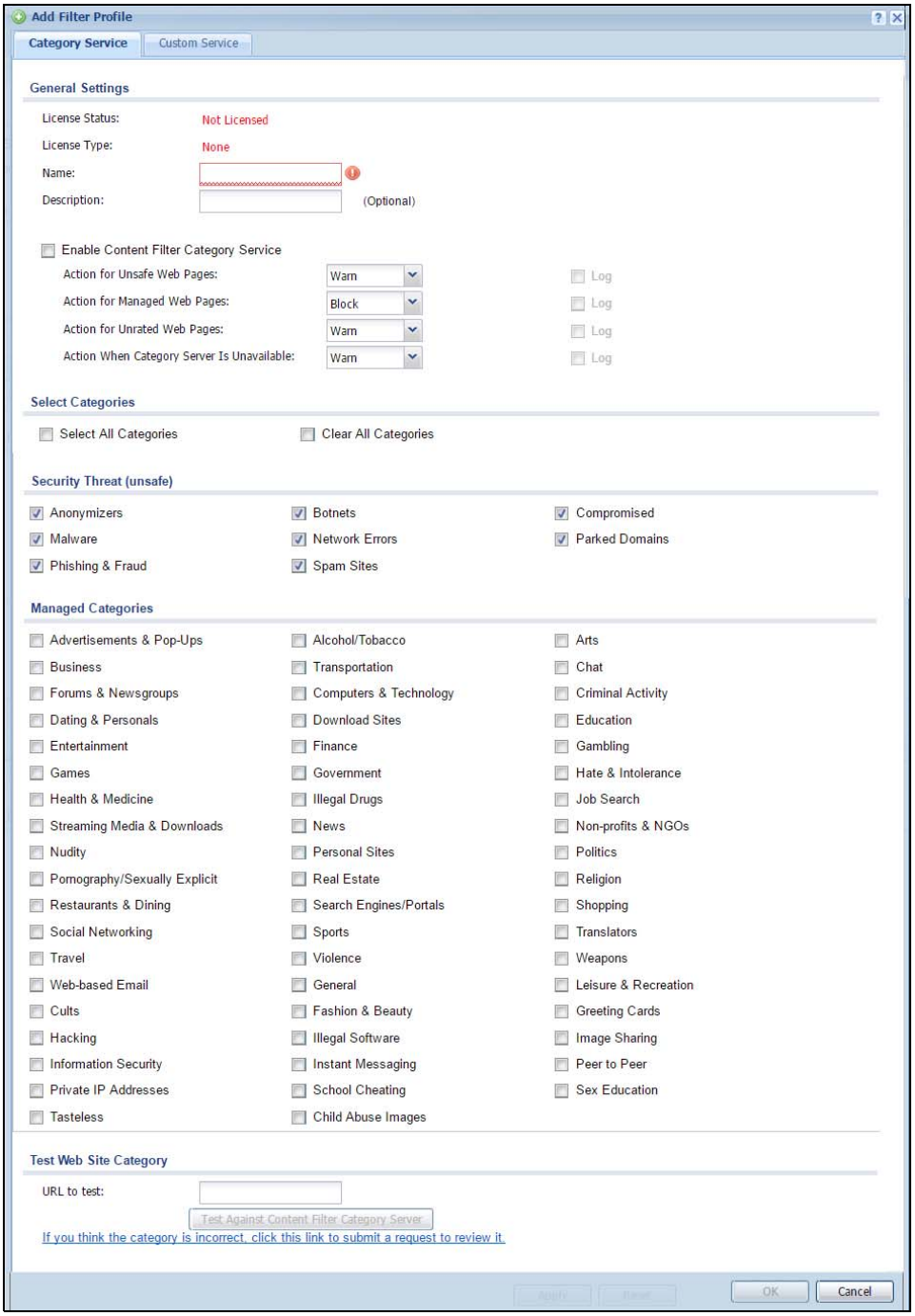
## 32.2.1 Add/Edit Content Filter Profile

Click **Configuration > UTM > Content Filter > Profile > Add/Edit** to open the **Add Filter Profile** screen. Configure **Category Service** and **Custom Service** tabs.

### 32.2.1.1 Category Service

Click the **Category Service** tab.

**Figure 267** Configuration > UTM Profile > Content Filter > Profile > Add/Edit Filter Profile > Category Service



The following table describes the labels in this screen.

Table 175 Configuration > UTM Profile > Content Filter > Profile > Add/Edit Filter Profile > Category Service

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| License Status | This read-only field displays the status of your content-filtering database service registration.<br><br>**Not Licensed** displays if you have not successfully registered and activated the service.<br><br>**Expired** displays if your subscription to the service has expired.<br><br>**Licensed** displays if you have successfully registered the UAG and activated the service.<br><br>You can view content filter reports after you register the UAG and activate the subscription service in the **Registration** screen. |
| License Type | This read-only field displays what kind of service registration you have for the content-filtering database.<br><br>**None** displays if you have not successfully registered and activated the service.<br><br>**Standard** displays if you have successfully registered the UAG and activated the standard content filtering service.<br><br>**Trial** displays if you have successfully registered the UAG and activated the trial service subscription. |
| 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.<br><br>This field is optional. |
| Enable Content Filter Category Service | 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. |
| Action for Unsafe Web Pages | Select **Pass** to allow users to access web pages that match the unsafe categories that you select below.<br><br>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.<br><br>Select **Warn** to display a warning message before allowing users to access web pages that match the unsafe categories that you select below.<br><br>Select **Log** to record attempts to access web pages that match the unsafe categories that you select below. |

Table 175 Configuration > UTM Profile > Content Filter > Profile > Add/Edit Filter Profile > Category Service (continued)

| LABEL | DESCRIPTION |
|---|---|
| Action for Managed Web Pages | Select **Pass** to allow users to access web pages that match the other categories that you select below.<br><br>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.<br><br>Select **Log** to record attempts to access web pages that match the other categories that you select below. |
| Action for Unrated Web Pages | Select **Pass** to allow users to access web pages that the external web filtering service has not categorized.<br><br>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.<br><br>Select **Warn** to display a warning message before allowing users to access web pages that the external web filtering service has not categorized.<br><br>Select **Log** to record attempts to access web pages that are not categorized. |
| Action When Category Server Is Unavailable | Select **Pass** to allow users to access any requested web page if the external content filtering database is unavailable.<br><br>Select **Block** to block access to any requested web page if the external content filtering database is unavailable.<br><br>Select **Warn** to display a warning message before allowing users to access any requested web page if the external content filtering database is unavailable.<br><br>The following are possible causes for the external content filtering server not being available:<br><br>• There is no response from the external content filtering server within the time period specified in the **Content Filter Server Unavailable Timeout** field.<br>• The UAG is not able to resolve the domain name of the external content filtering database.<br>• 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").<br><br>Select **Log** to record attempts to access web pages that occur when the external content filtering database is unavailable. |
| 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) | The categories of web pages that are known to pose a threat to users or their computers are:<br><br>• Anonymizers<br>• Botnets<br>• Compromised<br>• Malware<br>• Network Errors<br>• Parked Domains<br>• Phishing & Fraud<br>• Spam Sites |

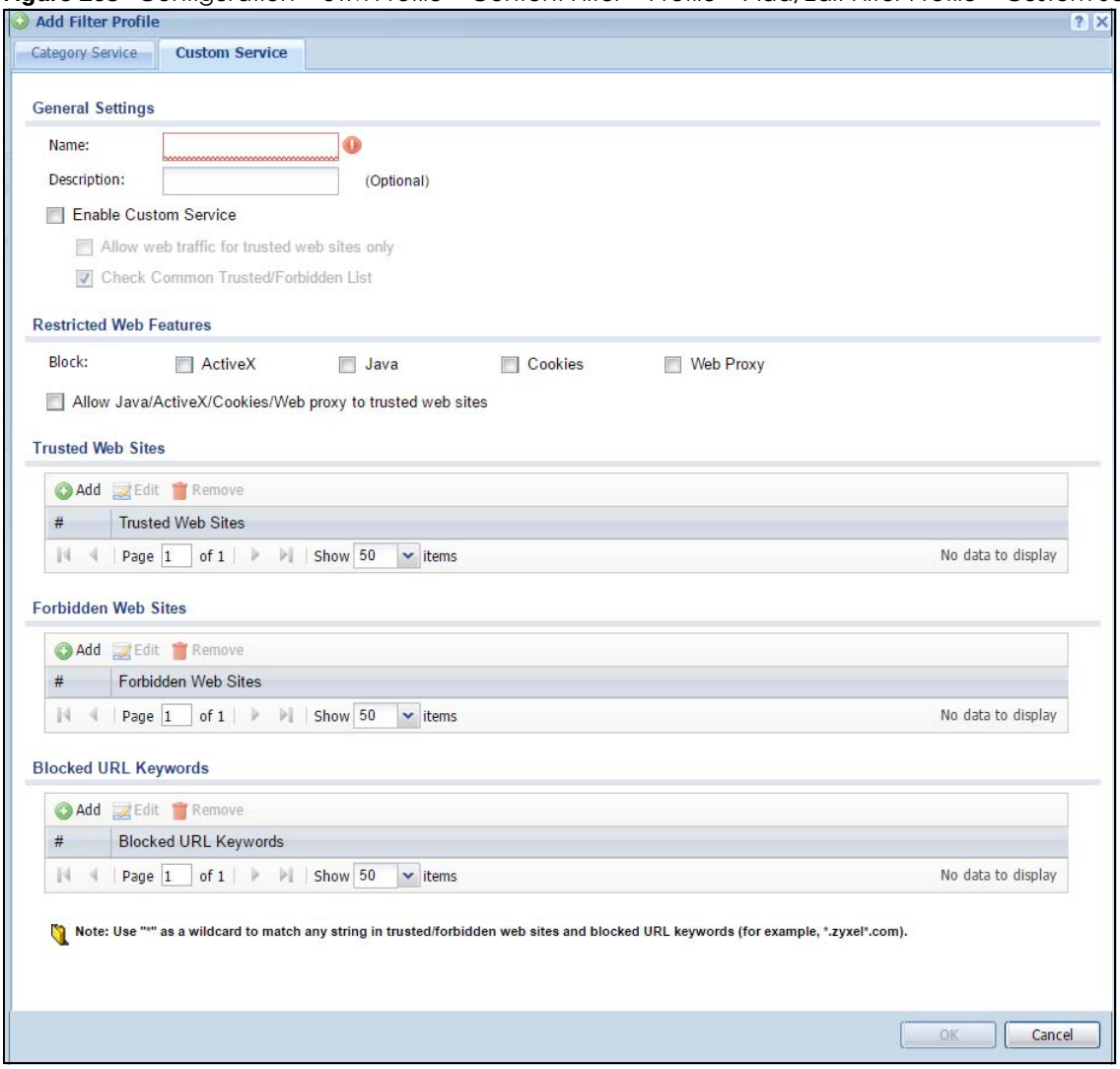
Table 175 Configuration > UTM Profile > Content Filter > Profile > Add/Edit Filter Profile > Category Service (continued)

| 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.<br>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.<br>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. |

### 32.2.1.2 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 268** Configuration > UTM Profile > Content Filter > Profile > Add/Edit Filter Profile > Custom Service




The following table describes the labels in this screen.

Table 176 Configuration > UTM Profile > Content Filter > Profile > Add/Edit Filter Profile > Custom Service

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| 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.<br><br>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. |

Table 176 Configuration > UTM Profile > Content Filter > Profile > Add/Edit Filter Profile > Custom Service

| LABEL | DESCRIPTION |
|---|---|
| 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. |
| Check Common Trusted/ Forbidden List | Select this check box to check the common trusted and forbidden web sites lists. See Section 32.3 on page 400 and Section 32.4 on page 401 for information on configuring these lists. |
| Restricted Web Features | Select the check box(es) to restrict a feature. Select the check box(es) to restrict a feature.<br>• When you download a page containing ActiveX or Java, that part of the web page will be blocked with an X.<br>• When you download a page coming from a Web Proxy, the whole web page will be blocked.<br>• When you download a page containing cookies, the cookies will be removed, but the page will not be blocked. |
| Block<br>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 | This column displays the trusted web sites already added.<br>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.<br>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. |
| 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. |

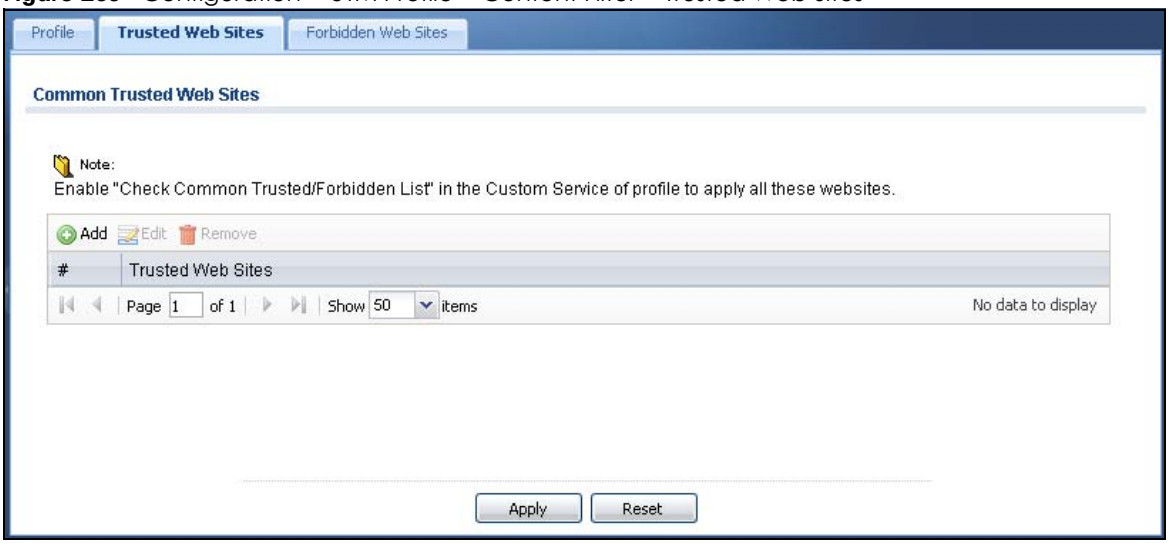
Table 176 Configuration > UTM Profile > Content Filter > Profile > Add/Edit Filter Profile > Custom Service

| LABEL | DESCRIPTION |
|---|---|
| Forbidden Web Sites | This list displays the forbidden web sites already added.<br>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.<br>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. |
| Blocked URL Keywords | This section allows you to block Web sites with URLs that contain certain keywords in the domain name or IP address. |
| 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 blocked URL keywords. |
| Blocked URL Keywords | This list displays the keywords already added.<br>Enter a keyword or a numerical IP address to block. You can also enter a numerical IP address.<br>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.<br>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). |
| OK | Click **OK** to save your changes back to the UAG. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

# 32.3 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 269** Configuration > UTM Profile > Content Filter > Trusted Web Sites




The following table describes the labels in this screen.

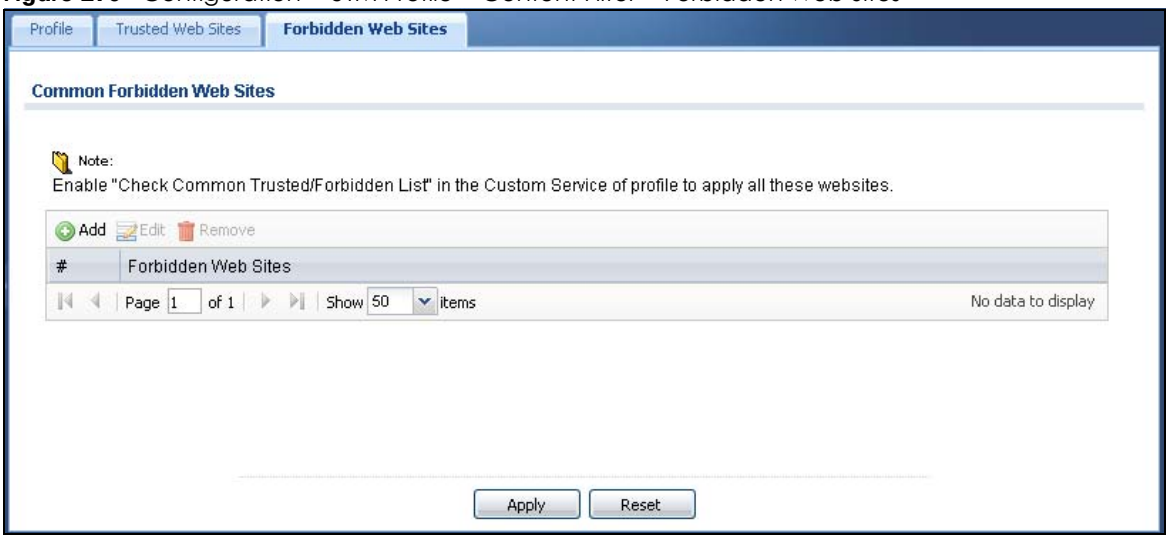
Table 177 Configuration > UTM Profile > Content Filter > Trusted Web Sites

| 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 Sites | This column displays the trusted web sites already added.<br><br>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.<br><br>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. |

# 32.4 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 270** Configuration > UTM Profile > Content Filter > Forbidden Web Sites




The following table describes the labels in this screen.

Table 178 Configuration > UTM Profile > Content Filter > Forbidden Web Sites

| LABEL | DESCRIPTION |
|---|---|
| Common Forbidden Web Sites | 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.<br>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.<br>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. |

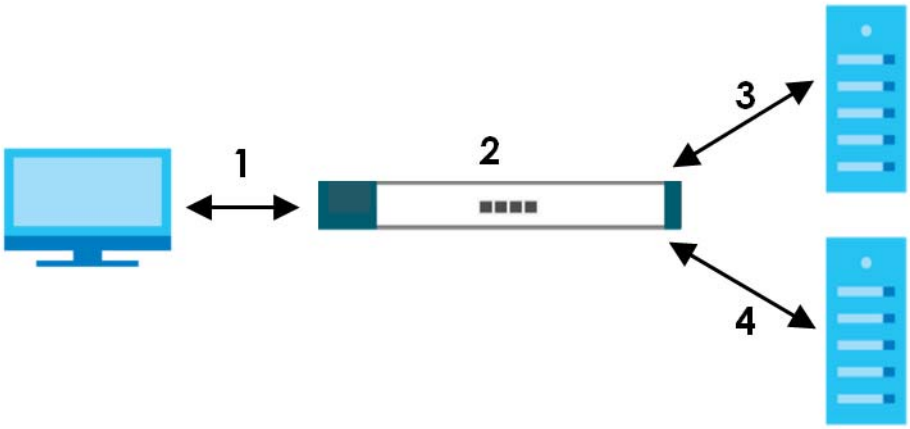
# 32.5 Content Filter Technical Reference

This section provides content filtering background information.

### External Content Filter Server Lookup Procedure

The content filter lookup process is described below.

**Figure 271** 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.

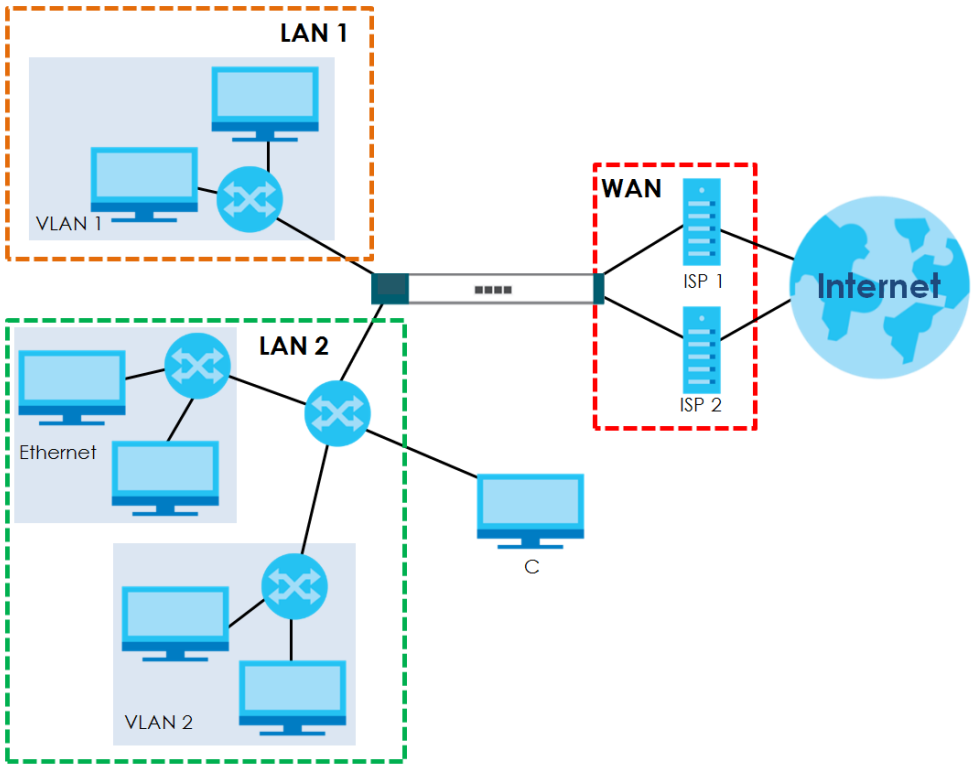
# CHAPTER 33
# Zones

## 33.1 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 272** Example: Zones




### 33.1.1 What You Can Do in this Chapter

Use the **Zone** screens (see Section 33.2 on page 405) to manage the UAG's zones.

### 33.1.2 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 272 on page 404, 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 272 on page 404, traffic between **VLAN1** and the Internet is inter-zone traffic. This is the normal case when zone-based security and policy settings apply.

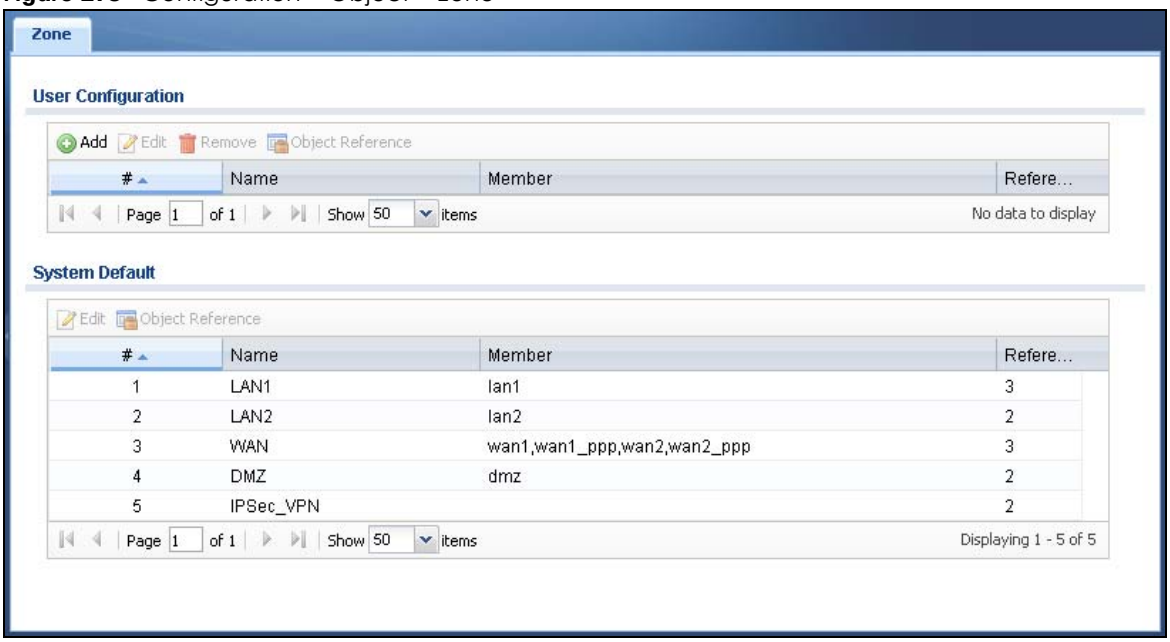
#### Extra-zone Traffic

- Extra-zone traffic is traffic to or from any interface that is not assigned to a zone. For example, in Figure 272 on page 404, 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.

## 33.2 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 273** Configuration > Object > Zone




The following table describes the labels in this screen.

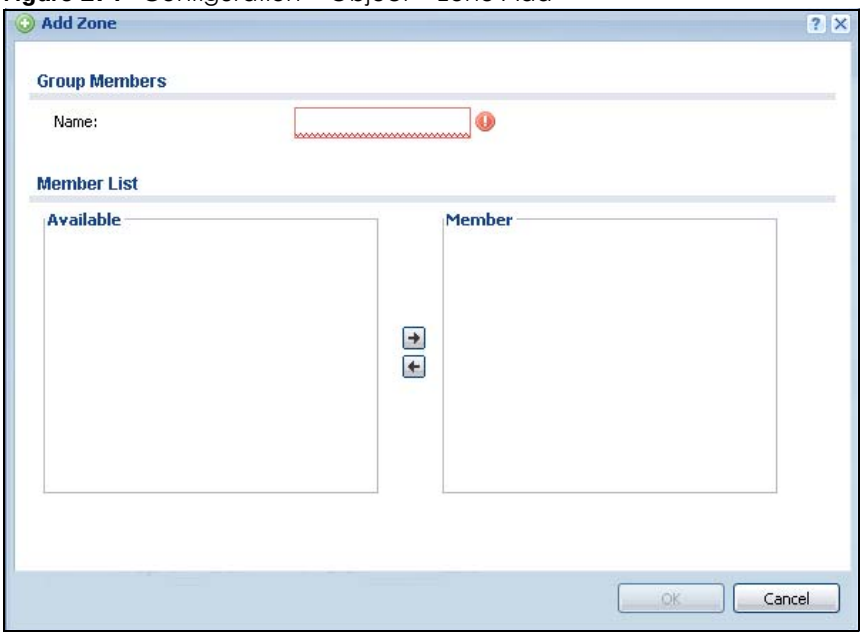
Table 179 Configuration > Object > Zone

| 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 180 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. |

## 33.2.1 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 33.2 on page 405), and click the **Add** icon or an **Edit** icon.

**Figure 274** Configuration > Object > Zone Add




The following table describes the labels in this screen.

Table 180 Configuration > Object > Zone > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Name | For a system default zone, the name is read only.<br>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.<br>**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. |

# CHAPTER 34
# User/Group

## 34.1 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.

### 34.1.1 What You Can Do in this Chapter

- The **User** screen (see Section 34.2 on page 410) provides a summary of all user accounts.
- The **Group** screen (see Section 34.3 on page 414) 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 34.4 on page 415) 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 34.5 on page 420) allows you to configure the MAC addresses of wireless clients for MAC authentication using the local user database.

### 34.1.2 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 181 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)<br>Perform basic diagnostics (CLI) | WWW, TELNET, SSH, Console |
| Access Users | | |
| ext-user | External user account | WWW |
| ext-group-user | External group user account | WWW |
| guest-manager | Create dynamic guest accounts | WWW |

Table 181 Types of User Accounts (continued)

| TYPE | ABILITIES | LOGIN METHOD(S) |
|---|---|---|
| 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 42 on page 473 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 41 on page 468 and Chapter 42 on page 473, 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 181 on page 408) 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 422 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 41.2.1 on page 470 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 34.4.2 on page 419 for a user-aware login example.

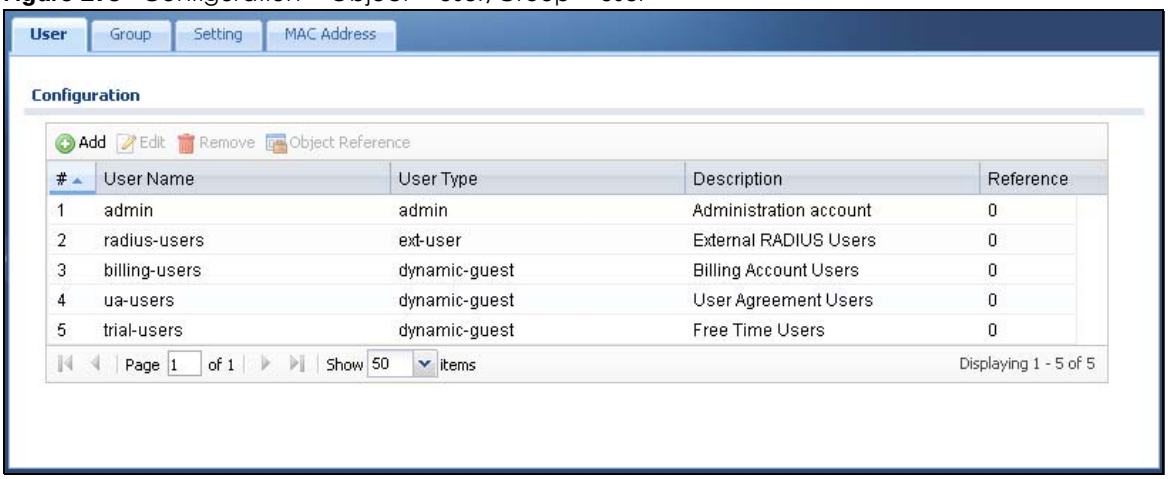
### Finding Out More

- See Section 34.6 on page 421 for some information on users who use an external authentication server in order to log in.

## 34.2 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 275** Configuration > Object > User/Group > User




The following table describes the labels in this screen.

Table 182 Configuration > Object > User/Group > User

| LABEL | DESCRIPTION |
|---|---|
| Configuration | |
| 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 180 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.<br>• **admin** - this user can look at and change the configuration of the UAG<br>• **limited-admin** - this user can look at the configuration of the UAG but not to change it<br>• **dynamic-guest** - this user has access to the UAG's services but cannot look at the configuration.<br>• **ext-user** - this user account is maintained in a remote server, such as RADIUS.<br>• **ext-group-user** - this user account is maintained in a remote server, such as RADIUS.<br>• **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 25.3.1 on page 318 for detailed information about the **Account Generator** screen.<br>• **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. |

## 34.2.1 User Add/Edit Screen

The **User Add/Edit** screen allows you to create a new user account or edit an existing one.

### 34.2.1.1 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]

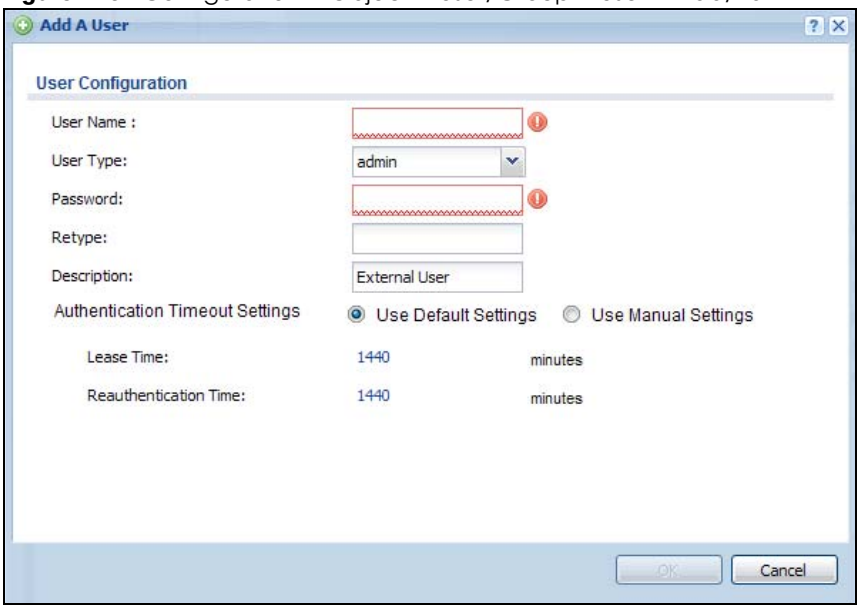
The first character must be alphabetical (A-Z a-z), an underscore (_), or a dash (-). Other limitations on user names are:

- 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 34.2 on page 410), and click either the **Add** icon or an **Edit** icon.

**Figure 276** Configuration > Object > User/Group > User > Add/Edit



The following table describes the labels in this screen.

Table 183 Configuration > Object > User/Group > User > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| User Configuration | |
| 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 34.2.1.1 on page 412. |
| User Type | This field displays the types of user accounts the UAG uses:<br>• **admin** - this user can look at and change the configuration of the UAG<br>• **limited-admin** - this user can look at the configuration of the UAG but not to change it<br>• **ext-user** - this user account is maintained in a remote server, such as RADIUS. See Ext-User Accounts on page 409 for more information about this type.<br>• **ext-group-user** - this user account is maintained in a remote server, such as RADIUS. See Ext-Group-User Accounts on page 409 for more information about this type.<br>• **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 25.3.1 on page 318 for detailed information about the **Account Generator** screen.<br>• **pre-subscriber** - this user has access to the UAG's services but cannot look at the configuration. |
| Password | This field is not available if you select the **ext-user** or **ext-group-user** type.<br>Enter the password of this user account. It can consist of 4 - 31 alphanumeric characters. |
| Retype | This field is not available if you select the **ext-user** or **ext-group-user** type. |
| Group Identifier | This field is available for a **ext-group-user** type user account.<br>Specify the value of the RADIUS server's **Group Membership Attribute** that identifies the group to which this user belongs. |
| 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 | If you select **Use Default Settings** in the **User Settings** field, the default lease time is shown.<br>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 34.4 on page 415), 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. |
| Reauthentication Time | If you select **Use Default Settings** in the **User Settings** field, the default lease time is shown.<br>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. |
| OK | Click **OK** to save your changes back to the UAG. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

# 34.3 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 277** Configuration > Object > User/Group > Group

The following table describes the labels in this screen. See Section 34.3.1 on page 414 for more information as well.

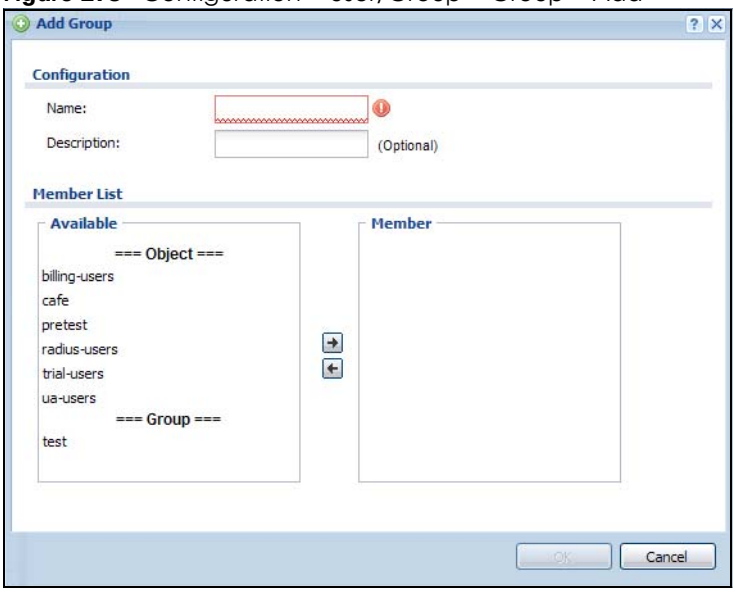
Table 184 Configuration > Object > User/Group > Group

| LABEL | DESCRIPTION |
|---|---|
| Configuration | |
| 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 180 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. |

## 34.3.1 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 34.3 on page 414), and click either the **Add** icon or an **Edit** icon.

**Figure 278** Configuration > User/Group > Group > Add




The following table describes the labels in this screen.

Table 185 Configuration > User/Group > Group > Add

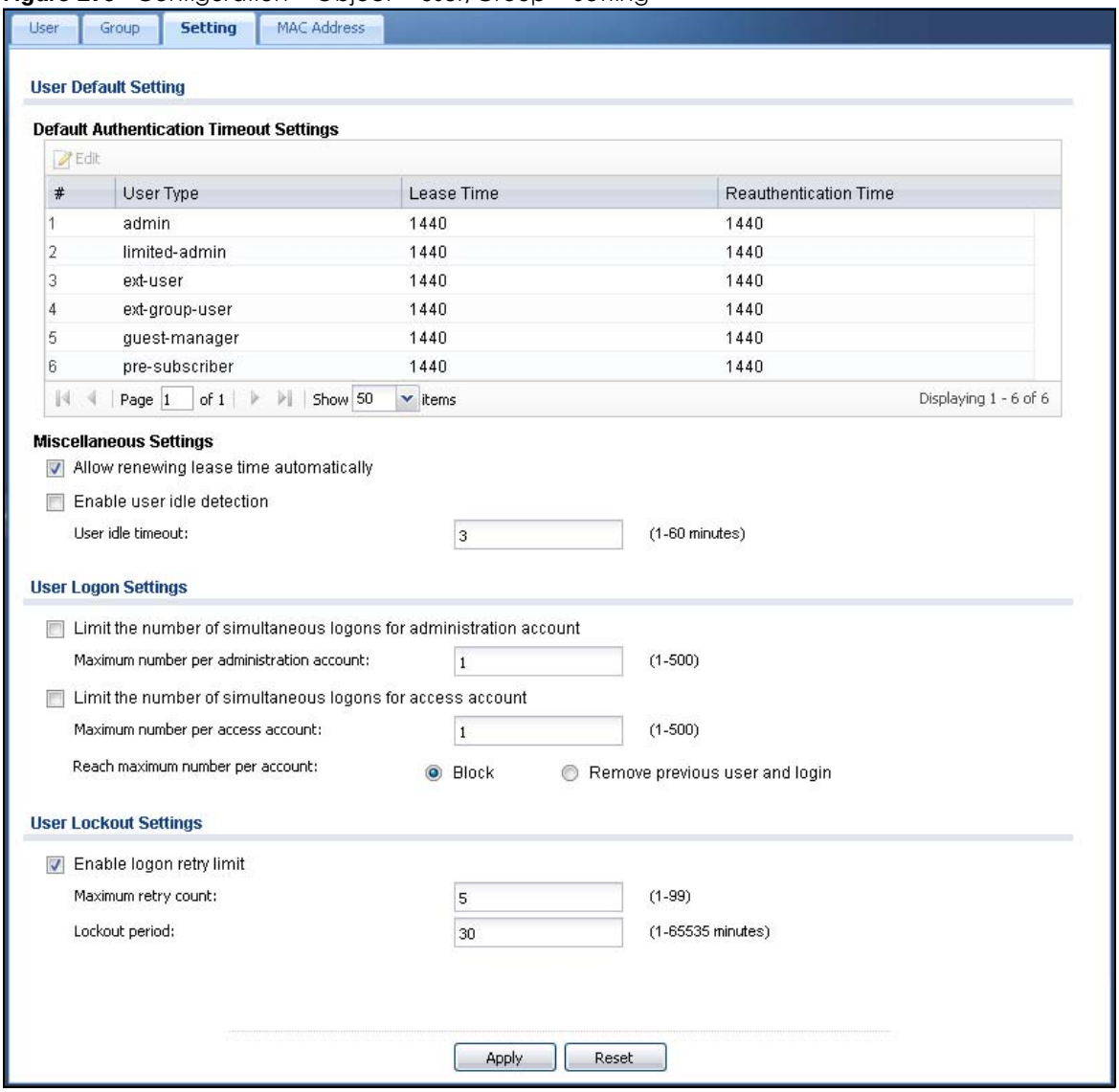
| LABEL | DESCRIPTION |
|---|---|
| Configuration | |
| Name | Type the name for this user group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User group names have to be different than user names. |
| 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.<br><br>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. |

# 34.4 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 279** Configuration > Object > User/Group > Setting




The following table describes the labels in this screen.

Table 186 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 186 Configuration > Object > User/Group > Setting (continued)

| LABEL | DESCRIPTION |
|---|---|
| User Type | These are the kinds of user account the UAG supports.<br>• **admin** - this user can look at and change the configuration of the UAG<br>• **limited-admin** - this user can look at the configuration of the UAG but not to change it<br>• **ext-user** - this user account is maintained in a remote server, such as RADIUS. See Ext-User Accounts on page 409 for more information about this type.<br>• **ext-group-user** - this user account is maintained in a remote server, such as RADIUS. See Ext-Group-User Accounts on page 409 for more information about this type.<br>• **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.<br>• **pre-subscriber** - this user has access to the UAG's services but cannot look at the configuration. |
| Lease Time | 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.<br>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 34.4 on page 415), 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. |
| Reauthentication Time | 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. |
| Miscellaneous Settings | |
| Allow renewing lease time automatically | 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. |
| Enable user idle detection | This is applicable for access users.<br>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. |
| User idle timeout | This is applicable for access users.<br>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. |
| User Logon Settings | |
| Limit number of simultaneous logons for administration account | 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. |
| Maximum number per administration account | 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. |
| Limit number of simultaneous logons for access account | 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. |
| Maximum number per access account | 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. |

Table 186 Configuration > Object > User/Group > Setting (continued)

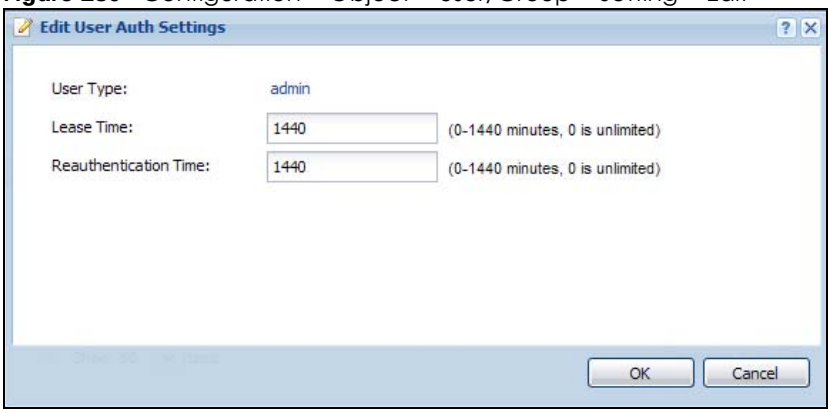
| LABEL | DESCRIPTION |
|---|---|
| Reach maximum number per account | Select **Block** to stop new users from logging in when the **Maximum number per access account** is reached.<br>Select **Remove previous user and login** to disassociate the first user that logged in and allow new user to log in 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. |

## 34.4.1 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 34.4 on page 415), and select one of the **Default Settings** section's entry and click the **Edit** icons.

**Figure 280** Configuration > Object > User/Group > Setting > Edit



The following table describes the labels in this screen.

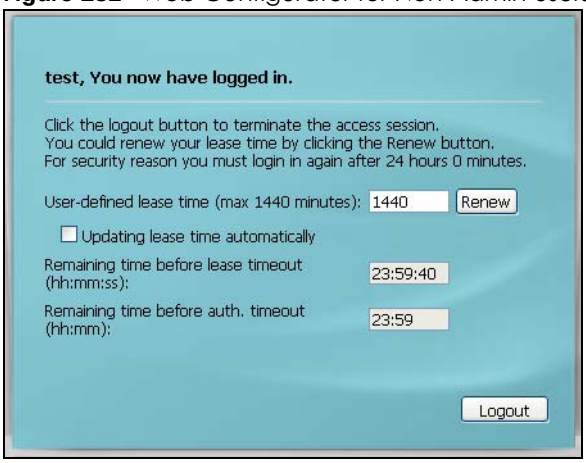
Table 187 Configuration > Object > User/Group > Setting > Edit

| LABEL | DESCRIPTION |
|---|---|
| User Type | This read-only field identifies the type of user account for which you are configuring the default settings.<br>• **admin** - this user can look at and change the configuration of the UAG<br>• **limited-admin** - this user can look at the configuration of the UAG but not to change it.<br>• **ext-user** - this user account is maintained in a remote server, such as RADIUS. See Ext-User Accounts on page 409 for more information about this type.<br>• **ext-group-user** - this user account is maintained in a remote server, such as RADIUS. See Ext-Group-User Accounts on page 409 for more information about this type.<br>• **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.<br>• **pre-subscriber** - this user has access to the UAG's services but cannot look at the configuration. |
| Lease Time | 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.<br>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 34.4 on page 415), 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. |
| Reauthentication Time | 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. |
| OK | Click **OK** to save your changes back to the UAG. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

## 34.4.2 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 281** Web Configurator for Non-Admin Users



The following table describes the labels in this screen.

Table 188 Web Configurator for Non-Admin Users

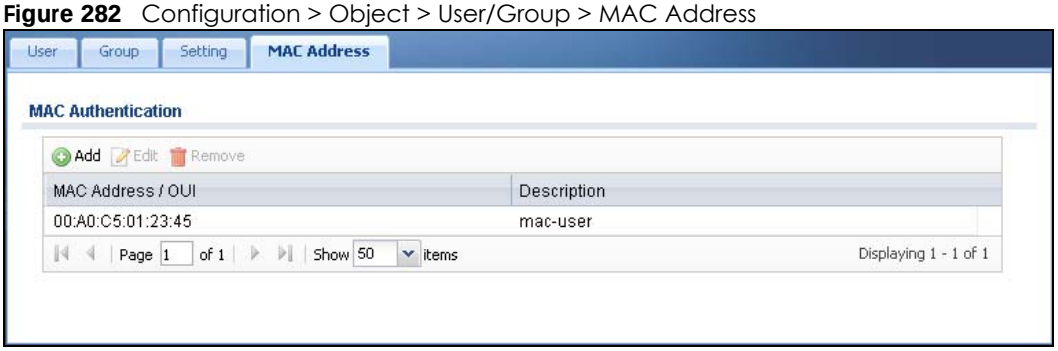
| LABEL | DESCRIPTION |
|---|---|
| User-defined lease time (max ... minutes) | Access users can specify a lease time shorter than or equal to the one that you specified. The default value is the lease time that you specified. |
| Renew | Access users can click this button to reset the lease time, the amount of time remaining before the UAG automatically logs them out. The UAG sets this amount of time according to the<br>• **User-defined lease time** field in this screen.<br>• **Lease time** field in the **User Add/Edit** screen(see Section 34.2.1 on page 411).<br>• **Lease time** field in the **Setting > Edit** screen(see Section 34.4 on page 415). |
| Updating lease time automatically | This box appears if you checked the **Allow renewing lease time automatically** box in the **Setting** screen. (See Section 34.4 on page 415.) 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. |

# 34.5 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 282** Configuration > Object > User/Group > MAC Address




The following table describes the labels in this screen.

Table 189 Configuration > Object > User/Group > MAC Address

| LABEL | DESCRIPTION |
|---|---|
| MAC Authentication | |
| Add | Click this to create a new entry. |

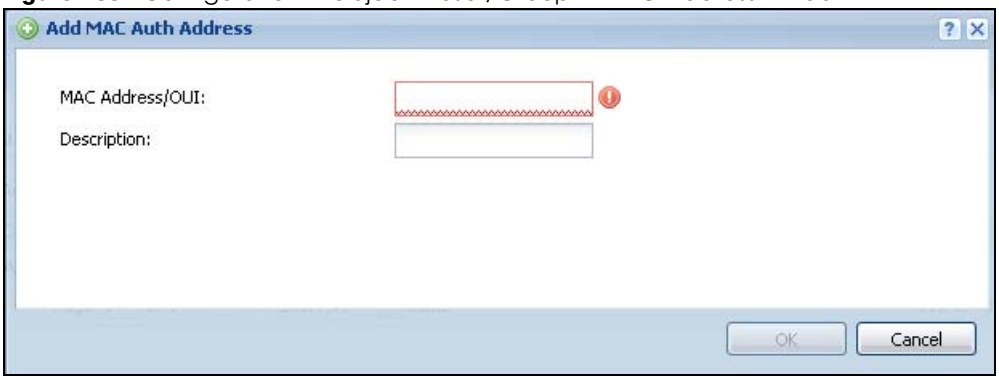
Table 189 Configuration > Object > User/Group > MAC Address (continued)

| 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. |
| # | 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. |

### 34.5.1 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 283** Configuration > Object > User/Group > MAC Address > Add




The following table describes the labels in this screen.

Table 190 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.<br>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. |

## 34.6 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 191 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 284** 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 47 on page 558 for more information about shell scripts.

# CHAPTER 35
# AP Profile

## 35.1 Overview

This chapter shows you how to configure preset profiles for the Access Points (APs) connected to your UAG's wireless network.

### 35.1.1 What You Can Do in this Chapter

- The **Radio** screen (Section 35.2 on page 424) creates radio configurations that can be used by the APs.
- The **SSID** screen (Section 35.3 on page 430) configures three different types of profiles for your networked APs.

### 35.1.2 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.

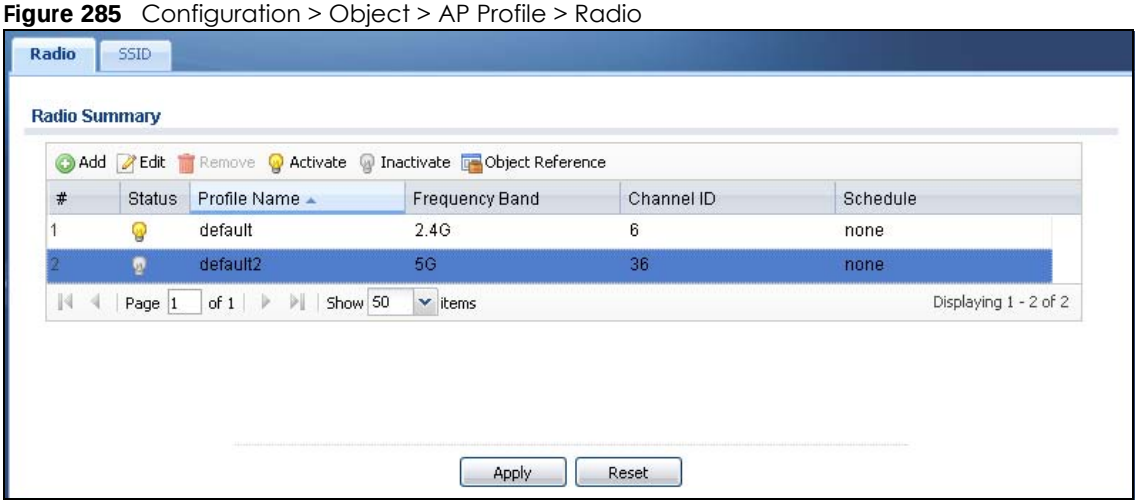
### IEEE 802.1x

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.

## 35.2 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 285** Configuration > Object > AP Profile > Radio




The following table describes the labels in this screen.

Table 192 Configuration > Object > AP Profile > Radio

| LABEL | DESCRIPTION |
|---|---|
| Radio Summary | |
| 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**. |

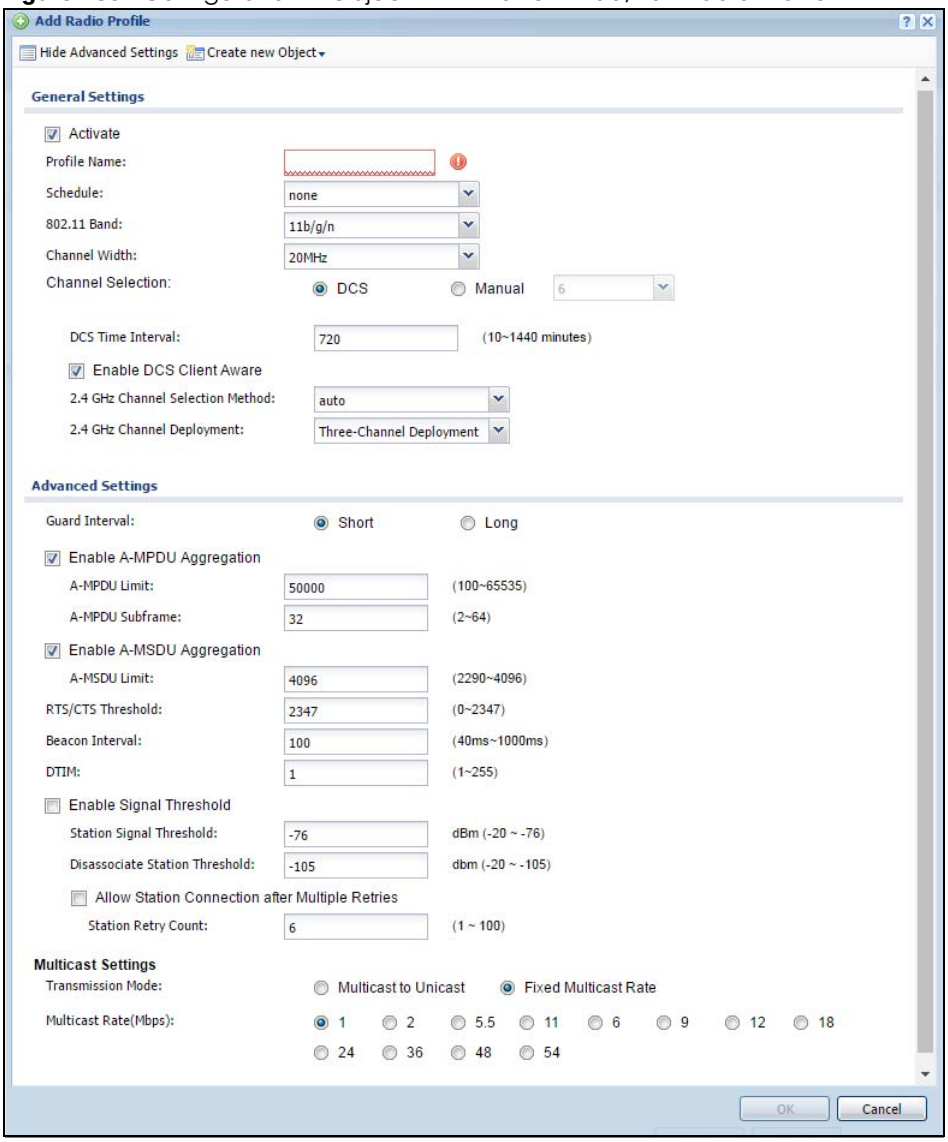
Table 192 Configuration > Object > AP Profile > Radio (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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.<br>**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. |

## 35.2.1 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 286** Configuration > Object > AP Profile > Add/Edit Radio Profile




The following table describes the labels in this screen.

Table 193 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. |

Table 193 Configuration > Object > AP Profile > Add/Edit Radio Profile (continued)

| LABEL | DESCRIPTION |
|---|---|
| Profile Name | Enter up to 31 alphanumeric characters to be used as this profile's name. Underscores are allowed. |
| 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. |
| 802.11 Band | Select how to let wireless clients connect to the AP.<br>**11b/g:** allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the AP. The AP adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices.<br>**11b/g/n:** allows IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the AP. The transmission rate of your AP might be reduced.<br>**11a:** allows only IEEE 802.11a compliant WLAN devices to associate with the AP.<br>**11a/n:** allows both IEEE802.11n and IEEE802.11a compliant WLAN devices to associate with the AP. The transmission rate of your AP might be reduced.<br>**11ac:** allows only IEEE802.11ac compliant WLAN devices to associate with the AP. |
| Channel Width | Select the wireless channel bandwidth you want the AP to use.<br>A standard 20 MHz channel offers transfer speeds of up to 144Mbps (2.4GHz) or 217Mbps (5GHZ) whereas a 40MHz channel uses two standard channels and offers speeds of up to 300Mbps (2.4GHz) or 450Mbps (5GHZ). An IEEE 802.11ac-specific 80MHz channel offers speeds of up to 1.3Gbps.<br>40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. A 80 MHz channel consists of two adjacent 40 MHz channels. The wireless clients must also support 40 MHz or 80 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal.<br>Because not all devices support 40 MHz and/or 80 MHz channels, select **20/40MHz** or **20/40/80MHz** to allow the AP to adjust the channel bandwidth automatically.<br>Select **20MHz** if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding. |
| Channel Selection | Check **Manual** to select the wireless channel which this radio profile should use.<br>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.<br>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.<br>Select **DCS** to have the AP 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.<br>Note: If you change the country code later, **Channel Selection** is set to **Manual** automatically. |
| DCS 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. |

Table 193 Configuration > Object > AP Profile > Add/Edit Radio Profile (continued)

| LABEL | DESCRIPTION |
|---|---|
| Enable DCS Client Aware | Select this to have the AP wait until all connected clients have disconnected before switching channels.<br>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 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.<br>Select **manual** and specify the channels the AP uses in the 2.4 GHz band. |
| 2.4 GHz Channel Deployment | This field is available only when you set **2.4 GHz Channel Selection Method** to **auto**.<br>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.<br>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. |
| Enable 5GHz DFS Aware | This field is available only when you select **11a**, **11a/n** or **11ac** in the **802.11 Band** field and set **5 GHz Channel Selection Method** to **auto**. |
| 5GHz Channel Selection Method | Select **auto** to have the AP search for available channels automatically in the 5 GHz band.<br>Select **manual** and specify the channels the AP uses in the 5 GHz band. |
| Advanced Settings | |
| Guard Interval | Set the guard interval for this radio profile to either **short** or **long**.<br>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.<br>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. |
| 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.<br>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. |

Table 193 Configuration > Object > AP Profile > Add/Edit Radio Profile (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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).<br>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. |
| 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.<br>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.<br>-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.<br>-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 |
| Multicast Settings | Use this section to set a transmission mode and maximum rate for multicast traffic. |
| Transmission Mode | Set how the AP handles multicast traffic.<br>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.<br>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. |
| 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 and 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. |

Table 193 Configuration > Object > AP Profile > Add/Edit Radio 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. |

# 35.3 SSID Screen

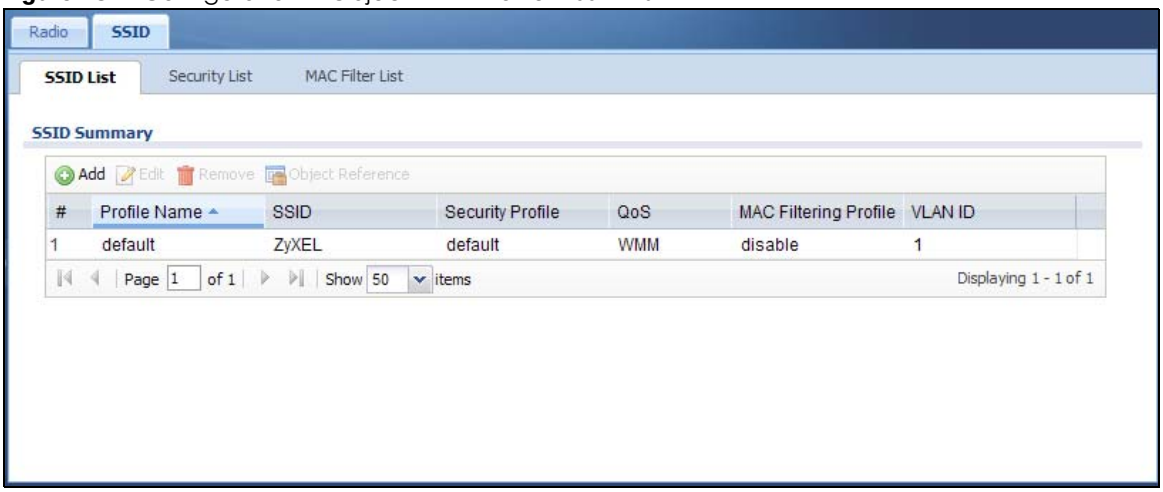
The SSID screens allow you to configure three different types of profiles for your networked APs: an SSID list, which can assign specific SSID configurations to your APs; a security list, which can assign specific encryption methods to the APs when allowing wireless clients to connect to them; and a MAC filter list, which can limit connections to an AP based on wireless clients MAC addresses.

## 35.3.1 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 287** Configuration > Object > AP Profile > SSID List




The following table describes the labels in this screen.

Table 194 Configuration > Object > AP Profile > SSID List

| LABEL | DESCRIPTION |
|---|---|
| SSID Summary | |
| 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). |

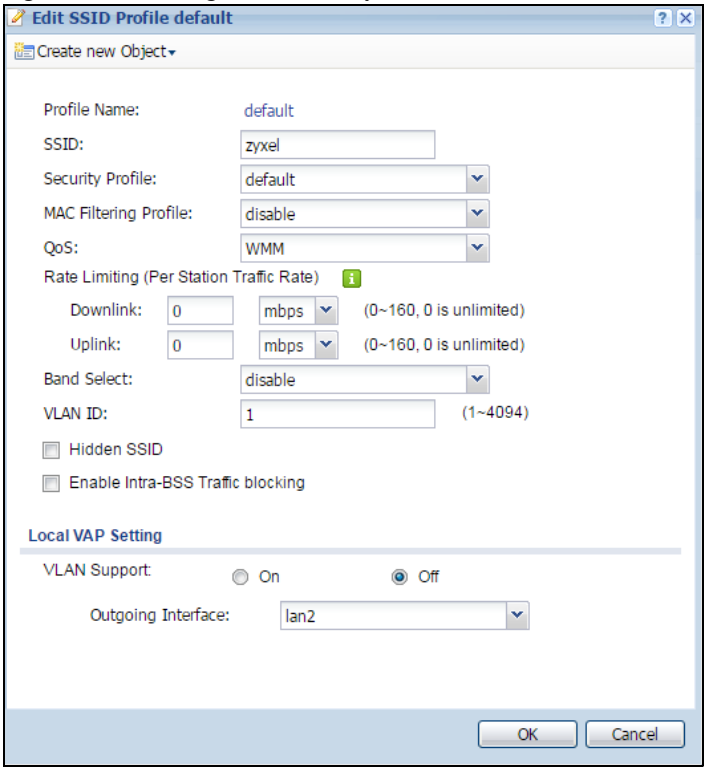
Table 194 Configuration > Object > AP Profile > SSID List (continued)

| LABEL | DESCRIPTION |
|---|---|
| # | 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. |

## 35.3.2 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 288** Configuration > Object > AP Profile > SSID List: Add/Edit SSID Profile




The following table describes the labels in this screen.

Table 195 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. |

Table 195 Configuration > Object > AP Profile > SSID List: Add/Edit SSID Profile (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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.<br><br>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.<br><br>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.<br><br>The **disable** setting means no MAC filtering is used. |
| QoS | 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.<br><br>QoS access categories are as follows:<br><br>**disable**: Turns off QoS for this SSID. All data packets are treated equally and not tagged with access categories.<br><br>**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.<br><br>**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.<br><br>**WMM_VIDEO**: All wireless traffic to the SSID is tagged as video data. This is recommended for activities like video conferencing.<br><br>**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.<br><br>**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. |
| 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 | 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.<br><br>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.<br><br>Otherwise, select **disable** to turn off this feature. |
| 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. |

Table 195 Configuration > Object > AP Profile > SSID List: Add/Edit SSID Profile (continued)

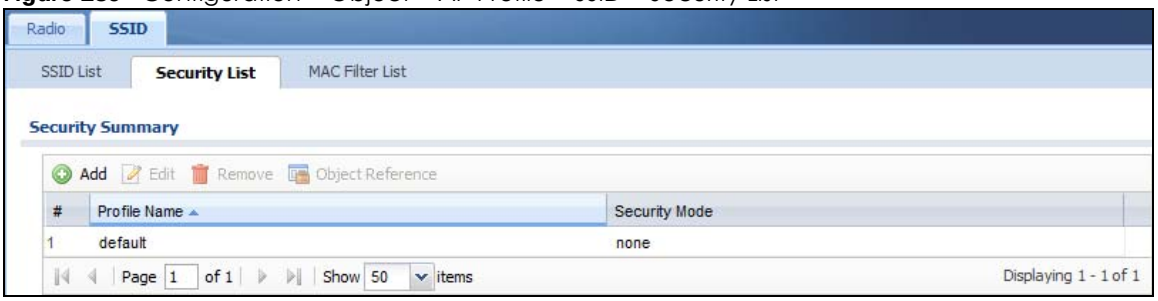
| LABEL | DESCRIPTION |
|---|---|
| Hidden SSID | Select this if you want to "hide" your SSID from wireless clients. This tells any wireless clients in the vicinity of the AP using this SSID profile not to display its SSID name as a potential connection. Not all wireless clients respect this flag and display it anyway.<br><br>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). |
| 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 Virtual AP (VAP). The VAP is the UAG's built-in wireless LAN module. |
| VLAN Support | Select **ON** to tag traffic from the selected outgoing interface of the local Virtual AP (VAP) with the VLAN ID specified in this SSID profile. Otherwise, select **Off**. |
| OK | Click **OK** to save your changes back to the UAG. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

## 35.3.3 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 289** Configuration > Object > AP Profile > SSID > Security List




The following table describes the labels in this screen.

Table 196 Configuration > Object > AP Profile > SSID > Security List

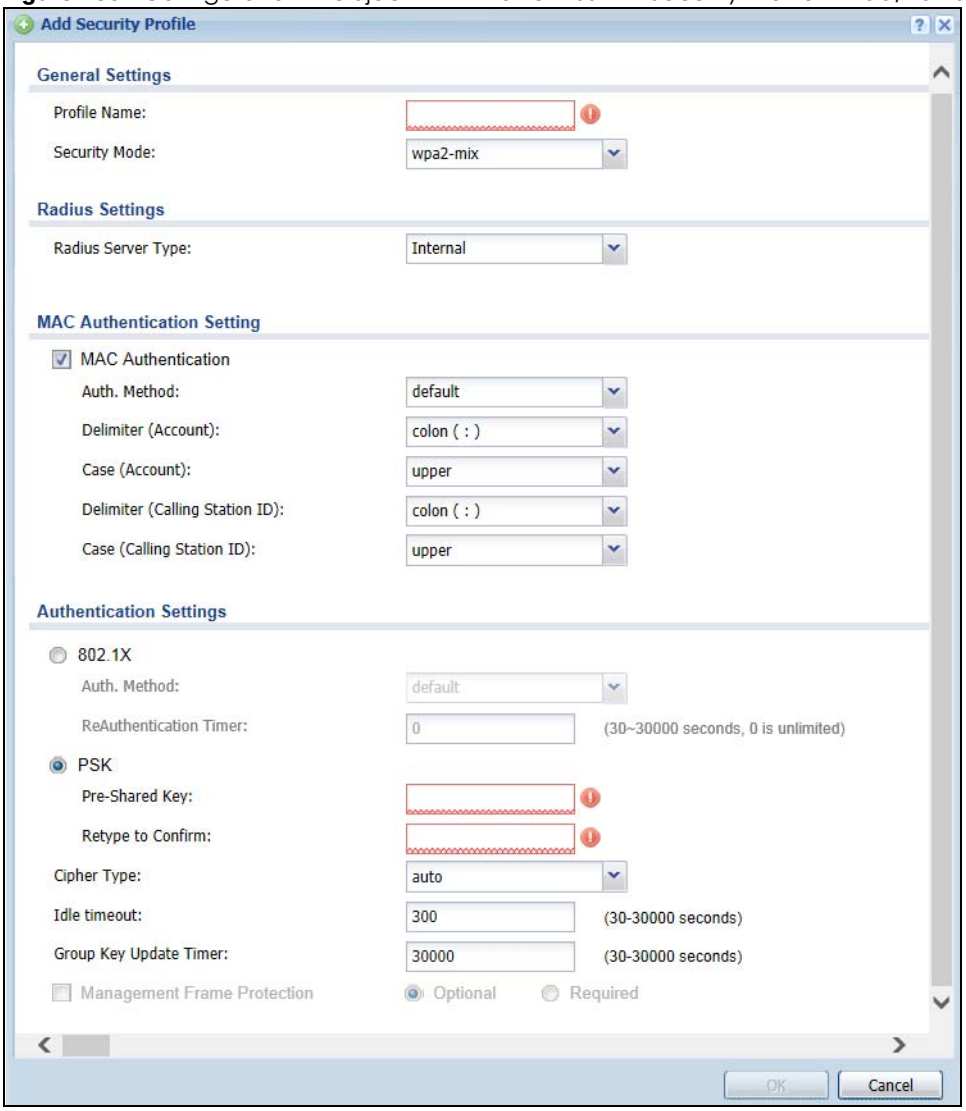
| LABEL | DESCRIPTION |
|---|---|
| Security Summary | |
| Add | Click this to add a new security profile. |
| Edit | Click this to edit the selected security profile. |
| Remove | Click this to remove the selected security profile. |
| Object Reference | Click this to view which other objects are linked 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). |

## 35.3.4 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 290** Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile




The following table describes the labels in this screen.

Table 197 Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| 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 197 Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile

| LABEL | DESCRIPTION |
|---|---|
| Radius Settings | |
| 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 Setting | |
| 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.<br>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**.<br>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.<br>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. |
| Authentication Settings | |
| 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**.<br>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. |

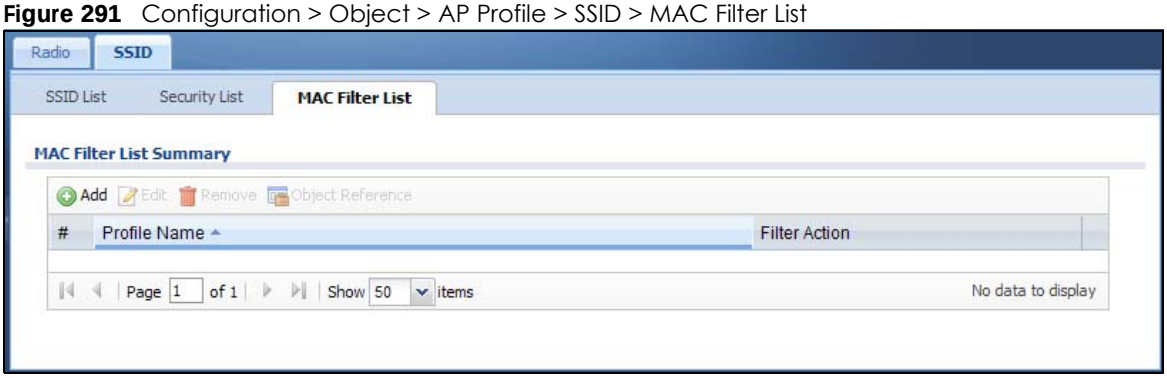
Table 197 Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile

| LABEL | DESCRIPTION |
|---|---|
| Key Length | Select the bit-length of the encryption key to be used in WEP connections.<br>If you select **WEP-64**:<br>• Enter 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x11AA22BB33) for each **Key** used.<br>or<br>• Enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for each **Key** used.<br>If you select **WEP-128**:<br>• Enter 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x00112233445566778899AABBCC) for each **Key** used.<br>or<br>• 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. |
| Retype to Confirm | Retype your new password for confirmation. |
| Cipher Type | Select an encryption cipher type from the list.<br>• **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.<br>• **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.<br>• **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 | This field is available only when you set **Security Mode** to **wpa2** or **wpa2-mix** and enable 802.1x authentication.<br>**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. |
| OK | Click **OK** to save your changes back to the UAG. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

## 35.3.5 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 291** Configuration > Object > AP Profile > SSID > MAC Filter List




The following table describes the labels in this screen.

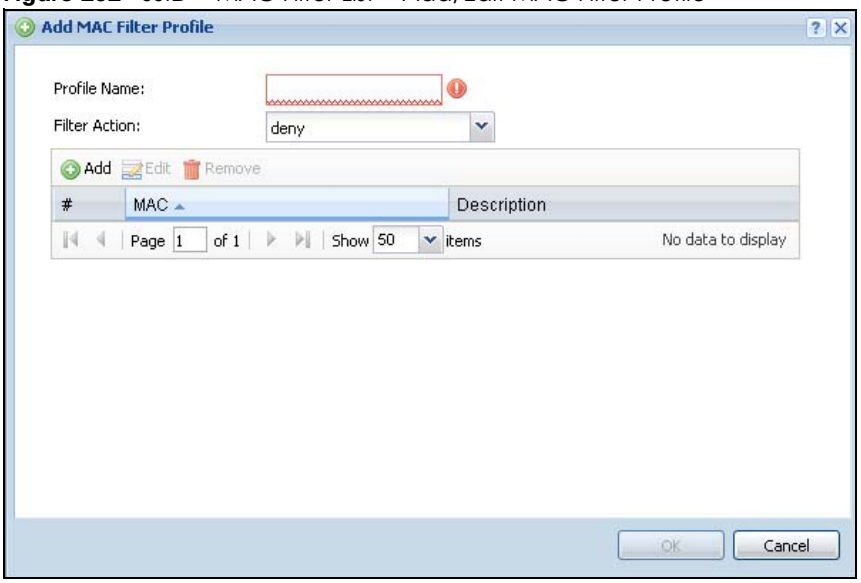
Table 198 Configuration > Object > AP Profile > SSID > MAC Filter List

| LABEL | DESCRIPTION |
|---|---|
| MAC Filter List Summary | |
| 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). |

## 35.3.6 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 292** SSID > MAC Filter List > Add/Edit MAC Filter Profile




The following table describes the labels in this screen.

Table 199 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. |

# CHAPTER 36
# MON Profile

## 36.1 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 160) to classify them as either rogue or friendly and then manage them accordingly.

### 36.1.1 What You Can Do in this Chapter

The **MON Profile** screen (Section 36.2 on page 439) creates preset monitor mode configurations that can be used by the APs.

### 36.1.2 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.

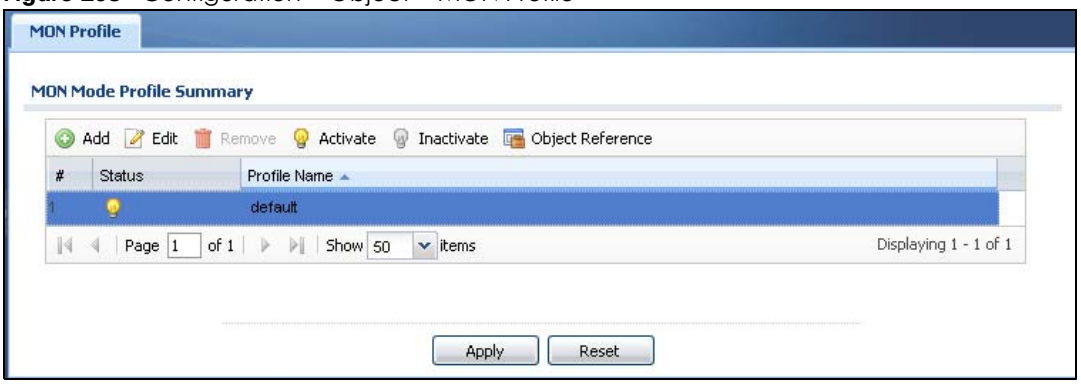
#### Passive Scan

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.

## 36.2 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 293** Configuration > Object > MON Profile




The following table describes the labels in this screen.

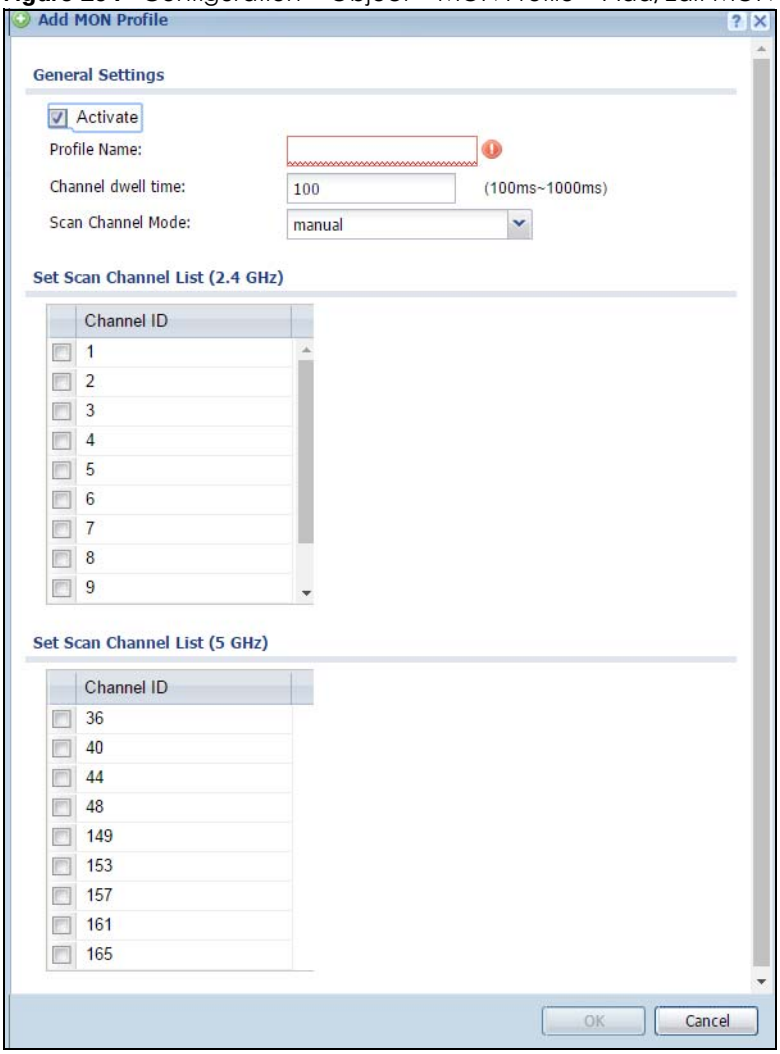
Table 200 Configuration > Object > MON Profile

| LABEL | DESCRIPTION |
|---|---|
| MON Mode Profile Summary | |
| 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. |

## 36.2.1 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 and existing monitor mode profile and click the **Edit** button.

**Figure 294** Configuration > Object > MON Profile > Add/Edit MON Profile




The following table describes the labels in this screen.

Table 201 Configuration > Object > MON Profile > Add/Edit MON Profile

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| 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.<br>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.<br>These channels are limited to the 2 GHz range (802.11 b/g/n). |

Table 201 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.<br>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. |

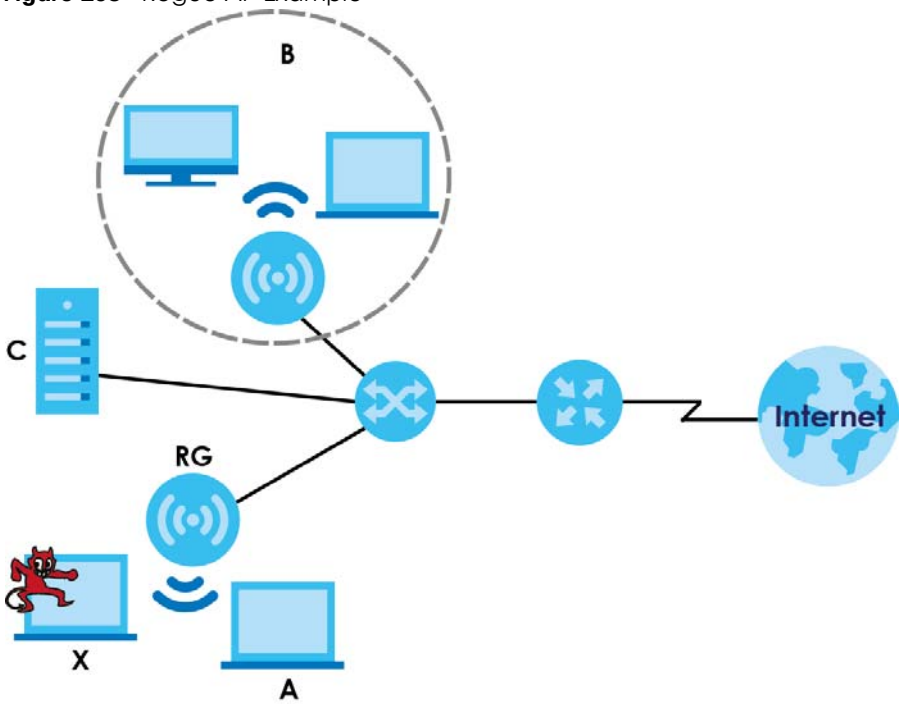
# 36.3 Technical Reference

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 295** 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.

# CHAPTER 37
# Application

## 37.1 Overview

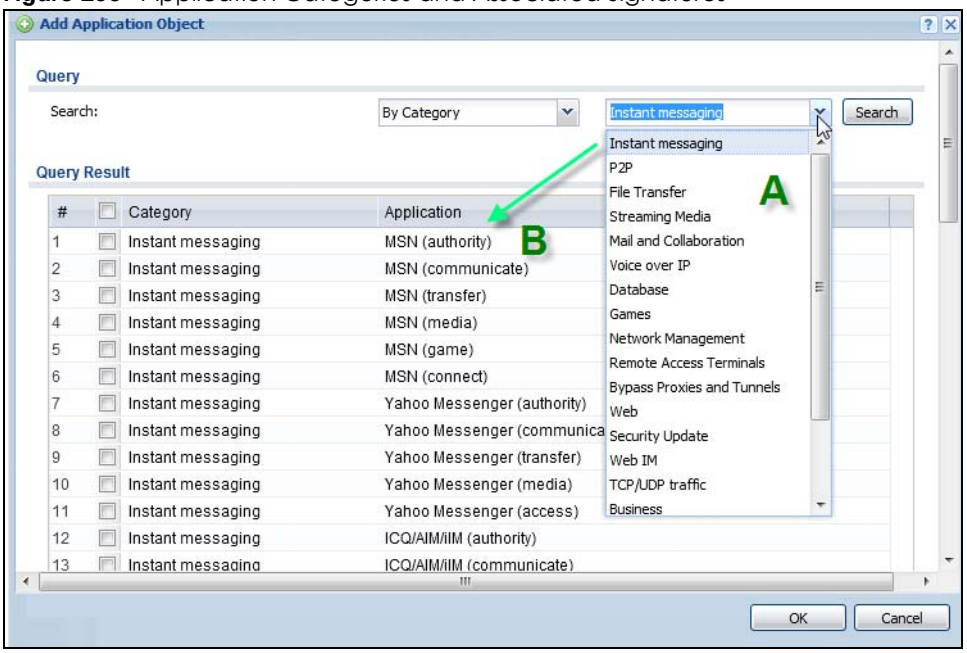
The UAG identifies applications by either their port or signature. Go to **Configuration > Licensing > Signature Update > AppPatrol** to check that you have the latest App Patrol signatures. These signatures are available to create application objects in **Configuration > Object > Application > Application**. Categories of applications include (at the time of writing):

Table 202 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 296** Application Categories and Associated Signatures



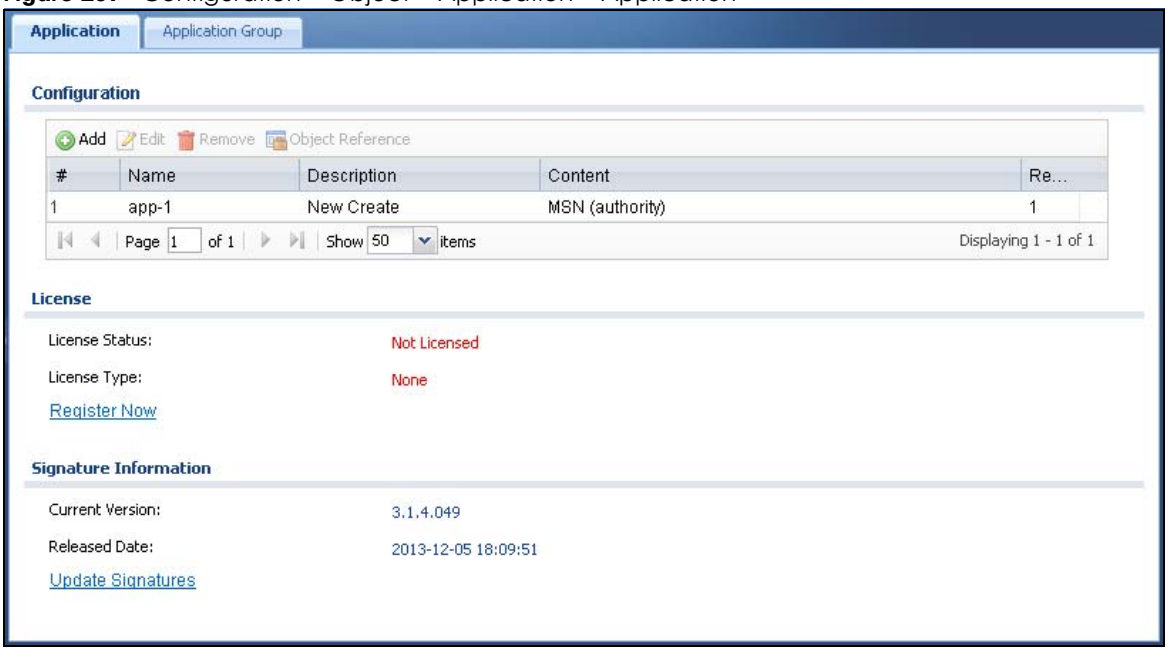
### 37.1.1 What You Can Do in this Chapter

- Use the **Application** screen (Section 37.2 on page 445) to create application objects that can be used in App Patrol profiles.
- Use the **Application Group** screen (Section 37.3 on page 449) to group application objects as an individual object that can be used in App Patrol profiles.

## 37.2 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 297** Configuration > Object > Application > Application




The following table describes the labels in this screen.

Table 203 Configuration > Object > Application > Application

| LABEL | DESCRIPTION |
|---|---|
| Configuration | |
| 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. |

Table 203 Configuration > Object > Application > Application (continued)

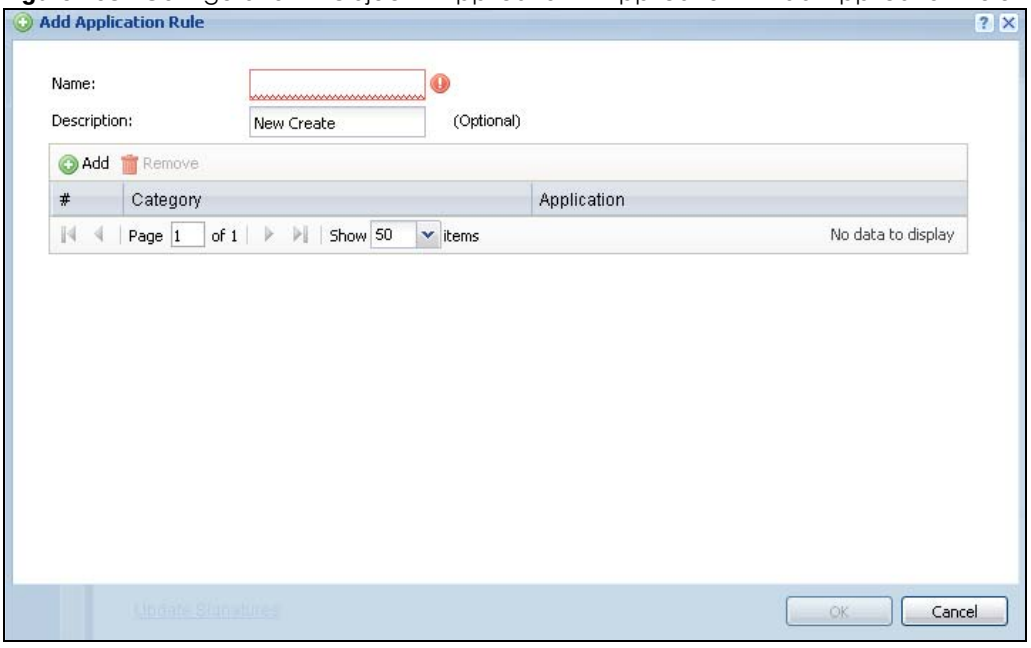
| LABEL | DESCRIPTION |
|---|---|
| Reference | This displays the number of times an object reference is used in a profile. |
| License | You need to buy a license or use a trial license in order to use AppPatrol signatures. These fields show license-related information. |
| License Status | This field shows whether you have activated an AppPatrol signatures license |
| License Type | This field shows the type of AppPatrol signatures license you have activated |
| Register Now | Click the link to go to myZyXEL.com where you can register your UAG and activate the service.<br>This link is available only when the service is not activated yet. |
| 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. |

## 37.2.1 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 298** Configuration > Object > Application > Application > Add Application Rule



The following table describes the labels in this screen.

Table 204 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. |

### 37.2.1.1 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 299** Configuration > Object > Application > Application > Add Application Rule > Add By Category

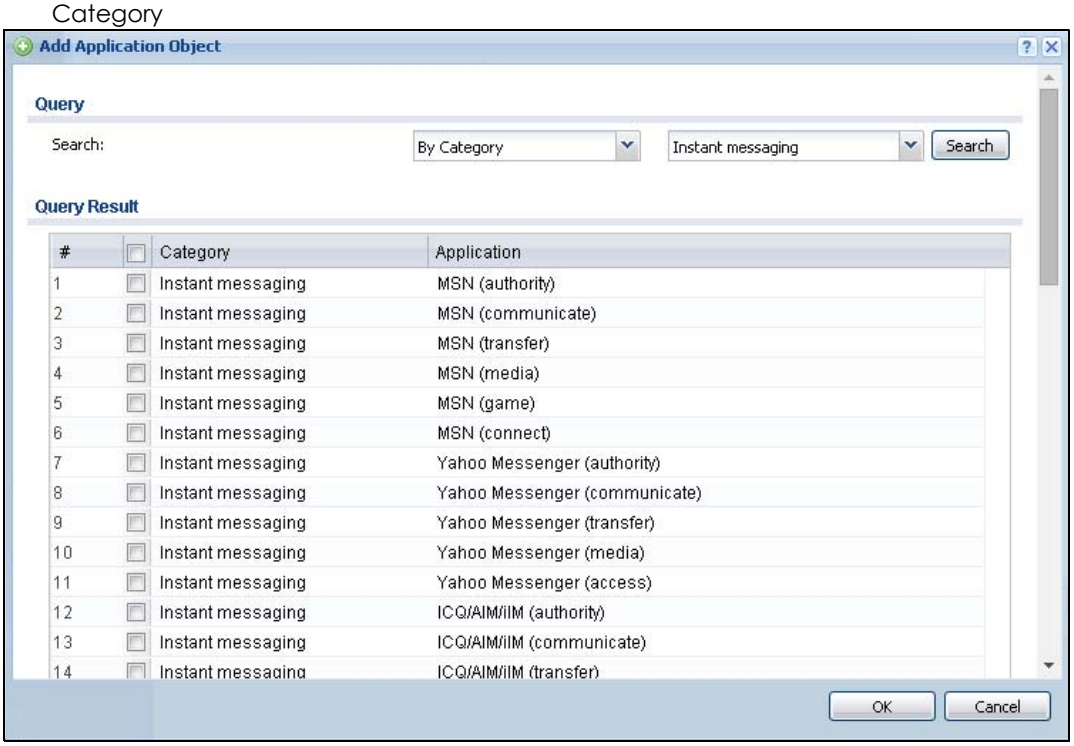
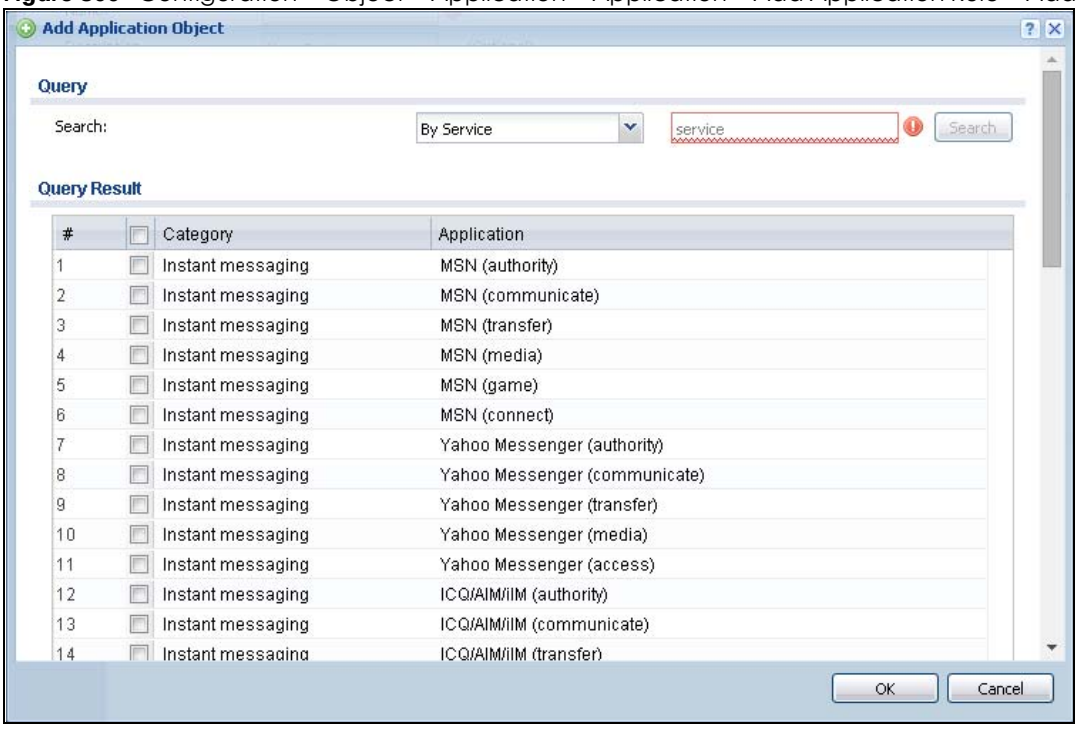


**Figure 300** Configuration > Object > Application > Application > Add Application Rule > Add By Service




The following table describes the labels in this screen.

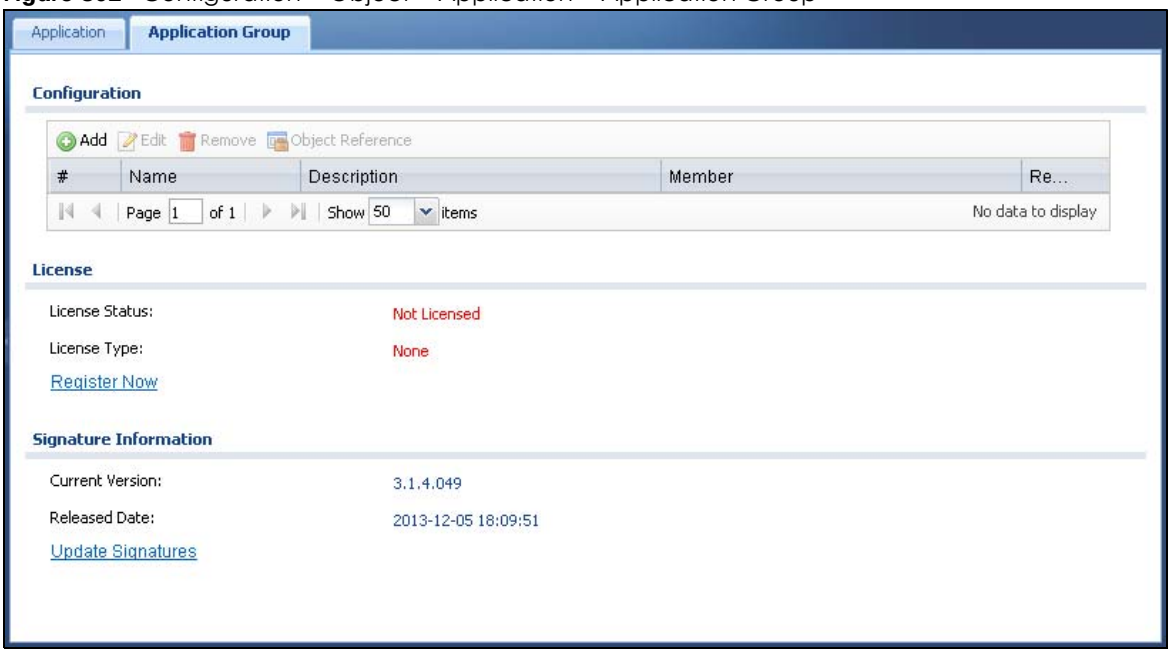
Table 205 Configuration > Object > Application > Application > Add Application Rule > Add Application Object

| LABEL | DESCRIPTION |
|---|---|
| Query | |
| Search | Choose signatures in one of the following ways:<br>• Select **By Category** then select a category in the adjacent drop-down list box to display all signatures of that category<br>• 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. |

# 37.3 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 301** Configuration > Object > Application > Application Group




The following table describes the labels in this screen.

Table 206 Configuration > Object > Application > Application Group

| LABEL | DESCRIPTION |
|---|---|
| Configuration | |
| 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. |

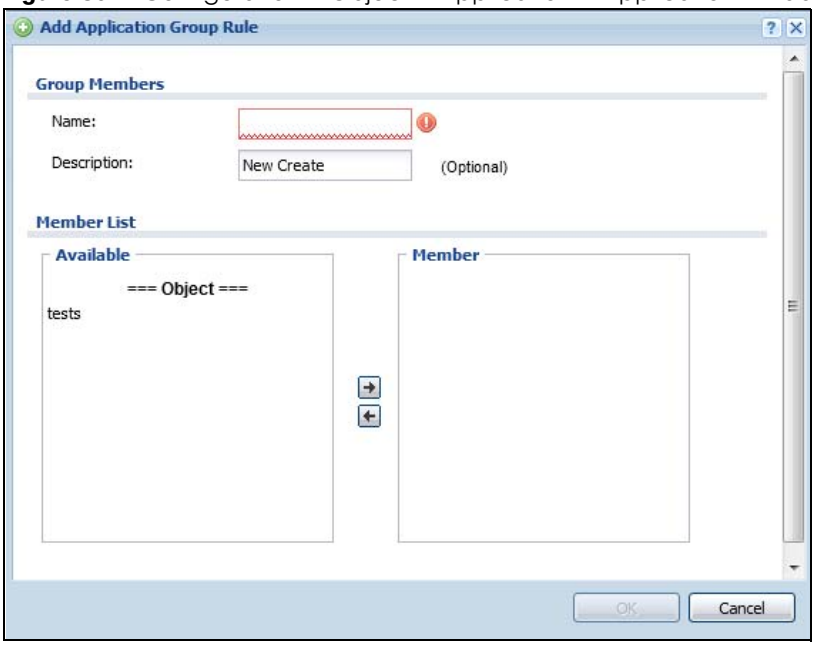
Table 206 Configuration > Object > Application > Application Group (continued)

| 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. |

## 37.3.1 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 302** Configuration > Object > Application > Application > Add Application Group Rule




The following table describes the labels in this screen.

Table 207 Configuration > Object > Application > Application > Add Application Group Rule

| LABEL | DESCRIPTION |
|---|---|
| Group Members | |
| 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 | 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.<br>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.<br>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. |

# CHAPTER 38
# Addresses

## 38.1 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.

### 38.1.1 What You Can Do in this Chapter

- The **Address** screen (Section 38.2 on page 451) 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 38.3 on page 453) and the **Address Group Add/Edit** screen, to maintain address groups in the UAG.

### 38.1.2 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.

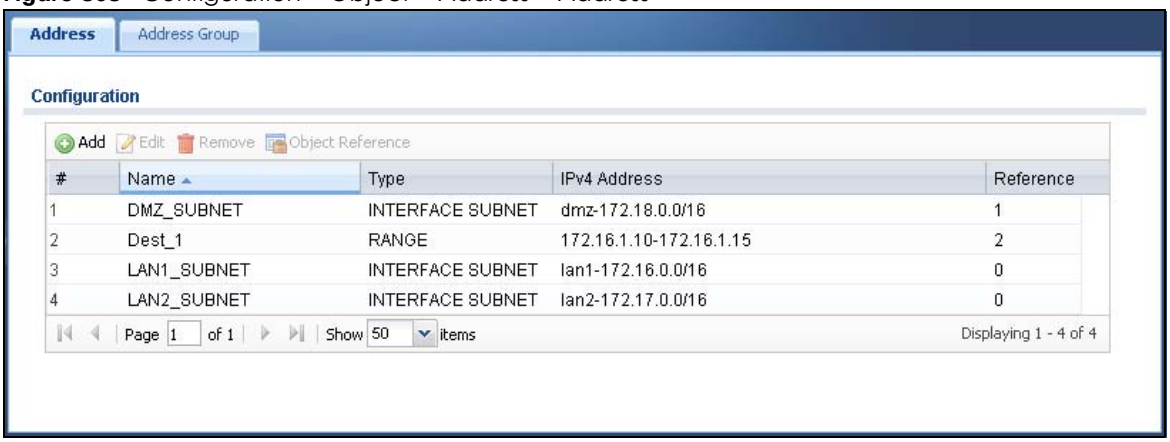
## 38.2 Address Summary Screen

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 303** Configuration > Object > Address > Address




The following table describes the labels in this screen. See Section 38.2.1 on page 452 for more information as well.

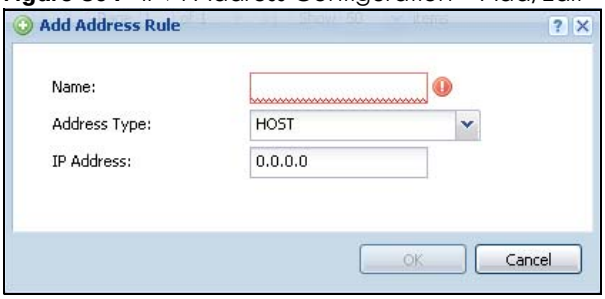
Table 208 Configuration > Object > Address > Address

| 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 180 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. |

## 38.2.1 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 38.2 on page 451), and click either the **Add** icon or an **Edit** icon in the **Configuration** section.

**Figure 304** IPv4 Address Configuration > Add/Edit




The following table describes the labels in this screen.

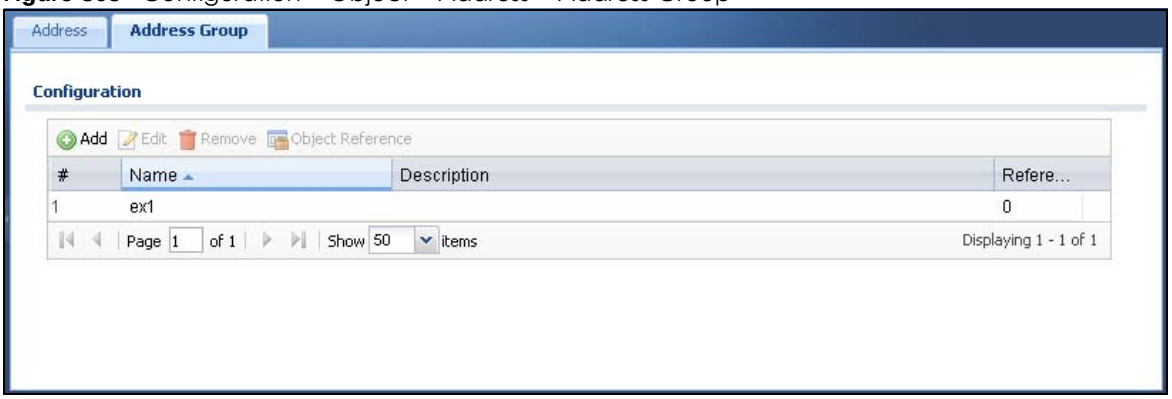
Table 209 IPv4 Address Configuration > Add/Edit

| 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**.<br><br>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. |

# 38.3 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 305** Configuration > Object > Address > Address Group




The following table describes the labels in this screen. See Section 38.3.1 on page 454 for more information as well.

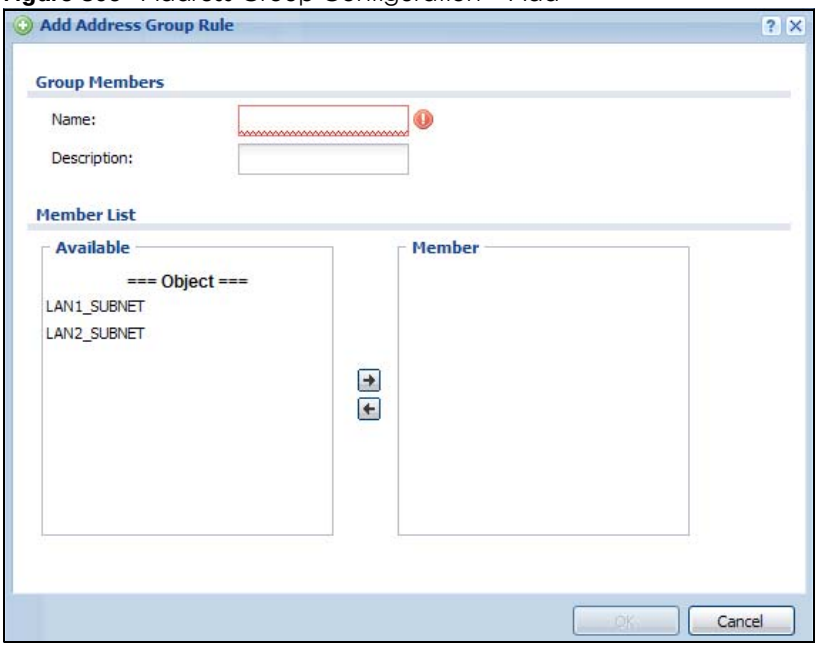
Table 210 Configuration > Object > Address > Address Group

| 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 180 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. |

## 38.3.1 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 38.3 on page 453), and click either the **Add** icon or an **Edit** icon in the **Configuration** section.

**Figure 306** Address Group Configuration > Add




The following table describes the labels in this screen.

Table 211 Address Group Configuration > Add

| LABEL | DESCRIPTION |
|---|---|
| Group Members | |
| 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 | 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.<br>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.<br>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. |

# CHAPTER 39
# Service

## 39.1 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.

### 39.1.1 What You Can Do in this Chapter

- Use the **Service** screens (Section 39.2 on page 457) to view and configure the UAG's list of services and their definitions.
- Use the **Service Group** screens (Section 39.2 on page 457) to view and configure the UAG's list of service groups.

### 39.1.2 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.

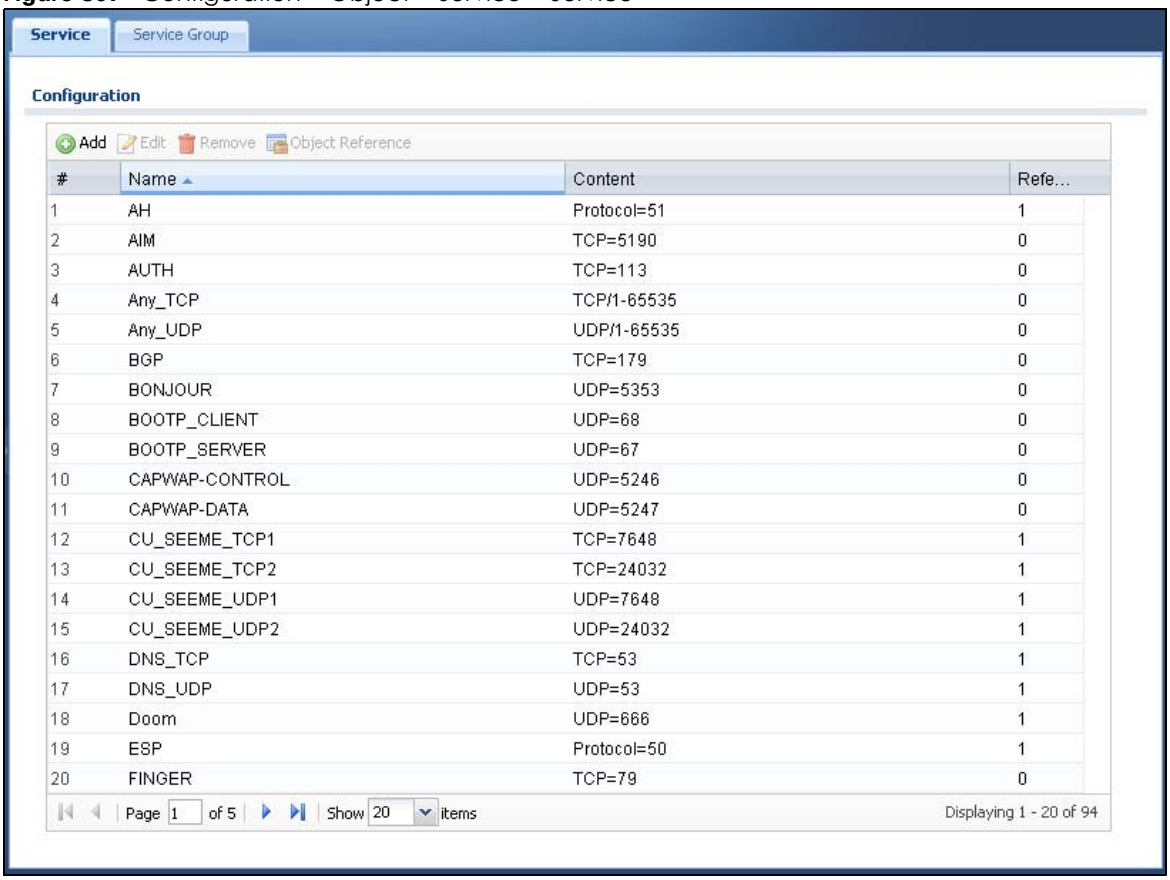
Use service groups when you want to create the same rule for several services, instead of creating separate rules for each service. Service groups may consist of services and other service groups. The sequence of members in the service group is not important.

# 39.2 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 307** Configuration > Object > Service > Service



The following table describes the labels in this screen.

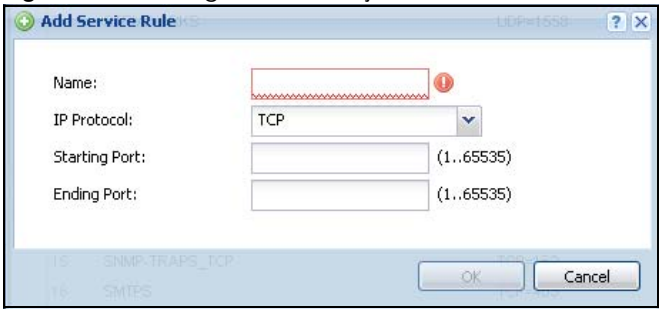
Table 212 Configuration > Object > Service > Service

| 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 180 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. |

## 39.2.1 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 39.2 on page 457), and click either the **Add** icon or an **Edit** icon.

**Figure 308** Configuration > Object > Service > Service > Edit




The following table describes the labels in this screen.

Table 213 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<br><br>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**.<br><br>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**.<br><br>Enter the number of the next-level protocol (IP protocol). Allowed values are 1 - 255. |

Table 213 Configuration > Object > Service > Service > Edit (continued)

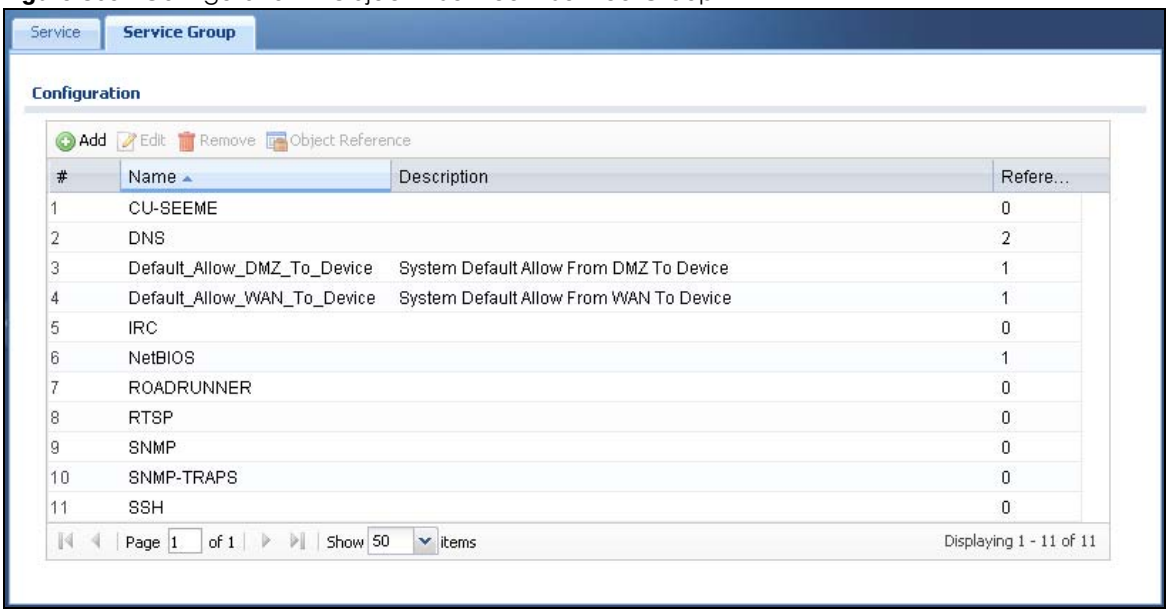
| LABEL | DESCRIPTION |
|---|---|
| OK | Click **OK** to save your changes back to the UAG. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

# 39.3 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 309** Configuration > Object > Service > Service Group




The following table describes the labels in this screen. See Section 39.3.1 on page 460 for more information as well.

Table 214 Configuration > Object > Service > Service 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 180 for an example. |
| # | This field is a sequential value, and it is not associated with a specific service group. |

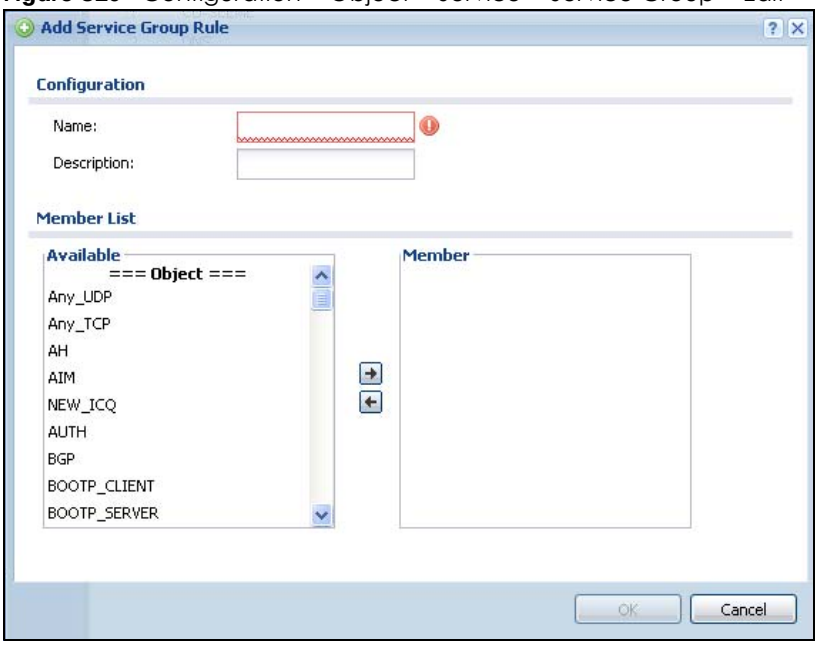
Table 214 Configuration > Object > Service > Service Group (continued)

| LABEL | DESCRIPTION |
|---|---|
| Name | This field displays the name of each service group.<br>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. |

## 39.3.1 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 39.3 on page 459), and click either the **Add** icon or an **Edit** icon.

**Figure 310** Configuration > Object > Service > Service Group > Edit




The following table describes the labels in this screen.

Table 215 Configuration > Object > Service > Service Group > Edit

| LABEL | DESCRIPTION |
|---|---|
| Configuration | |
| 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 | 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.<br>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.<br>Move any members you do not want included to the **Available** list. |

Table 215 Configuration > Object > Service > Service Group > 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. |

# CHAPTER 40 Schedules

## 40.1 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.

### 40.1.1 What You Can Do in this Chapter

- Use the **Schedule** summary screen (Section 40.2 on page 463) to see a list of all schedules in the UAG.
- Use the **One-Time Schedule Add/Edit** screen (Section 40.2.1 on page 464) to create or edit a one-time schedule.
- Use the **Recurring Schedule Add/Edit** screen (Section 40.2.2 on page 465) to create or edit a recurring schedule.
- Use the **Schedule Group** screen (Section 40.3 on page 466) to merge individual schedule objects as one object.

### 40.1.2 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.

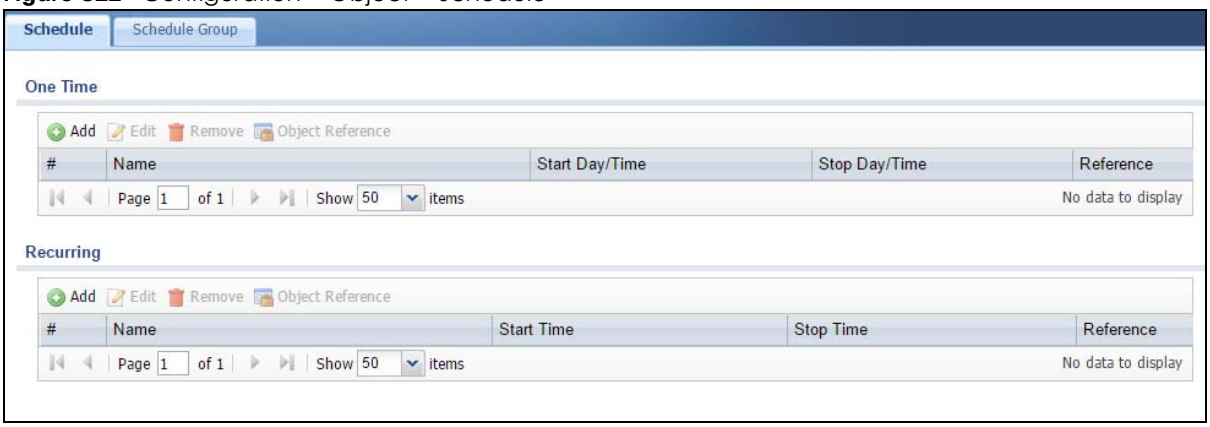
#### Finding Out More

- See Section 45.4 on page 497 for information about the UAG's current date and time.

# 40.2 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 311** Configuration > Object > Schedule




The following table describes the labels in this screen. See Section 40.2.1 on page 464 and Section 40.2.2 on page 465 for more information as well.

Table 216 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 180 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. |
| Reference | This displays the number of times an object reference is used in a profile. |
| 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 180 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. |

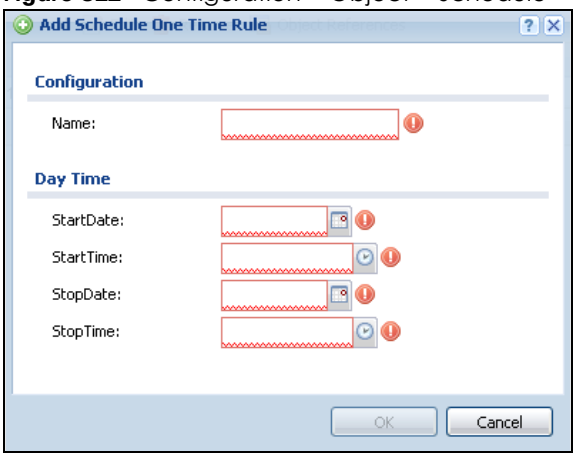
Table 216 Configuration > Object > Schedule (continued)

| LABEL | DESCRIPTION |
|---|---|
| Stop Time | This field displays the time at which the schedule ends. |
| Reference | This displays the number of times an object reference is used in a profile. |

## 40.2.1 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 40.2 on page 463), and click either the **Add** icon or an **Edit** icon in the **One Time** section.

**Figure 312** Configuration > Object > Schedule > Edit (One Time)




The following table describes the labels in this screen.

Table 217 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.<br>• **Year** - 1900 - 2999<br>• **Month** - 1 - 12<br>• **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.<br>• **Hour** - 0 - 23<br>• **Minute** - 0 - 59 |
| StopDate | Specify the year, month, and day when the schedule ends.<br>• **Year** - 1900 - 2999<br>• **Month** - 1 - 12<br>• **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.<br>• **Hour** - 0 - 23<br>• **Minute** - 0 - 59 |

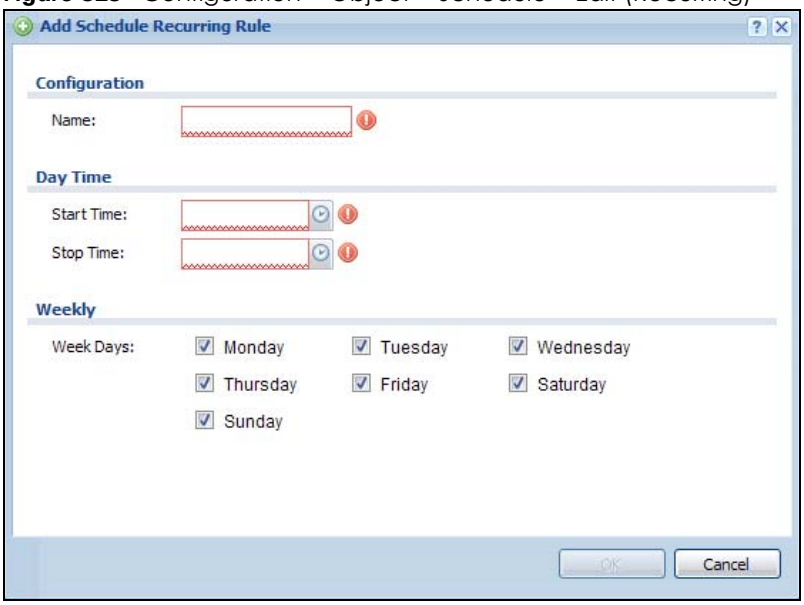
Table 217 Configuration > Object > Schedule > Edit (One Time) (continued)

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

## 40.2.2 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 40.2 on page 463), and click either the **Add** icon or an **Edit** icon in the **Recurring** section.

**Figure 313** 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 218 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.<br>• **Hour** - 0 - 23<br>• **Minute** - 0 - 59 |
| StopTime | Specify the hour and minute when the schedule ends each day.<br>• **Hour** - 0 - 23<br>• **Minute** - 0 - 59 |
| Weekly | |
| Week Days | Select each day of the week the recurring schedule is effective. |

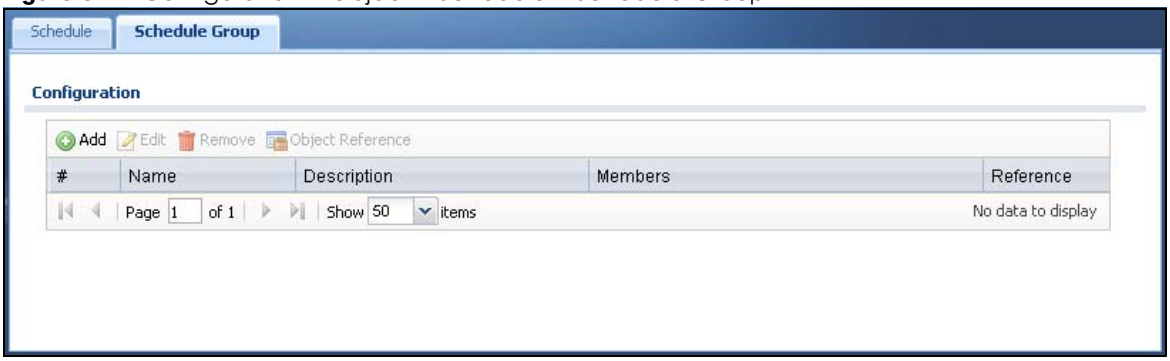
Table 218 Configuration > Object > Schedule > Edit (Recurring) (continued)

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

# 40.3 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 314** Configuration > Object > Schedule > Schedule Group




The following table describes the fields in the above screen.

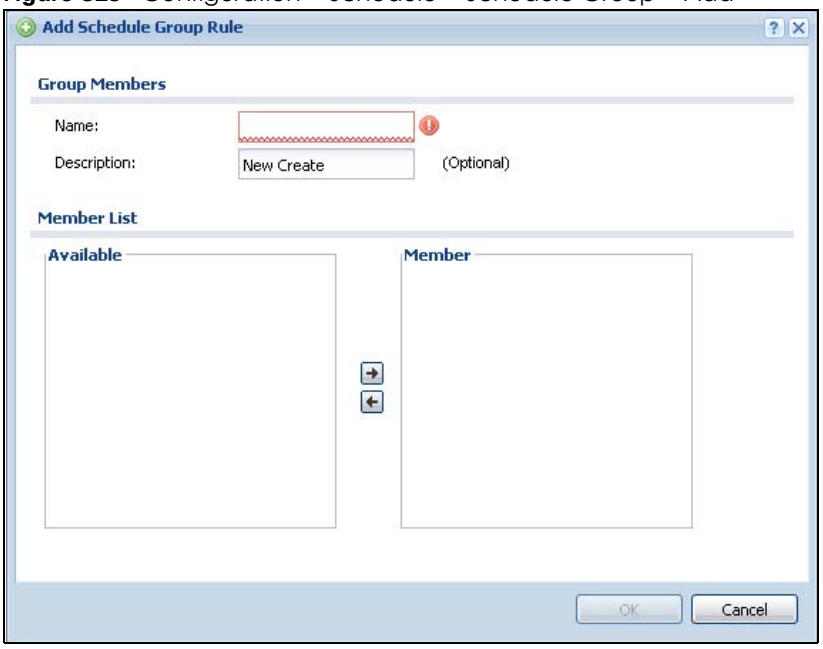
Table 219 Configuration > Object > Schedule > Schedule Group

| 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 Reference**s 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. |

## 40.3.1 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, and click either the **Add** icon or an **Edit** icon in the **Schedule Group** section.

**Figure 315** Configuration > Schedule > Schedule Group > Add




The following table describes the fields in the above screen.

Table 220 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 | 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.<br>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.<br>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. |

# CHAPTER 41
# AAA Server

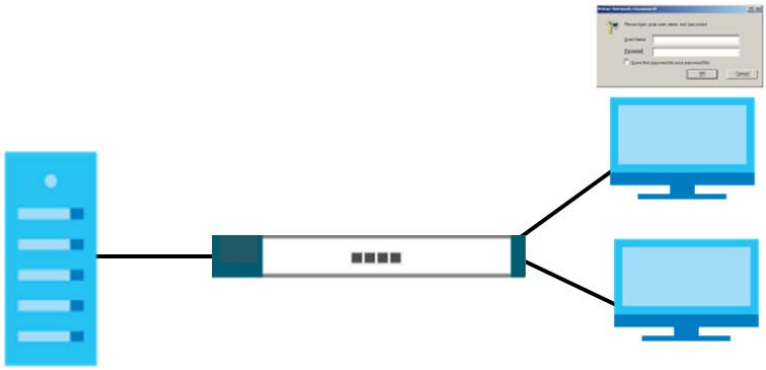
## 41.1 Overview

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 42 on page 473).

### 41.1.1 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 316** RADIUS Server Network Example



### 41.1.2 What You Can Do in this Chapter

Use the **Configuration > Object > AAA Server > RADIUS** screen (Section 41.2 on page 469) to configure the default external RADIUS server to use for user authentication.

### 41.1.3 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

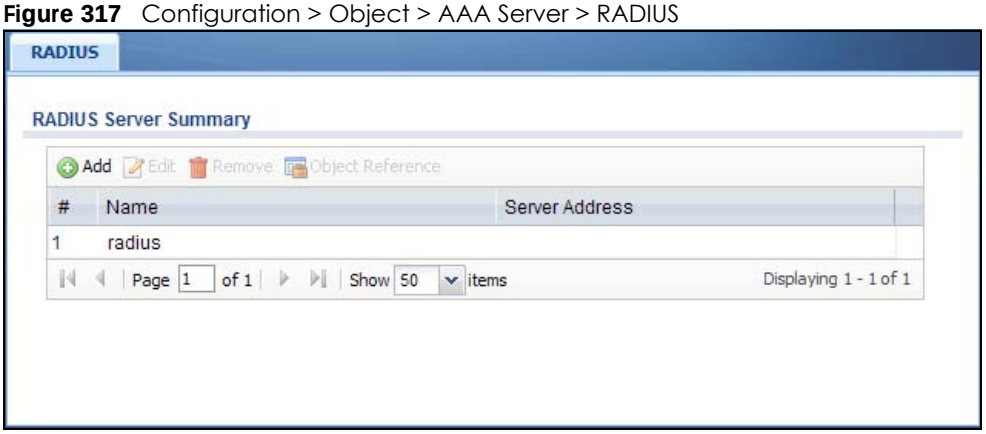
  RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external or built-in RADIUS server. RADIUS authentication allows you to validate a large number of users from a central location.

# 41.2 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 317** Configuration > Object > AAA Server > RADIUS




The following table describes the labels in this screen.

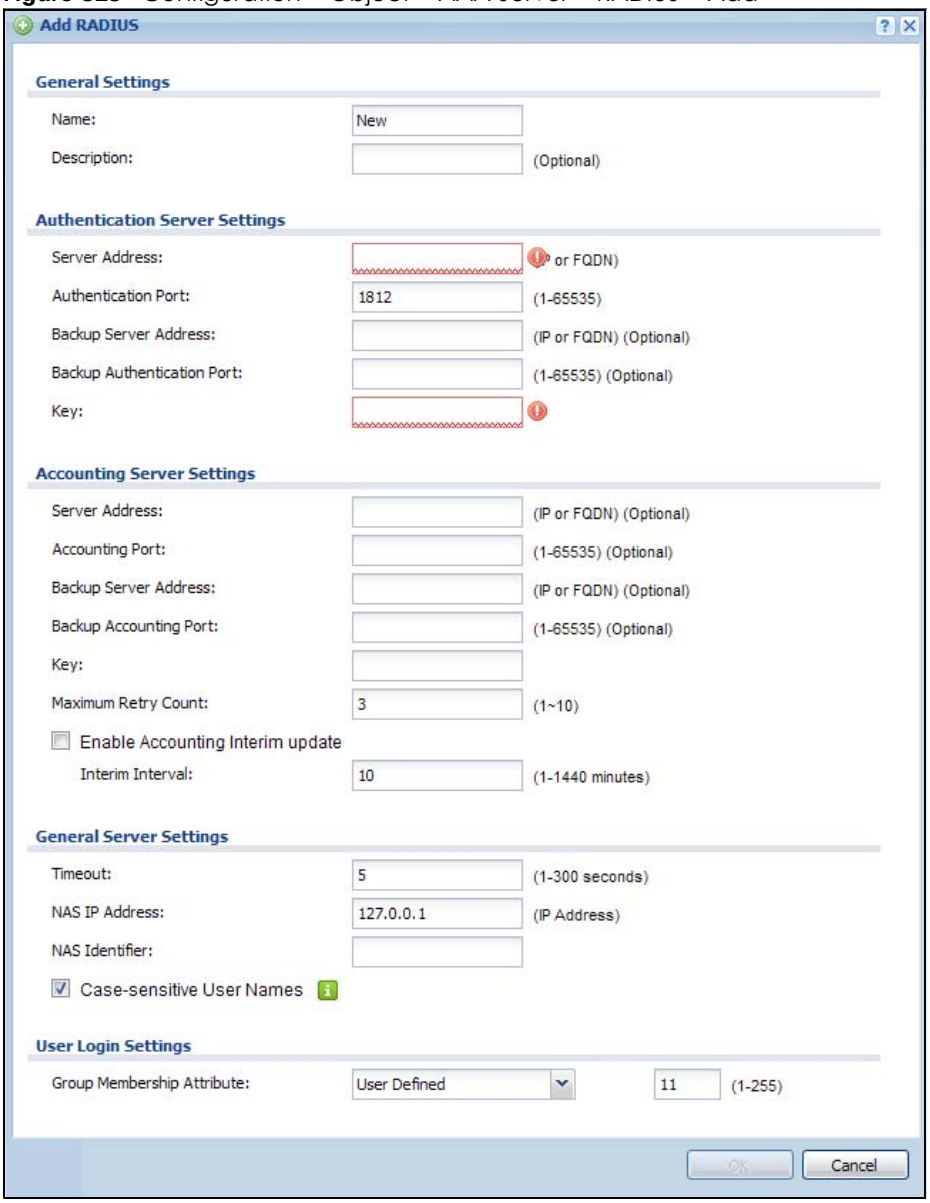
Table 221 Configuration > Object > AAA Server > RADIUS

| LABEL | DESCRIPTION |
|---|---|
| RADIUS Server Summary | |
| 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 180 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. |

## 41.2.1 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 318** Configuration > Object > AAA Server > RADIUS > Add




The following table describes the labels in this screen.

Table 222 Configuration > Object > AAA Server > RADIUS > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Name | Enter a descriptive name (up to 63 alphanumerical characters) for identification purposes. |
| Description | Enter the description of each server, if any. You can use up to 60 printable ASCII characters. |

Table 222 Configuration > Object > AAA Server > RADIUS > Add/Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. |
| 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 | Enter a password (up to 15 alphanumeric characters) as the key to be shared between the external authentication server and the UAG.<br>The key is not sent over the network. This key must be the same on the external authentication server and the UAG. |
| 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 | Enter a password (up to 15 alphanumeric characters) as the key to be shared between the external accounting server and the UAG.<br>The key is not sent over the network. This key must be the same on the external accounting server and the UAG. |
| Maximum Retry Count | 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.<br>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.<br>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. |
| 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 | Specify the timeout period (between 1 and 300 seconds) before the UAG disconnects from the RADIUS server. In this case, user authentication fails.<br>Search timeout occurs when either the user information is not in the RADIUS server or the RADIUS server is down. |
| 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. |

Table 222 Configuration > Object > AAA Server > RADIUS > Add/Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Case-sensitive User Names | Select this if the server checks the case of the usernames. |
| User Login Settings | |
| Group Membership Attribute | 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.<br>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.<br>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". |
| OK | Click **OK** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

# CHAPTER 42
# Authentication Method

## 42.1 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.

### 42.1.1 What You Can Do in this Chapter

- Use the **Configuration > Object > Auth. Method** screens (Section 42.2 on page 473) to create and manage authentication method objects.

### 42.1.2 Before You Begin

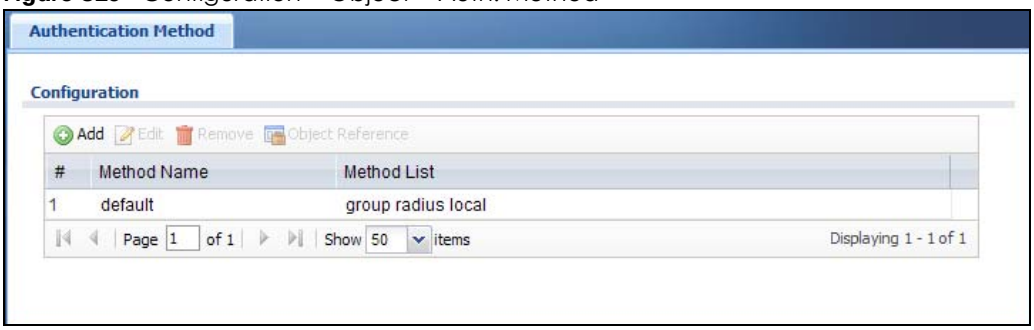
Configure AAA server objects (see Chapter 41 on page 468) before you configure authentication method objects.

## 42.2 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 319** Configuration > Object > Auth. Method



The following table describes the labels in this screen.

Table 223 Configuration > Object > Auth. Method

| LABEL | DESCRIPTION |
|---|---|
| Configuration | |
| 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 180 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. |

## 42.2.1 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.

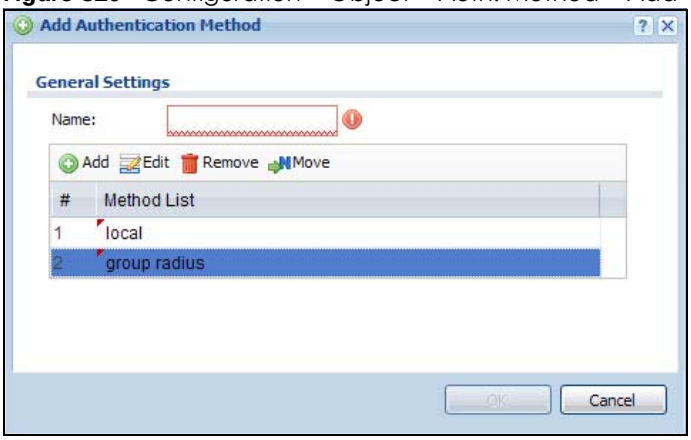
6 You can add up to four server objects to the table. The ordering of the **Method List** column is important. The UAG authenticates the users using the databases (in the local user database or the external authentication server) in the order they appear in this screen.

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 320** Configuration > Object > Auth. Method > Add




The following table describes the labels in this screen.

Table 224 Configuration > Object > Auth. Method > Add

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Name | Specify a descriptive name for identification purposes.<br>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.<br>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 41 on page 468 for more information).<br>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.<br>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. |

# CHAPTER 43 Certificates

## 43.1 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.

### 43.1.1 What You Can Do in this Chapter

- Use the **My Certificates** screens (see Section 43.2 on page 479 to Section 43.2.3 on page 485) to generate and export self-signed certificates or certification requests and import the CA-signed certificates.
- Use the **Trusted Certificates** screens (see Section 43.3 on page 486 to Section 43.3.2 on page 490) 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.

### 43.1.2 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 PKS#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.

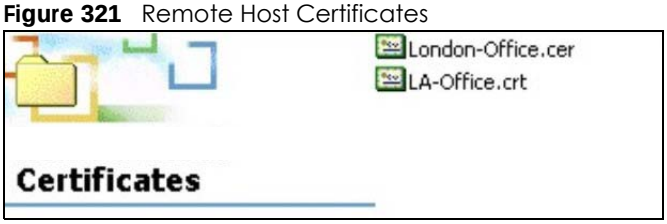
## 43.1.3 Verifying a Certificate

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.

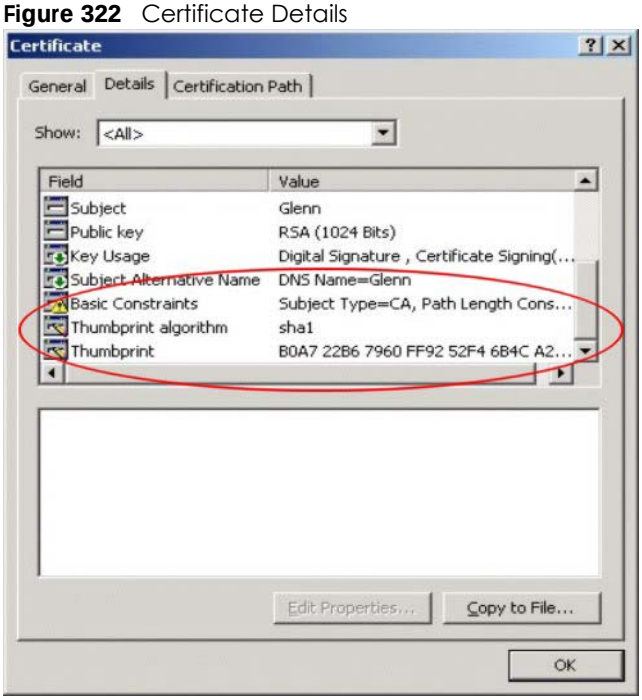
2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

**Figure 321** 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 322** Certificate Details

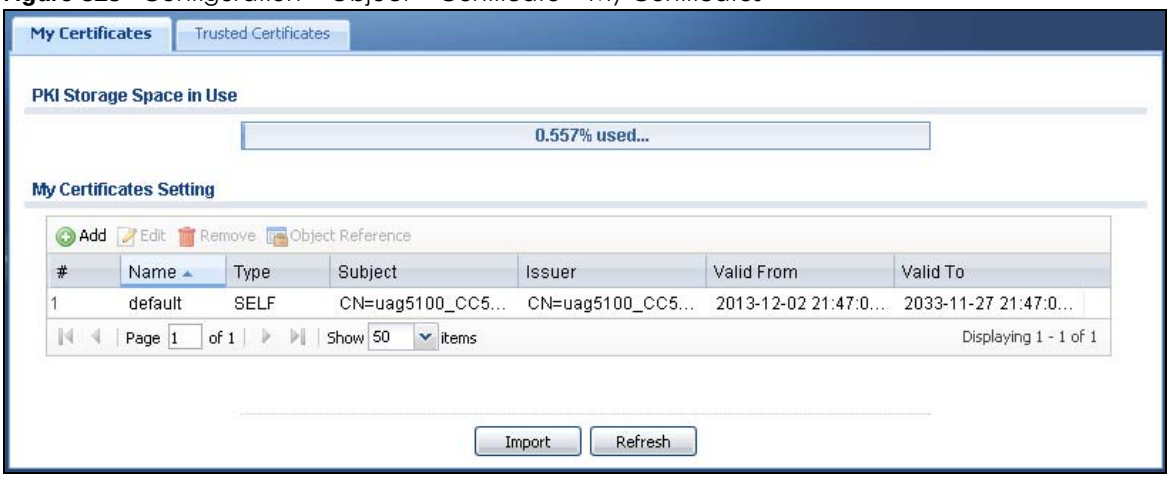


4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may very based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

# 43.2 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 323** Configuration > Object > Certificate > My Certificates




The following table describes the labels in this screen.

Table 225 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. |
| My Certificates Setting | |
| 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 180 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. |

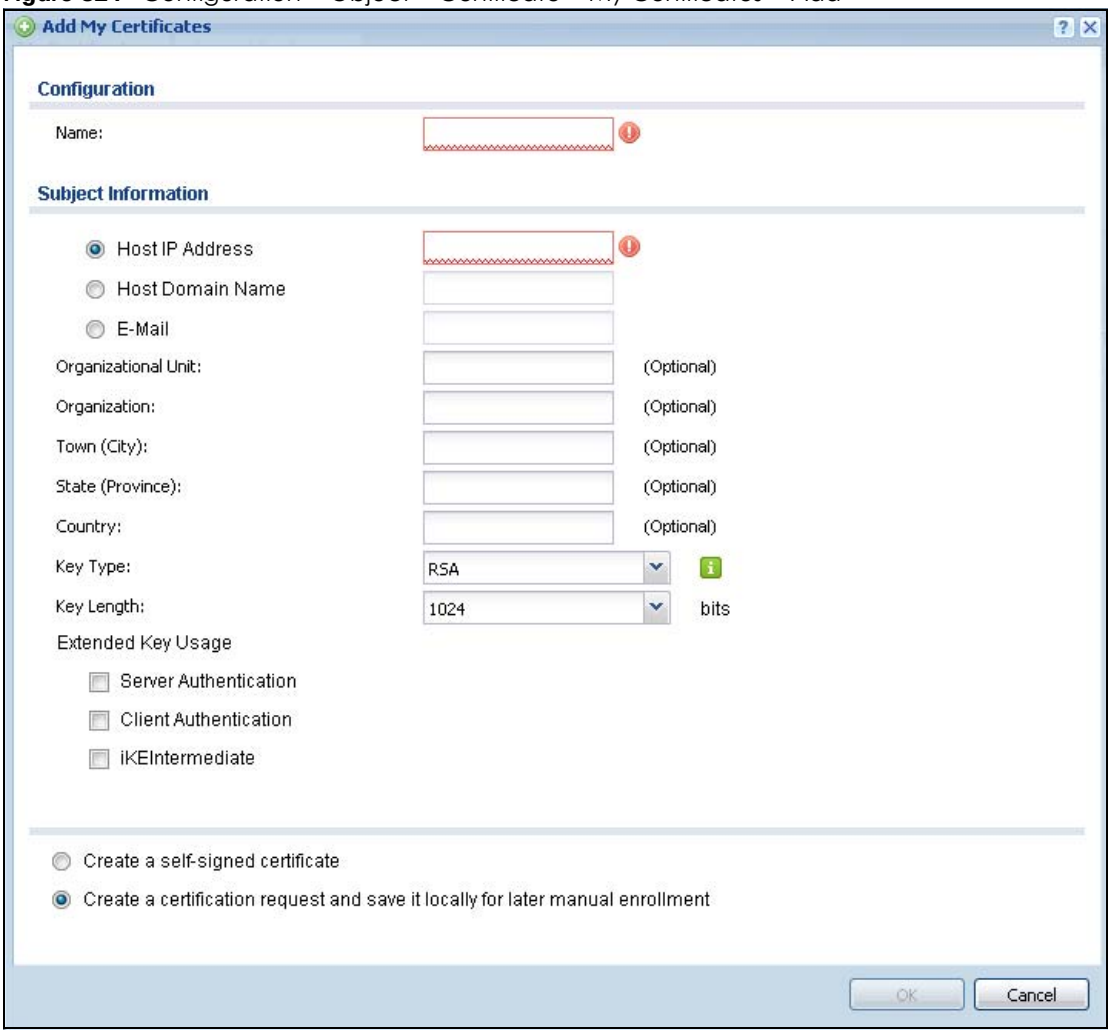
Table 225 Configuration > Object > Certificate > My Certificates (continued)

| LABEL | DESCRIPTION |
|---|---|
| Type | This field displays what kind of certificate this is.<br>**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.<br>**SELF** represents a self-signed certificate.<br>**CERT** represents a certificate issued by a certification authority. |
| 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 a certificate to the UAG. |
| Refresh | Click **Refresh** to display the current validity status of the certificates. |

## 43.2.1 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 324** Configuration > Object > Certificate > My Certificates > Add




The following table describes the labels in this screen.

Table 226 Configuration > Object > Certificate > My Certificates > Add

| LABEL | DESCRIPTION |
|---|---|
| Configuration | |
| Name | Type a name to identify this certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters. |
| Subject Information | 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.<br><br>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.<br><br>A domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods.<br><br>An e-mail address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore. |

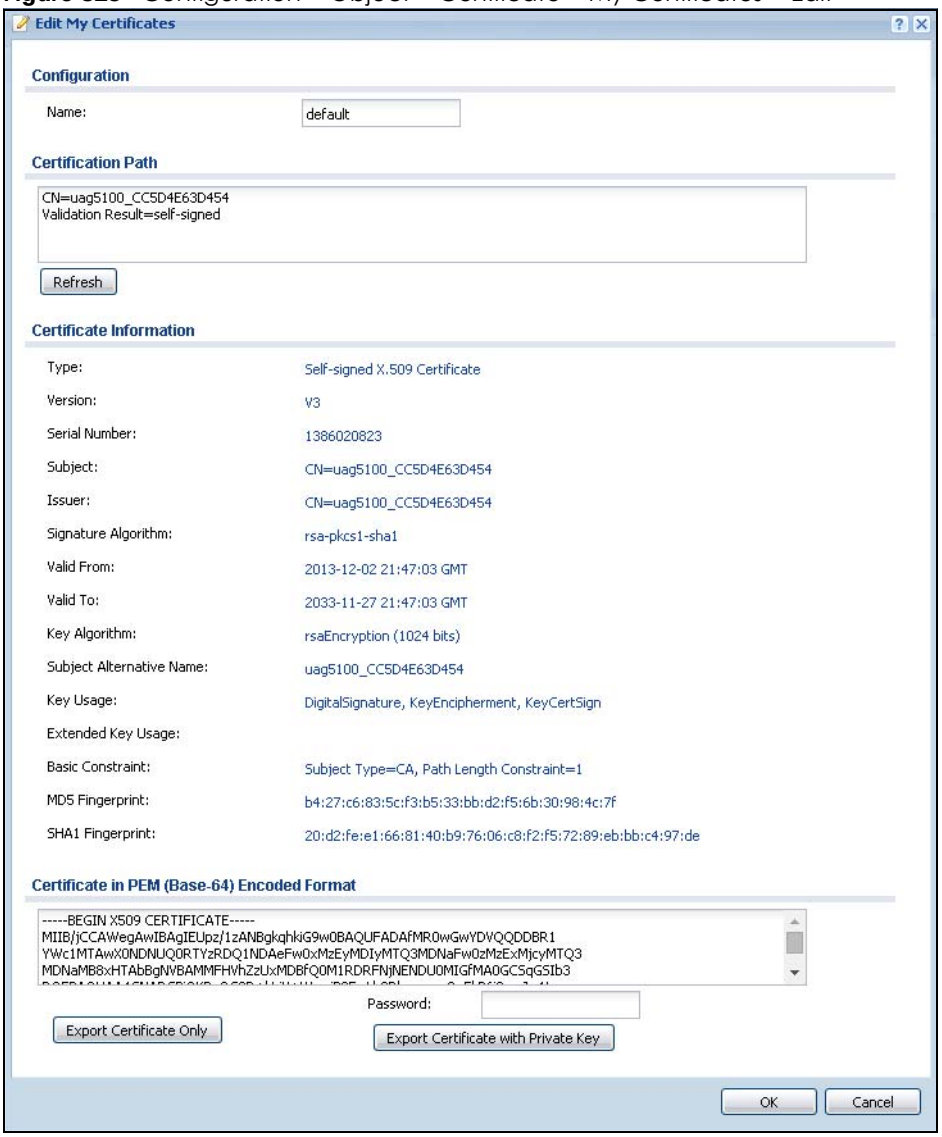
Table 226 Configuration > Object > Certificate > My Certificates > Add (continued)

| 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.<br>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.<br>Select **Client Authentication** to use the certificate's key to authenticate clients to the secure gateway.<br>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.<br>Copy the certification request from the **My Certificate Details** screen (see Section 43.2.2 on page 482) 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. |

## 43.2.2 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 325** Configuration > Object > Certificate > My Certificates > Edit




The following table describes the labels in this screen.

Table 227 Configuration > Object > Certificate > My Certificates > Edit

| LABEL | DESCRIPTION |
|---|---|
| Configuration | |
| 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.<br>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).<br>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 227 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.<br>With self-signed certificates, this is the same as the **Subject Name** field.<br>"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. |
| 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.<br>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.<br>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). |

Table 227 Configuration > Object > Certificate > My Certificates > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. |

## 43.2.3 The My Certificates Import Screen

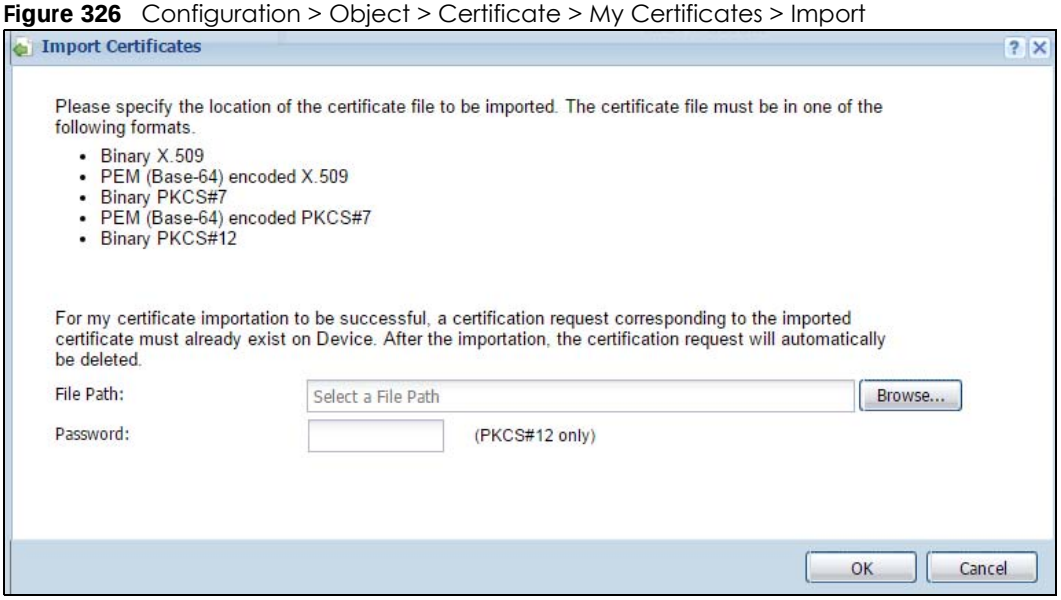
Click **Configuration > Object > Certificate > My Certificates > Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the UAG.

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 326** Configuration > Object > Certificate > My Certificates > Import



The following table describes the labels in this screen.

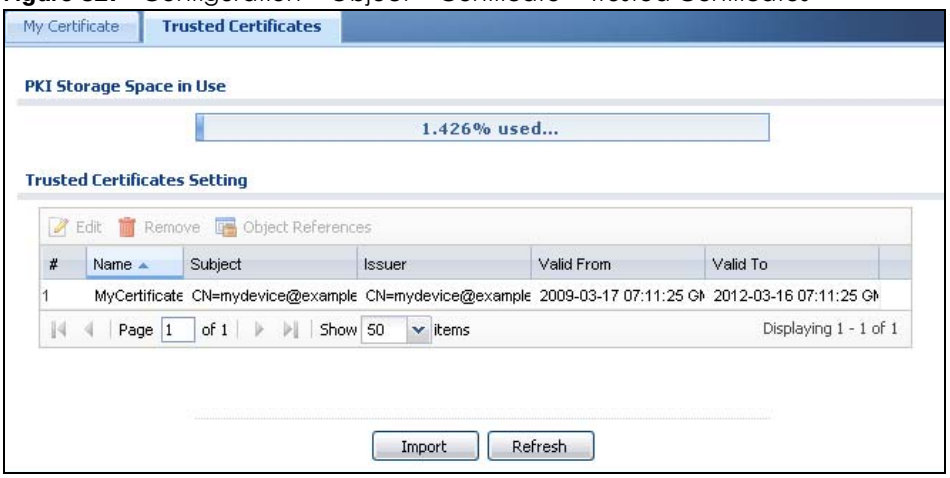
Table 228 Configuration > Object > Certificate > My Certificates > Import

| LABEL | DESCRIPTION |
|---|---|
| File Path | Type in the location of the file you want to upload in this field or click **Browse** to find it.<br>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. |

# 43.3 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 327** Configuration > Object > Certificate > Trusted Certificates




The following table describes the labels in this screen.

Table 229 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. |
| Trusted Certificates Setting | |
| 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. |

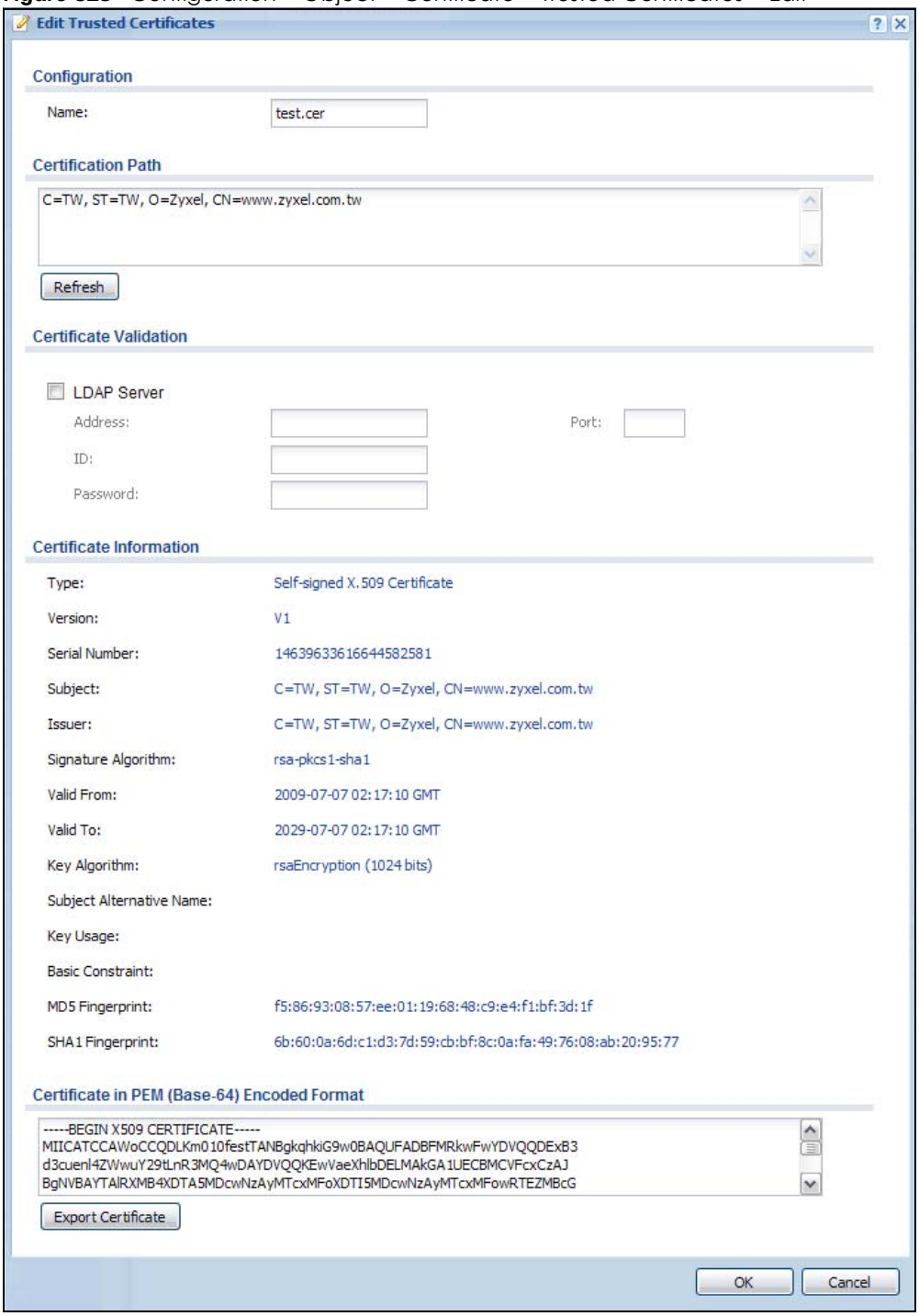
Table 229 Configuration > Object > Certificate > Trusted Certificates (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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 180 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. |

## 43.3.1 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 328** Configuration > Object > Certificate > Trusted Certificates > Edit




The following table describes the labels in this screen.

Table 230 Configuration > Object > Certificate > Trusted Certificates > Edit

| LABEL | DESCRIPTION |
|---|---|
| Configuration | |
| Name | This field displays the identifying name of this certificate. You can change the name. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters. |

Table 230 Configuration > Object > Certificate > Trusted Certificates > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. |
| Certificate Validation | |
| 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.<br>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). |
| 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. |

Table 230 Configuration > Object > Certificate > Trusted Certificates > Edit (continued)

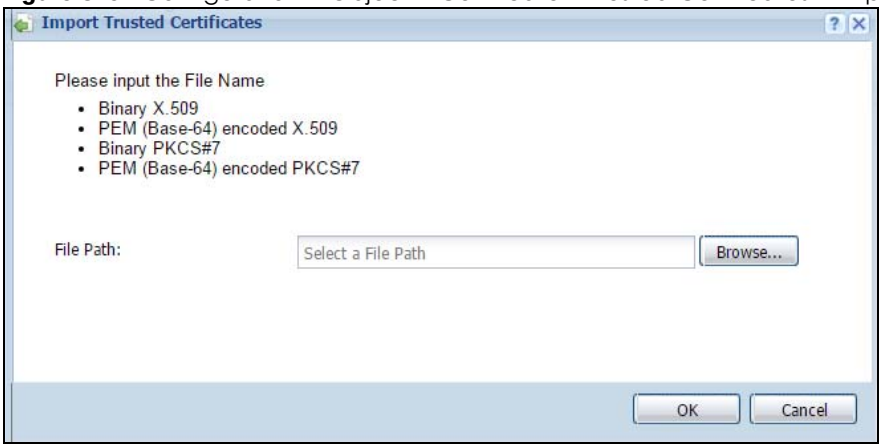
| LABEL | DESCRIPTION |
|---|---|
| Basic Constraint | This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the 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.<br>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. |

## 43.3.2 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 329** Configuration > Object > Certificate > Trusted Certificates > Import




The following table describes the labels in this screen.

Table 231 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.<br>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. |

Table 231 Configuration > Object > Certificate > Trusted Certificates > Import (continued)

| LABEL | DESCRIPTION |
|---|---|
| OK | Click **OK** to save the certificate on the UAG. |
| Cancel | Click **Cancel** to quit and return to the previous screen. |

# CHAPTER 44
# ISP Accounts

## 44.1 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 183 for information about PPPoE/PPTP interfaces.

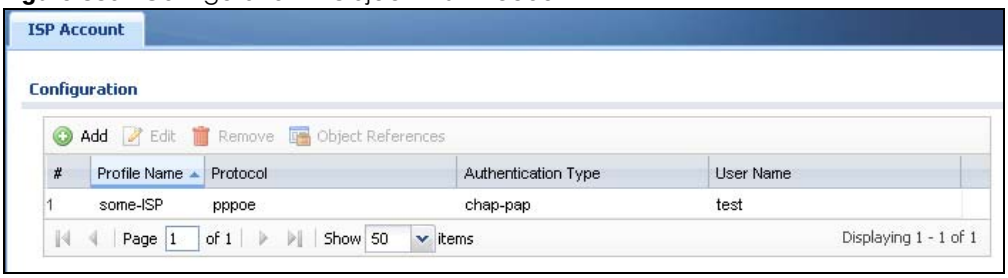
### 44.1.1 What You Can Do in this Chapter

Use the **Object** > **ISP Account** screens (Section 44.2 on page 492) to create and manage ISP accounts in the UAG.

## 44.2 ISP Account Summary

This screen provides a summary of ISP accounts in the UAG. To access this screen, click **Configuration > Object** > **ISP Account**.

**Figure 330** Configuration > Object > ISP Account




The following table describes the labels in this screen. See the ISP Account Add/Edit section below for more information as well.

Table 232 Configuration > Object > ISP Account

| 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. |

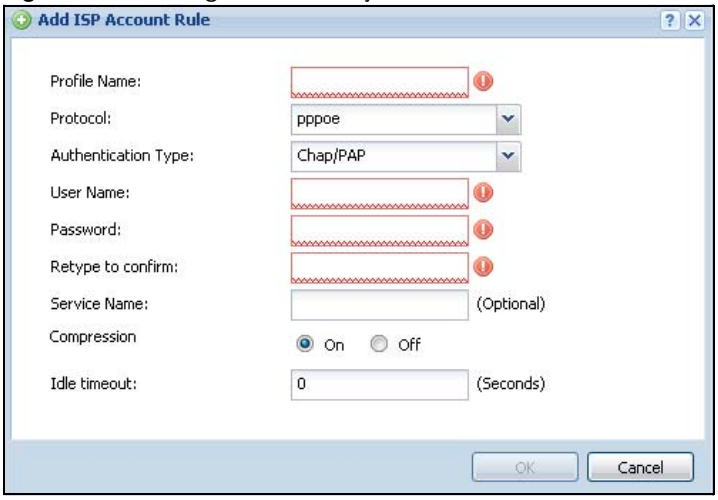
Table 232 Configuration > Object > ISP Account (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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 180 for an example. |
| # | 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. |

## 44.2.1 ISP Account Add/Edit

The **Add ISP Account Rule** 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 44.2 on page 492.) Then, click on an **Add** icon or **Edit** icon to open the **ISP Account Edit** screen below.

**Figure 331** Configuration > Object > ISP Account > Add/Edit




The following table describes the labels in this screen.

Table 233 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:<br>**pppoe** - This ISP account uses the PPPoE protocol.<br>**pptp** - This ISP account uses the PPTP protocol. |

Table 233 Configuration > Object > ISP Account > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Authentication Type | Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:<br>**CHAP/PAP** - Your UAG accepts either CHAP or PAP when requested by this remote node.<br>**Chap** - Your UAG accepts CHAP only.<br>**PAP** - Your UAG accepts PAP only.<br>**MSCHAP** - Your UAG accepts MSCHAP only.<br>**MSCHAP-V2** - Your UAG accepts MSCHAP-V2 only. |
| Encryption Method | 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:<br>**nomppe** - This ISP account does not use MPPE.<br>**mppe-40** - This ISP account uses 40-bit MPPE.<br>**mppe-128** - This ISP account uses 128-bit MMPE. |
| 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 | If this ISP account uses the PPPoE protocol, this field is not displayed.<br>If this ISP account uses the PPTP protocol, type the IP address or domain name of the PPTP server. |
| 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 | 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.<br>If this ISP account uses the PPTP protocol, this field is not displayed. |
| 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). |

# CHAPTER 45
# System

## 45.1 Overview

Use the system screens to configure general UAG settings.

### 45.1.1 What You Can Do in this Chapter

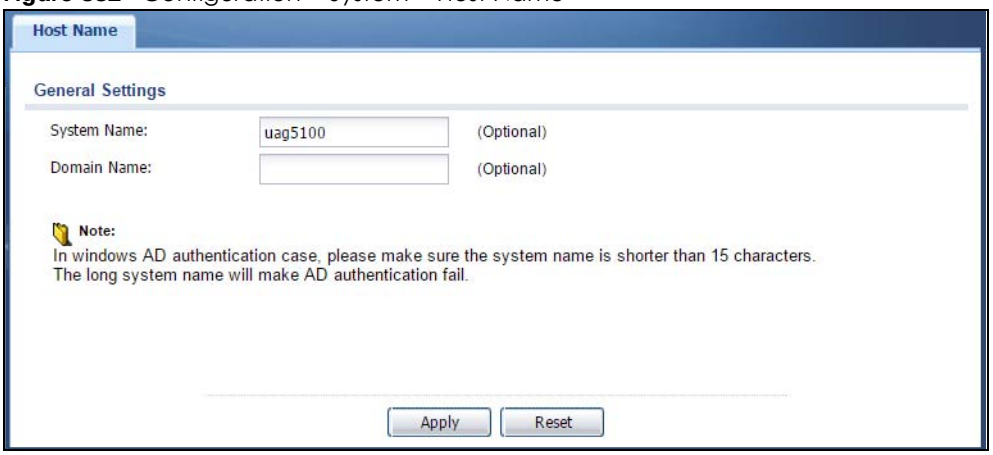
- Use the **System > Host Name** screen (see Section 45.2 on page 496) to configure a unique name for the UAG in your network.
- Use the **System > USB Storage** screen (see Section 45.3 on page 496) to configure the settings for the connected USB devices.
- Use the **System > Date/Time** screen (see Section 45.4 on page 497) to configure the date and time for the UAG.
- Use the **System > Console Speed** screen (see Section 45.5 on page 501) 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 45.6 on page 502) 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 45.7 on page 510) 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 45.8 on page 527) 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 45.9 on page 532) 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 45.10 on page 533) 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 47 on page 558 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 45.11 on page 534) 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 45.12 on page 537) to configure the UAG to operate as a RADIUS server.
- Use the **Language** screen (Section 45.13 on page 540) to set the user interface language for the UAG's Web Configurator screens.
- Use the **ZON** screen (Section 45.14 on page 540) to enable or disable ZDP discovery and LLDP discovery on the UAG.

Note: See each section for related background information and term definitions.

# 45.2 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 332** Configuration > System > Host Name




The following table describes the labels in this screen.

Table 234 Configuration > System > Host Name

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| 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. |

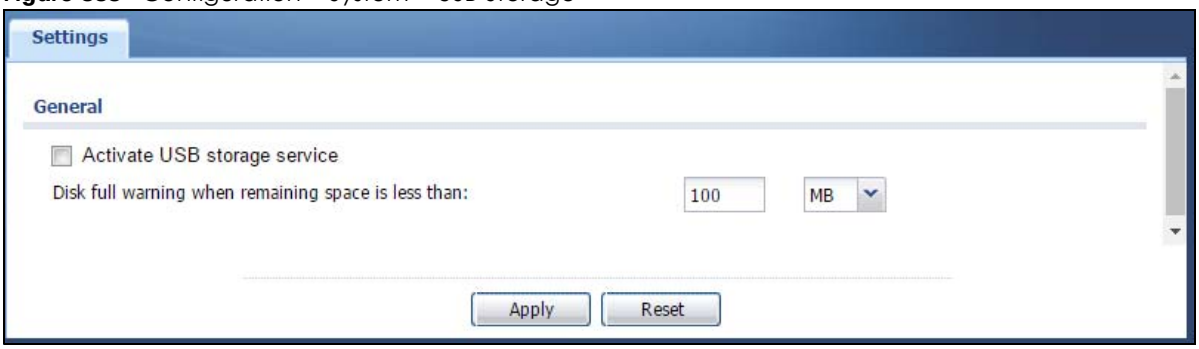
# 45.3 USB Storage

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 333** Configuration > System > USB Storage




The following table describes the labels in this screen.

Table 235 Configuration > System > USB Storage

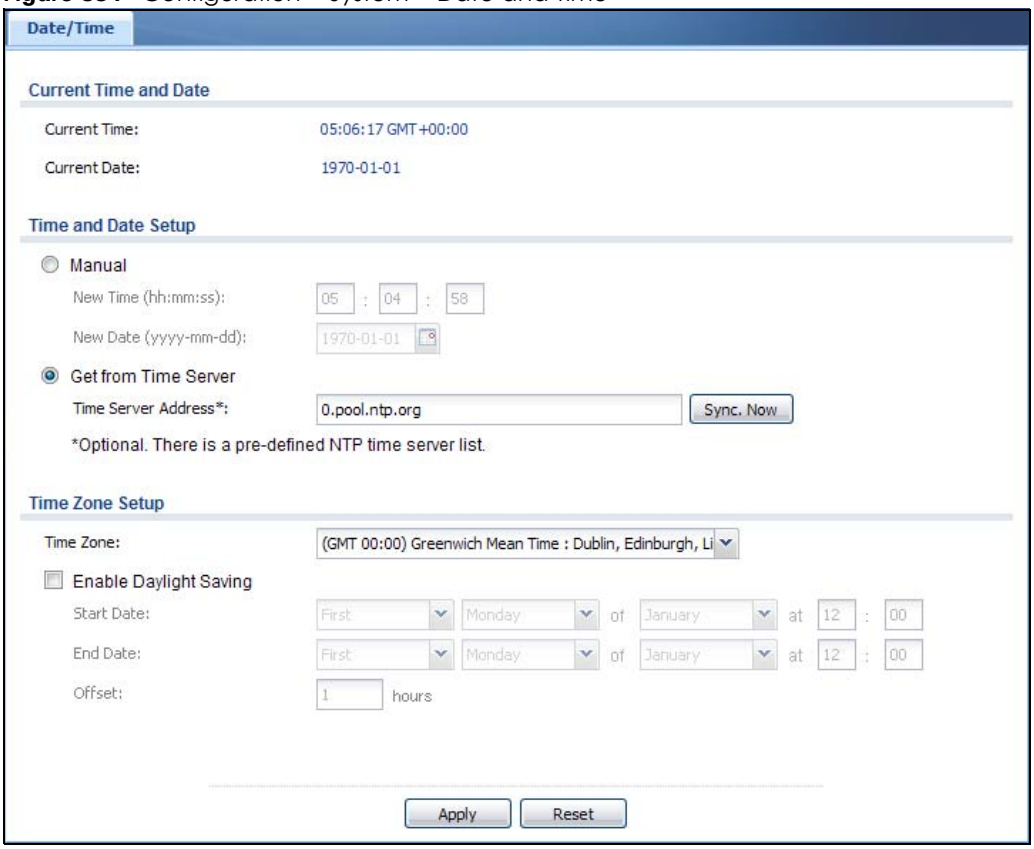
| LABEL | DESCRIPTION |
|---|---|
| General | |
| Activate USB storage service | Select this if you want to use the connected USB device(s). |
| Disk full warning when remaining space is less than | Set a number and select a unit (**MB** or **%**) to have the UAG send a warning message when the remaining 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. |

# 45.4 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 334** Configuration > System > Date and Time




The following table describes the labels in this screen.

Table 236 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.<br>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.<br>When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**. |

Table 236 Configuration > System > Date and Time (continued)

| LABEL | DESCRIPTION |
|---|---|
| Get from Time Server | 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.<br>• When the UAG starts up.<br>• When you click **Apply** or **Sync. Now** in this screen.<br>• 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 | 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.<br>Select this option if you use Daylight Saving Time. |
| Start Date | 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:<br>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.<br>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). |
| End Date | 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:<br>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.<br>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). |
| Offset | Specify how much the clock changes when daylight saving begins and ends.<br>Enter a number from 1 to 5.5 (by 0.5 increments).<br>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. |
| Apply | Click **Apply** to save your changes back to the UAG. |
| Reset | Click **Reset** to return the screen to its last-saved settings. |

## 45.4.1 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 237 Default Time Servers

| |
|---|
| 0.pool.ntp.org |
| 1.pool.ntp.org |
| 2.pool.ntp.org |

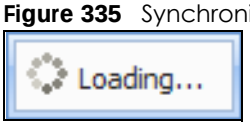
When the UAG uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the UAG goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

## 45.4.2 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 335** 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 237 on page 500).

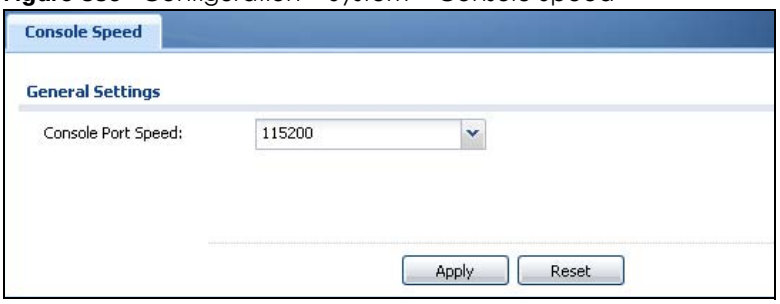
6 Click **Apply**.

# 45.5 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 336** Configuration > System > Console Speed




The following table describes the labels in this screen.

Table 238 Configuration > System > Console Speed

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| 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.<br>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. |

# 45.6 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.

## 45.6.1 DNS Server Address Assignment

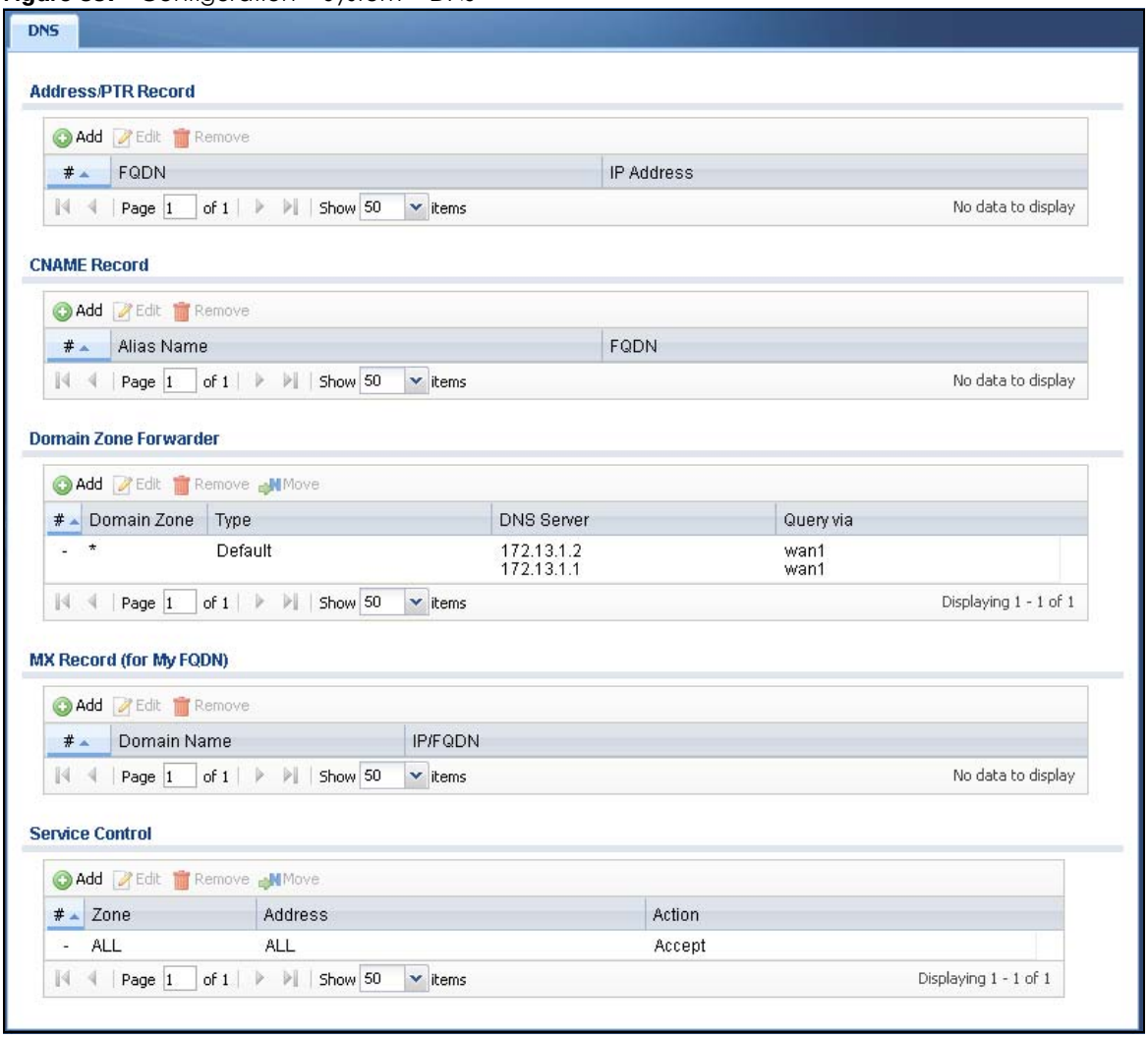
The UAG can get the DNS server addresses in the following ways.

- 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.

## 45.6.2 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 337** Configuration > System > DNS




The following table describes the labels in this screen.

Table 239 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. |
| 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 45.6.6 on page 506) for more details. |

Table 239 Configuration > System > DNS (continued)

| 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. 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.<br><br>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.<br><br>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.<br><br>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.<br><br>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. |
| 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. |

Table 239 Configuration > System > DNS (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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.<br>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**). |

## 45.6.3 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.

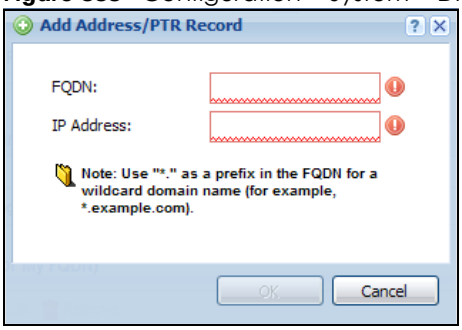
## 45.6.4 PTR Record

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.

## 45.6.5 Adding an Address/PTR Record

Click the **Add** icon in the **Address/PTR Record** table to add an address/PTR record.

**Figure 338** Configuration > System > DNS > Address/PTR Record Add




The following table describes the labels in this screen.

Table 240 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.<br><br>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 |

## 45.6.6 CNAME Record

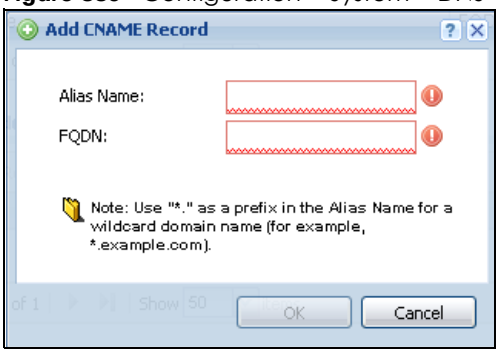
A Canonical Name Record or CNAME record is a type of resource record in the Domain Name System (DNS) that specifies that the domain name is an alias of another, canonical domain name. This allows users to set up a record for a domain name which translates to an IP address, in other words, the domain 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.

## 45.6.7 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 339** Configuration > System > DNS > CNAME Record > Add




The following table describes the labels in this screen.

Table 241 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.<br><br>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 |

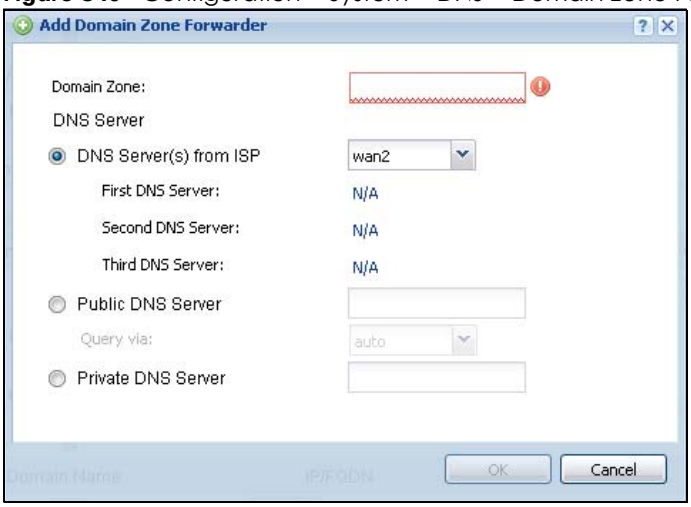
## 45.6.8 Domain Zone Forwarder

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.

## 45.6.9 Adding a Domain Zone Forwarder

Click the **Add** icon in the **Domain Zone Forwarder** table to add a domain zone forwarder record.

**Figure 340** Configuration > System > DNS > Domain Zone Forwarder Add




The following table describes the labels in this screen.

Table 242 Configuration > System > DNS > Domain Zone Forwarder Add

| LABEL | DESCRIPTION |
|---|---|
| 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. 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.<br><br>Enter * if all domain zones are served by the specified DNS server(s). |
| DNS Server | 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.<br><br>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.<br><br>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. |
| OK | Click **OK** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving |

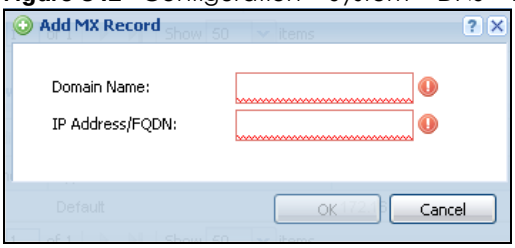
## 45.6.10 MX Record

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.

## 45.6.11 Adding a MX Record

Click the **Add** icon in the **MX Record** table to add a MX record.

**Figure 341** Configuration > System > DNS > MX Record Add




The following table describes the labels in this screen.

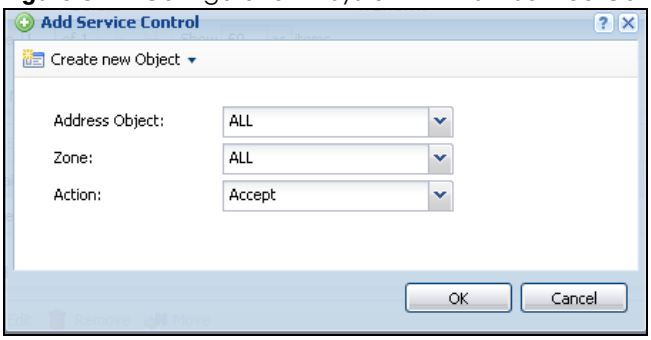
Table 243 Configuration > System > DNS > MX Record Add

| 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 |

## 45.6.12 Adding a DNS Service Control Rule

Click the **Add** icon in the **Service Control** table to add a service control rule.

**Figure 342** Configuration > System > DNS > Service Control Rule Add




The following table describes the labels in this screen.

Table 244 Configuration > System > DNS > Service Control 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.<br>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.<br>Select a predefined zone on which a DNS query to the UAG is allowed or denied. |
| Action | Select **Accept** to have the UAG allow the DNS queries from the specified computer.<br>Select **Deny** to have the UAG reject the DNS queries from the specified computer. |

Table 244 Configuration > System > DNS > Service Control Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| OK | Click **OK** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving |

# 45.7 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 301 for more on To-Device security policies.

To stop a service from accessing the UAG, clear **Enable** in the corresponding service screen.

## 45.7.1 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.

## 45.7.2 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.

## 45.7.3 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 43 on page 476 for more information).

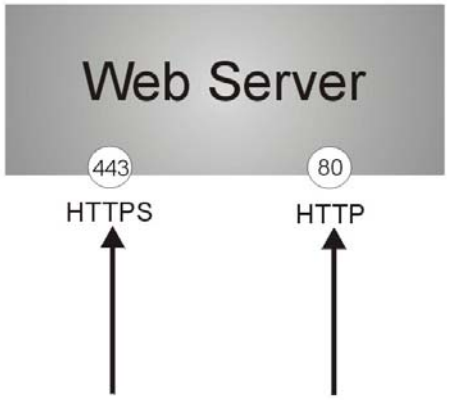
HTTPS on the UAG is used so that you can securely access the UAG using the Web Configurator. The SSL protocol specifies that the HTTPS server (the UAG) must always authenticate itself to the HTTPS client (the computer which requests the HTTPS connection with the UAG), whereas the HTTPS client only should 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 343** HTTP/HTTPS Implementation



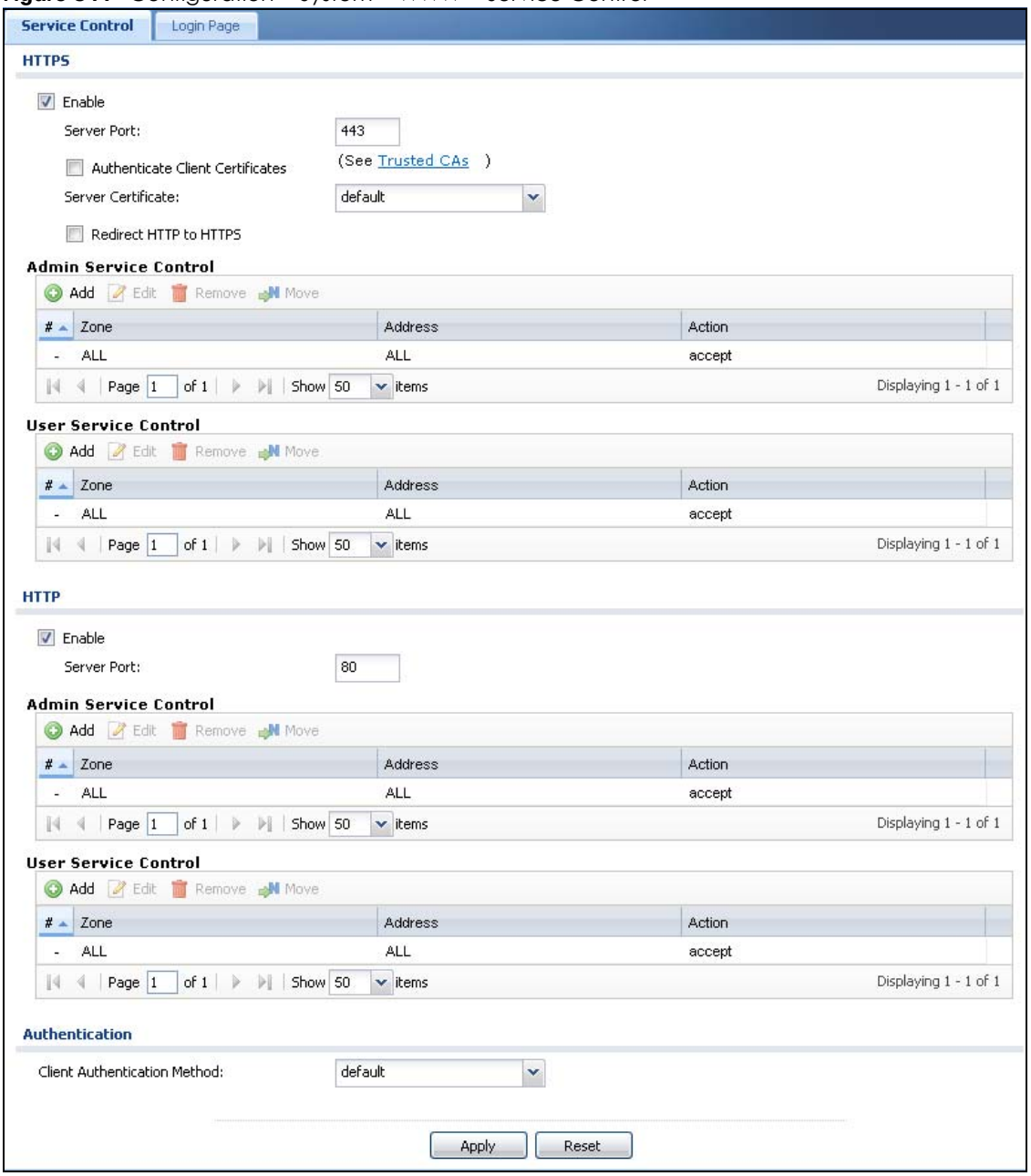

Note: If you disable **HTTP** in the **WWW** screen, then the UAG blocks all HTTP connection attempts.

## 45.7.4 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 344** Configuration > System > WWW > Service Control




The following table describes the labels in this screen.

Table 245 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. |
| 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. |

Table 245 Configuration > System > WWW > Service Control (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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 45.7.7.5 on page 522 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.<br><br>**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.<br><br>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. |
| 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.<br><br>**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. |

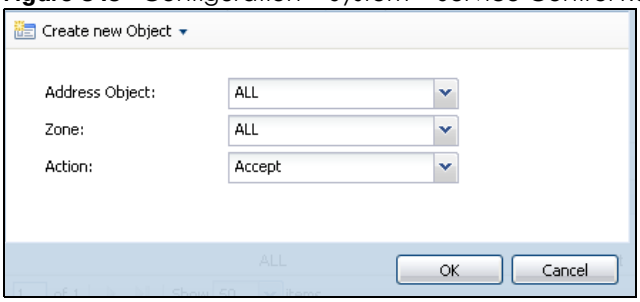
Table 245 Configuration > System > WWW > Service Control (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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.<br>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.<br>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. |

## 45.7.5 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 345** Configuration > System > Service Control Rule > Add/Edit




The following table describes the labels in this screen.

Table 246 Configuration > System > Service Control Rule > Add/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.<br>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.<br>Select a predefined UAG zone on which a incoming service is allowed or denied. |

Table 246 Configuration > System > Service Control Rule > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Action | Select **Accept** to allow the user to access the UAG from the specified computers.<br>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 |

## 45.7.6 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 34 on page 408 for more on access user accounts. You can configure both the desktop and mobile versions of the service pages. Users click a link in the pages to switch between the two versions.

**Figure 346** Configuration > System > WWW > Login Page (Desktop View)

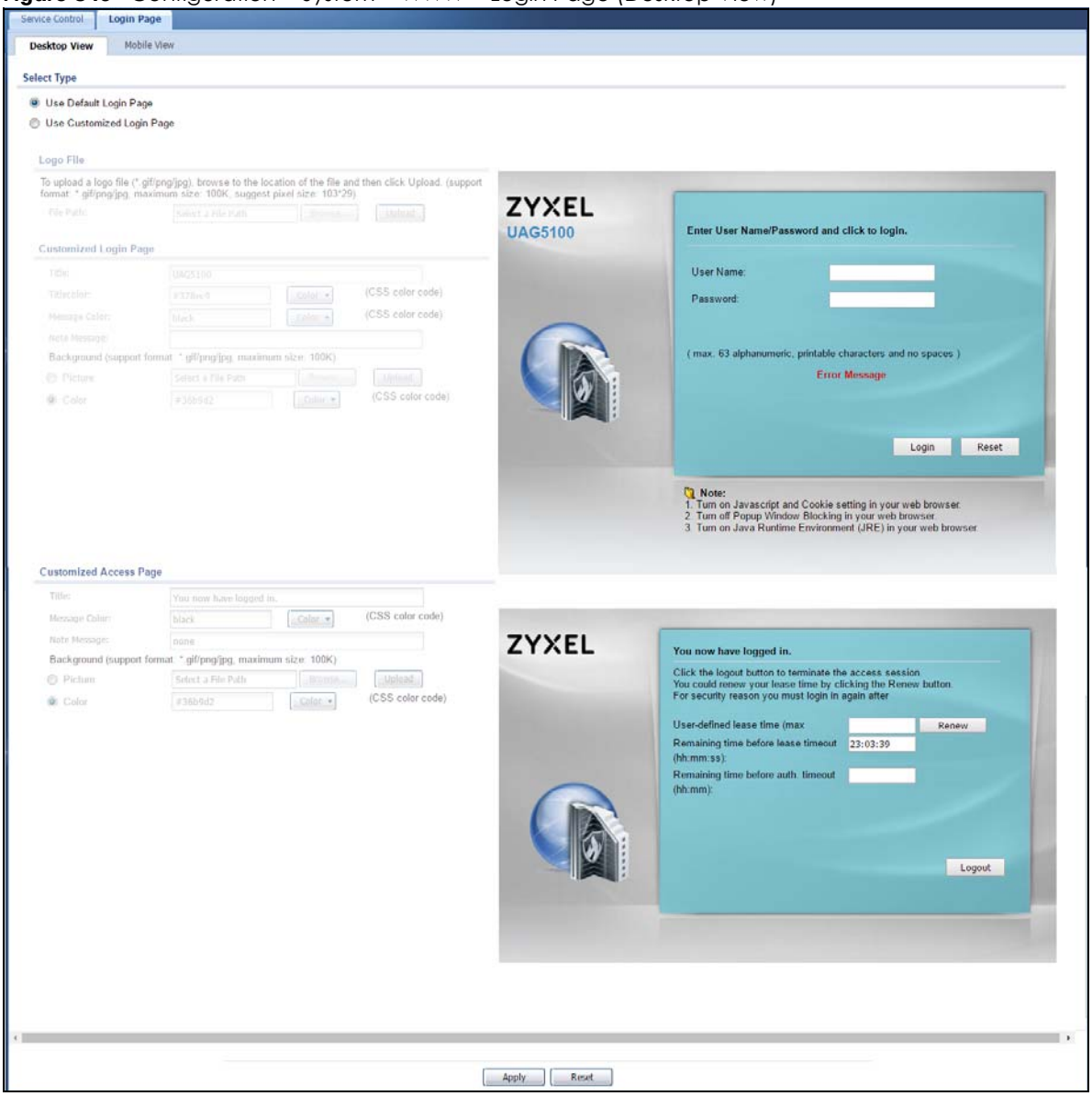
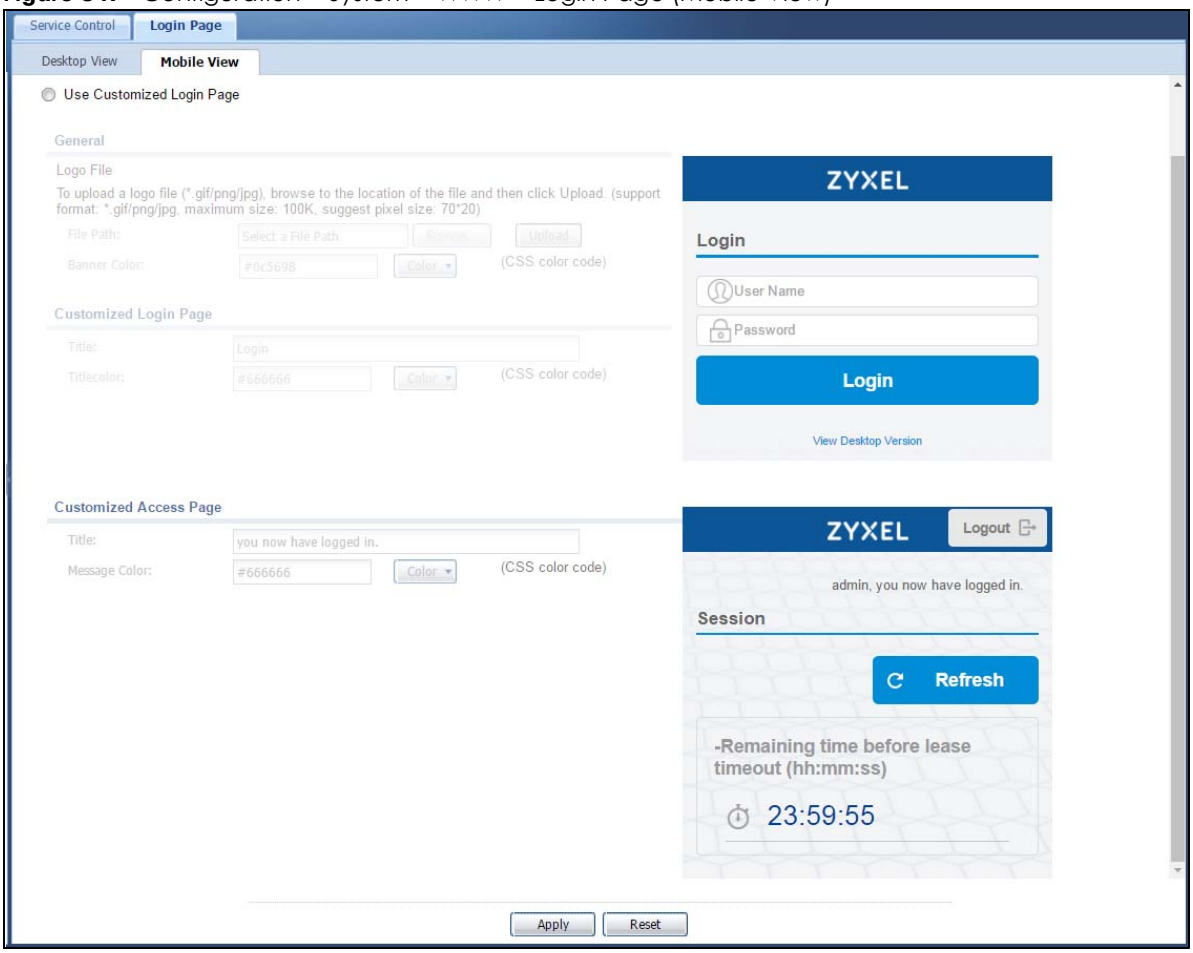


**Figure 347** Configuration > System > WWW > Login Page (Mobile View)




The following figures identify the parts you can customize in the login and access pages.

**Figure 348** Login Page Customization

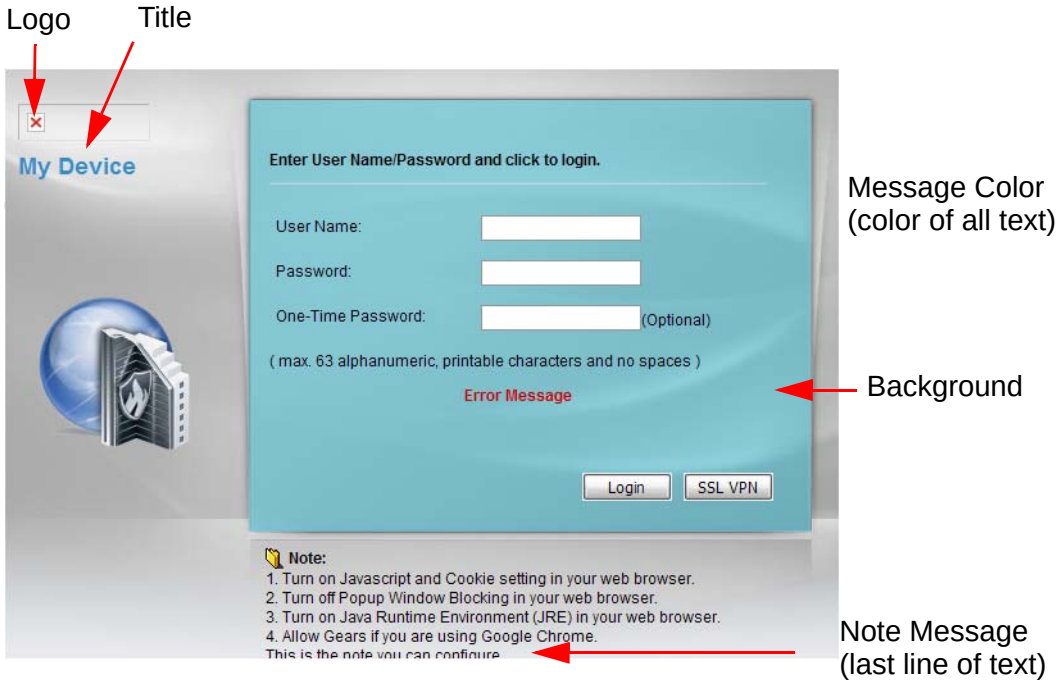
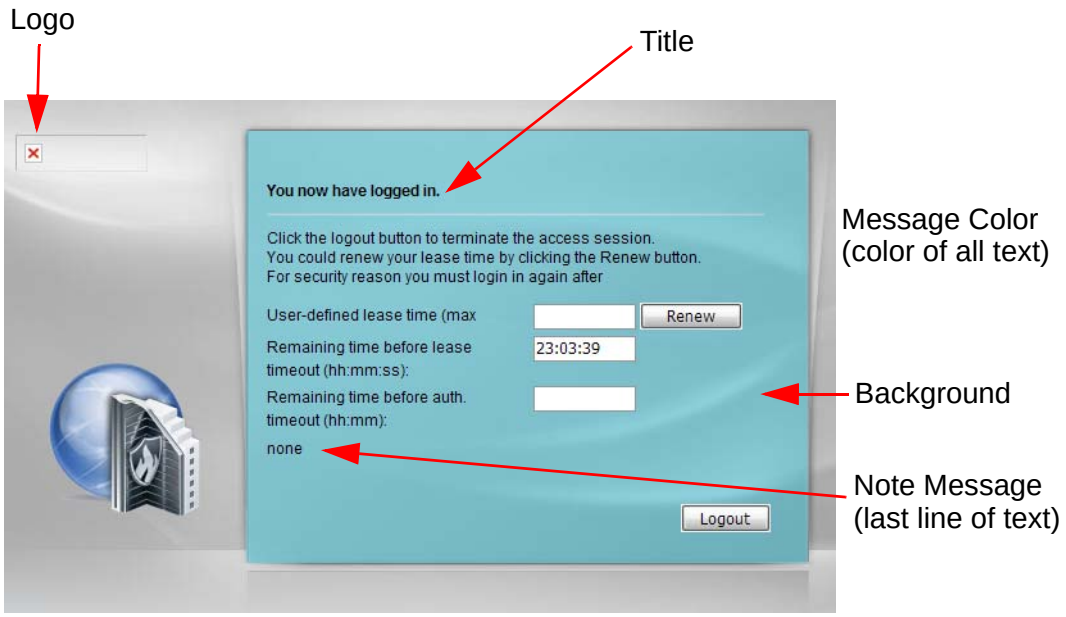



**Figure 349** Access Page Customization




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 247 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.<br>Specify the location and file name of the logo graphic or click **Browse** to locate it.<br>Note: Use a GIF, JPG, or PNG of 100 kilobytes or less.<br>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.<br>This field is not applicable to the mobile version. |
| Background | Set how the screen background looks.<br>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.<br>Note: Use a GIF, JPG, or PNG of 100 kilobytes or less.<br>To use a color, select **Color** and specify the color.<br>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.<br>This field is not applicable to the mobile version. |

Table 247 Configuration > System > WWW > Login Page

| LABEL | DESCRIPTION |
|---|---|
| Background | Set how the window's background looks.<br>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.<br>Note: Use a GIF, JPG, or PNG of 100 kilobytes or less.<br>To use a color, select **Color** and specify the color.<br>This field is not applicable to the mobile version. |
| Apply | Click **Apply** to save your changes back to the UAG. |
| Reset | Click **Reset** to return the screen to its last-saved settings. |

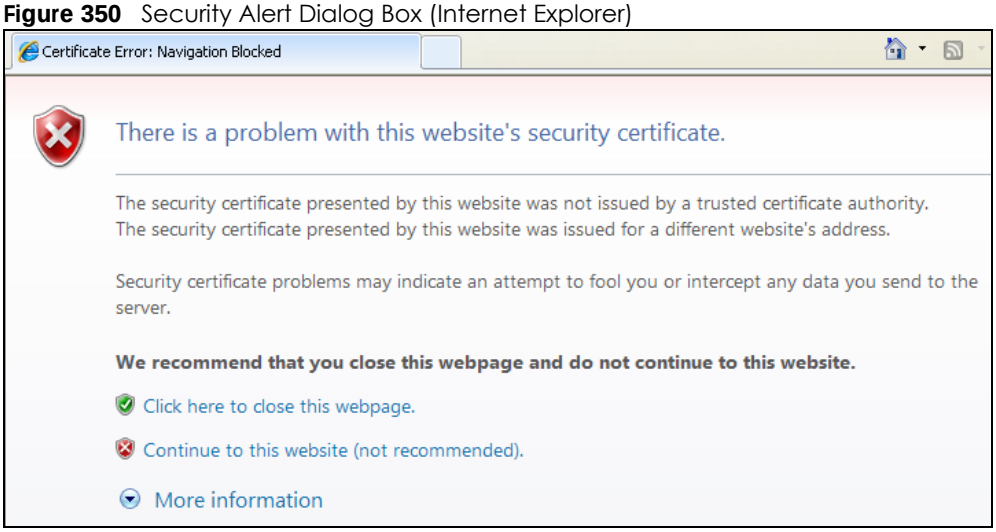
## 45.7.7 HTTPS Example

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.

### 45.7.7.1 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 350** 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.

### 45.7.7.2 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 351** Security Certificate 1 (Firefox)

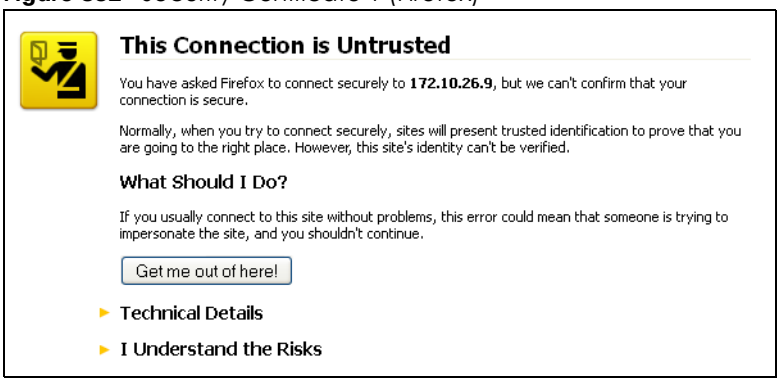
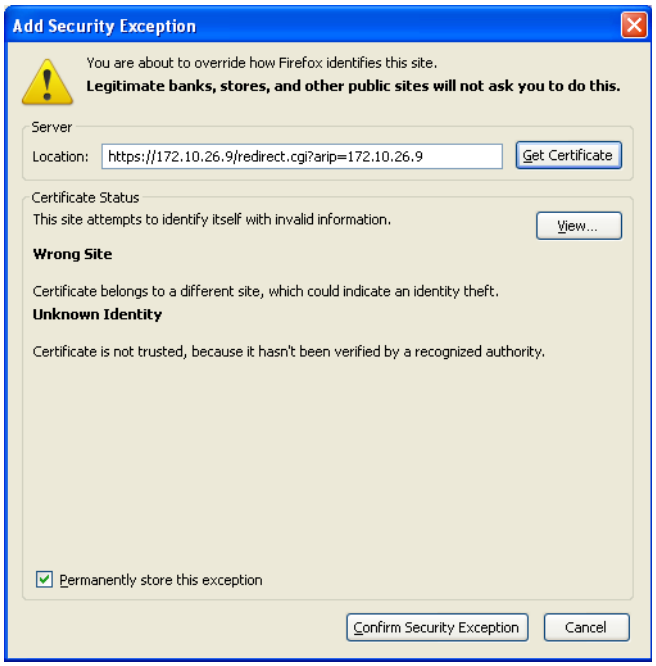



**Figure 352** Security Certificate 2 (Firefox)




## 45.7.7.3 Avoiding Browser Warning Messages

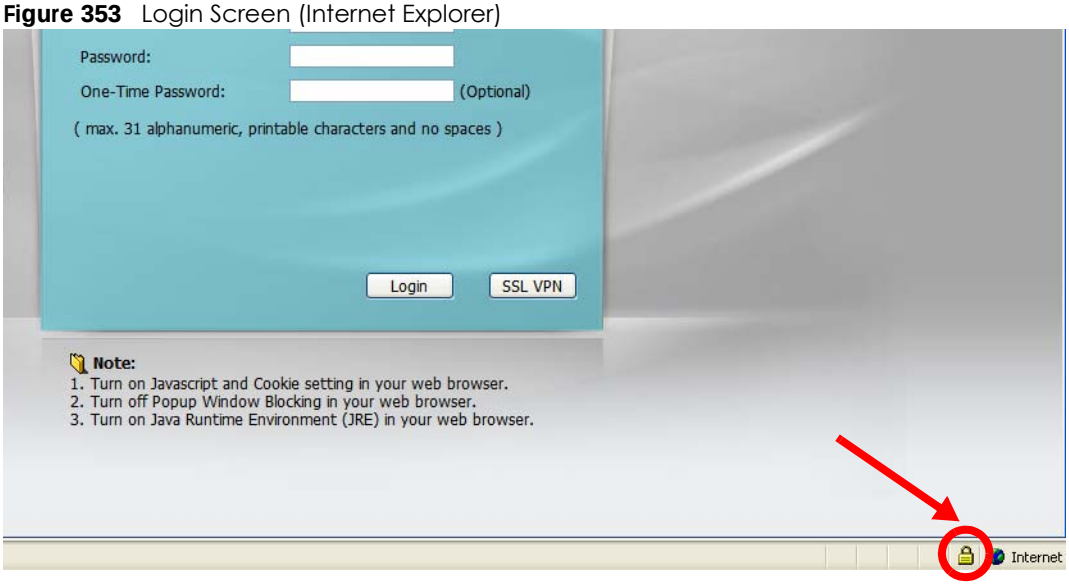
Here are the main reasons your browser displays warnings about the UAG's HTTPS server certificate and what you can do to avoid seeing the warnings:

- 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.

### 45.7.7.4 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 353** Login Screen (Internet Explorer)



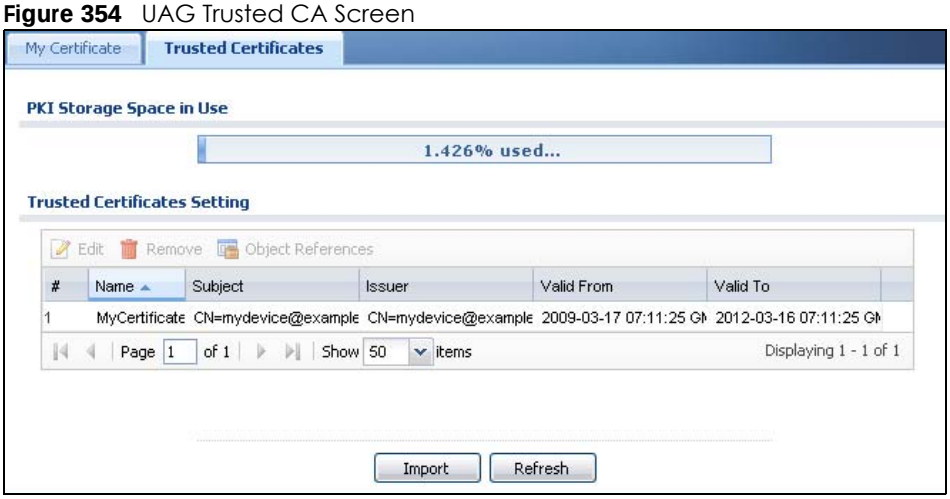

### 45.7.7.5 Enrolling and Importing SSL Client Certificates

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 354** UAG Trusted CA Screen

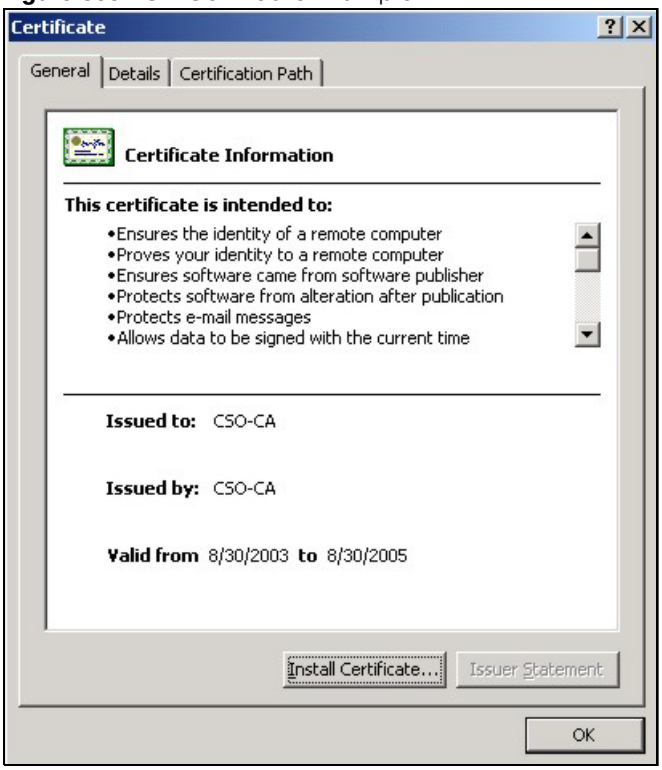



The CA sends you a package containing the CA's trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

#### 45.7.7.5.1 Installing the CA's Certificate

1 Double click the CA's trusted certificate to produce a screen similar to the one shown next.

**Figure 355** CA Certificate Example




2 Click **Install Certificate** and follow the wizard as shown earlier in this appendix.

#### 45.7.7.5.2 Installing Your Personal Certificate(s)

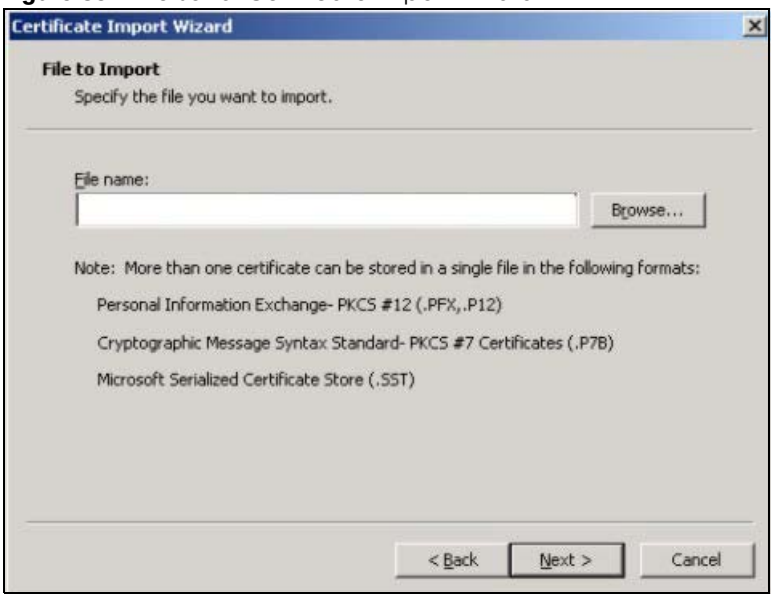
You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next

1 Click **Next** to begin the wizard.

**Figure 356** 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 357** Personal Certificate Import Wizard 2

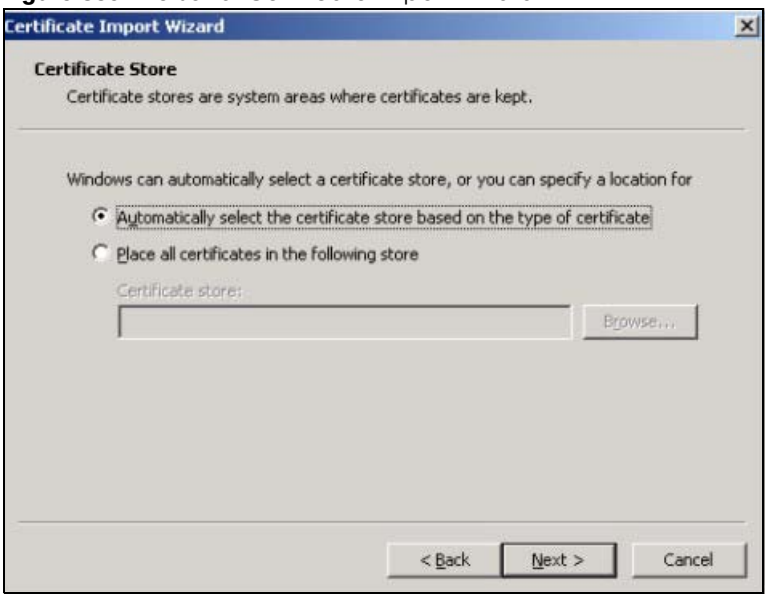



3 Enter the password given to you by the CA.

**Figure 358** Personal Certificate Import Wizard 3

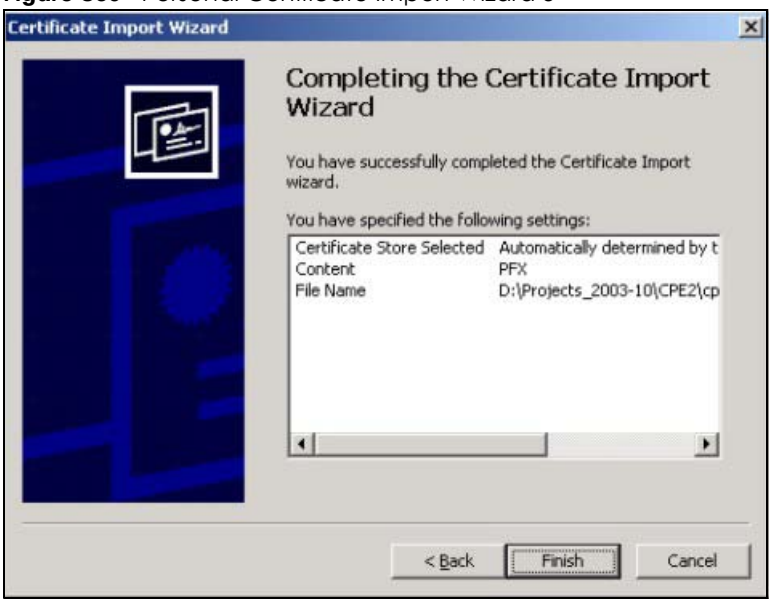
4 Have the wizard determine where the certificate should be saved on your computer or select **Place all certificates in the following store** and choose a different location.

**Figure 359** Personal Certificate Import Wizard 4




5 Click **Finish** to complete the wizard and begin the import process.

**Figure 360** Personal Certificate Import Wizard 5




6 You should see the following screen when the certificate is correctly installed on your computer.

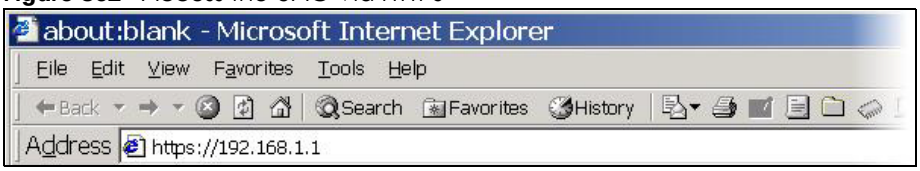
**Figure 361** Personal Certificate Import Wizard 6

### 45.7.7.6 Using a Certificate When Accessing the UAG Example

Use the following procedure to access the UAG via HTTPS.

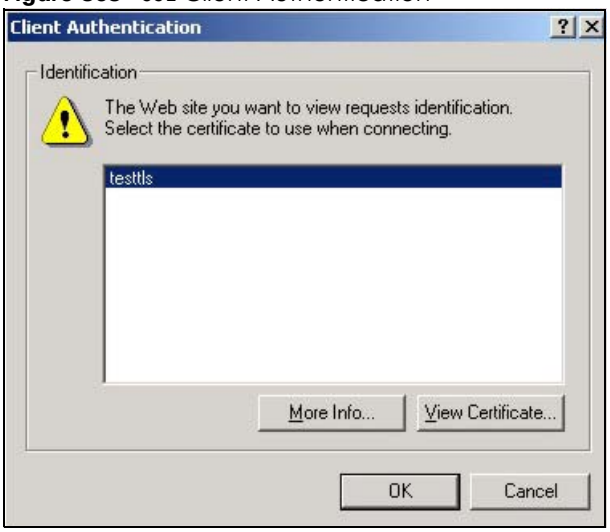
1 Enter 'https://UAG IP Address/ in your browser's web address field.

**Figure 362** Access the UAG Via HTTPS



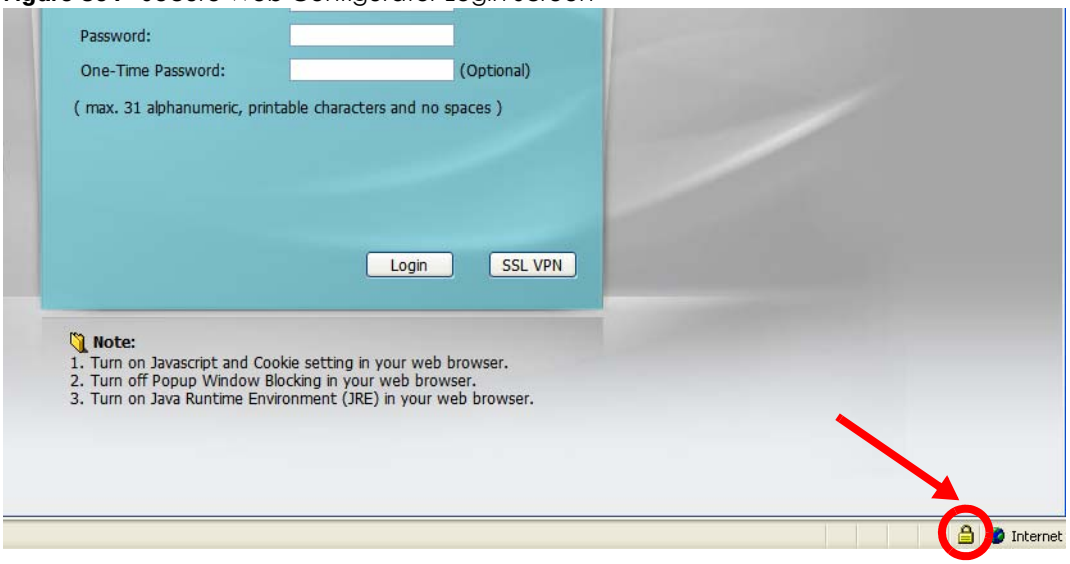

2 When **Authenticate Client Certificates** is selected on the UAG, the following screen asks you to select a personal certificate to send to the UAG. This screen displays even if you only have a single certificate as in the example.

**Figure 363** SSL Client Authentication




3 You next see the Web Configurator login screen.

**Figure 364** Secure Web Configurator Login Screen




# 45.8 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.

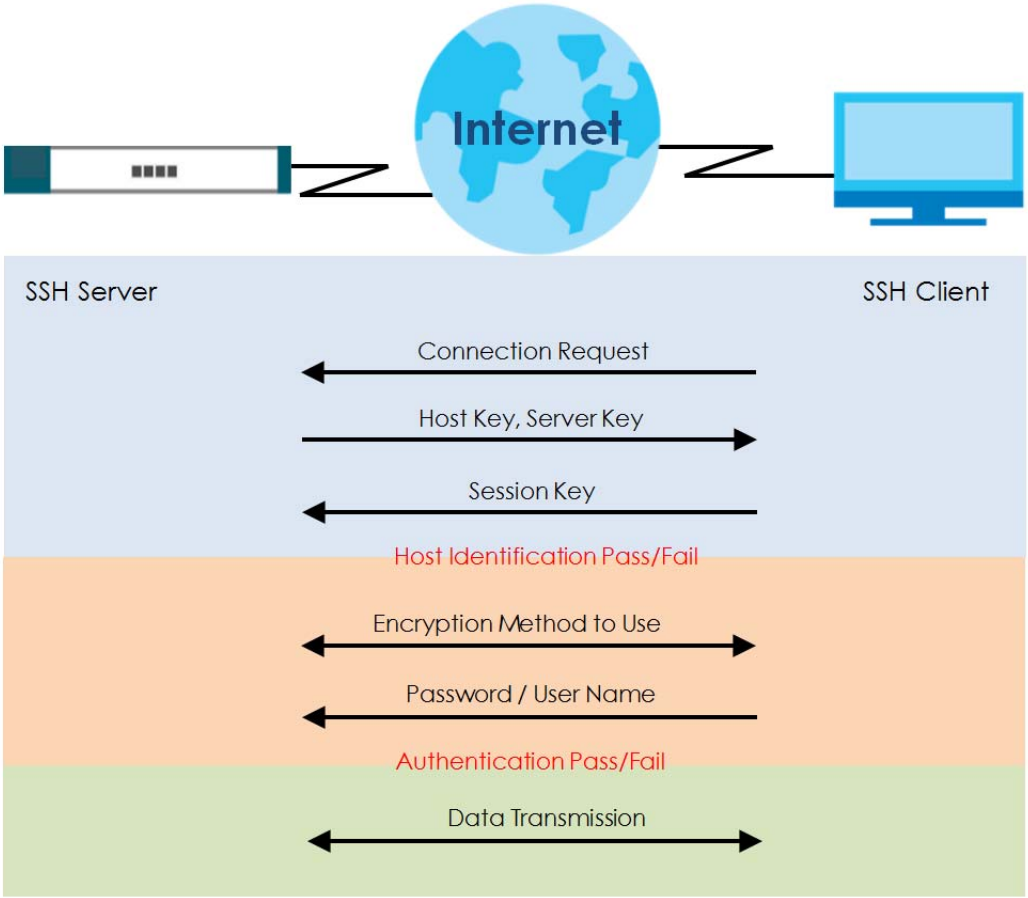
SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. In the following figure, computer A on the Internet uses SSH to securely connect to the WAN port of the UAG for a management session.

**Figure 365** SSH Communication Over the WAN Example

## 45.8.1 How SSH Works

The following figure is an example of how a secure connection is established between two remote hosts using SSH v1.

**Figure 366** 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.

## 45.8.2 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).

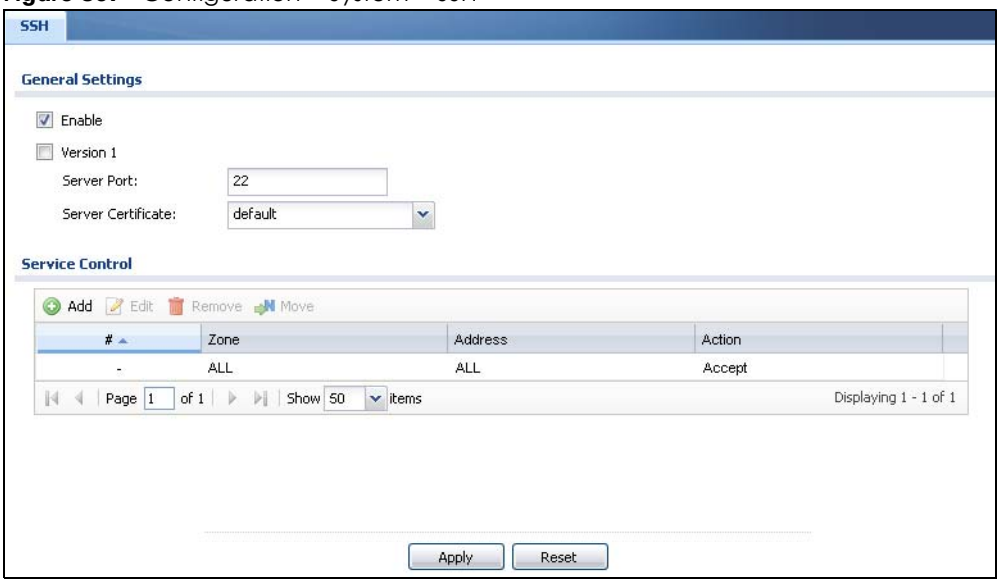
## 45.8.3 Requirements for Using SSH

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.

## 45.8.4 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 367** Configuration > System > SSH



The following table describes the labels in this screen.

Table 248 Configuration > System > SSH

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| 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. |
| 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 43 on page 476 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 246 on page 514 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. |

## 45.8.5 Secure Telnet Using SSH Examples

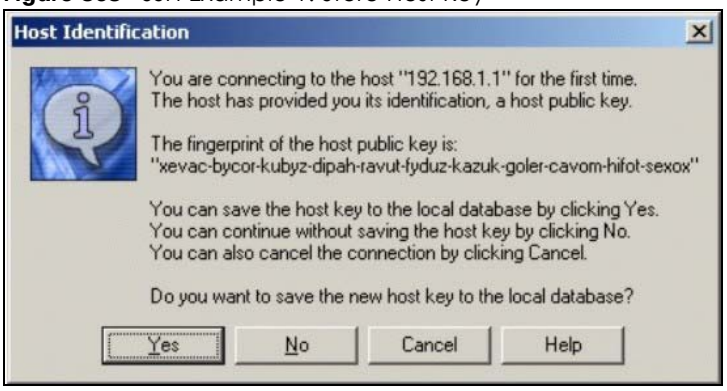
This section shows two examples using a command interface and a graphical interface SSH client program to remotely access the UAG. The configuration and connection steps are similar for most SSH client programs. Refer to your SSH client program user's guide.

### 45.8.5.1 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 368** SSH Example 1: Store Host Key




Enter the password to log in to the UAG. The CLI screen displays next.

### 45.8.5.2 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 369** 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 370** 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.

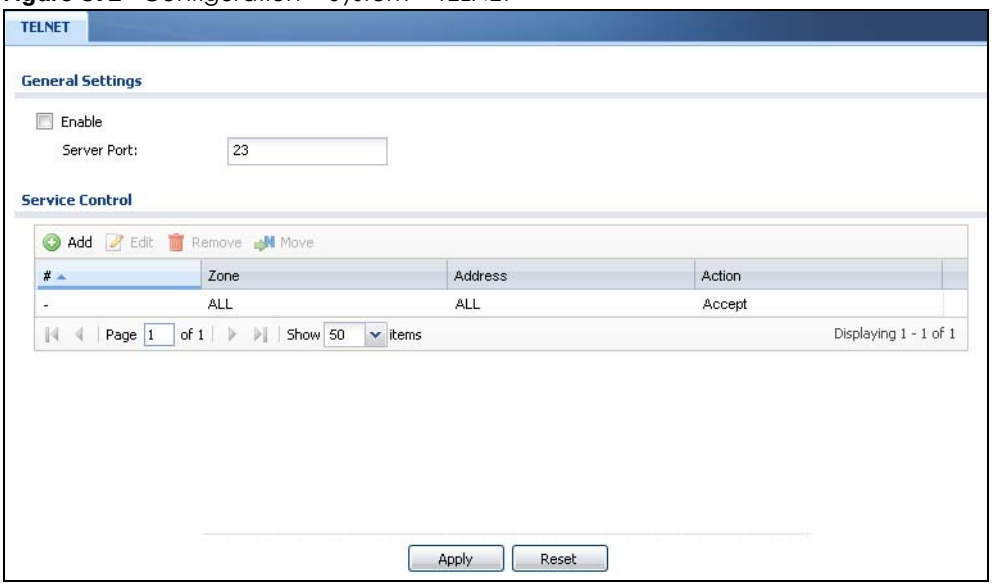
# 45.9 Telnet

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.

## 45.9.1 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 371** Configuration > System > TELNET




The following table describes the labels in this screen.

Table 249 Configuration > System > TELNET

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| 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 246 on page 514 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 249 Configuration > System > TELNET (continued)

| LABEL | DESCRIPTION |
|---|---|
| # | This the index number of the service control rule.<br><br>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. |

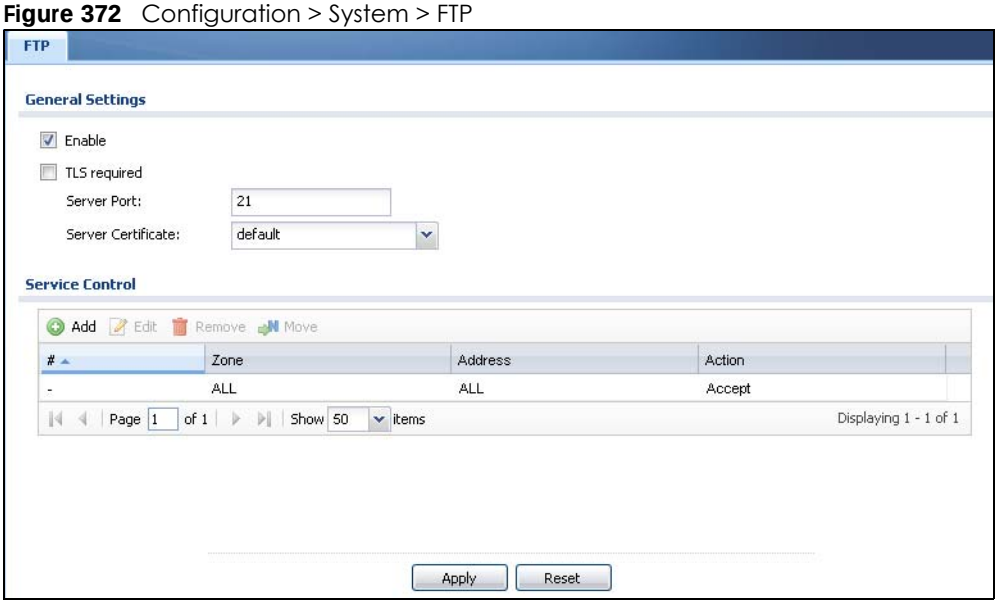
# 45.10 FTP

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 47 on page 558 for more information about firmware and configuration files.

## 45.10.1 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 372** Configuration > System > FTP



The following table describes the labels in this screen.

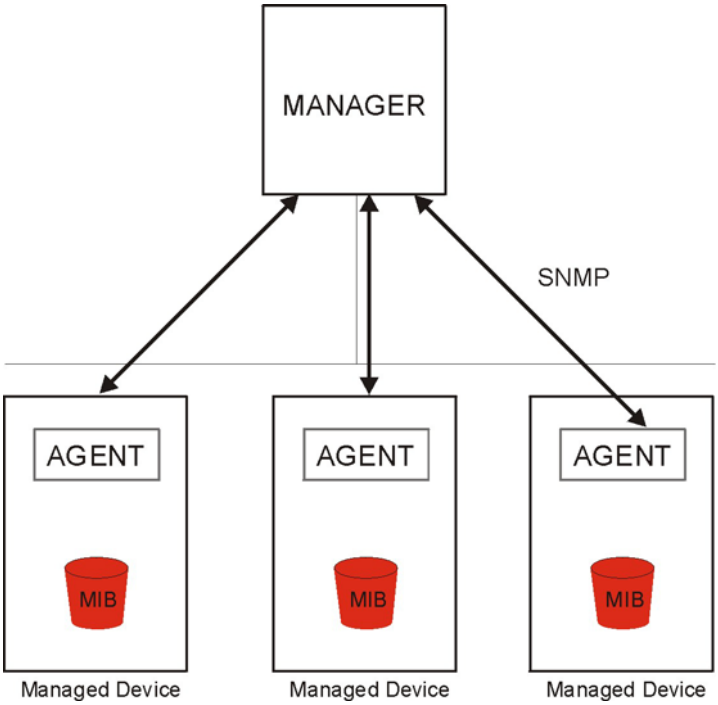
Table 250 Configuration > System > FTP

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| 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.<br>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 43 on page 476 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 246 on page 514 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.<br>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. |

# 45.11 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 373** 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.

## 45.11.1 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.

## 45.11.2 SNMP Traps

The UAG will send traps to the SNMP manager when any one of the following events occurs.

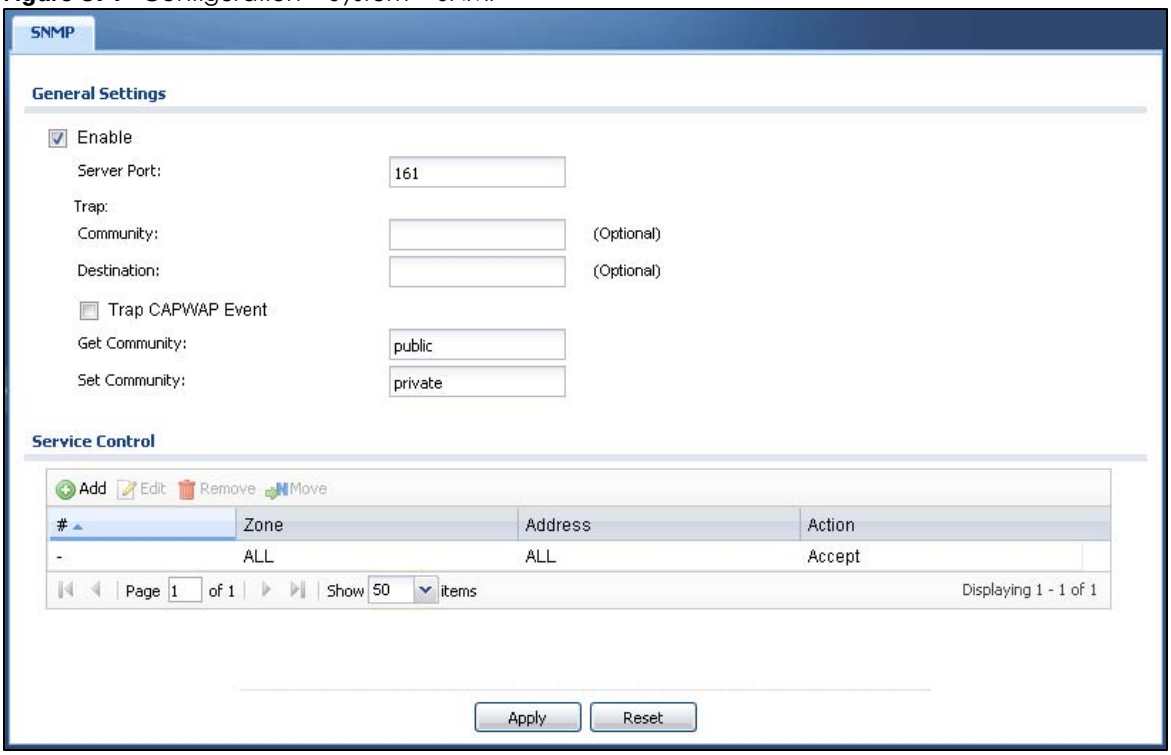
Table 251 SNMP Traps

| 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. |

## 45.11.3 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 374** Configuration > System > SNMP




The following table describes the labels in this screen.

Table 252 Configuration > System > SNMP

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| 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. |

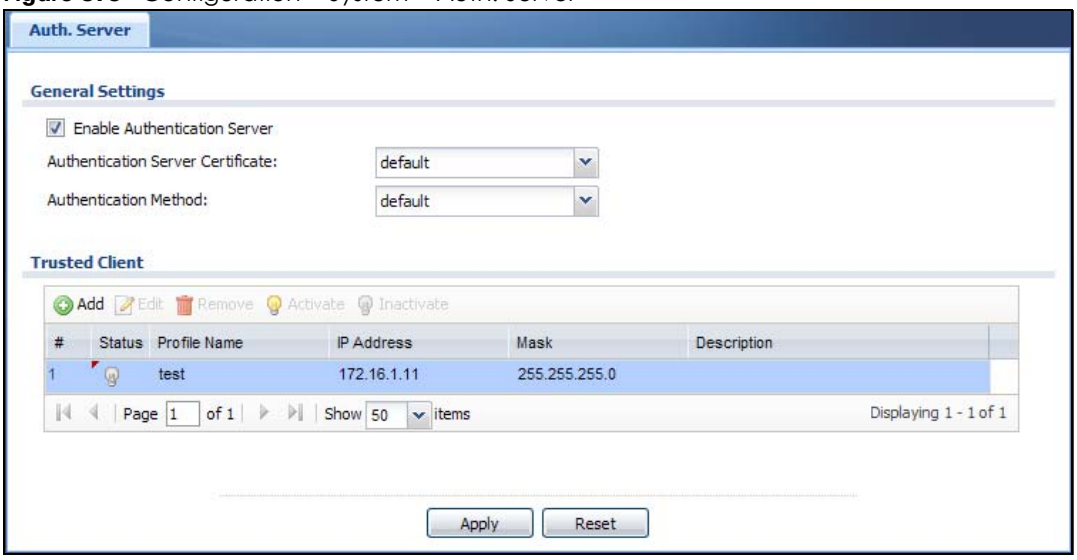
Table 252 Configuration > System > SNMP (continued)

| 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. |
| 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 246 on page 514 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.<br>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. |

# 45.12 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 375** Configuration > System > Auth. Server




The following table describes the labels in this screen.

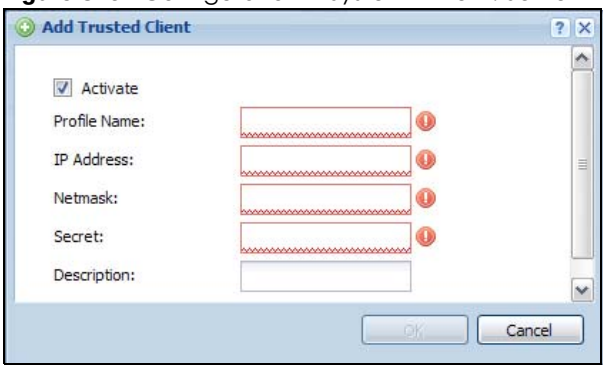
Table 253 Configuration > System > Auth. Server

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| 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. |

## 45.12.1 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 376** Configuration > System > Auth. Server > Add/Edit




The following table describes the labels in this screen.

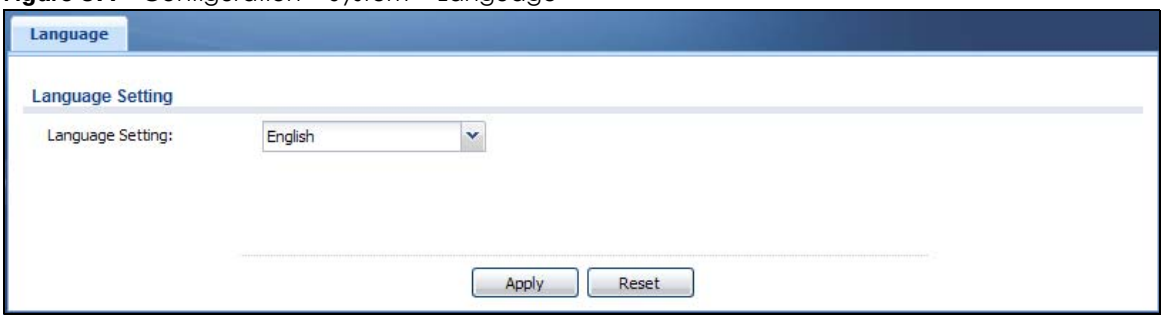
Table 254 Configuration > System > Auth. Server > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Activate | Select this check box to make this profile active. |
| Profile Name | Enter a descriptive name (up to 31 alphanumerical characters) for identification purposes.<br>The value in this field must begin with a letter and cannot exceed 31 characters. The valid characters are [0-9][a-z][A-Z][_-]. |
| 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.<br>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. |

# 45.13 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 377** Configuration > System > Language




The following table describes the labels in this screen.

Table 255 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. |

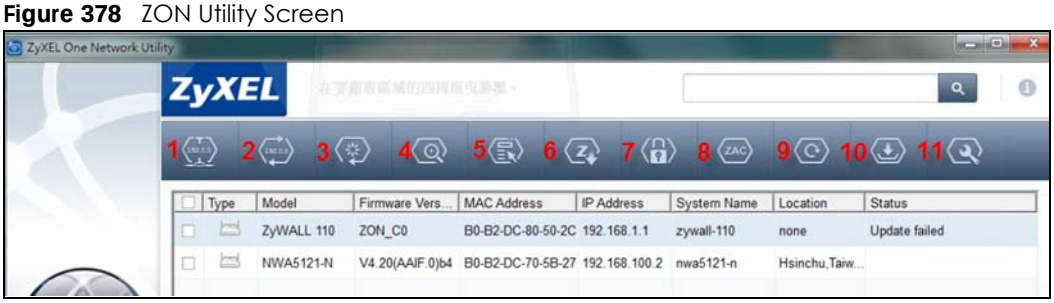
# 45.14 Zyxel One Network (ZON) Utility

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 378** 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 256 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 257 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. |

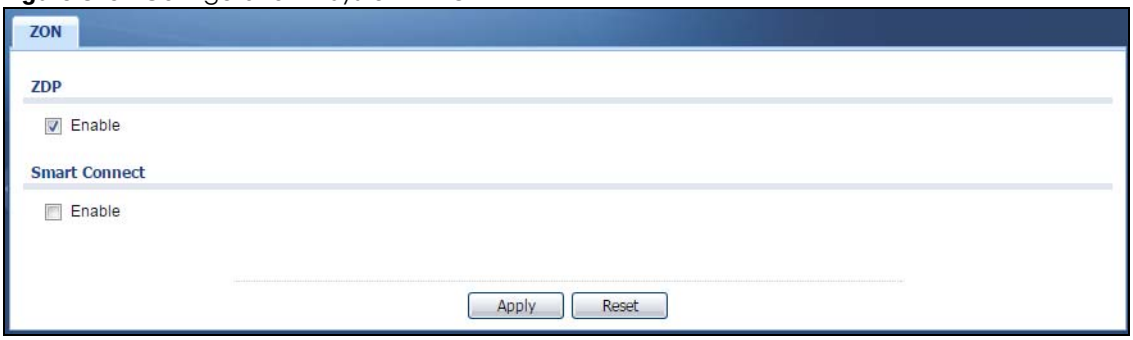
## 45.14.1 Zyxel One Network (ZON) System Screen

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 379** Configuration > System > ZON




The following table describes the labels in this screen.

Table 258 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. |

# CHAPTER 46
# Log and Report

## 46.1 Overview

Use these screens to configure daily reporting and log settings.

### 46.1.1 What You Can Do In this Chapter

- Use the **Email Daily Report** screen (Section 46.2 on page 543) to configure where and how to send daily reports and what reports to send.
- Use the **Log Settings** screens (Section 46.3 on page 545) 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.

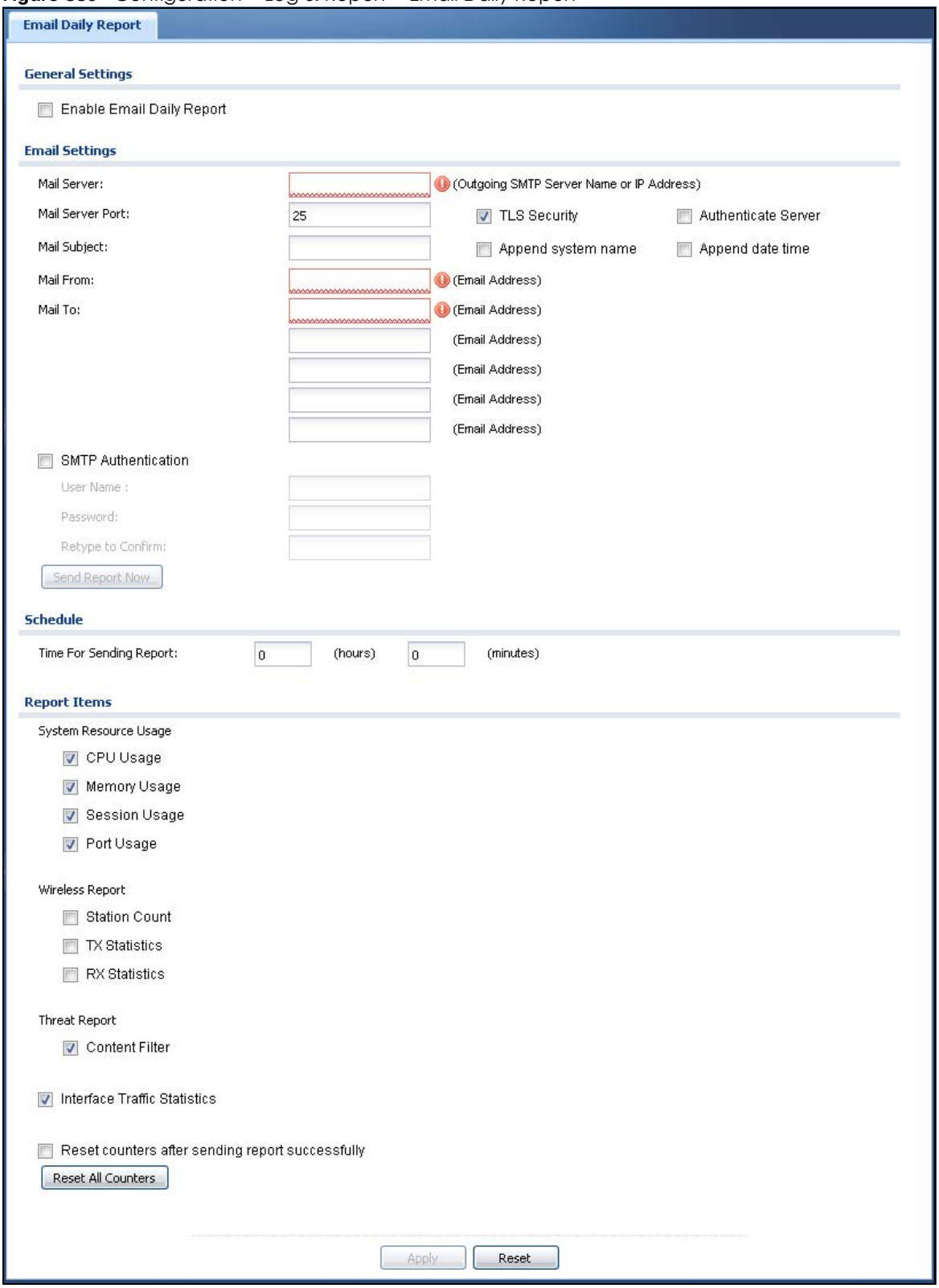
## 46.2 Email Daily Report

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 380** Configuration > Log & Report > Email Daily Report



The following table describes the labels in this screen.

Table 259 Configuration > Log & Report > Email Daily Report

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Enable Email Daily Report | Select this to send reports by e-mail every day. |
| Email Settings | |
| 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.<br>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. |

# 46.3 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.

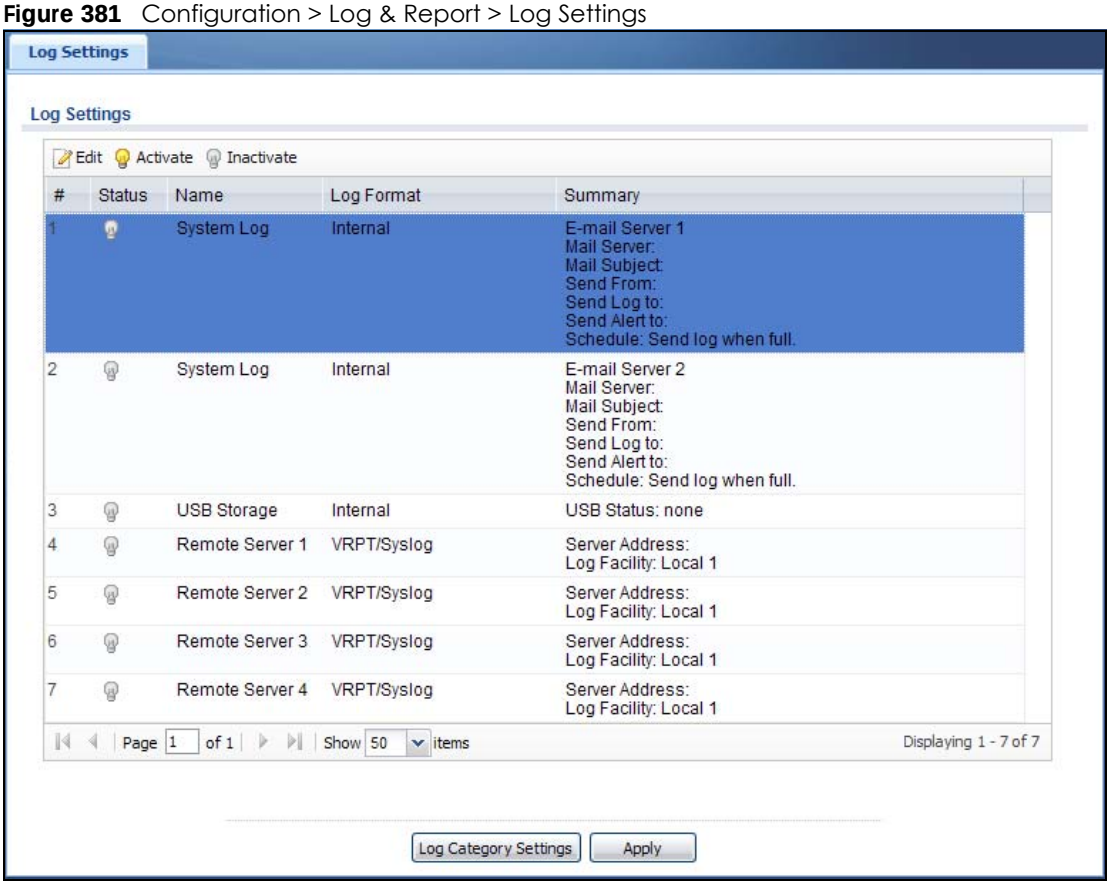
The **Log Settings** screens control what information the UAG saves in each log. You can also specify which log messages to e-mail for the system log, and where and how often to e-mail them. These screens also set for which events to generate alerts and where to email the alerts.

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.

## 46.3.1 Log Settings Summary

To access this screen, click **Configuration > Log & Report > Log Settings**.

**Figure 381** Configuration > Log & Report > Log Settings




The following table describes the labels in this screen.

Table 260 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**. |
| Inactivate | To turn off an entry, select it and click **Inactivate**. |

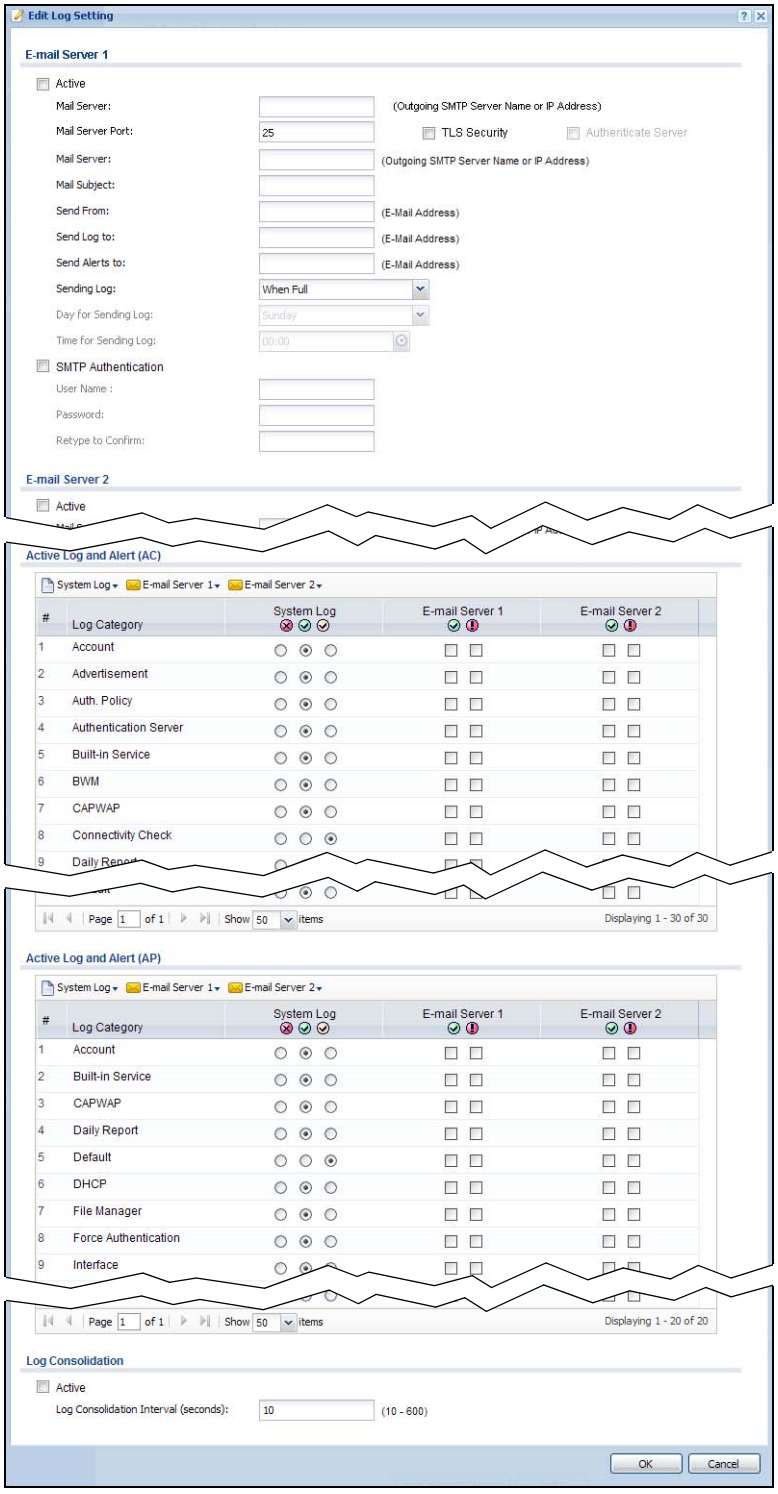
Table 260 Configuration > Log & Report > Log Settings (continued)

| LABEL | DESCRIPTION |
|---|---|
| # | 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.<br>**Internal** - system log; you can view the log on the **View Log** tab.<br>**VRPT/Syslog** - Zyxel's Vantage Report, syslog-compatible format.<br>**CEF/Syslog** - Common Event Format, syslog-compatible format. |
| Summary | This field is a summary of the settings for each log. Please see Section 46.3.2 on page 547 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. |

## 46.3.2 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 46.3.1 on page 546), and click the system log **Edit** icon.

**Figure 382** Configuration > Log & Report > Log Settings > Edit (System Log)



The following table describes the labels in this screen.

Table 261 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 | Use the **System Log** drop-down list to change the log settings for all of the log categories.<br>**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.<br>**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.<br>**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. |

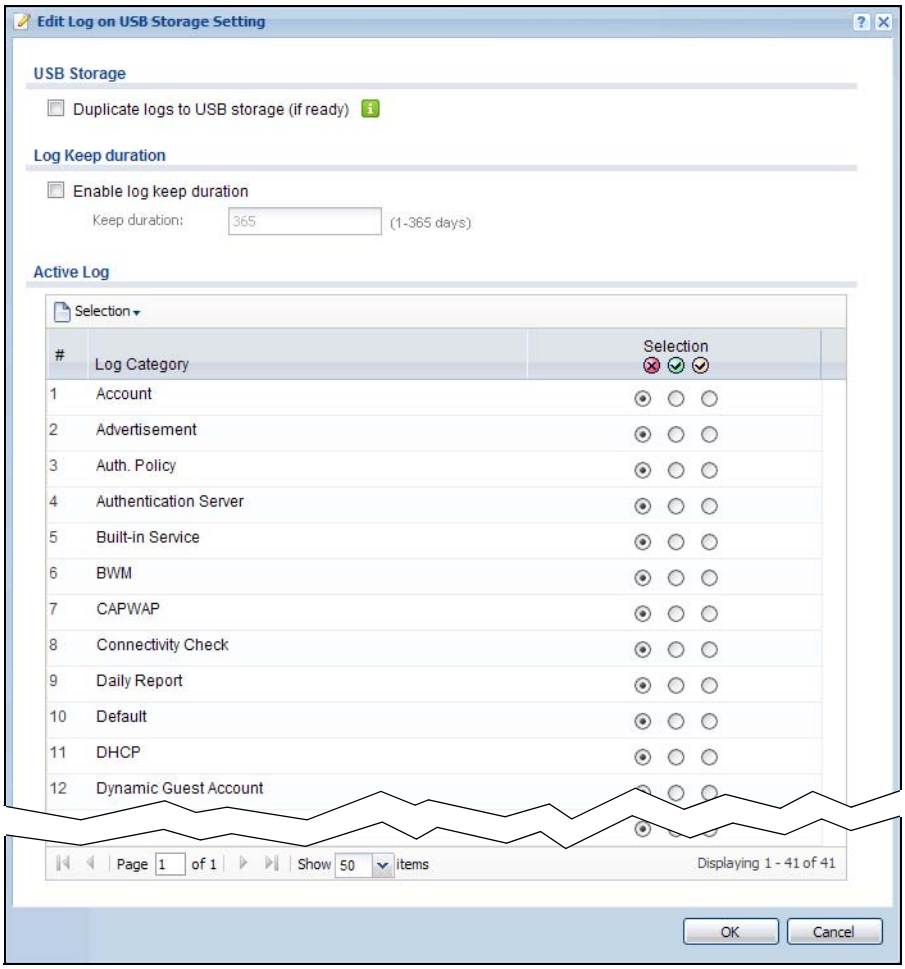
Table 261 Configuration > Log & Report > Log Settings > Edit (System Log) (continued)

| LABEL | DESCRIPTION |
|---|---|
| E-mail Server 1 | 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.<br>Using the **System Log** drop-down list to disable all logs overrides your e-mail server 1 settings.<br>**enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 1.<br>**enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 1. |
| E-mail Server 2 | 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.<br>Using the **System Log** drop-down list to disable all logs overrides your e-mail server 2 settings.<br>**enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 2.<br>**enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 2. |
| # | 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 | Select which events you want to log by **Log Category**. There are three choices:<br>**disable all logs** (red X) - do not log any information from this category<br>**enable normal logs** (green check mark) - create log messages and alerts from this category<br>**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. |
| 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 *x* 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 *x* 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. |

## 46.3.3 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 46.3.1 on page 546), and click the USB storage **Edit** icon.

**Figure 383** Configuration > Log & Report > Log Settings > Edit (USB Storage)




The following table describes the labels in this screen.

Table 262 Configuration > Log & Report > Log Settings > Edit (USB Storage)

| LABEL | DESCRIPTION |
|---|---|
| USB Storage | |
| 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. |
| Log Keep duration | |
| 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 | |

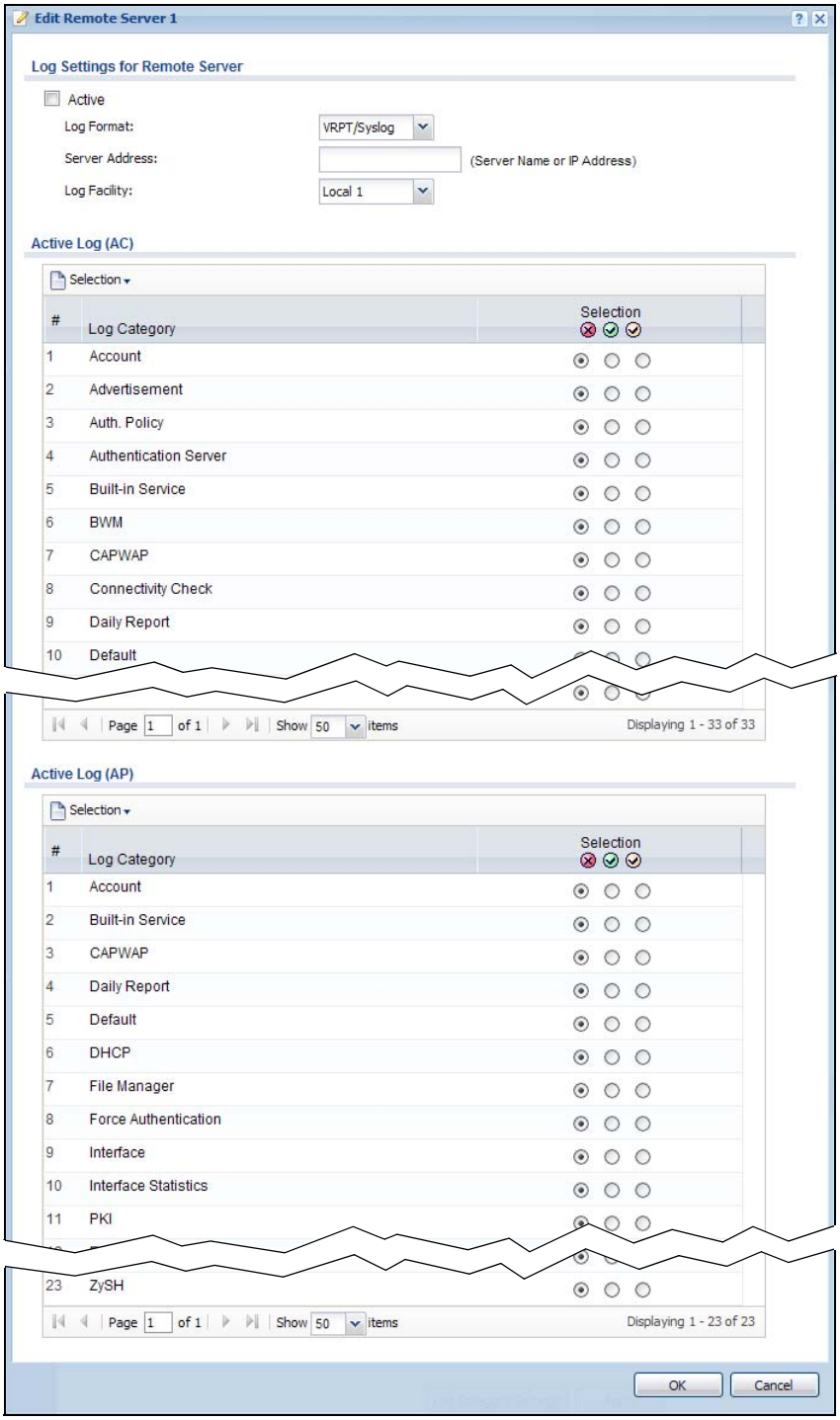
Table 262 Configuration > Log & Report > Log Settings > Edit (USB Storage) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Selection | Use the **Selection** drop-down list to change the log settings for all of the log categories.<br>**disable all logs** (red X) - do not send the remote server logs for any log category.<br>**enable normal logs** (green check mark) - send the remote server log messages and alerts for all log categories.<br>**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:<br>**disable all logs** (red X) - do not log any information from this category<br>**enable normal logs** (green check mark) - log regular information and alerts from this category<br>**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. |

## 46.3.4 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 46.3.1 on page 546), and click a remote server **Edit** icon.

**Figure 384** Configuration > Log & Report > Log Settings > Edit (Remote Server)



The following table describes the labels in this screen.

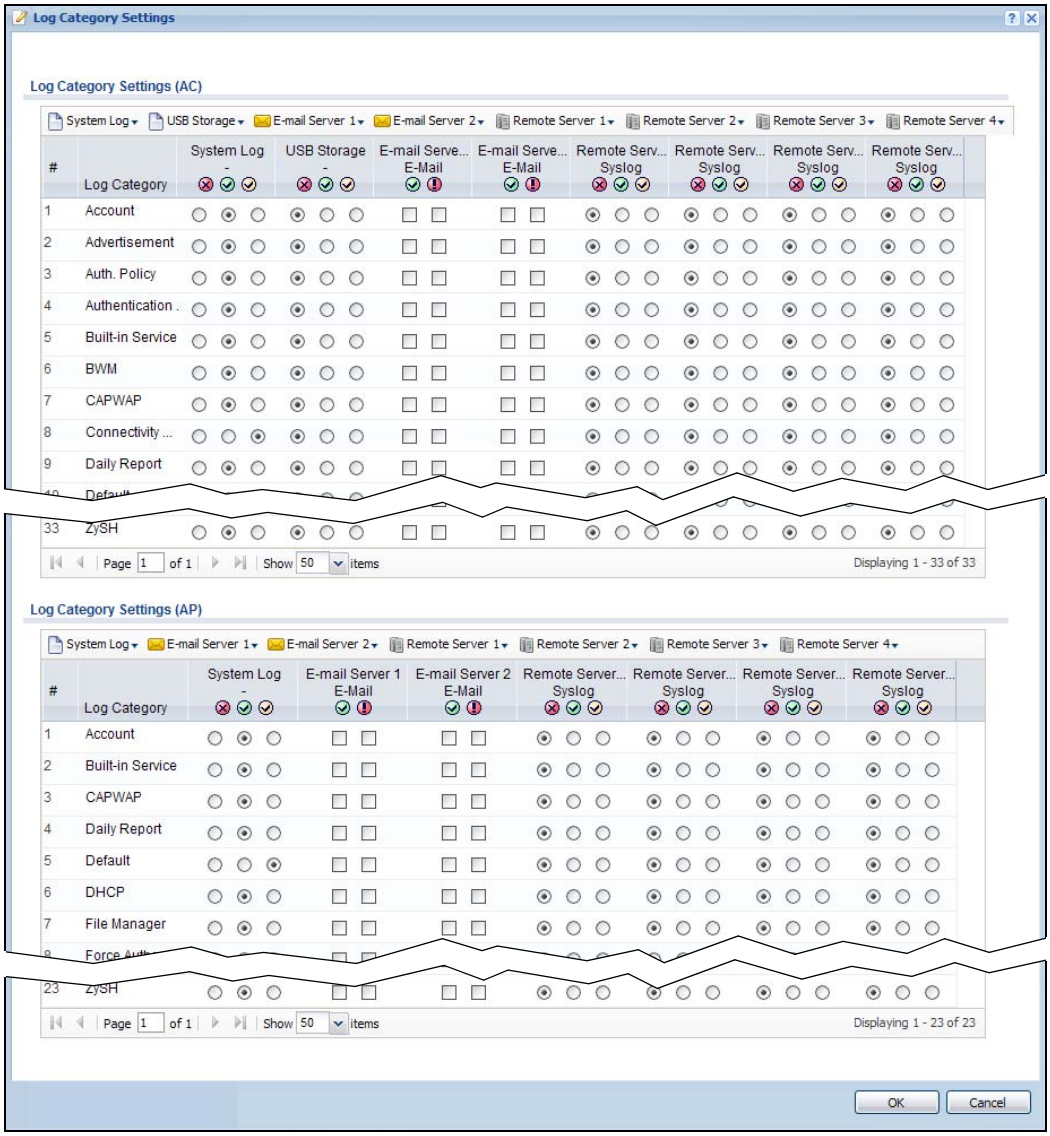
Table 263 Configuration > Log & Report > Log Setting > Edit (Remote Server)

| 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.<br>**VRPT/Syslog** - Zyxel's Vantage Report, syslog-compatible format.<br>**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 (AP/AC) | |
| Selection | Use the **Selection** drop-down list to change the log settings for all of the log categories.<br>**disable all logs** (red X) - do not send the remote server logs for any log category.<br>**enable normal logs** (green check mark) - send the remote server log messages and alerts for all log categories.<br>**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:<br>**disable all logs** (red X) - do not log any information from this category<br>**enable normal logs** (green check mark) - log regular information and alerts from this category<br>**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. |

## 46.3.5 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 46.3.1 on page 546), and click the **Log Category Settings** button.

**Figure 385** 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 46.3.2 on page 547, 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 264 Configuration > Log & Report > Log Setting > Log Category Settings

| LABEL | DESCRIPTION |
|---|---|
| Log Category Settings | |
| System Log | Use the **System Log** drop-down list to change the log settings for all of the log categories.<br>**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.<br>**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.<br>**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. |
| USB Storage | Use the **USB Storage** drop-down list to change the log settings for saving logs to a connected USB storage device.<br>**disable all logs** (red X) - do not log any information for any category to a connected USB storage device.<br>**enable normal logs** (green check mark) - create log messages and alerts for all categories and save them to a connected USB storage device.<br>**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. |
| E-mail Server 1 | 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.<br>Using the **System Log** drop-down list to disable all logs overrides your e-mail server 1 settings.<br>**enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 1.<br>**enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 1. |
| E-mail Server 2 | 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.<br>Using the **System Log** drop-down list to disable all logs overrides your e-mail server 2 settings.<br>**enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 2.<br>**enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 2. |
| Remote Server 1~4 | For each remote server, use the **Selection** drop-down list to change the log settings for all of the log categories.<br>**disable all logs** (red X) - do not send the remote server logs for any log category.<br>**enable normal logs** (green check mark) - send the remote server log messages and alerts for all log categories.<br>**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. |

Table 264 Configuration > Log & Report > Log Setting > Log Category Settings (continued)

| LABEL | DESCRIPTION |
|---|---|
| System Log | Select which events you want to log by **Log Category**. There are three choices:<br>**disable all logs** (red X) - do not log any information from this category<br>**enable normal logs** (green check mark) - create log messages and alerts from this category<br>**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. |
| USB Storage | Select which event log categories to save to a connected USB storage device. There are three choices:<br>**disable all logs** (red X) - do not log any information from this category<br>**enable normal logs** (green check mark) - save log messages and alerts from this category<br>**enable normal logs and debug logs** (yellow check mark) - save log messages, alerts, and debugging information from this category. |
| E-mail Server 1 E-mail | 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 E-mail | 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**. |
| Remote Server 1~4 Syslog | For each remote server, select what information you want to log from each **Log Category** (except **All Logs**; see below). Choices are:<br>**disable all logs** (red X) - do not log any information from this category<br>**enable normal logs** (green check mark) - log regular information and alerts from this category<br>**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. |

# CHAPTER 47
# File Manager

## 47.1 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.

### 47.1.1 What You Can Do in this Chapter

- Use the **Configuration File** screen (see Section 47.2 on page 560) 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 47.3 on page 564) to check your current firmware version and upload firmware to the UAG.
- Use the **Shell Script** screen (see Section 47.4 on page 565) to store, name, download, upload and run shell script files.

### 47.1.2 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 386** 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 265 Configuration Files and Shell Scripts in the UAG

| Configuration Files (.conf) | Shell Scripts (.zysh) |
|---|---|
| • Resets to default configuration.<br>• Goes into CLI **Configuration** mode.<br>• Runs the commands in the configuration file. | • Goes into CLI **Privilege** mode.<br>• Runs the commands in the shell script. |

You have to run the example in Figure 386 on page 559 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.

## 47.2 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.

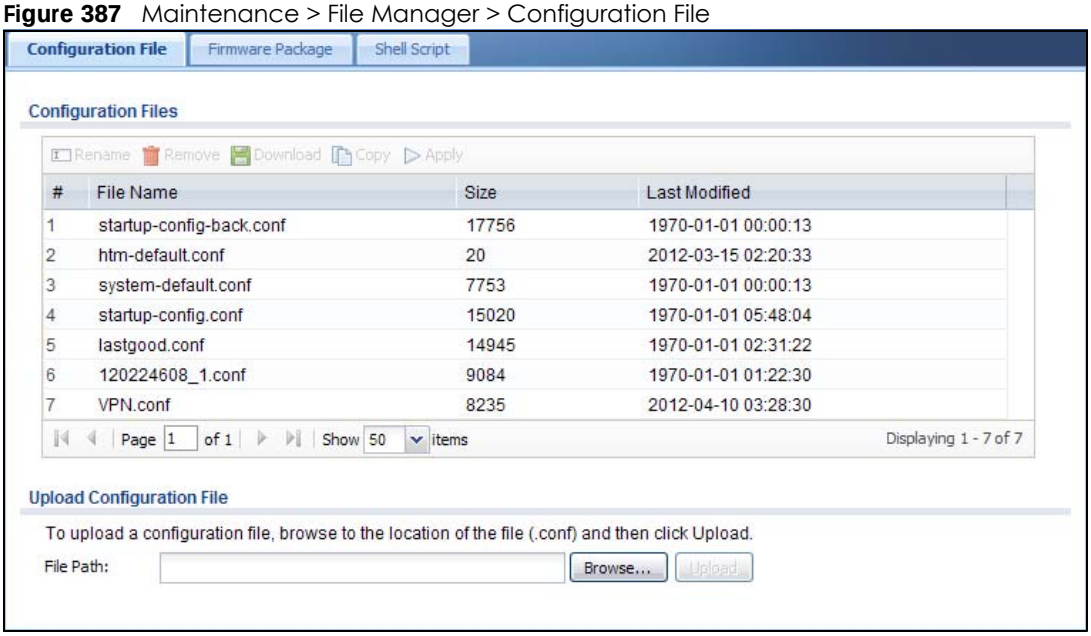
Once your UAG is configured and functioning properly, it is highly recommended that you back up your configuration file before making further configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

### 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 387** Maintenance > File Manager > Configuration File




**Do not turn off the UAG while configuration file upload is in progress.**

The following table describes the labels in this screen.

Table 266 Maintenance > File Manager > Configuration File

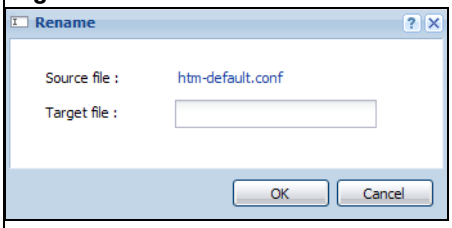
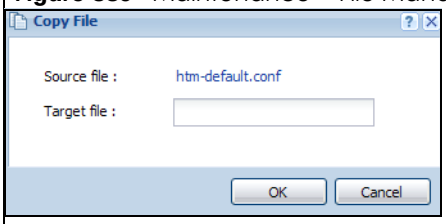
| LABEL | DESCRIPTION |
|---|---|
| Rename | Use this button to change the label of a configuration file on the UAG. You can only rename manually saved configuration files. You cannot rename the **lastgood.conf**, **system-default.conf** and **startup-config.conf** files.<br><br>You cannot rename a configuration file to the name of another configuration file in the UAG.<br><br>Click a configuration file's row to select it and click **Rename** to open the **Rename File** screen.<br><br>**Figure 388** Maintenance > File Manager > Configuration File > Rename<br>  <br><br>Specify the new name for the configuration file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-).<br><br>Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file. |
| Remove | Click a configuration file's row to select it and click **Remove** to delete it from the UAG. You can only delete manually saved configuration files. You cannot delete the **system-default.conf**, **startup-config.conf** and **lastgood.conf** files.<br><br>A pop-up window asks you to confirm that you want to delete the configuration file. Click **OK** to delete the configuration file or click **Cancel** to close the screen without deleting the configuration file. |
| Download | Click a configuration file's row to select it and click **Download** to save the configuration to your computer. |
| Copy | Use this button to save a duplicate of a configuration file on the UAG.<br><br>Click a configuration file's row to select it and click **Copy** to open the **Copy File** screen.<br><br>**Figure 389** Maintenance > File Manager > Configuration File > Copy<br>  <br><br>Specify a name for the duplicate configuration file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-).<br><br>Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file. |

Table 266 Maintenance > File Manager > Configuration File (continued)

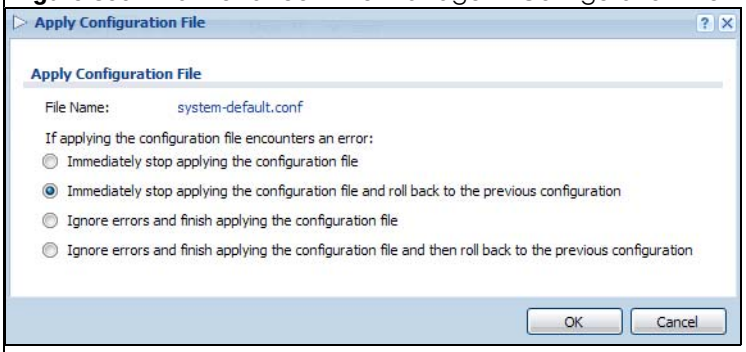
| LABEL | DESCRIPTION |
|---|---|
| Apply | Use this button to have the UAG use a specific configuration file.<br><br>Click a configuration file's row to select it and click **Apply** to have the UAG use that configuration file. The UAG does not have to restart in order to use a different configuration file, although you will need to wait for a few minutes while the system reconfigures.<br><br>The following screen gives you options for what the UAG is to do if it encounters an error in the configuration file.<br><br>**Figure 390** Maintenance > File Manager > Configuration File > Apply<br>  <br><br><br>**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.<br><br>**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.<br><br>**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.<br><br>**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.<br><br>Click **OK** to have the UAG start applying the configuration file or click **Cancel** to close the screen |
| # | 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. |
| File Name | This column displays the label that identifies a configuration file.<br><br>You cannot delete the following configuration files or change their file names.<br><br>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.<br><br>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 `write` command.<br><br>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. |
| Size | This column displays the size (in KB) of a configuration file. |

Table 266 Maintenance > File Manager > Configuration File (continued)

| LABEL | DESCRIPTION |
|---|---|
| Last Modified | This column displays the date and time that the individual configuration files were last changed or saved. |
| Upload Configuration File | The bottom part of the screen allows you to upload a new or previously saved configuration file from your computer to your UAG<br><br>You cannot upload a configuration file named **system-default.conf** or **lastgood.conf**.<br><br>If you upload **startup-config.conf**, it will replace the current configuration and immediately apply the new settings. |
| 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 fie 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. |

# 47.3 The Firmware Package Screen

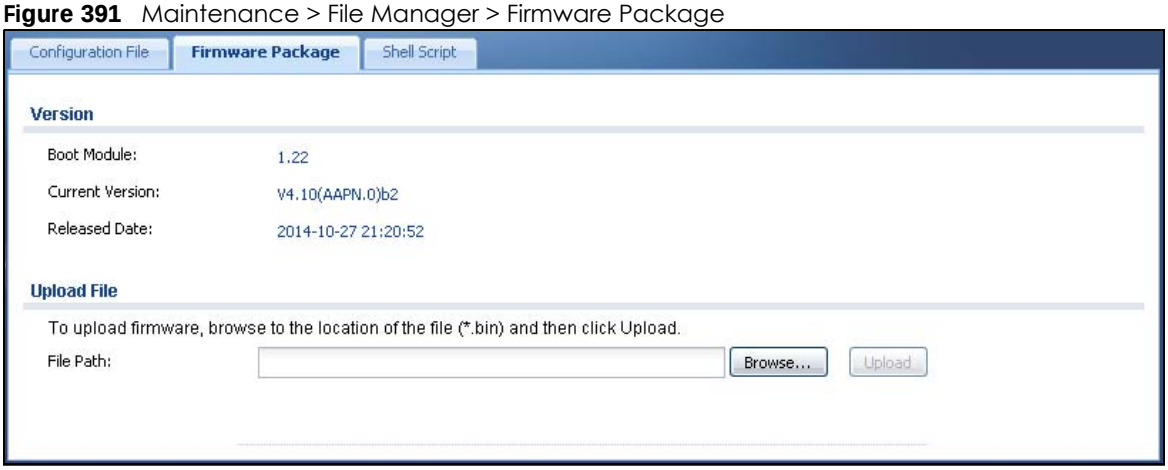
Click **Maintenance > File Manager > Firmware Package** to open the **Firmware Package** screen. Use the **Firmware Package** screen to check your current firmware version and upload firmware to the UAG.

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 391** Maintenance > File Manager > Firmware Package



The following table describes the labels in this screen.

Table 267 Maintenance > File Manager > Firmware Package

| LABEL | DESCRIPTION |
|---|---|
| Version | |
| 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. |
| Upload File | |
| 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. |

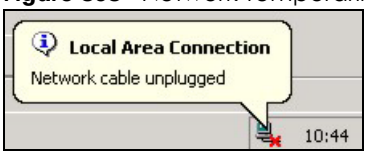
After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the UAG again.

**Figure 392** 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.

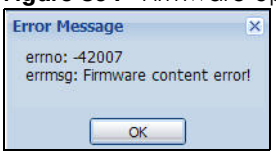
**Figure 393** Network Temporarily Disconnected




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 394** Firmware Upload Error



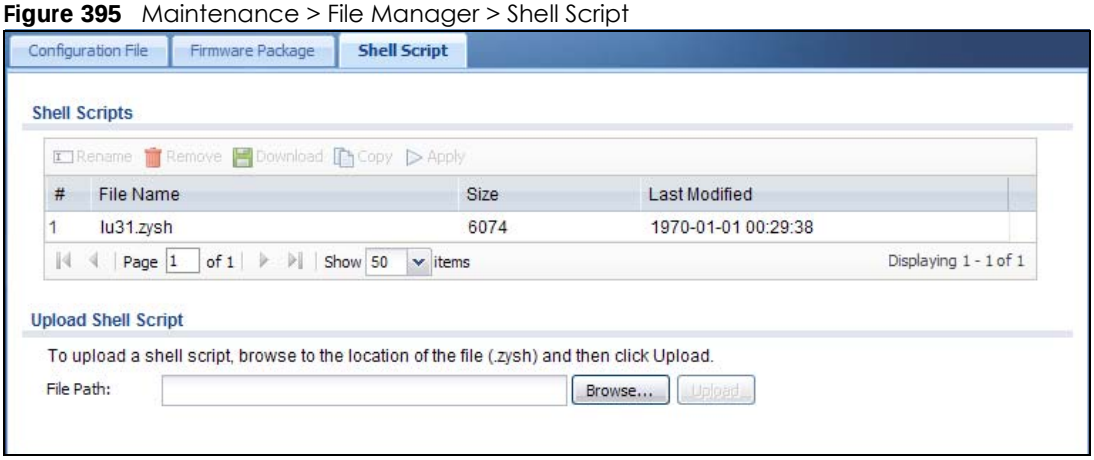

# 47.4 The Shell Script Screen

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 395** Maintenance > File Manager > Shell Script




Each field is described in the following table.

Table 268 Maintenance > File Manager > Shell Script

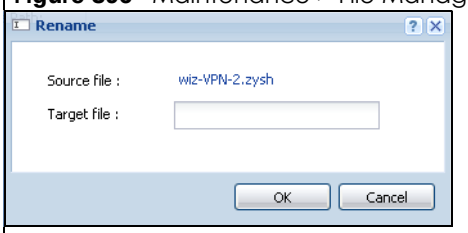
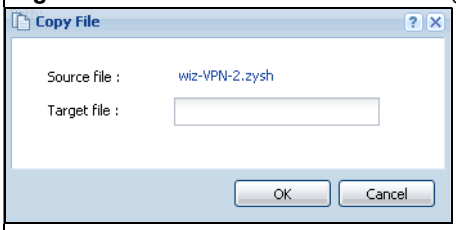
| LABEL | DESCRIPTION |
|---|---|
| Rename | Use this button to change the label of a shell script file on the UAG.<br><br>You cannot rename a shell script to the name of another shell script in the UAG.<br><br>Click a shell script's row to select it and click **Rename** to open the **Rename File** screen.<br><br>**Figure 396** Maintenance > File Manager > Shell Script > Rename<br>  <br><br><br>Specify the new name for the shell script file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-).<br><br>Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file. |
| Remove | Click a shell script file's row to select it and click **Remove** to delete the shell script file from the UAG.<br><br>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. |
| Download | Click a shell script file's row to select it and click **Download** to save the configuration to your computer. |

Table 268 Maintenance > File Manager > Shell Script (continued)

| LABEL | DESCRIPTION |
|---|---|
| Copy | Use this button to save a duplicate of a shell script file on the UAG.<br>Click a shell script file's row to select it and click **Copy** to open the **Copy File** screen.<br>**Figure 397** Maintenance > File Manager > Shell Script > Copy<br>  <br>Specify a name for the duplicate file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-).<br>Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file. |
| Apply | Use this button to have the UAG use a specific shell script file.<br>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. |
| # | This column displays the number for each shell script file entry. |
| File Name | This column displays the label that identifies a shell script file. |
| Size | This column displays the size (in KB) of a shell script file. |
| Last Modified | This column displays the date and time that the individual shell script files were last changed or saved. |
| 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. |

# CHAPTER 48
# Diagnostics

## 48.1 Overview

Use the diagnostics screens for troubleshooting.

### 48.1.1 What You Can Do in this Chapter

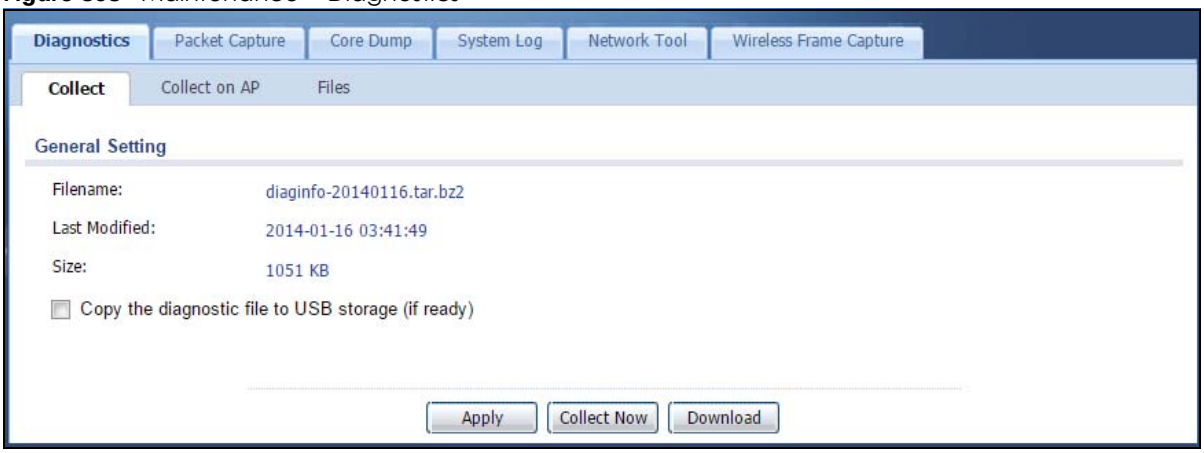
- Use the **Diagnostics** screen (see Section 48.2 on page 568) to generate a file containing the UAG's configuration and diagnostic information if you need to provide it to customer support during troubleshooting.
- Use the **Packet Capture** screens (see Section 48.3 on page 571) to capture packets going through the UAG.
- Use the **Core Dump** screens (see Section 48.4 on page 575) 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 48.5 on page 576) to download files of system logs from a connected USB storage device to your computer.
- Use the **Network Tool** screen (see Section 48.6 on page 577) to ping an IP address or trace the route packets take to a host.
- Use the **Wireless Frame Capture** screens (see Section 48.7 on page 578) to capture network traffic going through the AP interfaces connected to your UAG.

## 48.2 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 398** Maintenance > Diagnostics




The following table describes the labels in this screen.

Table 269 Maintenance > Diagnostics

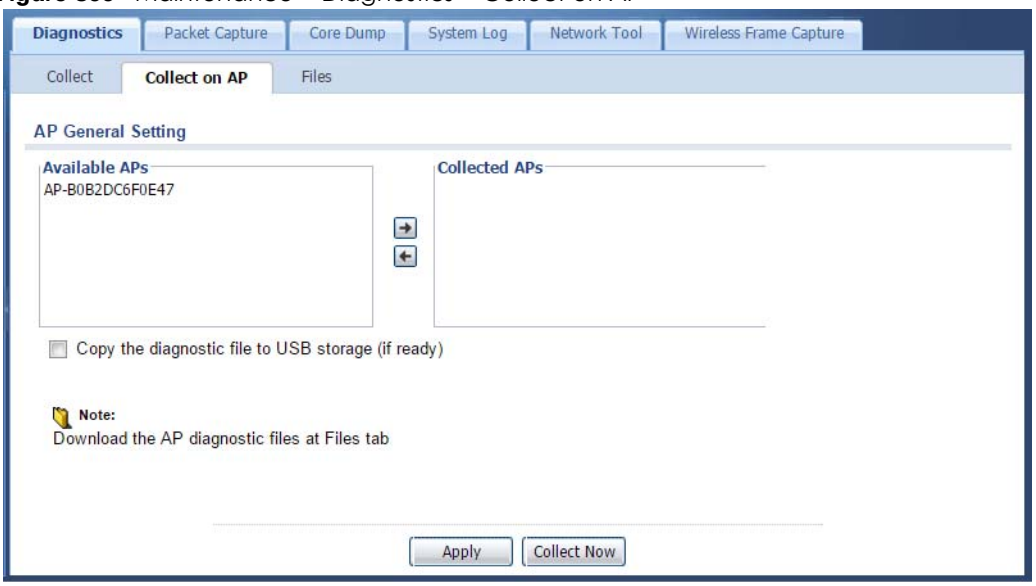
| LABEL | DESCRIPTION |
|---|---|
| Diagnostic Information Collector | |
| Filename | This is the name of the most recently created diagnostic file. |
| Last modified | This is the date and time that the last diagnostic file was created. The format is yyyy-mm-dd hh:mm:ss. |
| Size | This is the size 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. |

## 48.2.1 The Diagnostic Collect on AP Screen

The **Collect AP** screen provides an easy way for you to generate a file containing the UAG's connected APs configuration and diagnostic information. You may need to send this file to customer support for troubleshooting.

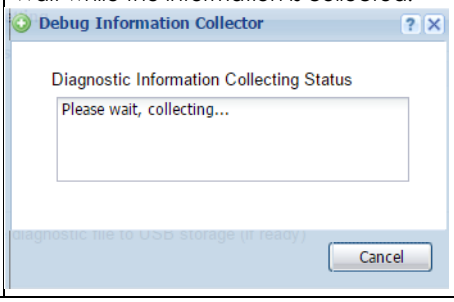
Click **Maintenance > Diagnostics > Collect on AP** to open this screen.

**Figure 399** Maintenance > Diagnostics > Collect on AP




The following table describes the labels in this screen.

Table 270 Maintenance > Diagnostics > Collect on AP

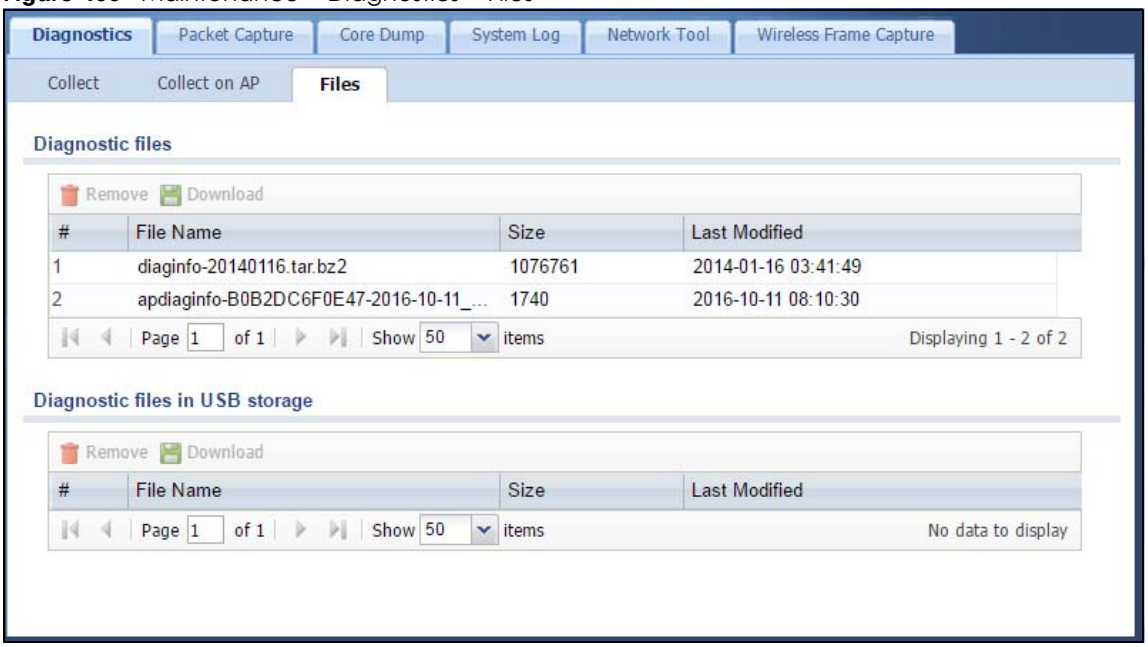
| LABEL | DESCRIPTION |
|---|---|
| AP General Setting | The **Available APs** list displays the names of the APs connected to your UAG. Select APs from the **Available APs** list to add them to your **Collected APs** list so the UAG can collect all the configuration and diagnostic information regarding these APs. |
| Copy the diagnostic file to USB storage (If ready) | Click this check box so that the diagnostic file obtained makes a copy in the USB storage. |
| Apply | Click **Apply** to save the changes to your UAG. |
| Collect Now | Click **Collect Now** to create the APs diagnostic file.<br>Wait while the information is collected.<br>  |



## 48.2.2 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 400** Maintenance > Diagnostics > Files




The following table describes the labels in this screen.

Table 271 Maintenance > Diagnostics > Files

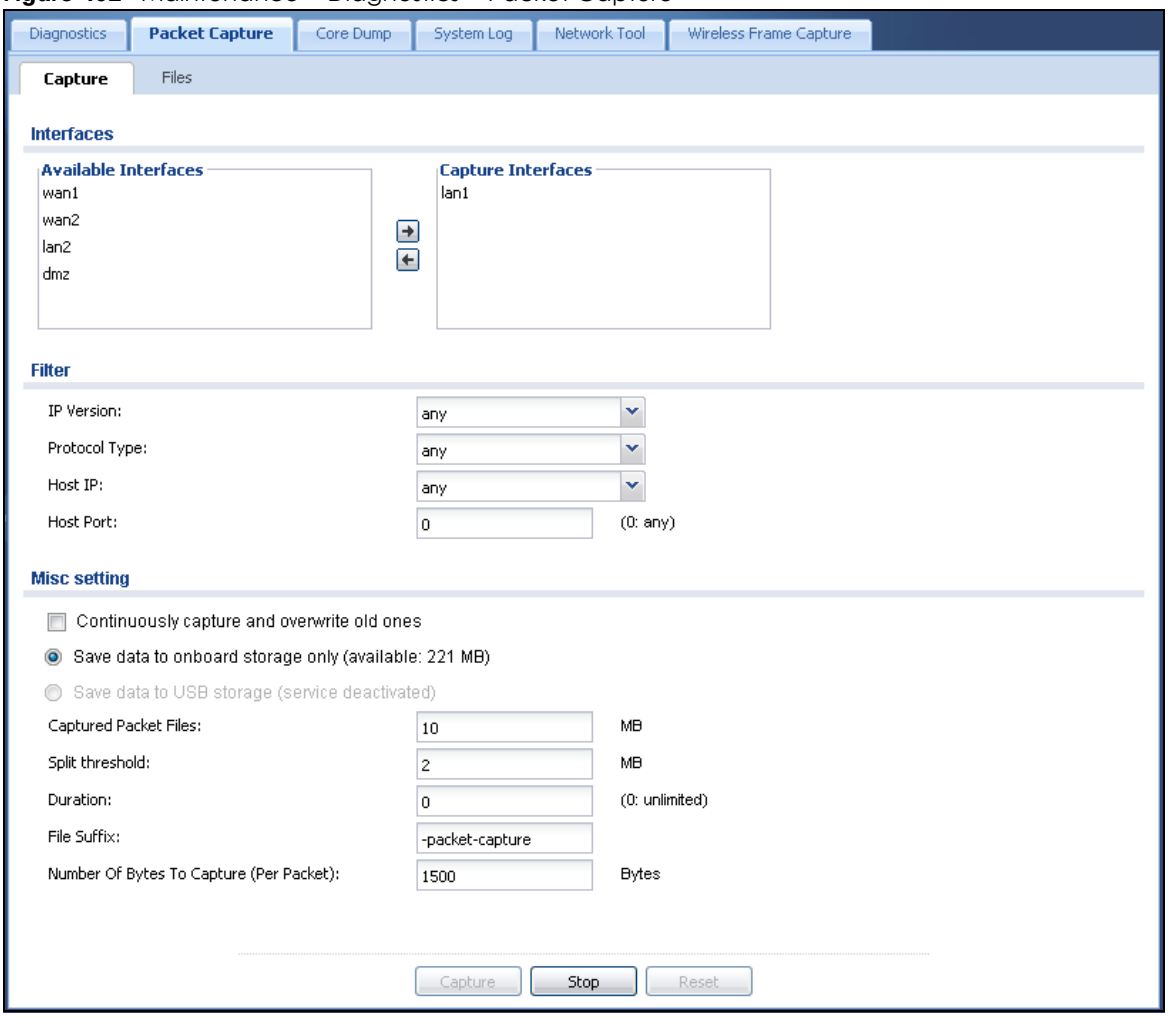
| LABEL | DESCRIPTION |
|---|---|
| Diagnostic files / Diagnostic files in USB storage | |
| Remove | Select files and click **Remove** to delete them from the UAG or the connected USB storage device. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete. |
| Download | Click a file to select it and click **Download** to save it to your computer. |
| # | 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. |

# 48.3 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 401** Maintenance > Diagnostics > Packet Capture




The following table describes the labels in this screen.

Table 272 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. |
| Filter | |
| 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. |
| Misc setting | |
| 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 272 Maintenance > Diagnostics > Packet Capture (continued)

| LABEL | DESCRIPTION |
|---|---|
| Save data to onboard storage only | Select this to have the UAG only store packet capture entries on the UAG. The available storage size is displayed as well.<br><br>Note: The UAG reserves some onboard storage space as a buffer. |
| Save data to USB storage | Select this to have the UAG store packet capture entries only on a USB storage device connected to the UAG.<br><br>Status:<br><br>**Unused** - the connected USB storage device was manually unmounted by using the **Remove Now** button or for some reason the UAG cannot mount it.<br><br>**none** - no USB storage device is connected.<br><br>**available** - you can have the UAG use the USB storage device. The available storage capacity also displays.<br><br>**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.<br><br>Note: The UAG reserves some USB storage space as a buffer. |
| Captured Packet Files | 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.<br><br>When saving packet captures to a connected USB storage device, specify a maximum limit in megabytes for each capture file.<br><br>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.<br><br>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. |
| 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 | 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.<br><br>The file name format is "interface name-file suffix.cap", for example "vlan2-packet-capture.cap". |
| 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. |

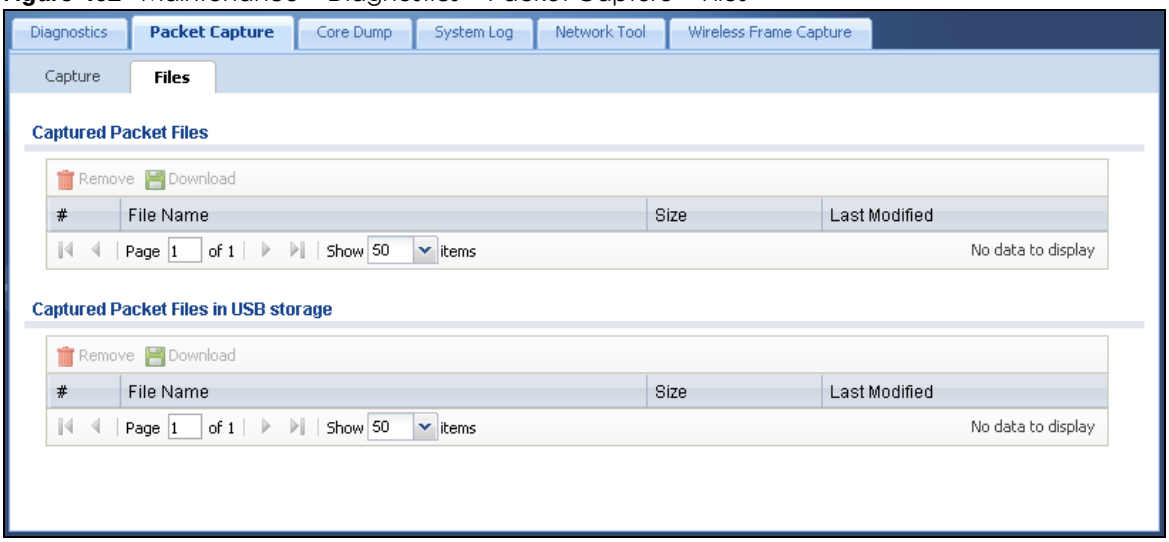
Table 272 Maintenance > Diagnostics > Packet Capture (continued)

| LABEL | DESCRIPTION |
|---|---|
| Capture | Click this button to have the UAG capture packets according to the settings configured in this screen.<br>You can configure the UAG while a packet capture is in progress although you cannot modify the packet capture settings.<br>The UAG's throughput or performance may be affected while a packet capture is in progress.<br>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. |
| 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. |

## 48.3.1 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 402** Maintenance > Diagnostics > Packet Capture > Files




The following table describes the labels in this screen.

Table 273 Maintenance > Diagnostics > Packet Capture > Files

| LABEL | DESCRIPTION |
|---|---|
| Captured Packet Files / Captures Packet Files in USB storage | |
| 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 273 Maintenance > Diagnostics > Packet Capture > Files (continued)

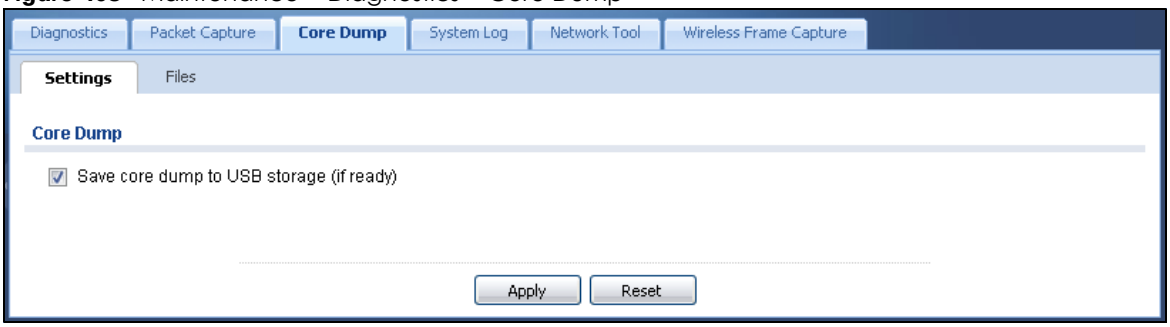
| LABEL | DESCRIPTION |
|---|---|
| # | This column displays the number for each packet capture file entry. The total number of packet capture files that you can save depends on the file sizes and the available flash storage space. |
| File Name | This column displays the label that identifies the file. 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. |

# 48.4 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 403** Maintenance > Diagnostics > Core Dump




The following table describes the labels in this screen.

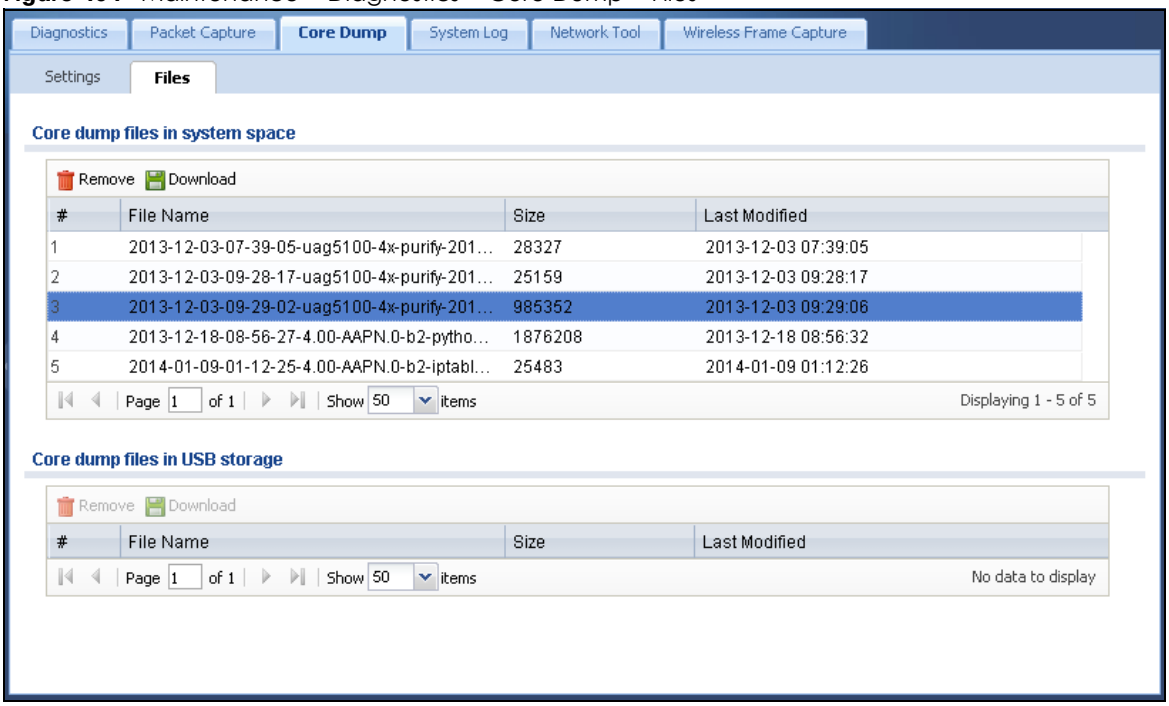
Table 274 Maintenance > Diagnostics > Core Dump

| 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. |

## 48.4.1 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 404** Maintenance > Diagnostics > Core Dump > Files




The following table describes the labels in this screen.

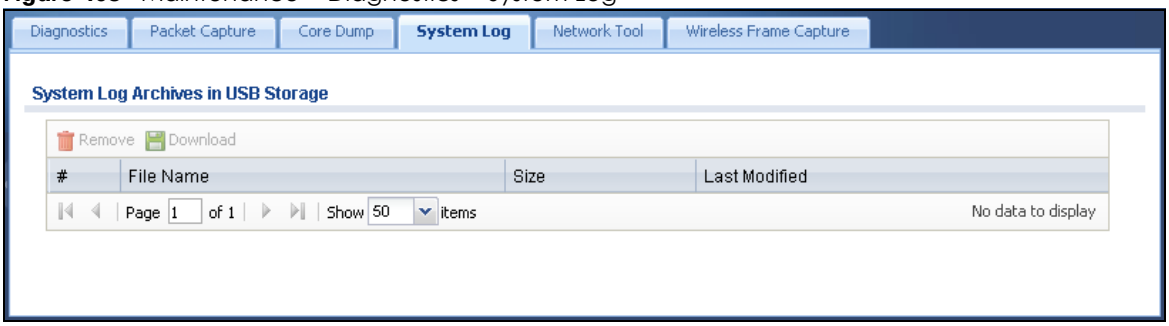
Table 275 Maintenance > Diagnostics > Core Dump > Files

| LABEL | DESCRIPTION |
|---|---|
| Core dump files in system space / Core dump files in USB storage | |
| 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. |
| # | 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. |

# 48.5 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 405** Maintenance > Diagnostics > System Log




The following table describes the labels in this screen.

Table 276 Maintenance > Diagnostics > System Log

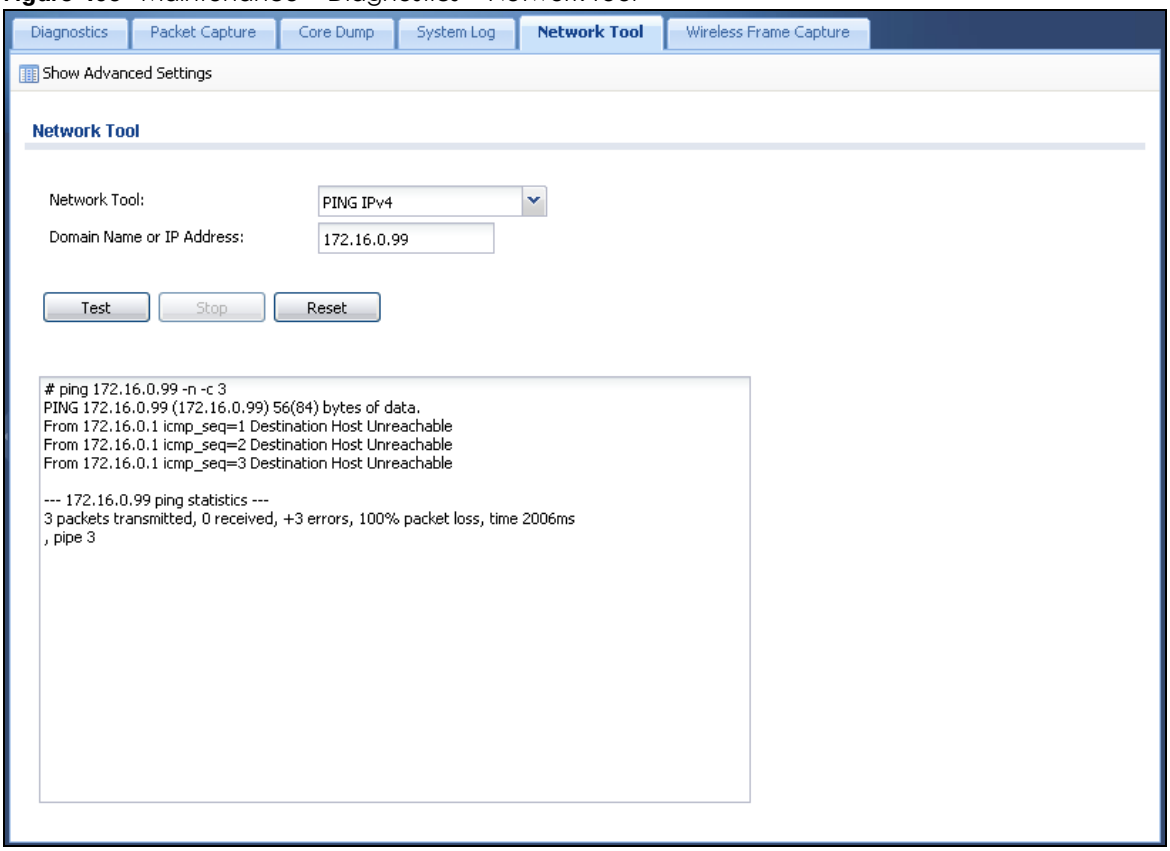
| LABEL | DESCRIPTION |
|---|---|
| System Log Archives in USB Storage | |
| Remove | Select files and click **Remove** to delete them from the connected USB storage device. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete. |
| Download | Click a file to select it and click **Download** to save it to your computer. |
| # | 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. |

# 48.6 The Network Tool Screen

Use this screen to ping or traceroute an IP address.

Click **Maintenance > Diagnostics > Network Tool** to display this screen.

**Figure 406** Maintenance > Diagnostics > Network Tool




The following table describes the labels in this screen.

Table 277 Maintenance > Diagnostics > Network Tool

| LABEL | DESCRIPTION |
|---|---|
| Network Tool | Select **PING IPv4** to ping the IP address that you entered.<br>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. |

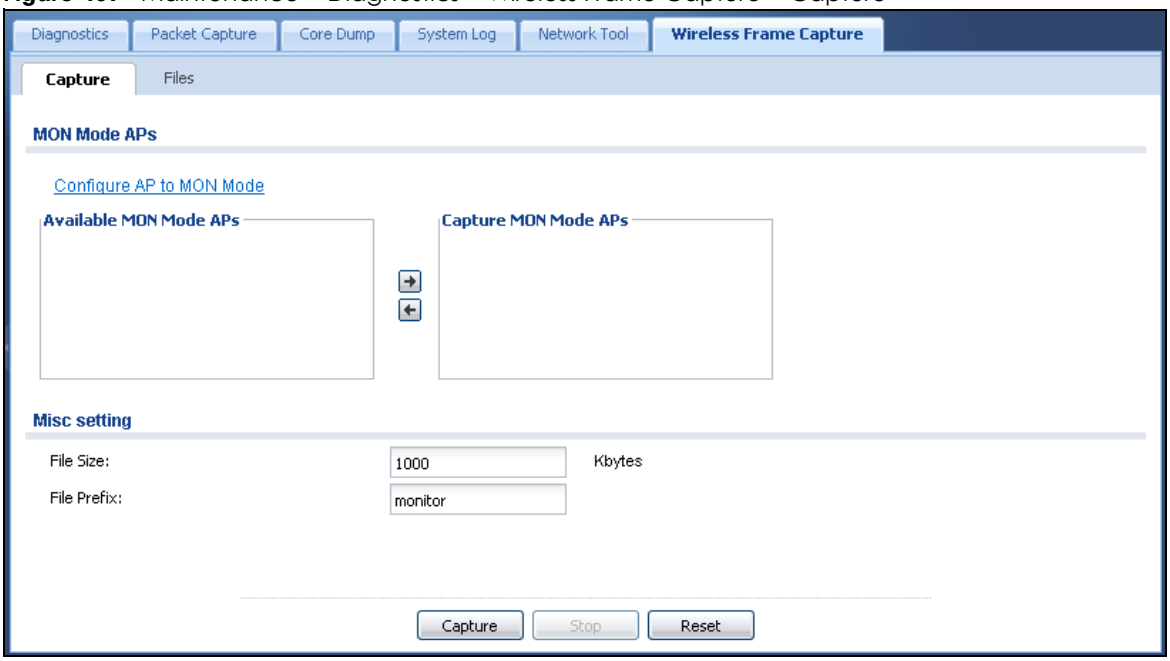
# 48.7 The Wireless Frame Capture Screen

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 407** Maintenance > Diagnostics > Wireless Frame Capture > Capture




The following table describes the labels in this screen.

Table 278 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.<br>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.<br>Note: If you have existing capture files you may need to set this size larger or delete existing capture files.<br>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.<br>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.<br>The file format is: [file prefix].cap. For example, “monitor.cap”. |

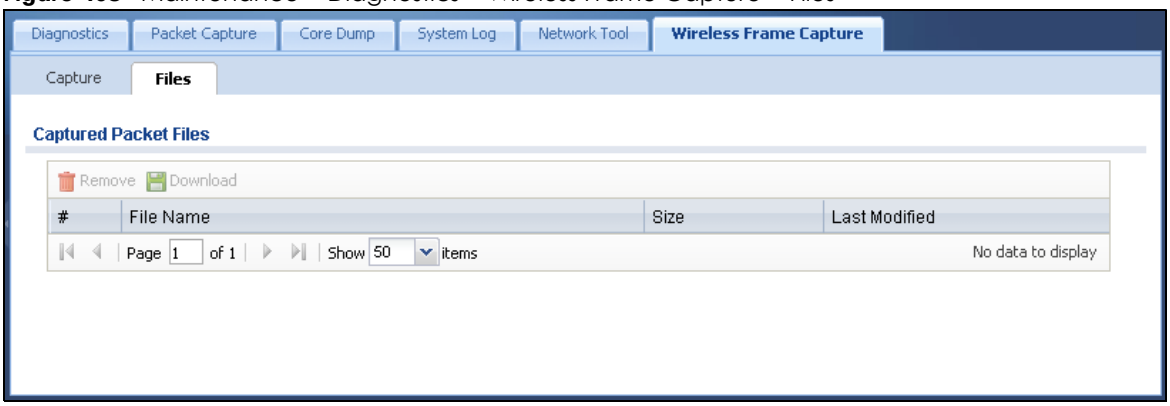
Table 278 Maintenance > Diagnostics > Wireless Frame Capture > Capture (continued)

| LABEL | DESCRIPTION |
|---|---|
| Capture | Click this button to have the UAG capture frames according to the settings configured in this screen.<br>You can configure the UAG while a frame capture is in progress although you cannot modify the frame capture settings.<br>The UAG's throughput or performance may be affected while a frame capture is in progress.<br>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. |
| 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. |

## 48.7.1 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 408** Maintenance > Diagnostics > Wireless Frame Capture > Files




The following table describes the labels in this screen.

Table 279 Maintenance > Diagnostics > Wireless Frame Capture > Files

| LABEL | DESCRIPTION |
|---|---|
| Captured Packet Files | |
| 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. |

# CHAPTER 49
# Packet Flow Explore

## 49.1 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.

### 49.1.1 What You Can Do in this Chapter

- Use the **Routing Status** screen (see Section 49.2 on page 581) to view the overall routing flow and each routing function's settings.
- Use the **SNAT Status** screen (see Section 49.3 on page 586) to view the overall source IP address conversion (SNAT) flow and each SNAT function's settings.

## 49.2 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 409** Maintenance > Packet Flow Explore > Routing Status (Direct Route)

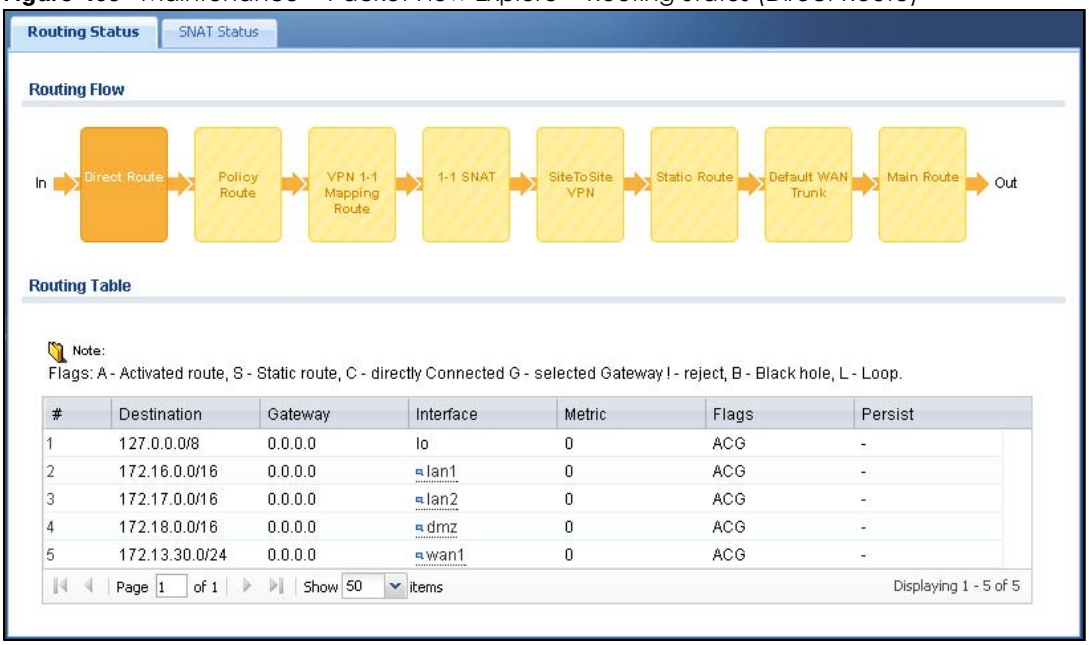



**Figure 410** Maintenance > Packet Flow Explore > Routing Status (Policy Route)

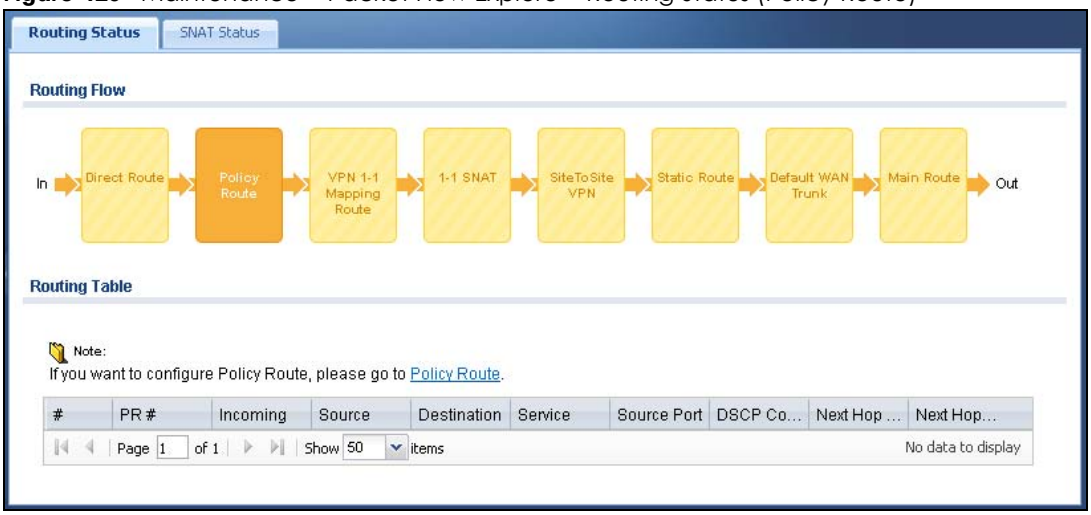


**Figure 411** Maintenance > Packet Flow Explore > Routing Status (VPN 1-1 Mapping Route)

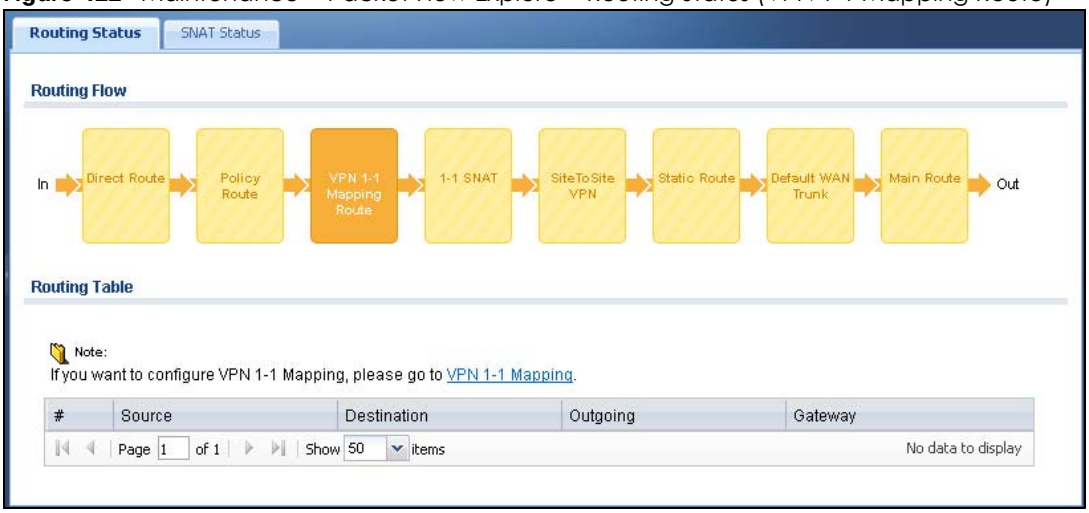



**Figure 412** Maintenance > Packet Flow Explore > Routing Status (1-1 SNAT)

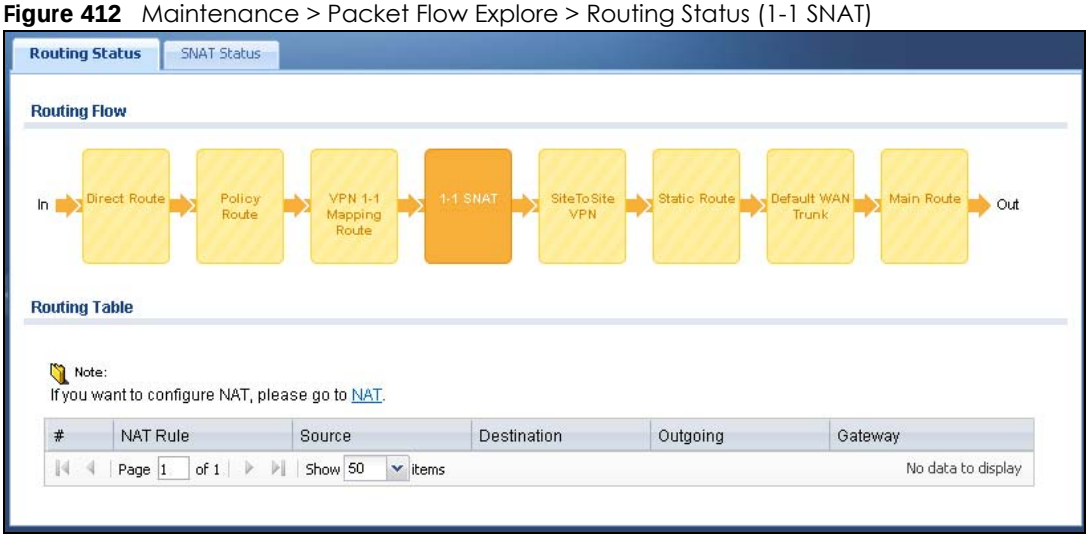



**Figure 413** Maintenance > Packet Flow Explore > Routing Status (SiteToSite VPN)

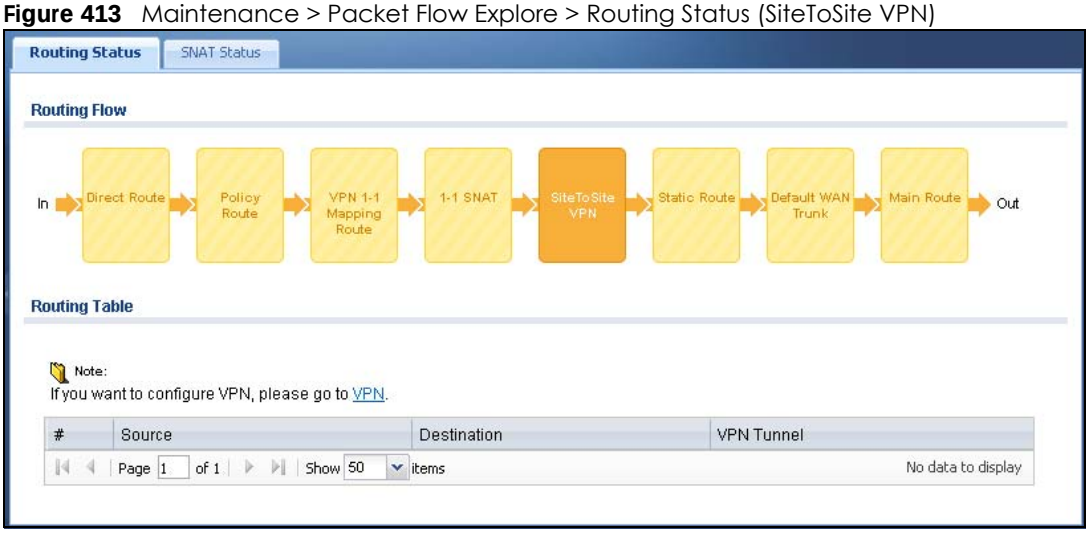


**Figure 414** Maintenance > Packet Flow Explore > Routing Status (Static Route)

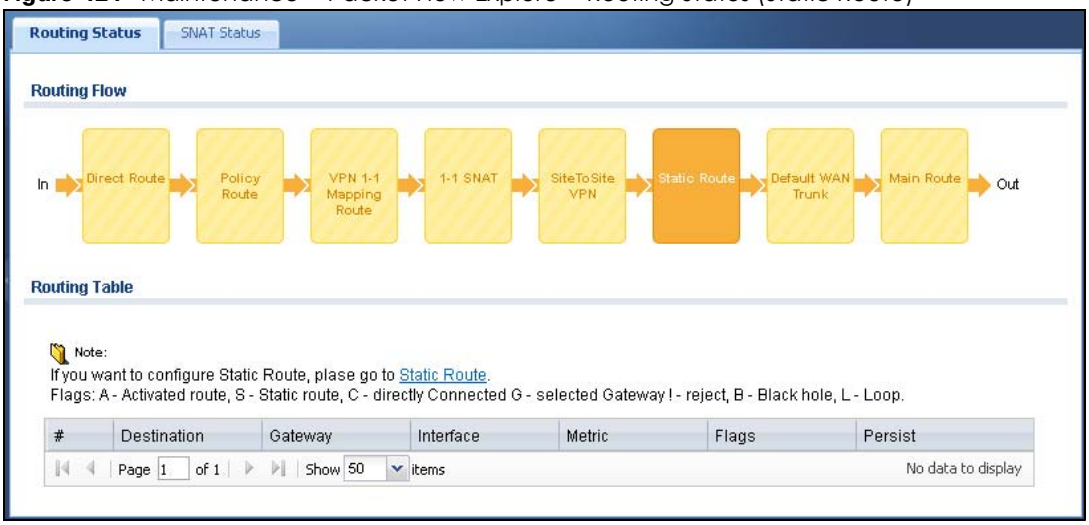



**Figure 415** Maintenance > Packet Flow Explore > Routing Status (Default WAN Trunk)

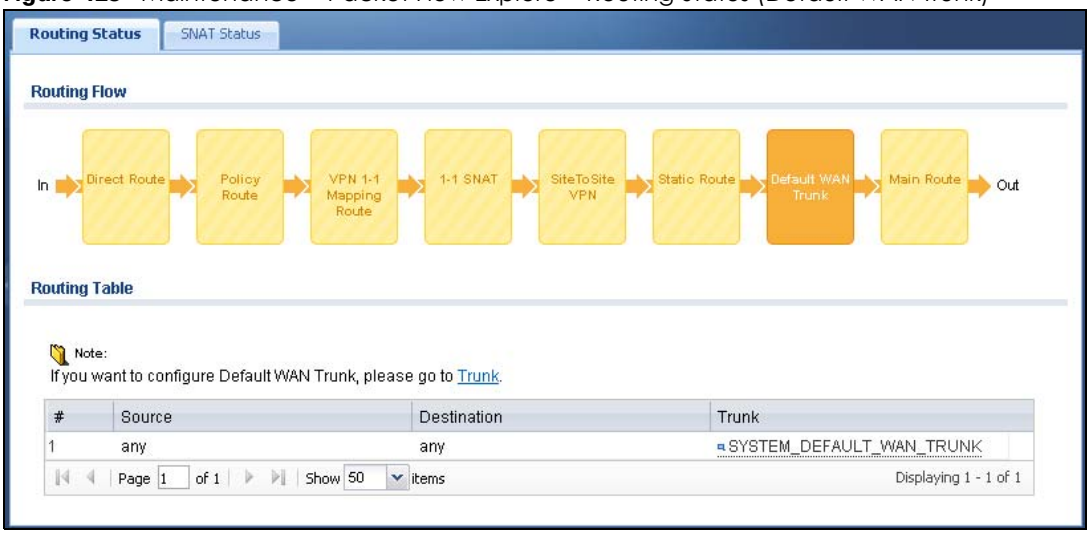
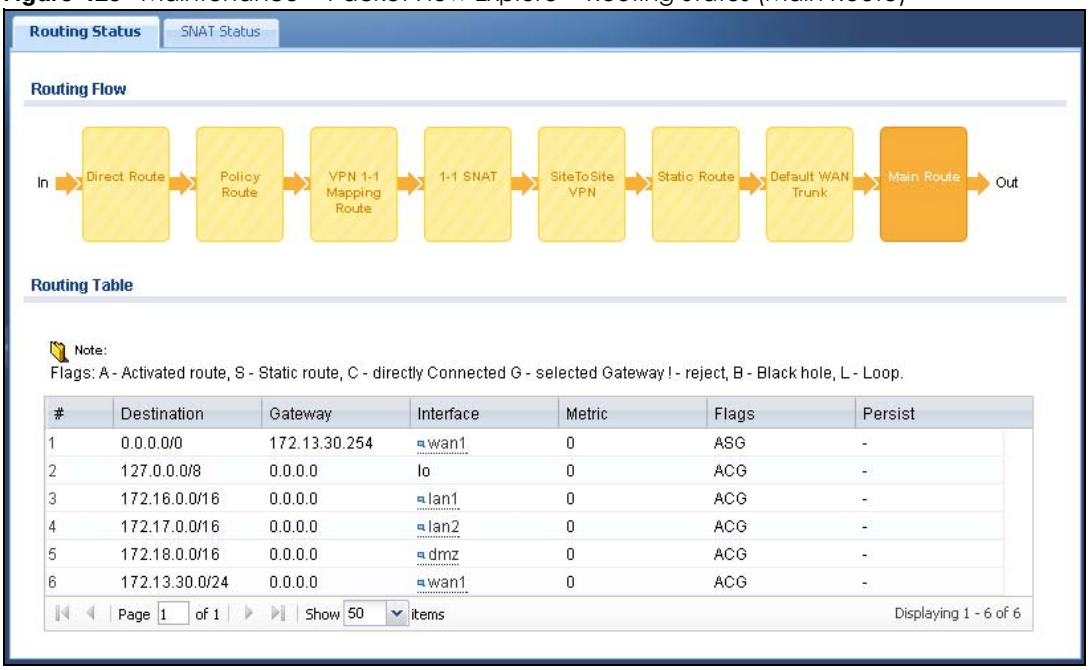


**Figure 416** Maintenance > Packet Flow Explore > Routing Status (Main Route)




The following table describes the labels in this screen.

Table 280 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:<br>• **A** - this route is currently activated.<br>• **S** - this is a static route.<br>• **C** - this is a direct connected route.<br>• **G** - the route is to a gateway (router) in the same network.<br>• **!** - this is a route which forces a route lookup to fail.<br>• **B** - this is a route which discards packets.<br>• **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. |
| Destination | This is the IP address(es) for the remote VPN network. |

Table 280 Maintenance > Packet Flow Explore > Routing Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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 220 for more information. |
| Next Hop Type | This is the type of the next hop to which packets are directed. |
| Next Hop Info | • This is the main route if the next hop type is **Auto**.<br>• This is the interface name and gateway IP address if the next hop type is **Interface / GW**.<br>• 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. |

# 49.3 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 417** Maintenance > Packet Flow Explore > SNAT Status (Policy Route SNAT)

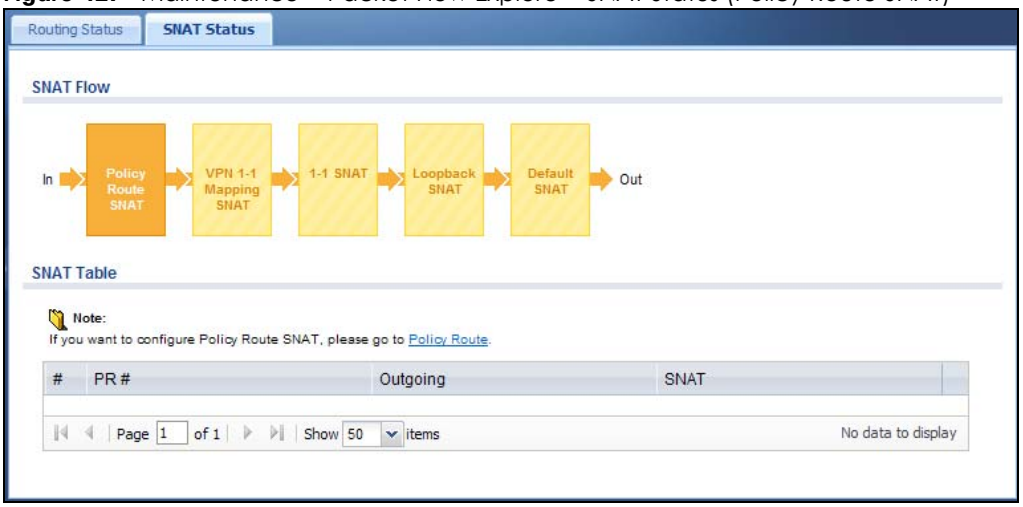



**Figure 418** Maintenance > Packet Flow Explore > SNAT Status (VPN 1-1 Mapping Route)

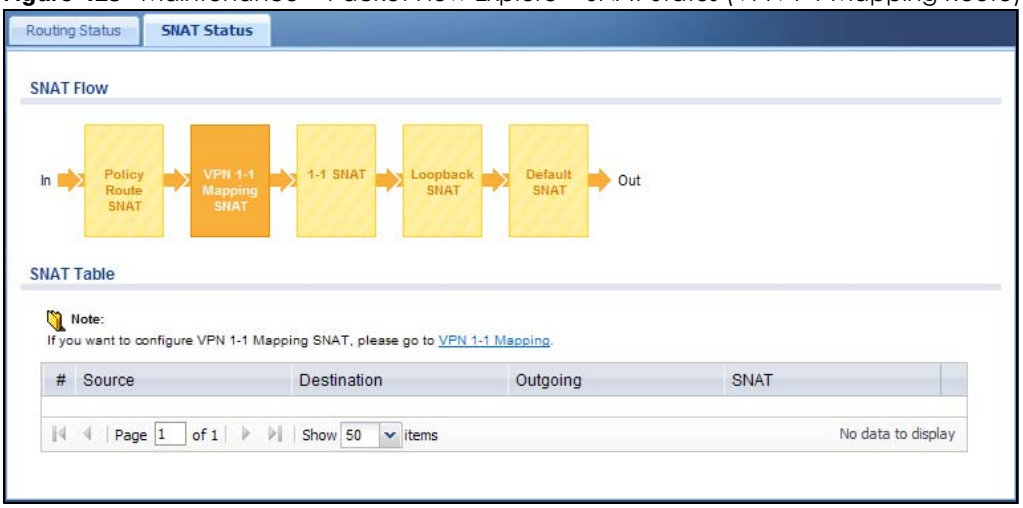


**Figure 419** Maintenance > Packet Flow Explore > SNAT Status (1-1 SNAT)

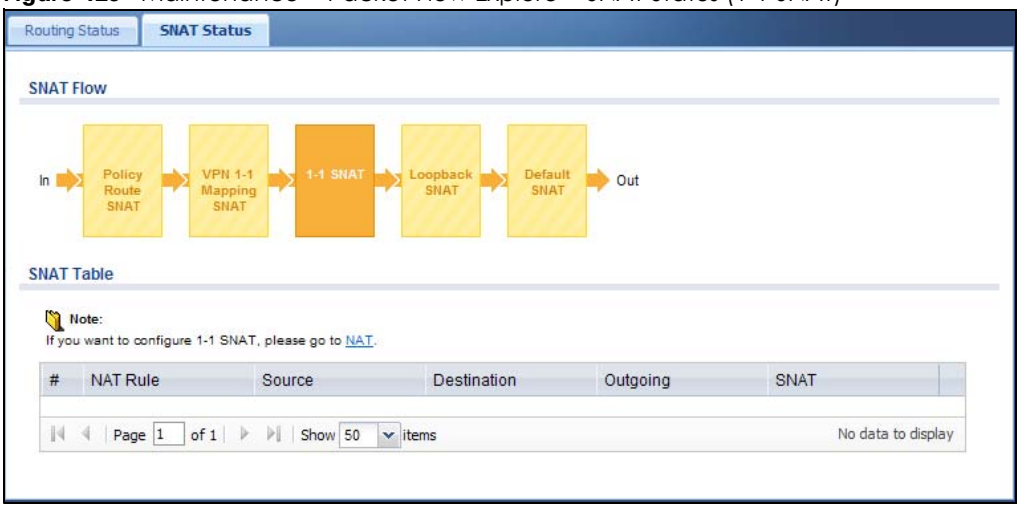



**Figure 420** Maintenance > Packet Flow Explore > SNAT Status (Loopback SNAT)

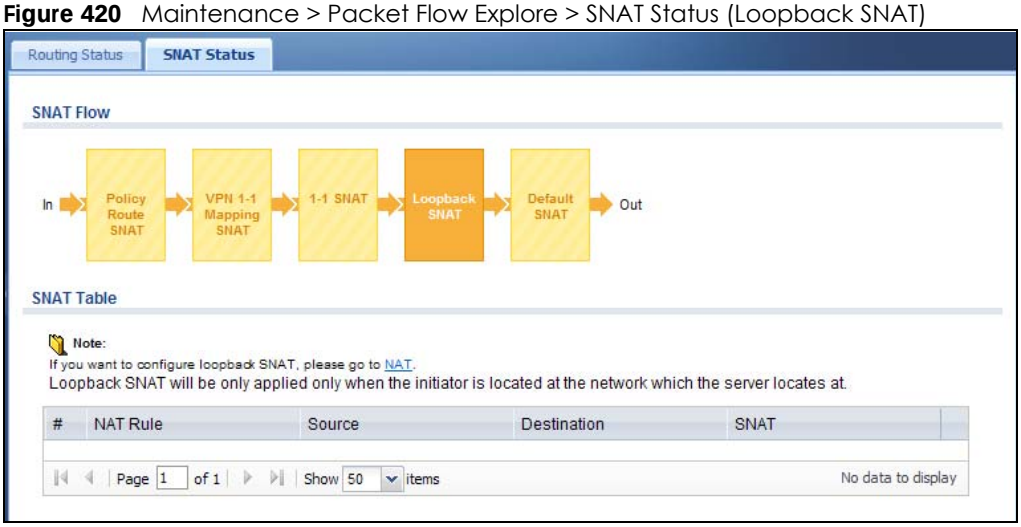
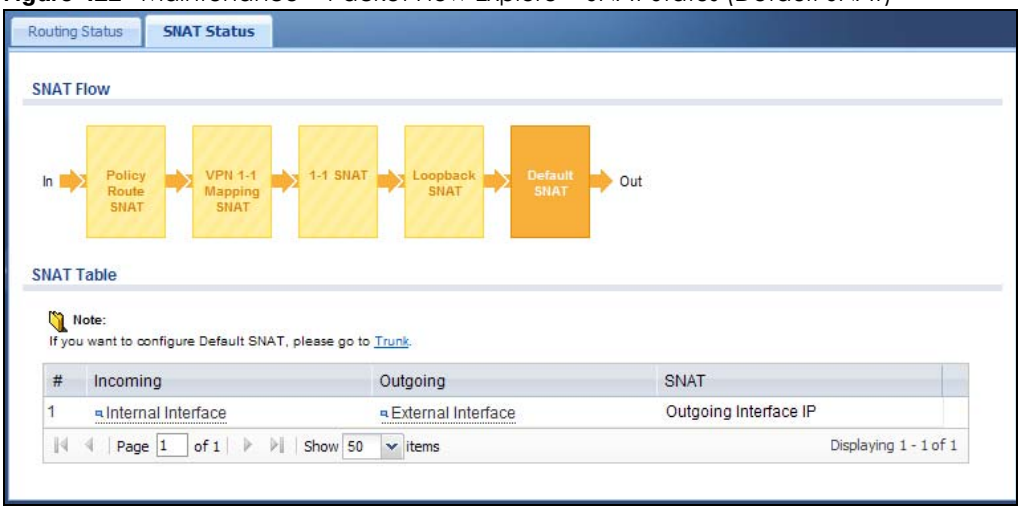



**Figure 421** Maintenance > Packet Flow Explore > SNAT Status (Default SNAT)



The following table describes the labels in this screen.

Table 281 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. |

# CHAPTER 50
# Reboot

## 50.1 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.

### 50.1.1 What You Need To Know

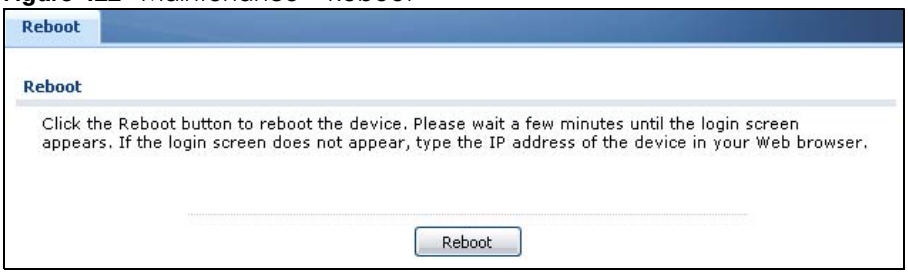
If you applied changes in the Web configurator, these were saved automatically and do not change when you reboot. If you made changes in the CLI, however, you have to use the `write` command to save the configuration before you reboot. Otherwise, the changes are lost when you reboot.

Reboot is different to reset; (see Section 52.1 on page 598) reset returns the device to its default configuration.

## 50.2 The Reboot Screen

The **Reboot** screen allows remote users to restart the device. To access this screen, click **Maintenance** > **Reboot**.

**Figure 422** 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.

# CHAPTER 51
# Shutdown

## 51.1 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.**

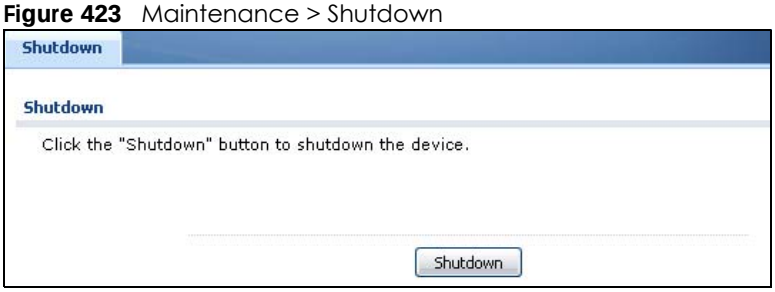
### 51.1.1 What You Need To Know

Shutdown writes all cached data to the local storage and stops the system processes.

## 51.2 The Shutdown Screen

To access this screen, click **Maintenance** > **Shutdown**.

**Figure 423** 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.

# CHAPTER 52
# Troubleshooting

This chapter offers some suggestions to solve problems you might encounter.

- You can also refer to the logs (see Chapter 7 on page 129).
- For the order in which the UAG applies its features and checks, see Chapter 49 on page 581.

## 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 302 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 41 on page 468 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 41 on page 468 and Chapter 42 on page 473, 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 PKS#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 47 on page 558 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.

# 52.1 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 50 on page 590.

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.

# 52.2 Getting More Troubleshooting Help

Search for support information for your model at www.zyxel.com for more troubleshooting suggestions.

# APPENDIX A
# 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.

See *http://www.zyxel.com/homepage.shtml* and also *http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml* for the latest information.

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/tw/zh/

### 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/
- http://www.zyxel.com/be/fr/

### Bulgaria

- Zyxel България
- http://www.zyxel.com/bg/bg/

### Czech Republic

- 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

### Italy

- Zyxel Communications Italy
- http://www.zyxel.it/

### 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 Communications ES Ltd
- 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/

### Brazil

- Zyxel Communications Brasil Ltda.
- https://www.zyxel.com/br/pt/

### Ecuador

- Zyxel Communication Corporation
- http://www.zyxel.com/ec/es/

## Middle East

### Israel

- Zyxel Communication Corporation
- http://il.zyxel.com/homepage.shtml

### Middle East

- Zyxel Communication Corporation
- http://www.zyxel.com/me/en/

## North America

### USA

- Zyxel Communications, Inc. - North America Headquarters
- http://www.zyxel.com/us/en/

## Oceania

### Australia

- Zyxel Communications Corporation
- http://www.zyxel.com/au/en/

## Africa

### South Africa

- Nology (Pty) Ltd.
- http://www.zyxel.co.za

# APPENDIX B ZYXEL Legal Information

## Copyright

Copyright © 2016 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.

## Disclaimer

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.

## Regulatory Notice and Statement

Model List: UAG5100

### United States of America

The following information applies if you use the product within USA area.

#### Federal Communications Commission (FCC) EMC Statement

- This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

  (1) This device may not cause harmful interference.

  (2) This device must accept any interference received, including interference that may cause undesired operations.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

### Canada

The following information applies if you use the product within Canada area.

#### Industry Canada ICES statement

CAN ICES-3 (A)/NMB-3(A)

### European Union

The following information applies if you use the product within the European Union.

#### CE EMC statement

WARNING: This equipment is compliant with Class A of EN55032. In a residential environment this equipment may cause radio interference.

### 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 | CZ | 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 obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- 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.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- 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.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. 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.
- Caution: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic device. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Use ONLY power wires of the appropriate wire gauge for your device. Connect it to a power supply of the correct voltage.
- Fuse Warning! Replace a fuse only with a fuse of the same type and rating.
- The POE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,

  - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;

  - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.
- This device must be grounded. Never defeat the ground conductor or operate the device in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:

  - Install the power supply before connecting the power cable to the power supply.

  - Unplug the power cable before removing the power supply.

  - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supply.

## Environment Statement

### European Union - Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.

## Environmental Product Declaration

| Български (Bulgarian) | | Čeština (Czech) | | Dansk (Danish) | | Deutsch (German) | |
|---|---|---|---|---|---|---|---|
| Екологична продуктова декларация | | Environmentální prohlášení o produktu | | Miljøvaredeklaration | | Produkt-Umweltdeklaration | |
| RoHS | Директива 2011/65/EC | RoHS | Směrnice 2011/65/EU | RoHS | Direktiv 2011/65/EU | RoHS | Richtlinie 2011/65/EU |
| WEEE | Директива 2012/19/EC | WEEE | Směrnice 2012/19/EU | WEEE | Direktiv 2012/19/EU | WEEE | Richtlinie 2012/19/EU |
| PPW | Директива 94/62/EO | PPW | Směrnice 94/62/ES | PPW | Direktiv 94/62/EF | PPW | Richtlinie 94/62/EG |
| REACH | РЕГЛАМЕНТ (ЕО) № 1907/2006 | REACH | Nařízení (ES) č. 1907/2006 | REACH | Forordning (EF) nr. 1907/2006 | REACH | VERORDNUNG (EG) Nr.1907/2006 |
| Име/ титла : | Richard Hsu / Quality Management Division Senior Manager | Jméno/ titul : | Richard Hsu / Quality Management Division Senior Manager | Navn/ titel : | Richard Hsu / Quality Management Division Senior Manager | Name/ titel : | Richard Hsu / Quality Management Division Senior Manager |
| Подпис : | Дата (дд/мм/гггг): 01/10/2014 | Podpis : | Datum (dd/mm/rrrr): 01/10/2014 | Underskrift : | Dato (dd/mm/åååå): 01/10/2014 | Unterschrift : | Datum (jjjj/mm/tt): 2014/10/01 |

| Eesti keel (Estonian) | | English | | Español (Spanish) | | Français (French) | |
|---|---|---|---|---|---|---|---|
| Toote keskkonnadeklaratsiooni | | Environmental product declaration | | Declaraciones Ambientales de Producto | | Profil environnemental de produit | |
| RoHS | Direktiiv 2011/65/EL | RoHS | Directive 2011/65/EU | RoHS | Directiva 2011/65/UE | RoHS | Directive 2011/65/UE |
| WEEE | Direktiiv 2012/19/EL | WEEE | Directive 2012/19/EU | WEEE | Directiva 2012/19/UE | WEEE | Directive 2012/19/UE |
| PPW | Direktiiv 94/62/EU | PPW | Directive 94/62/EC | PPW | Directiva 94/62/CE | PPW | Directive 94/62/CE |
| REACH | MÄÄRUS (EU) nr 1907/2006 | REACH | Regulation (EC) No 1907/2006 | REACH | REGLAMENTO (CE) nº 1907/2006 | REACH | REGLEMENT (CE) N° 1907/2006 |
| Nimi/ peal kiri : | Richard Hsu / Quality Management Division Senior Manager | Name/ title : | Richard Hsu / Quality Management Division Senior Manager | Nombre/ título : | Richard Hsu / Quality Management Division Senior Manager | Nom/ titre : | Richard Hsu / Quality Management Division Senior Manager |
| Allkiri : | Kuupäev (pp/kk/aaaa): 01/10/2014 | Signature : | Date (dd/mm/yyyy): 01/10/2014 | Firma : | Fecha (aaaa/mm/dd): 2014/10/01 | Signature : | Date (aaaa/mm/jj): 2014/10/01 |

| Hrvatski (Croatian) | | Italiano (Italian) | | Latviešu valoda(Latvian) | | Lietuvių kalba (Lithuanian) | |
|---|---|---|---|---|---|---|---|
| Deklaraciju o zbrinjavanju proizvoda | | Dichiarazione ambientale di prodotto | | Produkta vides ietekmējuma deklarācija | | Aplinkosauginę gaminio deklaraciją | |
| RoHS | Direktiva 2011/65/EU | RoHS | Direttiva 2011/65/UE | RoHS | Direktīva 2011/65/ES | RoHS | Direktyva 2011/65/ES |
| WEEE | Direktiva 2012/19/EU | WEEE | Direttiva 2012/19/UE | WEEE | Direktīva 2012/19/ES | WEEE | Direktyva 2012/19/ES |
| PPW | Direktiva 94/62/EZ | PPW | Direttiva 94/62/CE | PPW | Direktīva 94/62/EK | PPW | Direktyva 94/62/EB |
| REACH | Uredbe (EZ) br. 1907/2006 | REACH | REGOLAMENTO (CE) n. 1907/2006 | REACH | Regula (EK) Nr. 1907/2006 | REACH | REGLAMENTAS (EB) Nr. 1907/2006 |
| Ime/ naslov : | Richard Hsu / Quality Management Division Senior Manager | Nome/ titolo : | Richard Hsu / Quality Management Division Senior Manager | Nosaukums/ tituls : | Richard Hsu / Quality Management Division Senior Manager | Vardas/ titulas : | Richard Hsu / Quality Management Division Senior Manager |
| Potpis : | Datum (dd/mm/yyyy): 01/10/2014 | Firma : | Data (aaaa/mm/gg): 2014/10/01 | Paraksts : | Datums(dd/mm/gggg): 01/10/2014 | Parašas : | Data (dd/mm/mmmm): 01/10/2014 |

| Magyar (Hungarian) | | Malti (Maltese) | | Nederlands (Dutch) | | Polski (Polish) | |
|---|---|---|---|---|---|---|---|
| Környezetvédelmi terméknyilatkozatot | | Dikjarazzjoni Ambjentali dwar il-Prodott | | Milieuproductverklaring | | Deklarację środowiskową produktu | |
| RoHS | 2011/65/EU Irányelve | RoHS | Direttiva 2011/65/UE | RoHS | Richtlijn 2011/65/EU | RoHS | Dyrektywa 2011/65/UE |
| WEEE | 2012/19/EU Irányelve | WEEE | Direttiva 2012/19/UE | WEEE | Richtlijn 2012/19/EU | WEEE | Dyrektywa 2012/19/UE |
| PPW | 94/62/EK Irányelve | PPW | Direttiva 94/62/KE | PPW | Richtlijn 94/62/EG | PPW | Dyrektywa 94/62/WE |
| REACH | 1907/2006/EK Rendelete | REACH | REGOLAMENT (KE) NRU 1907/2006 | REACH | Verordening (EG) nr. 1907/2006 | REACH | Rozporządzenie (WE) nr 1907/2006 |
| Név/ cím : | Richard Hsu / Quality Management Division Senior Manager | Isem/ titolu : | Richard Hsu / Quality Management Division Senior Manager | Naam/ titel : | Richard Hsu / Quality Management Division Senior Manager | Nazwisko /tytuł : | Richard Hsu / Quality Management Division Senior Manager |
| Aláírás : | Dátum (éééé/hh/nn): 2014/10/01 | Firma : | Data (ssss/xx/jj): 2014/10/01 | Handtekening : | Datum (dd/mm/jaar): 01/10/2014 | Podpis : | Data (rrrr/mm/dd): 2014/10/01 |

| Português (Portuguese) | | Română (Romanian) | | Slovenčina (Slovak) | | Slovenščina (Slovene) | |
|---|---|---|---|---|---|---|---|
| Declaração ambiental do produto | | Declarație de mediu privind produsele | | Vyhlásenie o environmentálnom výrobku | | Okoljsko deklaracijo izdelka | |
| RoHS | Directiva 2011/65/UE | RoHS | Directiva 2011/65/UE | RoHS | Smernica 2011/65/EU | RoHS | Direktiva 2011/65/EU |
| WEEE | Directiva 2012/19/UE | WEEE | Directiva 2012/19/UE | WEEE | Smernica 2012/19/EU | WEEE | Direktiva 2012/19/EU |
| PPW | Directiva 94/62/CE | PPW | Directiva 94/62/CE | PPW | Smernica 94/62/ES | PPW | Direktiva 94/62/ES |
| REACH | Regulamento (CE) n.º 1907/2006 | REACH | REGULAMENTUL (CE) NR.907/2006 | REACH | Nariadenie (ES) č. 1907/2006 | REACH | Uredba (ES) št. 1907/2006 |
| Nome/ título : | Richard Hsu / Quality Management Division Senior Manager | Numele/ titlu : | Richard Hsu / Quality Management Division Senior Manager | Meno/ titul : | Richard Hsu / Quality Management Division Senior Manager | Ime/ naziv : | Richard Hsu / Quality Management Division Senior Manager |
| Assinatura : | Data (dd/mm/aaaa): 01/10/2014 | Semnătura : | Data (zz/ll/aaaa): 01/10/2014 | Podpis : | Dátum (dd/mm/rrrr): 01/10/2014 | Podpis : | Datum (dd/mm/llll): 01/10/2014 |

| Suomi (Finnish) | | Svenska (Swedish) | | Ελληνικά (Greek) | | Norsk (Norwegian) | |
|---|---|---|---|---|---|---|---|
| Standardiin perustuva ympäristötuoteseloste | | Miljöproduktdeklaration | | Περιβαλλοντική δήλωση προϊόντος | | Miljødeklarasjon | |
| RoHS | Direktiivi 2011/65/EU | RoHS | Direktiv 2011/65/EU | RoHS | Οδηγία 2011/65/ΕΕ | RoHS | Direktiv 2011/65/EU |
| WEEE | Direktiivi 2012/19/EU | WEEE | Direktiv 2012/19/EU | WEEE | Οδηγία 2012/19/ΕΕ | WEEE | Direktiv 2012/19/EU |
| PPW | Direktiivi 94/62/EY | PPW | Direktiv 94/62/EG | PPW | Οδηγία 94/62/ΕΚ | PPW | Direktiv 94/62/EF |
| REACH | ASETUS (EY) N:o 1907/2006 | REACH | Förordning (EG) nr 1907/2006 | REACH | Κανονισμοσ (ΕΚ) αριθ. 1907/2006 | REACH | Forordning (EF) nr. 1907/2006 |
| Nimi/ otsikko : | Richard Hsu / Quality Management Division Senior Manager | Namn/ titel : | Richard Hsu / Quality Management Division Senior Manager | Ονομα/ τίτλος : | Richard Hsu / Quality Management Division Senior Manager | Navn/ tittel : | Richard Hsu / Quality Management Division Senior Manager |
| Allekirjoitus : | Päivämäärä (pp/kk/vvvv): 01/10/2014 | Namnteckning : | Datum (dd/mm/åååå): 01/10/2014 | Υπογραφή : | Ημερομηνία (ηη/μμ/εεεε): 01/10/2014 | Signatur : | Dato (dd/mm/åååå): 01/10/2014 |

## 台灣

警告使用者：

- 這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。」

安全警告 - 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸
  - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
  - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座 ( 如：北美 / 台灣電壓 110V AC，歐洲是 230V AC)。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 設備必須接地，接地導線不允許被破壞或沒有適當安裝接地導線，如果不確定接地方式是否符合要求可聯繫相應的電氣檢驗機構檢驗。
- 如果您提供的系統中有提供熱插拔電源，連接或斷開電源請遵循以下指導原則
  - 先連接電源線至設備連，再連接電源。
  - 先斷開電源再拔除連接至設備的電源線。
  - 如果系統有多個電源，需拔除所有連接至電源的電源線再關閉設備電源。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  - 對永久連接之設備， 在設備外部須安裝可觸及之斷電裝置；
  - 對插接式之設備， 插座必須接近安裝之地點而且是易於觸及的。

## About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

### Explanation of the Symbols

| SYMBOL | EXPLANATION |
|---|---|
| | Alternating current (AC):<br>AC is an electric current in which the flow of electric charge periodically reverses direction. |
| | Direct current (DC):<br>DC if the unidirectional flow or movement of electric charge carriers. |
| | Earth; ground:<br>A wiring terminal intended for connection of a Protective Earthing Conductor. |
| | Class II equipment:<br>The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation. |

## 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 for global products, or at www.us.zyxel.com for North American products.

## Trademarks

ZyNOS (ZyXEL Network Operating System) and ZON (ZyXEL One Network)are registered trademarks of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

## 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. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

## Regulatory Notice and Statement

Model List:UAG2100,UAG4100

## UNITED STATES of AMERICA

The following information applies if you use the product within USA area.

### FCC EMC Statement

- The device complies with Part 15 of 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 device.
- 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 device 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 device does cause harmful interference to radio or television reception, which is found by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna
  - Increase the separation between the devices
  - Connect the equipment to an outlet other than the receiver's
  - Consult a dealer or an experienced radio/TV technician for assistance

The following information applies if you use the product with RF function within USA area.

### FCC Radiation Exposure Statement

- This device 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-247 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.
- 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.

### Antenna information

| TYPE | MANUFACTURER | GAIN | CONNECTOR |
|---|---|---|---|
| Omini-directional dipole | LYNwave | 3dBi | Reverse SMA plug |
| Omini-directional dipole | Master Wave | 3dBi | Reverse SMA plug |

If the product with 5G wireless function operating in 5150-5250 MHz and 5725-5850 MHz , the following attention must be paid,

- The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and
- The worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2(3) of RSS 247 shall be clearly indicated.

If the product with 5G wireless function operating in 5250-5350 MHz and 5470-5725 MHz , the following attention must be paid.

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit.
- 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.
- Le présent émetteur radio (2468C-Z2FPM9582, 2468C-Z5SPM9382) de modèle s'il fait partie du matériel de catégoriel) 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.

### Informations Antenne

| TYPE | FABRICANT | GAIN | CONNECTEUR |
|---|---|---|---|
| Omini-directional dipole | LYNwave | 3dBi | Reverse SMA plug |
| Omini-directional dipole | Master Wave | 3dBi | Reverse SMA plug |

Lorsque la fonction sans fil 5G fonctionnant en 5150-5250 MHz and 5725-5850 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes

- Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée pour l'exploitation point à point et l'exploitation non point à point, selon le cas;
- Les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, et énoncée à la section 6.2.2 3) du CNR-247, doivent être clairement indiqués.

Lorsque la fonction sans fil 5G fonctionnant en 5250-5350 MHz et 5470-5725 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes.

- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

### Industry Canada radiation exposure statement

This device complies with IC radiation exposure limits set forth for an uncontrolled environment. This device should be installed and operated with a minimum distance of 20 cm 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.

### CE EMC statement

WARNING: This equipment is compliant with Class A of EN55032. In a residential environment this equipment may cause radio interference.

### 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).
- This device is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range.

| | |
|---|---|
| Български (Bulgarian) | С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/ЕС. |
| 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 zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC. |
| Dansk (Danish) | Undertegnede Zyxel erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF. |
| Deutsch (German) | Hiermit erklärt 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 Zyxel ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ. |
| English | Hereby, Zyxel declares that this device 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 deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas. |
| Magyar (Hungarian) | Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EK irányelv egyéb elõírásainak. |
| Malti (Maltese) | Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti 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 cerinţele esenţiale şi 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 1999/5/EC) 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 1999/5/CE) 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 1999/5/EC) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:
- Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der Richtlinie 1999/5/CE folgen) mit Außnahme 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 frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC 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 | CZ | 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 | Switzerland | CH |
| Ireland | IE | Sweden | SE |
| 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 obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- 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.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- 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.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. 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.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,

  - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;

  - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

## Environment Statement

### European Union - Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

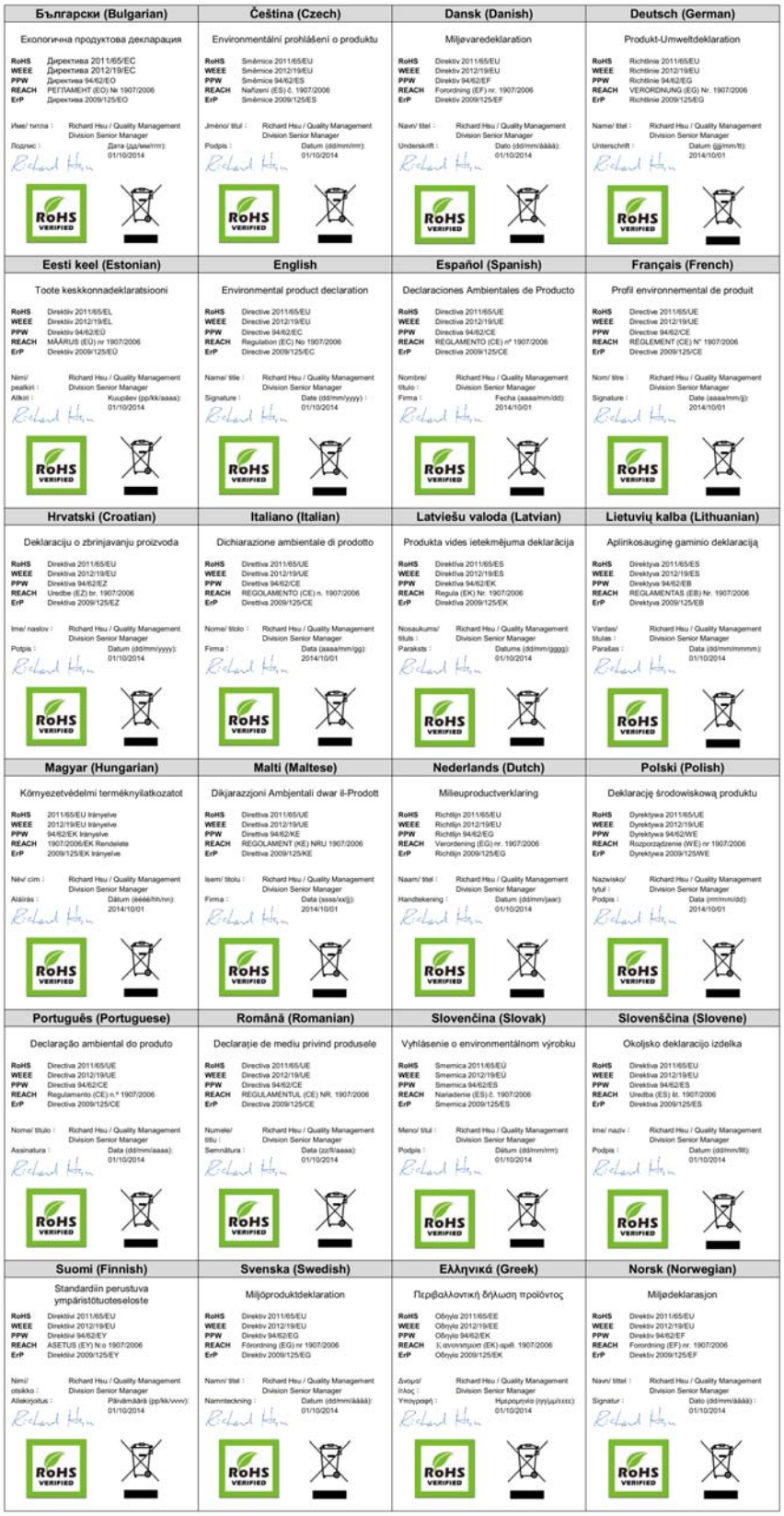
El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.

## Environmental Product Declaration



| Български (Bulgarian) | Čeština (Czech) | Dansk (Danish) | Deutsch (German) |
|---|---|---|---|
| Екологична продуктова декларация | Environmentální prohlášení o produktu | Miljøvaredeklaration | Produkt-Umweltdeklaration |
| RoHS Директива 2011/65/ЕС<br>WEEE Директива 2012/19/ЕС<br>PPW Директива 94/62/ЕО<br>REACH РЕГЛАМЕНТ (ЕО) № 1907/2006<br>ErP Директива 2009/125/ЕО | RoHS Směrnice 2011/65/EU<br>WEEE Směrnice 2012/19/EU<br>PPW Směrnice 94/62/ES<br>REACH Nařízení (ES) č. 1907/2006<br>ErP Směrnice 2009/125/ES | RoHS Direktiv 2011/65/EU<br>WEEE Direktiv 2012/19/EU<br>PPW Direktiv 94/62/EF<br>REACH Forordning (EF) nr. 1907/2006<br>ErP Direktiv 2009/125/EF | RoHS Richtlinie 2011/65/EU<br>WEEE Richtlinie 2012/19/EU<br>PPW Richtlinie 94/62/EG<br>REACH VERORDNUNG (EG) Nr. 1907/2006<br>ErP Richtlinie 2009/125/EG |
| Име/ титла : Richard Hsu / Quality Management Division Senior Manager<br>Подпис : Дата (дд/мм/гггг): 01/10/2014 | Jméno/ titul : Richard Hsu / Quality Management Division Senior Manager<br>Podpis : Datum (dd/mm/rrrr): 01/10/2014 | Navn/ titel : Richard Hsu / Quality Management Division Senior Manager<br>Underskrift : Dato (dd/mm/åååå): 01/10/2014 | Name/ titel : Richard Hsu / Quality Management Division Senior Manager<br>Unterschrift : Datum (tt/mm/jj): 2014/10/01 |
| **Eesti keel (Estonian)** | **English** | **Español (Spanish)** | **Français (French)** |
| Toote keskkonnadeklaratsiooni | Environmental product declaration | Declaraciones Ambientales de Producto | Profil environnemental de produit |
| RoHS Direktiiv 2011/65/EL<br>WEEE Direktiiv 2012/19/EL<br>PPW Direktiiv 94/62/EÜ<br>REACH MÄÄRUS (EÜ) nr 1907/2006<br>ErP Direktiiv 2009/125/EÜ | RoHS Directive 2011/65/EU<br>WEEE Directive 2012/19/EU<br>PPW Directive 94/62/EC<br>REACH Regulation (EC) No 1907/2006<br>ErP Directive 2009/125/EC | RoHS Directiva 2011/65/UE<br>WEEE Directiva 2012/19/UE<br>PPW Directiva 94/62/CE<br>REACH REGLAMENTO (CE) nº 1907/2006<br>ErP Directiva 2009/125/CE | RoHS Directive 2011/65/UE<br>WEEE Directive 2012/19/UE<br>PPW Directive 94/62/CE<br>REACH RÈGLEMENT (CE) N° 1907/2006<br>ErP Directive 2009/125/CE |
| Nimi/ pealkiri : Richard Hsu / Quality Management Division Senior Manager<br>Allkiri : Kuupäev (pp/kk/aaaa): 01/10/2014 | Name/ title : Richard Hsu / Quality Management Division Senior Manager<br>Signature : Date (dd/mm/yyyy) : 01/10/2014 | Nombre/ título : Richard Hsu / Quality Management Division Senior Manager<br>Firma : Fecha (aaaa/mm/dd): 2014/10/01 | Nom/ titre : Richard Hsu / Quality Management Division Senior Manager<br>Signature : Date (aaaa/mm/jj): 2014/10/01 |
| **Hrvatski (Croatian)** | **Italiano (Italian)** | **Latviešu valoda (Latvian)** | **Lietuvių kalba (Lithuanian)** |
| Deklaraciju o zbrinjavanju proizvoda | Dichiarazione ambientale di prodotto | Produkta vides ietekmējuma deklarācija | Aplinkosauginę gaminio deklaraciją |
| RoHS Direktiva 2011/65/EU<br>WEEE Direktiva 2012/19/EU<br>PPW Direktiva 94/62/EZ<br>REACH Uredbe (EZ) br. 1907/2006<br>ErP Direktiva 2009/125/EZ | RoHS Direttiva 2011/65/UE<br>WEEE Direttiva 2012/19/UE<br>PPW Direttiva 94/62/CE<br>REACH REGOLAMENTO (CE) n. 1907/2006<br>ErP Direttiva 2009/125/CE | RoHS Direktīva 2011/65/ES<br>WEEE Direktīva 2012/19/ES<br>PPW Direktīva 94/62/EK<br>REACH Regula (EK) Nr. 1907/2006<br>ErP Direktīva 2009/125/EK | RoHS Direktyva 2011/65/ES<br>WEEE Direktyva 2012/19/ES<br>PPW Direktyva 94/62/EB<br>REACH REGLAMENTAS (EB) Nr. 1907/2006<br>ErP Direktyva 2009/125/EB |
| Ime/ naslov : Richard Hsu / Quality Management Division Senior Manager<br>Potpis : Datum (dd/mm/yyyy): 01/10/2014 | Nome/ titolo : Richard Hsu / Quality Management Division Senior Manager<br>Firma : Data (aaaa/mm/gg): 2014/10/01 | Nosaukums/ tituls : Richard Hsu / Quality Management Division Senior Manager<br>Paraksts : Datums (dd/mm/gggg): 01/10/2014 | Vardas/ tituas : Richard Hsu / Quality Management Division Senior Manager<br>Parašas : Data (dd/mm/mmmm): 01/10/2014 |
| **Magyar (Hungarian)** | **Malti (Maltese)** | **Nederlands (Dutch)** | **Polski (Polish)** |
| Környezetvédelmi terméknyilatkozatot | Dikjarazzjoni Ambjentali dwar il-Prodott | Milieuproductverklaring | Deklarację środowiskową produktu |
| RoHS 2011/65/EU Irányelve<br>WEEE 2012/19/EU Irányelve<br>PPW 94/62/EK Irányelve<br>REACH 1907/2006/EK Rendelete<br>ErP 2009/125/EK Irányelve | RoHS Direttiva 2011/65/UE<br>WEEE Direttiva 2012/19/UE<br>PPW Direttiva 94/62/KE<br>REACH REGOLAMENT (KE) NRU 1907/2006<br>ErP Direttiva 2009/125/KE | RoHS Richtlijn 2011/65/EU<br>WEEE Richtlijn 2012/19/EU<br>PPW Richtlijn 94/62/EG<br>REACH Verordening (EG) nr. 1907/2006<br>ErP Richtlijn 2009/125/EG | RoHS Dyrektywa 2011/65/UE<br>WEEE Dyrektywa 2012/19/UE<br>PPW Dyrektywa 94/62/WE<br>REACH Rozporządzenie (WE) nr 1907/2006<br>ErP Dyrektywa 2009/125/WE |
| Név/ cím : Richard Hsu / Quality Management Division Senior Manager<br>Aláírás : Dátum (éééé/hh/nn): 2014/10/01 | Isem/ titolu : Richard Hsu / Quality Management Division Senior Manager<br>Firma : Data (ssss/xx/jj): 2014/10/01 | Naam/ titel : Richard Hsu / Quality Management Division Senior Manager<br>Handtekening : Datum (dd/mm/jaar): 01/10/2014 | Nazwisko/ tytuł : Richard Hsu / Quality Management Division Senior Manager<br>Podpis : Data (rr/mm/dd): 2014/10/01 |
| **Português (Portuguese)** | **Română (Romanian)** | **Slovenčina (Slovak)** | **Slovenščina (Slovene)** |
| Declaração ambiental do produto | Declaraţie de mediu privind produsele | Vyhlásenie o environmentálnom výrobku | Okoljsko deklaracijo izdelka |
| RoHS Directiva 2011/65/UE<br>WEEE Directiva 2012/19/UE<br>PPW Directiva 94/62/CE<br>REACH Regulamento (CE) n.º 1907/2006<br>ErP Directiva 2009/125/CE | RoHS Directiva 2011/65/UE<br>WEEE Directiva 2012/19/UE<br>PPW Directiva 94/62/CE<br>REACH REGULAMENTUL (CE) NR. 1907/2006<br>ErP Directiva 2009/125/CE | RoHS Smernica 2011/65/EÚ<br>WEEE Smernica 2012/19/EÚ<br>PPW Smernica 94/62/ES<br>REACH Nariadenie (ES) č. 1907/2006<br>ErP Smernica 2009/125/ES | RoHS Direktiva 2011/65/EU<br>WEEE Direktiva 2012/19/EU<br>PPW Direktiva 94/62/ES<br>REACH Uredba (ES) št. 1907/2006<br>ErP Direktiva 2009/125/ES |
| Nome/ título : Richard Hsu / Quality Management Division Senior Manager<br>Assinatura : Data (dd/mm/aaaa): 01/10/2014 | Numele/ titlu : Richard Hsu / Quality Management Division Senior Manager<br>Semnătura : Data (zz/ll/aaaa): 01/10/2014 | Meno/ titul : Richard Hsu / Quality Management Division Senior Manager<br>Podpis : Dátum (dd/mm/rrrr): 01/10/2014 | Ime/ naziv : Richard Hsu / Quality Management Division Senior Manager<br>Podpis : Datum (dd/mm/llll): 01/10/2014 |
| **Suomi (Finnish)** | **Svenska (Swedish)** | **Ελληνικά (Greek)** | **Norsk (Norwegian)** |
| Standardiin perustuva ympäristötuoteseloste | Miljöproduktdeklaration | Περιβαλλοντική δήλωση προϊόντος | Miljødeklarasjon |
| RoHS Direktiivi 2011/65/EU<br>WEEE Direktiivi 2012/19/EU<br>PPW Direktiivi 94/62/EY<br>REACH ASETUS (EY) N:o 1907/2006<br>ErP Direktiivi 2009/125/EY | RoHS Direktiv 2011/65/EU<br>WEEE Direktiv 2012/19/EU<br>PPW Direktiv 94/62/EG<br>REACH Förordning (EG) nr 1907/2006<br>ErP Direktiv 2009/125/EG | RoHS Οδηγία 2011/65/ΕΕ<br>WEEE Οδηγία 2012/19/ΕΕ<br>PPW Οδηγία 94/62/ΕΚ<br>REACH Ι), αναναημωση (ΕΚ) αριθ. 1907/2006<br>ErP Οδηγία 2009/125/ΕΚ | RoHS Direktiv 2011/65/EU<br>WEEE Direktiv 2012/19/EU<br>PPW Direktiv 94/62/EF<br>REACH Forordning (EF) nr. 1907/2006<br>ErP Direktiv 2009/125/EF |
| Nimi/ otsikko : Richard Hsu / Quality Management Division Senior Manager<br>Allekirjoitus : Päivämäärä (pp/kk/vvvv): 01/10/2014 | Namn/ titel : Richard Hsu / Quality Management Division Senior Manager<br>Namnteckning : Datum (dd/mm/åååå): 01/10/2014 | Όνομα/ Τίτλος : Richard Hsu / Quality Management Division Senior Manager<br>Υπογραφή : Ημερομηνία (ηη/μμ/ττττ): 01/10/2014 | Navn/ tittel : Richard Hsu / Quality Management Division Senior Manager<br>Signatur : Dato (dd/mm/åååå) : 01/10/2014 |

**台灣**

以下訊息僅適用於產品具有無線功能且銷售至台灣地區

- 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。
- 電磁波曝露量 MPE 標準值 1 $mW/cm^2$，送測產品實測值為： 0.150 $mW/cm^2$。本產品使用時建議應距離人體 20 cm。
- 無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用， 俟無干擾之虞，始得繼續使用。
- 無線資訊傳設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作， 發射的信號應維持於操作頻帶中

以下訊息僅適用於產品操作於 5.25-5.35 秭赫頻帶內並銷售至台灣地區

- 在 5.25-5.35 秭赫頻帶內操作之無線資訊傳輸設備，限於室內使用。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

- 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

安全警告 - 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸：
  - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
  - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座 ( 如：北美 / 台灣電壓 110V AC，歐洲是 230V AC)。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  - 對永久連接之設備， 在設備外部須安裝可觸及之斷電裝置；
  - 對插接式之設備， 插座必須接近安裝之地點而且是易於觸及的。

## About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

### Explanation of the Symbols

| SYMBOL | EXPLANATION |
|---|---|
| | Alternating current (AC):<br>AC is an electric current in which the flow of electric charge periodically reverses direction. |
| | Direct current (DC):<br>DC if the unidirectional flow or movement of electric charge carriers. |
| | Earth; ground:<br>A wiring terminal intended for connection of a Protective Earthing Conductor. |
| | Class II equipment:<br>The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation. |

## 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 for global products, or at www.us.zyxel.com for North American products.

## 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. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

# Index

## Symbols

## Numbers

3322 Dynamic DNS 229
3DES 365

## A

AAA
  port 471
AAA server 468
  and users 409
  local user database 469
  RADIUS 468, 469
  RADIUS group 470
  see also RADIUS
access 23
access users 408, 410
  custom page 515
  forcing login 275
  idle timeout 417
  logging in 275
  multiple logins 417
  see also users 408
  Web Configurator 419
access users, see also force user authentication policies
account
  user 408
accounting server 468
active protocol 369
  AH 369
  and encapsulation 370
  ESP 369
active sessions 83, 87, 100
ActiveX 399
AD
  port 471
address groups 451
  and content filtering 390, 391
  and FTP 534
  and SNMP 537
  and SSH 530
  and Telnet 533
  and WWW 514
address objects 451
  and content filtering 390, 391
  and FTP 534
  and NAT 225, 237
  and policy routes 224
  and SNMP 537
  and SSH 530
  and Telnet 533
  and VPN connections 349
  and WWW 514
  HOST 451
  RANGE 451
  SUBNET 451
  types of 451
address record 505
admin user
  troubleshooting 595, 596
admin users 408
  multiple logins 417
  see also users 408
Advanced Encryption Standard, see AES
AES 365
AF 227
AH 354, 369
  and transport mode 370
alerts 549, 550, 552, 554, 555, 556
ALG 254
  and NAT 254
  and policy routes 254
  and security policy 254
  and trunks 254
  FTP 254
  H.323 254

see also VoIP pass through 254
SIP 254
AP Group 151
Application Layer Gateway, see ALG
application patrol 385
actions 385
and security policy 385
classification 385
exceptions 385
port-less 385
ports 386
service ports 386
vs security policy 300
asymmetrical routes 302
allowing through the security policy 304
vs virtual interfaces 302
attacks
Denial of Service (DoS) 353
authentication
in IPSec 354
server 468
authentication algorithms 364, 365
and active protocol 365
MD5 365
SHA1 365
Authentication Header, see AH
authentication method objects 473
and users 409
and WWW 514
create 474
authentication policy
exceptional services 277
Authentication server
RADIUS client 539
authentication server 537
authentication type 67, 494
Authentication, Authorization, Accounting servers, see AAA server
authorization server 468


## B


backing up configuration files 560
bandwidth limit
troubleshooting 594
bandwidth management 375, 385
and schedules 380, 383
and user groups 380, 383
and users 380, 383
maximize bandwidth usage 379
see also application patrol 385
boot module 565
bridge interfaces 170, 197
and virtual interfaces of members 198
basic characteristics 170
effect on routing table 198
member interfaces 198
virtual 204
bridges 197


## C


CA
and certificates 477
CA (Certificate Authority), see certificates
Calling Station ID 435
capturing packets 571
CEF (Common Event Format) 547, 554
certificate
troubleshooting 596
Certificate Authority (CA)
see certificates
Certificate Revocation List (CRL) 477
certificates 476
advantages of 477
and CA 477
and FTP 534
and HTTPS 511
and IKE SA 369
and SSH 530
and VPN gateways 349
and WWW 513
certification path 477, 483, 489
expired 477
factory-default 477
file formats 477
fingerprints 484, 490
importing 480
in IPSec 361
not used for encryption 477
revoked 477

self-signed 477, 482
serial number 484, 489
storage space 479, 486
thumbprint algorithms 478
thumbprints 478
used for authentication 477
verifying fingerprints 478
certification requests 482
certifications 613
viewing 609, 617
Challenge Handshake Authentication Protocol (CHAP) 494
CHAP (Challenge Handshake Authentication Protocol) 494
CHAP/PAP 494
CLI 22, 26
button 26
messages 26
popup window 26
commands 22
sent by Web Configurator 26
Common Event Format (CEF) 547, 554
comparison table 20
compression (stac) 494
computer names 179, 195, 202, 208
configuration
information 568, 575
configuration file
troubleshooting 597
configuration files 558
at restart 560
backing up 560
downloading 562, 580
downloading with FTP 533
editing 558
how applied 559
lastgood.conf 561, 563
managing 560
startup-config.conf 563
startup-config-bad.conf 561
syntax 559
system-default.conf 563
uploading 564
uploading with FTP 533
use without restart 558
connection
troubleshooting 595
connectivity check 178, 188, 194, 203, 355
console port
speed 501
contact information 599
content filtering 390, 391
and address groups 390, 391
and address objects 390, 391
and registration 393, 395
and schedules 390, 391
and user groups 390
and users 390
by category 390, 391, 396
by keyword (in URL) 391, 400
by URL 391, 399, 401
by web feature 391, 399
categories 396
category service 395
default policy 391
external web filtering service 395, 403
filter list 391
managed web pages 396
policies 390, 391
registration status 393, 395
statistics 128
testing 397
uncategorized pages 396
unsafe web pages 395
URL for blocked access 393
cookies 22, 399
copyright 605
CPU usage 83, 86
current date/time 83, 497
and schedules 462
daylight savings 499
setting manually 500
time server 501
custom
access user page 515
login page 515
customer support 599


## D


Data Encryption Standard, see DES
date 497
daylight savings 499
DDNS 229

backup mail exchanger 233
mail exchanger 233
service providers 229
troubleshooting 594
Dead Peer Detection, see DPD
default
security policy behavior 301
Denial of Service (Dos) attacks 353
DES 365
device access
troubleshooting 592
DHCP 207, 496
and DNS servers 208
and domain name 496
and interfaces 207
client list 89
pool 208
static DHCP 208
diagnostics 568, 575
Diffie-Hellman key group 366
DiffServ 227
Digital Signature Algorithm public-key algorithm, see DSA
direct routes 221
disclaimer 605
DNS 502
address records 505
domain name forwarders 507
domain name to IP address 505
IP address to domain name 505
Mail eXchange (MX) records 508
pointer (PTR) records 505
DNS servers 68, 502, 507
and interfaces 208
domain name 496
Domain Name System, see DNS
DPD 363
DSA 482
DSCP 221, 224, 381, 383, 586
Dynamic Domain Name System, see DDNS
dynamic guest 104
dynamic guest account 104, 409
Dynamic Host Configuration Protocol, see DHCP.
DynDNS 229
DynDNS see also DDNS 229
Dynu 229


## E


e-mail
daily statistics report 543
Encapsulating Security Payload, see ESP
encapsulation
and active protocol 370
IPSec 354
transport mode 369
tunnel mode 369
VPN 369
encryption
IPSec 354
RSA 484
encryption algorithms 365
3DES 365
AES 365
and active protocol 365
DES 365
encryption method 494
enforcing policies in IPSec 353
ESP 354, 369
and transport mode 370
Ethernet interfaces 170
and routing protocols 173
basic characteristics 170
virtual 204
exceptional services 277
extended authentication
and VPN gateways 349
IKE SA 368
Extended Service Set IDentification 423
ext-user
troubleshooting 595


## F


FCC interference statement 605
file extensions
configuration files 558
shell scripts 558
file manager 558
Firefox 22
Firmware 158
firmware

and restart 564
boot module, see boot module
current version 82, 565
getting updated 564
uploading 564, 565
uploading with FTP 533
firmware upload
troubleshooting 597
flash usage 83
forcing login 275
FQDN 505
free guest account 342
free time 342
configuration 342
enable 342
FTP 533
additional signaling port 255
ALG 254
and address groups 534
and address objects 534
and certificates 534
and zones 534
signaling port 255
with Transport Layer Security (TLS) 534
Fully-Qualified Domain Name, see FQDN


## G


Generic Routing Encapsulation, see GRE.
GRE 209


## H


HTTP
over SSL, see HTTPS
redirect to HTTPS 513
vs HTTPS 511
HTTP redirect 246
and interfaces 249
and policy routes 247
and security policy 247
packet flow 247
troubleshooting 595
HTTPS 511
and certificates 511
authenticating clients 511
avoiding warning messages 521
example 520
vs HTTP 511
with Internet Explorer 520
with Netscape Navigator 520
HyperText Transfer Protocol over Secure Socket Layer, see HTTPS


## I


ICMP 456
IEEE 802.1q VLAN
IEEE 802.1x 424
IKE SA
aggressive mode 364, 367, 368
and certificates 369
and RADIUS 368
authentication algorithms 364, 365
content 366
Dead Peer Detection (DPD) 363
Diffie-Hellman key group 366
encryption algorithms 365
extended authentication 368
ID type 366
IP address, remote IPSec router 364
IP address, ZyXEL device 364
local identity 367
main mode 364, 367
NAT traversal 368
negotiation mode 364
password 368
peer identity 367
pre-shared key 366
proposal 364
see also VPN
user name 368
Instant Messenger (IM) 385
managing 385
interface
status 83, 96
troubleshooting 593
interfaces 169
and DNS servers 208
and HTTP redirect 249
and layer-3 virtualization 170

and NAT 237
and physical ports 169
and policy routes 225
and SMTP redirect 253
and static routes 227
and VPN gateways 349
and zones 169
as DHCP relays 207
as DHCP servers 207, 496
backup, see trunks
bandwidth management 207, 215, 217
bridge, see also bridge interfaces.
DHCP clients 206
Ethernet, see also Ethernet interfaces.
gateway 206
general characteristics 169
IP address 206
metric 206
MTU 207
overlapping IP address and subnet mask 206
port groups, see also port groups.
PPPoE/PPTP, see also PPPoE/PPTP interfaces.
prerequisites 171
relationships between 171
static DHCP 208
subnet mask 206
trunks, see also trunks.
types 170
virtual, see also virtual interfaces.
VLAN, see also VLAN interfaces.
Internet access
troubleshooting 592, 595
Internet Control Message Protocol, see ICMP
Internet Explorer 22
Internet Protocol Security, see IPSec
IP policy routing, see policy routes
IP protocols 456
and service objects 456
ICMP, see ICMP
TCP, see TCP
UDP, see UDP
IP static routes, see static routes
IP/MAC binding
example 263
exempt list 266
monitor 102
overview 263
static DHCP 266
IPSec 348
active protocol 354
AH 354
and certificates 349
authentication 354
certificates 361
connections 349
connectivity check 355
encapsulation 354
encryption 354
ESP 354
established in two phases 349
local network 348
local policy 353
NetBIOS 353
peer 348
Perfect Forward Secrecy 355
PFS 355
phase 2 settings 353
policy enforcement 353
remote IPSec router 348
remote network 348
remote policy 353
replay detection 353
SA life time 353
SA monitor 125
SA see also IPSec SA 369
see also VPN
static site-to-site 353
transport encapsulation 354
tunnel encapsulation 354
VPN gateway 349
IPSec SA
active protocol 369
authentication algorithms 364, 365
destination NAT for inbound traffic 372
encapsulation 369
encryption algorithms 365
local policy 369
NAT for inbound traffic 370
NAT for outbound traffic 370
Perfect Forward Secrecy (PFS) 370
proposal 370
remote policy 369
search by name 125
search by policy 125
see also IPSec
see also VPN
source NAT for inbound traffic 371
source NAT for outbound traffic 371

status 125
transport mode 369
tunnel mode 369
when IKE SA is disconnected 369
ISP account
CHAP 494
CHAP/PAP 494
MPPE 494
MSCHAP 494
MSCHAP-V2 494
PAP 494
ISP accounts 492
and PPPoE/PPTP interfaces 184, 492
authentication type 494
encryption method 494
stac compression 494


## J


Java 399
permissions 22
JavaScripts 22


## K


key pairs 476


## L


lastgood.conf 561, 563
layer-2 isolation 268
example 268
IP 269
LDAP
and users 409
port 471
least load first load balancing 211
LED suppression mode 143
LED troubleshooting 592
level-4 inspection 386
level-7 inspection 385
licensing 136
Link Layer Discovery Protocol (LLDP ) 108
LLDP (Link Layer Discovery Protocol) 108
load balancing 210
algorithms 211, 215, 217
least load first 211
round robin 211
see also trunks 210
session-oriented 211
spillover 212
weighted round robin 212
local user database 469
log
troubleshooting 597
log messages
categories 550, 552, 554, 555, 556
debugging 129
regular 129
types of 129
logged in users 90
login
custom page 515
logo
troubleshooting 597
logout
Web Configurator 24
logs
and security policy 307
e-mail profiles 546
e-mailing log messages 131, 549
formats 547
log consolidation 550
settings 545
syslog servers 546
system 546
types of 546


## M


MAC address 420
and VLAN 189
Ethernet interface 177
range 82
MAC authentication 435
Calling Station ID 435
case 435
delimiter 435

mac role 420
managed web pages 396
management access
troubleshooting 596
Management Information Base (MIB) 535
MD5 365
memory usage 83, 87
Message Digest 5, see MD5
messages
CLI 26
metrics, see reports
Microsoft
Challenge-Handshake Authentication Protocol (MSCHAP) 494
Challenge-Handshake Authentication Protocol Version 2 (MSCHAP-V2) 494
Point-to-Point Encryption (MPPE) 494
model name 82
monitor
SA 125
MPPE (Microsoft Point-to-Point Encryption) 494
MSCHAP (Microsoft Challenge-Handshake Authentication Protocol) 494
MSCHAP-V2 (Microsoft Challenge-Handshake Authentication Protocol Version 2) 494
multicast 429
multicast rate 429
My Certificates, see also certificates 479
myZyXEL.com 136, 139
accounts, creating 136

## N

NAT 227, 234
ALG, see ALG
and address objects 225
and address objects (HOST) 237
and ALG 254
and interfaces 237
and policy routes 219, 225
and security policy 303
and to-Device security policy 238
and VPN 368
loopback 239
port forwarding, see NAT
port translation, see NAT
traversal 368
NAT Port Mapping Protocol 256
NAT Traversal 256
NAT-PMP 256
NBNS 179, 195, 202, 208
NetBIOS
Broadcast over IPSec 353
Name Server, see NBNS.
Netscape Navigator 22
Network Address Translation, see NAT
Network Time Protocol (NTP) 500
No-IP 229

## O

objects
AAA server 468
addresses and address groups 451
authentication method 473
certificates 476
schedules 462
services and service groups 456
users, user groups 408
OSI level-4 386
OSI level-7 385
OUI 421

## P

packet
statistics 93, 94, 111
packet capture 571
files 570, 574, 575, 576
troubleshooting 598
packet captures
downloading files 571, 574, 576, 577
PAP (Password Authentication Protocol) 494
Password Authentication Protocol (PAP) 494
Peanut Hull 229
Peer-to-peer (P2P)
managing 385
Perfect Forward Secrecy (PFS) 355
Diffie-Hellman key group 370

PFS (Perfect Forward Secrecy) 355, 370
physical ports
packet statistics 93, 94, 111
pointer record 505
Point-to-Point Protocol over Ethernet, see PPPoE.
Point-to-Point Tunneling Protocol, see PPTP
policy enforcement in IPSec 353
policy route
troubleshooting 593
policy routes 218
actions 220
and address objects 224
and ALG 254
and HTTP redirect 247
and interfaces 225
and NAT 219
and schedules 224
and service objects 456
and SMTP redirect 251
and trunks 210, 225
and user groups 224
and users 224
and VPN 1-1 mapping 242
benefits 219
criteria 220
overriding direct routes 221
pop-up windows 22
port forwarding, see NAT
port groups 170, 172
port roles 171
and Ethernet interfaces 171
and physical ports 171
port translation, see NAT
power off 591
PPP 208
troubleshooting 594
PPP interfaces
subnet mask 206
PPPoE 208
and RADIUS 208
TCP port 1723 209
PPPoE/PPTP interfaces 170, 183
and ISP accounts 184, 492
basic characteristics 170
gateway 184
subnet mask 184
PPTP 208
and GRE 209
as VPN 209
pre-subscriber account 410
printer
status 123
printer firmware 332
printer list 332
printer management 332
problems 592
product registration 610
proxy servers 246
web, see web proxy servers
PTR record 505
Public-Key Infrastructure (PKI) 477
public-private key pairs 476

## Q

QoS 219, 376

## R

RADIUS 468, 469
advantages 468
and IKE SA 368
and PPPoE 208
and users 409
user attributes 422
RADIUS server 537
troubleshooting 595
reboot 590
vs reset 590
registration 136
and content filtering 393, 395
product 610
Remote Authentication Dial-In User Service, see RADIUS
remote management
FTP, see FTP
see also service control 510
Telnet 532
to-Device security policy 301
WWW, see WWW
remote network 348

replay detection 353
reports
collecting data 98
content filtering 128
daily 543
daily e-mail 543
specifications 100
traffic statistics 98
reset 598
vs reboot 590
RESET button 598
RFC
1631 (NAT) 227
2131 (DHCP) 207
2132 (DHCP) 207
2402 (AH) 354, 369
2406 (ESP) 354, 369
2516 (PPPoE) 208
2637 (PPTP) 208
2890 (GRE) 209
Rivest, Shamir and Adleman public-key algorithm (RSA) 482
round robin 211
routing
troubleshooting 594
routing protocols
and Ethernet interfaces 173
RSA 482, 484, 489
RSSI threshold 429

## S

schedule
troubleshooting 596
schedules 462
and bandwidth management 380, 383
and content filtering 390, 391
and current date/time 462
and policy routes 224
and security policy 307
one-time 462
recurring 462
types of 462
screen resolution 22
Secure Hash Algorithm, see SHA1
Secure Socket Layer, see SSL
security associations, see IPSec
security policy 300
actions 307
and ALG 254
and application patrol 385
and HTTP redirect 247
and logs 307
and NAT 303
and schedules 307
and service groups 306
and service objects 456
and services 306
and SMTP redirect 251
and user groups 307, 309
and users 307, 309
and VPN 1-1 mapping 242
and zones 301, 305
asymmetrical routes 302, 304
global rules 302
priority 305
rule criteria 302
session control 307
session limits 302
stateful inspection 301
to-Device, see to-Device security policy
triangle routes 302, 304
troubleshooting 593
vs application patrol 300
security settings
troubleshooting 593
serial number 82
service control 510
and to-Device security policy 510
and users 510
limitations 510
timeouts 510
service groups 457
and security policy 306
service objects 456
and IP protocols 456
and policy routes 456
and security policy 456
Service Set 423
service subscription status 138
services 456
and security policy 306
session control 307
session limits 302

sessions 100
sessions usage 83, 87
SHA1 365
shell script
troubleshooting 597
shell scripts 558
and users 422
downloading 566
editing 565
how applied 559
managing 566
syntax 559
uploading 567
Short Message Service 346
shutdown 591
signatures
updating 139
Simple Network Management Protocol, see SNMP
SMS 346
configuration 346
send account information 346
ViaNett account 346
SMS gateway 346
SMTP redirect
and interfaces 253
and policy routes 251
and security policy 251
packet flow 251
SNAT 227
troubleshooting 594
SNMP 534, 535
agents 535
and address groups 537
and address objects 537
and zones 537
Get 535
GetNext 535
Manager 535
managers 535
MIB 535
network components 535
Set 535
Trap 535
traps 536
versions 534
Source Network Address Translation, see SNAT
spillover (for load balancing) 212
SSH 527
and address groups 530
and address objects 530
and certificates 530
and zones 530
client requirements 529
encryption methods 529
for secure Telnet 530
how connection is established 528
versions 529
with Linux 531
with Microsoft Windows 530
SSL 511
stac compression 494
startup-config.conf 563
if errors 561
missing at restart 560
present at restart 561
startup-config-bad.conf 561
stateful inspection 301
static DHCP 266
static routes 219
and interfaces 227
metric 227
statistics
content filtering 128
daily e-mail report 543
traffic 98
status 80
streaming protocols management 385
subscription services
status 138
supported browsers 22
syslog 554
syslog servers, see also logs
system log, see logs
system name 82, 496
system reports, see reports
system uptime 82
system-default.conf 563

## T

TCP 456
connections 456

port numbers 456
Telnet 532
and address groups 533
and address objects 533
and zones 533
with SSH 530
throughput rate
troubleshooting 597
time 497
time servers (default) 500
to-Device security policy 301
and NAT 238
and remote management 301
and service control 510
global rules 301
trademarks 610
traffic statistics 98
Transmission Control Protocol, see TCP
transport encapsulation 354
Transport Layer Security (TLS) 534
triangle routes 302
allowing through the security policy 304
vs virtual interfaces 302
Triple Data Encryption Standard, see 3DES
troubleshooting 568, 575, 592
admin user 595, 596
bandwidth limit 594
certificate 596
configuration file 597
connection resets 595
DDNS 594
device access 592
ext-user 595
firmware upload 597
HTTP redirect 595
interface 593
Internet access 592, 595
LEDs 592
logo 597
logs 597
management access 596
packet capture 598
policy route 593
PPP 594
RADIUS server 595
routing 594
schedules 596
security policy 593
security settings 593
shell scripts 597
SNAT 594
throughput rate 597
VLAN 594
trunks 170, 210
and ALG 254
and policy routes 210, 225
member interface mode 215, 217
member interfaces 215, 217
see also load balancing 210
Trusted Certificates, see also certificates 486
tunnel encapsulation 354


## U


UDP 456
messages 456
port numbers 456
Universal Plug and Play 256
Application 256
security issues 257
unsafe web pages 395
updating
signatures 139
upgrading
firmware 564
uploading
configuration files 564
firmware 564
shell scripts 565
UPnP 256
usage
CPU 83, 86
flash 83
memory 83, 87
onboard flash 83
sessions 83, 87
USB storage
status 107
user authentication 408
external 409
local user database 469
user awareness 410
User Datagram Protocol, see UDP
user group objects 408

user groups 408, 410
and bandwidth management 380, 383
and content filtering 390
and policy routes 224
and security policy 307, 309
user name
rules 412
user objects 408
user sessions, see sessions
user-aware 279
users 408
access, see also access users
admin (type) 408
admin, see also admin users
and AAA servers 409
and authentication method objects 409
and bandwidth management 380, 383
and content filtering 390
and LDAP 409
and policy routes 224
and RADIUS 409
and security policy 307, 309
and service control 510
and shell scripts 422
attributes for Ext-User 409
attributes for RADIUS 422
attributes in AAA servers 422
currently logged in 83, 90
default lease time 417, 419
default reauthentication time 417, 419
default type for Ext-User 409
ext-group-user (type) 408
Ext-User (type) 409
ext-user (type) 408
groups, see user groups
guest-manager (type) 408
lease time 413
limited-admin (type) 408
lockout 418
reauthentication time 413
types of 408
user names 412

## V

Vantage Report (VRPT) 554
virtual interfaces 170, 204
basic characteristics 170
not DHCP clients 206
types of 204
vs asymmetrical routes 302
vs triangle routes 302
Virtual Local Area Network, see VLAN.
Virtual Private Network, see VPN
VLAN 189
advantages 189
and MAC address 189
ID 189
troubleshooting 594
VLAN interfaces 170, 190
and Ethernet interfaces 190, 594
basic characteristics 170
virtual 204
VoIP pass through
see also ALG 254
VPN 348
active protocol 369
and NAT 368
IKE SA, see IKE SA
IPSec 348
IPSec SA
proposal 365
security associations (SA) 349
see also IKE SA
see also IPSec 348
see also IPSec SA
status 88
VPN 1-1 mapping 241
and policy routes 242
and security policy 242
example 241
introduction 241
packet flow 242
pool profile 244
VPN connections
and address objects 349
VPN gateways
and certificates 349
and extended authentication 349
and interfaces 349
VRPT (Vantage Report) 554

## W

warranty 609, 617
note 610, 617
Web Configurator 21
access 23
access users 419
requirements 22
supported browsers 22
web features
ActiveX 399
cookies 399
Java 399
web proxy servers 399
web proxy servers 247, 399
see also HTTP redirect
weighted round robin (for load balancing) 212
WEP (Wired Equivalent Privacy) 424
Wi-Fi Protected Access 424
Windows Internet Naming Service, see WINS
Windows Internet Naming Service, see WINS.
WINS 179, 195, 202, 208
WINS server 179
Wizard Setup 50, 64
WPA 424
WPA2 424
WWW 511
and address groups 514
and address objects 514
and authentication method objects 514
and certificates 513
and zones 514
see also HTTP, HTTPS 511

## Z

ZON Utility 540
zones 404
and FTP 534
and interfaces 404
and security policy 301, 305
and SNMP 537
and SSH 530
and Telnet 533
and WWW 514
extra-zone traffic 405
inter-zone traffic 405
intra-zone traffic 405
types of traffic 405