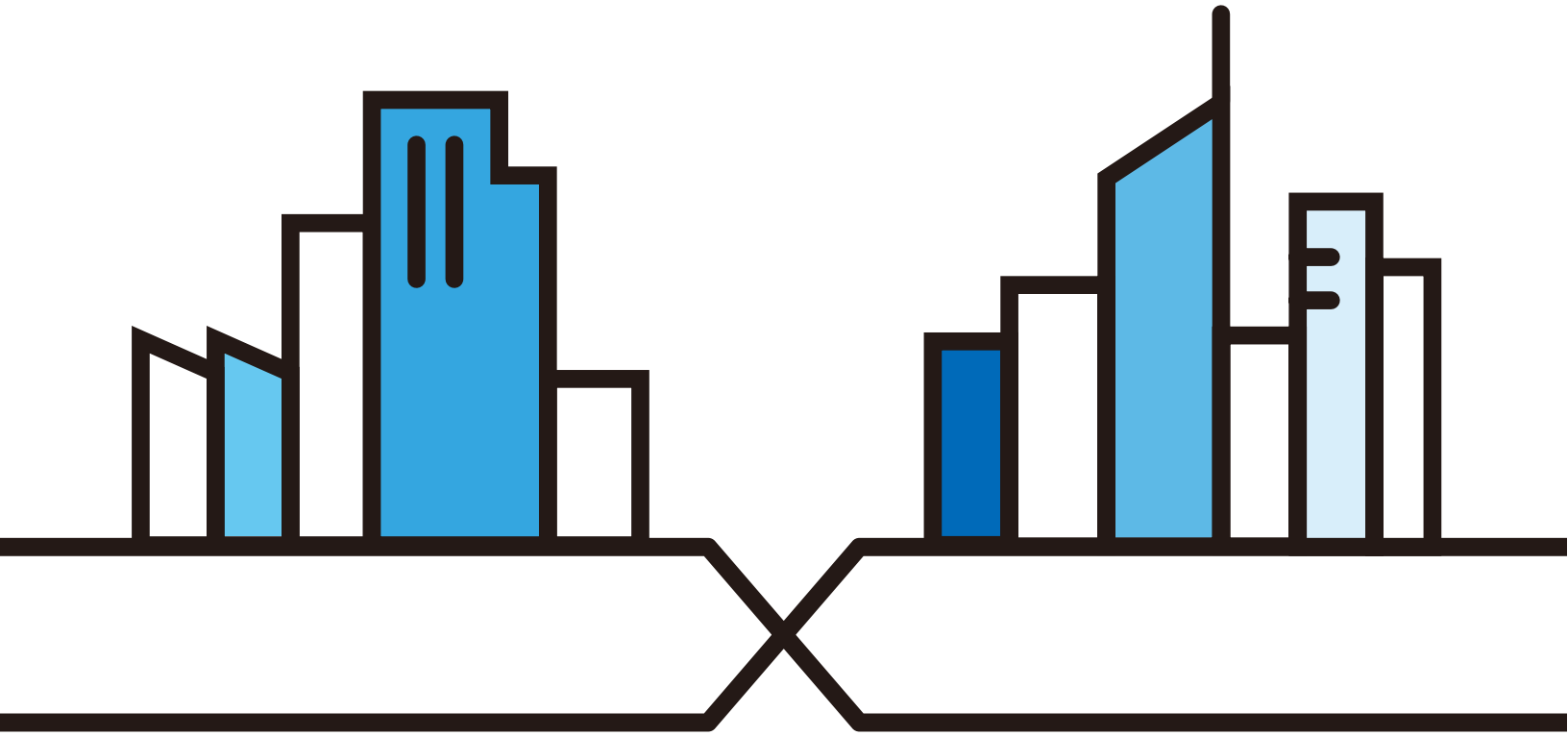
ZYXEL
Your Networking Ally

User's Guide

ZyWALL ATP Series

Default Login Details	
LAN Port IP Address	https://192.168.1.1
User Name	admin
Password	1234

Version 4.35 Edition 4, 11/2019



Copyright © 2019 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 product features or web configurator brand style. Every effort has been made to ensure that the information in this manual is accurate.

Note: The version number on the cover page refers to the Zyxel Device's latest firmware version to which this User's Guide applies.

Related Documentation

- Quick Start Guide

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

- CLI Reference Guide

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

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

- 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 Zyxel Device.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this guide.

Warnings tell you about things that could harm you or your device.

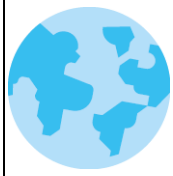
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- All models in this series may be referred to as the "Zyxel Device" in this guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Configuration > Network > Interface > Ethernet** means you first click **Configuration** in the navigation panel, then **Network**, then the **Interface** sub menu and finally the **Ethernet** tab to get to that screen.

Icons Used in Figures

Figures in this user guide may use the following generic icons. The Zyxel Device icon is not an exact representation of your device.

Zyxel Device	Generic Router	Wireless Router / Access Point
Switch	Firewall	Server
Internet 	Network Cloud	Smartphone
USB Dongle		

Contents Overview

Introduction 24
Initial Setup Wizard 48
Hardware, Interfaces and Zones 67
Quick Setup Wizards 75
Dashboard 109
Monitor 119
Licensing 186
Wireless 192
Interfaces 213
Routing 310
DDNS 337
NAT 343
Redirect Service 351
ALG 357
UPnP 364
IP/MAC Binding 379
Layer 2 Isolation 384
DNS Inbound LB 388
IPnP 394
IPSec VPN 396
SSL VPN 432
L2TP VPN 438
BWM (Bandwidth Management) 444
Web Authentication 460
Security Policy 489
Application Patrol 515
Content Filter 524
Anti-Malware 543
Reputation Filter 556
IDP 566
Sandboxing 584
Email Security 588
SSL Inspection 599
IP Exception 611
Object 614
Device HA 717
Cloud CNM 724
System 732
Log and Report 793

File Manager 806
Diagnostics 821
Packet Flow Explore 842
Shutdown 849
Troubleshooting 851

Table of Contents

Document Conventions 3

Contents Overview 4

Table of Contents 6

Part I: User's Guide 23

Chapter 1
Introduction 24

1.1 Overview 24
1.2 Registration at myZyxel 24
1.2.1 Grace Period 25
1.2.2 Applications 25
1.3 Management Overview 28
1.4 Web Configurator 29
1.4.1 Web Configurator Access 29
1.4.2 Web Configurator Screens Overview 32
1.4.3 Navigation Panel 37
1.4.4 Tables and Lists 44

Chapter 2
Initial Setup Wizard 48

2.1 Initial Setup Wizard Screens 48
2.1.1 Internet Access Setup - WAN Interface 48
2.1.2 Internet Access: Ethernet 49
2.1.3 Internet Access: PPPoE 50
2.1.4 Internet Access: PPTP 52
2.1.5 Internet Access: L2TP 54
2.1.6 Internet Access Setup - Second WAN Interface 56
2.1.7 Internet Access: Congratulations 57
2.1.8 Date and Time Settings 58
2.1.9 Register Device 58
2.1.10 Activate Service 60
2.1.11 Service Settings 61
2.1.12 Service Settings: SecuReporter 62
2.1.13 Wireless Settings: AP Controller 64
2.1.14 Wireless Settings: SSID & Security 64

2.1.15 Remote Management 65

Chapter 3
Hardware, Interfaces and Zones 67

3.1 Hardware Overview 67
3.1.1 Front Panels 67
3.1.2 Rear Panels 69
3.2 Mounting 70
3.2.1 Rack-mounting 70
3.2.2 Wall-mounting 71
3.3 Default Zones, Interfaces, and Ports 73
3.4 Stopping the Zyxel Device 74

Chapter 4
Quick Setup Wizards 75

4.1 Quick Setup Overview 75
4.2 WAN Interface Quick Setup 76
4.2.1 Choose an Ethernet Interface 76
4.2.2 Select WAN Type 77
4.2.3 Configure WAN IP Settings 77
4.2.4 ISP and WAN and ISP Connection Settings 78
4.2.5 Quick Setup Interface Wizard: Summary 81
4.3 VPN Setup Wizard 82
4.3.1 Welcome 82
4.3.2 VPN Setup Wizard: Wizard Type 83
4.3.3 VPN Express Wizard - Scenario 84
4.3.4 VPN Express Wizard - Configuration 85
4.3.5 VPN Express Wizard - Summary 85
4.3.6 VPN Express Wizard - Finish 86
4.3.7 VPN Advanced Wizard - Scenario 87
4.3.8 VPN Advanced Wizard - Phase 1 Settings 88
4.3.9 VPN Advanced Wizard - Phase 2 90
4.3.10 VPN Advanced Wizard - Summary 91
4.3.11 VPN Advanced Wizard - Finish 93
4.4 VPN Settings for Configuration Provisioning Wizard: Wizard Type 94
4.4.1 Configuration Provisioning Express Wizard - VPN Settings 94
4.4.2 Configuration Provisioning VPN Express Wizard - Configuration 95
4.4.3 VPN Settings for Configuration Provisioning Express Wizard - Summary 96
4.4.4 VPN Settings for Configuration Provisioning Express Wizard - Finish 97
4.4.5 VPN Settings for Configuration Provisioning Advanced Wizard - Scenario 98
4.4.6 VPN Settings for Configuration Provisioning Advanced Wizard - Phase 1 Settings 99
4.4.7 VPN Settings for Configuration Provisioning Advanced Wizard - Phase 2 101
4.4.8 VPN Settings for Configuration Provisioning Advanced Wizard - Summary 101

4.4.9 VPN Settings for Configuration Provisioning Advanced Wizard- Finish 104
4.5 VPN Settings for L2TP VPN Settings Wizard 104
4.5.1 L2TP VPN Settings 105
4.5.2 L2TP VPN Settings 106
4.5.3 VPN Settings for L2TP VPN Setting Wizard - Summary 106
4.5.4 VPN Settings for L2TP VPN Setting Wizard Completed 108

Chapter 5
Dashboard 109

5.1 Overview 109
5.1.1 What You Can Do in this Chapter 109
5.2 The General Screen 109
5.2.1 Device Information Screen 111
5.2.2 System Status Screen 112
5.2.3 Tx/Rx Statistics 112
5.2.4 The Latest Logs Screen 113
5.2.5 System Resources Screen 113
5.2.6 DHCP Table Screen 114
5.2.7 Number of Login Users Screen 115
5.2.8 Current Login User 116
5.2.9 VPN Status 116
5.2.10 SSL VPN Status 116
5.3 The Advanced Threat Protection Screen 117

Part II: Technical Reference 118

Chapter 6
Monitor 119

6.1 Overview 119
6.1.1 What You Can Do in this Chapter 119
6.2 The Port Statistics Screen 121
6.2.1 The Port Statistics Graph Screen 122
6.3 Interface Status Screen 123
6.4 The Traffic Statistics Screen 127
6.5 The Session Monitor Screen 129
6.6 The Login Users Screen 131
6.7 IGMP Statistics 133
6.8 The DDNS Status Screen 134
6.9 IP/MAC Binding 134
6.10 Cellular Status Screen 135
6.10.1 More Information 138

6.11 The UPnP Port Status Screen 139
6.12 USB Storage Screen 140
6.13 Ethernet Neighbor Screen 141
6.14 FQDN Object Screen 142
6.15 AP Information: AP List 144
6.15.1 AP List: More Information 146
6.15.2 AP List: Config AP 149
6.16 AP Information: Radio List 151
6.16.1 Radio List: More Information 153
6.17 AP Information: Top N APs 154
6.18 AP Information: Single AP 156
6.19 ZyMesh 157
6.20 SSID Info 158
6.21 Station Info: Station List 158
6.22 Station Info: Top N Stations 159
6.23 Station Info: Single Station 160
6.24 Detected Device 161
6.25 The IPSec Screen 162
6.26 The SSL Screen 164
6.27 The L2TP over IPSec Screen 164
6.28 The Content Filter Screen 165
6.29 The App Patrol Screen 167
6.30 The Anti-Malware Screen 168
6.31 The Reputation Filter Screen 170
6.32 The IDP Screen 172
6.33 The Email Security Screens 174
6.33.1 Email Security Summary 174
6.33.2 The Email Security Status Screen 176
6.34 The Sandboxing Screen 178
6.35 The SSL Inspection Screens 179
6.35.1 Certificate Cache List 180
6.36 Log Screens 181
6.36.1 View Log 181
6.36.2 View AP Log 183

Chapter 7
Licensing 186

7.1 Registration Overview 186
7.1.1 What you Need to Know 186
7.1.2 Registration Screen 187
7.1.3 Service Screen 187
7.2 Signature Update 189
7.2.1 What you Need to Know 189

7.2.2 The Signature Screen 190
7.2.3 Auto Update 190

Chapter 8
Wireless 192

8.1 Overview 192
8.1.1 What You Can Do in this Chapter 192
8.2 Controller Screen 192
8.3 AP Management Screens 193
8.3.1 Mgnt. AP List 193
8.3.2 AP Policy 197
8.3.3 AP Group 198
8.3.4 Firmware 204
8.4 Rogue AP 205
8.4.1 Add/Edit Rogue/Friendly List 207
8.5 Auto Healing 208
8.6 RTLS Overview 209
8.6.1 What You Can Do in this Chapter 209
8.6.2 Before You Begin 209
8.6.3 Configuring RTLS 210
8.7 Technical Reference 211
8.7.1 Dynamic Channel Selection 211
8.7.2 Load Balancing 212

Chapter 9
Interfaces 213

9.1 Interface Overview 213
9.1.1 What You Can Do in this Chapter 213
9.1.2 What You Need to Know 213
9.1.3 What You Need to Do First 218
9.2 Port Role 218
9.3 Port Configuration 219
9.4 Ethernet Summary Screen 220
9.4.1 Ethernet Edit 222
9.4.2 Proxy ARP 238
9.4.3 Virtual Interfaces 239
9.4.4 References 240
9.4.5 Add/Edit DHCPv6 Request/Release Options 241
9.4.6 Add/Edit DHCP Extended Options 242
9.5 PPP Interfaces 243
9.5.1 PPP Interface Summary 244
9.5.2 PPP Interface Add or Edit 245
9.6 Cellular Configuration Screen 250

9.6.1 Cellular Choose Slot 253
9.6.2 Add / Edit Cellular Configuration 253
9.7 Tunnel Interfaces 259
9.7.1 Configuring a Tunnel 261
9.7.2 Tunnel Add or Edit Screen 262
9.8 VLAN Interfaces 266
9.8.1 VLAN Summary Screen 267
9.8.2 VLAN Add/Edit 268
9.9 Bridge Interfaces 279
9.9.1 Bridge Summary 281
9.9.2 Bridge Add/Edit 282
9.10 VTI 293
9.10.1 Restrictions for IPSec Virtual Tunnel Interface 293
9.10.2 VTI Screen 294
9.10.3 VTI Add/Edit 294
9.11 Trunk Overview 298
9.11.1 What You Need to Know 298
9.12 The Trunk Summary Screen 301
9.12.1 Configuring a User-Defined Trunk 302
9.12.2 Configuring the System Default Trunk 304
9.13 Interface Technical Reference 305

Chapter 10
Routing 310

10.1 Policy and Static Routes Overview 310
10.1.1 What You Can Do in this Chapter 310
10.1.2 What You Need to Know 311
10.2 Policy Route Screen 312
10.2.1 Policy Route Edit Screen 314
10.3 IP Static Route Screen 319
10.3.1 Static Route Add/Edit Screen 319
10.4 Policy Routing Technical Reference 321
10.5 Routing Protocols Overview 321
10.5.1 What You Need to Know 322
10.6 The RIP Screen 322
10.7 The OSPF Screen 324
10.7.1 Configuring the OSPF Screen 327
10.7.2 OSPF Area Add/Edit Screen 328
10.7.3 Virtual Link Add/Edit Screen 330
10.8 BGP (Border Gateway Protocol) 331
10.8.1 Allow BGP Packets to Enter the Zyxel Device 332
10.8.2 Configuring the BGP Screen 332
10.8.3 The BGP Neighbors Screen 334

10.8.4 Example Scenario 335

Chapter 11
DDNS 337

11.1 DDNS Overview 337
11.1.1 What You Can Do in this Chapter 337
11.1.2 What You Need to Know 337
11.2 The DDNS Screen 338
11.2.1 The Dynamic DNS Add/Edit Screen 339

Chapter 12
NAT 343

12.1 NAT Overview 343
12.1.1 What You Can Do in this Chapter 343
12.1.2 What You Need to Know 343
12.2 The NAT Screen 344
12.2.1 The NAT Add/Edit Screen 346
12.3 NAT Technical Reference 349

Chapter 13
Redirect Service 351

13.1 Overview 351
13.1.1 HTTP Redirect 351
13.1.2 SMTP Redirect 351
13.1.3 What You Can Do in this Chapter 352
13.1.4 What You Need to Know 352
13.2 The Redirect Service Screen 354
13.2.1 The Redirect Service Edit Screen 355

Chapter 14
ALG 357

14.1 ALG Overview 357
14.1.1 What You Need to Know 357
14.1.2 Before You Begin 360
14.2 The ALG Screen 360
14.3 ALG Technical Reference 362

Chapter 15
UPnP 364

15.1 UPnP and NAT-PMP Overview 364
15.2 What You Need to Know 364
15.2.1 NAT Traversal 364
15.2.2 Cautions with UPnP and NAT-PMP 365

15.3 UPnP Screen 365
15.4 Technical Reference 366
15.4.1 Turning on UPnP in Windows 7 Example 366
15.4.2 Turn on UPnP in Windows 10 Example 370
15.4.3 Auto-discover Your UPnP-enabled Network Device 372
15.4.4 Web Configurator Easy Access in Windows 7 375
15.4.5 Web Configurator Easy Access in Windows 10 377

Chapter 16
IP/MAC Binding 379

16.1 IP/MAC Binding Overview 379
16.1.1 What You Can Do in this Chapter 379
16.1.2 What You Need to Know 379
16.2 IP/MAC Binding Summary 380
16.2.1 IP/MAC Binding Edit 381
16.2.2 Static DHCP Edit 382
16.3 IP/MAC Binding Exempt List 383

Chapter 17
Layer 2 Isolation 384

17.1 Overview 384
17.1.1 What You Can Do in this Chapter 384
17.2 Layer-2 Isolation General Screen 384
17.3 White List Screen 385
17.3.1 Add/Edit White List Rule 386

Chapter 18
DNS Inbound LB 388

18.1 DNS Inbound Load Balancing Overview 388
18.1.1 What You Can Do in this Chapter 388
18.2 The DNS Inbound LB Screen 389
18.2.1 The DNS Inbound LB Add/Edit Screen 390
18.2.2 The DNS Inbound LB Add/Edit Member Screen 392

Chapter 19
IPnP 394

19.1 IPnP Overview 394
19.1.1 What You Can Do in this Chapter 394
19.2 IPnP Screen 395

Chapter 20
IPSec VPN 396

20.1 Virtual Private Networks (VPN) Overview 396

20.1.1 What You Can Do in this Chapter 398
20.1.2 What You Need to Know 398
20.1.3 Before You Begin 401
20.2 The VPN Connection Screen 401
20.2.1 The VPN Connection Add/Edit Screen 403
20.3 The VPN Gateway Screen 410
20.3.1 The VPN Gateway Add/Edit Screen 411
20.4 VPN Concentrator 418
20.4.1 VPN Concentrator Requirements and Suggestions 418
20.4.2 VPN Concentrator Screen 419
20.4.3 The VPN Concentrator Add/Edit Screen 419
20.5 Zyxel Device IPSec VPN Client Configuration Provisioning 420
20.6 IPSec VPN Background Information 422

Chapter 21
SSL VPN 432

21.1 Overview 432
21.1.1 What You Can Do in this Chapter 432
21.1.2 What You Need to Know 432
21.2 The SSL Access Privilege Screen 433
21.2.1 The SSL Access Privilege Policy Add/Edit Screen 434
21.3 The SSL Global Setting Screen 436

Chapter 22
L2TP VPN 438

22.1 Overview 438
22.1.1 What You Can Do in this Chapter 438
22.1.2 What You Need to Know 438
22.2 L2TP VPN Screen 439
22.2.1 Example: L2TP and Zyxel Device Behind a NAT Router 441

Chapter 23
BWM (Bandwidth Management) 444

23.1 Overview 444
23.1.1 What You Can Do in this Chapter 444
23.1.2 What You Need to Know 444
23.2 The Bandwidth Management Configuration 448
23.2.1 The Bandwidth Management Add/Edit Screen 451

Chapter 24
Web Authentication 460

24.1 Web Auth Overview 460
24.1.1 What You Can Do in this Chapter 460

24.1.2 What You Need to Know 461
24.2 Web Authentication General Screen 461
24.2.1 User-aware Access Control Example 466
24.2.2 Authentication Type Screen 472
24.2.3 Custom Web Portal / User Agreement File Screen 476
24.3 SSO Overview 477
24.4 SSO - Zyxel Device Configuration 479
24.4.1 Configuration Overview 479
24.4.2 Configure the Zyxel Device to Communicate with SSO 479
24.4.3 Enable Web Authentication 480
24.4.4 Create a Security Policy 482
24.4.5 Configure User Information 483
24.4.6 Configure an Authentication Method 484
24.4.7 Configure Active Directory 485
24.5 SSO Agent Configuration 486

Chapter 25
Security Policy 489

25.1 Overview 489
25.2 One Security 490
25.3 What You Can Do in this Chapter 493
25.3.1 What You Need to Know 493
25.4 The Security Policy Screen 495
25.4.1 Configuring the Security Policy Control Screen 496
25.4.2 The Security Policy Control Add/Edit Screen 500
25.5 Anomaly Detection and Prevention Overview 501
25.5.1 The Anomaly Detection and Prevention General Screen 502
25.5.2 Creating New ADP Profiles 503
25.5.3 Traffic Anomaly Profiles 504
25.5.4 Protocol Anomaly Profiles 507
25.6 The Session Control Screen 510
25.6.1 The Session Control Add/Edit Screen 511
25.7 Security Policy Example Applications 512

Chapter 26
Application Patrol 515

26.1 Overview 515
26.1.1 What You Can Do in this Chapter 515
26.1.2 What You Need to Know 515
26.2 Application Patrol Profile 516
26.2.1 Apply to a Security Policy 517
26.2.2 The Application Patrol Profile Add/Edit Screen - My Application 520
26.2.3 The Application Patrol Profile Add/Edit Screen - Query Result 521

Chapter 27
Content Filter 524

27.1 Overview 524
27.1.1 What You Can Do in this Chapter 524
27.1.2 What You Need to Know 524
27.1.3 Before You Begin 526
27.2 Content Filter Profile Screen 526
27.2.1 Apply to a Security Policy 527
27.2.2 Content Filter Add Profile Category Service 530
27.2.3 Content Filter Add Filter Profile Custom Service 536
27.3 Content Filter Trusted Web Sites Screen 539
27.4 Content Filter Forbidden Web Sites Screen 540
27.5 Content Filter Technical Reference 541

Chapter 28
Anti-Malware 543

28.1 Overview 543
28.1.1 What You Can Do in this Chapter 547
28.2 Anti-Malware Screen 548
28.3 The Black List Screen 551
28.4 The White List Screen 552
28.5 Anti-Malware Signature Searching 553
28.6 Anti-Malware Technical Reference 554

Chapter 29
Reputation Filter 556

29.1 Overview 556
29.1.1 What You Need to Know 556
29.1.2 What You Can Do in this Chapter 556
29.2 IP Reputation Screen 556
29.2.1 IP Reputation White List Screen 559
29.2.2 IP Reputation Black List Screen 560
29.3 Botnet Filter Screen 561
29.3.1 Botnet Filter White List Screen 564
29.3.2 Botnet Filter Black List Screen 565

Chapter 30
IDP 566

30.1 Overview 566
30.1.1 What You Can Do in this Chapter 566
30.1.2 What You Need To Know 566
30.1.3 Before You Begin 566
30.2 The IDP Screen 566

30.2.1 Query Example 571
30.3 IDP Custom Signatures 572
30.3.1 Add / Edit Custom Signatures 573
30.3.2 Custom Signature Example 577
30.3.3 Applying Custom Signatures 579
30.3.4 Verifying Custom Signatures 580
30.4 The White List Screen 580
30.5 IDP Technical Reference 581

Chapter 31
Sandboxing 584

31.1 Overview 584
31.1.1 What You Need to Know 585
31.2 Sandboxing Screen 585

Chapter 32
Email Security 588

32.1 Overview 588
32.1.1 What You Can Do in this Chapter 588
32.1.2 What You Need to Know 588
32.2 Before You Begin 589
32.3 The Email Security Screen 590
32.4 The Black List / White List Screen 593
32.4.1 The Black or White List Add/Edit Screen 594
32.4.2 Regular Expressions in Black or White List Entries 595
32.5 Email Security Technical Reference 595

Chapter 33
SSL Inspection 599

33.1 Overview 599
33.1.1 What You Can Do in this Chapter 599
33.1.2 What You Need To Know 599
33.1.3 Before You Begin 600
33.2 The SSL Inspection Profile Screen 600
33.2.1 Apply to a Security Policy 601
33.2.2 Add / Edit SSL Inspection Profiles 604
33.3 Exclude List Screen 605
33.4 Certificate Update Screen 607
33.5 Install a CA Certificate in a Browser 608

Chapter 34
IP Exception 611

34.1 Overview 611

34.2 The IP Exception Screen 611
34.2.1 The IP Exception Add/Edit Screen 612

Chapter 35
Object 614

35.1 Zones Overview 614
35.1.1 What You Need to Know 614
35.1.2 The Zone Screen 615
35.2 User/Group Overview 617
35.2.1 What You Need To Know 617
35.2.2 User/Group User Summary Screen 619
35.2.3 User/Group Group Summary Screen 624
35.2.4 User/Group Setting Screen 625
35.2.5 User/Group MAC Address Summary Screen 630
35.2.6 User /Group Technical Reference 632
35.3 AP Profile Overview 632
35.3.1 Radio Screen 633
35.3.2 SSID Screen 639
35.4 MON Profile 648
35.4.1 Overview 648
35.4.2 Configuring MON Profile 649
35.4.3 Add/Edit MON Profile 650
35.4.4 Technical Reference 651
35.5 ZyMesh Overview 652
35.5.1 ZyMesh Profile 654
35.5.2 Add/Edit ZyMesh Profile 655
35.6 Address/Geo IP Overview 655
35.6.1 What You Need To Know 656
35.6.2 Address Summary Screen 656
35.6.3 Address Group Summary Screen 660
35.6.4 Geo IP Summary Screen 662
35.7 Service Overview 665
35.7.1 What You Need to Know 665
35.7.2 The Service Summary Screen 666
35.7.3 The Service Group Summary Screen 668
35.8 Schedule Overview 670
35.8.1 What You Need to Know 670
35.8.2 The Schedule Screen 670
35.8.3 The Schedule Group Screen 673
35.9 AAA Server Overview 675
35.9.1 Directory Service (AD/LDAP) 676
35.9.2 RADIUS Server 676
35.9.3 ASAS 676

35.9.4 What You Need To Know 677
35.9.5 Active Directory or LDAP Server Summary 678
35.9.6 RADIUS Server Summary 682
35.10 Auth. Method Overview 685
35.10.1 Before You Begin 685
35.10.2 Example: Selecting a VPN Authentication Method 685
35.10.3 Authentication Method Objects 686
35.10.4 Two-Factor Authentication VPN Access 688
35.10.5 Two-Factor Authentication Admin Access 691
35.11 Certificate Overview 693
35.11.1 What You Need to Know 693
35.11.2 Verifying a Certificate 695
35.11.3 The My Certificates Screen 696
35.11.4 The Trusted Certificates Screen 705
35.11.5 Certificates Technical Reference 710
35.12 ISP Account Overview 710
35.12.1 ISP Account Summary 710
35.13 DHCPv6 Overview 713
35.13.1 The DHCPv6 Request Screen 713
35.13.2 The DHCPv6 Lease Screen 715

Chapter 36
Device HA 717

36.1 Device HA Overview 717
36.1.1 What You Can Do in These Screens 717
36.2 Device HA Status 717
36.3 Device HA Pro 719
36.3.1 Deploying Device HA Pro 720
36.3.2 Configuring Device HA Pro 720
36.4 View Log 722

Chapter 37
Cloud CNM 724

37.1 Cloud CNM Overview 724
37.1.1 What You Can Do in this Chapter 724
37.2 Cloud CNM SecuManager 724
37.3 Cloud CNM SecuReporter 727

Chapter 38
System 732

38.1 Overview 732
38.1.1 What You Can Do in this Chapter 732
38.2 Host Name 733

38.3 USB Storage 733
38.4 Date and Time 734
38.4.1 Pre-defined NTP Time Servers List 737
38.4.2 Time Server Synchronization 737
38.5 Console Port Speed 738
38.6 DNS Overview 739
38.6.1 DNS Server Address Assignment 739
38.6.2 Configuring the DNS Screen 739
38.6.3 (IPv6) Address Record 743
38.6.4 PTR Record 743
38.6.5 Adding an (IPv6) Address/PTR Record 743
38.6.6 CNAME Record 744
38.6.7 Adding a CNAME Record 744
38.6.8 Domain Zone Forwarder 745
38.6.9 Adding a Domain Zone Forwarder 745
38.6.10 MX Record 746
38.6.11 Adding a MX Record 746
38.6.12 Security Option Control 747
38.6.13 Editing a Security Option Control 747
38.6.14 Adding a DNS Service Control Rule 748
38.7 WWW Overview 749
38.7.1 Service Access Limitations 749
38.7.2 System Timeout 749
38.7.3 HTTPS 749
38.7.4 Configuring WWW Service Control 750
38.7.5 Service Control Rules 753
38.7.6 Customizing the WWW Login Page 754
38.7.7 HTTPS Example 759
38.8 SSH 766
38.8.1 How SSH Works 767
38.8.2 SSH Implementation on the Zyxel Device 768
38.8.3 Requirements for Using SSH 768
38.8.4 Configuring SSH 768
38.8.5 Service Control Rules 769
38.8.6 Secure Telnet Using SSH Examples 770
38.9 Telnet 771
38.9.1 Configuring Telnet 771
38.9.2 Service Control Rules 773
38.10 FTP 773
38.10.1 Configuring FTP 773
38.10.2 Service Control Rules 775
38.11 SNMP 775
38.11.1 SNMPv3 and Security 776

38.11.2 Supported MIBs 777
38.11.3 SNMP Traps 777
38.11.4 Configuring SNMP 777
38.11.5 Add SNMPv3 User 780
38.11.6 Service Control Rules 780
38.12 Authentication Server 781
38.12.1 Add/Edit Trusted RADIUS Client 783
38.13 Notification > Mail Server 783
38.14 Notification > SMS 785
38.15 Language Screen 786
38.16 IPv6 Screen 787
38.17 Zyxel One Network (ZON) Utility 787
38.17.1 Requirements 788
38.17.2 Run the ZON Utility 788
38.17.3 Zyxel One Network (ZON) System Screen 792

Chapter 39
Log and Report 793

39.1 Overview 793
39.1.1 What You Can Do In this Chapter 793
39.2 Email Daily Report 793
39.3 Log Setting Screens 795
39.3.1 Log Setting Summary 795
39.3.2 Edit System Log Settings 796
39.3.3 Edit Log on USB Storage Setting 800
39.3.4 Edit Remote Server Log Settings 801
39.3.5 Log Category Settings Screen 803

Chapter 40
File Manager 806

40.1 Overview 806
40.1.1 What You Can Do in this Chapter 806
40.1.2 What you Need to Know 806
40.2 The Configuration File Screen 808
40.3 Firmware Management 812
40.3.1 Cloud Helper 812
40.3.2 The Firmware Management Screen 815
40.3.3 Firmware Upgrade via USB Stick 818
40.4 The Shell Script Screen 818

Chapter 41
Diagnostics 821

41.1 Overview 821

41.1.1 What You Can Do in this Chapter 821
41.2 The Diagnostics Screens 821
41.2.1 The Diagnostics Collect Screen 822
41.2.2 The Diagnostics Collect on AP Screen 823
41.2.3 The Diagnostics Files Screen 824
41.3 The Packet Capture Screen 825
41.3.1 The Packet Capture on AP Screen 828
41.3.2 The Packet Capture Files Screen 831
41.4 The CPU / Memory Status Screen 832
41.5 The System Log Screen 834
41.6 The Remote Assistance Screen 834
41.7 The Network Tool Screen 836
41.8 The Routing Traces Screen 838
41.9 The Wireless Frame Capture Screen 839
41.9.1 The Wireless Frame Capture Files Screen 841

Chapter 42
Packet Flow Explore 842

42.1 Overview 842
42.1.1 What You Can Do in this Chapter 842
42.2 The Routing Status Screen 842
42.3 The SNAT Status Screen 846

Chapter 43
Shutdown 849

43.1 Overview 849
43.1.1 What You Need To Know 849
43.2 The Shutdown Screen 849

Part III: Appendices and Troubleshooting 850

Chapter 44
Troubleshooting 851

44.1 Resetting the Zyxel Device 864
44.2 Getting More Troubleshooting Help 865

Appendix A Customer Support 866

Appendix B Product Features 872

Appendix C Legal Information 875

Index 883

PART I
User's Guide

CHAPTER 1
Introduction

1.1 Overview

Zyxel Device refers to these models as outlined below.

- ATP100
- ATP100W
- ATP200
- ATP500
- ATP700
- ATP800

Most screen shots in this guide come from the ATP200.

Note the following differences between the device models:

- ATP500 and ATP800 support Device HA Pro.
- Some interface names vary by model - see Table 14 on page 73 and Table 15 on page 73 for default port / interface name mapping. See Table 17 on page 73 for default interface / zone mapping.

See the product's datasheet for detailed information on a specific model.

1.2 Registration at myZyxel

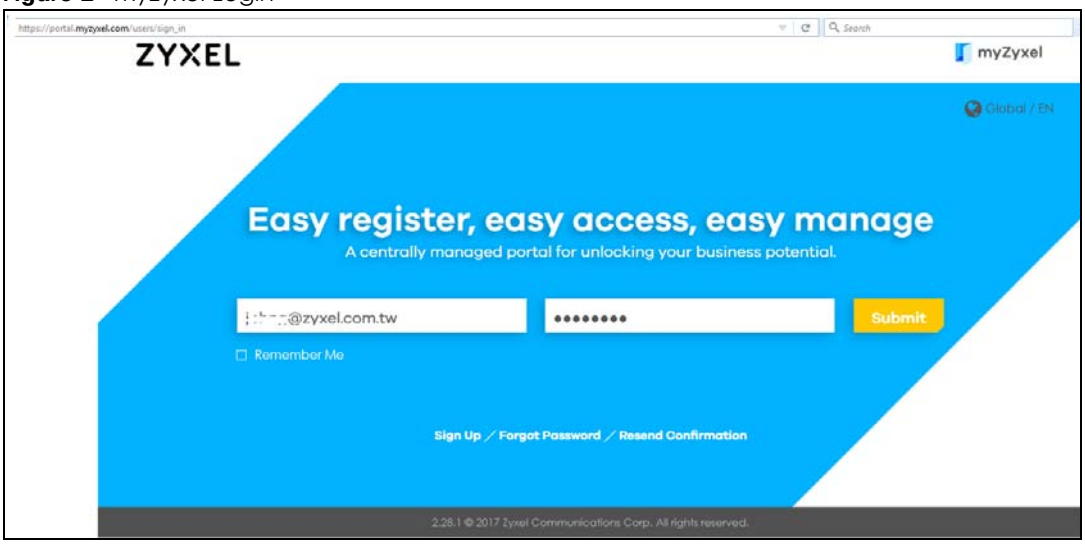
myZyxel is Zyxel's online services center where you can register your Zyxel Device and manage subscription services available for your Zyxel Device (see **Configuration > Licensing > Registration > Service** for services available for your Zyxel Device).

- For Zyxel Devices that already have firmware version 4.25 or later, you have to register your Zyxel Device and activate the corresponding service at myZyxel (through your Zyxel Device).
- For Zyxel Devices upgrading to firmware version 4.25 or later, you may skip registering your Zyxel Device and activating the corresponding service at myZyxel (through your Zyxel Device). However, it is highly recommended to at least register your Zyxel Device. At the time of writing, the Firmware Upgrade license providing Cloud Helper new firmware notifications, is free when you register your Zyxel Device.

Note: You need to create a myZyxel account at *http://portal.myZyxel.com* before you can register your device and activate the services at myZyxel.

You may need your Zyxel Device's serial number and LAN MAC address to register it at myZyxel. See the label at the back of the Zyxel Device's for details.

Figure 1 myZyxel Login



1.2.1 Grace Period

SecuReporter and service licenses have a 15-day grace period after a license expires. Services will continue to work in this period during which you will receive notifications to renew your license(s). New license(s) are valid for 1 year from the date of purchase.

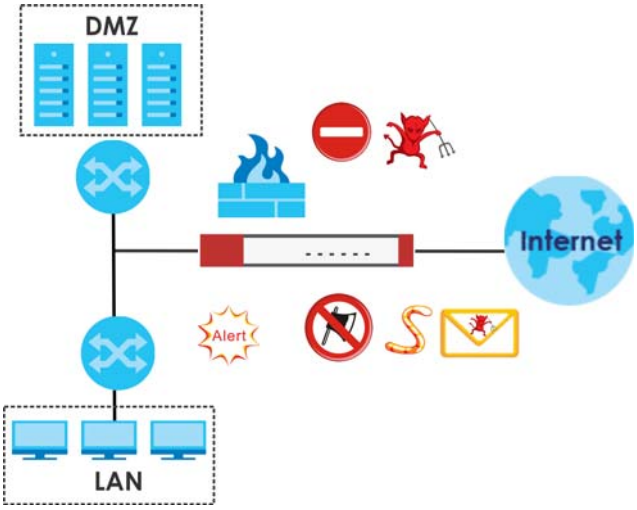
1.2.2 Applications

These are some Zyxel Device application scenarios.

Security Router

Security includes a Stateful Packet Inspection (SPI) firewall.

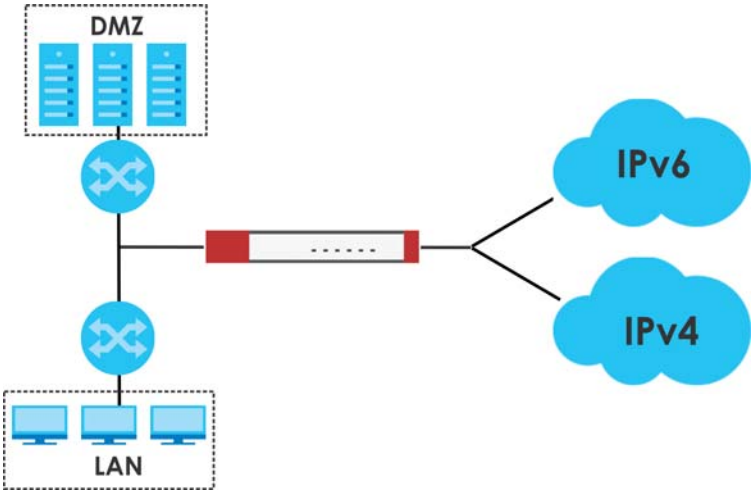
Figure 2 Applications: Security Router Applications: Security Router



IPv6 Routing

The Zyxel Device supports IPv6 Ethernet, PPP, VLAN, and bridge routing. You may also create IPv6 policy routes and IPv6 objects. The Zyxel Device can also route IPv6 packets through IPv4 networks using different tunneling methods.

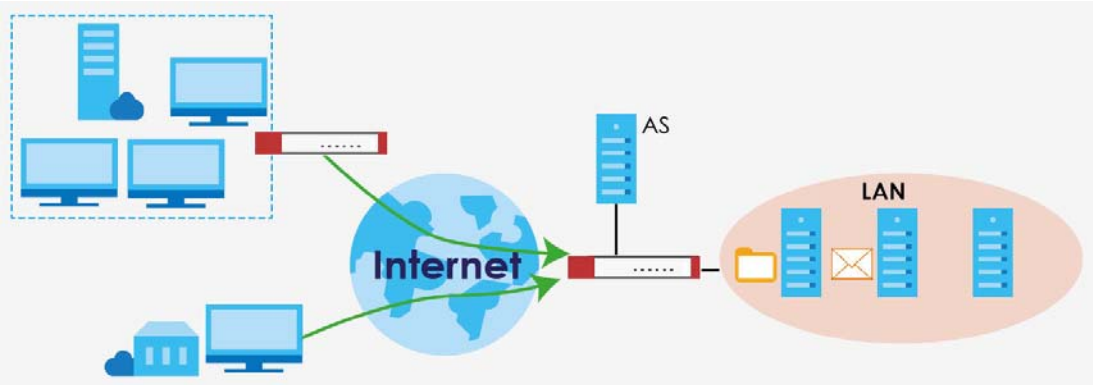
Figure 3 Applications: IPv6 Routing



VPN Connectivity

Set up VPN tunnels with other companies, branch offices, telecommuters, and business travelers to provide secure access to your network. AS is an Authentication Server in the below figure.

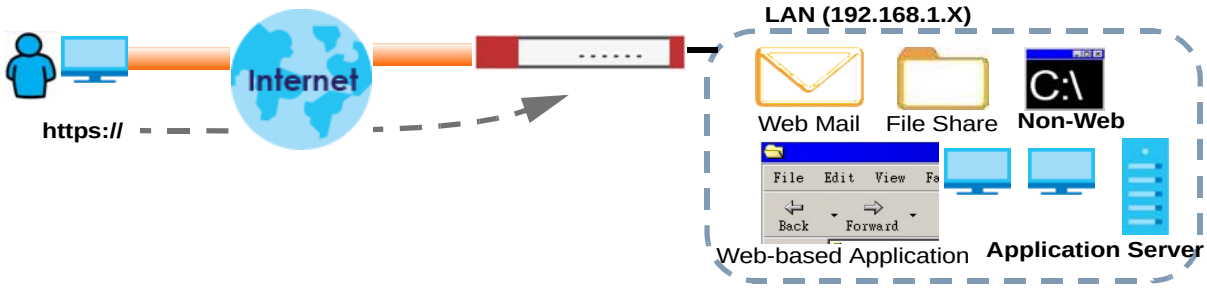
Figure 4 Applications: VPN Connectivity



SSL VPN Network Access

SSL VPN lets remote users use their web browsers for a very easy-to-use VPN solution. A user just browses to the Zyxel Device's web address and enters his user name and password to securely connect to the Zyxel Device's network. Here full tunnel mode creates a virtual connection for a remote user and gives him a private IP address in the same subnet as the local network so he can access network resources in the same way as if he were part of the internal network.

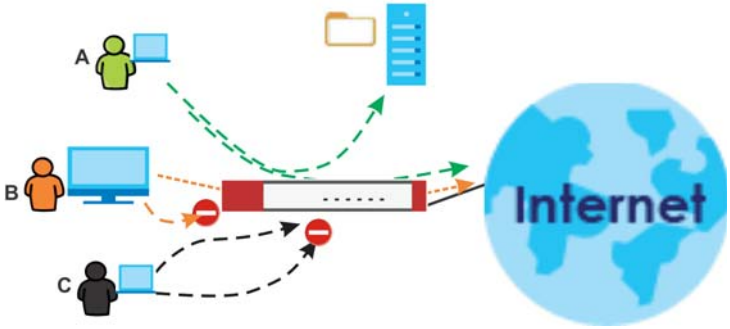
Figure 5 SSL VPN With Full Tunnel Mode



User-Aware Access Control

Set up security policies to restrict access to sensitive information and shared resources based on the user who is trying to access it. In the following figure user **A** can access both the Internet and an internal file server. User **B** has a lower level of access and can only access the Internet. User **C** is not even logged in, so and cannot access either the Internet or the file server.

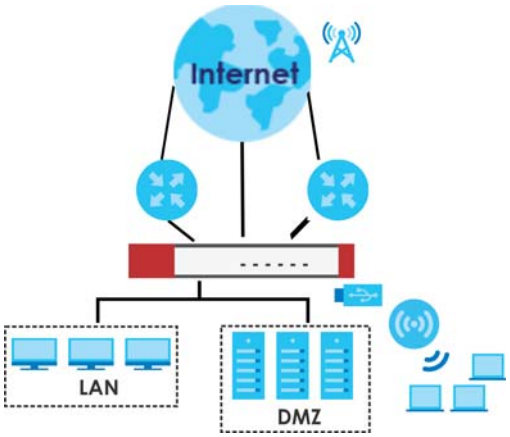
Figure 6 Applications: User-Aware Access Control



Load Balancing

Set up multiple connections to the Internet on the same port, or different ports, including cellular interfaces. In either case, you can balance the traffic loads between them.

Figure 7 Applications: Multiple WAN Interfaces



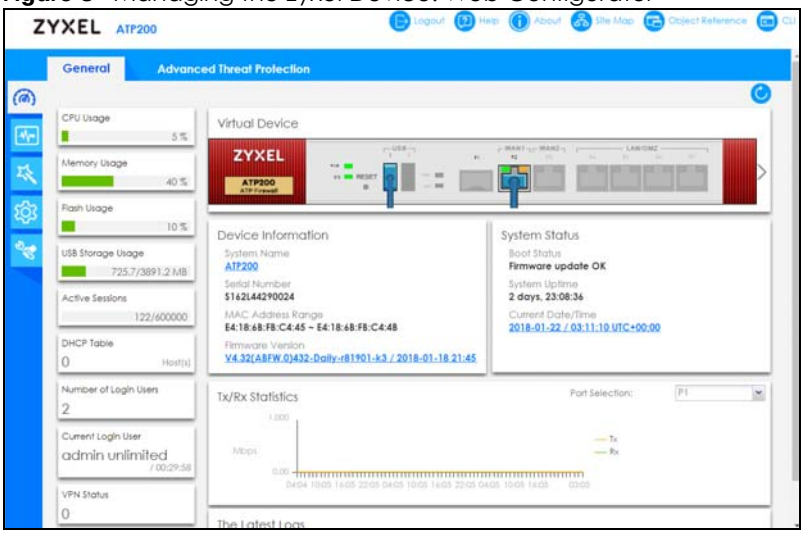
1.3 Management Overview

You can manage the Zyxel Device in the following ways.

Web Configurator

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

Figure 8 Managing the Zyxel Device: Web Configurator



Command-Line Interface (CLI)

The CLI allows you to use text-based commands to configure the Zyxel Device. 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 1 Console Port Default Settings

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

FTP

Use File Transfer Protocol for firmware upgrades and configuration backup/restore.

SNMP

The device can be monitored and/or managed by an SNMP manager. See Section 38.11 on page 775.

CloudCNM

Use the **CloudCNM** screen (see Section 38.15 on page 786) to enable and configure management of the Zyxel Device by a Central Network Management system.

Management Authentication

Managers must be authenticated with a username and password, using one of:

- Local Zyxel Device authentication
- An external RADIUS server
- An external LDAP server
- Certificates

1.4 Web Configurator

In order to use the Web Configurator, you must:

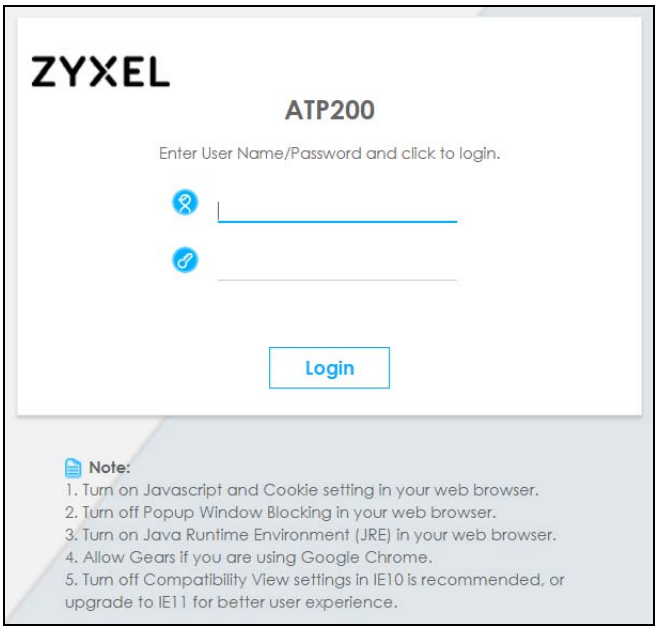
- Use one of the following web browser versions or later:
  - Internet Explorer 10.x, 11.x
  - Chrome latest version (45 or above)
  - Firefox latest version (45 or above)
  - Safari latest version (9.0 or above)
- Allow pop-up windows (blocked by default in some browsers)
- Enable JavaScripts, Java permissions, and cookies

The recommended screen resolution is 1024 x 768 pixels.

Note: Screenshots and graphics in this book may differ slightly from your product due to differences in product features or web configurator brand style. Most screen shots in this guide come from the USG110 and USG60W.

1.4.1 Web Configurator Access

1. Make sure your Zyxel Device hardware is properly connected. See the Quick Start Guide.
2. In your browser go to http://192.168.1.1. By default, the Zyxel Device automatically routes this request to its HTTPS server, and it is recommended to keep this setting. The **Login** screen appears.

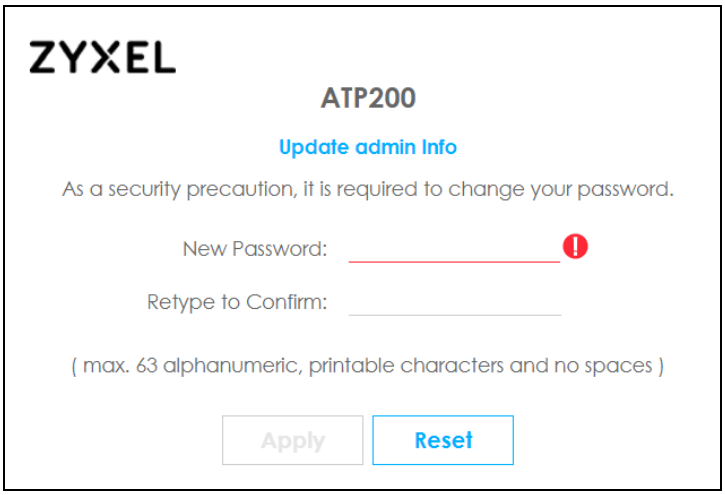


3 Type the user name (default: "admin") and password (default: "1234").

4 Click **Login**. After you log in for the first time using the default user name and password, you must change the default admin password in the **Update Admin Info** screen. Enter a new password of from 1 to 64 characters.

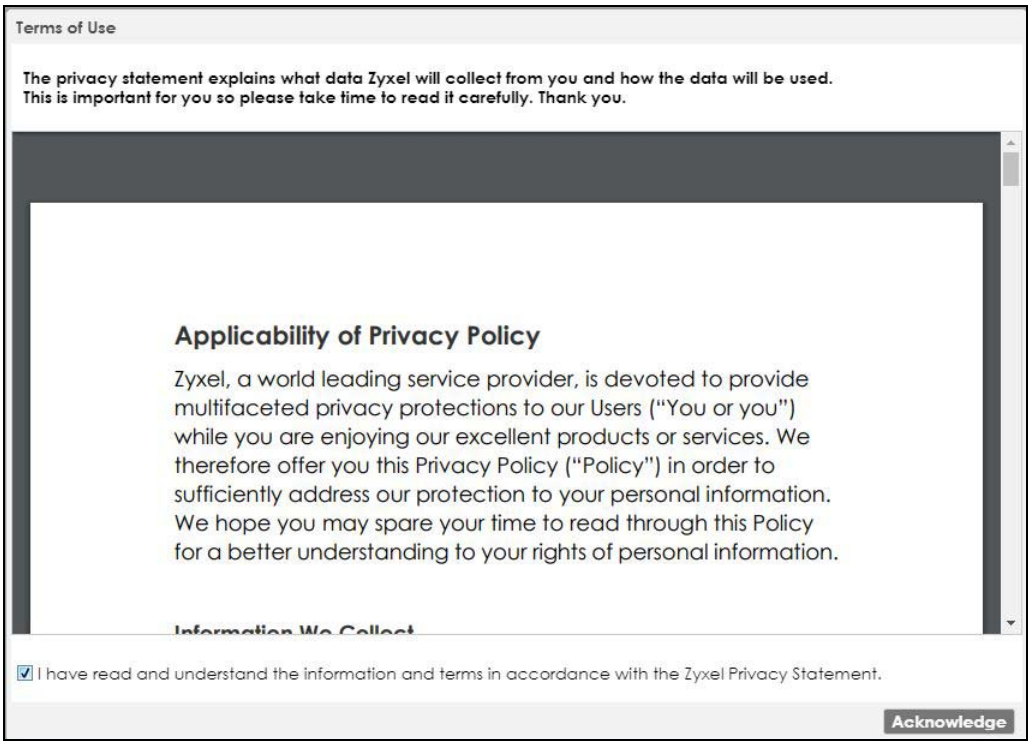
In **Configuration > Object > User/Group > Setting**, you can enable **Password Complexity** to require a new password to consist of at least 8 characters and at most 64, where at least 1 character must be a number, at least 1 a lower case letter, at least 1 an upper case letter and at least 1 a special character from the keyboard, such as !@#$%^&*()_+. You can also require periodic changing of the password in that screen by configuring **Password must changed every (days)**.

Make a note of your new password, enter it in the following screen, then click **Apply**.

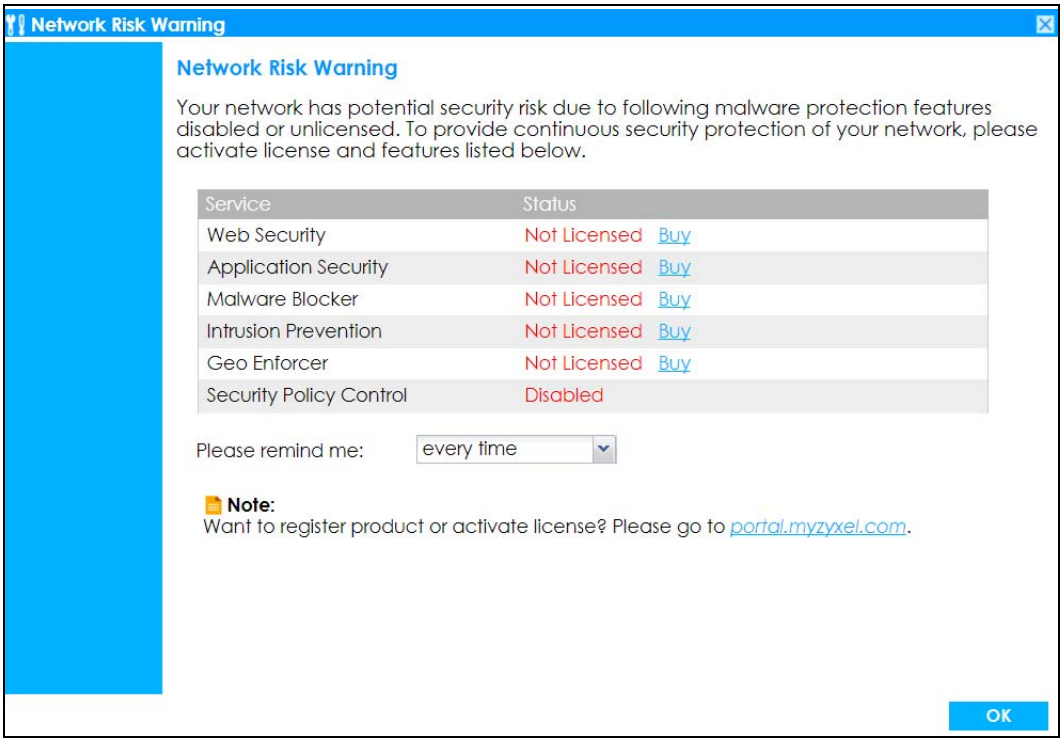


5 A **Terms of Use** screen displays. Read the statement, then click **Acknowledge** to proceed.

Note: If you are using an Internet Explorer browser, the **Terms of Use** will be downloaded automatically.



6 The **Network Risk Warning** screen displays any unregistered or disabled security services. If your Zyxel Device is not registered, you will see a prompt to register it. Select how often to display the screen and click **OK**.



If you select **Never** and you later want to bring this screen back, use these commands (note the space before the underscore).

```
Router> enable
Router#
Router# configure terminal
Router(config)#
Router(config)# service-register _setremind
after-10-days
after-180-days
after-30-days
every-time
never
Router(config)# service-register _setremind every-time
Router(config)#
```

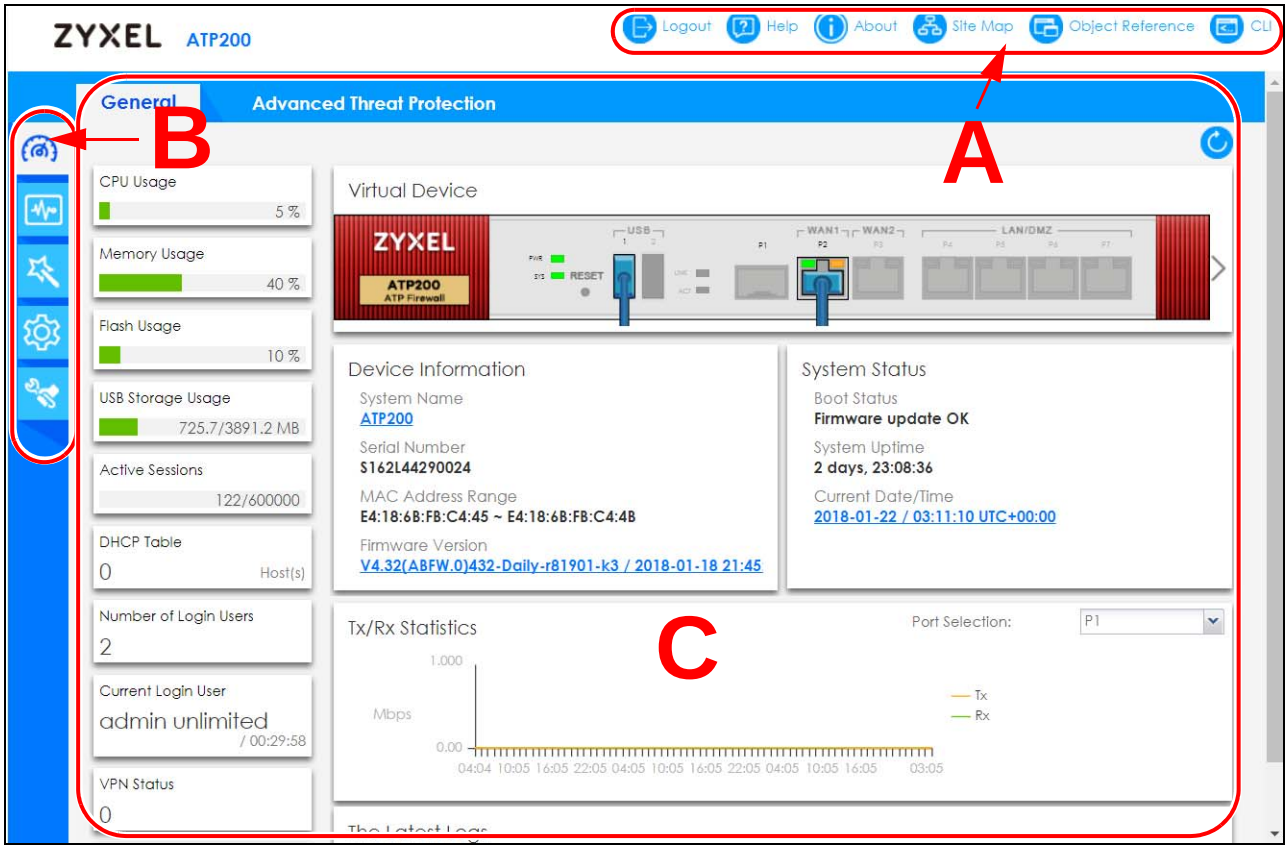
See the Command Line Interface (CLI) Reference Guide (RG) for details on all supported commands.

7 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 ZyWALL is using its default configuration; otherwise the dashboard appears.

1.4.2 Web Configurator Screens Overview

The Web Configurator screen is divided into these parts:

- **A** - title bar
- **B** - navigation panel
- **C** - main window



Title Bar

Figure 9 Title Bar

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

Table 2 Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
SecuReporter	Click this to open the SecuReporter portal page. This icon shows when the Zyxel Device is added to an organization.
Web Console	Click this to open one or multiple console windows 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. Logging in to the Zyxel Device with HTTPS, so you can open one or multiple console windows.
CLI	Click this to open a popup window that displays the CLI commands sent by the Web Configurator to the Zyxel Device.
Reference	Click this to check which configuration items reference an object.
Site Map	Click this to see an overview of links to the Web Configurator screens.
Forum	Go to https://businessforum.zyxel.com for product discussions.
Help	Click this to open the help page for the current screen.

Table 2 Title Bar: Web Configurator Icons (continued)

LABEL	DESCRIPTION
About	Click this to display basic information about the Zyxel Device.
Logout	Click this to log out of the Web Configurator.

About

Click **About** to display basic information about the Zyxel Device.

Figure 10 About

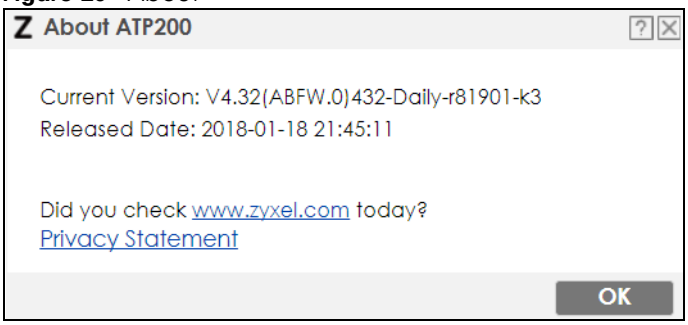


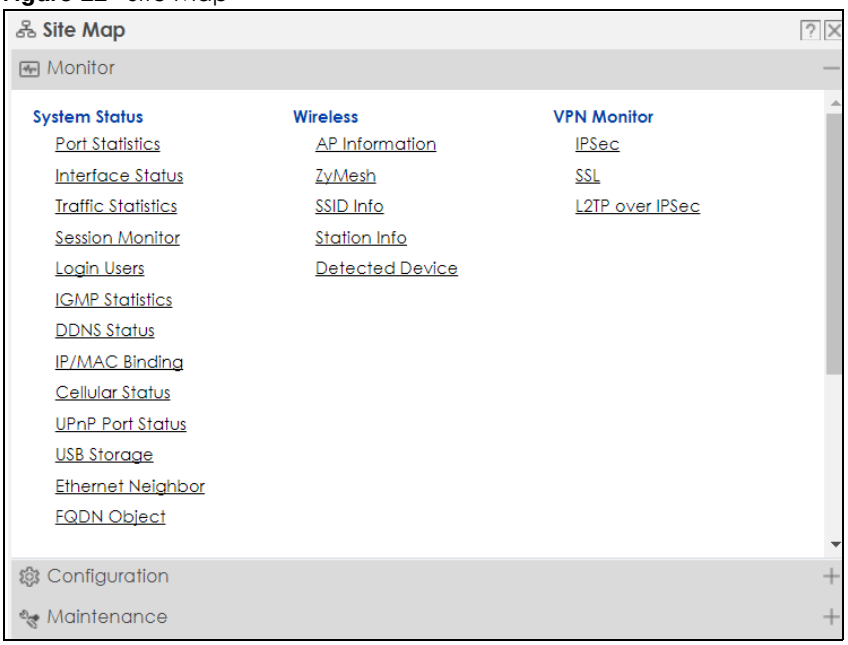
Table 3 About

LABEL	DESCRIPTION
Current Version	This shows the firmware version of the Zyxel Device.
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.

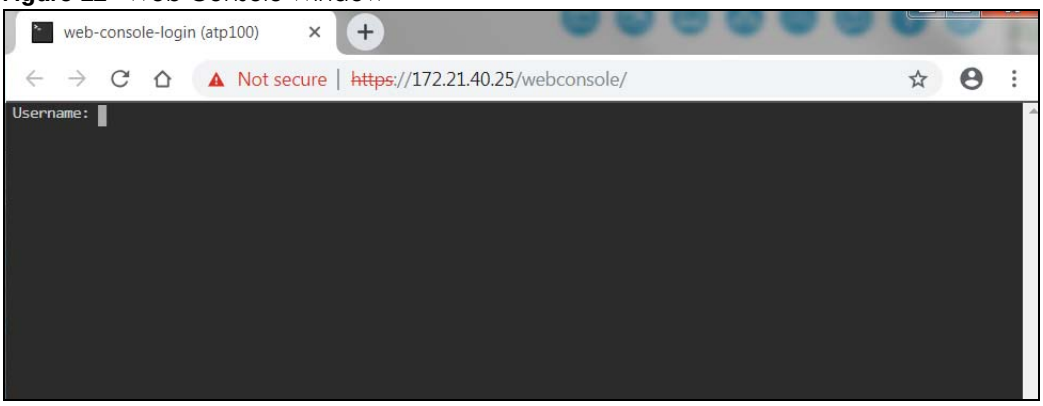
Figure 11 Site Map



Web Console

Click **Web Console** to open one or multiple console windows from which you can run CLI commands. You will be prompted to enter your user name and password. See the Command Reference Guide for information about the commands. Logging in to the Zyxel Device with HTTPS, so you can open one or multiple console windows.

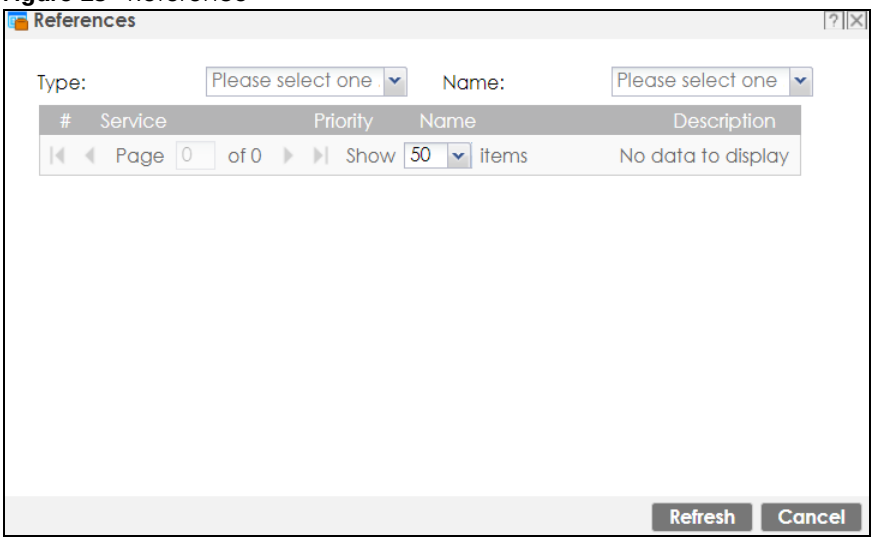
Figure 12 Web Console Window



Reference

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

Figure 13 Reference



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

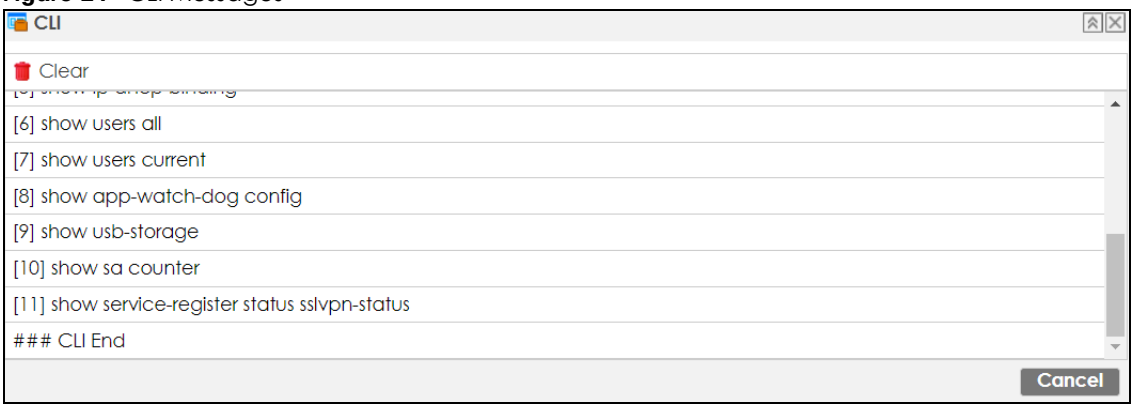
Table 4 Reference

LABEL	DESCRIPTION
Type	Select an object type to see the services.
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.

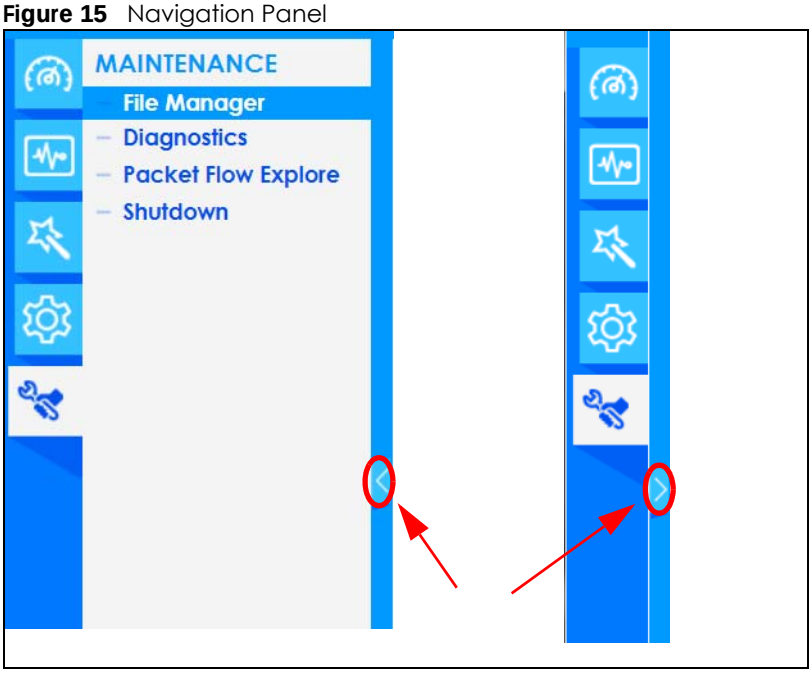
Figure 14 CLI Messages



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 Zyxel Device's navigation panel menus and their screens.

Figure 15 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 the Web Help for details on the dashboard.

Monitor Menu

The monitor menu screens display status and statistics information.

Table 5 Monitor Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
System Status		
Port Statistics	Port Statistics	Displays packet statistics for each physical port.
Interface Status	Interface Summary	Displays general interface information and packet statistics.
Traffic Statistics	Traffic Statistics	Collect and display traffic statistics.
Session Monitor	Session Monitor	Displays the status of all current sessions.
Login Users	Login Users	Lists the users currently logged into the Zyxel Device.
IGMP Statistics	IGMP Statistics	Collect and display IGMP statistics.
DDNS Status	DDNS Status	Displays the status of the Zyxel Device's DDNS domain names.
IP/MAC Binding	IP/MAC Binding	Lists the devices that have received an IP address from Zyxel Device interfaces using IP/MAC binding.
Cellular Status	Cellular Status	Displays details about the Zyxel Device's mobile broadband connection status.
UPnP Port Status	Port Statistics	Displays details about UPnP connections going through the Zyxel Device.
USB Storage	Storage Information	Displays details about USB device connected to the Zyxel Device.
Ethernet Neighbor	Ethernet Neighbor	View and manage the Zyxel Device's neighboring devices via Smart Connect (Layer Link Discovery Protocol (LLDP)). Use the Zyxel One Network (ZON) utility to view and manage the Zyxel Device's neighboring devices via the Zyxel Discovery Protocol (ZDP).
FQDN Object	FQDN Object	Displays FQDN (Fully Qualified Domain Name) object cache lists used in DNS queries.
Wireless		
AP Information	AP List	Lists APs managed by the Zyxel Device.
	Radio List	Lists wireless details of APs managed by the Zyxel Device.
	Top N APs	Lists managed APs with the most wireless traffic usage and most associated wireless stations.
	Single AP	Lists APs wireless traffic usage and associated wireless stations for a managed AP.
ZyMesh	ZyMesh Link Info	Display statistics about ZyMesh wireless connections between managed APs.
SSID Info	SSID Info	Display information about the SSID's wireless clients.
Station Info	Station List	Lists wireless clients associated with the APs managed by the Zyxel Device.
	Top N Stations	Lists wireless stations with the most wireless traffic usage.
	Single Station	Lists wireless traffic usage for an associated wireless station.
Detected Device	Detected Device	Display information about suspected rogue APs.
VPN Monitor		
IPSec	IPSec	Displays and manages the active IPSec SAs.

Table 5 Monitor Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
SSL	SSL	Lists users currently logged into the VPN SSL client portal. You can also log out individual users and delete related session information.
L2TP over IPSec	L2TP over IPSec	Displays details about current L2TP sessions.
Security Statistics		
Content Filter	Summary	Collect and display content filter statistics
App Patrol	Summary	Displays application patrol statistics.
Anti-Malware	Summary	Collect and display statistics on the malware that the Zyxel Device has detected.
IDP	Summary	Collect and display statistics on the intrusions that the Zyxel Device has detected.
Email Security	Summary	Collect and display spam statistics.
	Status	Displays how many mail sessions the ZyWALL is currently checking and DNSBL (Domain Name Service-based spam Black List) statistics.
Botnet Filter	Summary	Displays the IP addresses and URLs that are blocked by the Zyxel Device.
Sandboxing	Summary	Displays the sandboxing statistics.
SSL Inspection	Report	Collect and display SSL Inspection statistics.
	Certificate Cache List	Displays traffic to destination servers using certificates.
Log	View Log	Lists log entries.
	View AP Log	Lists AP log entries.

Configuration Menu

Use the configuration menu screens to configure the Zyxel Device's features.

Table 6 Configuration Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
Quick Setup		Quickly configure WAN interfaces or VPN connections.
Licensing		
Registration	Registration	Register the device and activate trial services.
	Service	View the licensed service status and upgrade licensed services.
Signature Update	Signature	Update signatures immediately or by a schedule.
Wireless		
Controller	Configuration	Configure manual or automatic controller registration.
AP Management	Mgnt AP List	Edit or remove entries in the lists of APs managed by the Zyxel Device.
	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 Zyxel Device.
Rogue AP	Rogue/Friendly AP List	Configure how the Zyxel Device monitors rogue APs.

Table 6 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
Auto Healing	Auto Healing	Enable auto healing to extend the wireless service coverage area of the managed APs when one of the APs fails.
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 Zyxel Device's flexible ports such as LAN, OPT, WLAN, or DMZ.
	Ethernet	Manage Ethernet interfaces and virtual Ethernet interfaces.
	PPP	Create and manage PPPoE and PPTP interfaces.
	Cellular	Configure a cellular Internet connection for an installed mobile broadband card.
	Tunnel	Configure tunneling between IPv4 and IPv6 networks.
	VLAN	Create and manage VLAN interfaces and virtual VLAN interfaces.
	Bridge	Create and manage bridges and virtual bridge interfaces.
	VTI	Configure IP address assignment and interface parameters for VTI (Virtual Tunnel Interface).
	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.
	RIP	Configure device-level RIP settings.
	OSPF	Configure device-level OSPF settings, including areas and virtual links.
	BGP	Configure exchange of Border Gateway Protocol (BGP) information over an IPSec tunnel.
DDNS	DDNS	Define and manage the Zyxel Device's DDNS domain names.
NAT	NAT	Set up and manage port forwarding rules.
Redirect Service	Redirect Service	Set up and manage HTTP and SMTP redirection rules.
ALG	ALG	Configure SIP, H.323, and FTP pass-through settings.
UPnP	UPnP	Configure interfaces that allow UPnP and NAT-PMP connections.
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 Zyxel Device does not apply IP/MAC binding.
Layer 2 Isolation	General	Enable layer-2 isolation on the Zyxel Device and the internal interface(s).
	White List	Enable and configure the white list.
DNS Inbound LB	DNS Load Balancing	Configure DNS Load Balancing.
IPnP	IPnP	Enable IPnP on the Zyxel Device and the internal interface(s).
VPN		
IPSec VPN	VPN Connection	Configure IPSec tunnels.
	VPN Gateway	Configure IKE tunnels.
	Concentrator	Combine IPSec VPN connections into a single secure network
	Configuration Provisioning	Set who can retrieve VPN rule settings from the Zyxel Device using the Zyxel Device IPSec VPN Client.

Table 6 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
SSL VPN	Access Privilege	Configure SSL VPN access rights for users and groups.
	Global Setting	Configure the Zyxel Device's SSL VPN settings that apply to all connections.
L2TP VPN	L2TP VPN	Configure L2TP over IPSec tunnels.
BWM	BWM	Enable and configure bandwidth management rules.
Web Authentication	Web Authentication General/ Authentication Type/Custom Web Portal File/Custom User Agreement File	Define a web portal and exempt services from authentication.
	SSO	Configure the Zyxel Device to work with a Single Sign On agent.
Security Policy		
Policy Control	Policy	Create and manage level-3 traffic rules and apply Security Service profiles.
ADP	General	Display and manage ADP bindings.
	Profile	Create and manage ADP profiles.
Session Control	Session Control	Limit the number of concurrent client NAT/security policy sessions.
Security Service		
AppPatrol	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.
Anti-Malware	Anti-Malware	Enable, specify actions to take when encountering malware or compressed files, and set up a black list to identify files with malware file patterns and a white list to identify files that should not be checked for malware.
	Signature	Search for particular signatures to get more information about them.
Reputation Filter	IP Reputation General/White List/ Black List	Enable IP reputation and specify what action the Zyxel Device takes when any IP address with bad reputation is detected. You can also set up a white list to identify which IPv4 addresses should be allowed, and a black list to identify which IPv4 addresses should be blocked.
	Botnet Filter General/White List/ Black List	Enable botnet filtering and specify what action the Zyxel Device takes when any suspicious activity is detected. You can also set up a white list to identify which IPv4 addresses and/or URLs should be allowed, and a black list to identify which IPv4 addresses and/or URLs should be blocked.
IDP	IDP	Enable and configure IDP settings. Create, import, or export custom signatures.
Sandboxing	Sandboxing	Enable sandboxing, and specify the actions the Zyxel Device takes when malicious or suspicious files are detected.
Botnet Filter	Botnet Filter	Enable botnet filtering and specify the actions.

Table 6 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
Email Security	Email Security	Turn email security on or off and manage email security policies. Create email security template(s) of settings to apply to a traffic flow using a security policy.
	Black/White List	Set up a black list to identify spam and a white list to identify legitimate email.
SSL Inspection	Profile	Decrypt HTTPS traffic for Security Service inspection. Create SSL Inspection template(s) of settings to apply to a traffic flow using a security policy.
	Exclude List	Configure services to be excluded from SSL Inspection.
	Certificate Update	Use this screen to update the latest certificates of servers using SSL connections to the Zyxel Device network.
IP Exception	IP Exception	Use this screen to view the IP exception list for the anti-malware and IDP (Intrusion, Detection, and Prevention) features. The Zyxel Device won't intercept nor inspect the incoming packets that match the rules in the IP exception list for the anti-malware and/or IDP (Intrusion, Detection, and Prevention) features.
Object		
Zone	Zone	Configure zone template(s) used to define various policies.
User/Group	User	Create and manage users.
	Group	Create and manage groups of users.
	Setting	Manage default settings for all users, general settings for user sessions, and rules to force user authentication.
	MAC Address	Configure the MAC addresses of wireless clients for MAC authentication using the local user database.
AP Profile	Radio	Create template(s) of radio settings to apply to policies as an object.
	SSID	Create template(s) of wireless settings to apply to radio profiles or policies as an object.
MON Profile	MON Profile	Create and manage rogue AP monitoring files that can be associated with different APs.
ZyMesh Profile	ZyMesh Profile	Create and manage ZyMesh files that can be associated with different APs.
Address/Geo IP	Address	Create and manage host, range, and network (subnet) addresses.
	Address Group	Create and manage groups of addresses to apply to policies as a single objects.
	Geo IP	Update the database of country-to-IP address mappings and manually configure country-to-IP address mappings for geographic address objects that can be used in security policies.
Service	Service	Create and manage TCP and UDP services.
	Service Group	Create and manage groups of services to apply to policies as a single object.
Schedule	Schedule	Create one-time and recurring schedules.
	Schedule Group	Create and manage groups of schedules to apply to policies as a single object.
AAA Server	Active Directory	Configure the Active Directory settings.
	LDAP	Configure the LDAP settings.
	RADIUS	Configure the RADIUS settings.

Table 6 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
Auth. Method	Authentication Method	Create and manage ways of authenticating users.
Certificate	My Certificates	Create and manage the Zyxel Device's certificates.
	Trusted Certificates	Import and manage certificates from trusted sources.
DHCPv6	Request	Configure IPv6 DHCP request type and interface information.
	Lease	Configure IPv6 DHCP lease type and interface information.
Cloud CNM	SecuManager	Enable and configure management of the Zyxel Device by a Central Network Management system.
	SecuReporter	Enable SecuReporter logging and access the SecuReporter security analytics portal that collects and analyzes logs from your Zyxel Device in order to identify anomalies, alert on potential internal / external threats, and report on network usage.
System		
Host Name	Host Name	Configure the system and domain name for the Zyxel Device.
USB Storage	Settings	Configure the settings for the connected USB devices.
Date/Time	Date/Time	Configure the current date, time, and time zone in the Zyxel Device.
Console Speed	Console Speed	Set the console speed.
DNS	DNS	Configure the DNS server and address records for the Zyxel Device.
WWW	Service Control	Configure HTTP, HTTPS, and general authentication.
	Login Page	Configure how the login and access user screens look.
SSH	SSH	Configure SSH server and SSH service settings.
TELNET	TELNET	Configure telnet server settings for the Zyxel Device.
FTP	FTP	Configure FTP server settings.
SNMP	SNMP	Configure SNMP communities and services.
Auth. Server	Auth. Server	Configure the Zyxel Device to act as a RADIUS server.
Notification	Mail Server	Configure a mail server with authentication to send reports and password expiration notification emails.
Language	Language	Select the Web Configurator language.
IPv6	IPv6	Enable IPv6 globally on the Zyxel Device here.
ZON	ZON	Use the Zyxel One Network (ZON) utility to view and manage the Zyxel Device's neighboring devices via the Zyxel Discovery Protocol (ZDP).
Log & Report		
Email Daily Report	Email Daily Report	Configure where and how to send daily reports and what reports to send.
Log Settings	Log Settings	Configure the system log, email 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 Zyxel Device.

Table 7 Maintenance Menu Screens Summary

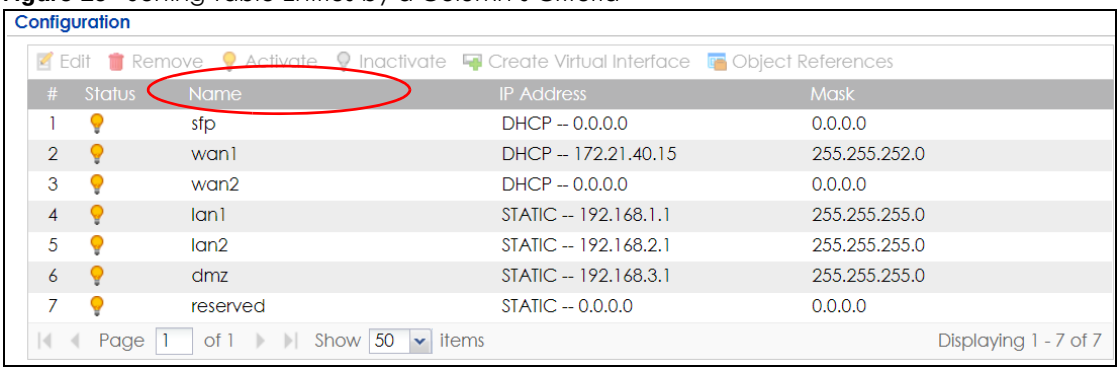
FOLDER OR LINK	TAB	FUNCTION
File Manager	Configuration File	Manage and upload configuration files for the Zyxel Device.
	Firmware Management	View the current firmware version and upload firmware. Reboot with your choice of firmware.
	Shell Script	Manage and run shell script files for the Zyxel Device.
Diagnostics	Diagnostics Collect Collect on AP Files	Collect diagnostic information.
	Packet Capture	Capture packets for analysis.
	CPU/Memory Status	View CPU and memory usage statistics.
	System Log	Connect a USB device to the Zyxel Device and archive the Zyxel Device system logs to it here.
	Remote Assistance	Configure and schedule external access to the Zyxel Device for troubleshooting.
	Network Tool	Identify problems with the connections. You can use Ping or Traceroute to help you identify problems.
	Routing Traces	Configure traceroute to identify where packets are dropped for troubleshooting.
	Wireless Frame Capture	Capture wireless frames from APs for analysis.
Packet Flow Explore	Routing Status	Check how the Zyxel Device determines where to route a packet.
	SNAT Status	View a clear picture on how the Zyxel Device converts a packet's source IP address and check the related settings.
Shutdown	Shutdown	Turn off the Zyxel Device.

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.

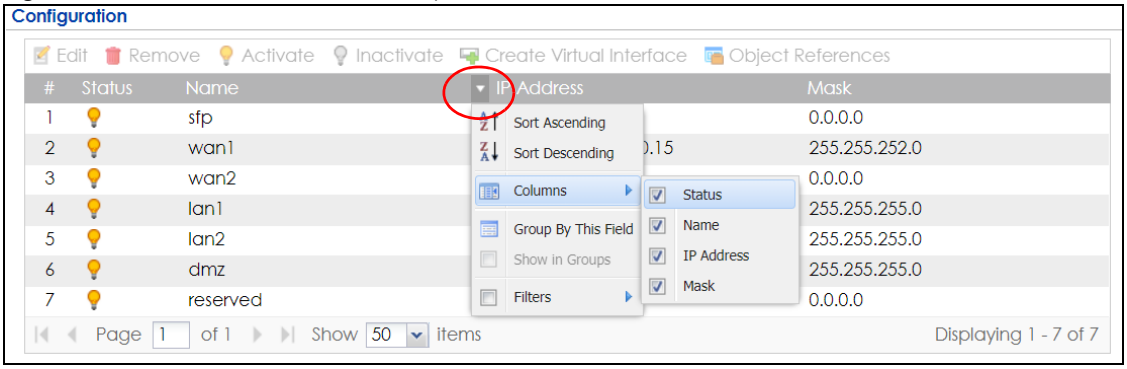
Figure 16 Sorting Table Entries by a Column's Criteria



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:

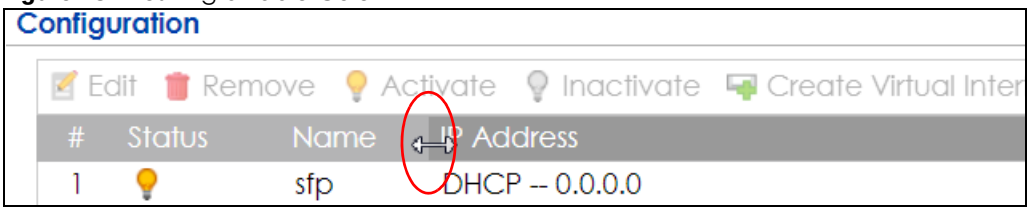
- Sort in ascending or descending (reverse) alphabetical order
- Select which columns to display
- Group entries by field
- Show entries in groups
- Filter by mathematical operators (<, >, or =) or searching for text

Figure 17 Common Table Column Options



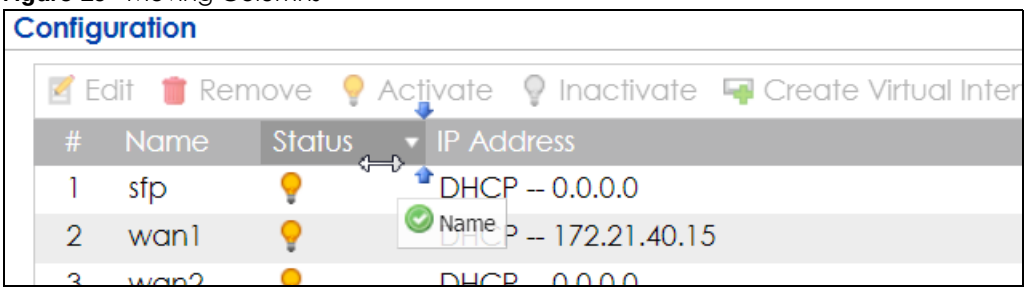
Select a column heading cell's right border and drag to re-size the column.

Figure 18 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 19 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 20 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 21 Common Table Icons

Here are descriptions for the most common table icons.

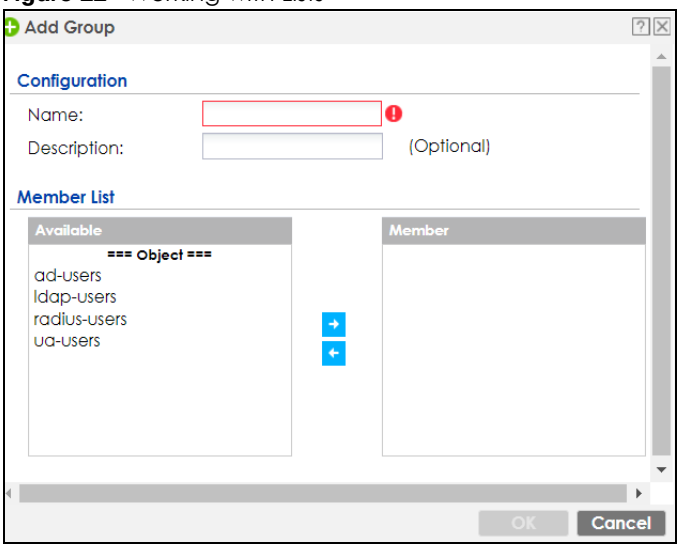
Table 8 Common Table Icons

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 Zyxel Device applies the table's entries in order like the 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 Zyxel Device 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**.
References	Select an entry and click **References** 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 22 Working with Lists



CHAPTER 2
Initial Setup Wizard

2.1 Initial Setup Wizard Screens

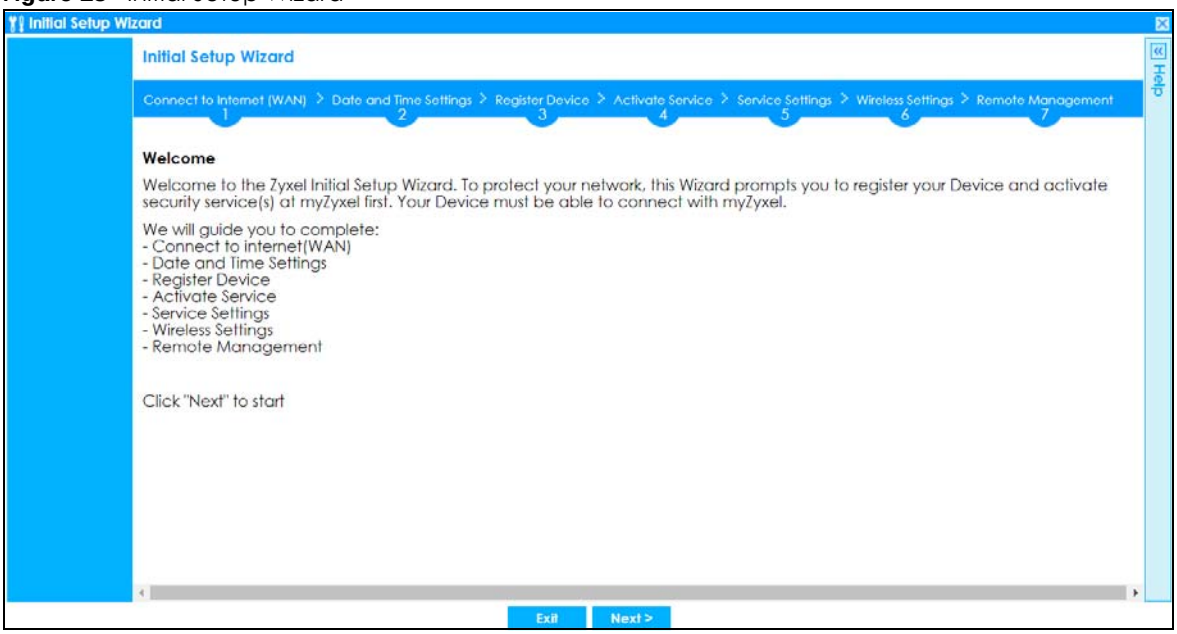
When you log into the Web Configurator for the first time or when you reset the Zyxel Device to its default configuration, the **Initial Setup Wizard** screen displays. This wizard helps you configure Internet connection settings and activate subscription services.

Note: For Zyxel Devices that already have firmware version 4.25 or later, you have to register your Zyxel Device and activate the corresponding service at myZyxel (through your Zyxel Device).

This chapter provides information on configuring the Web Configurator's **Initial Setup Wizard**. See the feature-specific chapters in this User's Guide for background information.

- Click the double arrow in the upper right corner to display or hide the help.
- Click **Logout** to exit the **Initial Setup Wizard** or click **Next** to continue the wizard. Click **Finish** at the end of the wizard to complete the wizard.

Figure 23 Initial Setup Wizard



2.1.1 Internet Access Setup - WAN Interface

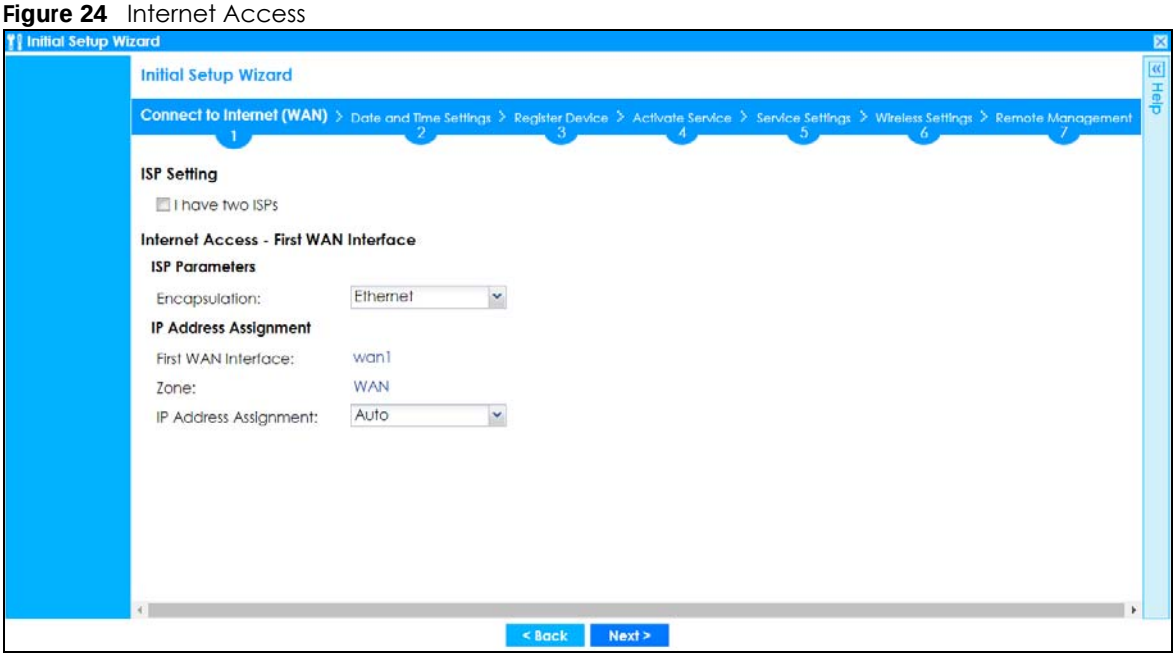
Use this screen to set how many WAN interfaces to configure and the first WAN interface's type of encapsulation and method of IP address assignment.

The screens vary depending on the encapsulation type. Refer to information provided by your ISP to know what to enter in each field.

Note: Enter the Internet access information exactly as your ISP gave it to you. Leave a field blank if you don't have that information.

- **I have two ISPs**: 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. Choose **PPPoE**, **PPTP** or **L2TP** for a dial-up connection according to the information from your ISP.
- **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 the ISP assigned a fixed IP address.

Figure 24 Internet Access



2.1.2 Internet Access: Ethernet

This screen is read-only if you set the previous screen's **IP Address Assignment** field to **Auto**. If you set the previous screen's **IP Address Assignment** field to **Static,** use this screen to configure your IP address settings.

- **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.

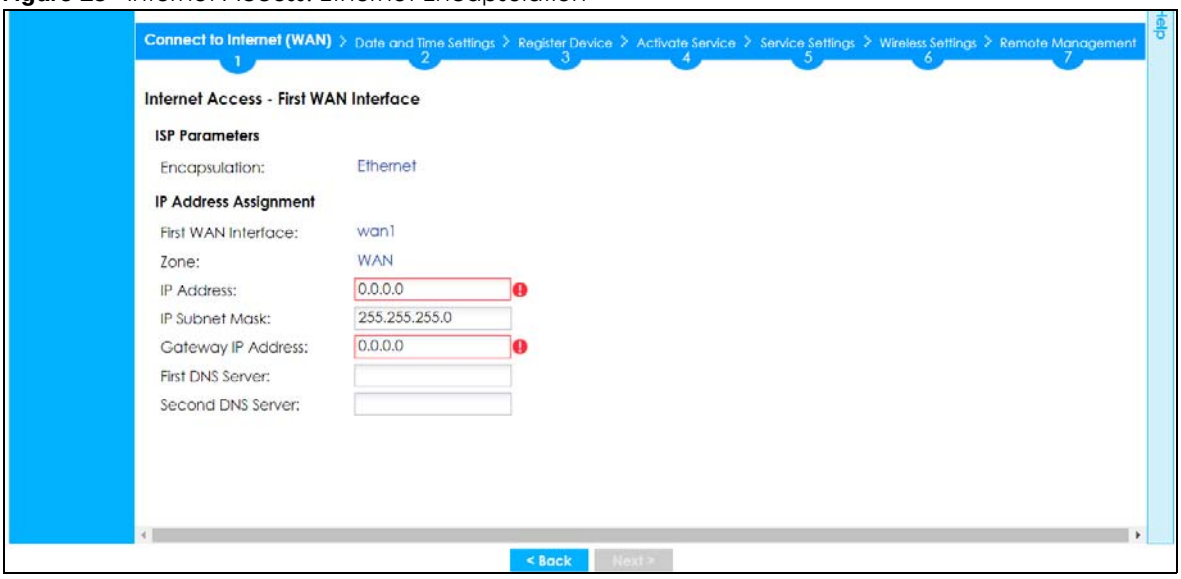
- **IP Subnet Mask**: Enter the subnet mask for this WAN connection's IP address.

- **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 Zyxel Device uses these (in the order you specify here) to resolve domain names for VPN, DDNS and the time server. Leave the field as 0.0.0.0 if you do not want to configure DNS servers.

2.1.2.1 Possible Errors

- Check that your cable connection is coming from the correct interface you're using for the WAN connection on the Zyxel Device.
- Check that the interface is connected to the device you're using for Internet access such as a broadband router and that the router is turned on. The LED of the interface you're using for the WAN connection on the Zyxel Device should be orange.
- If your Zyxel Device was not able to obtain an IP address, check that your Internet access information uses DHCP as the WAN connection type. If it fails again, check with your Internet service provider or administrator for correct WAN settings.
- If your Zyxel Device was not able to use the IP address entered, check that you were given an IP address, subnet mask and gateway address as part of your Internet access information. Re-enter your IP address, subnet mask and gateway IP address exactly as given. If it fails again, check with your Internet service provider or administrator for correct IP address, subnet mask and gateway address and other WAN settings.

Figure 25 Internet Access: Ethernet Encapsulation



2.1.3 Internet Access: PPPoE

2.1.3.1 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 Zyxel Device accepts either CHAP or PAP when requested by the remote node.

  - **Chap** - Your Zyxel Device accepts CHAP only.
  - **PAP** - Your Zyxel Device accepts PAP only.
  - **MSCHAP** - Your Zyxel Device accepts MSCHAP only.
  - **MSCHAP-V2** - Your Zyxel Device 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.

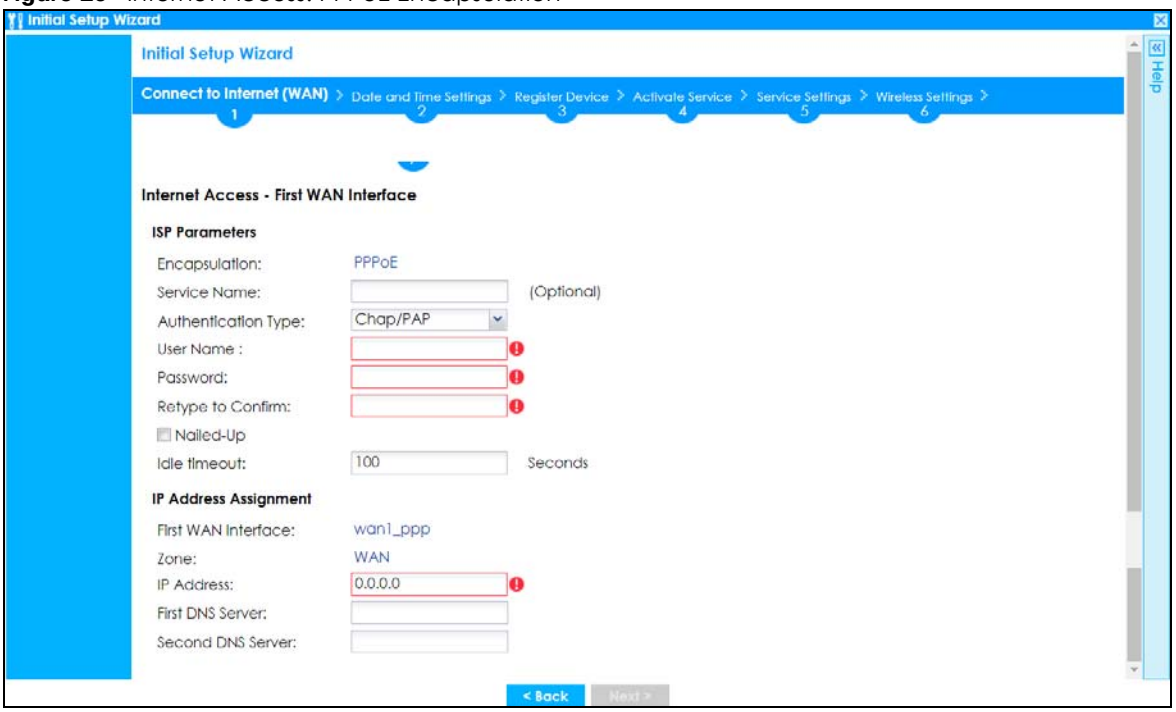
2.1.3.2 WAN IP Address Assignments

- **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 Zyxel Device uses these (in the order you specify here) to resolve domain names for VPN, 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.

2.1.3.3 Possible Errors

- Check that you're using the correct PPPoE **Service Name** and **Authentication Type**.
- Make sure that your Internet access information uses PPPoE as the WAN connection type. Re-enter your PPPoE user name and password exactly as given. If it fails again, check with your Internet service provider or administrator for correct WAN settings and user credentials.
- If you were given an IP address and DNS server information as part of your Internet access information, re-enter them exactly as given. If it fails again, check with your Internet service provider or administrator for correct IP address, subnet mask and gateway address and other WAN settings.

Figure 26 Internet Access: PPPoE Encapsulation



2.1.4 Internet Access: PPTP

2.1.4.1 ISP Parameters

- **Authentication Type** - Select an authentication protocol for outgoing calls. Options are:
  - **Chap/PAP** - Your Zyxel Device accepts either CHAP or PAP when requested by the remote node.
  - **Chap** - Your Zyxel Device accepts CHAP only.
  - **PAP** - Your Zyxel Device accepts PAP only.
  - **MSCHAP** - Your Zyxel Device accepts MSCHAP only.
  - **MSCHAP-V2** - Your Zyxel Device 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.

2.1.4.2 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 router through which this WAN connection will send traffic (the default gateway).
- **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.

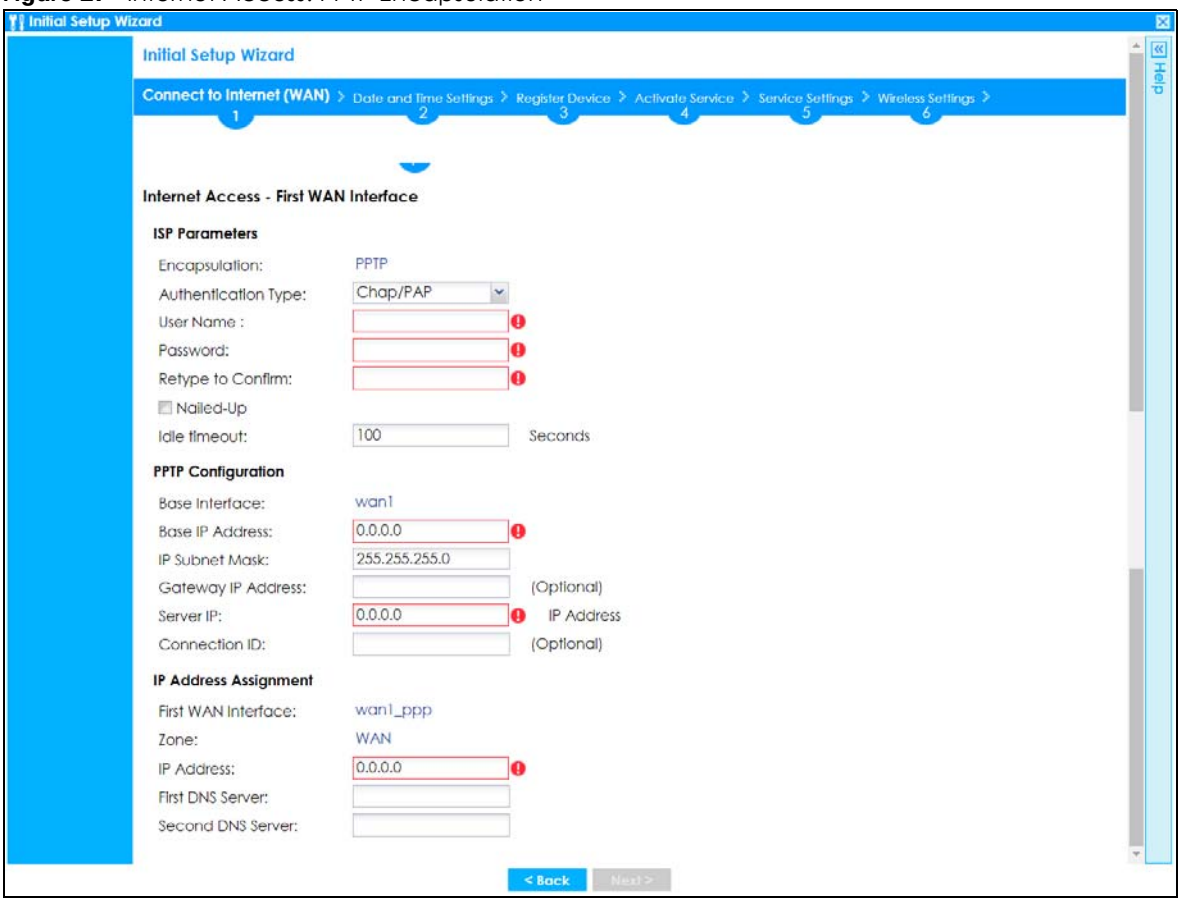
2.1.4.3 WAN IP Address Assignments

- **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 Zyxel Device uses these (in the order you specify here) to resolve domain names for VPN, DDNS and the time server. Leave the field as 0.0.0.0 if you do not want to configure DNS servers.

2.1.4.4 Possible Errors

- Check that you’re using the correct PPPT **Service IP**, **Base IP Address, IP Subnet Mask, Gateway IP Address, Connection ID** and **Authentication Type**.
- Make sure that your Internet access information uses PPTP as the WAN connection type. Re-enter your PPTP user name and password exactly as given. If it fails again, check with your Internet service provider or administrator for correct WAN settings and user credentials.
- If you were given an IP address and DNS server information as part of your Internet access information, re-enter them exactly as given. If it fails again, check with your Internet service provider or administrator for correct IP address, subnet mask and gateway address and other WAN settings.

Figure 27 Internet Access: PPTP Encapsulation



2.1.5 Internet Access: L2TP

2.1.5.1 ISP Parameters

- **Authentication Type** - Select an authentication protocol for outgoing connection requests. Options are:
  - **Chap/PAP** - Your Zyxel Device accepts either CHAP or PAP when requested by the remote node.
  - **Chap** - Your Zyxel Device accepts CHAP only.
  - **PAP** - Your Zyxel Device accepts PAP only.
  - **MSCHAP** - Your Zyxel Device accepts MSCHAP only.
  - **MSCHAP-V2** - Your Zyxel Device 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.

2.1.5.2 L2TP 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.

- **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).
- **Server IP**: Type the IP address of the L2TP server.

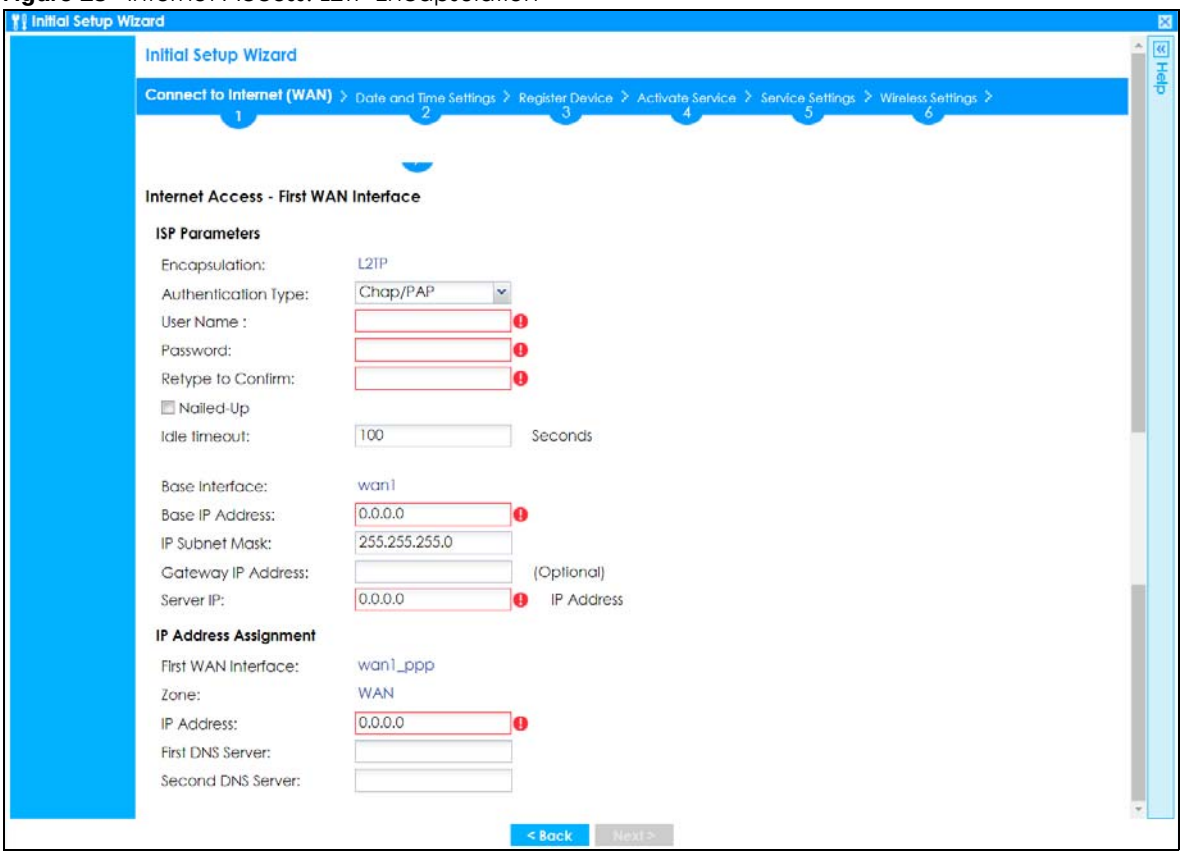
2.1.5.3 WAN IP Address Assignments

- **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 Zyxel Device uses these (in the order you specify here) to resolve domain names for VPN, DDNS and the time server. Leave the field as 0.0.0.0 if you do not want to configure DNS servers.

2.1.5.4 Possible Errors

- Check that you're using the correct L2PT **Server IP**, **Subnet Mask**, **Gateway IP Address, IP Subnet Mask** and **Authentication Type**.
- Make sure that your Internet access information uses L2TP as the WAN connection type. Re-enter your L2TP user name and password exactly as given. If it fails again, check with your Internet service provider or administrator for correct WAN settings and user credentials.
- If you were given an IP address and DNS server information as part of your Internet access information, re-enter them exactly as given. If it fails again, check with your Internet service provider or administrator for correct IP address, subnet mask and gateway address and other WAN settings.

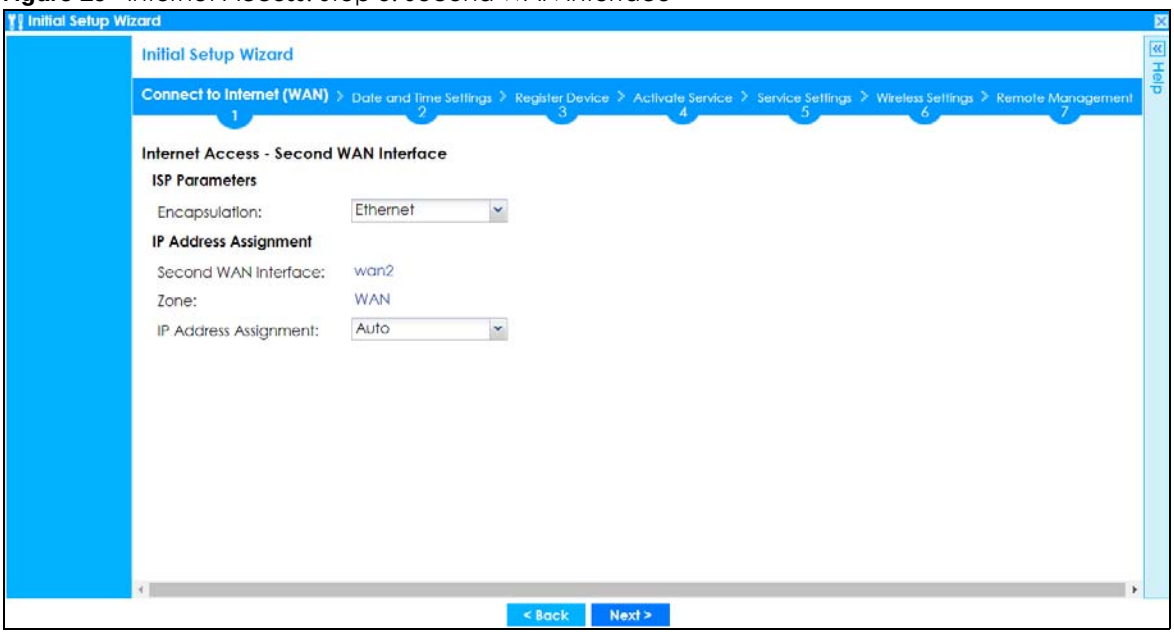
Figure 28 Internet Access: L2TP Encapsulation



2.1.6 Internet Access Setup - Second WAN Interface

If 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 2.1.1 on page 48).

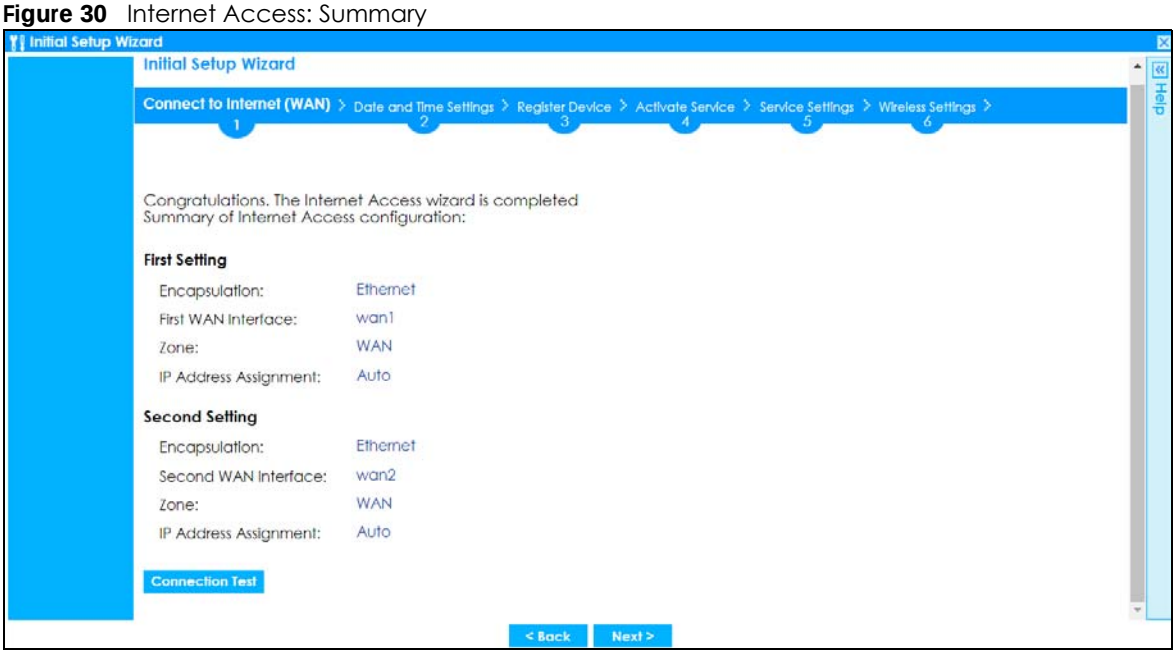
Figure 29 Internet Access: Step 3: Second WAN Interface



2.1.7 Internet Access: Congratulations

You have set up your Zyxel Device to access the Internet. A screen displays with your settings. Click **Connection Test** to check that you can access the Internet. If you cannot, click **Back** and confirm that you entered the settings correctly. If you have, check that you got the correct settings from your ISP or network administrator.

Figure 30 Internet Access: Summary

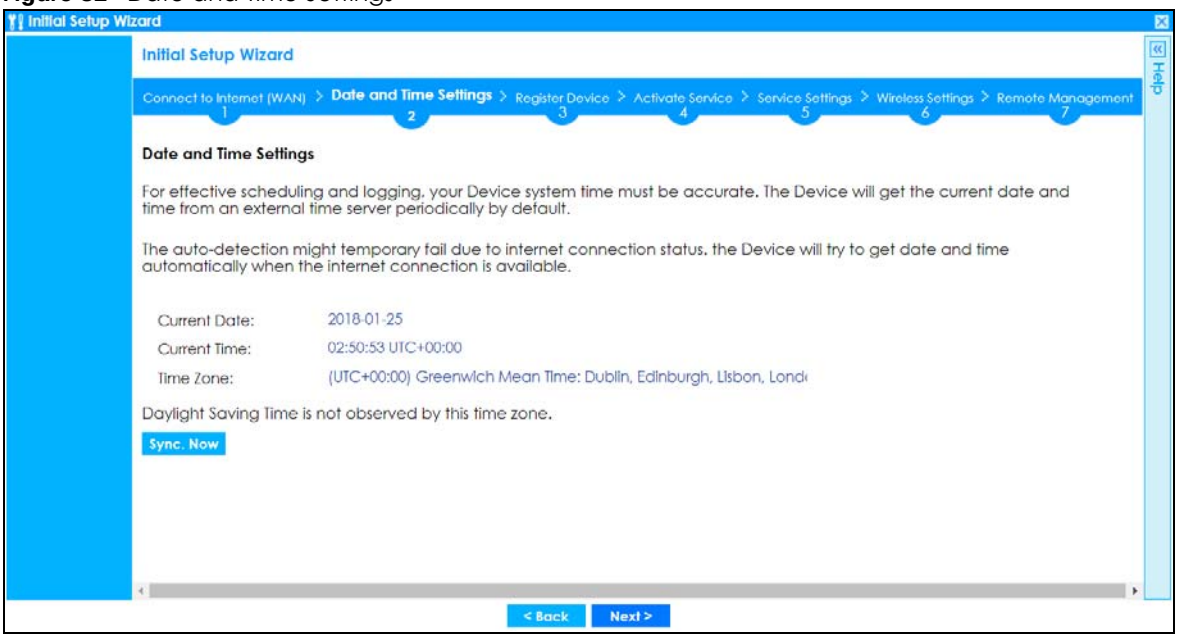


2.1.8 Date and Time Settings

It's important to have correct date and time values in the logs. The Zyxel Device can automatically update the time and date by detecting your time zone and whether Daylight Savings is in effect in that time zone.

If your Zyxel Device cannot get the correct date and time, it may not able to connect to a time server. Check that the Zyxel Device has Internet access, then click **Sync. Now**.

Figure 31 Date and Time Settings

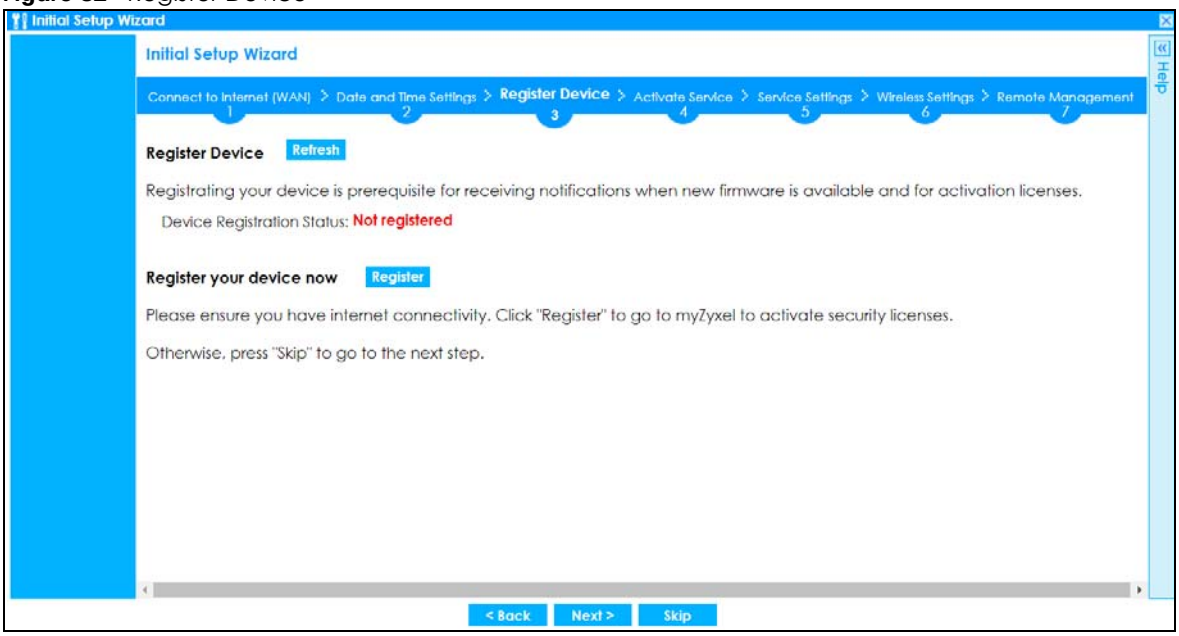


2.1.9 Register Device

Click the **Register** button in this screen to register your device at portal.myzyxel.com.

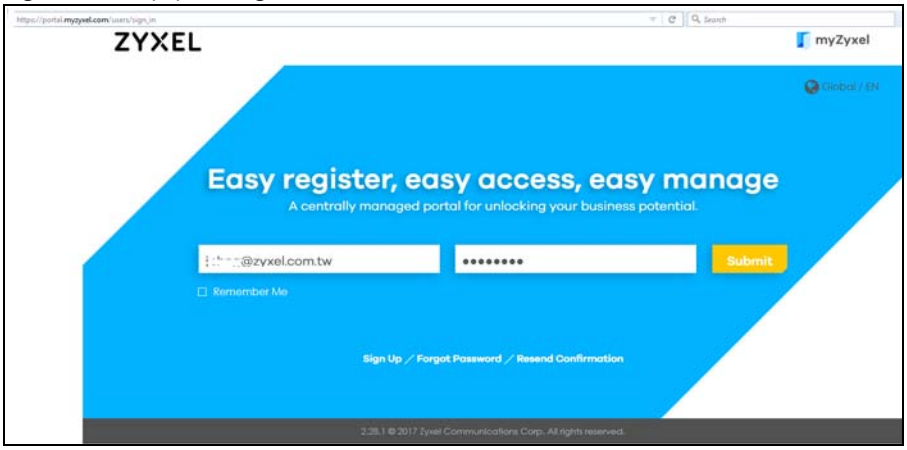
Note: The Zyxel Device must be connected to the Internet in order to register.

Figure 32 Register Device



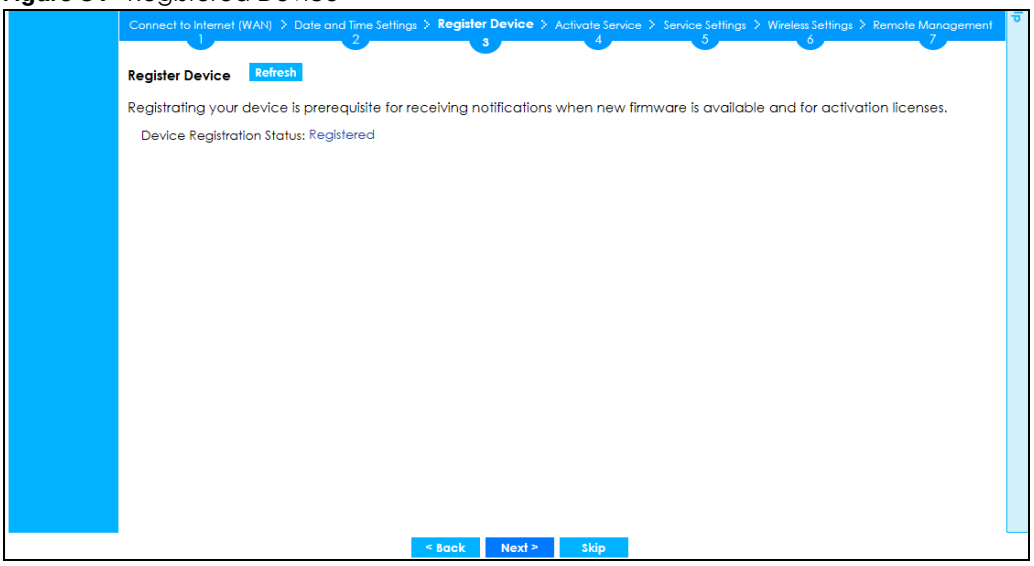
You may need the Zyxel Device's serial number and LAN MAC address to register it at myZyxel if you have not already done so. Refer to the label at the back of the Zyxel Device's for details.

Figure 33 myZyxel Login



Click **Refresh** or use the **Configuration > Licensing > Registration** screen to update your Zyxel Device registration status.

Figure 34 Registered Device



2.1.10 Activate Service

After you register your Zyxel Device, you can register for the services supported by your model. See Subscription Services Available on page 186 for more information on the subscription services for the two types of security packs.

Here are the services available for the Zyxel Device:

- Web Security (to access a database that can block websites by category)
- Application Security (to use signature for Application Patrol inspection and signatures to recognize unsolicited commercial or junk email suspected of being sent by spammers.)
- Malware Blocker (to detect malware patterns in files)
- Intrusion Prevention (to use signatures for Intrusion Detection and Prevention attacks)
- Geo Enforcer (to access a database of country-to-IP address mappings)
- Sandboxing (to specify the actions the Zyxel Device takes when malicious or suspicious files are detected)
- Reputation Filter (to recognize packets coming from IPv4 address with bad reputation)
- SecuReporter (to collect and analyze logs from your Zyxel Device in order to identify anomalies, alert on potential internal / external threats, and report on network usage)
- Managed AP Service (to manage more APs than the default for your Zyxel Device when the AP controller is enabled)

Click **Refresh** and wait a few moments for the registration information to update in this screen. If the page does not refresh, make sure the Internet connection is working and click **Refresh** again. To check your Internet connection, try to access the Internet from a computer connected to a LAN port on the Zyxel Device. If you cannot, then check your Internet access settings on the Zyxel Device.

Figure 35 Activate Service

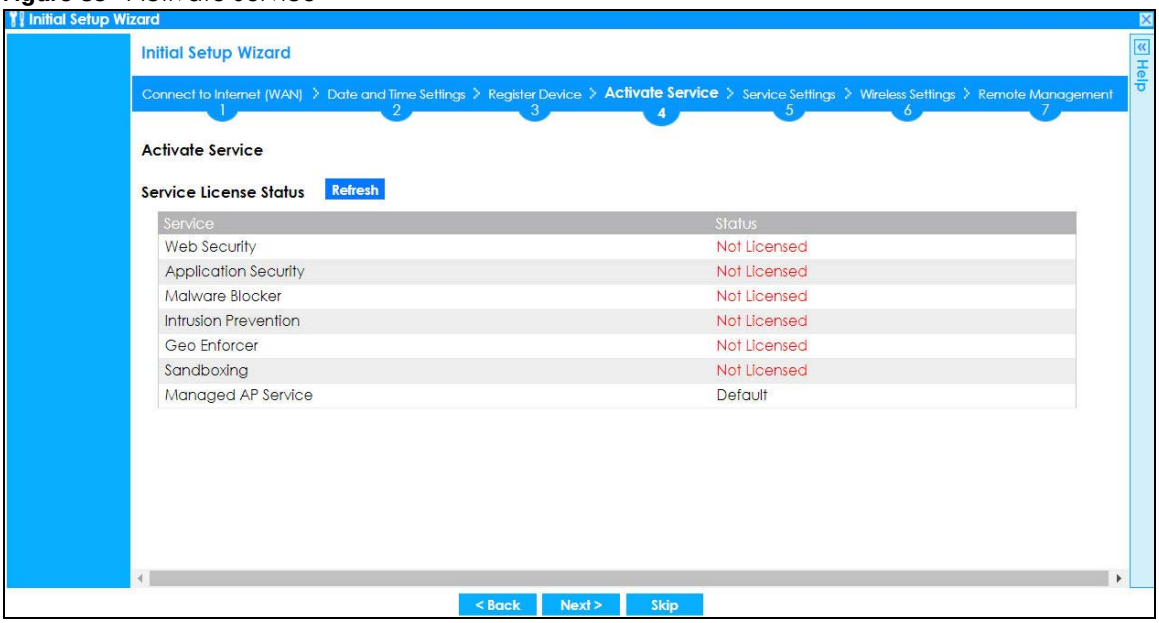
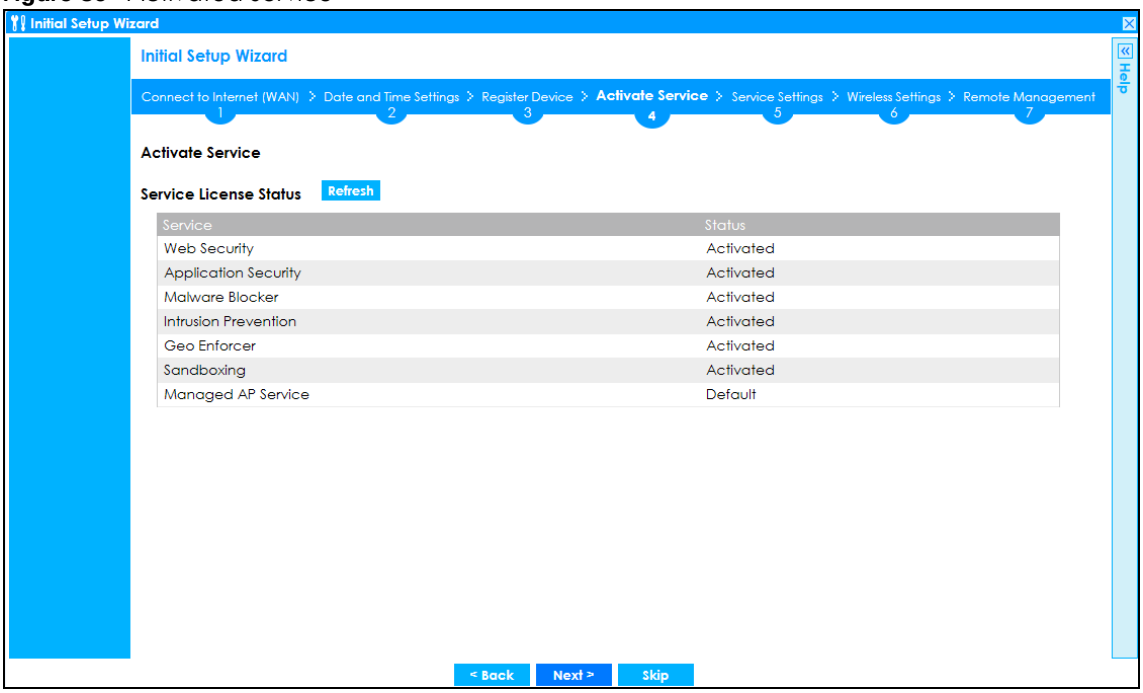


Figure 36 Activated Service



2.1.11 Service Settings

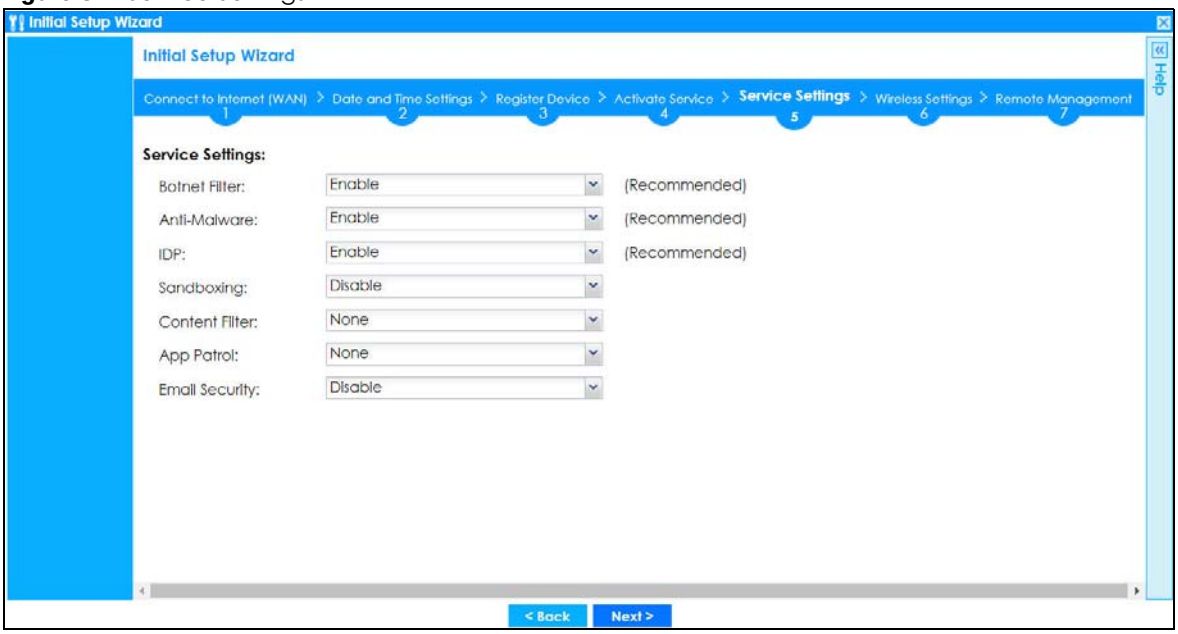
You can enable or disable the following features in this screen. This screen varies depending on the security pack that you purchase. See Subscription Services Available on page 186 for more information on the subscription services for the two types of security packs.

- **Botnet Filter**: Use this feature to detect and block connection attempts to or from the C&C server or known botnet IP addresses.
- **Anti-Malware**: Use this feature to protect your connected network from malware infection.

- **IDP**: Use this feature to detect malicious or suspicious packets and respond instantaneously.
- **IP Reputation**: Use this feature to recognize and filter packets coming from IPv4 address with bad reputation.
- **Sandboxing**: Use this feature to provide a safe environment to separate running programs from your network and host devices.
- **Content Filter**: Use this feature to control access to specific web sites or web content.
- **App Patrol**: Use this feature to manage the use of various applications on the network.
- **Email Security**: Use this feature to mark or discard spam (unsolicited commercial or junk email).
- **SecuReporter**: Use this feature to collect and analyze logs from your Zyxel Device in order to identify anomalies, alert on potential internal / external threats, and report on network usage.

  Select the **I have read SecuReporter GDPR and agree policy** check box to have SecuReporter collect and analyze logs from this Zyxel Device. This check box won't appear again if you have already selected this before.

Figure 37 Service Settings



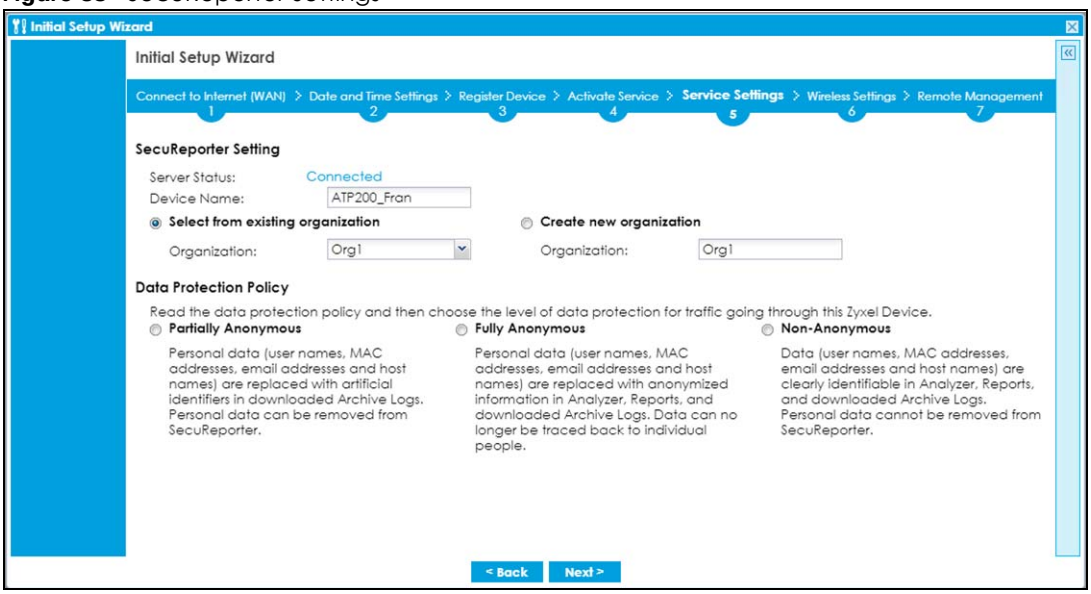
2.1.12 Service Settings: SecuReporter

Use this screen to add the Zyxel Device to a new or existing organization, and choose the level of data protection for traffic going through this Zyxel Device.

- **Server Status**: This is the connection status between the Zyxel Device and the SecuReporter server. This field shows **Connected** when the Zyxel Device can synchronize with the SecuReporter server. This field shows **Timeout** when the Zyxel Device can't synchronize with the SecuReporter server. This field shows **Fail** when the connection between the Zyxel Device and the SecuReporter server is down.
- **Device Name**: Enter the name of the Zyxel Device. This Zyxel Device will be added to a new or existing organization.
- **Organization**: This field appears if you haven't created an organization in the SecuReporter server. Type a name of up to 255 characters and description to create a new organization.
- **Select from existing organization**: Select an existing organization from the drop-down list box to add the Zyxel Device to the selected organization.

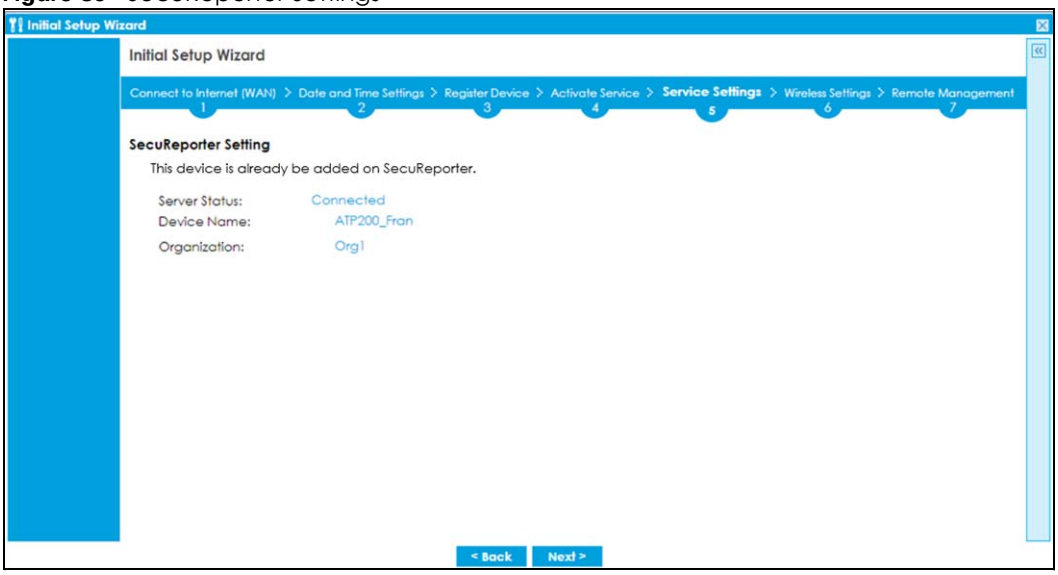
- **Create new organization**: Type a name of up to 255 characters and description to create a new organization.
- **Partially Anonymous**: Select this and personal data, such as user names, MAC addresses, email addresses, and host names, will be replaced with artificial identifiers in downloaded logs.
- **Fully Anonymous**: Select this and personal data, such as user names, MAC addresses, email addresses, and host names, will be replaced with anonymized information in downloaded logs.
- **Non-Anonymous**: Select this and personal data, such as user names, MAC addresses, email addresses, and host names, will be identifiable in downloaded logs.

Figure 38 SecuReporter Settings



The following screen appears when the Zyxel Device is already added in an organization.

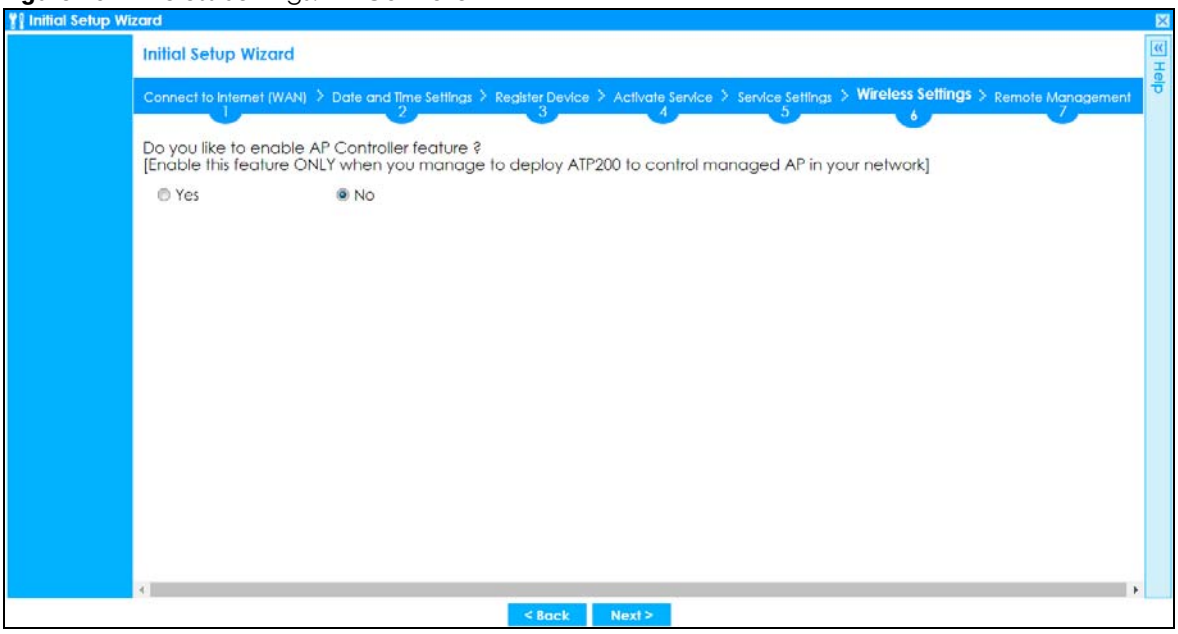
Figure 39 SecuReporter Settings



2.1.13 Wireless Settings: AP Controller

The Zyxel Device can act as an AP Controller that can manage APs in the same network as the Zyxel Device. Select **Yes** if you want your Zyxel Device to manage APs in your network; otherwise select **No**.

Figure 40 Wireless Settings: AP Controller



2.1.14 Wireless Settings: SSID & Security

Configure SSID and wireless security in this screen.

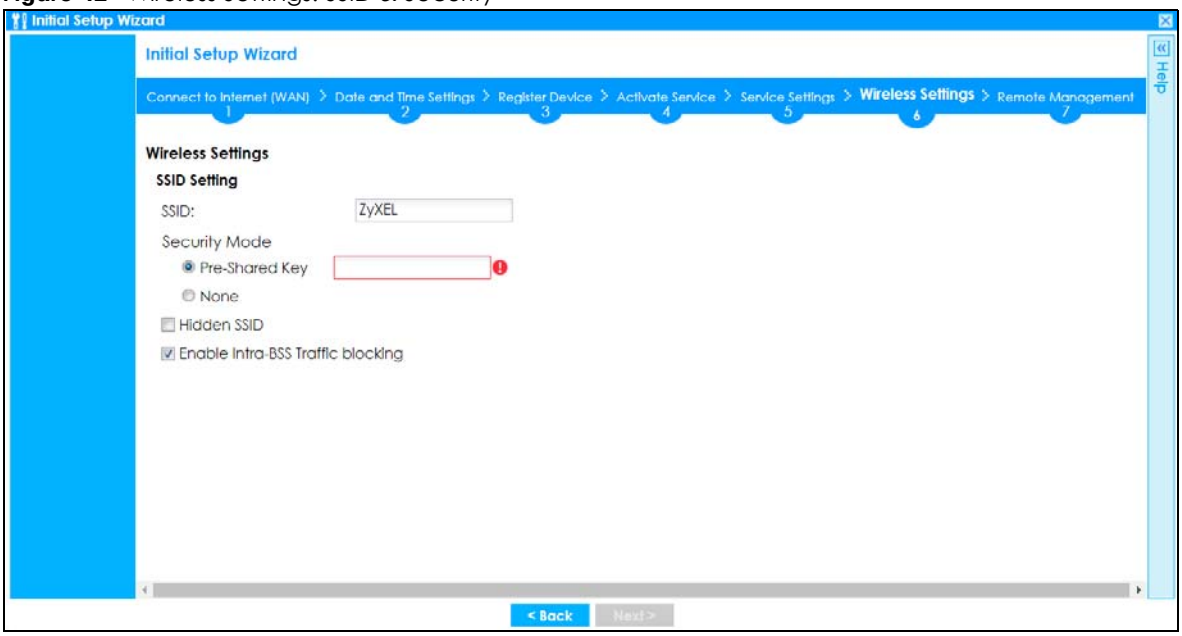
SSID Setting

- **SSID** - Enter a descriptive name of up to 32 printable characters for the wireless LAN.
- **Security Mode** - Select **Pre-Shared Key** to add security on this wireless network. Otherwise, select **None** to allow any wireless client to associate this network without authentication.
- **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.
- **Hidden SSID** - Select this 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.
- **Enable Intra-BSS Traffic Blocking** - Select this 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.

For Built-in Wireless AP Only

Bridged to: Zyxel Devices with W in the model name have a built-in AP. Select an interface to bridge with the built-in AP wireless network. Devices connected to this interface will then be in the same broadcast domain as devices in the AP wireless network.

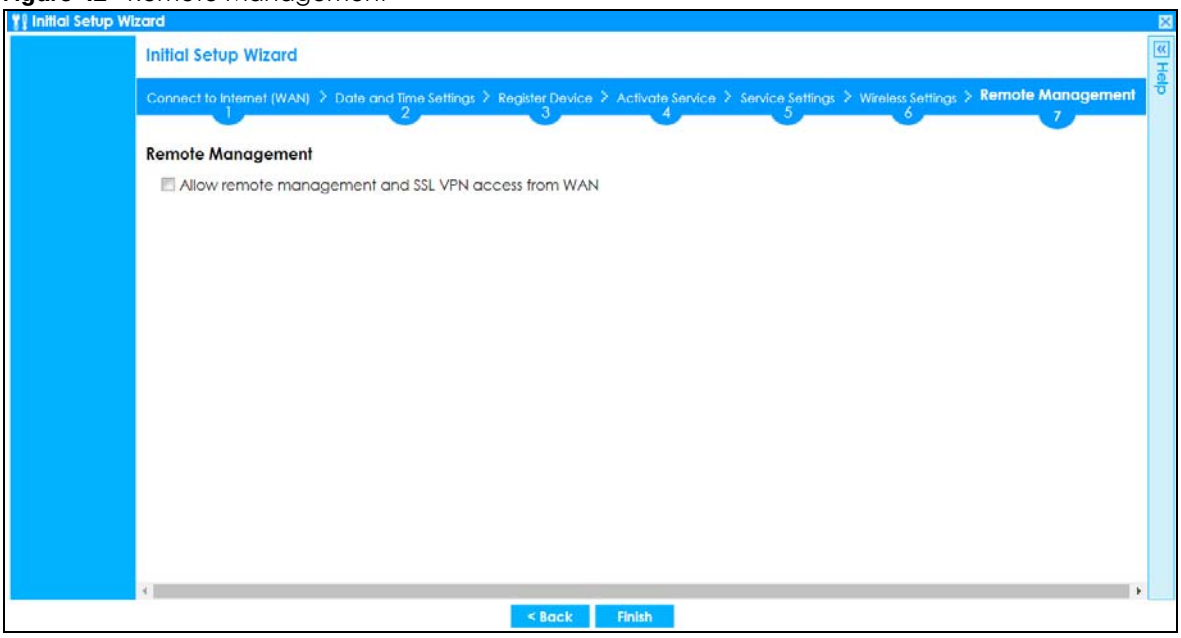
Figure 41 Wireless Settings: SSID & Security



2.1.15 Remote Management

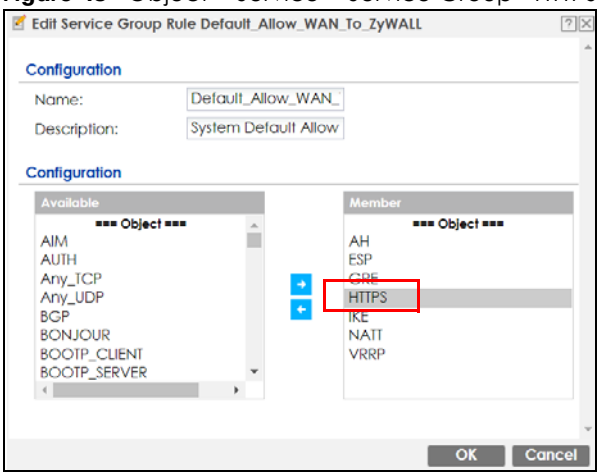
Select this to allow access to the Zyxel Device using HTTP or HTTPS from the Internet.

Figure 42 Remote Management



HTTPS is added to the **Default_Allow_WAN_to_ZyWALL** rule in **Object > Service > Service Group** screen when you enable **Remote Management**.

Figure 43 Object > Service > Service Group - HTTPS



CHAPTER 3
Hardware, Interfaces and Zones

3.1 Hardware Overview

This section describes the front and rear panels for each model.

The following table summarizes the port features of the Zyxel Device by model.

Table 9 ATP Series Comparison Table

ATP MODELS	ATP100/ATP100W	ATP200	ATP500	ATP700/ATP800
USB 3.0 Ports	1	2	2	2
1 Gbps SFP interface	1	1	1	2
10/100/1000 Mbps Ethernet WAN Ports	1	2	-	-
10/100/1000 Mbps Ethernet Ports	4	4	7	12
Console Port	1	1	1	1

3.1.1 Front Panels

The LED indicators are located on the front panel.

Figure 44 ATP100 Front Panel

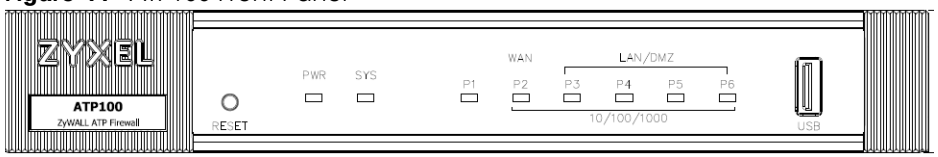


Figure 45 ATP100W Front Panel

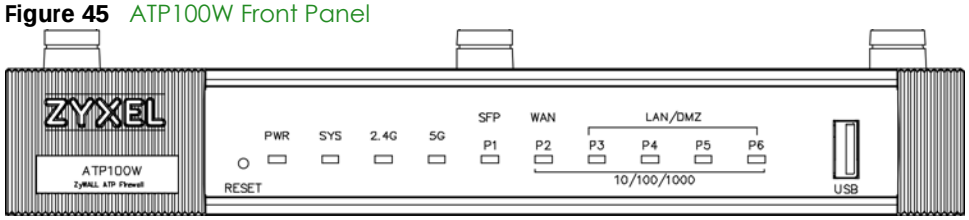


Figure 46 ATP200 Front Panel

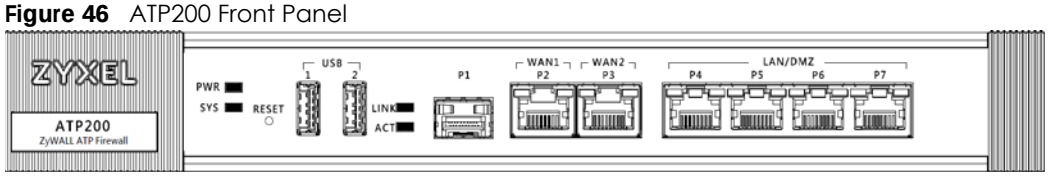


Figure 47 ATP500 Front Panel

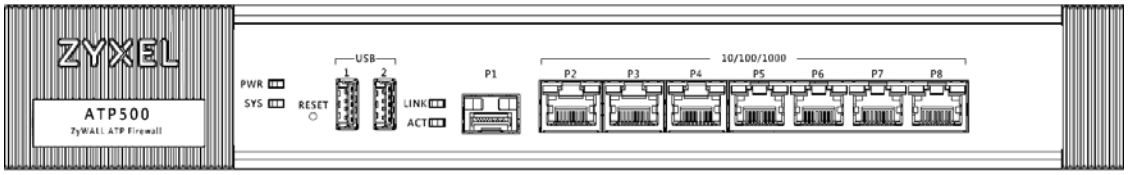
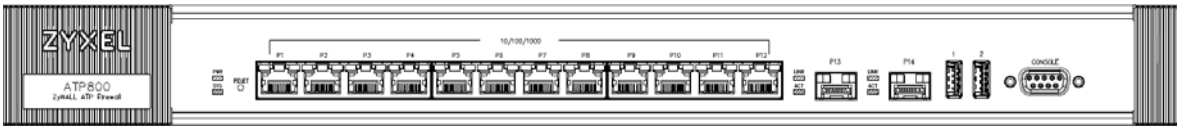


Figure 48 ATP700 / ATP800 Front Panel



The following table describes the front panel LEDs.

Table 10 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR		Off	The Zyxel Device is turned off.
	Green	On	The Zyxel Device 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. If the LED turns red again, then please contact your vendor.
SYS	Green	Off	The Zyxel Device is not ready or has failed.
		On	The Zyxel Device is ready and running.
		Blinking	The Zyxel Device is booting.
	Red	On	The Zyxel Device has an error or has failed.
2.4G	Green	Off	The 2.4G wireless interface is off.
		On	The 2.4G wireless interface is ready.
		Blinking	The 2.4G wireless connection is active.
5G	Green	Off	The 5G wireless interface is off.
		On	The 5G wireless interface is ready.
		Blinking	The 5G wireless connection is active.
P1 (SFP)			
LINK	Yellow	Off	There is no connection on this port.
		On	This port has a successful 1000 Mbps link.
	Green	Off	There is no connection on this port.
		On	This port has a successful 100 Mbps link.
ACT	Green	Off	There is no traffic on this port.
		Blinking	The Zyxel Device is sending or receiving packets on this port at 100/1000 Mbps.
P2, P3... (WAN/ LAN/ DMZ)	Yellow	Off	There is no connection on this port.
		On	This port has a successful 1000 Mbps link.
		Blinking	The Zyxel Device is sending or receiving packets on this port at 1000 Mbps.
	Green	Off	There is no connection on this port.
		On	This port has a successful 10/100 Mbps link.
		Blinking	The Zyxel Device is sending or receiving packets on this port at 10/100 Mbps.

The following table describes the ports on the front panel.

Table 11 Front Panel Ports

LABEL	DESCRIPTION
RESET	Press the button in for about 5 seconds (or until the **SYS** LED starts to blink), then release it to return the Zyxel Device to the factory defaults (password is 1234, LAN IP address 192.168.1.1 etc.)
CONSOLE	You can use the console port to manage the Zyxel Device using CLI commands. You will be prompted to enter your user name and password. See the Command Reference Guide for more information about the CLI. When configuring using the console port, you need a computer equipped with communications software configured to the following parameters: • Speed 115200 bps • Data Bits 8 • Parity None • Stop Bit 1 • Flow Control Off
USB	Connect a storage device for system logs (see **Maintenance > Diagnostics > System Log**) and storage (see **Configuration > System > USB Storage**).
P2-P7 (ATP200) P2-P8 (ATP500) P1-P12 (ATP700/ ATP800)	These are 1G RJ-45 Ethernet ports.

3.1.2 Rear Panels

The connection ports are located on the rear panel.

Figure 49 ATP100 Rear Panel

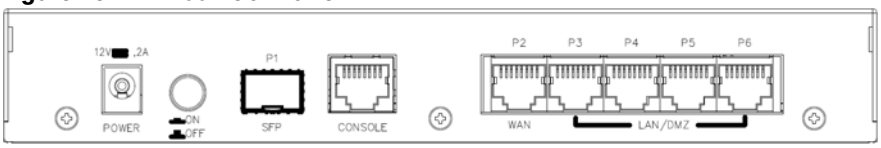


Figure 50 ATP100W Rear Panel

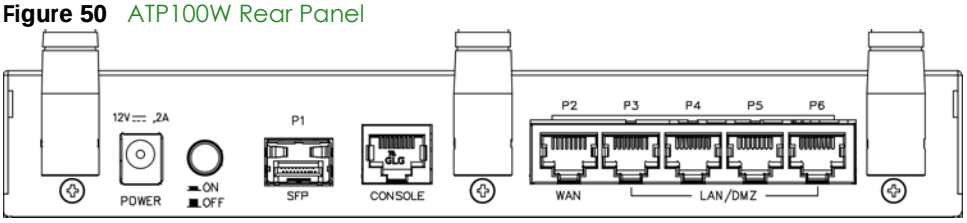


Figure 51 ATP200 Rear Panel

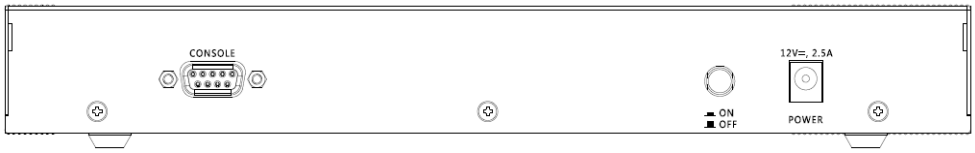


Figure 52 ATP500 Rear Panel

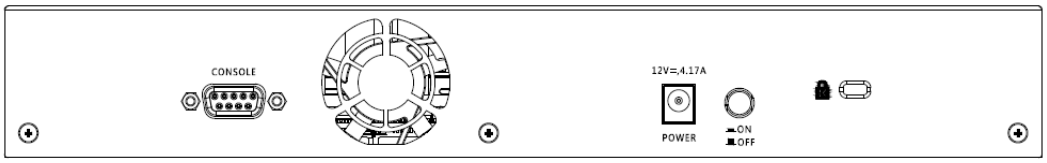
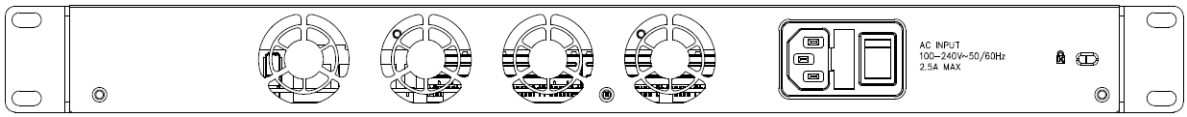


Figure 53 ATP700 / ATP800 Rear Panel



Note: Make sure you connect the Zyxel Device's power cord to a socket-outlet with an earthing connection or its equivalent.

The following table describes the items on the rear panel.

Table 12 Rear Panel Items

LABEL	DESCRIPTION
Console	You can use the console port to manage the Zyxel Device using CLI commands. You will be prompted to enter your user name and password. See the Command Reference Guide for more information about the CLI. When configuring using the console port, you need a computer equipped with communications software configured to the following parameters: • Speed 115200 bps • Data Bits 8 • Parity None • Stop Bit 1 • Flow Control Off
Power	Use the included power cord to connect the power socket to a power outlet. Turn the power switch on if your Zyxel Device has a power switch.
Lock	Attach a lock-and-cable from the Kensington lock (the small, metal-reinforced, oval hole) to a permanent object, such as a pole, to secure the Zyxel Device in place.
Fan	The fans are for cooling the Zyxel Device. Make sure they are not obstructed to allow maximum ventilation.

Note: Use an 8-wire Ethernet cable to run your Gigabit Ethernet connection at 1000 Mbps. Using a 4-wire Ethernet cable limits your connection to 100 Mbps. Note that the connection speed also depends on what the Ethernet device at the other end can support.

3.2 Mounting

The Zyxel Device can be mounted in a rack.

3.2.1 Rack-mounting

Use the following steps to mount the Zyxel Device 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 ZyWALL does not make

the rack unstable or top-heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

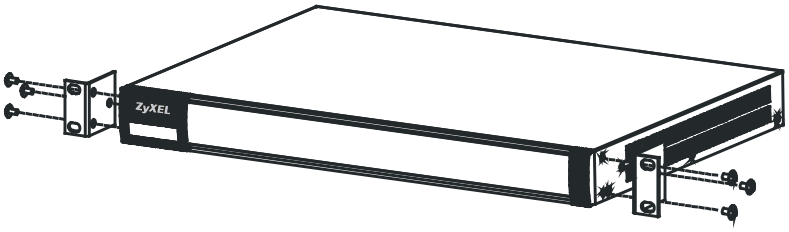
Note: Leave 10 cm of clearance at the sides and 20 cm in the rear.

Use a #2 Phillips screwdriver to install the screws.

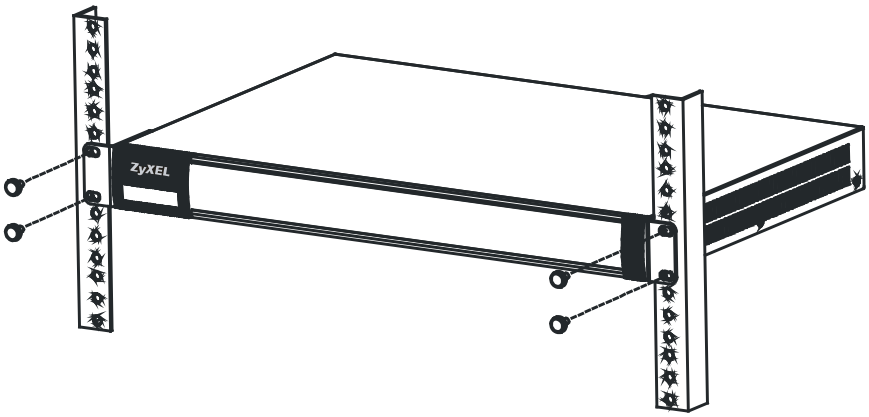
Note: Failure to use the proper screws may damage the unit.

1 Align one bracket with the holes on one side of the Zyxel Device 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 Zyxel Device in the rack and match up the bracket holes with the rack holes. Secure the Zyxel Device to the rack with the rack-mounting screws.



3.2.2 Wall-mounting

Do the following to attach your Zyxel Device to a wall. Only the devices listed in Table 13 on page 71 can be wall mounted.

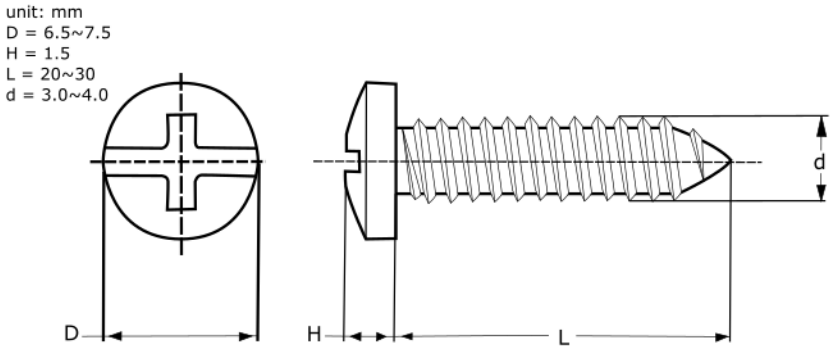
The following table lists the distance "X" between mounting holes for each model:

Table 13 Distance "X" between mounting holes

MODEL NAME	DISTANCE "X"
ATP100	174mm (6.85")
ATP100W	174mm (6.85")
ATP200	206mm (8.11")

1 Drill into a wall two holes 3 mm ~ 4 mm (0.12" ~ 0.16") wide, 20 mm ~ 30 mm (0.79" ~ 1.18") deep and a distance X (see the preceding table) apart. Place two screw anchors in the holes.

Figure 54 Wall mounting screw specifications



2 Screw two screws with 6 mm ~ 8 mm (0.24" ~ 0.31") wide heads into the screw anchors. Do not screw the screws all the way in to the wall; leave a small gap between the head of the screw and the wall.

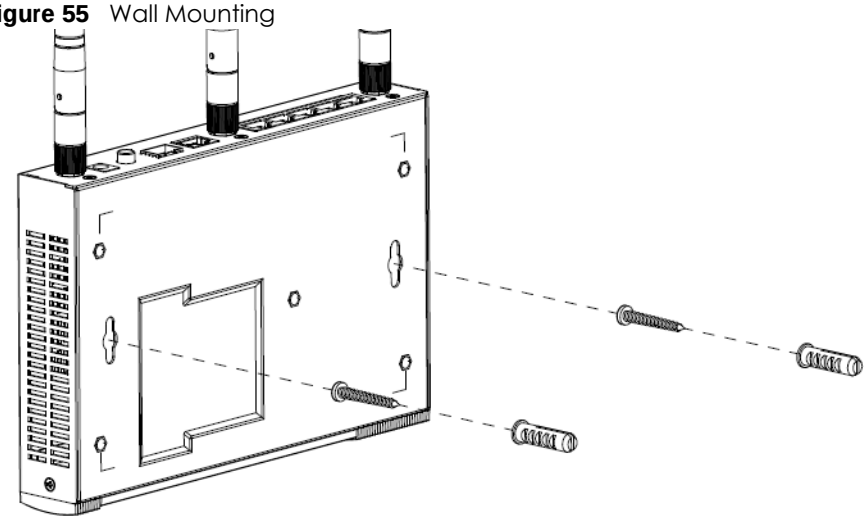
The gap must be big enough for the screw heads to slide into the screw slots and the connection cables to run down the back of the Zyxel Device.

Note: Make sure the screws are securely fixed to the wall and strong enough to hold the weight of the Zyxel Device with the connection cables.

3 Use the holes on the bottom of the Zyxel Device to hang the Zyxel Device on the screws.

Wall-mount the Zyxel Device horizontally. The Zyxel Device's side panels with ventilation slots should not be facing up or down as this position is less safe.

Figure 55 Wall Mounting



3.3 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 "wan1" or "wan2", "ge2" or" ge3".

An OPT (optional) Ethernet port can be configured as an additional WAN port, LAN, WLAN, or DMZ port.

The following table shows the default physical port and interface mapping for each model at the time of writing.

Table 14 Default Physical Port - Interface Mapping

PORT / INTERFACE	P1	P2	P3	P4	P5	P6	P7	P8
• ATP100/ATP100W	sfp	wan	lan1	lan1	lan1	opt		
• ATP200	sfp	wan	wan	lan1	lan1	lan1	lan1	
• ATP500	ge1	ge2	ge3	ge4	ge5	ge6	ge7	ge8

Table 15 Default Physical Port - Interface Mapping - ATP700 / ATP800

PORT / INTERFACE	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14
ATP800	ge1	ge2	ge3	ge4	ge5	ge6	ge7	ge8	ge9	ge10	ge11	ge12	ge13	ge14

The following table shows the default interface and zone mapping for each model at the time of writing.

Table 16 Default Zone - Interface Mapping

ZONE / INTERFACE	SFP	WAN	LAN1	LAN2	DMZ	OPT
• ATP100/ATP100W	sfp_ppp	WAN1_PPP	LAN1	LAN2	DMZ	opt_ppp

Table 17 Default Zone - Interface Mapping

ZONE / INTERFACE	WAN	LAN1	LAN2	DMZ	OPT	NO DEFAULT ZONE
• ATP200	WAN1 WAN1_PPP WAN2 WAN2_PPP	LAN1	LAN2	DMZ	SFP SFP_PPP	GE7 GE7_PPP GE8 GE8_PPP

Table 18 Default Zone - Interface Mapping

ZONE / INTERFACE	WAN	LAN	DMZ	OPT	NO DEFAULT ZONE
• ATP500	GE2 GE2_PPP GE3 GE3_PPP	GE4 GE5	GE6	GE1 GE1_PPP	GE7 GE7_PPP GE8 GE8_PPP
• ATP700 • ATP800	GE1 GE1_PPP GE2 GE2_PPP	GE3 GE4	GE5	GE13 GE13_PPP GE14 GE14_PPP	GE6~GE12 GE6_PPP~GE12_PPP

3.4 Stopping the Zyxel Device

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

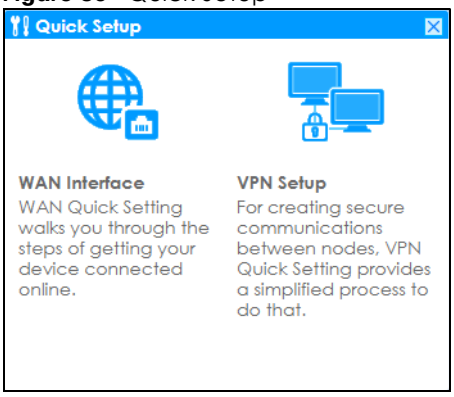
CHAPTER 4
Quick Setup Wizards

4.1 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 **Quick Setup** to open the first **Quick Setup** screen.

Figure 56 Quick Setup



- **WAN Interface**

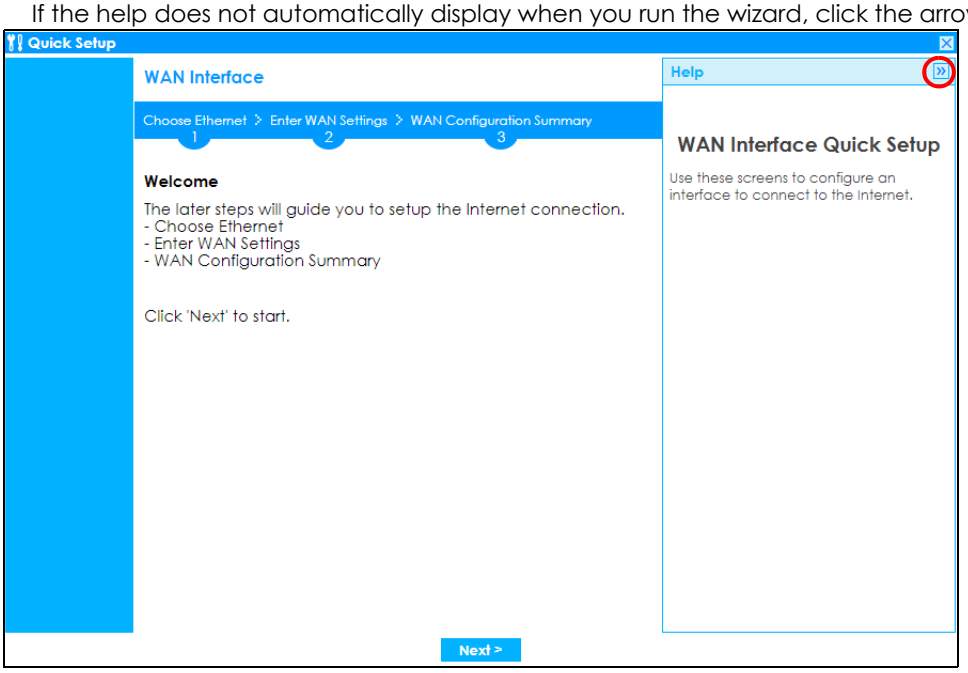
  Click this link to open a wizard to set up a WAN (Internet) connection. This wizard creates matching ISP account settings in the Zyxel Device if you use PPPoE or PPTP. See Section 4.2 on page 76.

- **VPN Setup**

  Use **VPN Setup** to configure a VPN (Virtual Private Network) rule for a secure connection to another computer or network. **Use VPN Settings for Configuration Provisioning** to set up a VPN rule that can be retrieved with the Zyxel Device IPSec VPN Client. You only need to enter a user name, password and the IP address of the Zyxel Device in the IPSec VPN Client to get all VPN settings automatically from the Zyxel Device. See Section 4.3 on page 82.Use **VPN Settings for L2TP VPN Settings** to configure the L2TP VPN for clients.

- Wizard Help

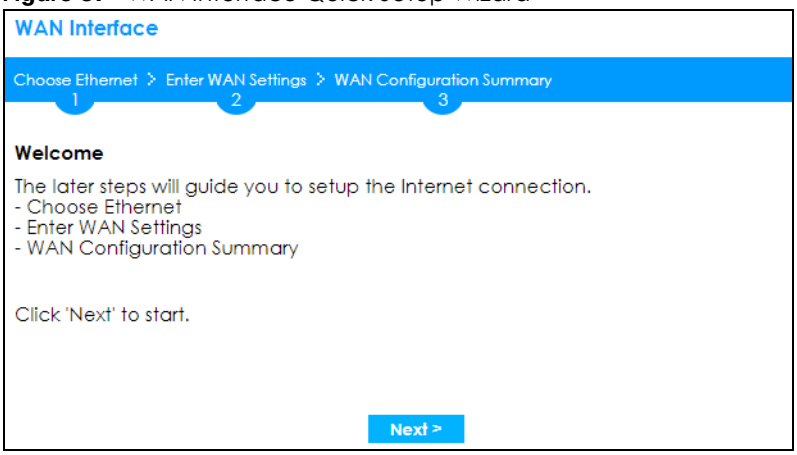
  If the help does not automatically display when you run the wizard, click the arrow to display it.



4.2 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**.

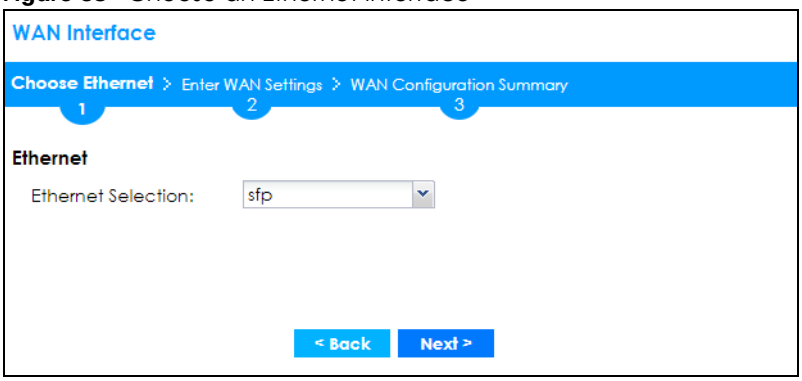
Figure 57 WAN Interface Quick Setup Wizard



4.2.1 Choose an Ethernet Interface

Select a WAN interface (names vary by model) that you want to configure for a WAN connection and click **Next**.

Figure 58 Choose an Ethernet Interface

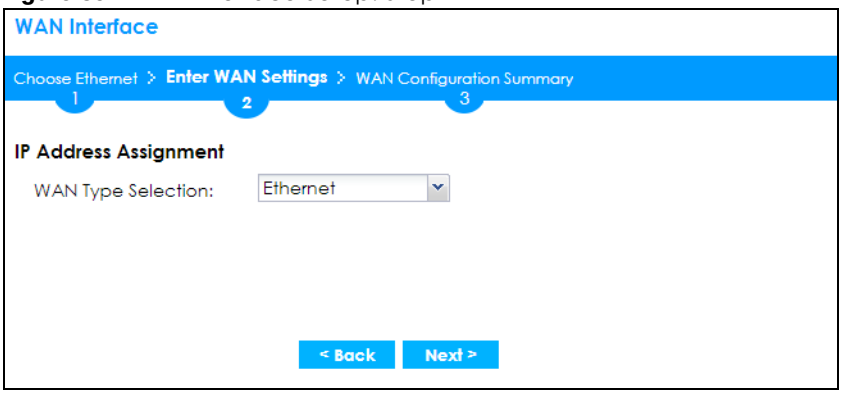


4.2.2 Select WAN Type

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**, **PPTP** or **L2TP** for a dial-up connection according to the information from your ISP.

Figure 59 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.

4.2.3 Configure WAN IP Settings

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

Figure 60 WAN Interface Setup: Step 2 Ethernet Dynamic IP

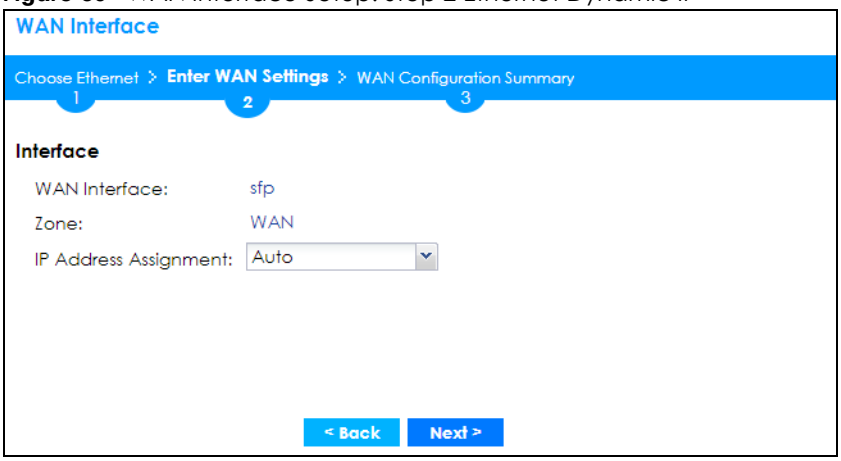
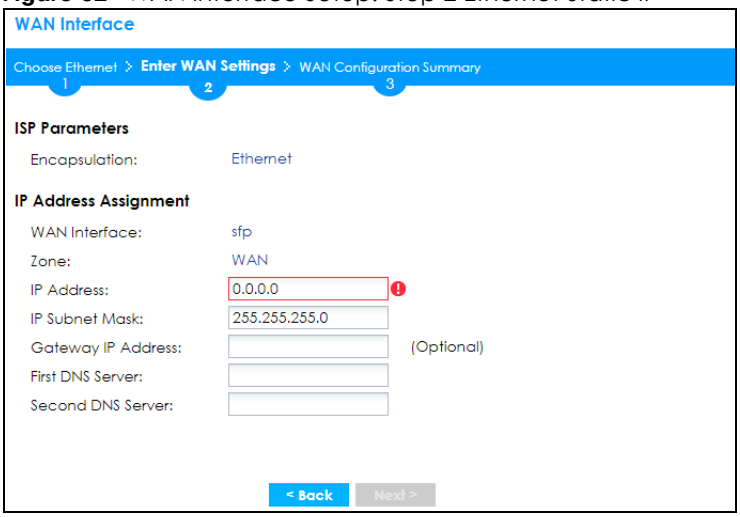


Figure 61 WAN Interface Setup: Step 2 Ethernet Static IP



- **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 and enter the IP address, subnet mask, gateway IP address (optional) and DNS server IP address(es).

4.2.4 ISP and WAN and ISP 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.

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

Figure 62 WAN and ISP Connection Settings: (PPTP)

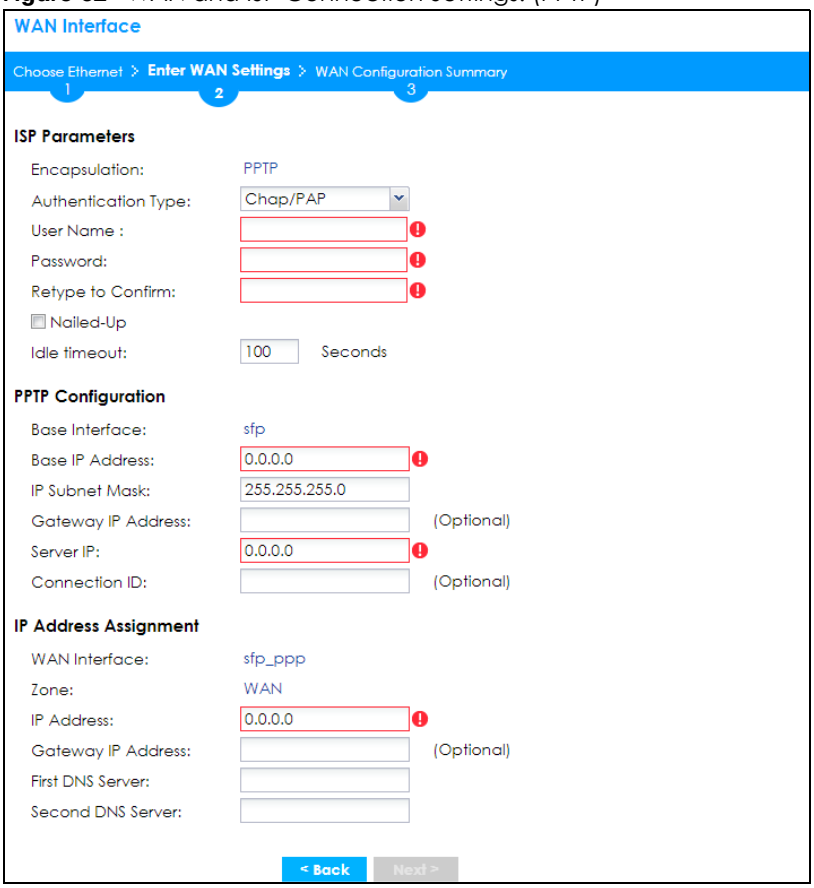


Figure 63 WAN and ISP Connection Settings: (PPPoE)

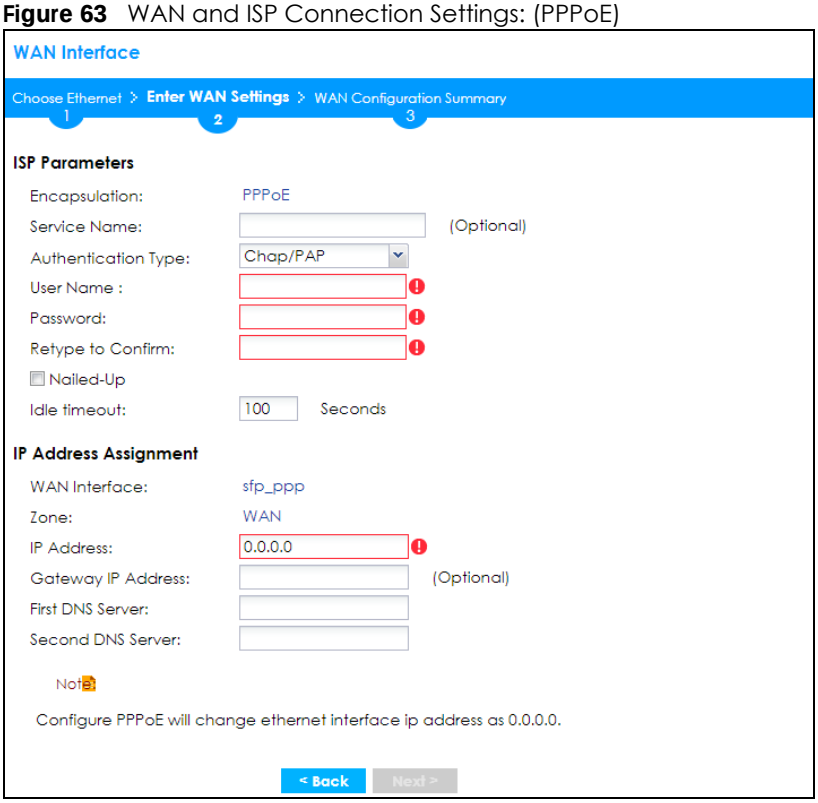
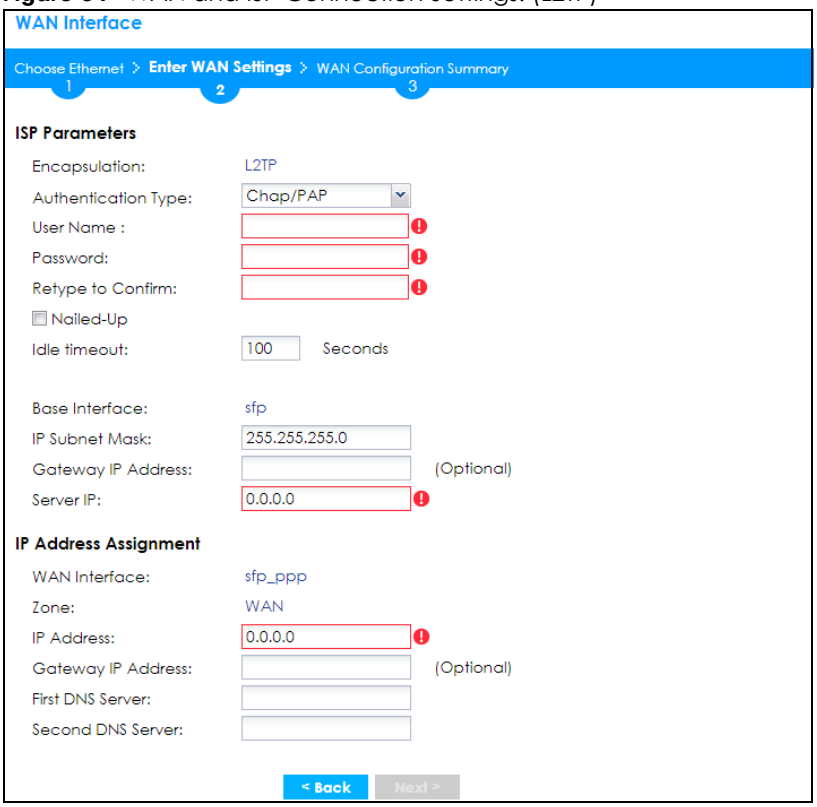


Figure 64 WAN and ISP Connection Settings: (L2TP)



- **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**: Type the PPPoE service name if you were given one by your ISP.
- **Authentication Type:** Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:
  - **CHAP/PAP** - Your Zyxel Device accepts either CHAP or PAP when requested by this remote node.
  - **CHAP** - Your Zyxel Device accepts CHAP only.
  - **PAP** - Your Zyxel Device accepts PAP only.
  - **MSCHAP** - Your Zyxel Device accepts MSCHAP only.
  - **MSCHAP-V2** - Your Zyxel Device 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.
- **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 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**: For PPTP or L2TP, type the gateway IP address if you were given one by your ISP.
- **Server IP**: Type the IP address of the PPTP server.
- **Connection ID:** Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your DSL modem. You can use alphanumeric and -_: characters, and it can be up to 31 characters long.

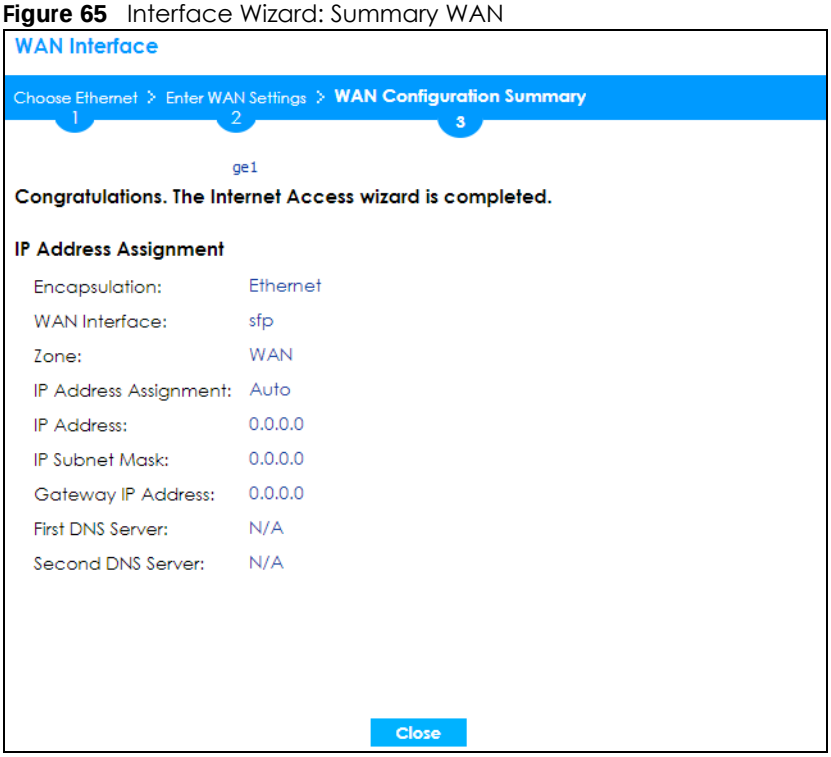
IP Address Assignment

- **WAN Interface**: This displays the identity of the interface you configure to connect with your ISP.
- **Zone**: This field displays to which security zone this interface and Internet connection will belong.
- **IP Address**: This field is read-only when the WAN interface uses a dynamic IP address. If your WAN interface uses a static IP address, enter it in this field.
- **IP Subnet Mask**: If your WAN interface uses Ethernet encapsulation with a static IP address, enter the subnet mask in this field.
- **Gateway IP Address**: Type the IP address of the Ethernet device connected to this WAN port.
- **First DNS Server / Second DNS Server**: These fields only display for an interface with a static IP address. Enter the DNS server IP address(es) in the field(s) to the right. Leave the field as **0.0.0.0** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.

4.2.5 Quick Setup Interface Wizard: Summary

This screen displays an example WAN interface's settings.

Figure 65 Interface Wizard: Summary WAN



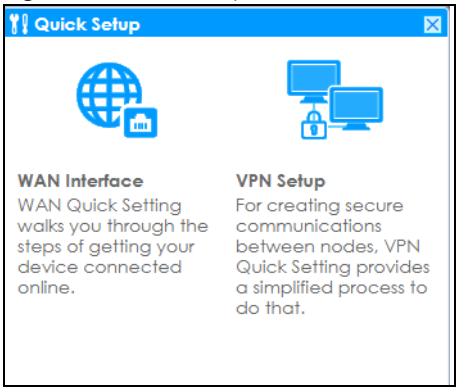
- **Encapsulation**: This displays what encapsulation this interface uses to connect to the Internet.

- **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 Zyxel Device 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 current IP address of the Zyxel Device WAN interface selected in this wizard.
- **IP Subnet Mask**: This field displays the subnet mask of the Zyxel Device WAN interface selected in this wizard.
- **Gateway IP Address:** This field displays the IP address of the Ethernet device connected to this WAN port.
- **First DNS Server /Second DNS Server**: If the **IP Address Assignment** is **Static**, these fields display the DNS server IP address(es).

4.3 VPN Setup Wizard

Click **VPN Setup** in the main **Quick Setup** screen to open the VPN Setup Wizard **Welcome** screen.

Figure 66 VPN Setup Wizard



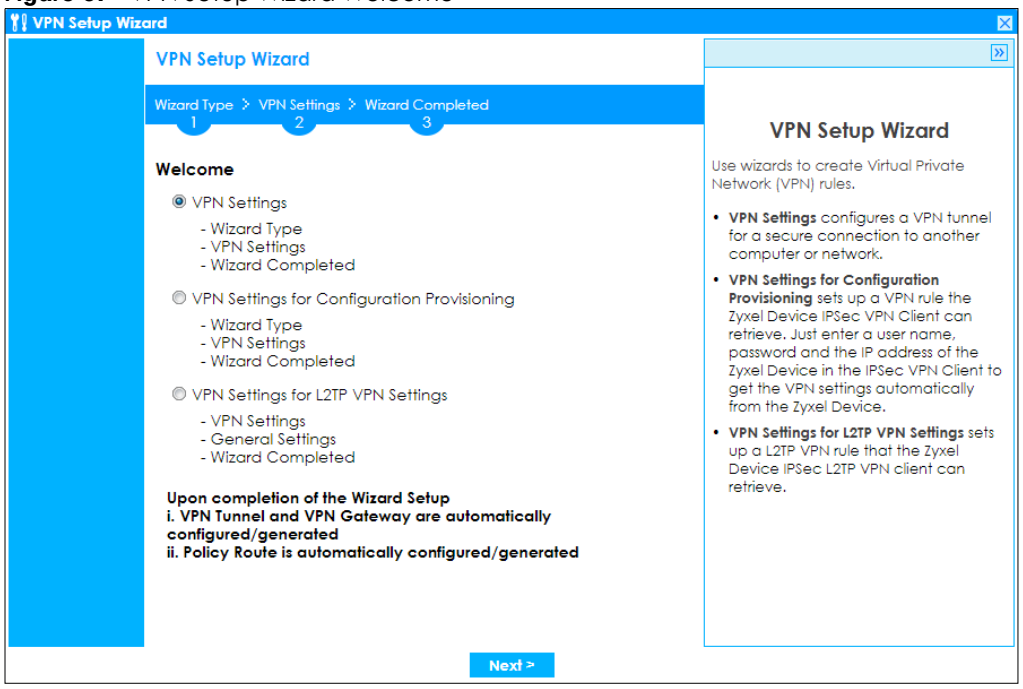
4.3.1 Welcome

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

- **VPN Settings** configures a VPN tunnel for a secure connection to another computer or network.

- **VPN Settings for Configuration Provisioning** sets up a VPN rule the Zyxel Device IPSec VPN Client can retrieve. Just enter a user name, password and the IP address of the Zyxel Device in the IPSec VPN Client to get the VPN settings automatically from the Zyxel Device.
- **VPN Settings for L2TP VPN Settings** sets up a L2TP VPN rule that the Zyxel Device IPSec L2TP VPN client can retrieve.

Figure 67 VPN Setup Wizard Welcome

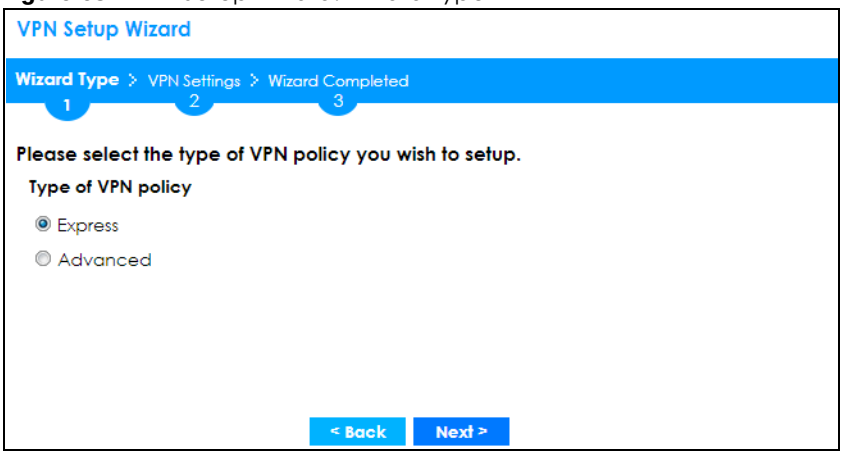


4.3.2 VPN Setup Wizard: Wizard Type

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings to connect to another ZLD-based Zyxel Device 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.

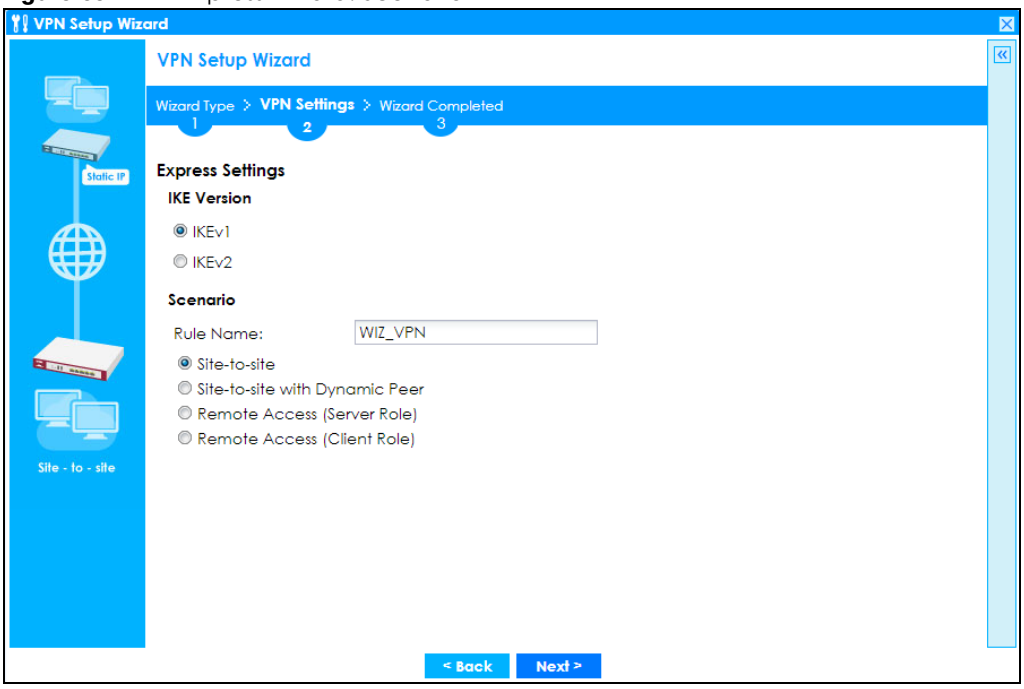
Figure 68 VPN Setup Wizard: Wizard Type



4.3.3 VPN Express Wizard - Scenario

Click the **Express** radio button as shown in Figure 68 on page 83 to display the following screen.

Figure 69 VPN Express Wizard: Scenario



IKE (Internet Key Exchange) Version: IKEv1 and IKEv2

IKE (Internet Key Exchange) is a protocol used in security associations to send data securely. IKE uses certificates or pre-shared keys for authentication and a Diffie–Hellman key exchange to set up a shared session secret from which encryption keys are derived.

IKEv2 supports Extended Authentication Protocol (EAP) authentication, and IKEv1 supports X-Auth. EAP is important when connecting to existing enterprise authentication systems.

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.

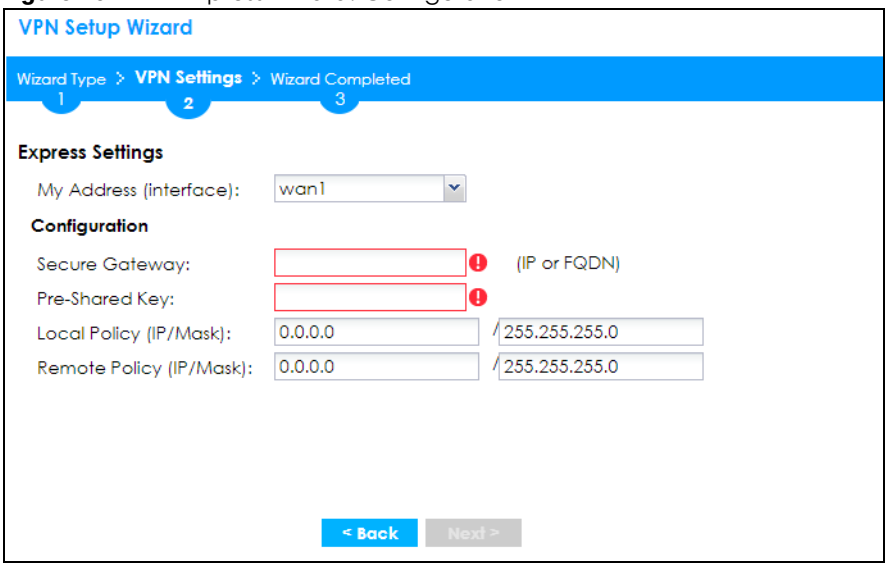
Select the scenario that best describes your intended VPN connection. The figure on the left of the screen changes to match the scenario you select.

- **Site-to-site** - The remote IPSec device has a static IP address or a domain name. This Zyxel Device can initiate the VPN tunnel.
- **Site-to-site with Dynamic Peer** - The remote IPSec device has a dynamic IP address. Only the remote IPSec device can initiate the VPN tunnel.
- **Remote Access (Server Role)** - Allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel.

- **Remote Access (Client Role)** - Connect to an IPSec server. This Zyxel Device is the client (dial-in user) and can initiate the VPN tunnel.

4.3.4 VPN Express Wizard - Configuration

Figure 70 VPN Express Wizard: Configuration

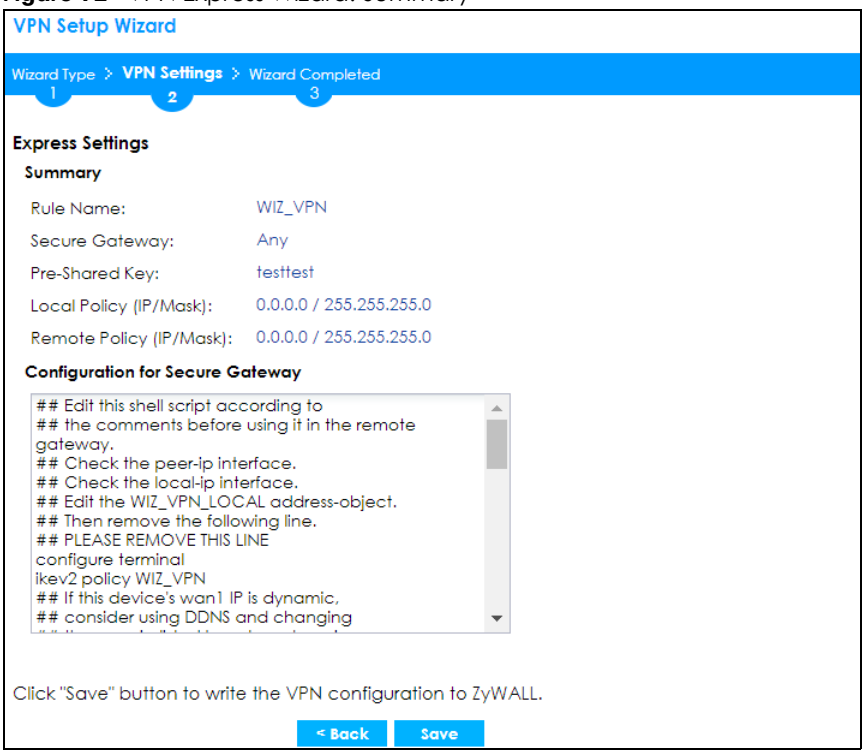


- **My Address (interface)**: Select an interface from the drop-down list box to use on your Zyxel Device.
- **Secure Gateway**: **Any** displays in this field if it is not configurable for the chosen scenario. Otherwise, enter the WAN IP address or domain name of the remote IPSec device (secure gateway) to identify the remote IPSec router by its IP address or a domain name. Use 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address.
- **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)**: **Any** displays in this field if it is not configurable for the chosen scenario. Otherwise, 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.

4.3.5 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 Zyxel Device's command line interface to configure it.

Figure 71 VPN Express Wizard: Summary

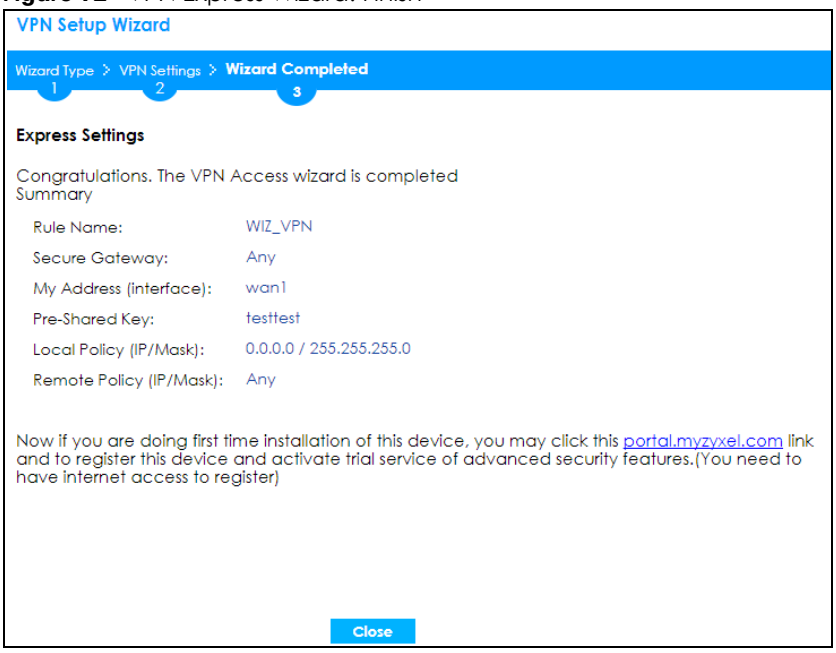


- **Rule Name**: Identifies the VPN gateway policy.
- **Secure Gateway**: IP address or domain name of the remote IPSec device. If this field displays **Any**, only the remote IPSec device can initiate the VPN connection.
- **Pre-Shared Key**: VPN tunnel password. It identifies a communicating party during a phase 1 IKE negotiation.
- **Local Policy**: IP address and subnet mask of the computers on the network behind your Zyxel Device 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. If this field displays **Any**, only the remote IPSec device can initiate the VPN connection.
- Copy and paste the **Configuration for Secure Gateway** commands into another ZLD-based Zyxel Device'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.

4.3.6 VPN Express Wizard - Finish

Now the rule is configured on the Zyxel Device. 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 72 VPN Express Wizard: Finish

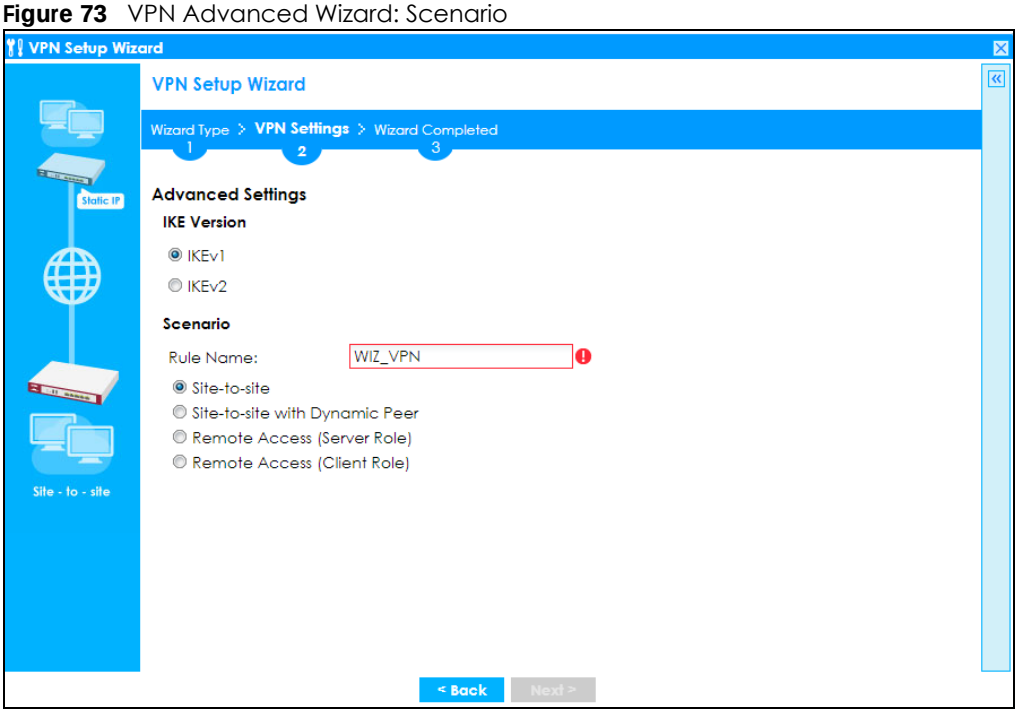


Click **Close** to exit the wizard.

4.3.7 VPN Advanced Wizard - Scenario

Click the **Advanced** radio button as shown in Figure 68 on page 83 to display the following screen.

Figure 73 VPN Advanced Wizard: Scenario



IKE (Internet Key Exchange) Version: IKEv1 and IKEv2

IKE (Internet Key Exchange) is a protocol used in security associations to send data securely. IKE uses certificates or pre-shared keys for authentication and a Diffie–Hellman key exchange to set up a shared session secret from which encryption keys are derived.

IKEv2 supports Extended Authentication Protocol (EAP) authentication, and IKEv1 supports X-Auth. EAP is important when connecting to existing enterprise authentication systems.

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.

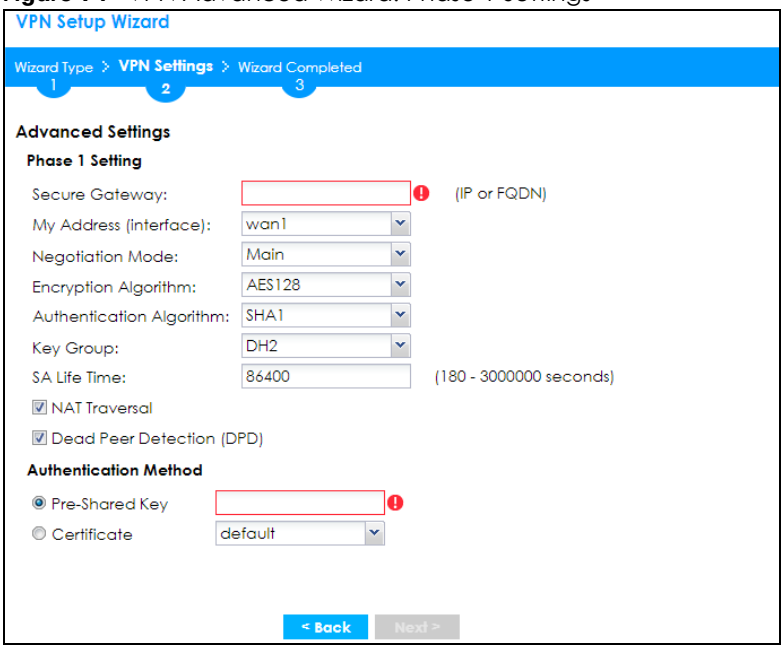
Select the scenario that best describes your intended VPN connection. The figure on the left of the screen changes to match the scenario you select.

- **Site-to-site** - The remote IPSec device has a static IP address or a domain name. This Zyxel Device can initiate the VPN tunnel.
- **Site-to-site with Dynamic Peer** - The remote IPSec device has a dynamic IP address. Only the remote IPSec device can initiate the VPN tunnel.
- **Remote Access (Server Role)** - Allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel.
- **Remote Access (Client Role)** - Connect to an IPSec server. This Zyxel Device is the client (dial-in user) and can initiate the VPN tunnel.

4.3.8 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 74 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 Zyxel Device.
- **Negotiation Mode**: This displays **Main** or **Aggressive**:
  - **Main** encrypts the ZyWALL/USG's and remote IPSec router's identities but takes more time to establish the IKE SA
  - **Aggressive** is faster but does not encrypt the identities.

The ZyWALL/USG and the remote IPSec router must use the same negotiation mode. 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 Zyxel Device 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).

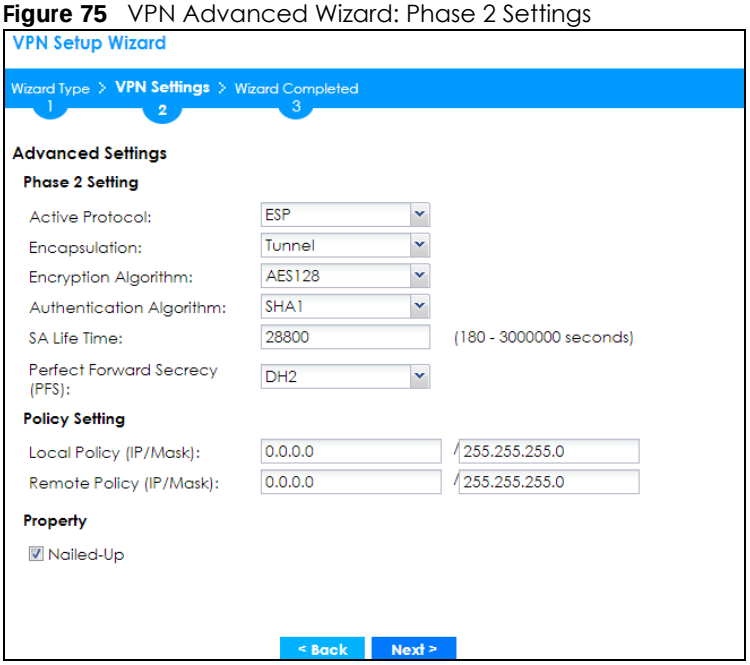
Note: The remote IPSec device must also have NAT traversal enabled. See the help in the main IPSec VPN screens for more information.

- **Dead Peer Detection (DPD)** has the Zyxel Device 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 Zyxel Device sends a message to the remote IPSec device. If it responds, the Zyxel Device transmits the data. If it does not respond, the Zyxel Device shuts down the IKE SA.
- **Authentication Method**: Select **Pre-Shared Key** to use a password or **Certificate** to use one of the Zyxel Device's certificates.

4.3.9 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 75 VPN Advanced Wizard: Phase 2 Settings



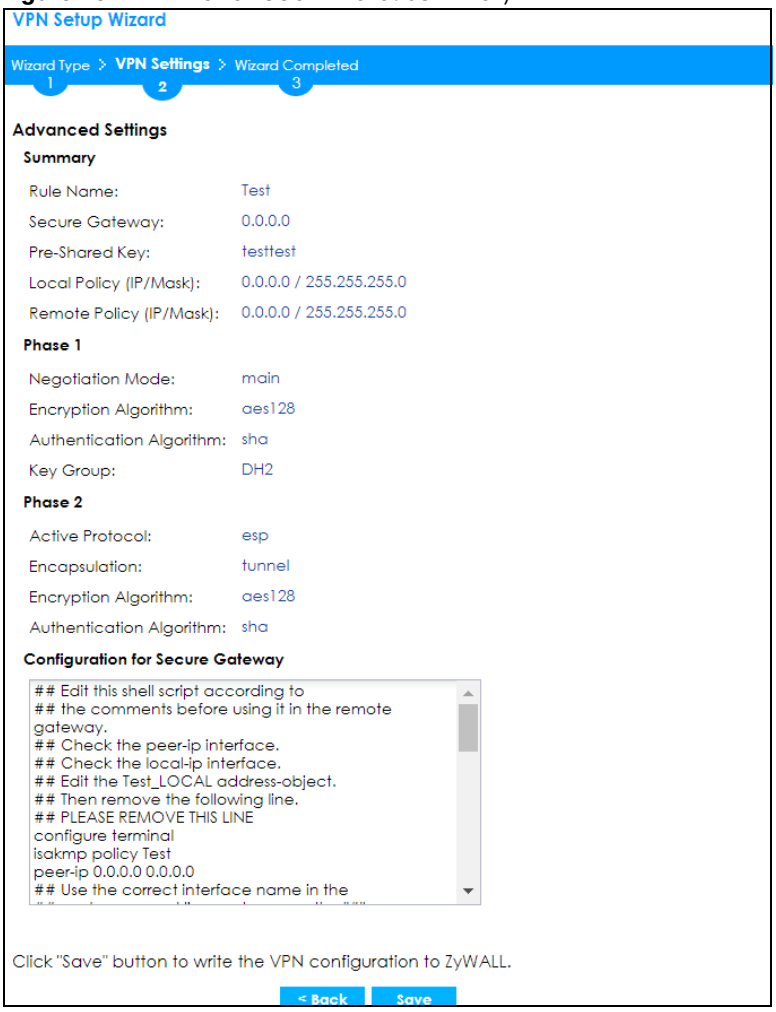
- **Active Protocol**: **ESP** is compatible with NAT, **AH** is not.
- **Encapsulation**: **Tunnel** is compatible with NAT, **Transport** is not.
- **Encryption Algorithm**: **3DES** and **AES** use encryption. The longer the **AES** key, the higher the security (this may affect throughput). **Null** 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 Zyxel Device 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 Zyxel Device automatically renegotiate the IPSec SA when the SA life time expires.

4.3.10 VPN Advanced Wizard - Summary

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

Figure 76 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 Zyxel Device 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 Zyxel Device 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.

Phase 1

- **Negotiation Mode**: This displays **Main** or **Aggressive**:
  - **Main** encrypts the ZyWALL/USG's and remote IPSec router's identities but takes more time to establish the IKE SA
  - **Aggressive** is faster but does not encrypt the identities.

The ZyWALL/USG and the remote IPSec router must use the same negotiation mode. Multiple SAs connecting through a secure gateway must have the same negotiation mode.

- **Encryption Algorithm**: This displays the encryption method used. The longer the key, the higher the security, the lower the throughput (possibly).
  - **DES** uses a 56-bit key.
  - **3DES** uses a 168-bit key.
  - **AES128** uses a 128-bit key
  - **AES192** uses a 192-bit key
  - **AES256** uses a 256-bit key.
- **Authentication Algorithm**: This displays the authentication algorithm used. The stronger the algorithm, the slower it is.
  - **MD5** gives minimal security.
  - **SHA1** gives higher security
  - **SHA256** gives the highest security.
- **Key Group**: This displays the Diffie-Hellman (DH) key group used. **DH5** is more secure than **DH1** or **DH2** (although it may affect throughput).
  - **DH1** uses a 768 bit random number.
  - **DH2** uses a 1024 bit (1Kb) random number.
  - **DH5** uses a 1536 bit random number.

Phase 2

- **Active Protocol**: This displays **ESP** (compatible with NAT) or **AH**.
- **Encapsulation**: This displays **Tunnel** (compatible with NAT) or **Transport**.
- **Encryption Algorithm**: This displays the encryption method used. The longer the key, the higher the security, the lower the throughput (possibly).
  - **DES** uses a 56-bit key.
  - **3DES** uses a 168-bit key.
  - **AES128** uses a 128-bit key
  - **AES192** uses a 192-bit key
  - **AES256** uses a 256-bit key.
  - **Null** uses no encryption.
- **Authentication Algorithm**: This displays the authentication algorithm used. The stronger the algorithm, the slower it is.
  - **MD5** gives minimal security.
  - **SHA1** gives higher security
  - **SHA256** gives the highest security.

Copy and paste the **Configuration for Remote Gateway** commands into another ZLD-based Zyxel Device's command line interface.

Click **Save** to save the VPN rule.

4.3.11 VPN Advanced Wizard - Finish

Now the rule is configured on the Zyxel Device. 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 77 VPN Wizard: Finish

Click **Close** to exit the wizard.

4.4 VPN Settings for Configuration Provisioning Wizard: Wizard Type

Use VPN Settings for Configuration Provisioning to set up a VPN rule that can be retrieved with the Zyxel Device IPSec VPN Client.

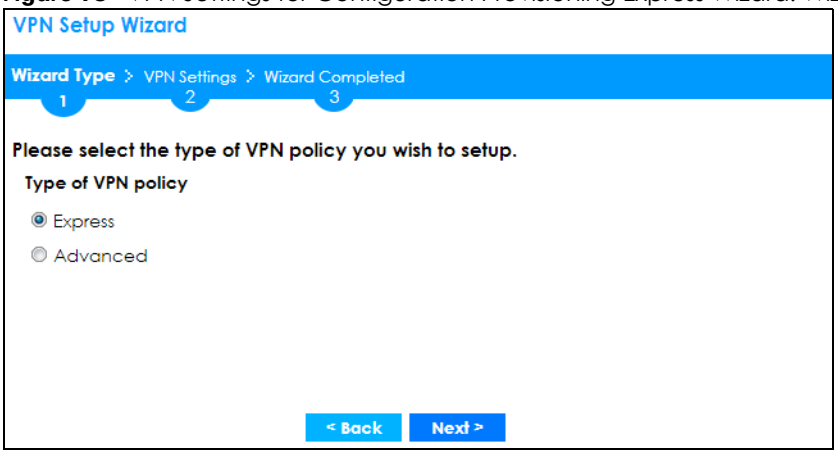
VPN rules for the Zyxel Device IPSec VPN Client have certain restrictions. They must *not* contain the following settings:

- **AH** active protocol
- **NULL** encryption
- **SHA512** authentication
- A subnet or range remote policy

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and to use a pre-shared key.

Choose **Advanced** to change the default settings and/or use certificates instead of a pre-shared key in the VPN rule.

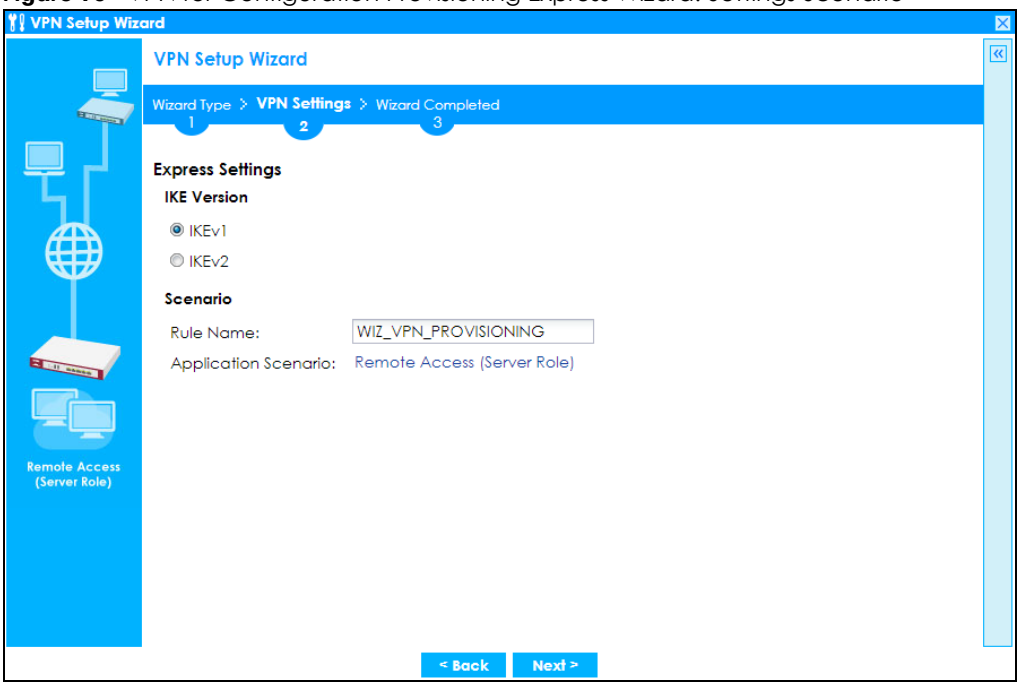
Figure 78 VPN Settings for Configuration Provisioning Express Wizard: Wizard Type



4.4.1 Configuration Provisioning Express Wizard - VPN Settings

Click the **Express** radio button as shown in the previous screen to display the following screen.

Figure 79 VPN for Configuration Provisioning Express Wizard: Settings Scenario

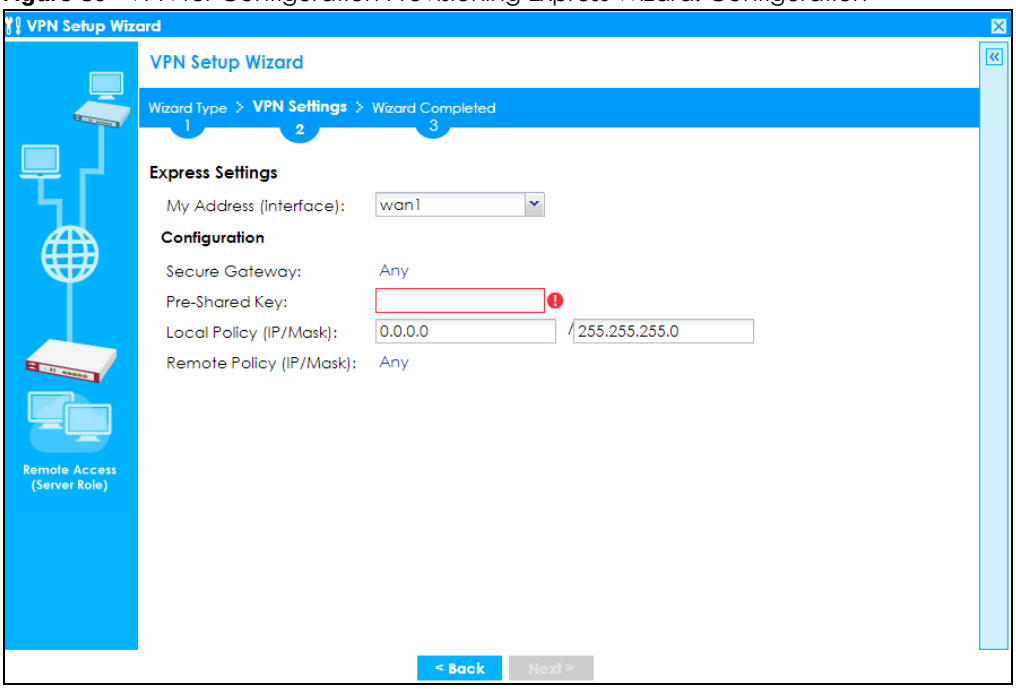


- **IKE** (Internet Key Exchange) is a protocol used in security associations to send data securely. IKE uses certificates or pre-shared keys for authentication and a Diffie–Hellman key exchange to set up a shared session secret from which encryption keys are derived.
- **IKEv2** supports Extended Authentication Protocol (EAP) authentication, and IKEv1 supports X-Auth. EAP is important when connecting to existing enterprise authentication systems.
- **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**: Only the **Remote Access (Server Role)** is allowed in this wizard. It allows incoming connections from the Zyxel Device IPSec VPN Client.

4.4.2 Configuration Provisioning VPN Express Wizard - Configuration

Click **Next** to continue the wizard.

Figure 80 VPN for Configuration Provisioning Express Wizard: Configuration

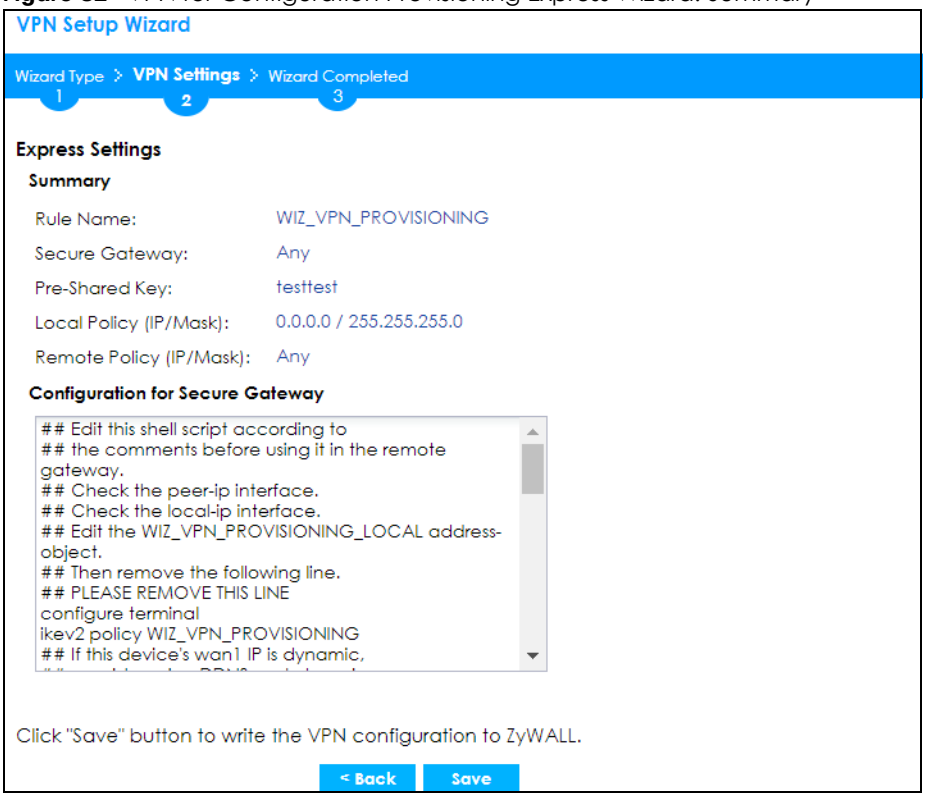


- **My Address (interface)**: Select an interface from the drop-down list box to use on your Zyxel Device.
- **Secure Gateway**: **Any** displays in this field because it is not configurable in this wizard. It allows incoming connections from the Zyxel Device IPSec VPN Client.
- **Pre-Shared Key**: Type 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. You can also specify a subnet. This must match the remote IP address configured on the remote IPSec device.
- **Remote Policy (IP/Mask)**: **Any** displays in this field because it is not configurable in this wizard.

4.4.3 VPN Settings for Configuration Provisioning Express Wizard - Summary

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

Figure 81 VPN for Configuration Provisioning Express Wizard: Summary

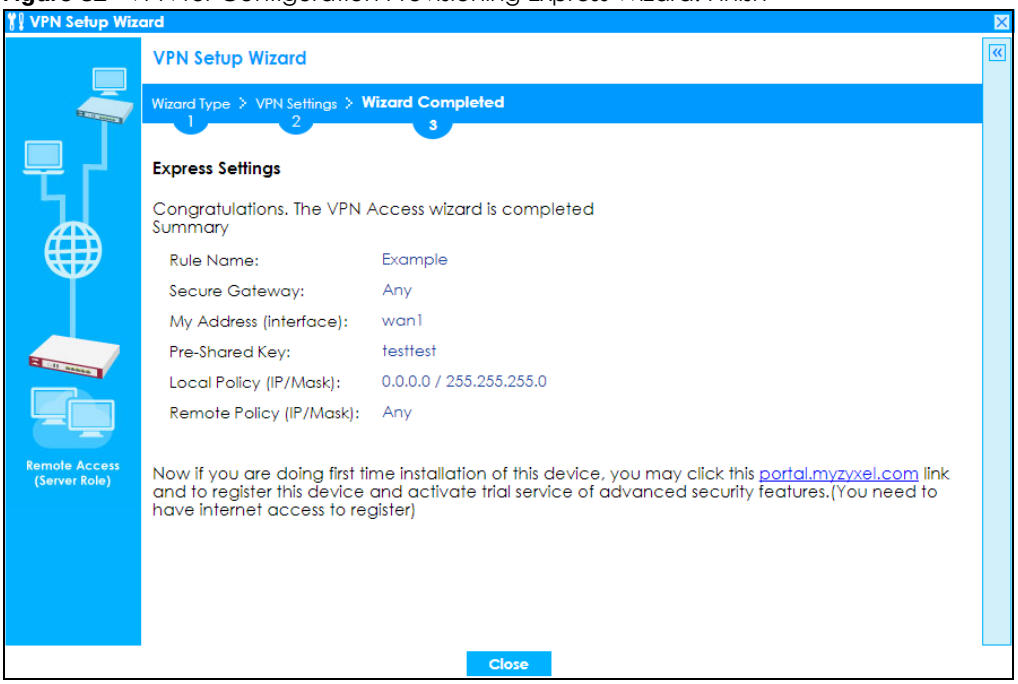


- **Rule Name**: Identifies the VPN gateway policy.
- **Secure Gateway**: **Any** displays in this field because it is not configurable in this wizard. It allows incoming connections from the Zyxel Device IPSec VPN Client.
- **Pre-Shared Key**: VPN tunnel password. It identifies a communicating party during a phase 1 IKE negotiation.
- **Local Policy**: (Static) IP address and subnet mask of the computers on the network behind your Zyxel Device that can be accessed using the tunnel.
- **Remote Policy**: **Any** displays in this field because it is not configurable in this wizard.
- The **Configuration for Secure Gateway** displays the configuration that the Zyxel Device IPSec VPN Client will get from the Zyxel Device.
- Click **Save** to save the VPN rule.

4.4.4 VPN Settings for Configuration Provisioning Express Wizard - Finish

Now the rule is configured on the Zyxel Device. The Phase 1 rule settings appear in the **Configuration > VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **Configuration > VPN > IPSec VPN > VPN Connection** screen. Enter the IP address of the Zyxel Device in the Zyxel Device IPSec VPN Client to get all these VPN settings automatically from the Zyxel Device.

Figure 82 VPN for Configuration Provisioning Express Wizard: Finish

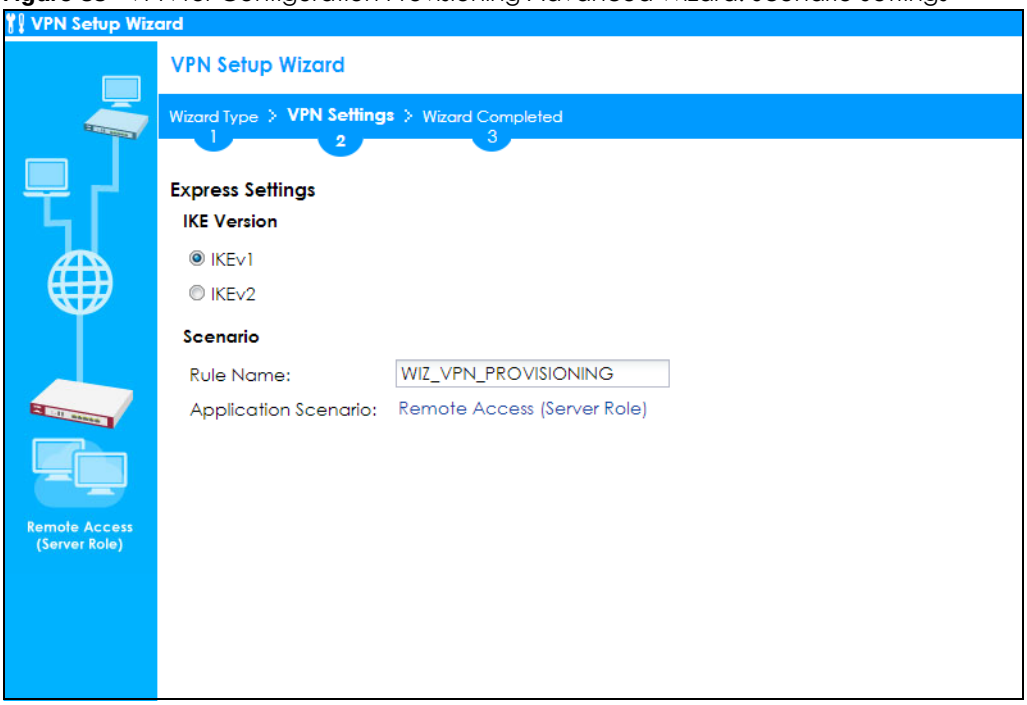


Click **Close** to exit the wizard.

4.4.5 VPN Settings for Configuration Provisioning Advanced Wizard - Scenario

Click the **Advanced** radio button as shown in the screen shown in Figure 78 on page 94 to display the following screen.

Figure 83 VPN for Configuration Provisioning Advanced Wizard: Scenario Settings



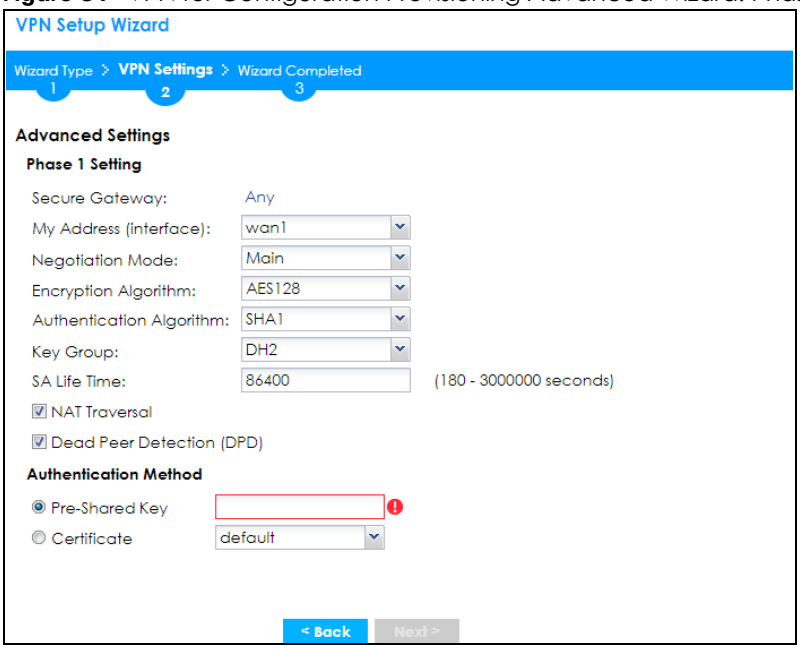
- **IKE** (Internet Key Exchange) is a protocol used in security associations to send data securely. IKE uses certificates or pre-shared keys for authentication and a Diffie–Hellman key exchange to set up a shared session secret from which encryption keys are derived.
- **IKEv2** supports Extended Authentication Protocol (EAP) authentication, and IKEv1 supports X-Auth. EAP is important when connecting to existing enterprise authentication systems.
- **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**: Only the **Remote Access (Server Role)** is allowed in this wizard. It allows incoming connections from the Zyxel Device IPSec VPN Client.

Click **Next** to continue the wizard.

4.4.6 VPN Settings for Configuration Provisioning 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 84 VPN for Configuration Provisioning Advanced Wizard: Phase 1 Settings



- **Secure Gateway**: **Any** displays in this field because it is not configurable in this wizard. It allows incoming connections from the Zyxel Device IPSec VPN Client.
- **My Address (interface)**: Select an interface from the drop-down list box to use on your Zyxel Device.
- **Negotiation Mode**: This displays **Main** or **Aggressive**:
  - **Main** encrypts the ZyWALL/USG's and remote IPSec router's identities but takes more time to establish the IKE SA
  - **Aggressive** is faster but does not encrypt the identities.

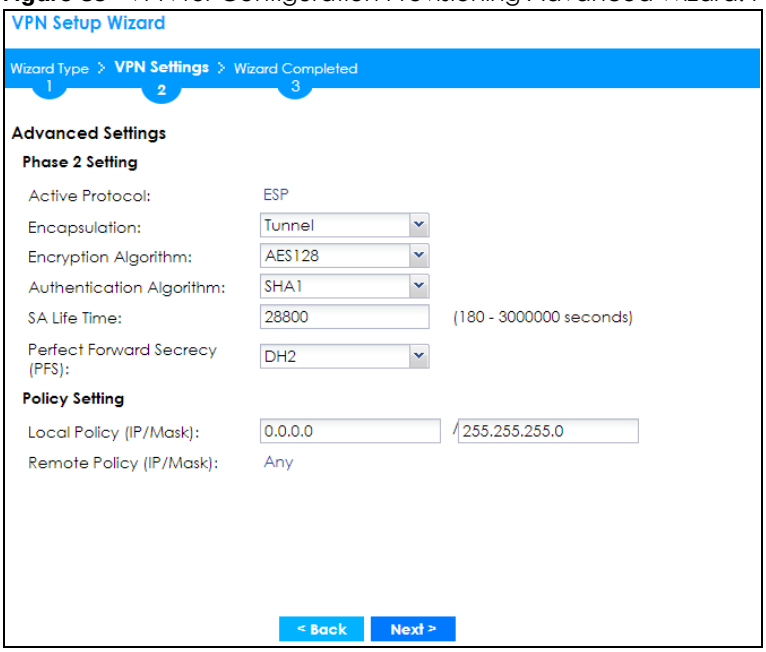
The ZyWALL/USG and the remote IPSec router must use the same negotiation mode. Multiple SAs connecting through a secure gateway must have the same negotiation mode.

- **Encryption Algorithm**: **3DES** and **AES** use encryption. The longer the key, the higher the security (this may affect throughput). Both sender and receiver must know 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 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. **MD5** gives minimal security. **SHA1** gives higher security and **SHA256** gives the highest security. 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 Zyxel Device renegotiates the IKE SA. A short SA life time increases security, but renegotiation temporarily disconnects the VPN tunnel.
- **Authentication Method**: Select **Pre-Shared Key** to use a password or **Certificate** to use one of the Zyxel Device's certificates.

4.4.7 VPN Settings for Configuration Provisioning Advanced Wizard - Phase 2

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

Figure 85 VPN for Configuration Provisioning Advanced Wizard: Phase 2 Settings

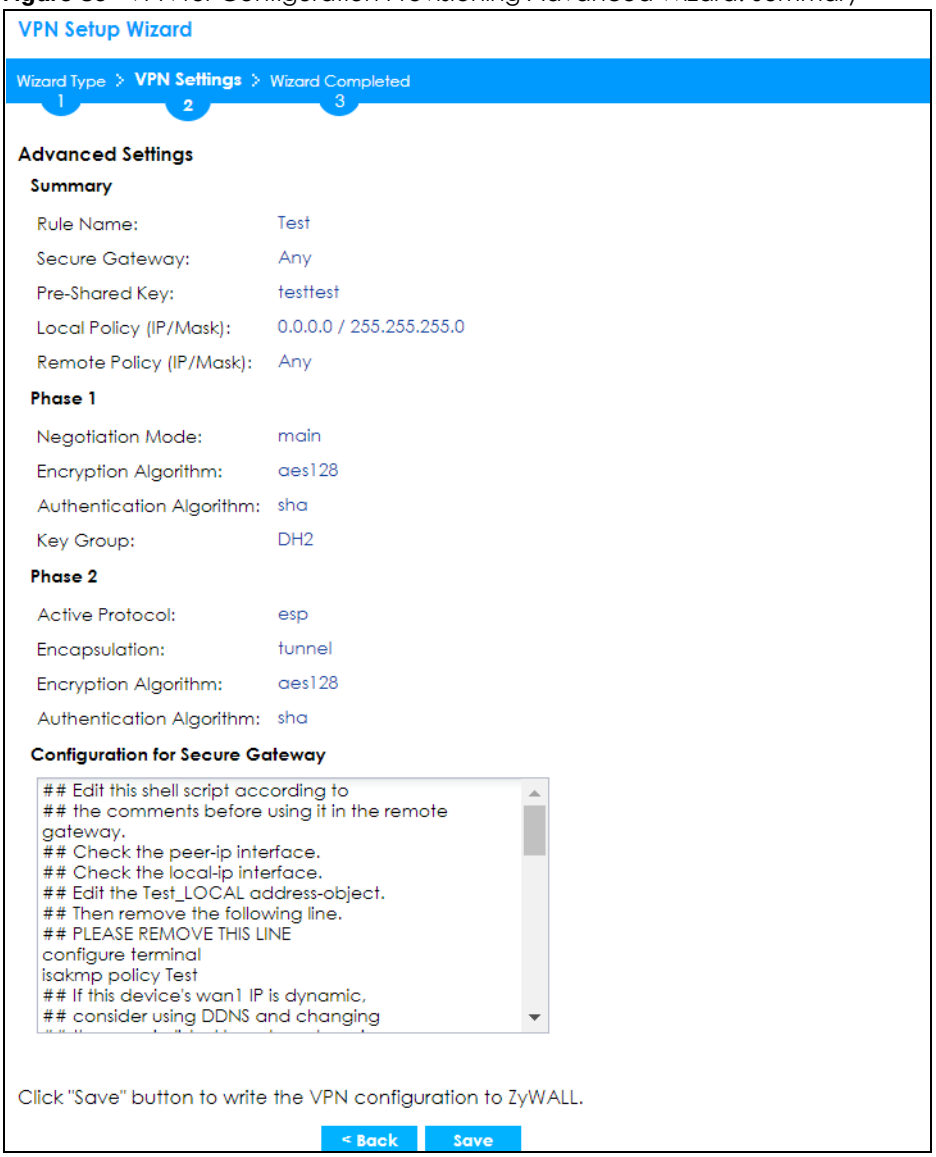


- **Active Protocol**: **ESP** is compatible with NAT. **AH** is not available in this wizard.
- **Encapsulation**: **Tunnel** is compatible with NAT, **Transport** is not.
- **Encryption Algorithm**: **3DES** and **AES** use encryption. The longer the **AES** key, the higher the security (this may affect throughput). **Null** uses no encryption.
- **Authentication Algorithm**: MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. **MD5** gives minimal security. **SHA1** gives higher security and **SHA256** gives the highest security. The stronger the algorithm, the slower it is.
- **SA Life Time**: Set how often the Zyxel Device 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)**: A**ny** displays in this field because it is not configurable in this wizard.
- **Nailed-Up**: This displays for the site-to-site and remote access client role scenarios. Select this to have the Zyxel Device automatically renegotiate the IPSec SA when the SA life time expires.

4.4.8 VPN Settings for Configuration Provisioning Advanced Wizard - Summary

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

Figure 86 VPN for Configuration Provisioning Advanced Wizard: Summary



Summary

- **Rule Name**: Identifies the VPN connection (and the VPN gateway).
- **Secure Gateway**: A**ny** displays in this field because it is not configurable in this wizard. It allows incoming connections from the Zyxel Device IPSec VPN Client.
- **Pre-Shared Key**: VPN tunnel password.
- **Local Policy**: IP address and subnet mask of the computers on the network behind your Zyxel Device that can use the tunnel.
- **Remote Policy**: **Any** displays in this field because it is not configurable in this wizard.

Phase 1

- **Negotiation Mode**: This displays **Main** or **Aggressive**:
  - **Main** encrypts the ZyWALL/USG's and remote IPSec router's identities but takes more time to establish the IKE SA

- **Aggressive** is faster but does not encrypt the identities.

The ZyWALL/USG and the remote IPSec router must use the same negotiation mode. Multiple SAs connecting through a secure gateway must have the same negotiation mode.

- **Encryption Algorithm**: This displays the encryption method used. The longer the key, the higher the security, the lower the throughput (possibly).
  - **DES** uses a 56-bit key.
  - **3DES** uses a 168-bit key.
  - **AES128** uses a 128-bit key
  - **AES192** uses a 192-bit key
  - **AES256** uses a 256-bit key.
- **Authentication Algorithm**: This displays the authentication algorithm used. The stronger the algorithm, the slower it is.
  - **MD5** gives minimal security.
  - **SHA1** gives higher security
  - **SHA256** gives the highest security.
- **Key Group**: This displays the Diffie-Hellman (DH) key group used. **DH5** is more secure than **DH1** or **DH2** (although it may affect throughput).
  - **DH1** uses a 768 bit random number.
  - **DH2** uses a 1024 bit (1Kb) random number.
  - **DH5** uses a 1536 bit random number.

Phase 2

- **Active Protocol**: This displays **ESP** (compatible with NAT) or **AH**.
- **Encapsulation**: This displays **Tunnel** (compatible with NAT) or **Transport**.
- **Encryption Algorithm**: This displays the encryption method used. The longer the key, the higher the security, the lower the throughput (possibly).
  - **DES** uses a 56-bit key.
  - **3DES** uses a 168-bit key.
  - **AES128** uses a 128-bit key
  - **AES192** uses a 192-bit key
  - **AES256** uses a 256-bit key.
  - **Null** uses no encryption.
- **Authentication Algorithm**: This displays the authentication algorithm used. The stronger the algorithm, the slower it is.
  - **MD5** gives minimal security.
  - **SHA1** gives higher security
  - **SHA256** gives the highest security.

The **Configuration for Secure Gateway** displays the configuration that the Zyxel Device IPSec VPN Client will get from the Zyxel Device.

Click **Save** to save the VPN rule.

4.4.9 VPN Settings for Configuration Provisioning Advanced Wizard- Finish

Now the rule is configured on the Zyxel Device. 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. Enter the IP address of the Zyxel Device in the Zyxel Device IPSec VPN Client to get all these VPN settings automatically from the Zyxel Device.

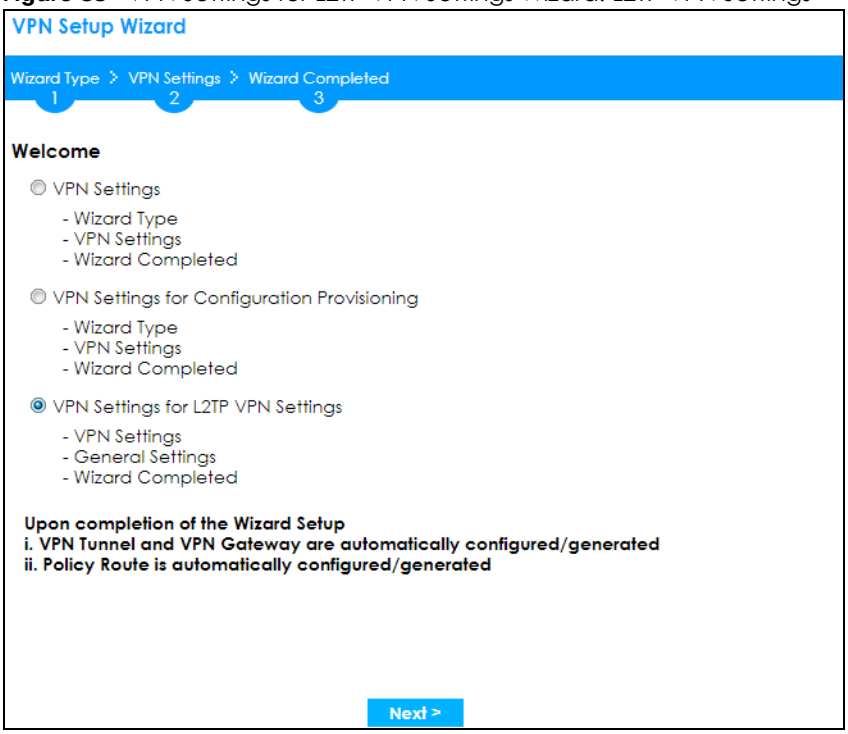
Figure 87 VPN for Configuration Provisioning Advanced Wizard: Finish

Click **Close** to exit the wizard.

4.5 VPN Settings for L2TP VPN Settings Wizard

Use **VPN Settings for L2TP VPN Settings** to set up an L2TP VPN rule. Click **Configuration > Quick Setup > VPN Setup** and select **VPN Settings for L2TP VPN Settings** to see the following screen.

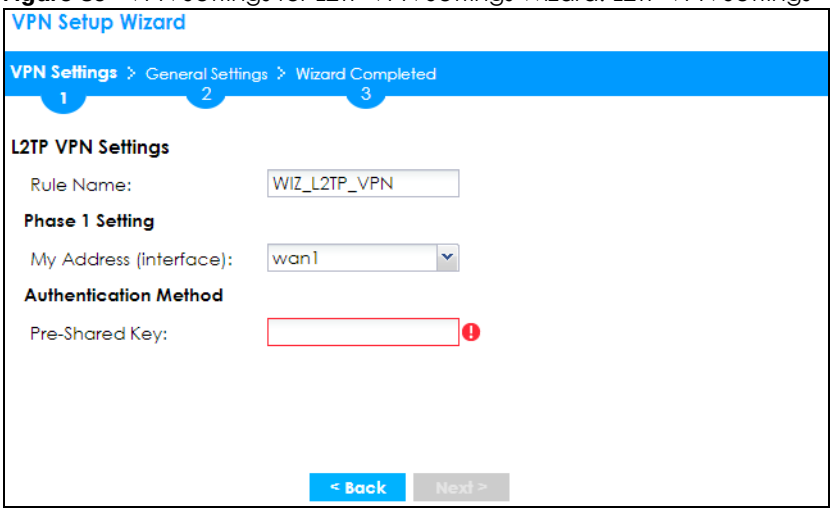
Figure 88 VPN Settings for L2TP VPN Settings Wizard: L2TP VPN Settings



Click **Next** to continue the wizard.

4.5.1 L2TP VPN Settings

Figure 89 VPN Settings for L2TP VPN Settings Wizard: L2TP VPN Settings

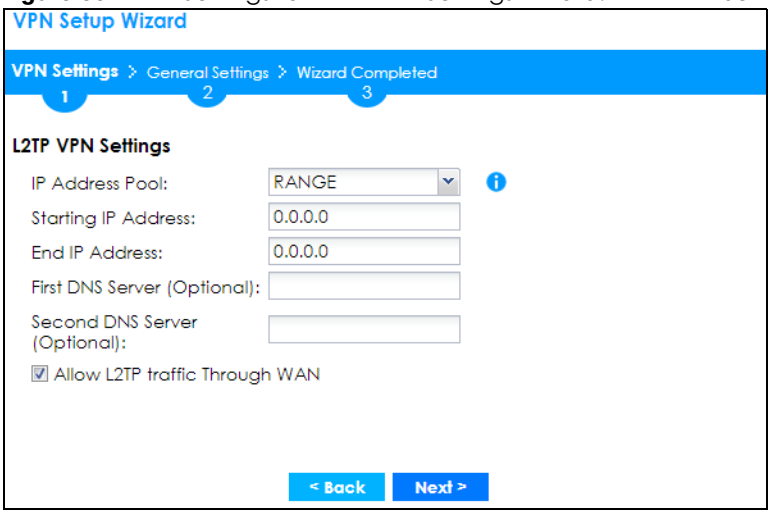


- **Rule Name**: Type the name used to identify this L2TP VPN connection (and L2TP VPN gateway). You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
- **My Address (interface)**: Select one of the interfaces from the pull down menu to apply the L2TP VPN rule.

- **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.
- Click **Next** to continue the wizard.

4.5.2 L2TP VPN Settings

Figure 90 VPN Settings for L2TP VPN Settings Wizard: L2TP VPN Settings



- **IP Address Pool**: Select Range or Subnet from the pull down menu. This IP address pool is used to assign to the L2TP VPN clients.
- **Starting IP Address**: Enter the starting IP address in the field.
- **End IP Address**: Enter the ending IP address in the field.
- **Network**: Enter the IPv4 IP address in this field if you selected **SUBNET**.
- **Netmask**: Enter the associated subnet mask of the subnet in this field.
- **First DNS Server (Optional)**: Enter the first DNS server IP address in the field. Leave the filed 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.
- **Second DNS Server (Optional)**: Enter the second DNS server IP address in the field. Leave the filed 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.
- **Allow L2TP traffic Through WAN**: Select this check box to allow traffic from L2TP clients to go to the Internet.

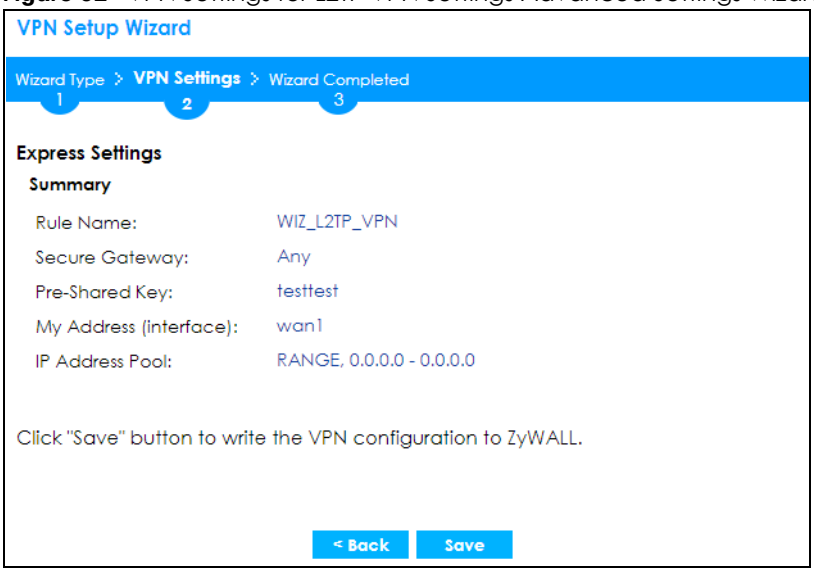
Click **Next** to continue the wizard.

Note: 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 Zyxel Device uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.

4.5.3 VPN Settings for L2TP VPN Setting Wizard - Summary

This is a read-only summary of the L2TP VPN settings.

Figure 91 VPN Settings for L2TP VPN Settings Advanced Settings Wizard: Summary

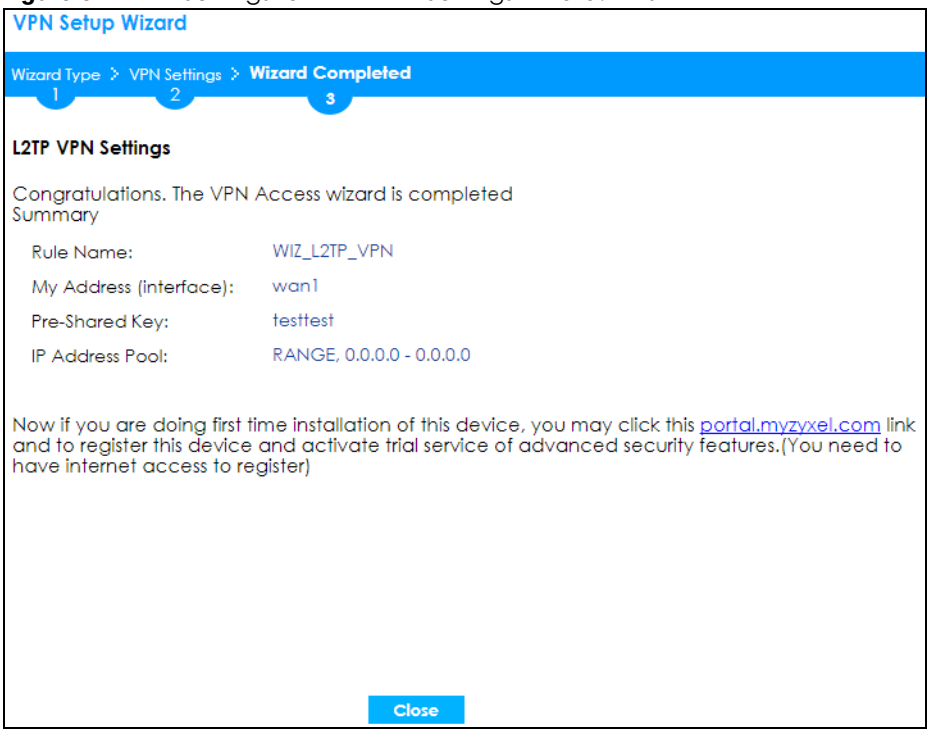


- **Rule Name**: Identifies the L2TP VPN connection (and the L2TP VPN gateway).
- **Secure Gateway "Any"** displays in this field because it is not configurable in this wizard. It allows incoming connections from the L2TP VPN Client.
- **Pre-Shared Key**: L2TP VPN tunnel password.
- **My Address (Interface)**: This displays the interface to use on your Zyxel Device for the L2TP tunnel.
- **IP Address Pool**: This displays the IP address pool used to assign to the L2TP VPN clients.

Click **Save** to complete the L2TP VPN Setting and the following screen will show.

4.5.4 VPN Settings for L2TP VPN Setting Wizard Completed

Figure 92 VPN Settings for L2TP VPN Settings Wizard: Finish



Now the rule is configured on the Zyxel Device. The L2TP VPN rule settings appear in the **Configuration > VPN > L2TP VPN** screen and also in the **Configuration > VPN > IPSec VPN > VPN Connection** and **VPN Gateway** screen.

CHAPTER 5
Dashboard

5.1 Overview

Use the **Dashboard** screens to check status information about the Zyxel Device.

5.1.1 What You Can Do in this Chapter

Use the main **Dashboard** screen to see the Zyxel Device's general device information, system status, and system resource usage. You can also display other status screens for more information.

Use the **Dashboard** screens to view the following.

- Device Information Screen on page 111
- System Status Screen on page 112
- Tx/Rx Statistics on page 112
- The Latest Logs Screen on page 113
- System Resources Screen on page 113
- DHCP Table Screen on page 114
- Number of Login Users Screen on page 115
- Current Login User on page 116
- VPN Status on page 116
- SSL VPN Status on page 116
- The Advanced Threat Protection Screen on page 117

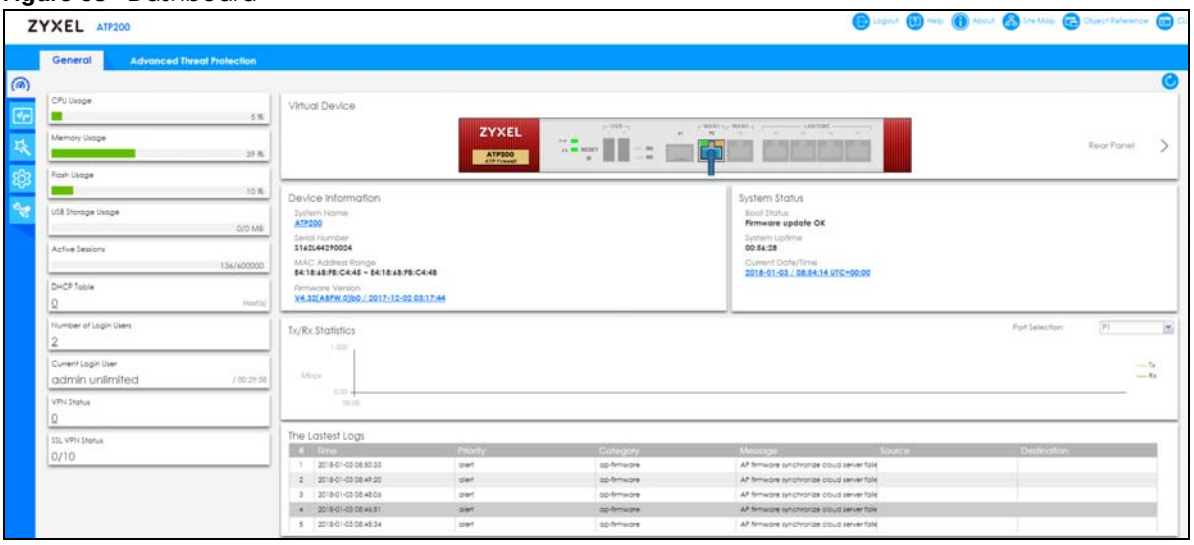
5.2 The General Screen

The **Dashboard** screen displays when you log into the Zyxel Device 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.

Click on the icon to go to the OneSecurity website where there is guidance on configuration walkthroughs, troubleshooting, and other information.

The following screen is an example of a Brand 2.0 web configurator web style.

Figure 93 Dashboard



The following table describes the labels in this screen.

Table 19 Dashboard

LABEL	DESCRIPTION
Refresh Now	Click this to update the widget's information immediately.
Virtual Device	
Rear Panel	Click this to view details about the Zyxel Device's rear panel. Hover your cursor over a connected interface or slot to display status details.
Front Panel	Click this to view details about the status of the Zyxel Device's front panel LEDs and connections. See Section 3.1.1 on page 67 for LED descriptions. An unconnected interface or slot appears grayed out.
	The following front and rear panel labels display when you hover your cursor over a connected interface or slot.
Name	This field displays the name of each interface.
Status	This field displays the current status of each interface or device installed in a slot. The possible values depend on what type of interface it is. **Inactive** - The Ethernet interface is disabled. **Down** - The Ethernet interface does not have any physical ports associated with it or the Ethernet interface is enabled but not connected. **Speed / Duplex** - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (**Full** or **Half**). The status for a WLAN card is **none**. For cellular (mobile broadband) interfaces, see Section 9.6 on page 250 for the status that can appear. For the auxiliary interface: **Inactive** - The auxiliary interface is disabled. **Connected** - The auxiliary interface is enabled and connected. **Disconnected** - The auxiliary interface is not connected.

Table 19 Dashboard (continued)

LABEL	DESCRIPTION
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. If the 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).

5.2.1 Device Information Screen

The **Device Information** screen displays Zyxel Device's system and model name, serial number, MAC address and firmware version shown in the below screen.

Figure 94 Dashboard > Device Information (Example)

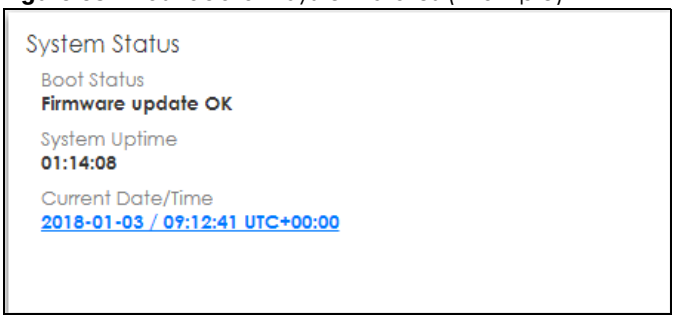
This table describes the fields in the above screen.

Table 20 Dashboard > Device Information

LABEL	DESCRIPTION
System Name	This field displays the name used to identify the Zyxel Device on any network. Click the link and open the **Host Name** screen where you can edit and make changes to the system and domain name.
Serial Number	This field displays the serial number of this Zyxel Device. The serial number is used for device tracking and control.
MAC Address Range	This field displays the MAC addresses used by the Zyxel Device. 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 Zyxel Device is currently running. Click the link to open the **Firmware Package** screen where you can upload firmware.

5.2.2 System Status Screen

Figure 95 Dashboard > System Status (Example)



This table describes the fields in the above screen.

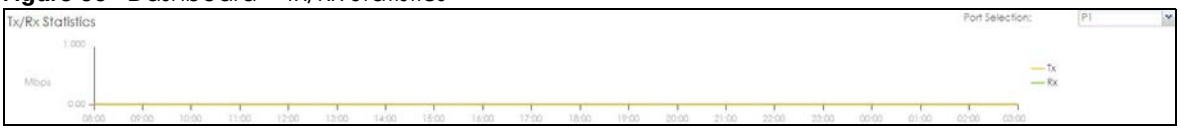
Table 21 Dashboard > System Status

LABEL	DESCRIPTION
Boot Status	This field displays details about the Zyxel Device's startup state. **OK** - The Zyxel Device started up successfully. **Firmware update OK** - A firmware update was successful. **Problematic configuration after firmware update** - The application of the configuration failed after a firmware upgrade. **System default configuration** - The Zyxel Device successfully applied the system default configuration. This occurs when the Zyxel Device starts for the first time or you intentionally reset the Zyxel Device to the system default settings. **Fallback to lastgood configuration** - The Zyxel Device was unable to apply the startup-config.conf configuration file and fell back to the lastgood.conf configuration file. **Fallback to system default configuration** - The Zyxel Device was unable to apply the lastgood.conf configuration file and fell back to the system default configuration file (system-default.conf). **Booting in progress** - The Zyxel Device is still applying the system configuration.
System Uptime	This field displays how long the Zyxel Device has been running since it last restarted or was turned on.
Current Date/Time	This field displays the current date and time in the Zyxel Device. The format is yyyy-mm-dd hh:mm:ss. Click on the link to see the **Date/Time** screen where you can make edits and changes to the date, time and time zone information.

5.2.3 Tx/Rx Statistics

This screen displays a line graph of packet statistics for each physical port.

Figure 96 Dashboard > Tx/Rx Statistics



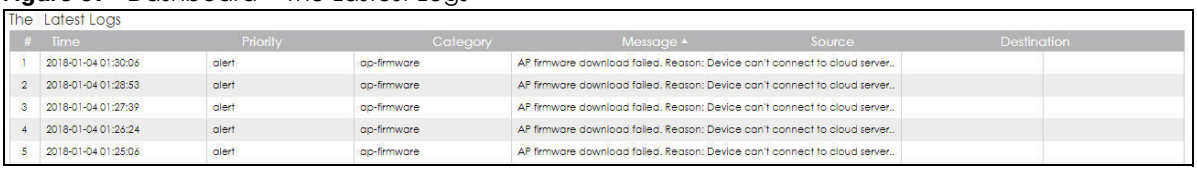
This table describes the fields in the above screen.

Table 22 Dashboard > The Lastest Logs

LABEL	DESCRIPTION
Mbps	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.

5.2.4 The Latest Logs Screen

Figure 97 Dashboard > The Lastest Logs


The Latest Logs

#	Time	Priority	Category	Message ▲	Source	Destination
1	2018-01-04 01:30:06	alert	ap-firmware	AP firmware download failed. Reason: Device can't connect to cloud server..		
2	2018-01-04 01:28:53	alert	ap-firmware	AP firmware download failed. Reason: Device can't connect to cloud server..		
3	2018-01-04 01:27:39	alert	ap-firmware	AP firmware download failed. Reason: Device can't connect to cloud server..		
4	2018-01-04 01:26:24	alert	ap-firmware	AP firmware download failed. Reason: Device can't connect to cloud server..		
5	2018-01-04 01:25:06	alert	ap-firmware	AP firmware download failed. Reason: Device can't connect to cloud server..		

This table describes the fields in the above screen.

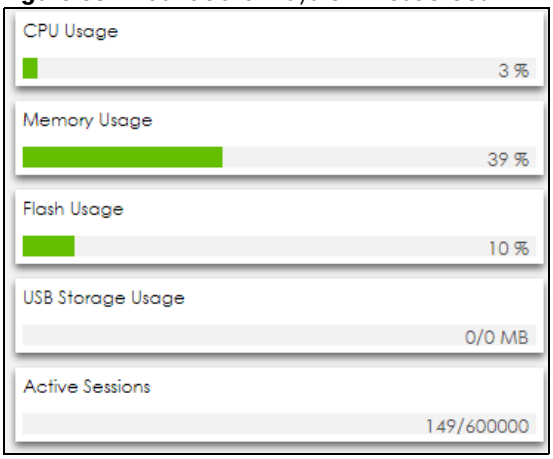
Table 23 Dashboard > The Lastest Logs

LABEL	DESCRIPTION
#	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.

5.2.5 System Resources Screen

Click the bar to see a graphic on that resource.

Figure 98 Dashboard > System Resources



This table describes the fields in the above screen.

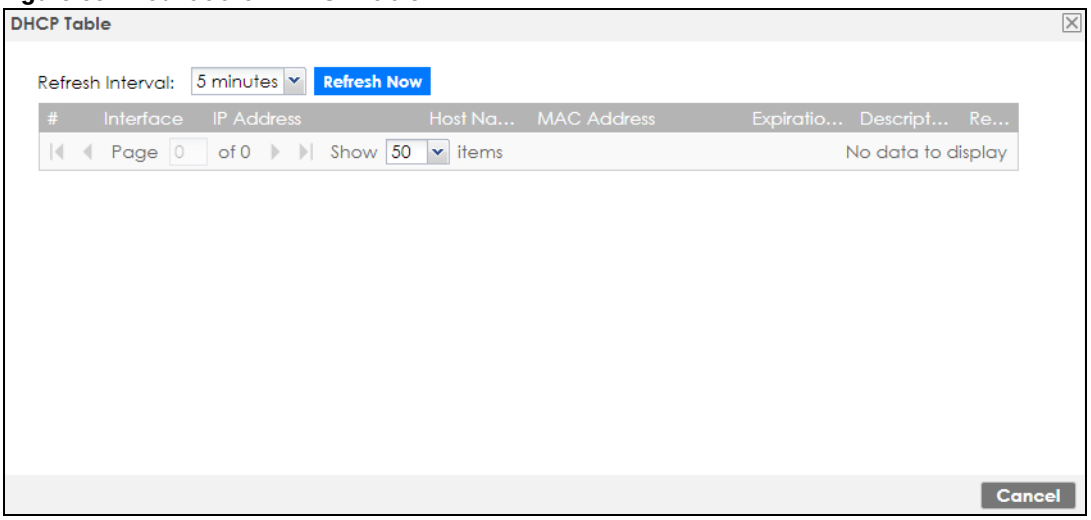
Table 24 Dashboard > System Resources

LABEL	DESCRIPTION
CPU Usage	This field displays what percentage of the Zyxel Device'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 Zyxel Device's recent CPU usage.
Memory Usage	This field displays what percentage of the Zyxel Device'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 Zyxel Device's recent memory usage.
Flash Usage	This field displays what percentage of the Zyxel Device's onboard flash memory is currently being used.
USB Storage Usage	This field shows how much storage in the USB device connected to the Zyxel Device is in use.
Active Sessions	This field shows how many sessions, established and non-established, that pass through/from/to/within the ZyWALL. 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 Zyxel Device's recent session usage.

5.2.6 DHCP Table Screen

Click on the number to look at the IP addresses currently assigned to DHCP clients and the IP addresses reserved for specific MAC addresses. The following screen will show.

Figure 99 Dashboard > DHCP Table



This table describes the fields in the above screen.

Table 25 Dashboard > DHCP Table

LABEL	DESCRIPTION
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.
#	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.

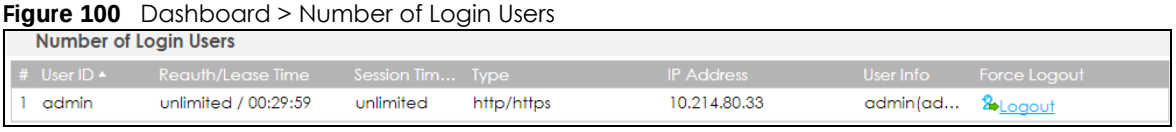
Table 25 Dashboard > DHCP Table (continued)

LABEL	DESCRIPTION
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 Zyxel Device 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.
Expiration Time	This is the period of time DHCP-assigned addresses is used.
Description	For a static DHCP entry, the host name or the description you configured shows here. This field is blank for dynamic DHCP entries.
Reserve	If this field is selected, this entry is a static DHCP entry. The IP address is reserved for the MAC address. If this field is clear, this entry is a dynamic DHCP entry. The IP address is assigned to a DHCP client. To create a static DHCP entry using an existing dynamic DHCP entry, select this field, and then click **Apply**. To remove a static DHCP entry, clear this field, and then click **Apply**.

5.2.7 Number of Login Users Screen

Click the Number of Login Users link to see the following screen.

Figure 100 Dashboard > Number of Login Users



This table describes the fields in the above screen.

Table 26 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 Zyxel Device.
Reauth/Lease Time	This field displays the amount of reauthentication time remaining and the amount of lease time remaining for each user.
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 Zyxel Device. This shows unlimited for an administrator account.
Type	This field displays the way the user logged in to the Zyxel Device.
IP address	This field displays the IP address of the computer used to log in to the Zyxel Device.

Table 26 Dashboard > Number of Login Users

LABEL	DESCRIPTION
User Info	This field displays the types of user accounts the Zyxel Device uses. If the user type is **ext-user** (external user), this field will show its external-group information when you move your mouse over it. If the external user matches two external-group objects, both external-group object names will be shown.
Force Logout	Click this icon to end a user's session.

5.2.8 Current Login User

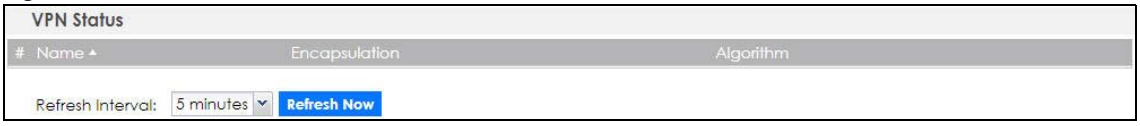
This field displays the user name used to log in to the current session, the amount of reauthentication time remaining, and the amount of lease time remaining.

Figure 101 Dashboard > Current Login User

5.2.9 VPN Status

Click on the link to look at the VPN tunnels that are currently established.

Figure 102 Dashboard > VPN Status



This table describes the fields in the above screen.

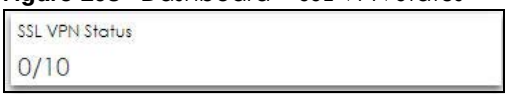
Table 27 Dashboard > VPN Status

LABEL	DESCRIPTION
#	This field is a sequential value and is not associated with any entry.
Name	This field displays the name of the VPN tunnel.
Encapsulation	This field displays the type of encapsulation the VPN tunnel uses.
Algorithm	This field displays the hash algorithm that the VPN tunnel uses to authenticate packet data.
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.

5.2.10 SSL VPN Status

The first number is the actual number of VPN tunnels up and the second number is the maximum number of SSL VPN tunnels allowed.

Figure 103 Dashboard > SSL VPN Status



5.3 The Advanced Threat Protection Screen

Use the **Advanced Threat Protection** screen to check security status information about the Zyxel Device.

Figure 104 Dashboard > Advanced Threat Protection

This screen gives the following information:

- The number of scanned traffic
- The number of the scanned connections for botnet filtering
- The number of the scanned files for sandboxing
- The number of the scanned files for anti-malware
- The number of the scanned connections for IDP
- The number of the scanned emails for email security
- The number of the scanned sites for content filtering
- Top 5 applications that are used the most
- Top 5 URLs that are detected the most
- IP reputation reports
- Botnet filtering reports
- Sandboxing reports
- Threat statistics

Click the **Refresh** icon to update the information in the window right away.

Part II
Technical Reference

CHAPTER 6
Monitor

6.1 Overview

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

6.1.1 What You Can Do in this Chapter

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

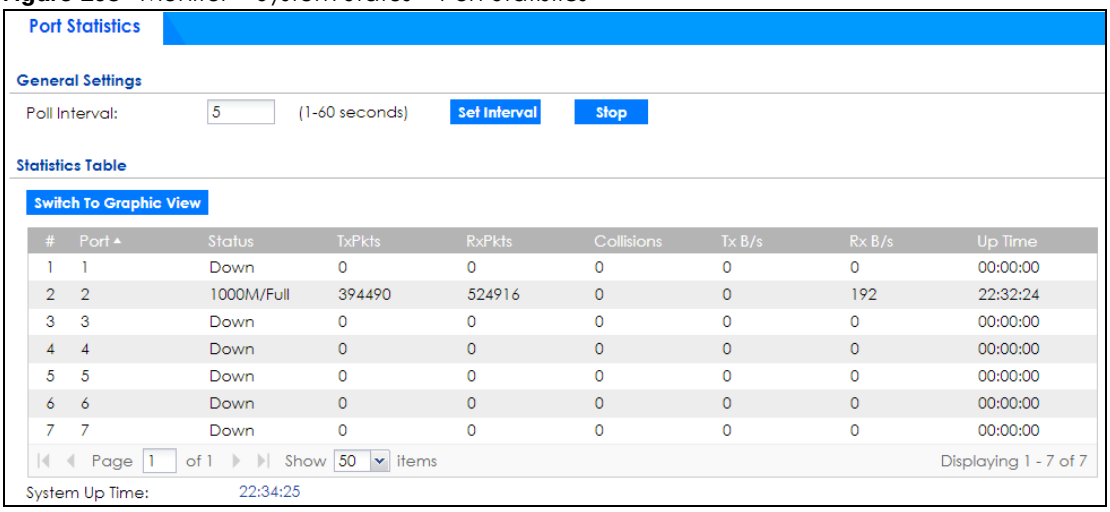
- Use the **System Status > Port Statistics** screen (see Section 6.2 on page 121) to look at packet statistics for each physical port.
- Use the **System Status > Port Statistics > Graph View** screen (see Section 6.2 on page 121) to look at a line graph of packet statistics for each physical port.
- Use the **System Status > Interface Status** screen (Section 6.3 on page 123) to see all of the Zyxel Device's interfaces and their packet statistics.
- Use the **System Status > Traffic Statistics** screen (see Section 6.4 on page 127) to start or stop data collection and view statistics.
- Use the **System Status > Session Monitor** screen (see Section 6.5 on page 129) to view sessions by user or service.
- Use the **System Status > IGMP Statistics** screen (see Section 6.7 on page 133) to view multicasting details.
- Use the **System Status > DDNS Status** screen (see Section 6.8 on page 134) to view the status of the Zyxel Device's DDNS domain names.
- Use the **System Status > IP/MAC Binding** screen (Section 6.9 on page 134) to view a list of devices that have received an IP address from Zyxel Device interfaces with IP/MAC binding enabled.
- Use the **System Status > Login Users** screen (Section 6.6 on page 131) to look at a list of the users currently logged into the Zyxel Device.
- Use the **System Status > Cellular Status** screen (Section 6.10 on page 135) to check your mobile broadband connection status.
- Use the **System Status > UPnP Port Status** screen (see Section 6.11 on page 139) to look at a list of the NAT port mapping rules that UPnP creates on the Zyxel Device.
- Use the **System Status > USB Storage** screen (Section 6.12 on page 140) to view information about a connected USB storage device.
- Use the **System Status > Ethernet Neighbor** screen (Section 6.13 on page 141) to view and manage the Zyxel Device's neighboring devices via Layer Link Discovery Protocol (LLDP).
- Use the **System Status > FQDN Object** screen (Section 6.14 on page 142) to display fully qualified domain name (FQDN) object cache lists used in DNS queries.
- Use the **Wireless > AP Information** > **AP List** screen (Section 6.15 on page 144) to display which APs are currently connected to the Zyxel Device.
- Use the **Wireless > AP Information** > **Radio List** screen (Section 6.16 on page 151) to display statistics about the wireless radio transmitters in each of the APs connected to the Zyxel Device.

- Use the **Wireless > AP Information** > **Top N APs** screen (Section 6.17 on page 154) to view managed APs with the most wireless traffic usage and most associated wireless stations.
- Use the **Wireless > AP Information** > **Single AP** screen (Section 6.18 on page 156) to view APs wireless traffic usage and associated wireless stations for a managed AP.
- Use the **Wireless > ZyMesh** screen (Section 6.19 on page 157) to display statistics about the ZyMesh wireless connections between the managed APs.
- Use the **Wireless > SSID Info** screen (Section 6.20 on page 158) to display the number of wireless clients that are currently connected to an SSID and the SSID's security mode.
- Use the **Wireless > Station Info** > **Station List** screen (Section 6.22 on page 159) to view information on connected wireless stations.
- Use the **Wireless > Station Info** > **Top N Stations** screen (Section 6.22 on page 159) to view wireless stations with the most wireless traffic usage.
- Use the **Wireless > Station Info** > **Single Station** screen (Section 6.23 on page 160) to view wireless traffic usage for an associated wireless station.
- Use the **Wireless > Detected Device** screen (Section 6.22 on page 159) to view information about suspected rogue APs.
- Use the **VPN Monitor** > **IPSec** screen (Section 6.25 on page 162) to display and manage active IPSec SAs.
- Use the **VPN Monitor > SSL** screen (see Section 6.26 on page 164) to list the users currently logged into the VPN SSL client portal. You can also log out individual users and delete related session information.
- Use the **VPN Monitor > L2TP over IPSec** screen (see Section 6.27 on page 164) to display and manage the Zyxel Device's connected L2TP VPN sessions.
- Use the **Security Statistics > Content Filter** screen (Section 6.28 on page 165) to start or stop data collection and view content filter statistics.
- Use the **Security Statistics > App Patrol** screen (see Section 6.29 on page 167) to start or stop data collection and view application statistics
- Use the **Security Statistics > Anti-Malware** screen (see Section 6.30 on page 168) to start or stop data collection and view malware statistics.
- Use the **Security Statistics > Reputation Filter** screen (see Section 6.31 on page 170) to view statistics of IP reputation and botnet filtering.
- Use the **Security Statistics > IDP** screen (Section 6.32 on page 172) to start or stop data collection and view IDP statistics.
- Use the **Security Statistics > Email Security** > **Summary** screen (Section 6.33 on page 174) to start or stop data collection and view spam statistics.
- Use the **Security Statistics > Email Security** > **Status** screen (Section 6.33.2 on page 176) to see how many mail sessions the Zyxel Device is currently checking and DNSBL statistics.
- Use the **Security Statistics > Sandboxing** screen (Section 6.34 on page 178) to start or stop data collection and view sandboxing statistics.
- Use the **Security Statistics > SSL Inspection** screen (Section 6.35 on page 179) to see a report on SSL Inspection and a certificate cache list.
- Use the **Log > View Log** screen (see Section 6.36.1 on page 181) to view the Zyxel Device's current log messages. You can change the way the log is displayed, you can email the log, and you can also clear the log in this screen.
- Use the **Log > View AP Log** screen (see Section 6.36.2 on page 183) to view the Zyxel Device's current wireless AP log messages.

6.2 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 105 Monitor > System Status > Port Statistics



The following table describes the labels in this screen.

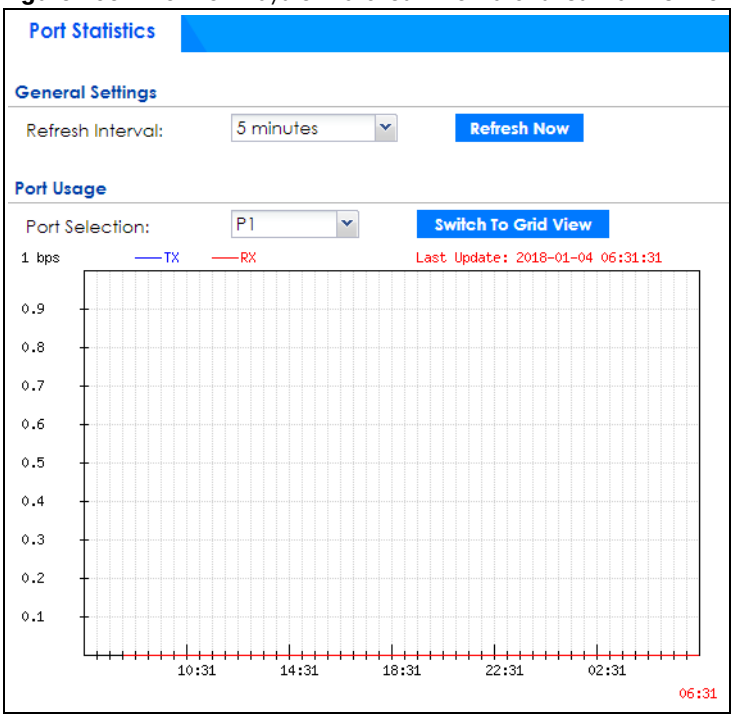
Table 28 Monitor > System Status > Port Statistics

LABEL	DESCRIPTION
Poll Interval	Enter how often you want this window to be updated automatically, and click **Set Interval**.
Set Interval	Click this to set the **Poll Interval** the screen uses.
Stop	Click this to stop the window from updating automatically. You can start it again by setting the **Poll Interval** and clicking **Set Interval**.
Switch to Graphic View	Click this to display the port statistics as a line graph.
#	This field is a sequential value, and it is not associated with a specific port.
Port	This field displays the physical port number.
Status	This field displays the current status of the physical port. **Down** - The physical port is not connected. **Speed / Duplex** - The physical port is connected. This field displays the port speed and duplex setting (**Full** or **Half**).
TxPkts	This field displays the number of packets transmitted from the Zyxel Device on the physical port since it was last connected.
RxPkts	This field displays the number of packets received by the Zyxel Device 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 Zyxel Device has been running since it last restarted or was turned on.

6.2.1 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 106 Monitor > System Status > Port Statistics > Switch to Graphic View



The following table describes the labels in this screen.

Table 29 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.
bps	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 Zyxel Device on the physical port since it was last connected.
RX	This line represents the traffic received by the Zyxel Device 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.

6.3 Interface Status Screen

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

Figure 107 Monitor > System Status > Interface Summary

Interface Summary

Interface Status

Name	Port/Bin...	Status	Zone	IP Addr/...	IP Assign...	Services	Action
sfp	P1	Down	OPT	0.0.0.0 / ...	Static	n/a	n/a
sfp_ppp	P1	Inactive	OPT	0.0.0.0 / ...	Dynamic	n/a	n/a
wan1	P2	1000M/Full	WAN	172.21.4...	DHCP cli...	n/a	Renew
wan1_ppp	P2	Inactive	WAN	0.0.0.0 / ...	Dynamic	n/a	n/a
wan2	P3	Down	WAN	0.0.0.0 / ...	DHCP cli...	n/a	Renew
wan2_ppp	P3	Inactive	WAN	0.0.0.0 / ...	Dynamic	n/a	n/a
lan1	P4, P5, P6	Down	LAN1	192.168....	Static	DHCP se...	n/a
lan2	n/a	Down	LAN2	192.168....	Static	DHCP se...	n/a
dmz	n/a	Down	DMZ	192.168....	Static	DHCP se...	n/a
reserved	P7	Down	n/a	0.0.0.0 / ...	Static	n/a	n/a

Tunnel Interface Status

Name	St...	Z...	IP Address	My Address	Remote Gateway A...	Mode

IPv6 Interface Status

Name	Port	Status	Zone	IP Address	Services	Action
sfp	P1	Down	OPT	::	n/a,n/a	n/a
sfp_ppp	P1	Inactive	OPT	::	n/a,n/a	n/a
wan1	P2	Inactive	WAN	::	n/a,n/a	n/a
wan1_ppp	P2	Inactive	WAN	::	n/a,n/a	n/a
wan2	P3	Down	WAN	::	n/a,n/a	n/a
wan2_ppp	P3	Inactive	WAN	::	n/a,n/a	n/a
lan1	P4, ...	Down	LAN1	::	n/a,n/a	n/a
lan2	n/a	Down	LAN2	::	n/a,n/a	n/a
dmz	n/a	Down	DMZ	::	n/a,n/a	n/a
reserved	P7	Down	n/a	::	n/a,n/a	n/a

Interface Statistics

Refresh

Name	Status	TxPkts	RxPkts	Tx B/s	Rx B/s
sfp	Down	0	0	0	0
wan1	1000M/Full	433507	686291	0	0
wan2	Down	9611	15283	0	0
lan1	Down	8926	3090	0	0
lan2	Down	0	0	0	0
dmz	Down	0	0	0	0
reserved	Down	0	0	0	0

Each field is described in the following table.

Table 30 Monitor > System Status > Interface Summary

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.	
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/Binding	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. For Ethernet interfaces: • **Inactive** - The Ethernet interface is disabled. • **Down** - The Ethernet interface does not have any physical ports associated with it or the Ethernet interface is enabled but not connected. • **Speed / Duplex** - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (**Full** or **Half**). For cellular (mobile broadband) interfaces, see Section 6.12 on page 140 the Web Help for the status that can appear. For the auxiliary interface: • **Inactive** - The auxiliary interface is disabled. • **Connected** - The auxiliary interface is enabled and connected. • **Disconnected** - The auxiliary interface is not connected. For virtual interfaces, this field always displays **Up**. If the virtual interface is disabled, it does not appear in the list. For VLAN and bridge interfaces, this field always displays **Up**. If the VLAN or bridge interface is disabled, it does not appear in the list. For PPP interfaces: • **Connected** - The PPP interface is connected. • **Disconnected** - The PPP interface is not connected. If the PPP interface is disabled, it does not appear in the list. For WLAN interfaces: • **Up** - The WLAN interface is enabled. • **Down** - The WLAN interface is disabled.
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. 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. • **Static** - This interface has a static IP address. • **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**, **DHCP server**, **DDNS**, **RIP**, and **OSPF**. This field displays **n/a** if the interface does not provide any services to the network.

Table 30 Monitor > System Status > Interface Summary

LABEL	DESCRIPTION
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**.
Tunnel Interface Status This displays the details of the Zyxel Device's configured tunnel interfaces.	
Name	This field displays the name of the interface.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Zone	This field displays the zone to which the interface is assigned.
IP Address	This is the IP address of the interface. If the interface is active (and connected), the Zyxel Device tunnels local traffic sent to this IP address to the **Remote Gateway Address**.
My Address	This is the interface or IP address uses to identify itself to the remote gateway. The Zyxel Device uses this as the source for the packets it tunnels to the remote gateway.
Remote Gateway Address	This is the IP address or domain name of the remote gateway to which this interface tunnels traffic.
Mode	This field displays the tunnel mode that you are using.
IPv6 Interface Status If an Ethernet interface does not have any physical ports associated with it, its entry is displayed in light gray text.	
Name	This field displays the name of each interface. 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.

Table 30 Monitor > System Status > Interface Summary

LABEL	DESCRIPTION
Status	This field displays the current status of each interface. The possible values depend on what type of interface it is. For Ethernet interfaces: • **Inactive** - The Ethernet interface is disabled. • **Down** - The Ethernet interface does not have any physical ports associated with it or the Ethernet interface is enabled but not connected. • **Speed / Duplex** - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (**Full** or **Half**). For cellular (mobile broadband) interfaces, see Section 6.12 on page 140 the Web Help for the status that can appear. For the auxiliary interface: • **Inactive** - The auxiliary interface is disabled. • **Connected** - The auxiliary interface is enabled and connected. • **Disconnected** - The auxiliary interface is not connected. For virtual interfaces, this field always displays **Up**. If the virtual interface is disabled, it does not appear in the list. For VLAN and bridge interfaces, this field always displays **Up**. If the VLAN or bridge interface is disabled, it does not appear in the list. For PPP interfaces: • **Connected** - The PPP interface is connected. • **Disconnected** - The PPP interface is not connected. If the PPP interface is disabled, it does not appear in the list. For WLAN interfaces: • **Up** - The WLAN interface is enabled. • **Down** - The WLAN interface is disabled.
Zone	This field displays the zone to which the interface is assigned.
IP Address	This field displays the current IPv6 address assigned to the interface. If the IPv6 address is ::, the interface is disabled or did not receive an IPv6 address via DHCP. If this interface is a member of an active virtual router, this field displays the IPv6 address it is currently using. This is either the static IPv6 address of the interface (if it is the master) or the management IPv6 address (if it is a backup).
Services	This field lists which services the interface provides to the network. Examples include **DHCP relay**, **DHCP server**, **DDNS**, **RIP**, and **OSPF**. 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.
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.

Table 30 Monitor > System Status > Interface Summary

LABEL	DESCRIPTION
Status	This field displays the current status of the interface. • **Down** - The interface is not connected. • **Speed / Duplex** - The interface is connected. This field displays the port speed and duplex setting (**Full** or **Half**). This field displays **Connected** and the accumulated connection time (hh:mm:ss) when the PPP interface is connected.
TxPkts	This field displays the number of packets transmitted from the Zyxel Device on the interface since it was last connected.
RxPkts	This field displays the number of packets received by the Zyxel Device 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.

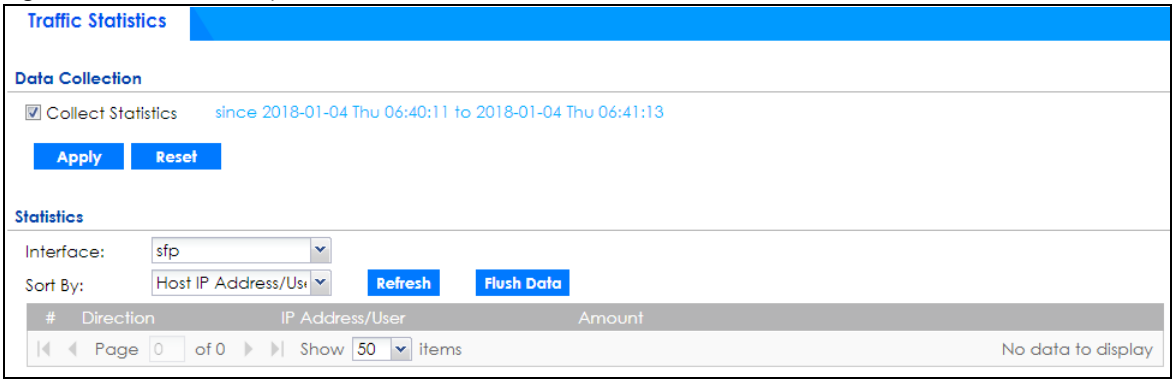
6.4 The Traffic Statistics Screen

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 Zyxel Device counts HTTP GET packets. Please see Table 31 on page 128 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 Zyxel Device 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 108 Monitor > System Status > Traffic Statistics



There is a limit on the number of records shown in the report. Please see Table 32 on page 129 for more information. The following table describes the labels in this screen.

Table 31 Monitor > System Status > Traffic Statistics

LABEL	DESCRIPTION
Data Collection	
Collect Statistics	Select this to have the Zyxel Device collect data for the report. If the Zyxel Device 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 Zyxel Device.
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.
Sort By	Select the type of report to display. Choices are: • **Host IP Address/User** - displays the IP addresses or users with the most traffic and how much traffic has been sent to and from each one. • **Service/Port** - displays the most-used protocols or service ports and the amount of traffic for each one. • **Web Site Hits** - displays the most-visited Web sites and how many times each one has been visited. • **Country** - displays the countries with the most traffic and the amount of traffic for each one. 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 **Traffic Type** 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. • **Ingress**- traffic is coming from the IP address or user to the Zyxel Device. • **Egress** - traffic is going from the Zyxel Device 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 32 on page 129.
Amount	This field displays how much traffic was sent or received from the indicated IP address or user. 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 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 32 on page 129.
	These fields are available when the **Traffic Type** 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 32 on page 129.
Protocol	This field indicates what protocol the service was using.
Direction	This field indicates whether the indicated protocol or service port is sending or receiving traffic. • **Ingress** - traffic is coming into the Zyxel Devicethrough the interface • **Egress** - traffic is going out from the Zyxel Device through the interface

Table 31 Monitor > System Status > Traffic Statistics (continued)

LABEL	DESCRIPTION
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 32 on page 129.
	These fields are available when the **Traffic Type** 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 Zyxel Device counts each page viewed on a Web site as another hit. The maximum number of domain names in this report is indicated in Table 32 on page 129.
Hits	This field displays how many hits the Web site received. The Zyxel Device counts hits by counting HTTP GET packets. Many Web sites have HTTP GET references to other Web sites, and the Zyxel Device counts these as hits too. The count starts over at zero if the number of hits passes the hit count limit. See Table 32 on page 129.
	These fields are available when the **Traffic Type** is **Country**.
#	This field is the rank of each record. The country name is sorted by the amount of traffic.
Direction	This field indicates whether the indicated protocol or service port is sending or receiving traffic. • **Ingress** - traffic is coming into the Zyxel Devicethrough the interface • **Egress** - traffic is going out from the Zyxel Device through the interface
Country Name	This field displays the name of the country.
Country	This field displays the country code.
Amount	This field displays how much traffic was sent or received from the indicated country. 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 32 on page 129. • **Ingress** - traffic is coming into the Zyxel Device from the country. • **Egress** - traffic is going from the Zyxel Device to the country.

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

Table 32 Maximum Values for Reports

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

6.5 The Session Monitor Screen

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

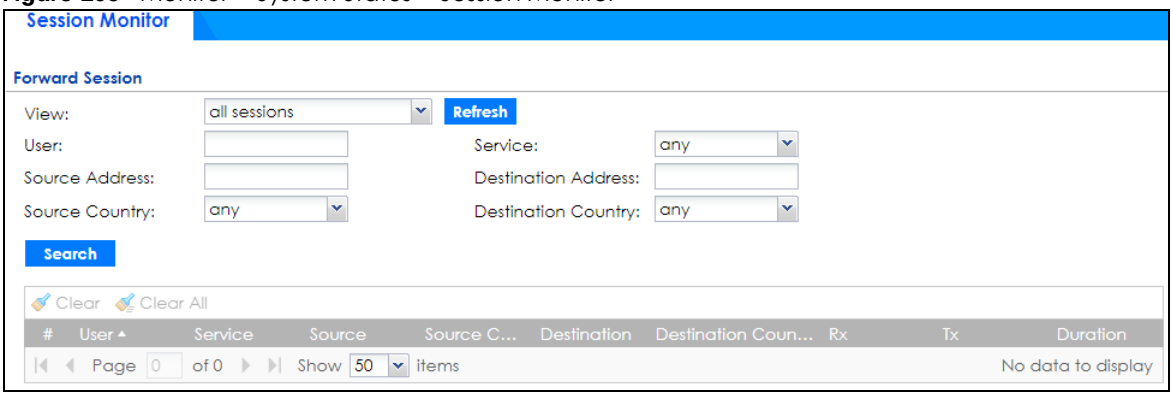
- User who started the session
- Protocol or service port used

- Source address
- Destination address
- Number of bytes received (so far)
- Number of bytes transmitted (so far)
- Duration (so far)

You can look at all established sessions that passed through the Zyxel Device 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 109 Monitor > System Status > Session Monitor



The following table describes the labels in this screen.

Table 33 Monitor > System Status > Session Monitor

LABEL	DESCRIPTION
View	Select how you want the established sessions that passed through the Zyxel Device to be displayed. Choices are: • **sessions by users** - display all active sessions grouped by user • **sessions by services** - display all active sessions grouped by service or protocol • **sessions by source IP** - display all active sessions grouped by source IP address • **session by source region** - display all active sessions grouped by where the traffic is coming from by country • **sessions by destination IP** - display all active sessions grouped by destination IP address • **sessions by destination region** - display all active sessions grouped by where the traffic is going to by country • **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**, **Destination Address, Source Country** and **Destination Country** fields display if you view all sessions. Select your desired filter criteria and click the Refresh button to filter the list of sessions.
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 Zyxel Device identifies the service by comparing the protocol and destination port of each packet to the protocol and port of each services that is defined.

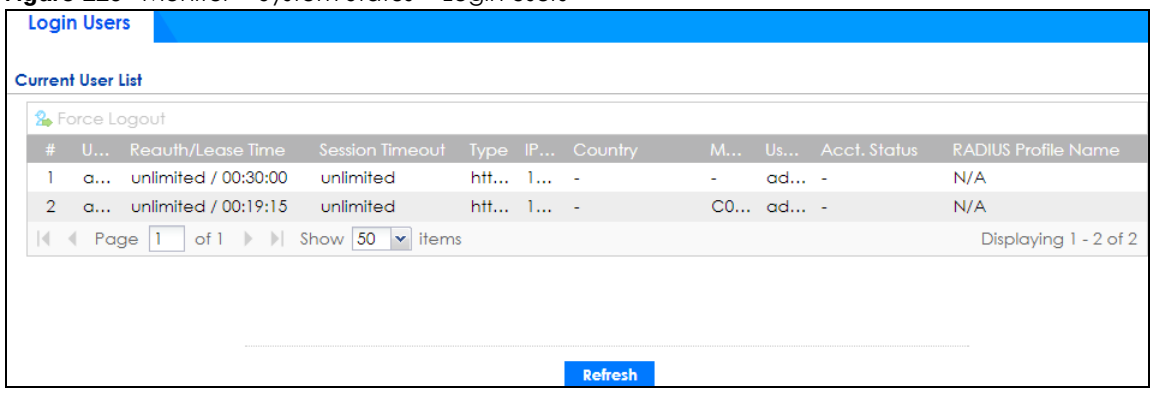
Table 33 Monitor > System Status > Session Monitor (continued)

LABEL	DESCRIPTION
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.
Source Country	This field displays when **View** is set to **all sessions**. Select the country where the traffic is coming from.
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.
Destination Country	This field displays when **View** is set to **all sessions**. Select the country where the traffic is going to.
Search	Click this to display all sessions in the table below according to the criteria you defined above.
Clear Clear All	Administrators can use these buttons to forcibly terminate selected TCP/UDP connections. Select one or multiple connections and then click **Clear**; click **Clear All** to terminate all connections displayed. Cleared sessions display in the **Log > View Log** screen.
#	This field is the rank of each record. The names are sorted by the name of user in active session. You can use the pull down menu on the right to choose sorting method.
User	This field displays the user in each active session. 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. 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. 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.
Source Country	This field displays the source country in each active session.
Destination	This field displays the destination IP address and port in each active session. 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.
Destination Country	This field displays the destination country in each active session.
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.

6.6 The Login Users Screen

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

Figure 110 Monitor > System Status > Login Users



The following table describes the labels in this screen.

Table 34 Monitor > System Status > Login Users

LABEL	DESCRIPTION
Force Logout	Select a user ID and click this icon to end a user's session.
#	This field is a sequential value and is not associated with any entry.
User ID	This field displays the user name of each user who is currently logged in to the Zyxel Device.
Reauth/Lease Time	This field displays the amount of reauthentication time remaining and the amount of lease time remaining for each user.
Session Timeout	This field displays the total account of time the account (authenticated by an external server) can use to log into the Zyxel Device or access the Internet through the Zyxel Device. This shows **unlimited** for an administrator account.
Type	This field displays the way the user logged in to the Zyxel Device.
IP Address	This field displays the IP address of the computer used to log in to the Zyxel Device.
Country	The Internet Assigned Numbers Authority (IANA) has reserved the following blocks of **Private IP** addresses specifically for private networks: • 10.0.0.0-10.255.255.255 • 172.16.0.0-172.31.255.255 • 192.168.0.0-192.168.255.255 • 224.0.0.0-239.255.255.255
MAC	This field displays the MAC address of the computer used to log in to the Zyxel Device.
User Info	This field displays the types of user accounts the Zyxel Device uses. If the user type is **ext-user** (external user), this field will show its external-group information when you move your mouse over it. If the external user matches two external-group objects, both external-group object names will be shown.
Acct. Status	For a captive portal login, this field displays the accounting status of the account used to log into the Zyxel Device. **Accounting-on** means accounting is being performed for the user login. **Accounting-off** means accounting has stopped for this user login. A "-" displays if accounting is not enabled for this login.

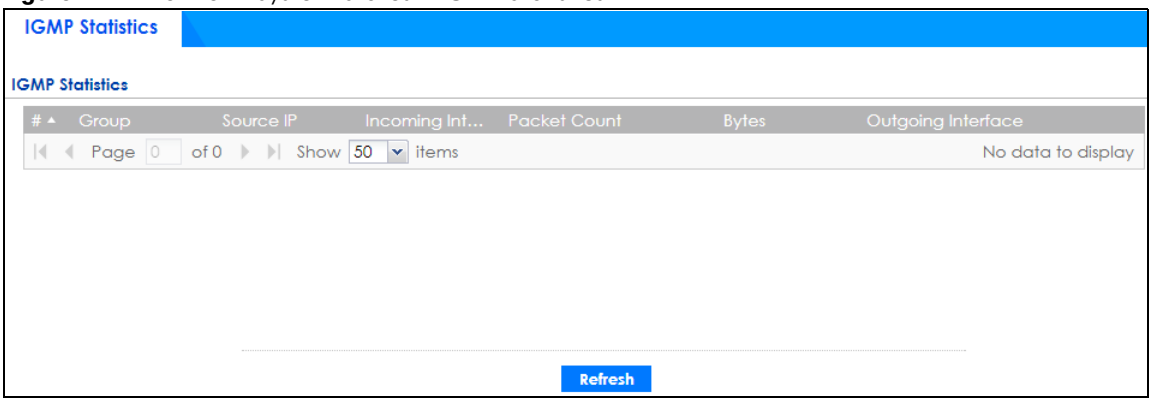
Table 34 Monitor > System Status > Login Users (continued)

LABEL	DESCRIPTION
RADIUS Profile Name	This field displays the name of the RADIUS profile used to authenticate the login through the captive portal. **N/A** displays for logins that do not use the captive portal and RADIUS server authentication.
Refresh	Click this button to update the information in the screen.

6.7 IGMP Statistics

The Internet Group Management Protocol (IGMP) Statistics is used by Zyxel Device IP hosts to inform adjacent router about multicast group memberships. It can also be used for one-to-many networking applications such as online streaming video and gaming, distribution of company newsletters, updating address book of mobile computer users in the field allowing more efficient use of resources when supporting these types of applications. Click **Monitor** > **System Status** > **IGMP Statistics** to open the following screen.

Figure 111 Monitor > System Status > IGMP Statistics



The following table describes the labels in this screen.

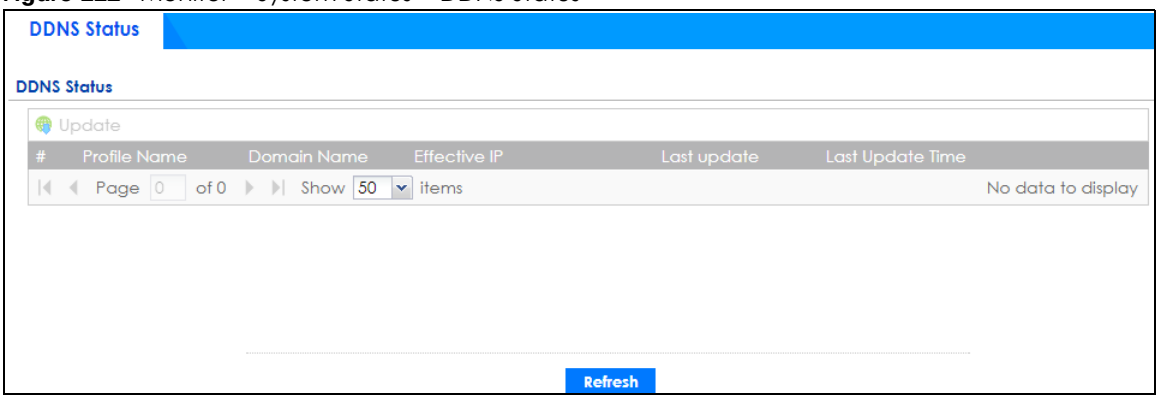
Table 35 Monitor > System Status > IGMP Statistics

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific I GMP Statistics.
Group	This field displays the group of devices in the IGMP.
Source IP	This field displays the host source IP information of the IGMP.
Incoming Interface	This field displays the incoming interface that's connected on the IGMP.
Packet Count	This field displays the packet size of the data being transferred.
Bytes	This field displays the size of the data being transferred in Byes.
Outgoing Interface	This field displays the outgoing interface that's connected on the IGMP.
Refresh	Click this button to update the information in the screen.

6.8 The DDNS Status Screen

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

Figure 112 Monitor > System Status > DDNS Status



The following table describes the labels in this screen.

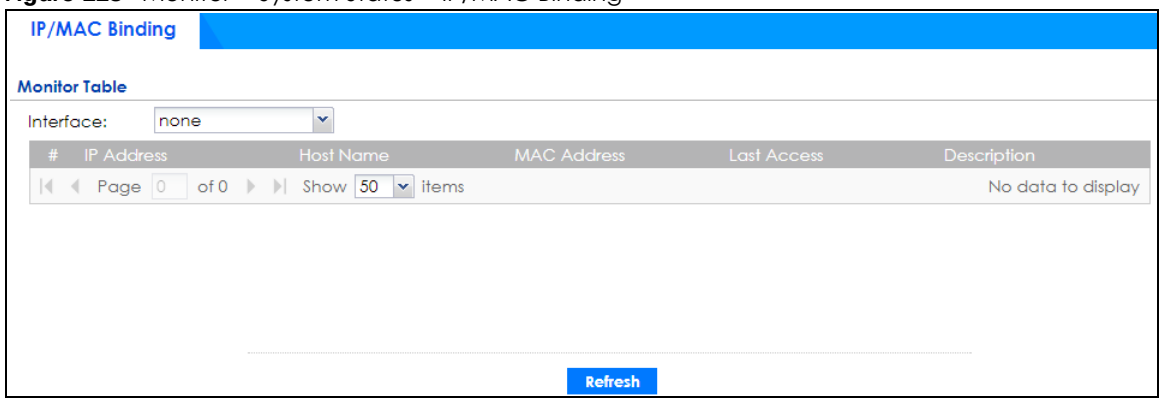
Table 36 Monitor > System Status > DDNS Status

LABEL	DESCRIPTION
Update	Click this to have the Zyxel Device update the profile to the DDNS server. The Zyxel Device attempts to resolve the IP address for the domain name.
#	This field is a sequential value, and it is not associated with a specific DDNS server.
Profile Name	This field displays the descriptive profile name for this entry.
Domain Name	This field displays each domain name the Zyxel Device can route.
Effective IP	This is the (resolved) IP address of the domain name.
Last Update	This shows whether the last attempt to resolve the IP address for the domain name was successful or not. **Updating** means the Zyxel Device 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).
Refresh	Click this button to update the information in the screen.

6.9 IP/MAC Binding

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

Figure 113 Monitor > System Status > IP/MAC Binding



The following table describes the labels in this screen.

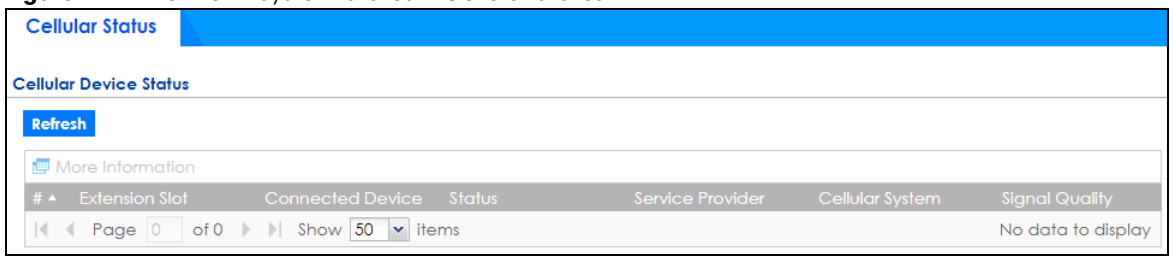
Table 37 Monitor > System Status > IP/MAC Binding

LABEL	DESCRIPTION
Interface	Select a Zyxel Device interface that has IP/MAC binding enabled to show to which devices it has assigned an IP address.
#	This field is a sequential value, and it is not associated with a specific IP/MAC binding entry.
IP Address	This is the IP address that the Zyxel Device assigned to a device.
Host Name	This field displays the name used to identify this device on the network (the computer name). The Zyxel Device 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 Zyxel Device through this interface.
Description	This field displays the description of the IP/MAC binding.
Refresh	Click this button to update the information in the screen.

6.10 Cellular Status Screen

This screen displays your mobile broadband connection status. Click **Monitor > System Status > Cellular Status** to display this screen.

Figure 114 Monitor > System Status > Cellular Status



The following table describes the labels in this screen.

Table 38 Monitor > System Status > Cellular Status

LABEL	DESCRIPTION
Refresh	Click this button to update the information in the screen.
More Information	Click this to display more information on your mobile broadband, such as the signal strength, IMEA/ESN and IMSI. This is only available when the mobile broadband device attached and activated on your Zyxel Device. Refer to Section 6.10.1 on page 138.
#	This field is a sequential value, and it is not associated with any interface.
Extension Slot	This field displays where the entry's cellular card is located.
Connected Device	This field displays the model name of the cellular card.

Table 38 Monitor > System Status > Cellular Status (continued)

LABEL	DESCRIPTION
Status	• **No device** - no mobile broadband device is connected to the Zyxel Device. • **No Service** - no mobile broadband network is available in the area; you cannot connect to the Internet. • **Limited Service** - returned by the service provider in cases where the SIM card is expired, the user failed to pay for the service and so on; you cannot connect to the Internet. • **Device detected** - displays when you connect a mobile broadband device. • **Device error** - a mobile broadband device is connected but there is an error. • **Probe device fail** - the Zyxel Device's test of the mobile broadband device failed. • **Probe device ok** - the Zyxel Device's test of the mobile broadband device succeeded. • **Init device fail** - the Zyxel Device was not able to initialize the mobile broadband device. • **Init device ok** - the Zyxel Device initialized the mobile broadband card. • **Check lock fail** - the Zyxel Device's check of whether or not the mobile broadband device is locked failed. • **Device locked** - the mobile broadband device is locked. • **SIM error** - there is a SIM card error on the mobile broadband device. • **SIM locked-PUK** - the PUK is locked on the mobile broadband device's SIM card. • **SIM locked-PIN** - the PIN is locked on the mobile broadband device's SIM card. • **Unlock PUK fail** - Your attempt to unlock a WCDMA mobile broadband device's PUK failed because you entered an incorrect PUK. • **Unlock PIN fail** - Your attempt to unlock a WCDMA mobile broadband device's PIN failed because you entered an incorrect PIN. • **Unlock device fail** - Your attempt to unlock a CDMA2000 mobile broadband device failed because you entered an incorrect device code. • **Device unlocked** - You entered the correct device code and unlocked a CDMA2000 mobile broadband device. • **Get dev-info fail** - The Zyxel Device cannot get cellular device information. • **Get dev-info ok** - The Zyxel Device succeeded in retrieving mobile broadband device information. • **Searching network** - The mobile broadband device is searching for a network. • **Get signal fail** - The mobile broadband device cannot get a signal from a network. • **Network found** - The mobile broadband device found a network. • **Apply config** - The Zyxel Device is applying your configuration to the mobile broadband device. • **Inactive** - The mobile broadband interface is disabled. • **Active** - The mobile broadband interface is enabled. • **Incorrect device** - The connected mobile broadband device is not compatible with the Zyxel Device. • **Correct device** - The Zyxel Device detected a compatible mobile broadband device. • **Set band fail** - Applying your band selection was not successful. • **Set band ok** - The Zyxel Device successfully applied your band selection. • **Set profile fail** - Applying your ISP settings was not successful. • **Set profile ok** - The Zyxel Device successfully applied your ISP settings. • **PPP fail** - The Zyxel Device failed to create a PPP connection for the cellular interface. • **Need auth-password** - You need to enter the password for the mobile broadband card in the cellular edit screen. • **Device ready** - The Zyxel Device successfully applied all of your configuration and you can use the mobile broadband connection.
Service Provider	This displays the name of your network service provider. This shows **Limited Service** if the service provider has stopped service to the mobile broadband card. For example if the bill has not been paid or the account has expired.

Table 38 Monitor > System Status > Cellular Status (continued)

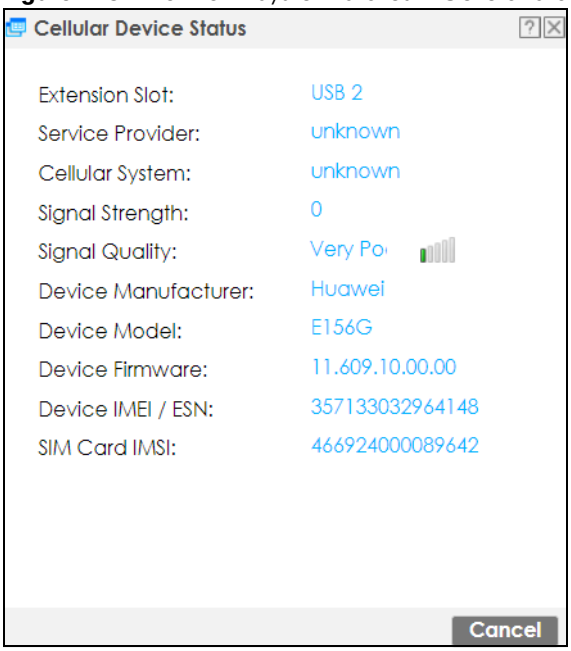
LABEL	DESCRIPTION
Cellular System	This field displays what type of cellular network the mobile broadband connection is using. The network type varies depending on the mobile broadband card you inserted and could be **UMTS**, **UMTS/HSDPA**, **GPRS** or **EDGE** when you insert a GSM mobile broadband card, or **1xRTT**, **EVDO Rev.0** or **EVDO Rev.A** when you insert a CDMA mobile broadband card.
Signal Quality	This displays the strength of the signal. The signal strength mainly depends on the antenna output power and the distance between your Zyxel Device and the service provider's base station.

6.10.1 More Information

This screen displays more information on your mobile broadband, such as the signal strength, IMEA/ESN and IMSI that helps identify your mobile broadband device and SIM card. Click **Monitor > System Status > Cellular Status > More Information** to display this screen.

Note: This screen is only available when the mobile broadband device is attached to and activated on the Zyxel Device.

Figure 115 Monitor > System Status > Cellular Status > More Information



The following table describes the labels in this screen.

Table 39 Monitor > System Status > Cellular Status > More Information

LABEL	DESCRIPTION
Extension Slot	This field displays where the entry's cellular card is located.
Service Provider	This displays the name of your network service provider. This shows **Limited Service** if the service provider has stopped service to the mobile broadband card. For example if the bill has not been paid or the account has expired.

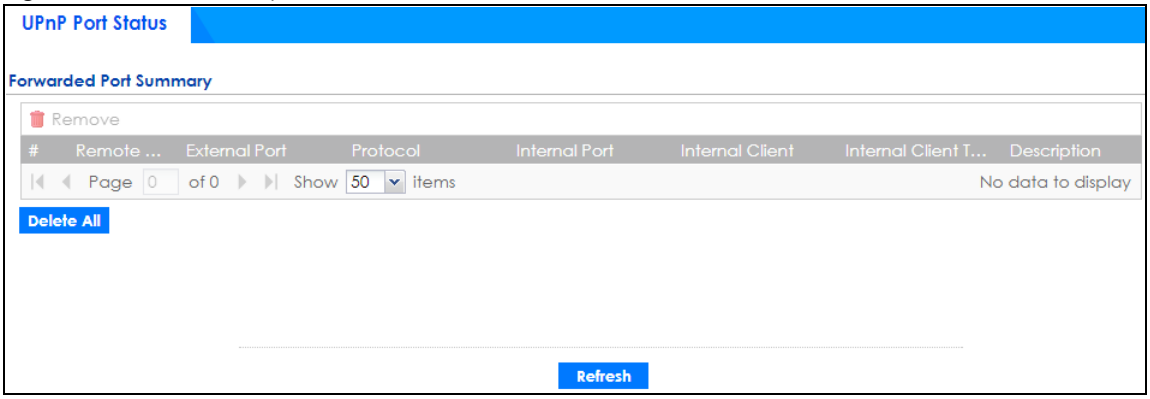
Table 39 Monitor > System Status > Cellular Status > More Information (continued)

LABEL	DESCRIPTION
Cellular System	This field displays what type of cellular network the mobile broadband connection is using. The network type varies depending on the mobile broadband card you inserted and could be **UMTS**, **UMTS/HSDPA**, **GPRS** or **EDGE** when you insert a GSM mobile broadband card, or **1xRTT**, **EVDO Rev.0** or **EVDO Rev.A** when you insert a CDMA mobile broadband card.
Signal Strength	This is the **Signal Quality** measured in dBm.
Signal Quality	This displays the strength of the signal. The signal strength mainly depends on the antenna output power and the distance between your Zyxel Device and the service provider's base station.
Device Manufacturer	This shows the name of the company that produced the mobile broadband device.
Device Model	This field displays the model name of the cellular card.
Device Firmware	This shows the software version of the mobile broadband device.
Device IMEI/ESN	IMEI (International Mobile Equipment Identity) is a 15-digit code in decimal format that identifies the mobile broadband device. ESN (Electronic Serial Number) is an 8-digit code in hexadecimal format that identifies the mobile broadband device.
SIM Card IMSI	IMSI (International Mobile Subscriber Identity) is a 15-digit code that identifies the SIM card.

6.11 The UPnP Port Status Screen

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

Figure 116 Monitor > System Status > UPnP Port Status



The following table describes the labels in this screen.

Table 40 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.

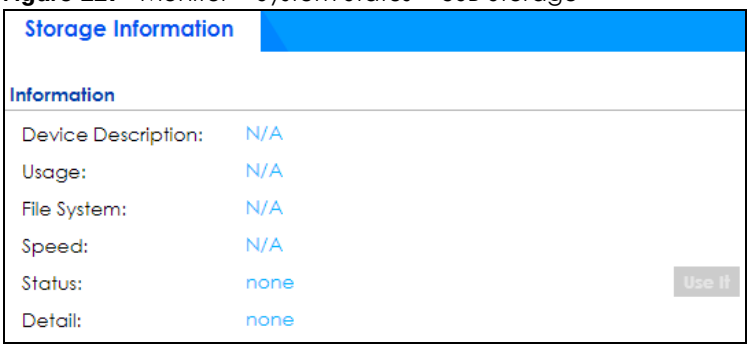
Table 40 Monitor > System Status > UPnP Port Status (continued)

LABEL	DESCRIPTION
Remote Host	This field displays the source IP address (on the WAN) of inbound IP packets. Since this is often a wild-card, the field may be blank. When the field is blank, the Zyxel Device forwards all traffic sent to the **External Port** on the WAN interface to the **Internal Client** on the **Internal Port**. When this field displays an external IP address, the NAT rule has the Zyxel Device forward inbound packets to the **Internal Client** from that IP address only.
External Port	This field displays the port number that the Zyxel Device "listens" non the WAN port) for connection requests destined for the NAT rule's **Internal Port** and **Internal Client**. The Zyxel Device 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 Zyxel Device 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).
Internal Port	This field displays the port number on the **Internal Client** to which the Zyxel Device 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.

6.12 USB Storage Screen

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

Figure 117 Monitor > System Status > USB Storage



The following table describes the labels in this screen.

Table 41 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.

Table 41 Monitor > System Status > USB Storage (continued)

LABEL	DESCRIPTION
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 Zyxel Device, such as NTFS.
Speed	This field displays the connection speed the USB storage device supports.
Status	**Ready** - you can have the Zyxel Device use the USB storage device. Click **Remove Now** to stop the Zyxel Device from using the USB storage device so you can remove it. **Unused** - the connected USB storage device was manually unmounted by using the **Remove Now** button or for some reason the Zyxel Device cannot mount it. Click **Use It** to have the Zyxel Device mount a connected USB storage device. This button is grayed out if the file system is not supported (unknown) by the Zyxel Device. **none** - no USB storage device is connected.
Detail	This field displays any other information the Zyxel Device retrieves from the USB storage device. • **Deactivated** - the use of a USB storage device is disabled (turned off) on the Zyxel Device. • **OutofSpace** - the available disk space is less than the disk space full threshold. • **Mounting** - the Zyxel Device is mounting the USB storage device. • **Removing** - the Zyxel Device is unmounting the USB storage device. • **none** - the USB device is operating normally or not connected.

6.13 Ethernet Neighbor Screen

The Ethernet Neighbor screen allows you to view the Zyxel Device'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 Zyxel Device that you're logged into using the web configurator.

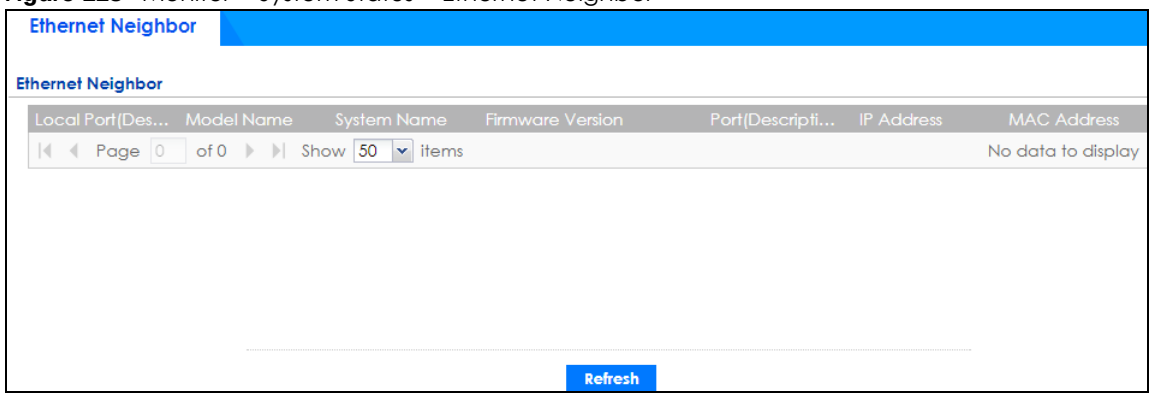
LLDP is a layer-2 protocol that allows a network device to advertise its identity and capabilities on the local network. It also allows the device to maintain and store information from adjacent devices which are directly connected to the network device. This helps you discover network changes and perform 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 118 Monitor > System Status > Ethernet Neighbor



The following table describes the fields in the previous screen.

Table 42 Monitor > System Status > Ethernet Neighbor

LABEL	DESCRIPTION
Local Port (Description)	This field displays the port of the Zyxel Device, on which the neighboring device is discovered. For Zyxel Devices that support **Port Role**, if ports 3 to 5 are grouped together and there is a connection to P5 only, the Zyxel Device will display P3 as the interface port number (even though there is no connection to that port).
Model Name	This field displays the model name of the discovered device.
System Name	This field displays the system name of the discovered device.
Firmware Version	This field displays the firmware version of the discovered device.
Port (Description)	This field displays the first internal port on the discovered device. Internal is an interface type displayed in the **Network > Interface > Ethernet > Edit** screen. For example, if P1 and P2 are WAN, P3 to P5 are LAN, and P6 is DMZ, then Zyxel Device will display P3 as the first internal interface port number. For Zyxel Devices that support **Port Role**, if ports 3 to 5 are grouped together and there is a connection to P5 only, the Zyxel Device 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 Address	This field displays the MAC address of the discovered device.
Refresh	Click this button to update the information in the screen.

6.14 FQDN Object Screen

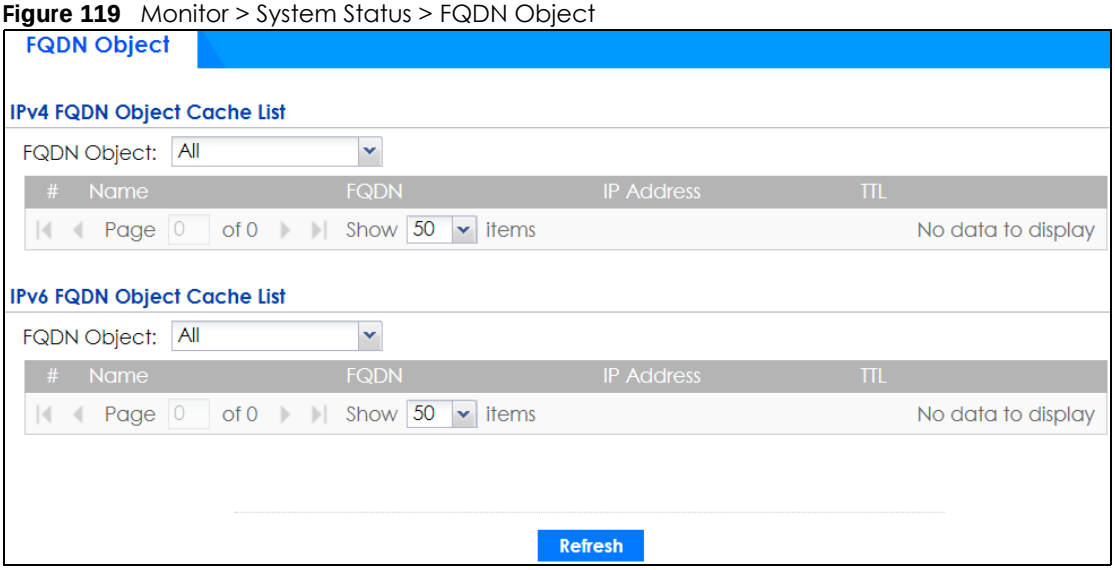
Click **Monitor > System Status > FQDN Object** to open the **FQDN Object** screen. View FQDN-to-IP address mappings cached in this screen. An FQDN is resolved to its IP address using the DNS server configured on the Zyxel Device. If the Zyxel Device receives a DNS query for an FQDN and the Zyxel Device has an FQDN cache entry, the Zyxel Device can map the IP address in a DNS response without having to query a DNS name server. The Zyxel Device updates FQDN-to-IP address mappings when the TTL (Time To Live) setting expires.

You can configure FQDN objects in **Configuration > Object > Address/Geo IP > Address** or **Configuration > Object > Address/Geo IP > Address Group**.

FQDN can be used in Security Policy, Policy Route, BWM and Web Authentication profiles as source and destination criteria. FQDN with a wildcard (for example, *.zyxel.com) can be used in these profiles as destination criteria only.

Suppose you want to block certain users from going to a website with a dynamically updated IP address using DDNS. Create an FQDN object for the website in **Object > Address**, and then create a Security Policy in **Security Policy > Policy Control > Add**. Use the FQDN object to identify the website as a destination, and configure specific users to block. When a user tries to connect to the forbidden website, the Zyxel Device first checks the IP address - website mapping in response to the DNS query and then finds the FQDN object match. The Security Policy that has this FQDN object match can then block the configured users from accessing the website.

Figure 119 Monitor > System Status > FQDN Object



The following table describes the fields in the previous screen.

Table 43 Monitor > System Status > FQDN Object

LABEL	DESCRIPTION
IPv4 FQDN Object Cache List You must first configure IPv4 FQDN objects in **Configuration > Object > Address/Geo IP** in the **IPv4 Address Configuration** field.	
FQDN Object	Select a previously created object from the drop-down list box to display related FQDN object caches used in DNS queries.
#	This is the index number of the FQDN entry.
Name	This field displays the name of the selected FQDN object used in DNS queries.
FQDN	This field displays a host's fully qualified domain name.
IP Address	This field displays the mapping of the FQDN to an IP address. This is the IP address of a host.
TTL	This field displays the number of seconds the Zyxel Device holds IP address - FQDN object mapping in its cache. The mapping is updated when the TTL (Time To Live) setting expires.
IPv6 FQDN Object Cache List You must first configure IPv6 FQDN objects in **Configuration > Object > Address/Geo IP** in the **IPv6 Address Configuration** field.	

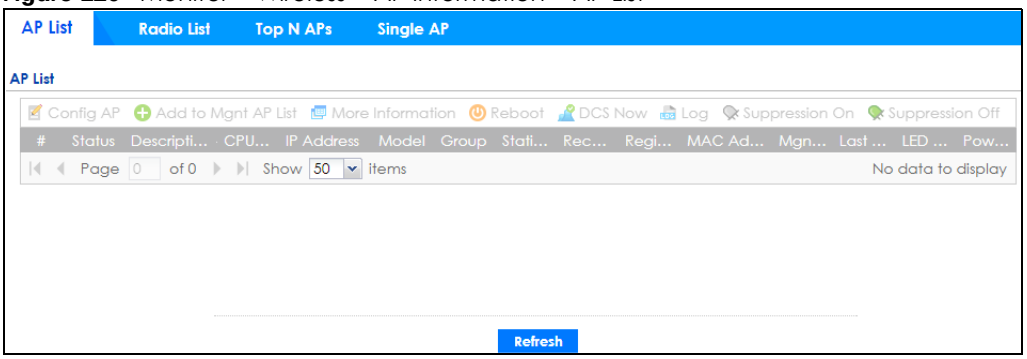
Table 43 Monitor > System Status > FQDN Object

LABEL	DESCRIPTION
FQDN Object	Select an object from the drop-down list box to display related IPv6 FQDN object caches used in DNS queries.
#	This is the index number of the IPv6 FQDN entry.
Name	This field displays the name of the selected IPv6 FQDN object used in DNS queries.
FQDN	This field displays a host's fully qualified domain name.
IP Address	This field displays the mapping of the FQDN to an IPv6 address. This is the IPv6 address of a host.
TTL	This field displays the number of seconds the Zyxel Device holds IP address - FQDN object mapping in its cache. The mapping is updated when the TTL (Time To Live) setting expires.
Refresh	Click this button to update the information in the screen.

6.15 AP Information: AP List

The **AP Information** menu contains **AP List, Radio List, Top N APs** and **Single AP** screens. Click **Monitor > Wireless > AP Information** to display the **AP List** screen.

Figure 120 Monitor > Wireless > AP Information > AP List



The following table describes the labels in this screen.

Table 44 Monitor > Wireless > AP Information > AP List

LABEL	DESCRIPTION
Config AP	Select an AP and click this to change the selected AP's group, radio, VLAN and port settings.
Add to Mgnt AP List	Click this to add new Access Points
More Information	Click this icon to see AP Information and Station count.
Reboot	Select an AP and click this button to force it 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. Note: You should have enabled DCS in the applied AP radio profile before the APs can use DCS. Note: DCS is not supported on the radio which is working in repeater AP mode.

Table 44 Monitor > Wireless > AP Information > AP List (continued)

LABEL	DESCRIPTION
Log	Select an AP and click this button to go to the **Monitor > Log > View AP Log** screen to view the selected AP's current log messages.
Suppression On	Click this button to turn suppression on.
Suppression Off	Click this button to turn suppression off.
#	This field is a sequential value, and it is not associated with a specific AP.
Status	This field displays the on-line or off-line status of the AP, move the cursor to the AP icon and a status pop up message will appear.
Description	This field displays the AP's description, which you can configure by selecting the AP's entry and clicking the **Edit** button.
CPU Usage	This field displays what percentage of the AP's processing capability is currently being used.
IP Address	This field displays the IP 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 Zyxel Device and the information is unavailable as a result.
Group	This displays the name of the AP group to which the AP belongs.
Station	This field displays the station count information.
Recent On-line Time	This field displays the latest date and time that the AP was logged on.
Registration	This field displays the registration information of the AP. You can set the AP's registration at Configuration > Wireless > Controller screen. APs must be connected to the Zyxel Device by a wired connection or network.
MAC Address	This field displays the MAC address of the AP.
Mgnt. VLAN ID (AC/AP)	This displays the Access Controller (the Zyxel Device) and runtime management VLAN ID setting for the AP. **VLAN Conflict** displays if the AP's management VLAN ID does not match the **Mgmnt. VLAN ID(AC)**. This field displays **n/a** if the Zyxel Device cannot get VLAN information from the AP.
Last Off-line Time	This field displays the date and time that the AP was last logged out.

Table 44 Monitor > Wireless > AP Information > AP List (continued)

LABEL	DESCRIPTION
LED Status	This field displays the AP LED status. **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. 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. A green LED icon signifies that the AP LED suppression mode is disabled and the AP LEDs stay lit after the AP is ready. A sun icon signifies that the AP's locator LED is blinking. A circle signifies that the AP's locator LED is extinguished.
Power Mode	This field displays the AP's power status. **Full** - the AP receives power using a power adapter and/or through a PoE switch/ injector using IEEE 802.3at PoE plus. The PoE device that supports IEEE 802.3at PoE Plus can supply power of up to 30W per Ethernet port. **Limited** - the AP receives power through a PoE switch/injector using IEEE 802.3af PoE even when it is also connected to a power source using a power adaptor. The PoE device that supports IEEE 802.3af PoE can supply power of up to 15.4W per Ethernet port. When the AP is in limited power mode, the AP throughput decreases and has just one transmitting radio chain. It always shows Full if the AP does not support power detection.

The following table describes the icons in this screen.

Table 45 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: • This AP has a runtime management VLAN ID setting that conflicts with the VLAN ID setting on the Access Controller (the Zyxel Device). • A setting the Zyxel Device assigns to this AP does not match the AP's capability.

6.15.1 AP List: 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 121 Monitor > Wireless > AP Information > AP List > More Information

The following table describes the labels in this screen.

Table 46 Monitor > Wireless > AP Information > AP List > More Information

LABEL	DESCRIPTION
Configuration Status	This displays whether or not any of the AP's configuration is in conflict with the Zyxel Device's settings for the AP.
Non Support	If any of the AP's configuration conflicts with the Zyxel Device'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 Zyxel Device's settings for the AP.
Port Status	
Port	This shows the name of the physical Ethernet port on the Zyxel Device.

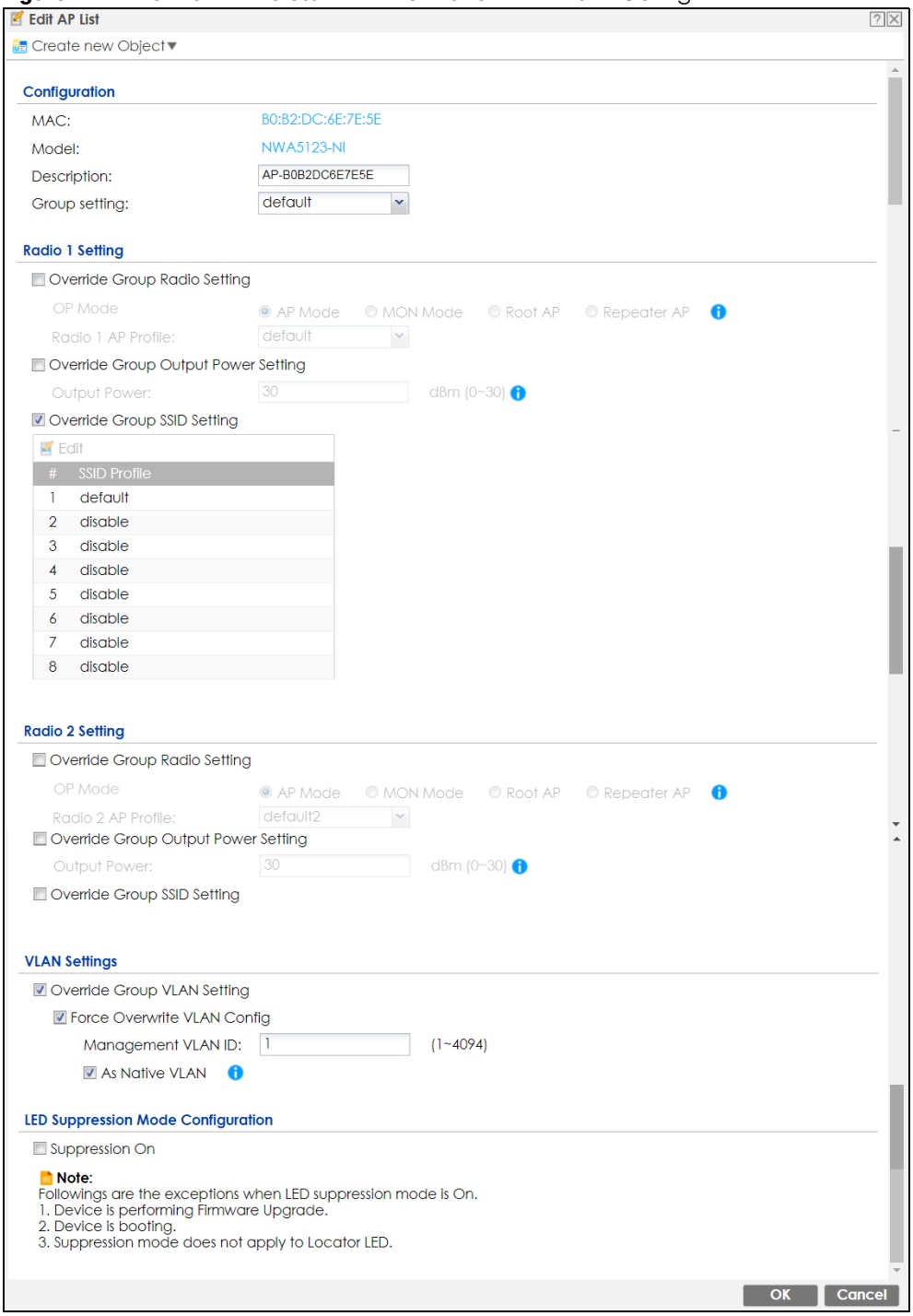
Table 46 Monitor > Wireless > AP Information > AP List > More Information (continued)

LABEL	DESCRIPTION
Status	This field displays the current status of each physical port on the AP. **Down** - The port is not connected. **Speed / Duplex** - The port is connected. This field displays the port speed and duplex setting (**Full** or **Half**).
PVID	This shows the port's PVID. A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines.
Up Time	This field displays how long the physical port has been connected.
VLAN Configuration	
Name	This shows the name of the VLAN.
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.
Ethernet Neighbor	
Local Port (Description)	This field displays the port of the Zyxel Device, on which the neighboring device is discovered. For Zyxel Devices that support **Port Role**, if ports 3 to 5 are grouped together and there is a connection to P5 only, the Zyxel Device will display P3 as the interface port number (even though there is no connection to that port).
Model Name	This field displays the model name of the discovered device.
System Name	This field displays the system name of the discovered device.
Firmware Version	This field displays the firmware version of the discovered device.
Port (Description)	This field displays the first internal port on the discovered device. Internal is an interface type displayed in the **Network > Interface > Ethernet > Edit** screen. For example, if P1 and P2 are WAN, P3 to P5 are LAN, and P6 is DMZ, then Zyxel Device will display P3 as the first internal interface port number. For Zyxel Devices that support **Port Role**, if ports 3 to 5 are grouped together and there is a connection to P5 only, the Zyxel Device 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 Address	This field displays the MAC address of the discovered device.
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 Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

6.15.2 AP List: Config AP

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

Figure 122 Monitor > Wireless > AP Information > AP List > Config AP



Each field is described in the following table.

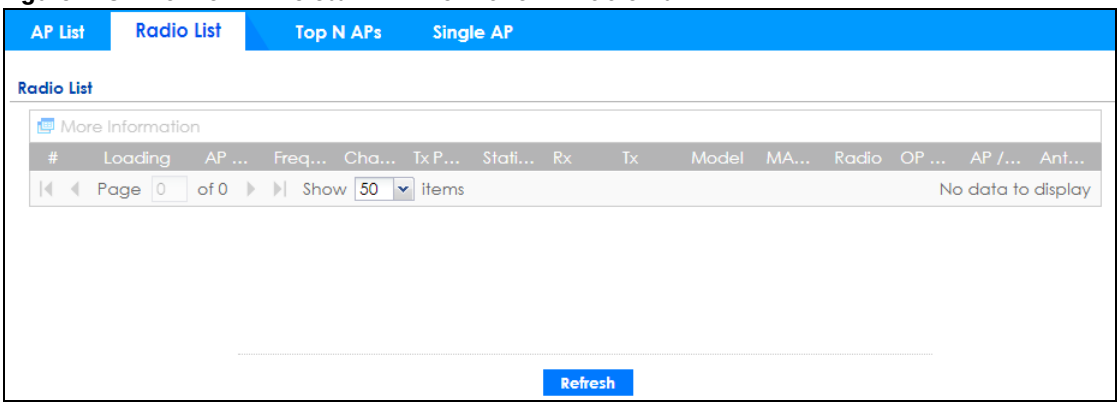
Table 47 Monitor > Wireless > AP Information > AP List > Config AP

LABEL	DESCRIPTION
Create new Object	Use this menu to create a new **Radio Profile** object to associate with this AP.
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 Zyxel Device 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 an AP group to which you want this AP to belong.
Radio 1/2 Setting	
Override Group Radio Setting	Select this option to overwrite the AP radio settings with the settings you configure here.
Radio 1/2 OP Mode	Select the operating mode for radio 1 or radio 2. **AP Mode** means the AP can receive connections from wireless clients and pass their data traffic through to the Zyxel Device to be managed (or subsequently passed on to an upstream gateway for managing). **MON Mode** means the AP monitors the broadcast area for other APs, then passes their information on to the Zyxel Device 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.
Radio 1/2 Profile	Select a 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 output power of the AP.
Override Group SSID Setting	Select this option to overwrite the AP SSID profile setting with the setting you configure here. 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.
Override Group VLAN Setting	Select this option to overwrite the AP VLAN setting with the setting you configure here.
Force Overwrite VLAN Config	Select this to have the Zyxel Device 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 Zyxel Device and not one assigned to it from outside the network.
Suppression On	Select this option to enable the AP's LED suppression mode. All the LEDs of the AP will turn off after the AP is ready. If the check box is unchecked, it means the LEDs will stay lit after the AP is ready.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to close the window with changes unsaved.

6.16 AP Information: Radio List

Click **Monitor > Wireless > AP Information > Radio List** to display the **Radio List** screen.

Figure 123 Monitor > Wireless > AP Information > Radio List



The following table describes the labels in this screen.

Table 48 Monitor > Wireless > AP Information > Radio List

LABEL	DESCRIPTION
More Information	Click this icon to see the traffic statistics, station count, SSID, Security Mode and VLAN ID information on the AP.
#	This field is a sequential value, and it is not associated with a specific radio.
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	Enter a description for this AP. You can use up to 31 characters, spaces and underscores allowed.
Frequency Band	This field displays the WLAN frequency band using the IEEE 802.11 a/b/g/n standard of 2.4 or 5 GHz.
Channel ID	This field displays the WLAN channels using the IEEE 802.11 protocols.
Tx Power	This shows the radio's output power (in dBm).
Station	This field displays the station count information.
Rx	This field displays the total number of bytes received by the radio.
Tx	This field displays the total number of bytes transmitted by the radio.
Model	This field displays the AP's hardware model information. It displays **N/A** (not applicable) only when the AP disconnects from the Zyxel Device and the information is unavailable as a result.
MAC Address	This field displays the MAC address of the AP.
Radio	This field displays the Radio number. For example 1.
OP Mode	This field displays the operating mode of the AP. It displays **n/a** for the profile for a radio not using an AP profile. **AP Mode** means the AP can receive connections from wireless clients and pass their data traffic through to the Zyxel Device to be managed (or subsequently passed on to an upstream gateway for managing).

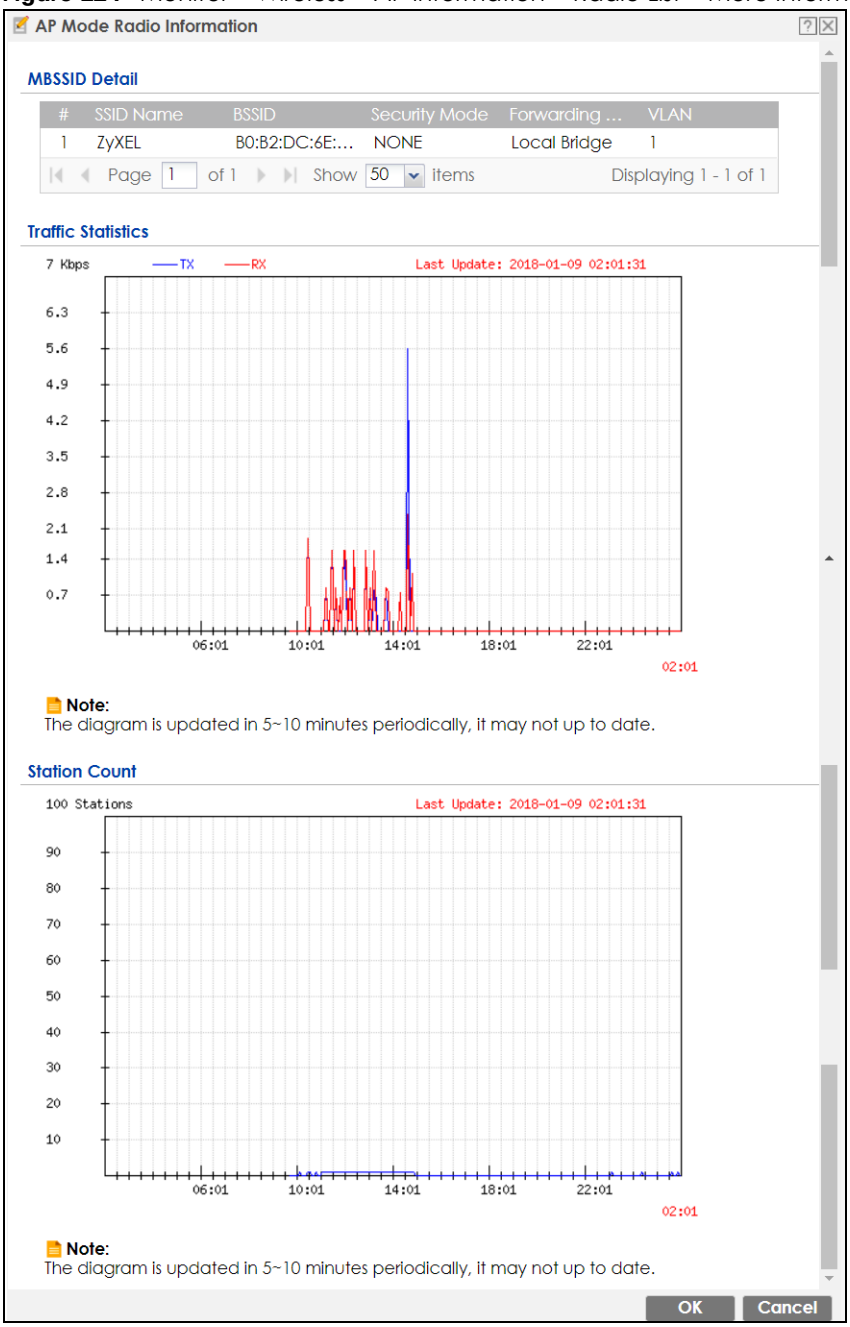
Table 48 Monitor > Wireless > AP Information > Radio List

LABEL	DESCRIPTION
AP / ZyMesh Profile	This indicates the AP radio and ZyMesh profile names to which the radio belongs.
Antenna	This indicates the antenna orientation for the radio (**Wall** or **Ceiling**). 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.

6.16.1 Radio List: More 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 124 Monitor > Wireless > AP Information > Radio List > More Information



The following table describes the labels in this screen.

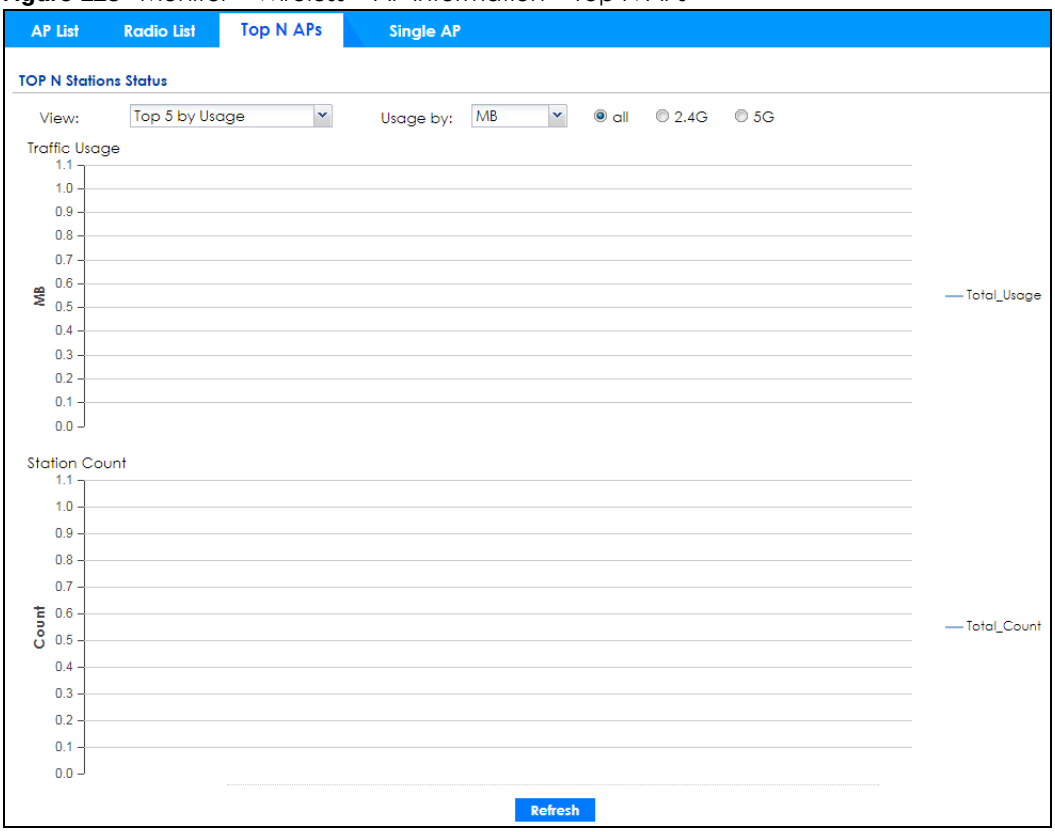
Table 49 Monitor > Wireless > AP Information > Radio List > More Information

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.
Forwarding Mode	This field indicates the forwarding mode (**Local Bridge** or **Tunnel**) associated with the SSID profile.
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.

6.17 AP Information: Top N APs

Use this screen to view the top five or top ten wireless traffic usage and associated wireless stations for the preceding 24 hours. Click **Monitor > Wireless > AP Information > Top N APs** to display the **Top N APs** screen.

Figure 125 Monitor > Wireless > AP Information > Top N APs



The following table describes the labels in this screen.

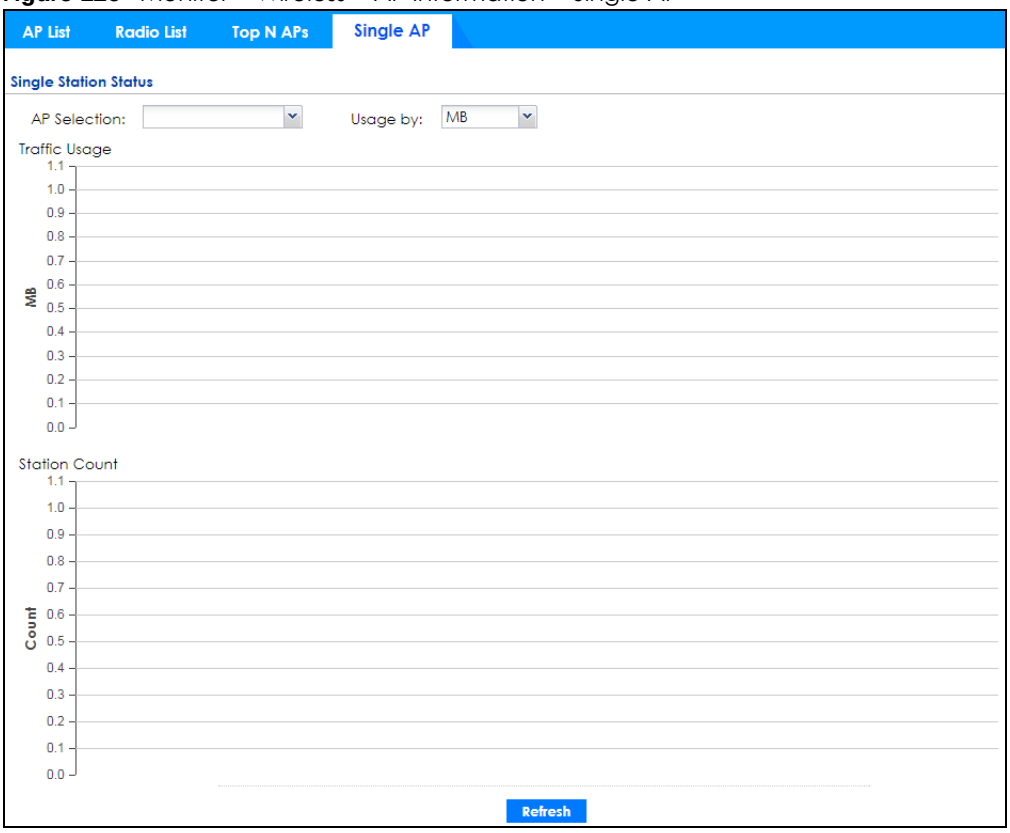
Table 50 Monitor > Wireless > AP Information > Top N APs

LABEL	DESCRIPTION
View	Select this to view the top five or top ten wireless traffic usage and associated wireless stations for the preceding 24 hours.
Usage by	If you view the data usage by **Usage**, select the frequency band and the measure unit in GB or MB to display the graph. If you view the date usage by **Station Number**, select the measure unit in GB or MB to display the graph.
Traffic Usage	This graph displays the overall traffic information about the top five or top ten wireless traffic for the preceding 24 hours.
y-axis	The y-axis represents the amount of traffic in megabytes/gigabytes.
x-axis	The x-axis represents the time over which wireless traffic flows transmitting from/to the AP.
Station Count	This graph displays information about all the wireless stations that have connected to the AP for the preceding 24 hours.
y-axis	The y-axis represents the number of connected wireless stations.
x-axis	The x-axis represents the time over which a wireless client was connected.
Refresh	Click **Refresh** to update this screen.

6.18 AP Information: Single AP

Use this screen to view wireless traffic usage and wireless stations for a managed AP. Click **Monitor > Wireless > AP Information > Single AP** to display the **Single AP** screen.

Figure 126 Monitor > Wireless > AP Information > Single AP



The following table describes the labels in this screen.

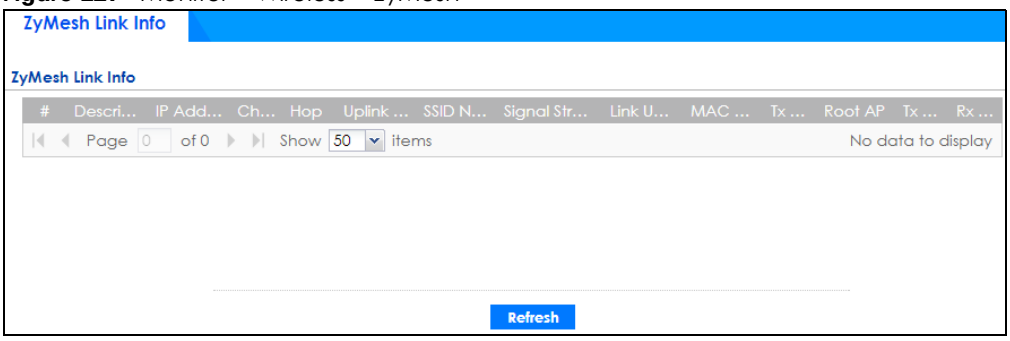
Table 51 Monitor > Wireless > AP Information > Single AP

LABEL	DESCRIPTION
AP Selection	Select a managed AP from the drop-down list box to view its wireless traffic usage and wireless stations.
Usage by	Select the measure unit in GB or MB to display the graph.
Traffic Usage	This graph displays the overall traffic information about the AP you specified for the preceding 24 hours.
y-axis	The y-axis represents the amount of traffic in megabytes/gigabytes.
x-axis	The x-axis represents the time over which wireless traffic flows transmitting from/to the AP.
Station Count	This graph displays information about all the wireless stations that have connected to the AP for the preceding 24 hours.
y-axis	The y-axis represents the number of connected wireless stations.
x-axis	The x-axis represents the time over which a wireless client was connected.
Refresh	Click **Refresh** to update this screen.

6.19 ZyMesh

Use this screen to view the ZyMesh traffic statistics between the managed APs. Click **Monitor > Wireless > ZyMesh** to display this screen.

Figure 127 Monitor > Wireless > ZyMesh



The following table describes the labels in this screen.

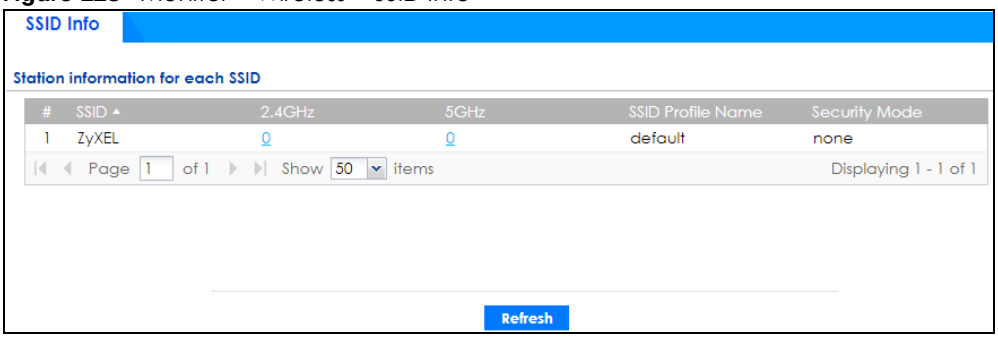
Table 52 Monitor > Wireless > ZyMesh

LABEL	DESCRIPTION
#	This field displays the index number of the managed AP (in repeater mode) in this list.
Description	This field displays the descriptive name of the managed AP (in repeater mode).
IP Address	This field displays the IP address of the managed AP (in repeater mode).
Channel ID	This field displays the number of the channel used by the managed AP (in repeater mode).
Hop	This is the hop count of the managed AP. For example, "1" means the managed AP is connected to a root AP directly. "2" means there is another repeater AP between the managed AP and the root AP.
Uplink AP Info	This shows the role and descriptive name of the managed AP to which this managed AP is connected wirelessly.
SSID Name	This indicates the name of the wireless network (SSID) the managed AP uses to associated with another managed AP.
Signal Strength	Before the slash, this shows the signal strength the uplink AP (a root AP or a repeater) receives from this managed AP (in repeater mode). After the slash, this shows the signal strength this managed AP (in repeater mode) receives from the uplink AP.
Link Up Time	This field displays the time the managed AP first associated with the root AP or repeater.
MAC Address	This field displays the MAC address of the managed AP (in repeater mode).
Tx Power	This field displays the output power of the managed AP (in repeater mode).
Root AP	This field displays the descriptive name of the root AP to which the managed AP is connected wirelessly.
Tx Rate	This field displays the maximum transmission rate of the root AP or repeater to which the managed AP is connected.
Rx Rate	This field displays the maximum reception rate of the root AP or repeater to which the managed AP is connected.
Refresh	Click **Refresh** to update this screen.

6.20 SSID Info

Use this screen to view the number of wireless clients currently connected to an SSID and the security type used by the SSID. Click **Monitor > Wireless > SSID Info** to display this screen.

Figure 128 Monitor > Wireless > SSID Info



The following table describes the labels in this screen.

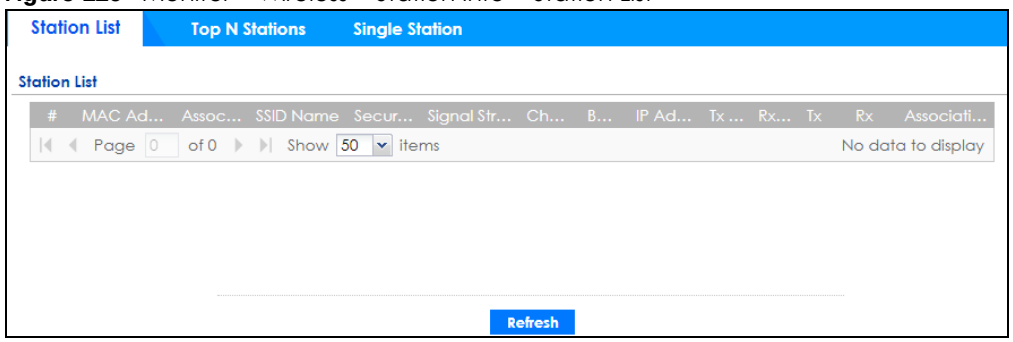
Table 53 Monitor > Wireless > SSID Info

LABEL	DESCRIPTION
#	This is the SSID's index number in this list.
SSID	This indicates the name of the wireless network to which the client is connected. A single AP can have multiple SSIDs or networks.
2.4GHz	This shows the number of wireless clients which are currently connected to the SSID using the 2.4 GHz frequency band, Click the number to go to the **Station Info > Station List** screen. See Section 6.22 on page 159.
5GHz	This shows the number of wireless clients which are currently connected to the SSID using the 5 GHz frequency band, Click the number to go to the **Station Info > Station List** screen. See Section 6.22 on page 159.
SSID Profile Name	This indicates the name of the SSID profile in which the SSID is defined,
Security Mode	This indicates which secure encryption methods is being used by the SSID.
Refresh	Click **Refresh** to update this screen.

6.21 Station Info: Station List

The **Station Info** menu contains **Station List**, **Top N Stations** and **Single Station** screens. This screen displays information about connected wireless stations. Click **Monitor > Wireless > Station Info > Station List** to display this screen.

Figure 129 Monitor > Wireless > Station Info > Station List



The following table describes the labels in this screen.

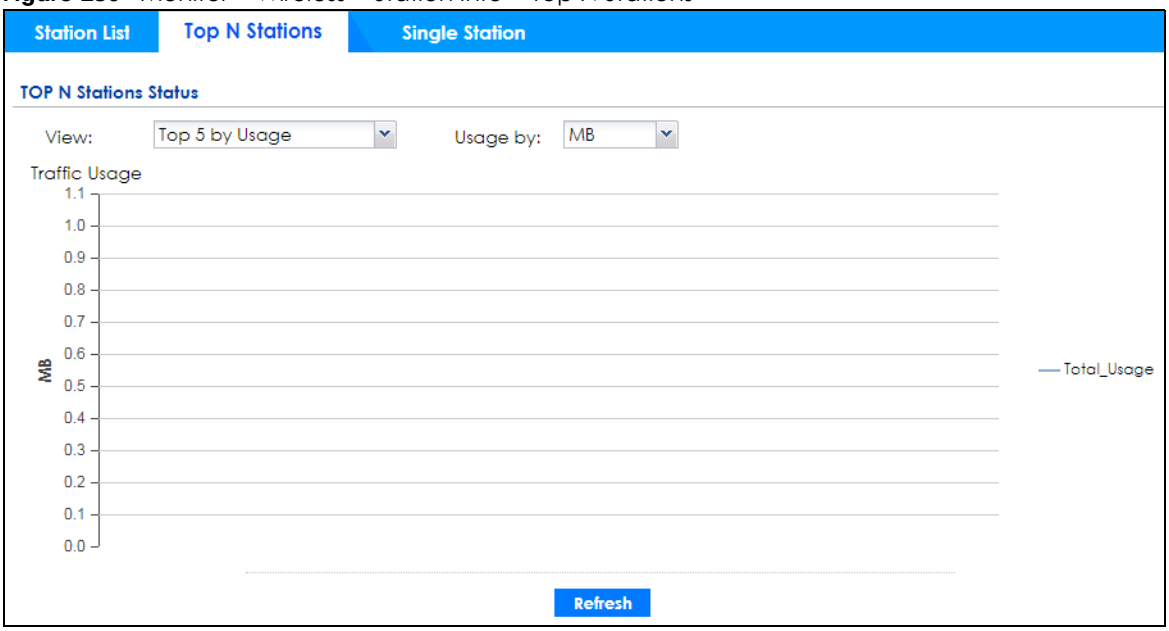
Table 54 Monitor > Wireless > Station Info > Station List

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific station.
MAC Address	This field displays the MAC address of the station.
Associated AP	This field displays the APs that are associated with the station.
SSID Name	This field displays the SSID names of the station.
Security Mode	This field displays the security mode the station is using.
Signal Strength	This field displays the signal strength of the station.
Channel	This field displays the number of the channel used by the station to connect to the network.
Band	This field displays the frequency band which is currently being used by the station.
IP Address	This field displays the IP address of the station.
Tx Rate	This field displays the transmit data rate of the station.
Rx Rate	This field displays the receive data rate of the station.
Tx	This field displays the number of bytes transmitted from the station.
Rx	This field displays the number of bytes received by the station.
Association Time	This field displays the time duration the station was online and offline.
Refresh	Click **Refresh** to update this screen.

6.22 Station Info: Top N Stations

Use this screen to view the top five or top ten traffic statistics of the wireless stations. Click **Monitor > Wireless > Station Info > Top N Stations** to display this screen.

Figure 130 Monitor > Wireless > Station Info > Top N Stations



The following table describes the labels in this screen.

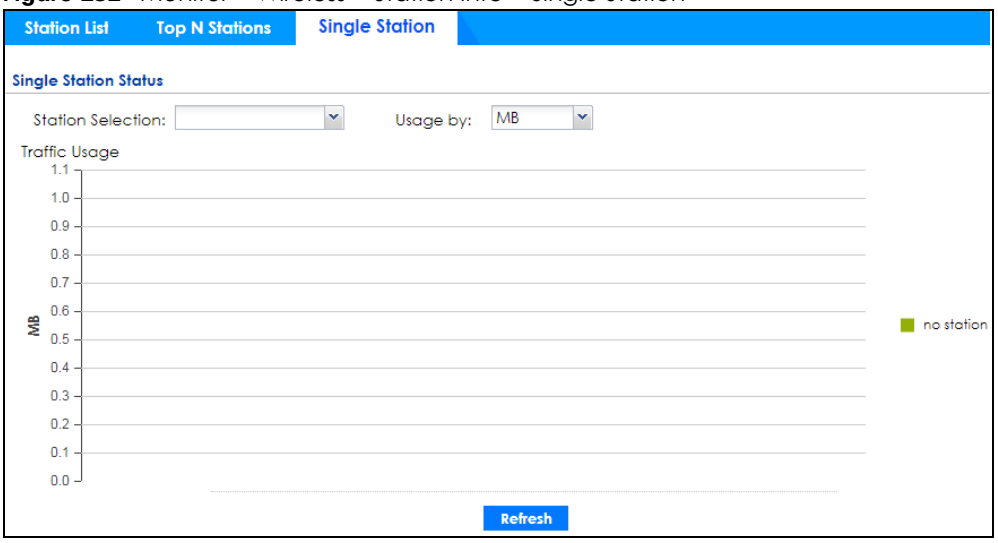
Table 55 Monitor > Wireless > Station Info > Top N Stations

LABEL	DESCRIPTION
View	Select this to view the top five or top ten traffic statistics of the wireless stations.
Usage by	Select the measure unit in GB or MB to display the graph.
Traffic Usage	This graph displays the overall traffic information about the stations for the preceding 24 hours.
y-axis	This axis represents the amount of data moved across stations in megabytes per second.
Refresh	Click **Refresh** to update this screen.

6.23 Station Info: Single Station

Use this screen to view traffic statistics of the wireless station you specified. Click **Monitor > Wireless > Station Info > Single Station** to display this screen.

Figure 131 Monitor > Wireless > Station Info > Single Station



The following table describes the labels in this screen.

Table 56 Monitor > Wireless > Station Info > Single Station

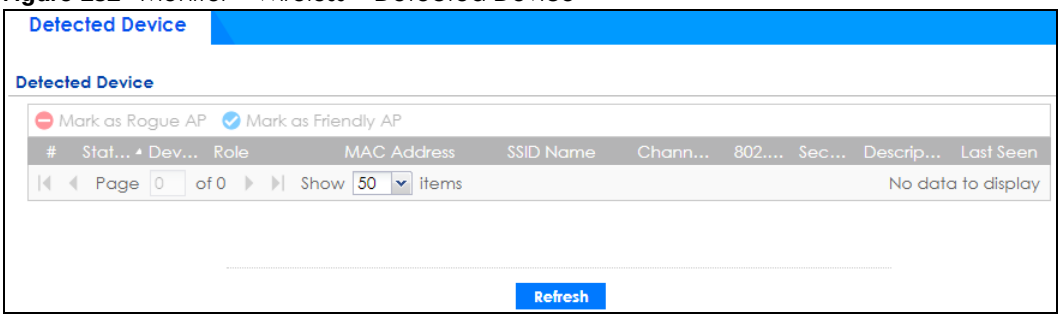
LABEL	DESCRIPTION
Station Selection	Select this to view the traffic statistics of the wireless station.
Usage by	Select the measure unit in GB or MB to display the graph.
Traffic Usage	This graph displays the overall traffic information about the station over the preceding 24 hours.
y-axis	This axis represents the amount of data moved across this station in megabytes per second.
Refresh	Click **Refresh** to update this screen.

6.24 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 Zyxel Device must be set to monitor mode (in the **Configuration > Wireless > AP Management** screen) in order to detect other wireless devices in its vicinity.

Figure 132 Monitor > Wireless > Detected Device



The following table describes the labels in this screen.

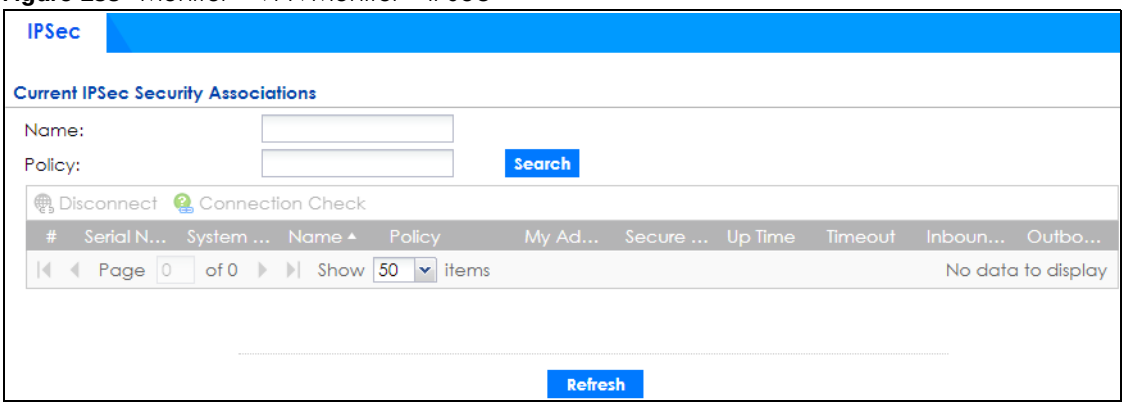
Table 57 Monitor > Wireless > Detected Device

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.
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.
#	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.
Last Seen	This indicates the last time the device was detected by the Zyxel Device.
Refresh	Click this to refresh the items displayed on this page.

6.25 The IPSec Screen

You can use the **IPSec Monitor** 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 133 Monitor > VPN Monitor > IPSec



Each field is described in the following table.

Table 58 Monitor > VPN Monitor > IPSec

LABEL	DESCRIPTION
Name	Type 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 _+-.()!$*^:? | {}[]<>/ characters. See Section on page 163 for more details.
Policy	Type the IP address(es) or names of the local and remote policies for an IPSec SA and click **Search** to find it. You can use a keyword or regular expression. Use up to 30 alphanumeric and _+-.()!$*^:? | {}[]<>/ characters. See Section on page 163 for more details.
Search	Click this button to search for an IPSec SA that matches the information you specified above.
Disconnect	Select an IPSec SA and click this button to disconnect it.
Connection Check	Select an IPSec SA and click this button to check the connection.
#	This field is a sequential value, and it is not associated with a specific SA.
Serial Number	This field displays the serial number of this Zyxel Device.
System Name	This field displays the name used to identify the Zyxel Device.
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.
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. This field displays **N/A** if the IPSec SA uses manual keys.
Timeout	This field displays how many seconds remain in the SA life time, before the Zyxel Device automatically disconnects the IPSec SA. This field displays **N/A** if the IPSec SA uses manual keys.
Inbound (Bytes)	This field displays the amount of traffic that has gone through the IPSec SA from the remote IPSec router to the Zyxel Device since the IPSec SA was established.
Outbound (Bytes)	This field displays the amount of traffic that has gone through the IPSec SA from the Zyxel Device to the remote IPSec router since the IPSec SA was established.

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 Zyxel Device 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.

6.26 The SSL Screen

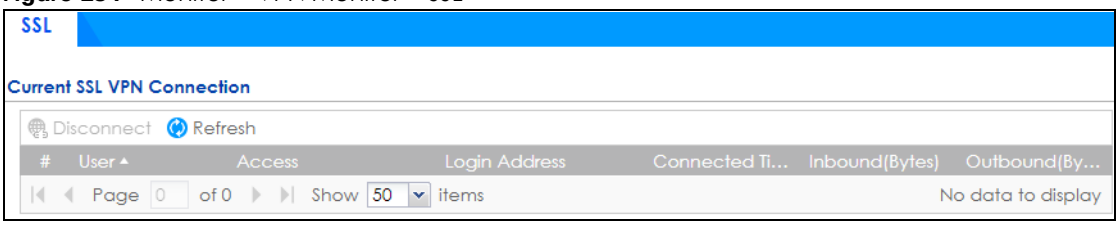
The Zyxel Device keeps track of the users who are currently logged into the VPN SSL client. Click **Monitor > VPN Monitor > SSL** to display the user list.

Use this screen to do the following:

- View a list of active SSL VPN connections.
- Log out individual users and delete related session information.

Once a user logs out, the corresponding entry is removed from the screen.

Figure 134 Monitor > VPN Monitor > SSL



The following table describes the labels in this screen.

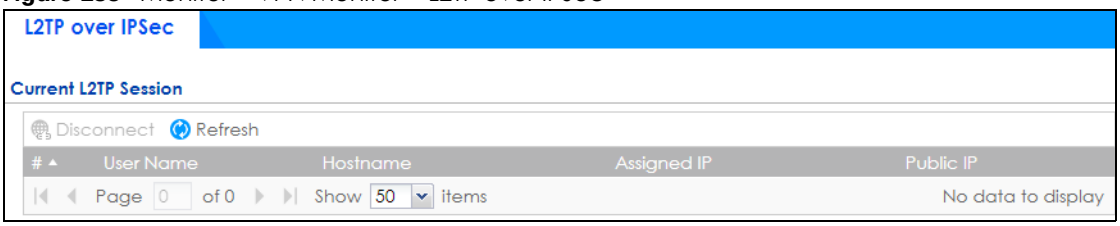
Table 59 Monitor > VPN Monitor > SSL

LABEL	DESCRIPTION
Disconnect	Select a connection and click this button to terminate the user's connection and delete corresponding session information from the Zyxel Device.
Refresh	Click **Refresh** to update this screen.
#	This field is a sequential value, and it is not associated with a specific SSL.
User	This field displays the account user name used to establish this SSL VPN connection.
Access	This field displays the name of the SSL VPN application the user is accessing.
Login Address	This field displays the IP address the user used to establish this SSL VPN connection.
Connected Time	This field displays the time this connection was established.
Inbound (Bytes)	This field displays the number of bytes received by the Zyxel Device on this connection.
Outbound (Bytes)	This field displays the number of bytes transmitted by the Zyxel Device on this connection.

6.27 The L2TP over IPSec Screen

Click **Monitor > VPN Monitor > L2TP over IPSec** to open the following screen. Use this screen to display and manage the Zyxel Device's connected L2TP VPN sessions.

Figure 135 Monitor > VPN Monitor > L2TP over IPSec



The following table describes the fields in this screen.

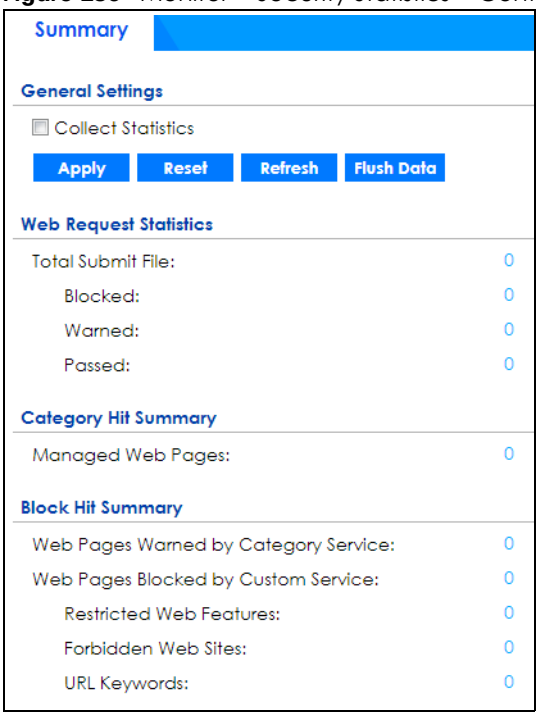
Table 60 Monitor > VPN Monitor > L2TP over IPSec

LABEL	DESCRIPTION
Disconnect	Select a connection and click this button to disconnect it.
Refresh	Click **Refresh** to update this screen.
#	This field is a sequential value, and it is not associated with a specific L2TP VPN session.
User Name	This field displays the remote user's user name.
Hostname	This field displays the name of the computer that has this L2TP VPN connection with the Zyxel Device.
Assigned IP	This field displays the IP address that the Zyxel Device assigned for the remote user's computer to use within the L2TP VPN tunnel.
Public IP	This field displays the public IP address that the remote user is using to connect to the Internet.

6.28 The Content Filter Screen

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

Figure 136 Monitor > Security Statistics > Content Filter



The following table describes the labels in this screen.

Table 61 Monitor > Security Statistics > Content Filter

LABEL	DESCRIPTION
General Settings	
Collect Statistics	Select this check box to have the Zyxel Device collect content filtering statistics. The collection starting time displays after you click **Apply**. All of the statistics in this screen are for the time period starting at the time displayed here. The format is year, month, day and hour, minute, second. All of the statistics are erased if you restart the Zyxel Device or click **Flush Data**. Collecting starts over and a new collection start time displays.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
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 Submit File	This field displays the number of web pages that the Zyxel Device's content filter feature has checked.
Blocked	This is the number of web pages that the Zyxel Device blocked access.
Warned	This is the number of web pages for which the Zyxel Device displayed a warning message to the access requesters.
Passed	This is the number of web pages to which the Zyxel Device allowed access.
Category Hit Summary	
Managed Web Pages	This is the number of requested web pages that the Zyxel Device's content filtering service identified as belonging to a category that was selected to be managed.
Block Hit Summary	

Table 61 Monitor > Security Statistics > Content Filter (continued)

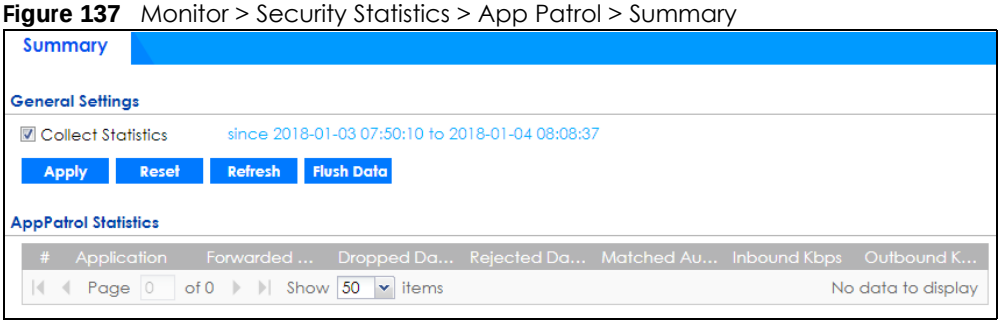
LABEL	DESCRIPTION
Web Pages Warned by Category Service	This is the number of web pages that matched an external database content filtering category selected in the Zyxel Device and for which the Zyxel Device displayed a warning before allowing users access.
Web Pages Blocked by Custom Service	This is the number of web pages to which the Zyxel Device 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 ZyWALL 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 Zyxel Device 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 Zyxel Device did not allow access because they contained one of the content filtering custom service's list of forbidden keywords.

6.29 The App Patrol Screen

Application patrol provides a convenient way to manage the use of various applications on the network. It manages general protocols (for example, HTTP and FTP) and instant messenger (IM), peer-to-peer (P2P), Voice over IP (VoIP), and streaming (RSTP) applications. You can even control the use of a particular application's individual features (like text messaging, voice, video conferencing, and file transfers).

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

Figure 137 Monitor > Security Statistics > App Patrol > Summary



The following table describes the labels in this screen.

Table 62 Monitor > Security Statistics > App Patrol > Summary

LABEL	DESCRIPTION
Collect Statistics	Select this check box to have the Zyxel Device collect app patrol statistics. The collection starting time displays after you click **Apply**. All of the statistics in this screen are for the time period starting at the time displayed here. The format is year, month, day and hour, minute, second. All of the statistics are erased if you restart the Zyxel Device or click **Flush Data**. Collecting starts over and a new collection start time displays.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

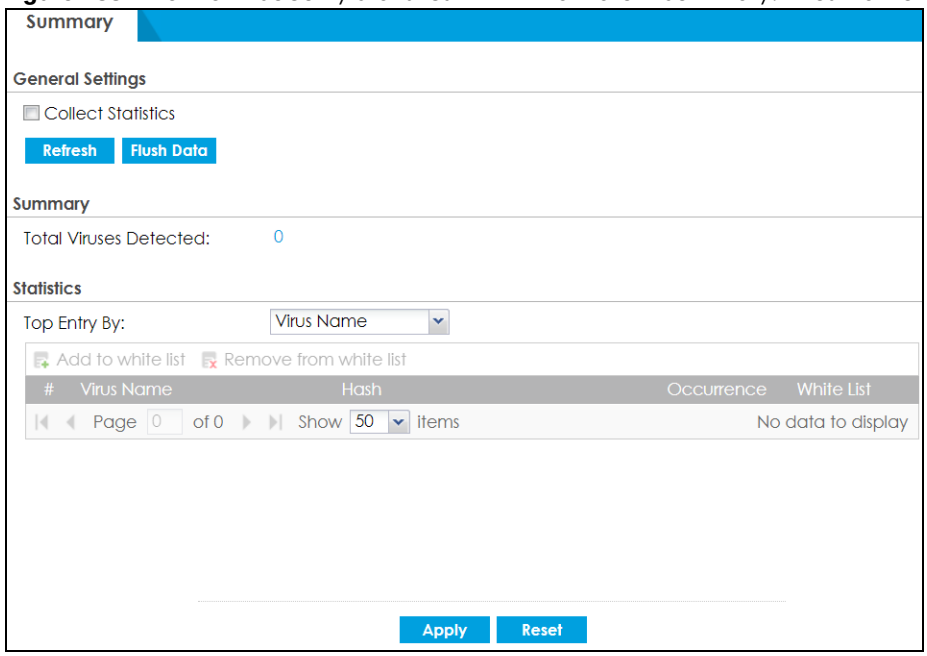
Table 62 Monitor > Security Statistics > App Patrol > Summary

LABEL	DESCRIPTION
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 Zyxel Device has sent (in kilobytes).
Dropped Data (KB)	This is how much of the application's traffic the Zyxel Device 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 Zyxel Device 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 Zyxel Device identified by examining the IP payload.
Inbound Kbps	This field displays the amount of the application's traffic that has gone to the ZyWALL (in kilo bits per second).
Outbound Kbps	This field displays the amount of the application's traffic that has gone from the ZyWALL (in kilo bits per second).

6.30 The Anti-Malware Screen

Click **Monitor > Security Statistics > Anti-Malware > Summary** to display the following screen. This screen displays anti-malware statistics.

Figure 138 Monitor > Security Statistics > Anti-Malware > Summary: Virus Name



The following table describes the labels in this screen.

Table 63 Monitor > Security Statistics > Anti-Malware > Summary: Virus Name

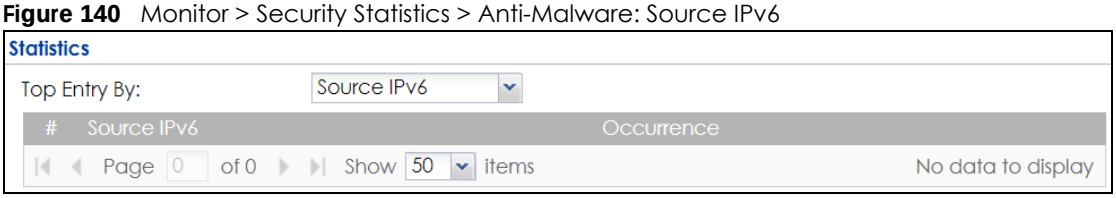
LABEL	DESCRIPTION
Collect Statistics	Select this check box to have the Zyxel Device collect anti-malware statistics. The collection starting time displays after you click **Apply**. All of the statistics in this screen are for the time period starting at the time displayed here. The format is year, month, day and hour, minute, second. All of the statistics are erased if you restart the Zyxel Device or click **Flush Data**. Collecting starts over and a new collection start time displays.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
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.
Total Viruses Detected	This field displays the number of different viruses that the Zyxel Device has detected.
Top Entries By	Use this field to have the following (read-only) table display the top anti-malware log entries by **Virus Name**, **Source IP**, and **Destination IP, Source IPv6** and **Destination IPv6**. This table displays the most common, recent virus logs. See the log screen for less common virus logs or use a syslog server to record all virus logs. Select **Virus Name** to list the most common viruses that the Zyxel Device has detected. Select **Source IP** to list the source IP addresses from which the Zyxel Device has detected the most virus-infected files. Select **Destination IP** to list the most common destination IP addresses for virus-infected files that Zyxel Device has detected. Select **Source IPv6** to list the source IPv6 addresses from which the Zyxel Device has detected the most virus-infected files. Select **Destination IPv6** to list the most common destination IPv6 addresses for virus-infected files that Zyxel Device has detected.
Add to white list	Select an entry and click this to add it to the anti-malware white list.
Remove from white list	Select an entry and click this to remove it from the anti-malware white list.
#	This field displays the entry's rank in the list of the top entries.
Virus name	This column displays when you display the entries by **Virus Name**. This displays the name of a detected virus.
Hash	This column displays a hash value, MD5 (Message Digest 5) and SHA (Secure Hash Algorithm), of the detected virus file. MD5 and SHA are hash algorithms used to authenticate packet data.
Source IP	This column displays when you display the entries by **Source IP.** It shows the source IP address of virus-infected files that the Zyxel Device has detected.
Source IPv6	his column displays when you display the entries by **Source IPv6.** It shows the source IPv6 address of virus-infected files that the Zyxel Device has detected.
Destination IP	This column displays when you display the entries by **Destination IP.** It shows the destination IP address of virus-infected files that the Zyxel Device has detected.
Destination IPv6	This column displays when you display the entries by **Destination IPv6.** It shows the destination IPv6 address of virus-infected files that the Zyxel Device has detected.
Occurrences	This field displays how many times the Zyxel Device has detected the event described in the entry.
White List	Click this to add this signature to the anti-malware white list. Click this to remove this signature from the anti-malware white list.

The statistics display as follows when you display the top entries by source IP.

Figure 139 Monitor > Security Statistics > Anti-Malware > Summary: Source IP

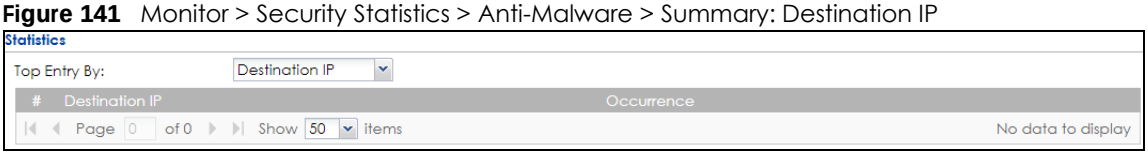
The statistics display as follows when you display the top entries by source IPv6.

Figure 140 Monitor > Security Statistics > Anti-Malware: Source IPv6



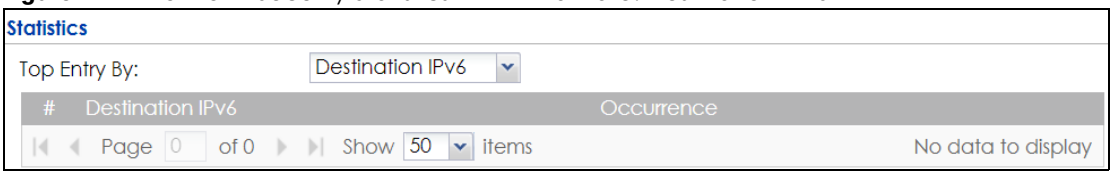
The statistics display as follows when you display the top entries by destination IP.

Figure 141 Monitor > Security Statistics > Anti-Malware > Summary: Destination IP



The statistics display as follows when you display the top entries by destination IPv6.

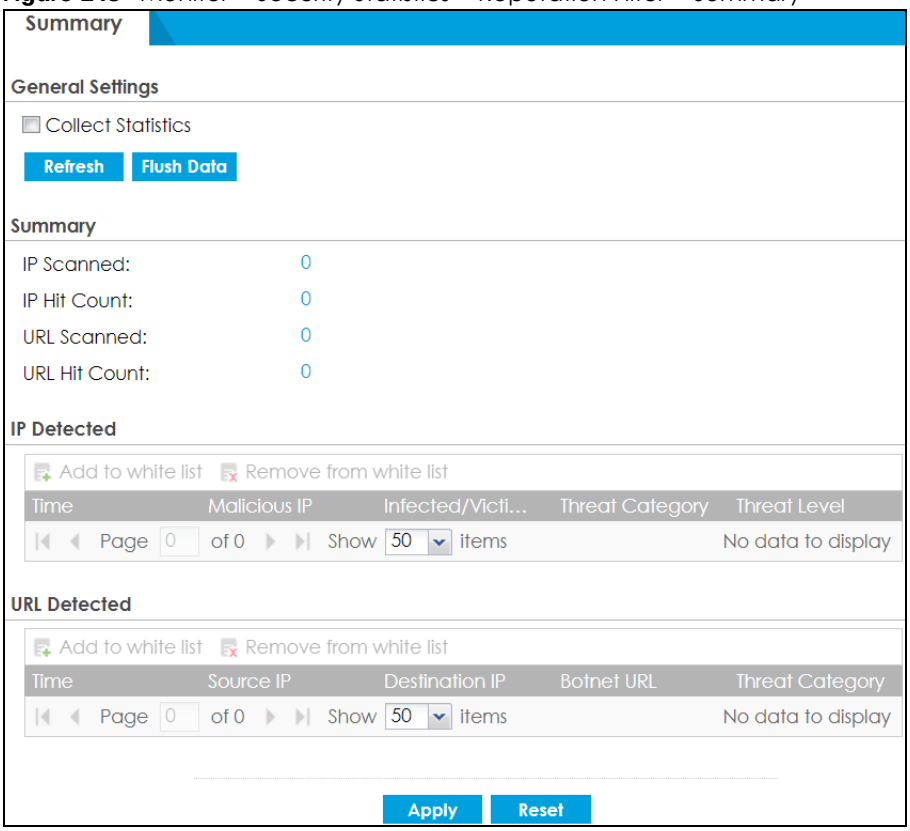
Figure 142 Monitor > Security Statistics > Anti-Malware: Destination IPv6



6.31 The Reputation Filter Screen

Click **Monitor > Security Statistics > Reputation Filter > Summary** to display the following screen. This screen displays statistics of IP reputation and botnet filtering.

Figure 143 Monitor > Security Statistics > Reputation Filter > Summary



The following table describes the labels in this screen.

Table 64 Monitor > Security Statistics > Reputation Filter > Summary

LABEL	DESCRIPTION
Collect Statistics	Select this check box to have the Zyxel Device collect anti-malware statistics. The collection starting time displays after you click **Apply**. All of the statistics in this screen are for the time period starting at the time displayed here. The format is year, month, day and hour, minute, second. All of the statistics are erased if you restart the Zyxel Device or click **Flush Data**. Collecting starts over and a new collection start time displays.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
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.
Summary	
IP Scanned	This field displays the total number of IPv4 addresses that have been scanned.
IP Hit Count	This field displays the total number of the hit counts on the scanned IPv4 addresses.
URL Scanned	This field displays the total number of URLs that have been scanned.
URL Hit Count	This field displays the total number of the hit counts on the scanned URLs.
IP Detected	
Add to white list	Select an entry and click this to add it to the IP reputation white list.
Remove from white list	Select an entry and click this to remove it from the IP reputation white list.
Time	This field displays the date and time the entry was created.
Malicious IP	This field displays the IPv4 address with bad reputation.

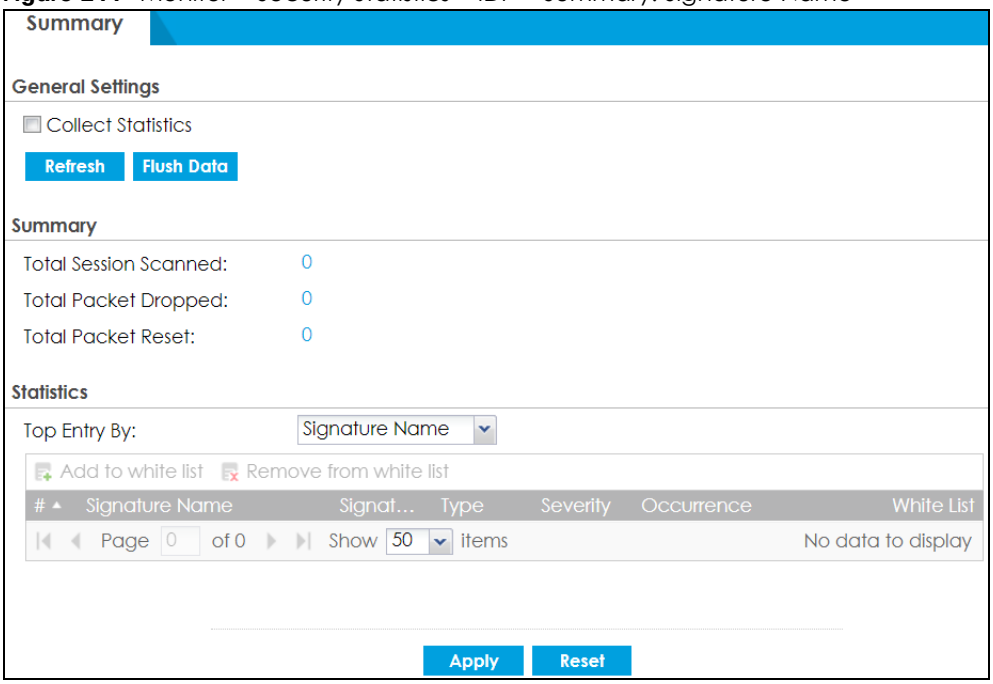
Table 64 Monitor > Security Statistics > Reputation Filter > Summary (continued)

LABEL	DESCRIPTION
Infected/Victim Host	This field displays the MAC address of the infected host.
Threat Category	This field displays the category of the entry.
Threat Level	This field displays the threat level of the entry.
URL Detected	
Add to white list	Select an entry and click this to add it to the botnet filtering white list.
Remove from white list	Select an entry and click this to remove it from the botnet filtering white list.
Time	This field displays the date and time the entry was created.
Source IP	This field displays the source IP address of traffic that you want to trace.
Destination IP	This field displays the destination IP address of traffic.
Botnet URL	This field displays the URL of an infected website or a botnet C&C server.
Threat Category	This field displays the category of the entry.

6.32 The IDP Screen

Click **Monitor > Security Statistics > IDP > Summary** to display the following screen. This screen displays IDP (Intrusion Detection and Prevention) statistics.

Figure 144 Monitor > Security Statistics > IDP > Summary: Signature Name



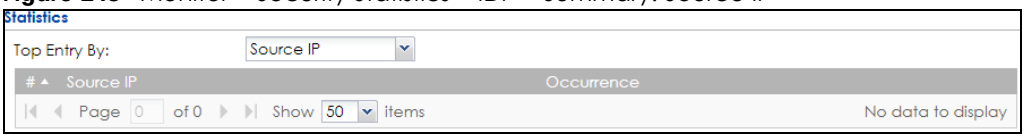
The following table describes the labels in this screen.

Table 65 Monitor > Security Statistics > IDP > Summary

LABEL	DESCRIPTION
Collect Statistics	Select this check box to have the Zyxel Device collect IDP statistics. The collection starting time displays after you click **Apply**. All of the statistics in this screen are for the time period starting at the time displayed here. The format is year, month, day and hour, minute, second. All of the statistics are erased if you restart the Zyxel Device or click **Flush Data**. Collecting starts over and a new collection start time displays.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
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.
Total Session Scanned	This field displays the number of sessions that the Zyxel Device has checked for intrusion characteristics.
Total Packet Dropped	The Zyxel Device can detect and drop malicious packets from network traffic. This field displays the number of packets that the Zyxel Device has dropped.
Total Packet Reset	The Zyxel Device can detect and drop malicious packets from network traffic. This field displays the number of packets that the Zyxel Device has reset.
Top Entries By	Use this field to have the following (read-only) table display the top IDP log entries by **Signature Name**, **Source IP** or **Destination IP**. This table displays the most common, recent IDP logs. See the log screen for less common IDP logs or use a syslog server to record all IDP logs. Select **Signature Name** to list the most common signatures that the Zyxel Device has detected. Select **Source IP** to list the source IP addresses from which the Zyxel Device has detected the most intrusion attempts. Select **Destination IP** to list the most common destination IP addresses for intrusion attempts that the Zyxel Device has detected.
Add to white list	Select a signature and click this to add the selected signature to the IDP white list.
Remove from white list	Select a signature and click this to remove the selected signature from the IDP white list.
#	This field displays the entry's rank in the list of the top entries.
Signature Name	This column displays when you display the entries by **Signature Name**. The signature name identifies the type of intrusion pattern. Click the hyperlink for more detailed information on the intrusion.
Signature ID	This column displays when you display the entries by **Signature Name**. The signature ID is a unique value given to each intrusion detected.
Type	This column displays when you display the entries by **Signature Name**. It shows the categories of intrusions.
Severity	This column displays when you display the entries by **Signature Name**. It shows the level of threat that the intrusions may pose.
Source IP	This column displays when you display the entries by **Source.** It shows the source IP address of the intrusion attempts.
Destination IP	This column displays when you display the entries by **Destination.** It shows the destination IP address at which intrusion attempts were targeted.
Occurrences	This field displays how many times the Zyxel Device has detected the event described in the entry.
White List	Click this to add this signature to the IDP white list. Click this to remove this signature from the IDP white list.

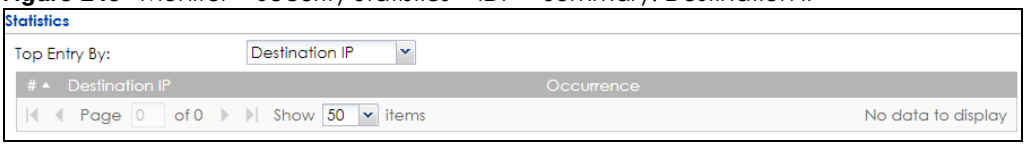
The statistics display as follows when you display the top entries by source.

Figure 145 Monitor > Security Statistics > IDP > Summary: Source IP



The statistics display as follows when you display the top entries by destination.

Figure 146 Monitor > Security Statistics > IDP > Summary: Destination IP



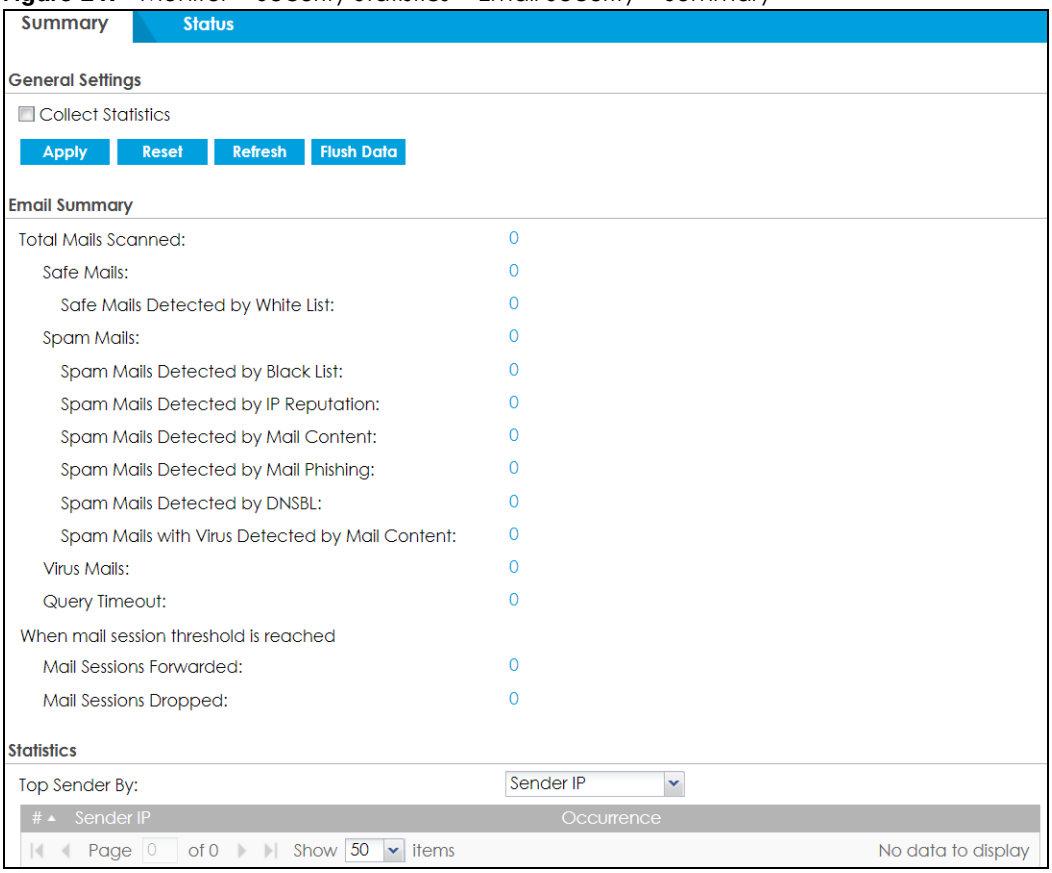
6.33 The Email Security Screens

The **Email Security** menu contains the **Summary** and **Status** screens.

6.33.1 Email Security Summary

Click **Monitor > Security Statistics > Email Security** > **Summary** to display the following screen. This screen displays spam statistics.

Figure 147 Monitor > Security Statistics > Email Security > Summary



The following table describes the labels in this screen.

Table 66 Monitor > Security Statistics > Email Security > Summary

LABEL	DESCRIPTION
Collect Statistics	Select this check box to have the Zyxel Device collect email security statistics. The collection starting time displays after you click **Apply**. All of the statistics in this screen are for the time period starting at the time displayed here. The format is year, month, day and hour, minute, second. All of the statistics are erased if you restart the Zyxel Device or click **Flush Data**. Collecting starts over and a new collection start time displays.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
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.
Email Summary	
Total Mails Scanned	This field displays the number of emails that the Zyxel Device's email security feature has checked.
Safe Mails	This is the number of emails that the Zyxel Device has determined to not be spam.
Safe Mails Detected by White list	This is the number of emails that matched an entry in the Zyxel Device's email security white list.
Spam Mails	This is the number of emails that the Zyxel Device has determined to be spam.
Spam Mails Detected by Black List	This is the number of emails that matched an entry in the Zyxel Device's email security black list.

Table 66 Monitor > Security Statistics > Email Security > Summary (continued)

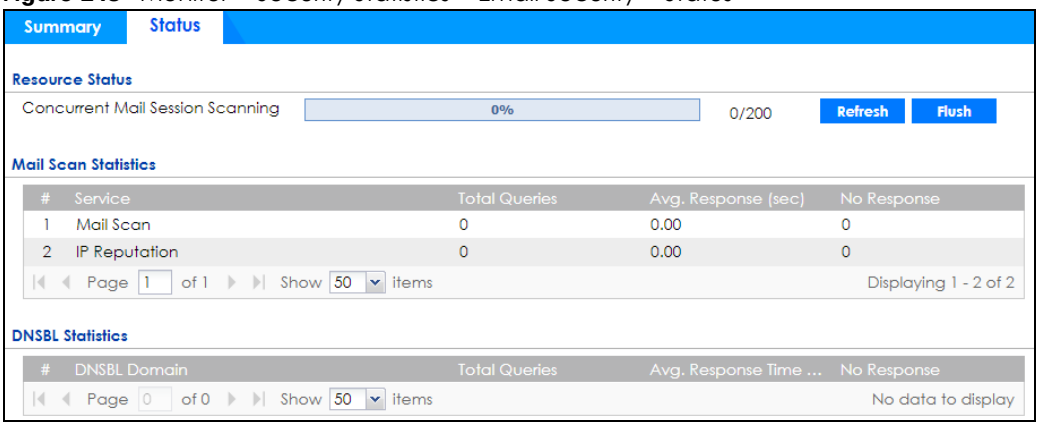
LABEL	DESCRIPTION
Spam Mails Detected by IP Reputation	This is the number of emails that the Zyxel Device has determined to be spam by IP Reputation. Spam or Unwanted Bulk Email is determined by the sender's IP address.
Spam Mails Detected by Mail Content	This is the number of emails that the Zyxel Device has determined to have malicious contents.
Spam Mails Detected by Phishing	This is the number of emails that the Zyxel Device has determined to be spam sent by phishing websites.
Spam Mails Detected by DNSBL	The Zyxel Device can check the sender and relay IP addresses in an email's header against DNS (Domain Name Service)-based spam Black Lists (DNSBLs). This is the number of emails that had a sender or relay IP address in the header which matched one of the DNSBLs that the Zyxel Device uses.
Spam Mails with Virus Detected by Mail Content	This is the number of emails that the Zyxel Device has determined to have malicious contents and attached with virus.
Virus Mails	This is the number of emails that the Zyxel Device has determined to be attached with virus.
Query Timeout	This is how many queries that were sent to the Zyxel Device's configured list of DNSBL domains or Mail Scan services and did not receive a response in time.
When mail session threshold is reached	
Mail Sessions Forwarded	This is how many email sessions the Zyxel Device allowed because they exceeded the maximum number of email sessions that the email security feature can check at a time. You can see the Zyxel Device's threshold of concurrent email sessions in the **Email Security > Status** screen. Use the **Email Security > Summary** screen to set whether the Zyxel Device forwards or drops sessions that exceed this threshold.
Mail Sessions Dropped	This is how many email sessions the Zyxel Device dropped because they exceeded the maximum number of email sessions that the email security feature can check at a time. You can see the Zyxel Device's threshold of concurrent email sessions in the **Email Security > Status** screen. Use the **Email Security > Summary** screen to set whether the Zyxel Device forwards or drops sessions that exceed this threshold.
Statistics	
Top Sender By	Use this field to list the top email or IP addresses from which the Zyxel Device has detected the most spam. Select **Sender IP** to list the source IP addresses from which the Zyxel Device has detected the most spam. Select **Sender Email Address** to list the top email addresses from which the Zyxel Device has detected the most spam.
#	This field displays the entry's rank in the list of the top entries.
Sender IP	This column displays when you display the entries by **Sender IP**. It shows the source IP address of spam emails that the Zyxel Device has detected.
Sender Email Address	This column displays when you display the entries by **Sender Email Address**. This column displays the email addresses from which the Zyxel Device has detected the most spam.
Occurrence	This field displays how many spam emails the Zyxel Device detected from the sender.

6.33.2 The Email Security Status Screen

Click **Monitor > Security Statistics > Email Security** > **Status** to display the **Email Security Status** screen.

Use the **Email Security Status** screen to see how many email sessions the email security feature is scanning and statistics for the DNSBLs.

Figure 148 Monitor > Security Statistics > Email Security > Status



The following table describes the labels in this screen.

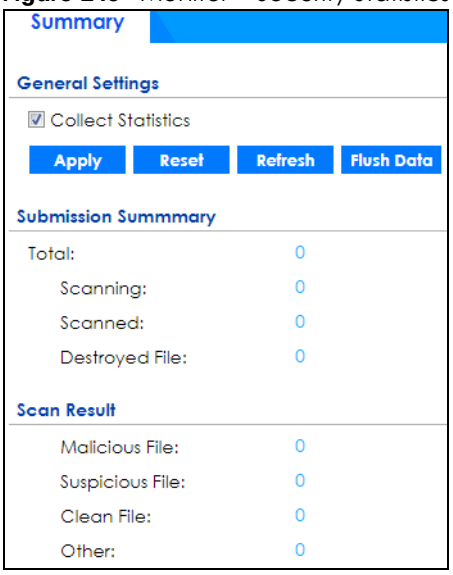
Table 67 Monitor > Security Statistics > Email Security > Status

LABEL	DESCRIPTION
Resource Status	
Concurrent Mail Session Scanning	The darker shaded part of the bar shows how much of the Zyxel Device's total spam checking capability is currently being used. The lighter shaded part of the bar and the pop-up show the historical high. The first number to the right of the bar is how many email sessions the Zyxel Device is presently checking for spam. The second number is the maximum number of email sessions that the Zyxel Device can check at once. An email session is when an email client and email server (or two email servers) connect through the Zyxel Device.
Refresh	Click this button to update the information displayed on this screen.
Flush	Click this button to clear the DNSBL statistics. This also clears the concurrent mail session scanning bar's historical high.
Mail Scan Statistics	These are the statistics for the service the Zyxel Device uses. These statistics are for when the Zyxel Device actually queries the service servers.
#	This is the entry's index number in the list.
Service	This displays the name of the service.
Total Queries	This is the total number of queries the Zyxel Device has sent to this service.
Avg. Response Time (sec)	This is the average for how long it takes to receive a reply from this service.
No Response	This is how many queries the Zyxel Device sent to this service without receiving a reply.
DNSBL Statistics	These are the statistics for the DNSBL the Zyxel Device uses. These statistics are for when the Zyxel Device actually queries the DNSBL servers. Matches for DNSBL responses stored in the cache do not affect these statistics.
#	This is the entry's index number in the list.
DNSBL Domain	These are the DNSBLs the Zyxel Device uses to check sender and relay IP addresses in emails.
Total Queries	This is the total number of DNS queries the Zyxel Device has sent to this DNSBL.
Avg. Response Time (sec)	This is the average for how long it takes to receive a reply from this DNSBL.
No Response	This is how many DNS queries the Zyxel Device sent to this DNSBL without receiving a reply.

6.34 The Sandboxing Screen

Click **Monitor > Security Statistics > Sandboxing** to display the following screen. This screen displays sandboxing statistics.

Figure 149 Monitor > Security Statistics > Sandboxing



The following table describes the labels in this screen.

Table 68 Monitor > Security Statistics > Sandboxing

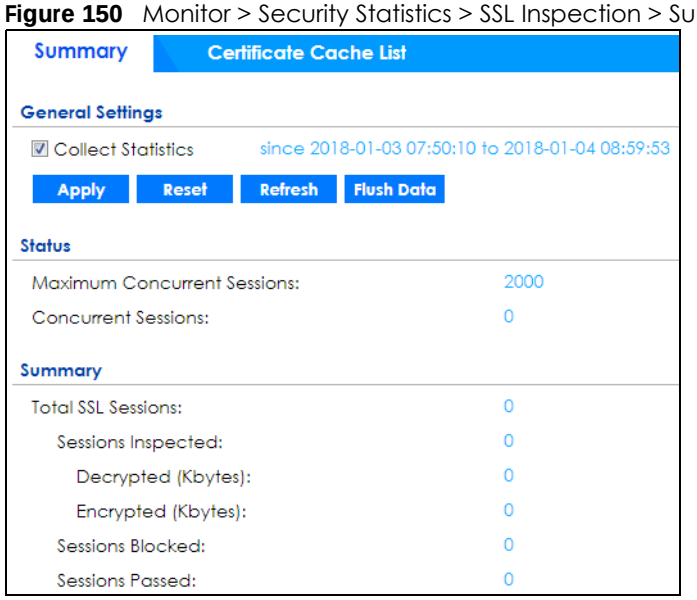
LABEL	DESCRIPTION
Collect Statistics	Select this check box to have the Zyxel Device collect sandboxing statistics. The collection starting time displays after you click **Apply**. All of the statistics in this screen are for the time period starting at the time displayed here. The format is year, month, day and hour, minute, second. All of the statistics are erased if you restart the Zyxel Device or click **Flush Data**. Collecting starts over and a new collection start time displays.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
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.
Total	This field displays the total number of files that the Zyxel Device sent to the Defend Center for analysis.
Scanning	This field displays the total number of files that the Zyxel Device is still scanning.
Scanned	This field displays the total number of files that have been scanned.
Destroyed Files	This shows the number of files that have been destroyed.
Malicious Files	This shows the number of malicious files that have been detected. Malicious files are files given a high score for malware characteristics by the Defend Center.
Suspicious Files	This shows the number of suspicious files that have been detected. Suspicious files are files given a medium score for malware characteristics by the Defend Center.
Safe File	This shows the number of clean files that have been detected. Safe files are files given a low score for malware characteristics by the Defend Center.
Other	This shows the number of internal and external networks errors.

6.35 The SSL Inspection Screens

The Zyxel Device uses SSL Inspection to decrypt SSL traffic, sends it to the Security Service engines for inspection, then encrypts traffic that passes inspection and forwards it. You must enable SSL Inspection if you want to use Content Filtering 2.0 Safe Search.

Click **Monitor > Security Statistics > SSL Inspection > Summary** to display the following screen.

Figure 150 Monitor > Security Statistics > SSL Inspection > Summaryt



The following table describes the labels in this screen.

Table 69 Monitor > Security Statistics > SSL Inspection > Summary

LABEL	DESCRIPTION
Collect Statistics	Select this check box to have the Zyxel Device collect SSL Inspection statistics. The collection starting time displays after you click **Apply**. All of the statistics in this screen are for the time period starting at the time displayed here. The format is year, month, day and hour, minute, second. All of the statistics are erased if you restart the Zyxel Device or click **Flush Data**. Collecting starts over and a new collection start time displays.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
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.
Status	
Maximum Concurrent Sessions	This shows the maximum number of simultaneous SSL Inspection sessions allowed for your Zyxel Device model.
Concurrent Sessions	This shows the actual number of simultaneous SSL Inspection sessions in progress.
Summary	
Total SSL Sessions	This is the total of SSL sessions inspected and number of sessions blocked and number of sessions passed since data was last flushed or the Zyxel Device last rebooted after **Collect Statistics** was enabled.
Sessions Inspected	This shows the total number of SSL sessions inspected since data was last flushed or the Zyxel Device last rebooted after **Collect Statistics** was enabled

Table 69 Monitor > Security Statistics > SSL Inspection > Summary (continued)

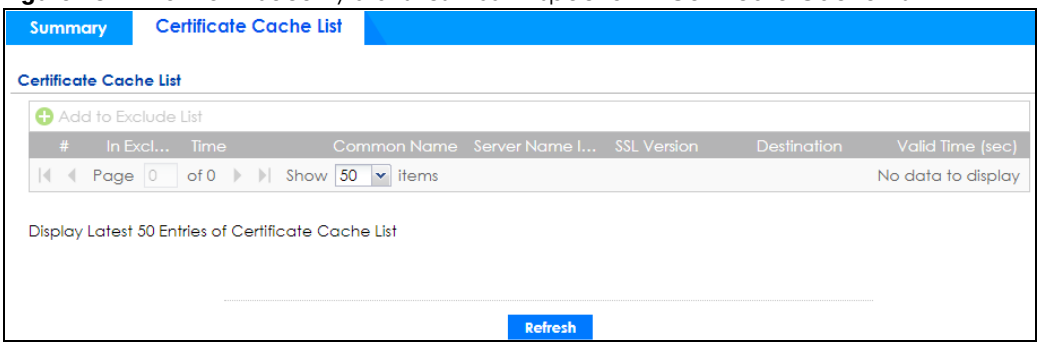
LABEL	DESCRIPTION
Decrypted (Kbytes)	This shows the number of kilobytes (KB) of data that was decrypted for Security Service inspection.
Encrypted (Kbytes)	This shows the number of kilobytes (KB) of data that was re-encrypted after Security Service inspection and then forwarded.
Sessions Blocked	This shows the number of SSL sessions blocked.
Sessions Passed	This shows the number of SSL sessions passed.

6.35.1 Certificate Cache List

SSL traffic to a server to be excluded from SSL Inspection is identified by its certificate. Traffic in an **Exclude List** is not intercepted by **SSL Inspection**.

Click **Monitor > Security Statistics > SSL Inspection > Certificate Cache List** to display a screen that shows details on SSL traffic going to servers identified by its certificate and an option to add that traffic to the **Exclude List**.

Figure 151 Monitor > Security Statistics > SSL Inspection > Certificate Cache List



The following table describes the labels in this screen.

Table 70 Monitor > Security Statistics > SSL Inspection > Certificate Cache List

LABEL	DESCRIPTION
Certificate Cache List	
Add to Exclude list	Select and item in the list and click this icon to add the common name (CN) to the **Exclude List**.
#	This field is a sequential value, and it is not associated with a specific entry.
In Exclude List	If any one of common name, DNS name, email address or IP address of the certificate is in the **Exclude List**, then traffic to the server identified by the certificate is excluded from inspection. The icons here are defined as follows: • Gray: The identity of the certificate is not in the **Exclude List** • Green: The common name of the certificate is in the **Exclude List** • Yellow: The common name of certificate is not in the **Exclude List** but one of the DNS name, email address or IP address is**.**
Time	This is the latest date (yyyy-mm-dd) and time (hh-mm-ss) that the record in the certificate cache list was met.
Common Name	This displays the common name in the certificate of the SSL traffic destination server.

Table 70 Monitor > Security Statistics > SSL Inspection > Certificate Cache List (continued)

LABEL	DESCRIPTION
Server Name Indication	Server Name Indication (SNI) is the domain name entered in the browser, FTP client, etc. to begin the SSL session with the server. It allows multiple SSL sessions to the same IP address and port number with different certificates from different SNI. This field displays the SNI for this SSL session.
SSL Version	This field shows the SSL version. SSLv3/TLS1.0 is currently supported.
Destination	This displays the IP address and port number of the SSL traffic destination server.
Valid Time	This displays the cache item expiry time in seconds. The cache item is deleted when the remaining time expires.
Refresh	Click this button to update the information in the screen.

6.36 Log Screens

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 or user). You can also look at the debugging log by selecting **Debug Log**. All debugging messages have the same priority.

6.36.1 View Log

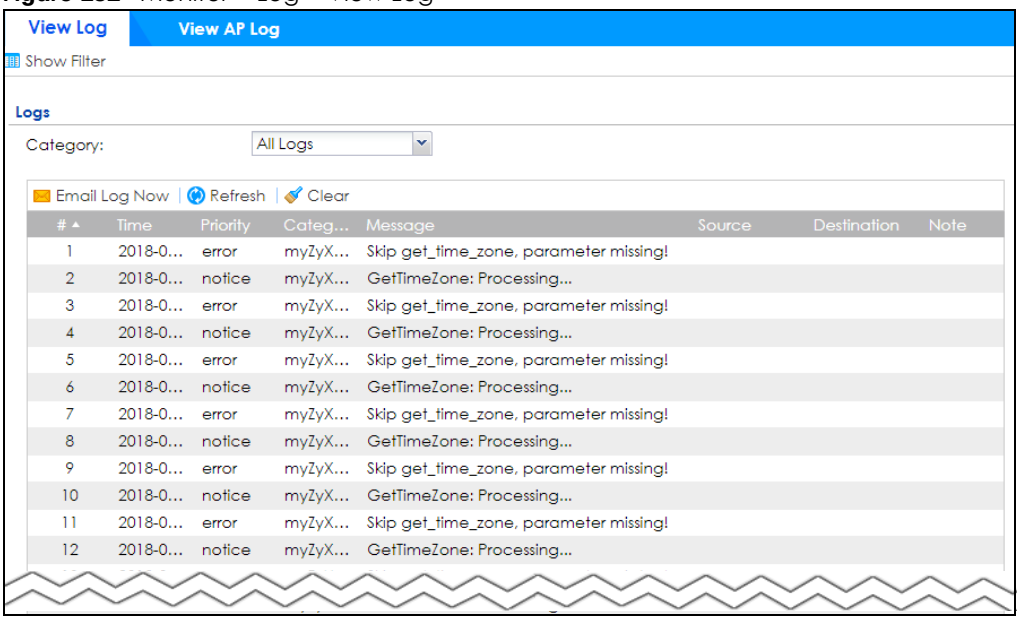
To access this screen, click **Monitor > Log**. The log is displayed in the following screen.

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

- The maximum possible number of log messages in the Zyxel Device 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. The Web Configurator saves the filter settings if you leave the **View Log** screen and return to it later.

Figure 152 Monitor > Log > View Log



The following table describes the labels in this screen.

Table 71 Monitor > Log > View Log

LABEL	DESCRIPTION
Show (Hide) Filter	Click this button to show or hide criteria that allow you to filter logs that will be displayed. If the filter settings are hidden, the **Category**, **Email Log Now**, **Refresh**, and **Clear** fields are available. If the filter settings are shown, the **Category**, **Priority**, **Source Address**, **Destination Address**, **Source Interface**, **Destination Interface**, **Service**, **Keyword**, **Protocol** and **Search** fields are available.
Category	Select the type 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 grayed out 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. Type the source interface of the incoming packet that generated the log message.
Destination Interface	This displays when you show the filter. Type the interface of the destination of the incoming packet when the log message was generated.
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.

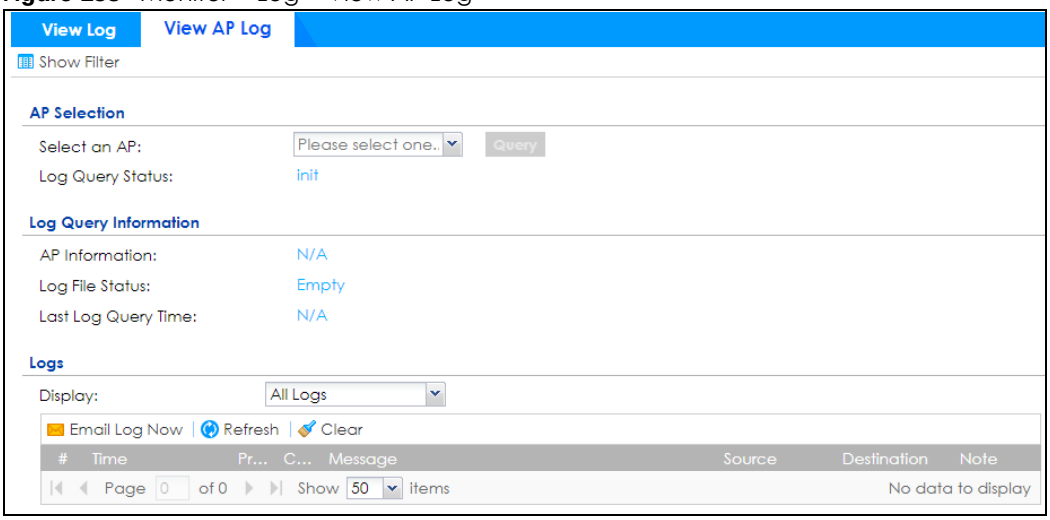
Table 71 Monitor > Log > View Log (continued)

LABEL	DESCRIPTION
Keyword	This displays when you show the filter. Type a keyword to look for in the **Message**, **Source**, **Destination** and **Note** fields. If a match is found in any field, the log message is displayed. You can use up to 63 alphanumeric characters and the underscore, as well as punctuation marks ()' ,.;?! +-*/= #$% @ ; the period, double quotes, and brackets are not allowed.
Protocol	This displays when you show the filter. Select a service protocol whose log messages you would like to see.
Search	This displays when you show the filter. Click this button to update the log using the current filter settings.
Reset	Click **Reset** to return the screen to its last-saved settings.
Email Log Now	Click this button to send log message(s) to the **Active** email address(es) specified in the **Send Log To** field on the **Log Settings** page.
Refresh	Click this button to update the information in the screen.
Clear	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 **Category** field above.
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 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.

6.36.2 View AP Log

Click on **Monitor > Log > View AP Log** to open the following screen.

Figure 153 Monitor > Log > View AP Log



The following table describes the labels in this screen.

Table 72 Monitor > Log > View AP Log

LABEL	DESCRIPTION
Show Filter	Click this button to show or hide the filter settings. If the filter settings are hidden, the **Display**, **Email Log Now**, **Refresh**, and **Clear** fields are available. If the filter settings are shown, the **Display**, **Priority**, **Source Address**, **Destination Address**, **Source Interface**, **Destination Interface**, **Service**, **Keyword**, **Protocol**, and **Search** fields are available.
Select an AP	Click the pull down menu to choose an AP.
Query	Click Query to create a Query log.
Log Query Status	The field displays the
AP Information	This field displays the AP information. N/A is displayed when
Log File Status	This field displays how many logs are available. It will display Empty if there's none.
Last Log Query Time	This field displays the most recent time a log query was solicited.
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	Type the IP address of the source AP.
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. Type the source interface of the incoming packet that generated the log message.
Destination Interface	This displays when you show the filter. Type the interface of the destination of the incoming packet when the log message was generated.
Service	Select a policy service available from Zyxel Device from the pull down menu.
Keyword	Type a keyword of the policy service available from Zyxel Device to search for a log.
Protocol	Select the protocol of the AP from the pull down menu.

Table 72 Monitor > Log > View AP Log (continued)

LABEL	DESCRIPTION
Search	Click this to start the search.
Email Log Now	Click this button to send log message(s) to the **Active** email address(es) specified in the **Send Log To** field on the **Log Settings** page.
Refresh	Click this button to update the information in the screen.
Clear	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 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**.
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 message of the log.
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 field displays any additional information about the log message.

CHAPTER 7
Licensing

7.1 Registration Overview

Use the **Configuration > Licensing > Registration** screens to register your Zyxel Device and manage its service subscriptions.

- Use the **Registration** screen (see Section 7.1.2 on page 187) to refresh Zyxel Device registration, go to portal.myZyxel.com to register your Zyxel Device and activate a service, such as content filtering.
- Use the **Service** screen (see Section 7.1.3 on page 187) to display the status of your service registrations and upgrade licenses.

7.1.1 What you Need to Know

This section introduces the topics covered in this chapter.

Subscription Services Available

See **Configuration > Licensing > Registration > Service** for the subscription services that your Zyxel Device supports. Zyxel offers two types of security packs for your Zyxel Device. The subscription services you can use on the Zyxel Device vary depending on the security pack license you purchase. See the table below for services available in each pack.

Table 73 Security Packs and Subscription Services

SERVICE MODULE	SERVICE	GOLD SECURITY PACK
Web Security	Content Filter	V
	Botnet Filter	
Application Security	App Patrol	V
	Email Security	
Malware Blocker	Anti-Malware & Cloud Query	V
	Threat Intelligence Machine Learning	V
Intrusion Prevention	IDP	V
Geo Enforcer	Geo IP	V
Reputation Filter	IP Reputation	V
Sandboxing	Sandboxing	V
Managed AP Service	Wireless Controller	V (Unlimited)
SecuReporter	SecuReporter	1-Year Standard Service • Unlimited log retention period • Log analysis for 30 days

You can purchase an iCard and enter its license key at myZyxel to extend a service.

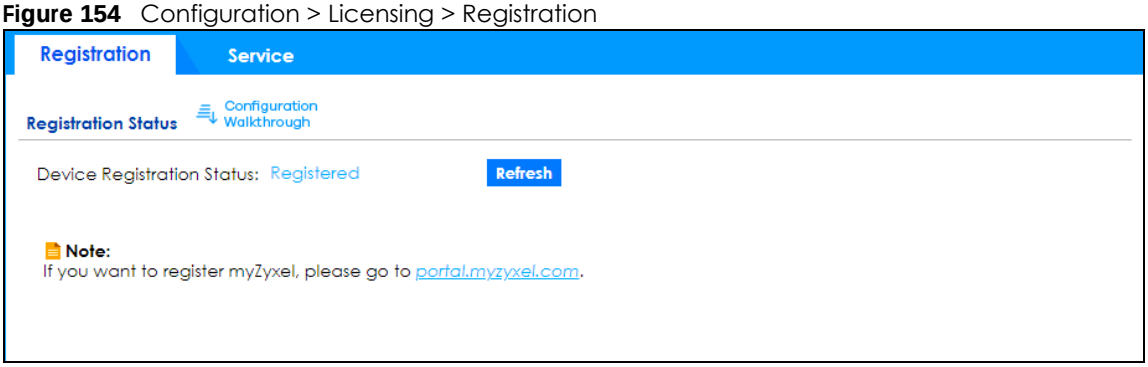
Note: The trial gold security pack license is not transferable.

7.1.2 Registration Screen

Click the link in this screen to register your Zyxel Device at myZyxel. Then click **Refresh** in this screen and wait a few moments for the registration information to update. If the page does not refresh, make sure the Internet connection is working and click **Refresh** again. The Zyxel Device should already have Internet access and be able to access myZyxel. Click **Configuration > Licensing > Registration** in the navigation panel to open the screen as shown next.

Click on the icon to go to the OneSecurity website where there is guidance on configuration walkthrough and other information.

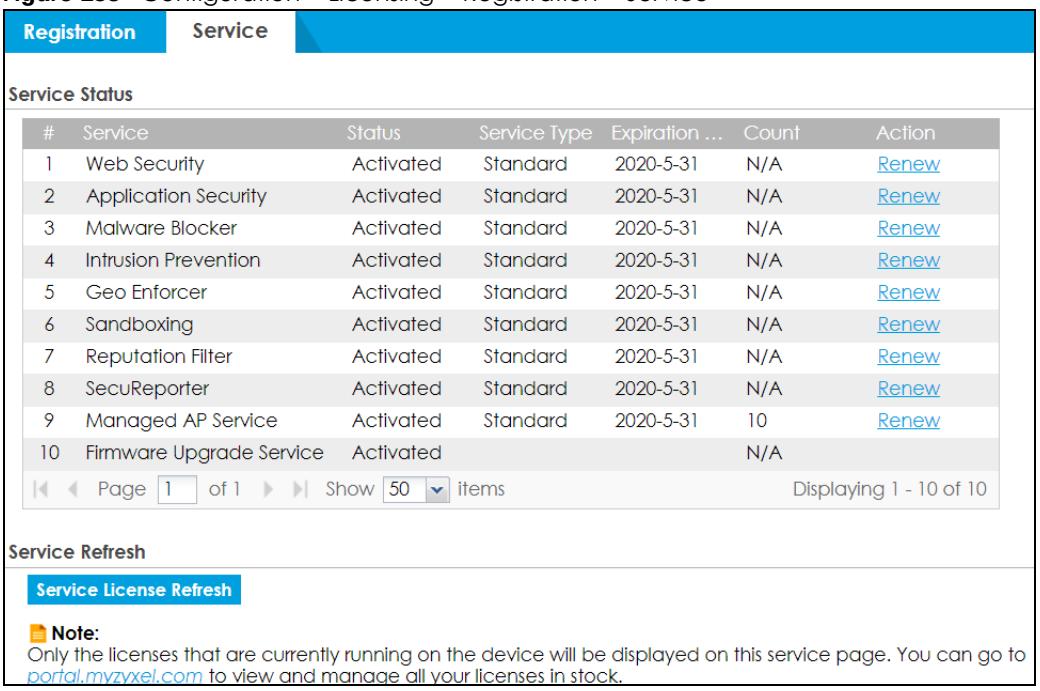
Figure 154 Configuration > Licensing > Registration



7.1.3 Service Screen

Use this screen to display the status of your service registrations and upgrade licenses. To activate or extend a standard service subscription, purchase an iCard and enter the iCard's PIN number (license key) at myZyxel. Click **Activate** in this screen to enable both Trial and Standard services on this Zyxel Device. Click **Configuration > Licensing > Registration** > **Service** to open the screen as shown next.

Figure 155 Configuration > Licensing > Registration > Service



The following table describes the labels in this screen.

Table 74 Configuration > Licensing > Registration > Service

LABEL	DESCRIPTION
Service Status	
#	This is the entry's position in the list.
Service	This lists the name of services or service modules that are available on the Zyxel Device.
Web Security	This is a license to a database that can block websites by category, such as Gambling.
Application Security	This is a license for signatures for Application Patrol inspection and signatures to recognize unsolicited commercial or junk email suspect of being sent by spammers.
Malware Blocker	This is a license for signatures to detect malware patterns in files.
Intrusion Prevention	This is a license for signatures for Intrusion Detection and Prevention attacks.
Geo Enforcer	This is a license to a database of country-to-IP address mappings.
Sandboxing	This is a license to create a virtual sandboxing environment to separate running programs from your network and host devices.
Reputation Filter	This is a license for IP reputation to recognize packets coming from IPv4 address with bad reputation.
SecuReporter	This is a license that allows SecuReporter to collect and analyze logs from your Zyxel Device in order to identify anomalies, alert on potential internal / external threats, and report on network usage.
Managed AP Service	This is a license to manage more APs than the default for your Zyxel Device when the AP controller is enabled.
Firmware Upgrade Service	This is a free license to get Cloud Helper notifications when new firmware is available. You must register your Zyxel Device at myZyxel.
Device HA Pro	This is a license for professional High Availability (HA) that lets a backup Zyxel Device automatically take over if the master Zyxel Device fails.

Table 74 Configuration > Licensing > Registration > Service (continued)

LABEL	DESCRIPTION
Status	This field displays whether a service license is enabled at myZyxel (**Activated**) or not (**Not Activated**) or expired (**Expired**). It displays the remaining Grace Period if your license has **Expired**. It displays **Not Licensed** if there isn't a license to be activated for this service. **Default** displays for quantity-based licenses when the Zyxel Device is currently using the allowed free number without a license. For example, if a Zyxel Device is allowed to manage x number of APs without a license and it is currently using that number, then Managed AP Service **Status** displays **Default**.
Service 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.
Expiration Date	This field displays the date your service license expires or the date the grace period expires if the license has already expired. You can continue to use IDP/AppPatrol, Anti-Malware, Content Filter, Email Security during the grace period. After the grace period ends, all of these features are disabled.
Count	This field displays how many instances of a service you can use with your current license. **N/A** means a count does not apply to this service.
Action	If you need a license or a trial license has expired, click **Buy** to buy a new one. If a **Standard** license has expired, click **Renew** to extend the license. Then, click **Activate** to connect with the myZyxel server to activate the new license.
Service License Refresh	Click this button to renew service license information (such as the registration status and expiration day). Note: It is recommended you use this button after you register for a new service.

7.2 Signature Update

This section shows you how to update the signature packages of the Zyxel Device.

- Use the **Configuration > Licensing > Signature Update** screen (Section 7.2.2 on page 190) to update the signatures used for a service, such as IDP and application patrol.

7.2.1 What you Need to Know

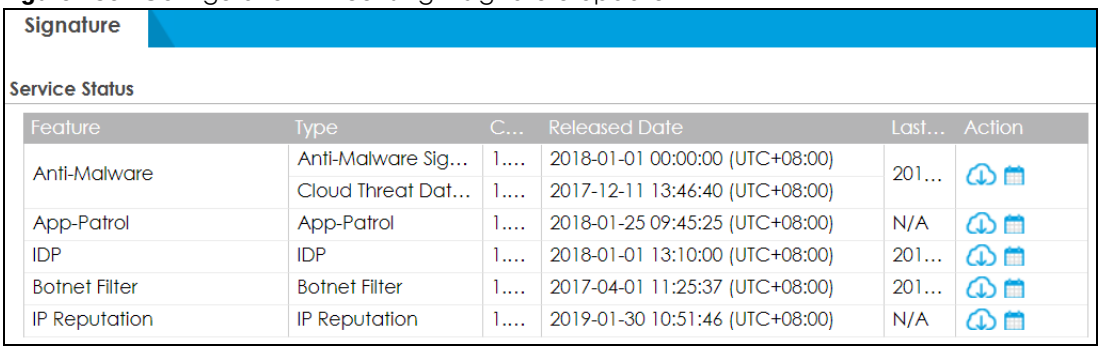
- You need a valid service registration to update the anti-malware signatures, the botnet filter signatures, the IDP signatures and the App-Patrol signatures.
- You do not need a service registration to update the system-protection signatures.
- Schedule signature updates for a day and time when your 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 Zyxel Device does not have to reboot when you upload new signatures.

7.2.2 The Signature Screen

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

Figure 156 Configuration > Licensing > Signature Update



The following table describes the labels in this screen.

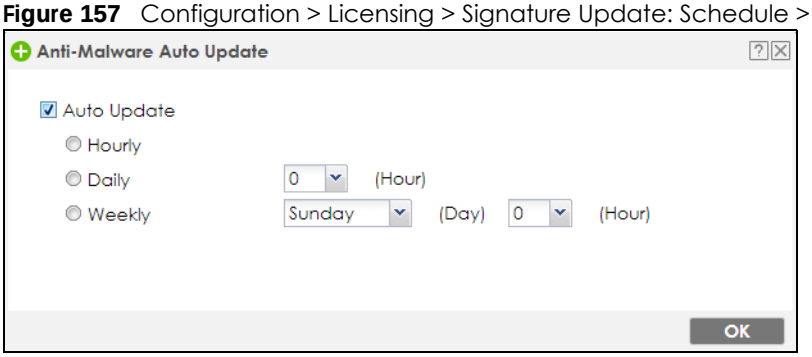
Table 75 Configuration > Licensing > Signature Update

LABEL	DESCRIPTION
Service Status	The following fields display the status and information on the current signature set that the Zyxel Device is using.
Feature	This field displays the name of the services available on the Zyxel Device.
Type	This field displays the type of service engine used by the Zyxel Device.
Current Version	This field displays the signatures version number currently used by the Zyxel Device. This number gets larger as new signatures are added.
Released Date	This field displays the date and time the set was released.
Last Sync	This field displays the date and time the Zyxel Device last checked for new signatures at myZyxel.
Action	Click the **Update** icon to have the Zyxel Device immediately check for new signatures at myZyxel. If new signatures are found, they are then downloaded to the Zyxel Device. Click the **Schedule** icon to have the Zyxel Device automatically check for new signatures regularly at the time and day specified. You should select a time when your network is not busy for minimal interruption.

7.2.3 Auto Update

Click the **Schedule** icon of a service to display the following screen.

Figure 157 Configuration > Licensing > Signature Update: Schedule > Auto Update



The following table describes the labels in this screen.

Table 76 Configuration > Licensing > Signature Update: Schedule > Auto Update

LABEL	DESCRIPTION
Auto Update	Select this check box to have the Zyxel Device automatically check for new signatures regularly at the time and day specified. You should select a time when your network is not busy for minimal interruption.
Hourly	Select this option to have the Zyxel Device check for new signatures every hour.
Daily	Select this option to have the Zyxel Device check for new signatures every day 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 Zyxel Device check for new signatures once a week on the day and at the time specified.
OK	Click this button to save your changes to the Zyxel Device.

CHAPTER 8
Wireless

8.1 Overview

Use the **Wireless** screens to configure how the Zyxel Device manages supported Access Points (APs). Supported APs should be in managed mode. See the product page **Licenses** tab for a list of supported APs.

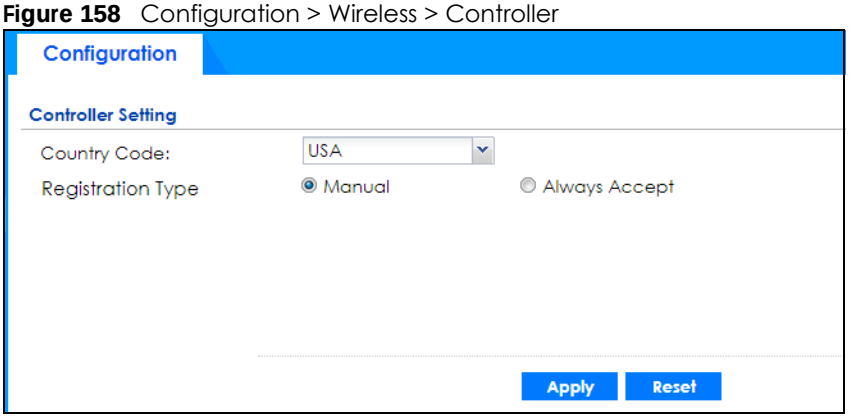
8.1.1 What You Can Do in this Chapter

- Use the **Controller** screen (Section 8.2 on page 192) to set how the Zyxel Device allows new APs to connect to the network and set the country code of APs that are connected to the Zyxel Device.
- Use the **AP Management** screens (Section 8.3 on page 193) to manage all of the APs connected to the Zyxel Device.
- Use the **Rogue AP** screen (Section 8.4 on page 205) to assign APs either to the rogue AP list or the friendly AP list.
- Use the **Auto Healing** screen (Section 8.5 on page 208) to extend the wireless service coverage area of the managed APs when one of the APs fails.
- Use the **RTLS** screen (Section 8.6 on page 209) to allow managed APs with battery-powered Wi-Fi tags be part of Ekahau RTLS (Real Time Location Service). RTLS can track the location of APs managed by the Zyxel Device to create maps, alerts, and reports.

8.2 Controller Screen

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

Figure 158 Configuration > Wireless > Controller



Each field is described in the following table.

Table 77 Configuration > Wireless > Controller

LABEL	DESCRIPTION
Country Code	Select the country code of APs that are connected to the Zyxel Device to be the same as where the Zyxel Device is located/installed. The available channels vary depending on the country you selected.
Registration Type	Select **Manual** to add each AP to the Zyxel Device for management, or **Always Accept** to automatically add APs to the Zyxel Device for management. If you select **Manual**, then go to **Monitor > Wireless > AP Information > AP List**, select an AP to be managed and then click **Add to Mgnt AP List**. That AP will then appear in **Configuration > Wireless > Controller > Mgnt. AP List**. 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. APs must be connected to the Zyxel Device by a wired connection or network.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

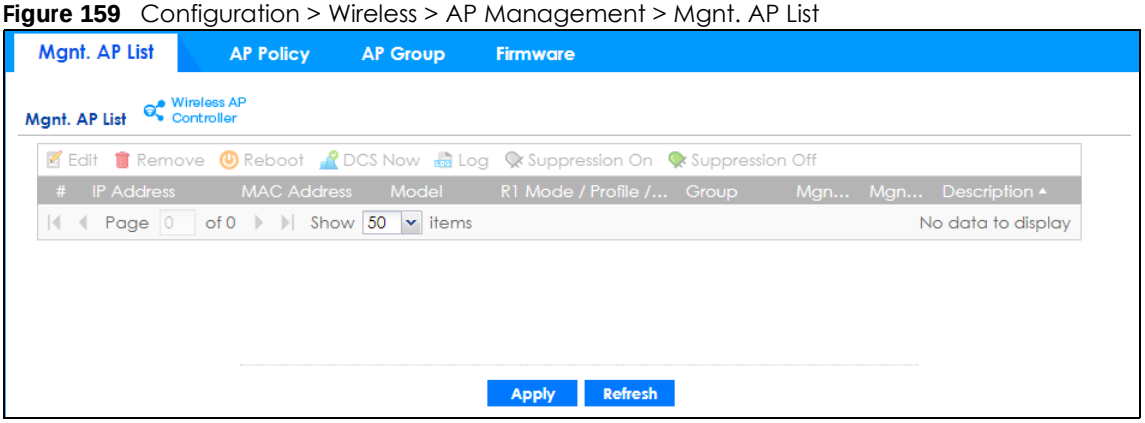
8.3 AP Management Screens

Use these screens to manage all of the APs connected to the Zyxel Device. Click **Configuration > Wireless > AP Management** to access these screens.

Click on the icon to go to the OneSecurity website where there is guidance on configuration walkthroughs and other information.

8.3.1 Mgnt. AP List

Figure 159 Configuration > Wireless > AP Management > Mgnt. AP List



Each field is described in the following table.

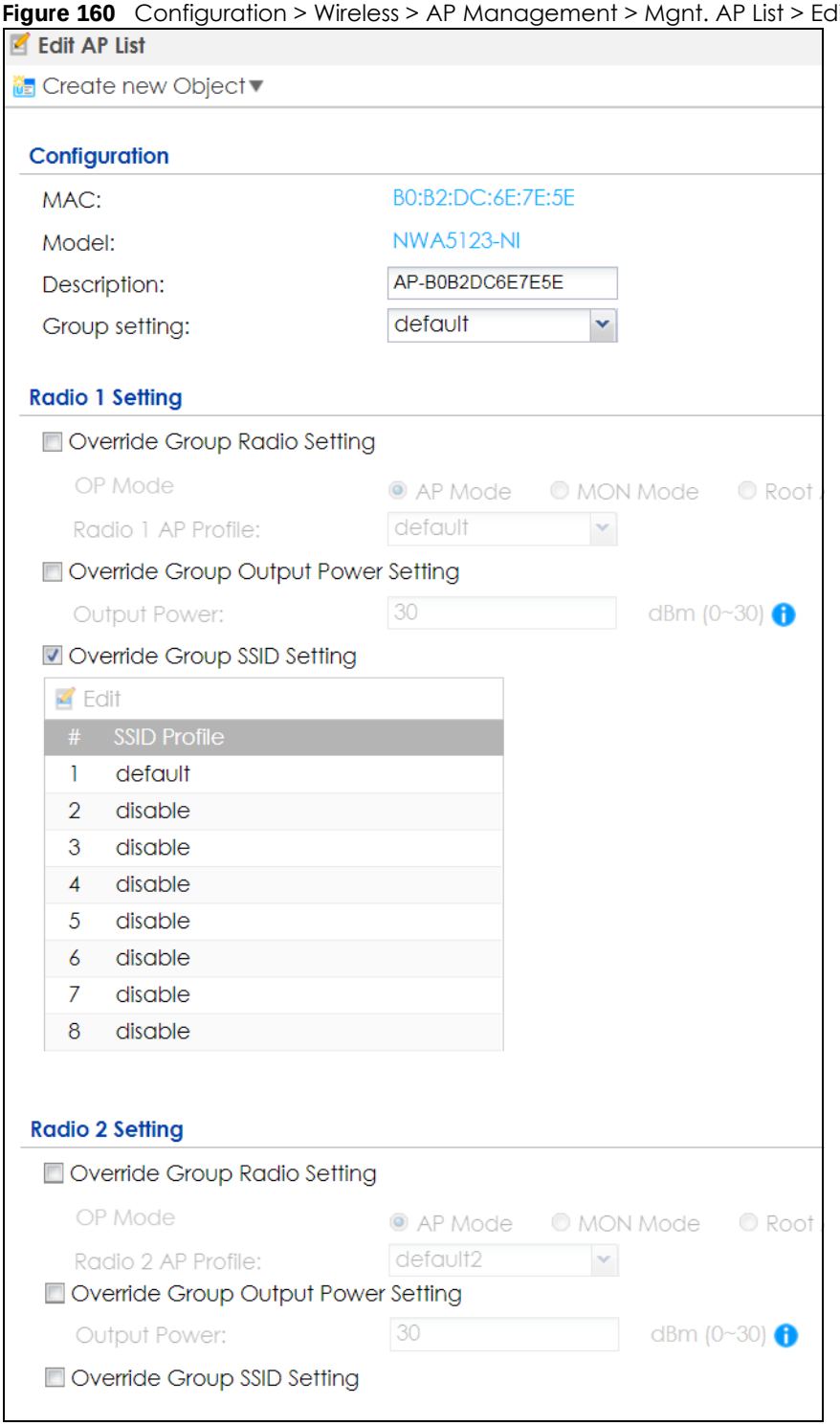
Table 78 Configuration > Wireless > AP Management > Mgnt. AP List

LABEL	DESCRIPTION
Edit	Select an AP and click this button to edit its properties.
Remove	Select an AP and click this button to remove it from the list. Note: If in the **Configuration > Wireless > Controller** screen you set the **Registration Type** to **Always Accept**, then as soon as you remove an AP from this list it reconnects.
Reboot	Select an AP and click this button to force it 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. Note: You should have enabled DCS in the applied AP radio profile before the APs can use DCS. Note: DCS is not supported on the radio which is working in repeater AP mode.
Log	Select an AP and click this button to go to the **Monitor > Log > View AP Log** screen to view the selected AP's current log messages.
Suppression On	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.
Suppression Off	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.
#	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 Zyxel Device and the information is unavailable as a result.
R1 Mode / Profile / ZyMesh Profile	This field displays the operating mode (**AP**, **MON**, **rootap**, or **repeater**), AP radio profile name and ZyMesh profile name for Radio 1. It displays **-** for the ZyMesh profile for a radio not using a ZyMesh profile.
R2 Mode / Profile / ZyMesh Profile	This field displays the operating mode (**AP**, **MON**, **rootap**, or **repeater**), AP radio profile name and ZyMesh profile name for Radio 2. It displays **-** for the ZyMesh profile for a radio not using a ZyMesh profile.
Group	This field displays the name of the AP group to which the AP belongs. The group becomes editable immediately upon clicking.
Mgnt. VLAN ID(AC)	This displays the Access Controller (the Zyxel Device) 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 Zyxel Device 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.

8.3.1.1 Edit AP List

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

Figure 160 Configuration > Wireless > AP Management > Mgnt. AP List > Edit AP List



Each field is described in the following table.

Table 79 Configuration > Wireless > AP Management > Mgnt. AP List > Edit AP List

LABEL	DESCRIPTION
Create new Object	Use this menu to create a new **Radio Profile** object to associate with this AP.
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 Zyxel Device 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 an AP group to which you want this AP to belong.
Radio 1/2 Setting	
Override Group Radio Setting	Select this option to overwrite the AP radio settings with the settings you configure here.
OP Mode	Select the operating mode for radio 1 or radio 2. **AP Mode** means the AP can receive connections from wireless clients and pass their data traffic through to the Zyxel Device to be managed (or subsequently passed on to an upstream gateway for managing). **MON Mode** means the AP monitors the broadcast area for other APs, then passes their information on to the Zyxel Device 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. **Root AP** means the radio acts as an AP and also supports the wireless connections with other APs (in repeater mode) to form a ZyMesh to extend its wireless network. **Repeater AP** means the radio can establish a wireless connection with other APs (in either root AP or repeater mode). Note: To prevent bridge loops, do NOT set both radios on a managed AP to **Repeater AP** mode. Note: The root AP and repeater AP(s) in a ZyMesh must use the same country code and AP radio profile settings in order to communicate with each other. Note: Ensure you restart the managed AP after you change its operating mode.
Radio 1/2 AP Profile	Select an AP profile from the list. If no profile exists, you can create a new one through the **Create new Object** menu.
Radio 1/2 Profile	Select a monitor profile from the list. If no profile exists, you can create a new one through the **Create new Object** menu.
Radio 1/2 ZyMesh Profile	This field is available only when the radio is in **Root AP** or **Repeater AP** mode. Select the ZyMesh profile the radio uses to connect to a root AP or repeater.
Enable Wireless Bridging	This field is available only when the radio is in **Repeater AP** mode. Select this option to enable wireless bridging on the radio. The managed AP must support LAN provision and the radio should be in repeater mode. VLAN and bridge interfaces are created automatically according to the LAN port's VLAN settings. When wireless bridging is enabled, the managed repeater AP can still transmit data through its Ethernet port(s) after the ZyMesh link is up. Be careful to avoid bridge loops. The managed APs in the same ZyMesh must use the same static VLAN ID.
Override Group Output Power Setting	Select this option to overwrite the AP output power setting with the setting you configure here.

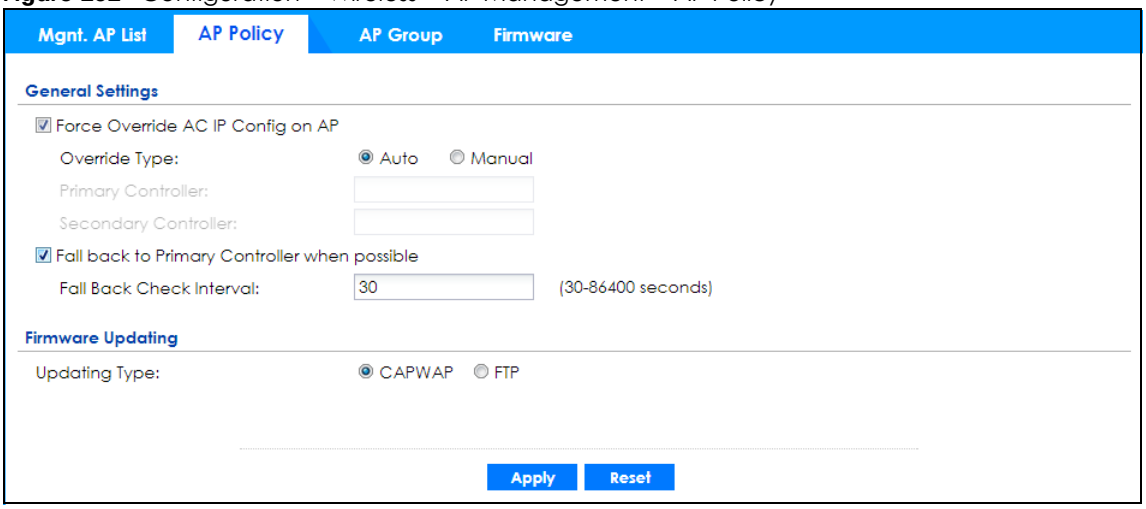
Table 79 Configuration > Wireless > AP Management > Mgnt. AP List > Edit AP List (continued)

LABEL	DESCRIPTION
Output Power	Set the output power of the AP.
Override Group SSID Setting	Select this option to overwrite the AP SSID profile setting with the setting you configure here. 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.
Override Group VLAN Setting	Select this option to overwrite the AP VLAN setting with the setting you configure here.
Force Overwrite VLAN Config	Select this to have the Zyxel Device 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 Zyxel Device and not one assigned to it from outside the network.
Suppression On	Select this option to enable the AP's LED suppression mode. All the LEDs of the AP will turn off after the AP is ready. If the check box is unchecked, it means the LEDs will stay lit after the AP is ready.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to close the window with changes unsaved.

8.3.2 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 161 Configuration > Wireless > AP Management > AP Policy



Each field is described in the following table.

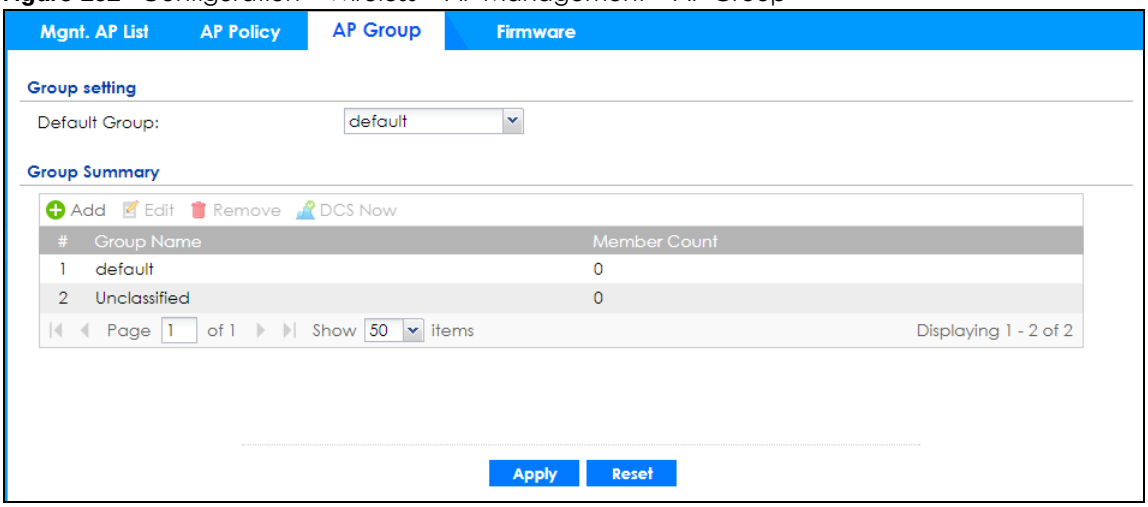
Table 80 Configuration > Wireless > AP Management > AP Policy

LABEL	DESCRIPTION
Force Override AC IP Config on AP	Select this to have the Zyxel Device change the AP controller's IP address on the managed AP(s) to match the configuration in this screen.
Override Type	Select **Auto** to have the managed AP(s) automatically send broadcast packets to find any other available AP controllers. Select **Manual** to replace the AP controller's IP address configured on the managed AP(s) with the one(s) you specified below.
Primary Controller	Specify the IP address of the primary AP controller if you set **Override Type** to **Manual**.
Secondary Controller	Specify the IP address of the secondary AP controller if you set **Override Type** to **Manual**.
Fall back to Primary Controller when possible	Select this option to have the managed AP(s) change back to associate with the primary AP controller as soon as the primary AP controller is available.
Fall Back Check Interval	Set how often the managed AP(s) check whether the primary AP controller is available.
Firmware Updating	
Updating Type	Specify how you want the Zyxel Device to upgrade AP firmware. Select **CAPWAP** to have the Zyxel Device use CAPWAP (Control and Provisioning of Wireless Access Points protocol) to automatically update firmware on the managed APs. Select **FTP** to allow the managed APs to download the latest firmware from the Zyxel Device using FTP.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

8.3.3 AP Group

Use this screen to configure AP groups, which define the radio, port, VLAN and load balancing settings and apply the settings to all APs in the group. An AP can belong to one AP group at a time. Click **Configuration > Wireless > AP Management > AP Group** to access this screen.

Figure 162 Configuration > Wireless > AP Management > AP Group



Each field is described in the following table.

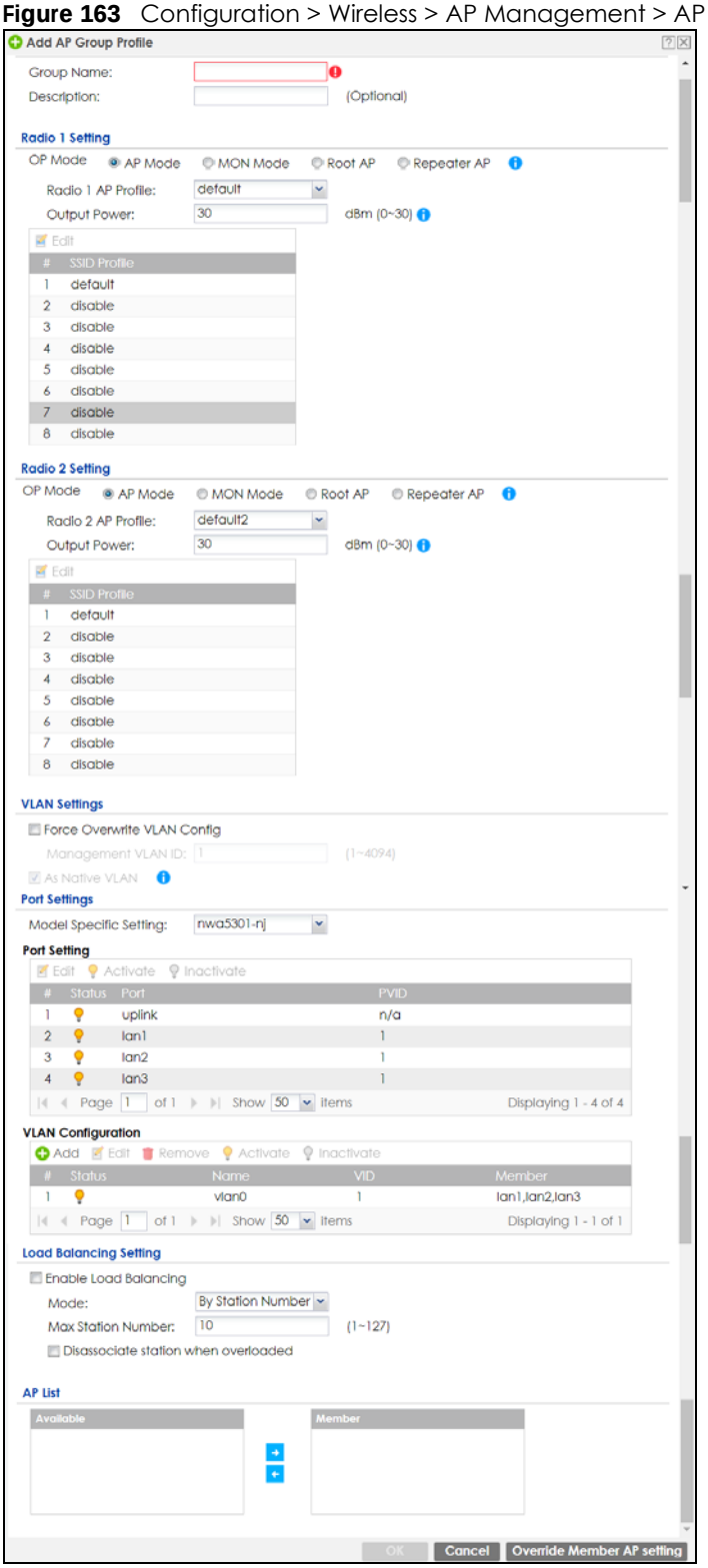
Table 81 Configuration > Wireless > AP Management > AP Group

LABEL	DESCRIPTION
Group Setting	
Default Group	Select a group that is used as the default group. Any AP that is not configured to associate with a specific AP group belongs to the default group automatically.
Group Summary	
Add	Click this button to create a new AP group.
Edit	Select an entry and click this button to edit its properties.
Remove	Select an entry and click this button to remove it from the list. Note: You cannot remove a group with which an AP is associated.
DCS Now	Select one or multiple groups and click this button to use DCS (Dynamic Channel Selection) to allow the APs in the group(s) to automatically find a less-used channel in an environment where there are many APs and there may be interference. Note: You should have enabled DCS in the applied AP radio profile before the APs can use DCS. Note: DCS is not supported on the radio which is working in repeater AP mode.
#	This is the index number of the group in the list.
Group Name	This is the name of the group.
Member Count	This is the total number of APs which belong to this group.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

8.3.3.1 Add/Edit AP Group

Click **Add** or select an AP group and click the **Edit** button in the **Configuration > Wireless > AP Management > AP Group** table to display this screen.

Figure 163 Configuration > Wireless > AP Management > AP Group > Add/Edit



Each field is described in the following table.

Table 82 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. **AP Mode** means the AP can receive connections from wireless clients and pass their data traffic through to the Zyxel Device to be managed (or subsequently passed on to an upstream gateway for managing). **MON Mode** means the AP monitors the broadcast area for other APs, then passes their information on to the Zyxel Device 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. **Root AP** means the radio acts as an AP and also supports the wireless connections with other APs (in repeater mode) to form a ZyMesh to extend its wireless network. **Repeater AP** means the radio can establish a wireless connection with other APs (in either root AP or repeater mode). Note: To prevent bridge loops, do NOT set both radios on a managed AP to **Repeater AP** mode. Note: The root AP and repeater AP(s) in a ZyMesh must use the same country code and AP radio profile settings in order to communicate with each other. Note: Ensure you restart the managed AP after you change its operating mode.
Radio 1/2 AP Profile	Select an AP profile from the list. If no profile exists, you can create a new one through the **Create new Object** menu.
Radio 1/2 Profile	Select a monitor profile from the list. If no profile exists, you can create a new one through the **Create new Object** menu.
Radio 1/2 ZyMesh Profile	This field is available only when the radio is in **Root AP** or **Repeater AP** mode. Select the ZyMesh profile the radio uses to connect to a root AP or repeater.
Enable Wireless Bridging	This field is available only when the radio is in **Repeater AP** mode. Select this option to enable wireless bridging on the radio. The managed AP must support LAN provision and the radio should be in repeater mode. VLAN and bridge interfaces are created automatically according to the LAN port's VLAN settings. When wireless bridging is enabled, the managed repeater AP can still transmit data through its Ethernet port(s) after the ZyMesh link is up. Be careful to avoid bridge loops. The managed APs in the same ZyMesh must use the same static VLAN ID.
Output Power	Set the maximum output power of the AP. 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. Note: Reducing the output power also reduces the Zyxel Device's effective broadcast radius.
Edit	Select an SSID and click this button to reassign it. The selected SSID becomes editable immediately upon clicking.

Table 82 Configuration > Wireless > AP Management > AP Group > Add/Edit (continued)

LABEL	DESCRIPTION
#	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	
Force Overwrite VLAN Config	Select this to have the Zyxel Device 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 Zyxel Device 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.
Port Setting	You can activate or deactivate a non-uplink port.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Activate/Inactivate	To turn on an entry, select it and click **Activate**. To turn off an entry, 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. 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	Select this to enable load balancing on the Zyxel Device. Use this section to configure wireless network traffic load balancing between the managed APs in this group. Note: Load balancing is not supported on the radio which is working in root AP or repeater AP mode.

Table 82 Configuration > Wireless > AP Management > AP Group > Add/Edit (continued)

LABEL	DESCRIPTION
Mode	Select a mode by which load balancing is carried out. Select **By Station Number** to balance network traffic based on the number of specified stations connected to an AP. Select **By Traffic Level** to balance network traffic based on the volume generated by the stations connected to an AP. 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. 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 begins load balancing its connections.
Traffic Level	Select the threshold traffic level at which the AP begins load balancing its connections (**Low**, **Medium**, **High**). The maximum bandwidth allowed for each level is: • **Low** - 11 Mbps, • **Medium** - 23 Mbps • **High** - 35M bps
Disassociate station when overloaded	This function is enabled by default and the disassociation priority is always **Signal Strength** when you set **Mode** to **By Smart Classroom**. Select this option to disassociate wireless clients connected to the AP when it becomes overloaded. If you do not enable this option, then the AP simply delays the connection until it can afford the bandwidth it requires, or it transfers the connection to another AP within its broadcast radius. The disassociation priority is determined automatically by the Zyxel Device and is as follows: • **Idle Timeout** - Devices that have been idle the longest will be disassociated first. If none of the connected devices are idle, then the priority shifts to **Signal Strength**. • **Signal Strength** - Devices with the weakest signal strength will be disassociated first. Note: If you enable this function, you should ensure that there are multiple APs within the broadcast radius that can accept any rejected or kicked wireless clients; otherwise, a wireless client attempting to connect to an overloaded AP will be kicked continuously and never be allowed to connect.
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 Zyxel Device.
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.

8.3.4 Firmware

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

When an AP connects to the Zyxel Device wireless controller, the Zyxel Device will check if the AP has the same firmware version as the AP firmware on the Zyxel Device. If yes, then the Zyxel Device 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 Zyxel Device (and reboot).

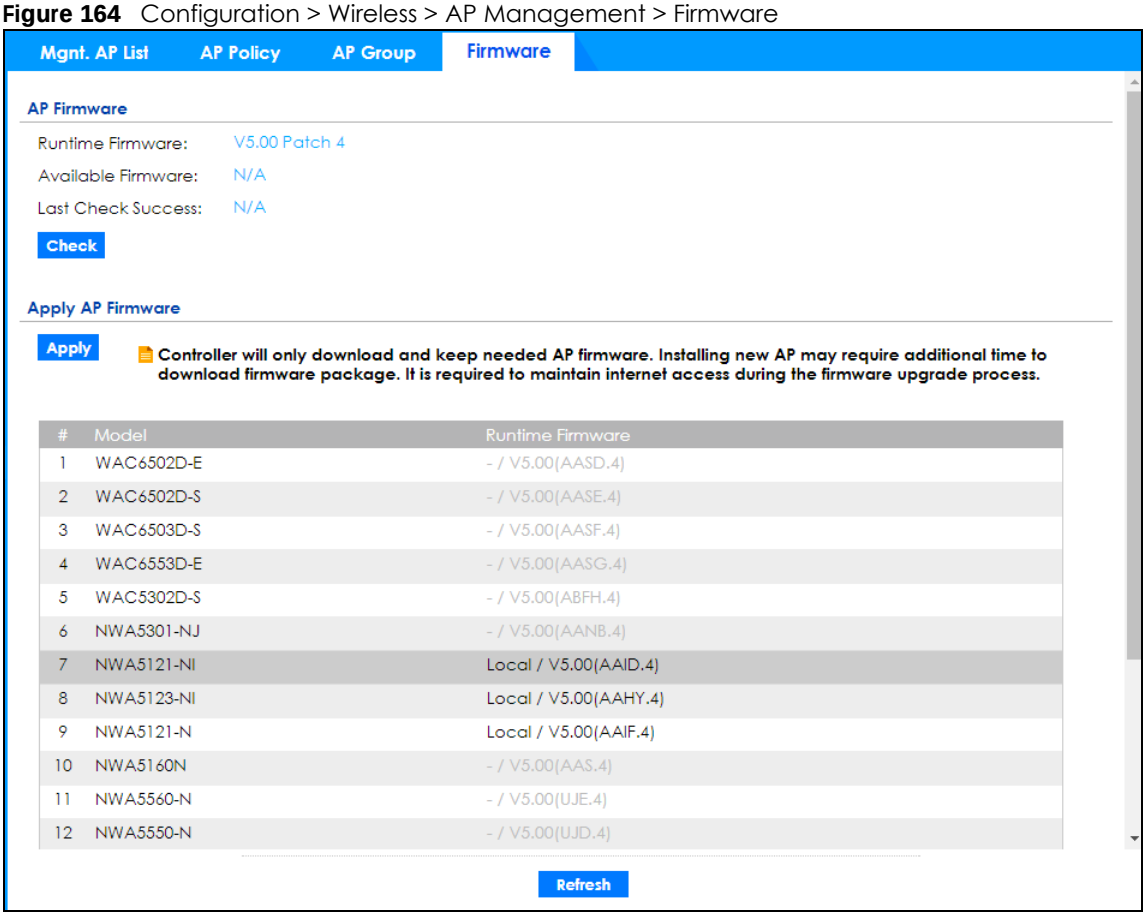
The Zyxel Device should always have the latest AP firmware so that:

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

Use **Check** to see if the Zyxel Device has the latest AP firmware. Use **Apply** to have the Zyxel Device download the latest AP firmware (see **More Details** for more information on the firmware) from the firmware server. If the Zyxel Device does not have enough space for the latest AP firmware, then the Zyxel Device will delete an existing firmware that no AP is using before downloading the new AP firmware.

Click **Configuration > Wireless > AP Management > Firmware** to access this screen.

Figure 164 Configuration > Wireless > AP Management > Firmware



Each field is described in the following table.

Table 83 Configuration > Wireless > AP Management > Firmware

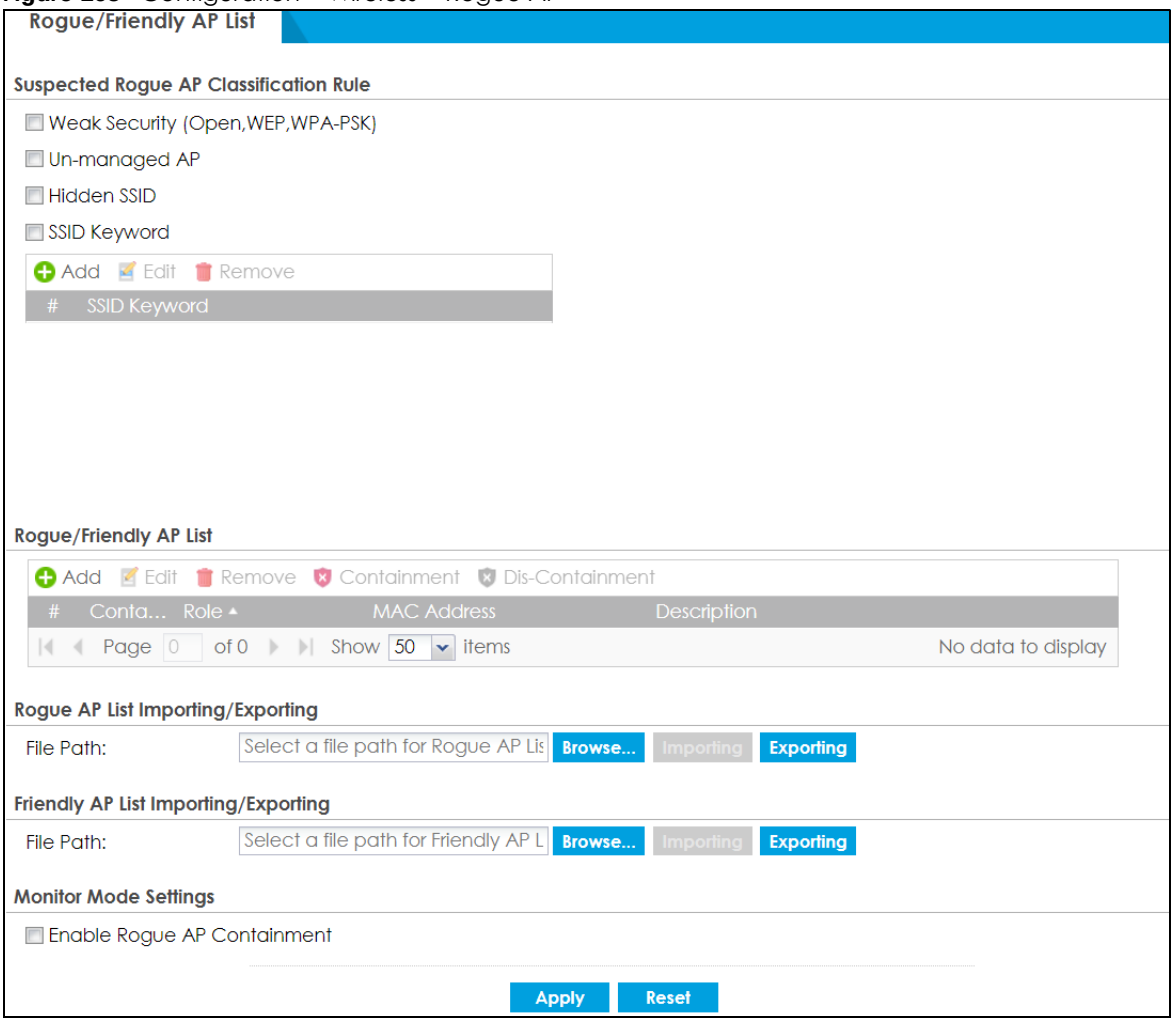
LABEL	DESCRIPTION
AP Firmware	
Runtime Firmware	This displays the current AP firmware version on the Zyxel Device. The Zyxel Device must have the latest AP firmware to manage all supported APs.
Available Firmware	This field displays if there is a later AP firmware version available on the firmware server. It displays **N/A** if the Zyxel Device cannot connect with the firmware server. Check that the Zyxel Device has Internet access if **N/A** displays and then click the **Check** button below. If a newer Zyxel Device AP firmware is available, its version number and a **More Details** icon displays here. Available Firmware: V5.00 Patch 4 -5.10(.2) 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 Zyxel Device display the latest AP firmware version available on the firmware server.
Apply AP Firmware	Due to space limitations, the Zyxel Device only downloads and keeps AP firmware for APs it is currently managing. If you connect a new AP to the Zyxel Device, the Zyxel Device 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 Zyxel Device. Firmware for APs that the Zyxel Device already has displays in bold; firmware that the Zyxel Device 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.

8.4 Rogue AP

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 > Rogue AP** to access this screen.

Figure 165 Configuration > Wireless > Rogue AP



Each field is described in the following table.

Table 84 Configuration > Wireless > Rogue AP

LABEL	DESCRIPTION
Suspected Rogue AP Classification Rule	Click the check boxes (**Weak Security (Open, WEP, WPA-PSK)**, **Un-managed AP**, **Hidden SSID**, **SSID Keyword**) of the characteristics an AP should have for the Zyxel Device to rule it as a rogue AP.
Add	Click this to add an SSID Keyword.
Edit	Select an SSID Keyword and click this button to modify it.
Remove	Select an existing SSID keyword and click this button to delete it.
#	This is the SSID Keyword's index number in this list.
SSID Keyword	This field displays the SSID Keyword.
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.

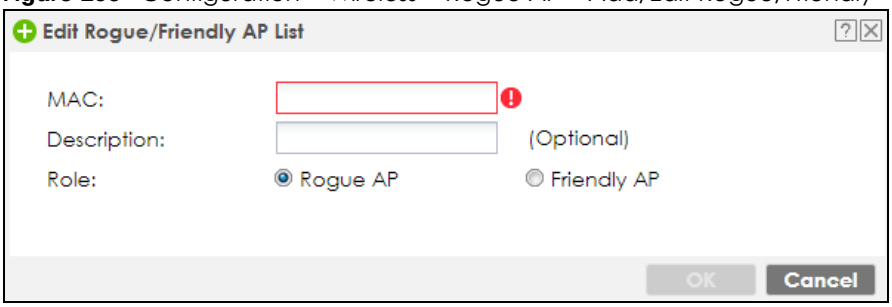
Table 84 Configuration > Wireless > Rogue AP (continued)

LABEL	DESCRIPTION
Containment	Click this button to quarantine the selected AP. A quarantined AP cannot grant access to any network services. Any stations that attempt to connect to a quarantined AP are disconnected automatically.
Dis-Containment	Click this button to take the selected AP out of quarantine. An unquarantined AP has normal access to the network.
#	This field is a sequential value, and it is not associated with any interface.
Containment	This field indicates the selected AP's containment status.
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 Zyxel Device.
Exporting	Click this button to export the current list of either rogue APs or friendly APS.
Monitor Mode Settings	
Enable Rogue AP Containment	Select this to enable rogue AP containment.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

8.4.1 Add/Edit Rogue/Friendly List

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

Figure 166 Configuration > Wireless > Rogue AP > Add/Edit Rogue/Friendly



Each field is described in the following table.

Table 85 Configuration > Wireless > Rogue AP > 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.

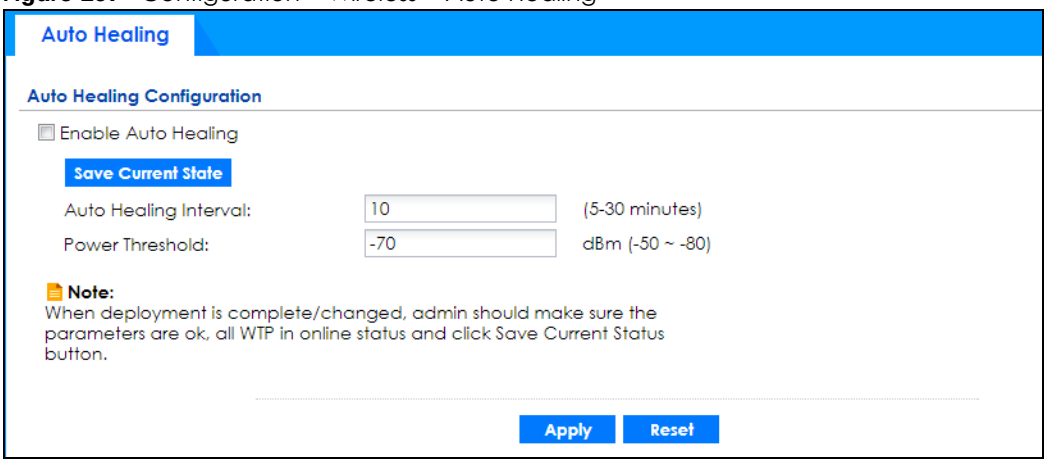
Table 85 Configuration > Wireless > Rogue AP > Add/Edit Rogue/Friendly (continued)

LABEL	DESCRIPTION
Role	Select either **Rogue AP** or **Friendly AP** for the AP's role.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to close the window with changes unsaved.

8.5 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 167 Configuration > Wireless > Auto Healing



Each field is described in the following table.

Table 86 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 manged APs immediately scan their neighborhoods three times in a row and update their neighbor lists to the AP controller (Zyxel Device).
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 (Zyxel Device). An AP is considered "failed" if the AP controller obtains the same scan result that the AP is missing from the neighbor list of other APs three times.
Power Threshold	Set the power level (in dBm) to which the neighbor APs of the failed AP increase their output power in order to extend their wireless service coverage areas. When the failed AP is working again, its neighbor APs return their output power to the original level.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

8.6 RTLS Overview

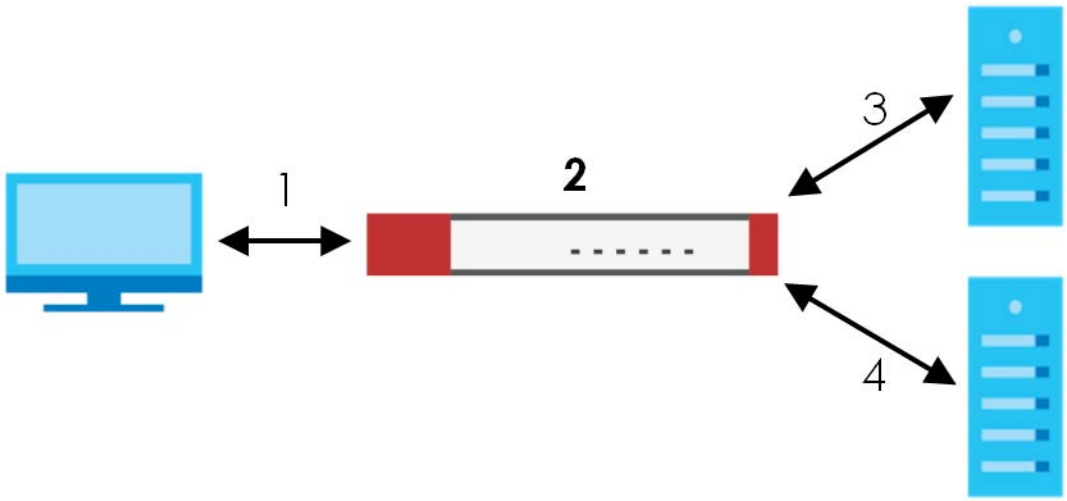
Ekahau RTLS (Real Time Location Service) tracks battery-powered Wi-Fi tags attached to APs managed by the Zyxel Device to create maps, alerts, and reports.

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 Zyxel Device 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 Zyxel Device.
3. The Zyxel Device forwards the signal measurements to the Ekahau RTLS Controller.
4. The Ekahau RTLS Controller calculates the tag positions.

Figure 168 RTLS Example



8.6.1 What You Can Do in this Chapter

Use the **RTLS** screen (Section 8.6.3 on page 210) to use the managed APs as part of an Ekahau RTLS (Real Time Location Service) to track the location of Ekahau Wi-Fi tags.

8.6.2 Before You Begin

You need:

- At least three APs managed by the Zyxel Device (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 Zyxel Device 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.

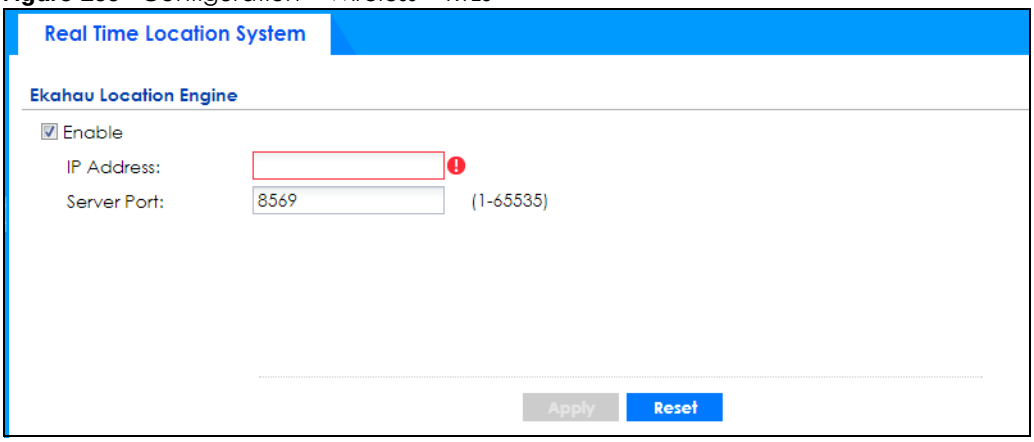
Table 87 RTLS Traffic Port Numbers

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

8.6.3 Configuring RTLS

Click **Configuration > Wireless > RTLS** to open this screen. Use this screen to turn RTLS (Real Time Location System) on or off and specify the IP address and server port of the Ekahau RTLS Controller.

Figure 169 Configuration > Wireless > RTLS



The following table describes the labels in this screen.

Table 88 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.

Table 88 Configuration > Wireless > RTLS (continued)

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

8.7 Technical Reference

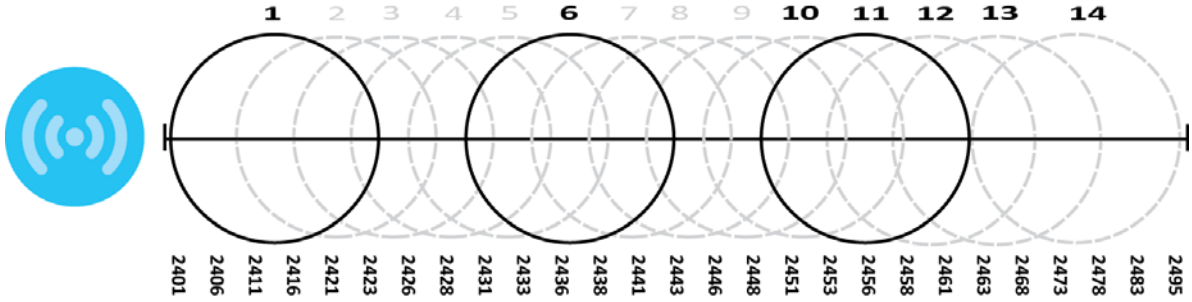
The following section contains additional technical information about wireless features.

8.7.1 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.

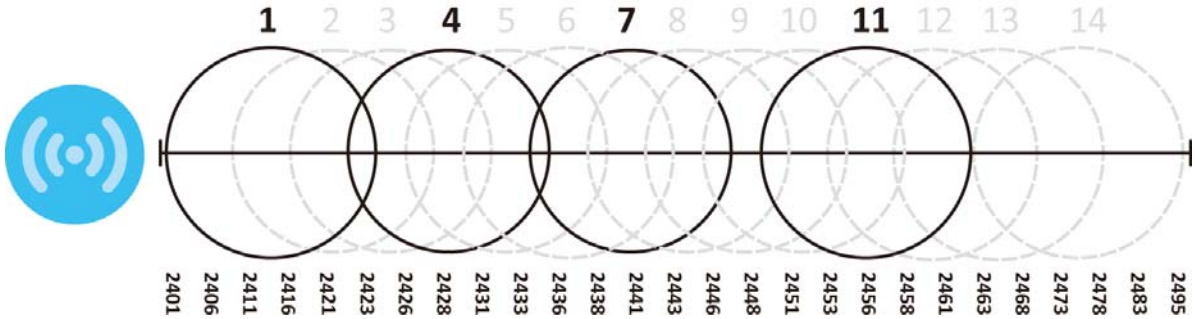
In the 2.4 GHz spectrum, each channel from 1 to 13 is broken up into discrete 22 MHz segments that are spaced 5 MHz apart. Channel 1 is centered on 2.412 GHz while channel 13 is centered on 2.472 GHz.

Figure 170 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.

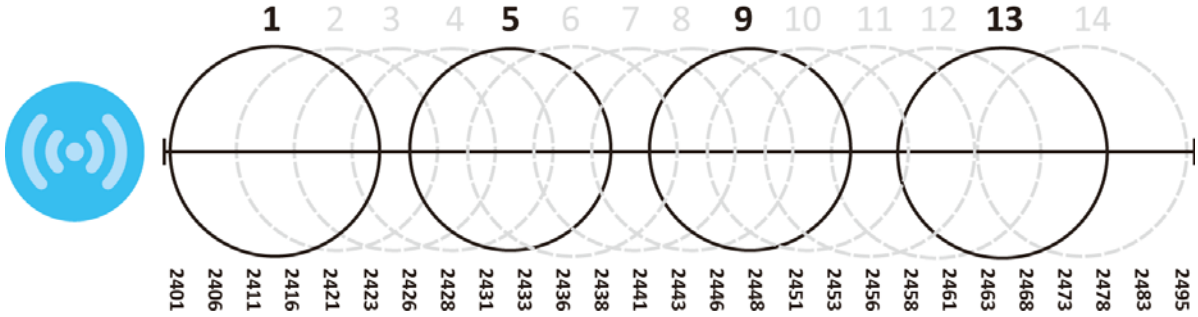
Figure 171 An Example Four-Channel Deployment



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 172 An Alternative Four-Channel Deployment



8.7.2 Load Balancing

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

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

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 9
Interfaces

9.1 Interface Overview

Use the **Interface** screens to configure the Zyxel Device'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 Zyxel Device. For example, You connect the LAN network to the LAN interface.
- **Zones** are groups of interfaces used to ease security policy configuration.

9.1.1 What You Can Do in this Chapter

- Use the **Port Role** screen (Section 9.2 on page 218) to create port groups and to assign physical ports and port groups to Ethernet interfaces.
- Use the **Port Configuration** screen (Section 9.3 on page 219) to configure Zyxel Device port settings.
- Use the **Ethernet** screens (Section 9.4 on page 220) to configure the Ethernet interfaces. Ethernet interfaces are the foundation for defining other interfaces and network policies. RIP and OSPF are also configured in these interfaces.
- Use the **PPP** screens (Section 9.5 on page 243) for PPPoE, PPTP or L2TP Internet connections.
- Use the **Cellular** screens (Section 9.6 on page 250) to configure settings for interfaces for Internet connections through an installed mobile broadband card.
- Use the **Tunnel** screens (Section 9.7 on page 259) to configure tunnel interfaces to be used in Generic Routing Encapsulation (GRE), IPv6 in IPv4, and 6to4 tunnels.
- Use the **VLAN** screens (Section 9.8 on page 266) to divide the physical network into multiple logical networks. VLAN interfaces receive and send tagged frames. The Zyxel Device automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- Use the **Bridge** screens (Section 9.9 on page 279) to combine two or more network segments into a single network.
- Use the **VTI** screens (Section 9.10 on page 293) to encrypt or decrypt IPv4 traffic from or to the interface according to the IP routing table.
- Use the **Trunk** screens (Section 9.11 on page 298) to configure load balancing.

9.1.2 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 Zyxel Device.

- Setting interfaces to the same port role forms a port group. Port groups creates 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** or **Interface > Port Groups** 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. RIP and OSPF are also configured in these interfaces.
- **Tunnel interfaces** send IPv4 or IPv6 packets from one network to a specific network through the Internet or a public network.
- **VLAN interfaces** receive and send tagged frames. The Zyxel Device 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 Zyxel Device. 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/L2TP interfaces.
- **Cellular interfaces** are for mobile broadband WAN connections via a connected mobile broadband device.
- **Virtual interfaces** provide additional routing information in the Zyxel Device. 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. The other types of interfaces--Ethernet, PPP, cellular, 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 89 Ethernet, PPP, Cellular, VLAN, Bridge, and Virtual Interface Characteristics

CHARACTERISTICS	ETHERNET	ETHERNET	PPP	CELLULAR	VLAN	BRIDGE	VIRTUAL
Name*	wan1, wan2	lan1, lan2, dmz	ppp*x*	cellular*x*	vlan*x*	br*x*	**
Configurable Zone	No	No	Yes	Yes	Yes	Yes	No
IP Address Assignment							
Static IP address	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DHCP client	Yes	No	Yes	Yes	Yes	Yes	No
Routing metric	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Interface Parameters							

Table 89 Ethernet, PPP, Cellular, VLAN, Bridge, and Virtual Interface Characteristics (continued)

CHARACTERISTICS	ETHERNET	ETHERNET	PPP	CELLULAR	VLAN	BRIDGE	VIRTUAL
Bandwidth restrictions	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Packet size (MTU)	Yes	Yes	Yes	Yes	Yes	Yes	No
DHCP							
DHCP server	No	Yes	No	No	Yes	Yes	No
DHCP relay	No	Yes	No	No	Yes	Yes	No
Connectivity Check	Yes	No	Yes	Yes	Yes	Yes	No

Note: - * 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, wan2, lan1, lan2, dmz; 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 Zyxel Device, 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 90 Relationships Between Different Types of Interfaces

INTERFACE	REQUIRED PORT / INTERFACE
Ethernet interface	physical port
VLAN interface	Ethernet interface
bridge interface	Ethernet interface* VLAN interface*
PPP interface	Ethernet interface* VLAN interface* bridge interface WAN1, WAN2, OPT*

Table 90 Relationships Between Different Types of Interfaces (continued)

INTERFACE	REQUIRED PORT / INTERFACE
virtual interface (virtual Ethernet interface) (virtual VLAN interface) (virtual bridge interface)	 Ethernet interface* VLAN interface* bridge interface
trunk	Ethernet interface Cellular interface VLAN interface bridge interface PPP interface

Note: * 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.

IPv6 Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10^{38} IP addresses.

IPv6 Addressing

An 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) from the left is the network prefix.

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows.

Table 91 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

Stateless Autoconfiguration

With stateless autoconfiguration in IPv6, addresses can be uniquely and automatically generated. Unlike DHCPv6 (Dynamic Host Configuration Protocol version six) which is used in IPv6 stateful autoconfiguration, the owner and status of addresses don't need to be maintained by a DHCP server. Every IPv6 device is able to generate its own and unique IP address automatically when IPv6 is initiated on its interface. It combines the prefix and the interface ID (generated from its own Ethernet MAC address) to form a complete IPv6 address.

When IPv6 is enabled on a device, its interface automatically generates a link-local address (beginning with fe80).

When the Zyxel Device's WAN interface is connected to an ISP with a router and the Zyxel Device is set to automatically obtain an IPv6 network prefix from the router for the interface, it generates another address which combines its interface ID and global and subnet information advertised from the router. (In IPv6, all network interfaces can be associated with several addresses.) This is a routable global IP address.

Prefix Delegation

Prefix delegation enables an IPv6 router (the Zyxel Device) to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Zyxel Device uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the router passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

IPv6 Router Advertisement

An IPv6 router sends router advertisement messages periodically to advertise its presence and other parameters to the hosts in the same network.

DHCPv6

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

Each DHCP client and server has a unique DHCP Unique IDentifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not change over time even after you reboot the device.

9.1.3 What You Need to Do First

For IPv6 settings, go to the **Configuration** > **System** > **IPv6** screen to enable IPv6 support on the Zyxel Device first.

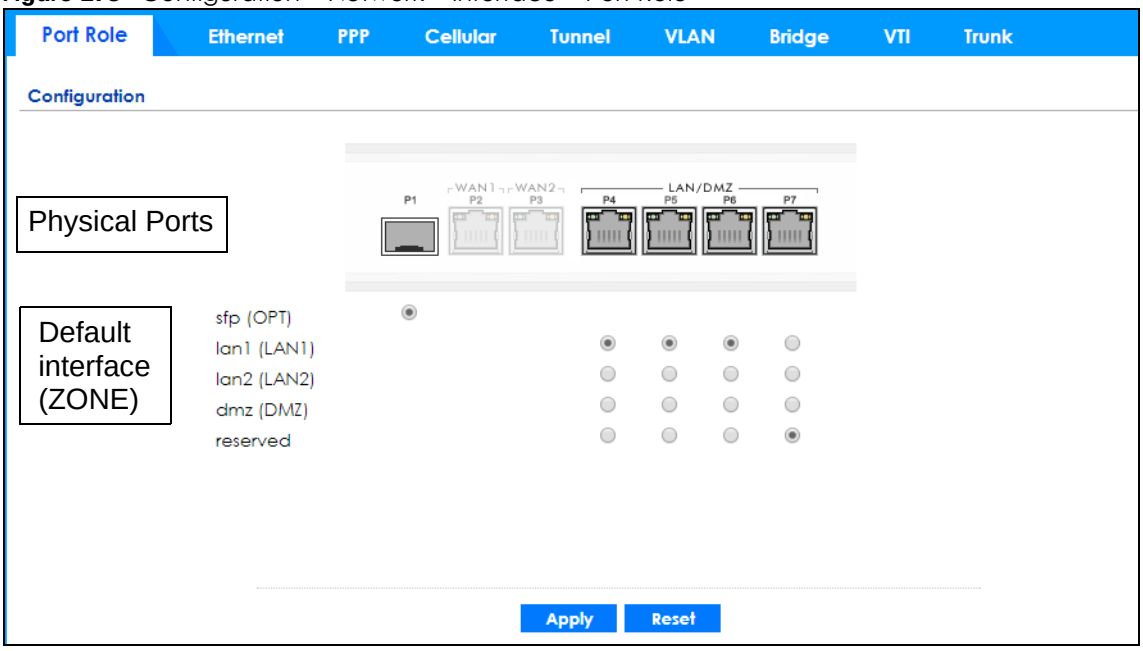
9.2 Port Role

To access this screen, click **Configuration > Network > Interface > Port Role**. Use the **Port Role** screen to set the Zyxel Device's flexible ports as part of the **lan1**, **lan2**, **ext-wlan, ext-lan** 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**, **ext-wlan, ext-lan** 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 Zyxel Device's **lan1**, **lan2**, **ext-wlan**, **ext-lan** or **dmz** IP address.
- Use the appropriate **lan1**, **lan2**, **ext-wlan**, **ext-lan** or **dmz** IP address to access the Zyxel Device.

Figure 173 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 LAN radio button to use the port as part of the LAN interface. The port will use the Zyxel Device's LAN 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 Zyxel Device.

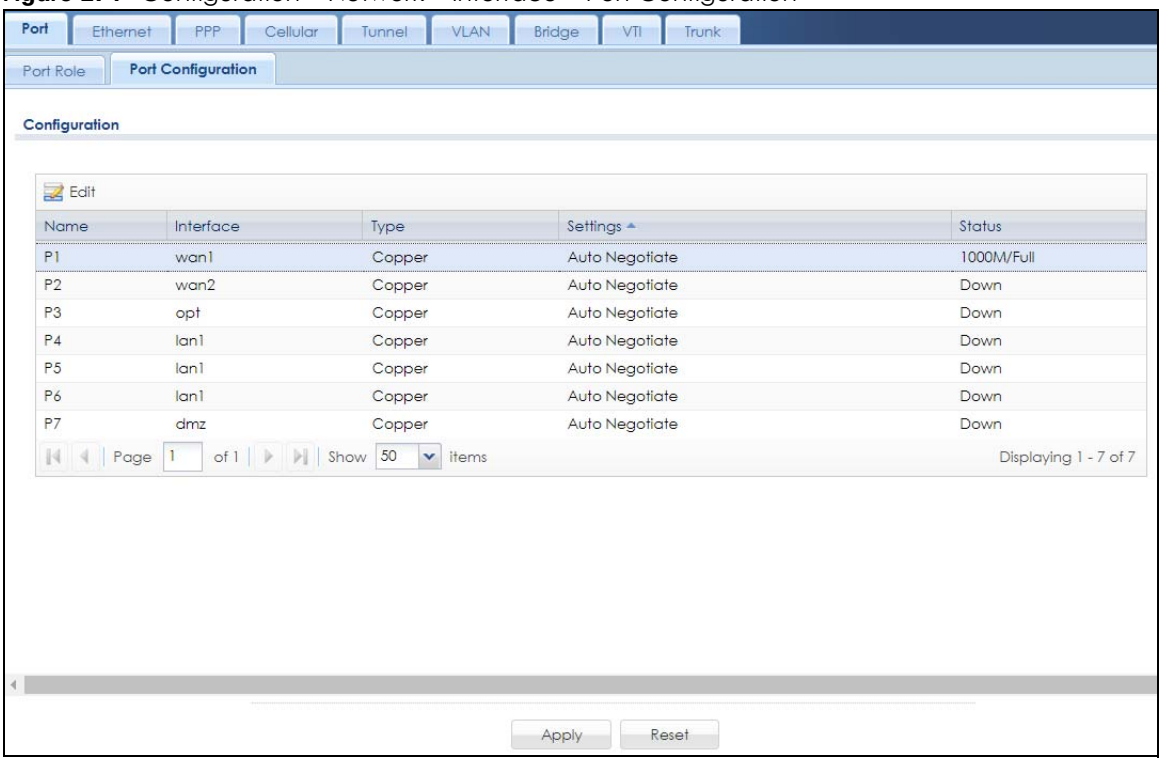
Click **Reset** to change the port groups to their current configuration (last-saved values).

9.3 Port Configuration

Use this screen to configure port settings. Click **Configuration** > **Network** > **Interface** > **Port Configuration** in the navigation panel to display the configuration screen.

Note: You can't configure the speed and duplex mode of the fiber ports on the USG2200 and UGS2200-VPN.

Figure 174 Configuration > Network > Interface > Port Configuration



Each field is described in the following table.

Table 92 Configuration > Network > Interface > Port Configuration

LABEL	DESCRIPTION
Edit	Select an entry, and click this button to configure the speed and the duplex mode of the Ethernet connection on this port.
Name	This field displays the name of the port.
Interface	This field displays the interface for the port.
Type	This field displays the cable type that is used on the port.
Settings	Select the speed and the duplex mode of the Ethernet connection on this port. Choices are **Auto Negotiate**, **1000Mbps-Full Duplex**, **100Mbps-Full Duplex**, **100Mbps-Half Duplex**, **10Mbps-Full Duplex**, and **10Mbps-Half Duplex**. Selecting **Auto Negotiate** allows one port to negotiate with a peer port automatically to obtain the connection speed (of up to 1000M) and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Zyxel Device negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the Zyxel Device determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Zyxel Device's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.
Status	This field displays the speed and the duplex mode of the Ethernet connection on the port.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

9.4 Ethernet Summary Screen

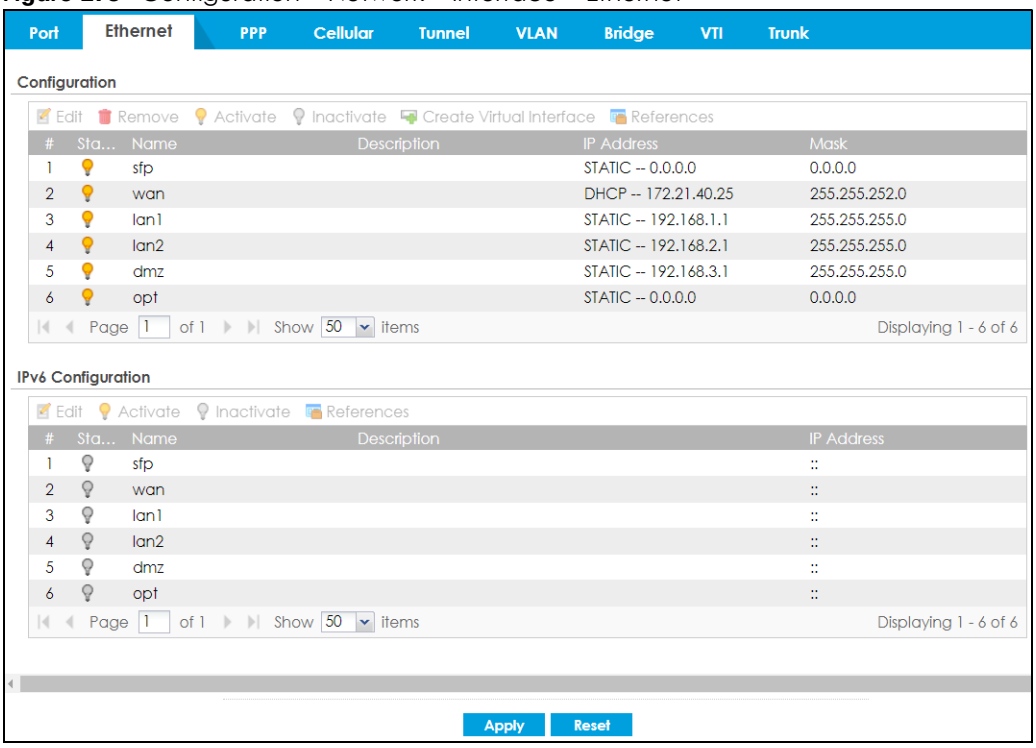
This screen lists every Ethernet interface and virtual interface created on top of Ethernet interfaces. If you enabled IPv6 in the **Configuration** > **System** > **IPv6** screen, you can also configure Ethernet interfaces used for your IPv6 networks on this screen. To access this screen, click **Configuration > 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, the Ethernet interface is effectively removed from the Zyxel Device, 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. The Zyxel Device supports the following routing protocols: RIP, OSPF and BGP. See Chapter 10 on page 321 for background information about these routing protocols.

Figure 175 Configuration > Network > Interface > Ethernet



Each field is described in the following table.

Table 93 Configuration > Network > Interface > Ethernet

LABEL	DESCRIPTION
Configuration / IPv6 Configuration	Use the **Configuration** section for IPv4 network settings. Use the **IPv6 Configuration** section for IPv6 network settings if you connect your Zyxel Device to an IPv6 network. Both sections have similar fields as described below.
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 Zyxel Device 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**.
References	Select an entry and click **References** to open a screen that shows which settings use the entry. See Section 9.4.4 on page 240 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.
Description	This field displays the description of the interface.

Table 93 Configuration > Network > Interface > Ethernet (continued)

LABEL	DESCRIPTION
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0 (in the IPv4 network) or :: (in the IPv6 network), the interface does not have an IP address yet. In the IPv4 network, this screen also shows whether the IP address is a static IP address (**STATIC**) or dynamically assigned (**DHCP**). IP addresses are always static in virtual interfaces. In the IPv6 network, this screen also shows whether the IP address is a static IP address (**STATIC**), link-local IP address (**LINK LOCAL**), dynamically assigned (**DHCP**), or an IPv6 StateLess Address AutoConfiguration IP address (**SLAAC**). See Section 9.1.2 on page 213 for more information about IPv6.
Mask	This field displays the interface's subnet mask in dot decimal notation.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

9.4.1 Ethernet Edit

The **Ethernet Edit** screen lets you configure IP address assignment, interface parameters, RIP settings, OSPF settings, DHCP settings, connectivity check, and MAC address settings. To access this screen, click an **Edit** icon in the **Ethernet Summary** screen. (See Section 9.4 on page 220.)

The OPT interface's **Edit** > **Configuration** screen is shown here as an example. The screens for other interfaces are similar and contain a subset to the OPT interface screen's fields.

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

With RIP, you can use Ethernet interfaces to do the following things.

- Enable and disable RIP in the underlying physical port or port group.
- Select which direction(s) routing information is exchanged - The Zyxel Device can receive routing information, send routing information, or do both.
- Select which version of RIP to support in each direction - The Zyxel Device supports RIP-1, RIP-2, and both versions.
- Select the broadcasting method used by RIP-2 packets - The Zyxel Device can use subnet broadcasting or multicasting.

With OSPF, you can use Ethernet interfaces to do the following things.

- Enable and disable OSPF in the underlying physical port or port group.
- Select the area to which the interface belongs.
- Override the default link cost and authentication method for the selected area.
- Select in which direction(s) routing information is exchanged - The Zyxel Device can receive routing information, send routing information, or do both.

Set the priority used to identify the DR or BDR if one does not exist.

9.4.1.1 IGMP Proxy

Internet Group Management Protocol (IGMP) proxy is used for multicast routing. IGMP proxy enables the Zyxel Device to issue IGMP host messages on behalf of hosts that the Zyxel Device discovered on its IGMP-enabled interfaces. The Zyxel Device acts as a proxy for its hosts. Refer to the following figure.

- DS: Downstream traffic
- US: Upstream traffic
- R: Router
- MS: Multicast Server
- Enable IGMP Upstream (US) on the Zyxel Device interface that connects to a router (R) running IGMP that is closer to the multicast server (MS).
- Enable IGMP Downstream on the Zyxel Device interface which connects to the multicast hosts.

Figure 176 IGMP Proxy

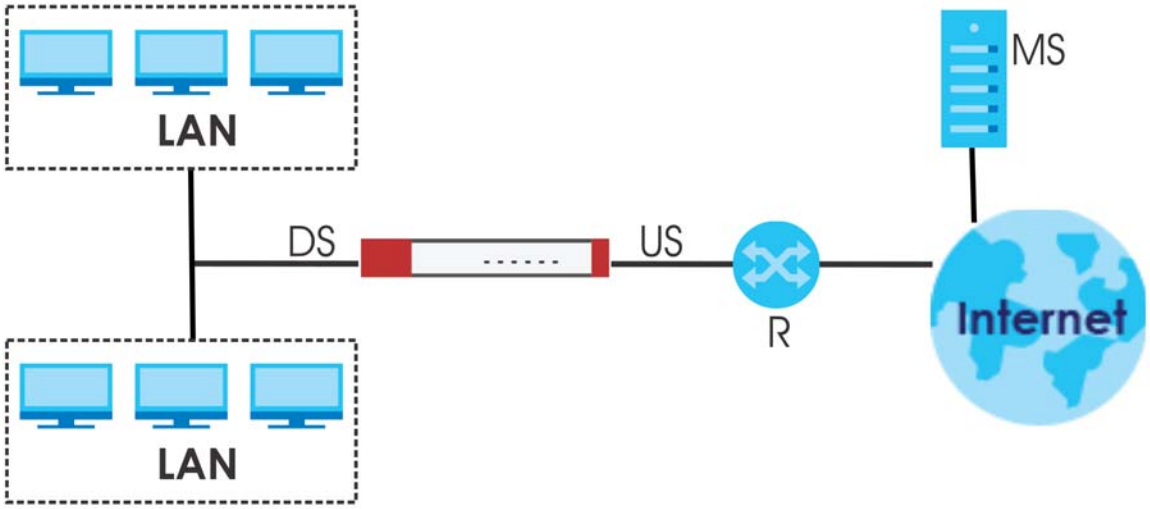


Figure 177 Configuration > Network > Interface > Ethernet > Edit (External Type)

Edit Ethernet

IPv4 View ▼ | Hide Advanced Settings | Create New Object

General Settings

☑ Enable Interface

Interface Properties

Interface Type: external
Interface Name: wan
Port: P2
Zone: WAN
MAC Address: BC:CF:4F:47:7A:43
Description: (Optional)

IP Address Assignment

◉ Get Automatically 172.21.40.25
Advance
DHCP Option 60: (Optional)

○ Use Fixed IP Address
IP Address:
Subnet Mask:
Gateway: (Optional)
Metric: 0 (0-15)
☐ Enable IGMP Support
◉ IGMP Upstream
○ IGMP Downstream

Interface Parameters

Egress Bandwidth: 1048576 Kbps
Advance
Ingress Bandwidth: 1048576 Kbps
MTU: 1500 Bytes

Connectivity Check

☐ Enable Connectivity Check
Check Method: icmp
Check Period: 30 (5-600 seconds)
Check Timeout: 5 (1-10 seconds)
Check Fail Tolerance: 5 (1-10)
◉ Check Default Gateway 172.21.43.254
○ Check These Addresses (Domain Name or IP Address)
(Optional)
Probe Succeeds When: any one respond(s)
Advance

RIP Setting

☐ Enable RIP
Direction: BiDir
Send Version: 2
Receive Version: 2
☐ V2-Broadcast

OSPF Setting

Area: none
Priority: 1 (0-255)
Link Cost: 10 (1-65535)
☐ Passive Interface
Authentication: None

MAC Address Setting

MAC Address Setting
Use Default MAC Address
BC:CF:4F:47:7A:43
Overwrite Default MAC Address
00:00:00:00:00:00
Clone by host
Proxy ARP
Enable Proxy ARP
Add
Remove
#
IP Address
Page
0
of 0
Show
50
items
No data to display
Related Setting
Configure PPPoE/PPTP
OK
Cancel

Figure 178 Configuration > Network > Interface > Ethernet > Edit (Internal Type)

Edit Ethernet

IPv4 View ▼ Hide Advanced Settings Create New Object

General Settings

Enable Interface

Interface Properties

Interface Type: internal
Interface Name: lan1
Port: P3, P4, P5
Zone: LAN1
MAC Address: BC:CF:4F:47:7A:44
Description: (Optional)

IP Address Assignment

IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Enable IGMP Support
IGMP Upstream
IGMP Downstream

Interface Parameters

Egress Bandwidth: 1048576 Kbps
Advance
Ingress Bandwidth: 1048576 Kbps
MTU: 1500 Bytes

Advance

Connectivity Check

Enable Connectivity Check
Check Method: icmp
Check Period: 30 (5-600 seconds)
Check Timeout: 5 (1-10 seconds)
Check Fail Tolerance: 5 (1-10)
Check These Addresses: (Domain Name or IP Address)
(Optional)
Probe Succeeds When: any one respond(s)

DHCP Setting

DHCP: DHCP Server
IP Pool Start Address: 192.168.1.33 Pool Size: 200
First DNS Server (Optional): ZyWALL
Second DNS Server (Optional): None
Third DNS Server (Optional): None
First WINS Server (Optional):
Second WINS Server (Optional):
Default Router: lan1 IP
Lease Time: infinite
2 days 0 hours (Optional) 0 minutes (Optional)

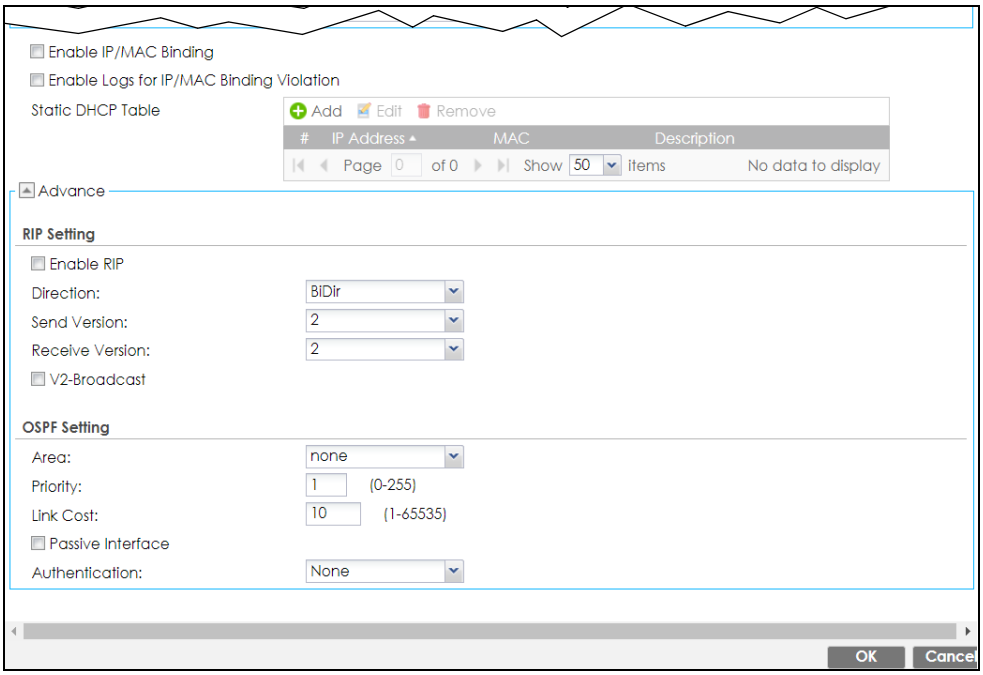
Advance
Extended Options

Add Edit Remove

#	Name	Code	Type	Value
Page 0 of 0 Show 50 items				No data to display

PXE Server:
PXE Boot Loader File:

Enable IP/MAC Binding
Enable Logs for IP/MAC Binding Violation
Static DHCP Table Add


Enable IP/MAC Binding
Enable Logs for IP/MAC Binding Violation
Static DHCP Table
Add
Edit
Remove
IP Address MAC Description
Page 0 of 0 Show 50 items No data to display
Advance
RIP Setting
Enable RIP
Direction: BiDir
Send Version: 2
Receive Version: 2
V2-Broadcast
OSPF Setting
Area: none
Priority: 1 (0-255)
Link Cost: 10 (1-65535)
Passive Interface
Authentication: None
OK
Cance

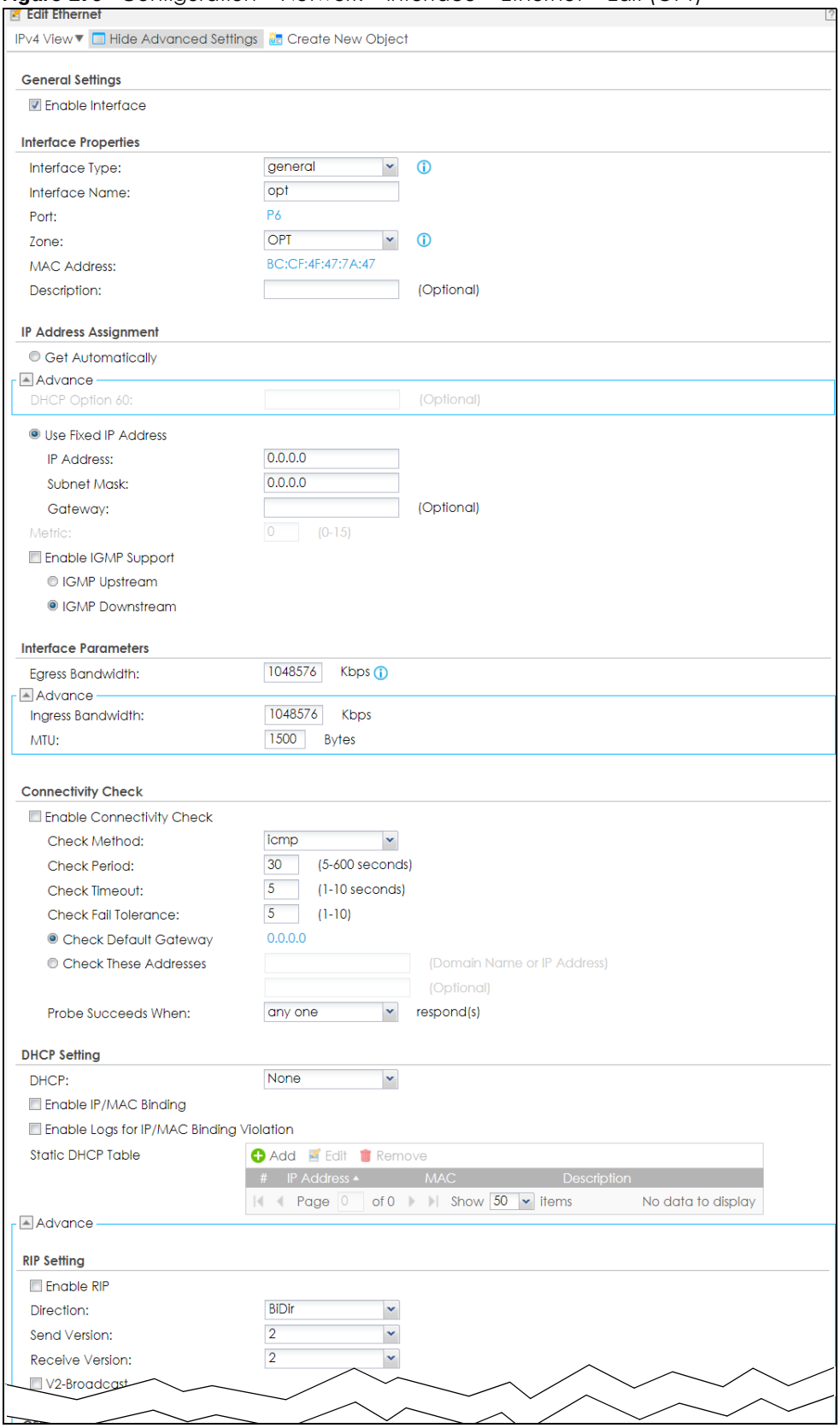



Figure 179 Configuration > Network > Interface > Ethernet > Edit (OPT)