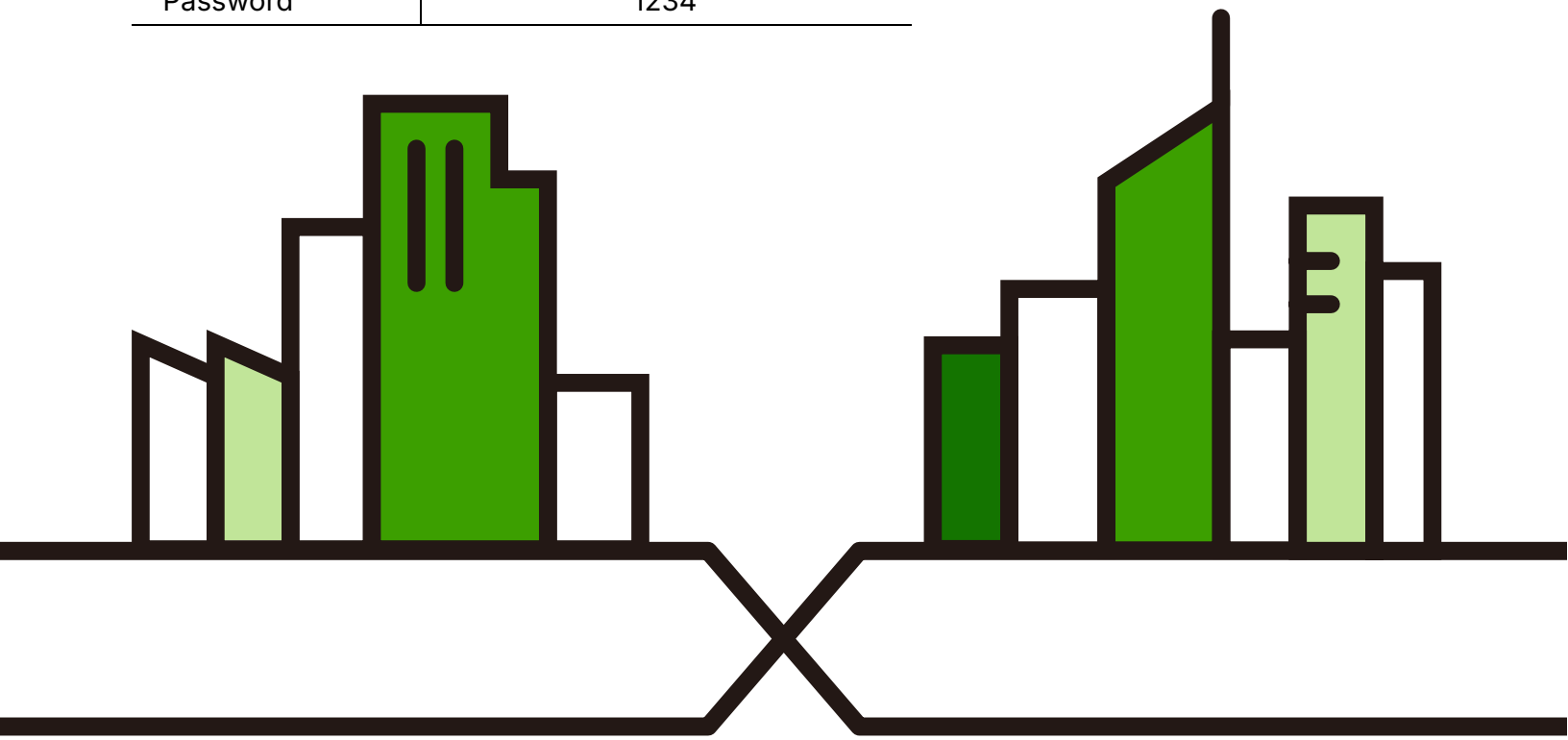
User's Guide

ZyWALL USG FLEX 50(AX) Series

Version 5.42 Edition 1, 1/2026

Default Login Details	
Login IP Address	https://(IP assigned by NCC) or https://myrouter.local or https://192.168.1.1
User Name	admin
Password	1234



Copyright © 2026 Zyxel and/or its affiliates. All rights reserved.

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.

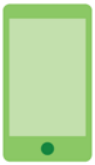
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

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

Contents Overview

Introduction 24
Web Configurator 39
Initial Setup Wizard 58
Hardware, Interfaces and Zones 85
Easy Mode 94
Quick Setup Wizards 158
Dashboard 204
Monitor 215
Licensing 266
Wireless 271
Interfaces 285
Routing 387
DDNS 414
NAT 420
Redirect Service 429
ALG 435
UPnP 442
IP/MAC Binding 458
Layer 2 Isolation 463
DNS Inbound LB 467
IPSec VPN 473
SSL VPN 511
L2TP VPN 517
BWM (Bandwidth Management) 523
Web Authentication 540
Security Policy 570
Content Filter 602
Anti-Spam 651
Astra Cloud Security 667
Object 669
Mgmt. & Analytics 766
System 779
Log and Report 843
File Manager 856
Diagnostics 876
Packet Flow Explore 893
Shutdown 900
Troubleshooting 903

Table of Contents

Document Conventions 3

Contents Overview 4

Table of Contents 5

Part I: User's Guide 23

Chapter 1
Introduction 24

1.1 Overview 24
1.1.1 Model Feature Differences 24
1.2 On Premises Mode 25
1.3 Monitor Mode 26
1.4 Nebula Mode 27
1.4.1 NCC Portal 28
1.4.2 Your Zyxel Device 28
1.4.3 Activation Email 29
1.5 Changing the Mode 30
1.5.1 From Nebula Mode to On Premises Mode 30
1.5.2 From On Premises Mode to Nebula Mode 32
1.5.3 From Nebula Mode to Cloud Monitoring Mode 32
1.6 Registration at Zyxel 32
1.6.1 Applications 33
1.7 Management Overview 36
1.8 Remote Access to the Zyxel Device Networks 38

Chapter 2
Web Configurator 39

2.1 Overview 39
2.2 Web Configurator Access 39
2.3 Security Best Practices 40
2.3.1 Two-Factor Authentication 41
2.3.2 Password Change 41
2.3.3 Security Policy Control 42
2.3.4 Security Check for Web Interface 42
2.3.5 Security Risk Warning 43
2.4 Web Configurator Screens Overview 44

2.5 Navigation Panel 48
2.6 Tables and Lists 54

Chapter 3
Initial Setup Wizard 58

3.1 Initial Setup Wizard: Select Management Mode 58
3.1.1 Welcome Screen 59
3.1.2 Internet Access Setup - WAN Interface 59
3.1.3 Internet Access: Ethernet 61
3.1.4 Internet Access: PPPoE 62
3.1.5 Internet Access: PPTP 63
3.1.6 Internet Access: L2TP 65
3.1.7 Internet Access Setup - Second WAN Interface 67
3.1.8 Internet Access: Congratulations 68
3.1.9 Date and Time Settings 69
3.1.10 Register Device 69
3.1.11 Activate Service 71
3.1.12 Service Settings 72
3.1.13 Service Settings: SecuReporter 73
3.1.14 Wireless Settings: Management Mode 74
3.1.15 Wireless Settings: AP Controller 75
3.1.16 Wireless Settings: SSID & Security 75
3.1.17 Remote Management 76
3.2 Nebula Mode Initial Setup Wizard 77
3.2.1 Connect to Internet (WAN) 78
3.2.2 Internet Access: Ethernet 79
3.2.3 Internet Access: PPPoE 80
3.2.4 Internet Access: Congratulations 82
3.2.5 QR Code 83

Chapter 4
Hardware, Interfaces and Zones 85

4.1 Hardware Overview 85
4.1.1 Front Panels 85
4.1.2 Rear Panels 87
4.1.3 Console Port Pin Connection 89
4.2 Installation Scenarios 90
4.2.1 Desk-mounting 90
4.2.2 Wall-mounting 91
4.3 Default Zones, Interfaces, and Ports 93
4.4 Stopping the Zyxel Device 93

Chapter 5
Easy Mode 94

5.1 Overview 94
5.1.1 Objects and Rules 94
5.1.2 Wizards and Links 95
5.1.3 Easy Mode Settings 96
5.1.4 Easy Mode Dashboard 97
5.2 Initial Setup Wizard - Language and Overview 99
5.2.1 Initial Setup Wizard - Internet 100
5.2.2 Initial Setup Wizard - Internet Access Errors 100
5.2.3 Initial Setup Wizard - Date and Time 102
5.2.4 Initial Setup Wizard - Register Device 103
5.2.5 Initial Setup Wizard - Activate Services 104
5.2.6 Initial Setup Wizard - Wi-Fi 106
5.2.7 Initial Setup Wizard - Congratulations 107
5.3 Initial Setup Wizard - Security Service 108
5.4 Initial Setup Wizard - Port Forwarding 110
5.5 Initial Setup Wizard - Guest LAN 111
5.5.1 Connecting AP Scenarios 112
5.6 Initial Setup Wizard - VPN 114
5.6.1 VPN Setup Wizard: Wizard Type 115
5.6.2 VPN Express Wizard - Scenario 115
5.6.3 VPN Express Wizard - Configuration 118
5.6.4 VPN Express Wizard - Summary 118
5.6.5 VPN Express Wizard - Finish 119
5.6.6 VPN Advanced Wizard - Scenario 120
5.6.7 VPN Advanced Wizard - Phase 1 Settings 121
5.6.8 VPN Advanced Wizard - Phase 2 123
5.6.9 VPN Advanced Wizard - Summary 124
5.6.10 VPN Advanced Wizard - Finish 126
5.7 VPN Settings for Configuration Provisioning Wizard: Wizard Type 127
5.7.1 Configuration Provisioning Express Wizard - VPN Settings 128
5.7.2 Configuration Provisioning VPN Express Wizard - Configuration 129
5.7.3 VPN Settings for Configuration Provisioning Express Wizard - Summary 130
5.7.4 VPN Settings for Configuration Provisioning Express Wizard - Finish 131
5.7.5 VPN Settings for Configuration Provisioning Advanced Wizard - Scenario 131
5.7.6 VPN Settings for Configuration Provisioning Advanced Wizard - Phase 1 Settings 132
5.7.7 VPN Settings for Configuration Provisioning Advanced Wizard - Phase 2 134
5.7.8 VPN Settings for Configuration Provisioning Advanced Wizard - Summary 135
5.7.9 VPN Settings for Configuration Provisioning Advanced Wizard- Finish 137
5.8 VPN Settings for L2TP VPN Settings Wizard 138
5.8.1 L2TP VPN Settings 1 140
5.8.2 L2TP VPN Settings 2 140
5.8.3 VPN Settings for L2TP VPN Setting Wizard - Summary 141
5.8.4 VPN Settings for L2TP VPN Setting Wizard Completed 142

5.9 Port Forwarding 143
5.9.1 Port Forwarding > Add Client 144
5.9.2 Port Forwarding > Add Service 144
5.9.3 Port Forwarding > UPnP 144
5.10 Wi-Fi and Guest Network Wizard 146
5.10.1 Guest LAN (Wired Network) 147
5.10.2 Connecting AP Scenarios 148
5.11 Security Service Wizard 149
5.11.1 Security Service Wizard 2 - Content Filter Categories 150
5.11.2 Security Service Wizard 3 - Websites 152
5.11.3 Security Service Wizard 4 - Exemptions 153
5.11.4 Security Service Wizard 5 - IDP/AV 154
5.12 MyZyxel Portal 155
5.13 Threat Intelligence Portal 155

Chapter 6
Quick Setup Wizards 158

6.1 Quick Setup Overview 158
6.2 WAN Interface Quick Setup 159
6.2.1 Choose an Ethernet Interface 159
6.2.2 Select WAN Type 160
6.2.3 Configure WAN IP Settings 160
6.2.4 ISP and WAN and ISP Connection Settings 161
6.2.5 Quick Setup Interface Wizard: Summary 164
6.3 Remote Access VPN Setup-Scenario 165
6.3.1 IKEv2 IPSec Client- VPN Configuration 166
6.3.2 IKEv2 IPSec Client- User Authentication 168
6.3.3 IKEv2 IPSec Client- Summary 168
6.3.4 IKEv2 IPSec Client-Config Provision 169
6.3.5 L2TP over IPSec Client-VPN Configuration 170
6.3.6 L2TP over IPSec Client- User Authentication 171
6.3.7 L2TP over IPSec Client- Summary 172
6.3.8 L2TP over IPSec Client-Config Provision 173
6.4 VPN Setup Wizard 173
6.4.1 Welcome 173
6.4.2 VPN Setup Wizard: Wizard Type 174
6.4.3 VPN Express Wizard - Scenario 175
6.4.4 VPN Express Wizard - Configuration 176
6.4.5 VPN Express Wizard - Summary 176
6.4.6 VPN Express Wizard - Finish 177
6.4.7 VPN Advanced Wizard - Scenario 178
6.4.8 VPN Advanced Wizard - Phase 1 Settings 179
6.4.9 VPN Advanced Wizard - Phase 2 181

6.4.10 VPN Advanced Wizard - Summary 182
6.4.11 VPN Advanced Wizard - Finish 184
6.5 VPN Settings for Configuration Provisioning Wizard: Wizard Type 185
6.5.1 Configuration Provisioning Express Wizard - VPN Settings 185
6.5.2 Configuration Provisioning VPN Express Wizard - Configuration 186
6.5.3 VPN Settings for Configuration Provisioning Express Wizard - Summary 187
6.5.4 VPN Settings for Configuration Provisioning Express Wizard - Finish 188
6.5.5 VPN Settings for Configuration Provisioning Advanced Wizard - Scenario 189
6.5.6 VPN Settings for Configuration Provisioning Advanced Wizard - Phase 1 Settings 190
6.5.7 VPN Settings for Configuration Provisioning Advanced Wizard - Phase 2 191
6.5.8 VPN Settings for Configuration Provisioning Advanced Wizard - Summary 192
6.5.9 VPN Settings for Configuration Provisioning Advanced Wizard - Finish 195
6.6 VPN Settings for L2TP VPN Settings Wizard 195
6.6.1 L2TP VPN Settings 196
6.6.2 L2TP VPN Settings 197
6.6.3 VPN Settings for L2TP VPN Setting Wizard - Summary 197
6.6.4 VPN Settings for L2TP VPN Setting Wizard - Completed 199
6.7 Wireless Setup Wizard 199
6.7.1 SSID 200
6.7.2 Radio 200
6.7.3 Summary 202
6.7.4 Wizard Completed 202

Chapter 7
Dashboard 204

7.1 Overview 204
7.1.1 What You Can Do in this Chapter 204
7.2 The General Screen 204
7.2.1 Device Information Screen 206
7.2.2 System Status Screen 207
7.2.3 Tx/Rx Statistics 207
7.2.4 The Latest Logs Screen 208
7.2.5 System Resources Screen 208
7.2.6 DHCP Table Screen 210
7.2.7 Number of Login Users Screen 211
7.2.8 Current Login User 212
7.2.9 VPN Status 212
7.2.10 SSL VPN Status 212
7.3 The VPN Screen 213

Part II: Technical Reference 214

Chapter 8
Monitor 215

8.1 Overview 215
8.1.1 What You Can Do in this Chapter 215
8.2 The Port Statistics Screen 216
8.2.1 The Port Statistics Graph Screen 217
8.3 Interface Status Screen 218
8.4 The Traffic Statistics Screen 222
8.5 The Session Monitor Screen 225
8.6 The DHCP Table Screen 227
8.7 The Device Insight Screen 228
8.7.1 The Device Insight Edit Screen 231
8.7.2 The Device Insight Feedback Screen 231
8.8 The Login Users Screen 232
8.9 IGMP Statistics 234
8.10 The DDNS Status Screen 235
8.11 IP/MAC Binding 235
8.12 Cellular Status Screen 236
8.12.1 More Information 239
8.13 The UPnP Port Status Screen 240
8.14 USB Storage Screen 241
8.15 Ethernet Neighbor Screen 242
8.16 FQDN Object Screen 243
8.17 AP Information: Radio List 245
8.17.1 Radio List: More Information 247
8.18 SSID Info 248
8.19 Station Info: Station List 249
8.20 Station Info: Top N Stations 251
8.21 Station Info: Single Station 252
8.22 The IPSec Screen 253
8.22.1 Regular Expressions in Searching IPSec SAs 255
8.23 The SSL Screen 255
8.24 The L2TP over IPSec Screen 256
8.25 The Content Filter Screen 257
8.25.1 Web Content Filter 257
8.25.2 DNS Content Filter 258
8.26 The Anti-Spam Screens 259
8.26.1 Anti-Spam Summary 259
8.26.2 The Anti-Spam Status Screen 261
8.27 Log Screens 263
8.27.1 View Log 263

Chapter 9
Licensing 266

9.1 Registration Overview 266
9.1.1 What you Need to Know 266
9.1.2 Registration Screen 267
9.1.3 Service Screen 267

Chapter 10
Wireless 271

10.1 Overview 271
10.1.1 What You Can Do in this Chapter 271
10.2 Built-in AP 271
10.2.1 Wireless > Built-in AP > General > Add/Edit SSID 272
10.2.2 Wireless > Built-in AP > Radio 276
10.3 Technical Reference 282
10.3.1 Dynamic Channel Selection 282
10.3.2 Load Balancing 284

Chapter 11
Interfaces 285

11.1 Interface Overview 285
11.1.1 What You Can Do in this Chapter 285
11.1.2 What You Need to Know 286
11.1.3 What You Need to Do First 290
11.2 Port Role 290
11.3 Port Group 291
11.4 Port Configuration 292
11.5 Ethernet Summary Screen 294
11.5.1 Ethernet Edit 296
11.5.2 Proxy ARP 312
11.5.3 Virtual Interfaces 313
11.5.4 References 314
11.5.5 Add/Edit DHCPv6 Request/Release Options 315
11.5.6 Add/Edit DHCP Extended Options 316
11.6 PPP Interfaces 317
11.6.1 PPP Interface Summary 318
11.6.2 PPP Interface Add or Edit 319
11.7 Cellular Configuration Screen 324
11.7.1 Cellular Choose Slot 327
11.7.2 Add / Edit Cellular Configuration 327
11.8 Tunnel Interfaces 333
11.8.1 Configuring a Tunnel 335
11.8.2 Tunnel Add or Edit Screen 336

11.9 VLAN Interfaces 340
11.9.1 VLAN Summary Screen 341
11.9.2 VLAN Add/Edit 342
11.10 Bridge Interfaces 354
11.10.1 Bridge Summary 355
11.10.2 Bridge Add/Edit 357
11.11 VTI 367
11.11.1 Restrictions for IPSec Virtual Tunnel Interface 368
11.11.2 VTI Screen 368
11.11.3 VTI Add/Edit 369
11.12 Trunk Overview 373
11.12.1 What You Need to Know 373
11.13 The Trunk Summary Screen 376
11.13.1 Configuring a User-Defined Trunk 377
11.13.2 Configuring the System Default Trunk 379
11.14 Example: WAN Trunk Failover 380
11.15 Example: Trunk Tagged VLAN Traffic to a Switch 382
11.16 Interface Technical Reference 382

Chapter 12
Routing 387

12.1 Policy and Static Routes Overview 387
12.1.1 What You Can Do in this Chapter 387
12.1.2 What You Need to Know 388
12.2 Policy Route Screen 389
12.2.1 Policy Route Edit Screen 391
12.3 IP Static Route Screen 396
12.3.1 Static Route Add/Edit Screen 396
12.4 Policy Routing Technical Reference 398
12.5 Routing Protocols Overview 398
12.5.1 What You Need to Know 399
12.6 The RIP Screen 399
12.7 The OSPF Screen 401
12.7.1 Configuring the OSPF Screen 404
12.7.2 OSPF Area Add/Edit Screen 405
12.7.3 Virtual Link Add/Edit Screen 407
12.8 BGP (Border Gateway Protocol) 408
12.8.1 Allow BGP Packets to Enter the Zyxel Device 408
12.8.2 Configuring the BGP Screen 409
12.8.3 The BGP Neighbors Screen 411
12.8.4 Example Scenario 412

Chapter 13
DDNS 414

13.1 DDNS Overview 414
13.1.1 What You Can Do in this Chapter 414
13.1.2 What You Need to Know 414
13.2 The DDNS Screen 415
13.2.1 The Dynamic DNS Add/Edit Screen 416

Chapter 14
NAT 420

14.1 Overview 420
14.2 NAT Overview 420
14.2.1 What You Can Do in this Chapter 420
14.2.2 What You Need to Know 421
14.3 The NAT Screen 422
14.3.1 The NAT Add/Edit Screen 423
14.4 NAT Technical Reference 426

Chapter 15
Redirect Service 429

15.1 Overview 429
15.1.1 HTTP Redirect 429
15.1.2 SMTP Redirect 429
15.1.3 What You Can Do in this Chapter 430
15.1.4 What You Need to Know 430
15.2 The Redirect Service Screen 432
15.2.1 The Redirect Service Edit Screen 433

Chapter 16
ALG 435

16.1 ALG Overview 435
16.1.1 What You Need to Know 435
16.1.2 Before You Begin 438
16.2 The ALG Screen 438
16.3 ALG Technical Reference 440

Chapter 17
UPnP 442

17.1 UPnP and NAT-PMP Overview 442
17.2 What You Need to Know 442
17.2.1 NAT Traversal 442
17.2.2 Cautions with UPnP and NAT-PMP 443
17.3 UPnP Screen 443
17.4 Technical Reference 444
17.4.1 Turning on UPnP in Windows 7 Example 444

17.4.2 Turn on UPnP in Windows 10 Example 448
17.4.3 Auto-discover Your UPnP-enabled Network Device 450
17.4.4 Web Configurator Easy Access in Windows 7 453
17.4.5 Web Configurator Easy Access in Windows 10 455

Chapter 18
IP/MAC Binding 458

18.1 IP/MAC Binding Overview 458
18.1.1 What You Can Do in this Chapter 458
18.1.2 What You Need to Know 458
18.2 IP/MAC Binding Summary 459
18.2.1 IP/MAC Binding Edit 460
18.2.2 Static DHCP Edit 461
18.3 IP/MAC Binding Exempt List 462

Chapter 19
Layer 2 Isolation 463

19.1 Overview 463
19.1.1 What You Can Do in this Chapter 463
19.2 Layer-2 Isolation General Screen 464
19.3 Allow List Screen 465
19.3.1 Add/Edit Allow List Rule 466

Chapter 20
DNS Inbound LB 467

20.1 DNS Inbound Load Balancing Overview 467
20.1.1 What You Can Do in this Chapter 467
20.2 The DNS Inbound LB Screen 468
20.2.1 The DNS Inbound LB Add/Edit Screen 469
20.2.2 The DNS Inbound LB Add/Edit Member Screen 471

Chapter 21
IPSec VPN 473

21.1 Virtual Private Networks (VPN) Overview 473
21.1.1 What You Can Do in this Chapter 475
21.1.2 What You Need to Know 475
21.1.3 Before You Begin 478
21.2 The VPN Connection Screen 478
21.2.1 The VPN Connection Add/Edit Screen 480
21.3 The VPN Gateway Screen 487
21.3.1 The VPN Gateway Add/Edit Screen 488
21.4 VPN Concentrator 495
21.4.1 VPN Concentrator Requirements and Suggestions 495

21.4.2 VPN Concentrator Screen 495
21.4.3 The VPN Concentrator Add/Edit Screen 496
21.5 Zyxel Device IPSec VPN Client Configuration Provisioning 497
21.6 Example: IPSec VPN with IKEv2 on a Mobile Phone 499
21.6.1 Configuration on Android 499
21.6.2 Configuration on iOS 500
21.7 IPSec VPN Background Information 500

Chapter 22
SSL VPN 511

22.1 Overview 511
22.1.1 What You Can Do in this Chapter 511
22.1.2 What You Need to Know 511
22.2 The SSL Access Privilege Screen 512
22.2.1 The SSL Access Privilege Policy Add/Edit Screen 514
22.3 The SSL Global Setting Screen 516

Chapter 23
L2TP VPN 517

23.1 Overview 517
23.1.1 What You Can Do in this Chapter 517
23.1.2 What You Need to Know 517
23.2 L2TP VPN Screen 518
23.2.1 Example: L2TP and Zyxel Device Behind a NAT Router 520

Chapter 24
BWM (Bandwidth Management) 523

24.1 Overview 523
24.1.1 What You Can Do in this Chapter 523
24.1.2 What You Need to Know 523
24.2 The Bandwidth Management Configuration 527
24.2.1 The Bandwidth Management Add/Edit Screen 530
24.3 Example: Prioritize a Specific Application 538

Chapter 25
Web Authentication 540

25.1 Web Auth Overview 540
25.1.1 What You Can Do in this Chapter 540
25.1.2 What You Need to Know 541
25.2 Web Authentication General Screen 542
25.2.1 User-Authentication Access Control Example 547
25.2.2 Authentication Type Screen 553
25.2.3 Custom Web Portal / User Agreement File Screen 557

25.3 SSO Overview 558
25.4 SSO - Zyxel Device Configuration 560
25.4.1 Configuration Overview 560
25.4.2 Configure the Zyxel Device to Communicate with SSO 560
25.4.3 Enable Web Authentication 561
25.4.4 Create a Security Policy 563
25.4.5 Configure User Information 564
25.4.6 Configure an Authentication Method 564
25.4.7 Configure Active Directory 565
25.5 SSO Agent Configuration 566

Chapter 26
Security Policy 570

26.1 Overview 570
26.2 What You Can Do in this Chapter 571
26.2.1 What You Need to Know 571
26.3 The Security Policy Screen 572
26.3.1 Configuring the Security Policy Control Screen 573
26.3.2 The Security Check for Web Interface Screen 576
26.3.3 The Security Policy Control Add/Edit Screen 580
26.3.4 Example: Allow a Server to Ping the Zyxel Device Without Creating Logs 582
26.3.5 Example: Create a Guest Network with Internet Access Only 584
26.4 Anomaly Detection and Prevention Overview 587
26.4.1 The Anomaly Detection and Prevention General Screen 587
26.4.2 Creating New ADP Profiles 588
26.4.3 Traffic Anomaly Profiles 590
26.4.4 Protocol Anomaly Profiles 592
26.4.5 The ADP Allow List Screen 595
26.4.6 Creating New ADP Allow List Rule 596
26.5 The Session Control Screen 596
26.5.1 The Session Control Add/Edit Screen 598
26.6 Security Policy Example Applications 599

Chapter 27
Content Filter 602

27.1 Overview 602
27.1.1 What You Can Do in this Chapter 602
27.1.2 What You Need to Know 602
27.1.3 Before You Begin 604
27.2 Web Content Filter General Screen 605
27.2.1 Apply to a Security Policy 607
27.2.2 Web Content Filter Add Category Service 609
27.2.3 Content Filter Add Filter Profile Custom Service 622

27.3 Web Content Filter Trusted Web Sites Screen 625
27.4 Web Content Filter Forbidden Web Sites Screen 626
27.5 DNS Content Filter General Screen 627
27.5.1 DNS Content Filter Add Profile 629
27.6 DNS Content Filter Allow List Screen 642
27.7 DNS Content Filter Block List Screen 643
27.8 Content Filter Technical Reference 644
27.9 Example: Block LAN Users From Using a Remote WAN Application 645

Chapter 28
Anti-Spam 651

28.1 Overview 651
28.1.1 What You Can Do in this Chapter 651
28.1.2 What You Need to Know 651
28.2 Before You Begin 652
28.3 The Anti-Spam Profile Screen 653
28.3.1 The Anti-Spam Profile Add or Edit Screen 654
28.4 The Mail Scan Screen 656
28.5 The Anti-Spam Block List Screen 657
28.5.1 The Anti-Spam Block or Allow List Add/Edit Screen 659
28.5.2 Regular Expressions in Block or Allow List Entries 660
28.6 The Anti-Spam Allow List Screen 660
28.7 The DNSBL Screen 662
28.8 Anti-Spam Technical Reference 663

Chapter 29
Astra Cloud Security 667

29.1 Overview 667
29.2 Astra Cloud Security Screen 667

Chapter 30
Object 669

30.1 The Device Insight Screen 669
30.1.1 Device Insight Add/Edit Screen 670
30.1.2 Example: Block a Profile 671
30.2 Zones Overview 675
30.2.1 What You Need to Know 676
30.2.2 The Zone Screen 677
30.3 User/Group Overview 678
30.3.1 What You Need To Know 679
30.3.2 User/Group User Summary Screen 681
30.3.3 User Add/Edit General Screen 682
30.3.4 User Add/Edit Two-factor Authentication Screen 686

30.3.5 User/Group Group Summary Screen 697
30.3.6 User/Group Setting Screen 699
30.3.7 User/Group MAC Address Summary Screen 703
30.3.8 User /Group Technical Reference 705
30.4 Address/Geo IP Overview 706
30.4.1 What You Need To Know 706
30.4.2 Address Summary Screen 707
30.4.3 Address Group Summary Screen 711
30.4.4 Geo IP Summary Screen 713
30.5 Service Overview 716
30.5.1 What You Need to Know 716
30.5.2 The Service Summary Screen 717
30.5.3 The Service Group Summary Screen 719
30.6 Schedule Overview 721
30.6.1 What You Need to Know 721
30.6.2 The Schedule Screen 721
30.6.3 The Schedule Group Screen 724
30.7 AAA Server Overview 726
30.7.1 Directory Service (AD/LDAP) 726
30.7.2 RADIUS Server 727
30.7.3 ASAS 727
30.7.4 What You Need To Know 728
30.7.5 Active Directory or LDAP Server Summary 729
30.7.6 RADIUS Server Summary 732
30.8 Auth. Method Overview 735
30.8.1 Before You Begin 735
30.8.2 Example: Selecting a VPN Authentication Method 735
30.8.3 Authentication Method Objects 736
30.8.4 Two-Factor Authentication 738
30.8.5 Two-Factor Authentication VPN Access 741
30.8.6 Two-Factor Authentication Admin Access 743
30.8.7 Example: Admin Login with Two-factor Authentication by SMS 744
30.9 Certificate Overview 745
30.9.1 What You Need to Know 745
30.9.2 Verifying a Certificate 747
30.9.3 The My Certificates Screen 748
30.9.4 The Trusted Certificates Screen 757
30.9.5 Certificates Technical Reference 762
30.10 ISP Account Overview 762
30.10.1 ISP Account Summary 762

Chapter 31
Mgmt. & Analytics 766

31.1 Mgmt. & Analytics Overview 766
31.1.1 What You Can Do in this Chapter 766
31.2 Cloud CNM SecuManager 766
31.3 Cloud CNM SecuReporter 769
31.4 Nebula 773
31.4.1 Cloud Monitoring Mode 773
31.4.2 Cloud Management Scenario A - Native Mode 775

Chapter 32
System 779

32.1 Overview 779
32.1.1 What You Can Do in this Chapter 779
32.2 Host Name 780
32.3 USB Storage 780
32.4 Date and Time 782
32.4.1 Pre-defined NTP Time Servers List 785
32.4.2 Time Server Synchronization 785
32.5 Console Port Speed 786
32.6 DNS Overview.....787
32.6.1 DNS Server Address Assignment 787
32.6.2 Configuring the DNS Screen 787
32.6.3 (IPv6) Address Record 790
32.6.4 PTR Record 791
32.6.5 Adding an (IPv6) Address/PTR Record 791
32.6.6 CNAME Record 791
32.6.7 Adding a CNAME Record 792
32.6.8 Domain Zone Forwarder 792
32.6.9 Adding a Domain Zone Forwarder 792
32.6.10 MX Record 793
32.6.11 Adding a MX Record 793
32.6.12 Security Option Control 794
32.6.13 Editing a Security Option Control 794
32.6.14 Adding a DNS Service Control Rule 795
32.7 WWW Overview 796
32.7.1 Service Access Limitations 796
32.7.2 System Timeout 797
32.7.3 HTTPS 797
32.7.4 Configuring WWW Service Control 798
32.7.5 Service Control Rules 801
32.7.6 Customizing the WWW Login Page 802
32.7.7 HTTPS Example 807
32.8 SSH 814
32.8.1 SSH Implementation on the Zyxel Device 815

32.8.2 Requirements for Using SSH 815
32.8.3 Configuring SSH 815
32.8.4 Service Control Rules 816
32.8.5 SSH Example 817
32.9 Telnet 818
32.9.1 Configuring Telnet 818
32.9.2 Service Control Rules 820
32.10 FTP 820
32.10.1 Configuring FTP 820
32.10.2 Service Control Rules 822
32.11 SNMP 822
32.11.1 SNMPv3 and Security 823
32.11.2 Supported MIBs 824
32.11.3 SNMP Traps 824
32.11.4 Configuring SNMP 824
32.11.5 Add SNMPv3 User 827
32.11.6 Service Control Rules 827
32.12 Authentication Server 828
32.12.1 Add/Edit Trusted RADIUS Client 830
32.13 Notification > Mail Server 831
32.14 Notification > SMS 832
32.15 Notification > Response Message 833
32.16 Language Screen 834
32.17 IPv6 Screen 835
32.18 Zyxel One Network (ZON) Utility 836
32.18.1 Requirements 836
32.18.2 Run the ZON Utility 837
32.18.3 Zyxel One Network (ZON) System Screen 840
32.19 Advanced Screen 841
32.19.1 Fast Forwarding Technical Reference 841

Chapter 33
Log and Report 843

33.1 Overview 843
33.1.1 What You Can Do In this Chapter 843
33.2 Email Daily Report 843
33.3 Log Setting Screens 845
33.3.1 Log Setting Summary 845
33.3.2 Edit System Log Settings 847
33.3.3 Edit Log on USB Storage Setting 850
33.3.4 Edit Remote Server Log Settings 851
33.3.5 Log Category Settings Screen 853

Chapter 34
File Manager 856

34.1 Overview 856
34.1.1 What You Can Do in this Chapter 856
34.1.2 What you Need to Know 856
34.2 The Configuration Screen 860
34.2.1 The Configuration Schedule Backup Screen 865
34.3 Firmware Management 866
34.3.1 Cloud Helper 866
34.3.2 The Firmware Management Screen 868
34.3.3 Firmware Upgrade through USB Stick 872
34.3.4 Firmware Integrity Check 872
34.4 The Shell Script Screen 873

Chapter 35
Diagnostics 876

35.1 Overview 876
35.1.1 What You Can Do in this Chapter 876
35.2 The Diagnostics Screens 876
35.2.1 Scripts 876
35.2.2 The Diagnostics Controller Screen 877
35.2.3 The Diagnostics Files Screen 879
35.3 The Packet Capture Screen 880
35.3.1 The Packet Capture Files Screen 883
35.4 The CPU / Memory Status Screen 884
35.5 The System Log Screen 885
35.6 The Network Tool Screen 886
35.7 The Routing Traces Screen 890
35.8 The Wireless Frame Capture Screen 891
35.8.1 The Wireless Frame Capture Files Screen 892

Chapter 36
Packet Flow Explore 893

36.1 Overview 893
36.1.1 What You Can Do in this Chapter 893
36.2 Routing Status 893
36.3 The SNAT Status Screen 897

Chapter 37
Shutdown 900

37.1 Overview 900
37.1.1 What You Need To Know 900
37.2 The Shutdown / Reboot Screen 900

Part III: Appendices and Troubleshooting 902

Chapter 38
Troubleshooting.....903

38.1 Resetting the Zyxel Device 918
38.2 Getting More Troubleshooting Help 918

Appendix A Customer Support 919

Appendix B Product Features..... 925

Appendix C Legal Information..... 929

Index..... 937

PART I
User's Guide

CHAPTER 1 Introduction

1.1 Overview

Zyxel Device refers to these models as outlined below.

- USG FLEX 50 (USG20-VPN)
- USG FLEX 50AX
- USG20W-VPN

1.1.1 Model Feature Differences

Note the following differences between these models:

Table 1 USG FLEX 50 Series Model Feature Comparison

FEATURE/MODEL	USG FLEX 50 (USG20-VPN)	USG20W-VPN	USG FLEX 50AX
Microsoft Azure	YES	YES	YES
Amazon VPC	CLI only	CLI only	CLI only
Anomaly Detection & Prevention	YES	YES	YES
Anti-Spam	YES	YES	YES
IPS (IDP)	NO	NO	NO
Anti-Malware	NO	NO	NO
App Patrol	NO	NO	NO
Web Security (Content Filtering)	YES	YES	YES
SecuReporter	YES	YES	YES
Reputation Filter (IP & DNS)	NO	NO	NO
URL Threat Filter	NO	NO	NO
Sandboxing	NO	NO	NO
IP Exception	NO	NO	NO
AP Controller	NO	NO	NO
Device HA Pro	NO	NO	NO
Easy Mode	YES	YES	NO
Hotspot Management	NO	NO	NO
Concurrent Device Upgrade	NO	NO	NO
LAG	NO	NO	NO
Port Group	NO	NO	NO
Port Role	YES	YES	YES
SD-WAN Mode	NO	NO	NO
SSL Application	YES	YES	YES

Table 1 USG FLEX 50 Series Model Feature Comparison (continued)

FEATURE/MODEL	USG FLEX 50 (USG20-VPN)	USG20W-VPN	USG FLEX 50AX
SSL encrypted traffic inspection	YES	YES	YES
Bundled UTM Feature License Validity	1 year	1 year	1 year
WiFi functionality (built-in)	NO	YES	YES
Virtual Server Load Balancing	NO	NO	NO
Built-in AP	NO	YES	YES
Management by Nebula Control Center (NCC)	YES	YES	YES

- Not all models support all features. See Table 1.1.1 on page 24 for the specific features that your model supports.

Table 2 Security Feature List

• Application Security (Application Patrol)	• Intrusion Prevention System (IPS)
• Anomaly Detection & Prevention (ADP)	• Web Filtering (Content Filtering)
• Malware Blocker (Anti-Virus)	• Email Security (Anti-Spam)
• Secure Socket Layer (SSL) encrypted traffic Inspection	

The following security features work without a security license:

- Configuration > Content Filter > Trusted Web Sites
- Configuration > Anti-Spam/Email Security > Block/Allow List

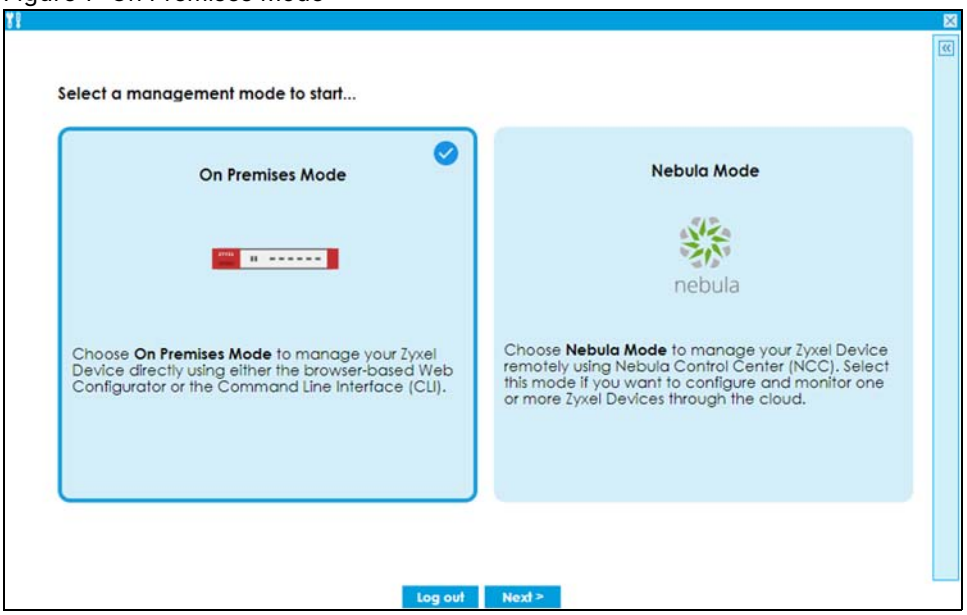
For information on interface names by model, default port or interface name mapping, and default interface or zone mapping please see Section 4.3 on page 93.

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

1.2 On Premises Mode

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. Choose On Premises Mode to manage your Zyxel Device directly using either the browser-based Web Configurator or the Command Line Interface (CLI).

Figure 1 On Premises Mode



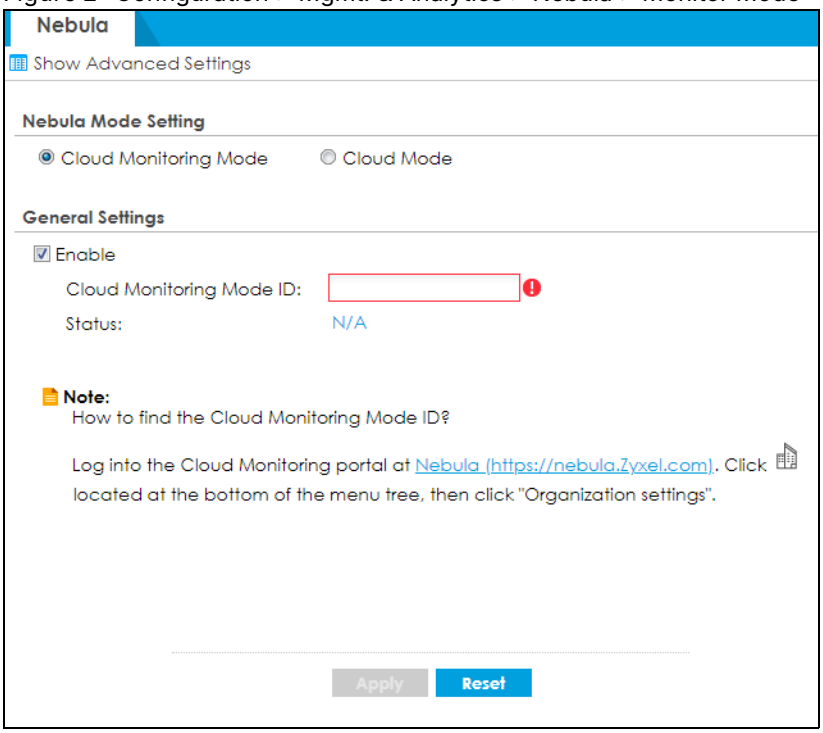
Follow the wizard to configure the Zyxel Device network settings to manage your Zyxel Device directly. Note that once you complete the device registration step and register your Zyxel Device at portal.myzyxel.com, you cannot change to Nebula Mode unless you reset the Zyxel Device.

1.3 Monitor Mode

Select Monitor Mode in Configuration > Mgmt. & Analytics > Nebula > Monitor Mode to monitor your Zyxel Device using Nebula Control Center (NCC) but configure settings on the web configurator at the same time. You must have created an organization and a site on NCC first.

Note: You cannot set the Zyxel Device to Monitor Mode if Device HA is enabled on the Zyxel Device.

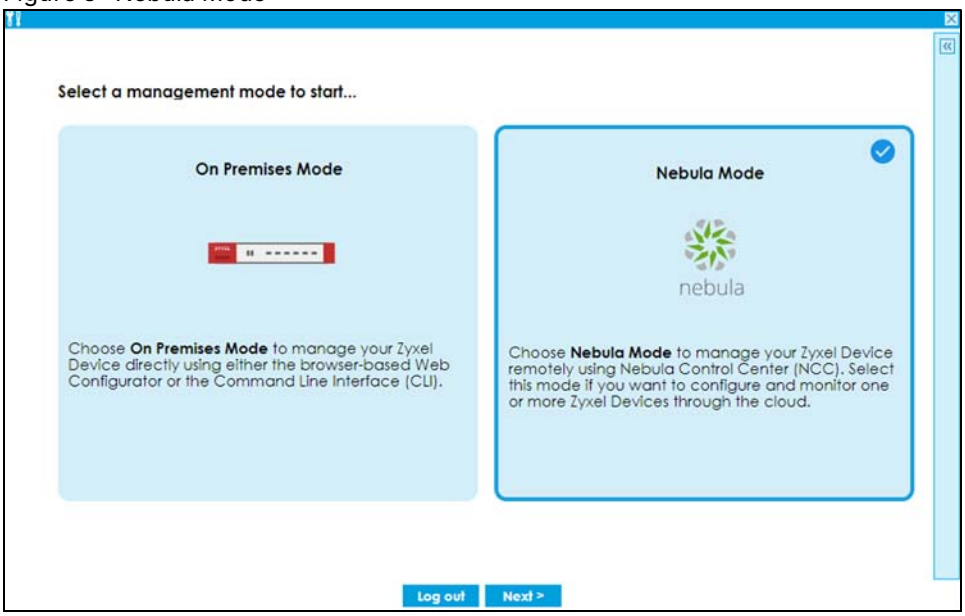
Figure 2 Configuration > Mgmt. & Analytics > Nebula > Monitor Mode



1.4 Nebula Mode

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. Choose Nebula Mode to manage your Zyxel Device remotely using Nebula Control Center (NCC). Select this mode if you want to configure and monitor one or more Zyxel Devices through the cloud.

Figure 3 Nebula Mode



Follow the wizard to configure the Zyxel Device network settings to connect to NCC. Note that once you complete th WAN configuration step, you cannot change to On Premises Mode unless you reset the Zyxel Device.

Nebula Control Center (NCC) is an Internet portal that allows you to configure and monitor groups of Zyxel Devices in organizations. You cannot manage a Zyxel Device directly through the Web Configurator or Command Line Interface (CLI) when NCC is managing the Zyxel Device. See Table 1.1.1 on page 24 to see which Zyxel Devices can be managed by NCC.

Follow this procedure to have NCC manage your Zyxel Device.

1.4.1 NCC Portal

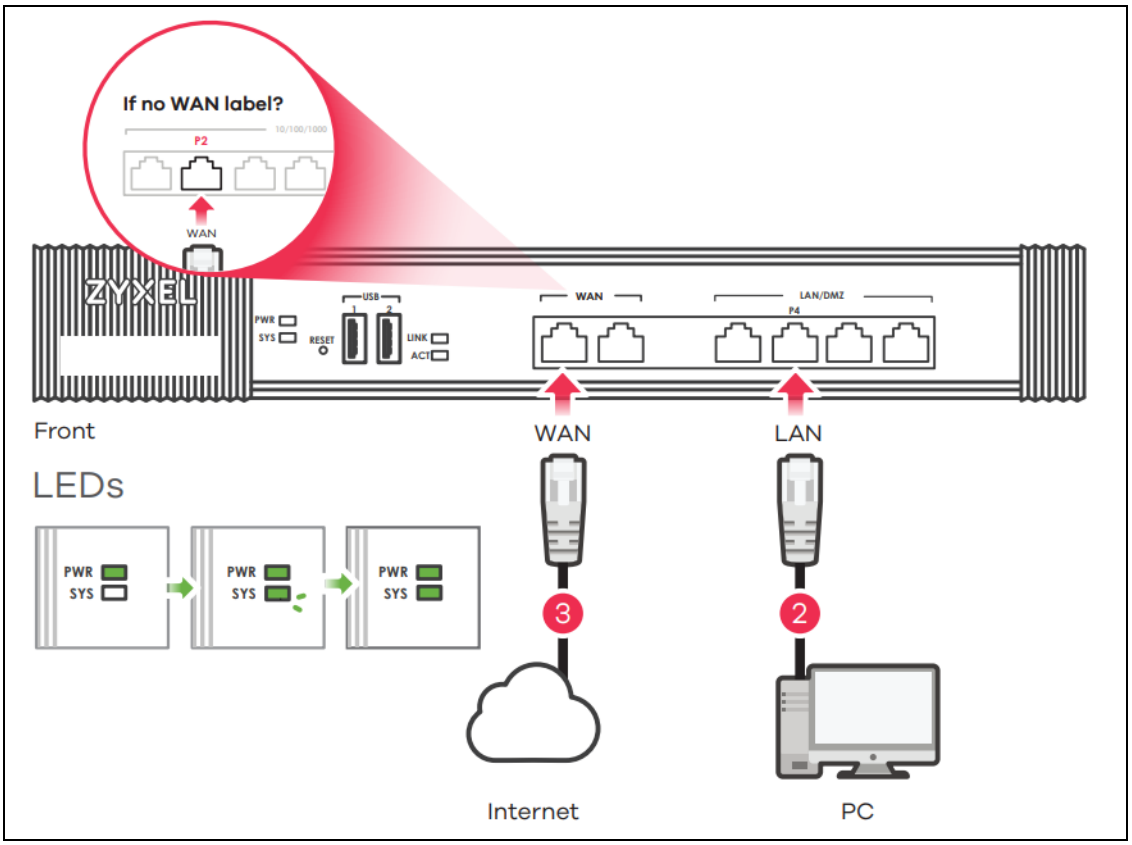
You should already have created an account at myZyxel.com. Follow these steps at the NCC portal.

1. Log into NCC (*https://nebula.zyxel.com*) with your Zyxel account. If you do not have a Zyxel account, you will be redirected to another screen to create one.
2. After you log in, click Go under Nebula Control Center and then Let's Start to run the NCC setup wizard. Create an organization and a site or select an existing site.
3. Add the Zyxel Device to this site by entering its MAC address and serial number. You'll find the MAC address and serial number of the Zyxel Device on its label or scan the QR code using the Nebula Mobile app.
4. Configure the WAN interface that the Zyxel Device will use to connect to NCC through the Internet.
5. If you're given a choice, select Native Mode. If you cannot select Native Mode, configure the email address of the person who will configure the Zyxel Device for management by NCC. An email will be sent to this person containing an activation link that allows management of the Zyxel Device by NCC.

1.4.2 Your Zyxel Device

The person who will configure the Zyxel Device for management by NCC should follow this procedure.

1. Use an Ethernet cable to connect the WAN port of the Zyxel Device (P1 or P2) to the Ethernet port of a device that will provide Internet access.



2 Use another Ethernet cable to connect the LAN port of the Zyxel Device (P3 or P4) to your computer. Make sure your computer can receive an IP address automatically. This is the default for all computers, so the computer should be fine unless you changed it.

3 Connect the power port to an appropriate power source and turn on the Zyxel Device. Wait for the SYS LED to turn solid green.

4 Back up your current configuration before passing management to NCC. Log into the web configurator, and go to Maintenance > File Manager > Configuration File. Select startup-config.conf, then click Download.

5 If you cannot select Native Mode, reset the Zyxel Device to the factory defaults. Push the Reset button until the port connection LEDs turn off (after about 5 seconds). Your Zyxel Device will reboot to the factory defaults and all previous configurations will be erased.

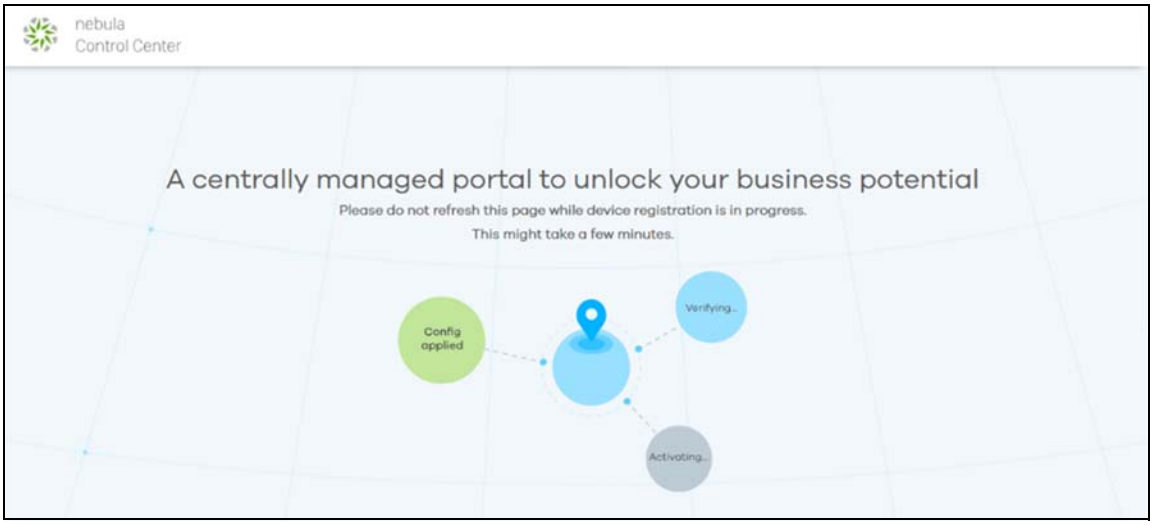
   Skip this step if you did not configure your Zyxel Device before (including just logging in and changing the default password.). You must reset the Zyxel Device if it does not have the factory default configuration.

1.4.3 Activation Email

If you cannot select Native Mode in the NCC setup wizard, do the following after the Zyxel Device is on:

1 Check your mailbox for an email from NCC. You may need to check your spam folder

2 Follow the instructions in the email if you did not complete the instructions above. Look for an activation link in the email. Click the activation link or copy the link to your web browser. You will see a screen saying NCC registration is in process. Please wait.



3 When you see a screen saying NCC registration has succeeded, management of your Zyxel Device has passed to Nebula Control Center. The NCC administrator can now configure and manage your device.

Note: ZTP is supported in firmware version 5.37 or earlier.

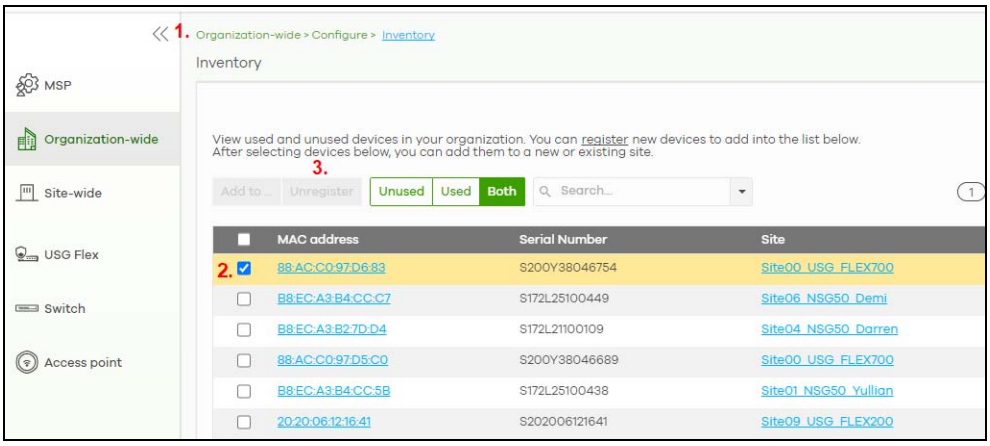
1.5 Changing the Mode

Follow the steps below to change your Zyxel Device from On Premises Mode to Nebula Mode or from Nebula Mode to On Premises Mode.

1.5.1 From Nebula Mode to On Premises Mode

Follow this procedure if you want to manage the Zyxel Device directly using the web configurator or CLI.

1 Log into NCC (*https://nebula.zyxel.com*) with your Zyxel account. Go to Organization-wide > License & Inventory > Devices.



2 Select the Zyxel Device you want to remove from NCC. You must know the MAC address and serial number.

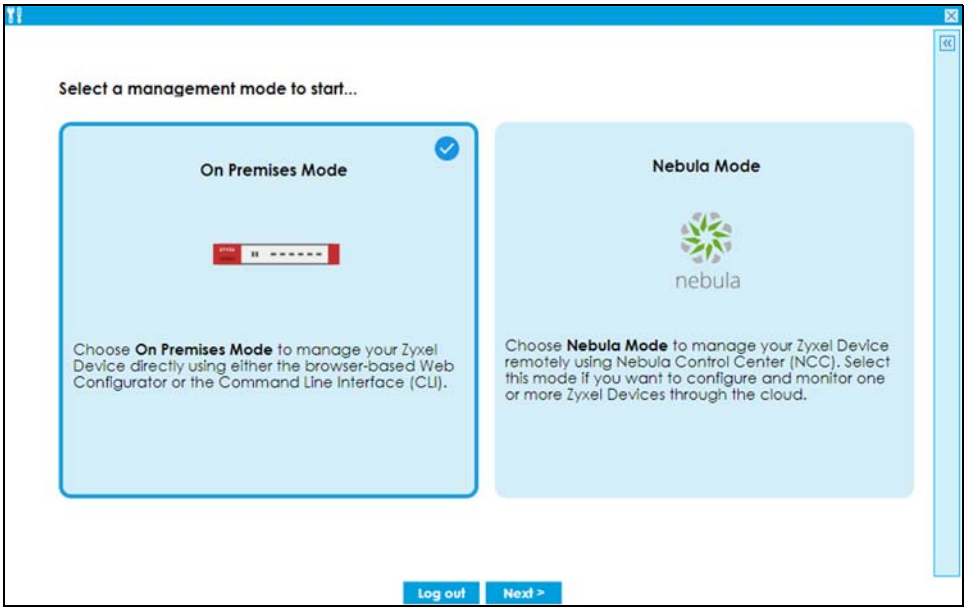
3 Click Remove from organization.

4 If the Zyxel Device is connected to NCC, the Zyxel Device will automatically reset after you remove the Zyxel Device from the organization and site.

If the Zyxel Device is not connected to NCC, press the reset button. The Zyxel Device will reboot to the factory defaults.

All NCC configurations for the Zyxel Device will be erased.

5 Log into the Zyxel Device. Run the wizard and choose On Premises Mode.



6 To restore your previous configuration, log into the web configurator, and go to Maintenance > File Manager > Configuration File.

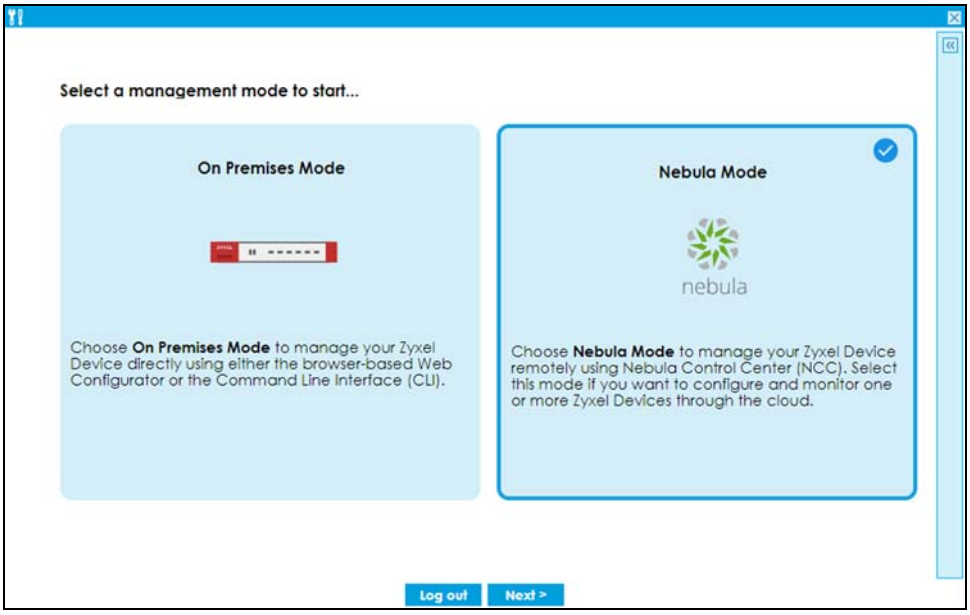
7 Under Upload Configuration File, click Browse, select the startup-config.conf on your computer that you backed up previously and click Upload. The Zyxel Device will then return to the previous settings.

1.5.2 From On Premises Mode to Nebula Mode

1 Back up your current configuration in Maintenance > File Manager > Configuration File.

2 Reset the Zyxel Device to the factory default by pushing the Reset button until the port connection LEDs turn off (after about 5 seconds). Your Zyxel Device will reboot to the factory defaults.

3 Log into the Zyxel Device. Run the wizard and choose Nebula Mode.



4 If you have a choice of Native Mode or ZTP, select Native Mode.

1.5.3 From Nebula Mode to Cloud Monitoring Mode

See Cloud Monitoring Mode to Nebula Mode if you want to monitor the Zyxel Device using Nebula Control Center (NCC) while configuring settings on the web configurator at the same time.

1.6 Registration at Zyxel

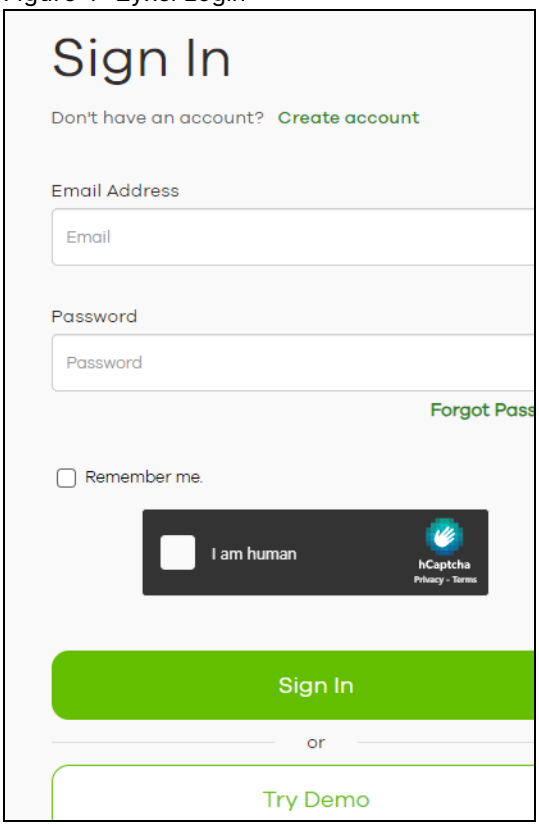
portal.myZyxel.com is Zyxel's online services center where you can register your Zyxel Device and manage subscription services available for your Zyxel Device (see Configuration > Licensing > Registration > Service for services available for your Zyxel Device).

- 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 Zyxel (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 Zyxel (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 Zyxel account at *http://portal.myZyxel.com* before you can register your device and activate the services at Zyxel.

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

Figure 4 Zyxel Login



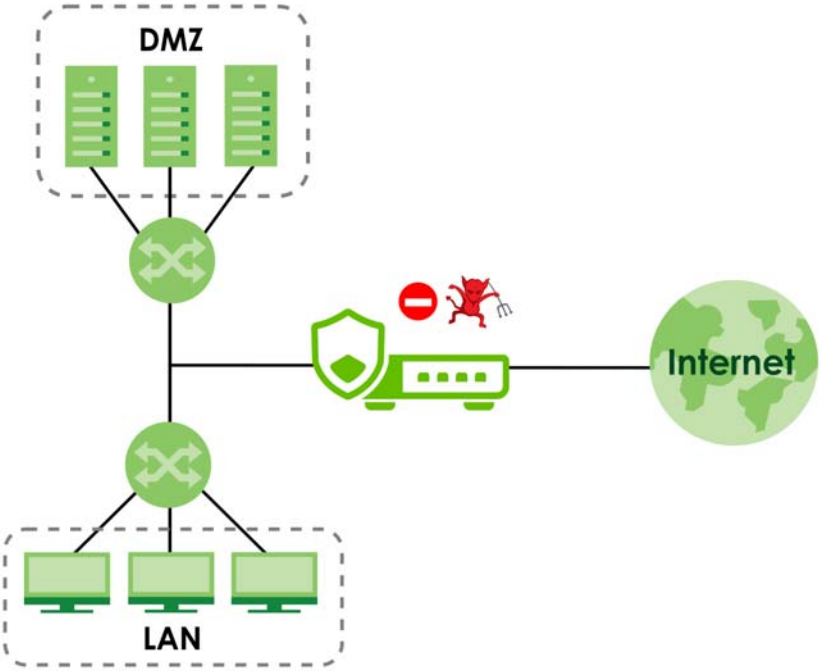
1.6.1 Applications

These are some Zyxel Device application scenarios.

Security Router

Security includes a Stateful Packet Inspection (SPI) firewall.

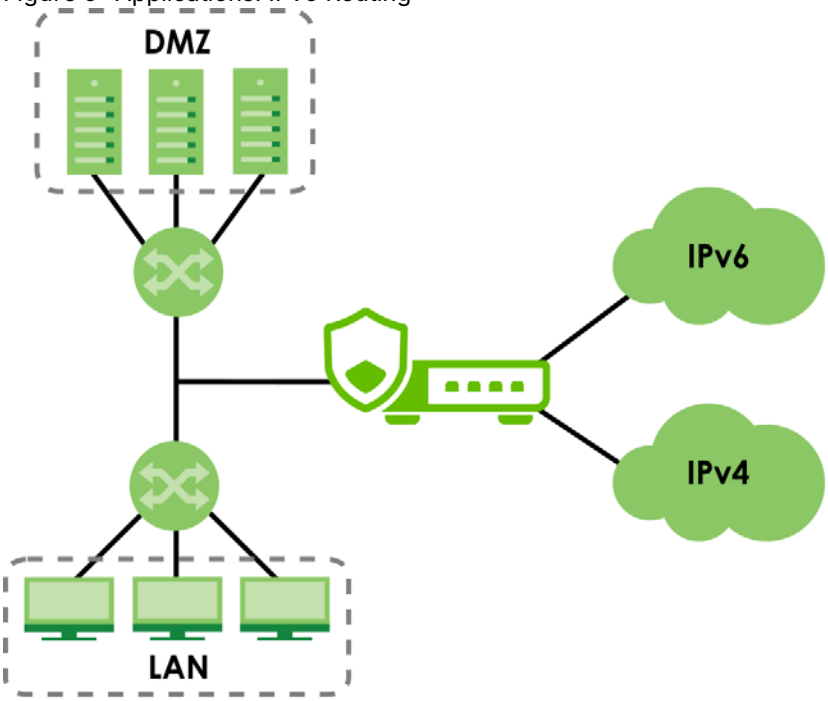
Figure 5 Applications: Security Router Applications: Security Router



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.

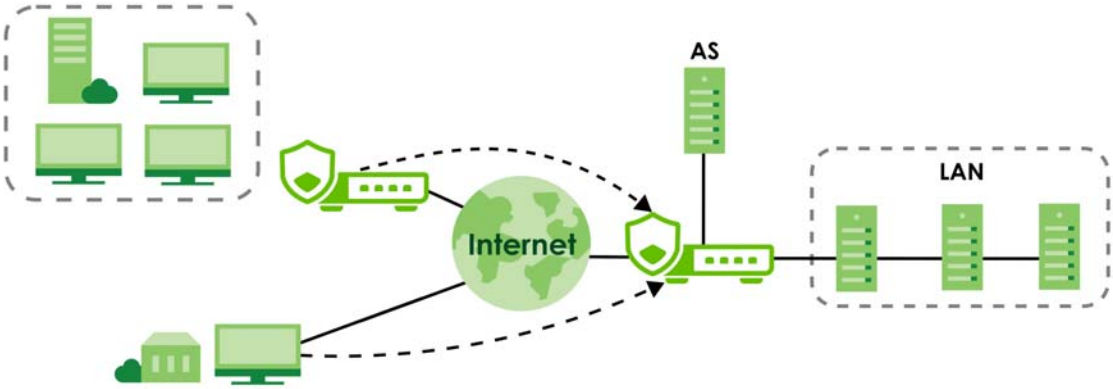
Figure 6 Applications: IPv6 Routing



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 7 Applications: VPN Connectivity



SSL VPN Network Access

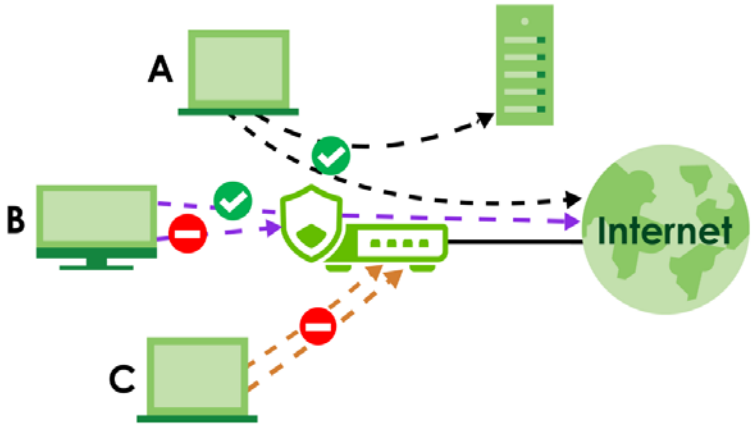
SSL VPN lets remote users use their web browsers for a very easy-to-use VPN solution. A user just browses to the Zyxel Device's web address and enters his user name and password to securely connect to the Zyxel Device's network. Here full tunnel mode creates a virtual connection for a remote user and 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 8 SSL VPN With Full Tunnel Mode

User-Authentication 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.

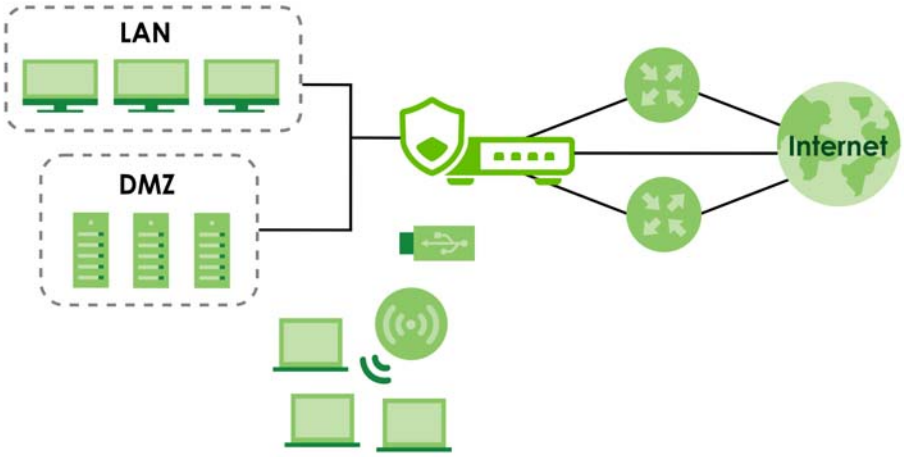
Figure 9 Applications: User-Authentication Access Control



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 10 Applications: Multiple WAN Interfaces



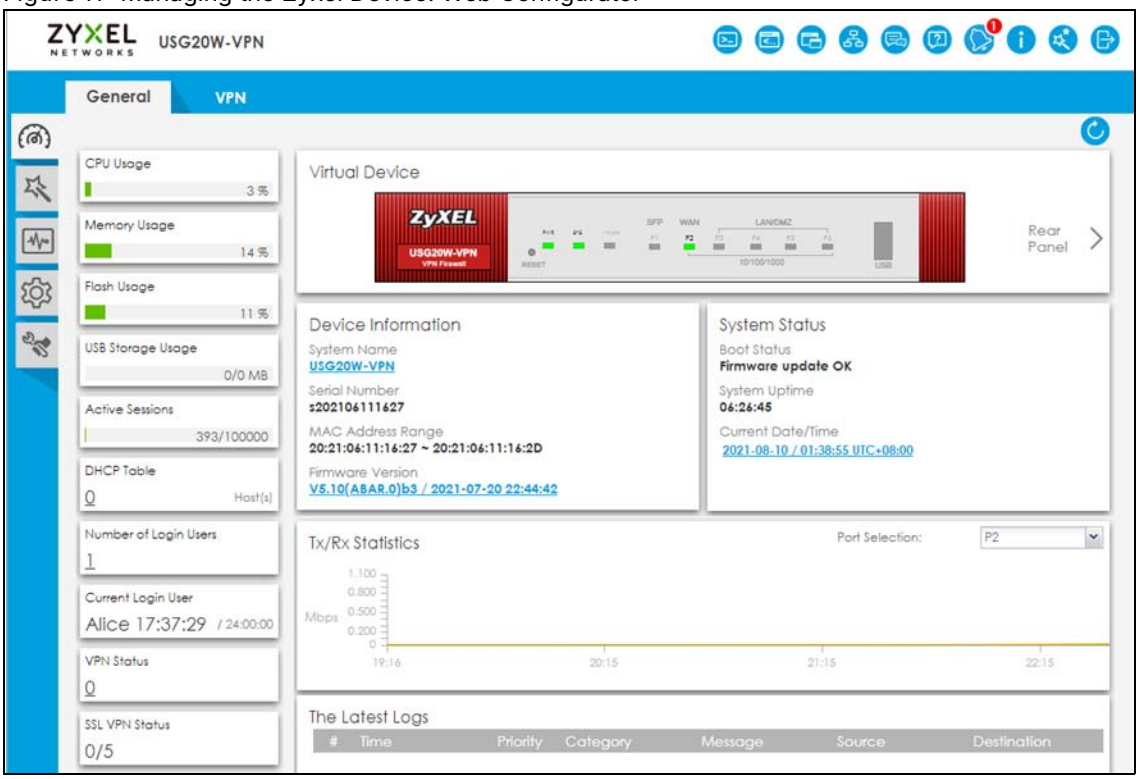
1.7 Management Overview

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 11 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 through the physical or Web Configurator console port. See the Command Reference Guide for CLI details. The default settings for the console port are:

Table 3 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 or restore.

SNMP

The device can be monitored and/or managed by an SNMP manager. See Section 32.11 on page 822.

CloudCNM

Use the CloudCNM screen (see Section 32.16 on page 834) 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

1.8 Remote Access to the Zyxel Device Networks

Your Zyxel Device keeps your networks safe while allowing external access by applying the security measures below:

- Two-Factor Authentication: Use two-factor authentication to have double-layer security to access the Zyxel Device. The first layer is the VPN client/Zyxel Device's login user name / password. The second layer is an authorized SMS (through mobile phone number) or email address. See Section 30.8.4 on page 738 for more information on two-factor authentication.
- Device Insight: The Zyxel Device can identify and display the basic information and status of clients that are connected to the Zyxel Device networks in Monitor > Network Status > Device Insight. See Section 8.7 on page 228 for more information on viewing the device insight.

  Create device insight profiles in Configuration > Object > Device Insight to block specified clients from accessing the Internet or the Zyxel Device. See Section 30.1 on page 669 for more information on creating and using the device insight profiles.
- IPSec VPN: You can create highly secure connections with IKEv2 or EAP authentication to access networks behind the Zyxel Device. For example, home workers can securely access company resources if they have proper authentication. See Chapter 21 on page 473 for more information on IPSec VPN.
- Upload Bandwidth Limit: Zyxel subscription-based SecuExtender IPSec VPN clients with Windows version 5.6.80.007 or later or macOS version 1.2.0.7 or later support upload bandwidth limit. Use this to set the maximum bandwidth for uploading traffic from IPSec VPN clients over IPSec VPN tunnels. See Section 21.5 on page 497 for more information on upload bandwidth limit.

CHAPTER 2
Web Configurator

2.1 Overview

The Web Configurator is an HTML-based management interface that allows easy system setup and management through Internet browser. Use a browser that supports HTML5, such as Microsoft Edge, Mozilla Firefox, or Google Chrome.

In order to use the Web Configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

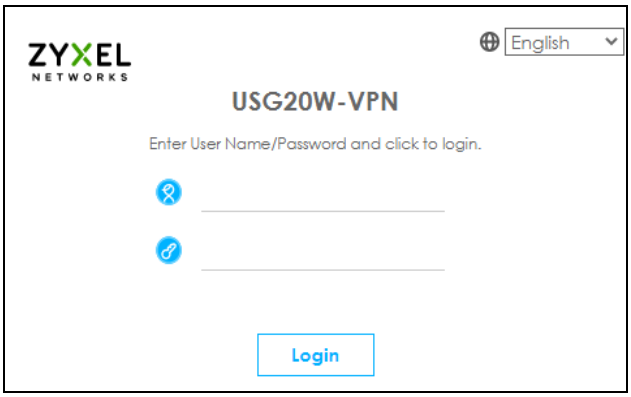
The recommended minimum screen resolution is 1024 x 768 pixels.

Note: Screenshots and graphics in this book may differ slightly from your product due to differences in product features or Web Configurator brand style.

2.2 Web Configurator Access

This section shows how to access the Web Configurator.

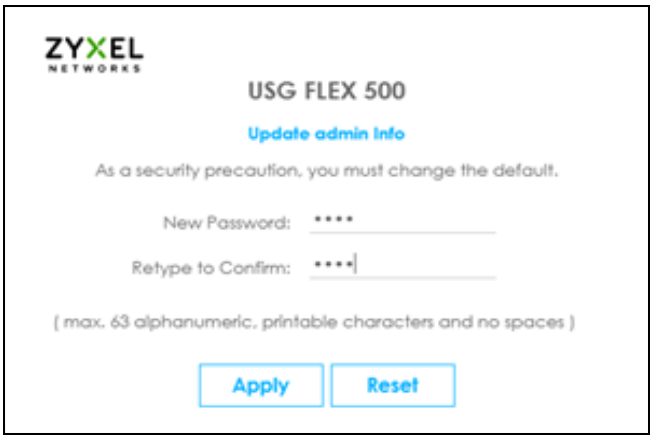
1. Make sure your Zyxel Device hardware is properly connected. See the Quick Start Guide.
2. In your browser go to https://192.168.1.1 or https://myrouter.local. By default, the Zyxel Device automatically routes this request to its HTTPS server, and it is recommended to keep this setting. The Login screen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



If you want to change the display language for the Zyxel Device's Web Configurator screens, select from the drop-down list box. You can also change the display language in Configuration > System > Language.

3 Enter the user name (default: "admin") and password (default: "1234"). Click Login.

4 If this is your first login, change the default admin password on the Update Admin Info screen. Enter a new password, then click Apply. Log in again using the user name (default: admin) and your new password. Click Login. Refer to Chapter 3 on page 58 to begin the initial setup.

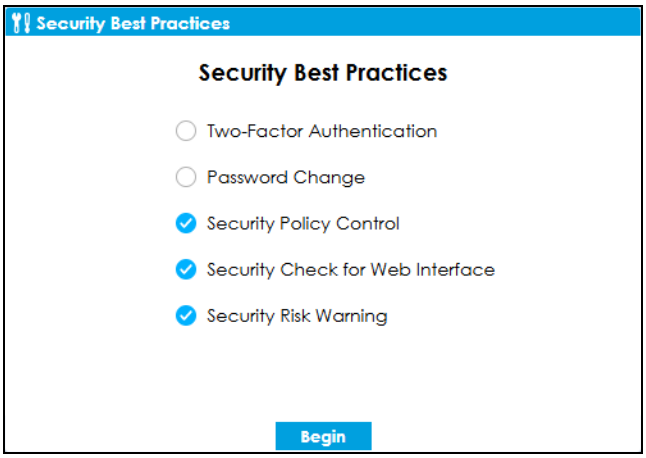


Note: In Configuration > Object > User/Group > Setting, you can enable Password Complexity to require a new password to consist of at least 8 characters and at most 64, where at least 1 character must be a number, at least 1 a lower case letter, at least 1 an upper case letter and at least 1 a special 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).

2.3 Security Best Practices

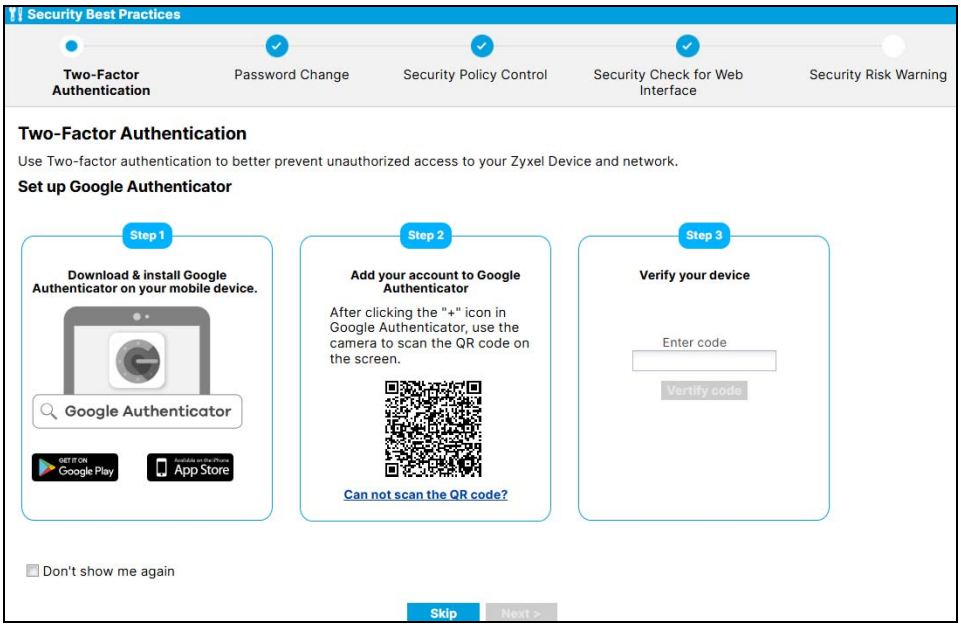
For a secure network, we recommend configuring the Zyxel Device with two-factor authentication, regularly changing your password, and completing the security settings.

The Security Best Practices screen appears after each login to remind you of the recommended security settings. Click Begin to start the setup. A checkmark indicates a completed setup.



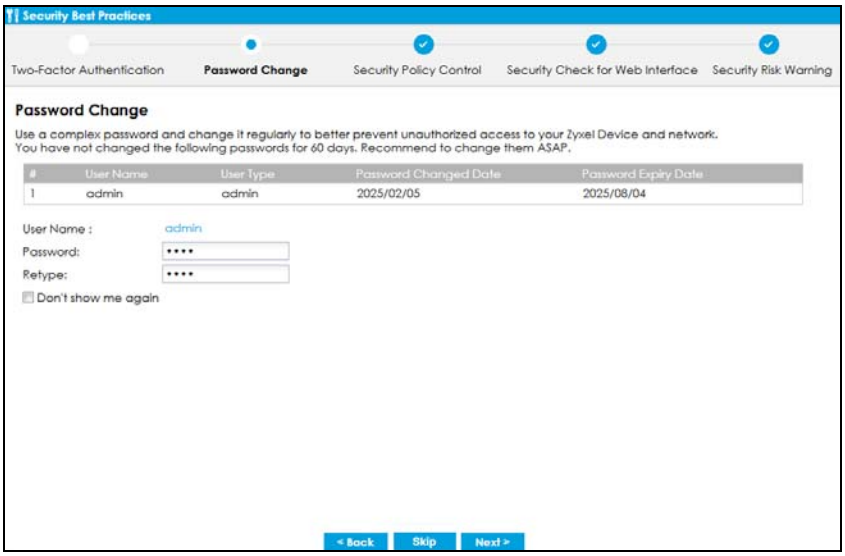
2.3.1 Two-Factor Authentication

Enhance security with two-factor authentication by using Google Authenticator to access the Zyxel Device. Follow the instructions on the screen to set up the two-factor authentication. See Google Authentication on page 740 for more information.



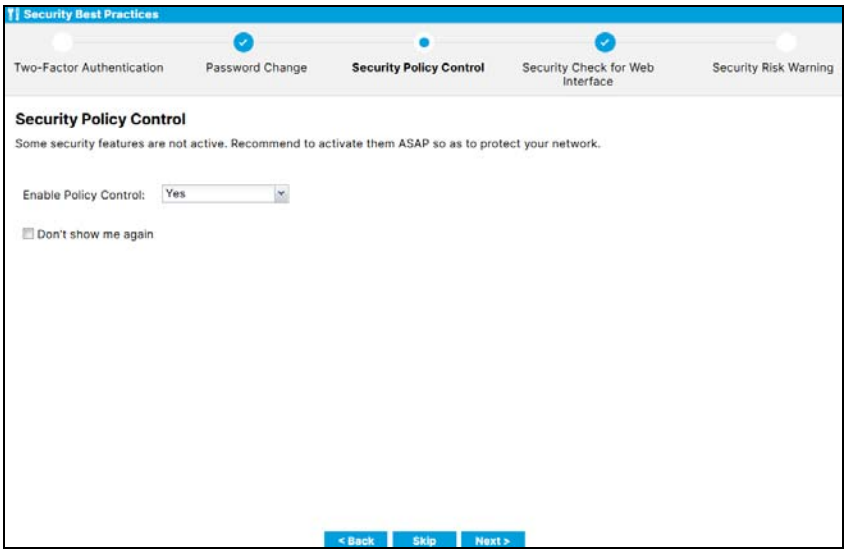
2.3.2 Password Change

Regularly changing passwords can enhance security by reducing the risk of unauthorized access. Depending on the password change interval under Login Security in Configuration > Object > User/Group > Setting, the password must be changed every set number of days.



2.3.3 Security Policy Control

Use this screen to activate the security configuration. Select Yes from the drop-down list, then click Next to activate the security policy configured in Configuration > Security Policy > Policy Control > Policy.



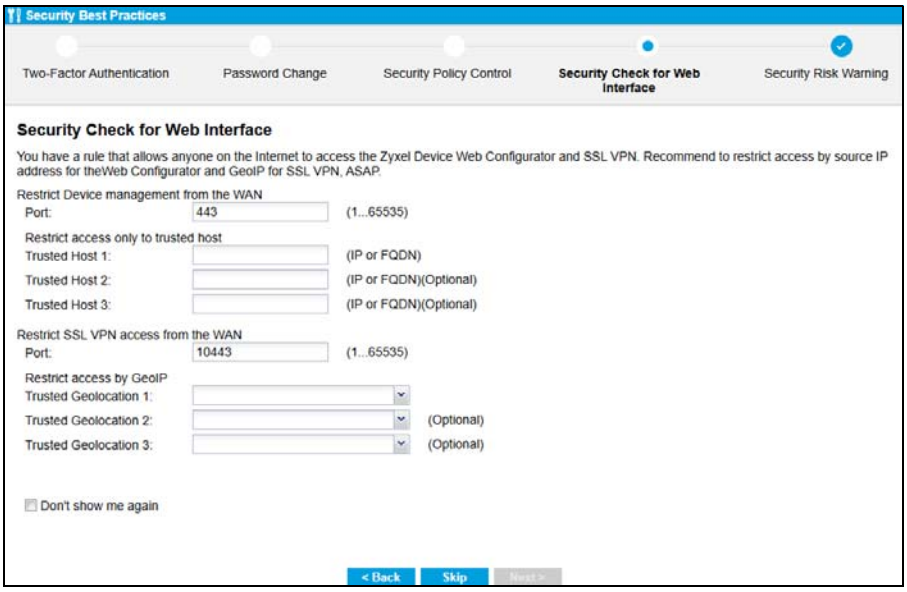
2.3.4 Security Check for Web Interface

When the Zyxel Device detects a rule that allows unrestricted Internet access to the Web Configurator and SSL VPN, restrict the access by using the source IP address for the Web Configurator and the GeoIP for SSL VPN.

Use this screen to configure settings to secure your Zyxel Device. You can configure:

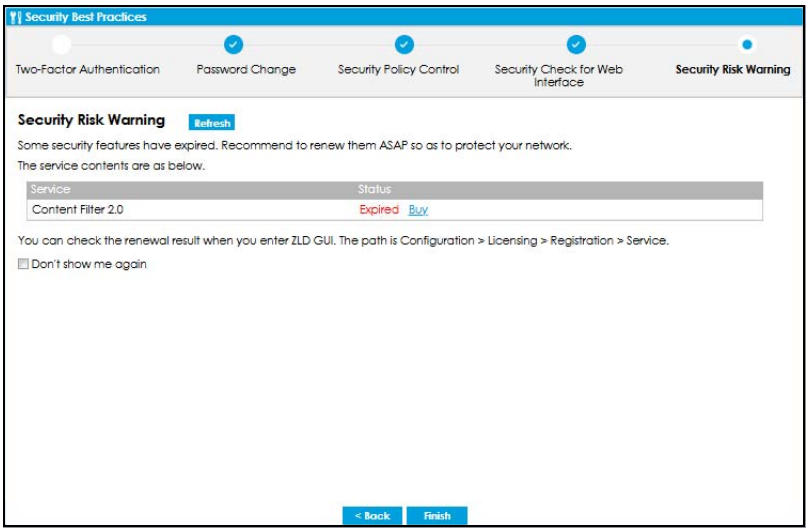
- Secure SSL access from the Internet to the Zyxel Device.
- Secure SSL access from the Internet to the network behind the Zyxel Device.

See Chapter 26 on page 576 for more information.



2.3.5 Security Risk Warning

Keep the licenses up to date to receive critical security enhancements, avoid malware risks, and ensure optimal performance. Click Renew to extend the license. See Section 9.1.3 on page 267 for more information.



Other Security Measures

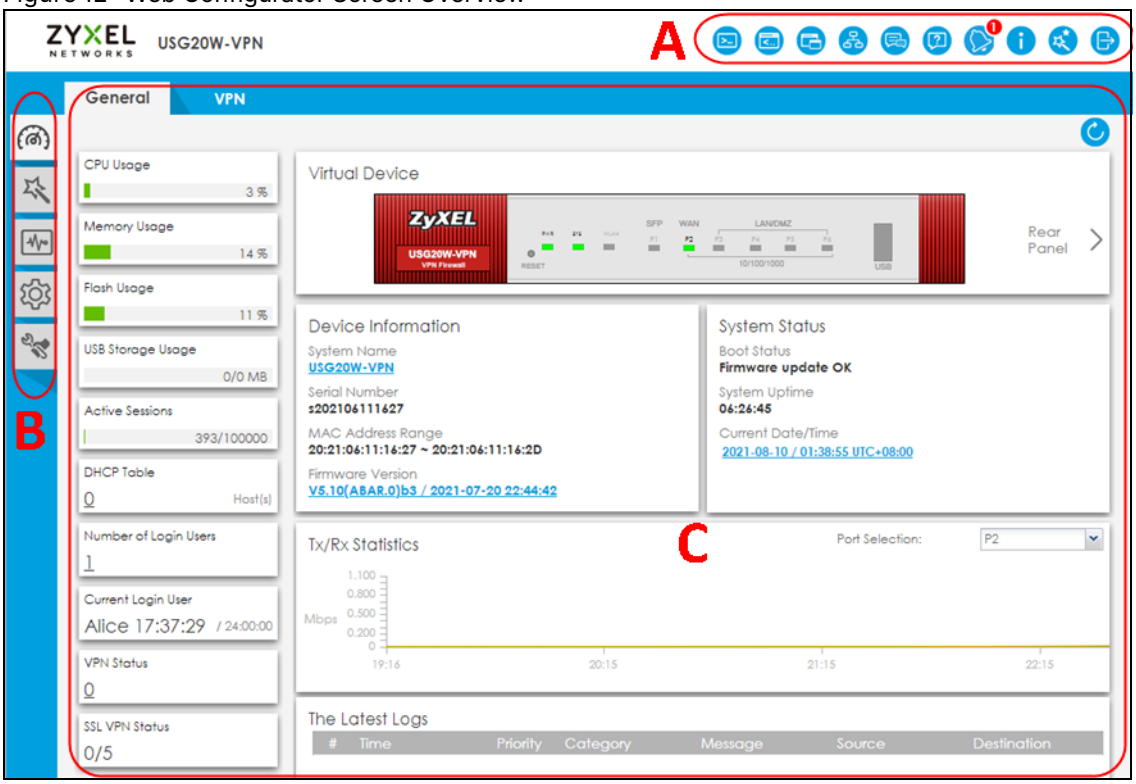
New firmware contains patches to enhance security. Make sure to check for new firmware regularly and update firmware in Maintenance > Firmware Management.

2.4 Web Configurator Screens Overview

The Web Configurator screen is divided into these parts:

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

Figure 12 Web Configurator Screen Overview



Title Bar

Figure 13 Title Bar

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

Table 4 Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
SecuReporter	This icon shows when SecuReporter is enabled and the Zyxel Device is added to an organization. Click this to open the SecuReporter portal page.
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.

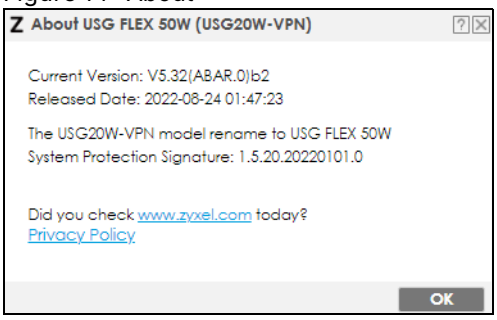
Table 4 Title Bar: Web Configurator Icons (continued)

LABEL	DESCRIPTION
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.
Community	Go to *https://community.zyxel.com* for product discussions.
Help	Click this to open the help page for the current screen.
Notification	Only Admin or Limited Admin can see notifications. Notifications display what's new in the Zyxel Device firmware (ZLD), information on security services about to expire. Slide the switch to Off if you don't want notifications. Click an item to see more details on it. Click the Refresh icon or refresh the browser page to update notifications. The latest notification appears at the top. An item is removed once it has been read. Up to five notifications can be shown here. If there are more than five notifications, then click All Notifications to see them.
About	Click this to display basic information about the Zyxel Device.
Easy Mode	Click this to go to the Initial Setup Wizard in Easy Mode, and enter Easy Mode every time you log in.
Logout	Click this to log out of the Web Configurator.

About

Click About to display basic information about the Zyxel Device.

Figure 14 About



This table describes the fields in this screen.

Table 5 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.

Table 5 About (continued)

LABEL	DESCRIPTION
System Protection Signature	This shows the system protection signature version of the Zyxel Device. These signatures do not require a license. The Zyxel Device will synch with the Cloud Helper Server every day to update these signatures automatically. System protection signatures protect your Zyxel Device and local networks from web attacks, such as command injection, cross-site scripting and path traversal. Command injection: This is an attack in which an attacker uses the Zyxel Device vulnerabilities to execute commands to control your Zyxel Device. Cross-site scripting: This is an attack in which an attacker implants malicious scripts in a website. When you visit this website, the malicious scripts are sent and executed on your web browser. Path traversal: This is an attack that allows an attacker to access files you store in the web root folder.
OK	Click this to close the screen.

Site Map

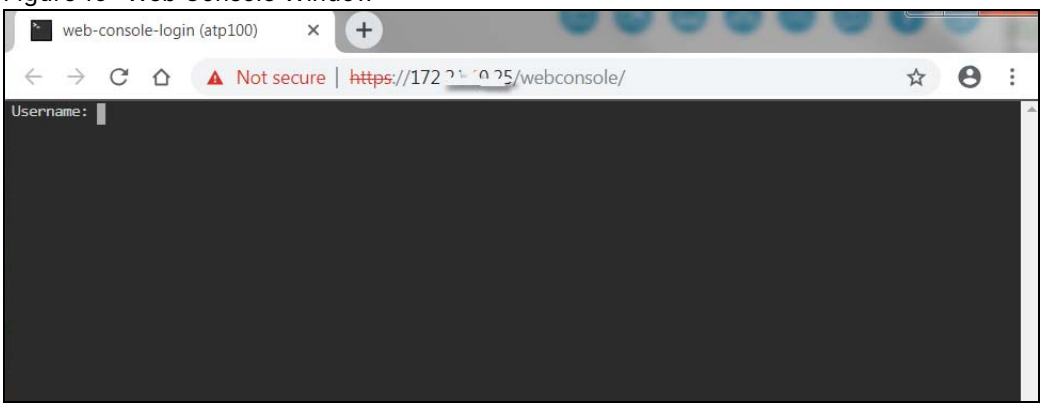
Click Site MAP to see an overview of links to the Web Configurator screens. Click a screen's link to go to that screen.

Figure 15 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.

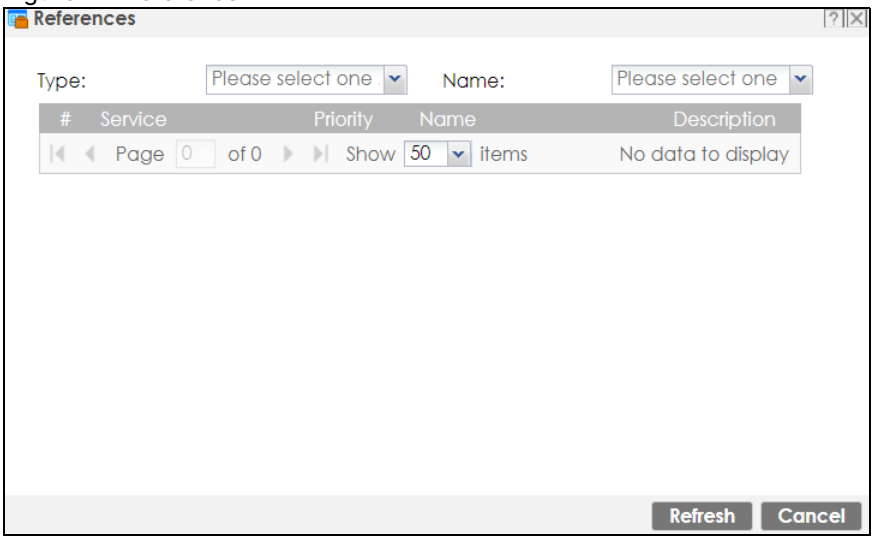
Figure 16 Web Console Window



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 17 Reference



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

Table 6 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.

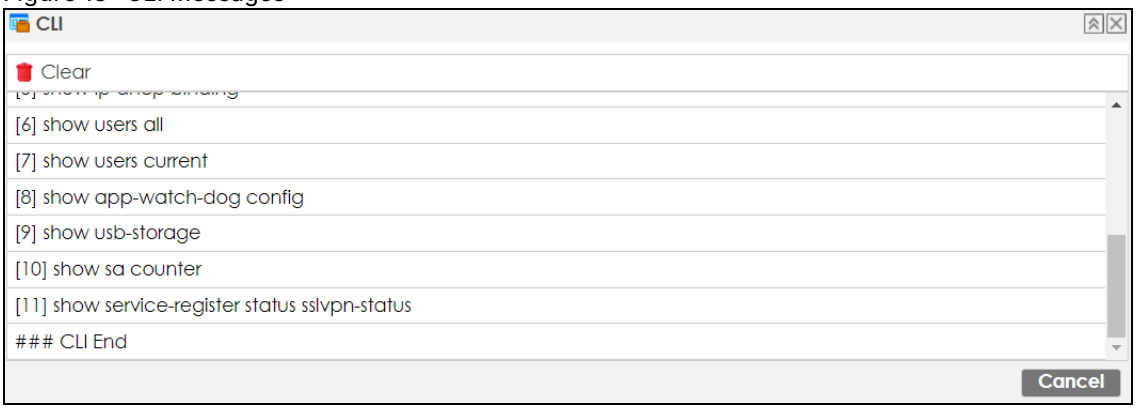
Table 6 Reference (continued)

LABEL	DESCRIPTION
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.

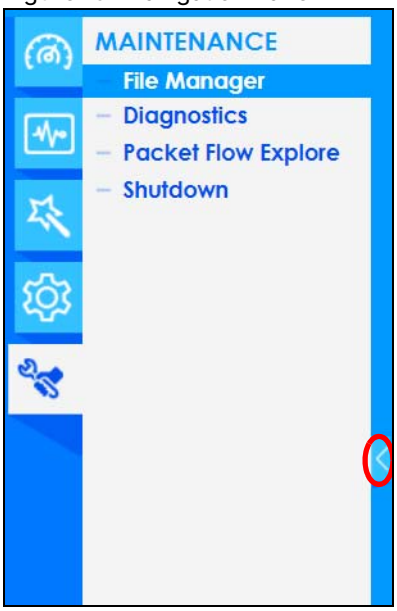
Figure 18 CLI Messages



2.5 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 19 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 7 Monitor Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
Traffic Statistics		
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.
Network Status		
DHCP Table	DHCP Table	Displays a list of interfaces and their DHCP-assigned IP addresses.
Device Insight	Device Insight	Displays a list of WiFi and wireless clients connected to the Zyxel Device networks.
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 through Smart Connect (Layer Link Discovery Protocol (LLDP)). Use the Zyxel One Network (ZON) utility to view and manage the Zyxel Device’s neighboring devices through 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	Radio List	Lists wireless details of APs managed by the Zyxel Device.
SSID Info	SSID Info	Display information about the AP’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.
VPN Monitor		

Table 7 Monitor Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
IPSec	IPSec	Displays and manages the active IPSec SAs.
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	Web Content Filter	Collect and display web content filter statistics.
	DNS Content Filter	Collect and display DNS content filter statistics.
Anti-Spam	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.
Log	View Log	Lists log entries.

Configuration Menu

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

Table 8 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.
Wireless		
Built-in AP	General	Allow WiFi clients to access your Zyxel Device wirelessly to connect to the network.
Network		
Interface	Port Port Role/Port Group/ Port Configuration	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.

Table 8 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
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 interfaces.
	Allow List	Enable and configure the allow list.
DNS Inbound LB	DNS Load Balancing	Configure DNS Load Balancing.
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.
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.
	Allow List	Create an allow list for certain IP or services to let them pass the ADP flood detection.
Session Control	Session Control	Limit the number of concurrent client NAT/security policy sessions.

Table 8 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
Security Service		
Content Filter	Web Content Filter: General	Create and manage the detailed filtering rules for content filtering profiles and then apply to a traffic flow using a security policy.
	Web Content Filter: Trusted Web Sites	Create a list of allowed web sites that bypass content filtering policies.
	Web Content Filter: Forbidden Web Sites	Create a list of web sites to block regardless of content filtering policies.
	DNS Content Filter: General	Create and manage the detailed filtering rules for DNS content filtering profiles and then apply to a traffic flow using a security policy.
	DNS Content Filter: Allow List	Create a list of allowed web sites that bypass DNS content filtering policies.
	DNS Content Filter: Block List	Create a list of web sites to block regardless of content filtering policies.
Anti-Spam	Profile	Turn anti-spam on or off and manage anti-spam policies. Create anti-spam template(s) of settings to apply to a traffic flow using a security policy.
	Mail Scan	Configure e-mail scanning details.
	Block/Allow List	Set up a block list to identify spam and an allow list to identify legitimate e-mail.
	DNSBL	Have the Zyxel Device check e-mail against DNS Block Lists.
Object		
Device Insight	Device Insight	Configure profiles to block specified clients from accessing the Internet or the Zyxel Device.
Zone	Zone	Configure zone templates 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.
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 8 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
Auth. Method	Authentication Method	Create and manage ways of authenticating users.
	Two-factor Authentication	Configure SMS or email authentication to access the Zyxel Device through a VPN tunnel.
Certificate	My Certificates	Create and manage the Zyxel Device's certificates.
	Trusted Certificates	Import and manage certificates from trusted sources.
ISP Account	ISP Account	Create and manage ISP account information for PPPoE/PPTP interfaces.
Mgmt. & Analytics	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 or external threats, and report on network usage.
	Nebula	Use this screen to let Nebula manage your Zyxel Device.
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.
	SMS	Enable the SMS service to send dynamic guest account information in text messages and authorization for VPN tunnel access to a secured network.
	Response Message	Create a web page when access to a website is restricted due to a security service.
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 through the Zyxel Discovery Protocol (ZDP).
Advanced	Fast Forwarding	Enable fast forwarding to maximizes the network performance of the Zyxel Device.
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 9 Maintenance Menu Screens Summary

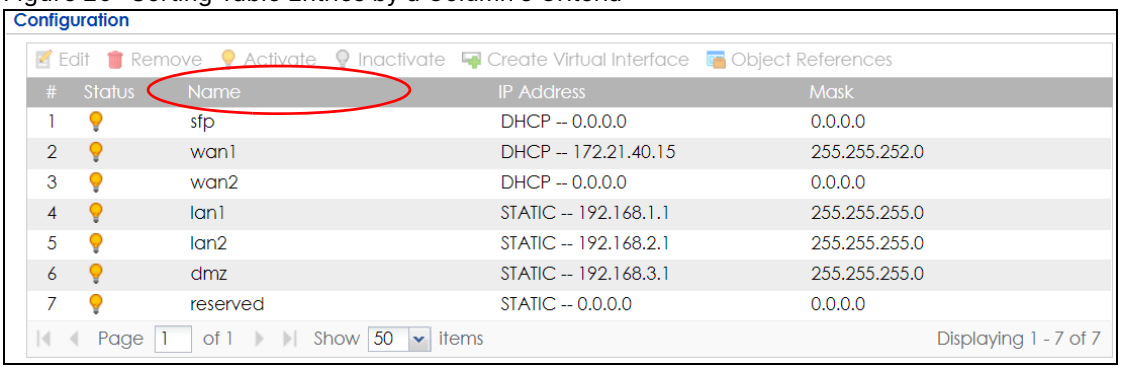
FOLDER OR LINK	TAB	FUNCTION
File Manager	Configuration File	Manage and upload configuration files for the Zyxel Device.
	Firmware Management	View the current firmware version and upload firmware. Reboot with your choice of firmware.
	Shell Script	Manage and run shell script files for the Zyxel Device.
Diagnostics	Diagnostics	Collect diagnostic information. This screen includes the sub-tabs below: • Controller • Filer
	Packet Capture	Capture packets for analysis. This screen includes the sub-tabs below: • Capture • Files
	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.
	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/ Reboot	Shutdown/ Reboot	Turn off or restart the Zyxel Device.

2.6 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.

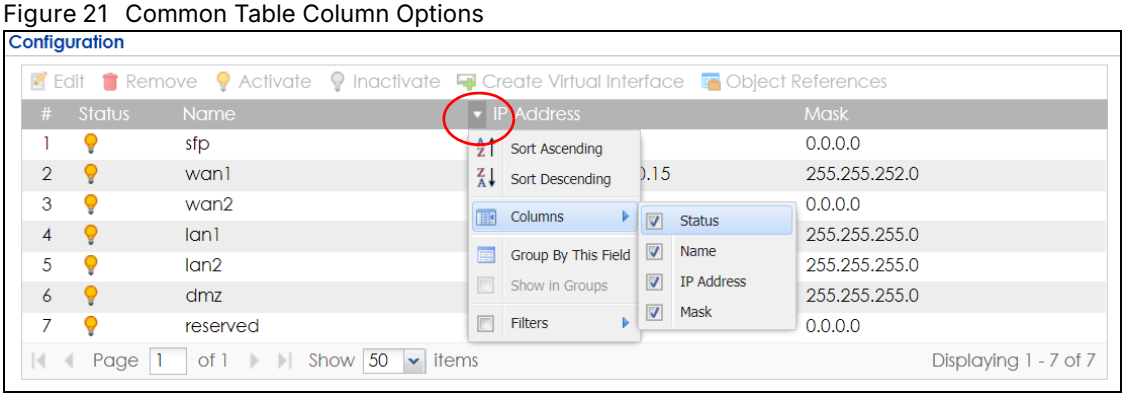
Figure 20 Sorting Table Entries by a Column's Criteria



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:

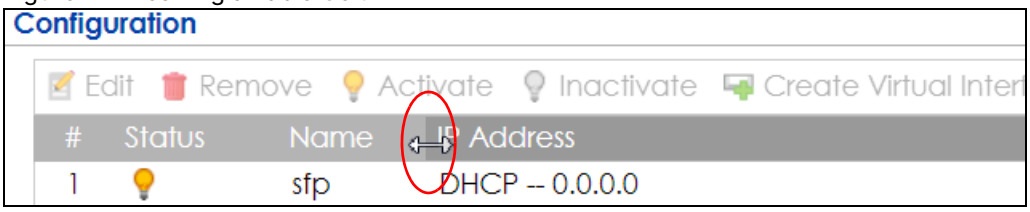
- Sort in ascending or descending (reverse) alphabetical order
- Select which columns to display
- Group entries by field
- Show entries in groups
- Filter by mathematical operators (<, >, or =) or searching for text

Figure 21 Common Table Column Options



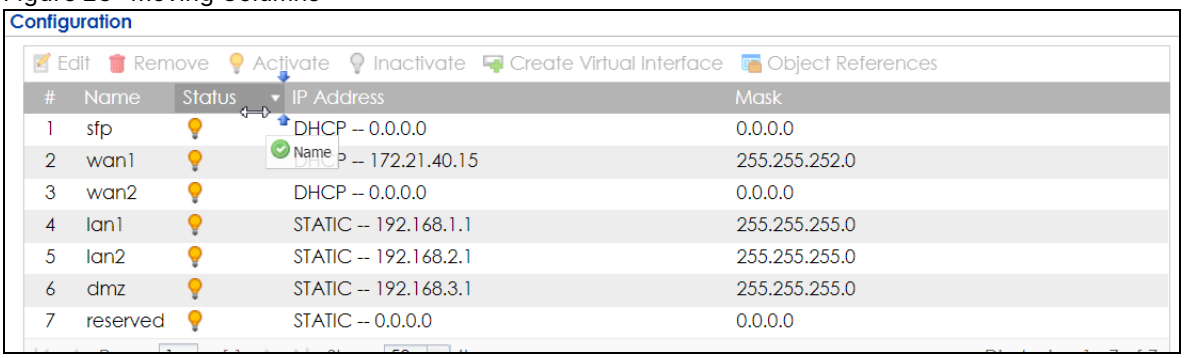
Select a column heading cell's right border and drag to re-size the column.

Figure 22 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 23 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 24 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 25 Common Table Icons

Here are descriptions for the most common table icons.

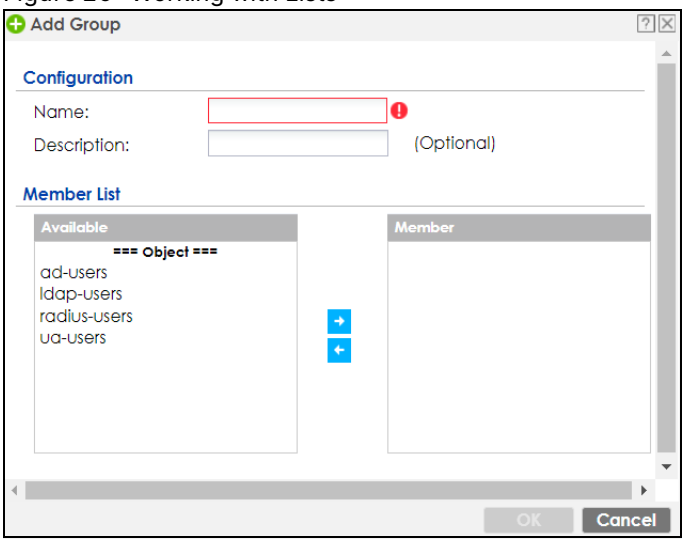
Table 10 Common Table Icons

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 enter a number for where you want to put that entry and press [ENTER] to move the entry to the number that you entered. For example, if you enter 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 26 Working with Lists



CHAPTER 3
Initial Setup Wizard

3.1 Initial Setup Wizard: Select Management Mode

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 Zyxel Account (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.

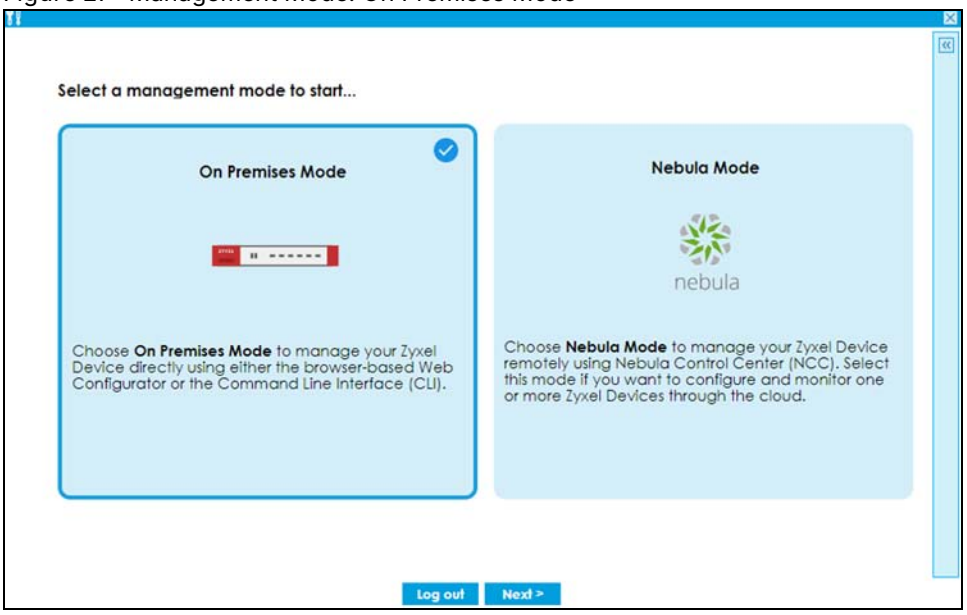
- Click the double arrow in the upper right corner to display or hide the help.
- Click Logout to exit the Initial Setup Wizard or click Next to continue the wizard. Click Finish at the end of the wizard to complete the wizard.

Select On Premises Mode to manage your Zyxel Device using the Web Configurator or the Command Line Interface (CLI). Use this mode to secure your networks with the Zyxel Device security services. Follow the On Premises mode wizard to set up your Zyxel Device, such as configuring the WAN settings, registering your Zyxel Device and allowing remote access to your Zyxel Device.

Select Nebula Mode to manage your Zyxel Device using Nebula Control Center (NCC). NCC is a cloud based network management system that allows you to remotely manage and monitor your Zyxel Device. Use this mode to manage your Zyxel Device with accounts at different privilege levels. You can also manage your Zyxel Device licenses and status through NCC. Follow the Nebula mode wizard to configure the WAN settings to pass the management of your Zyxel Device to NCC.

Note: You need to press the reset button to change the Zyxel Device mode once you finish the wizard. You will not see this screen if you reset the Zyxel Device through the web configurator or the CLI.

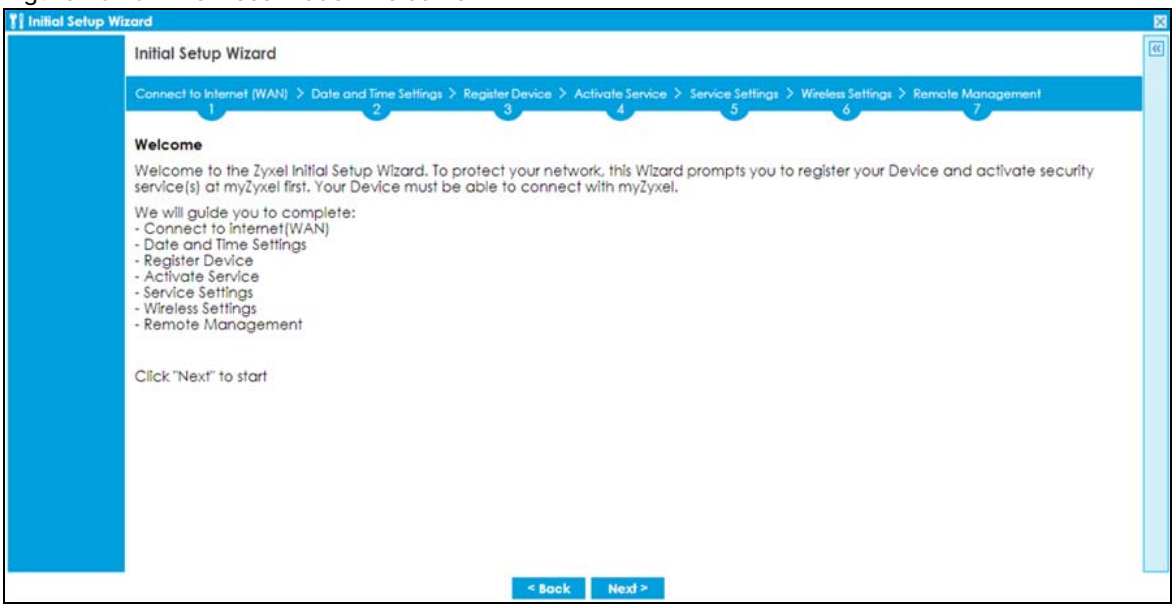
Figure 27 Management Mode: On Premises Mode



3.1.1 Welcome Screen

Select On Premises Mode in the previous screen to show the Welcome screen. Use this screen to see the settings you can configure using the On Premises mode initial setup wizard.

Figure 28 On Premises Mode- Welcome



3.1.2 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.

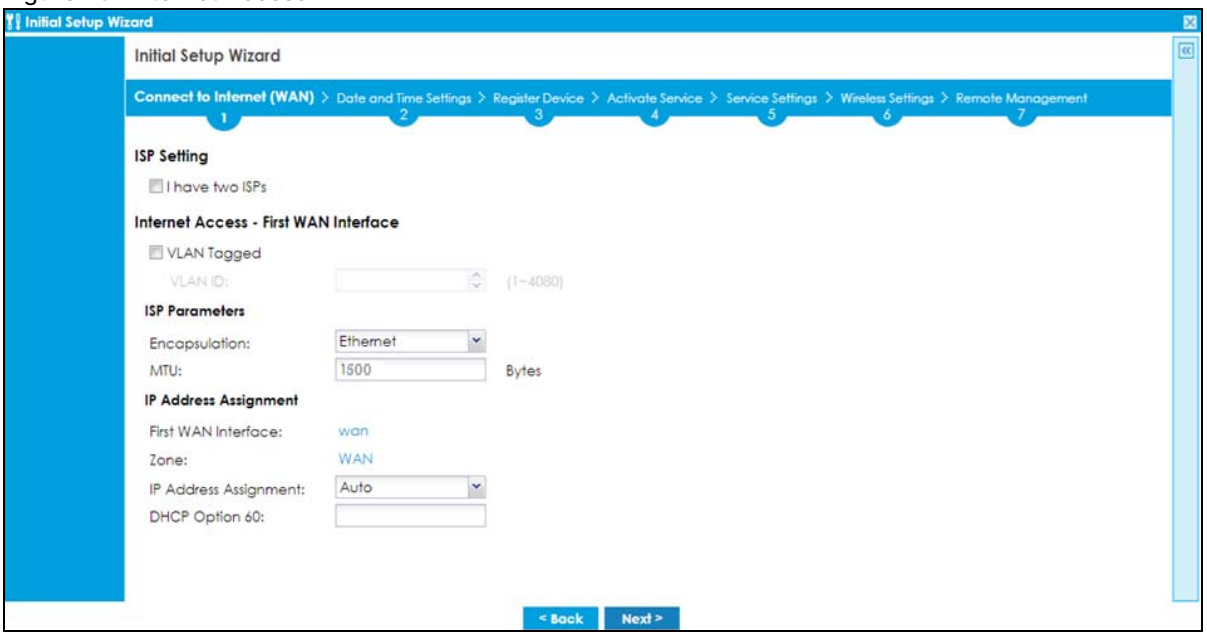
The screens vary depending on the encapsulation type. Refer to information provided by your ISP to know what to enter in each field.

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.
- VLAN Tagged: Select this to tag the traffic going out from the Zyxel Device. Enter a VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1-4080.
- 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.
- MTU: The Maximum Transmission Unit. Enter the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device divides it into smaller fragments. Allowed values are 576-1500. Usually, this value is 1500.
- 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.
- DHCP Option 60: This field will show if you choose Auto as the IP Address Assignment. DHCP Option 60 is used by the Zyxel Device for identification to the DHCP server using the VCI (Vendor Class Identifier) on the DHCP server. The Zyxel Device adds it in the initial DHCP discovery message that a DHCP client broadcasts in search of an IP address. The DHCP server can assign different IP addresses or options to clients with the specific VCI or reject the request from clients without the specific VCI.

  Enter a string using up to 63 of these characters [a-zA-Z0-9!\"#$%&\'()*+,-./:;<=>?@\[\\\]^_`{}] to identify this Zyxel Device to the DHCP server. For example, Zyxel-TW.

Figure 29 Internet Access



3.1.3 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.

- VLAN ID: This displays the VLAN ID tag for the traffic going out from the Zyxel Device, which you configured in the previous screen.
- Encapsulation: This displays the type of Internet connection you are configuring.
- MTU: This displays the maximum size of each data packet that can move through this interface.
- 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.
- DHCP Option 60: This field will show if you selected Auto as the IP Address Assignment in the previous screen. This displays the string you configured to identify DHCP server using VCI.

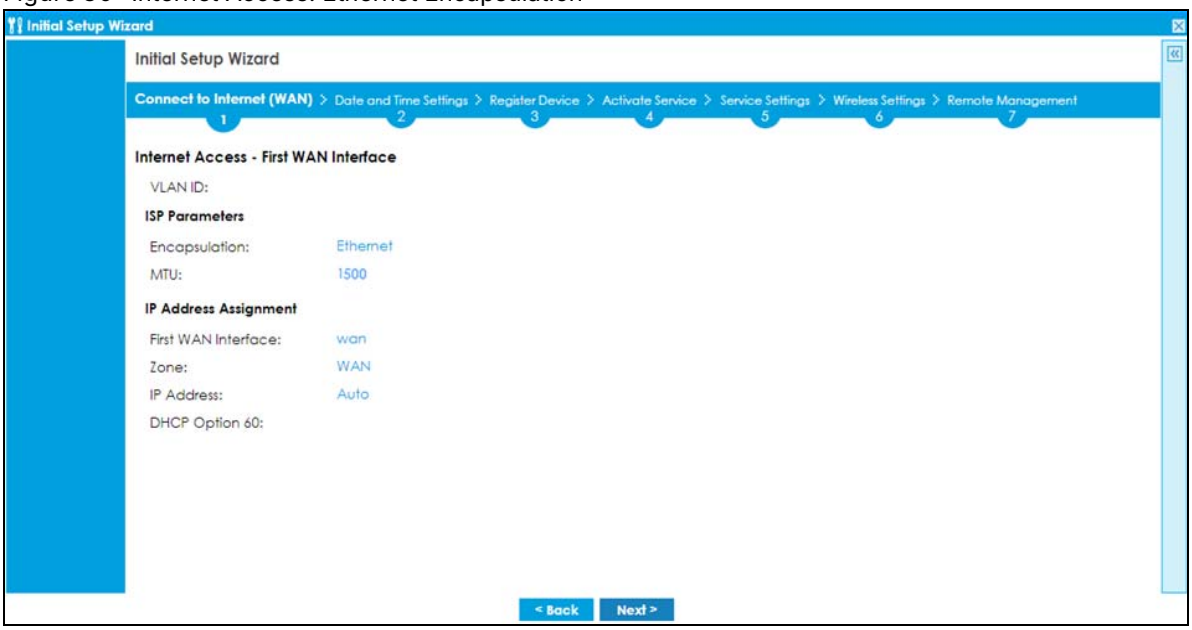
The following fields display if you selected static IP address assignment.

- 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.

3.1.3.1 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 30 Internet Access: Ethernet Encapsulation



3.1.4 Internet Access: PPPoE

3.1.4.1 Internet Access - First WAN Interface

- VLAN ID: This displays the VLAN ID tag for the traffic going out from the Zyxel Device, which you configured in the previous screen.

3.1.4.2 ISP Parameters

- VLAN ID: This displays the VLAN ID tag for the traffic going out from the Zyxel Device, which you configured in the previous screen.
- Encapsulation: This displays the type of Internet connection you are configuring.
- MTU: This displays the maximum size of each data packet that can move through this interface.
- Enter 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 -_@$./ characters, and it can be up to 64 characters long.
- Authentication Type - Select an authentication protocol for outgoing connection requests. Options are:
  - Chap/PAP - Your Zyxel Device accepts either CHAP or PAP when requested by the remote node.
  - Chap - Your Zyxel Device accepts CHAP only.
  - PAP - Your Zyxel Device accepts PAP only.
  - MSCHAP - Your Zyxel Device accepts MSCHAP only.
  - MSCHAP-V2 - Your Zyxel Device accepts MSCHAP-V2 only.
- Enter the User Name given to you by your ISP. You can use alphanumeric and -_@$./ characters, and it can be up to 31 characters long.
- Enter 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, enter the Idle Timeout in seconds that elapses before the router automatically disconnects from the PPPoE server.

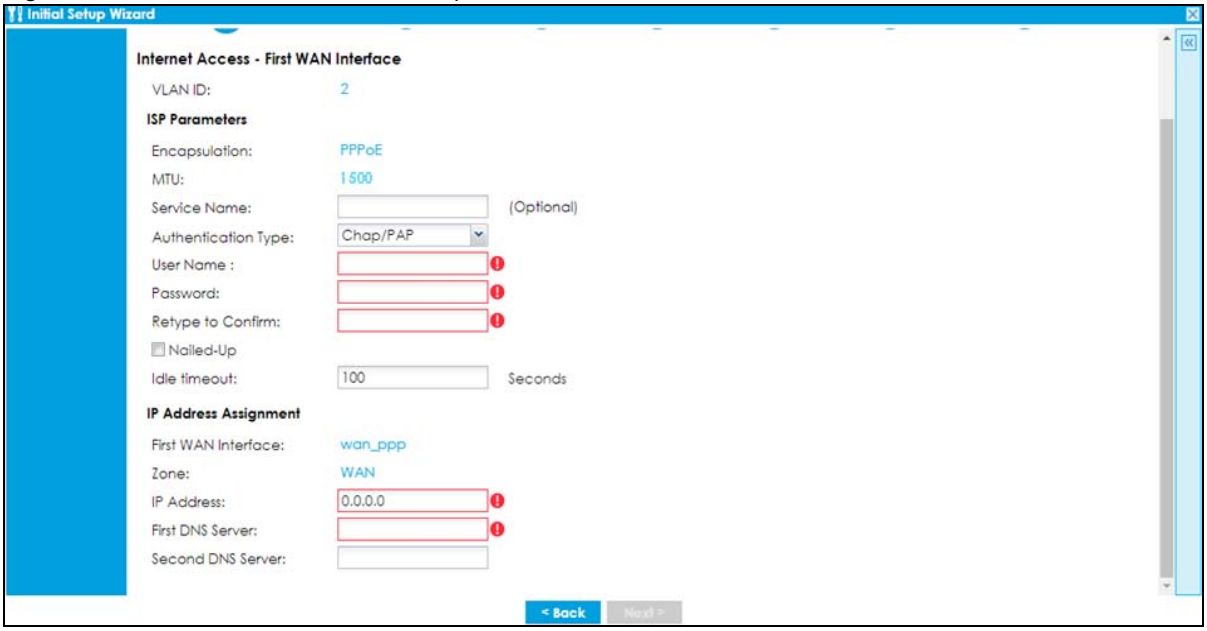
3.1.4.3 WAN IP Address Assignments

- 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. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.

3.1.4.4 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 31 Internet Access: PPPoE Encapsulation



3.1.5 Internet Access: PPTP

3.1.5.1 ISP Parameters

- MTU: This displays the maximum size of each data packet that can move through this interface.
- 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.
- Enter the User Name given to you by your ISP. You can use alphanumeric and -_@$./ characters, and it can be up to 31 characters long.
- Enter the Password associated with the user name. Use up to 64 ASCII characters except the [] and ?. This field can be blank. Re-enter your password in the next field to confirm it.
- Select Nailed-Up if you do not want the connection to time out. Otherwise, enter the Idle Timeout in seconds that elapses before the router automatically disconnects from the PPTP server.

3.1.5.2 PPTP Configuration

- Base Interface: This identifies the Ethernet interface you configure to connect with a modem or router.
- Enter a Base IP Address (static) assigned to you by your ISP.
- Enter 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: Enter the IP address of the PPTP server.
- Enter 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.

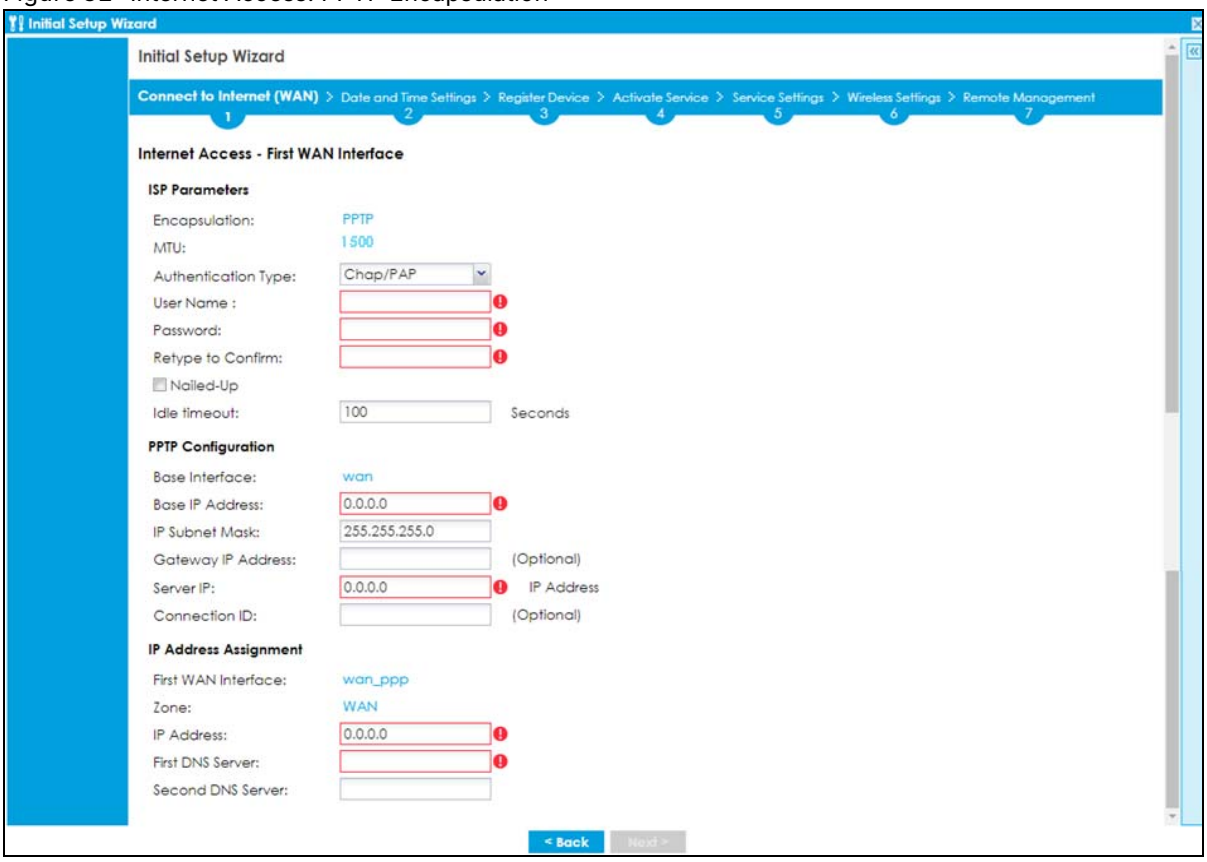
3.1.5.3 WAN IP Address Assignments

- 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.

3.1.5.4 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 32 Internet Access: PPTP Encapsulation



3.1.6 Internet Access: L2TP

3.1.6.1 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.
- Enter the User Name given to you by your ISP. You can use alphanumeric and -_@$./ characters, and it can be up to 31 characters long.
- Enter 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, enter the Idle Timeout in seconds that elapses before the router automatically disconnects from the PPPoE server.

3.1.6.2 L2TP Configuration

- Base Interface: This identifies the Ethernet interface you configure to connect with a modem or router.
- Enter 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: Enter the IP address of the L2TP server.

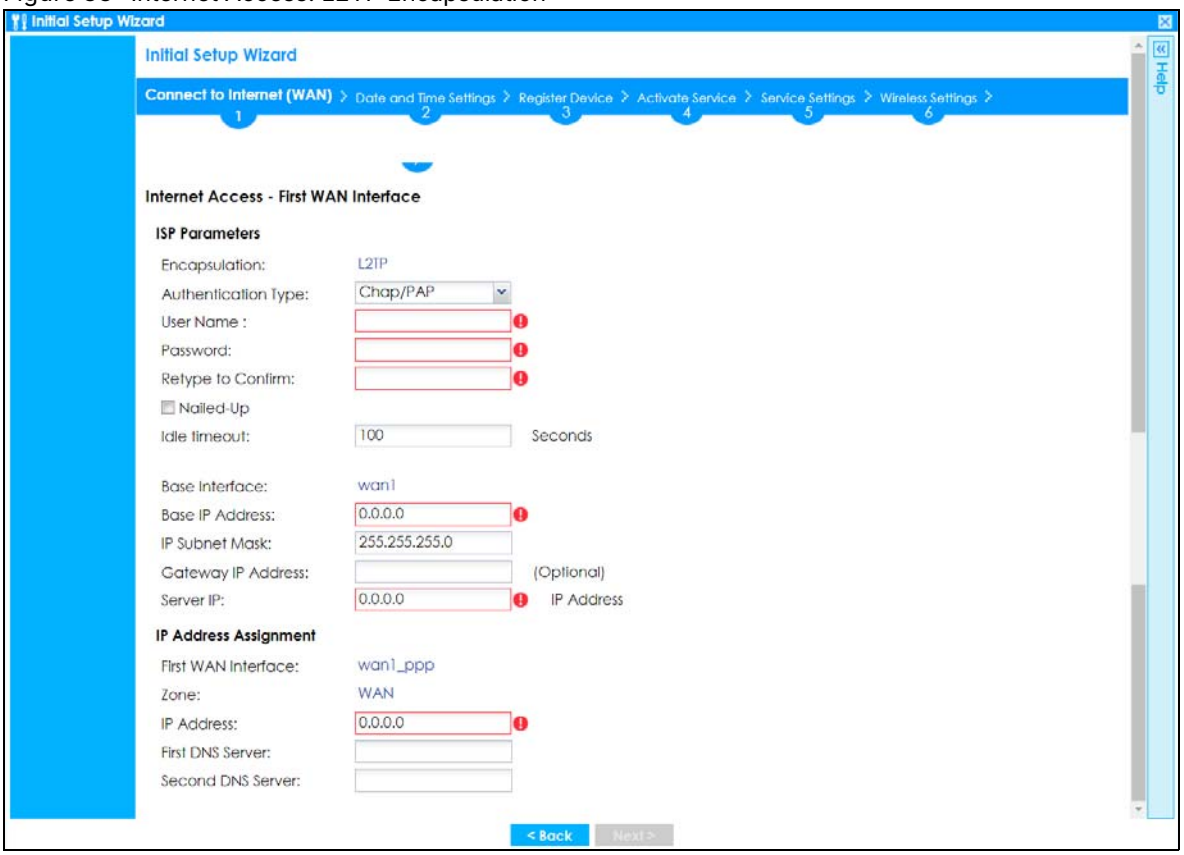
3.1.6.3 WAN IP Address Assignments

- 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.

3.1.6.4 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.

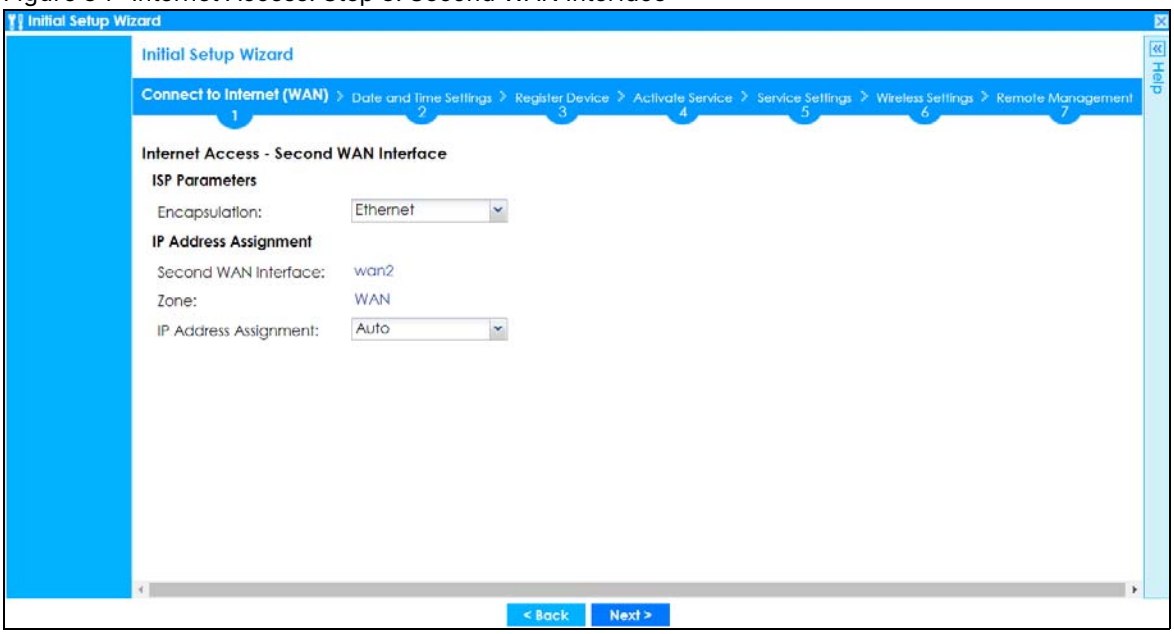
Figure 33 Internet Access: L2TP Encapsulation



3.1.7 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 3.1.2 on page 59).

Figure 34 Internet Access: Step 3: Second WAN Interface



3.1.8 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.

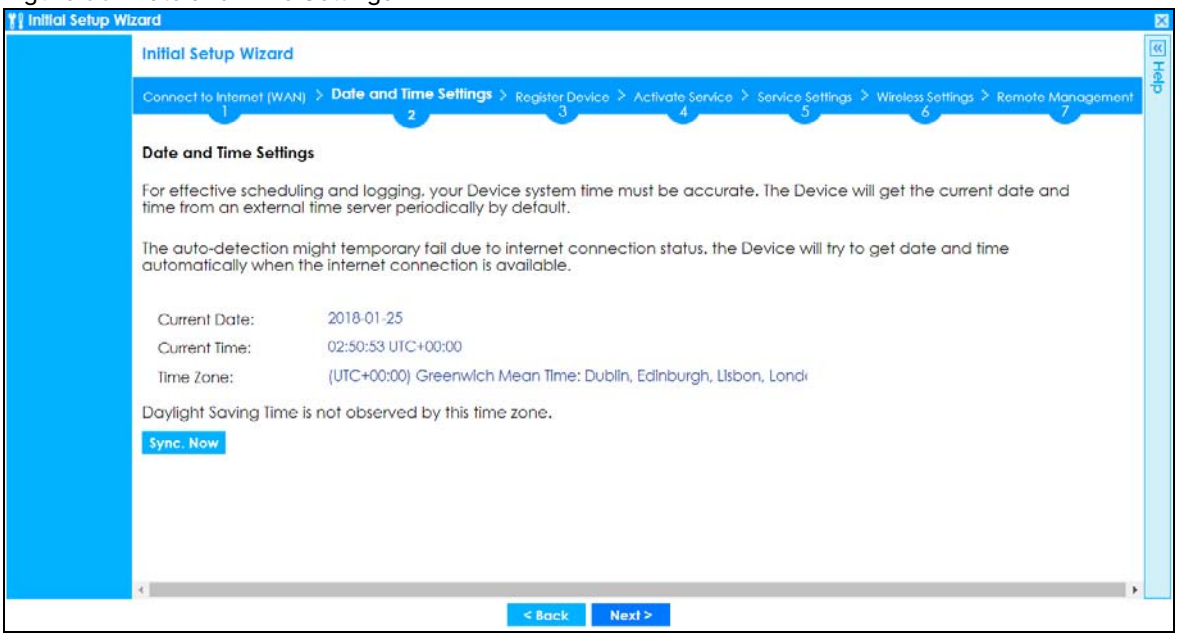
Figure 35 Internet Access: Summary

3.1.9 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 36 Date and Time Settings

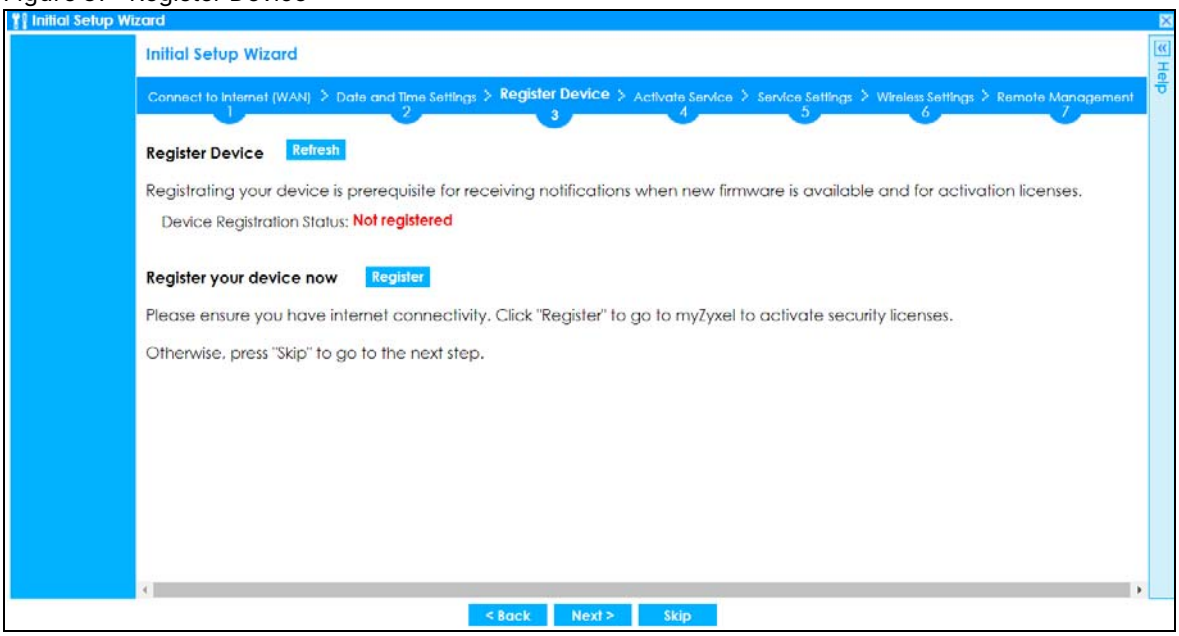


3.1.10 Register Device

Click the Register button in this screen to register your device at account.zyxel.com.

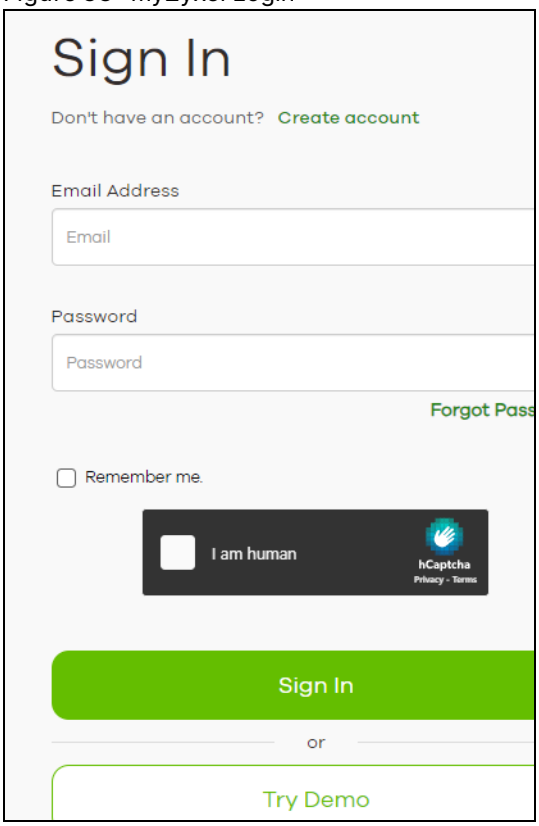
Note: The Zyxel Device must be connected to the Internet in order to register.

Figure 37 Register Device



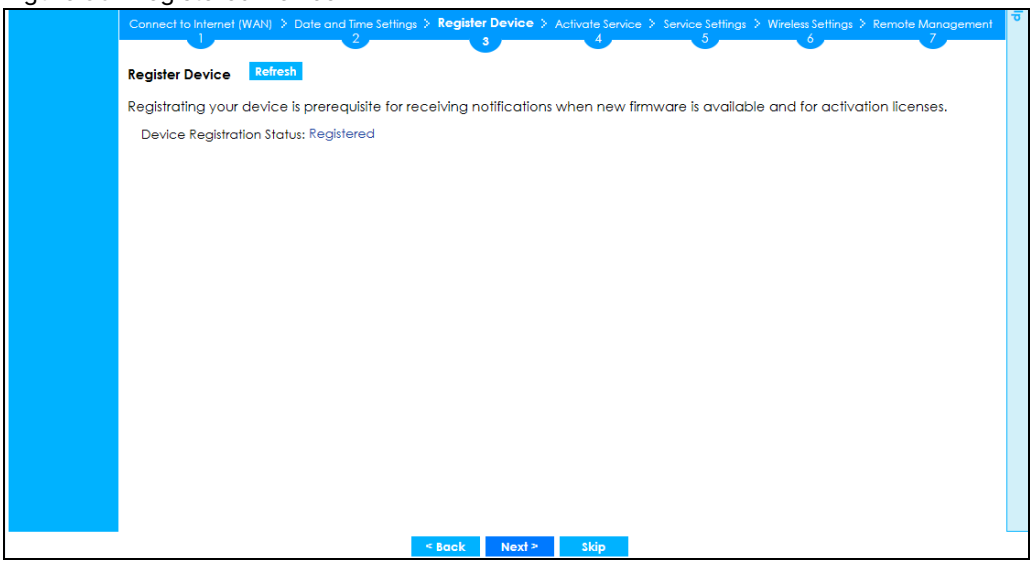
You may need the Zyxel Device's serial number and LAN MAC address to register it at Zyxel Account if you have not already done so. Refer to the label at the back of the Zyxel Device's for details.

Figure 38 myZyxel Login



Click Refresh or use the Configuration > Licensing > Registration screen to update your Zyxel Device registration status. Please note that you cannot change to Nebula Mode once you click Next unless you reset the Zyxel Device.

Figure 39 Registered Device



3.1.11 Activate Service

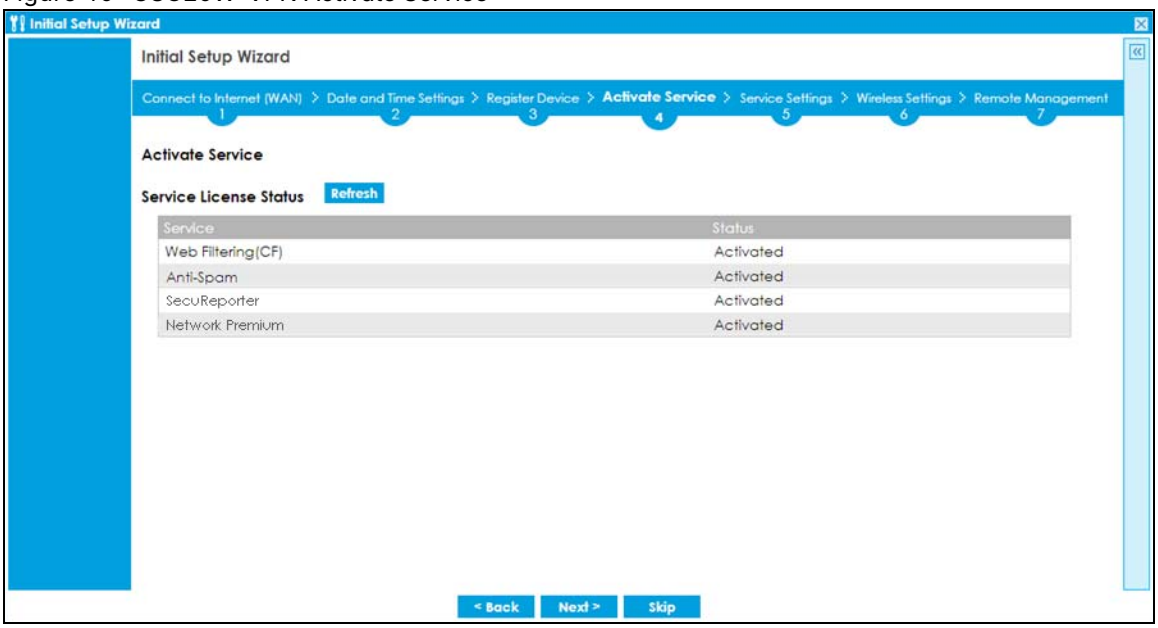
After you register your Zyxel Device, you can register for the services supported by your model. See Subscription Services Available on page 266 for more information on the subscription services for the two types of security packs.

Here are the services available for the Zyxel Device:

- Web Filtering (CF): access a database that can block websites by category.
- Anti-Spam: use anti-spam signatures to mark or discard spam (unsolicited commercial or junk email).
- SecuReporter: collect and analyze logs from your Zyxel Device in order to identify anomalies, notify you of potential internal or external threats, and report on network usage.
- Network Premium: allow users to log in once to get access to permitted resources.

Note: USG FLEX 50AX does not support anti-spam.

Figure 40 USG20W-VPN Activate Service



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.

Note: Refer to Check if Your Zyxel Device Has an Inactive License to check for any inactive licenses assigned to your Zyxel Device.

3.1.12 Service Settings

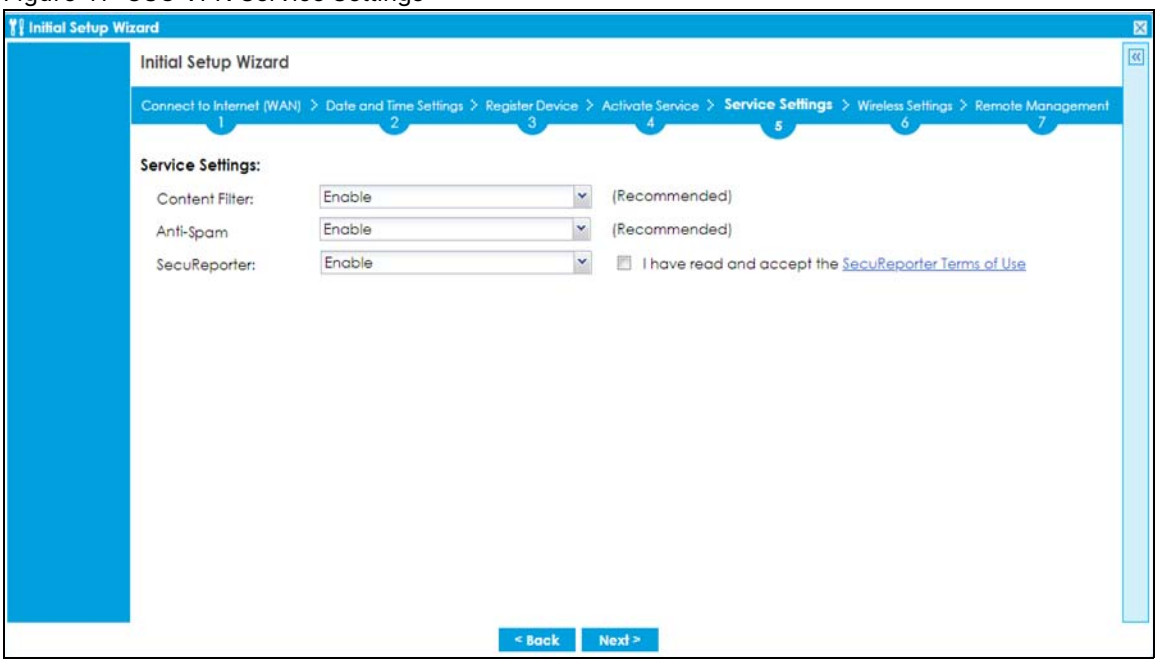
You can enable or disable the following features in this screen. This screen varies depending on the security pack that you purchase. See Subscription Services Available on page 266 for more information on the subscription services for the two types of security packs.

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

- Content Filter: Use this feature to access a database that can block websites by category.
- Anti-Spam: 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, notify you of potential internal or external threats, and report on network usage.

Note: USG FLEX 50AX does not support anti-spam.

Figure 41 USG VPN Service Settings

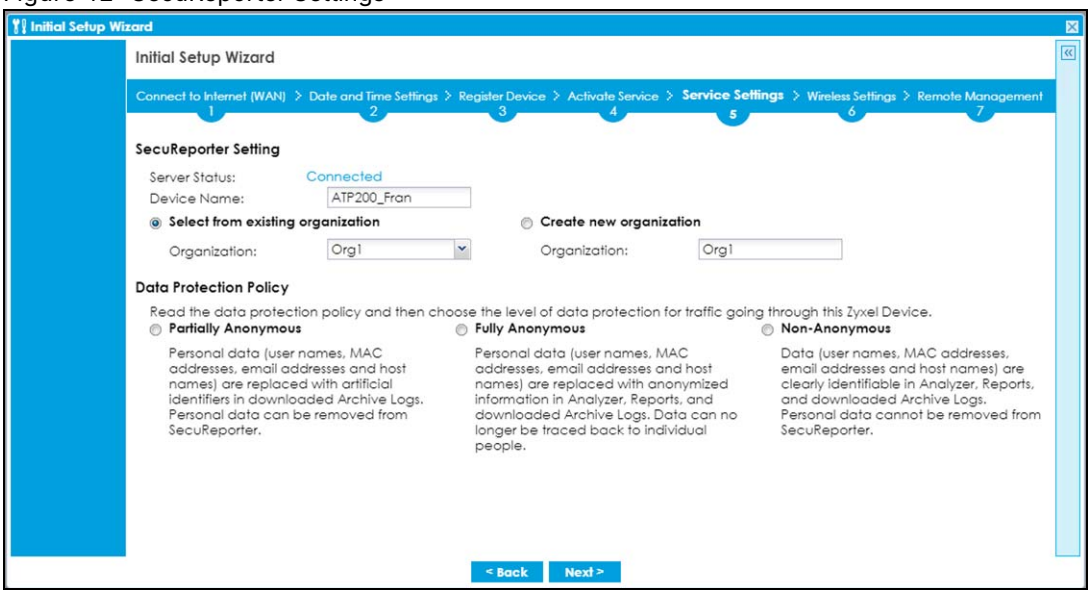


3.1.13 Service Settings: SecuReporter

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.

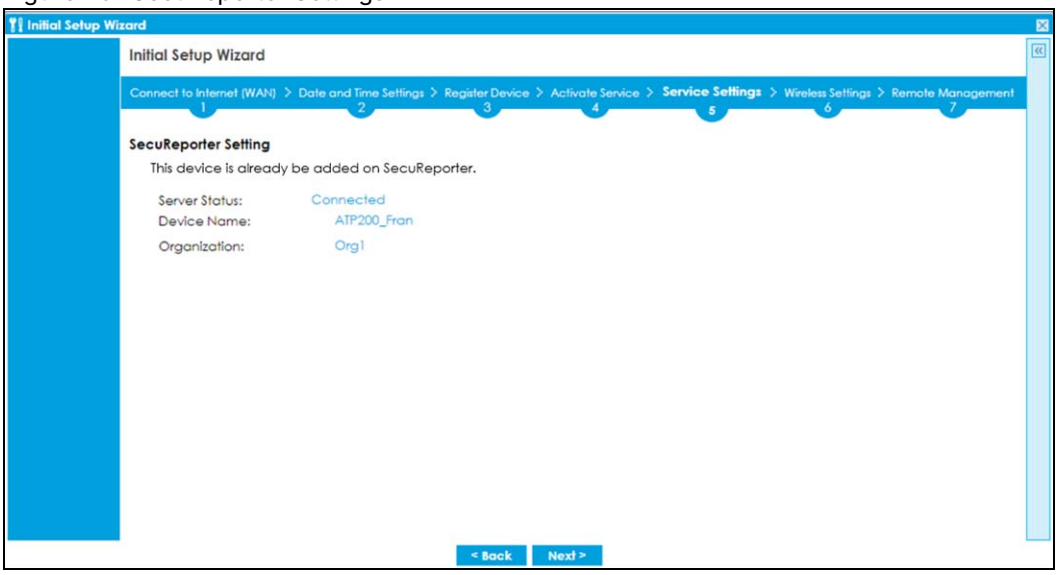
- Server Status: This is the connection status between the Zyxel Device and the SecuReporter server. This field shows Connected when the Zyxel Device can synchronize with the SecuReporter server. This field shows Timeout when the Zyxel Device can't synchronize with the SecuReporter server. This field 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. Enter 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: Enter 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 42 SecuReporter Settings



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

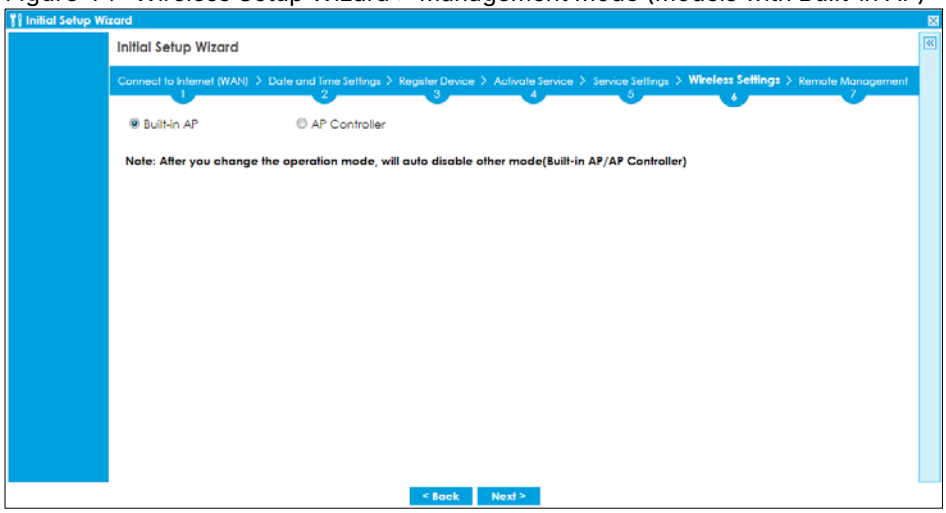
Figure 43 SecuReporter Settings



3.1.14 Wireless Settings: Management Mode

The Management Mode screen appears for Zyxel Devices that have a built-in AP. Select Built-in AP if you want WiFi clients to access your Zyxel Device wirelessly. Select AP Controller to allow the Zyxel Device to manage APs in the same network as the Zyxel Device. Both modes cannot work simultaneously. Click Next to continue the wizard.

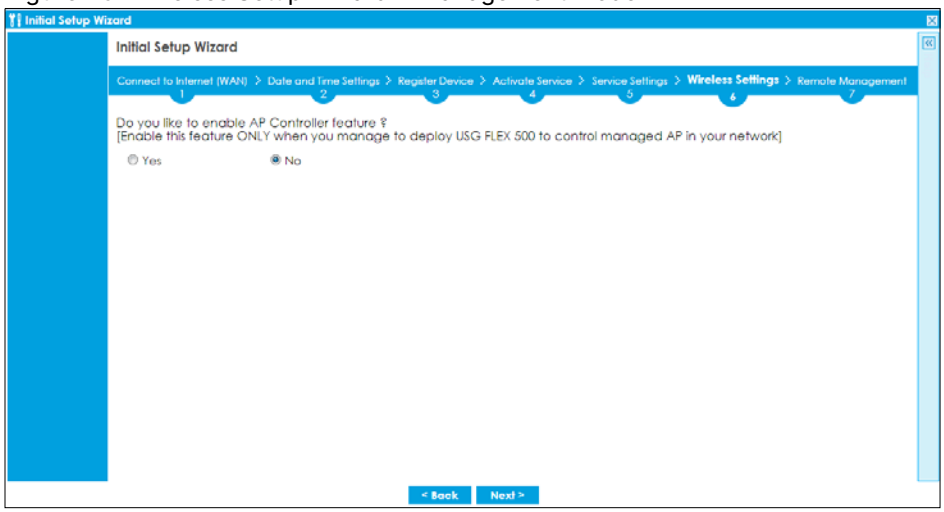
Figure 44 Wireless Setup Wizard > Management Mode (Models with Built-in AP)



3.1.15 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 45 Wireless Setup Wizard > Management Mode



3.1.16 Wireless Settings: SSID & Security

Configure SSID and wireless security in this screen.

SSID Setting

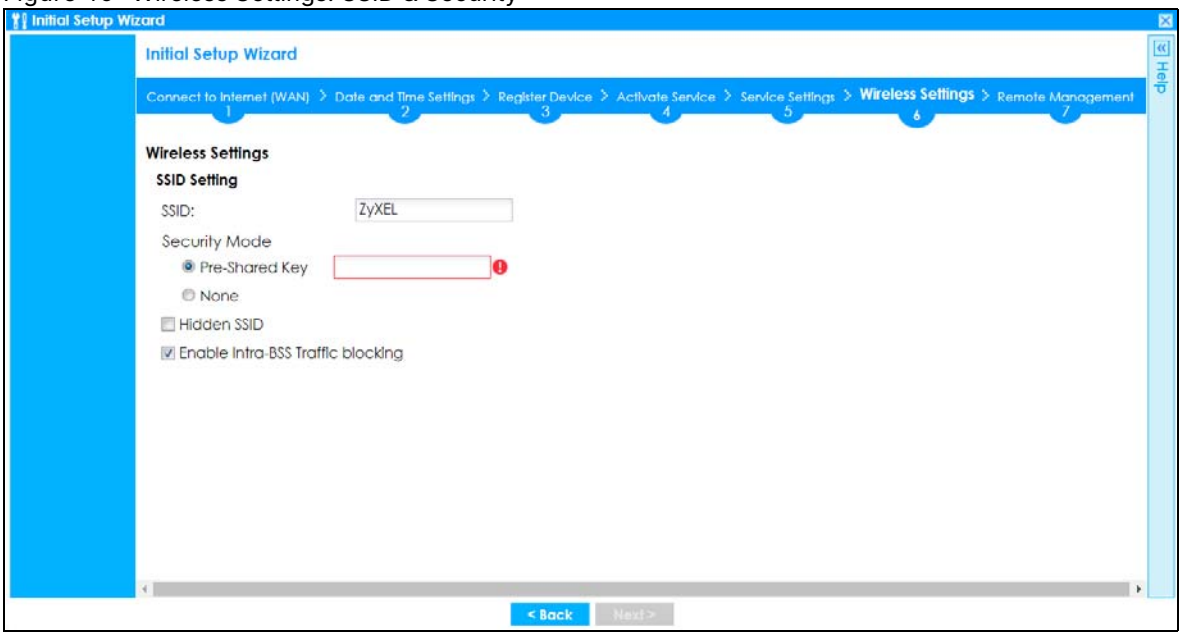
- SSID - Enter a descriptive name of up to 32 printable characters for the wireless LAN.
- Security Mode - Select Pre-Shared Key to add security on this wireless network. Otherwise, select None to allow any wireless client to associate this network without authentication.
- Pre-Shared Key - Enter a pre-shared 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 Zyxel Devices with Built - in 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.

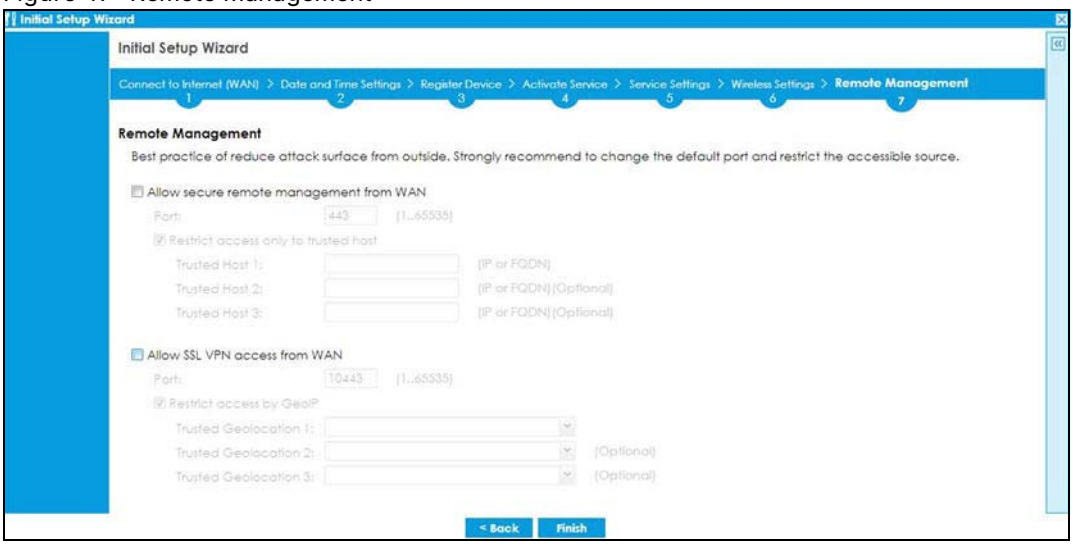
Figure 46 Wireless Settings: SSID & Security



3.1.17 Remote Management

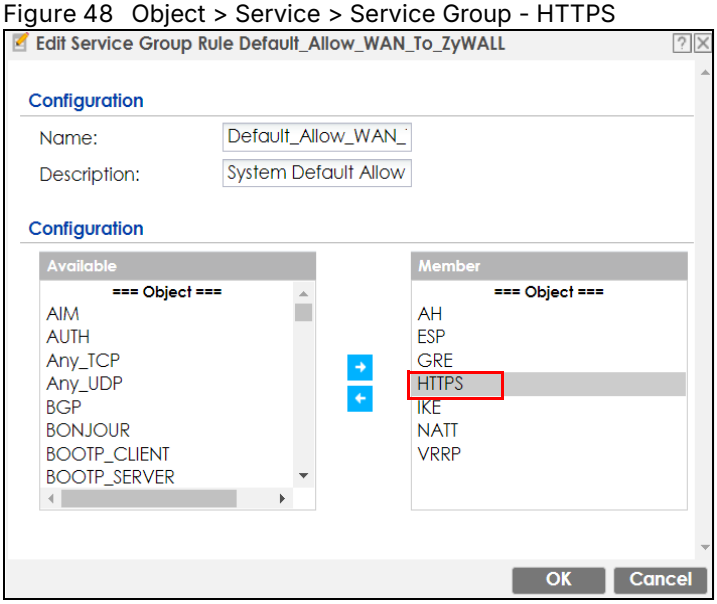
Configure settings in this screen to add a rule that has priority over other rules in Policy Control. It restricts access to the web configurator and SSL VPN service from the Internet.

Figure 47 Remote Management



- Enable Allow secure remote management from WAN to create a rule in the Policy Control screen. It allows you to access the Zyxel Device from the WAN using HTTPS.
- Enable Restrict access only to trusted host to have the Zyxel Device allow access only from the IP addresses or FQDNs specified in the fields below.
- Enable Allow SSL VPN access from WAN to allow access to the Zyxel Device remotely through the SSL VPN tunnel.
- Enable Restrict access by GeoIP to have the Zyxel Device allow access only from countries specified in the fields below.

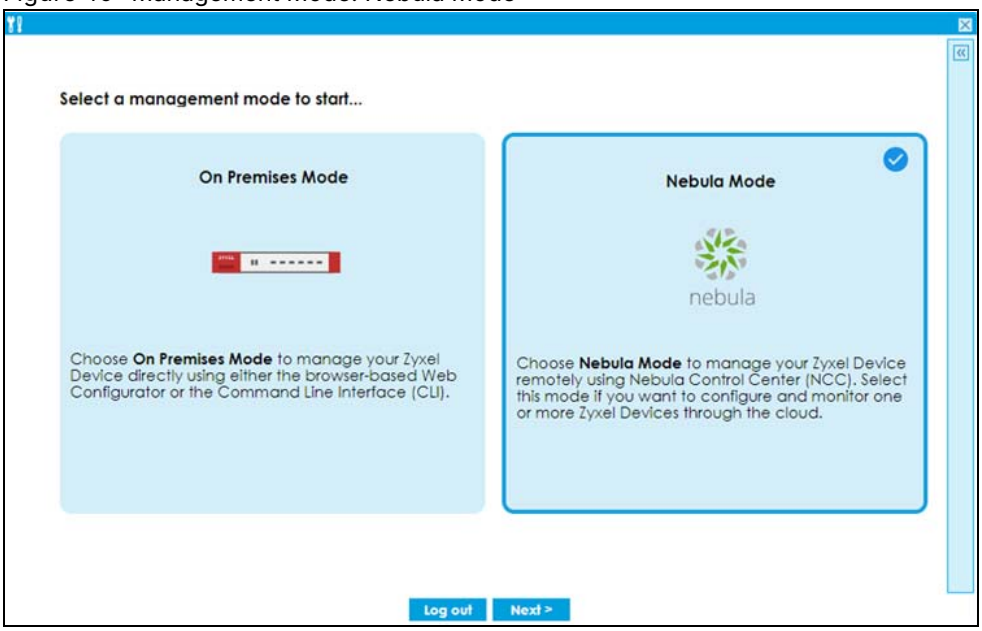
Figure 48 Object > Service > Service Group - HTTPS



3.2 Nebula Mode Initial Setup Wizard

Select Nebula Mode to manage and monitor your Zyxel Device remotely. Follow the wizard to configure the WAN settings to pass the management of your Zyxel Device to NCC.

Figure 49 Management Mode: Nebula Mode



3.2.1 Connect to Internet (WAN)

Configure the WAN interface that the Zyxel Device will use to connect to Nebula through the Internet.

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.

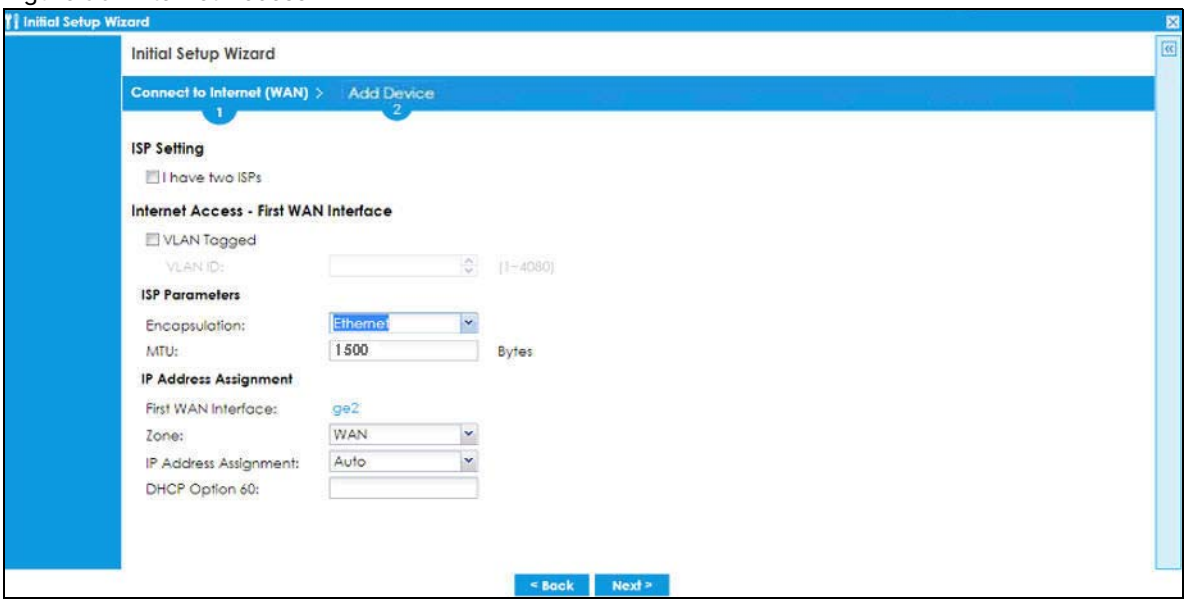
Note: Enter the Internet access information exactly as your ISP gave it to you. Leave a field blank if you don't have that information.

- 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.
- VLAN Tagged: Select this to tag the traffic going out from the Zyxel Device. Enter a VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1-4080.
- Encapsulation: Choose the Ethernet option when the WAN port is used as a regular Ethernet. Choose PPPoE for a dial-up connection according to the information from your ISP.
- MTU: The Maximum Transmission Unit. Enter the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device divides it into smaller fragments. Allowed values are 576-1500. Usually, this value is 1500.
- WAN Interface: This is the interface you are configuring for Internet access.
- 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.

- DHCP Option 60: This field will show if you choose Auto as the IP Address Assignment. DHCP Option 60 is used by the Zyxel Device for identification to the DHCP server using the VCI (Vendor Class Identifier) on the DHCP server. The Zyxel Device adds it in the initial DHCP discovery message that a DHCP client broadcasts in search of an IP address. The DHCP server can assign different IP addresses or options to clients with the specific VCI or reject the request from clients without the specific VCI.

  Enter a string using up to 63 of these characters [a-zA-Z0-9!\"#$%&\'()*+,-./:;<=>?@\[\\\]^_`{}] to identify this Zyxel Device to the DHCP server. For example, Zyxel-TW.

Figure 50 Internet Access



3.2.2 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.

- VLAN ID: This displays the VLAN ID tag for the traffic going out from Zyxel Device you configured in the previous screen.
- Encapsulation: This displays the type of Internet connection you are configuring.
- MTU: This displays the maximum size of each data packet that can move through this interface.
- First WAN Interface: This is the number of the interface that will connect with your ISP.
- IP Address: Enter your (static) public IP address. Auto displays if you selected Auto as the IP Address Assignment in the previous screen.
- DHCP Option 60: This field will show if you selected Auto as the IP Address Assignment in the previous screen. This displays the string you configured to identify DHCP server using VCI.

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

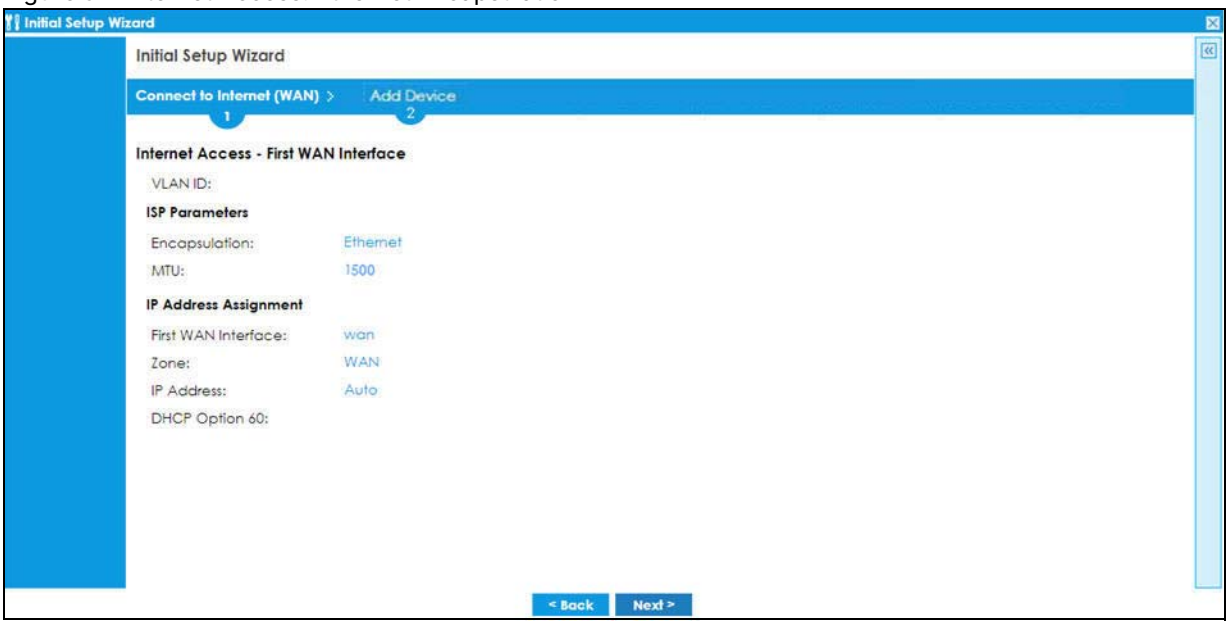
- IP Subnet Mask: Enter the subnet mask for this WAN connection's IP address.
- Gateway IP Address: Enter the IP address of the router through which this WAN connection will send traffic (the default gateway).

- 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. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.

3.2.2.1 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 51 Internet Access: Ethernet Encapsulation



3.2.3 Internet Access: PPPoE

Internet Access - First WAN Interface

- VLAN ID: This displays the VLAN ID tag for the traffic going out from the Zyxel Device, which you configured in the previous screen.

ISP Parameters

- Encapsulation: This displays the type of Internet connection you are configuring.

- MTU: This displays the maximum size of each data packet that can move through this interface.
- Enter 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 -_@$./ characters, and it can be up to 64 characters long.
- Authentication Type - Select an authentication protocol for outgoing connection requests. Options are:
  - Chap/PAP - Your Zyxel Device accepts either CHAP or PAP when requested by the remote node.
  - Chap - Your Zyxel Device accepts CHAP only.
  - PAP - Your Zyxel Device accepts PAP only.
  - MSCHAP - Your Zyxel Device accepts MSCHAP only.
  - MSCHAP-V2 - Your Zyxel Device accepts MSCHAP-V2 only.
- Enter the User Name given to you by your ISP. You can use alphanumeric and -_@$./ characters, and it can be up to 31 characters long.
- Enter the Password associated with the user name. Use up to 64 ASCII characters except the [] and ?. This field can be blank.

IP Address Assignments

- WAN Interface: This is the name of the interface that will connect with your ISP.
- IP Address: This displays Auto as the IP Address Assignment is set to Auto in the previous screen.

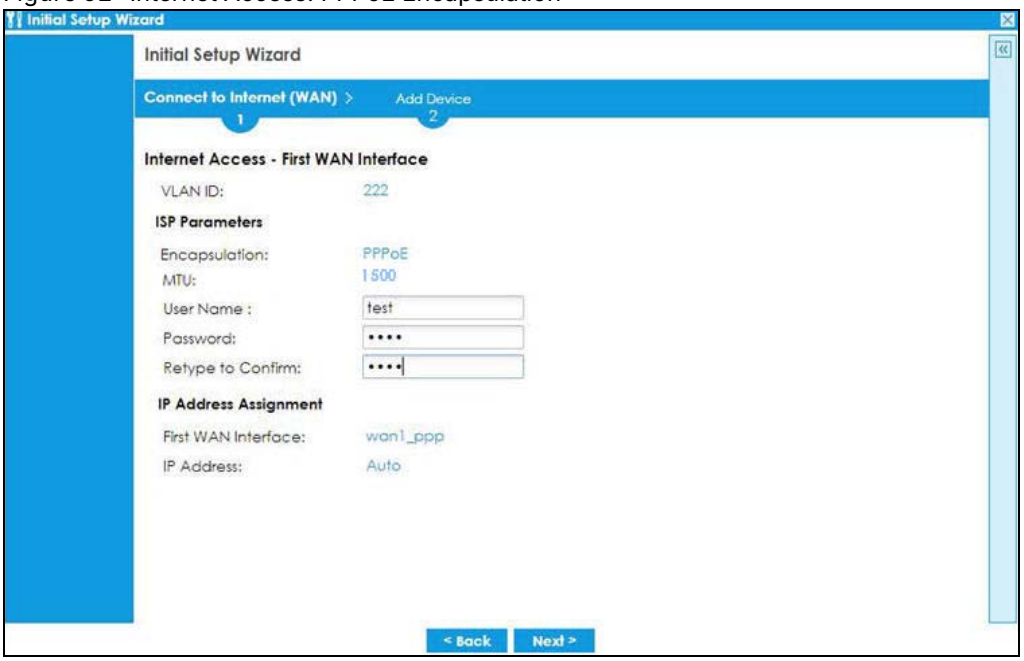
The following fields display if you selected static IP address assignment.

- 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. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.

3.2.3.1 Possible Errors

- 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.

Figure 52 Internet Access: PPPoE Encapsulation



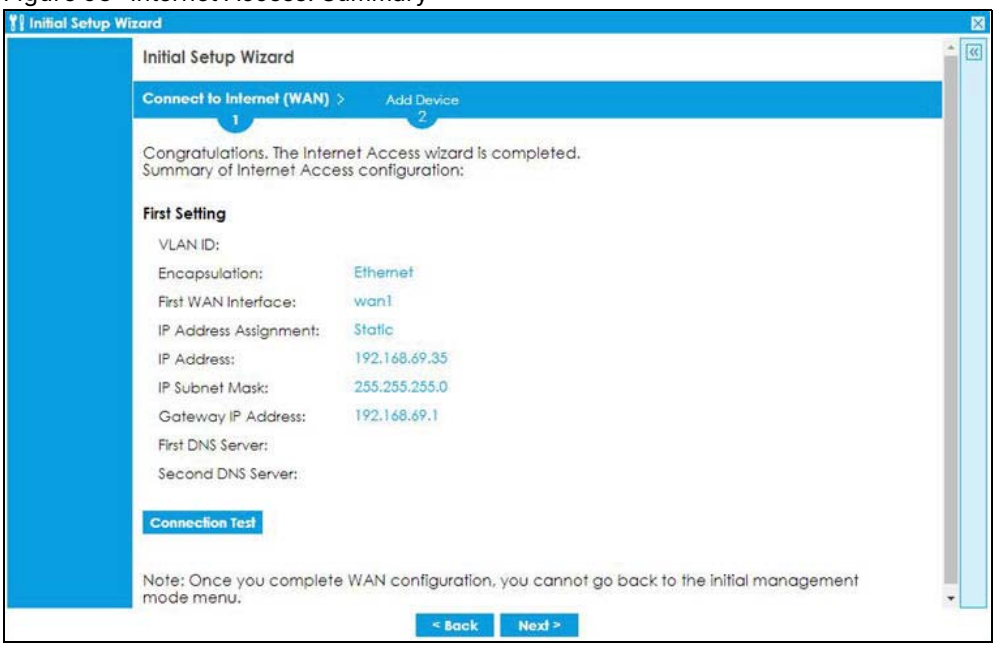
3.2.4 Internet Access: Congratulations

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.

Click Next to go to the next screen to finish the Nebula mode wizard. Please note that you cannot change to On Premises Mode once you click Next unless you reset the Zyxel Device.

If you cannot access Nebula through the Internet after you left this screen, log in to the Zyxel Device using the support account. Use the Local GUI web configurator for troubleshooting.

Figure 53 Internet Access: Summary

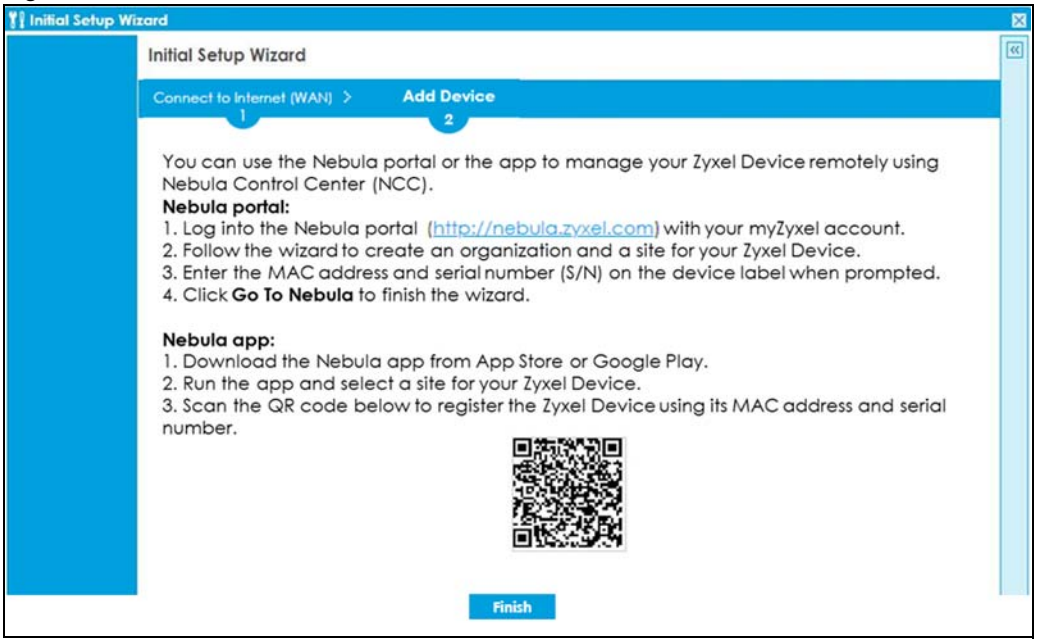


3.2.5 QR Code

Click the link to go to Nebula. Follow the steps in this screen to run the Nebula setup wizard.

Create an organization and a site. Add the Zyxel Device to this site by entering its MAC address and serial number. Select Native Mode when you're given a choice. Click Finish to close the wizard.

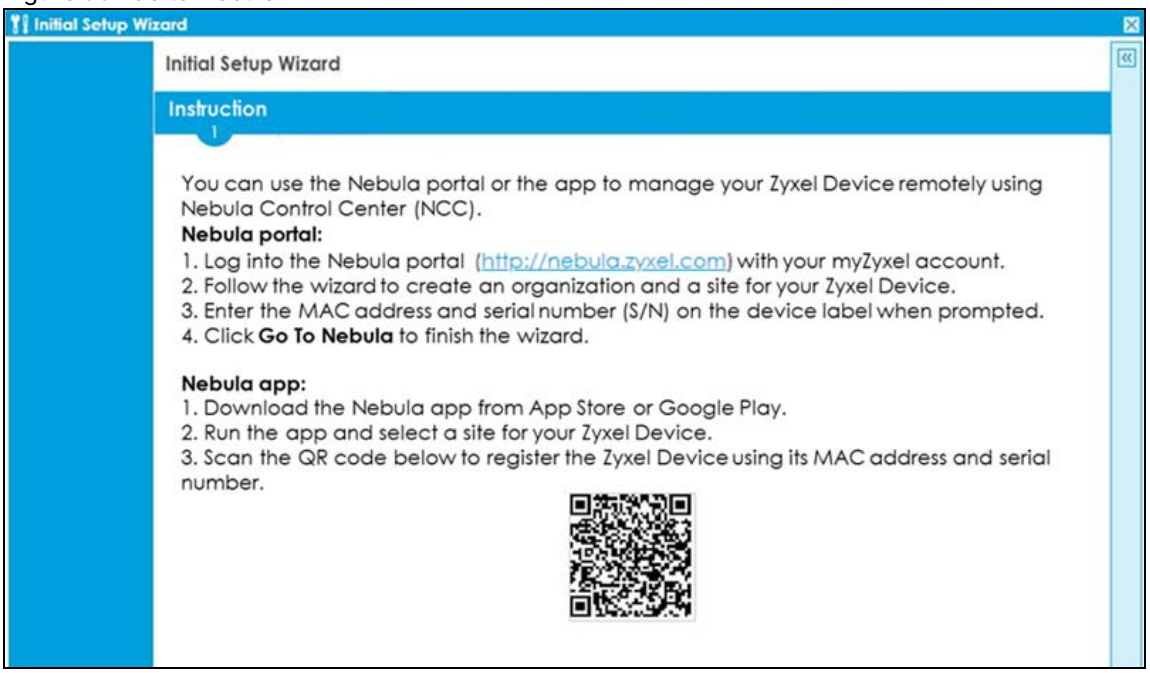
Figure 54 Go to Nebula



If you see this screen right after you select Nebula Mode, click the link or the Go to Nebula button to go to Nebula directly. Follow the steps in this screen to run the Nebula setup wizard.

Configure the WAN interface that the Zyxel Device will use to connect to Nebula through the Internet on the Nebula setup wizard. Configure an email address to receive the activation link. Follow the steps in the email to allow automatic management of the Zyxel Device by Nebula (ZTP). Click Back to go back to the management mode selection screen.

Figure 55 Go to Nebula



CHAPTER 4
Hardware, Interfaces and Zones

4.1 Hardware Overview

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

4.1.1 Front Panels

The LED indicators are located on the front panel.

Figure 56 USG FLEX 50 (USG20-VPN) Front Panel

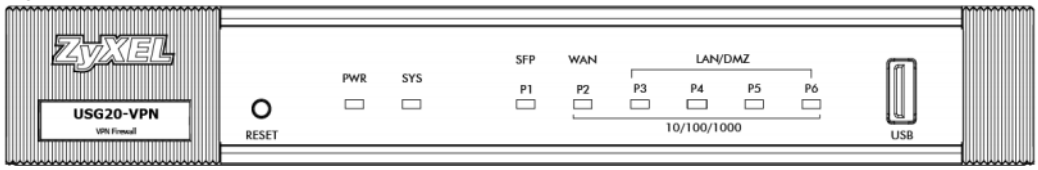


Figure 57 USG FLEX 50AX Front Panel

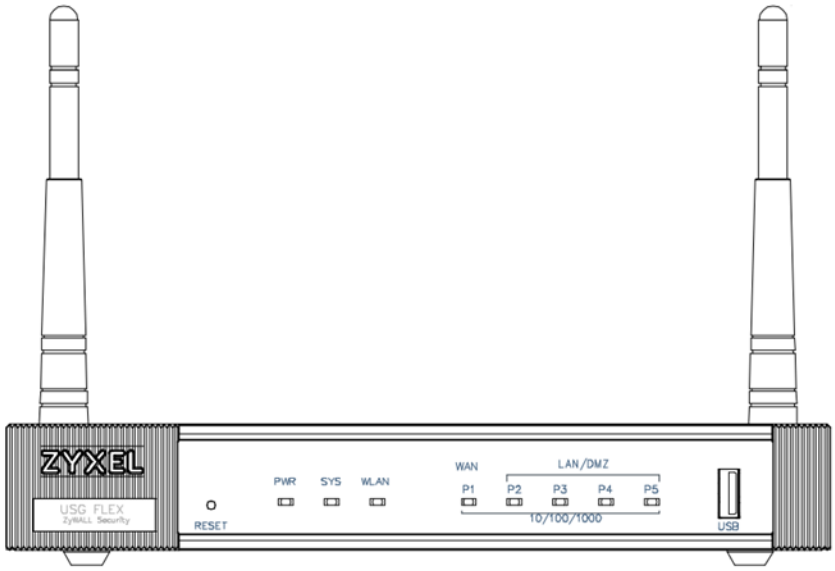
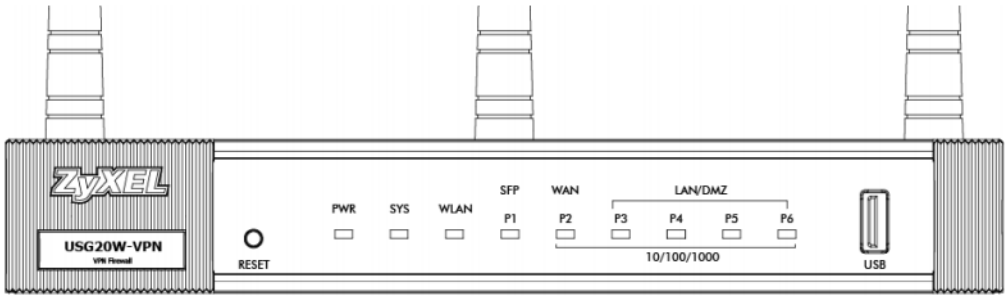


Figure 58 USG20W-VPN Front Panel



The following table describes the front panel LEDs.

Table 11 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.
USB	Green	Off	No device is connected to the Zyxel Device's USB port or the connected device is not supported by the Zyxel Device.
		On	A mobile broadband USB card or USB storage device is connected to the USB port.
	Orange	On	Connected to a mobile broadband network through the connected mobile broadband USB card.
P1, P2...	Green	Off	There is no traffic 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.
	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.

The following table describes the ports on the front panel.

Table 12 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).
P1 ~ P6	These are 1G RJ-45 Ethernet ports.

4.1.2 Rear Panels

The connection ports are located on the rear panel.

Figure 59 USG FLEX 50/USG20-VPN / USG20W-VPN Rear Panel

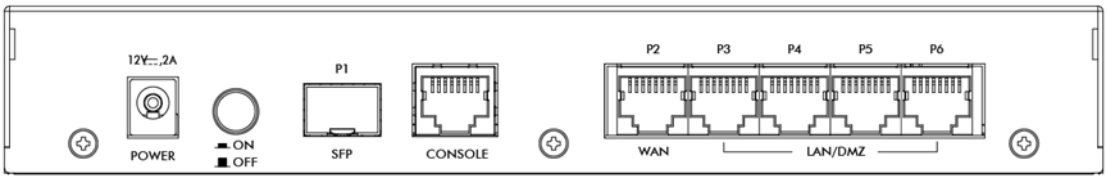
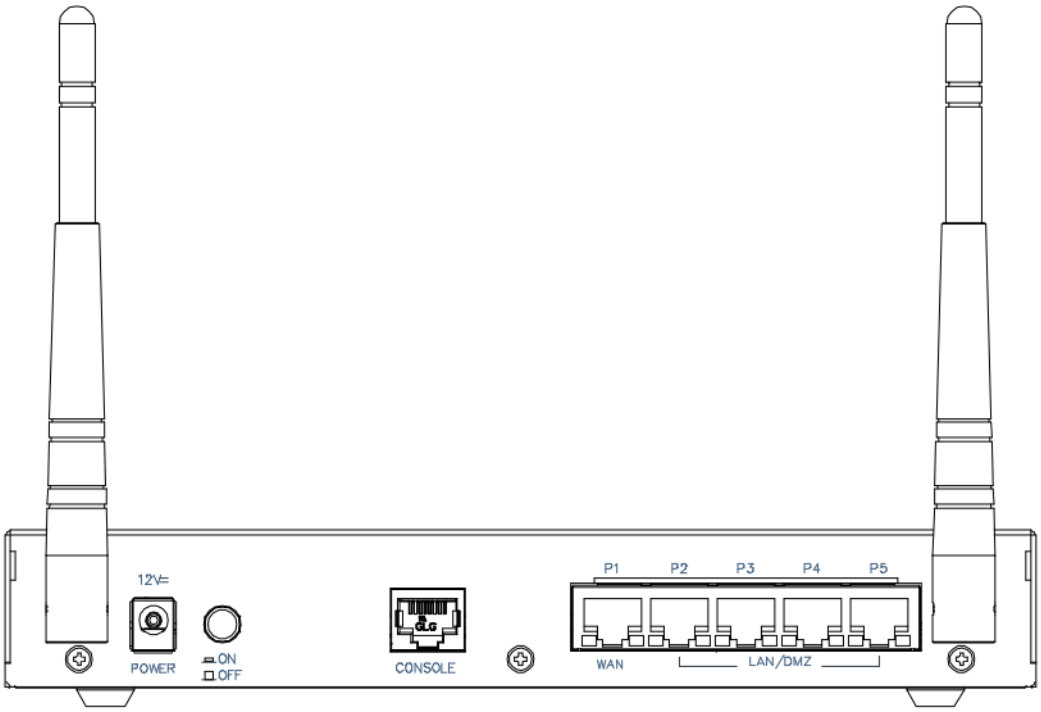


Figure 60 USG FLEX 50AX Rear Panel



The following table describes the items on the rear panel.

Table 13 Rear Panel Items

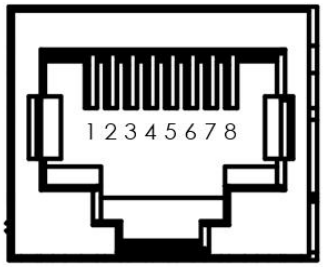
LABEL	DESCRIPTION
Console	You can use the console port to manage the Zyxel Device using CLI commands. You will be prompted to enter your user name and password. See the Command Reference Guide for more information about the CLI. When configuring using the console port, you need a computer equipped with 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.

4.1.3 Console Port Pin Connection

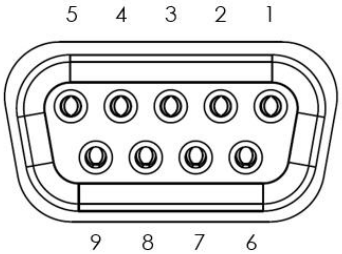
The RJ-45 connector pins are as follows.

Figure 61 RJ-45 Connector Pins



The DB-9 connector pins are as follows.

Figure 62 DB-9 Connector Pins



These are the cable pinouts for RJ-45 to DB-9.

Table 14 Cable Pinouts for RJ-45 to DB-9

CONSOLE PORT / RJ-45 PIN	SIGNAL	DB-9 PIN
1	DTR	6
2	DSR	4
3	RxD	3
4	CTS	7
5	GND	5
6	TxD	2
7	RTS	8
8	NC	1, 9

These are the signal names.

Table 15 Signal Names

SIGNAL	SIGNAL NAME
RxD	Receive Data
TxD	Transmit Data
DTR	Data Terminal Ready
GND	Ground
DSR	Data Set Ready

Table 15 Signal Names

SIGNAL	SIGNAL NAME
RTS	Request to Send
CTS	Clear to Send
RI	Ring Indicator
NC	Not Connected

4.2 Installation Scenarios

The Zyxel Device can be:

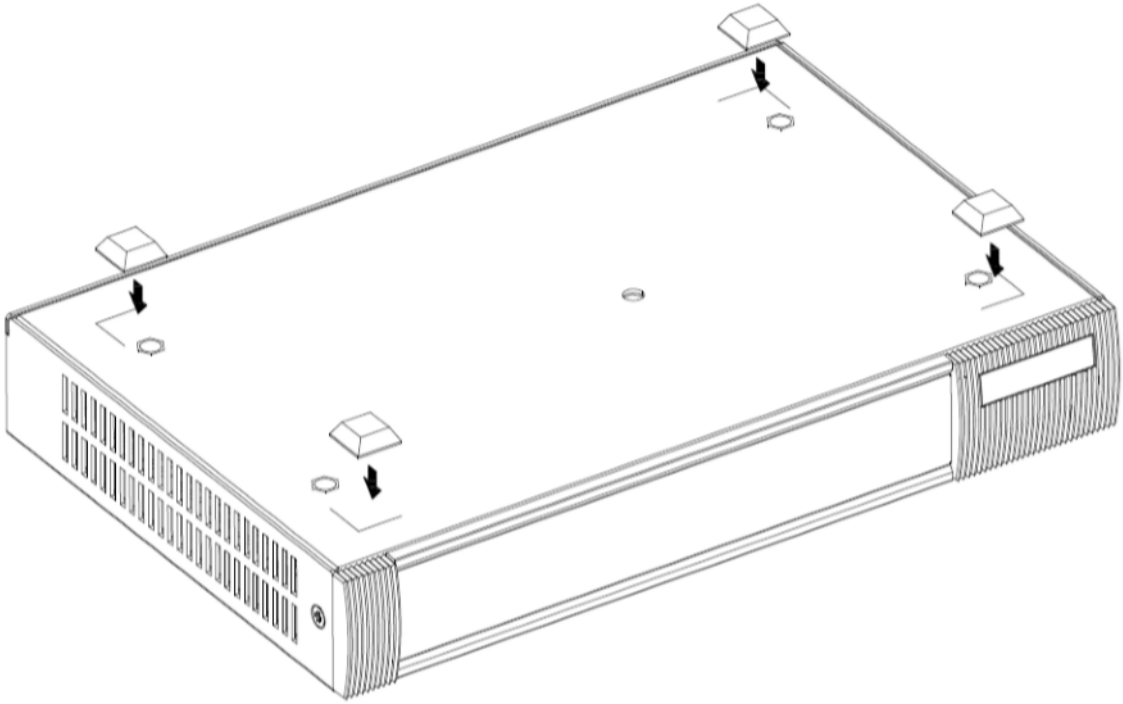
- Placed on a desk.
- Wall-mounted on a wall.

WARNING! Do NoT block the ventilation holes on the Zyxel Device. Allow 100 mm clearance for the ventilation holes to prevent your Zyxel Device from overheating. Do not store things on the Zyxel Device. Do not place a Zyxel Device on another high temperature device. Overheating could affect the performance of your Zyxel Device, or even damage it.

4.2.1 Desk-mounting

1. Make sure the Zyxel Device is clean and dry.
2. Remove the adhesive backing from the rubber feet.
3. Attach the rubber feet to each corner on the bottom of the Zyxel Device. These rubber feet help protect the Zyxel Device from shock or vibration, and allow air circulation.

Figure 63 Attaching Rubber Feet



4.2.2 Wall-mounting

Do the following to attach the Zyxel Device to a wall.

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

Table 16 Distance “X” between mounting holes

MODEL NAME	DISTANCE “X”
USG FLEX 50 (USG20-VPN)	174 mm (6.85”)
USG FLEX 50W (USG20W-VPN)	174 mm (6.85”)

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 64 Wall Mounting Screw Specifications

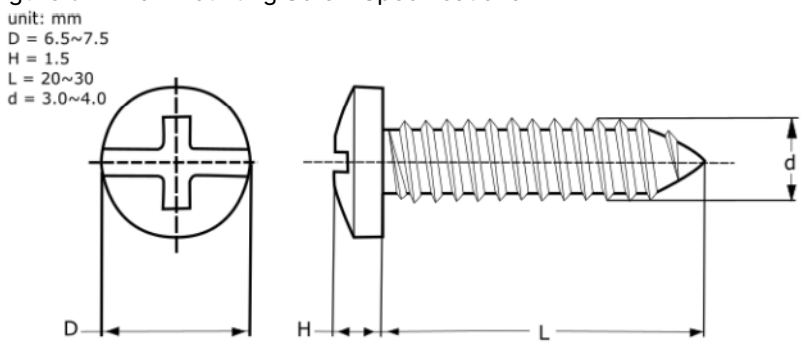
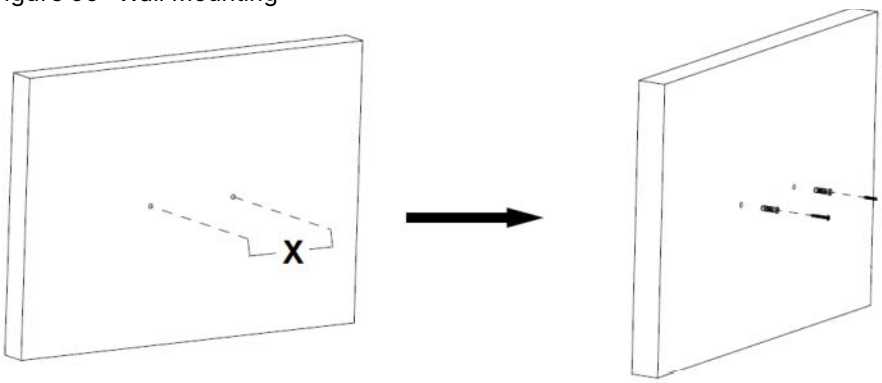


Figure 65 Wall Mounting

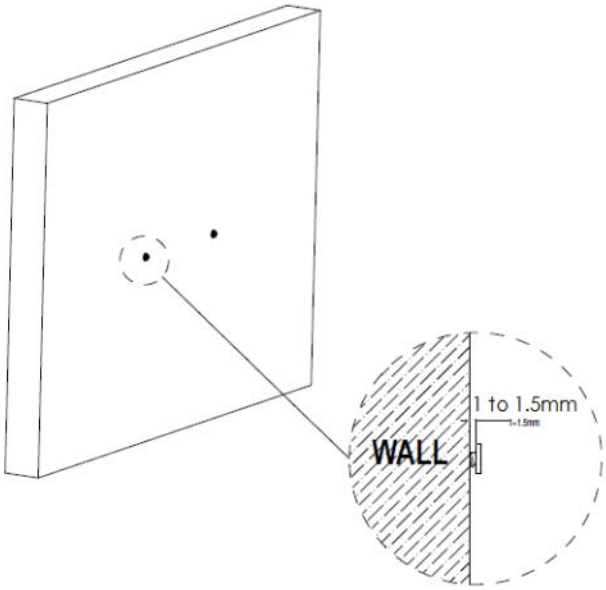


2 Screw two screws with 6 mm ~ 8 mm (0.24" ~ 0.31") wide heads into the screw anchors. Do not screw the screws all the way in to the wall; leave a small gap of between 1 ~ 1.5 mm (0.04″ ~ 0.06″) between the head of the screw and the wall.

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.

Figure 66 Gap for Cables



3 Use the holes on 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.

4.3 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 17 Default Physical Port - Interface Mapping

PORT / INTERFACE	P1	P2	P3	P4	P5	P6	P7	P8
USG FLEX 50 (USG20-VPN)	sfp	wan	lan1	lan1	lan1	lan1		
USG FLEX 50AX	wan	lan1	lan1	lan1	opt			
USG20W-VPN	sfp	wan	lan1	lan1	lan1	lan1		

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

Table 18 Default Zone - Interface Mapping

ZONE / INTERFACE	WAN	LAN1	LAN2	DMZ	OPT	NO DEFAULT ZONE
USG FLEX 50 (USG20-VPN)/ USG FLEX 50AX/ USG20W-VPN	WAN WAN_PPP	LAN1	LAN2	DMZ	OPT OPT_PPP	

4.4 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 5
Easy Mode

5.1 Overview

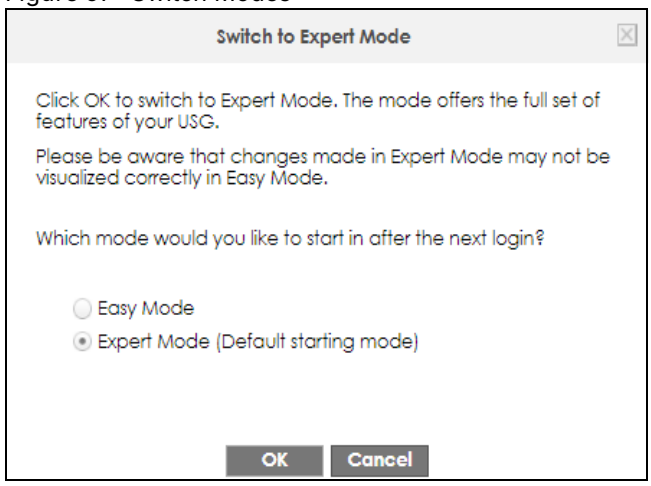
Easy Mode contains wizards that help you configure the Zyxel Device, links to portals and the advanced menus in Expert Mode.

Note: See Section 1.1 on page 24 to see which models support Easy Mode wizards.

Use the Easy Mode screens if you have a relatively simple network environment with one WAN (WAN1) and one LAN (LAN1) connections. If your Zyxel Device has two WAN ports, use WAN1 as the WAN connection. If you use WAN2 as the WAN connection or want to use both WAN ports, then please use the Expert Mode screens.

If you prefer to start directly with the advanced screens, then simply click Expert Mode and select the Expert Mode option.

Figure 67 Switch Modes



Note: Enabling guest network renames the OPT or P6 port to "guest". Go to the Configuration > Network > Interface > Port Role screen in Expert Mode to check. A guest interface is created. The OPT port or the highest-numbered copper Ethernet port in the Zyxel Device will be bound with the guest interface. If Device HA is used, then the second-highest numbered port will be used instead.

5.1.1 Objects and Rules

The Zyxel Device automatically creates EZ_ objects and rules in Expert Mode for settings configured in Easy Mode. The following table shows whether you can edit or delete the EZ_ objects and rules in the listed screens. When creating objects and rules in Expert Mode, you cannot use "EZ_" at the beginning of the name.

Go back to Easy Mode to edit your settings on EZ_ rules. If you edit an EZ_ rule in Expert Mode, the corresponding policies created in Easy Mode may work differently.

You cannot delete EZ_ objects or rules if they are used in a policy. To delete an EZ_ object or rule, you need to delete all corresponding policies. If you delete an EZ_ object or rule in Expert Mode, the corresponding policies created in Easy Mode may not work.

Table 19 Editing & Deleting EZ_ Objects

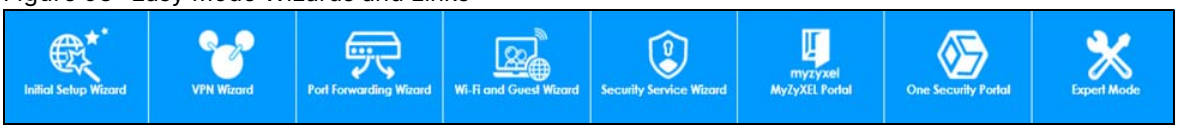
OBJECT/ RULE	SCREEN	EDIT	DELETE
X: The action is not allowed. V: The action is allowed.			
guest interface	Configuration > Network > Interface > Ethernet	X	X
Content filtering	Configuration > UTM Profile	V	V
IDP		V	V
Anti-Virus		V	V
Static DHCP Binding	Configuration > Network > IP/MAC Binding	X	V
Address		X	V
Connection	Configuration > VPN > IPSec VPN	X	V
Gateway		X	V
AP group	Configuration > Wireless	X	V
Radio		X	V
NAT	Configuration > Network > NAT	X	V
Security policy	Configuration > Security Policy	X	V
Zone	Configuration > Object	X	V
AP profile		X	V
Security		X	V
SSID		X	V
Address/Geo IP		X	V
Service		X	V

5.1.2 Wizards and Links

In the wizards, click the question mark on the right ? to display or hide the help. Click Next > to continue to the following screen, < Back to return to the previous screen and Exit or X (top right) to close the wizard screen without saving any changes.

The following are the Easy Mode wizards and links.

Figure 68 Easy Mode Wizards and Links



- Initial Setup Wizard for Internet access - you should have your Internet access account information at hand
- VPN Wizard for a site-to-site tunnel between Zyxel Device networks, a tunnel from a remote client using the Zyxel client VPN software to the Zyxel Device network, or a tunnel from a remote client using other VPN software to the Zyxel Device network
- Port Forwarding Wizard to set up a server, such as a NAS in your network that you or other people can access from outside the network
- Wi-Fi and Guest Wizard to set up a wireless name and security for normal and guest (Internet only) wireless access to the Zyxel Device
- Security Service Wizard to configure subscriptions for content filtering, IDP, and anti-virus services.

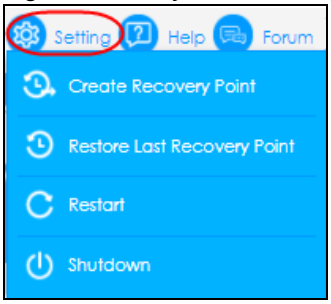
There are also links to:

- MyZyxel Portal where you can subscribe for security services such as content filtering, IDP, and anti-virus
- One Security Portal where you can get configuration walkthroughs, troubleshooting help and other help on security services and VPN
- Expert Mode which contains all the advanced menus.

5.1.3 Easy Mode Settings

Click to display the Easy Mode Settings menu.

Figure 69 Easy Mode Settings



- Create Recovery Point - a recovery point is a point to which all the Zyxel Device's configuration can be reset to after you click Create Recovery Point. Choose this when you have some configurations done and everything is working correctly.
- Restore Last Recovery Point - choose this if you have problems with recent configurations done on the Zyxel Device and you want to return to a previous configuration point where everything was working correctly. You will lose all configurations done after the restore point.
- Restart - reboot the Zyxel Device after upgrading new firmware. It may also be useful when troubleshooting. Changes in the Web configurator are saved automatically and do not change when you reboot. If you made changes in the CLI, however, you have to use the write command to save the configuration before you reboot.
- Shutdown - use this to safely turn off the Zyxel Device in preparation for disconnecting the power. Shutdown writes all cached data to the local storage and stops the system processes. It does not turn off the power. Wait for the device to shut down before you manually turn off or remove the power.

5.1.4 Easy Mode Dashboard

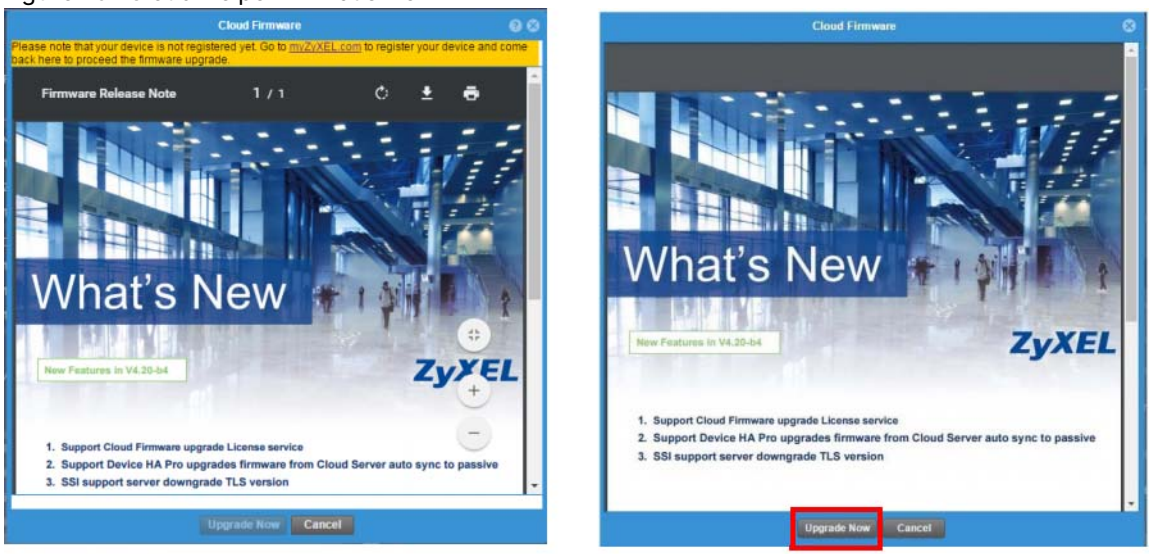
Cloud Helper

Click the Cloud Helper icon

to check if there is new firmware available at myZyxel.

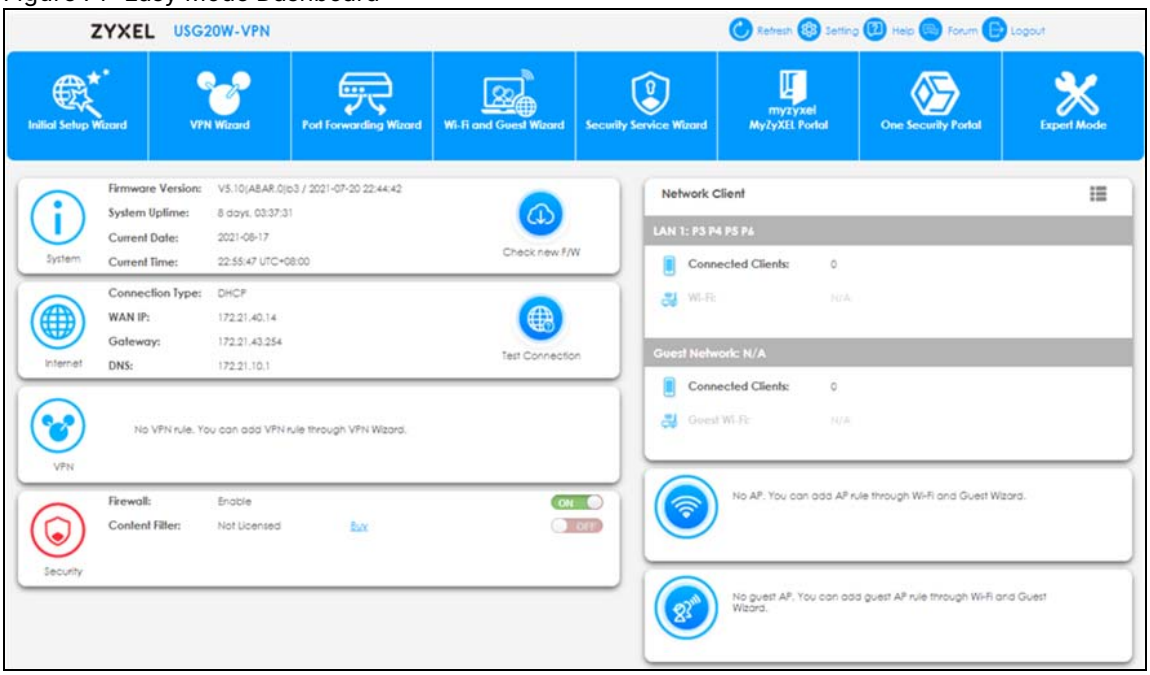
If there is new firmware available at myZyxel, then the icon displays a red N. Click the icon with the red N to display a What's New pop-up screen. You need a Firmware Upgrade license to upgrade the firmware. If you do not have a license, Upgrade Now is grayed out. If you have a license, click Upgrade Now to directly upgrade firmware. The Zyxel Device will reboot automatically.

Figure 70 Cloud Helper - What's New



The Easy Mode dashboard is shown next.

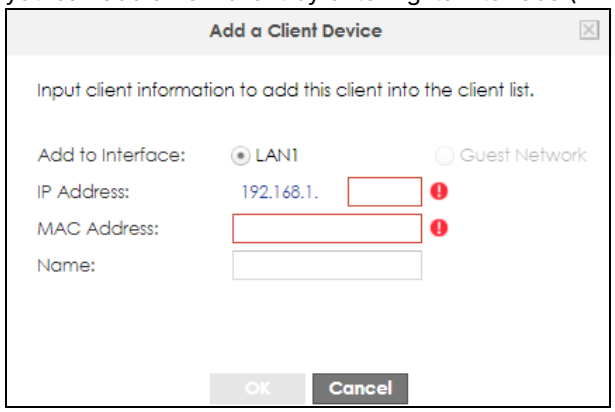
Figure 71 Easy Mode Dashboard



The Easy Mode dashboard contains the following.

- System information, such as firmware version, the length of time the Zyxel Device has been on, date and time.
- Internet information such as Internet connection type, WAN IP address and a button to test the connection.
- VPN tunnel information and a button to monitor and create VPN tunnels.
- Security information such as if the firewall is enabled and if supported security services are licensed. You will be prompted to create a secure policy when a service is licensed and you turn it on in order for the service to be used.
- Network Client

Click the settings icon to manage clients. Click + to add a new network client. In the pop-up screen, you can add a new client by entering its interface (LAN1 or Guest), IP Address, MAC Address and Name.



This is the information you see under Network Client:

- LAN information on wired and wireless connections to the Zyxel Device
- Guest Network information on guest wired and wireless connections to the Zyxel Device
- Wi-Fi button to change Wi-Fi channel
- Guest button turn the guest wireless network off or on.

5.2 Initial Setup Wizard - Language and Overview

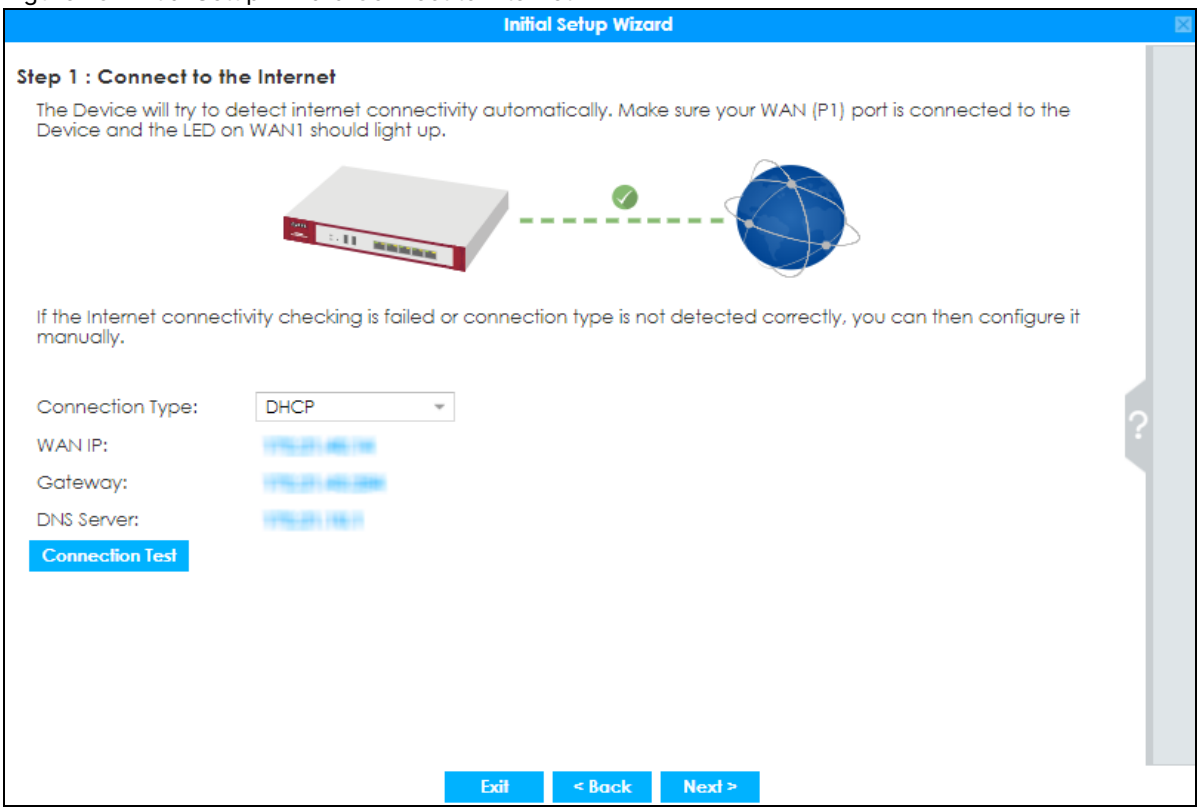
Figure 72 Initial Setup Wizard Language

Choose the language for the Easy Mode and Expert Mode screens.

The initial wizard helps you set up basic options as shown in the screen. At the end, you will have the choice of finishing the wizard or continuing the wizard to configure the optional features as listed. If you choose to finish the wizard, you can configure the optional features later using their own separate links in the Easy Mode main screen.

5.2.1 Initial Setup Wizard - Internet

Figure 73 Initial Setup Wizard Connect to Internet



This screen displays the Internet settings if the Zyxel Device can detect them automatically.

If the Zyxel Device cannot detect the Internet settings automatically, then you have to enter them manually.

- Choose DHCP if you were not given a specific IP address for the Zyxel Device. This allows the Zyxel Device to be able to get one automatically.
- Choose Ethernet Fixed IP if you were given a specific IP address for the Zyxel Device.
- Choose PPPoE if you were given a PPPoE user name and password.

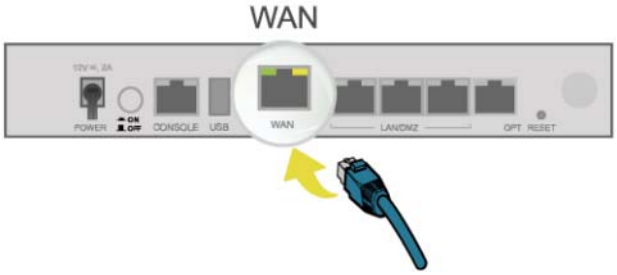
Note: Enter the Internet access information exactly as your ISP gave you.

5.2.2 Initial Setup Wizard - Internet Access Errors

These are some things you can do if you see Internet access error messages.

WAN 1 Down

Check that your cable connection from the WAN1 interface on the Zyxel Device 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 WAN1 interface on the Zyxel Device should be orange.



PPPoE Error

Your Zyxel Device was not able to obtain an IP address. Check 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 for correct WAN settings and user credentials.

DHCP Error

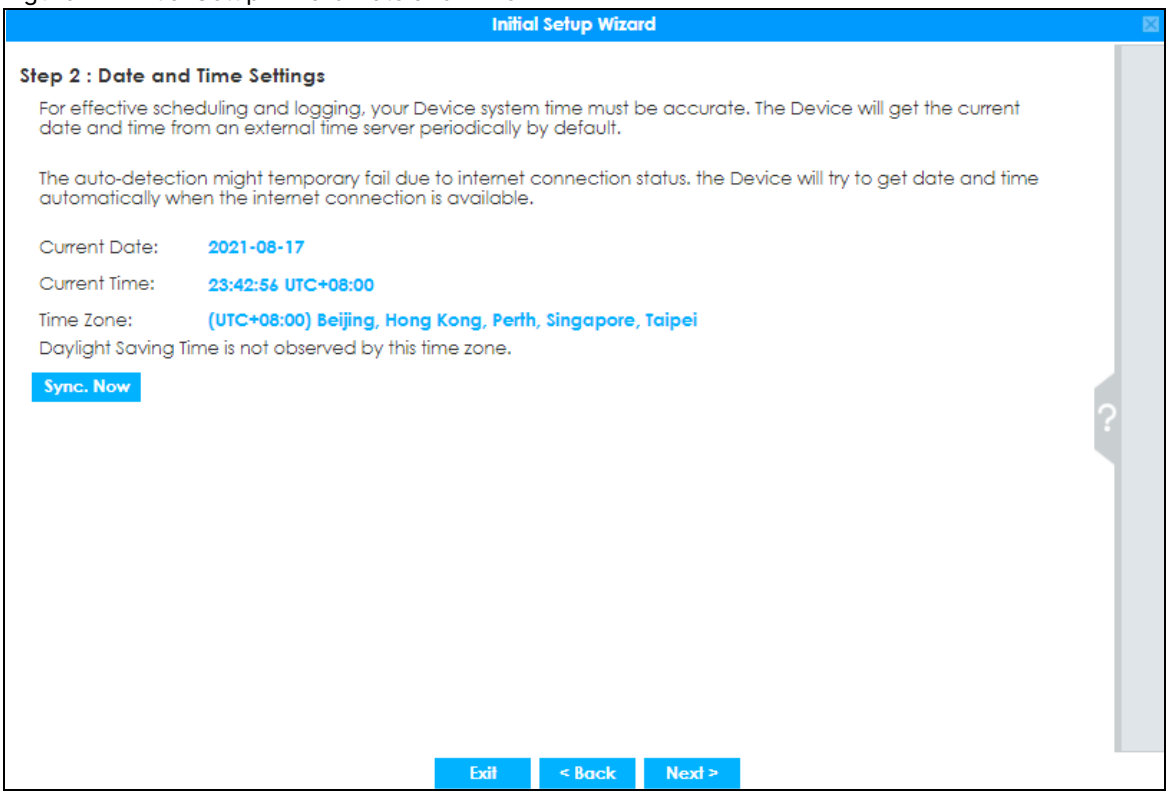
Your Zyxel Device was not able to obtain an IP address. Check that your Internet access information uses DHCP as the WAN connection type. If it fails again, check with your Internet service provider for correct WAN settings and user credentials.

Ethernet Fixed IP Error

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 address exactly as given. If it fails again, check with your Internet service provider for correct IP address, subnet mask and gateway address and other WAN settings.

5.2.3 Initial Setup Wizard - Date and Time

Figure 74 Initial Setup Wizard Date and Time



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 Synch Now.

5.2.4 Initial Setup Wizard - Register Device

Figure 75 Initial Setup Wizard Non-Registered Device

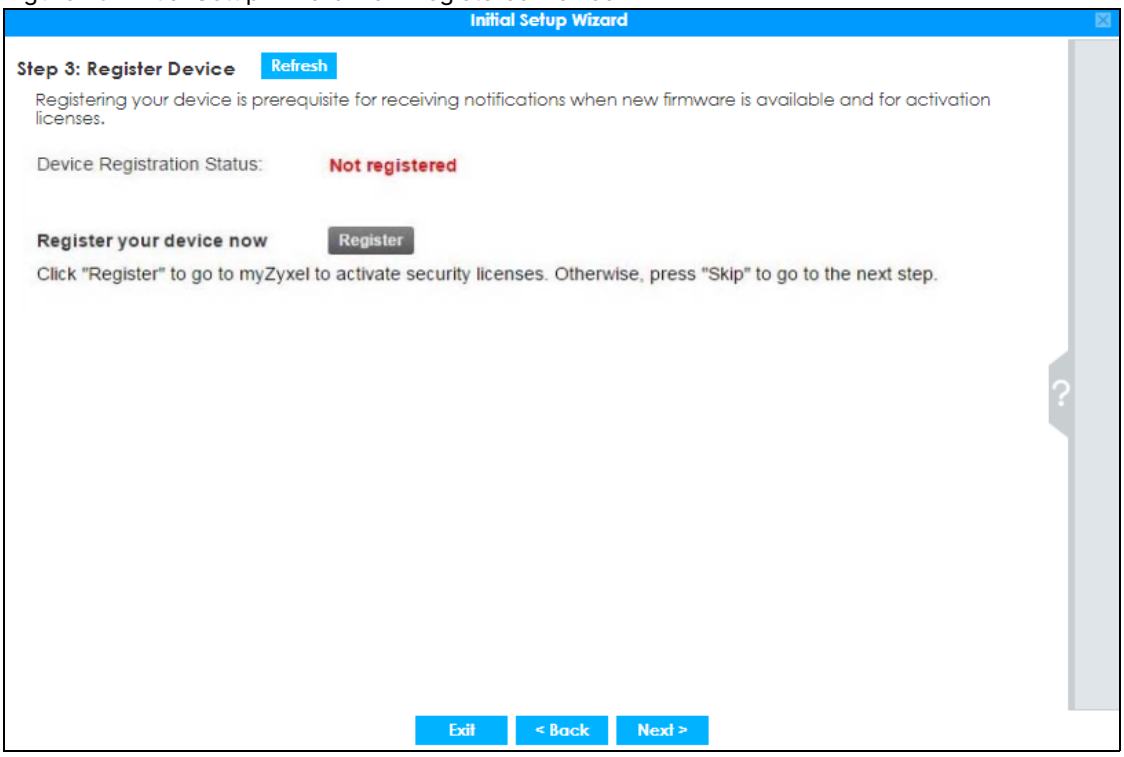
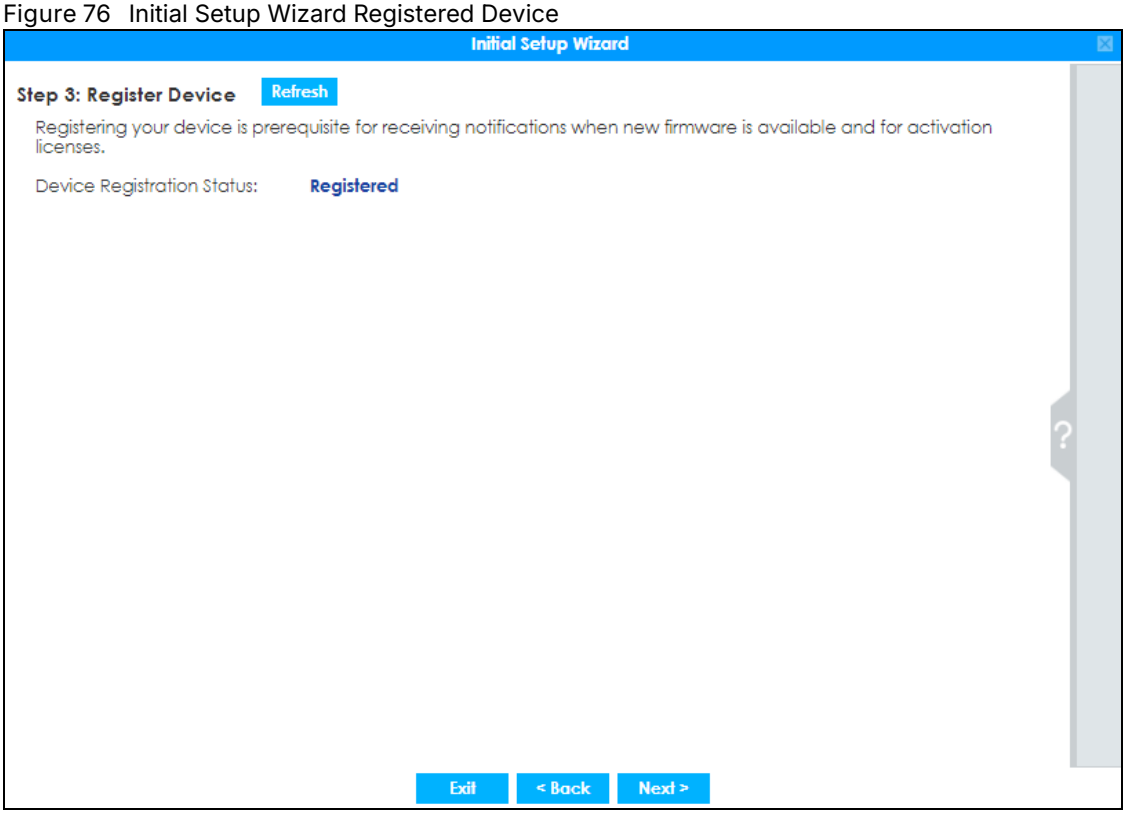


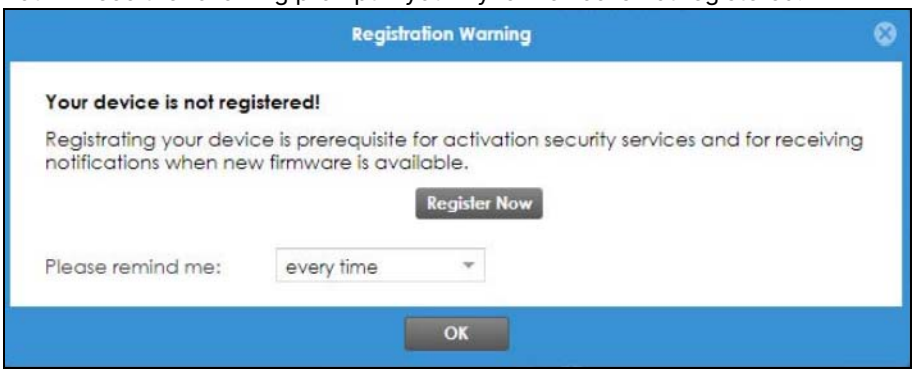
Figure 76 Initial Setup Wizard Registered Device



- 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, you may skip registering your Zyxel Device and activating the corresponding service at myZyxel. However, it is highly recommended to at least register your Zyxel Device.

You will see the following prompt if your Zyxel Device is not registered.



Click the Register button in this screen to register your device at portal.myzyxel.com. You need to create a myZyxel account at portal.myzyxel.com before you can register your device and activate the services at myZyxel.

When registering the Zyxel Device at myZyxel, if you are prompted for the Zyxel Device's serial number and LAN MAC address, see the label at the back of the Zyxel Device's.

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

5.2.5 Initial Setup Wizard - Activate Services

Figure 77 Initial Setup Wizard Non-Activated Services

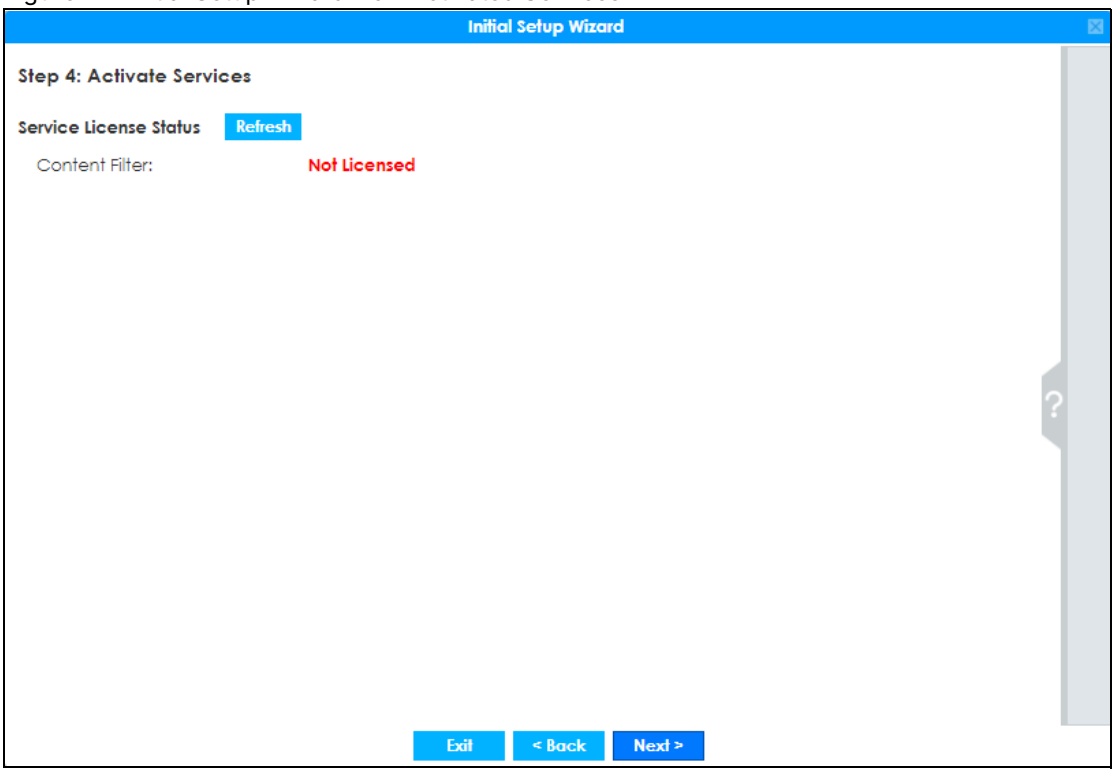
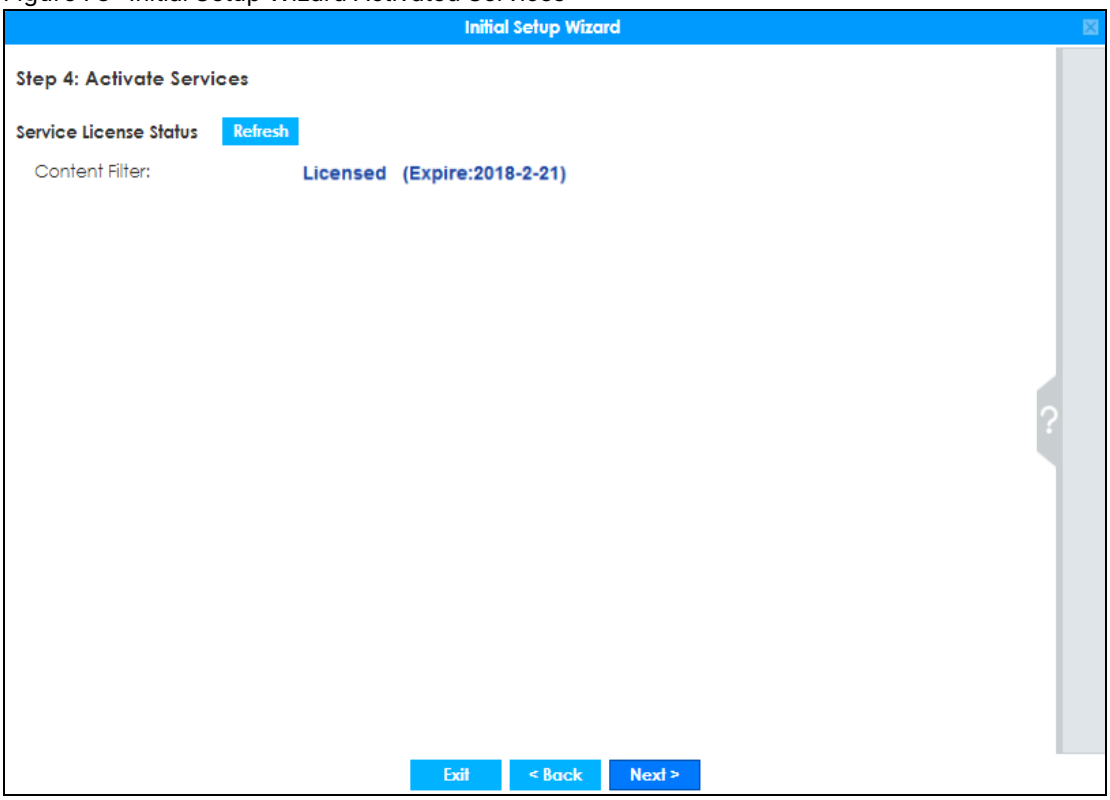


Figure 78 Initial Setup Wizard Activated Services



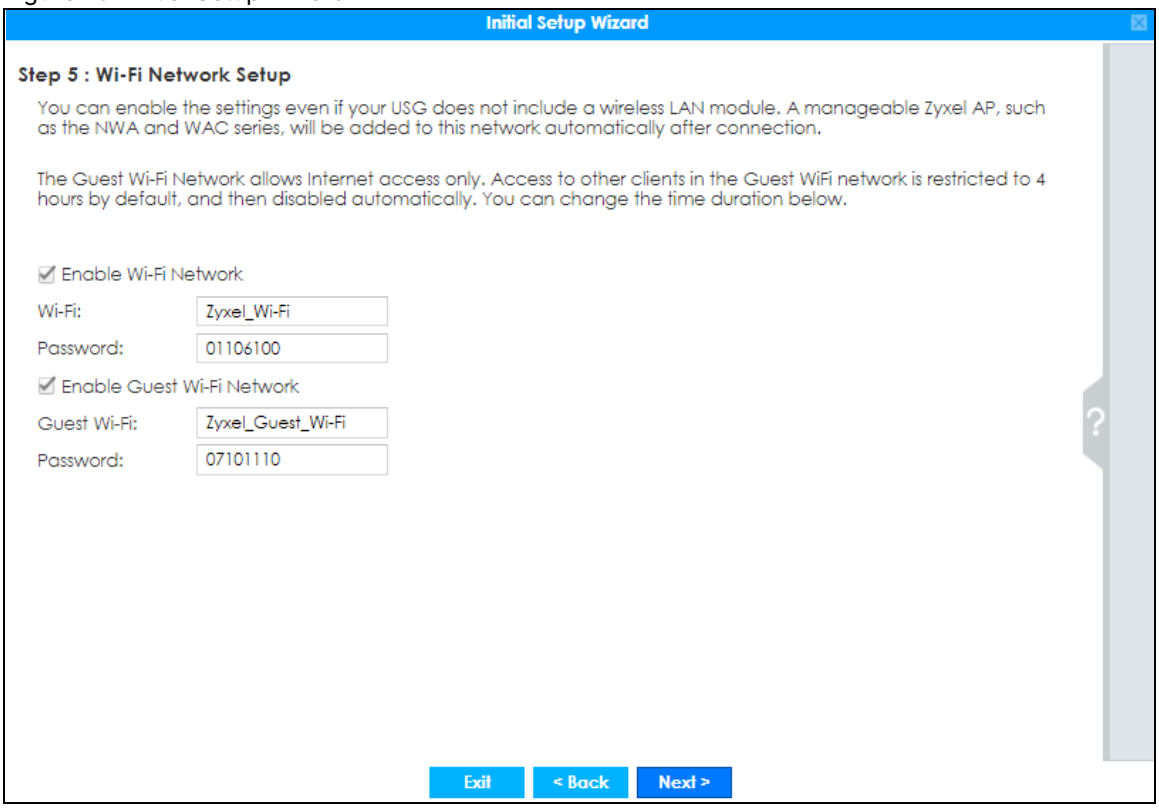
After you register your Zyxel Device, you can activate the services supported by your model if you have service licenses. Examples of services are:

- Content Filter (to block websites by category, such as Gambling)
- IDP (to recognize and drop traffic with Intrusion, Detection & Protection attack patterns)
- Anti-Virus (to detect virus patterns in files)
- Anti-Spam (to mark or discard unsolicited commercial or junk e-mail suspect of being sent by spammers).

Click Refresh and wait a few moments for the service 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.

5.2.6 Initial Setup Wizard - Wi-Fi

Figure 79 Initial Setup Wizard Wi-Fi



Select Enable Wi-Fi Network if you want wireless devices to be able to wirelessly access the Zyxel Device and all resources connected to the Zyxel Device. Configure a descriptive name of from 1 to 32 alpha-numeric characters, hyphens or underscores (a-z A-Z 0-9 -_) for the wireless network name (Wi-Fi). Set a Password of between 8 and 63 printable ASCII characters (including spaces and symbols) or 64 hexadecimal characters (0-9 a-f) that wireless users will have to enter for access to the Zyxel Device wireless network.

Note: You must change the Password to continue.

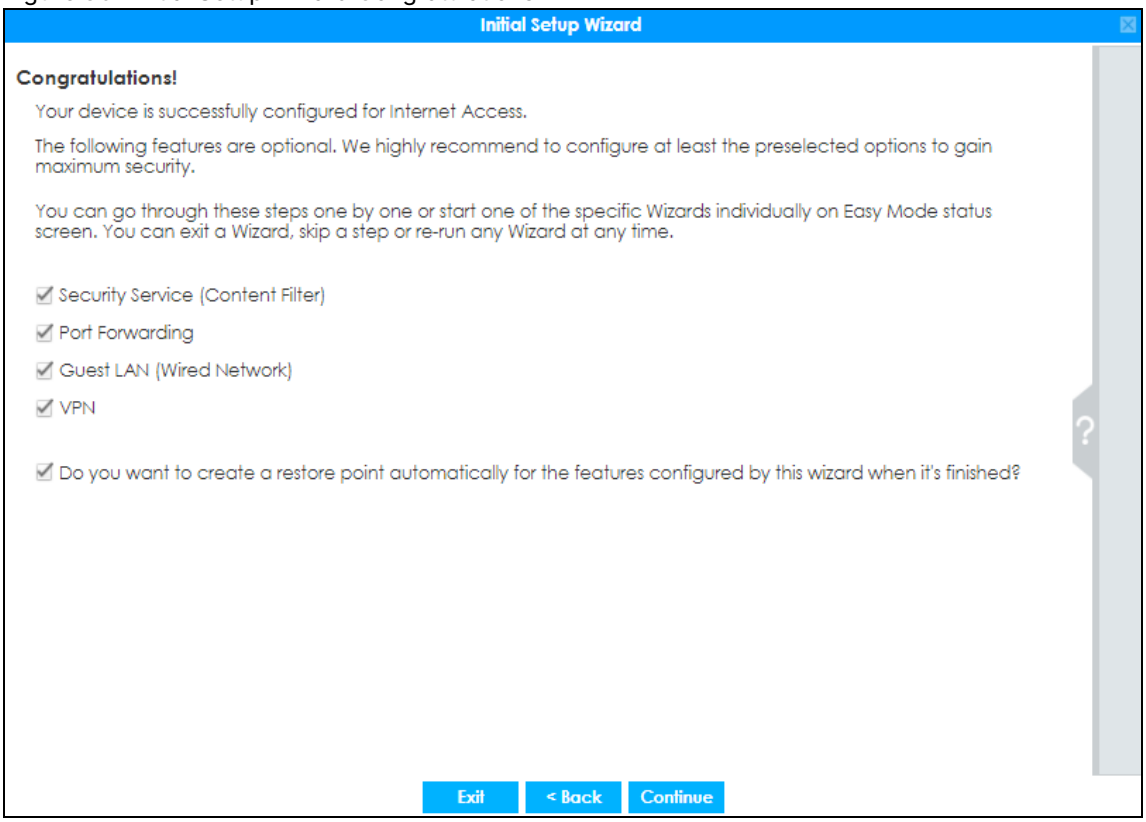
Select Enable Guest Wi-Fi Network if you want wireless devices to only be able to wirelessly access the Internet through the Zyxel Device for up to 4 hours. Configure a descriptive name of from 1 to 32 alpha-numeric characters, hyphens or underscores (a-z A-Z 0-9 -_) for the wireless network name (Wi-Fi). Set a Password of between 8 and 63 printable ASCII characters (including spaces and symbols) or 64 hexadecimal characters (0-9 a-f) that wireless users will have to enter for access to the Zyxel Device Guest wireless network.

The Guest Wi-Fi Network allows Internet access only for up to 4 hours by default. Log in again if the time has elapsed. You can change the default time for Guest Wi-Fi access in the Wi-Fi and Guest Wizard.

The Zyxel Device uses WPA2-PSK with AES encryption so wireless clients must be able to support AES encryption to wirelessly connect to the Zyxel Device using WPA2-PSK.

5.2.7 Initial Setup Wizard - Congratulations

Figure 80 Initial Setup Wizard Congratulations



This screen shows if your Internet access is successfully configured. You can save changes and exit the Initial Wizard here by clearing Security Service, Port Forwarding, Guest LAN and VPN service selections and clicking Finish. Alternatively, select desired security services to continue configuring them as part of the Initial Wizard (Finish becomes Continue). If you want to configure these services later you can access them from the tabs in the dashboard.

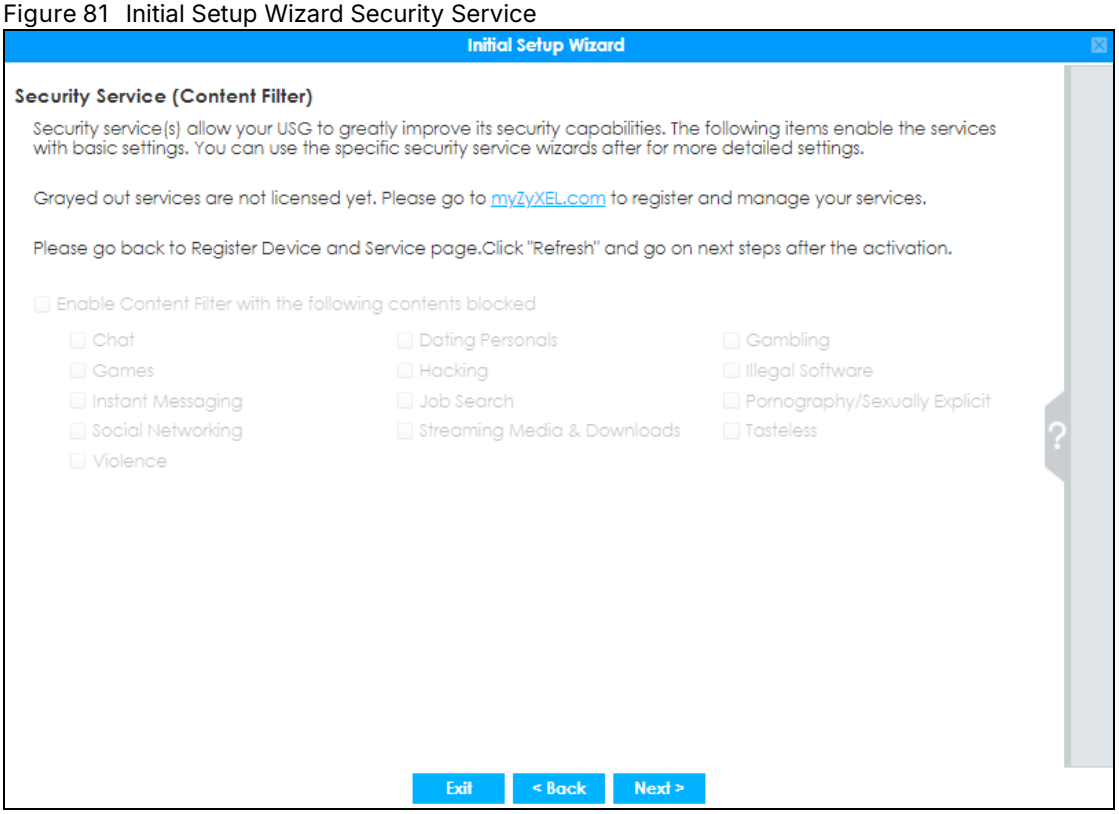
Select from the following to continue configuring in this screen:

- Security Service (Content Filter, IDP, Anti Virus) to configure subscriptions for these services
- Port Forwarding to set up a server in your network that people outside the network can access
- Guest LAN (Wired Network) to set up a guest network where users can access the Internet only from a wired connection to the OPT port for a limited time
- VPN for a site-to-site tunnel between Zyxel Device networks, a tunnel from a remote client using the Zyxel client VPN software to the Zyxel Device network, or a tunnel from a remote client using other VPN software to the Zyxel Device network.

A restore point is a recovery point where you can reset the Zyxel Device's configuration to if you have problems later.

5.3 Initial Setup Wizard - Security Service

Figure 81 Initial Setup Wizard Security Service



Configure licensed (non-grayed-out) services in this screen. After you buy a license for a service, you must activate it at myZyxel. Make sure the Zyxel Device Internet connection is working correctly.

Select Enable Content Filter to block websites by category, such as Chat websites. Note that if you select Chat, the Content Filter blocks chat websites and not chat apps. Therefore, the Skype app can still be used although the Skype website would be blocked. Select the categories you want to block.

- Chat: Sites that enable web-based exchange of real time messages through chat services or chat rooms. For example, me.sohu.com, blufiles.storage.live.com.
- Dating & Personals: Sites that promote networking for interpersonal relationships such as dating and marriage. Includes sites for match-making, online dating, spousal introduction. For example, www.i-part.com.tw, www.imatchi.com.
- Gambling: Sites that offer or are related to online gambling, lottery, casinos and betting agencies involving chance. For example, www.taiwanlottery.com.tw, www.i-win.com.tw, www.hkjc.com.
- Games: Sites relating to computer or other games, information about game producers, or how to obtain cheat codes. Game-related publication sites. For example, www.gamer.com.tw, www.wowtaiwan.com.tw, tw.lineage.gamania.com.
- Hacking: Sites that promote or give advice about how to gain unauthorized access to proprietary computer systems, for the purpose of stealing information, perpetrating fraud, creating viruses, or committing other illegal activity related to theft of digital information. For example, www.hackbase.com, www.chinahacker.com.
- Illegal Software: Sites that illegally distribute software or copyrighted materials such as movies or music, software cracks, illicit serial numbers, illegal license key generators. For example, www.zhaokey.com.cn, www.tiansha.net.

- Instant Messaging: Sites that enable logging in to instant messaging services such as ICQ, AOL Instant Messenger, IRC, MSN, Jabber, Yahoo Messenger, and the like. For example, www.meebo.com, www.aim.com, www. ebuddy.com.
- Job Search: Sites containing job listings, career information, assistance with job searches (such as resume writing, interviewing tips, etc.), employment agencies or head hunters. For example, www.104.com.tw, www.1111.com.tw, www.yes123.com.tw.
- Pornography/Sexually Explicit: Sites that contain explicit sexual content. Includes adult products such as sex toys, CD-ROMs, and videos, adult services such as videoconferencing, escort services, and strip clubs, erotic stories and textual descriptions of sexual acts. For example, www.dvd888.com, www.18center.com, blog.sina.com.tw.
- Social Networking: Sites that enable social networking for online communities of various topics, for friendship, dating, or professional reasons. For example, www.facebook.com, www.flickr.com, www.groups.google.com.
- Streaming Media & Downloads: Sites that deliver streaming content, such as Internet radio, Internet TV or MP3 and live or archived media download sites. Includes fan sites, or official sites run by musicians, bands, or record labels. For example, www.youtube.com, pfp.sina.com.cn, my.xunlei.com.
- Tasteless: Sites with offensive or tasteless content such as bathroom humor or profanity. For example, comedycentral.com, dilbert.com.
- Violence: Sites that contain images or text depicting or advocating physical assault against humans, animals, or institutions. Sites of a particularly gruesome nature such as shocking depictions of blood or wounds, or cruel animal treatment. For example, crimescene.com, deathnet.com, michiganmilitia.com.

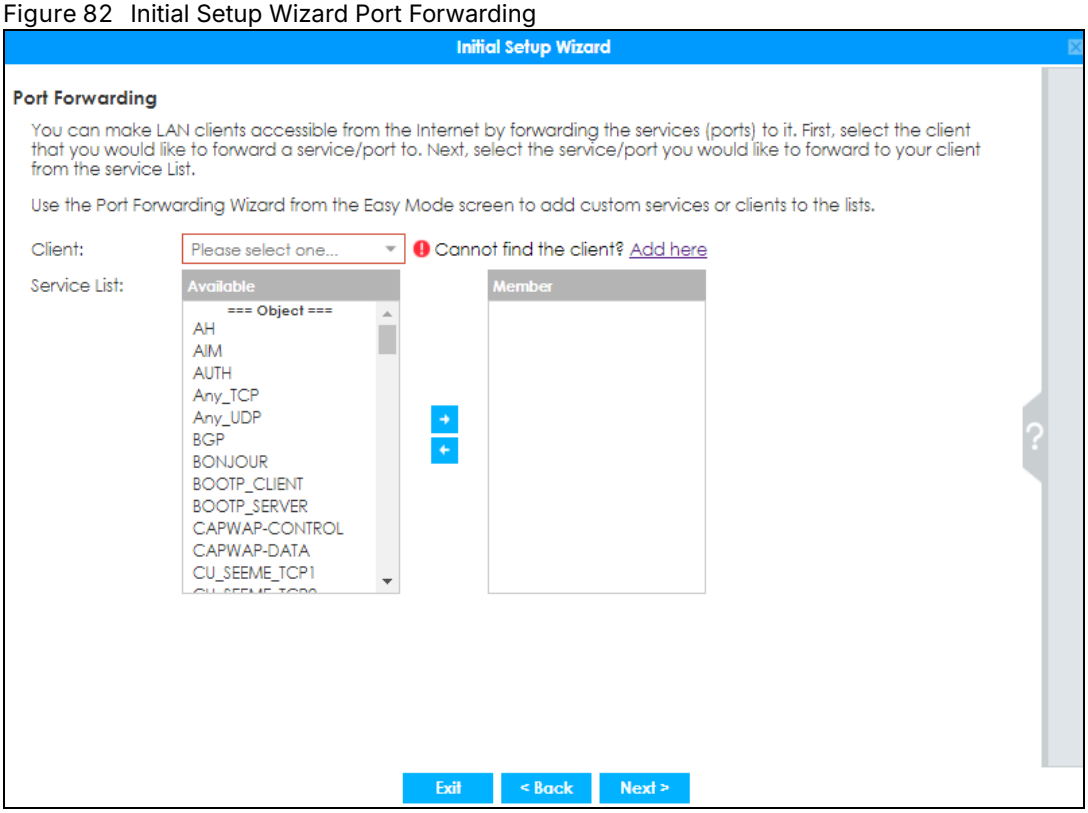
Select Enable IDP to drop traffic with recognized Intrusion, Detection & Protection attack patterns.

Select Enable Anti-Virus to detect virus patterns in files.

Use the Security Service Wizard if you need more detailed settings. Grayed-out services are not licensed yet. Please go to portal.myzyxel.com to register and manage your services.

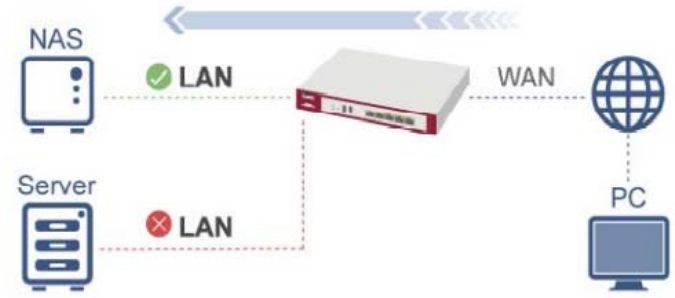
5.4 Initial Setup Wizard - Port Forwarding

Figure 82 Initial Setup Wizard Port Forwarding



NAT port forwarding allows the Zyxel Device to direct incoming traffic from the Internet to the correct virtual server in your network. For example, if you have a NAS server in your network that you or other people need access to from outside your network, select the IP address of the NAS from Client. Then, select the service(s) that your NAS provides (for example FTP, HTTP, HTTPS) from the Available box and use the right arrow to move each service to the Member box.

Even though the NAS is in your local network receiving the protection of the Zyxel Device, you can still access that NAS using these services from anywhere outside your network.



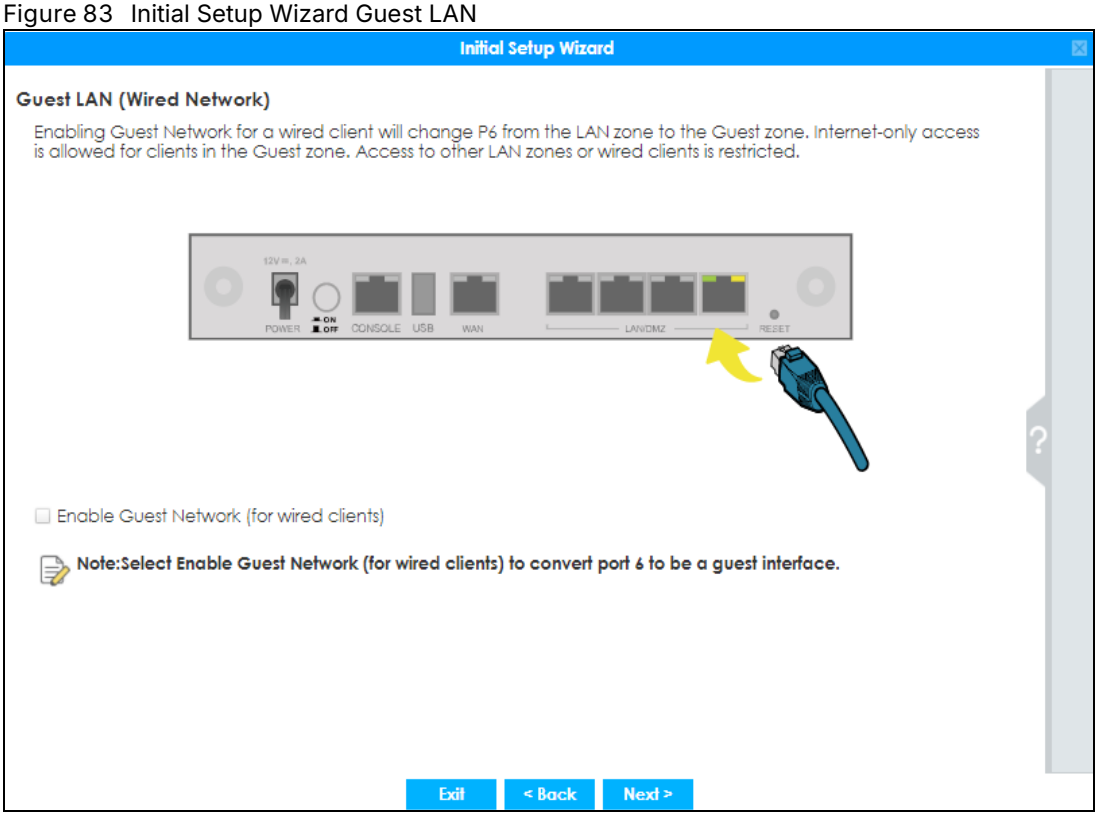
Run the main Port Forwarding Wizard if you cannot see service you need in the list. In that wizard you can define other services.

A client or device in your network acting as a server for forwarded services (for example, the NAS) needs to have a static address. If the client selected does not have a static IP address, the IP address may change when the client reboots, so the Zyxel Device may not be able to find it. If this happens, check for

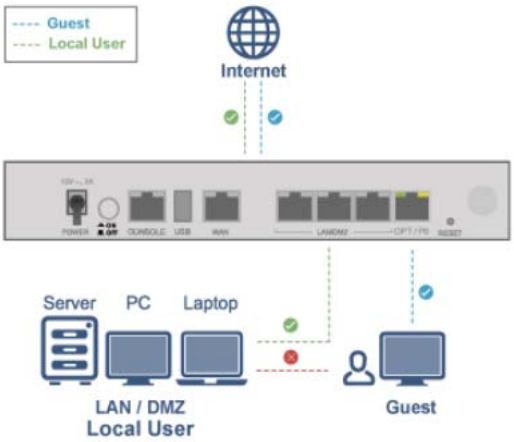
the new IP address of the client. Then add the new IP address by clicking Add here and entering it in the pop-up screen.

5.5 Initial Setup Wizard - Guest LAN

Figure 83 Initial Setup Wizard Guest LAN



Select Enable Guest Network (for wired clients) to convert the OPT or P6 port (depending on your model) to be a guest port and isolate it from the LAN/DMZ ports. Devices connected to the guest port are allowed Internet access only and do not have access to networks connected to the other ports.

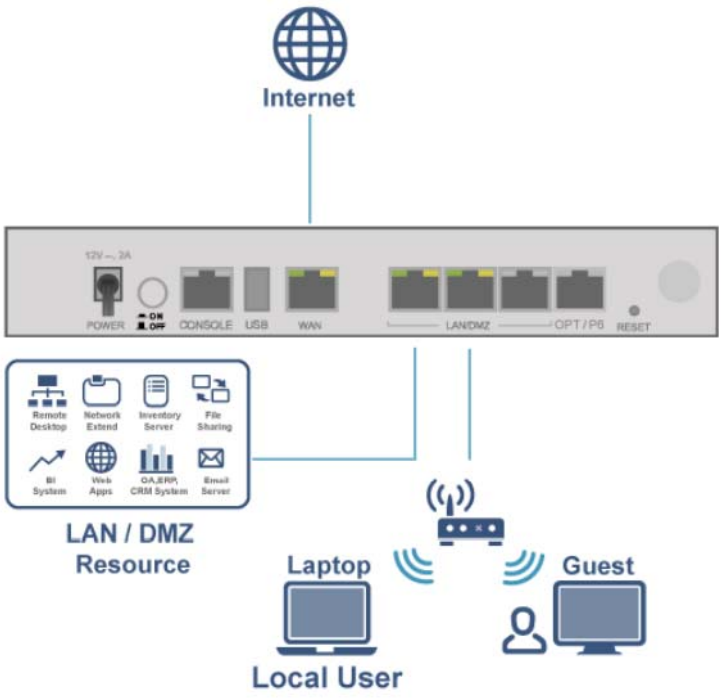


When the OPT or P6 port is not a guest port, then guest devices connected to that port can communicate with all networks, including devices connected to the LAN/DMZ ports. If that is not your intention, make

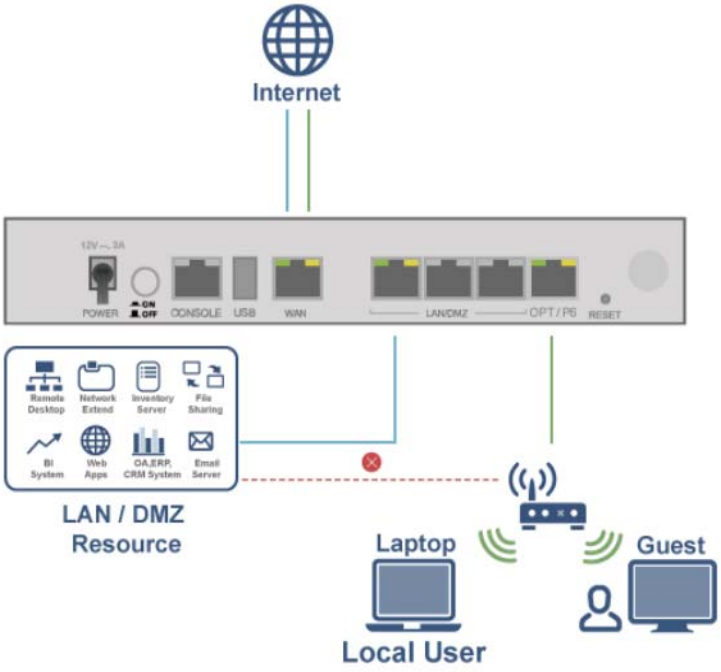
sure Enable Guest Network (for wired clients) is selected and that guest devices are only connected to the OPT or P6 port on the Zyxel Device.

5.5.1 Connecting AP Scenarios

If you connect an AP to a LAN port, then users can use the AP's SSID to wirelessly access all wired resources connected to the LAN ports and Internet access.

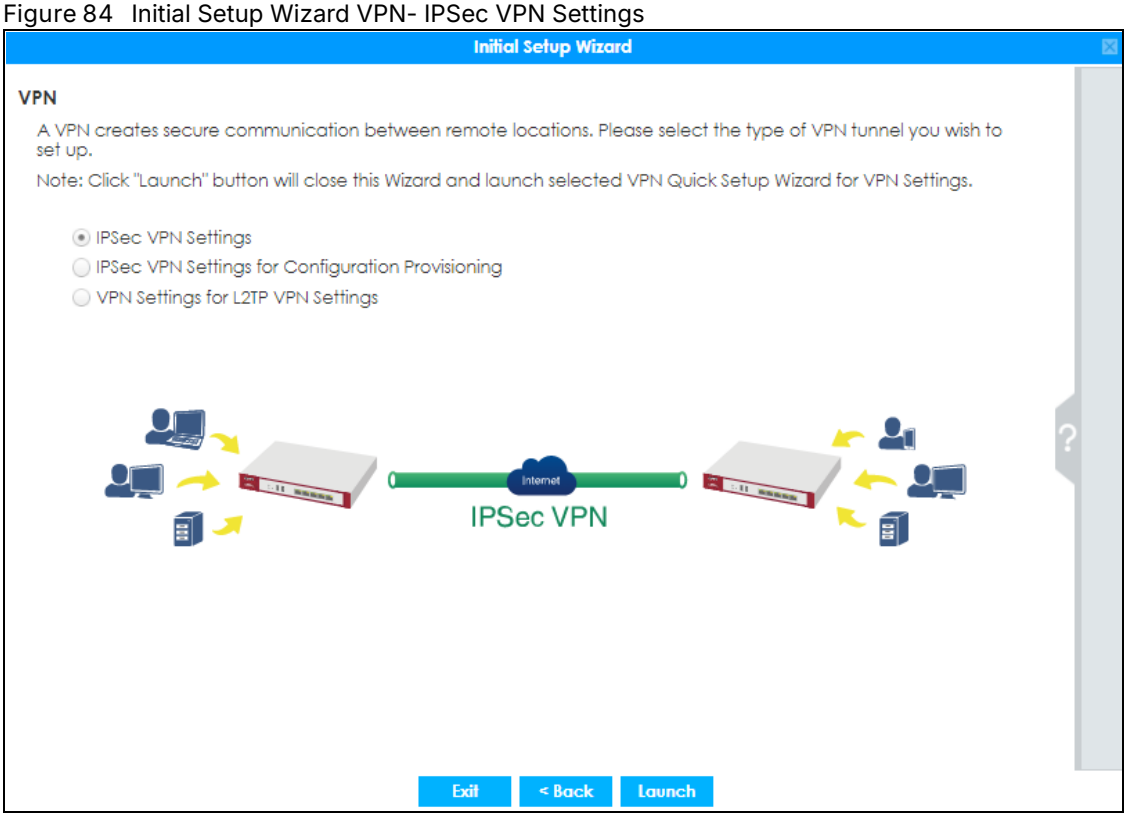


If you connect an AP to the Guest port, then users can use the AP's SSID to wirelessly access all wired resources connected to the Guest port (only) and Internet access. You must select both Enable Guest Wi-Fi Network and Guest LAN (Wired Network).



5.6 Initial Setup Wizard - VPN

Figure 84 Initial Setup Wizard VPN- IPSec VPN Settings



A VPN is a secure, private connection between two end points. An end point could be a VPN gateway like the Zyxel Device itself or a computer with VPN software installed. Select a VPN wizard type and click Launch to begin that wizard and end the Initial Setup Wizard with changes saved. Click Exit to leave the wizard with changes unsaved.

- Select IPSec VPN Settings to create a secure, private connection between two Zyxel Devices. Two networks (sites) behind the Zyxel Devices can then communicate securely with each other.
  Make sure that the settings on both Zyxel Devices are correct and reciprocal. What is a local setting for one should be the equivalent remote setting on the other. Make sure the pre-shared key, negotiation mode, encryption, authentication settings, DH key group and so on are the same on both Zyxel Devices.

  Make sure that both Zyxel Devices are able to communicate with each other. Try pinging one gateway from a computer behind the other.

  Make sure that there is not a firewall blocking VPN traffic in front of one of the Zyxel Devices.
- Select IPSec VPN Settings for Configuration Provisioning to create a secure, private connection between a Zyxel Device and a computer with Zyxel client VPN software installed. See the client VPN software's help to see how to configure it. The computer with client VPN software installed and the Zyxel Device can then communicate securely with each other.
  Make sure the client VPN software is installed and configured correctly on the computer. See the client VPN software's help if anything is unclear.

  Make sure the VPN settings such as the pre-shared key (or certificate), negotiation mode, encryption, authentication settings, DH key group on the computer and the Zyxel Device are correct. Make sure that the client is able to communicate with the Zyxel Device. Try pinging the Zyxel Device from the client.

- Select VPN Settings for L2TP VPN Settings to create a secure, private connection between the Zyxel Device and a computer with L2TP VPN software installed. Many computer operating systems come with L2TP installed. See your computer's help to see how to configure it. The L2TP computer and the Zyxel Device will then communicate securely with each other.

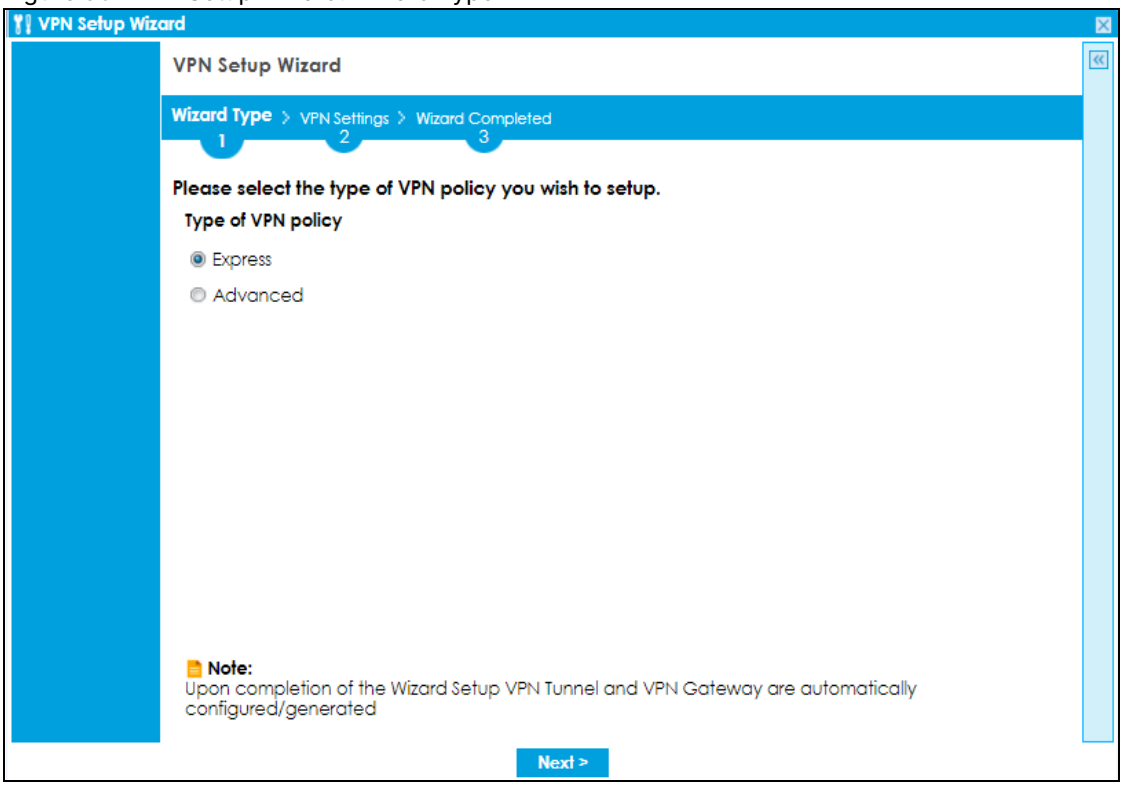
  Make sure that the computer with L2TP is able to communicate with the Zyxel Device. Try pinging the Zyxel Device from the computer. Make sure that L2TP traffic is allowed through the WAN on the Zyxel Device.

5.6.1 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.

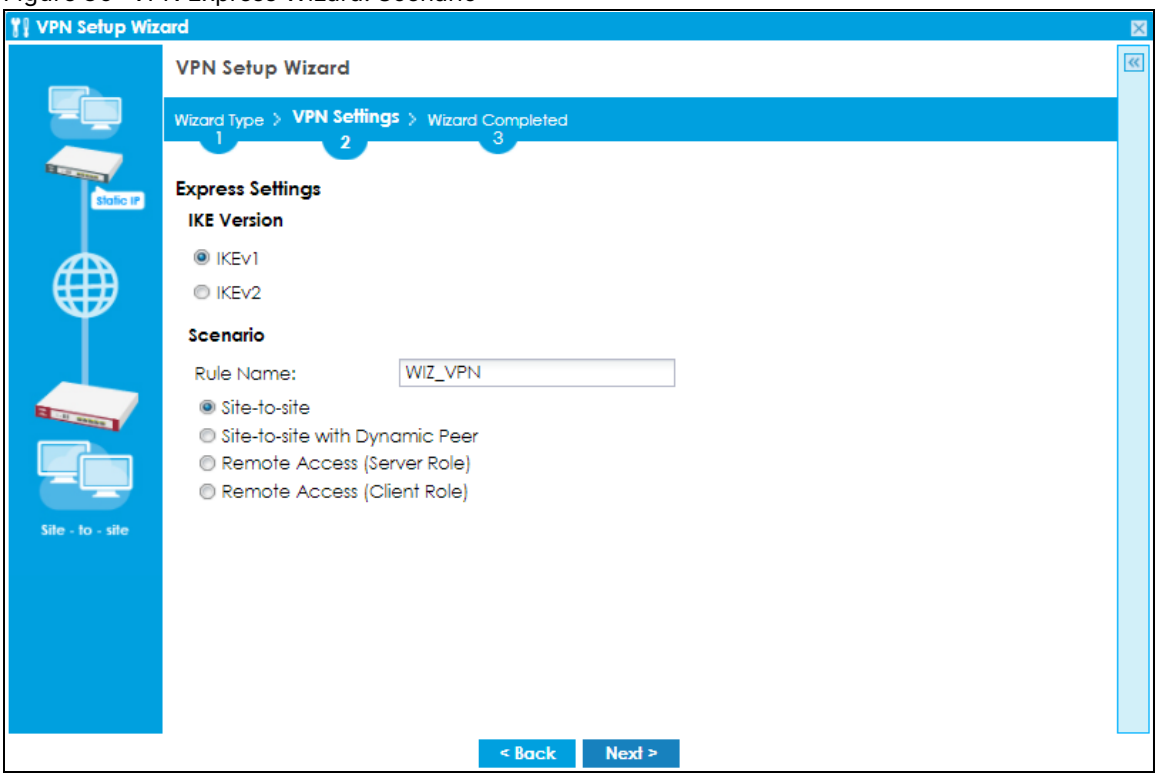
Figure 85 VPN Setup Wizard: Wizard Type



5.6.2 VPN Express Wizard - Scenario

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

Figure 86 VPN Express Wizard: Scenario



IKE (Internet Key Exchange) Version: IKE 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: Enter 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.

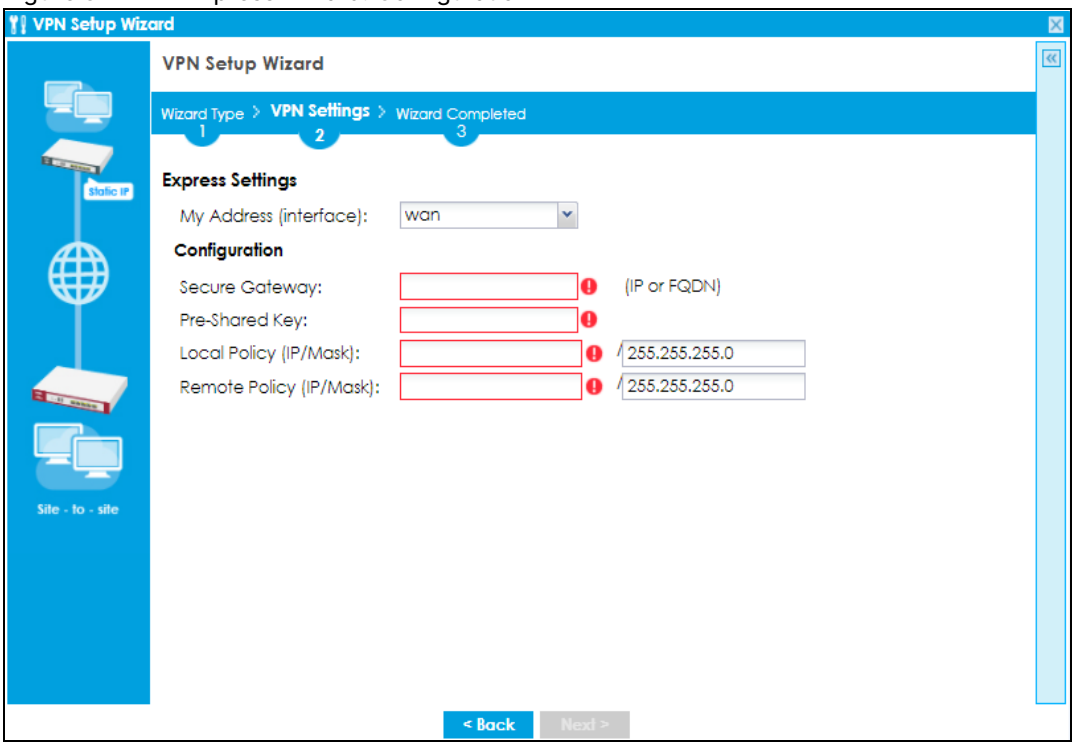
Select the scenario that best describes your intended VPN connection. The figure on the left of the screen changes to match the scenario you select.

SITE-TO-SITE	SITE-TO-SITE WITH DYNAMIC PEER	REMOTE ACCESS (SERVER ROLE)	REMOTE ACCESS (CLIENT ROLE)

- Site-to-site - choose this if the remote IPSec router has a static IP address or a domain name. This Zyxel Device can initiate the VPN tunnel. The remote IPSec router can also initiate the VPN tunnel if this Zyxel Device has a static IP address or a domain name.
- Site-to-site with Dynamic Peer - choose this if the remote IPSec router has a dynamic IP address. You don't specify the remote IPSec router's address, but you specify the remote policy (the addresses of the devices behind the remote IPSec router). This Zyxel Device must have a static IP address or a domain name. Only the remote IPSec router can initiate the VPN tunnel.
- Remote Access (Server Role) - choose this to allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. You don't specify the addresses of the client IPSec routers or the remote policy. This creates a dynamic IPSec VPN rule that can let multiple clients connect. Only the clients can initiate the VPN tunnel.
- Remote Access (Client Role) - choose this to connect to an IPSec server. This Zyxel Device is the client (dial-in user). Client role Zyxel Devices initiate IPSec VPN connections to a server role Zyxel Device. This Zyxel Device can have a dynamic IP address. The IPSec server doesn't configure this Zyxel Device's IP address or the addresses of the devices behind it. Only this Zyxel Device can initiate the VPN tunnel.

5.6.3 VPN Express Wizard - Configuration

Figure 87 VPN Express Wizard: Configuration

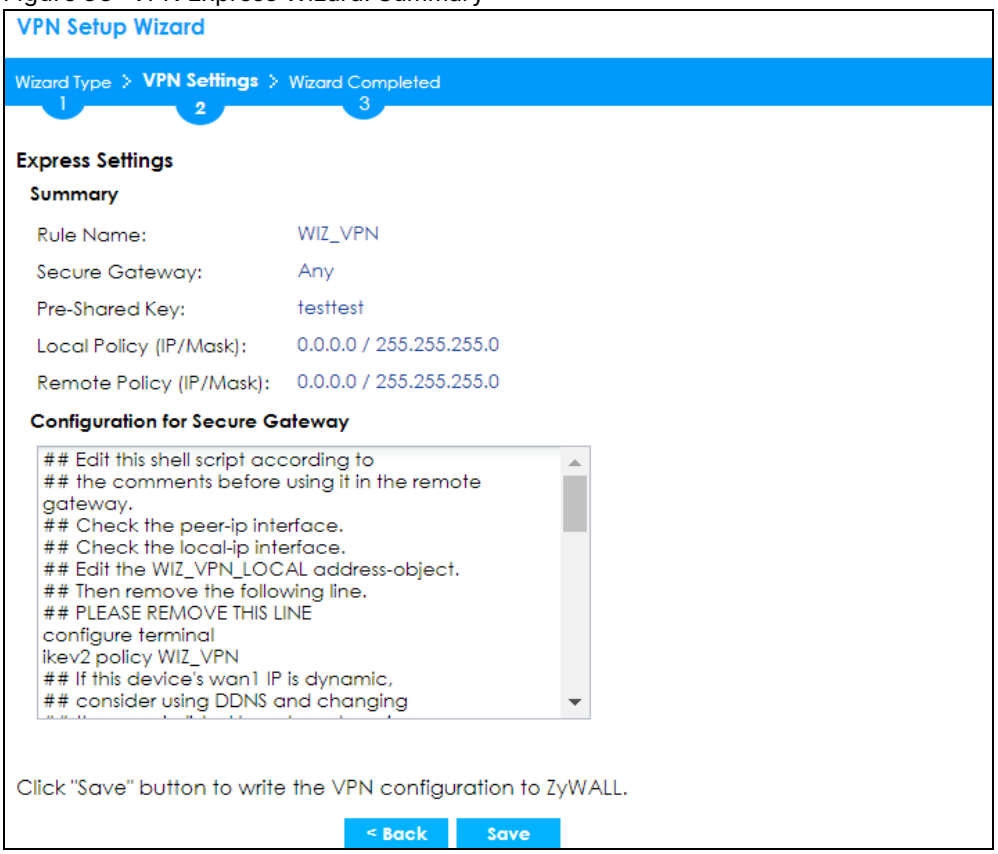


- My Address (interface): Select an interface from the drop-down list box to use on your Zyxel Device.
- Secure Gateway: Any displays in this field if it is not configurable for the chosen scenario. Otherwise, enter the WAN IP address or domain name of the remote IPSec device (secure gateway) to identify 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: Enter the password. Both ends of the VPN tunnel must use the same password. Use up to 128 case-sensitive ASCII characters or up to 128 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): Enter 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, enter the IP address of a computer behind the remote IPSec device. You can also specify a subnet. This must match the local IP address configured on the remote IPSec device.

5.6.4 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 88 VPN Express Wizard: Summary

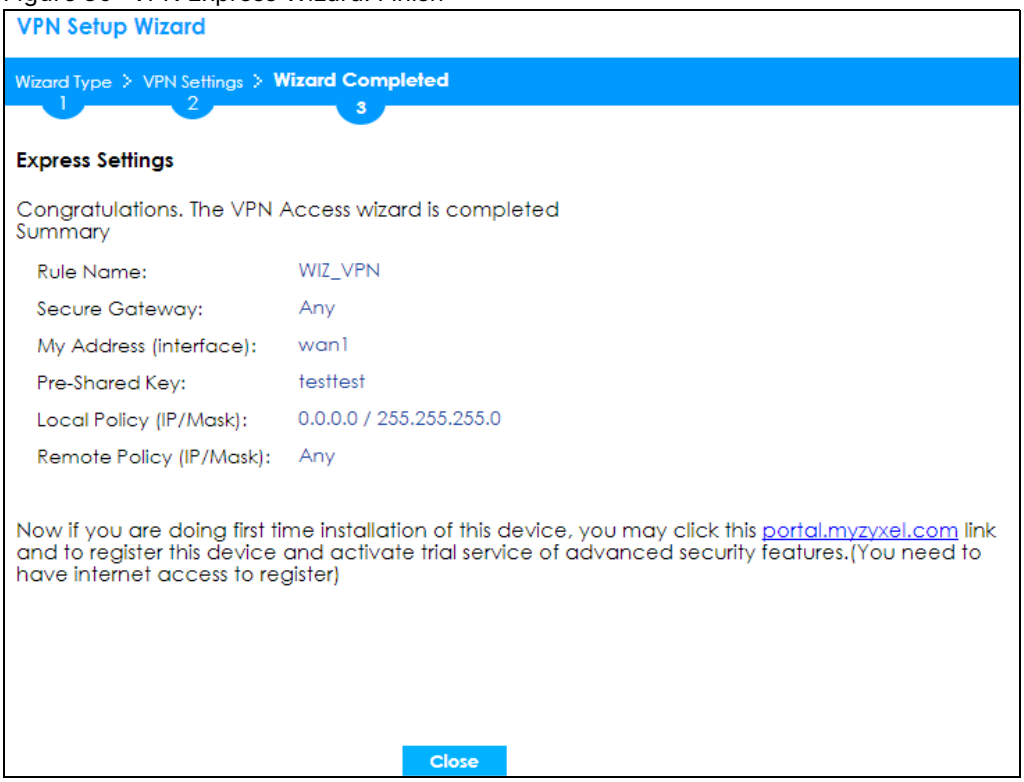


- Rule Name: Identifies the VPN gateway policy.
- Secure Gateway: IP address or domain name of the remote IPSec device. If this field displays Any, only the remote IPSec device can initiate the VPN connection.
- Pre-Shared Key: VPN tunnel password. It identifies a communicating party during a phase 1 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.

5.6.5 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 89 VPN Express Wizard: Finish

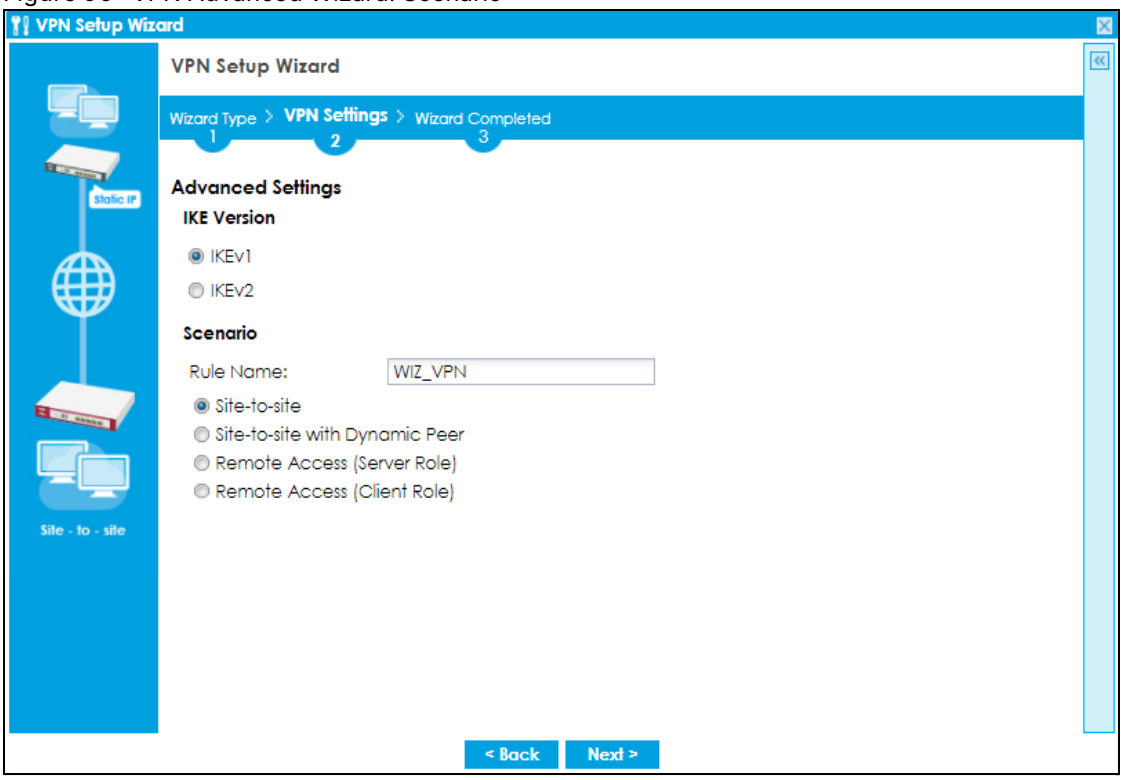


Click Close to exit the wizard.

5.6.6 VPN Advanced Wizard - Scenario

Click the Advanced radio button as shown in Figure 85 on page 115 to display the following screen.

Figure 90 VPN Advanced Wizard: Scenario



IKE (Internet Key Exchange) Version: IKE 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: Enter 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.

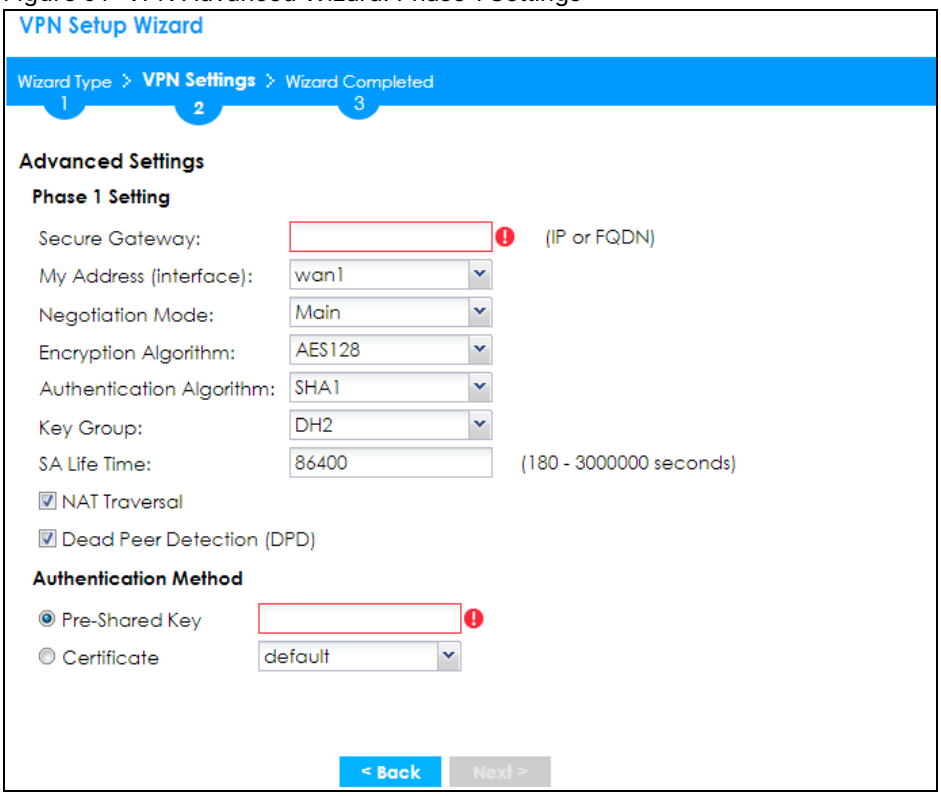
Select the scenario that best describes your intended VPN connection. The figure on the left of the screen changes to match the scenario you select.

- 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.

5.6.7 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 91 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).

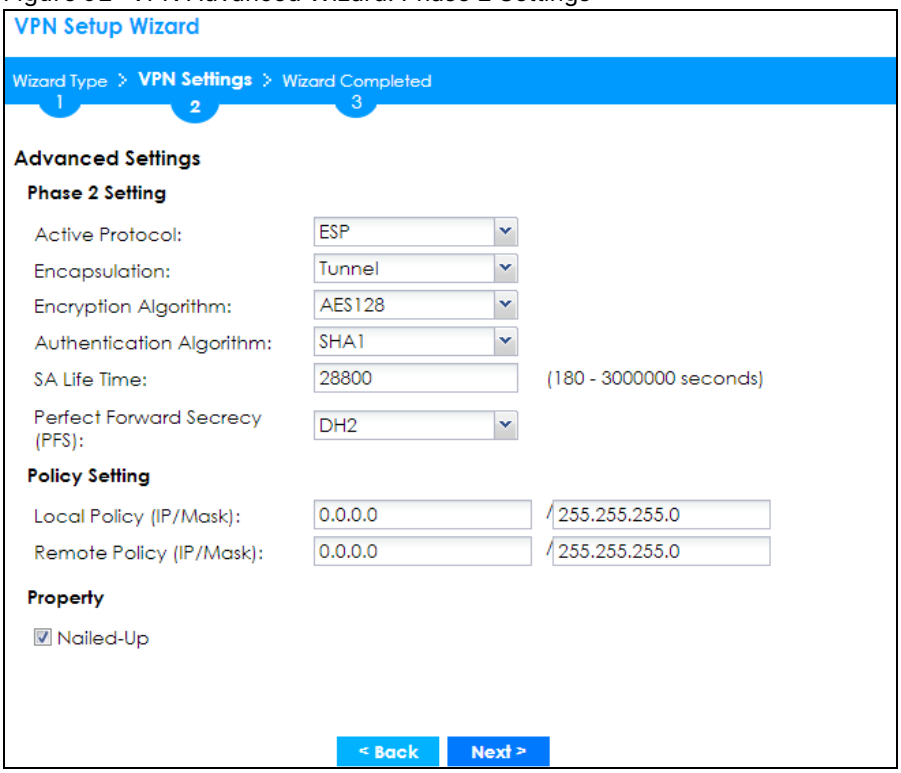
Note: The remote IPSec device must also have NAT traversal enabled. See the help in the main IPSec VPN screens for more information.

- 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.

5.6.8 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 92 VPN Advanced Wizard: Phase 2 Settings



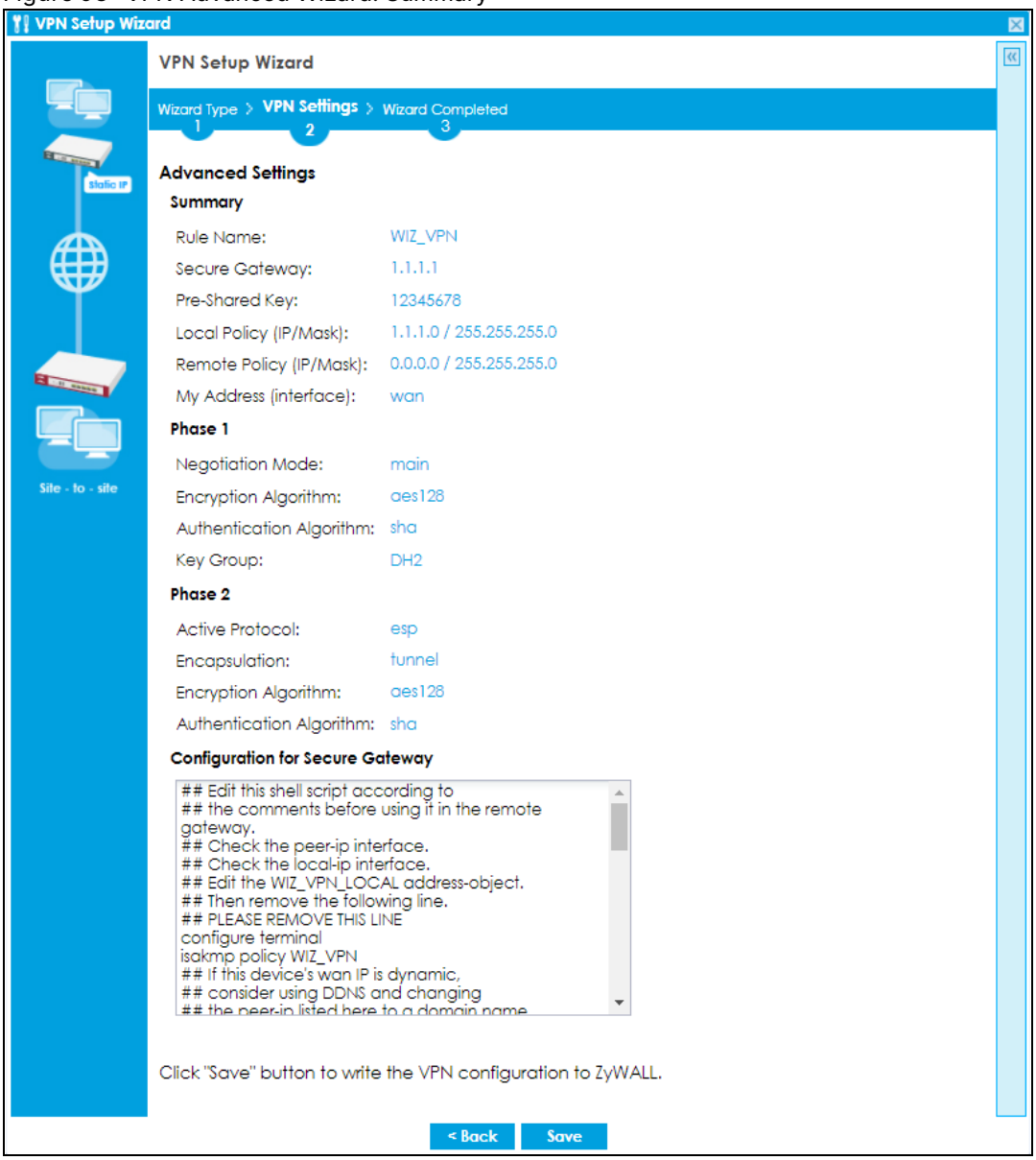
- Active Protocol: ESP is compatible with NAT, AH is not.
- Encapsulation: Tunnel is compatible with NAT, Transport is not.
- Encryption Algorithm: 3DES and AES use encryption. The longer the AES key, the higher the security (this may affect throughput). Null uses no encryption.
- Authentication Algorithm: 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): Enter 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): Enter 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.

5.6.9 VPN Advanced Wizard - Summary

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

Figure 93 VPN Advanced Wizard: Summary

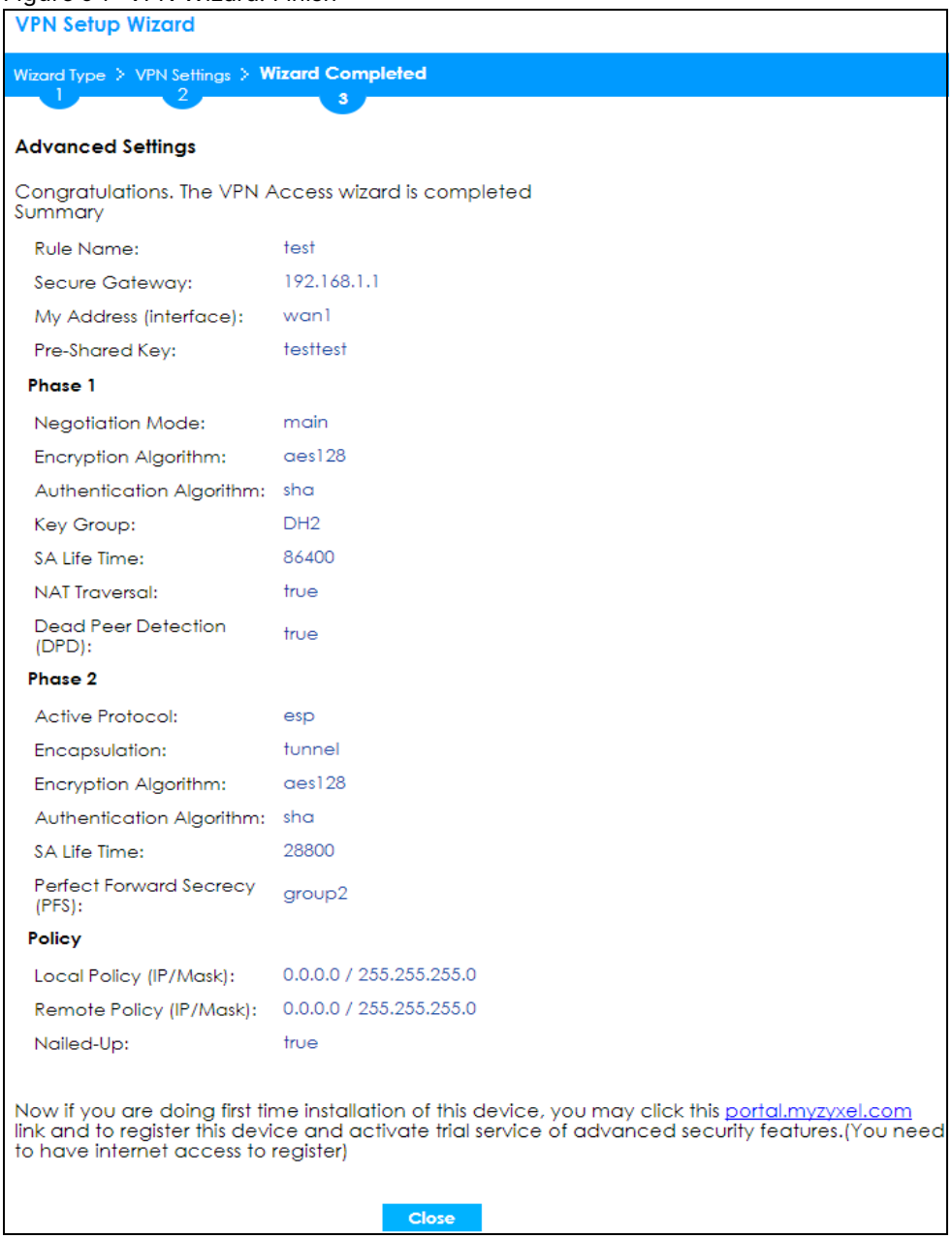


- Rule Name: Identifies the VPN connection (and the VPN gateway).
- Secure Gateway: IP address or domain name of the remote IPSec device.
- Pre-Shared Key: VPN tunnel password.
- Local Policy: IP address and subnet mask of the computers on the network behind your Zyxel Device that can use the tunnel.
- Remote Policy: IP address and subnet mask of the computers on the network behind the remote IPSec device that can use the tunnel.
- 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.

5.6.10 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 94 VPN Wizard: Finish

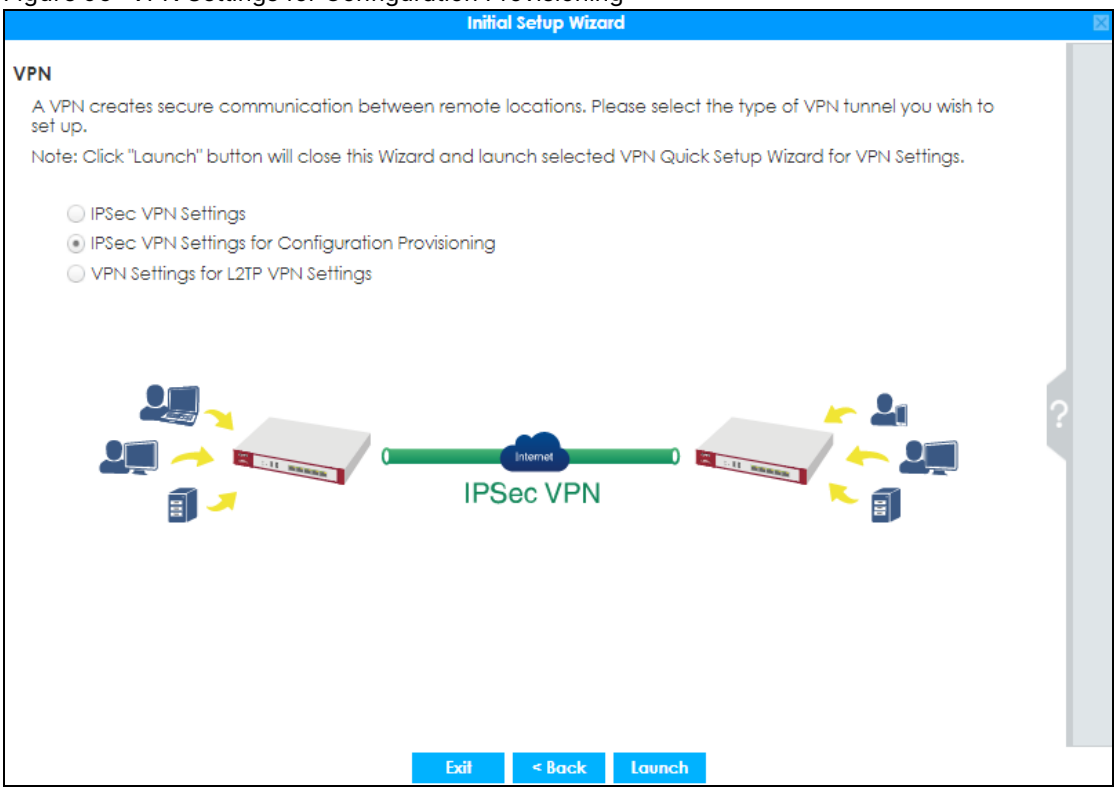


Click Close to exit the wizard.

5.7 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.

Figure 95 VPN Settings for Configuration Provisioning



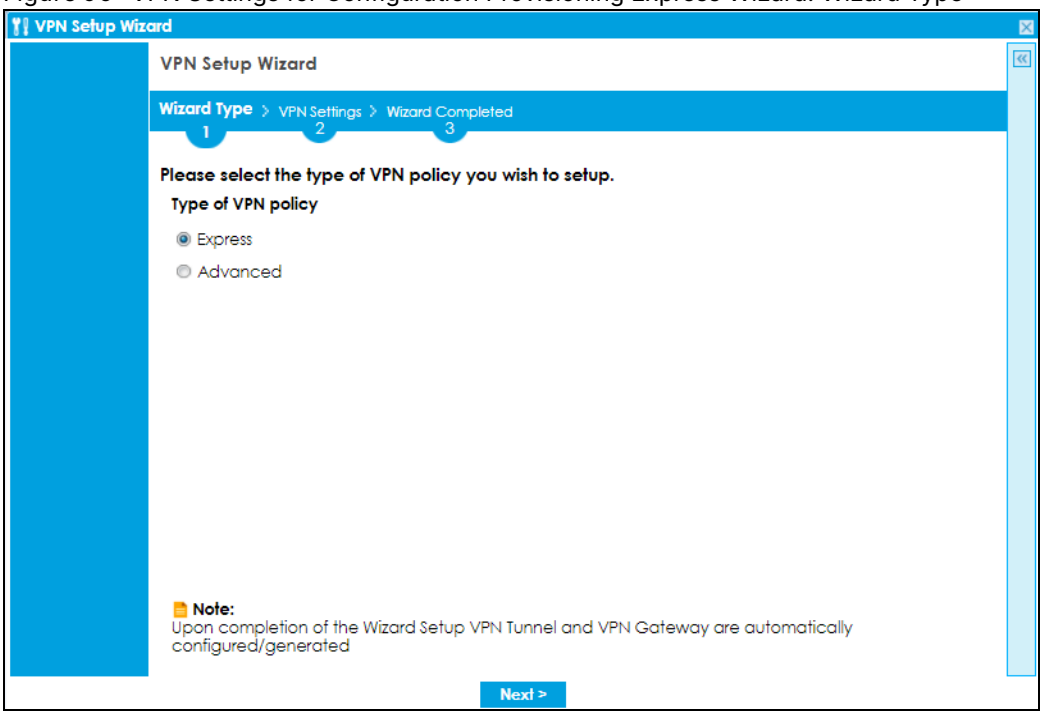
VPN rules for the Zyxel Device IPSec VPN Client have certain restrictions. They must *not* contain the following settings:

- 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.

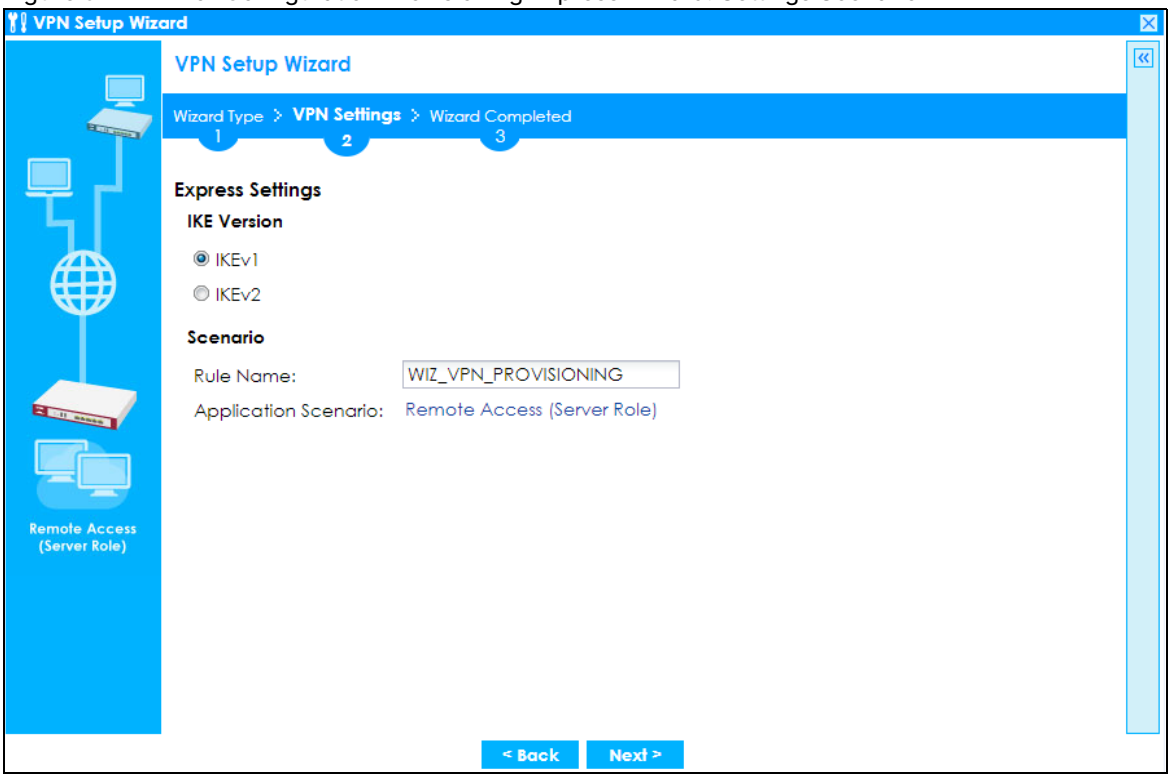
Figure 96 VPN Settings for Configuration Provisioning Express Wizard: Wizard Type



5.7.1 Configuration Provisioning Express Wizard - VPN Settings

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

Figure 97 VPN for Configuration Provisioning Express Wizard: Settings Scenario



IKE (Internet Key Exchange) Version: IKE 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.

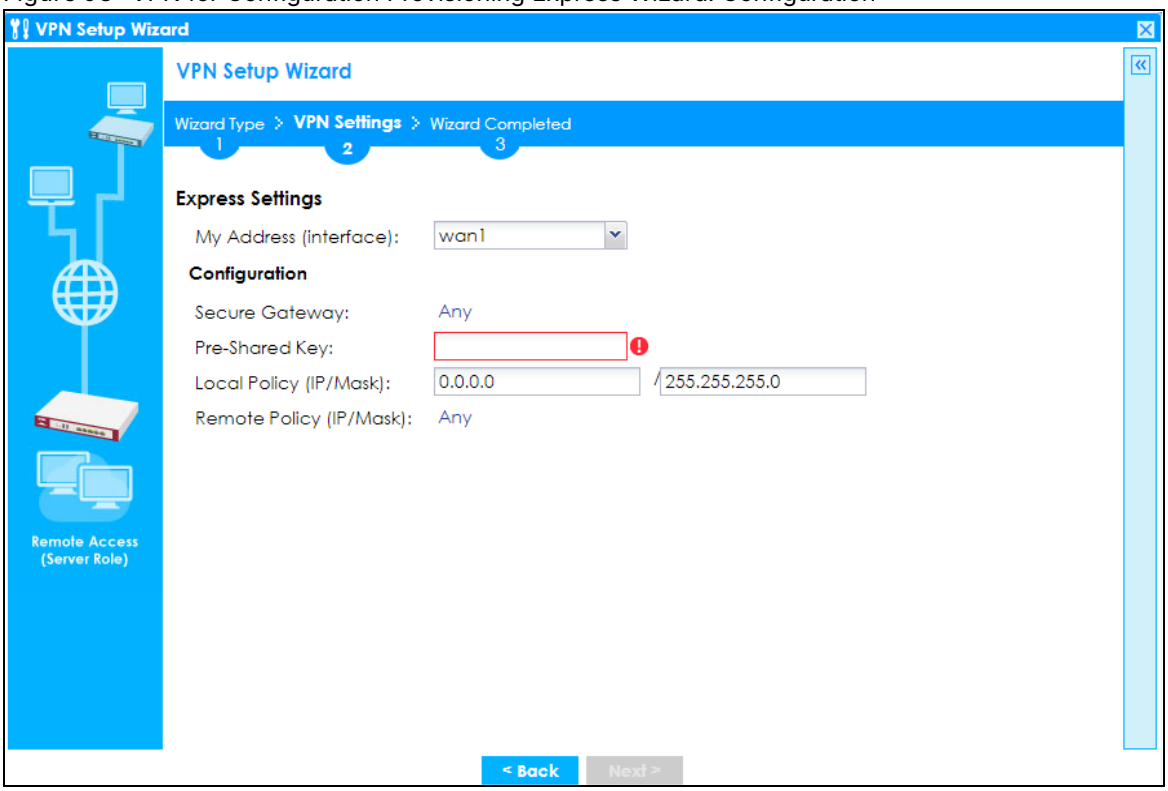
Rule Name: Enter the name used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

Application Scenario: Only the Remote Access (Server Role) is allowed in this wizard. It allows incoming connections from the Zyxel Device IPSec VPN Client.

5.7.2 Configuration Provisioning VPN Express Wizard - Configuration

Click Next to continue the wizard.

Figure 98 VPN for Configuration Provisioning Express Wizard: Configuration



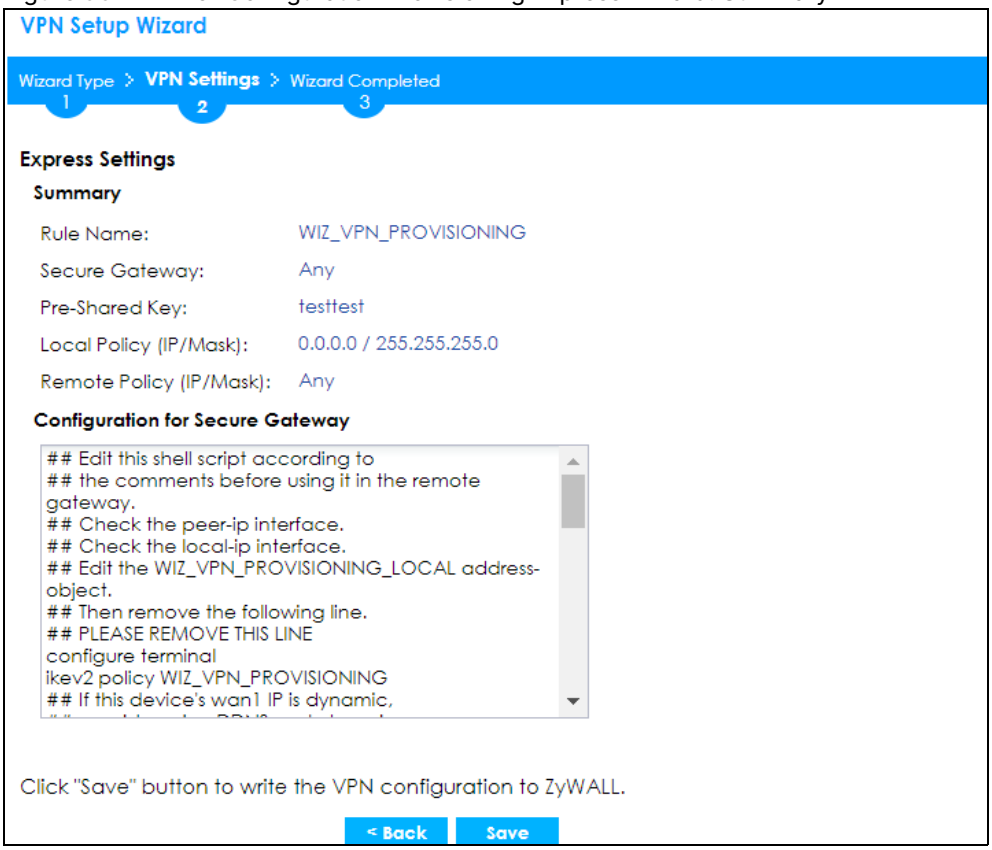
- My Address (interface): Select an interface from the drop-down list box to use on your Zyxel Device.
- Secure Gateway: Any displays in this field because it is not configurable in this wizard. It allows incoming connections from the Zyxel Device IPSec VPN Client.
- Pre-Shared Key: Enter the password. Both ends of the VPN tunnel must use the same password. Use up to 128 case-sensitive ASCII characters or up to 128 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): Enter 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.

5.7.3 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 99 VPN for Configuration Provisioning Express Wizard: Summary

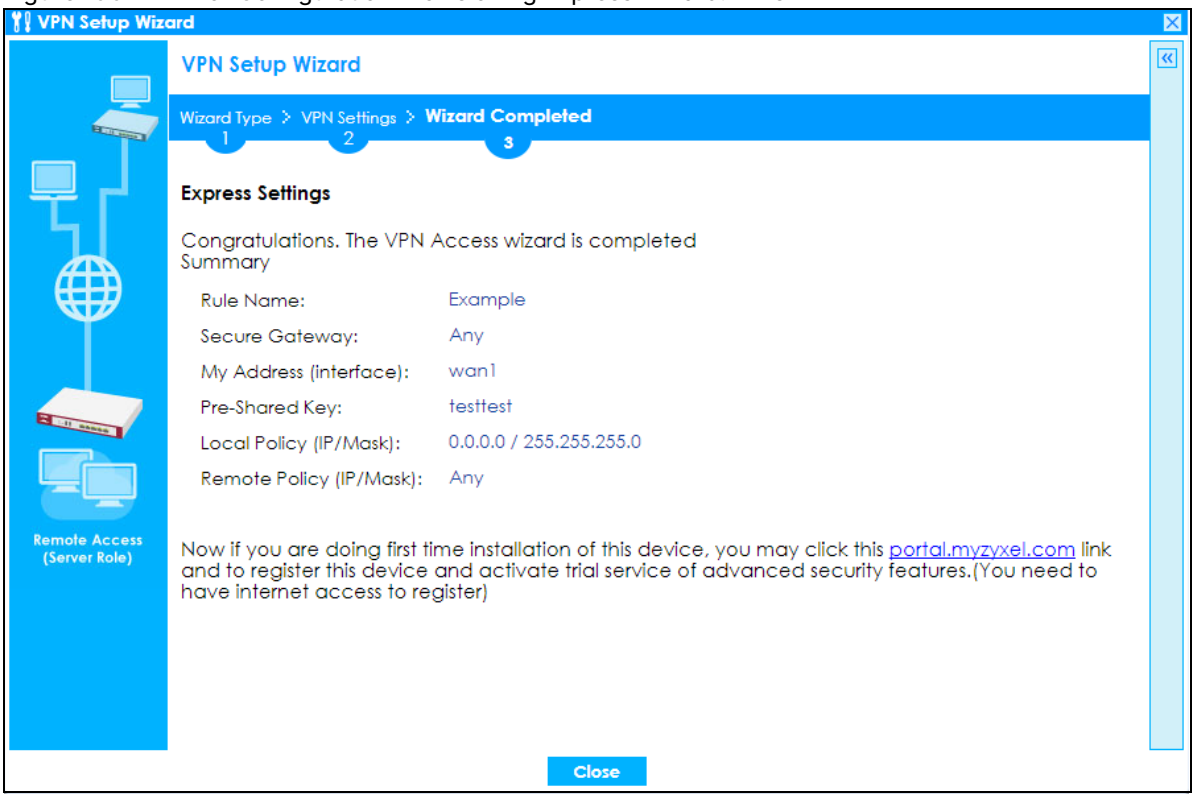


- Rule Name: Identifies the VPN gateway policy.
- Secure Gateway: Any displays in this field because it is not configurable in this wizard. It allows incoming connections from the Zyxel Device IPSec VPN Client.
- Pre-Shared Key: VPN tunnel password. It identifies a communicating party during a phase 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.

5.7.4 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 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 100 VPN for Configuration Provisioning Express Wizard: Finish

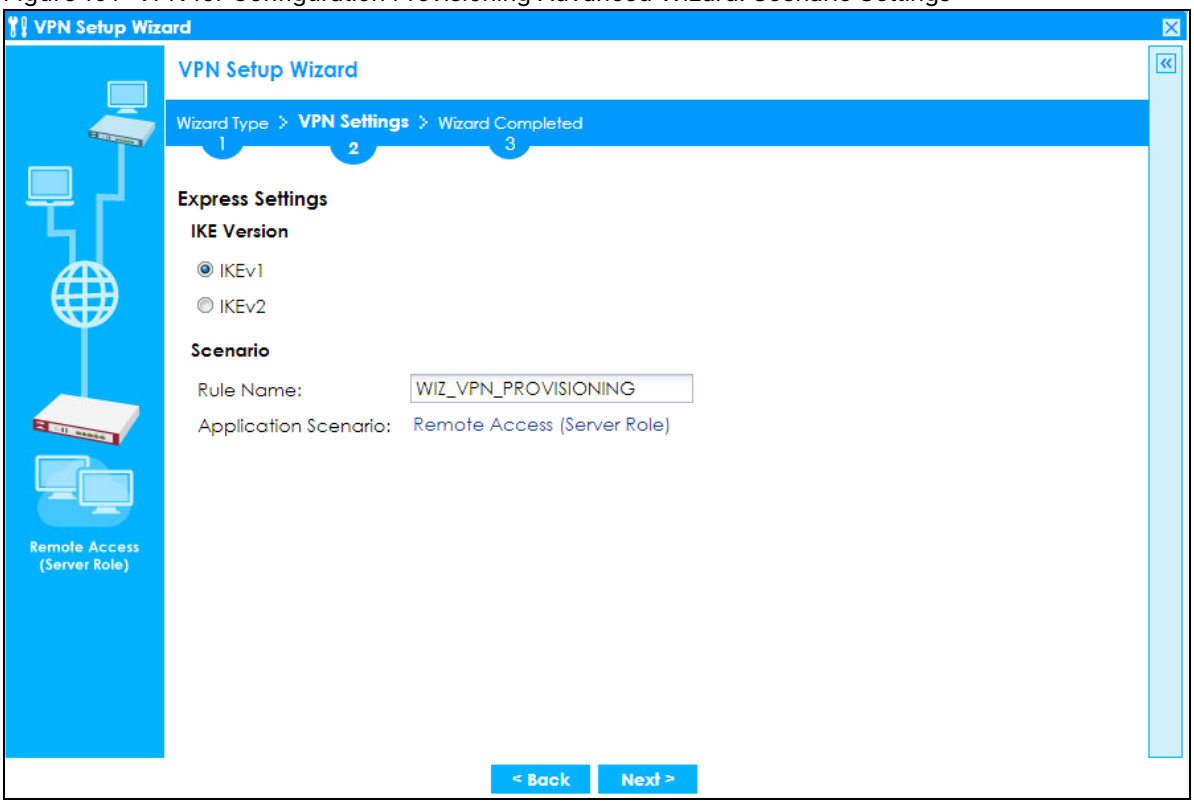


Click Close to exit the wizard.

5.7.5 VPN Settings for Configuration Provisioning Advanced Wizard - Scenario

Click the Advanced radio button as shown in the screen shown in Figure 96 on page 128 to display the following screen.

Figure 101 VPN for Configuration Provisioning Advanced Wizard: Scenario Settings



IKE (Internet Key Exchange) Version: IKE 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: Enter 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.

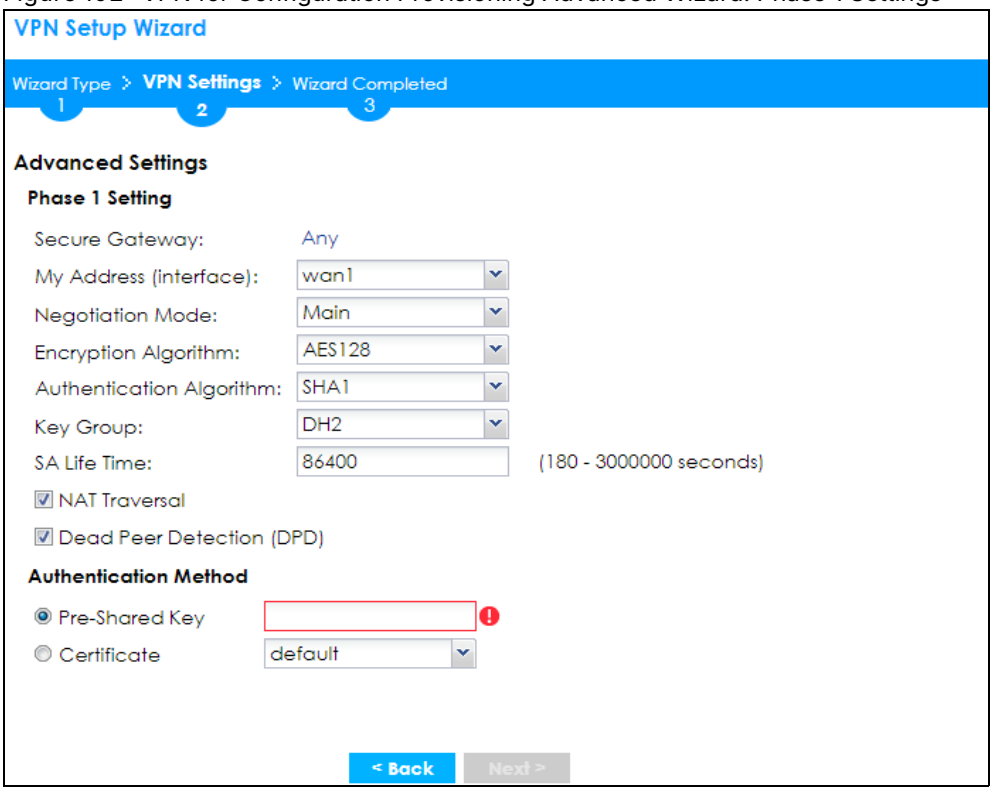
Application Scenario: Only the Remote Access (Server Role) is allowed in this wizard. It allows incoming connections from the Zyxel Device IPSec VPN Client.

Click Next to continue the wizard.

5.7.6 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 102 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.

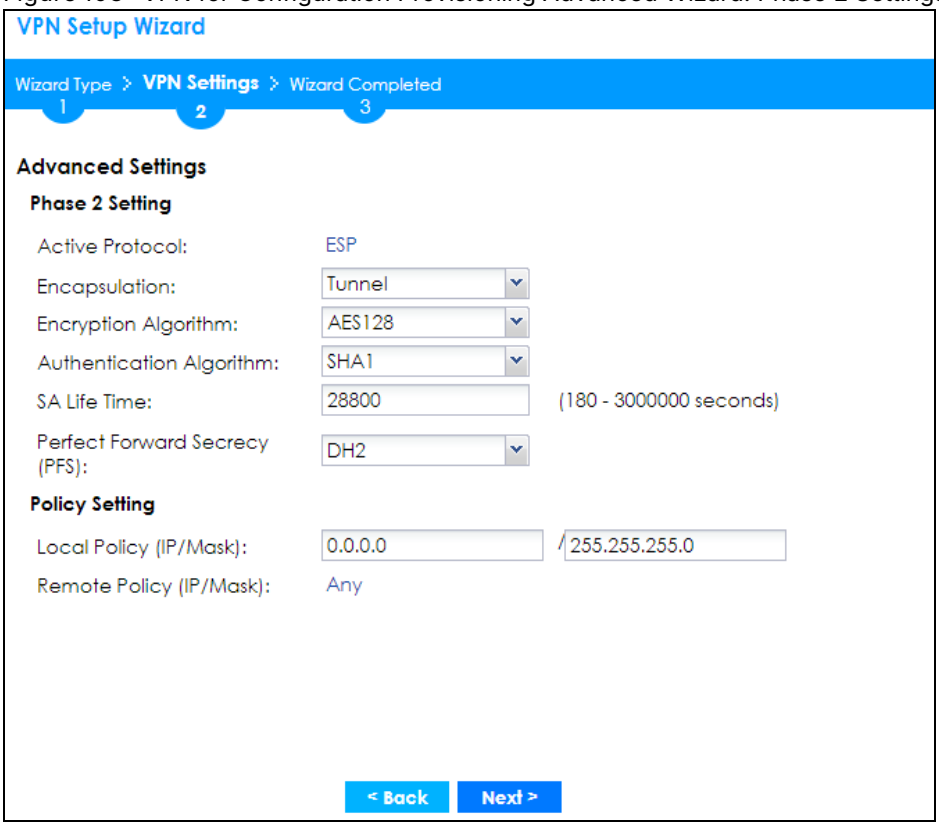
- Encryption Algorithm: 3DES and AES use encryption. The longer the key, the higher the security (this may affect throughput). Both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES 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.

5.7.7 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 103 VPN for Configuration Provisioning Advanced Wizard: Phase 2 Settings



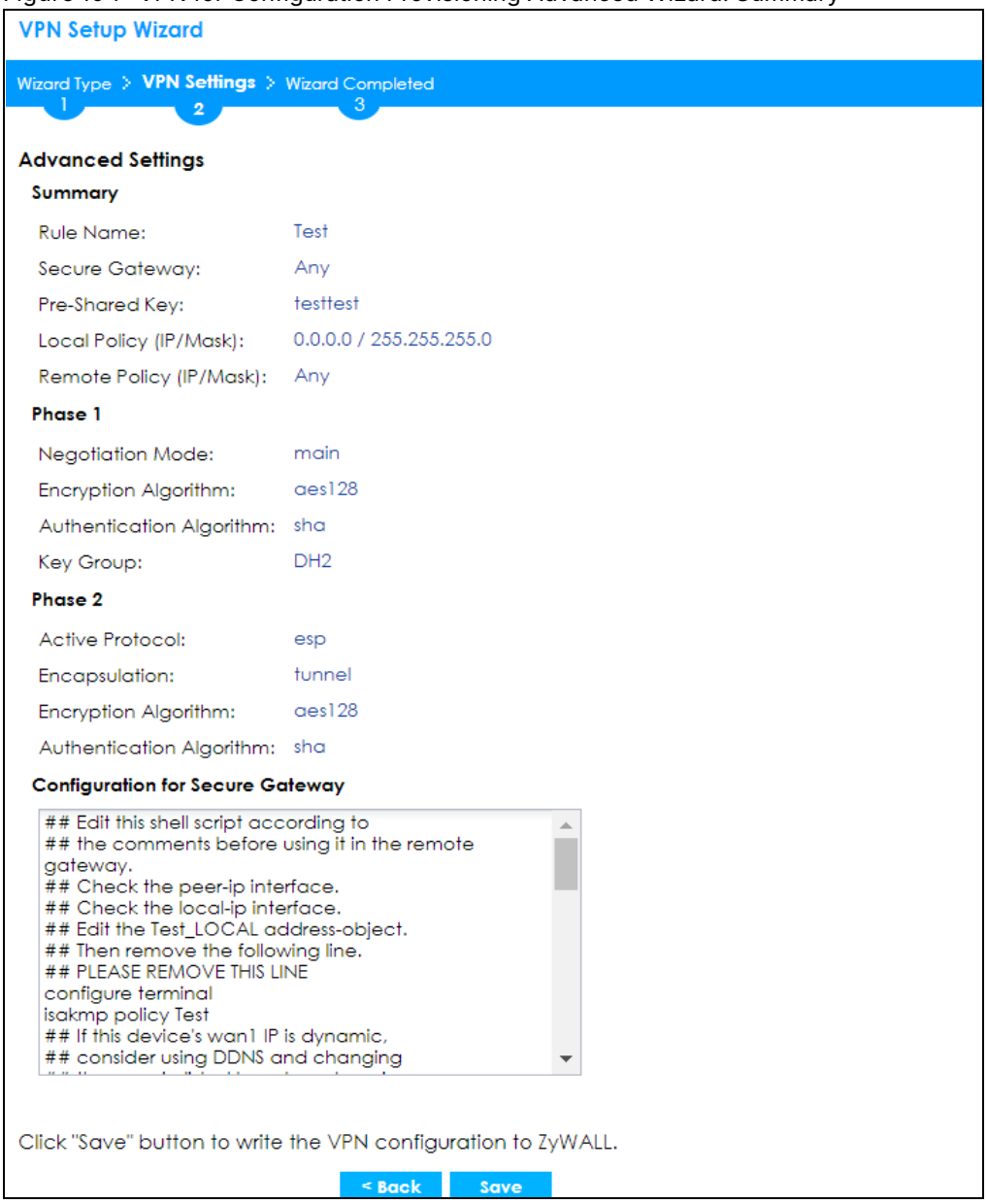
- Active Protocol: ESP is compatible with NAT. AH is not available in this wizard.
- Encapsulation: Tunnel is compatible with NAT, Transport is not.
- Encryption Algorithm: 3DES and AES use encryption. The longer the AES key, the higher the security (this may affect throughput). Null uses no encryption.
- 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): Enter 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.

- 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.

5.7.8 VPN Settings for Configuration Provisioning Advanced Wizard - Summary

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

Figure 104 VPN for Configuration Provisioning Advanced Wizard: Summary



- Rule Name: Identifies the VPN connection (and the VPN gateway).
- 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.

- 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.

5.7.9 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.

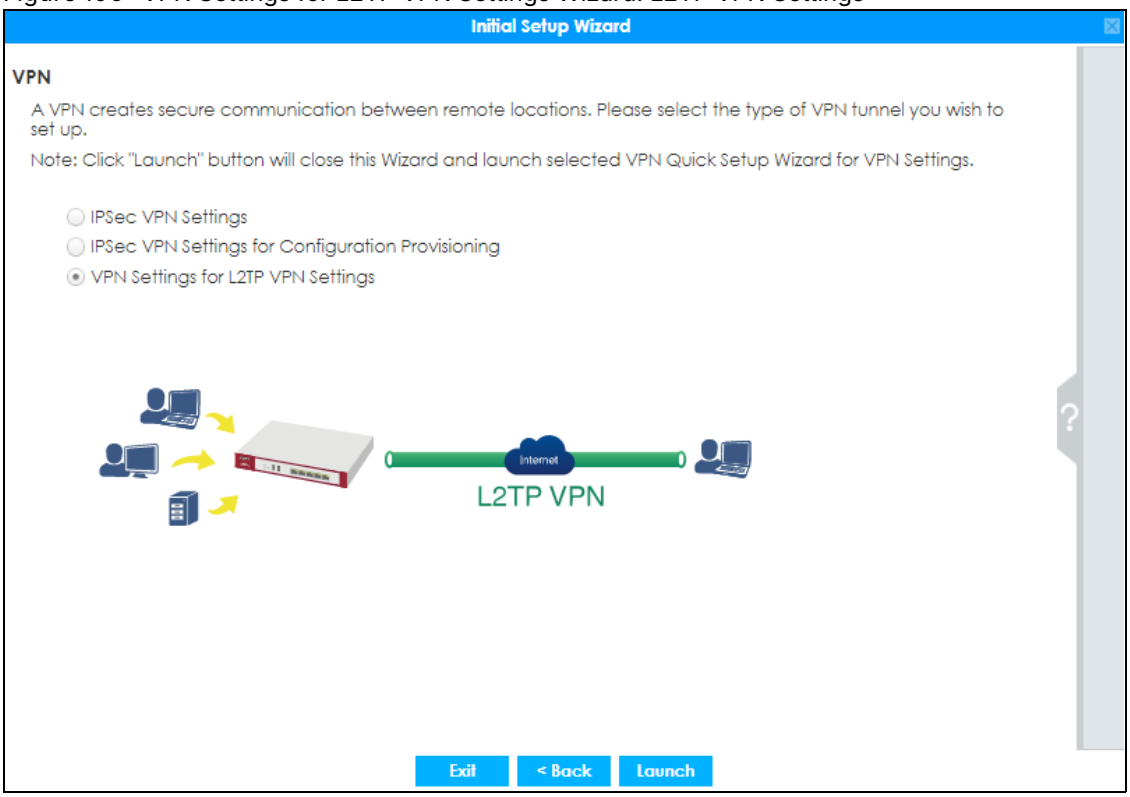
Figure 105 VPN for Configuration Provisioning Advanced Wizard: Finish

Click Close to exit the wizard.

5.8 VPN Settings for L2TP VPN Settings Wizard

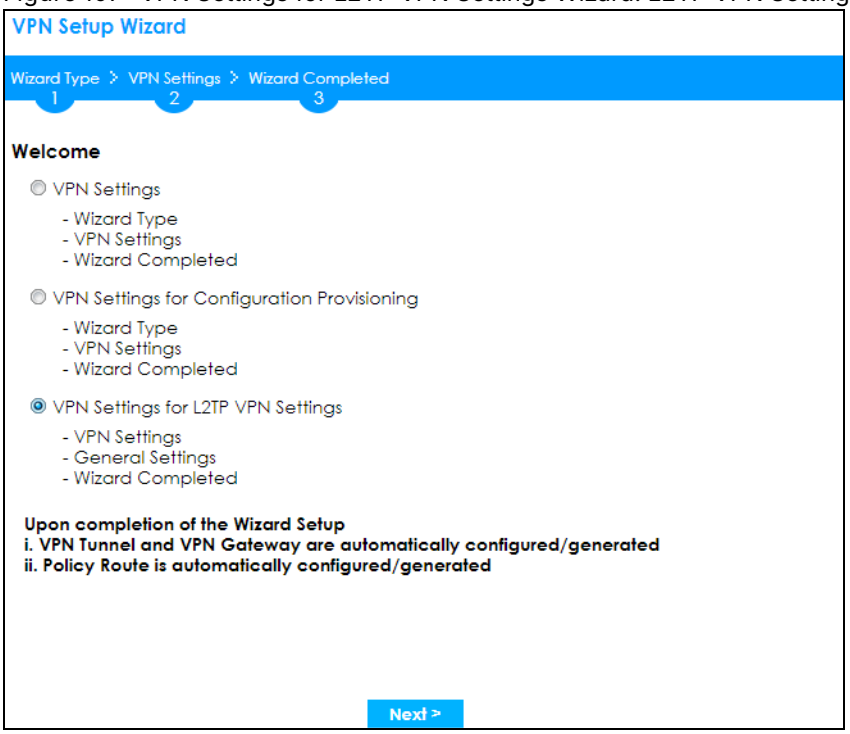
Use VPN Settings for L2TP VPN Settings to set up an L2TP VPN rule.

Figure 106 VPN Settings for L2TP VPN Settings Wizard: L2TP VPN Settings



Click Configuration > Quick Setup > VPN Settings and select VPN Settings for L2TP VPN Settings to see the following screen.

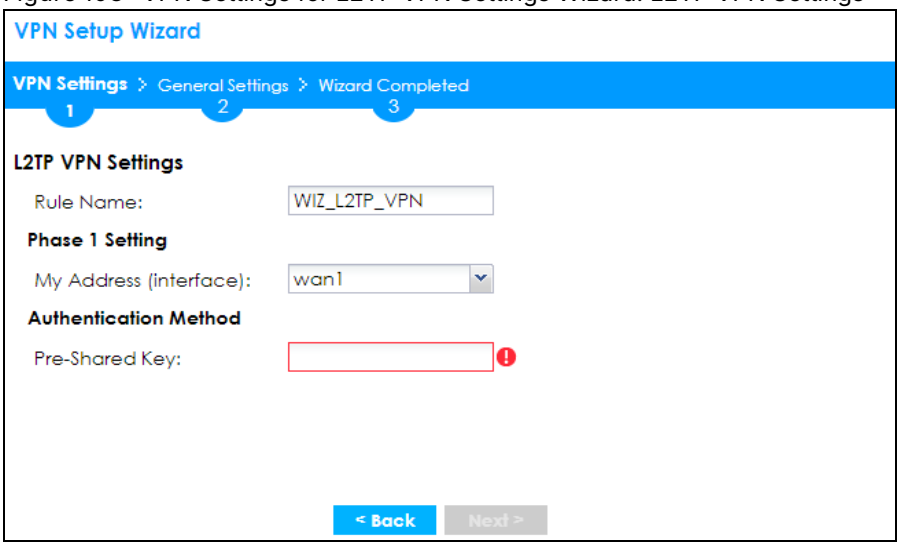
Figure 107 VPN Settings for L2TP VPN Settings Wizard: L2TP VPN Settings



Click Next to continue the wizard.

5.8.1 L2TP VPN Settings 1

Figure 108 VPN Settings for L2TP VPN Settings Wizard: L2TP VPN Settings

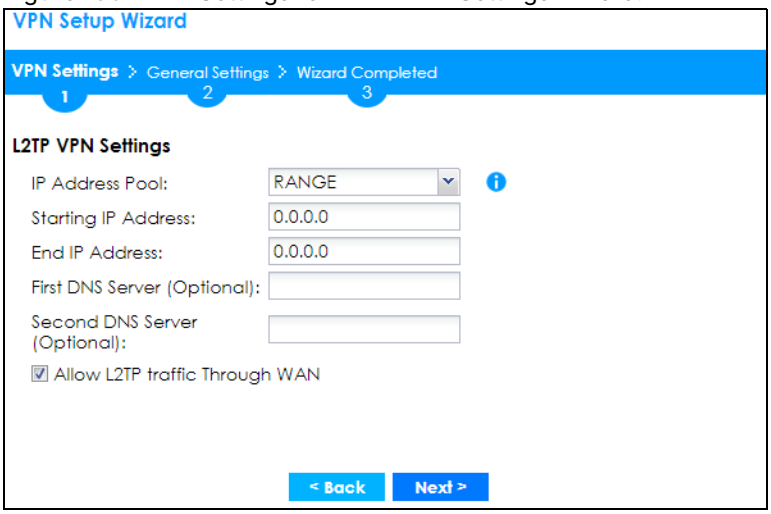


- Rule Name: Enter the name used to identify this L2TP VPN connection (and L2TP VPN gateway). You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
- My Address (interface): Select one of the interfaces from the pull down menu to apply the L2TP VPN rule.
- Pre-Shared Key: Enter the password. Both ends of the VPN tunnel must use the same password. Use up to 128 case-sensitive ASCII characters or up to 128 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.

5.8.2 L2TP VPN Settings 2

Figure 109 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.
- 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 checkbox to allow traffic from L2TP clients to go to the Internet.

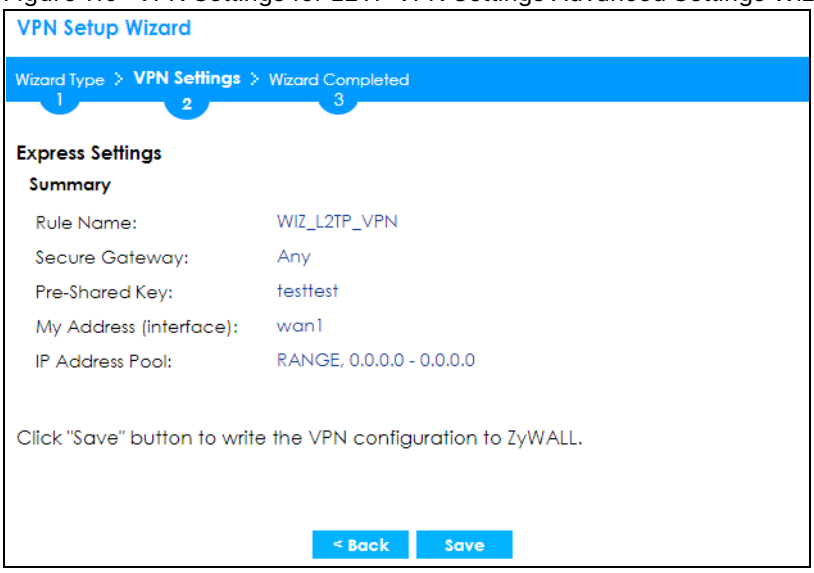
Click Next to continue the wizard.

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.

5.8.3 VPN Settings for L2TP VPN Setting Wizard - Summary

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

Figure 110 VPN Settings for L2TP VPN Settings Advanced Settings Wizard: Summary

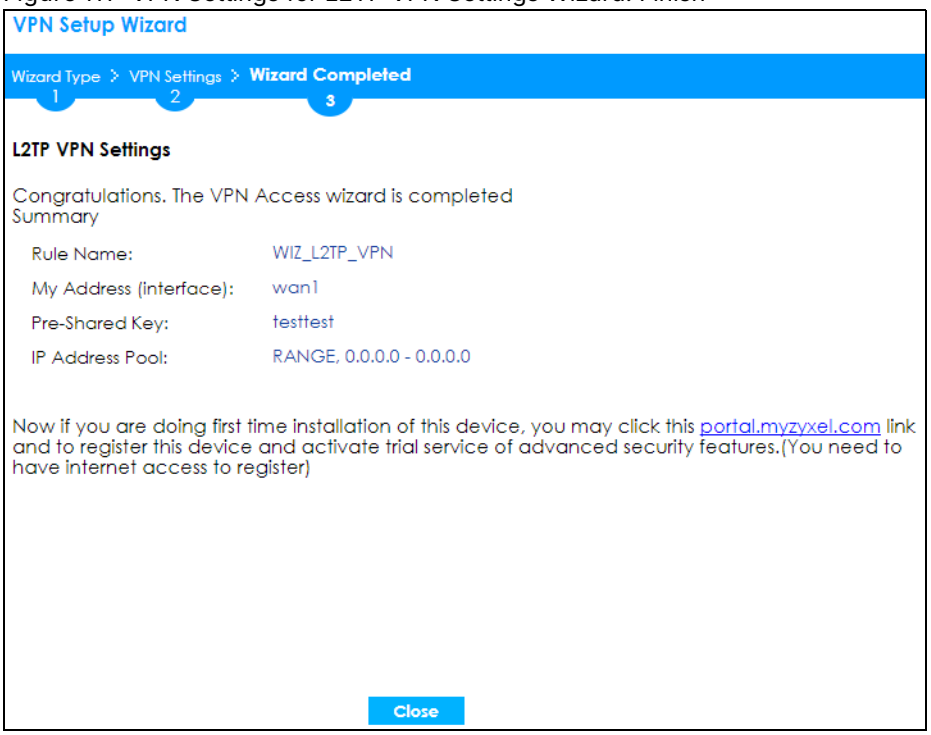


- Rule Name: Identifies the L2TP VPN connection (and the L2TP VPN gateway).
- Secure Gateway "Any" displays in this field because it is not configurable in this wizard. It allows incoming connections from the L2TP VPN Client.
- Pre-Shared Key: L2TP VPN tunnel password.
- My Address (Interface): This 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.

5.8.4 VPN Settings for L2TP VPN Setting Wizard Completed

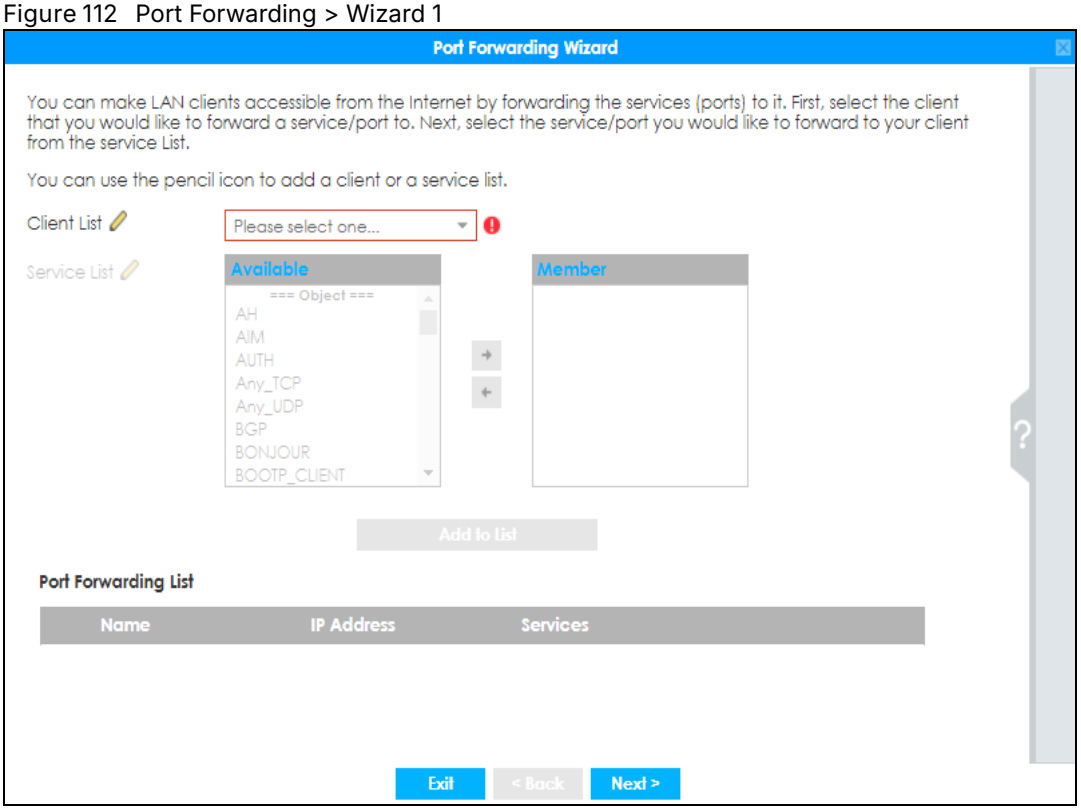
Figure 111 VPN Settings for L2TP VPN Settings Wizard: Finish



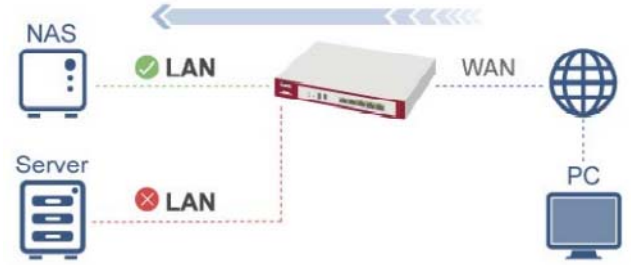
Now the rule is configured on the Zyxel Device. The L2TP VPN rule settings appear in the VPN > L2TP VPN screen and also in the VPN > IPSec VPN > VPN Connection and VPN Gateway screen.

5.9 Port Forwarding

Figure 112 Port Forwarding > Wizard 1



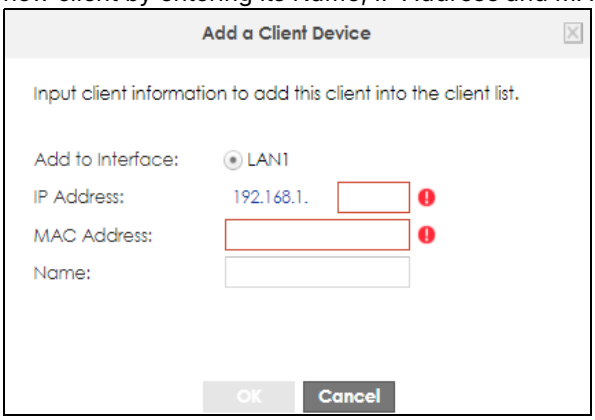
NAT port forwarding allows the Zyxel Device to direct incoming traffic from the Internet to the correct virtual server in your network. Even though the NAS is in your local network receiving the protection of the Zyxel Device, you can still access that NAS using these services from anywhere outside your network.



For example, if you have a NAS server in your network that you or other people need access to from outside your network, select the IP address of the NAS from Client. Then, select the service(s) that your NAS provides (for example FTP, HTTP, HTTPS) from the Available box and use the right arrow to move each service to the Member box.

5.9.1 Port Forwarding > Add Client

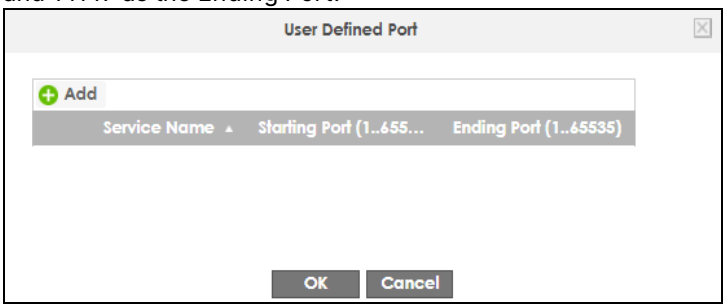
Click the Edit next to Client List if you cannot see the client in the list. In the pop-up screen, you can add a new client by entering its Name, IP Address and MAC Address.



A client or device in your network acting as a server for forwarded services (for example, the NAS) needs to have a static address. If the client selected does not have a static IP address, the IP address may change when the client reboots, so the Zyxel Device may not be able to find it. If this happens, check for the new IP address of the client. Then add the new IP address by clicking the Edit icon next to Client List and entering it in the pop-up screen.

5.9.2 Port Forwarding > Add Service

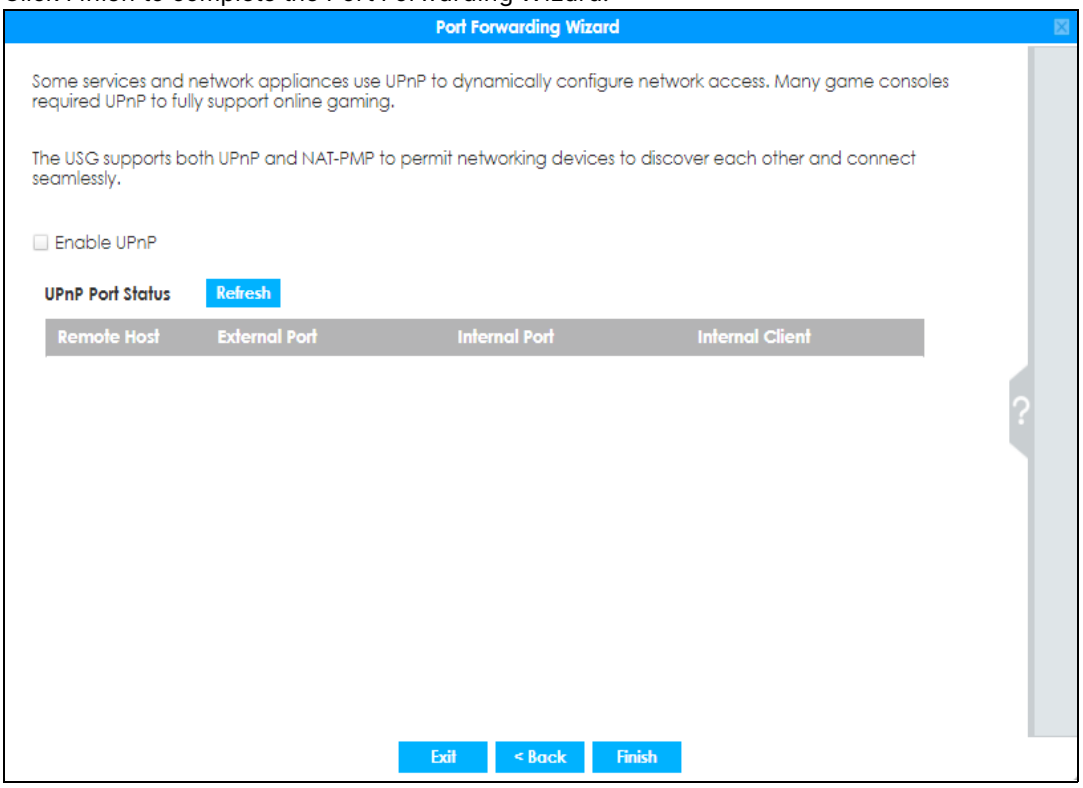
Click the Edit icon next to Service List if you cannot see the service in the list. In the pop-up screen, click Add, then enter the service name and port range that defines the service. For example, if you have a FileZilla Server in your network, then enter FileZilla Server as the Service Name, 14147 as the Starting Port and 14147 as the Ending Port.



5.9.3 Port Forwarding > UPnP

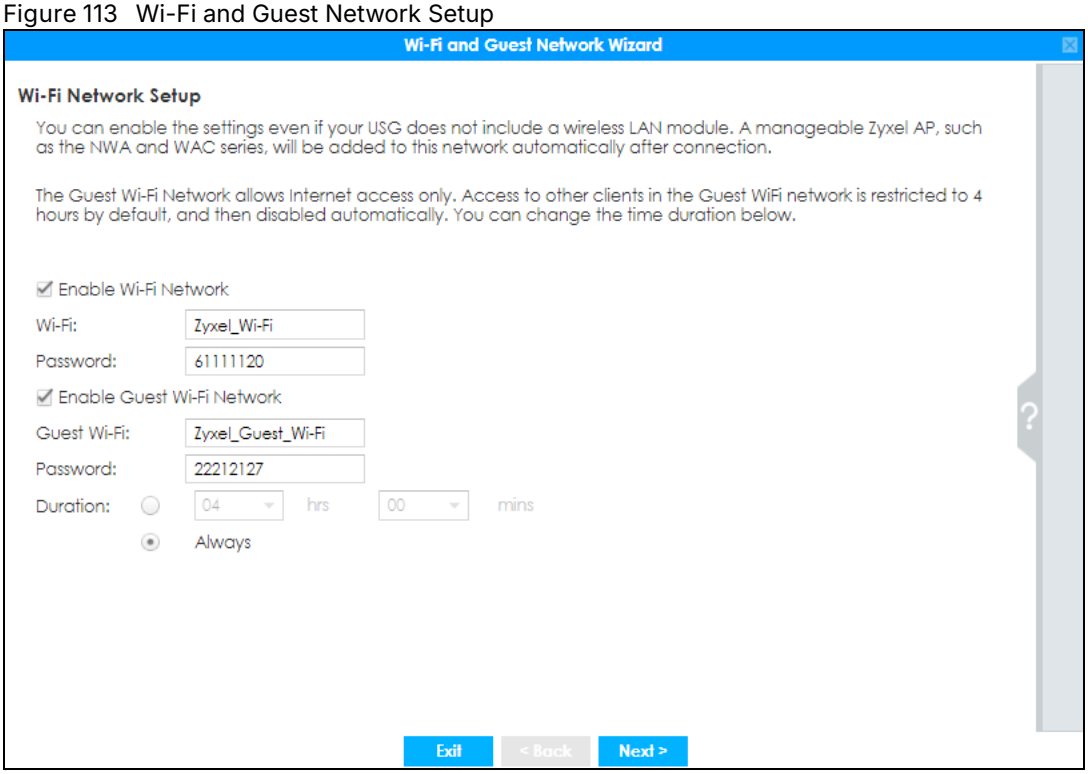
The Zyxel Device supports both UPnP (Universal Plug and Play) and NAT-PMP (NAT Port Mapping Protocol) to permit networking devices to discover each other and connect seamlessly. An enabled-UPnP or NAT-PMP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. If you have a service that requires UPnP or NAT-PMP, such as a game server, then select Enable UPnP in this screen and click Refresh. All UPnP-enabled or NAT-PMP-enabled devices may communicate freely with each other without additional configuration. Do not select Enable UPnP if this is not your intention.

Click Finish to complete the Port Forwarding Wizard.



5.10 Wi-Fi and Guest Network Wizard

Figure 113 Wi-Fi and Guest Network Setup



Select Enable Wi-Fi Network if you want wireless devices to be able to wirelessly access the Zyxel Device and all resources connected to the Zyxel Device. Configure a descriptive name of from 1 to 32 alpha-numeric characters, hyphens or underscores (a-z A-Z 0-9 -_) for the wireless network name (Wi-Fi). Set a Password of between 8 and 63 printable ASCII characters (including spaces and symbols) or 64 hexadecimal characters (0-9 a-f) that wireless users will have to enter for access to the Zyxel Device wireless network.

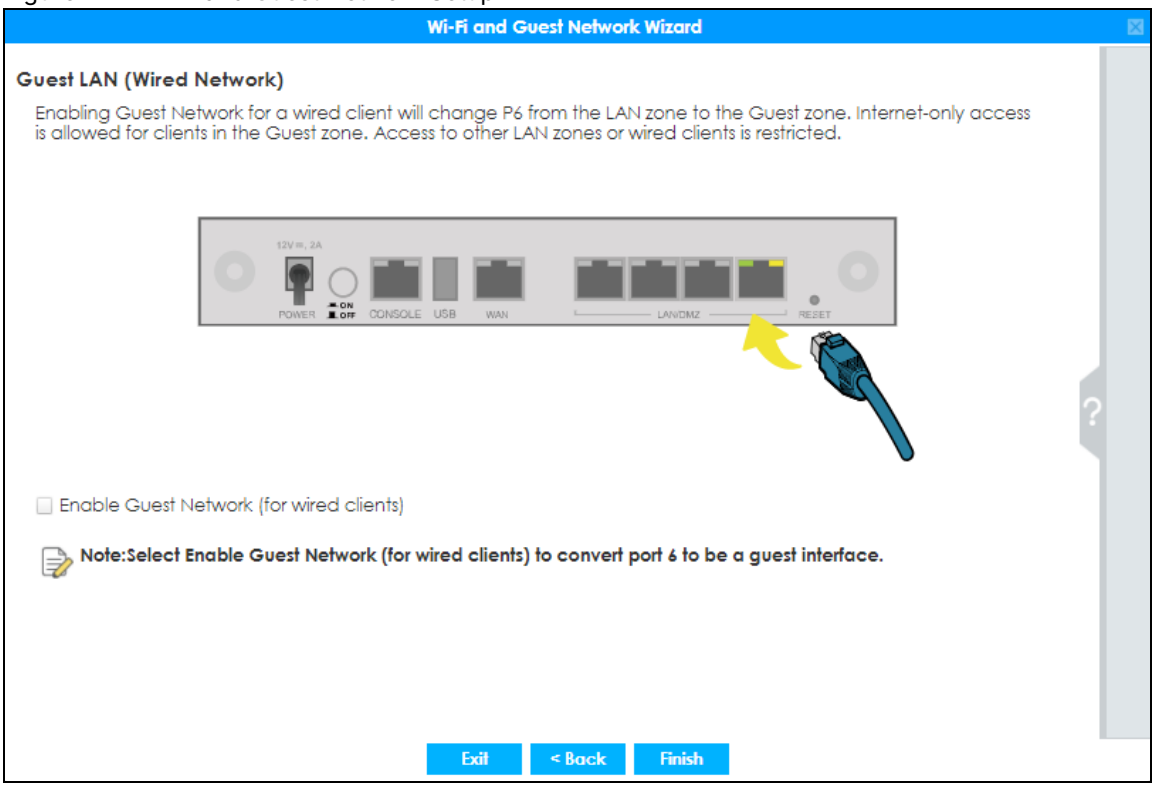
Select Enable Guest Wi-Fi Network if you want wireless devices to only be able to wirelessly access the Internet through the Zyxel Device for up to the period specified in Duration. Configure a descriptive name of from 1 to 32 alpha-numeric characters, hyphens or underscores (a-z A-Z 0-9 -_) for the wireless network name (Wi-Fi). Set a Password of between 8 and 63 printable ASCII characters (including spaces and symbols) or 64 hexadecimal characters (0-9 a-f) that wireless users will have to enter for access to the Zyxel Device Guest wireless network.

The Guest Wi-Fi Network allows Internet access for up to the period specified in Duration. Wireless users will have to log in again if the time has elapsed.

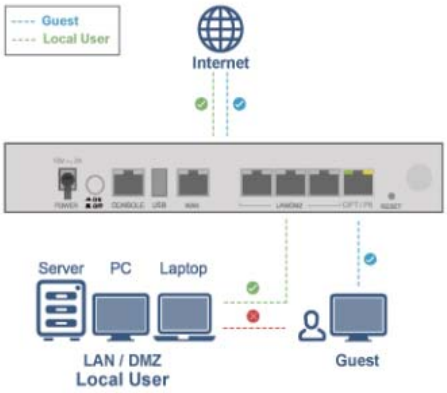
The Zyxel Device uses WPA2-PSK with AES encryption so wireless clients must be able to support AES encryption to wirelessly connect to the Zyxel Device using WPA2-PSK.

5.10.1 Guest LAN (Wired Network)

Figure 114 Wi-Fi and Guest Network Setup



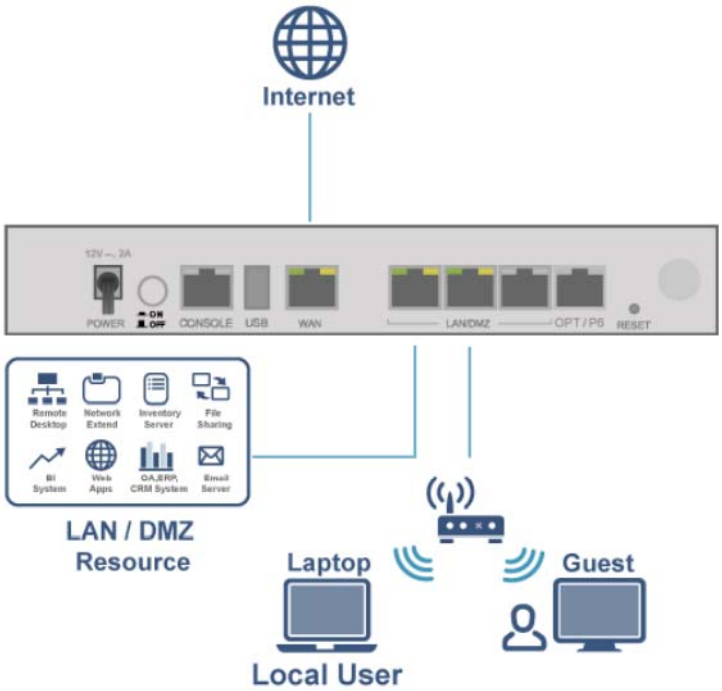
Select Enable Guest Network (for wired clients) to convert the OPT or P6 port (depending on your model) to be a guest port and isolate it from the LAN/DMZ ports. Devices connected to the guest port are allowed Internet access only and do not have access to networks connected to the other ports.



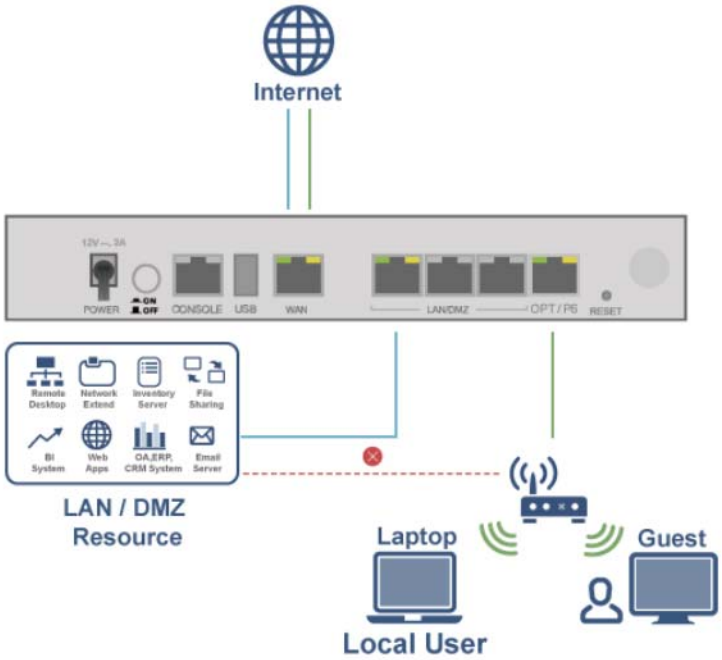
When the OPT or P6 port is not a guest port, then guest devices connected to that port can communicate with all networks, including devices connected to the LAN/DMZ ports. To avoid this, make sure Enable Guest Network (for wired clients) is selected and that guest devices are only connected to the OPT or P6 port on the Zyxel Device.

5.10.2 Connecting AP Scenarios

If you connect an AP to a LAN port, then users can use the AP's SSID to wirelessly access all wired resources connected to the LAN ports and Internet access.

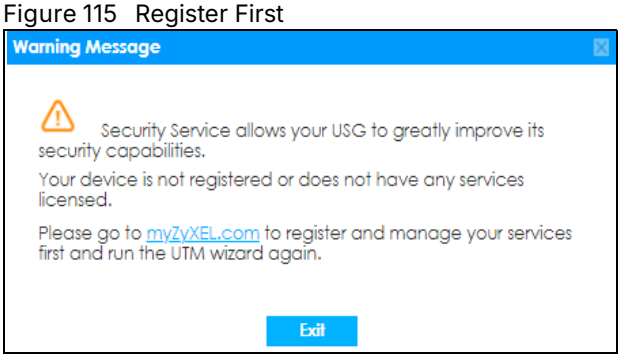


If you connect an AP to the Guest port, then users can use the AP's SSID to wirelessly access all wired resources connected to the Guest port (only) and Internet access. You must select both Enable Guest Wi-Fi Network and Guest LAN (Wired Network).



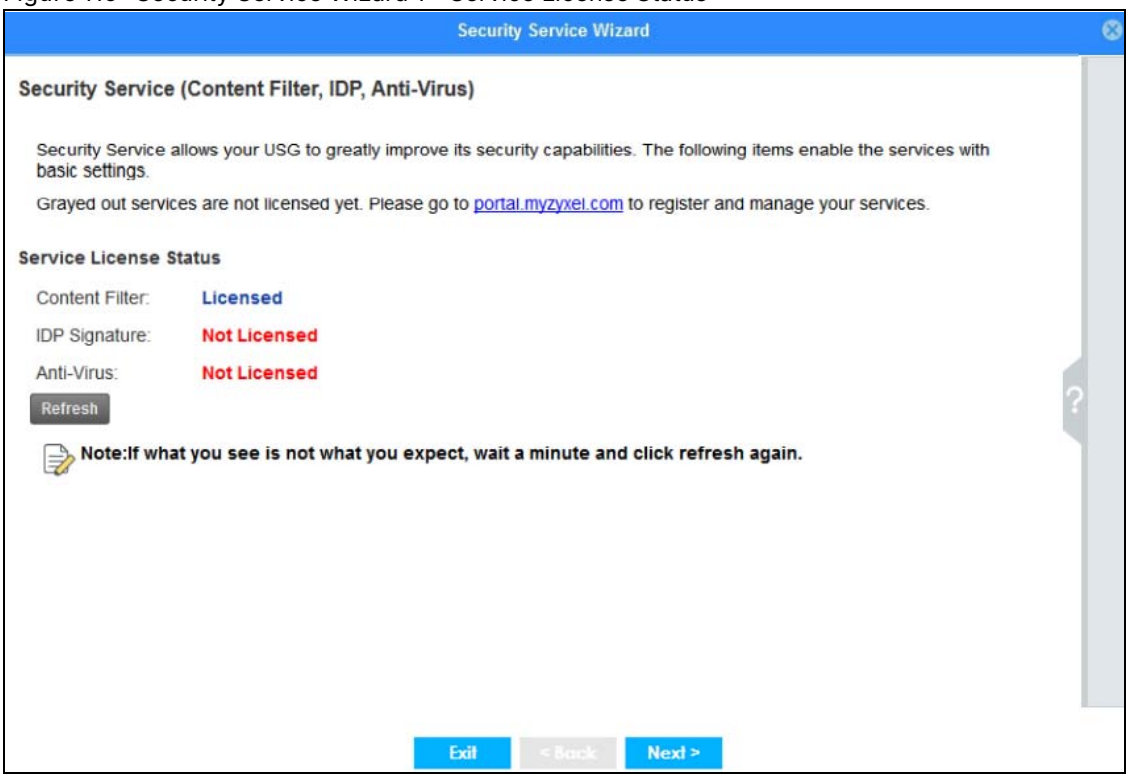
5.11 Security Service Wizard

Figure 115 Register First



You must first register the Zyxel Device at portal.myzyxel.com and activate licenses for required services.

Figure 116 Security Service Wizard 1 - Service License Status



This screen shows if you have registered your Zyxel Device at *portal.myzyxel.com*. After you register your Zyxel Device, you can register for the services supported by your model. For example, some models only support content filtering.

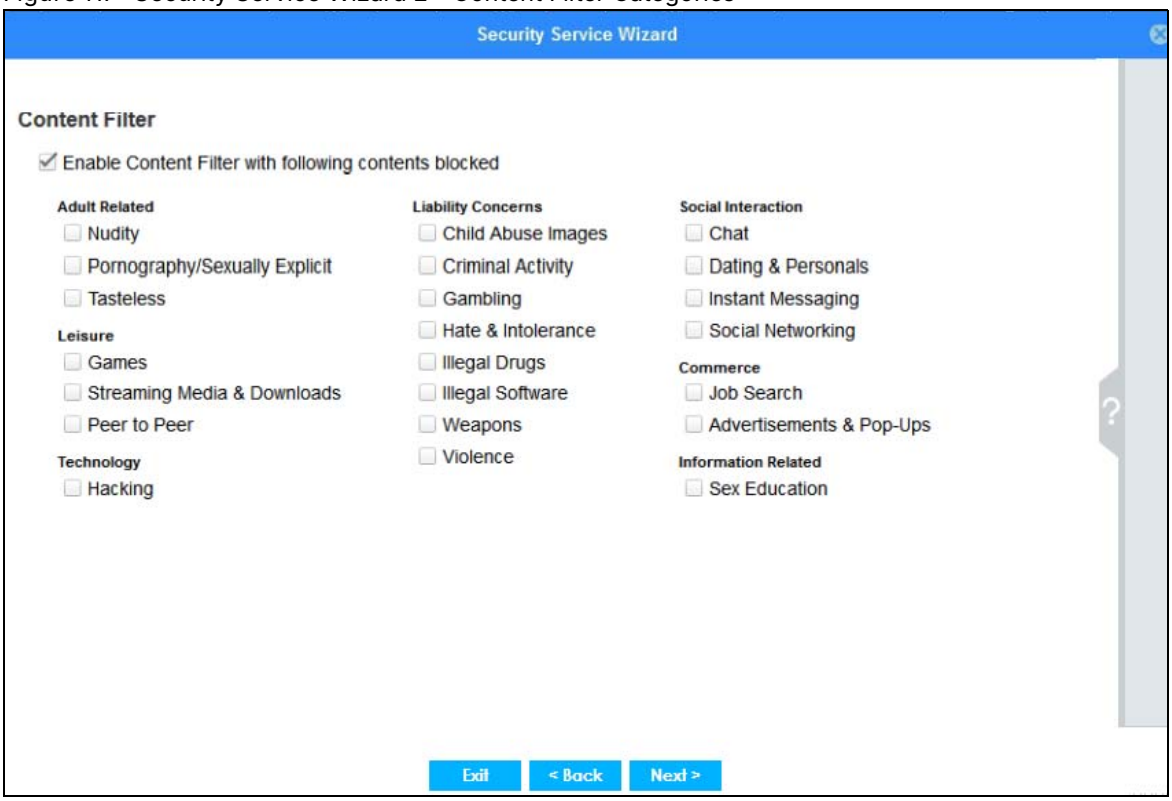
- Content Filtering (to block websites by category, such as Gambling)
- IDP (to recognize and drop traffic with Intrusion, Detection & Protection attack patterns)
- Anti-Virus (to detect virus patterns in files)

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.

5.11.1 Security Service Wizard 2 - Content Filter Categories

Figure 117 Security Service Wizard 2 - Content Filter Categories



Configure licensed (non-grayed-out) services in this screen. After you buy a license for a service, you must activate it at myZyxel. Make sure the Zyxel Device Internet connection is working correctly.

Select Enable Content Filter with following contents blocked to block websites by category, such as Chat websites. Note that if you select Chat, the Content Filter blocks chat websites and not chat apps. Therefore, the Skype app can still be used although the Skype website would be blocked. Select the categories you want to block.

- Adult Related
  - Nudity: Sites that contain full or partial nudity that are not necessarily overtly sexual in intent. Includes sites that advertise or sell lingerie, intimate apparel, or swim wear. For example, www.easyshop.com.tw, www.faster-swim.com.tw, image.baidu.com.
  - Pornography/Sexually Explicit: Sites that contain explicit sexual content. Includes adult products such as sex toys, CD-ROMs, and videos, adult services such as videoconferencing, escort services, and strip clubs, erotic stories and textual descriptions of sexual acts. For example, www.dvd888.com, www.18center.com, blog.sina.com.tw.
  - Tasteless: Sites with offensive or tasteless content such as bathroom humor or profanity. For example, comedycentral.com, dilbert.com.
- Leisure

  - Games: Sites relating to computer or other games, information about game producers, or how to obtain cheat codes. Game-related publication sites. For example, www.gamer.com.tw, www.wowtaiwan.com.tw, tw.lineage.gamania.com.
  - Streaming Media & Downloads: Sites that deliver streaming content, such as Internet radio, Internet TV or MP3 and live or archived media download sites. Includes fan sites, or official sites run by musicians, bands, or record labels. For example, www.youtube.com, pfp.sina.com.cn, my.xunlei.com.
  - Peer to Peer: Sites that enable direct exchange of files between users without dependence on a central server. For example, www.eyny.com.
- Technology
  - Hacking: Sites that promote or give advice about how to gain unauthorized access to proprietary computer systems, for the purpose of stealing information, perpetrating fraud, creating viruses, or committing other illegal activity related to theft of digital information. For example, www.hackbase.com, www.chinahacker.com.
- Liability Concerns
  - Child Abuse Images: Sites that portray or discuss children in sexual or other abusive acts. For example, a.uuzhijia.info.
  - Criminal Activity: Sites that offer advice on how to commit illegal or criminal activities, or to avoid detection. These can include how to commit murder, build bombs, pick locks, etc. Also includes sites with information about illegal manipulation of electronic devices, hacking, fraud and illegal distribution of software. For example, www.hackbase.com, jia.hackbase.com, ad.adver.com.tw.
  - Gambling: Sites that offer or are related to online gambling, lottery, casinos and betting agencies involving chance. For example, www.taiwanlottery.com.tw, www.i-win.com.tw, www.hkjc.com.
  - Hate & Intolerance: Sites that promote a supremacist political agenda, encouraging oppression of people or groups of people based on their race, religion, gender, age, disability, sexual orientation or nationality. For example, www.racist-jokes.com, aryan-nations.org, whitepower.com.
  - Illegal Drugs: Sites with information on the purchase, manufacture, and use of illegal or recreational drugs and their paraphernalia, and misuse of prescription drugs and other compounds For example, www.cannabis.net, www.amphetamines.com.
  - Illegal Software: Sites that illegally distribute software or copyrighted materials such as movies or music, software cracks, illicit serial numbers, illegal license key generators. For example, www.zhaokey.com.cn, www.tiansha.net.
  - Weapons: Sites that depict, sell, review or describe guns and weapons, including for sport. For example, www.ak-47.net, warfare.ru.
  - Violence: Sites that contain images or text depicting or advocating physical assault against humans, animals, or institutions. Sites of a particularly gruesome nature such as shocking depictions of blood or wounds, or cruel animal treatment. For example, crimescene.com, deathnet.com, michiganmilitia.com.
- Social Interaction
  - Chat: Sites that enable web-based exchange of real time messages through chat services or chat rooms. For example, me.sohu.com, blufiles.storage.live.com.
  - Dating & Personals: Sites that promote networking for interpersonal relationships such as dating and marriage. Includes sites for match-making, online dating, spousal introduction. For example, www.i-part.com.tw, www.imatchi.com.
  - Instant Messaging: Sites that enable logging in to instant messaging services such as ICQ, AOL Instant Messenger, IRC, MSN, Jabber, Yahoo Messenger, and the like. For example, www.meebo.com, www.aim.com, www. ebuddy.com.
  - Social Networking: Sites that enable social networking for online communities of various topics, for friendship, dating, or professional reasons. For example, www.facebook.com, www.flickr.com, www.groups.google.com.

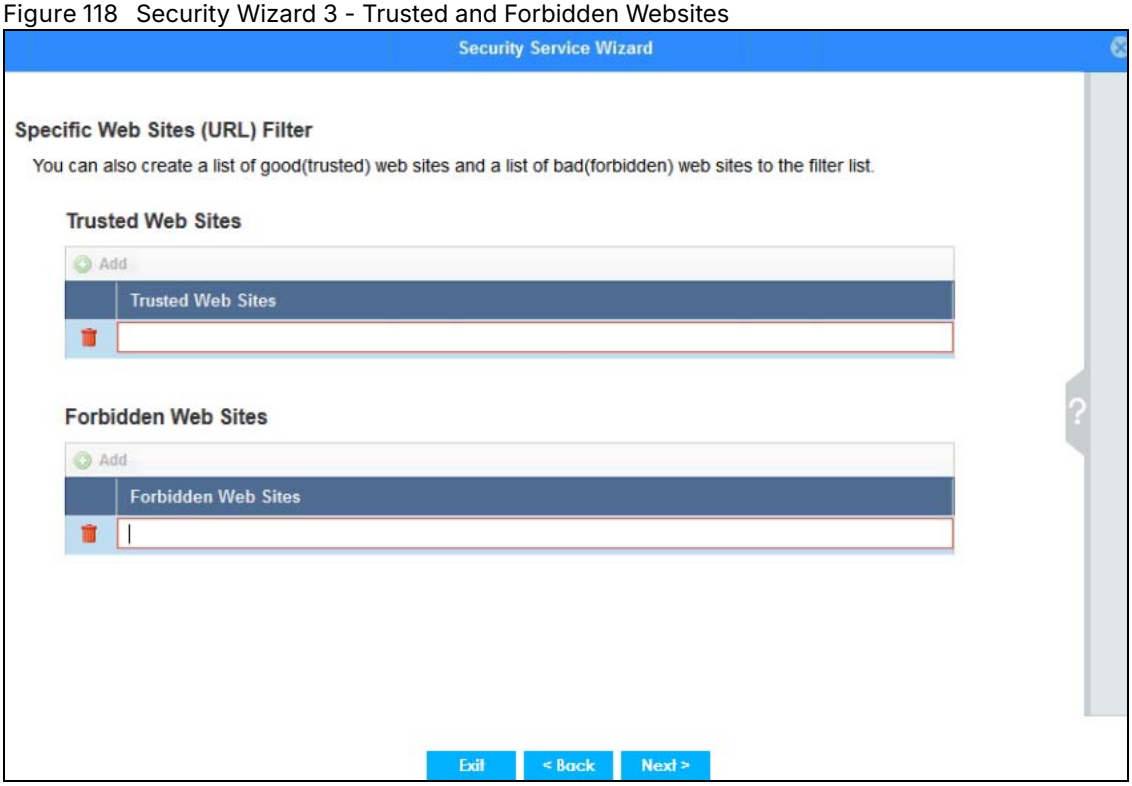
- Commerce
  - Job Search: Sites containing job listings, career information, assistance with job searches (such as resume writing, interviewing tips, etc.), employment agencies or head hunters. For example, www.104.com.tw, www.1111.com.tw, www.yes123.com.tw.
  - Advertisements & Pop-Ups: Sites that provide advertising graphics or other ad content files such as banners and pop-ups. For example, pagead2.googlesyndication.com, ad.yieldmanager.com.
- Information Related
  - Sex Education: Sites relating to sex education, including subjects such as respect for partner, abortion, gay and lesbian lifestyle, contraceptives, sexually transmitted diseases, and pregnancy. For example, apps.rockyou.com, www.howmama.com.tw, www.mombaby.com.tw.

Select Enable IDP to drop traffic with recognized Intrusion, Detection & Protection attack patterns.

Select Enable Anti-Virus to detect virus patterns in files.

5.11.2 Security Service Wizard 3 - Websites

Figure 118 Security Wizard 3 - Trusted and Forbidden Websites



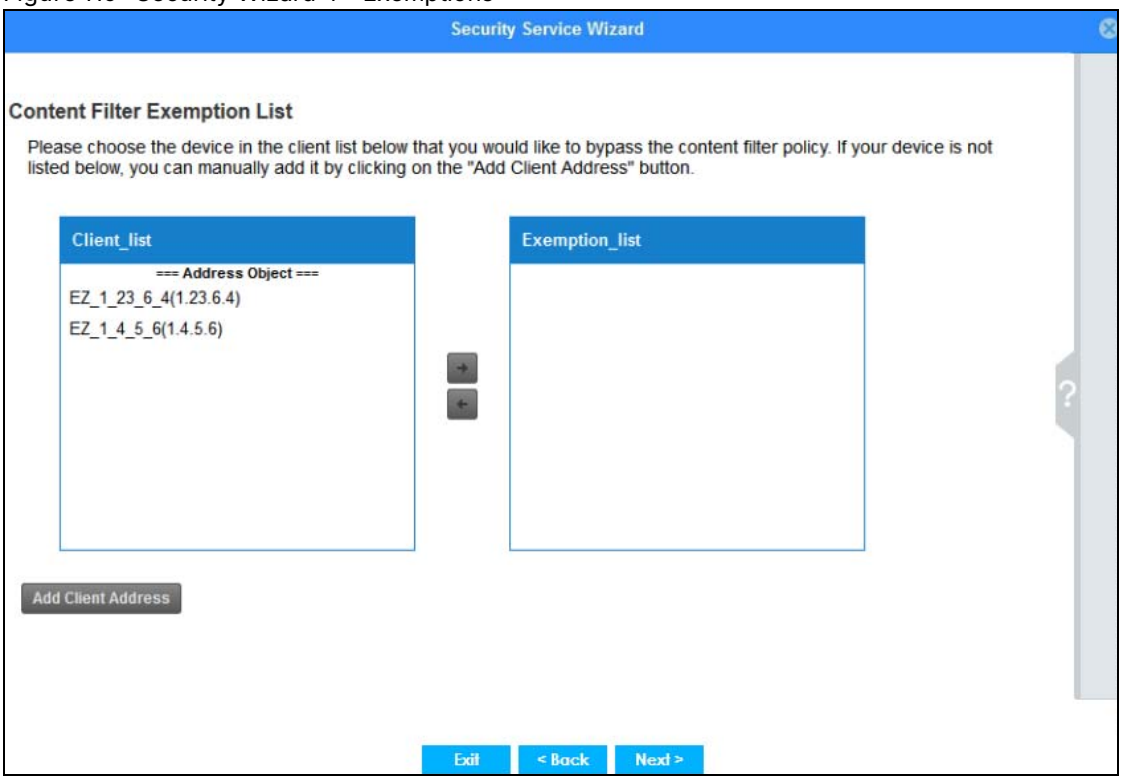
Here, you can create a list of good (trusted) web site addresses and a list of bad (forbidden) web site addresses. Click Add to create a new trusted or forbidden web site. Enter host names such as www.good-site.com or www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include “http://”. All sub-domains are allowed. For example, entering “*.zyxel.com” also allows or forbids “www.zyxel.com”, “partner.zyxel.com”, “press.zyxel.com”, and so on. You can also enter just a top level domain. For example, enter “*.com” to allow or forbid all .com domains.

Use up to 127 characters (0-9a-z-). The casing does not matter. “*” can be used as a wild-card to match any string. The entry must contain at least one period “.” or it will be invalid.

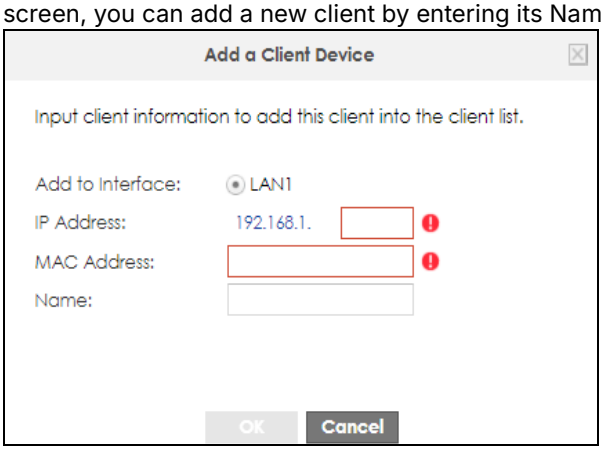
Click the trash can to remove a trusted or forbidden web site.

5.11.3 Security Service Wizard 4 - Exemptions

Figure 119 Security Wizard 4 - Exemptions

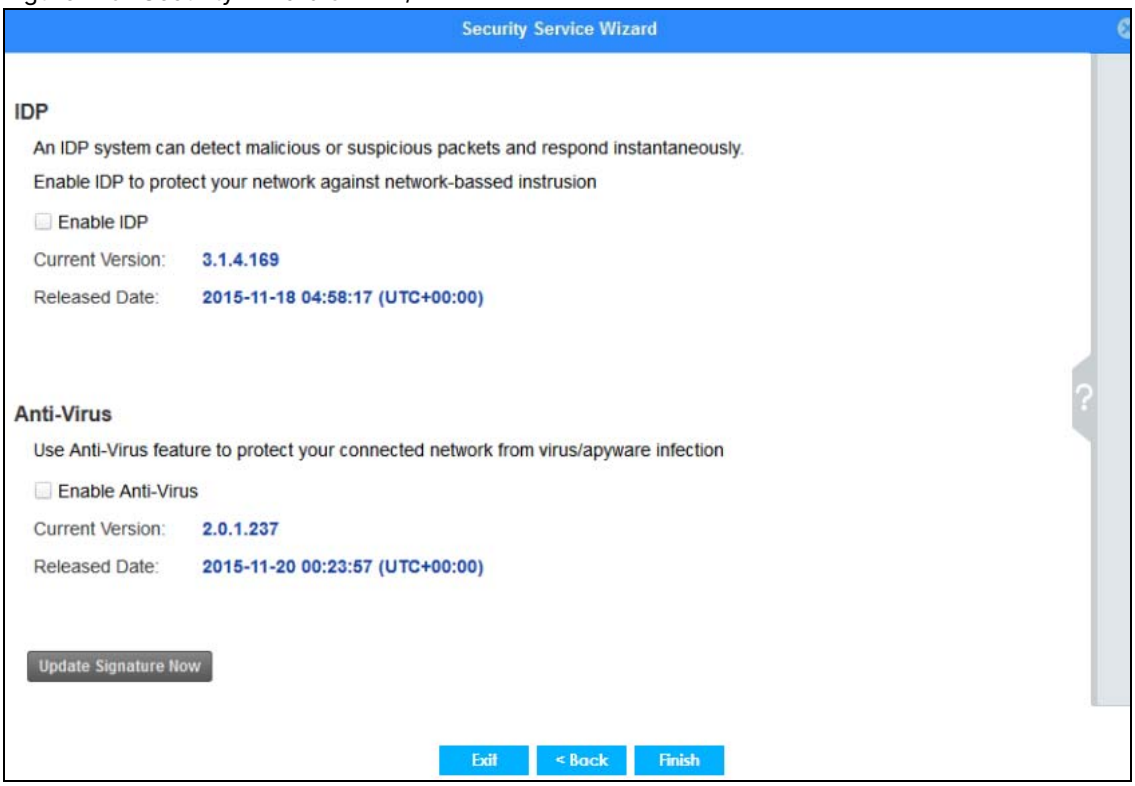


Select devices which are exempted from content file category and trusted/forbidden web site policies. Click Add Client Address under Client List if you cannot see the client to exempt in the list. In the pop-up screen, you can add a new client by entering its Name, IP Address and MAC Address.



5.11.4 Security Service Wizard 5 - IDP/AV

Figure 120 Security Wizard 5 - IDP/AV

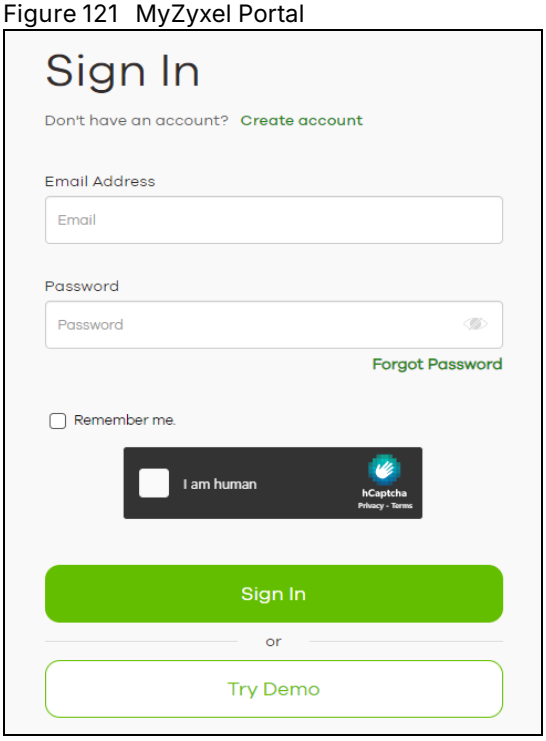


IDP (Intrusion, Detection and Prevention) consists of a set of signatures which examine packet content for known malicious data. You need to subscribe for IDP service in order to be able to download new signatures. It's important to keep the signatures up to date as new types of malicious data are constantly evolving.

Use the Zyxel Device's Anti-Virus (AV) feature to protect your connected network from virus/spyware infection. A computer virus is a small program designed to corrupt and/or alter the operation of other legitimate programs. A worm is a self-replicating virus that resides in active memory and duplicates itself. Zyxel Device's Anti-Virus consists of a set of signatures which examine packet content for known viruses and worms. You need to subscribe for AV service in order to be able to download new signatures. It's important to keep the signatures up to date as new viruses and worms are constantly evolving.

5.12 MyZyxel Portal

Figure 121 MyZyxel Portal



myZyxel is Zyxel's online services center where you can register your Zyxel Device and manage subscription services available for the Zyxel Device. To update signature files or use a subscription service, you have to register the Zyxel Device and activate the corresponding service at myZyxel (through the Zyxel Device).

Use the MyZyxel Portal link to create an account at myZyxel.

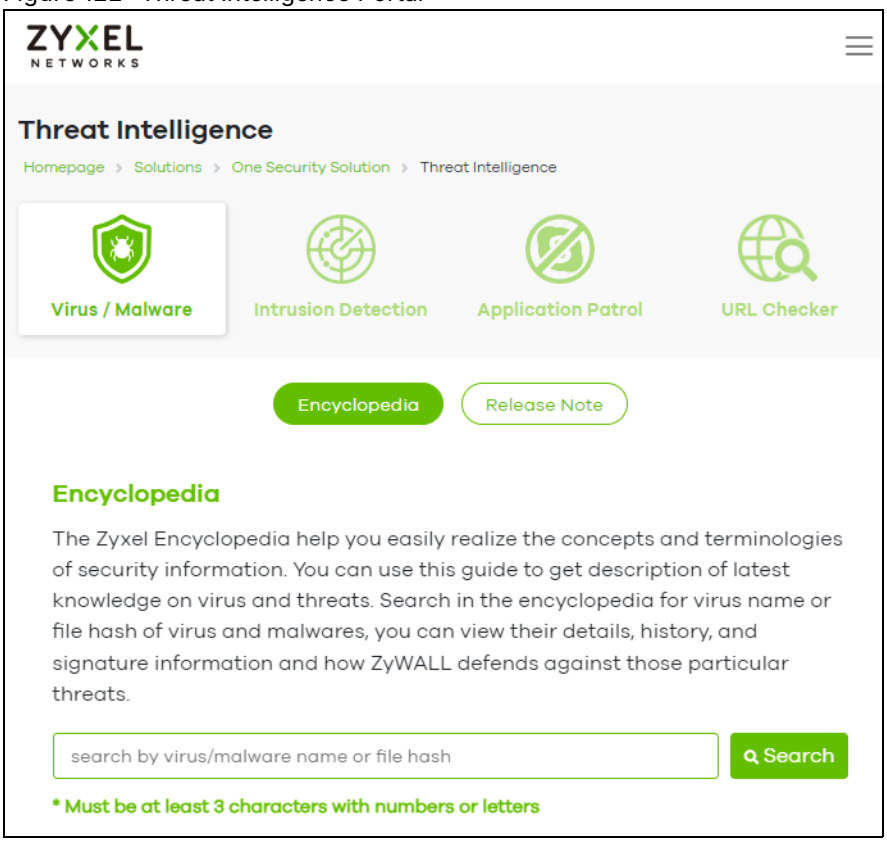
Then, register your device. You may need your Zyxel Device's serial number and LAN MAC address to register it at myZyxel. Refer to the myZyxel web site's on-line help for details.

To have the Zyxel Device use subscription services, please purchase an iCard and enter the license key from it at MyZyxel Portal (through the Zyxel Device).

5.13 Threat Intelligence Portal

Threat Intelligence (*https://threatintelligence.zyxel.com*) is a website offering guidance on Virus/Malware, Intrusion Detection, Application Patrol and URL Checker.

Figure 122 Threat Intelligence Portal



The following table describes the features on this website.

Table 20 Threat Intelligence Links

ICON	SCREEN
Virus/Malware Virus / Malware	Click this icon for more information on viruses and malware. A computer virus is a type of malware designed to corrupt and alter the operation of other legitimate programs. Malware is malicious software that damages computers and computer systems.
Intrusion Detection Intrusion Detection	Click this icon for more information on Intrusion Detection, which can detect malicious or suspicious packets used in network-based intrusions.
Application Patrol Application Patrol	Click this icon for more information on Application Patrol, which identifies traffic that passes through the Zyxel Device, so you can decide whether to deny, allow or reject specific types of traffic. Traffic not recognized by Application Patrol signatures is ignored.
URL Checker URL Checker	Click this icon for more information on URL Checker, which allows you to search for a URL and check what type of website it is. For example, *www.google.com* is a portal site and search engine, while *www.zyxel.com* is a business, software, and hardware site.

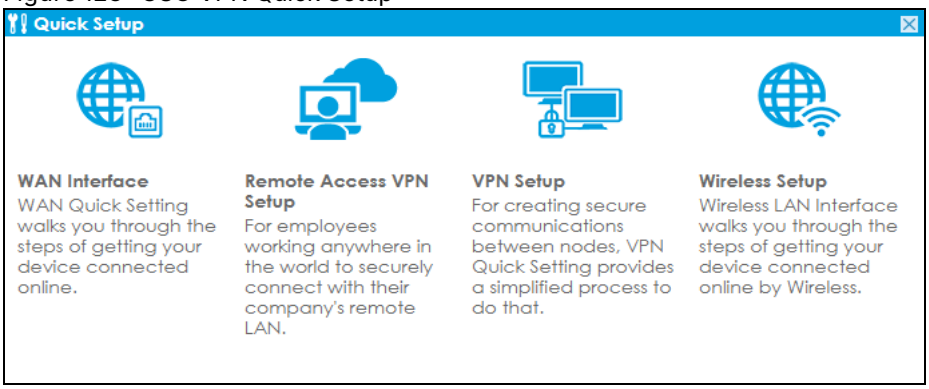
CHAPTER 6
Quick Setup Wizards

6.1 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 123 USG VPN 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 6.2 on page 159.

- Remote Access VPN Setup

  Click this link to open a wizard to configure a VPN (Virtual Private Network) rule for a secure connection to another computer or network. Zyxel VPN Client creates a full or split tunnel VPN rule for clients with SecuExtender IPSec. L2TP over IPSec Client creates full tunnel VPN rule for clients with supported mobile devices.

- VPN Setup

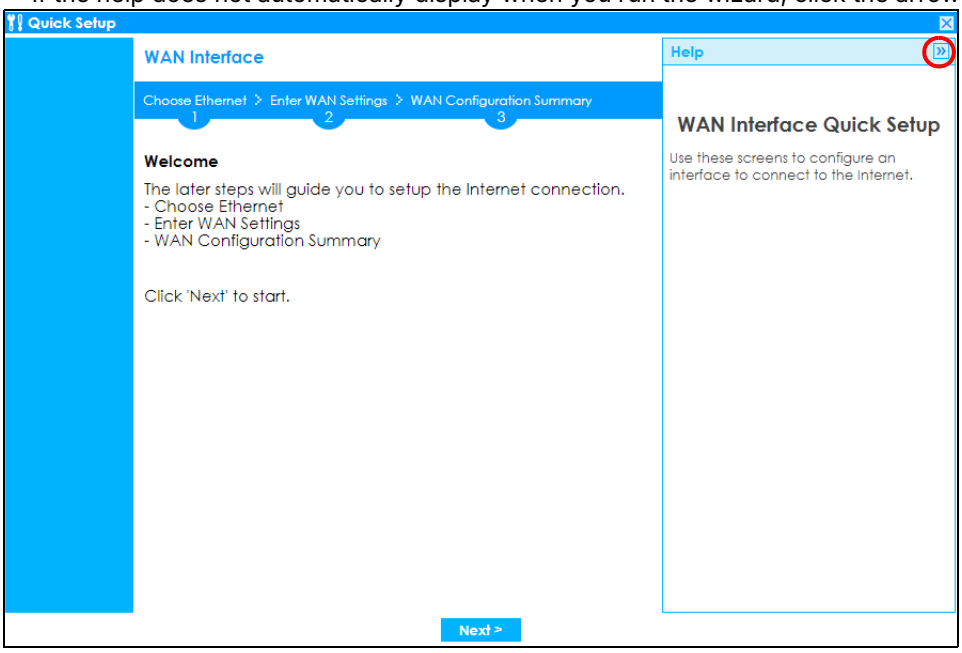
  Use VPN Setup to configure a VPN (Virtual Private Network) rule for a secure connection to another computer or network. Use VPN Settings for Configuration Provisioning to set up a VPN rule that can be retrieved with the Zyxel Device IPSec VPN Client. You only need to enter a user name, password and the IP address of the Zyxel Device in the IPSec VPN Client to get all VPN settings automatically from the Zyxel Device. See Section 6.4 on page 173. Use VPN Settings for L2TP VPN Settings to configure the L2TP VPN for clients.

- Wireless Setup

  Use this wizard to configure the Zyxel Device as an AP Controller that can manage APs in the same network as the Zyxel Device or the built-in AP if your Zyxel Device has this feature.

- Wizard Help

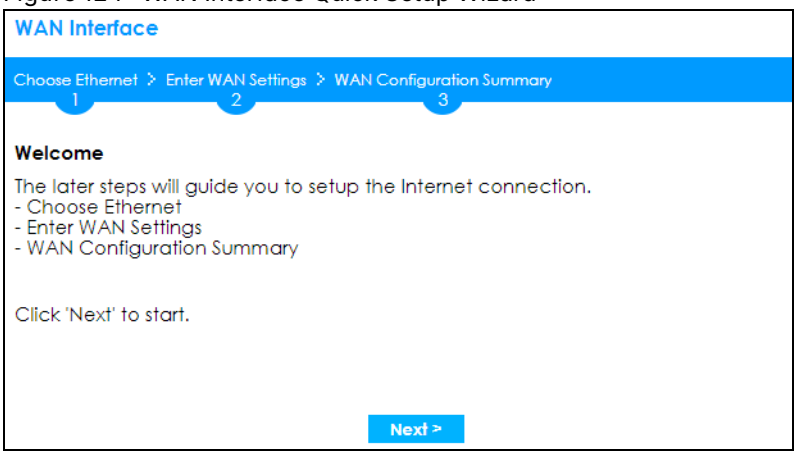
  If the help does not automatically display when you run the wizard, click the arrow to display it.



6.2 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.

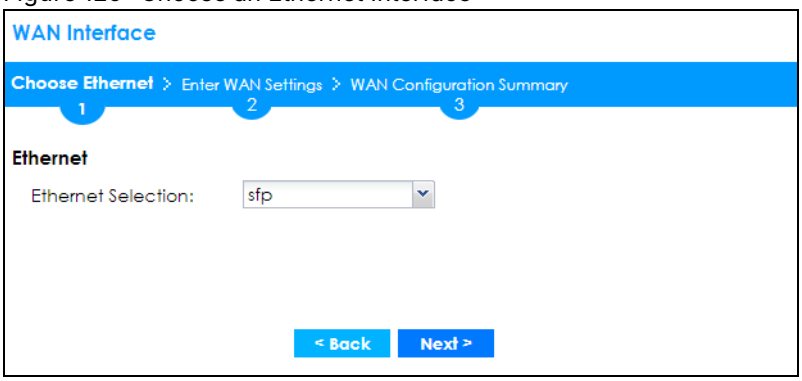
Figure 124 WAN Interface Quick Setup Wizard



6.2.1 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 125 Choose an Ethernet Interface

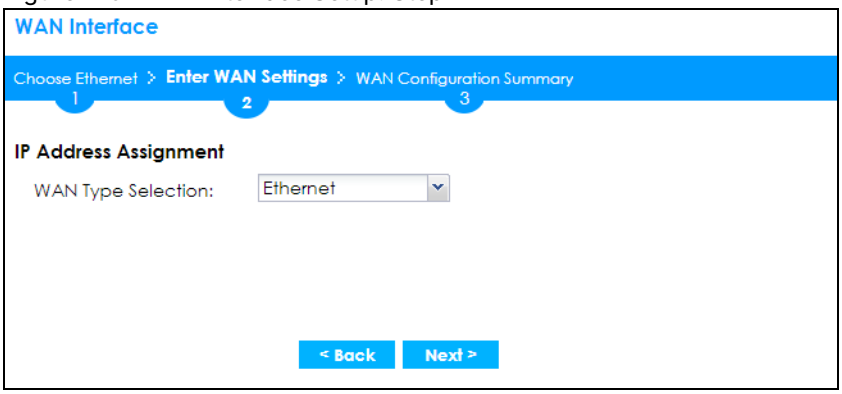


6.2.2 Select WAN Type

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 126 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.

6.2.3 Configure WAN IP Settings

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

Figure 127 WAN Interface Setup: Step 2 Ethernet Dynamic IP

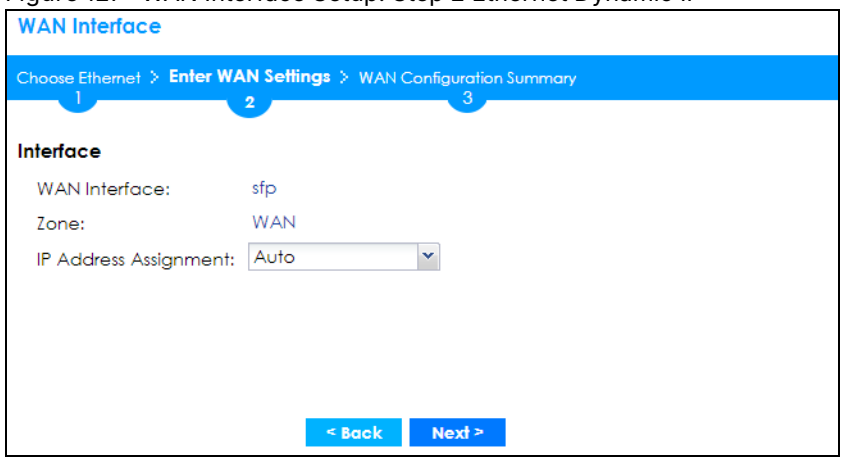
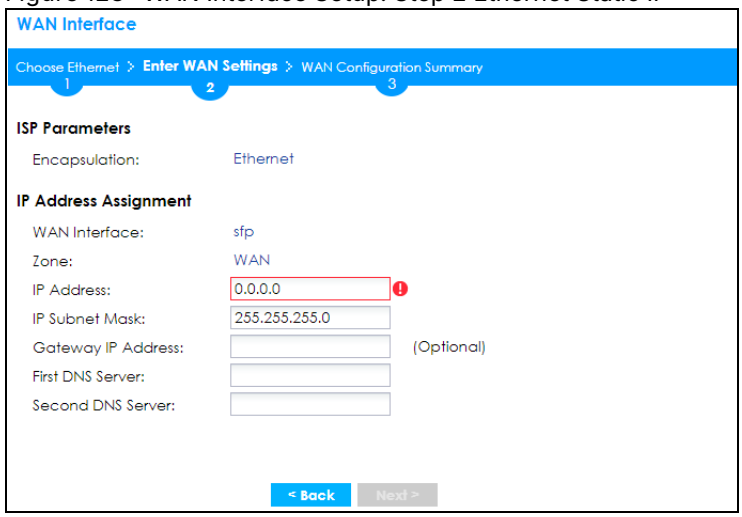


Figure 128 WAN Interface Setup: Step 2 Ethernet Static IP



- 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).

6.2.4 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 129 WAN and ISP Connection Settings: (PPTP)

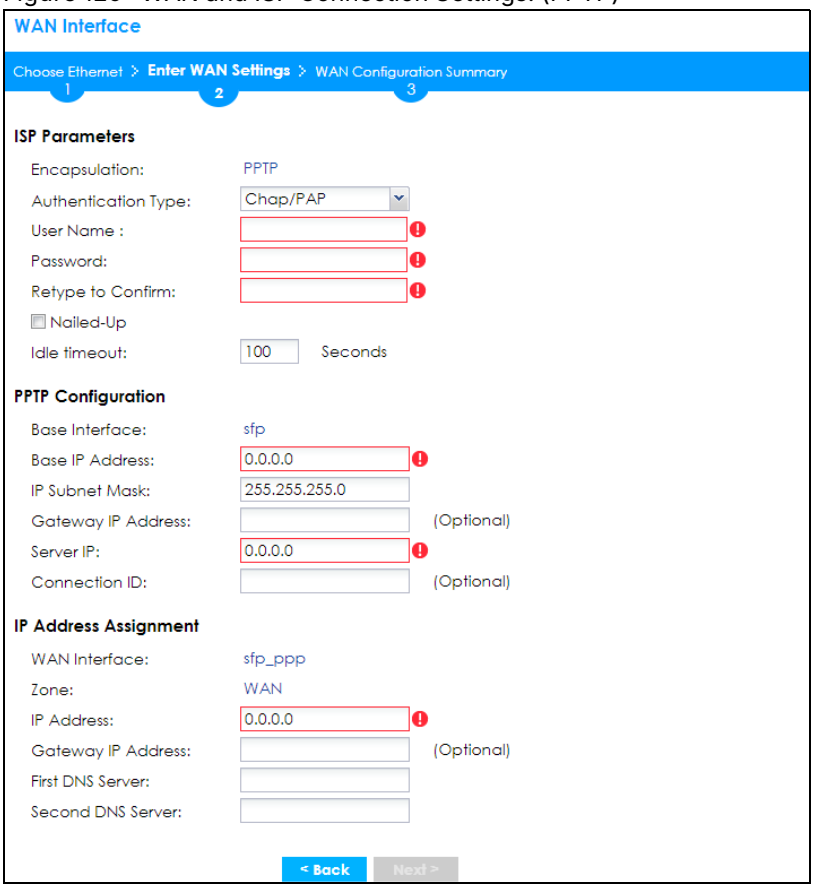


Figure 130 WAN and ISP Connection Settings: (PPPoE)

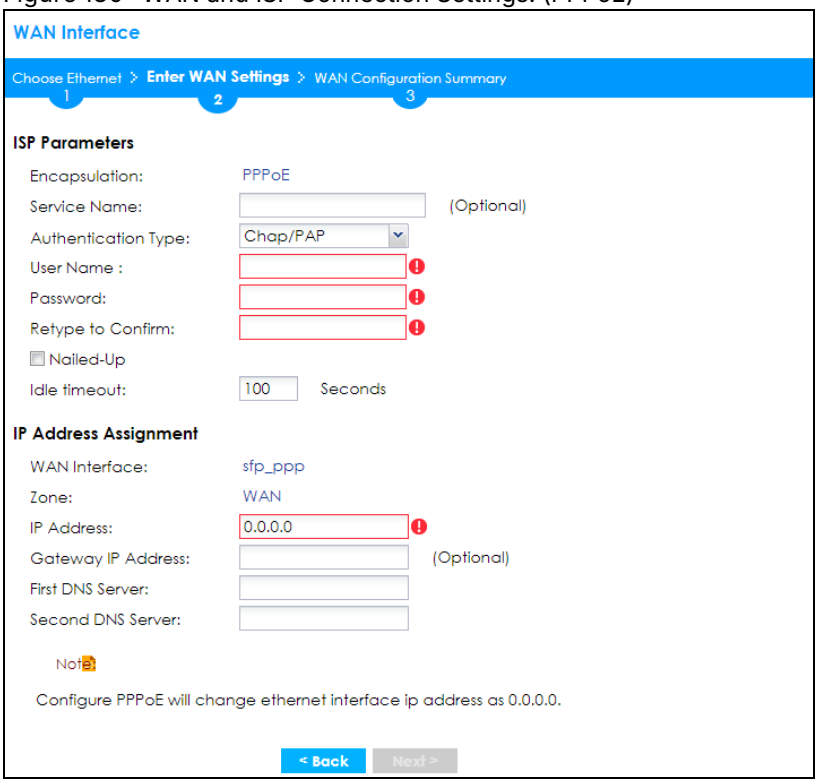
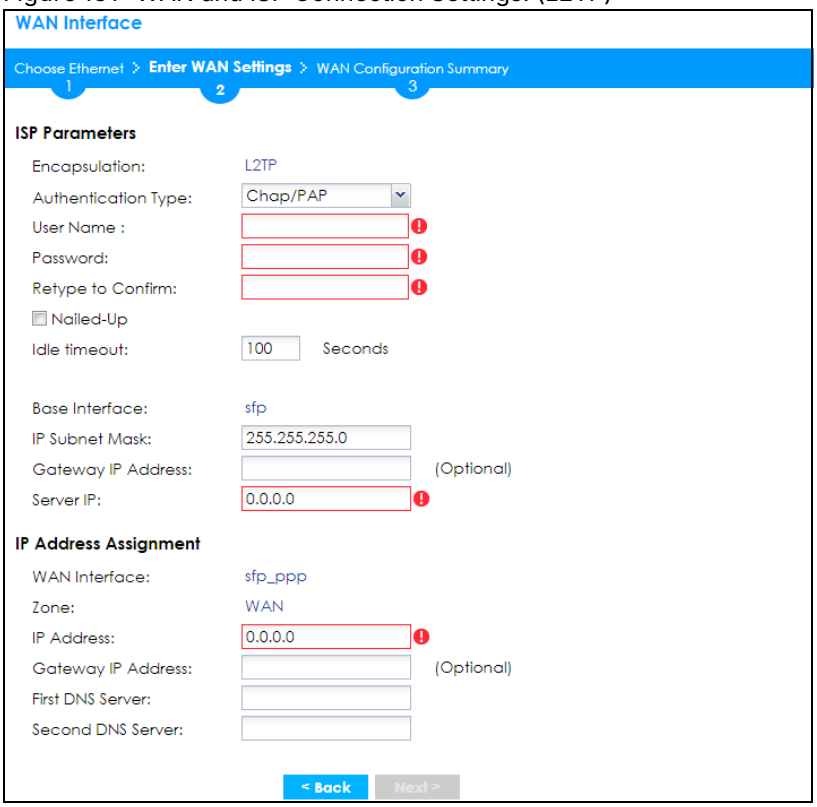


Figure 131 WAN and ISP Connection Settings: (L2TP)



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: Enter 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: Enter 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: Enter 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: Enter your password again for confirmation.
- Nailed-Up: Select Nailed-Up if you do not want the connection to time out.
- Idle Timeout: Enter 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: Enter the (static) IP address assigned to you by your ISP.

- IP Subnet Mask: Enter the subnet mask assigned to you by your ISP (if given).
- Gateway IP Address: For PPTP or L2TP, enter the gateway IP address if you were given one by your ISP.
- Server IP: Enter 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.

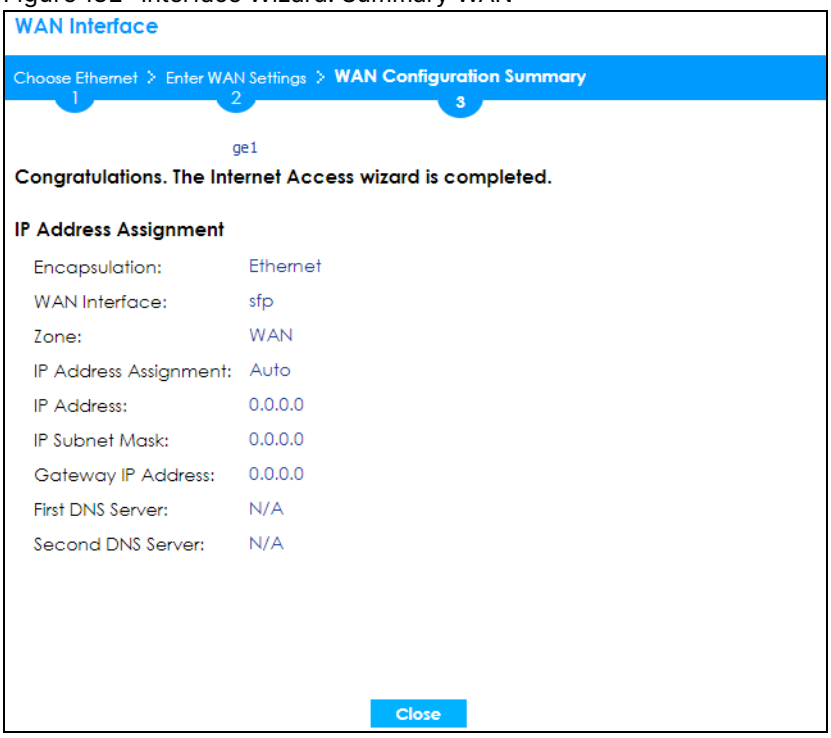
IP Address Assignment

- 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: Enter 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.

6.2.5 Quick Setup Interface Wizard: Summary

This screen displays an example WAN interface's settings.

Figure 132 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).

6.3 Remote Access VPN Setup-Scenario

The purpose of this wizard is to create VPN rules to securely access a company's network from anywhere.

Use the IKEv2 IPSec Client scenario if the VPN client has a SecuExtender VPN client or a non-SecuExtender VPN client.

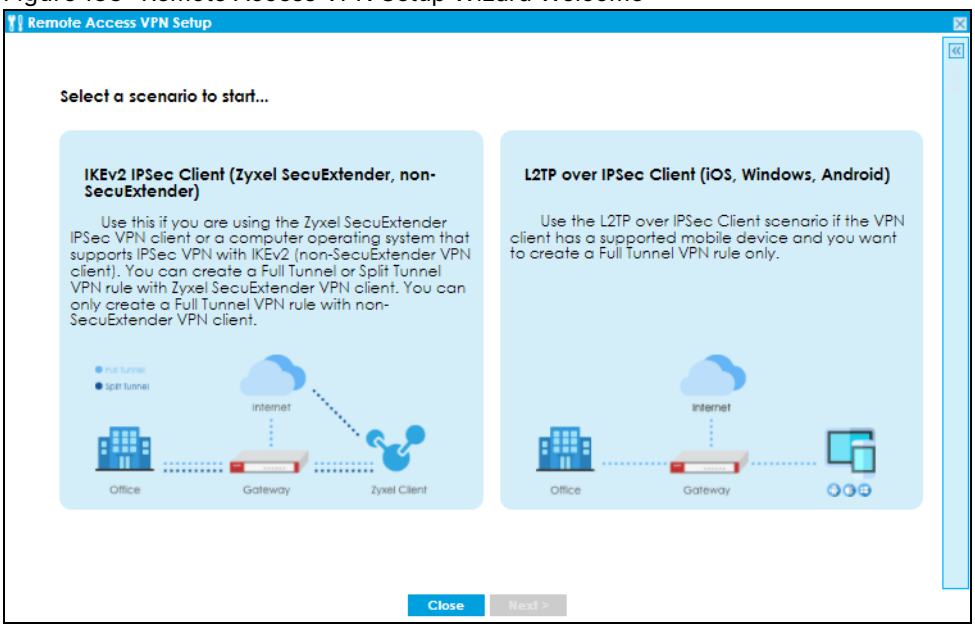
A non-SecuExtender VPN client is a computer or mobile operating system that supports IPSec VPN with IKEv2. The supported computer or mobile operating systems are:

- Windows 8 and later versions.
- iOS 14.8 and later versions.
- macOS 10.12 and later versions.
- Android 10.0 and later versions. Install strongSwan on your device first.

Use the L2TP over IPSec Client scenario if the VPN client has a supported computer or mobile operating system. This scenario supports clients with:

- Windows 8 and later versions.
- iOS 13 and later versions.
- macOS 10.12.2 and later versions.
- Android 10.0 and later versions.

Figure 133 Remote Access VPN Setup Wizard Welcome



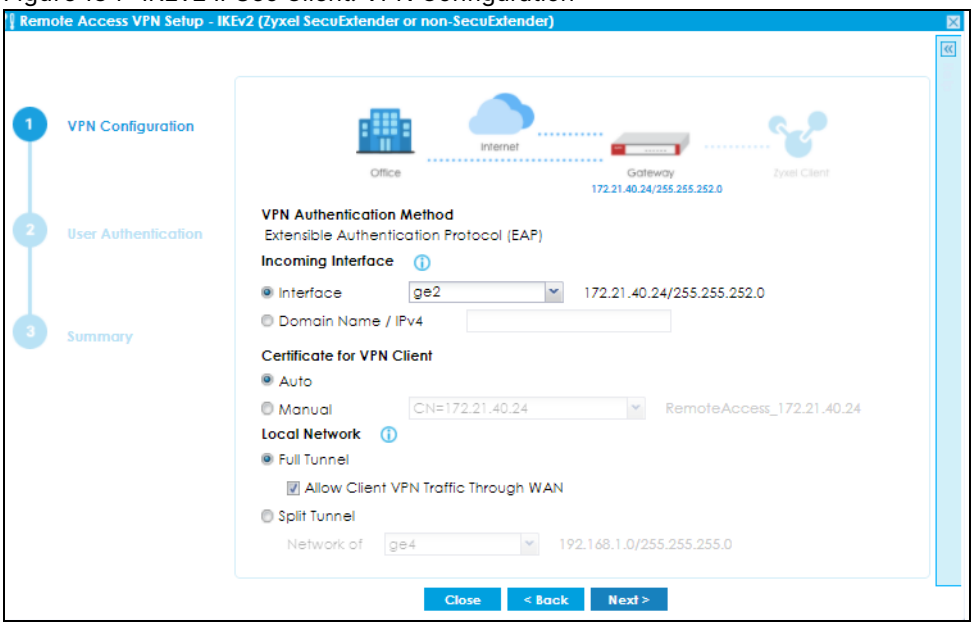
6.3.1 IKEv2 IPSec Client- VPN Configuration

This is for:

- A client using the Zyxel VPN Client with SecuExtender IPSec that wants to create a Full Tunnel or Split Tunnel VPN rule.
- A client using a non-SecuExtender VPN client that wants to create a Full Tunnel VPN rule.

Use this screen to configure basic settings such as pre-shared key, incoming interface and tunnel mode.

Figure 134 IKEv2 IPSec Client: VPN Configuration

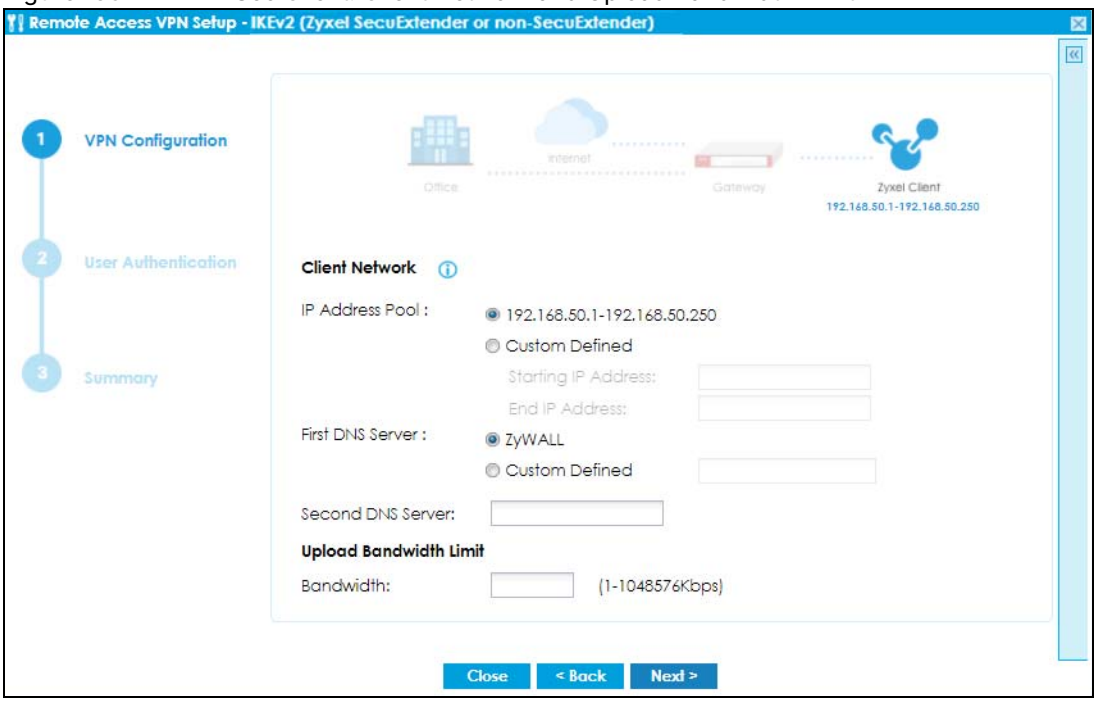


- The IKEv2 IPSec Client scenario supports Extended Authentication Protocol (EAP) authentication. EAP is important when connecting to existing enterprise authentication systems.
- Choose Interface if you want to use a pre-configured interface on the Zyxel Device. Select an interface from the drop-down list box for incoming traffic to your Zyxel Device.
- Choose Domain Name/ IPv4 if you are using a static IP address or if you are using DDNS to assign the interface a dynamic IP address. Enter the domain name or the IP address in the text box. For example, vpn.zyxel.com.
- Choose Auto to have the Zyxel Device generate a certificate from the current wizard settings. This is the certificate the Zyxel Device uses to identify itself when setting up the VPN tunnel.
- Choose Manual to select an existing certificate from the drop down list box. This field is not available if there is no existing certificate for the wizard rule you are configuring.

Note: Please make sure the Host IP Address or the Host Domain Name in the certificate you want to select matches the incoming interface IP Address or Domain Name. If a VPN client is on the WAN, the IP Address or the Domain Name must be public. Create a new certificate in Configuration > Object > Certificate > My Certificate if no existing certificate matches the wizard rule IP Address or Domain Name.

- Full Tunnel encrypts all traffic through the VPN. Clear Allow Client VPN Traffic Through WAN if you want to block traffic from the remote client to the Internet. Select Allow Client VPN Traffic Through WAN to allow only traffic encrypted by the Zyxel Device from the remote client to the Internet.
- Split Tunnel only encrypts traffic going to a networks behind the Zyxel Device. Select the interface to the LAN, DMZ or guest network from the drop-down list box. Traffic going to the Internet through this interface is encrypted. Traffic going to the Internet from the remote client does not go through the Zyxel Device and is not encrypted.

Figure 135 IKEv2 IPSec Client: Client Network and Upload Bandwidth Limit



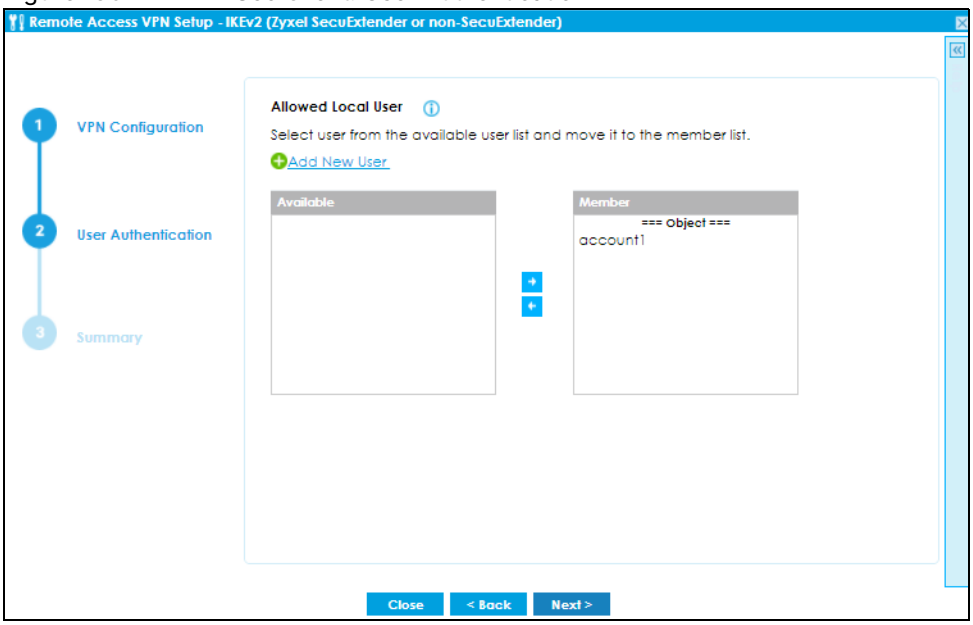
- The IP Address Pool is used to assign IP addresses to the VPN clients. You can define the range of the IP Address Pool by entering a starting IP address and an ending IP address under Customer Defined.
- The Domain Name System (DNS) maps a domain name to an IP address and vice versa. The Zyxel Device uses these to resolve domain names for VPN. The Zyxel Device can act as a DNS proxy. Alternatively, assign a custom DNS server that is reachable from the network behind the Zyxel Device.

- For the Second DNS Server, enter a secondary DNS server's IP address that is checked if the first one is unavailable.
- Upload Bandwidth Limit is only available for Zyxel subscription-based SecuExtender IPSec VPN clients with Windows versions 5.6.80.007 or later or macOS versions 1.2.0.7 or later.
- Use Upload Bandwidth Limit to set the maximum bandwidth for uploading traffic from Zyxel IPSec VPN clients over IPSec VPN tunnels.You can also change the bandwidth limit in Configuration > VPN > IPSec VPN > Configuration Provisioning.

6.3.2 IKEv2 IPSec Client- User Authentication

Use this screen to add users to allow them to access the VPN tunnel.

Figure 136 IKEv2 IPSec Client: User Authentication

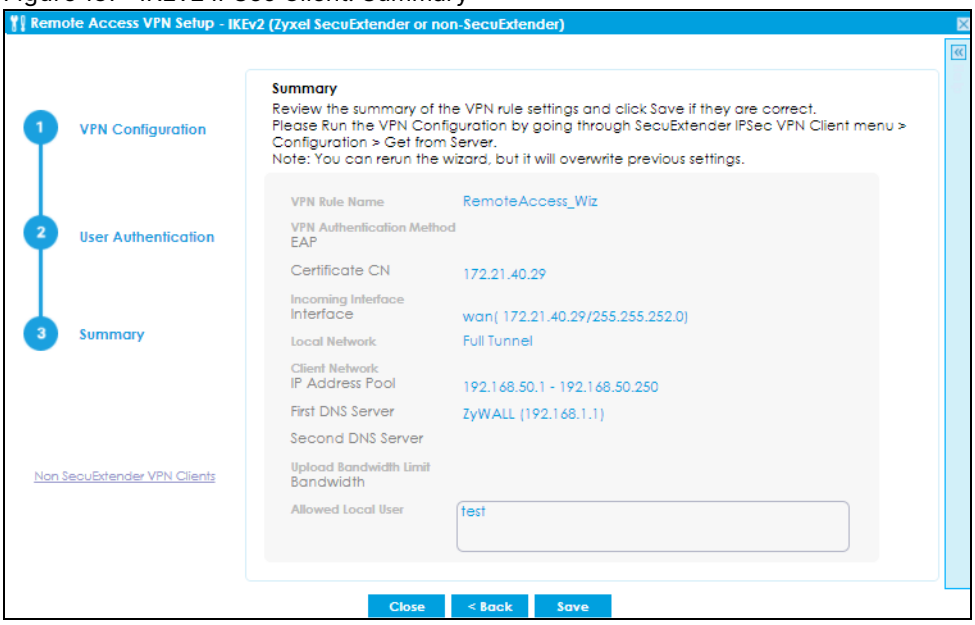


- Only local users configured on the Zyxel Device can be added to the Member list to be allowed VPN access in the wizard.
- If you want to add users from external databases, you may modify the rule in Configuration > Object > User/Group > User > Add A User in Expert Mode.

6.3.3 IKEv2 IPSec Client- Summary

Use this screen to view the summary of your previous configuration.

Figure 137 IKEv2 IPSec Client: Summary

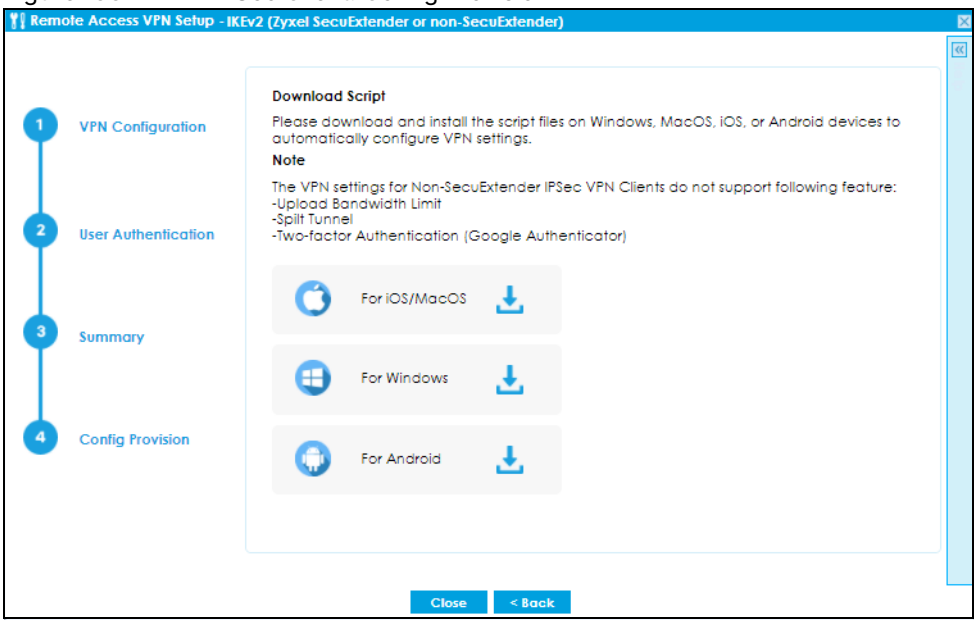


- The default name for the VPN rule created using the wizard is RemoteAccess_Wiz.
- After you click Save, the RemoteAccess_Wiz rule now appears in VPN > IPSec VPN > VPN Connection and VPN > IPSec VPN > VPN Gateway. If you modify a rule created using the wizard here, please change the name. If you want to rerun the wizard without changing the name, you will be prompted to overwrite the previously modified VPN rule.

6.3.4 IKEv2 IPSec Client-Config Provision

Click Non SecuExtender VPN Client on the left to show the following screen. This scenario is for VPN clients without SecuExtender IPSec. Use this screen to download a VPN configuration script to send to VPN clients using supported operating systems.

Figure 138 IKEv2 IPSec Client: Config Provision



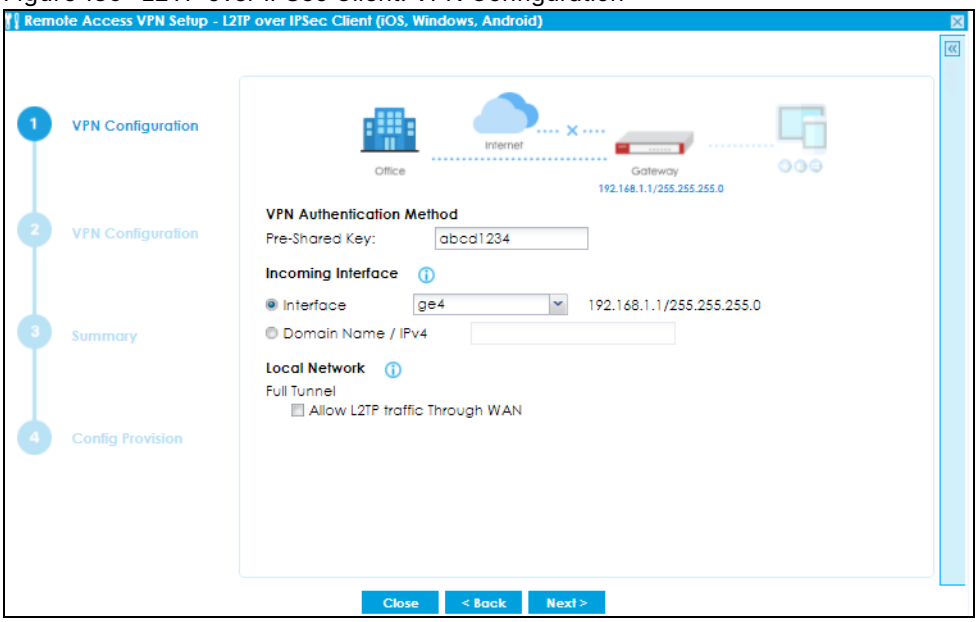
To use the Download Script, your device needs to support:

- For supported Windows, iOS and macOS clients, click the link to download the VPN configuration script and send it to the remote VPN client.
- For Android clients, install strongSwan on your Android device first. Then click the link to download the VPN configuration script and send it to the client along with the Pre-Shared Key.

6.3.5 L2TP over IPSec Client-VPN Configuration

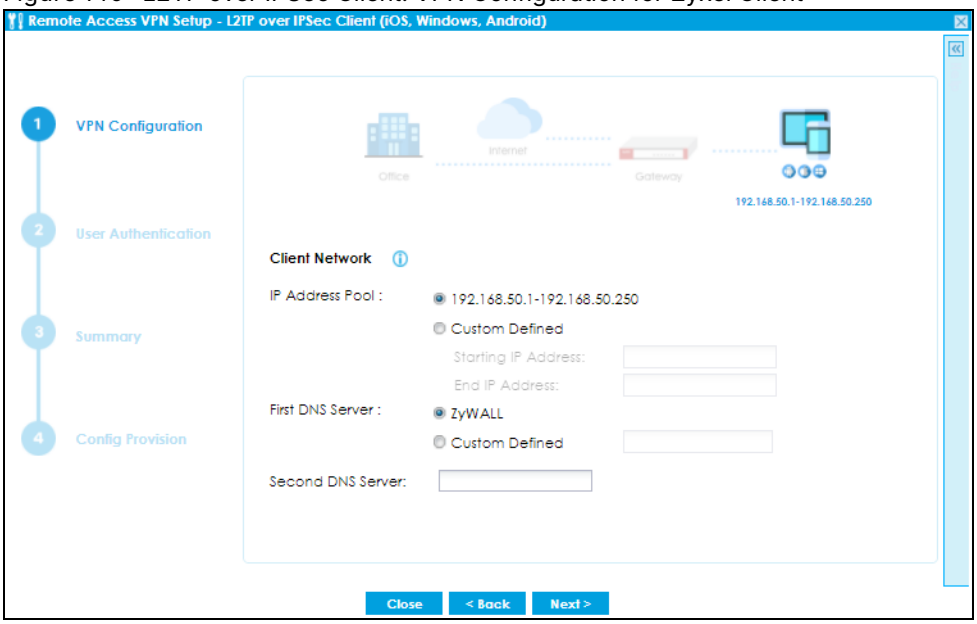
This scenario is for a client using a L2TP over IPSec Client with supported computer or mobile operating systems that wants to create a Full Tunnel VPN rule only. Use this screen to configure basic settings such as pre-shared key, incoming interface and tunnel mode.

Figure 139 L2TP over IPSec Client: VPN Configuration



- For Pre-Shared Key, enter 8-128 alphanumeric characters (0-9, a-z, A_Z) or 8-128 pairs of hexadecimal characters (0-9, A-F) beginning with 0x.
- Choose Interface if you want to use a pre-configured interface on the Zyxel Device. Select an interface from the drop-down list box for incoming traffic to your Zyxel Device.
- Choose Domain Name/ IPv4 if you are using a static IP address or if you are using DDNS to assign the interface a dynamic IP address. Enter the domain name or the IP address in the text box. For example, vpn.zyxel.com.
- Full Tunnel encrypts all traffic through the VPN. Clear Allow Client VPN Traffic Through WAN if you want to block remote traffic from the remote client to the Internet. Select Allow Client VPN Traffic Through WAN to allow only traffic encrypted by the Zyxel Device from the remote client to the Internet.

Figure 140 L2TP over IPSec Client: VPN Configuration for Zyxel Client

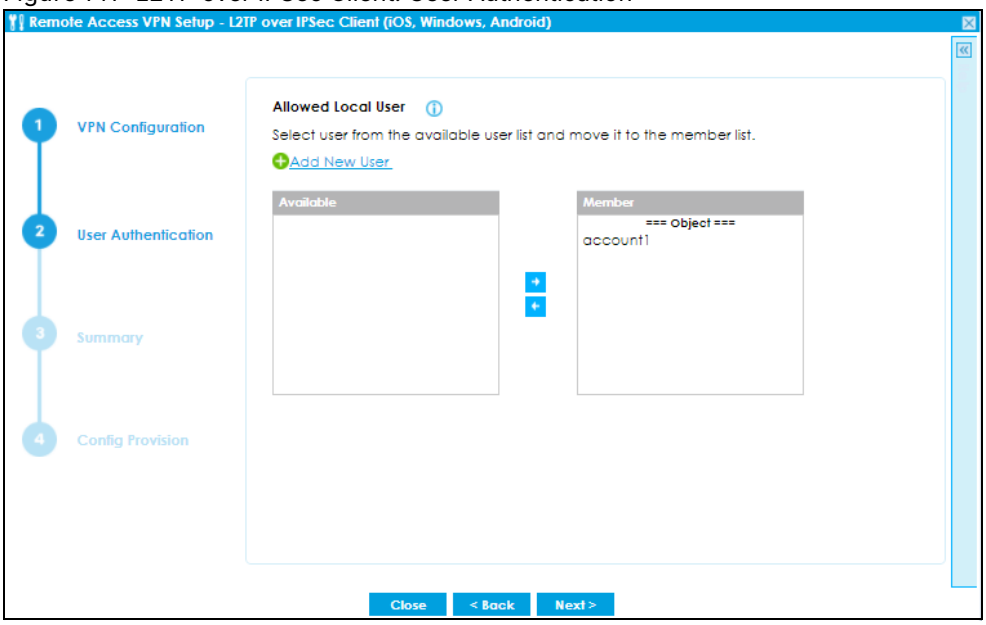


- The IP Address Pool is used to assign to the L2TP VPN clients. Alternatively, you can define the range of the IP Address Pool by entering a starting IP address and an ending IP address under Customer Defined.
- The Domain Name System (DNS) maps a domain name to an IP address and vice versa. The Zyxel Device uses these to resolve domain names for VPN. The Zyxel Device can act as a DNS proxy. Alternatively, assign a custom DNS server that is reachable from then network behind the Zyxel Device.
- For the Second DNS Server, enter a secondary DNS server's IP address that is checked if the first one is unavailable.

6.3.6 L2TP over IPSec Client- User Authentication

Use this screen to add users to allow them to access the VPN.

Figure 141 L2TP over IPSec Client: User Authentication



- Only local users configured on the Zyxel Device can be added to the Member list to be allowed VPN access in the wizard.
- If you want to add users from external databases, you may modify the rule in Configuration > Object > User/Group > User > Add A User in Expert Mode.

6.3.7 L2TP over IPSec Client- Summary

Use this screen to view the summary of your previous configuration.

Figure 142 L2TP over IPSec Client: User Summary

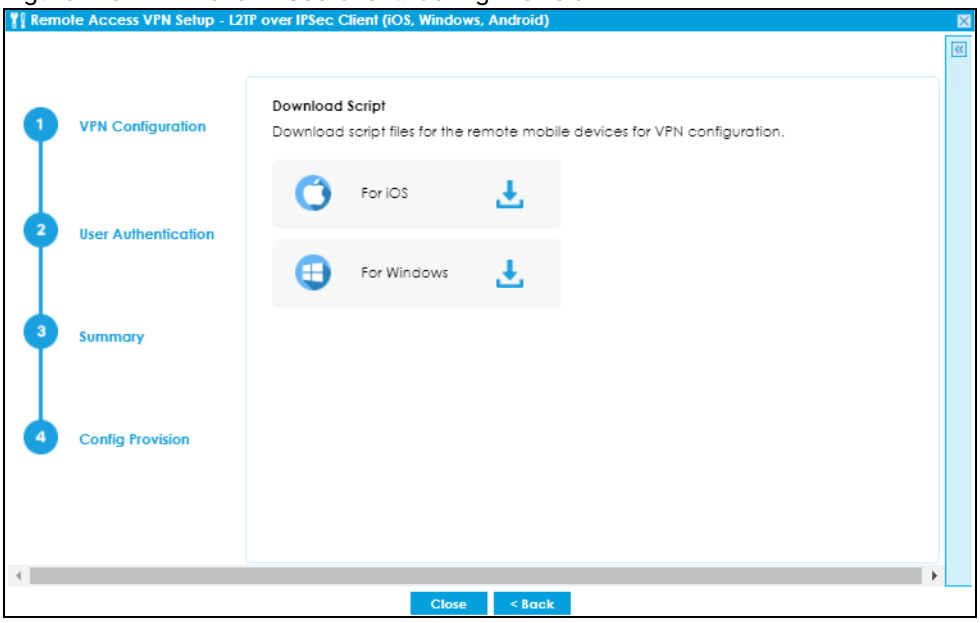
- The default name for the VPN rule created using the wizard is RemoteAccess_L2TP_Wiz.

- After you click Save, the RemoteAccess_L2TP_Wiz rule now appears in VPN > L2TP VPN. If you modify a rule created using the wizard here, please change the name. If you want to rerun the wizard without changing the name, you will be prompted to overwrite the previously modified VPN rule.

6.3.8 L2TP over IPSec Client-Config Provision

Use this screen to download a VPN configuration script to send to VPN clients using supported operating systems.

Figure 143 L2TP over IPSec Client: Config Provision



To use the Download Script, your device needs to support:

- For Windows, iOS and macOS clients, click the link to download the VPN configuration script and send it to the remote VPN client.
- For and Android and Windows 7 clients, you need to configure the rule manually. Send the Pre-Shared Key and the Zyxel Device interface IP or domain name to the client. Users with Android 10.0 and later versions or Windows 7 must configure an L2TP over IPSec rule on their mobile device using this information.

6.4 VPN Setup Wizard

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

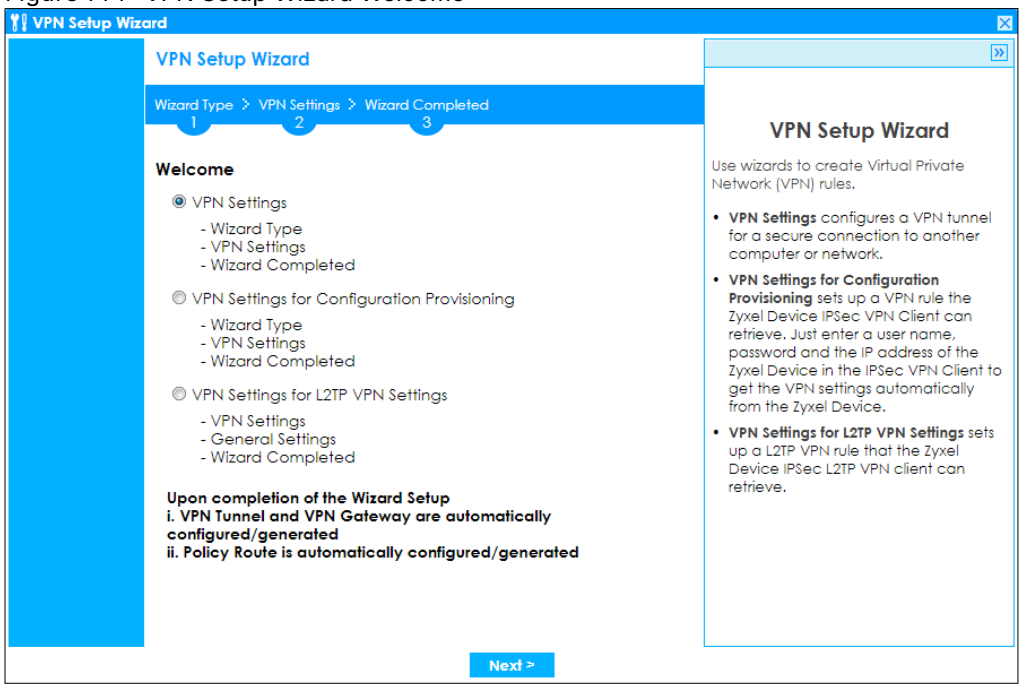
6.4.1 Welcome

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 144 VPN Setup Wizard Welcome

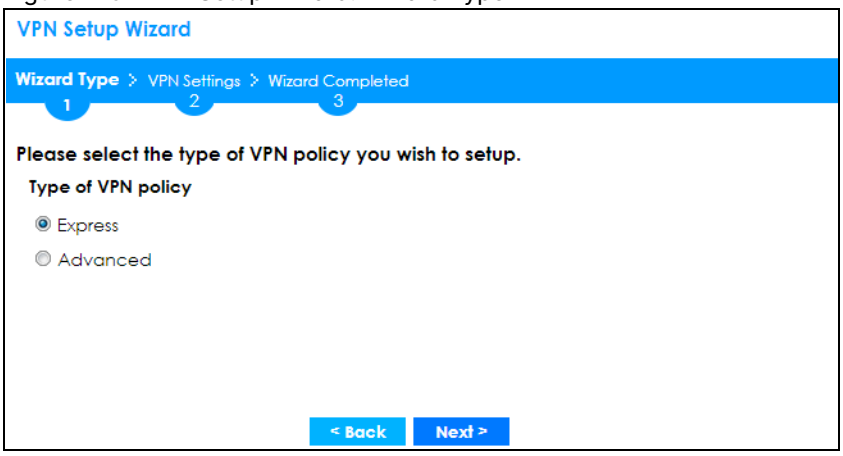


6.4.2 VPN Setup Wizard: Wizard Type

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.

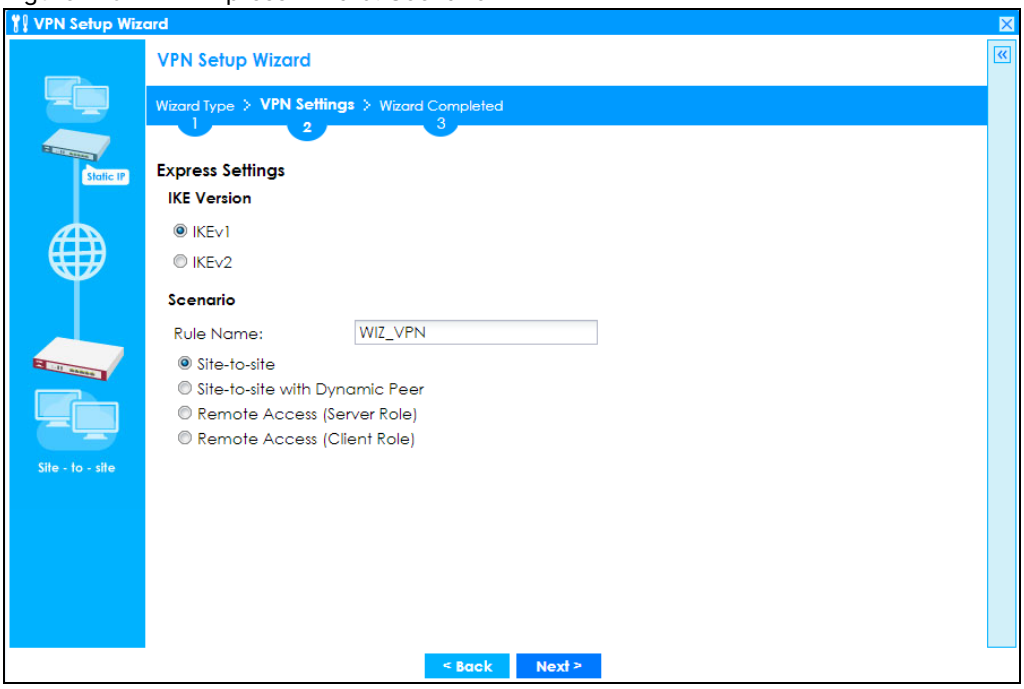
Figure 145 VPN Setup Wizard: Wizard Type



6.4.3 VPN Express Wizard - Scenario

Click the Express radio button as shown in Figure 145 on page 174 to display the following screen.

Figure 146 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: Enter 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.

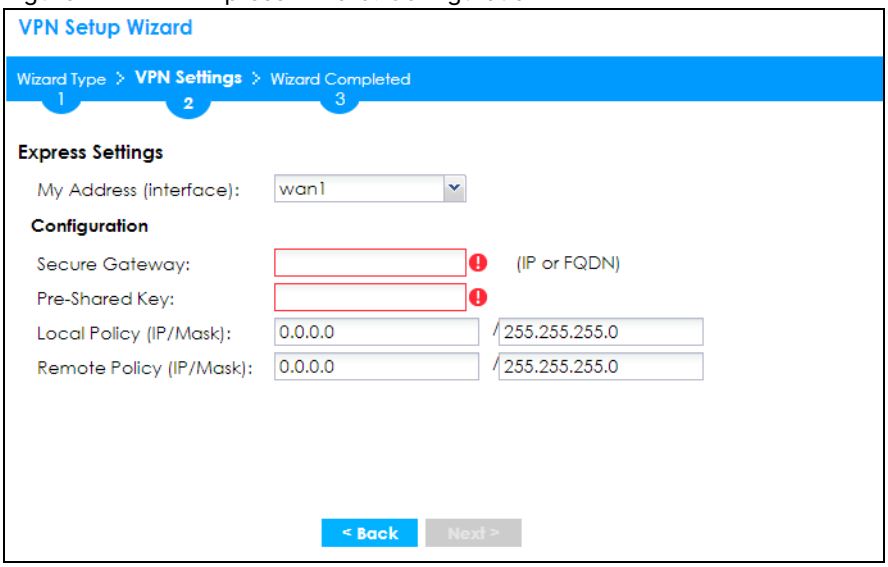
Select the scenario that best describes your intended VPN connection. The figure on the left of the screen changes to match the scenario you select.

- 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.

6.4.4 VPN Express Wizard - Configuration

Figure 147 VPN Express Wizard: Configuration

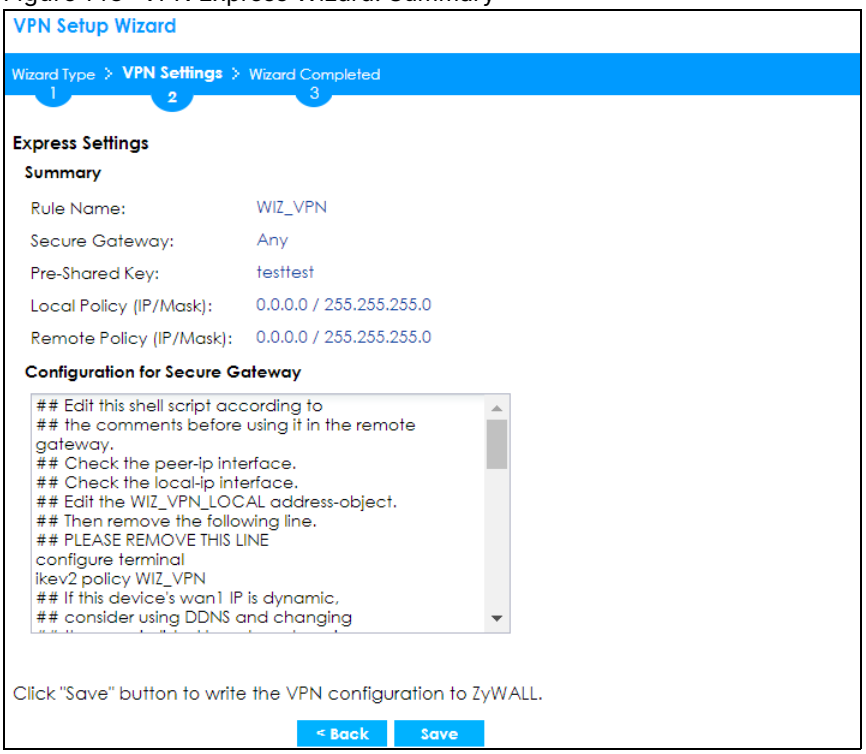


- My Address (interface): Select an interface from the drop-down list box to use on your Zyxel Device.
- Secure Gateway: Any displays in this field if it is not configurable for the chosen scenario. Otherwise, enter the WAN IP address or domain name of the remote IPSec device (secure gateway) to identify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

6.4.5 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 148 VPN Express Wizard: Summary

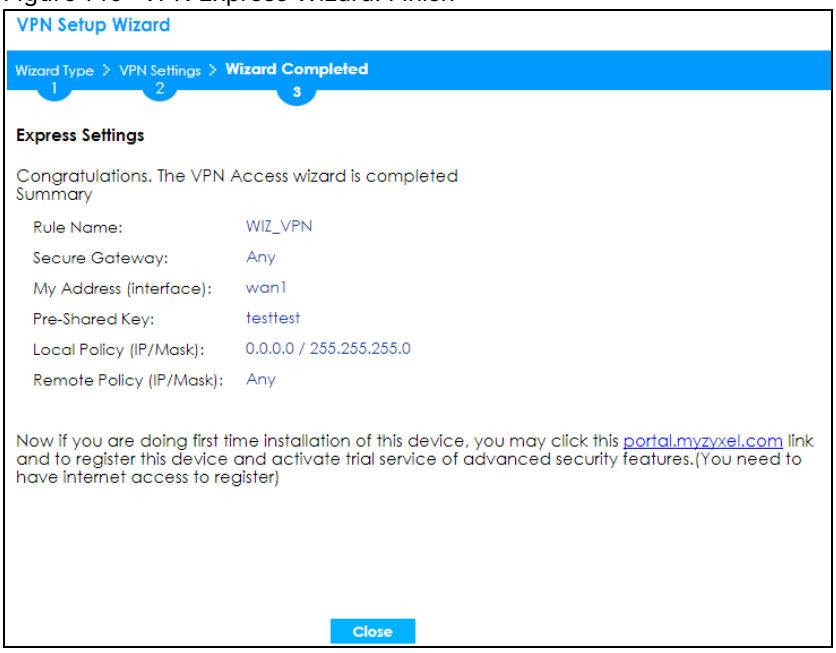


- Rule Name: Identifies the VPN gateway policy.
- Secure Gateway: IP address or domain name of the remote IPSec device. If this field displays Any, only the remote IPSec device can initiate the VPN connection.
- Pre-Shared Key: VPN tunnel password. It identifies a communicating party during a phase 1 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.

6.4.6 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 149 VPN Express Wizard: Finish

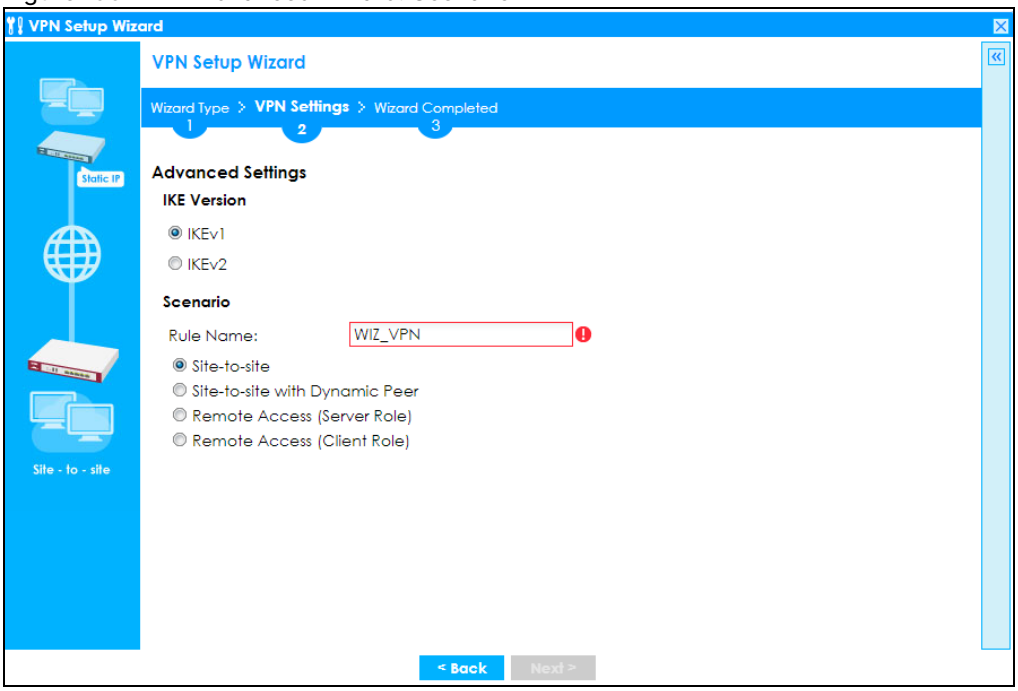


Click Close to exit the wizard.

6.4.7 VPN Advanced Wizard - Scenario

Click the Advanced radio button as shown in Figure 145 on page 174 to display the following screen.

Figure 150 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: Enter 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.

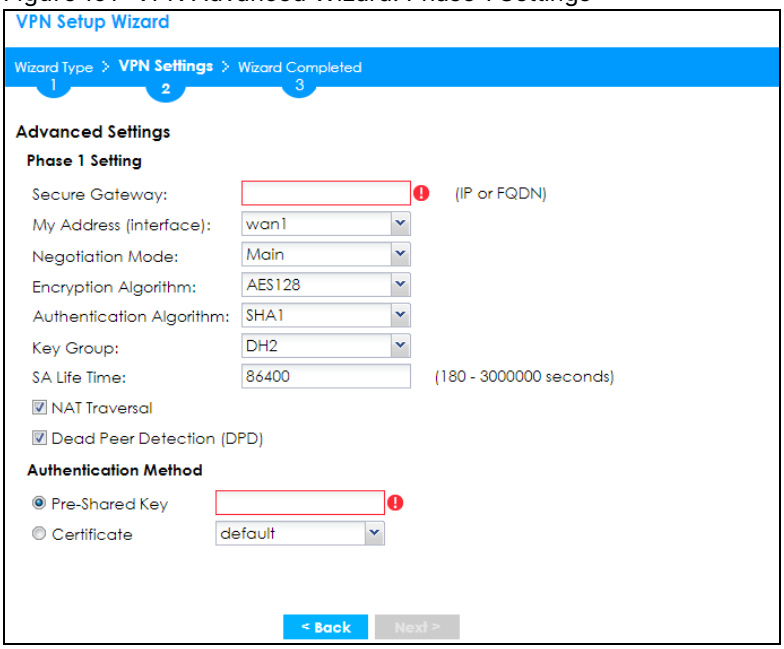
Select the scenario that best describes your intended VPN connection. The figure on the left of the screen changes to match the scenario you select.

- 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.

6.4.8 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 151 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 Zyxel Device'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 Zyxel Device 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).

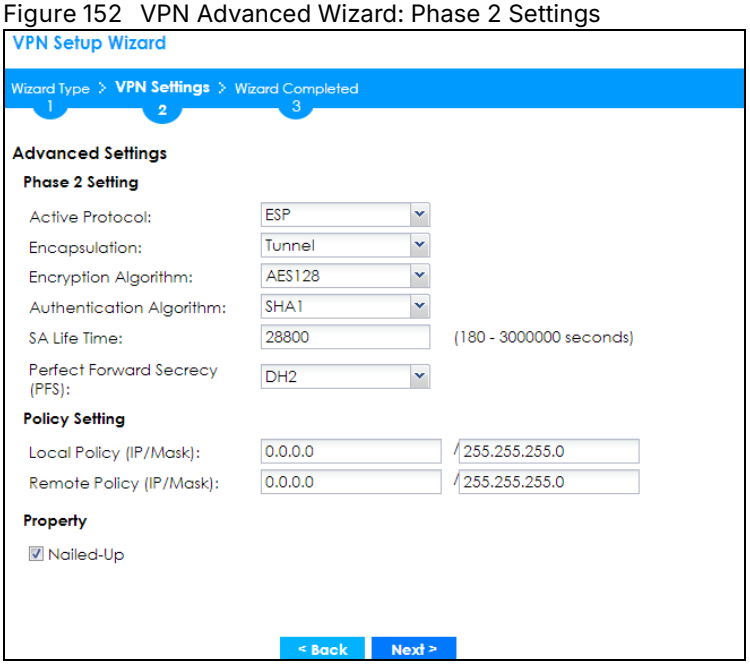
Note: The remote IPSec device must also have NAT traversal enabled. See the help in the main IPSec VPN screens for more information.

- 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.

6.4.9 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 152 VPN Advanced Wizard: Phase 2 Settings



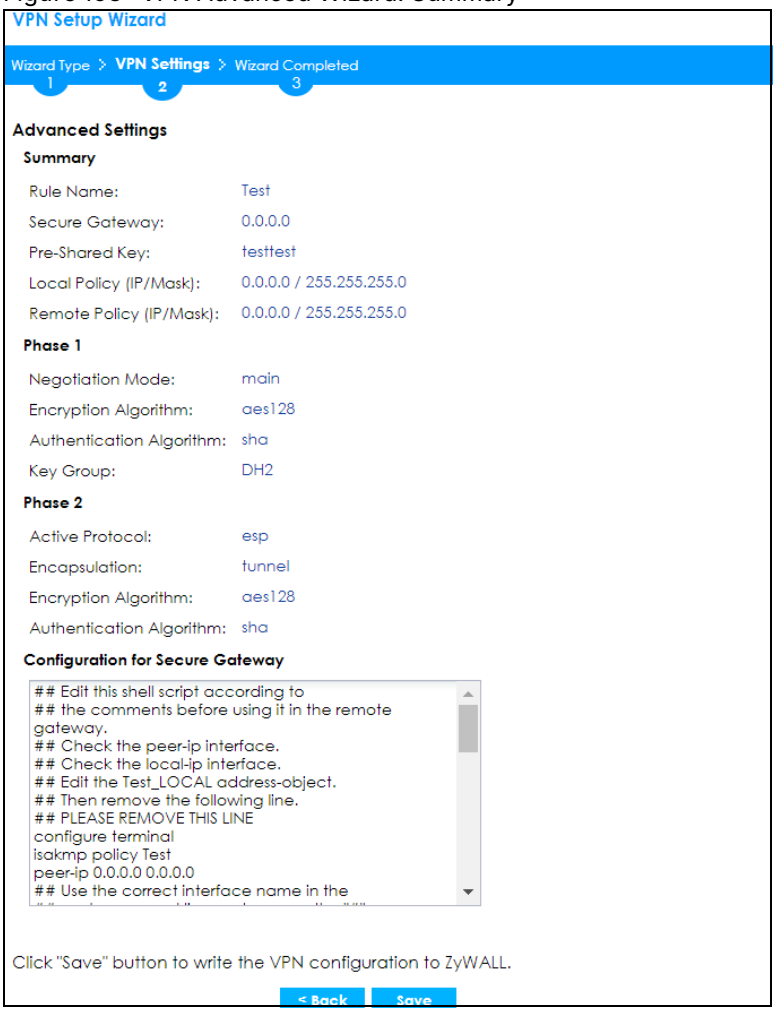
- Active Protocol: ESP is compatible with NAT, AH is not.
- Encapsulation: Tunnel is compatible with NAT, Transport is not.
- Encryption Algorithm: 3DES and AES use encryption. The longer the AES key, the higher the security (this may affect throughput). Null uses no encryption.
- Authentication Algorithm: 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): Enter 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): Enter 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.

6.4.10 VPN Advanced Wizard - Summary

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

Figure 153 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 Zyxel Device'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 Zyxel Device 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.

6.4.11 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 154 VPN Wizard: Finish

Click Close to exit the wizard.

6.5 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.

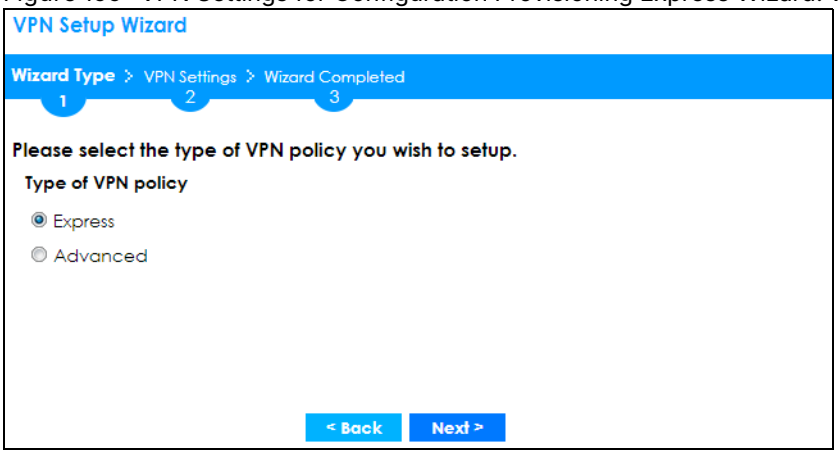
VPN rules for the Zyxel Device IPSec VPN Client have certain restrictions. They must *not* contain the following settings:

- 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.

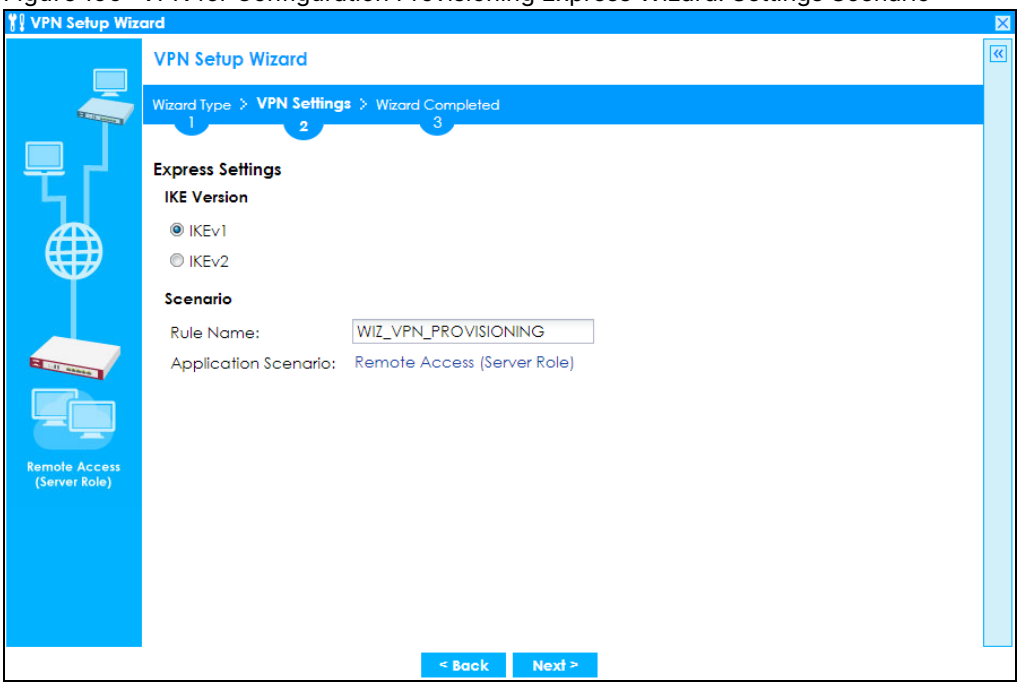
Figure 155 VPN Settings for Configuration Provisioning Express Wizard: Wizard Type



6.5.1 Configuration Provisioning Express Wizard - VPN Settings

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

Figure 156 VPN for Configuration Provisioning Express Wizard: Settings Scenario

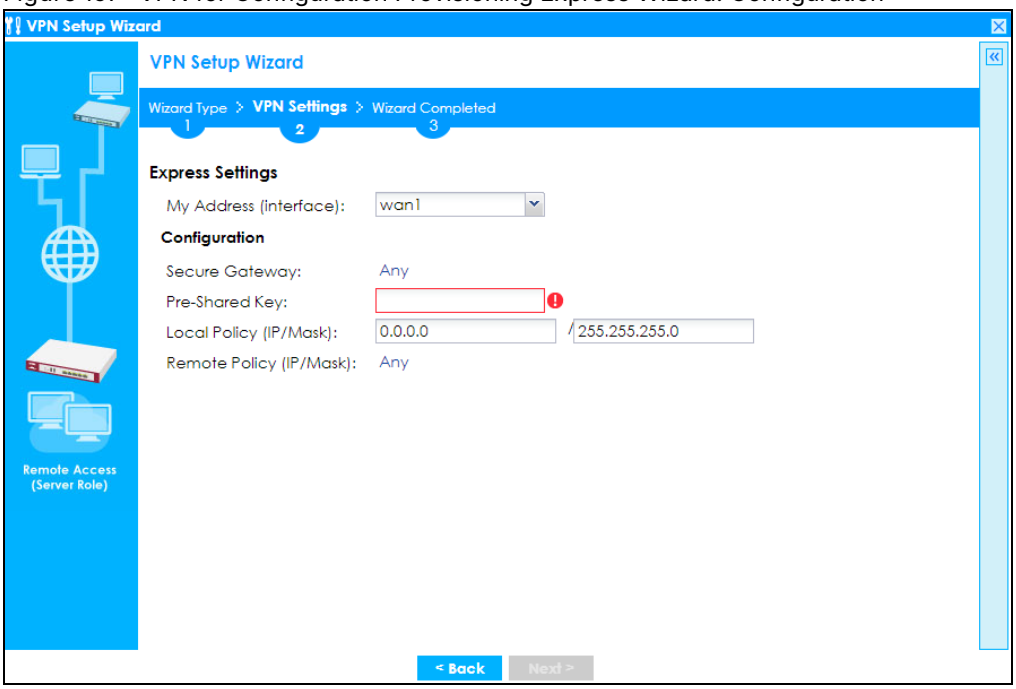


- IKE (Internet Key Exchange) is a protocol used in security associations to send data securely. IKE uses certificates or pre-shared keys for authentication and a Diffie–Hellman key exchange to set up a shared session secret from which encryption keys are derived.
- IKEv2 supports Extended Authentication Protocol (EAP) authentication, and IKEv1 supports X-Auth. EAP is important when connecting to existing enterprise authentication systems.
- Rule Name: Enter 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.

6.5.2 Configuration Provisioning VPN Express Wizard - Configuration

Click Next to continue the wizard.

Figure 157 VPN for Configuration Provisioning Express Wizard: Configuration

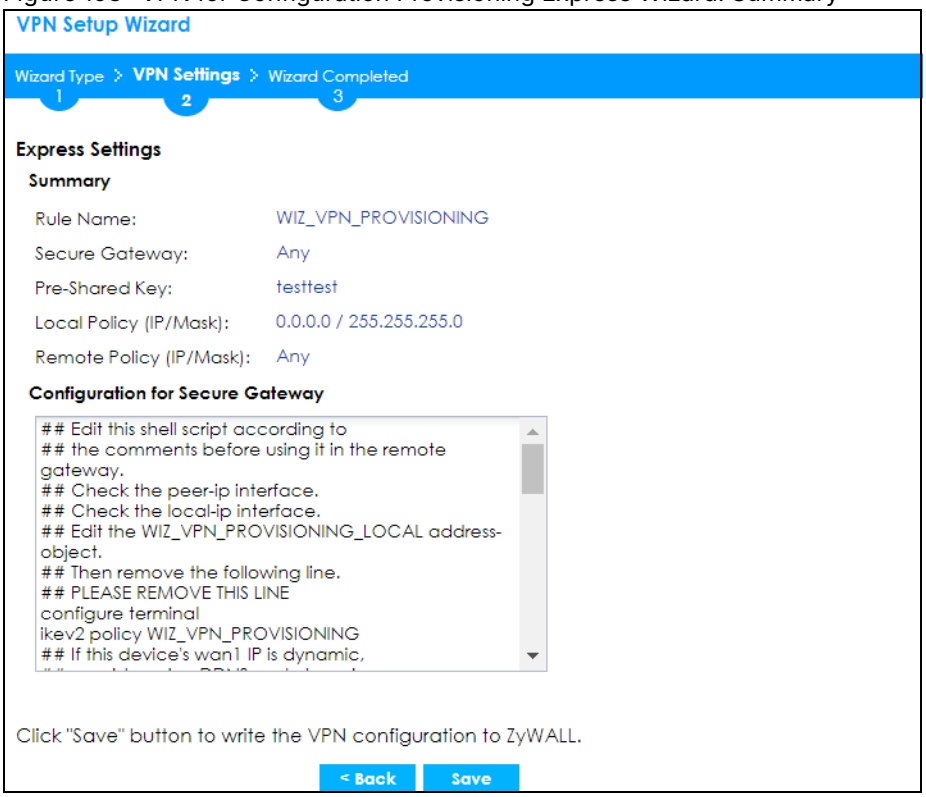


- My Address (interface): Select an interface from the drop-down list box to use on your Zyxel Device.
- Secure Gateway: Any displays in this field because it is not configurable in this wizard. It allows incoming connections from the Zyxel Device IPSec VPN Client.
- Pre-Shared Key: Enter the password. 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): Enter 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.

6.5.3 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 158 VPN for Configuration Provisioning Express Wizard: Summary

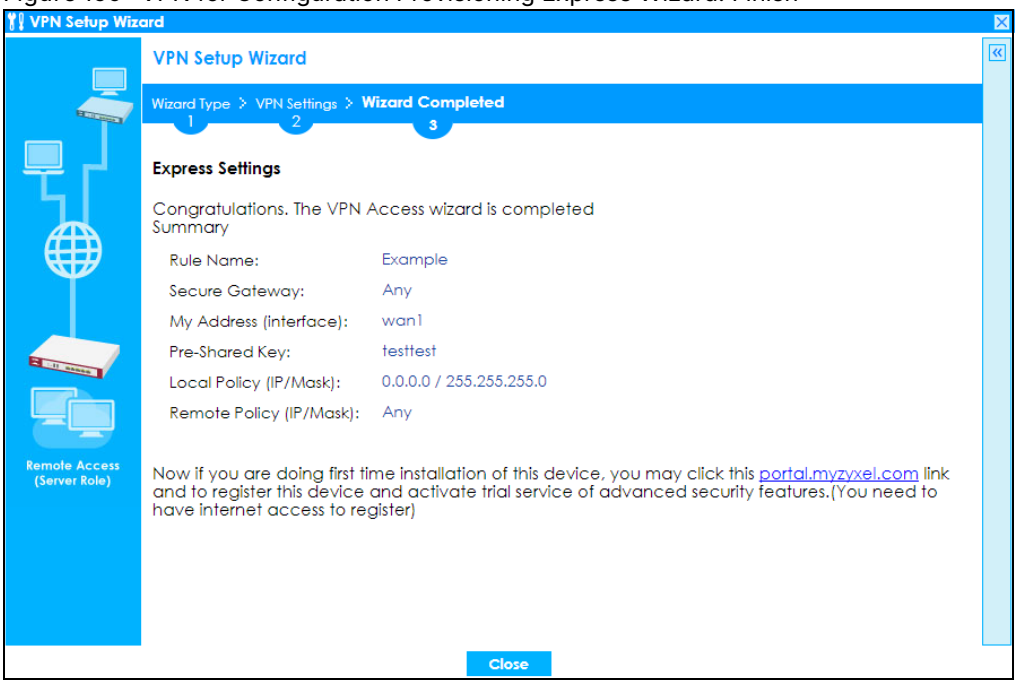


- Rule Name: Identifies the VPN gateway policy.
- Secure Gateway: Any displays in this field because it is not configurable in this wizard. It allows incoming connections from the Zyxel Device IPSec VPN Client.
- Pre-Shared Key: VPN tunnel password. It identifies a communicating party during a phase 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.

6.5.4 VPN Settings for Configuration Provisioning Express Wizard - Finish

The rule is now 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 159 VPN for Configuration Provisioning Express Wizard: Finish

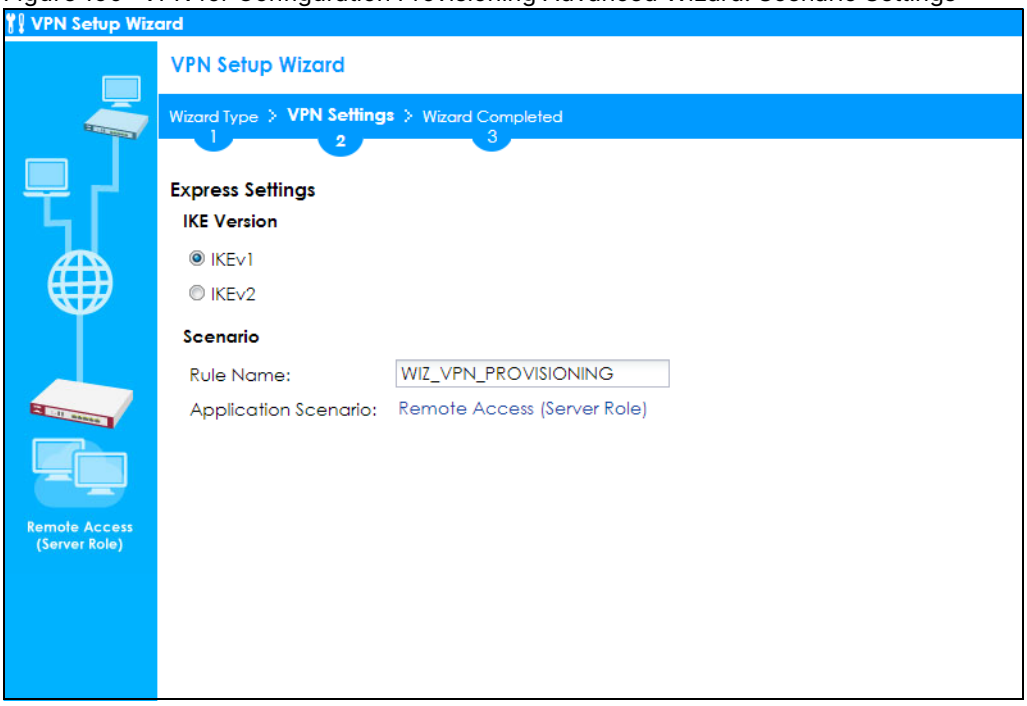


Click Close to exit the wizard.

6.5.5 VPN Settings for Configuration Provisioning Advanced Wizard - Scenario

Click the Advanced radio button as shown in Figure 155 on page 185 to display the following screen.

Figure 160 VPN for Configuration Provisioning Advanced Wizard: Scenario Settings



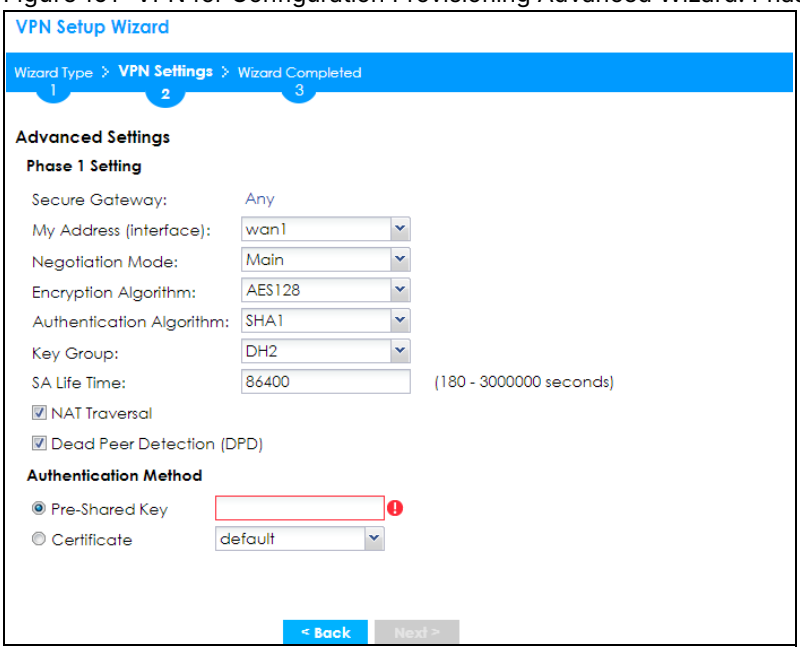
- IKE (Internet Key Exchange) is a protocol used in security associations to send data securely. IKE uses certificates or pre-shared keys for authentication and a Diffie–Hellman key exchange to set up a shared session secret from which encryption keys are derived.
- IKEv2 supports Extended Authentication Protocol (EAP) authentication, and IKEv1 supports X-Auth. EAP is important when connecting to existing enterprise authentication systems.
- Rule Name: Enter 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.

6.5.6 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 161 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 Zyxel Device'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.

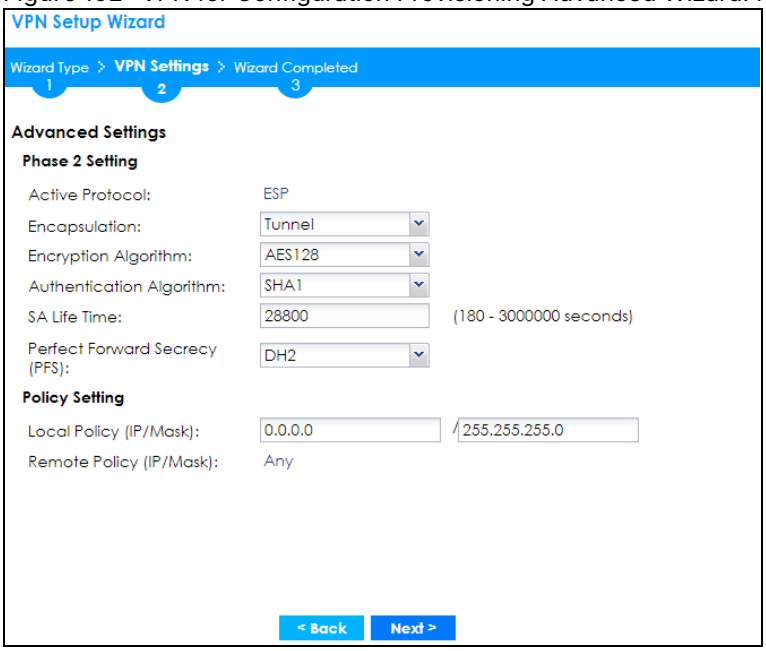
The Zyxel Device and the remote IPSec router must use the same negotiation mode. Multiple SAs connecting through a secure gateway must have the same negotiation mode.

- 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.

6.5.7 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 162 VPN for Configuration Provisioning Advanced Wizard: Phase 2 Settings



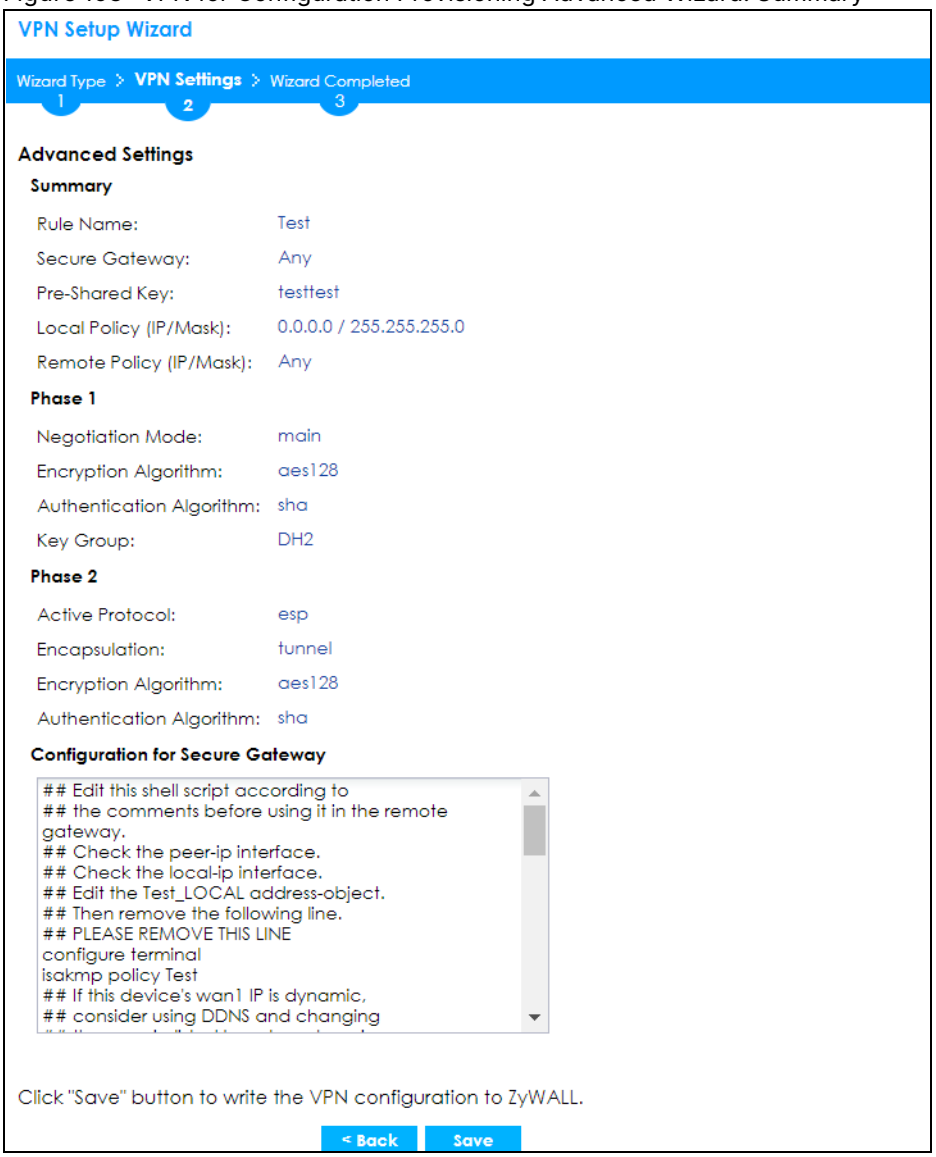
- Active Protocol: ESP is compatible with NAT. AH is not available in this wizard.
- Encapsulation: Tunnel is compatible with NAT, Transport is not.
- Encryption Algorithm: 3DES and AES use encryption. The longer the AES key, the higher the security (this may affect throughput). Null uses no encryption.
- 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): Enter 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.
- 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.

6.5.8 VPN Settings for Configuration Provisioning Advanced Wizard - Summary

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

Figure 163 VPN for Configuration Provisioning Advanced Wizard: Summary



Summary

- Rule Name: Identifies the VPN connection (and the VPN gateway).
- 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.
- 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 Zyxel Device'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 Zyxel Device 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.

6.5.9 VPN Settings for Configuration Provisioning Advanced Wizard - Finish

The rule is now 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.

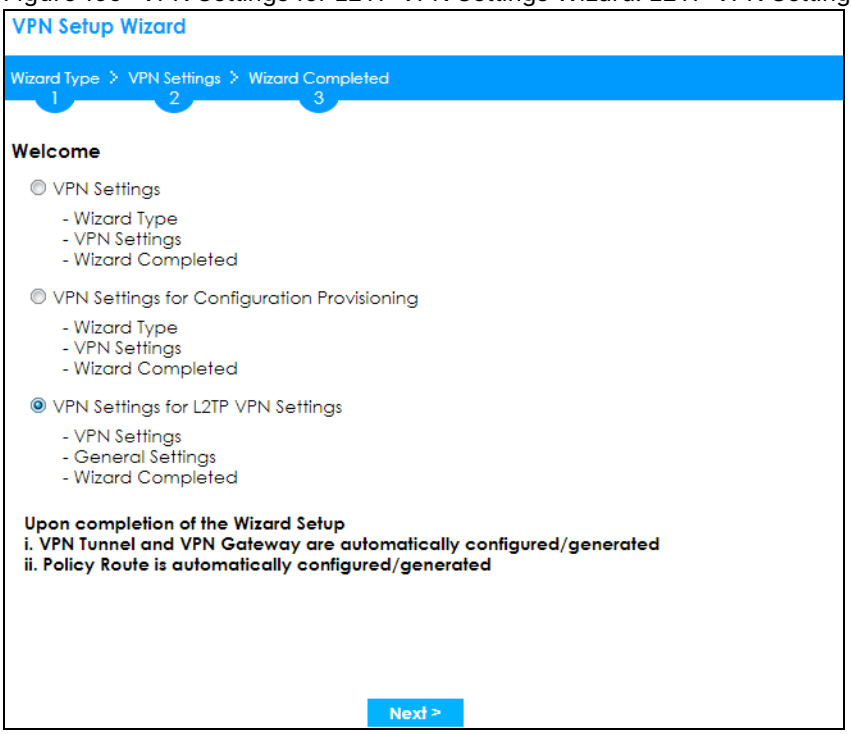
Figure 164 VPN for Configuration Provisioning Advanced Wizard: Finish

Click Close to exit the wizard.

6.6 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.

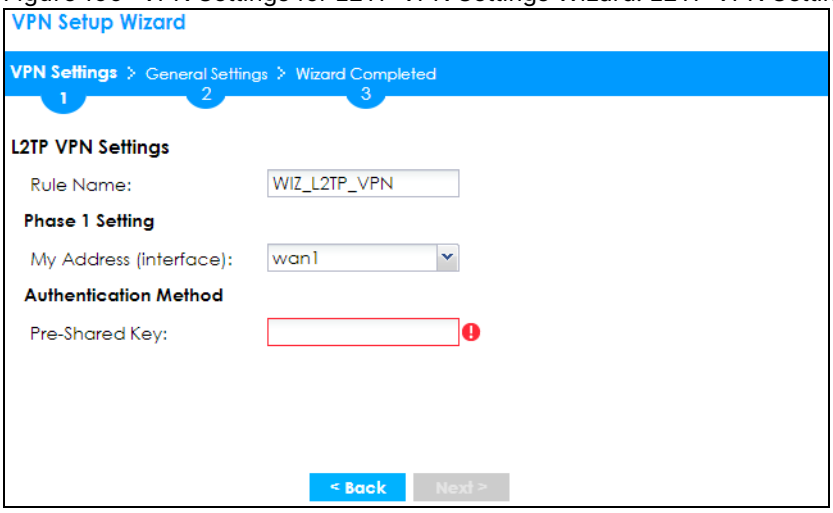
Figure 165 VPN Settings for L2TP VPN Settings Wizard: L2TP VPN Settings



Click Next to continue the wizard.

6.6.1 L2TP VPN Settings

Figure 166 VPN Settings for L2TP VPN Settings Wizard: L2TP VPN Settings

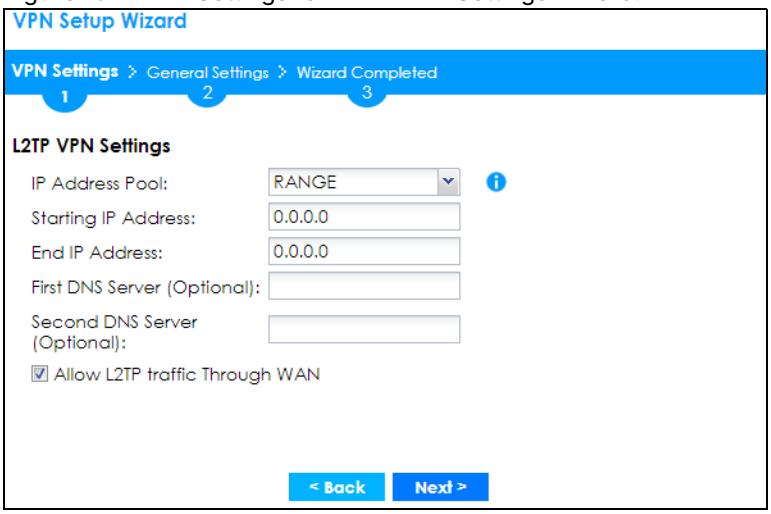


- Rule Name: Enter the name used to identify this L2TP VPN connection (and L2TP VPN gateway). You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
- My Address (interface): Select one of the interfaces from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

- Pre-Shared Key: Enter 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.

6.6.2 L2TP VPN Settings

Figure 167 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 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.
- Second DNS Server (Optional): Enter the second DNS server IP address in the field. 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.
- Allow L2TP traffic Through WAN: Select this checkbox to allow traffic from L2TP clients to go to the Internet.

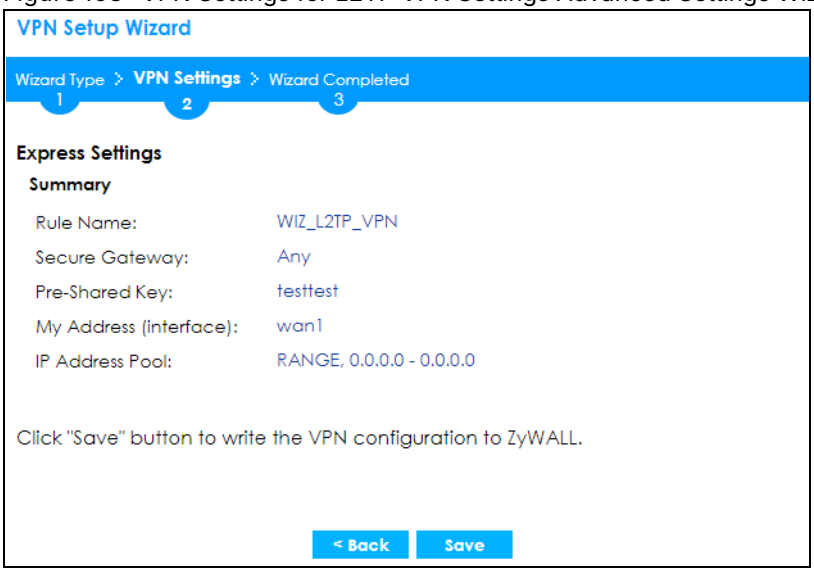
Click Next to continue the wizard.

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.

6.6.3 VPN Settings for L2TP VPN Setting Wizard - Summary

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

Figure 168 VPN Settings for L2TP VPN Settings Advanced Settings Wizard: Summary

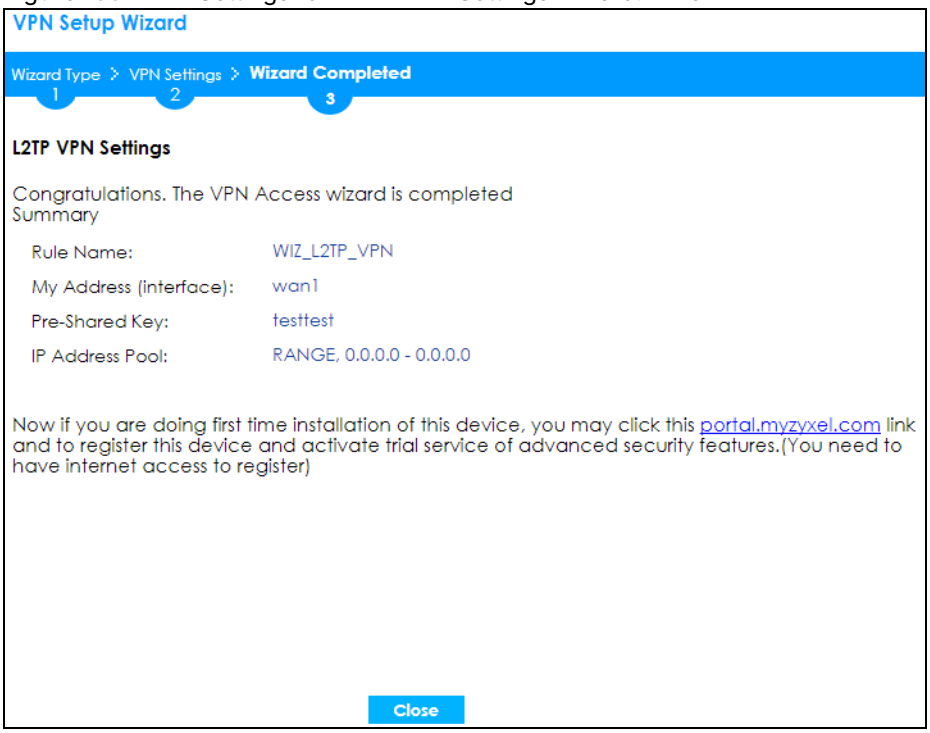


- Rule Name: Identifies the L2TP VPN connection (and the L2TP VPN gateway).
- Secure Gateway: Any displays in this field because it is not configurable in this wizard. It allows incoming connections from the L2TP VPN Client.
- Pre-Shared Key: L2TP VPN tunnel password.
- My Address (Interface): This displays 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.

6.6.4 VPN Settings for L2TP VPN Setting Wizard - Completed

Figure 169 VPN Settings for L2TP VPN Settings Wizard: Finish

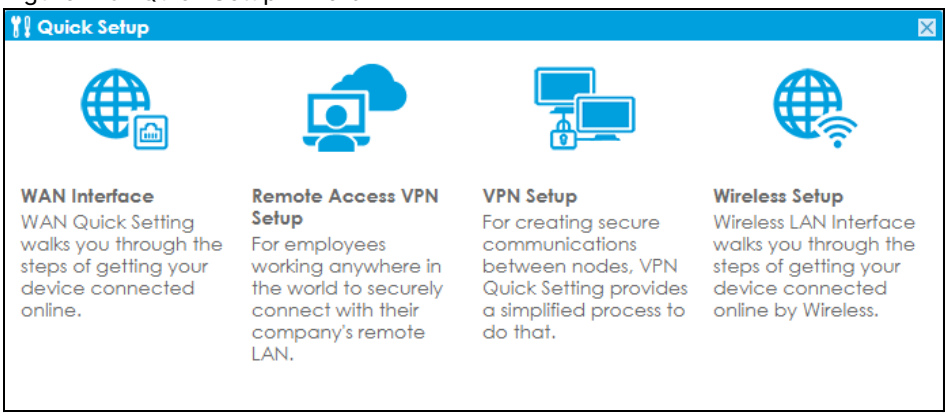


Te rule is now configured on the Zyxel Device. The L2TP VPN rule settings appear in the Configuration > VPN > L2TP VPN screen and also in the Configuration > VPN > IPSec VPN > VPN Connection and VPN Gateway screen.

6.7 Wireless Setup Wizard

Click Wireless Setup in the main Quick Setup screen to begin the wireless setup wizard. Changes in the wizard are not saved until you save them in the Summary screen.

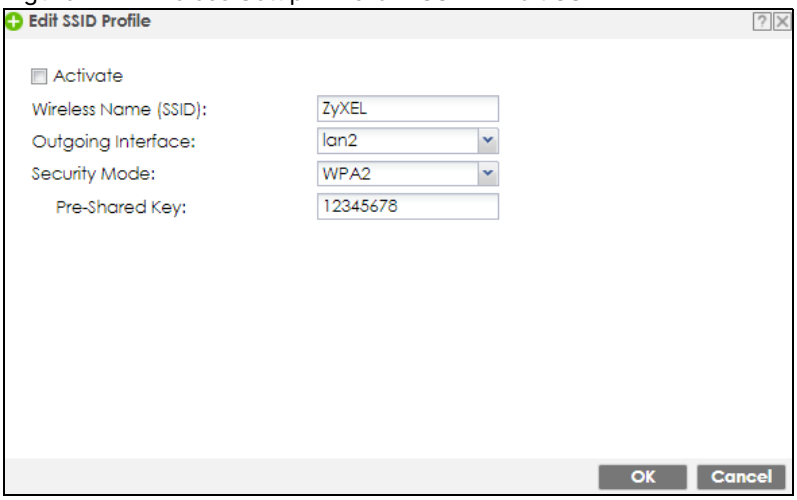
Figure 170 Quick Setup Wizard



6.7.1 SSID

Use the SSID screen to manage internal WiFi networks in the Zyxel Device that are identified by SSID. Select a WiFi network, then click Edit to create or change WiFi network settings.

Figure 171 Wireless Setup Wizard > SSID > Edit SSID



- Select Activate to enable the WiFi network for users connected to the Zyxel Device.
- The Wireless Name (SSID) identifies the WiFi network. Enter a unique SSID for each WiFi network.
- Select the Outgoing Interface that the wireless network uses to transmit packets.
- Use Security Mode to authenticate WiFi clients using the local database on the Zyxel Device with a pre-shared key. WPA is a wireless security standard for encryption, authentication and key management. Only WPA2 is supported in the wireless wizard. If you want to use WEP or WPA, then use the Configuration > Wireless screens.

  Select WPA2, then enter a Pre-Shared Key. Select Open if you do not want security for this WiFi network (not recommended).

Click OK to save your settings and return to the wireless setup wizard. Click Cancel to not save your settings and return to the wireless setup wizard. Click Next to continue the wireless setup wizard.

6.7.2 Radio

The next screen in the wireless setup wizard is Radio.

Figure 172 Wireless Setup Wizard > Radio: 2.4G

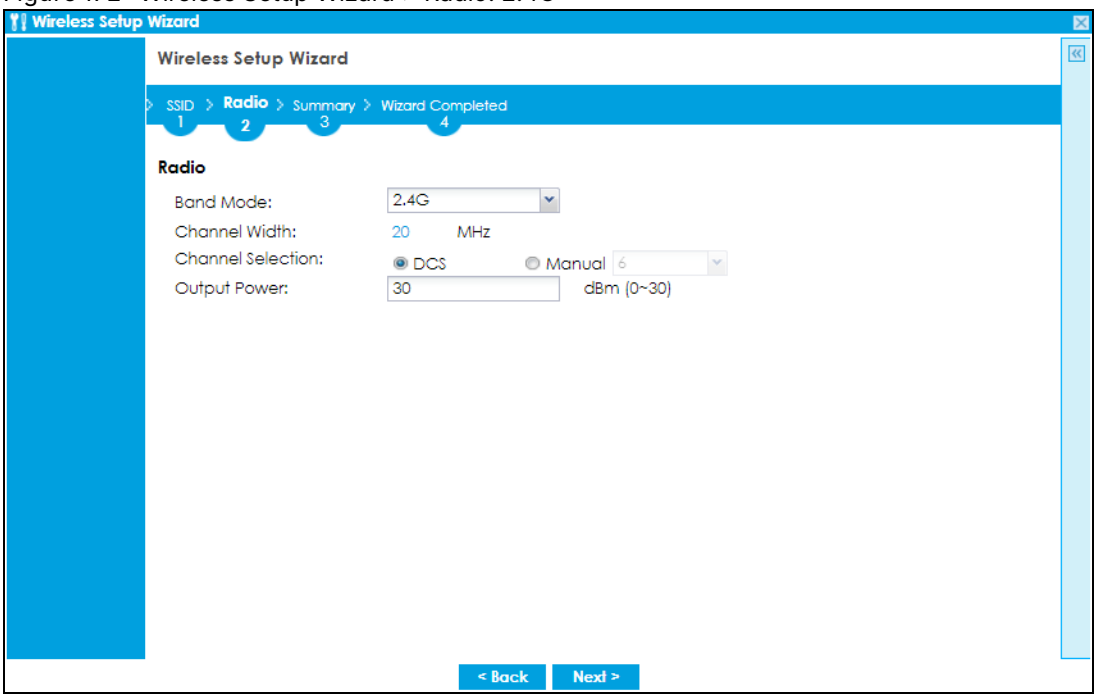


Figure 173 Wireless Setup Wizard > Radio: 5G

- Select the wireless band which this wireless network uses. 2.4GHz is the frequency used by IEEE 802.11b/g/n/ax wireless clients. 5GHz is the frequency used by IEEE802.11ax/ac/a/n wireless clients.
- Select DCS (Dynamic Channel Selection) to allow the Zyxel Device to automatically select a less-used channel in an environment where there are many WiFi devices and there may be interference. DCS is not supported on a Zyxel Device which is in repeater mode. Alternatively, select Manual to choose a specific channel that the Zyxel Device must use.
- Set the Output Power of the Zyxel Device. The greater the output power, the greater the WiFi coverage of the Zyxel Device. Too great an output power may cause interference with other WiFi devices.

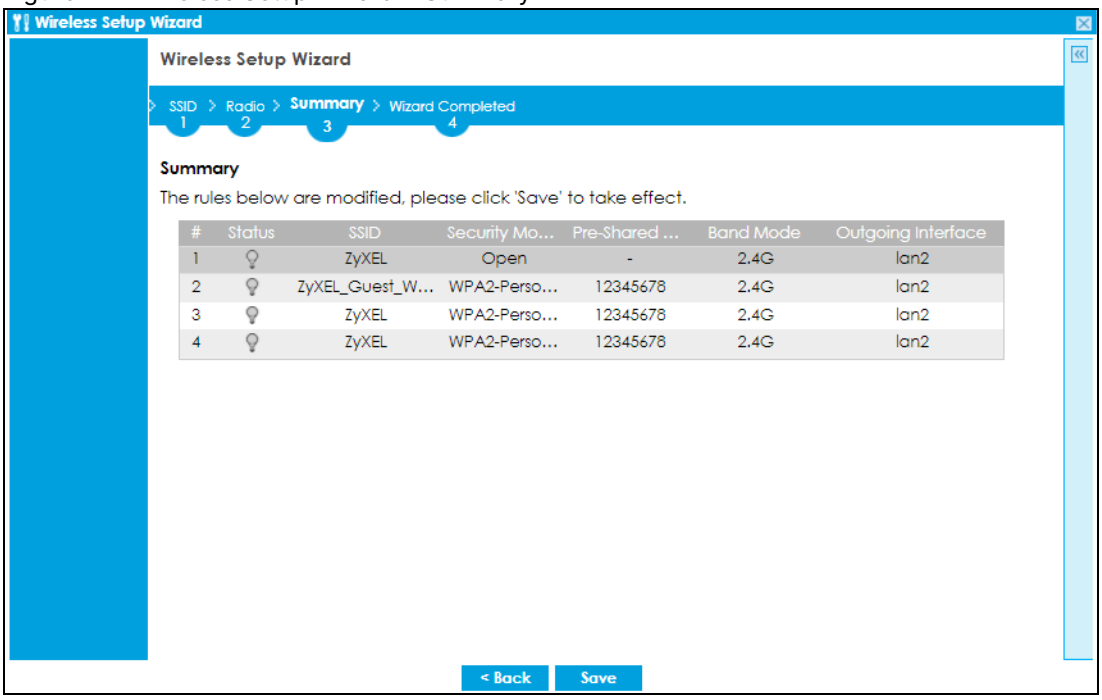
- Select the WiFi channel bandwidth you want the Zyxel Device to use.
  - 40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput.
  - An 80 MHz channel consists of two adjacent 40 MHz channels. The WiFi clients must also support 40 MHz or 80 MHz.
  - Select 20 MHz if the Zyxel Device is in a location with WiFi signal obstructions, or if you want to lessen radio interference with other WiFi clients in the coverage area, or the WiFi clients do not support channel bonding.
  - Select 40MHz, 80MHz, 160 MHz or 320 MHz to allow the Zyxel Device to adjust the channel bandwidth automatically where not all its WiFi clients support 40 MHz, 80 MHz, 160 MHz and/or 320MHz channels.

Note: If the environment has poor signal-to-noise ratio (SNR), the Zyxel Device will switch to a lower bandwidth automatically.

6.7.3 Summary

The next screen in the wireless setup wizard is Summary.

Figure 174 Wireless Setup Wizard > Summary

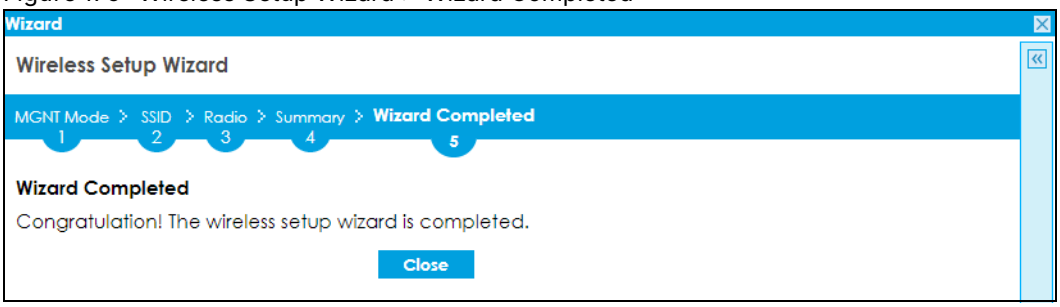


Review your settings in the Summary screen, then click Save to save the changes to the Zyxel Device. Click Back if you want to make more changes.

6.7.4 Wizard Completed

The next screen in the wireless wizard is Wizard Completed.

Figure 175 Wireless Setup Wizard > Wizard Completed



This screen shows that your changes have been successfully saved to the Zyxel Device. Click Close to exit the wizard. Run the wizard again if you want to make changes.

Chapter 7
Dashboard

7.1 Overview

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

7.1.1 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.

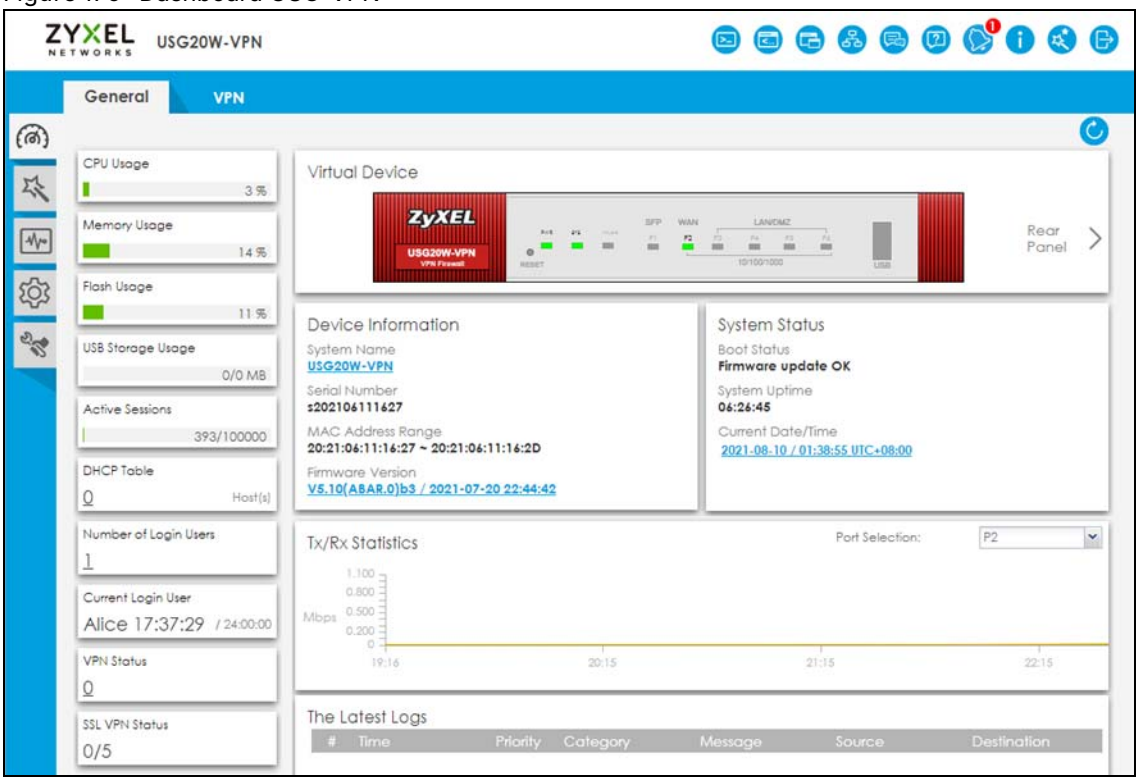
- Device Information Screen on page 206
- System Status Screen on page 207
- Tx/Rx Statistics on page 207
- The Latest Logs Screen on page 208
- System Resources Screen on page 208
- DHCP Table Screen on page 210
- Number of Login Users Screen on page 211
- Current Login User on page 212
- VPN Status on page 212
- SSL VPN Status on page 212
- The VPN Screen on page 213

7.2 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.

Figure 176 Dashboard USG-VPN



The following table describes the labels in this screen.

Table 21 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 15.18.1 on page 24 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.

Table 21 Dashboard (continued)

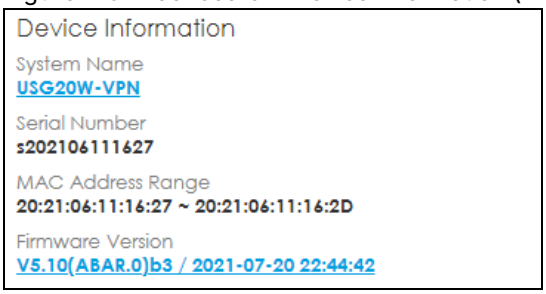
LABEL	DESCRIPTION
Status	This field displays the current status of each interface or device installed in a slot. The possible values depend on what type of interface it is. Inactive - The Ethernet interface is disabled. Down - The Ethernet interface does not have any physical ports associated with it 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 11.7 on page 324 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.
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).

7.2.1 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 177

Figure 178 Dashboard > Device Information (Example)



The table describes the fields in this screen.

Table 22 Dashboard > Device Information

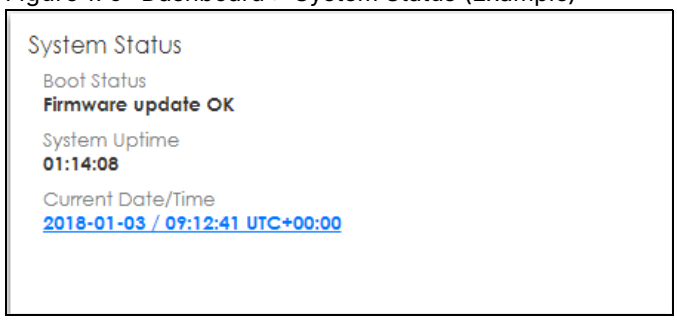
LABEL	DESCRIPTION
System Name	This field displays the name used to identify the Zyxel Device on any network. Click the link and open the Host Name screen where you can edit and make changes to the system and domain name.
Serial Number	This field displays the serial number of this Zyxel Device. The serial number is used for device tracking and control.

Table 22 Dashboard > Device Information

LABEL	DESCRIPTION
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.

7.2.2 System Status Screen

Figure 179 Dashboard > System Status (Example)



The table describes the fields in the screen.

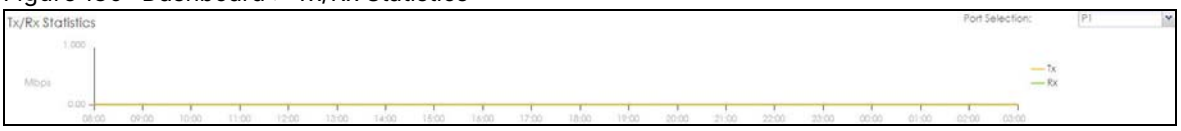
Table 23 Dashboard > System Status

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.

7.2.3 Tx/Rx Statistics

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

Figure 180 Dashboard > Tx/Rx Statistics



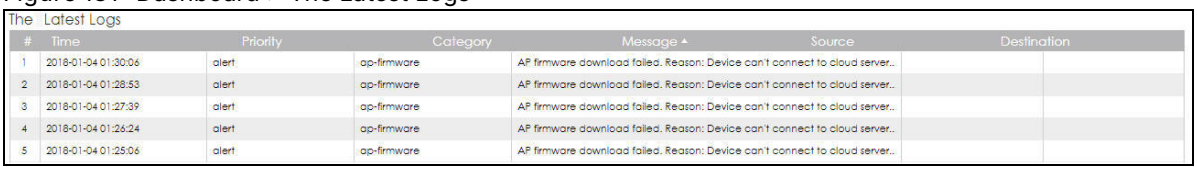
This table describes the fields in the above screen.

Table 24 Dashboard > Tx/Rx Statistics

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.

7.2.4 The Latest Logs Screen

Figure 181 Dashboard > The Latest Logs



The table describes the fields in the screen.

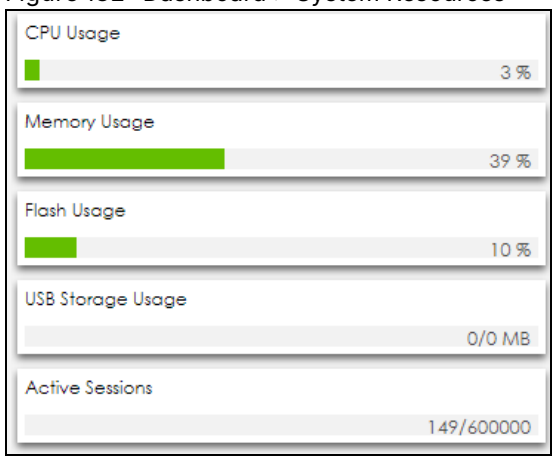
Table 25 Dashboard > The Latest Log

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.

7.2.5 System Resources Screen

These fields display the percentage of system resources that are used.

Figure 182 Dashboard > System Resources



The table describes the fields in the screen.

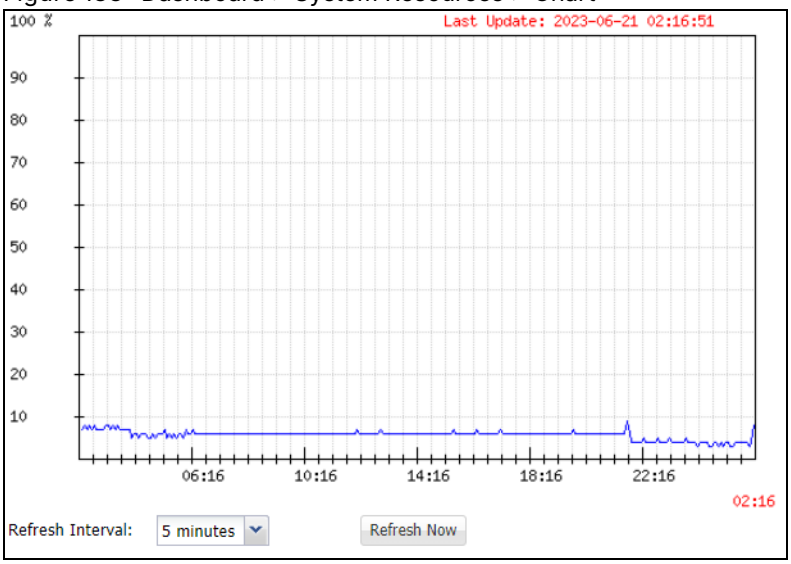
Table 26 Dashboard > System Resources

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.

7.2.5.1 System Resources Chart

The following screen displays when you click the system resources bar.

Figure 183 Dashboard > System Resources > Chart



The table describes the fields in the screen.

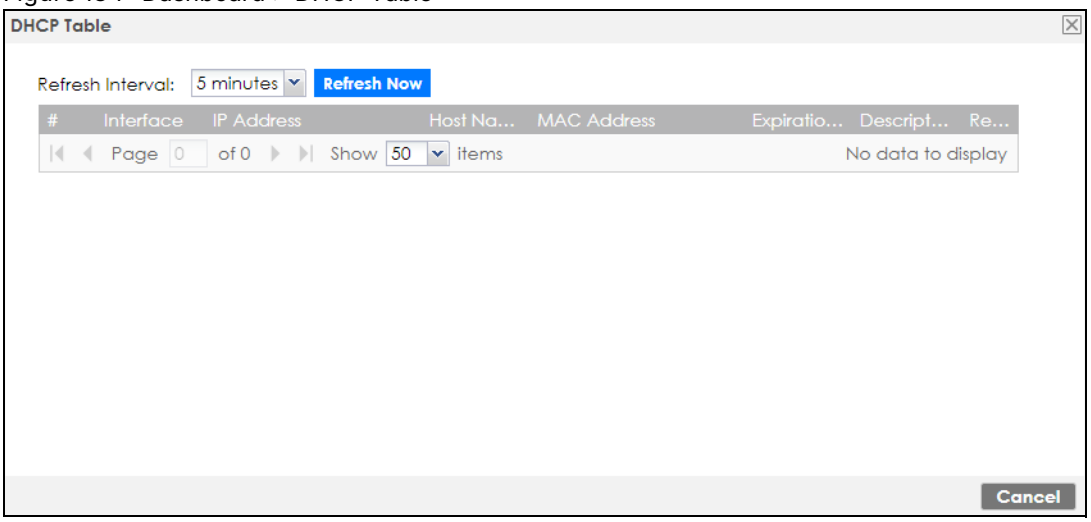
Table 27 Dashboard > System Resources > Chart

LABEL	DESCRIPTION
Data Collecting Interval	This field displays the time interval in minutes the Zyxel Device collects the system resources data.
Chart Refresh Interval	Select a time interval in minutes for renewing the system resources chart.

7.2.6 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 184 Dashboard > DHCP Table



This table describes the fields in the above screen.

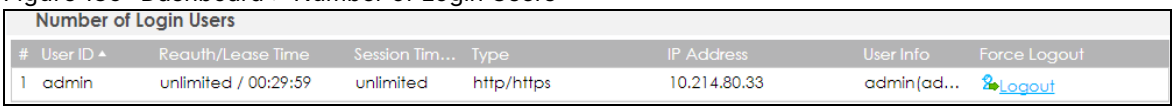
Table 28 Dashboard > DHCP Table

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.
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.

7.2.7 Number of Login Users Screen

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

Figure 185 Dashboard > Number of Login Users



The table describes the fields in the screen.

Table 29 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.

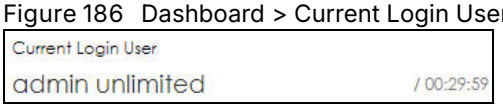
Table 29 Dashboard > Number of Login Users (continued)

LABEL	DESCRIPTION
IP address	This field displays the IP 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.
Force Logout	Click this icon to end a user's session.

7.2.8 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.

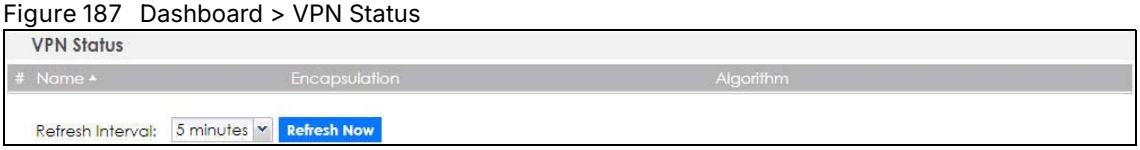
Figure 186 Dashboard > Current Login User



7.2.9 VPN Status

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

Figure 187 Dashboard > VPN Status



This table describes the fields in the above screen.

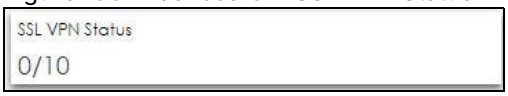
Table 30 Dashboard > VPN Status

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.

7.2.10 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.

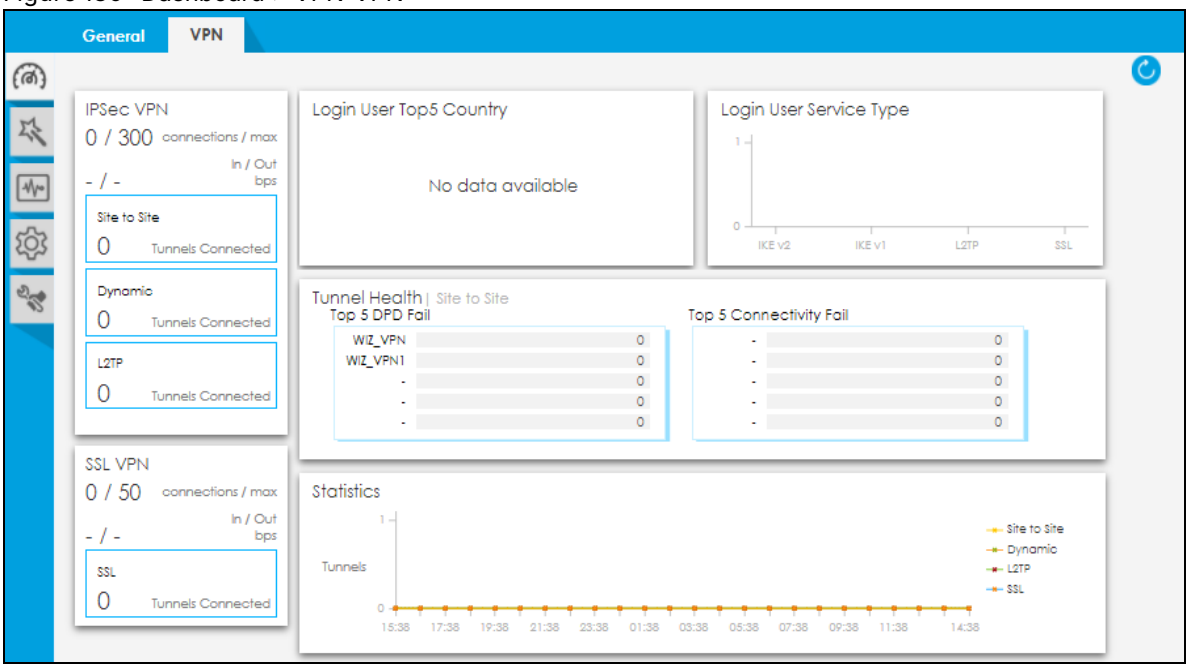
Figure 188 Dashboard > SSL VPN Status



7.3 The VPN Screen

VPN models have a VPN tab. If no VPN tunnels are configured, a link to Configuration > VPN > IPSec VPN screen appears.

Figure 189 Dashboard > VPN-VPN



This screen gives information such as:

- The actual number of connections and the maximum number of tunnel connections for each VPN type (IPSec/L2TP/SSL)
- The Incoming and Outgoing traffic amount in bps for each VPN type (IPSec/L2TP/SSL)
- The number of connected tunnels for each type of tunnel: Site to Site/Dynamic/ L2TP / SSL
- The Top 5 Logged in VPN Users per country
- The Top 5 Logged in VPN Users per Service Type
- The Top 5 Logged in VPN Users that are online
- Tunnel Health by Top 5 DPD (Dead Peer Detection) failures
- The Top 5 connectivity Failures
- Graphical tunnel statistics

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

Part II
Technical Reference

CHAPTER 8
Monitor

8.1 Overview

Use the Monitor screens to check status and statistics information.

8.1.1 What You Can Do in this Chapter

Use the Monitor screens for the following.

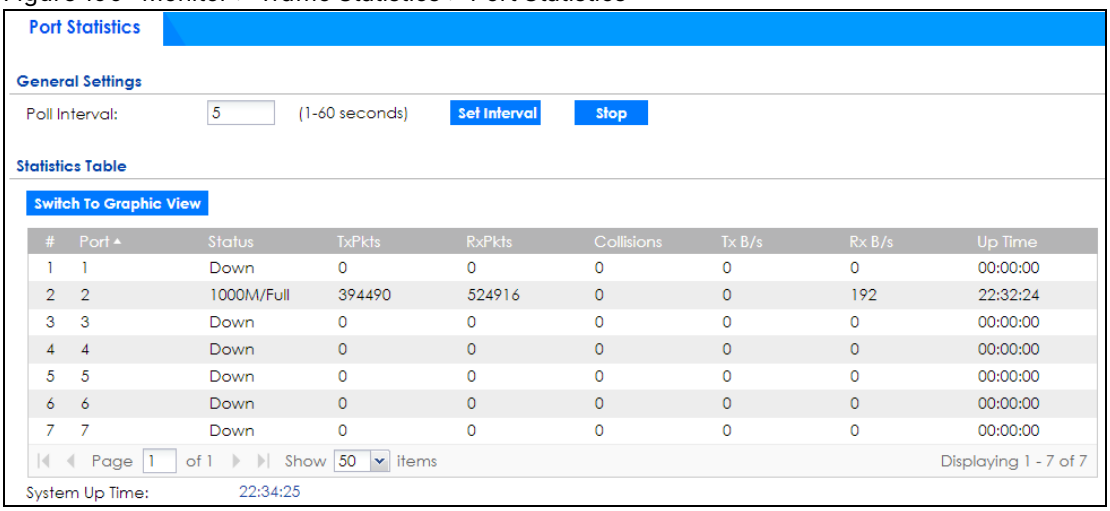
- Use the Traffic Statistics > Port Statistics screen (see Section 8.2.1 on page 217) to look at packet statistics for each physical port.
- Use the Traffic Statistics > Port Statistics > Graph View screen (see Section 8.2.1 on page 217) to look at a line graph of packet statistics for each physical port.
- Use the Traffic Statistics > Interface Status screen (Section 8.3 on page 218) to see all of the Zyxel Device's interfaces and their packet statistics.
- Use the Traffic Statistics > Traffic Statistics screen (see Section 8.4 on page 222) to start or stop data collection and view statistics.
- Use the Traffic Statistics > Session Monitor screen (see Section 8.5 on page 225) to view sessions by user or service.
- Use the Network Status > DHCP Table screen (see Section 8.6 on page 227) to view a list of interfaces and their DHCP-assigned IP addresses.
- Use the Network Status > Device Insight screen (see Section 8.7 on page 228) to view the status of the clients connected to the Zyxel Device.
- Use the Network Status > Login Users screen (Section 8.6 on page 227) to look at a list of the users currently logged into the Zyxel Device.
- Use the Network Status > IGMP Statistics screen (see Section 8.9 on page 234) to view multicasting details.
- Use the Network Status > DDNS Status screen (see Section 8.10 on page 235) to view the status of the Zyxel Device's DDNS domain names.
- Use the Network Status > IP/MAC Binding screen (Section 8.11 on page 235) to view a list of devices that have received an IP address from Zyxel Device interfaces with IP/MAC binding enabled.
- Use the Network Status > Cellular Status screen (Section 8.12 on page 236) to check your mobile broadband connection status.
- Use the Network Status > UPnP Port Status screen (see Section 8.13 on page 240) to look at a list of the NAT port mapping rules that UPnP creates on the Zyxel Device.
- Use the Network Status > USB Storage screen (Section 8.14 on page 241) to view information about a connected USB storage device.
- Use the Network Status > Ethernet Neighbor screen (Section 8.15 on page 242) to view and manage the Zyxel Device's neighboring devices through Layer Link Discovery Protocol (LLDP).
- Use the Network Status > FQDN Object screen (Section 8.16 on page 243) to display fully qualified domain name (FQDN) object cache lists used in DNS queries.

- Use the Wireless > AP Information > Radio List screen (Section 8.17 on page 245) to display statistics about the wireless radio transmitters in each of the APs connected to the Zyxel Device.
- Use the Wireless > SSID Info screen (Section 8.18 on page 248) 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 8.19 on page 249) to view information on connected wireless stations.
- Use the Wireless > Station Info > Top N Stations screen (Section 8.20 on page 251) to view wireless stations with the most wireless traffic usage.
- Use the Wireless > Station Info > Single Station screen (Section 8.21 on page 252) to view wireless traffic usage for an associated wireless station.
- Use the VPN Monitor > IPSec screen (Section 8.22 on page 253) to display and manage active IPSec SAs.
- Use the VPN Monitor > SSL screen (see Section 8.23 on page 255) 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 8.24 on page 256) to display and manage the Zyxel Device's connected L2TP VPN sessions.
- Use the Security Statistics > Content Filter screen (Section 8.25 on page 257) to start or stop data collection and view content filter statistics.
- Use the Security Statistics > Anti-Spam > Summary screen (Section 8.26 on page 259) to start or stop data collection and view spam statistics.
- Use the Security Statistics > Anti-Spam > Status screen (Section 8.26.2 on page 261) to see how many mail sessions the Zyxel Device is currently checking and DNSBL statistics.
- Use the Log > View Log screen (see Section 8.27.1 on page 263) 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.

8.2 The Port Statistics Screen

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

Figure 190 Monitor > Traffic Statistics > Port Statistics



The following table describes the labels in this screen.

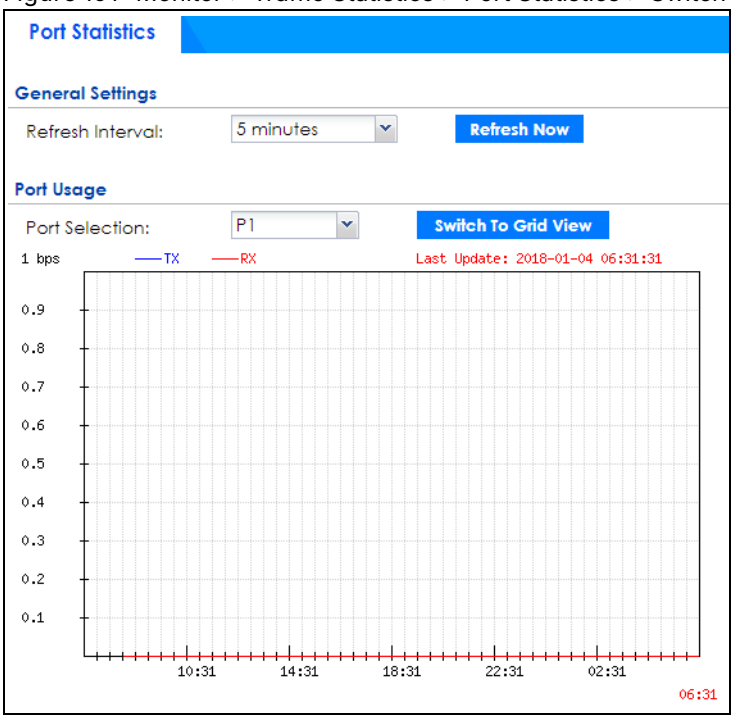
Table 31 Monitor > Traffic Statistics > Port Statistics

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.

8.2.1 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 on the Status screen and then the Switch to Graphic View Button.

Figure 191 Monitor > Traffic Statistics > Port Statistics > Switch to Graphic View



The following table describes the labels in this screen.

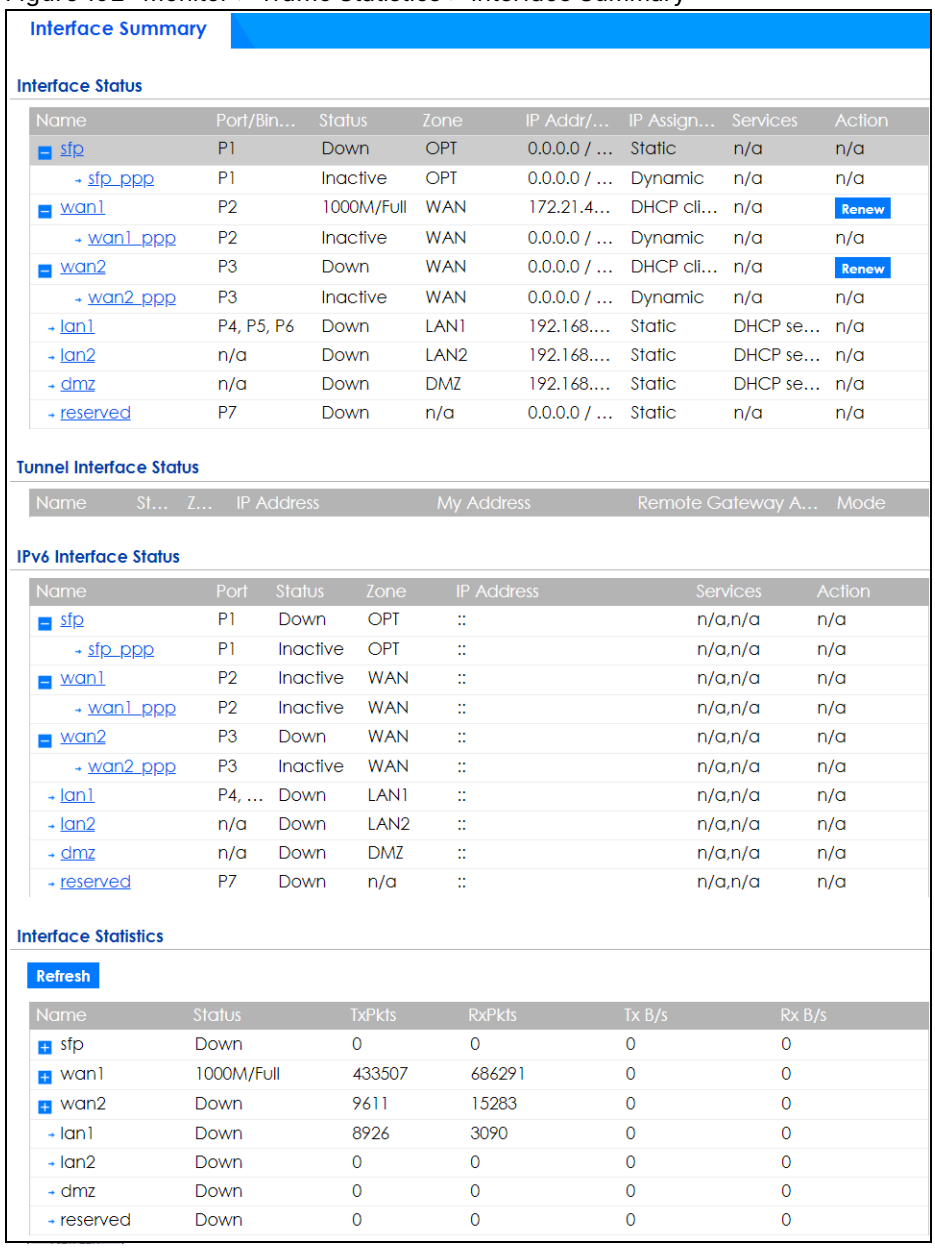
Table 32 Monitor > Traffic Statistics > Port Statistics > Switch to Graphic View

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.

8.3 Interface Status Screen

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

Figure 192 Monitor > Traffic Statistics > Interface Summary



Each field is described in the following table.

Table 33 Monitor > Traffic Statistics > 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.

Table 33 Monitor > Traffic Statistics > 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 8.14 on page 241 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 through 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.
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.

Table 33 Monitor > Traffic Statistics > Interface Summary

LABEL	DESCRIPTION
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.
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 8.14 on page 241 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 through 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.

Table 33 Monitor > Traffic Statistics > 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.
Interface Statistics This table provides packet statistics for each interface.	
Refresh	Click this button to update the information on 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.
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.

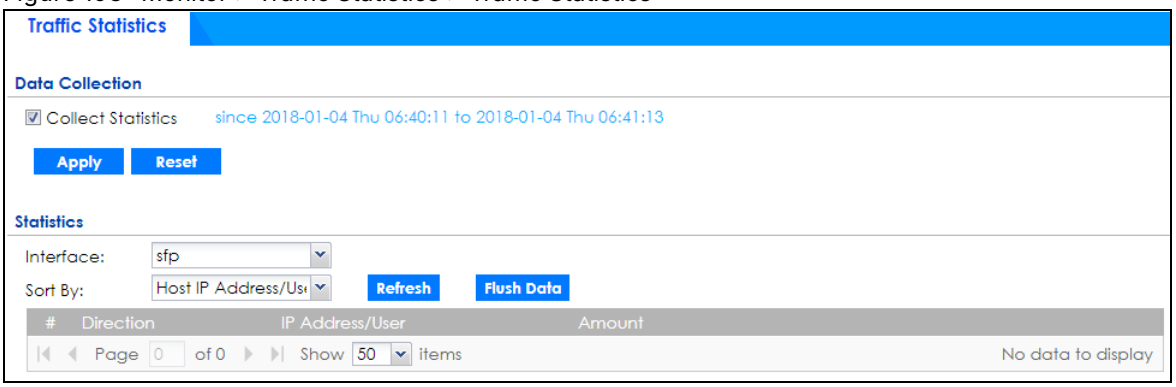
8.4 The Traffic Statistics Screen

Click Monitor > Traffic Statistics > 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 34 on page 223 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 on the Traffic Statistics screen.

Figure 193 Monitor > Traffic Statistics > Traffic Statistics



There is a limit on the number of records shown in the report. Please see Table 35 on page 224 for more information. The following table describes the labels in this screen.

Table 34 Monitor > Traffic Statistics > 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 35 on page 224.
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 35 on page 224.

Table 34 Monitor > Traffic Statistics > Traffic Statistics (continued)

LABEL	DESCRIPTION
	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 35 on page 224.
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
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 35 on page 224.
	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 35 on page 224.
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 35 on page 224.
	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 35 on page 224. • 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 35 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.

8.5 The Session Monitor Screen

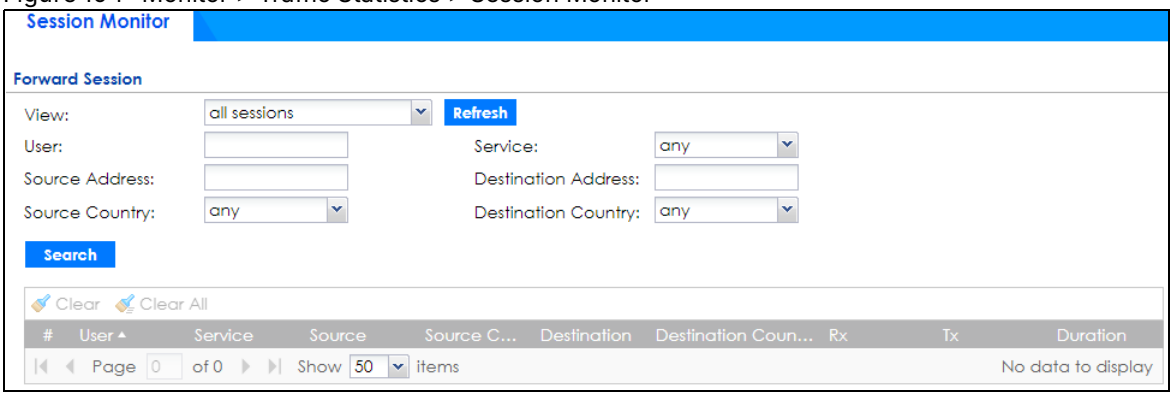
The Session Monitor screen displays all established sessions that pass through the Zyxel Device for debugging or statistical analysis. It is not possible to manage sessions in this screen. The following information is displayed.

- 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 > Traffic Statistics > Session Monitor to display the following screen.

Figure 194 Monitor > Traffic Statistics > Session Monitor



The following table describes the labels in this screen.

Table 36 Monitor > Traffic Statistics > 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.

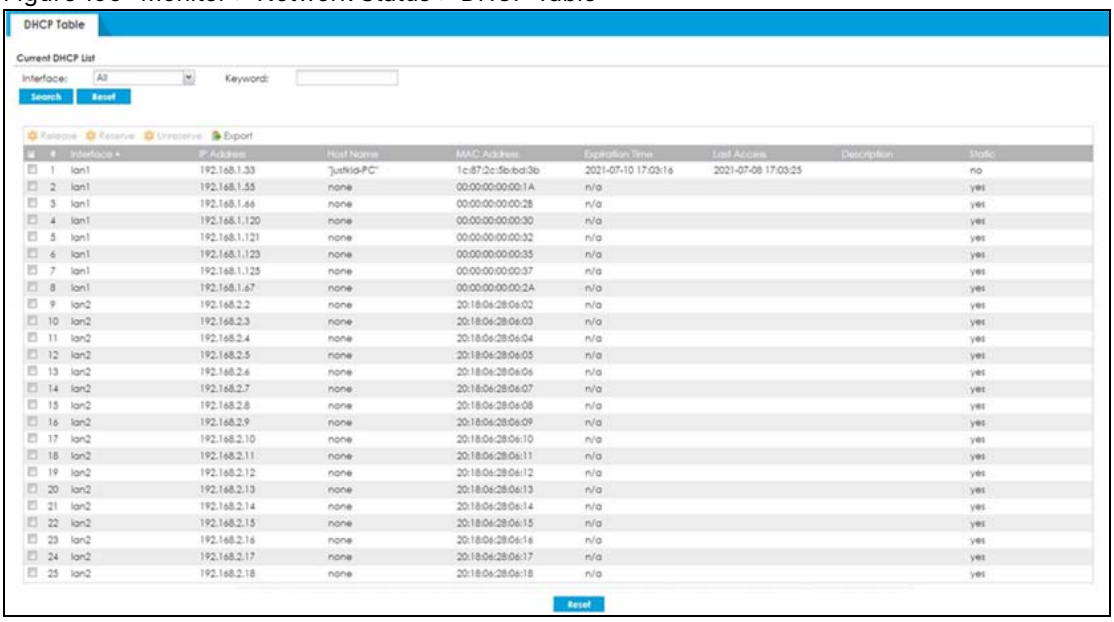
Table 36 Monitor > Traffic Statistics > Session Monitor (continued)

LABEL	DESCRIPTION
	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. Enter the user whose sessions you want to view. It is not possible to enter 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.
Source Address	This field displays when View is set to all sessions. Enter 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. Enter 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 on 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.

8.6 The DHCP Table Screen

Use this screen to look at a list of interfaces and their DHCP-assigned IP addresses. To access this screen, click Monitor > Network Status > DHCP Table.

Figure 195 Monitor > Network Status > DHCP Table



The following table describes the labels in this screen.

Table 37 Monitor > Network Status > DHCP Table

LABEL	DESCRIPTION
Current DHCP List	
Interface	Select a Zyxel Device interface that has DHCP enabled to show to which devices it has assigned DHCP IP addresses.
Keyword	Enter a keyword to display the interfaces and their information, such as IP addresses, MAC addresses and so on. The field is case-sensitive.
Search	Click to update the list of interfaces shown in the table below based on the search criteria. Your search criteria is retained when navigating between screens.
Reset	Click to return this search criteria to the factory defaults and display all interfaces with DHCP enabled.
Release	Select an entry and click on this button to let other devices use the dynamic DHCP that is currently assigned to the selected entry.
Reserve	Select an entry and click on this button to set the entry as a static DHCP entry. The IP address will be reserved for the MAC address after you click this button.
Unreserve	Select an entry and click on this button to set the entry from a static DHCP entry to a dynamic DHCP entry. The IP address is assigned to a DHCP client.
Export	To export as a csv file on your computer, select them and click Export. Click Save in the file download dialogue box and then select a location and name for the file. You can edit the file after it is saved on your computer. To import the file you export here to recover the settings you configure now later on the Zyxel Device, go to Configuration > Network > Interface > Ethernet/VLAN > DCHP Setting.

Table 37 Monitor > Network Status > DHCP Table (continued)

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific entry.
Interface	This field identifies the interface that assigned an IP address to a DHCP client.
IP Address	This field displays the IP address currently assigned to a DHCP client or reserved for a specific MAC address. Click the column's heading cell to sort the table entries by IP address. Click the heading cell again to reverse the sort order.
Host Name	This field displays the name used to identify this device on the network (the computer name). The 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 displays the date and time the DHCP-assigned address will be renewed.
Last Access	This is when the last time any traffic pass through the interface.
Description	For a static DHCP entry, the host name or the description you configured shows here. This field is blank for dynamic DHCP entries.
Static	This field displays if the address in the IP address field is reserved for the clients connected to this interface. Yes means that the clients connected to the interface will always get the IP address shown in the table.

8.7 The Device Insight Screen

The Device Insight screen displays the status of the clients connected to the Zyxel Device, such as if a client is sending traffic to the Zyxel Device or if a client's MAC address is in the CDR block list. See Chapter on page 497 for more information on CDR.

It also displays the basic information and the status of the clients. The clients show in this screen may include clients connected to the Zyxel Device:

- Using wired connections.
- Through access points (APs) using wired connections.
- Through access points (APs) using WiFi connections.
- Through bulit-in access points using WiFi connections.
- Using SecuExtender (IPSec VPN clients).

Use Device Insight to identify and monitor clients connected to the Zyxel Device internal LAN/VLAN DMZ networks in the same IP subnet. This feature collects client information, including:

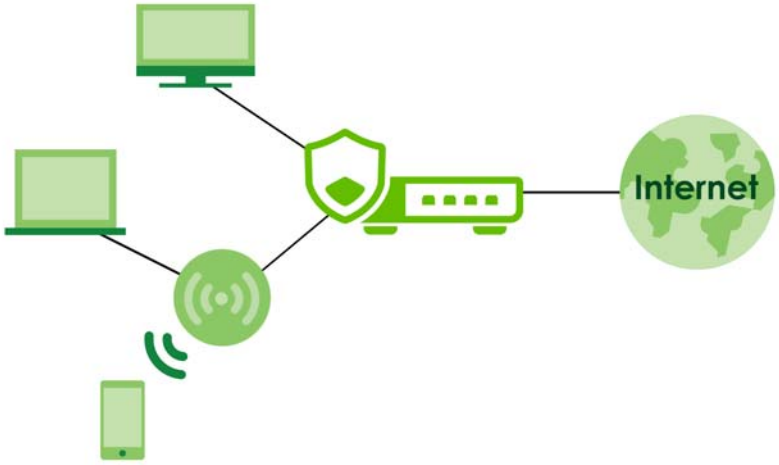
- Hostname
- IP address and MAC address
- Operating system
- Category, such as mobile phones or computers
- Connected interface

You can create a profile based on clients' categories and operating systems, and then apply the created profile to the Zyxel Device security policies. See Section 30.1 on page 669 for more information on creating and using Device Insight profiles.

Note: To collect clients' information using Device Insight, the clients must be in the same IP subnet in the LAN/VLAN/DMZ networks behind the Zyxel Device. Information from clients that are in different IP subnets in the LAN/VLAN/DMZ networks might not be collected correctly as traffic must pass through another router or a layer-3 switch to the Zyxel Device.

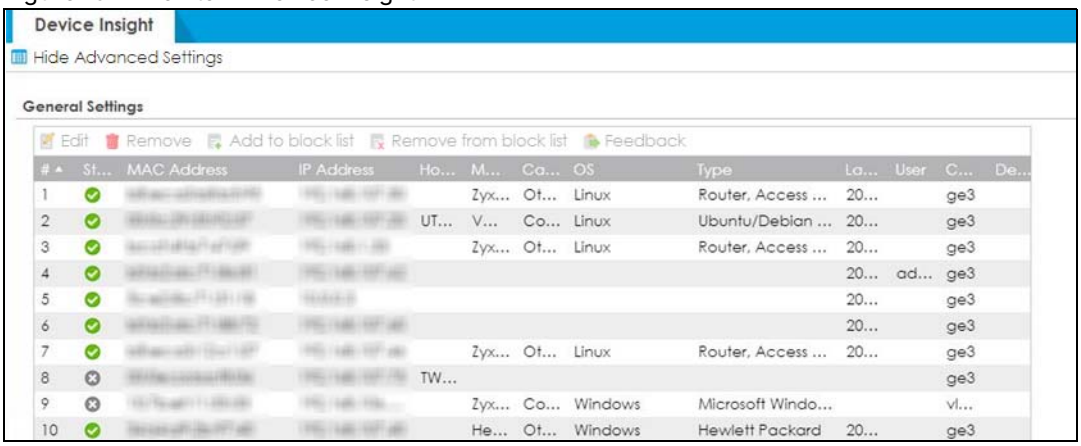
In the graphic below, A client connected to the Zyxel Device using a wired connection. A client connected to the Zyxel Device through an AP using a wired connection. A client connected to the Zyxel Device through an AP using a WiFi connection.

Figure 196 Clients' Device Insight Example



Click Monitor> Device Inventory to show the following screen.

Figure 197 Monitor > Device Insight



The following table describes the labels in this screen.

Table 38 Monitor > Network Status > Device Insight

LABEL	DESCRIPTION
Hide/Show Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Edit	Double-click an entry or select it and click Edit to modify the entry's settings in the Description field.
Remove	Select an entry and click Remove to remove a client from the table that's no longer connected to your network. For example, guest A visited your company over a month ago. Guest A used his cellphone to connect to your Zyxel Device networks. His cellphone was identified and shown in the Device Insight table. Guest A has left for over a month and you're sure he will not return in the near future. You can use the Remove button to remove his device from this table. Guest A's device will be identified and shown in the table again if he connects to your Zyxel Device networks in the future. Please note that clients that are blocked cannot be removed. Make sure to unblock clients before you remove them.
Add to block list	Select an entry and click Add to block list to stop the selected client from connecting to the Zyxel Device.
Remove from block list	Select an entry and click Remove from block list to allow the selected client to connect to the Zyxel Device.
Feedback	Select an entry and click Feedback to report on a client that is wrongly identified regarding its Category, Operating System or Type.
#	This field is a sequential value, and it is not associated with a specific service.
Status	This field displays the status of the clients. On line ( )- The VPN connection between the client and the Zyxel Device is up. Off line ( )- The VPN connection between the client and the Zyxel Device is down. Block ( )- The client is blocked from the connection to the Zyxel Device. CDR Block ( )- The client's MAC address is blocked by CDR.
MAC Address	This field displays the MAC address of the client.
IP Address	This field displays the IP address of the client.
Hostname	This field displays the name used to identify this device on the network.
Manufacturer	This field displays the manufacturer of the client, such as Apple or Samsung.
Category	This field displays the type of the device of the client, such as printer or smart TV.
OS	This field displays the operating system of the client.
OS Version	This field displays the version of the operating system of the client.
Type	This field displays the model names of the client.
First-seen	This field displays the time when the client first sends traffic to the Zyxel Device.
Last-seen	This field displays the time when the client last sends traffic to the Zyxel Device.
User	This field displays the type of user account the client uses. See Section 30.3 on page 678 for more information the user account types.
Auth method	This field displays the authentication method that is used to authenticate the client.
TX rate (Kbps)	This field displays the transmission rate of the client to which the Zyxel Device is connected.
RX rate (Kbps)	This field displays the reception rate of the client to which the Zyxel Device is connected.

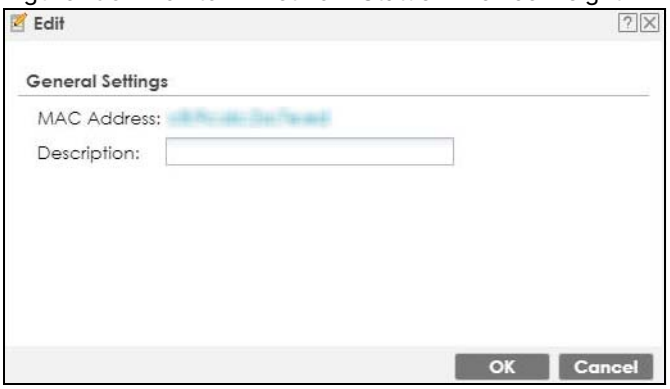
Table 38 Monitor > Network Status > Device Insight (continued)

LABEL	DESCRIPTION
Connected to	This field displays if the client is connected directly to the Zyxel Device or to an AP that is connected to the Zyxel Device.
Description	This field displays the descriptive name of the client.

8.7.1 The Device Insight Edit Screen

Use this screen to edit the description for connected clients. Click Monitor > Network Status > Device Insight > Edit to display the following screen.

Figure 198 Monitor > Network Status > Device Insight > Edit



The following table describes the labels in this screen.

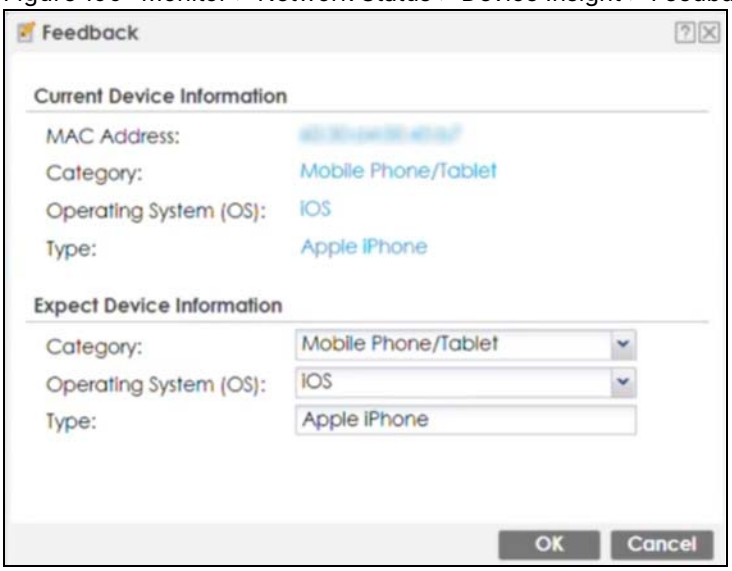
Table 39 Monitor > Network Status > Device Insight > Edit

LABEL	DESCRIPTION
Description	Enter a descriptive name for this client. You can use up to 31 characters, spaces and underscores are allowed.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving your changes.

8.7.2 The Device Insight Feedback Screen

Use this screen to report on clients that are wrongly identified. Click Monitor > Network Status > Device Insight > Feedback to display the following screen.

Figure 199 Monitor > Network Status > Device Insight > Feedback



The following table describes the labels in this screen.

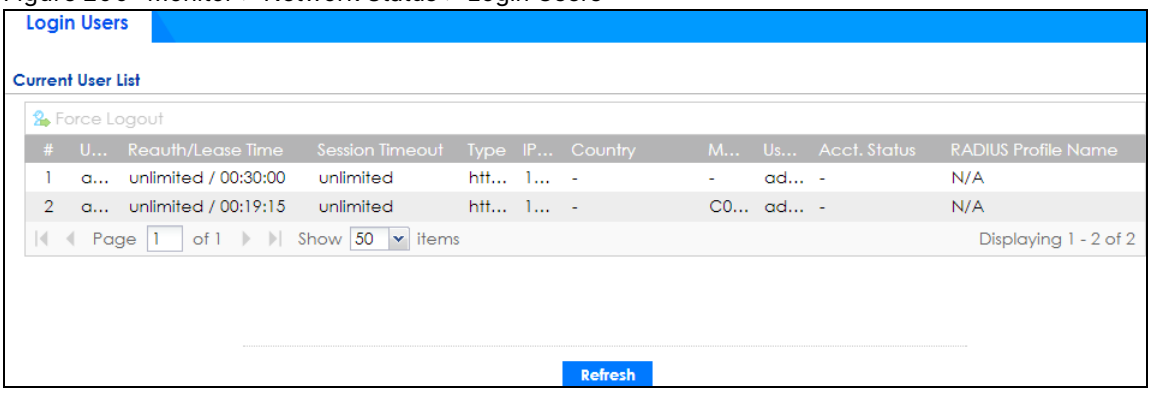
Table 40 Monitor > Network Status > Device Insight > Feedback

LABEL	DESCRIPTION
Current Device Information	
MAC address	This field displays the MAC address of the client.
Category	This field displays the type of the device of the client, such as printer or smart TV.
Operating System	This field displays the operating system of the client.
Type	This field displays the model names of the client.
Expect Device Information	
Category	This field will display the current type of the client device identified by the Zyxel Device. If you think it's wrong, select the type of device you believe is correct from the drop-down list box. If it is correct, leave it as it is.
Operating System	This field will display the current operating system of the client identified by the Zyxel Device. If you think it's wrong, select the operating system you believe is correct from the drop-down list box. If it is correct, leave it as it is.
Type	This field will display the current model name of the client identified by the Zyxel Device. If you think it's wrong, enter the model name you believe is correct. If it is correct, leave it as it is.
OK	Click OK to send your feedback to the Zyxel database.
Cancel	Click Cancel to exit this screen without saving your changes.

8.8 The Login Users Screen

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

Figure 200 Monitor > Network Status > Login Users



The following table describes the labels in this screen.

Table 41 Monitor > Network Status > Login Users

LABEL	DESCRIPTION
Force Logout	Select a user row 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. See Section 30.3.2 on page 681 for more information on the reauthentication time and lease time.
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 into the Zyxel Device. The user can log into the Zyxel Device using HTTP, HTTPS, Telnet, SSH, FTP and console.
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 IPv4 addresses: • 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 The Zyxel Device cannot identify a user's country if the user accessed the Zyxel Device using one of the private IPv4 addresses listed above. This field will display a hyphen (-).
MAC	This field displays the MAC address of the computer used to log into 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. See Section 30.3.1 on page 679 for more information on the user accounts.
Created Date	This field displays the date the account was created. This field displays a hyphen (-) if the account was created on a Zyxel Device with firmware version earlier than 5.10.

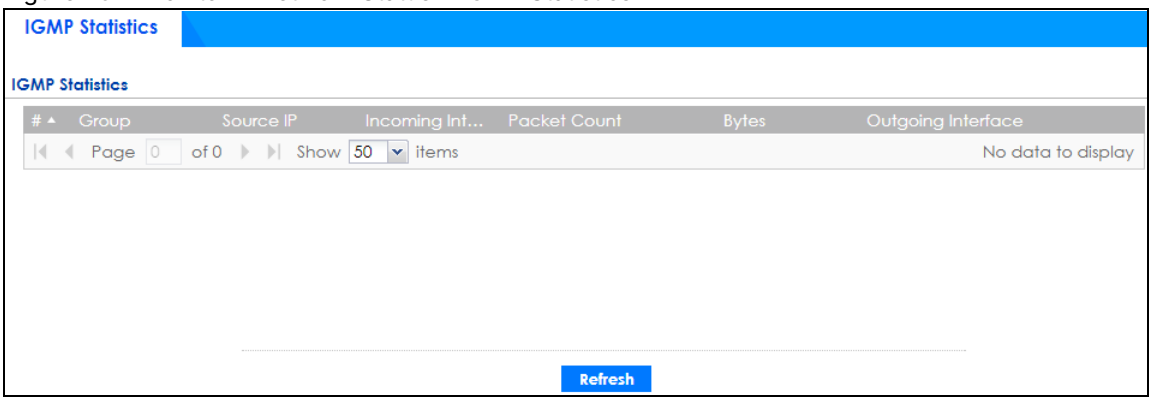
Table 41 Monitor > Network Status > Login Users (continued)

LABEL	DESCRIPTION
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.
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 on the screen.

8.9 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 > Network Status > IGMP Statistics to open the following screen.

Figure 201 Monitor > Network Status > IGMP Statistics



The following table describes the labels in this screen.

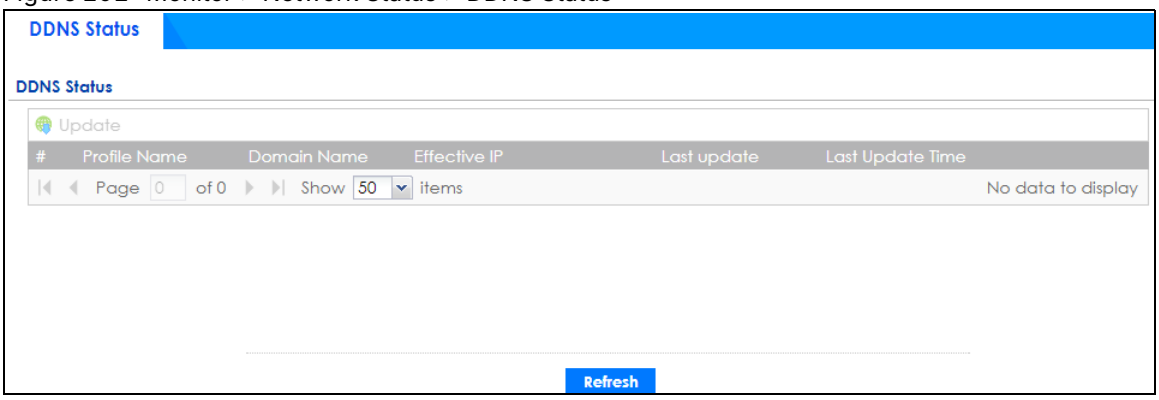
Table 42 Monitor > Network Status > IGMP Statistics

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 on the screen.

8.10 The DDNS Status Screen

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

Figure 202 Monitor > Network Status > DDNS Status



The following table describes the labels in this screen.

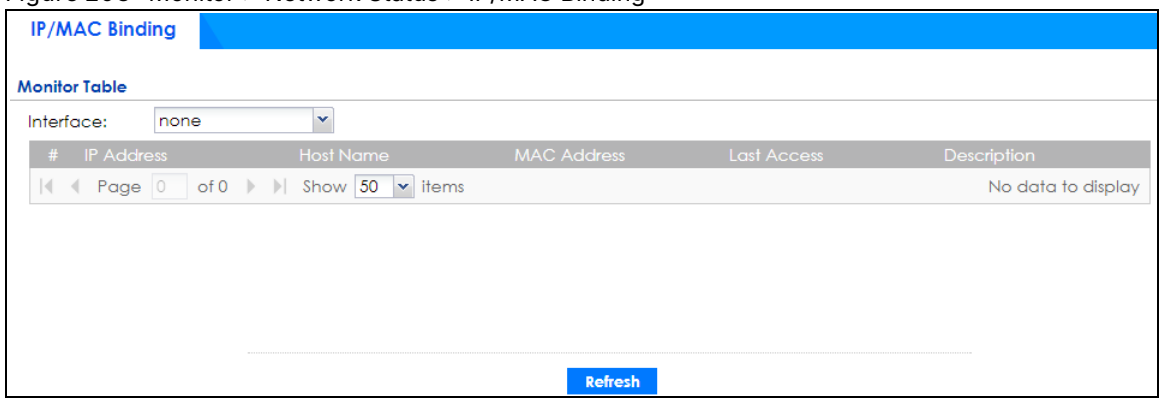
Table 43 Monitor > Network Status > DDNS Status

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 on the screen.

8.11 IP/MAC Binding

Click Monitor > Network 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 203 Monitor > Network Status > IP/MAC Binding



The following table describes the labels in this screen.

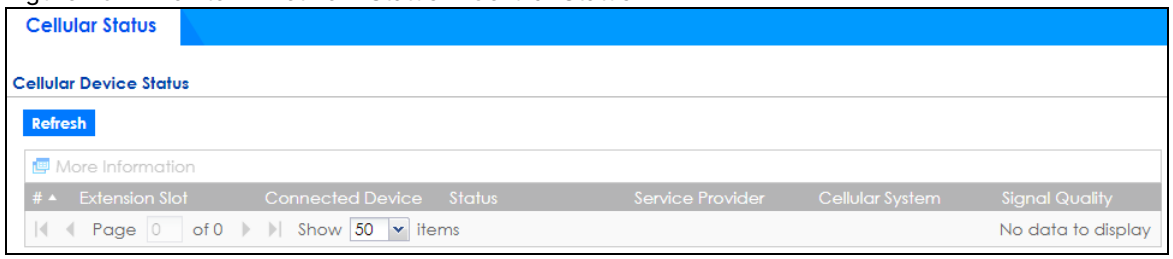
Table 44 Monitor > Network Status > IP/MAC Binding

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 on the screen.

8.12 Cellular Status Screen

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

Figure 204 Monitor > Network Status > Cellular Status



The following table describes the labels in this screen.

Table 45 Monitor > Network Status > Cellular Status

LABEL	DESCRIPTION
Refresh	Click this button to update the information on 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 8.12.1 on page 239.
#	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 45 Monitor > Network 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 on 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 45 Monitor > Network Status > Cellular Status (continued)

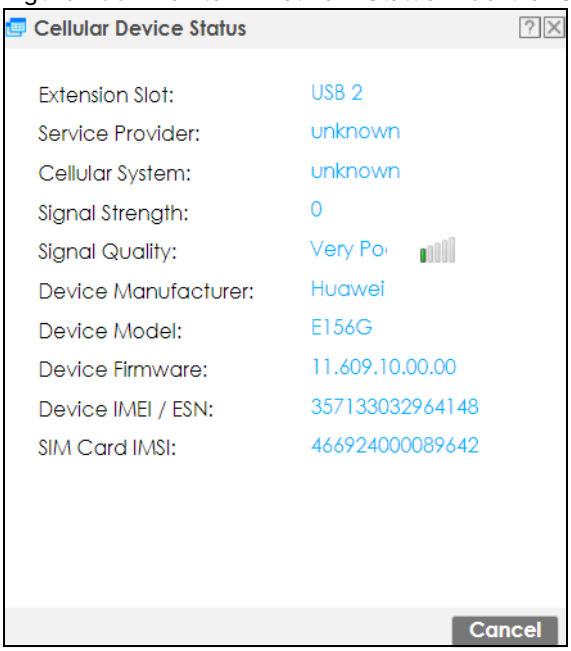
LABEL	DESCRIPTION
Cellular System	This field displays what type of cellular network the mobile broadband connection is using. The network type varies depending on the mobile broadband card you inserted and could be UMTS, UMTS/HSDPA, GPRS or EDGE when you insert a GSM mobile broadband card, or 1xRTT, 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.

8.12.1 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 > Network 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 205 Monitor > Network Status > Cellular Status > More Information



The following table describes the labels in this screen.

Table 46 Monitor > Network 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.

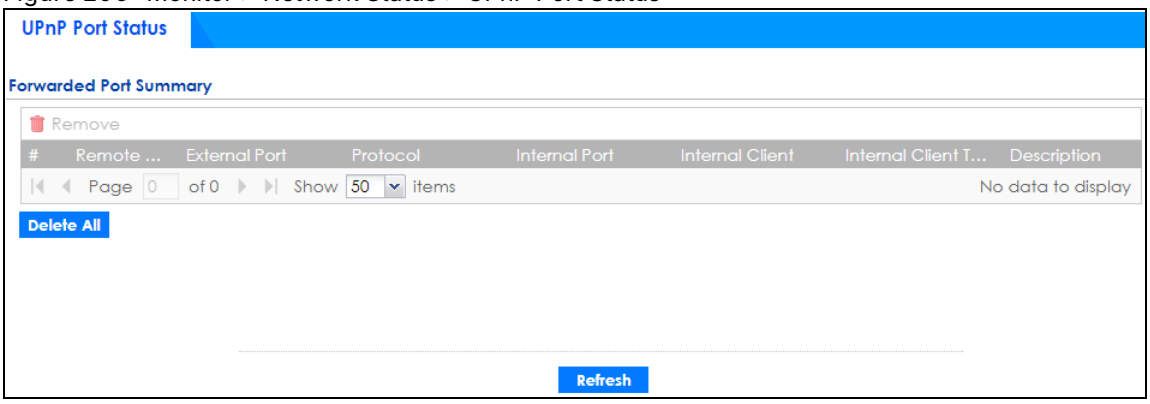
Table 46 Monitor > Network Status > Cellular Status > More Information (continued)

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.

8.13 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 > Network Status > UPnP Port Status.

Figure 206 Monitor > Network Status > UPnP Port Status



The following table describes the labels in this screen.

Table 47 Monitor > Network 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.

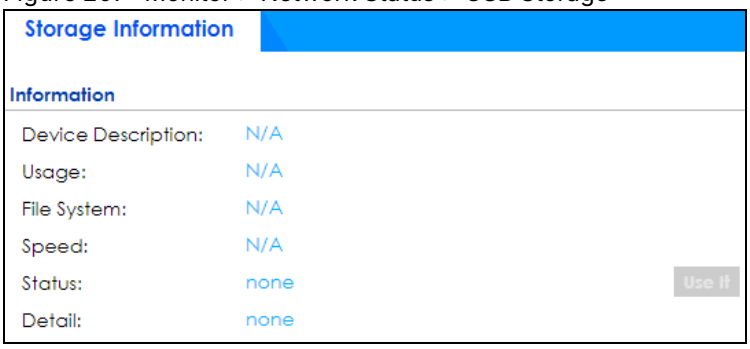
Table 47 Monitor > Network Status > UPnP Port Status (continued)

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 on the screen.

8.14 USB Storage Screen

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

Figure 207 Monitor > Network Status > USB Storage



The following table describes the labels in this screen.

Table 48 Monitor > Network 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 48 Monitor > Network 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.

8.15 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.

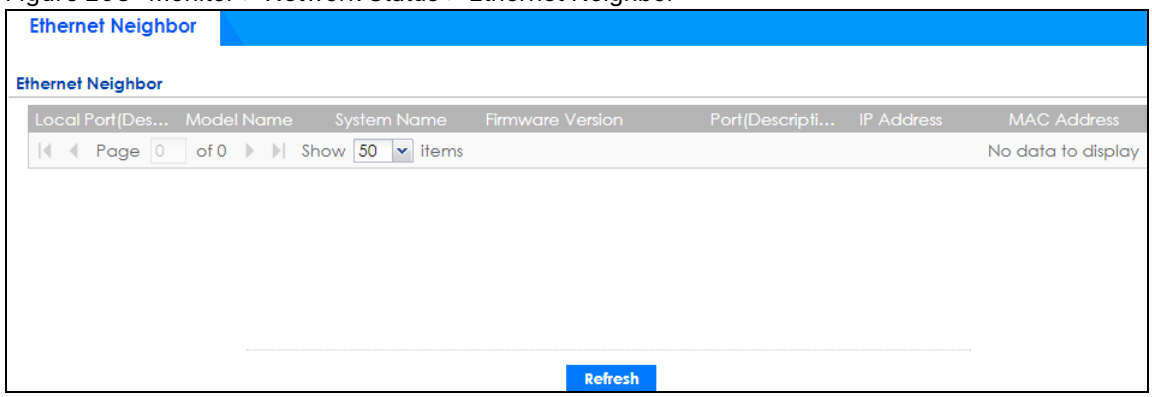
LLDP is a layer-2 protocol that allows a network device to advertise its identity and capabilities on the local network. It also allows the device to maintain and store information from adjacent devices which are directly connected to the network device. This helps you discover network changes and perform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

Note: Enable Smart Connect on 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 on the same network as the computer on which the ZON utility is installed.

Click Monitor > Network Status > Ethernet Neighbor to see the following screen

Figure 208 Monitor > Network Status > Ethernet Neighbor



The following table describes the fields on the previous screen.

Table 49 Monitor > Network 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 on 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 on the screen.

8.16 FQDN Object Screen

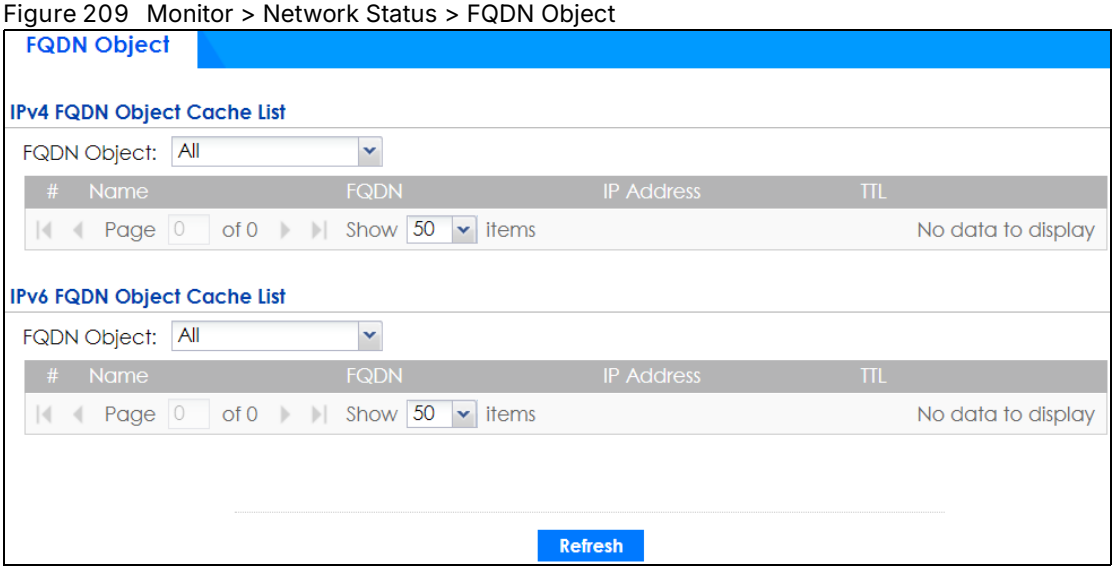
Click Monitor > Network Status > FQDN Object to open the FQDN Object screen. View FQDN-to-IP address mappings cached in this screen. An FQDN is resolved to its IP address using the DNS server configured on the Zyxel Device. If the Zyxel Device receives a DNS query for an FQDN and the Zyxel Device has 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 209 Monitor > Network Status > FQDN Object



The following table describes the fields on the previous screen.

Table 50 Monitor > Network 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.	

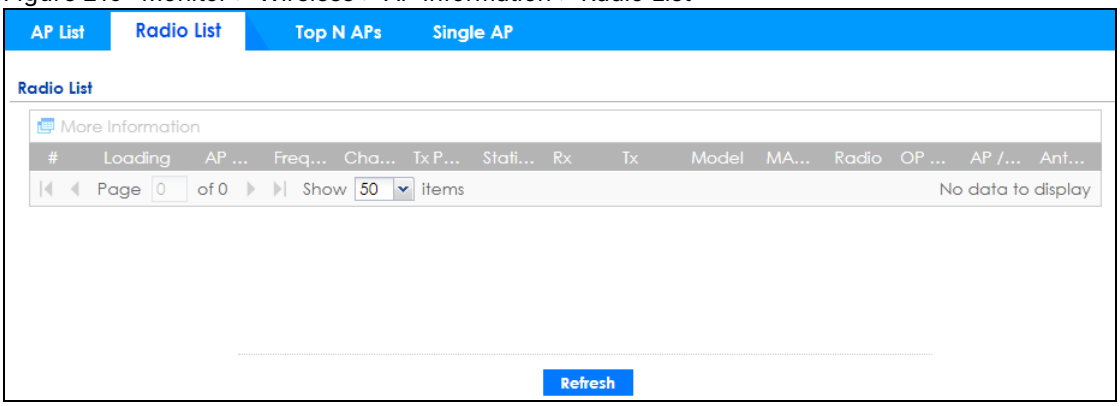
Table 50 Monitor > Network Status > FQDN Object

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 on the screen.

8.17 AP Information: Radio List

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

Figure 210 Monitor > Wireless > AP Information > Radio List



The following table describes the labels in this screen.

Table 51 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.
Enable Column Freeze	Select this to lock the index columns in place while scrolling to the right.
#	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.

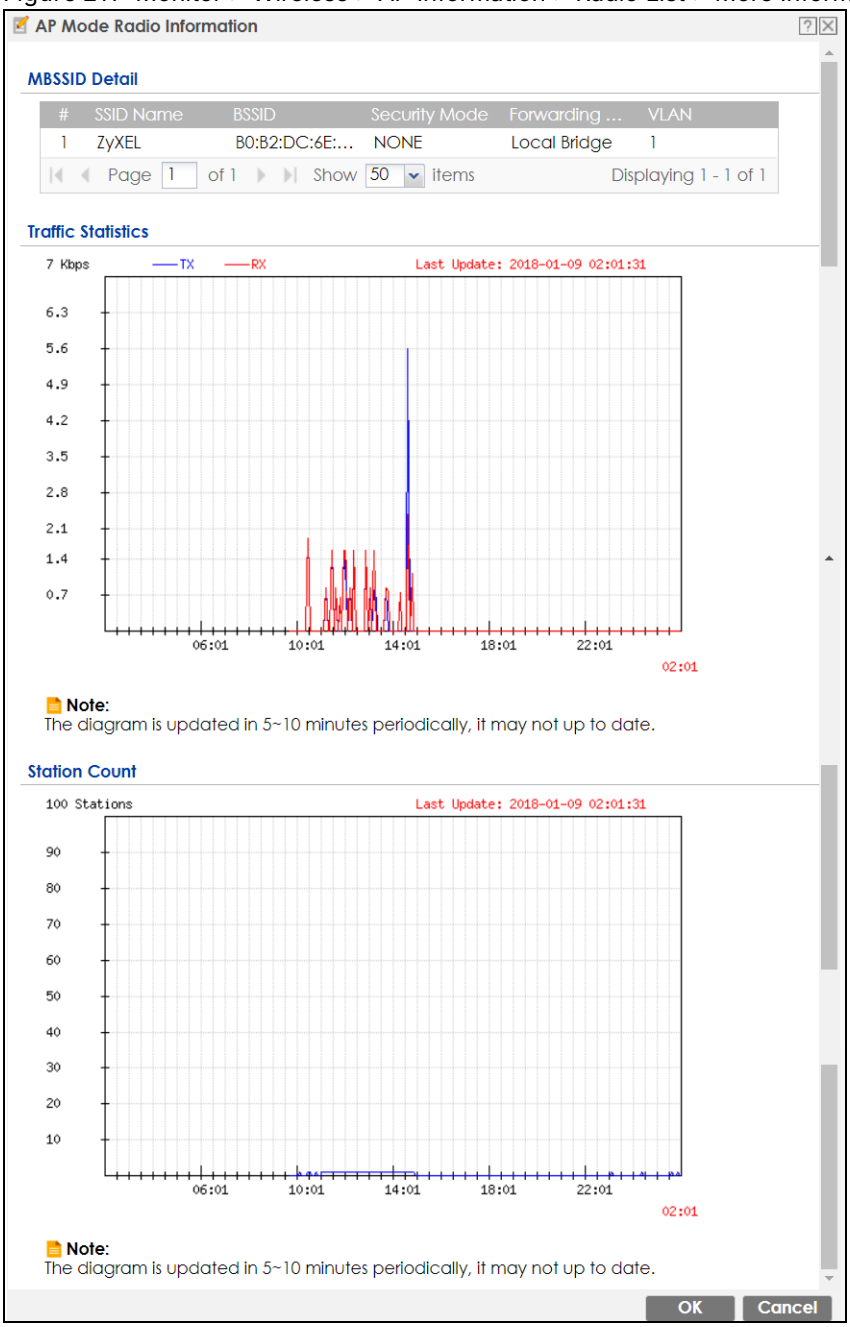
Table 51 Monitor > Wireless > AP Information > Radio List

LABEL	DESCRIPTION
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).

8.17.1 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 on the Radio List screen.

Figure 211 Monitor > Wireless > AP Information > Radio List > More Information



The following table describes the labels in this screen.

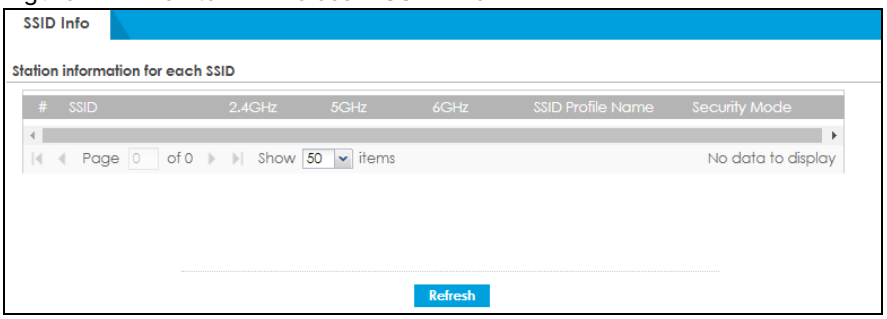
Table 52 Monitor > Wireless > AP Information > Radio List > More Information

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.

8.18 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 212 Monitor > Wireless > SSID Info



The following table describes the labels in this screen.

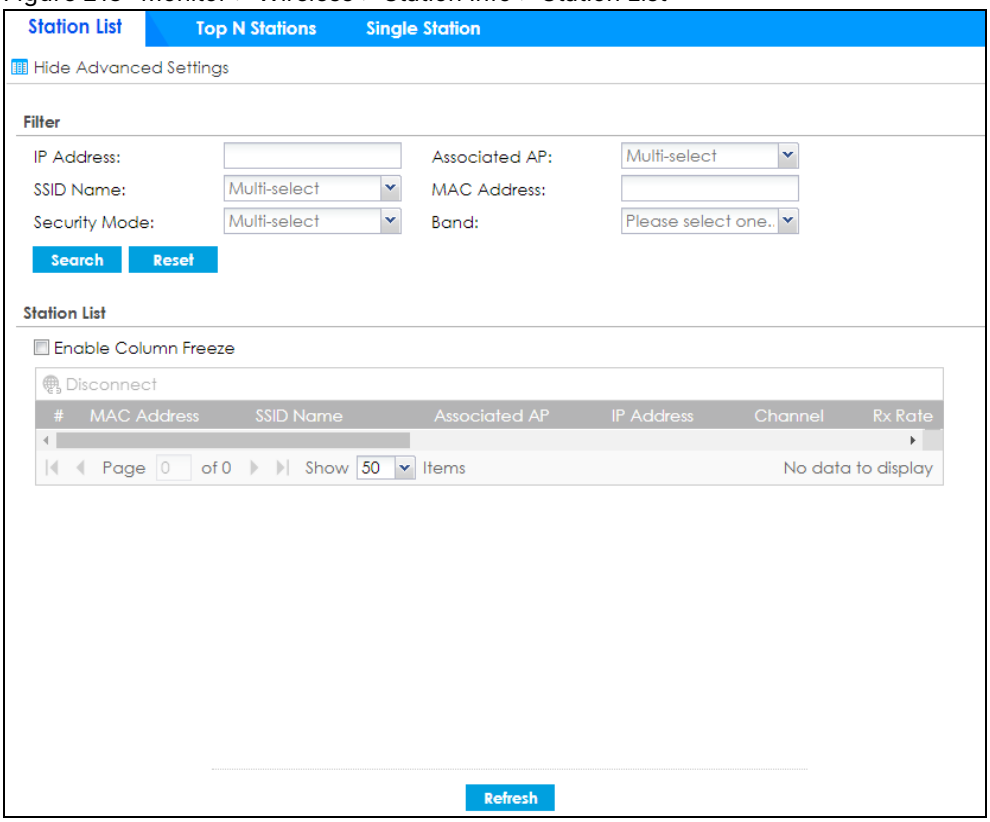
Table 53 Monitor > Wireless > SSID Info

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 8.20 on page 251.
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 8.20 on page 251.
6GHz	This shows the number of wireless clients which are currently connected to the SSID using the 6 GHz frequency band, Click the number to go to the Station Info > Station List screen. See Section 8.20 on page 251.
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.

8.19 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 213 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
Hide/Show Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Show Filter/ Hide Filer	Click this button to show or hide the filter settings.
Filter	
IP Address	Enter the IP address of the station you want to display. This field is case-sensitive.
Associated AP	Select the AP(s) with which the stations you want to display associate.
SSID Name	Select the SSID(s) to which the stations you want to display are connected.
MAC Address	Enter the MAC address of the station you want to display. This field is case-sensitive.
Security Mode	Select the security mode(s) used by the stations you want to display.
Account	Enter the user account name of the station you want to display. This field is case-sensitive.
Login Type	Select the login method(s) used by the stations you want to display.
Band	Select the frequency band used by the stations you want to display.
Search	Click this to update the list of stations based on the search criteria. Your search criteria is retained when navigating between screens.
Reset	Click this to return the search criteria to the factory defaults and display all connected stations without a filter.
Enable Column Freeze	Select this to lock the index columns in place while scrolling to the right.
Station List	

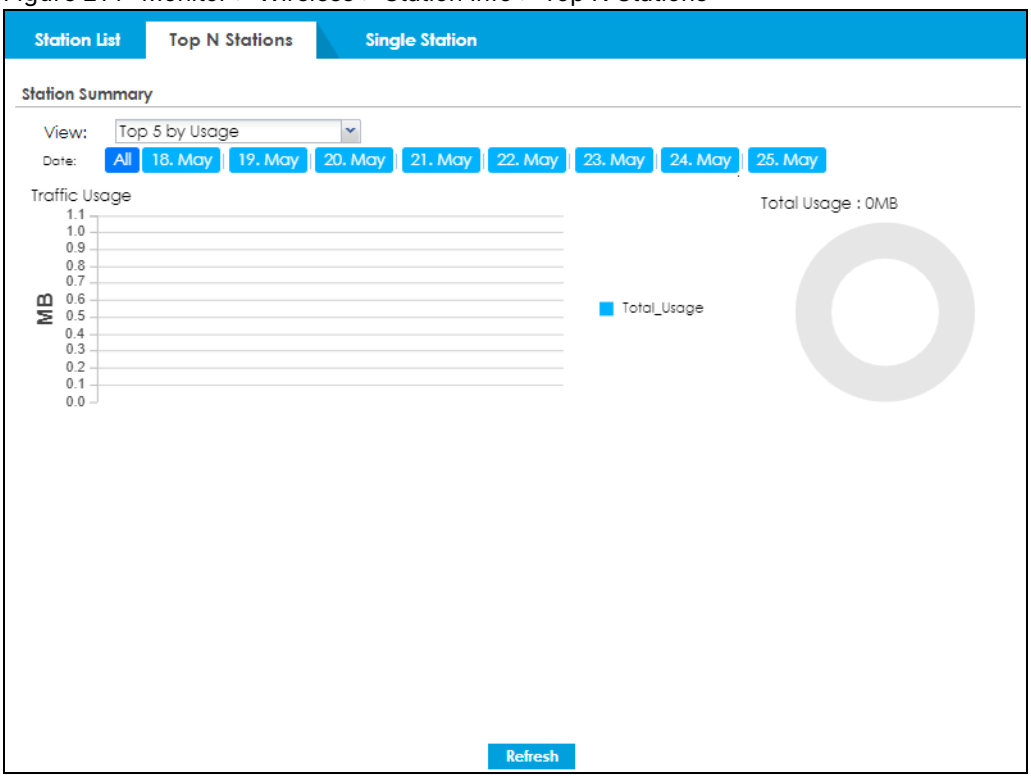
Table 54 Monitor > Wireless > Station Info > Station List (continued)

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.
SSID Name	This field displays the SSID names of the station.
Associated AP	This field displays the APs that are associated with the station.
IP Address	This field displays the IP address of the station.
Channel	This field displays the number of the channel used by the station to connect to the network.
Rx Rate	This field displays the receive data rate of the station.
Tx Rate	This field displays the transmit data rate of the station.
Signal Strength	This field displays the signal strength of the station.
Association Time	This field displays the time duration the station was online and offline.
Enterprise	This field displays the RADIUS server of the station.
Captive Portal	This displays whether the station logged into the network through the captive portal login page.
MAC Auth	This displays whether the station logged into the network through MAC authentication.
Band	This field displays the frequency band which is currently being used by the station.
Capability	This displays the supported standard currently being used by the station or the standards supported by the station.
802.11 Features	This displays whether the station supports IEEE802.11r, IEEE 802.11k, IEEE 802.11v or none of the above (N/A).
Security Mode	This field displays the security mode the station is using.
Download	This field displays the number of bytes received by the station.
Upload	This field displays the number of bytes transmitted from the station.
Refresh	Click Refresh to update this screen.

8.20 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 214 Monitor > Wireless > Station Info > Top N Stations



The following table describes the labels in this screen.

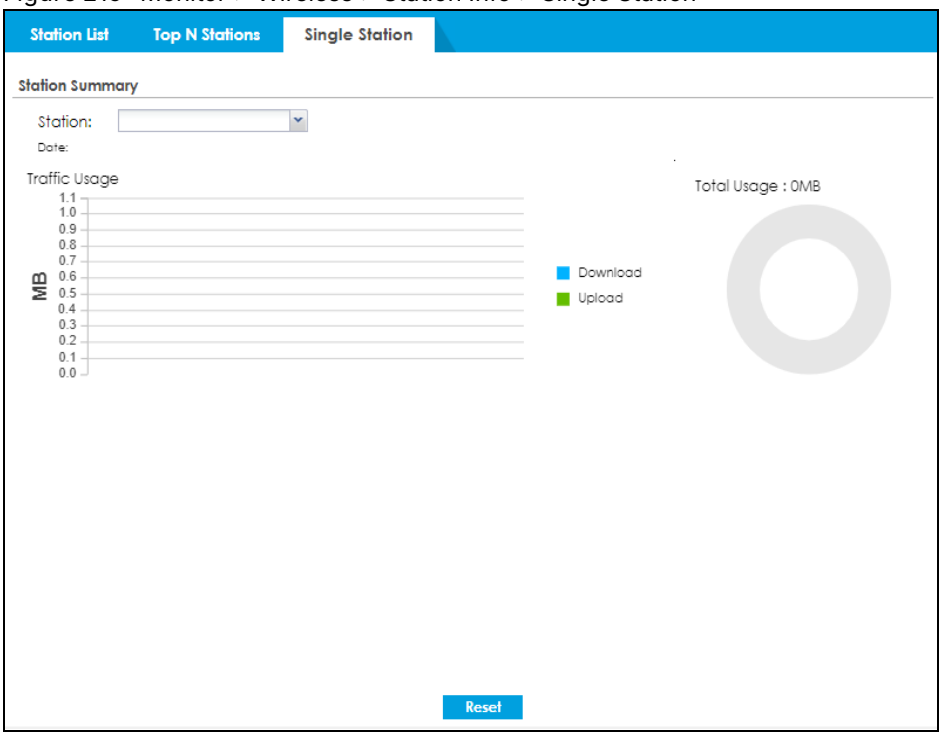
Table 55 Monitor > Wireless > Station Info > Top N Stations

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.

8.21 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 215 Monitor > Wireless > Station Info > Single Station



The following table describes the labels in this screen.

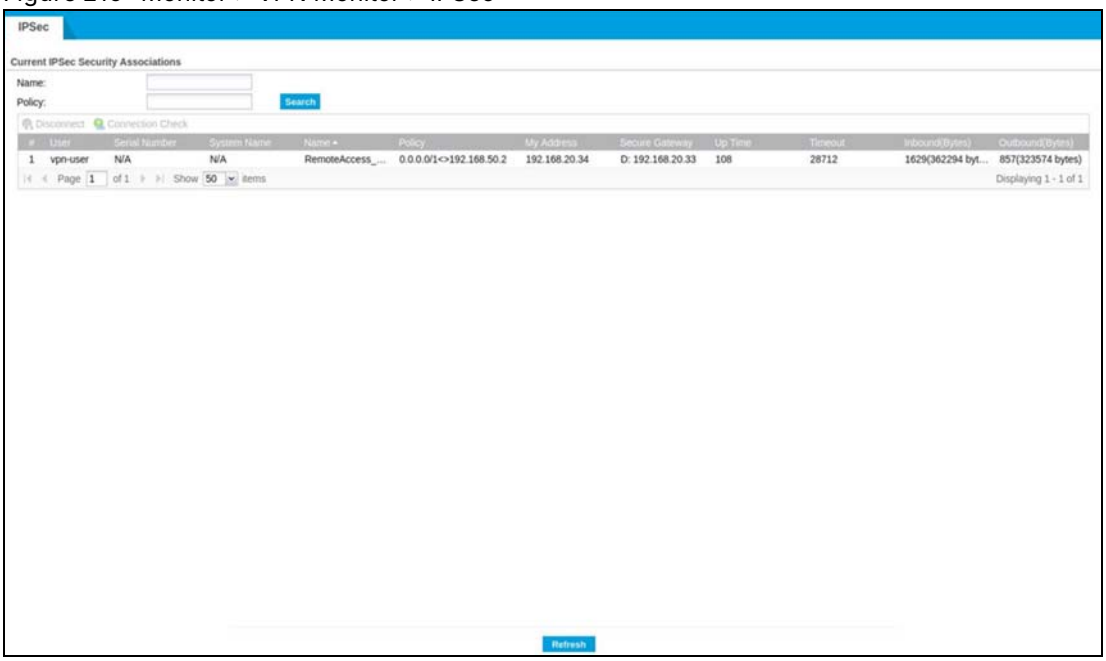
Table 56 Monitor > Wireless > Station Info > Single Station

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.

8.22 The IPSec Screen

You can use the IPSec 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 216 Monitor > VPN Monitor > IPSec



Each field is described in the following table.

Table 57 Monitor > VPN Monitor > IPSec

LABEL	DESCRIPTION
Name	Enter the name of a IPSec SA here and click Search to find it (if it is associated). You can use a keyword or regular expression. Use up to 30 alphanumeric and _+-.()!$*^:?|{}[]<>/ characters. See Section 8.22.1 on page 255 for more details.
Policy	Enter the IP address(es) or names of the local and remote policies for an IPSec SA and click Search to find it. You can use a keyword or regular expression. Use up to 30 alphanumeric and _+-.()!$*^:?|{}[]<>/ characters. See Section 8.22.1 on page 255 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.
User	This field only displays the client names if they're using EAP or X-auth for authentication. If a client is connected to the Zyxel Device without using Extended Authentication Protocol (EAP) or X-Auth, this field will be empty.
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.

Table 57 Monitor > VPN Monitor > IPSec (continued)

LABEL	DESCRIPTION
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.

8.22.1 Regular Expressions in Searching IPSec SAs

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

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

A * in the middle of a VPN connection or policy name has the 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.

8.23 The SSL Screen

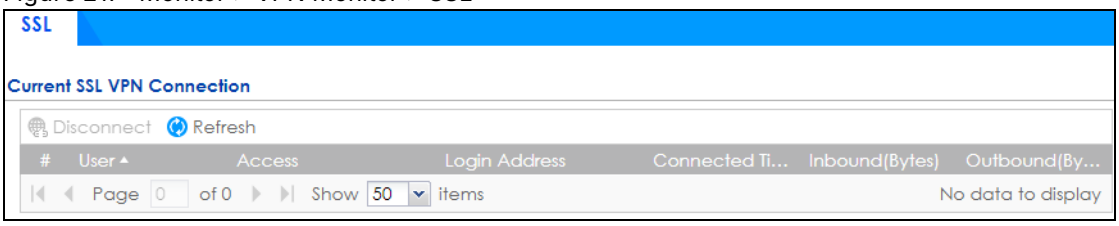
The Zyxel Device keeps track of the users who are currently logged into the VPN SSL client. Click Monitor > VPN Monitor > SSL to display the user list.

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 217 Monitor > VPN Monitor > SSL



The following table describes the labels in this screen.

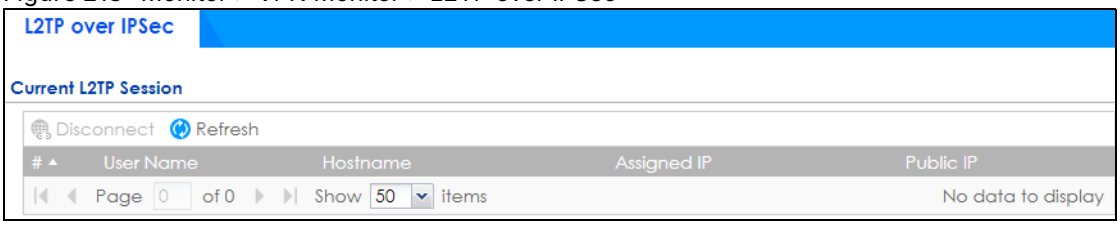
Table 58 Monitor > VPN Monitor > SSL

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.

8.24 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 218 Monitor > VPN Monitor > L2TP over IPSec



The following table describes the fields in this screen.

Table 59 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.

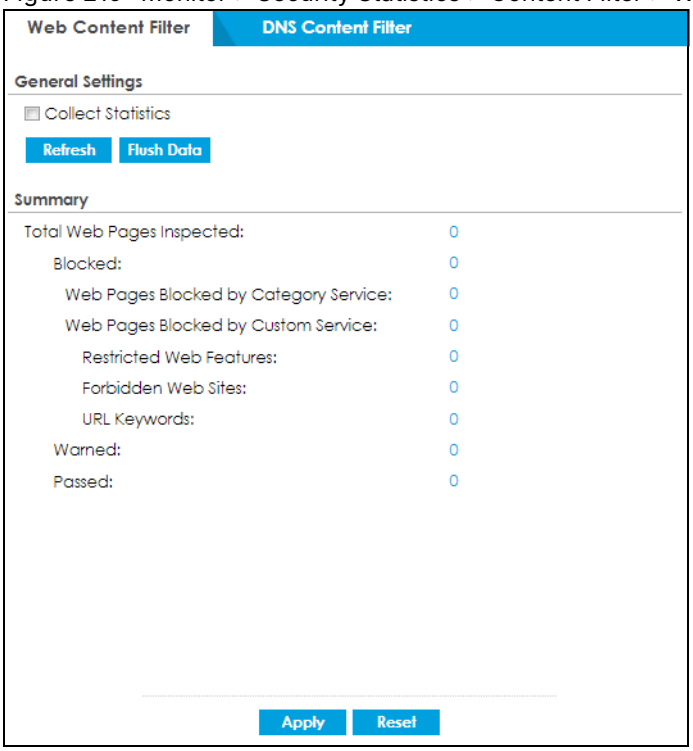
8.25 The Content Filter Screen

Click Monitor > Security Statistics > Content Filter to display the following screens.These screens display some basic statistics on web content filter and DNS content filer, such as the number of web pages and FQDNs inspected.

8.25.1 Web Content Filter

This screens display web content filter statistics.

Figure 219 Monitor > Security Statistics > Content Filter > Web Content Filter



The following table describes the labels in this screen.

Table 60 Monitor > Security Statistics > Content Filter > Web Content Filter

LABEL	DESCRIPTION
General Settings	
Collect Statistics	Select this checkbox to have the Zyxel Device collect web 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.
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	
Total Web Page Inspected	This field displays the number of web pages that the Zyxel Device's web content filter feature has checked.

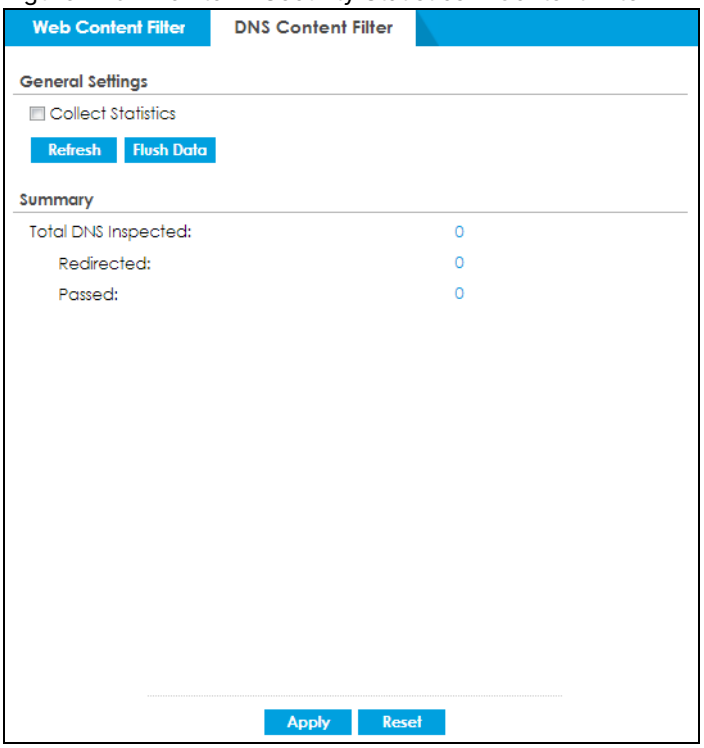
Table 60 Monitor > Security Statistics > Content Filter > Web Content Filter (continued)

LABEL	DESCRIPTION
Blocked	This is the number of web pages that the Zyxel Device blocked access.
Web Pages Blocked by Category Service	This is the number of web pages that matched an external database web content filtering category selected in the Zyxel Device and for which the Zyxel Device displayed a warning before allowing users access.
Web Page Blocked by Custom Service	This is the number of web pages to which the Zyxel Device did not allow access due to the web 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.
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.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

8.25.2 DNS Content Filter

This screens display DNS content filter statistics.

Figure 220 Monitor > Security Statistics > Content Filter > DNS Content Filter



The following table describes the labels in this screen.

Table 61 Monitor > Security Statistics > Content Filter > DNS Content Filter

LABEL	DESCRIPTION
General Settings	
Collect Statistics	Select this checkbox to have the Zyxel Device collect DNS 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.
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	
Total DNS Inspected	This field displays the number of FQDNs that the Zyxel Device's DNS content filter feature has checked.
Redirected	This is the number of FQDNs that the Zyxel Device redirects.
Passed	This is the number of FQDNs to which the Zyxel Device allowed access.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

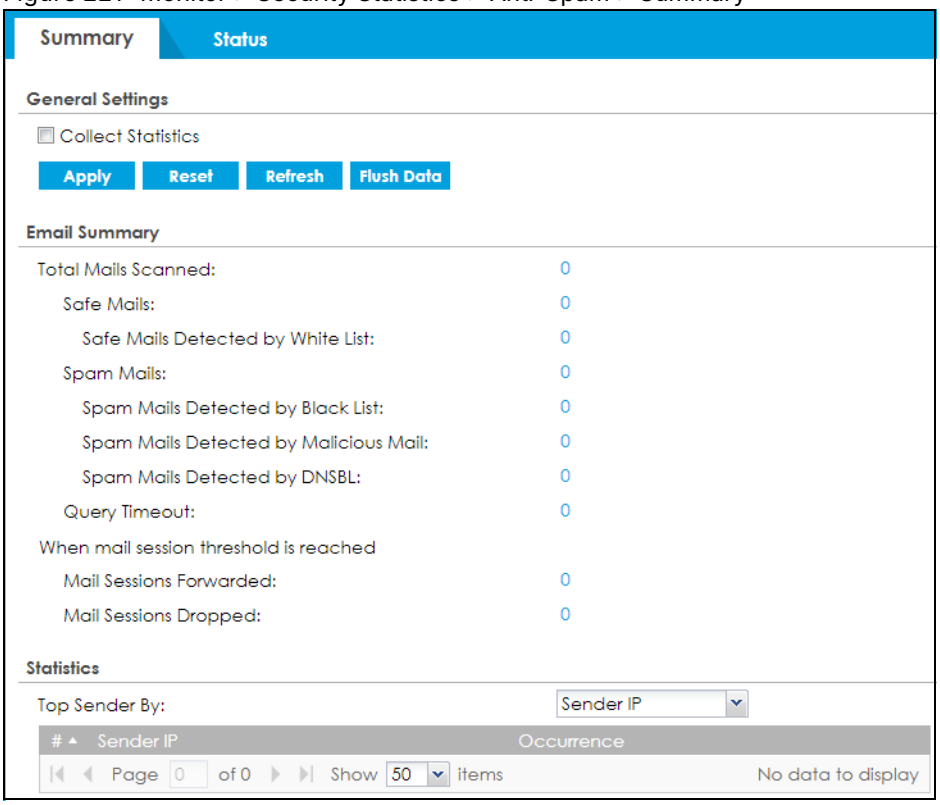
8.26 The Anti-Spam Screens

The Anti-Spam menu contains the Summary and Status screens.

8.26.1 Anti-Spam Summary

Click Monitor > Security Statistics > Anti-Spam > Summary to display the following screen. This screen displays spam statistics.

Figure 221 Monitor > Security Statistics > Anti-Spam > Summary



The following table describes the labels in this screen.

Table 62 Monitor > Security Statistics > Anti-Spam > 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 Allow list	This is the number of emails that matched an entry in the Zyxel Device's email security allow list.
Spam Mails	This is the number of emails that the Zyxel Device has determined to be spam.
Spam Mails Detected by Block List	This is the number of emails that matched an entry in the Zyxel Device's email security block list.
Spam Mails Detected by Malicious Mail	This is the number of emails that the Zyxel Device has determined to have malicious contents.

Table 62 Monitor > Security Statistics > Anti-Spam > Summary (continued)

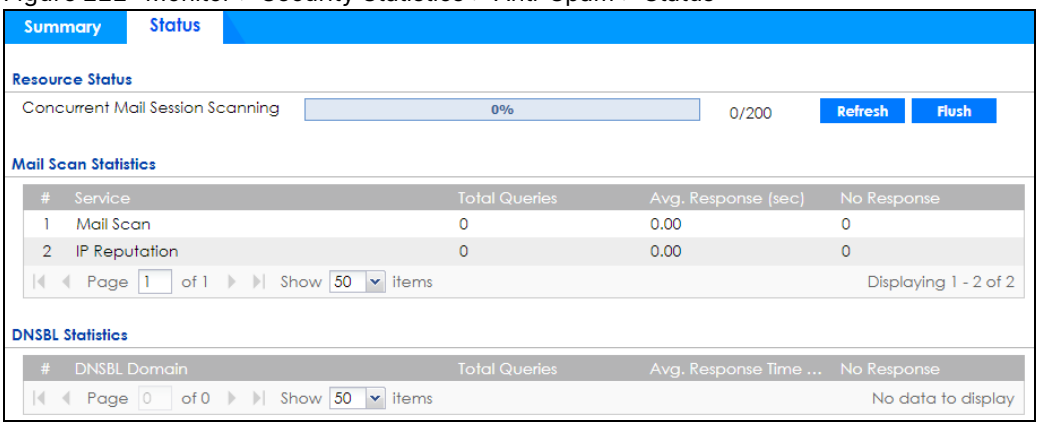
LABEL	DESCRIPTION
Spam Mails Detected by DNSBL	The Zyxel Device can check the sender and relay IP addresses in an email's header against DNS (Domain Name Service)-based spam Black Lists (DNSBLs). This is the number of emails that had a sender or relay IP address in the header which matched one of the DNSBLs that the Zyxel Device uses.
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 on 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 on 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.

8.26.2 The Anti-Spam Status Screen

Click Monitor > Security Statistics > Anti-Spam > Status to display the Anti-Spam Status screen.

Use the Anti-Spam Status screen to see how many email sessions the email security feature is scanning and statistics for the DNSBLs.

Figure 222 Monitor > Security Statistics > Anti-Spam > Status



The following table describes the labels in this screen.

Table 63 Monitor > Security Statistics > Anti-Spam > 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.

8.27 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.

8.27.1 View Log

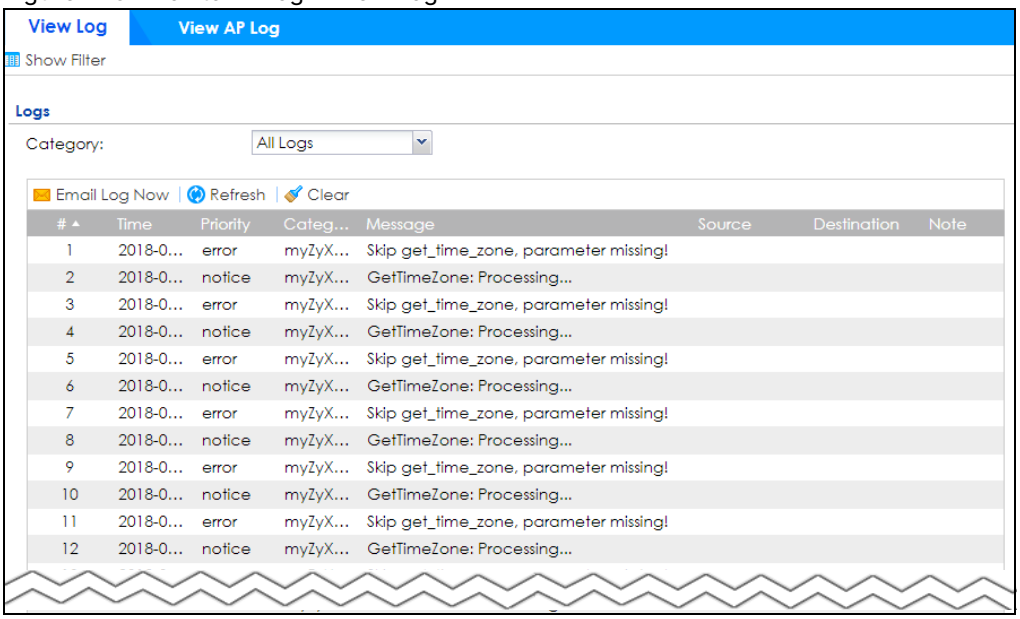
To access this screen, click Monitor > Log. The log is displayed on the following screen.

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 223 Monitor > Log > View Log



The following table describes the labels in this screen.

Table 64 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. Enter 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. Enter 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. Enter the source interface of the incoming packet that generated the log message.
Destination Interface	This displays when you show the filter. Enter 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.
Keyword	This displays when you show the filter. Enter 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 messages to the Active email addresses specified in the Send Log To field on the Log Settings page. Please note that only the following log messages will be sent: • Log messages that have not been sent before, and • log messages that match the categories you selected in Configuration > Log & Report > Log Settings > Edit > Active Log and Alert.
Refresh	Click this button to update the information on 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.

Table 64 Monitor > Log > View Log (continued)

LABEL	DESCRIPTION
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.

CHAPTER 9
Licensing

9.1 Registration Overview

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

- Use the Registration screen (see Section 9.1.2 on page 267) 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 9.1.3 on page 267) to display the status of your service registrations and upgrade licenses.

9.1.1 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.

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

License Update

Licenses are updated using port 443. Make sure TCP service port 443 is allowed on the router connected to the Zyxel Device.

Features Available Without a License

You can use the following Zyxel Device features without a license:

Table 65 Features Available Without a License

MONITOR	CONFIGURATION	MAINTENANCE
Traffic Statistics	Wireless	File Manager
Wireless	Network	Diagnostics
VPN Monitor	VPN	Packet Flow Explore
Log	BWM	Shutdown/Reboot
	Web Authentication	
	Security Policy	
	Object	

Table 65 Features Available Without a License

MONITOR	CONFIGURATION	MAINTENANCE
	System	
	Log & Report	

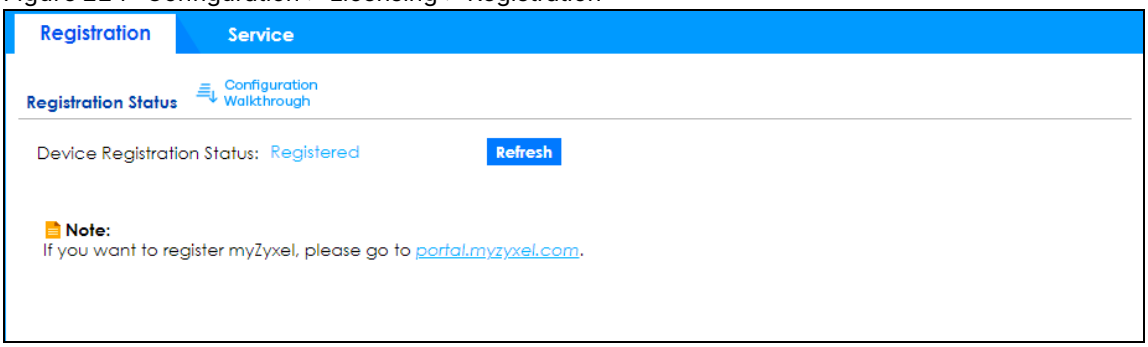
Please note that you cannot use the security services if your Zyxel Device does not have a license. Your Zyxel Device and network will be exposed to threats and attacks. We strongly recommend you to buy a license to better protect your Zyxel Device and network.

9.1.2 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 224 Configuration > Licensing > Registration



9.1.3 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 NCC or myZyxel.

The Service screen may show different services depending on the licenses you purchase or activate.

- Managed AP Service will be replaced by Secure WiFi when it's activated.

Note: Anti-Malware signatures contain Anti-Malware signatures and Threat Intelligence Machine Learning (TIML) signatures for Sandboxing. Both sets of signatures are included in the Gold Security Pack license, but only Anti-Malware signatures are included in the UTM license. If your Gold Security Pack license expires and you replace it with a UTM license, then your Sandboxing (TIML) signatures will not be updated and Sandboxing will not work. If your Gold Security Pack license expires, you should replace it with another Gold Security Pack license.

Check if Your Zyxel Device Has an Inactive License

After purchasing a license, assign it to your Zyxel Device. You have to activate the assigned license manually before your Zyxel Device can use it.

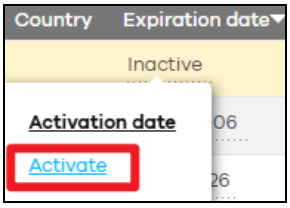
Follow the steps below to check if a license is assigned to your Zyxel Device and activate it (if not yet activated) through NCC or myZyxel.

Through NCC

1 Go to *NCC* and log in.

2 Go to Organization-wide > Device. Find your Zyxel Device and check the Expiration date field for the assigned license's status.

3 If the license has not been activated, hover over Inactive and click Activate to activate it on your Zyxel Device.



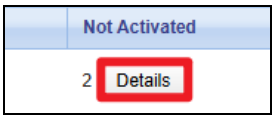
Through myZyxel

1 Go to *myZyxel* and log in.

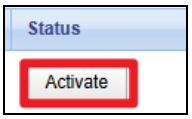
2 Go to Device Management > My Devices. Find your Zyxel Device and click its MAC Address.

3 Go to Linked Services to see the licenses assigned to your Zyxel Device. Check the Not Activated field to see the number of inactive licenses.

4 If there is any license that has not been activated, click Details.

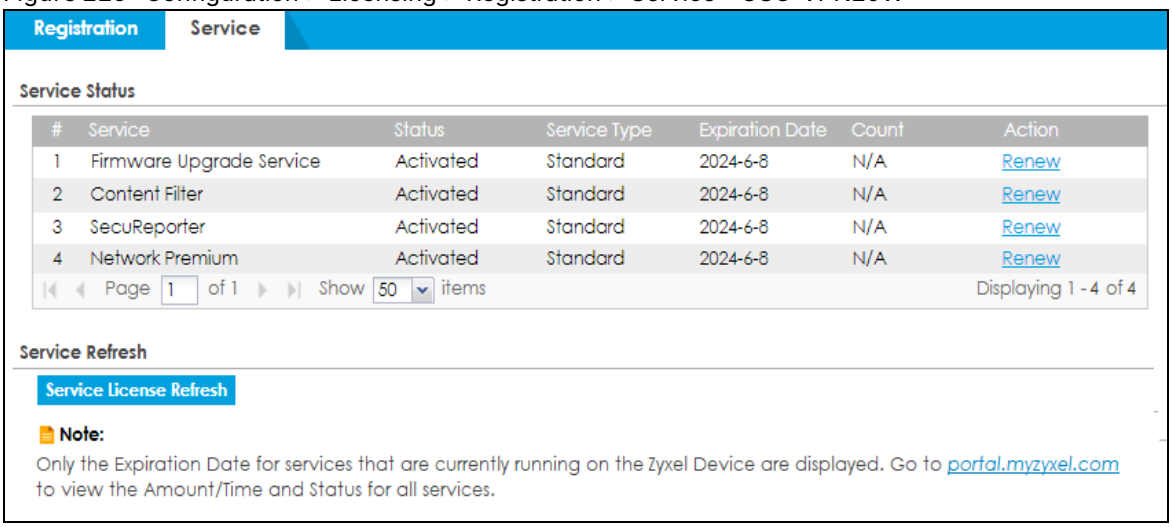


5 Click Activate to activate it on your Zyxel Device.



Click Configuration > Licensing > Registration > Service to display the following screen.

Figure 225 Configuration > Licensing > Registration > Service - USG-VPN20W



The following table describes the labels in this screen.

Table 66 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.
Content Filter	This is a license to a database that can block websites by category, such as Gambling.
SecuReporter	This is a license that allows SecuReporter to collect and analyze logs from your Zyxel Device in order to identify anomalies, notify you of potential internal or external threats, and report on network usage. The Zyxel Device retains logs up to 1 year.
Network Premium	This is a license to use Single-Sign On (SSO) that allows the Zyxel Device to communicate with an SSO agent.
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.
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.

Table 66 Configuration > Licensing > Registration > Service (continued)

LABEL	DESCRIPTION
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.

CHAPTER 10
Wireless

10.1 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.

10.1.1 What You Can Do in this Chapter

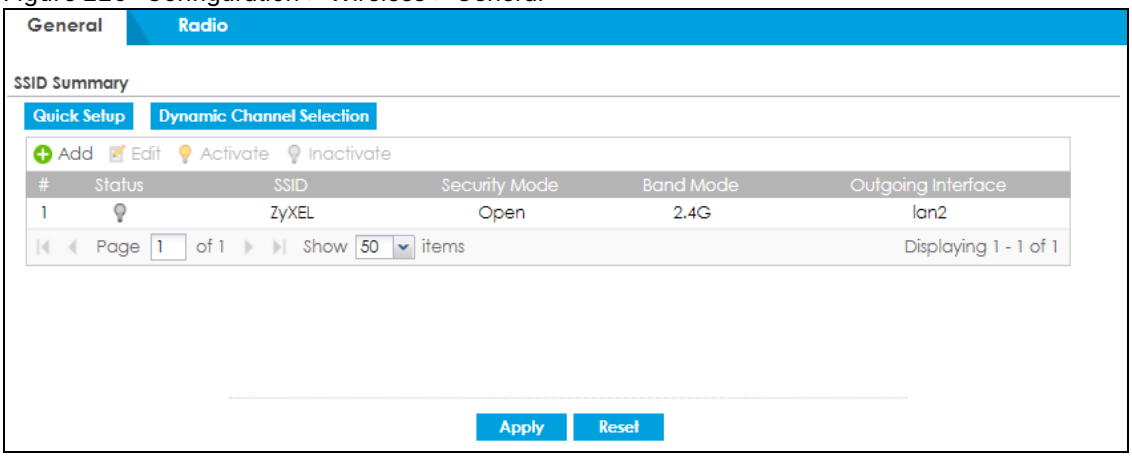
- Use the Built-in AP screen (Section 10.2 on page 271) to allow WiFi clients to access your Zyxel Device wirelessly to connect to the network.

10.2 Built-in AP

Use this screen to allow WiFi clients to access your Zyxel Device wirelessly to connect to the network.

The Configuration > Wireless > Built-in AP displays showing AP information in Built-in AP Mode.

Figure 226 Configuration > Wireless > General



Each field is described in the following table.

Table 67 Configuration > Wireless > General

LABEL	DESCRIPTION
SSID Summary	
Quick Setup	Click this to go to the Quick Setup Wireless Wizard to configure a wireless network.
Dynamic Channel Selection	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.

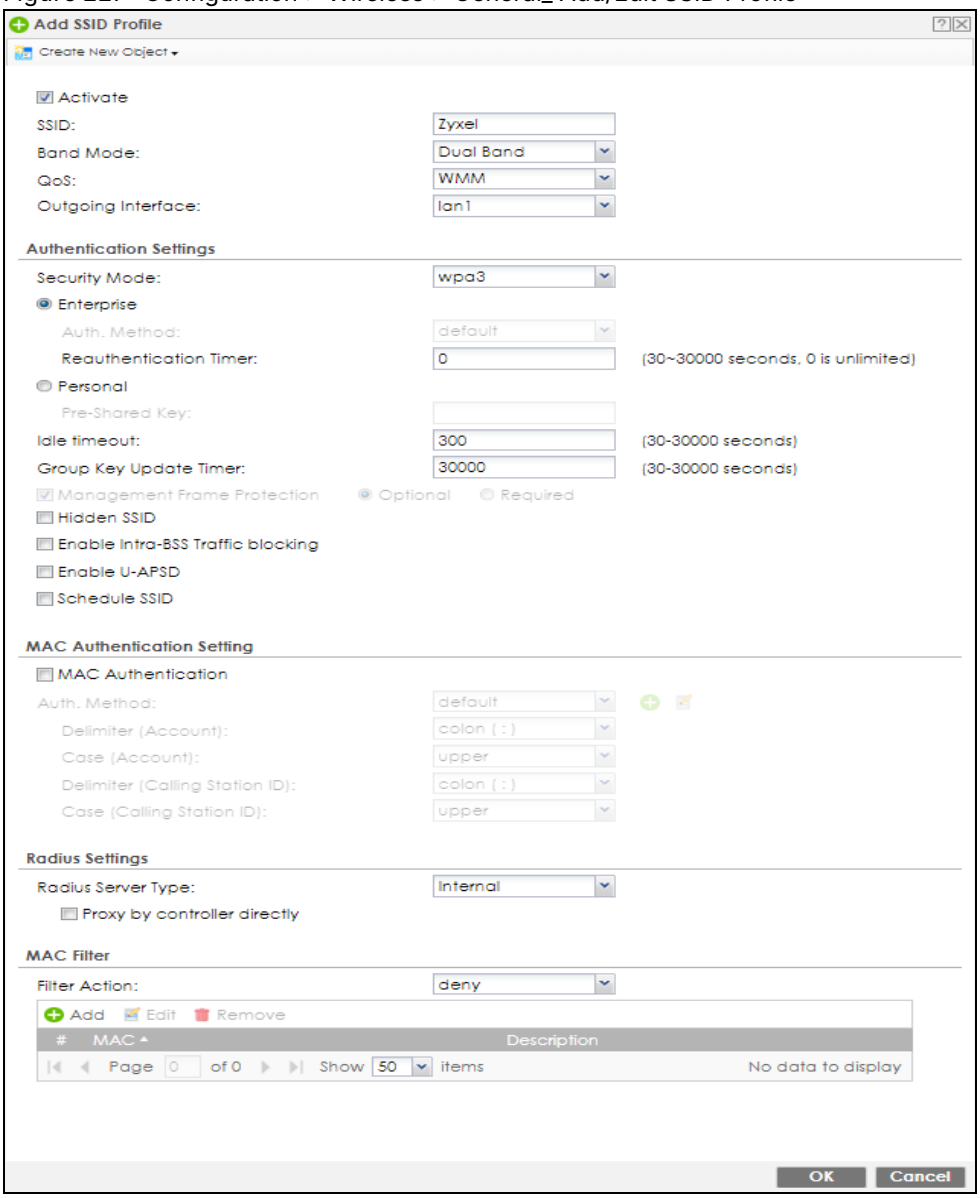
Table 67 Configuration > Wireless > General (continued)

LABEL	DESCRIPTION
Add	Click this to configure a new wireless network. You can configure up to 4 SSID profiles.
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 wireless network's index number in this list.
Status	This displays whether or not the wireless network is activated.
SSID	This shows the name of the wireless network.
Security Mode	This shows the security used for this wireless network. No security allows any wireless client to associate with this network without authentication.
Band Mode	This shows the wireless band which this wireless network uses. 2.4 GHz is the frequency used by IEEE 802.11b/g/n/ax wireless clients. 5 GHz is the frequency used by IEEE 802.11ax/ac/a/n wireless clients.
Outgoing Interface	This is the outgoing interface that the wireless network uses to transmit packets.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

10.2.1 Wireless > Built-in AP > General > Add/Edit SSID

This screen allows you to create a new SSID profile or edit an existing one. An SSID, or Service Set IDentifier, is the name of the wireless network to which a wireless client can connect. To access this screen, click the Add button or select an entry from the list in Configuration > Wireless > Built-in AP then and click the Edit button.

Figure 227 Configuration > Wireless > General_ Add/Edit SSID Profile



Each field is described in the following table.

Table 68 Configuration > Object > AP Profile > SSID > SSID List > Add/Edit SSID Profile

LABEL	DESCRIPTION
Activate	To turn on an entry, select Activate. To turn off an entry, select it and click Inactivate.
SSID	Enter the SSID name for this profile. This is the name visible on the network to wireless clients. Enter up to 32 characters, spaces and underscores are allowed.
Band Mode	This shows the wireless band which this wireless network uses. 2.4 GHz is the frequency used by IEEE 802.11b/g/n/ax wireless clients. 5 GHz is the frequency used by IEEE 802.11ax/ac/a/n wireless clients.

Table 68 Configuration > Object > AP Profile > SSID > SSID List > Add/Edit SSID Profile (continued)

LABEL	DESCRIPTION
QoS	Select a Quality of Service (QoS) access category to associate with this SSID. Access categories minimize the delay of data packets across a wireless network. Certain categories, such as video or voice, are given a higher priority due to the time sensitive nature of their data packets. QoS access categories are as follows: disable: Turns off QoS for this SSID. All data packets are treated equally and not tagged with access categories. WMM: Enables automatic tagging of data packets. The Zyxel Device assigns access categories to the SSID by examining data as it passes through it and making a best guess effort. If something looks like video traffic, for instance, it is tagged as such. WMM_VOICE: All wireless traffic to the SSID is tagged as voice data. This is recommended if an SSID is used for activities like placing and receiving VoIP phone calls. WMM_VIDEO: All wireless traffic to the SSID is tagged as video data. This is recommended for activities like video conferencing. WMM_BEST_EFFORT: All wireless traffic to the SSID is tagged as “best effort,” meaning the data travels the best route it can without displacing higher priority traffic. This is good for activities that do not require the best bandwidth throughput, such as surfing the Internet. WMM_BACKGROUND: All wireless traffic to the SSID is tagged as low priority or “background traffic”, meaning all other access categories take precedence over this one. If traffic from an SSID does not have strict throughput requirements, then this access category is recommended. For example, an SSID that only has network printers connected to it.
Outgoing Interface	Select the outgoing interface that the wireless network uses to transmit packets.
Authentication Settings	
Security Mode	Select a security mode from the list: open, wep, wpa2 or wpa2-mix.
Enterprise	Select this to enable 802.1x secure authentication with a RADIUS server.
Auth. Method	This field is available only when you select the RADIUS Server Type to Internal. Select an authentication method if you have created any on the Configuration > Object > Auth. Method screen.
Reauthentication Timer	Enter the interval (in seconds) between authentication requests. Enter a 0 for unlimited requests.
Personal	Select this option to use a Pre-Shared Key with WPA encryption.
Pre-Shared Key	Enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
Cipher Type	Select an encryption cipher type from the list. • auto - This automatically chooses the best available cipher based on the cipher in use by the wireless client that is attempting to make a connection. • aes - This is the Advanced Encryption Standard encryption method. It is a more recent development over TKIP and considerably more robust. Not all wireless clients may support this.
Idle Timeout	Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued.
Group Key Update Timer	Enter the interval (in seconds) at which the AP updates the group WPA encryption key.
Pre-Authentication	This field is available only when you set Security Mode to wpa2 or wpa2-mix and enable 802.1x authentication. Enable or Disable pre-authentication to allow the AP to send authentication information to other APs on the network, allowing connected wireless clients to switch APs without having to re-authenticate their network connection.

Table 68 Configuration > Object > AP Profile > SSID > SSID List > Add/Edit SSID Profile (continued)

LABEL	DESCRIPTION
Management Frame Protection	This field is available only when you select wpa2 in the Security Mode field and set Cipher Type to aes. Data frames in 802.11 WLANs can be encrypted and authenticated with WEP, WPA or WPA2. But 802.11 management frames, such as beacon/probe response, association request, association response, de-authentication and disassociation are always unauthenticated and unencrypted. IEEE 802.11w Protected Management Frames allows APs to use the existing security mechanisms (encryption and authentication methods defined in IEEE 802.11i WPA/WPA2) to protect management frames. This helps prevent wireless DoS attacks. Select the checkbox to enable management frame protection (MFP) to add security to 802.11 management frames. Select Optional if you do not require the wireless clients to support MFP. Management frames will be encrypted if the clients support MFP. Select Required and wireless clients must support MFP in order to join the Zyxel Device's wireless network.
Hidden SSID	Select this if you want to "hide" your SSID from wireless clients. This tells any wireless clients in the vicinity of the AP using this SSID profile not to display its SSID name as a potential connection. Not all wireless clients respect this flag and display it anyway. When a SSID is "hidden" and a wireless client cannot see it, the only way you can connect to the SSID is by manually entering the SSID name in your wireless connection setup screen(s) (these vary by client, client connectivity software, and operating system).
Enable Intra-BSS Traffic Blocking	Select this option to prevent crossover traffic from within the same SSID on the Zyxel Device.
Enable U-APSD	Select this option to enable Unscheduled Automatic Power Save Delivery (U-APSD), which is also known as WMM-Power Save. This helps increase battery life for battery-powered wireless clients connected to the Zyxel Device using this SSID profile.
Enable ARP Proxy	The Address Resolution Protocol (ARP) is a protocol for mapping an IP address to a MAC address. An ARP broadcast is sent to all devices on the same Ethernet network to request the MAC address of a target IP address. Select this option to allow the Zyxel Device to answer ARP requests for an IP address on behalf of a client associated with this SSID. This can reduce broadcast traffic and improve network performance.
Schedule SSID	Select this option and set whether the SSID is enabled or disabled on each day of the week. You also need to select the hour and minute (in 24-hour format) to specify the time period of each day during which the SSID is enabled/enabled.
MAC Authentication	Select this to use an external server or the Zyxel Device's local database to authenticate wireless clients by their MAC addresses. Users cannot get an IP address if the MAC authentication fails. An external server can use the wireless client's account (username/password) or Calling Station ID for MAC authentication. Configure the ones the external server uses.
Delimiter (Account)	Select the separator the external server uses for the two-character pairs within account MAC addresses.
Case (Account)	Select the case (upper or lower) the external server requires for letters in the account MAC addresses.
Delimiter (Calling Station ID)	RADIUS servers can require the MAC address in the Calling Station ID RADIUS attribute. Select the separator the external server uses for the pairs in calling station MAC addresses.
Case (Calling Station ID)	Select the case (upper or lower) the external server requires for letters in the calling station MAC addresses.
Radius Settings	
Radius Server Type	Select Internal to use the Zyxel Device's internal authentication database, or External to use an external RADIUS server for authentication.

Table 68 Configuration > Object > AP Profile > SSID > SSID List > Add/Edit SSID Profile (continued)

LABEL	DESCRIPTION
Proxy by controller directly	Select this to allow the Zyxel Device to answer authentication requests on behalf of an external RADIUS server.
MAC Filter	
Filter Action	Select allow to permit the wireless client with the MAC addresses in this profile to connect to the network through the associated SSID; select deny to block the wireless clients with the specified MAC addresses.
Add	Click this to add a MAC address to the profile's list.
Edit	Click this to edit the selected MAC address in the profile's list.
Remove	Click this to remove the selected MAC address from the profile's list.
#	This field is a sequential value, and it is not associated with a specific user.
MAC	This field specifies a MAC address associated with this profile. You can click the MAC address to make it editable.
Description	This field displays a description for the MAC address associated with this profile. You can click the description to make it editable. Enter up to 60 characters, spaces and underscores allowed.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving your changes.

10.2.2 Wireless > Built-in AP > Radio

This screen allows you to create radio profiles for the Zyxel Device. A radio profile is a list of settings that a Zyxel Device can use to configure its radio transmitter(s).To access this screen click Configuration > Wireless > Built-in AP > Radio.

Figure 228 Wireless > Built-in AP > Radio

General | Radio

Hide Advanced Settings

2.4GHz General Settings

802.11 Band: 11b/g/n
Channel Width: 20MHz
Channel Selection: DCS Manual 6
Output Power: 30 dBm (0~30)
Enable DCS Client Aware
2.4 GHz Channel Selection Method: auto
2.4 GHz Channel Deployment: Three-Channel Deployment
Time Interval
DCS Time Interval: 720 (10~1440 minutes)
Schedule

Advance
Guard Interval: Short Long
Enable A-MPDU Aggregation
A-MPDU Limit: 50000 (100~65535)
A-MPDU Subframe: 32 (2~64)
Enable A-MSDU Aggregation
A-MSDU Limit: 4096 (2290~4096)
RTS/CTS Threshold: 2347 (0~2347)
Beacon Interval: 100 (40ms~1000ms)
DTIM: 1 (1~255)
Enable Signal Threshold
Station Signal Threshold: -76 dBm (-20 ~ -76)
Disassociate Station Threshold: -88 dbm (-20 ~ -105)
Allow Station Connection after Multiple Retries
Station Retry Count: 1 (1 ~ 100)
Allow 802.11n/ac stations only

Multicast Settings
Transmission Mode: Multicast to Unicast Fixed Multicast Rate
Multicast Rate(Mbps): 1 2 5.5 11 6 9 12 18 24 36 48 54

5GHz General Settings

802.11 Band: 11ac
Channel Width: 20/40/80MHz
Channel Selection: DCS Manual 36
Output Power: 30 dBm (0~30)
Enable DCS Client Aware
Avoid 5 GHz DFS Channel
5 GHz Channel Selection Method: auto
Time Interval
DCS Time Interval: 720 (10~1440 minutes)
Schedule

Advance
Guard Interval: Short Long
Enable A-MPDU Aggregation
A-MPDU Limit: 50000 (100~65535)
A-MPDU Subframe: 32 (2~64)
Enable A-MSDU Aggregation
A-MSDU Limit: 4096 (2290~4096)
RTS/CTS Threshold: 2347 (0~2347)
Beacon Interval: 100 (40ms~1000ms)
DTIM: 1 (1~255)
Enable Signal Threshold
Station Signal Threshold: -76 dBm (-20 ~ -76)
Disassociate Station Threshold: -88 dbm (-20 ~ -105)
Allow Station Connection after Multiple Retries
Station Retry Count: 1 (1 ~ 100)
Allow 802.11n/ac stations only

Multicast Settings
Transmission Mode: Multicast to Unicast Fixed Multicast Rate
Multicast Rate(Mbps): 6 9 12 18 24 36 48 54

Apply Reset

The following table describes the labels in this screen.

Table 69 Wireless > Built-in AP > Radio

LABEL	DESCRIPTION
Hide / Show Advanced Settings	Click this to hide or show the Advanced Settings in this window.
2.4GHz General Settings	
802.11 Band	Select how to let wireless clients connect to the AP. • 11b/g: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the AP. The AP adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices. • 11b/g/n: allows IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the AP. The transmission rate of your AP might be reduced. • 11ax: allows IEEE802.11b, IEEE802.11g, IEEE802.11n, and IEEE802.11ax compliant WLAN devices to associate with the Zyxel Device. If the WLAN device isn't compatible with 802.11ax, the Zyxel Device will communicate with the WLAN device using 802.11n, and so on.
Channel Width	Select the wireless channel bandwidth you want the AP to use. A standard 20 MHz channel offers transfer speeds of up to 144Mbps (2.4GHz) or 217Mbps (5GHZ) whereas a 40MHz channel uses two standard channels and offers speeds of up to 300Mbps (2.4GHz) or 450Mbps (5GHZ). 40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. Because not all devices support all channels, select 20/40MHz to allow the AP to adjust the channel bandwidth automatically. Select 20MHz if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding. Note: If the environment has poor signal-to-noise (SNR), the Zyxel Device will switch to a lower bandwidth.
Channel Selection	Select the wireless channel which this radio profile should use. It is recommended that you choose the channel least in use by other APs in the region where this profile will be implemented. This will reduce the amount of interference between wireless clients and the AP to which this profile is assigned. Select DCS to have the AP automatically select the radio channel upon which it broadcasts by scanning the area around it and determining what channels are currently being used by other devices. Note: If you change the country code later, Channel Selection is set to Manual automatically. Select Manual and specify the channels the AP uses.
Output Power	Enter the maximum output power of the Zyxel Device. If there is a high density of APs in an area, decrease the output power of the Zyxel Device to reduce interference with other APs. Reducing the output power also reduces the Zyxel Device's effective broadcast radius.
Enable DCS Client Aware	This field is available when you set Channel Selection to DCS. Select this to have the AP wait until all connected clients have disconnected before switching channels. If you disable this then the AP switches channels immediately regardless of any client connections. In this instance, clients that are connected to the AP when it switches channels are dropped.

Table 69 Wireless > Built-in AP > Radio

LABEL	DESCRIPTION
2.4 GHz Channel Selection Method	This field is available when you set Channel Selection to DCS. Select auto to have the AP search for available channels automatically in the 2.4 GHz band. The available channels vary depending on what you select in the 2.4 GHz Channel Deployment field. Select manual and specify the channels the AP uses in the 2.4 GHz band.
Channel ID	This field is available only when you set Channel Selection to DCS and set 2.4 GHz Channel Selection Method to manual. Select the checkboxes of the channels that you want the AP to use.
2.4 GHz Channel Deployment	This field is available only when you set Channel Selection to DCS and set 2.4 GHz Channel Selection Method to auto. Select Three-Channel Deployment to limit channel switching to channels 1,6, and 11, the three channels that are sufficiently attenuated to have almost no impact on one another. In other words, this allows you to minimize channel interference by limiting channel-hopping to these three “safe” channels. Select Four-Channel Deployment to limit channel switching to four channels. Depending on the country domain, if the only allowable channels are 1-11 then the Zyxel Device uses channels 1, 4, 7, 11 in this configuration; otherwise, the Zyxel Device uses channels 1, 5, 9, 13 in this configuration. Four channel deployment expands your pool of possible channels while keeping the channel interference to a minimum.
Time Interval	Select this option to have the Zyxel Device survey the other APs within its broadcast radius at the end of the specified time interval.
DCS Time Interval	This field is available when you set Channel Selection to DCS. Enter a number of minutes. This regulates how often the AP surveys the other APs within its broadcast radius. If the channel on which it is currently broadcasting suddenly comes into use by another AP, the AP will then dynamically select the next available clean channel or a channel with lower interference.
Schedule	Select this option to have the Zyxel Device survey the other APs within its broadcast radius at a specific time on selected days of the week.
Start Time	Specify the time of the day (in 24-hour format) to have the Zyxel Device use DCS to automatically scan and find a less-used channel.
Week Days	Select each day of the week to have the Zyxel Device use DCS to automatically scan and find a less-used channel.
Advanced Settings	
Guard Interval	This field is available only when the channel width is 20/40MHz or 20/40/80MHz. Set the guard interval for this radio profile to either Short or Long. The guard interval is the gap introduced between data transmission from users in order to reduce interference. Reducing the interval increases data transfer rates but also increases interference. Increasing the interval reduces data transfer rates but also reduces interference.
Enable A-MPDU Aggregation	Select this to enable A-MPDU aggregation. Message Protocol Data Unit (MPDU) aggregation collects Ethernet frames along with their 802.11n headers and wraps them in a 802.11n MAC header. This method is useful for increasing bandwidth throughput in environments that are prone to high error rates.
A-MPDU Limit	Enter the maximum frame size to be aggregated.
A-MPDU Subframe	Enter the maximum number of frames to be aggregated each time.

Table 69 Wireless > Built-in AP > Radio

LABEL	DESCRIPTION
Enable A-MSDU Aggregation	Select this to enable A-MSDU aggregation. Mac Service Data Unit (MSDU) aggregation collects Ethernet frames without any of their 802.11n headers and wraps the header-less payload in a single 802.11n MAC header. This method is useful for increasing bandwidth throughput. It is also more efficient than A-MPDU except in environments that are prone to high error rates.
A-MSDU Limit	Enter the maximum frame size to be aggregated.
RTS/CTS Threshold	Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions). A wireless client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS/CTS equal to or higher than the fragmentation threshold to turn RTS/CTS off.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. A high value helps save current consumption of the access point.
DTIM	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255.
Enable Signal Threshold	Select the checkbox to use the signal threshold to ensure wireless clients receive good throughput. This allows only wireless clients with a strong signal to connect to the AP. Clear the checkbox to not require wireless clients to have a minimum signal strength to connect to the AP.
Station Signal Threshold	Set a minimum client signal strength. A wireless client is allowed to connect to the AP only when its signal strength is stronger than the specified threshold. -20 dBm is the strongest signal you can require and -76 is the weakest.
Disassociate Station Threshold	Set a minimum kick-off signal strength. When a wireless client’s signal strength is lower than the specified threshold, the Zyxel Device disconnects the wireless client from the AP. -20 dBm is the strongest signal you can require and -90 is the weakest.
Allow Station Connection after Multiple Retries	Select this option to allow a wireless client to try to associate with the AP again after it is disconnected due to weak signal strength.
Station Retry Count	Set the maximum number of times a wireless client can attempt to re-connect to the AP.
Allow 802.11n/ac stations only	Only select this if you want to deny 802.11b/g/n clients access to the radio.
Multicast Settings	Use this section to set a transmission mode and maximum rate for multicast traffic.
Transmission Mode	Set how the AP handles multicast traffic. Select Multicast to Unicast to broadcast wireless multicast traffic to all of the wireless clients as unicast traffic. Unicast traffic dynamically changes the data rate based on the application’s bandwidth requirements. The retransmit mechanism of unicast traffic provides more reliable transmission of the multicast traffic, although it also produces duplicate packets. Select Fixed Multicast Rate to send wireless multicast traffic at a single data rate. You must know the multicast application’s bandwidth requirements and set it in the following field.
Multicast Rate (Mbps)	If you set the multicast transmission mode to fixed multicast rate, set the data rate for multicast traffic here. For example, to deploy 4 Mbps video, select a fixed multicast rate higher than 4 Mbps.

Table 69 Wireless > Built-in AP > Radio

LABEL	DESCRIPTION
5GHz General Settings	
802.11 Band	Select how to let wireless clients connect to the AP. • 11a: allows only IEEE 802.11a compliant WLAN devices to associate with the Zyxel Device. • 11a/n: allows both IEEE802.11n and IEEE802.11a compliant WLAN devices to associate with the Zyxel Device. • 11ac: allows IEEE802.11n, IEEE802.11a, and IEEE802.11ac compliant WLAN devices to associate with the Zyxel Device. If the WLAN device isn't compatible with 802.11ac, the Zyxel Device will communicate with the WLAN device using 802.11n, and so on. • 11ax: allows IEEE802.11b, IEEE802.11g, IEEE802.11n, and IEEE802.11ax compliant WLAN devices to associate with the Zyxel Device. If the WLAN device isn't compatible with 802.11ax, the Zyxel Device will communicate with the WLAN device using 802.11n, and so on.
Channel Width	Select the channel bandwidth you want to use for your wireless network. Select 20 MHz if you want to lessen radio interference with other wireless devices in your neighborhood. Select 20/40 MHz to allow the Zyxel Device to choose the channel bandwidth (20 or 40 MHz) that has least interference. Select 20/40/80 MHz to allow the Zyxel Device to choose the channel bandwidth (20 or 40 or 80 MHz) that has least interference. This option is available only when you select 11ac or 11ax in the 802.11 Mode field. Note: If the environment has poor signal-to-noise ratio (SNR), the Zyxel Device will switch to a lower bandwidth.
Channel Selection	Select the wireless channel which this radio profile should use. It is recommended that you choose the channel least in use by other APs in the region where this profile will be implemented. This will reduce the amount of interference between wireless clients and the AP to which this profile is assigned. Select DCS to have the AP automatically select the radio channel upon which it broadcasts by scanning the area around it and determining what channels are currently being used by other devices. Note: If you change the country code later, Channel Selection is set to Manual automatically. Select Manual and specify the channels the AP uses.
Output Power	Enter the maximum output power of the Zyxel Device. If there is a high density of APs in an area, decrease the output power of the Zyxel Device to reduce interference with other APs. Reducing the output power also reduces the Zyxel Device's effective broadcast radius.
Enable DCS Client Aware	This field is available when you set Channel Selection to DCS. Select this to have the AP wait until all connected clients have disconnected before switching channels. If you disable this then the AP switches channels immediately regardless of any client connections. In this instance, clients that are connected to the AP when it switches channels are dropped.

Table 69 Wireless > Built-in AP > Radio

LABEL	DESCRIPTION
Avoid 5 GHz DFS Channel	This field is available only when you set 802.11 Band to 5G, Channel Selection to DCS and 5 GHz Channel Selection Method to auto. Dynamic Frequency Selection (DFS) is a channel WiFi allocation scheme that allows APs to use channels in the 5 Ghz band normally reserved for radar. Before using a DFS channel, an AP must ensure there is no radar present by performing a Channel Availability Check (CAC). This check takes 1-10 minutes, depending on the country in which the AP is located. Select this if you don't want to wait for the Zyxel Device to perform a CAC before using a channel by forcing the Zyxel Device to only use the non-DFS channels. Clear this to allow the Zyxel Device to use the DFS channels for more channel options.
5 GHz Channel Selection Method	This field is available when you set Channel Selection to DCS. Select auto to have the AP search for available channels automatically in the 5 GHz band. The available channels vary depending on what you select in the 5 GHz Channel Deployment field. Select manual and specify the channels the AP uses in the 5 GHz band.
Channel ID	This field is available only when you set Channel Selection to DCS and set 5 GHz Channel Selection Method to manual. Select the checkboxes of the channels that you want the AP to use.
Time Interval	Select this option to have the Zyxel Device survey the other APs within its broadcast radius at the end of the specified time interval.
DCS Time Interval	This field is available when you set Channel Selection to DCS. Enter a number of minutes. This regulates how often the AP surveys the other APs within its broadcast radius. If the channel on which it is currently broadcasting suddenly comes into use by another AP, the AP will then dynamically select the next available clean channel or a channel with lower interference.
Schedule	Select this option to have the Zyxel Device survey the other APs within its broadcast radius at a specific time on selected days of the week.
Start Time	Specify the time of the day (in 24-hour format) to have the Zyxel Device use DCS to automatically scan and find a less-used channel.
Week Days	Select each day of the week to have the Zyxel Device use DCS to automatically scan and find a less-used channel.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving your changes.

10.3 Technical Reference

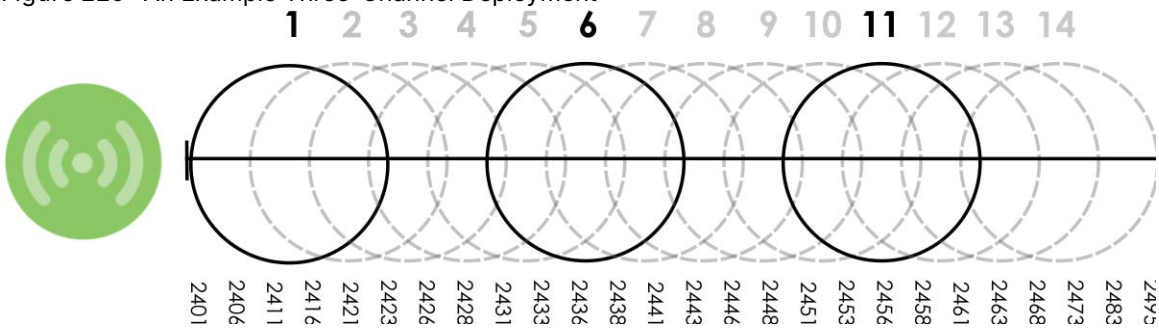
The following section contains additional technical information about wireless features.

10.3.1 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.

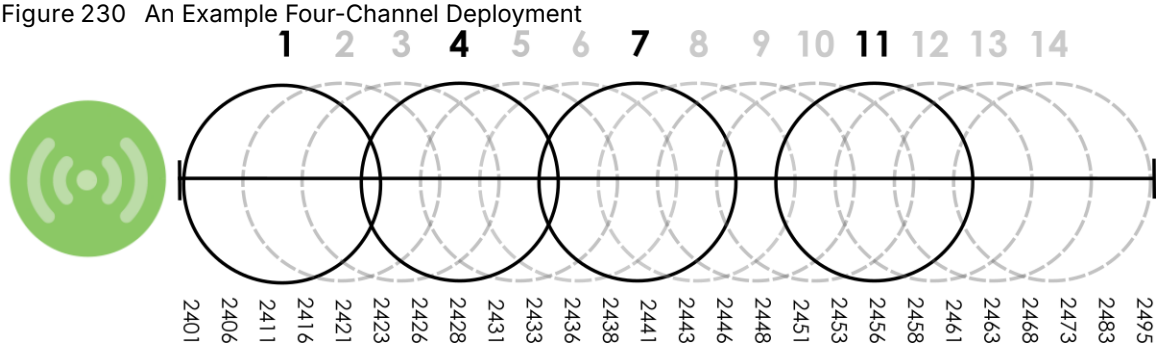
In the 2.4 GHz spectrum, each channel from 1 to 13 is broken up into discrete 22 MHz segments that are spaced 5 MHz apart. Channel 1 is centered on 2.412 GHz while channel 13 is centered on 2.472 GHz.

Figure 229 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.

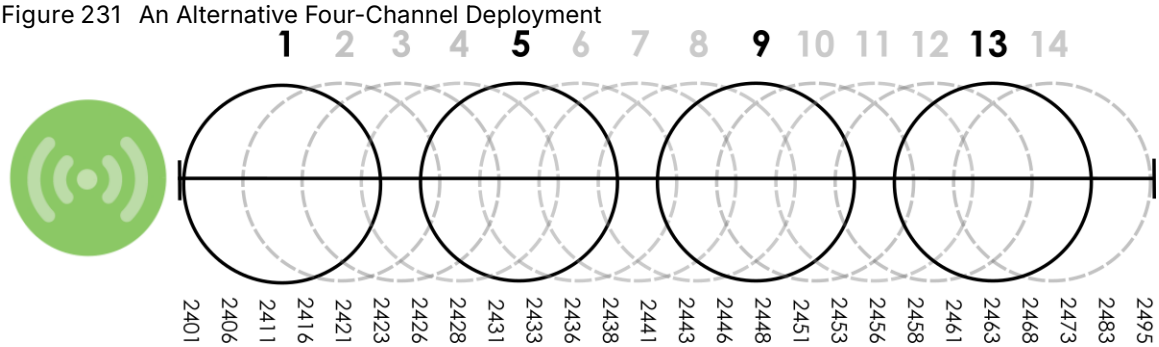
Figure 230 An Example Four-Channel Deployment



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 231 An Alternative Four-Channel Deployment



10.3.2 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 11
Interfaces

11.1 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.

11.1.1 What You Can Do in this Chapter

- Use the Port Role screen (Section 11.2 on page 290) to set the Zyxel Device's physical ports to ZONE interfaces.
- Use the Port Group screen (Section 11.3 on page 291) to create port groups and to assign port groups to Ethernet interfaces.
- Use the Port Configuration screen (Section 11.4 on page 292) to configure Zyxel Device port settings.
- Use the Ethernet screens (Section 11.5 on page 294) 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 11.6 on page 317) for PPPoE, PPTP or L2TP Internet connections.
- Use the Cellular screens (Section 11.7 on page 324) to configure settings for interfaces for Internet connections through an installed mobile broadband card.
- Use the Tunnel screens (Section 11.8 on page 333) to configure tunnel interfaces to be used in Generic Routing Encapsulation (GRE), IPv6 in IPv4, and 6to4 tunnels.
- Use the VLAN screens (Section 11.9 on page 340) 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 11.10 on page 354) to combine two or more network segments into a single network.
- Use the VTI screens (Section 11.11 on page 367) to encrypt or decrypt IPv4 traffic from or to the interface according to the IP routing table.
- Use the Trunk screens (Section 11.12 on page 373) to configure load balancing.

11.1.2 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 through 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 70 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

Table 70 Ethernet, PPP, Cellular, VLAN, Bridge, and Virtual Interface Characteristics (continued)

CHARACTERISTICS	ETHERNET	ETHERNET	PPP	CELLULAR	VLAN	BRIDGE	VIRTUAL
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							
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 71 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 71 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 72 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 on 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.

11.1.3 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.

11.2 Port Role

To access this screen, click Configuration > Network > Interface > Port Role. Use the Port Role screen to set the Zyxel Device’s physical ports to ZONE 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 on the same subnet as the Zyxel Device's interface IP address.
- Use the appropriate interface IP address to access the Zyxel Device.

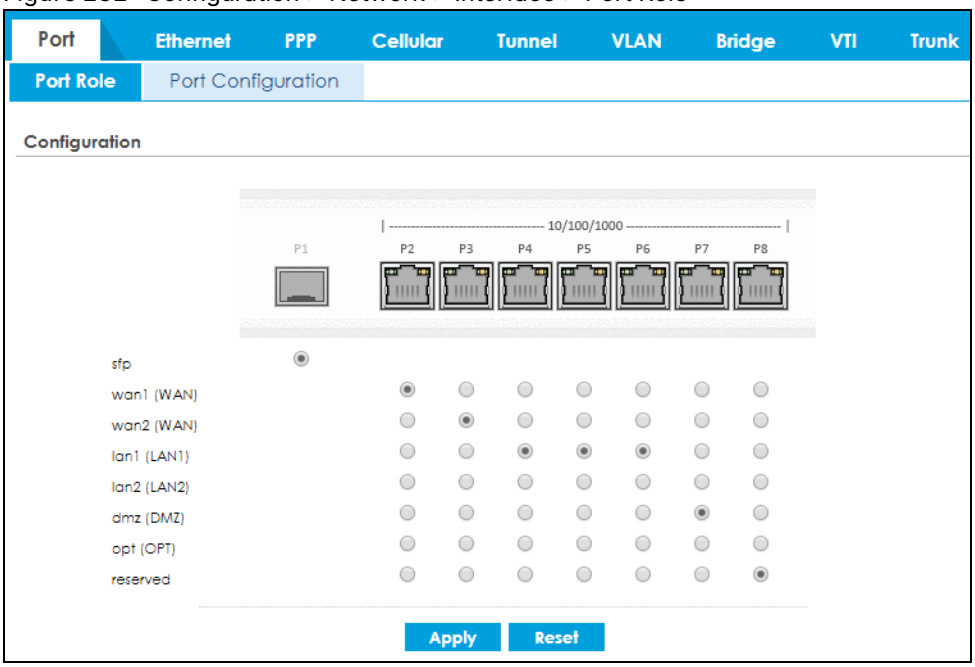
The physical Ethernet ports are shown at the top and the Ethernet interfaces and zones are shown at the bottom of the screen. Use the radio buttons to select for which interface (network) you want to use each physical port. For example, select a port’s LAN radio button to use the port as part of the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

Please note that not all Zyxel Device models support port role, see Section 1.1.1 on page 24 for more information.

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).

Figure 232 Configuration > Network > Interface > Port Role



11.3 Port Group

To access this screen, click Configuration > Network > Interface > Port Group. When you assign more than one physical port to a network, you create a port group. Use the Port Group screen to create port groups and to assign port groups to Ethernet interfaces. Port groups have the following characteristics:

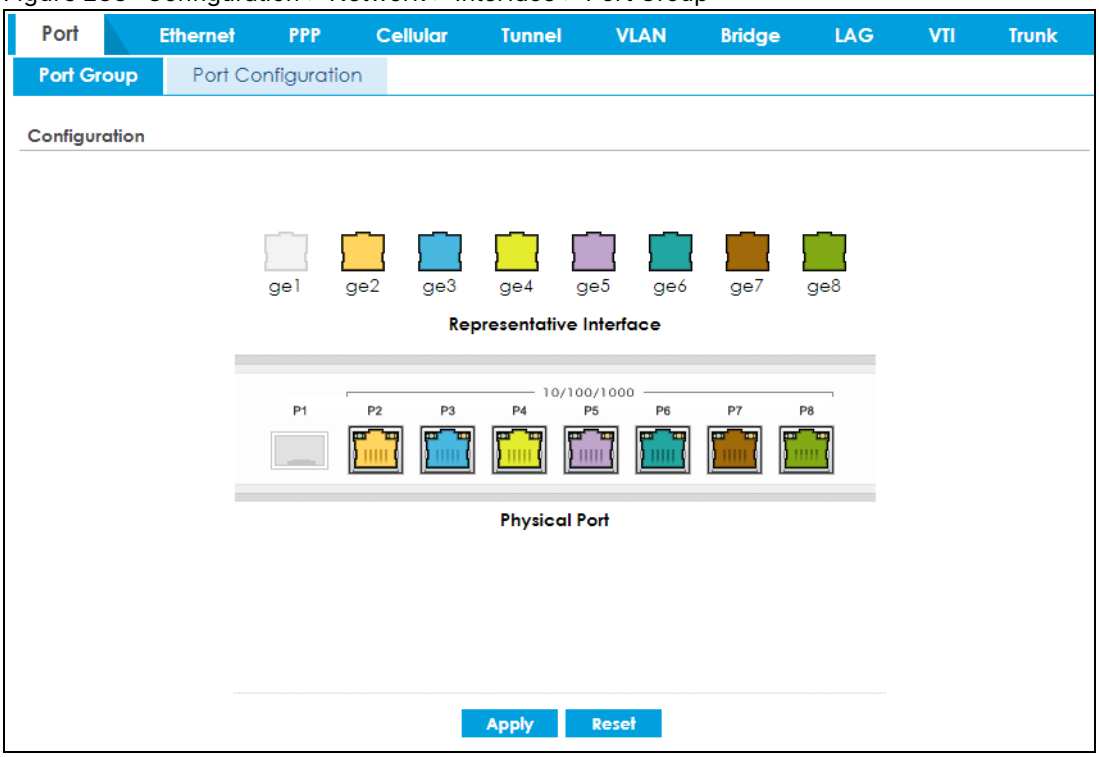
- There is a layer-2 Ethernet switch between physical ports in the port group. This provides wire-speed throughput but no security.
- It can increase the bandwidth between the port group and other interfaces.
- The port group uses a single MAC address.

Please note that not all Zyxel Device models support port role, see Section 1.1.1 on page 24 for more information.

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).

Figure 233 Configuration > Network > Interface > Port Group

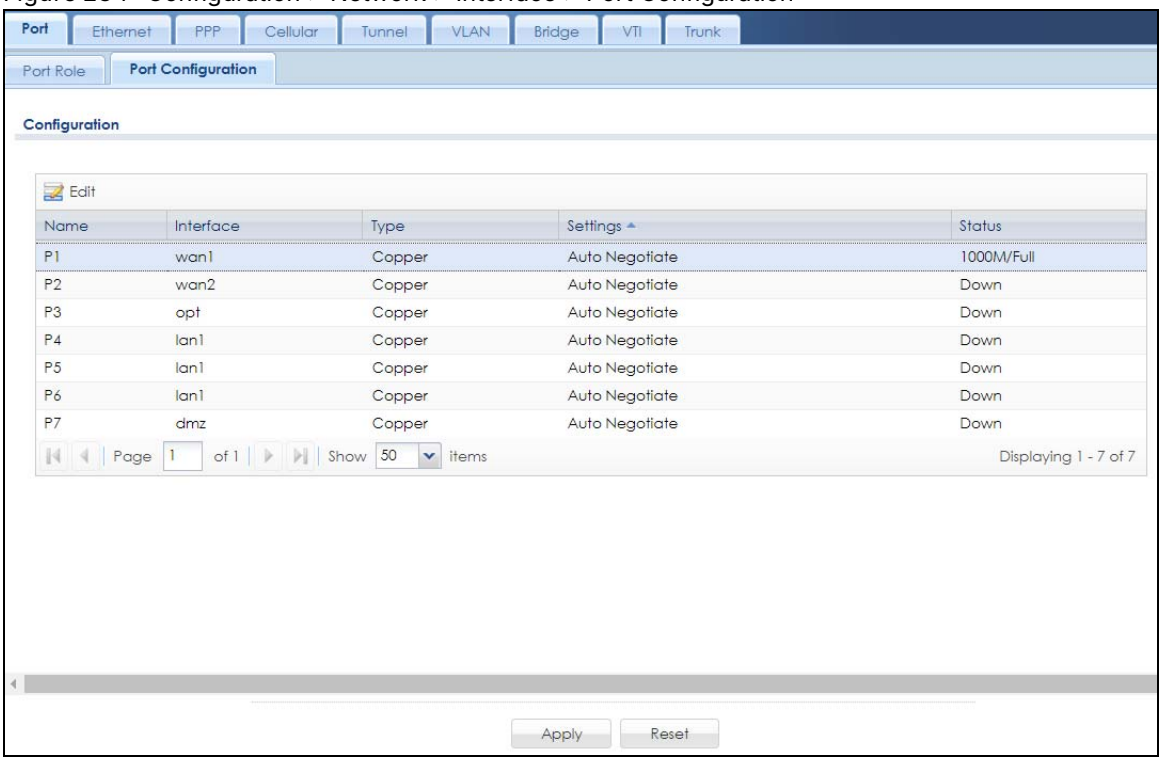


11.4 Port Configuration

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

Note: You cannot configure the speed and duplex mode of fiber ports.

Figure 234 Configuration > Network > Interface > Port Configuration



Each field is described in the following table.

Table 73 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.

11.5 Ethernet Summary Screen

This screen lists every Ethernet interface and virtual interface created on top of Ethernet interfaces. If you enabled IPv6 on 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.

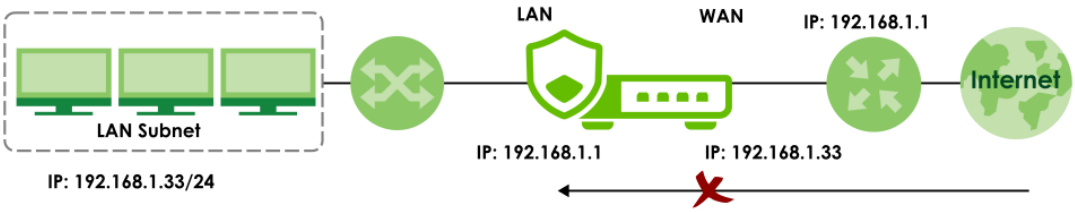
Unlike other types of interfaces, you cannot create new Ethernet interfaces nor can you delete any of them. If an Ethernet interface does not have any physical ports assigned to it, the Ethernet interface is effectively removed from the Zyxel Device, but you can still configure it.

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 12 on page 398 for background information about these routing protocols.

The default IPv4 LAN subnet range starts from 192.168.1.0/24. If the Zyxel Device WAN IPv4 address conflicts with the LAN IPv4 address, clients on the LAN will not be able to access the Internet.

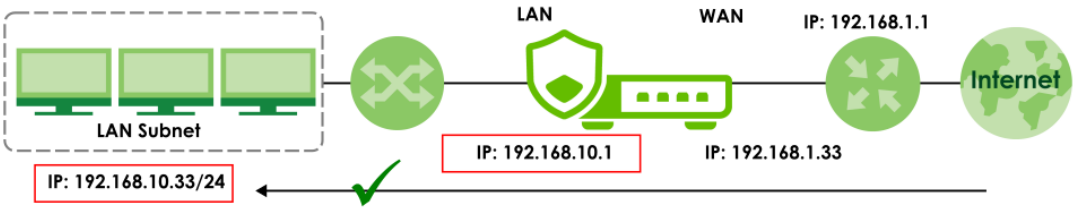
Figure 235 IP Address Conflict



The following list shows some examples of what the IPv4 LAN subnet range will change to if it conflicts with the WAN IPv4 address.

- 192.168.1.0/24 will change to 192.168.10.0/24.
- 192.168.2.0/24 will change to 192.168.11.0/24.
- 192.168.3.0/24 will change to 192.168.12.0/24.
- 192.168.4.0/24 will change to 192.168.13.0/24.

Figure 236 IP Address Change



If you upgrade the Zyxel Device firmware version from 4.29 to 5.31, and your Ethernet settings in the Zyxel Device firmware version 4.29 meets the conditions listed below, the default LAN subnet will change when

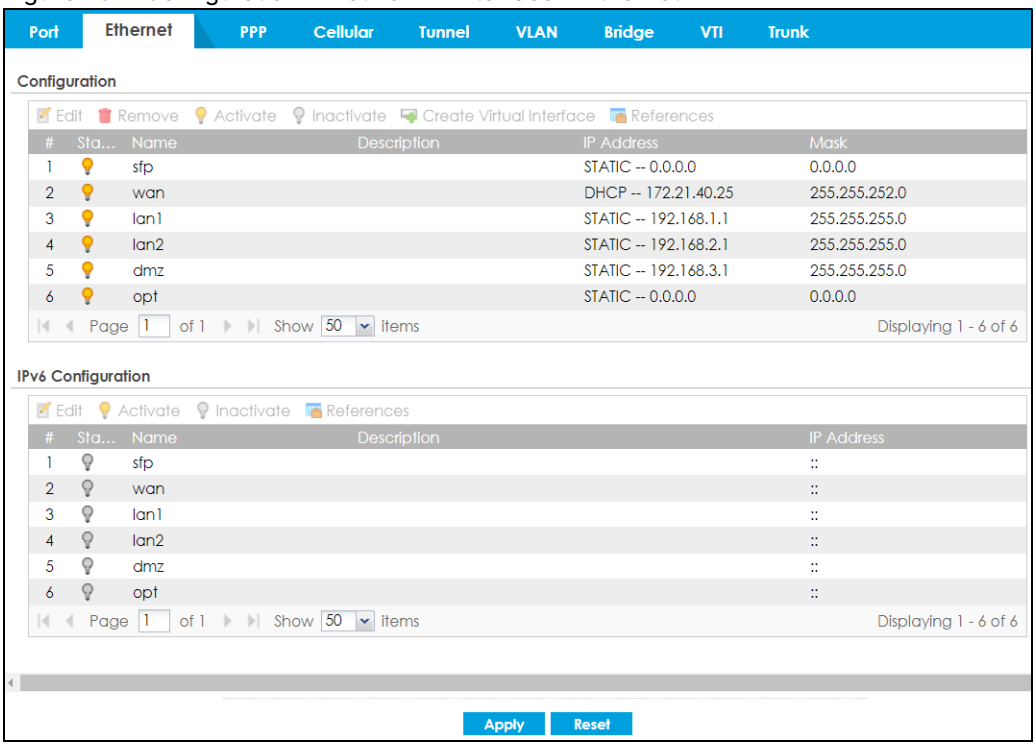
the IPv4 address the WAN interface gets from the DHCP server conflicts with any IPv4 address in the default LAN subnet:

- The WAN is using a static IPv4 address.
- The WAN is using a dynamically assigned IPv4 address.
- The WAN is using an IPv4 address assigned by the PPPoE server.

If the Zyxel Device is using firmware version 5.31, when the WAN IPv4 address conflicts with any IPv4 address in the default LAN subnet, the Zyxel Device will only change the default LAN subnet if it is in default settings.

When you configure the WAN or the LAN IPv4 networks, please note that they must not conflict with each other. The Zyxel Device will not automatically change the LAN IPv4 subnet if the WAN IPv4 address conflicts with the LAN IPv4 networks you configure.

Figure 237 Configuration > Network > Interface > Ethernet



Each field is described in the following table.

Table 74 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.

Table 74 Configuration > Network > Interface > Ethernet (continued)

LABEL	DESCRIPTION
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 11.5.4 on page 314 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.
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0 (on the IPv4 network) or :: (on the IPv6 network), the interface does not have an IP address yet. On 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. On 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 11.1.2 on page 286 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.

11.5.1 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 on the Ethernet Summary screen. (See Section 11.5 on page 294.)

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.

11.5.1.1 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 238 IGMP Proxy

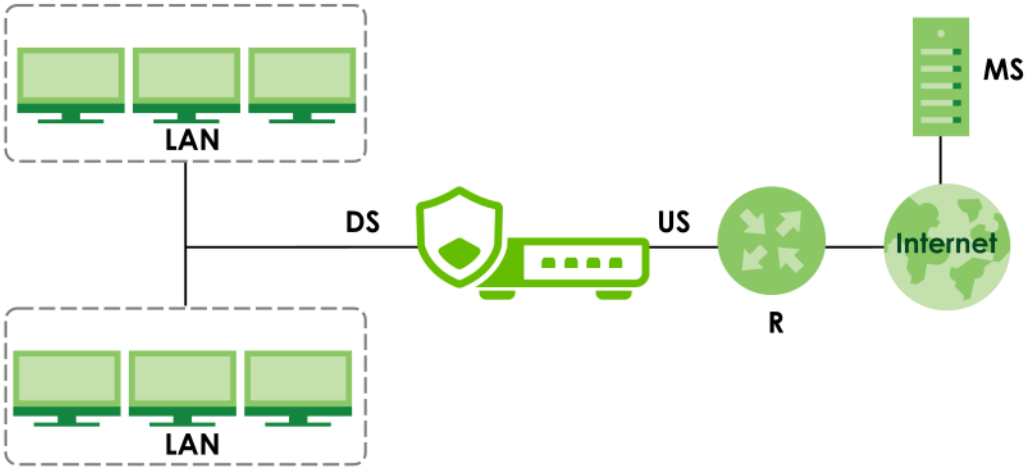
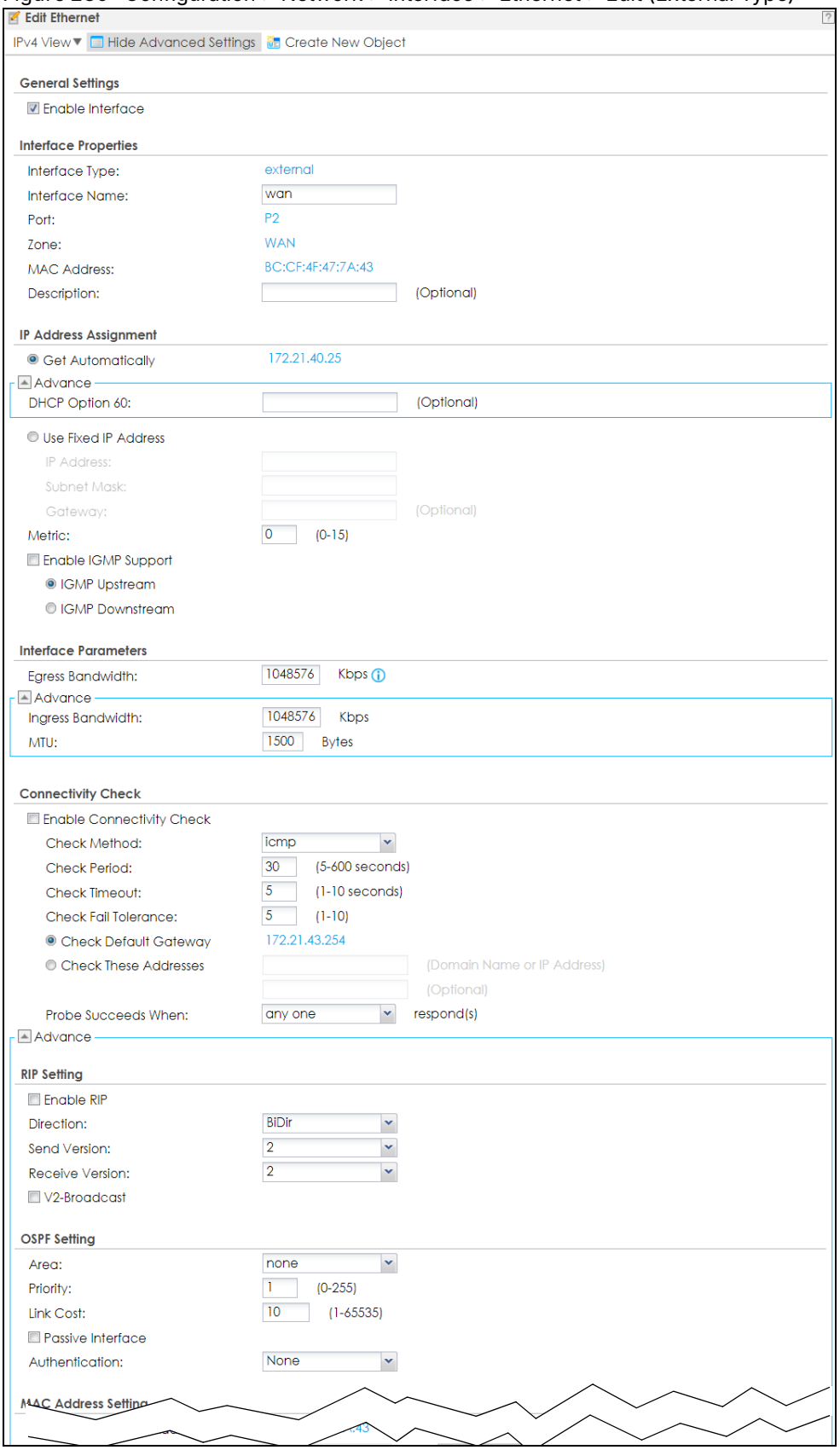
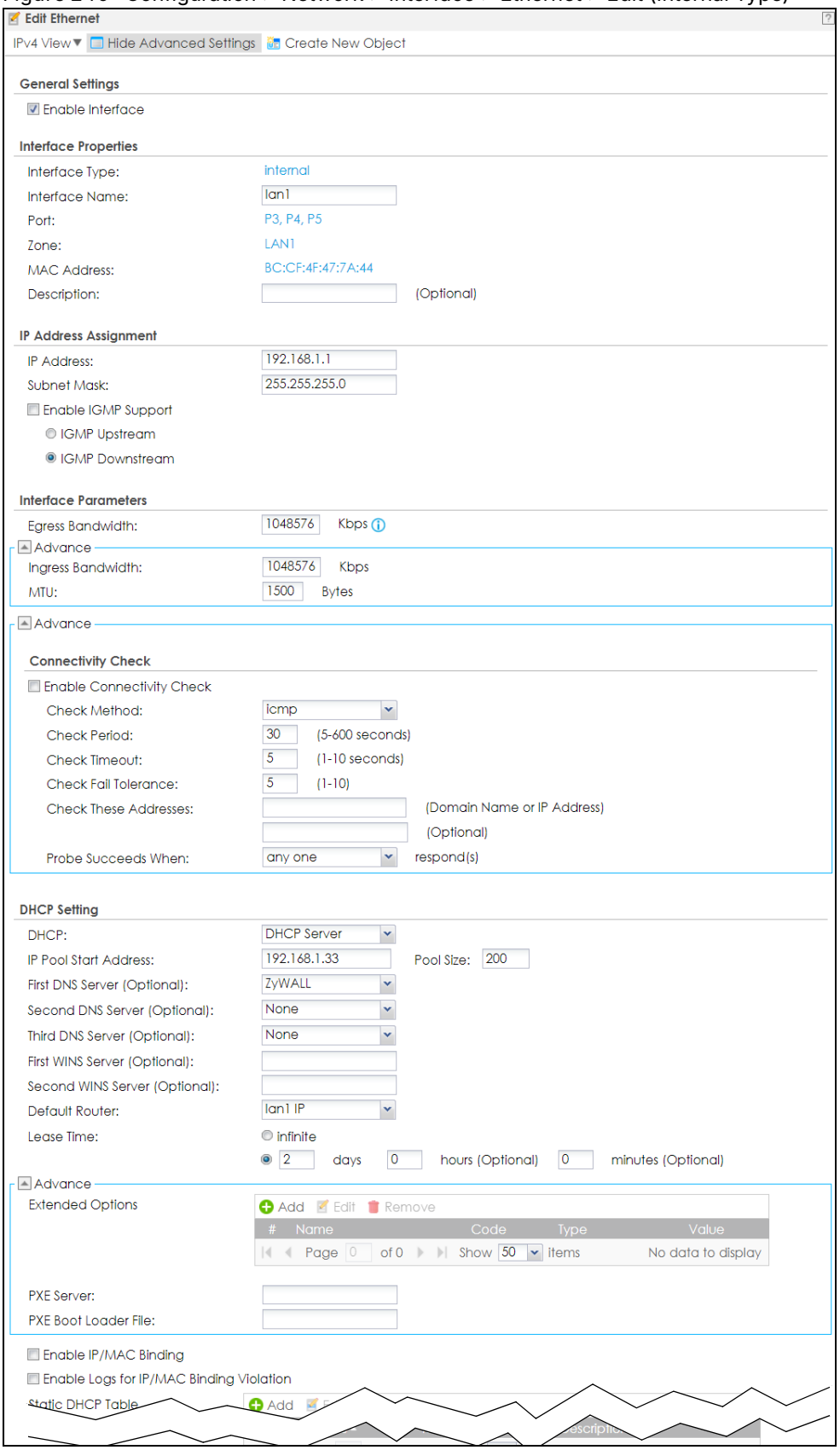


Figure 239 Configuration > Network > Interface > Ethernet > Edit (External Type)



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 240 Configuration > Network > Interface > Ethernet > Edit (Internal Type)



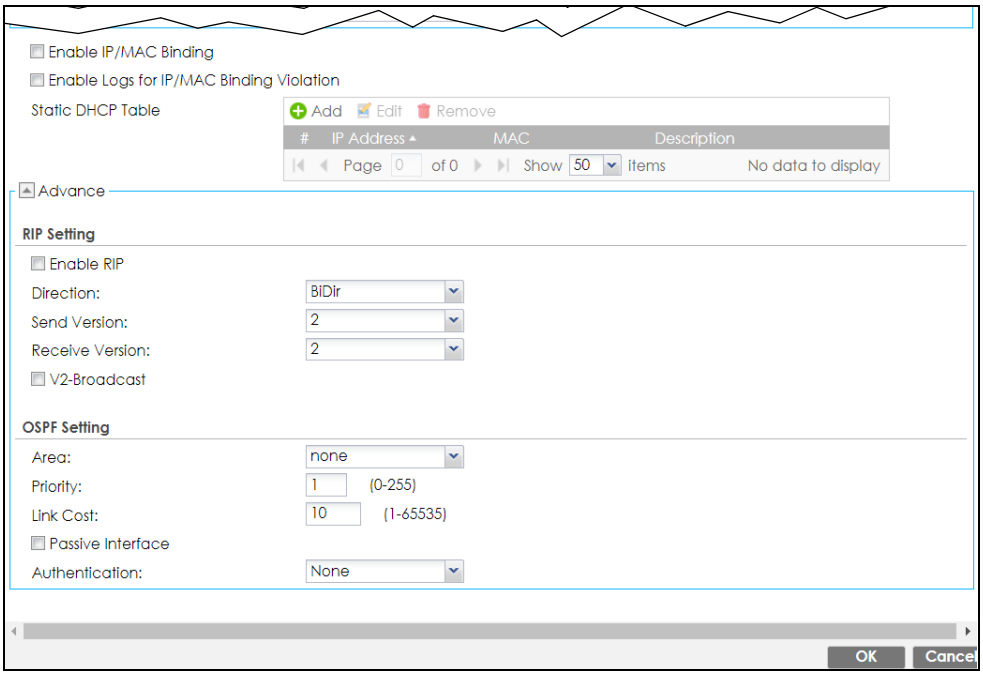
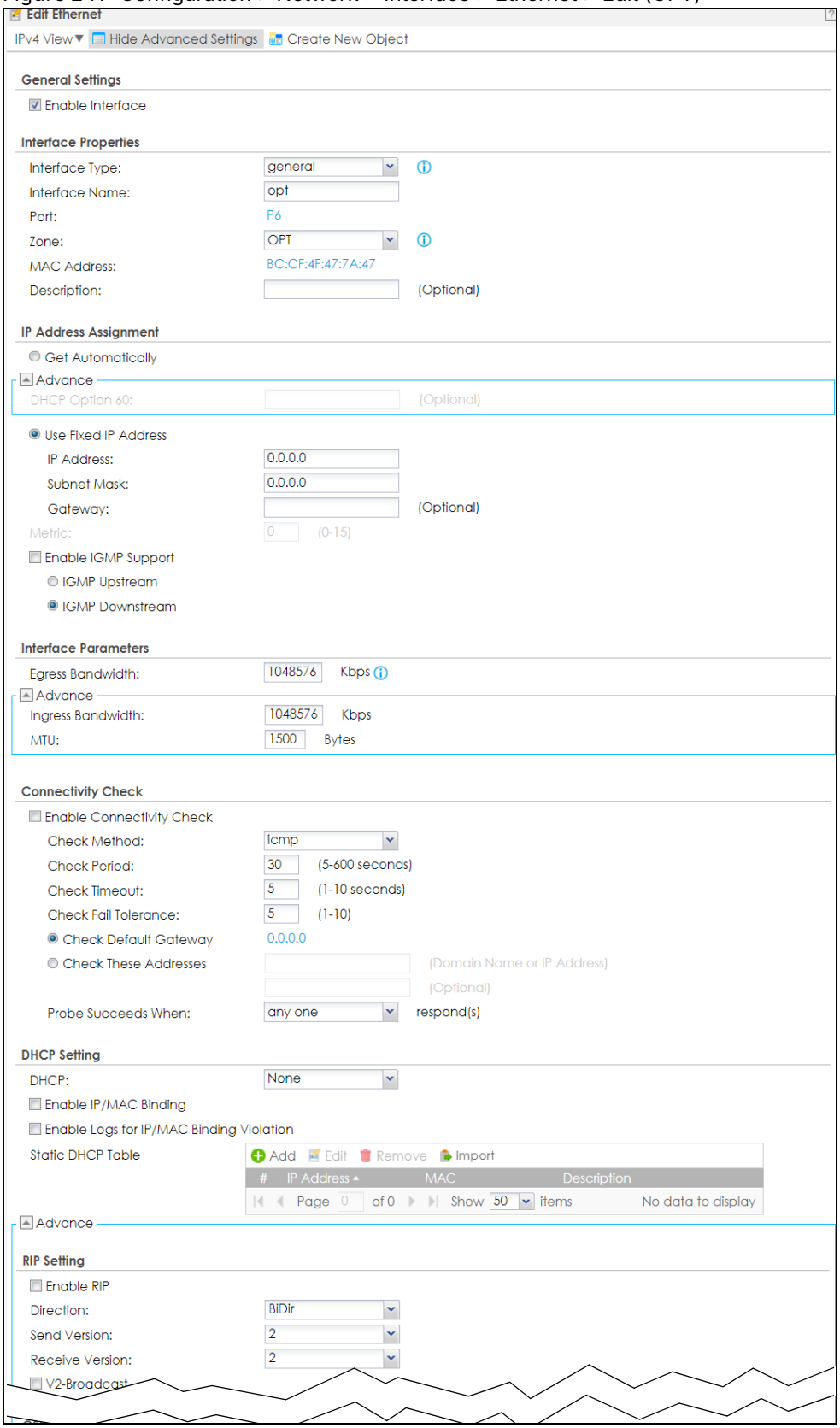
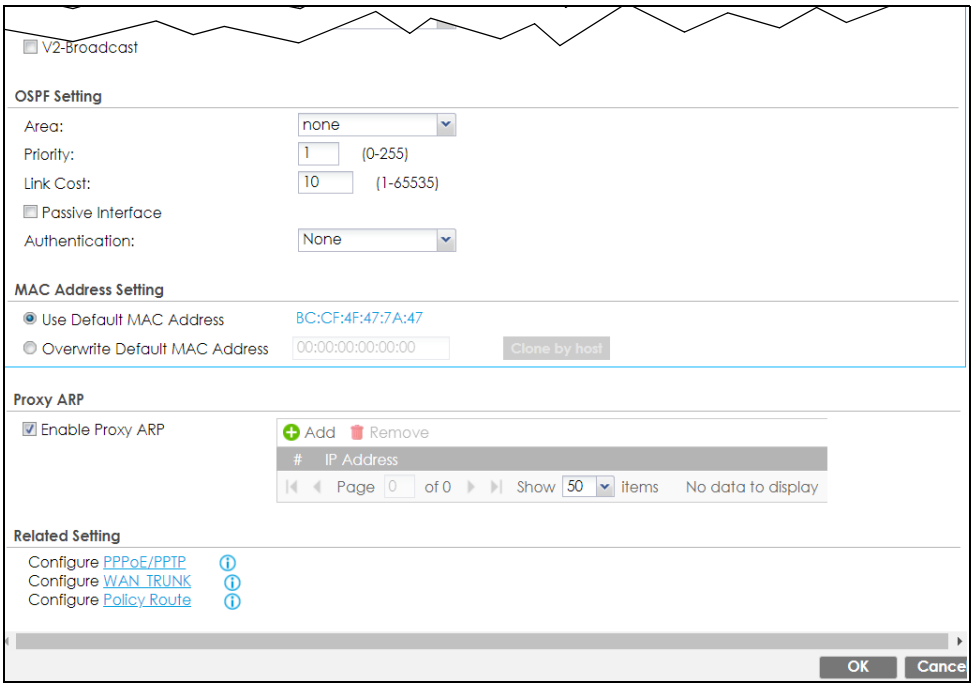

Enable IP/MAC Binding
Enable Logs for IP/MAC Binding Violation
Static DHCP Table
Add
Edit
Remove
IP Address MAC Description
Page 0 of 0 Show 50 items No data to display
Advance
RIP Setting
Enable RIP
Direction: BiDir
Send Version: 2
Receive Version: 2
V2-Broadcast
OSPF Setting
Area: none
Priority: 1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

Figure 241 Configuration > Network > Interface > Ethernet > Edit (OPT)





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

Table 75 Configuration > Network > Interface > Ethernet > Edit

LABEL	DESCRIPTION
IPv4/IPv6 View / IPv4 View / IPv6 View	Use this button to display both IPv4 and IPv6, IPv4-only, or IPv6-only configuration fields.
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create New Object	Click this button to create a DHCPv6 lease or DHCPv6 request object that you may use for the DHCPv6 settings in this screen.
General Settings	
Enable Interface	Select this to enable this interface. Clear this to disable this interface.
General IPv6 Setting	
Enable IPv6	Select this to enable IPv6 on this interface. Otherwise, clear this to disable it.
Interface Properties	
Interface Type	This field is configurable for the OPT interface only. Select to which type of network you will connect this interface. When you select internal or external the rest of the screen's options automatically adjust to correspond. The Zyxel Device automatically adds default route and SNAT settings for traffic it routes from internal interfaces to external interfaces; for example LAN to WAN traffic. internal is for connecting to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The Zyxel Device automatically adds default SNAT settings for traffic flowing from this interface to an external interface. external is for connecting to an external network (like the Internet). The Zyxel Device automatically adds this interface to the default WAN trunk. For general, the rest of the screen's options do not automatically adjust and you must manually configure a policy route to add routing and SNAT settings for the interface.
Interface Name	Specify a name for the interface. It can use alphanumeric characters, hyphens, and underscores, and it can be up to 11 characters long.

Table 75 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Port	This is the name of the Ethernet interface's physical port.
MAC Address	This field is read-only. This is the MAC address that the Ethernet interface uses.
Description	Enter a description of this interface. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long. Spaces are allowed, but the string can't start with a space.
IP Address Assignment	These IP address fields configure an IPv4 IP address on the interface itself. If you change this IP address on the interface, you may also need to change a related address object for the network connected to the interface. For example, if you use this screen to change the IP address of your LAN interface, you should also change the corresponding LAN subnet address object.
Get Automatically	This option appears when Interface Type is external or general. Select this to make the interface a DHCP client and automatically get the IP address, subnet mask, and gateway address from a DHCP server.
DHCP Option 60	DHCP Option 60 is used by the Zyxel Device for identification to the DHCP server using the VCI (Vendor Class Identifier) on the DHCP server. The Zyxel Device adds it in the initial DHCP discovery message that a DHCP client broadcasts in search of an IP address. The DHCP server can assign different IP addresses or options to clients with the specific VCI or reject the request from clients without the specific VCI. Enter a string using up to 63 of these characters [a-zA-Z0-9!\"#$%&\'()*+,-./:;<=>?@\[\\\]^_`{}] to identify this Zyxel Device to the DHCP server. For example, Zyxel-TW.
Use Fixed IP Address	This option appears when Interface Type is external or general. Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers on the network.
Gateway	This option appears when Interface Type is external or general. Enter the IP address of the gateway. The Zyxel Device sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	This option appears when Interface Type is external or general. Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
Enable IGMP Support	Select this to allow the Zyxel Device to act as an IGMP proxy for hosts connected on the IGMP downstream interface.
IGMP Upstream	Enable IGMP Upstream on the interface which connects to a router running IGMP that is closer to the multicast server.
IGMP Downstream	Enable IGMP Downstream on the interface which connects to the multicast hosts.
IPv6 Address Assignment	These IP address fields configure an IPv6 IP address on the interface itself.
Enable Stateless Address Auto-configuration (SLAAC)	Select this to enable IPv6 stateless auto-configuration on this interface. The interface will generate an IPv6 IP address itself from a prefix obtained from an IPv6 router on the network.
Link-Local Address	This displays the IPv6 link-local address and the network prefix that the Zyxel Device generates itself for the interface.
IPv6 Address/ Prefix Length	Enter the IPv6 address and the prefix length for this interface if you want to use a static IP address. This field is optional. The prefix length indicates what the left-most part of the IP address is the same for all computers on the network, that is, the network address.
Gateway	Enter the IPv6 address of the default outgoing gateway using colon (:) hexadecimal notation.

Table 75 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Metric	Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
Address from DHCPv6 Prefix Delegation	Use this table to have the Zyxel Device obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ. You have to also enter a suffix address which is appended to the delegated prefix to form an address for this interface. See Prefix Delegation on page 289 for more information. To use prefix delegation, you must: • Create at least one DHCPv6 request object before configuring this table. • The external interface must be a DHCPv6 client. You must configure the DHCPv6 request options using a DHCPv6 request object with the type of prefix-delegation. • Assign the prefix delegation to an internal interface and enable router advertisement on that interface.
Add	Click this to create an entry.
Edit	Select an entry and click this to change the settings.
Remove	Select an entry and click this to delete it from this table.
References	Select an entry and click References to check which settings use the entry.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use from the drop-down list.
Suffix Address	Enter the ending part of the IPv6 address, a slash (/), and the prefix length. The Zyxel Device will append it to the delegated prefix. For example, you got a delegated prefix of 2003:1234:5678/48. You want to configure an IP address of 2003:1234:5678:1111::1/128 for this interface, then enter ::1111:0:0:0:1/128 in this field.
Address	This field displays the combined IPv6 IP address for this interface. Note: This field displays the combined address after you click OK and reopen this screen.
DHCPv6 Setting	
DHCPv6	Select N/A to not use DHCPv6. Select Client to set this interface to act as a DHCPv6 client. Select Server to set this interface to act as a DHCPv6 server which assigns IP addresses and provides subnet mask, gateway, and DNS server information to clients. Select Relay to set this interface to route DHCPv6 requests to the DHCPv6 relay server you specify. The DHCPv6 server(s) may be on another network.
DUID	This field displays the DHCP Unique IDentifier (DUID) of the interface, which is unique and used for identification purposes when the interface is exchanging DHCPv6 messages with others. See DHCPv6 on page 289 for more information.
DUID as MAC	Select this if you want the DUID is generated from the interface's default MAC address.
Customized DUID	If you want to use a customized DUID, enter it here for the interface.
Enable Rapid Commit	Select this to shorten the DHCPv6 message exchange process from four to two steps. This function helps reduce heavy network traffic load. Note: Make sure you also enable this option in the DHCPv6 clients to make rapid commit work.
Information Refresh Time	Enter the number of seconds a DHCPv6 client should wait before refreshing information retrieved from DHCPv6.

Table 75 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Request Address	This field is available if you set this interface to DHCPv6 Client. Select this to get an IPv6 IP address for this interface from the DHCP server. Clear this to not get any IP address information through DHCPv6.
DHCPv6 Request Options / DHCPv6 Lease Options	If this interface is a DHCPv6 client, use this section to configure DHCPv6 request settings that determine what additional information to get from the DHCPv6 server. If the interface is a DHCPv6 server, use this section to configure DHCPv6 lease settings that determine what additional information to offer to the DHCPv6 clients.
Add	Click this to create an entry in this table. See Section 11.5.5 on page 315 for more information.
Remove	Select an entry and click this to delete it from this table.
References	Select an entry and click References to open a screen that shows which settings use the entry. See Section 11.5.4 on page 314 for an example.
#	This field is a sequential value, and it is not associated with any entry.
Name	This field displays the name of the DHCPv6 request or lease object.
Type	This field displays the type of the object.
Value	This field displays the IPv6 prefix that the Zyxel Device obtained from an uplink router (Server is selected) or will advertise to its clients (Client is selected).
Interface	When Relay is selected, select this checkbox and an interface from the drop-down list if you want to use it as the relay server.
Relay Server	When Relay is selected, select this checkbox and enter the IP address of a DHCPv6 server as the relay server.
IPv6 Router Advertisement Setting	
Enable Router Advertisement	Select this to enable this interface to send router advertisement messages periodically. See IPv6 Router Advertisement on page 289 for more information.
Advertised Hosts Get Network Configuration From DHCPv6	Select this to have the Zyxel Device indicate to hosts to obtain network settings (such as prefix and DNS settings) through DHCPv6. Clear this to have the Zyxel Device indicate to hosts that DHCPv6 is not available and they should use the prefix in the router advertisement message.
Advertised Hosts Get Other Configuration From DHCPv6	Select this to have the Zyxel Device indicate to hosts to obtain DNS information through DHCPv6. Clear this to have the Zyxel Device indicate to hosts that DNS information is not available in this network.
Router Preference	Select the router preference (Low, Medium or High) for the interface. The interface sends this preference in the router advertisements to tell hosts what preference they should use for the Zyxel Device. This helps hosts to choose their default router especially when there are multiple IPv6 router on the network. Note: Make sure the hosts also support router preference to make this function work.
MTU	The Maximum Transmission Unit. Enter the maximum size of each IPv6 data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device discards the packet and sends an error message to the sender to inform this.
Hop Limit	Enter the maximum number of network segments that a packet can cross before reaching the destination. When forwarding an IPv6 packet, IPv6 routers are required to decrease the Hop Limit by 1 and to discard the IPv6 packet when the Hop Limit is 0.
Advertised Prefix Table	Configure this table only if you want the Zyxel Device to advertise a fixed prefix to the network.
Add	Click this to create an IPv6 prefix address.

Table 75 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
IPv6 Address/ Prefix Length	Enter the IPv6 network prefix address and the prefix length. The prefix length indicates what the left-most part of the IP address is the same for all computers on the network, that is, the network address.
Advertised Prefix from DHCPv6 Prefix Delegation	This table is available when the Interface Type is internal. Use this table to configure the network prefix if you want to use a delegated prefix as the beginning part of the network prefix.
Add	Click this to create an entry in this table.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use for generating the network prefix for the network.
Suffix Address	Enter the ending part of the IPv6 network address plus a slash (/) and the prefix length. The Zyxel Device will append it to the selected delegated prefix. The combined address is the network prefix for the network. For example, you got a delegated prefix of 2003:1234:5678/48. You want to divide it into 2003:1234:5678:1111/64 for this interface and 2003:1234:5678:2222/64 for another interface. You can use ::1111/64 and ::2222/64 for the suffix address respectively. But if you do not want to divide the delegated prefix into subnetworks, enter ::0/48 here, which keeps the same prefix length (/48) as the delegated prefix.
Address	This is the final network prefix combined by the delegated prefix and the suffix. Note: This field displays the combined address after you click OK and reopen this screen.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Enter the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
Connectivity Check	These fields appear when Interface Properties is External or General. The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the Zyxel Device stops routing to the gateway. The Zyxel Device resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.

Table 75 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Check Method	Select the method that the gateway allows. Select icmp to have the Zyxel Device regularly ping the gateway you specify to make sure it is still available. Select tcp to have the Zyxel Device regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the Zyxel Device stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address on the field next to it.
Check Port	This field only displays when you set the Check Method to tcp. Specify the port number to use for a TCP connectivity check.
Check these addresses	Enter one or two domain names or IP addresses for the connectivity check.
Probe Succeeds When	This field applies when you specify two domain names or IP addresses for the connectivity check. Select any one if you want the check to pass if at least one of the domain names or IP addresses responds. Select all if you want the check to pass only if both domain names or IP addresses respond.
DHCP Setting	This section appears when Interface Type is internal or general.
DHCP	Select what type of DHCP service the Zyxel Device provides to the network. Choices are: None - the Zyxel Device does not provide any DHCP services. There is already a DHCP server on the network. DHCP Relay - the Zyxel Device routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. DHCP Server - the Zyxel Device assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The Zyxel Device is the DHCP server for the network.
	These fields appear if the Zyxel Device is a DHCP Relay.
Relay Server 1	Enter the IP address of a DHCP server for the network.
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.
	These fields appear if the Zyxel Device is a DHCP Server.
IP Pool Start Address	Enter the IP address from which the Zyxel Device begins allocating IP addresses. If you want to assign a static IP address to a specific computer, use the Static DHCP Table. If this field is blank, the Pool Size must also be blank. In this case, the Zyxel Device can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.

Table 75 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's Subnet Mask. For example, if the Subnet Mask is 255.255.255.0 and IP Pool Start Address is 10.10.10.10, the Zyxel Device can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses. If this field is blank, the IP Pool Start Address must also be blank. In this case, the Zyxel Device can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
First DNS Server, Second DNS Server, Third DNS Server	Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. Custom Defined - enter a static IP address. From ISP - select the DNS server that another interface received from its DHCP server. Zyxel Device - the DHCP clients use the IP address of this interface and the Zyxel Device works as a DNS relay.
First WINS Server, Second WINS Server	Enter the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Default Router	If you set this interface to DHCP Server, you can select to use either the interface's IP address or another IP address as the default router. This default router will become the DHCP clients' default gateway. To use another IP address as the default router, select Custom Defined and enter the IP address.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: infinite - select this if IP addresses never expire. days, hours, and minutes - select this to enter how long IP addresses are valid.
Extended Options	This table is available if you selected DHCP server. Configure this table if you want to send more information to DHCP clients through DHCP packets.
Add	Click this to create an entry in this table. See Section 11.5.6 on page 316.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
Name	This is the name of the DHCP option.
Code	This is the code number of the DHCP option.
Type	This is the type of the set value for the DHCP option.
Value	This is the value set for the DHCP option.
PXE Server	PXE (Preboot eXecution Environment) allows a client computer to use the network to boot up and install an operating system through a PXE-capable Network Interface Card (NIC). PXE is available for computers on internal interfaces to allow them to boot up using boot software on a PXE server. The Zyxel Device acts as an intermediary between the PXE server and the computers that need boot software. The PXE server must have a public IPv4 address. You must enable DHCP Server on the Zyxel Device so that it can receive information from the PXE server.
PXE Boot Loader File	A boot loader is a computer program that loads the operating system for the computer. Enter the exact file name of the boot loader software file, including filename extension, that is on the PXE server. If the wrong filename is entered, then the client computers cannot boot.

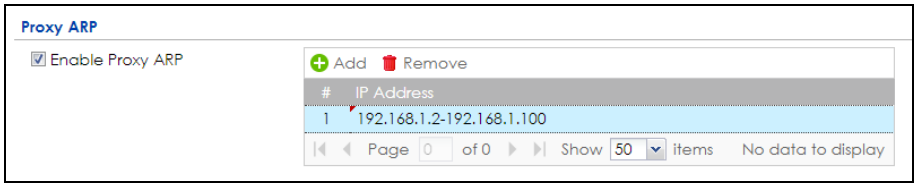
Table 75 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Enable IP/MAC Binding	Select this option to have this interface enforce links between specific IP addresses and specific MAC addresses. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.
Enable Logs for IP/MAC Binding Violation	Select this option to have the Zyxel Device generate a log if a device connected to this interface attempts to use an IP address that is bound to another device's MAC address.
Static DHCP Table	Configure a list of static IP addresses the Zyxel Device assigns to computers connected to the interface. Otherwise, the Zyxel Device assigns an IP address dynamically using the interface's IP Pool Start Address and Pool Size.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Import	Click this to import a previously saved file (.csv) to the Zyxel Device. The IP/MAC binding settings and description to identify these settings in the file will be applied to the Zyxel Device. The previously saved csv file may be a file you configured, or a file you exported at Monitor> System Status> DHCP Table if you want to recover settings configured before. Configure your csv file in the order of IP address, MAC address and description. Spaces are allowed. Separate each item with a comma, for example, 1.1.1.1,22:22:33:44:55:02,test. Press enter to configure the next group in a new line. Your currently configured IP/MAC binding settings and entries description will be overwritten once you import the file. Make sure to click Export to export your settings as a file for backup in Monitor > System Status > DHCP Table first.
File Path	Enter the file path and name of the DHCP settings file you want to import in the text box (or click Browse to find it on your computer) and then click Upload to transfer the file to the Zyxel Device.
#	This field is a sequential value, and it is not associated with a specific entry.
IP Address	Enter the IP address to assign to a device with this entry's MAC address.
MAC	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
RIP Setting	See Section 12.6 on page 399 for more information about RIP.
Enable RIP	Select this to enable RIP in this interface.
Direction	This field is effective when RIP is enabled. Select the RIP direction from the drop-down list box. BiDir - This interface sends and receives routing information. In-Only - This interface receives routing information. Out-Only - This interface sends routing information.
Send Version	This field is effective when RIP is enabled. Select the RIP version(s) used for sending RIP packets. Choices are 1, 2, and 1 and 2.
Receive Version	This field is effective when RIP is enabled. Select the RIP version(s) used for receiving RIP packets. Choices are 1, 2, and 1 and 2.
V2-Broadcast	This field is effective when RIP is enabled. Select this to send RIP-2 packets using subnet broadcasting; otherwise, the Zyxel Device uses multicasting.
OSPF Setting	See Section 12.7 on page 401 for more information about OSPF.
Area	Select the area in which this interface belongs. Select None to disable OSPF in this interface.

Table 75 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Priority	Enter the priority (between 0 and 255) of this interface when the area is looking for a Designated Router (DR) or Backup Designated Router (BDR). The highest-priority interface identifies the DR, and the second-highest-priority interface identifies the BDR. Set the priority to zero if the interface can not be the DR or BDR.
Link Cost	Enter the cost (between 1 and 65,535) to route packets through this interface.
Passive Interface	Select this to stop forwarding OSPF routing information from the selected interface. As a result, this interface only receives routing information.
Authentication	Select an authentication method, or disable authentication. To exchange OSPF routing information with peer border routers, you must use the same authentication method that they use. Choices are: Same-as-Area - use the default authentication method in the area None - disable authentication Text - authenticate OSPF routing information using a plain-text password MD5 - authenticate OSPF routing information using MD5 encryption
Text Authentication Key	This field is available if the Authentication is Text. Enter the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MD5 Authentication ID	This field is available if the Authentication is MD5. Enter the ID for MD5 authentication. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the Authentication is MD5. Enter the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MAC Address Setting	This section appears when Interface Properties is External or General. Have the interface use either the factory assigned default MAC address, a manually specified MAC address, or clone the MAC address of another device or computer.
Use Default MAC Address	Select this option to have the interface use the factory assigned default MAC address. By default, the Zyxel Device uses the factory assigned MAC address to identify itself.
Overwrite Default MAC Address	Select this option to have the interface use a different MAC address. Either enter the MAC address in the fields or click Clone by host and enter the IP address of the device or computer whose MAC you are cloning. Once it is successfully configured, the address will be copied to the configuration file. It will not change unless you change the setting or upload a different configuration file.
Proxy ARP	Proxy ARP is available for external or general interfaces on the Zyxel Device. See Section 11.5.2 on page 312 for more information on Proxy ARP.
Enable Proxy ARP	Select this to allow the Zyxel Device to answer external interface ARP requests on behalf of a device on its internal interface. Interfaces supported are: • Ethernet • VLAN • Bridge See Section 11.5.2 on page 312 for more information.

Table 75 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Add	Click Add to create an IPv4 Address, an IPv4 CIDR (for example, 192.168.1.1/24) or an IPv4 Range (for example, 192.168.1.2-192.168.1.100) as the target IP address. The Zyxel Device answers external ARP requests only if they match one of these inputted target IP addresses. For example, if the IPv4 Address is 192.168.1.5, then the Zyxel Device will answer ARP requests coming from the WAN only if it contains 192.168.1.5 as the target IP address. Select an existing entry and click Remove to delete that entry. 
Related Setting	
Configure PPPoE/PPTP	Click PPPoE/PPTP if this interface's Internet connection uses PPPoE or PPTP or L2TP.
Configure VLAN	Click VLAN if you want to configure a VLAN interface for this Ethernet interface.
Configure WAN TRUNK	Click WAN TRUNK to go to a screen where you can set this interface to be part of a WAN trunk for load balancing.
Configure Policy Route	Click Policy Route to go to the policy route summary screen where you can manually associate traffic with this interface. You must manually configure a policy route to add routing and SNAT settings for an interface with the Interface Type set to general. You can also configure a policy route to override the default routing and SNAT behavior for an interface with an Interface Type of internal or external.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

11.5.2 Proxy ARP

An Address Resolution Protocol (ARP) is a protocol for mapping an IP address to a MAC address. An ARP broadcast is sent to all devices on the same Ethernet network to request the MAC address of a target IP address.

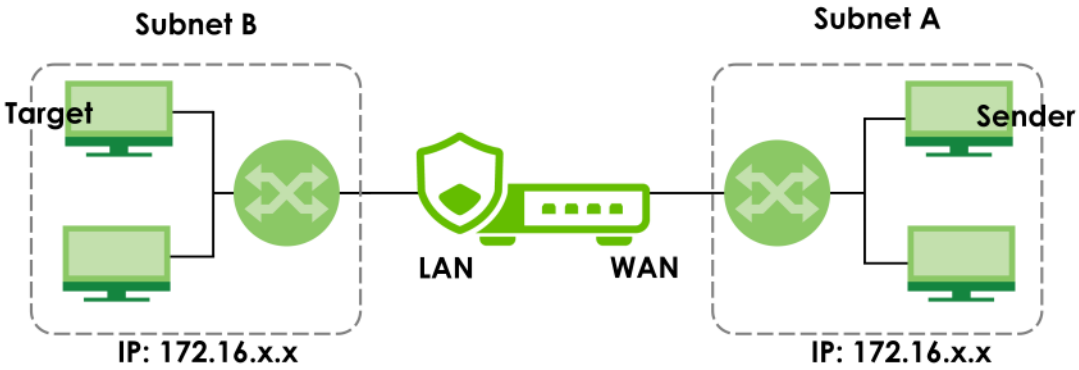
In the following figure, a host in a WAN subnet (A) broadcasts an ARP request to all devices within its network in order to find the MAC address of a target IP address (172.16.x.x). However, the target IP address may be in another subnet (B) that has the same network IP address (172.16.x.x). A router, such as the Zyxel Device, does not forward broadcasts, so the request will not reach its destination.

Enable Proxy ARP (RFC 1027) to allow the Zyxel Device to answer external interface ARP requests on behalf of a device on its internal interface. Interfaces supported are:

- Ethernet
- VLAN
- Bridge

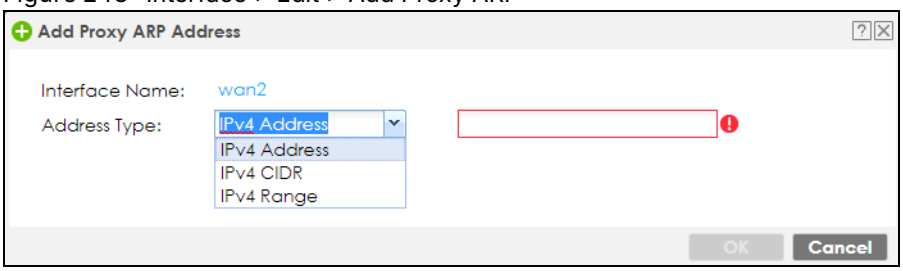
The Zyxel Device sends its external MAC address to the WAN sender as the destination for the target IP address. From then on the sender will send packets containing that target IP address directly to the external interface of the Zyxel Device. The Zyxel Device then forwards the packet to the correct target IP address in its LAN.

Figure 242 Proxy ARP



To allow the Zyxel Device to answer external interface ARP requests on behalf of a device on a supported interface, select the interface, click Add or Edit, then click Add in the Proxy ARP section of the screen.

Figure 243 Interface > Edit > Add Proxy ARP



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

Table 76 Interface > Edit > Add Proxy ARP

LABEL	DESCRIPTION
Interface Name	This identifies the interface for which the configuration settings that use it are displayed.
Address Type	Choose IPv4 Address, or IPv4 CIDR (for example, 192.168.1.1/24) or an IPv4 Range (for example, 192.168.1.2-192.168.1.100) and then enter the target IP address information. The Zyxel Device answers external ARP requests only if they match one of these inputted target IP addresses. For example, if the IPv4 Address is 192.168.1.5, then the Zyxel Device will answer ARP requests coming from the WAN only if it contains 192.168.1.5 as the target IP address.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

11.5.3 Virtual Interfaces

Use virtual interfaces to tell the Zyxel Device where to route packets. Virtual interfaces can also be used in VPN gateways (see IPSec VPN) and VRRP groups (see Device HA).

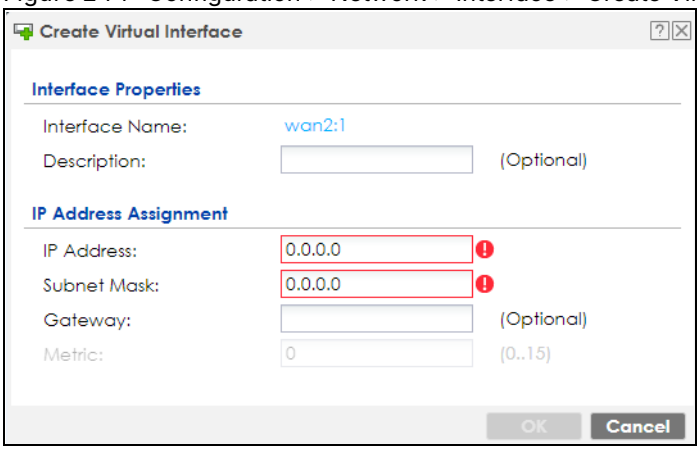
Virtual interfaces can be created on top of Ethernet interfaces, VLAN interfaces, or bridge interfaces. Virtual VLAN interfaces recognize and use the same VLAN ID. Otherwise, there is no difference between each type of virtual interface. Network policies (for example, security policies) that apply to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

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

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

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

Figure 244 Configuration > Network > Interface > Create Virtual Interface



Each field is described in the table below.

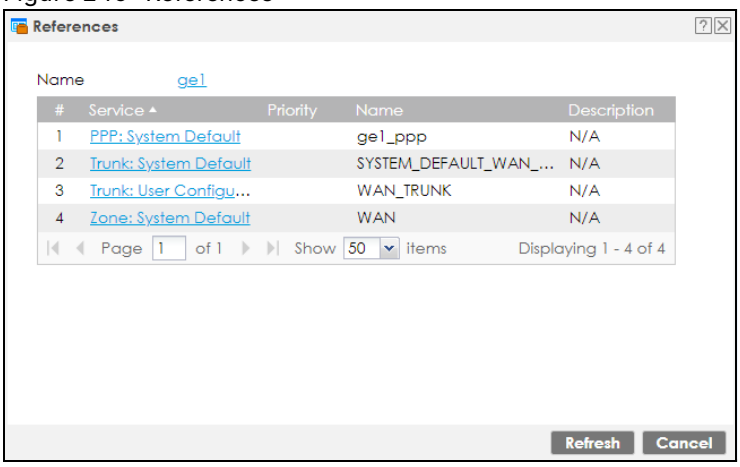
Table 77 Configuration > Network > Interface > Create Virtual Interface

LABEL	DESCRIPTION
Interface Properties	
Interface Name	This field is read-only. It displays the name of the virtual interface, which is automatically derived from the underlying Ethernet interface, VLAN interface, or bridge interface.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
IP Address Assignment	
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers on the network.
Gateway	Enter the IP address of the gateway. The Zyxel Device sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

11.5.4 References

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

Figure 245 References



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

Table 78 References

LABEL	DESCRIPTION
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.

11.5.5 Add/Edit DHCPv6 Request/Release Options

When you configure an interface as a DHCPv6 server or client, you can additionally add DHCPv6 request or lease options which have the Zyxel Device to add more information in the DHCPv6 packets. To open the screen, click Configuration > Network > Interface > Ethernet > Edit, select DHCPv6 Server or DHCPv6 Client in the DHCPv6 Setting section, and then click Add in the DHCPv6 Request Options or DHCPv6 Lease Options table.

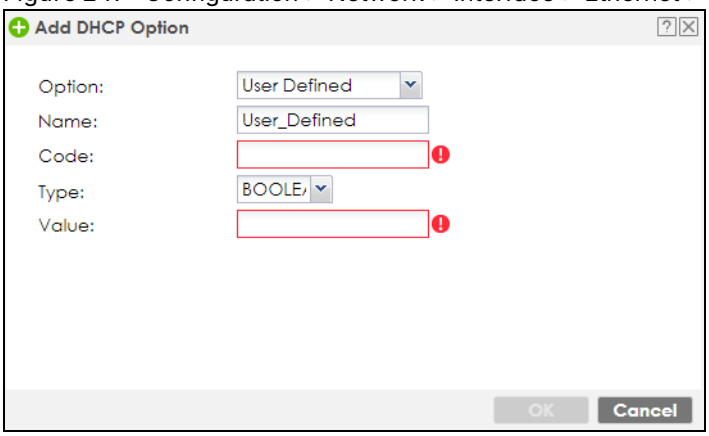
Figure 246 Configuration > Network > Interface > Ethernet > Edit > Add DHCPv6 Request/Lease Options

Select a DHCPv6 request or lease object in the Select one object field and click OK to save it. Click Cancel to exit without saving the setting.

11.5.6 Add/Edit DHCP Extended Options

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

Figure 247 Configuration > Network > Interface > Ethernet > Edit > Add/Edit Extended Options



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

Table 79 Configuration > Network > Interface > Ethernet > Edit > Add/Edit Extended Options

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

Table 79 Configuration > Network > Interface > Ethernet > Edit > Add/Edit Extended Options (continued)

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

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

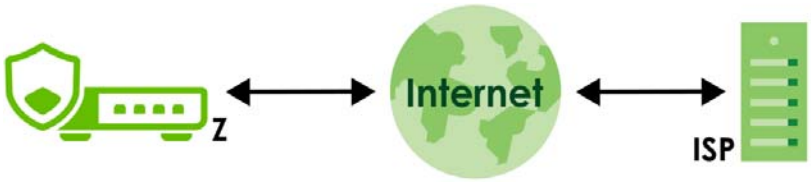
Table 80 DHCP Extended Options

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

11.6 PPP Interfaces

Use PPPoE/PPTP/L2TP interfaces to connect to your ISP. This way, you do not have to install or manage PPPoE/PPTP/L2TP software on each computer on the network.

Figure 248 Example: PPPoE/PPTP/L2TP Interfaces



PPPoE/PPTP/L2TP interfaces are similar to other interfaces in some ways. They have an IP address, subnet mask, and gateway used to make routing decisions; they restrict bandwidth and packet size; and they can verify the gateway is available. There are two main differences between PPPoE/PPTP/L2TP interfaces and other interfaces.

- You must also configure an ISP account object for the PPPoE/PPTP/L2TP interface to use.

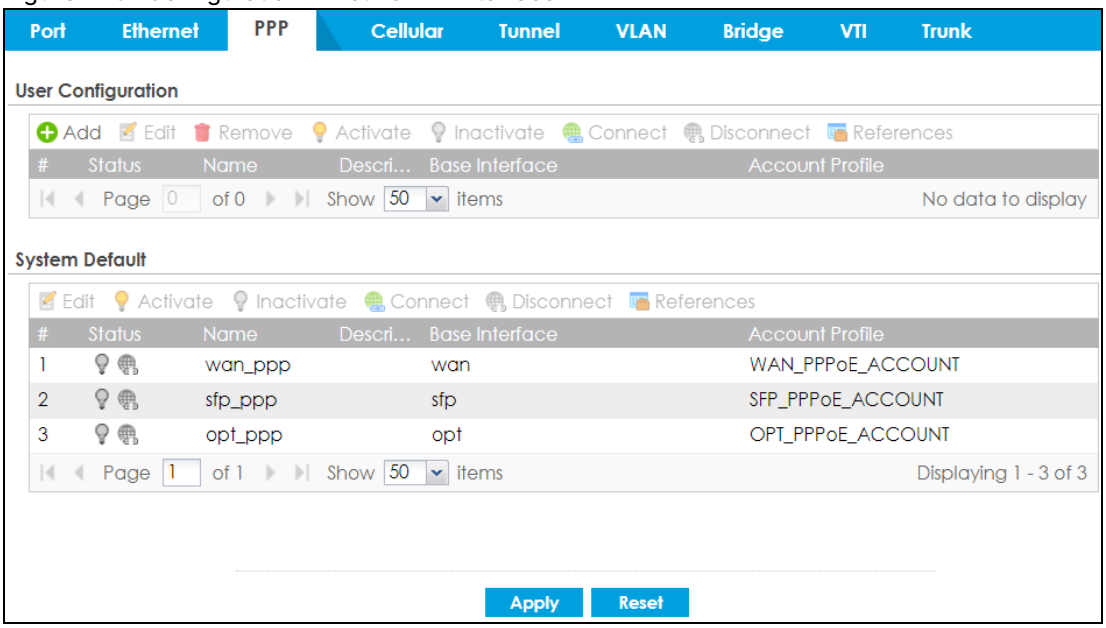
  Each ISP account specifies the protocol (PPPoE or PPTP or L2TP), as well as your ISP account information. If you change ISPs later, you only have to create a new ISP account, not a new PPPoE/PPTP/L2TP interface. You should not have to change any network policies.
- You do not set up the subnet mask or gateway.

  PPPoE/PPTP/L2TP interfaces are interfaces between the Zyxel Device and only one computer. Therefore, the subnet mask is always 255.255.255.255. In addition, the Zyxel Device always treats the ISP as a gateway.

11.6.1 PPP Interface Summary

This screen lists every PPPoE/PPTP/L2TP interface. To access this screen, click Configuration > Network > Interface > PPP.

Figure 249 Configuration > Network > Interface > PPP



Each field is described in the table below.

Table 81 Configuration > Network > Interface > PPP

LABEL	DESCRIPTION
User Configuration / System Default	The Zyxel Device comes with the (non-removable) System Default PPP interfaces pre-configured. You can create (and delete) User Configuration PPP interfaces. System Default PPP interfaces vary by model.
Add	Click this to create a new user-configured PPP interface.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove a user-configured PPP interface, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.

Table 81 Configuration > Network > Interface > PPP (continued)

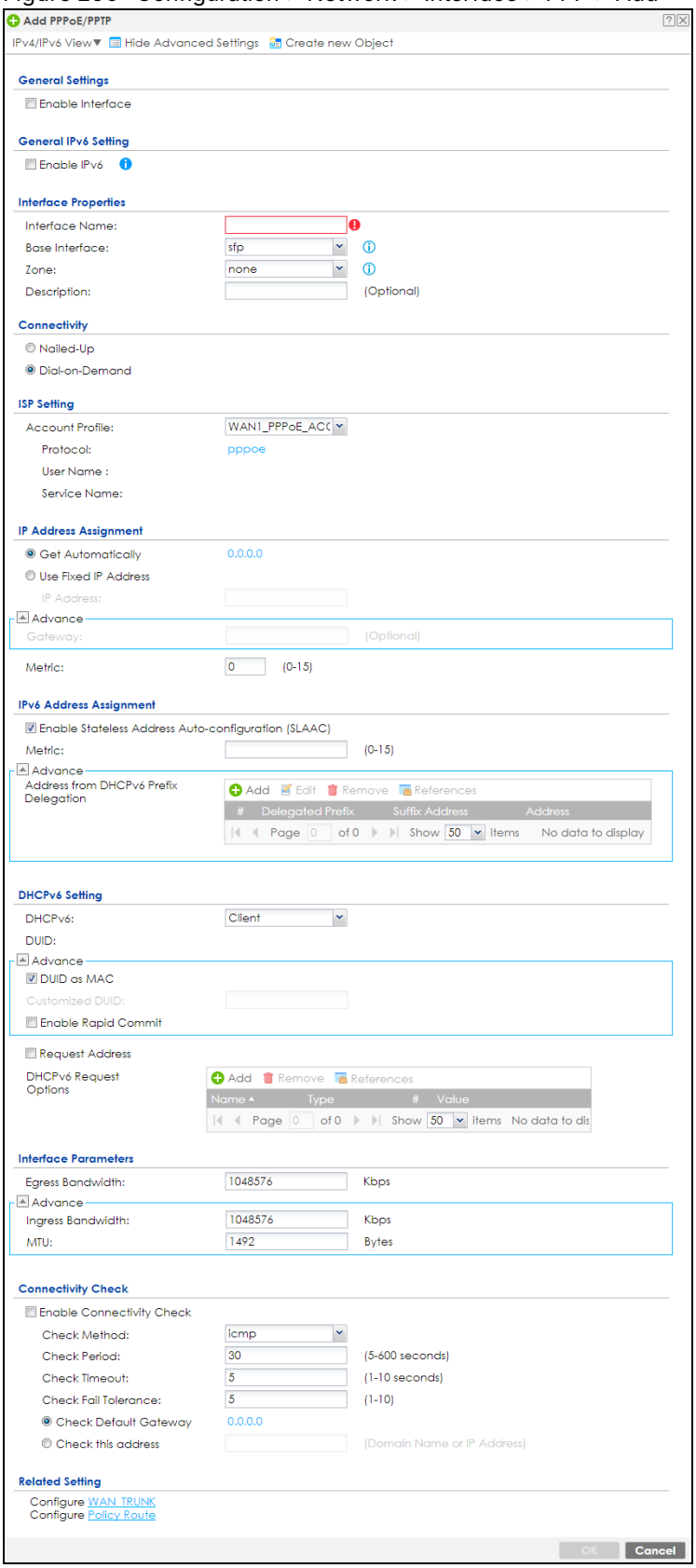
LABEL	DESCRIPTION
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Connect	To connect an interface, select it and click Connect. You might use this in testing the interface or to manually establish the connection for a Dial-on-Demand PPPoE/PPTP interface.
Disconnect	To disconnect an interface, select it and click Disconnect. You might use this in testing the interface.
References	Select an entry and click References to open a screen that shows which settings use the entry. See Section 11.5.4 on page 314 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The connect icon is lit when the interface is connected and dimmed when it is disconnected.
Name	This field displays the name of the interface.
Description	This field displays the description of the interface.
Base Interface	This field displays the interface on the top of which the PPPoE/PPTP/L2TP interface is.
Account Profile	This field displays the ISP account used by this PPPoE/PPTP interface.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

11.6.2 PPP Interface Add or Edit

Note: You have to set up an ISP account before you create a PPPoE/PPTP/L2TP interface.

This screen lets you configure a PPPoE or PPTP or L2TP interface. If you enabled IPv6 on the Configuration > System > IPv6 screen, you can also configure PPP interfaces used for your IPv6 networks on this screen. To access this screen, click the Add icon or an Edit icon on the PPP Interface screen.

Figure 250 Configuration > Network > Interface > PPP > Add



Each field is explained in the following table.

Table 82 Configuration > Network > Interface > PPP > Add

LABEL	DESCRIPTION
IPv4/IPv6 View / IPv4 View / IPv6 View	Use this button to display both IPv4 and IPv6, IPv4-only, or IPv6-only configuration fields.
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create New Object	Click this button to create an ISP Account or a DHCPv6 request object that you may use for the ISP or DHCPv6 settings in this screen.
General Settings	
Enable Interface	Select this to enable this interface. Clear this to disable this interface.
General IPv6 Setting	
Enable IPv6	Select this to enable IPv6 on this interface. Otherwise, clear this to disable it.
Interface Properties	
Interface Name	Specify a name for the interface. It can use alphanumeric characters, hyphens, and underscores, and it can be up to 11 characters long.
Base Interface	Select the interface upon which this PPP interface is built. Note: Multiple PPP interfaces can use the same base interface.
Zone	Select the zone to which this PPP interface belongs. The zone determines the security settings the Zyxel Device uses for the interface.
Description	Enter a description of this interface. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long. Spaces are allowed, but the string can't start with a space.
Connectivity	
Nailed-Up	Select this if the PPPoE/PPTP/L2TP connection should always be up. Clear this to have the Zyxel Device establish the PPPoE/PPTP/L2TP connection only when there is traffic. You might use this option if a lot of traffic needs to go through the interface or it does not cost extra to keep the connection up all the time.
Dial-on-Demand	Select this to have the Zyxel Device establish the PPPoE/PPTP/L2TP connection only when there is traffic. You might use this option if there is little traffic through the interface or if it costs money to keep the connection available.
ISP Setting	
Account Profile	Select the ISP account that this PPPoE/PPTP/L2TP interface uses. The drop-down box lists ISP accounts by name. Use Create new Object if you need to configure a new ISP account (see Chapter 30 on page 762 for details).
Protocol	This field is read-only. It displays the protocol specified in the ISP account.
User Name	This field is read-only. It displays the user name for the ISP account.
Service Name	This field is read-only. It displays the PPPoE service name specified in the ISP account. This field is blank if the ISP account uses PPTP.
IP Address Assignment	Click Show Advanced Settings to display more settings. Click Hide Advanced Settings to display fewer settings.
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address automatically. The subnet mask and gateway are always defined automatically in PPPoE/PPTP/L2TP interfaces.
Use Fixed IP Address	Select this if you want to specify the IP address manually.
IP Address	This field is enabled if you select Use Fixed IP Address. Enter the IP address for this interface.

Table 82 Configuration > Network > Interface > PPP > Add (continued)

LABEL	DESCRIPTION
Gateway	This field is enabled if you select Use Fixed IP Address. Enter the IP address of the gateway. The Zyxel Device sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (the ISP) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
IPv6 Address Assignment	These IP address fields configure an IPv6 IP address on the interface itself.
Enable Stateless Address Auto-configuration (SLAAC)	Select this to enable IPv6 stateless auto-configuration on this interface. The interface will generate an IPv6 IP address itself from a prefix obtained from an IPv6 router on the network.
Metric	Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
Address from DHCPv6 Prefix Delegation	Use this table to have the Zyxel Device obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ. You have to also enter a suffix address which is appended to the delegated prefix to form an address for this interface. See Prefix Delegation on page 289 for more information. To use prefix delegation, you must: • Create at least one DHCPv6 request object before configuring this table. • The external interface must be a DHCPv6 client. You must configure the DHCPv6 request options using a DHCPv6 request object with the type of prefix-delegation. • Assign the prefix delegation to an internal interface and enable router advertisement on that interface.
Add	Click this to create an entry.
Edit	Select an entry and click this to change the settings.
Remove	Select an entry and click this to delete it from this table.
References	Select an entry and click References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use from the drop-down list.
Suffix Address	Enter the ending part of the IPv6 address, a slash (/), and the prefix length. The Zyxel Device will append it to the delegated prefix. For example, you got a delegated prefix of 2003:1234:5678/48. You want to configure an IP address of 2003:1234:5678:1111::1/128 for this interface, then enter ::1111:0:0:0:1/128 in this field.
Address	This field displays the combined IPv6 IP address for this interface. Note: This field displays the combined address after you click OK and reopen this screen.
DHCPv6 Setting	
DHCPv6	Select Client to obtain an IP address and DNS information from the service provider for the interface. Otherwise, select N/A to disable the function.
DUID	This field displays the DHCP Unique IDentifier (DUID) of the interface, which is unique and used for identification purposes when the interface is exchanging DHCPv6 messages with others. See DHCPv6 on page 289 for more information.

Table 82 Configuration > Network > Interface > PPP > Add (continued)

LABEL	DESCRIPTION
DUID as MAC	Select this if you want the DUID is generated from the interface's default MAC address.
Customized DUID	If you want to use a customized DUID, enter it here for the interface.
Enable Rapid Commit	Select this to shorten the DHCPv6 message exchange process from four to two steps. This function helps reduce heavy network traffic load. Note: Make sure you also enable this option in the DHCPv6 clients to make rapid commit work.
Request Address	Select this to get an IPv6 IP address for this interface from the DHCP server. Clear this to not get any IP address information through DHCPv6.
DHCPv6 Request Options	Use this section to configure DHCPv6 request settings that determine what additional information to get from the DHCPv6 server.
Add	Click this to create an entry in this table. See Section 11.5.6 on page 316 for more information.
Remove	Select an entry and click this to delete it from this table.
References	Select an entry and click References to open a screen that shows which settings use the entry. See Section 11.5.4 on page 314 for an example.
Name	This field displays the name of the DHCPv6 request object.
Type	This field displays the type of the object.
Value	This field displays the IPv6 prefix that the Zyxel Device will advertise to its clients.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Enter the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device divides it into smaller fragments. Allowed values are 576 - 1492. Usually, this value is 1492.
Connectivity Check	The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the Zyxel Device stops routing to the gateway. The Zyxel Device resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select icmp to have the Zyxel Device regularly ping the gateway you specify to make sure it is still available. Select tcp to have the Zyxel Device regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the Zyxel Device stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.

Table 82 Configuration > Network > Interface > PPP > Add (continued)

LABEL	DESCRIPTION
Check Port	This field only displays when you set the Check Method to tcp. Specify the port number to use for a TCP connectivity check.
Related Setting	
Configure WAN TRUNK	Click WAN TRUNK to go to a screen where you can configure the interface as part of a WAN trunk for load balancing.
Policy Route	Click Policy Route to go to the screen where you can manually configure a policy route to associate traffic with this interface.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

11.7 Cellular Configuration Screen

Mobile broadband is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices.

Note: The actual data rate you obtain varies depending on the mobile broadband device you use, the signal strength to the service provider's base station, and so on.

You can configure how the Zyxel Device's mobile broadband device connects to a network (refer to Section 11.7.1 on page 327):

- You can set the mobile broadband device to connect only to the home network, which is the network to which you are originally subscribed.
- You can set the mobile broadband device to connect to other networks if the signal strength of the home network is too low or it is unavailable.

3G

3G (Third Generation) is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices.

4G

4G is the fourth generation of the mobile telecommunications technology and a successor of 3G. Both the WiMAX and Long Term Evolution (LTE) standards are the 4G candidate systems. 4G only supports all-IP-based packet-switched telephony services and is required to offer Gigabit speed access.

Note: The actual data rate you obtain varies depending on your mobile environment. The environmental factors may include the number of mobile devices which are currently connected to the mobile network, the signal strength to the mobile network, and so on.

See the following table for a comparison between 2G, 2.5G, 2.75G, 3G and 4G wireless technologies.

Table 83 2G, 2.5G, 2.75G, 3G, 3.5G and 4G Wireless Technologies

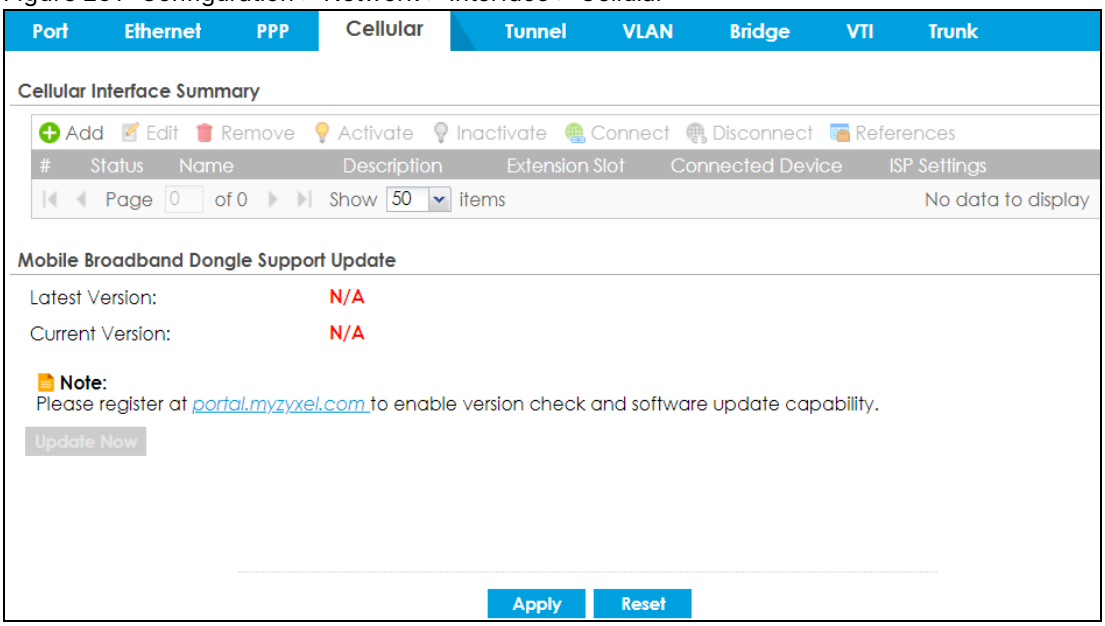
NAME	TYPE	MOBILE PHONE AND DATA STANDARDS		DATA SPEED
		GSM-BASED	CDMA-BASED	
2G	Circuit-switched	GSM (Global System for Mobile Communications), Personal Handy-phone System (PHS), etc.	Interim Standard 95 (IS-95), the first CDMA-based digital cellular standard pioneered by Qualcomm. The brand name for IS-95 is cdmaOne. IS-95 is also known as TIA-EIA-95.	Slow
2.5G	Packet-switched	GPRS (General Packet Radio Services), High-Speed Circuit-Switched Data (HSCSD), etc.	CDMA2000 is a hybrid 2.5G / 3G protocol of mobile telecommunications standards that use CDMA, a multiple access scheme for digital radio. CDMA2000 1xRTT (1 times Radio Transmission Technology) is the core CDMA2000 wireless air interface standard. It is also known as 1x, 1xRTT, or IS-2000 and considered to be a 2.5G or 2.75G technology.	
2.75G	Packet-switched	Enhanced Data rates for GSM Evolution (EDGE), Enhanced GPRS (EGPRS), etc.		
3G	Packet-switched	UMTS (Universal Mobile Telecommunications System), a third-generation (3G) wireless standard defined in ITU specification, is sometimes marketed as 3GSM. The UMTS uses GSM infrastructures and W-CDMA (Wideband Code Division Multiple Access) as the air interface. The International Telecommunication Union (ITU) is an international organization within which governments and the private sector coordinate global telecom networks and services.	CDMA2000 EV-DO (Evolution-Data Optimized, originally 1x Evolution-Data Only), also referred to as EV-DO, EVDO, or just EV, is an evolution of CDMA2000 1xRTT and enables high-speed wireless connectivity. It is also denoted as IS-856 or High Data Rate (HDR).	
3.5G	Packet-switched	HSDPA (High-Speed Downlink Packet Access) is a mobile telephony protocol, used for UMTS-based 3G networks and allows for higher data transfer speeds.		
4G/LTE	Packet-switched	The LTE (Long Term Evolution) standard is based on the GSM and UMTS network technologies.		Fast

To change your mobile broadband WAN settings, click Configuration > Network > Interface > Cellular.

Note: Install (or connect) a compatible mobile broadband USB device to use a cellular connection.

Note: The WAN IP addresses of a Zyxel Device with multiple WAN interfaces must be on different subnets.

Figure 251 Configuration > Network > Interface > Cellular



The following table describes the labels in this screen.

Table 84 Configuration > Network > Interface > Cellular

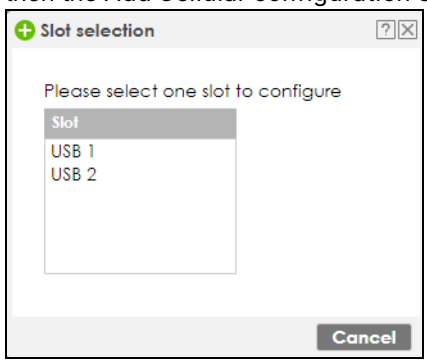
LABEL	DESCRIPTION
Add	Click this to create a new cellular interface.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
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 interface, select it and click Connect. You might use this in testing the interface or to manually establish the connection.
Disconnect	To disconnect an interface, select it and click Disconnect. You might use this in testing the interface.
References	Select an entry and click References to open a screen that shows which settings use the entry. See Section 11.5.4 on page 314 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The connect icon is lit when the interface is connected and dimmed when it is disconnected.
Name	This field displays the name of the interface.
Description	This field displays the description of the interface.
Extension Slot	This field displays where the entry's cellular card is located.
Connected Device	This field displays the name of the cellular card.
ISP Settings	This field displays the profile of ISP settings that this cellular interface is set to use.
Mobile Broadband Dongle Support	You should have registered your Zyxel Device at myZyxel. myZyxel hosts a list of supported mobile broadband dongle devices. You should have an Internet connection to access this website.

Table 84 Configuration > Network > Interface > Cellular (continued)

LABEL	DESCRIPTION
Latest Version	This displays the latest supported mobile broadband dongle list version number.
Current Version	This displays the currently supported (by the Zyxel Device) mobile broadband dongle list version number.
Update Now	If the latest version number is greater than the current version number, then click this button to download the latest list of supported mobile broadband dongle devices to the Zyxel Device.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

11.7.1 Cellular Choose Slot

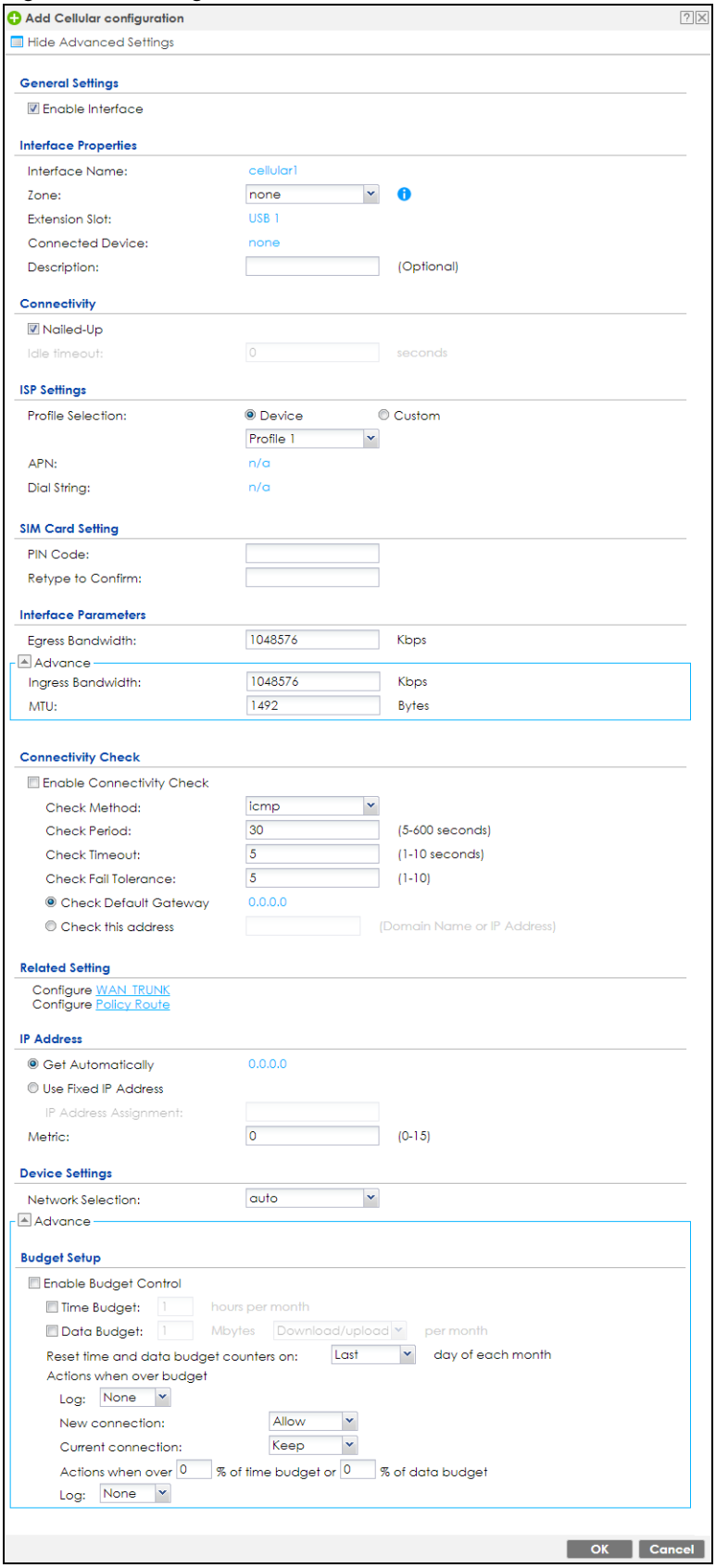
To change your mobile broadband settings, click Configuration > Network > Interface > Cellular > Add (or Edit). In the pop-up window that displays, select the slot that contains the mobile broadband device, then the Add Cellular configuration screen displays.



11.7.2 Add / Edit Cellular Configuration

This screen displays after you select the slot that contains the mobile broadband device in the previous pop-up window.

Figure 252 Configuration > Network > Interface > Cellular > Add / Edit



The following table describes the labels in this screen.

Table 85 Configuration > Network > Interface > Cellular > Add / Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
General Settings	
Enable Interface	Select this option to turn on this interface.
Interface Properties	
Interface Name	Select a name for the interface.
Zone	Select the zone to which you want the cellular interface to belong. The zone determines the security settings the Zyxel Device uses for the interface.
Extension Slot	This is the USB slot that you are configuring for use with a mobile broadband card.
Connected Device	This displays the manufacturer and model name of your mobile broadband card if you inserted one in the Zyxel Device. Otherwise, it displays none.
Description	Enter a description of this interface. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long. Spaces are allowed, but the string can't start with a space.
Connectivity	
Nailed-Up	Select this if the connection should always be up. Clear this to have the Zyxel Device to establish the connection only when there is traffic. You might not nail up the connection if there is little traffic through the interface or if it costs money to keep the connection available.
Idle timeout	This value specifies the time in seconds (0~360) that elapses before the Zyxel Device automatically disconnects from the ISP's server. Zero disables the idle timeout.
ISP Settings	
Profile Selection	Select Device to use one of the mobile broadband device's profiles of device settings. Then select the profile (use Profile 1 unless your ISP instructed you to do otherwise). Select Custom to configure your device settings yourself.
APN	This field is read-only if you selected Device in the profile selection. Select Custom in the profile selection to be able to manually input the APN (Access Point Name) provided by your service provider. This field applies with a GSM or HSDPA mobile broadband card. Enter the APN from your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge method. Enter 1 to 63 single-byte characters, including a-zA-Z0-9$-./@_ !"#%&'()*+,;:<=>?[\]^'{|}~ and spaces are not allowed.
Dial String	Enter the dial string if your ISP provides a string, which would include the APN, to initialize the mobile broadband card. Enter 1 to 31 single-byte characters, including a-zA-Z0-9!#$%&'()*+,-./;:<=>@\^_'{|}~ "[]?and spaces are not allowed. This field is available only when you insert a GSM mobile broadband card.

Table 85 Configuration > Network > Interface > Cellular > Add / Edit (continued)

LABEL	DESCRIPTION
Authentication Type	The Zyxel Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: None: No authentication for outgoing calls. CHAP - Your Zyxel Device accepts CHAP requests only. PAP - Your Zyxel Device accepts PAP requests only.
User Name	This field displays when you select an authentication type other than None. This field is read-only if you selected Device in the profile selection. If this field is configurable, enter the user name for this mobile broadband card exactly as the service provider gave it to you. You can use 1 ~ 64 alphanumeric and #:%-_@$./ characters. The first character must be alphanumeric or -_@$./. Spaces are not allowed.
Password	This field displays when you select an authentication type other than None. This field is read-only if you selected Device in the profile selection and the password is included in the mobile broadband card's profile. If this field is configurable, enter the password for this SIM card exactly as the service provider gave it to you. You can use 0 ~ 63 alphanumeric and ~!@#$%^&*()_-+={}|;:'<,>./ characters. Spaces are not allowed.
Retype to Confirm	This field displays when you select an authentication type other than None. This field is read-only if you selected Device in the profile selection and the password is included in the mobile broadband card's profile. If this field is configurable, re-enter the password for this SIM card exactly as the service provider gave it to you.
SIM Card Setting	
PIN Code	This field displays with a GSM or HSDPA mobile broadband card. A PIN (Personal Identification Number) code is a key to a mobile broadband card. Without the PIN code, you cannot use the mobile broadband card. Enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly, the mobile broadband card may be blocked by your ISP and you cannot use the account to access the Internet. If your ISP disabled PIN code authentication, enter an arbitrary number.
Retype to Confirm	Enter the PIN code again to confirm it.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can send through the interface to the network. Allowed values are 0 - 1048576. This setting is used in WAN load balancing and bandwidth management.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Enter the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device divides it into smaller fragments. Allowed values are 576 - 1492. Usually, this value is 1492.
Connectivity Check	The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the Zyxel Device stops routing to the gateway. The Zyxel Device resumes routing to the gateway the first time the gateway passes the connectivity check.

Table 85 Configuration > Network > Interface > Cellular > Add / Edit (continued)

LABEL	DESCRIPTION
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select icmp to have the Zyxel Device regularly ping the gateway you specify to make sure it is still available. Select tcp to have the Zyxel Device regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the Zyxel Device stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the Check Method to tcp. Specify the port number to use for a TCP connectivity check.
Related Setting	
Configure WAN TRUNK	Click WAN TRUNK to go to a screen where you can configure the interface as part of a WAN trunk for load balancing.
Configure Policy Route	Click Policy Route to go to the policy route summary screen where you can configure a policy route to override the default routing and SNAT behavior for the interface.
IP Address Assignment	
Get Automatically	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address Assignment	Enter the cellular interface's WAN IP address in this field if you selected Use Fixed IP Address.
Metric	Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
Device Settings	

Table 85 Configuration > Network > Interface > Cellular > Add / Edit (continued)

LABEL	DESCRIPTION
Band Selection	This field appears if you selected a mobile broadband device that allows you to select the type of network to use. Select the type of mobile broadband service for your mobile broadband connection. If you are unsure what to select, check with your mobile broadband service provider to find the mobile broadband service available to you in your region. Select auto to have the card connect to an available network. Choose this option if you do not know what networks are available. You may want to manually specify the type of network to use if you are charged differently for different types of network or you only have one type of network available to you. Select GPRS / EDGE (GSM) only to have this interface only use a 2.5G or 2.75G network (respectively). If you only have a GSM network available to you, you may want to select this so the Zyxel Device does not spend time looking for a WCDMA network. Select UMTS / HSDPA (WCDMA) only to have this interface only use a 3G or 3.5G network (respectively). You may want to do this if you want to make sure the interface does not use the GSM network. Select LTE only to have this interface only use a 4G LTE network. This option only appears when a dongle for 4G technology is inserted.
Network Selection	Home network is the network to which you are originally subscribed. Select Home to have the mobile broadband device connect only to the home network. If the home network is down, the Zyxel Device’s mobile broadband Internet connection is also unavailable. Select Auto (Default) to allow the mobile broadband device to connect to a network to which you are not subscribed when necessary, for example when the home network is down or another mobile broadband base station's signal is stronger. This is recommended if you need continuous Internet connectivity. If you select this, you may be charged using the rate of a different network.
Budget Setup	
Enable Budget Control	Select this to set a monthly limit for the user account of the installed mobile broadband card. You can set a limit on the total traffic and/or call time. The Zyxel Device takes the actions you specified when a limit is exceeded during the month.
Time Budget	Select this and specify the amount of time (in hours) that the mobile broadband connection can be used within one month. If you change the value after you configure and enable budget control, the Zyxel Device resets the statistics.
Data Budget	Select this and specify how much downstream and/or upstream data (in Mega bytes) can be transmitted through the mobile broadband connection within one month. Select Download to set a limit on the downstream traffic (from the ISP to the Zyxel Device). Select Upload to set a limit on the upstream traffic (from the Zyxel Device to the ISP). Select Download/Upload to set a limit on the total traffic in both directions. If you change the value after you configure and enable budget control, the Zyxel Device resets the statistics.
Reset time and data budget counters on	Select the date on which the Zyxel Device resets the budget every month. If the date you selected is not available in a month, such as 30th or 31st, the Zyxel Device resets the budget on the last day of the month.
Reset time and data budget counters	This button is available only when you enable budget control in this screen. Click this button to reset the time and data budgets immediately. The count starts over with the mobile broadband connection’s full configured monthly time and data budgets. This does not affect the normal monthly budget restart; so if you configured the time and data budget counters to reset on the second day of the month and you use this button on the first, the time and data budget counters will still reset on the second.

Table 85 Configuration > Network > Interface > Cellular > Add / Edit (continued)

LABEL	DESCRIPTION
Actions when over budget	Specify the actions the Zyxel Device takes when the time or data limit is exceeded.
Log	Select None to not create a log, Log to create a log, or Log-alert to create an alert log. If you select Log or Log-alert you can also select recurring every to have the Zyxel Device send a log or alert for this event periodically. Specify how often (from 1 to 65535 minutes) to send the log or alert.
New connection	Select Allow to permit new mobile broadband connections or Disallow to drop/block new mobile broadband connections.
Current connection	Select Keep to maintain an existing mobile broadband connection or Drop to disconnect it. You cannot set New connection to Allow and Current connection to Drop at the same time. If you set New connection to Disallow and Current connection to Keep, the Zyxel Device allows you to transmit data using the current connection, but you cannot build a new connection if the existing connection is disconnected.
Actions when over % of time budget or % of data budget	Specify the actions the Zyxel Device takes when the specified percentage of time budget or data limit is exceeded. Enter a number from 1 to 99 in the percentage fields. If you change the value after you configure and enable budget control, the Zyxel Device resets the statistics.
Log	Select None to not create a log when the Zyxel Device takes this action, Log to create a log, or Log-alert to create an alert log. If you select Log or Log-alert you can also select recurring every to have the Zyxel Device send a log or alert for this event periodically. Specify how often (from 1 to 65535 minutes) to send the log or alert.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

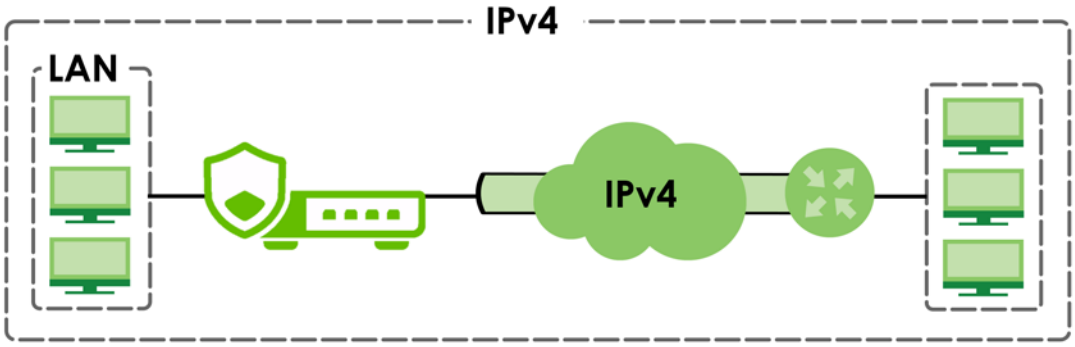
11.8 Tunnel Interfaces

The Zyxel Device uses tunnel interfaces in Generic Routing Encapsulation (GRE), IPv6 in IPv4, and 6to4 tunnels.

GRE Tunneling

GRE tunnels encapsulate a wide variety of network layer protocol packet types inside IP tunnels. A GRE tunnel serves as a virtual point-to-point link between the Zyxel Device and another router over an IPv4 network. At the time of writing, the Zyxel Device only supports GRE tunneling in IPv4 networks.

Figure 253 GRE Tunnel Example



IPv6 Over IPv4 Tunnels

To route traffic between two IPv6 networks over an IPv4 network, an IPv6 over IPv4 tunnel has to be used.

Figure 254 IPv6 over IPv4 Network

On the Zyxel Device, you can either set up a manual IPv6-in-IPv4 tunnel or an automatic 6to4 tunnel. The following describes each method:

IPv6-in-IPv4 Tunneling

Use this mode on the WAN of the Zyxel Device if

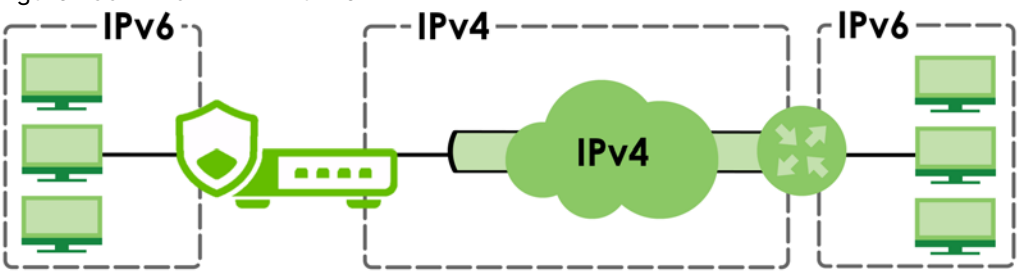
- your Zyxel Device has a public IPv4 IP address given from your ISP,

and

- you want to transmit your IPv6 packets to one and only one remote site whose LAN network is also an IPv6 network.

With this mode, the Zyxel Device encapsulates IPv6 packets within IPv4 packets across the Internet. You must know the WAN IP address of the remote gateway device. This mode is normally used for a site-to-site application such as two branch offices.

Figure 255 IPv6-in-IPv4 Tunnel



In the Zyxel Device, you must also manually configure a policy route for an IPv6-in-IPv4 tunnel to make the tunnel work.

6to4 Tunneling

This mode also enables IPv6 packets to cross IPv4 networks. Unlike IPv6-in-IPv4 tunneling, you do not need to configure a policy route for a 6to4 tunnel. Through your properly pre-configuring the destination router's IP address in the IP address assignments to hosts, the Zyxel Device can automatically forward 6to4 packets to the destination they want to go. A 6to4 relay router is required to route 6to4 packets to a native IPv6 network if the packet's destination do not match your specified criteria.

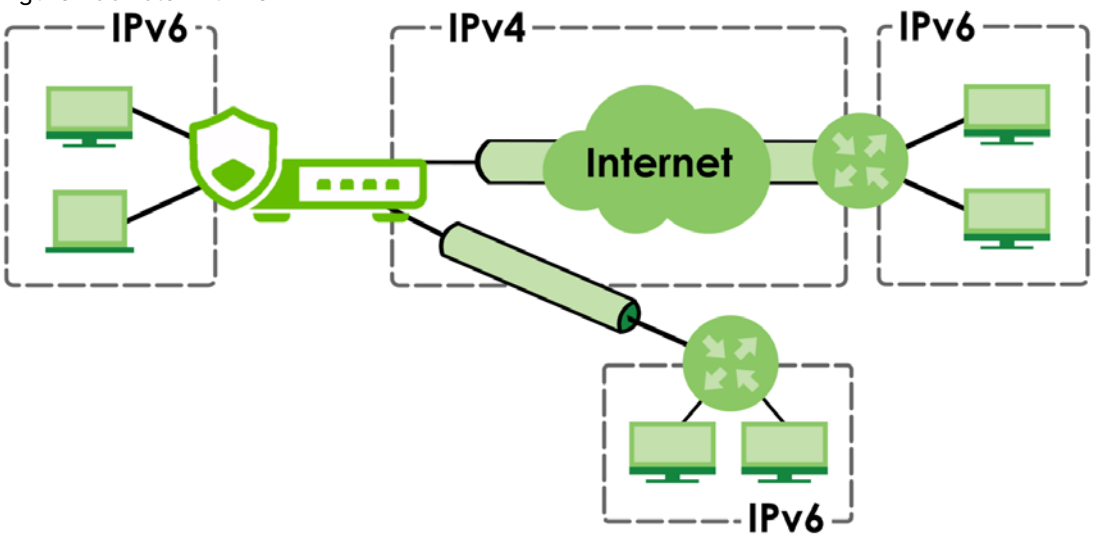
In this mode, the Zyxel Device should get a public IPv4 address for the WAN. The Zyxel Device adds an IPv4 IP header to an IPv6 packet when transmitting the packet to the Internet. In reverse, the Zyxel Device removes the IPv4 header from an IPv6 packet when receiving it from the Internet.

An IPv6 address using the 6to4 mode consists of an IPv4 address, the format is as the following:

2002:[a public IPv4 address in hexadecimal]::/48

For example, a public IPv4 address is 202.156.30.41. The converted hexadecimal IP string is ca.9c.1Ee.29. The IPv6 address prefix becomes 2002:ca9c:1e29::/48.

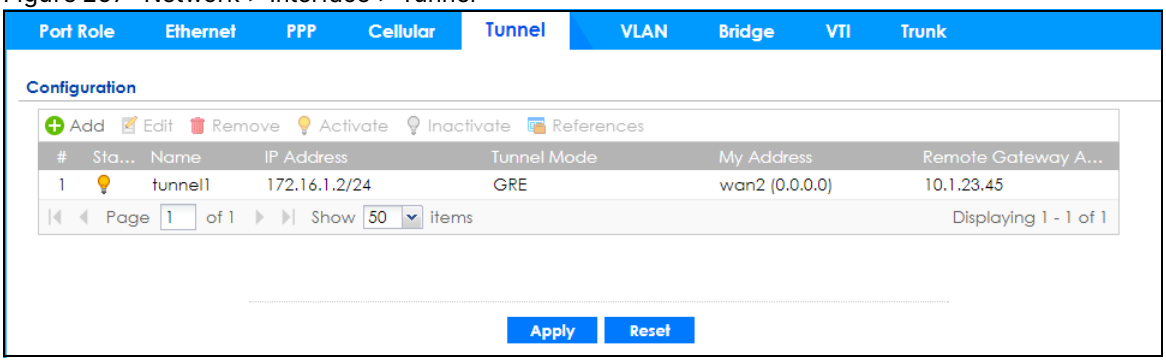
Figure 256 6to4 Tunnel



11.8.1 Configuring a Tunnel

This screen lists the Zyxel Device's configured tunnel interfaces. To access this screen, click Network > Interface > Tunnel.

Figure 257 Network > Interface > Tunnel



Each field is explained in the following table.

Table 86 Network > Interface > Tunnel

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

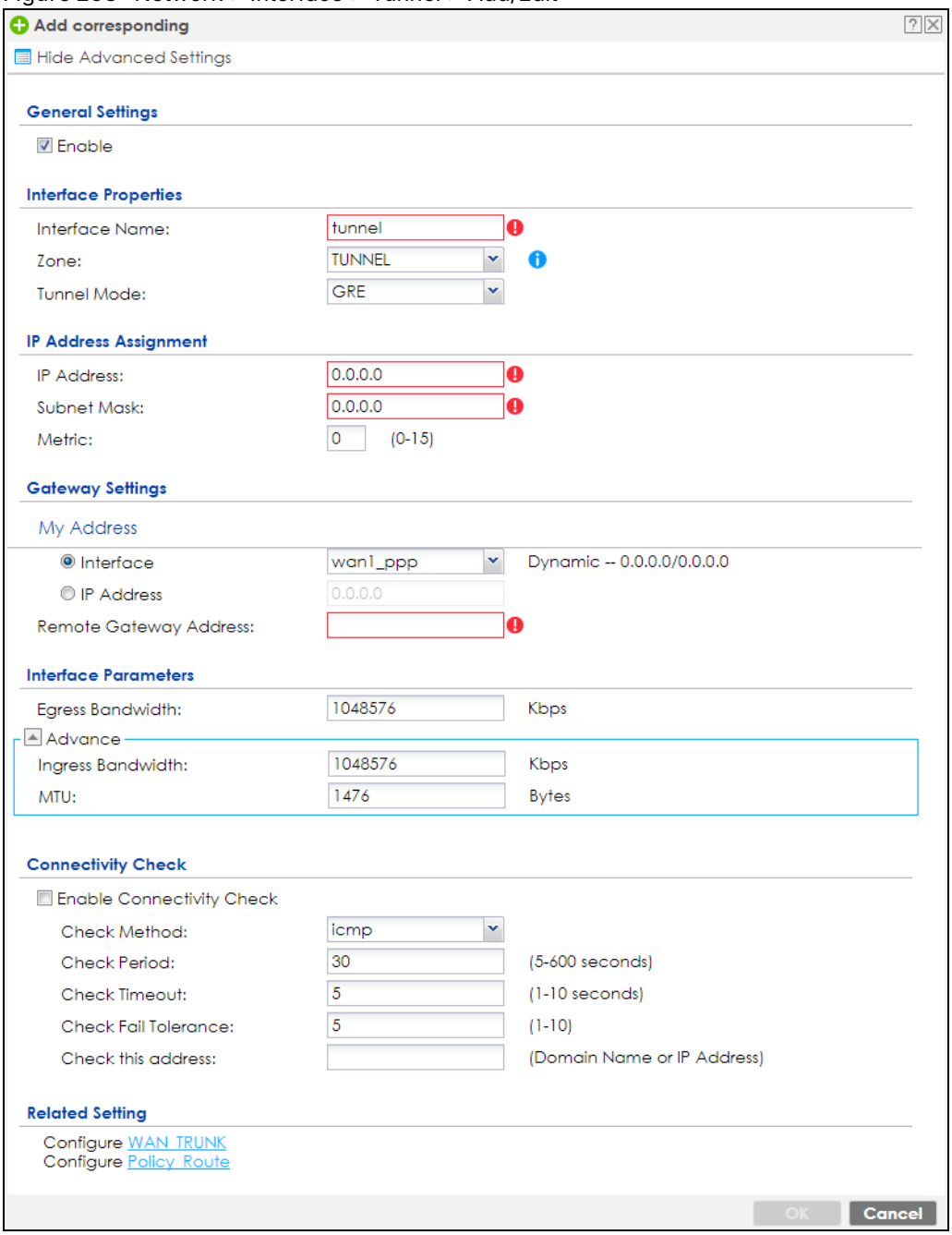
Table 86 Network > Interface > Tunnel (continued)

LABEL	DESCRIPTION
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
References	Select an entry and click References to open a screen that shows which settings use the entry. See Section 11.5.4 on page 314 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the interface.
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.
Tunnel Mode	This is the tunnel mode of the interface (GRE, IPv6-in-IPv4 or 6to4). This field also displays the interface's IPv4 IP address and subnet mask if it is a GRE tunnel. Otherwise, it displays the interface's IPv6 IP address and prefix length.
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.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to begin configuring this screen afresh.

11.8.2 Tunnel Add or Edit Screen

This screen lets you configure a tunnel interface. Click Configuration > Network > Interface > Tunnel > Add (or Edit) to open the following screen.

Figure 258 Network > Interface > Tunnel > Add/Edit



Each field is explained in the following table.

Table 87 Network > Interface > Tunnel > Add/Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
General Settings	
Enable	Select this to enable this interface. Clear this to disable this interface.
Interface Properties	

Table 87 Network > Interface > Tunnel > Add/Edit (continued)

LABEL	DESCRIPTION
Interface Name	This field is read-only if you are editing an existing tunnel interface. Enter the name of the tunnel interface. The format is tunnel*x*, where *x* is 0 - 3. For example, tunnel0.
Zone	Use this field to select the zone to which this interface belongs. This controls what security settings the Zyxel Device applies to this interface.
Tunnel Mode	Select the tunneling protocol of the interface (GRE, IPv6-in-IPv4 or 6to4). See Section 11.8 on page 333 for more information.
IP Address Assignment	This section is available if you are configuring a GRE tunnel.
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers on the network.
Metric	Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
IPv6 Address Assignment	This section is available if you are configuring an IPv6-in-IPv4 or a 6to4 tunnel.
IPv6 Address/ Prefix Length	Enter the IPv6 address and the prefix length for this interface if you want to use a static IP address. This field is optional. The prefix length indicates what the left-most part of the IP address is the same for all computers on the network, that is, the network address.
Metric	Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
6to4 Tunnel Parameter	This section is available if you are configuring a 6to4 tunnel which encapsulates IPv6 to IPv4 packets.
6to4 Prefix	Enter the IPv6 prefix of a destination network. The Zyxel Device forwards IPv6 packets to the hosts on the matched network. If you enter a prefix starting with 2002, the Zyxel Device will forward the matched packets to the IPv4 IP address converted from the packets' destination address. The IPv4 IP address can be converted from the next 32 bits after the prefix you specified in this field. See 6to4 Tunneling on page 334 for an example. The Zyxel Device forwards the unmatched packets to the specified Relay Router.
Relay Router	Enter the IPv4 address of a 6to4 relay router which helps forward packets between 6to4 networks and native IPv6 networks.
Remote Gateway Prefix	Enter the IPv4 network address and network bits of a remote 6to4 gateway, for example, 14.15.0.0/16. This field works if you enter a 6to4 Prefix not starting with 2002 (2003 for example). The Zyxel Device forwards the matched packets to a remote gateway with the network address you specify here, and the bits converted after the 6to4 Prefix in the packets. For example, you configure the 6to4 prefix to 2003:A0B::/32 and the remote gateway prefix to 14.15.0.0/16. If a packet's destination is 2003:A0B:1011:5::8, the Zyxel Device forwards the packet to 14.15.16.17, where the network address is 14.15.0.0 and the host address is the remain bits converted from 1011 after the packet's 6to4 prefix (2003:A0B).
Gateway Settings	
My Address	Specify the interface or IP address to use as the source address for the packets this interface tunnels to the remote gateway. The remote gateway sends traffic to this interface or IP address.

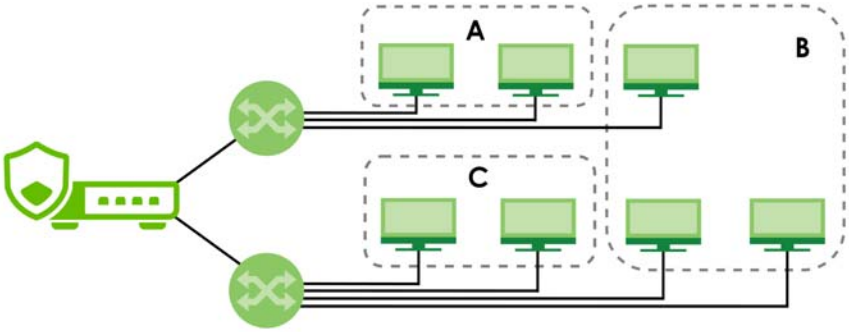
Table 87 Network > Interface > Tunnel > Add/Edit (continued)

LABEL	DESCRIPTION
Remote Gateway Address	Enter the IP address or domain name of the remote gateway to which this interface tunnels traffic. Automatic displays in this field if you are configuring a 6to4 tunnel. It means the 6to4 tunnel will help forward packets to the corresponding remote gateway automatically by looking at the packet's destination address.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can send through the interface to the network. Allowed values are 0 - 1048576. This setting is used in WAN load balancing and bandwidth management.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Enter the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
Connectivity Check	This section is available if you are configuring a GRE tunnel. The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the Zyxel Device stops routing to the gateway. The Zyxel Device resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select icmp to have the Zyxel Device regularly ping the gateway you specify to make sure it is still available. Select tcp to have the Zyxel Device regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the Zyxel Device stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field displays when you set the Check Method to tcp. Specify the port number to use for a TCP connectivity check.
Related Setting	
WAN TRUNK	Click this link to go to a screen where you can configure WAN trunk load balancing.
Policy Route	Click this link to go to the screen where you can manually configure a policy route to associate traffic with this interface.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

11.9 VLAN Interfaces

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

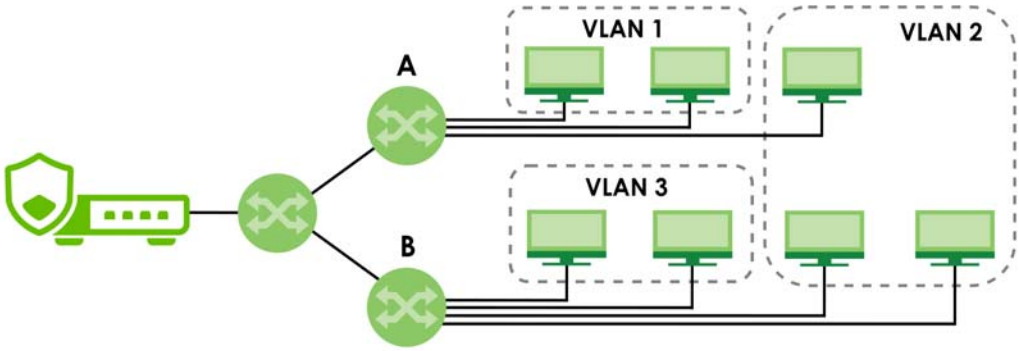
Figure 259 Example: Before VLAN



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

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

Figure 260 Example: After VLAN



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

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

This approach provides a few advantages.

- Increased performance - In VLAN 2, the extra switch should route traffic inside the sales department faster than the router does. In addition, broadcasts are limited to smaller, more logical groups of users.
- Higher security - If each computer has a separate physical connection to the switch, then broadcast traffic in each VLAN is never sent to computers in another VLAN.

- Better manageability - You can align network policies more appropriately for users. For example, you can create different content filtering rules for each VLAN (each department in the example above), and you can set different bandwidth limits for each VLAN. These rules are also independent of the physical network, so you can change the physical network without changing policies.

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

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

VLAN Interfaces Overview

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

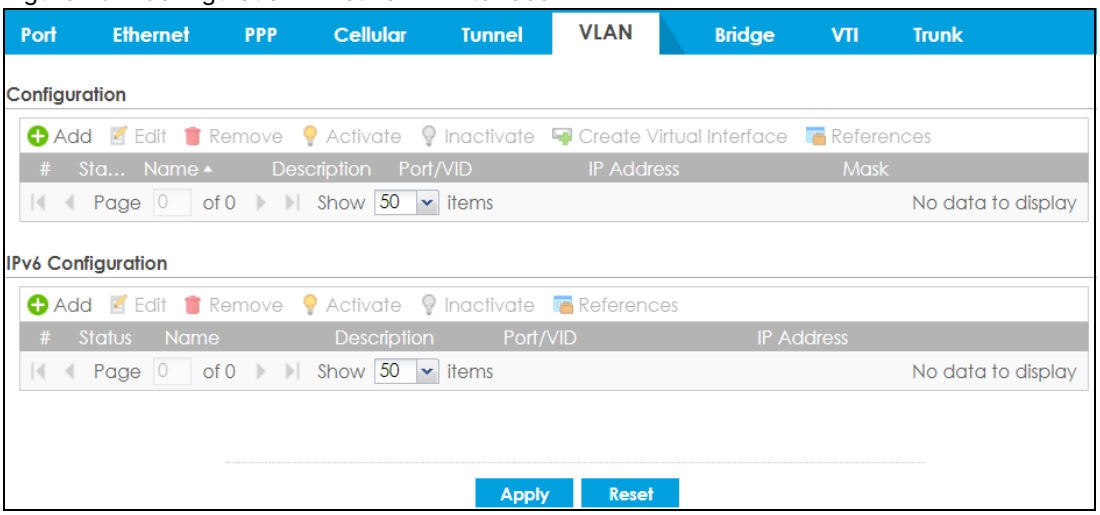
Note: Each VLAN interface is created on top of only one Ethernet interface.

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

11.9.1 VLAN Summary Screen

This screen lists every VLAN interface and virtual interface created on top of VLAN interfaces. If you enabled IPv6 on the Configuration > System > IPv6 screen, you can also configure VLAN interfaces used for your IPv6 networks on this screen. To access this screen, click Configuration > Network > Interface > VLAN.

Figure 261 Configuration > Network > Interface > VLAN



Each field is explained in the following table.

Table 88 Configuration > Network > Interface > VLAN

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 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.
Create Virtual Interface	To open the screen where you can create a virtual interface, select an 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 11.5.4 on page 314 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.
Port/VID	For VLAN interfaces, this field displays • the Ethernet interface on which the VLAN interface is created • the VLAN ID For virtual interfaces, this field is blank.
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet. This screen also shows whether the IP address is a static IP address (STATIC) or dynamically assigned (DHCP). IP addresses are always static in virtual interfaces.
Mask	This field displays the interface's subnet mask in dot decimal notation.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

11.9.2 VLAN Add/Edit

Select an existing entry on the previous screen and click Edit or click Add to create a new entry. The following screen appears.

Figure 262 Configuration > Network > Interface > VLAN > Add /Edit

Add VLAN

IPv4/IPv6 View ▼ Hide Advanced Settings Create New Object

General Settings

Enable Interface

General IPv6 Setting

Enable IPv6

Interface Properties

Interface Type: general

Interface Name: vlan

Zone: LAN1

Base Port: sfp

VLAN ID: (1-4094)

Advance

Priority Code: 0 (0-7)

Description: (Optional)

IP Address Assignment

Get Automatically

Advance

DHCP Option 60: (Optional)

Use Fixed IP Address

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: (Optional)

Metric: 0 (0-15)

Enable IGMP Support

IGMP Upstream

IGMP Downstream

IPv6 Address Assignment

Enable Stateless Address Auto-configuration (SLAAC)

Link-Local Address: n/a

IPv6 Address/Prefix Length: (Optional)

Advance

Gateway: (Optional)

Metric: (0-15)

Address from DHCPv6 Prefix Delegation

Add Edit Remove References

#	Delegated Prefix	Suffix Address	Address

Page 0 of 0 Show 50 items No data to display

DHCPv6 Setting

DHCPv6: N/A

IPv6 Router Advertisement Setting

Enable Router Advertisement

Advance

Advertised Hosts Get Network Configuration From DHCPv6

Advertised Hosts Get Other Configuration From DHCPv6

Router Preference: Medium

Advance

MTU: 1480 (1280-1500)

Hop Limit: 64 (1-255)

Advertised Prefix Table

Add Edit Remove

#	IPv6 Address/Prefix Length

Page 0 of 0 Show 50 items No data to display

Advance

Advertised Prefix from DHCPv6 Prefix Delegation

Add Edit Remove References

#	Delegated Prefix	Suffix Address	Address

Page 0 of 0 Show 50 items No data to display

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 0.0.0.0

Check These Addresses (Domain Name or IP Address)

(Optional)

Probe Succeeds When: any one respond(s)

DHCP Setting

DHCP: None

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

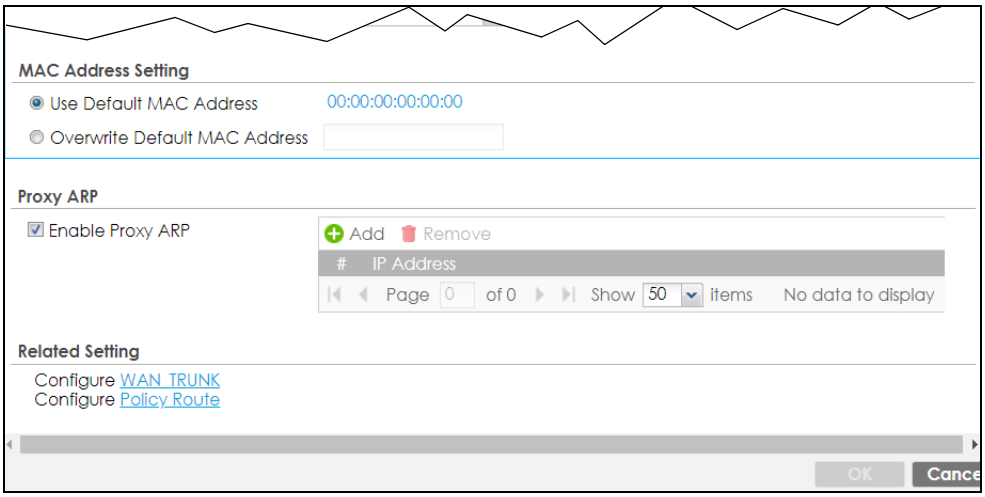
Area: none

Priority: 1 (0-255)

Link Cost: 10 (1-65535)

Passive Interface

Authentication: None



Each field is explained in the following table.

Table 89 Configuration > Network > Interface > VLAN > Add / Edit

LABEL	DESCRIPTION
IPv4/IPv6 View / IPv4 View / IPv6 View	Use this button to display both IPv4 and IPv6, IPv4-only, or IPv6-only configuration fields.
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create New Object	Click this button to create a DHCPv6 lease or DHCPv6 request object that you may use for the DHCPv6 settings in this screen.
General Settings	
Enable Interface	Select this to turn this interface on. Clear this to disable this interface.
General IPv6 Setting	
Enable IPv6	Select this to enable IPv6 on this interface. Otherwise, clear this to disable it.
Interface Properties	
Interface Type	Select one of the following option depending on the type of network to which the Zyxel Device is connected or if you want to additionally manually configure some related settings. internal is for connecting to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The Zyxel Device automatically adds default SNAT settings for traffic flowing from this interface to an external interface. external is for connecting to an external network (like the Internet). The Zyxel Device automatically adds this interface to the default WAN trunk. For general, the rest of the screen's options do not automatically adjust and you must manually configure a policy route to add routing and SNAT settings for the interface.
Interface Name	This field is read-only if you are editing an existing VLAN interface. Enter the number of the VLAN interface. You can use a number from 0~4094. For example, use vlan0, vlan8, and so on. The total number of VLANs you can configure on the Zyxel Device depends on the model.
Zone	Select the zone to which the VLAN interface belongs.
Base Port	Select the Ethernet interface on which the VLAN interface runs.
VLAN ID	Enter the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 - 4094. (0 and 4095 are reserved.)
Priority Code	This is a 3-bit field within a 802.1Q VLAN tag that's used to prioritize associated outgoing VLAN traffic. "0" is the lowest priority level and "7" is the highest. See Table 159 on page 530. The setting configured in Configuration > BWM overwrites the priority setting here.

Table 89 Configuration > Network > Interface > VLAN > Add / Edit (continued)

LABEL	DESCRIPTION
Description	Enter a description of this interface. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long. Spaces are allowed, but the string can't start with a space.
IP Address Assignment	
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address, subnet mask, and gateway automatically. You should not select this if the interface is assigned to a VRRP group.
DHCP Option 60	DHCP Option 60 is used by the Zyxel Device for identification to the DHCP server using the VCI (Vendor Class Identifier) on the DHCP server. The Zyxel Device adds it in the initial DHCP discovery message that a DHCP client broadcasts in search of an IP address. The DHCP server can assign different IP addresses or options to clients with the specific VCI or reject the request from clients without the specific VCI. Enter a string using up to 63 of these characters [a-zA-Z0-9!\"#$%&\'()*+,-./:;<=>?@\[\\\]^_`{}] to identify this Zyxel Device to the DHCP server. For example, Zyxel-TW.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	This field is enabled if you select Use Fixed IP Address. Enter the IP address for this interface.
Subnet Mask	This field is enabled if you select Use Fixed IP Address. Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers on the network.
Gateway	This field is enabled if you select Use Fixed IP Address. Enter the IP address of the gateway. The Zyxel Device sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
Enable IGMP Support	Select this to allow the Zyxel Device to act as an IGMP proxy for hosts connected on the IGMP downstream interface.
IGMP Upstream	Enable IGMP Upstream on the interface which connects to a router running IGMP that is closer to the multicast server.
IGMP Downstream	Enable IGMP Downstream on the interface which connects to the multicast hosts.
IPv6 Address Assignment	These IP address fields configure an IPv6 IP address on the interface itself.
Enable Stateless Address Auto-configuration (SLAAC)	Select this to enable IPv6 stateless auto-configuration on this interface. The interface will generate an IPv6 IP address itself from a prefix obtained from an IPv6 router on the network.
Link-Local address	This displays the IPv6 link-local address and the network prefix that the Zyxel Device generates itself for the interface.
IPv6 Address/ Prefix Length	Enter the IPv6 address and the prefix length for this interface if you want to configure a static IP address for this interface. This field is optional. The prefix length indicates what the left-most part of the IP address is the same for all computers on the network, that is, the network address.
Gateway	Enter the IPv6 address of the default outgoing gateway using colon (:) hexadecimal notation.

Table 89 Configuration > Network > Interface > VLAN > Add / Edit (continued)

LABEL	DESCRIPTION
Metric	Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
Address from DHCPv6 Prefix Delegation	Use this table to have the Zyxel Device obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ. You have to also enter a suffix address which is appended to the delegated prefix to form an address for this interface. See Prefix Delegation on page 289 for more information. To use prefix delegation, you must: • Create at least one DHCPv6 request object before configuring this table. • The external interface must be a DHCPv6 client. You must configure the DHCPv6 request options using a DHCPv6 request object with the type of prefix-delegation. • Assign the prefix delegation to an internal interface and enable router advertisement on that interface.
Add	Click this to create an entry.
Edit	Select an entry and click this to change the settings.
Remove	Select an entry and click this to delete it from this table.
References	Select an entry and click References to open a screen that shows which settings use the entry. See Section 11.5.4 on page 314 for an example.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use from the drop-down list.
Suffix Address	Enter the ending part of the IPv6 address, a slash (/), and the prefix length. The Zyxel Device will append it to the delegated prefix. For example, you got a delegated prefix of 2003:1234:5678/48. You want to configure an IP address of 2003:1234:5678:1111::1/128 for this interface, then enter ::1111:0:0:0:1/128 in this field.
Address	This field displays the combined IPv6 IP address for this interface. Note: This field displays the combined address after you click OK and reopen this screen.
DHCPv6 Setting	
DHCPv6	Select N/A to not use DHCPv6. Select Client to set this interface to act as a DHCPv6 client. Select Server to set this interface to act as a DHCPv6 server which assigns IP addresses and provides subnet mask, gateway, and DNS server information to clients. Select Relay to set this interface to route DHCPv6 requests to the DHCPv6 relay server you specify. The DHCPv6 server(s) may be on another network.
DUID	This field displays the DHCP Unique IDentifier (DUID) of the interface, which is unique and used for identification purposes when the interface is exchanging DHCPv6 messages with others. See DHCPv6 on page 289 for more information.
DUID as MAC	Select this to have the DUID generated from the interface's default MAC address.
Customized DUID	If you want to use a customized DUID, enter it here for the interface.
Enable Rapid Commit	Select this to shorten the DHCPv6 message exchange process from four to two steps. This function helps reduce heavy network traffic load. Note: Make sure you also enable this option in the DHCPv6 clients to make rapid commit work.

Table 89 Configuration > Network > Interface > VLAN > Add / Edit (continued)

LABEL	DESCRIPTION
Information Refresh Time	Enter the number of seconds a DHCPv6 client should wait before refreshing information retrieved from DHCPv6.
Request Address	This field is available if you set this interface to DHCPv6 Client. Select this to get an IPv6 IP address for this interface from the DHCP server. Clear this to not get any IP address information through DHCPv6.
DHCPv6 Request Options / DHCPv6 Lease Options	If this interface is a DHCPv6 client, use this section to configure DHCPv6 request settings that determine what additional information to get from the DHCPv6 server. If this interface is a DHCPv6 server, use this section to configure DHCPv6 lease settings that determine what to offer to the DHCPv6 clients.
Add	Click this to create an entry in this table. See Section 11.5.5 on page 315 for more information.
Remove	Select an entry and click this to delete it from this table.
References	Select an entry and click References to open a screen that shows which settings use the entry. See Section 11.5.4 on page 314 for an example.
#	This field is a sequential value, and it is not associated with any entry.
Name	This field displays the name of the DHCPv6 request or lease object.
Type	This field displays the type of the object.
Value	This field displays the IPv6 prefix that the Zyxel Device obtained from an uplink router (Server is selected) or will advertise to its clients (Client is selected).
Interface	When Relay is selected, select this checkbox and an interface from the drop-down list if you want to use it as the relay server.
Relay Server	When Relay is selected, select this checkbox and enter the IP address of a DHCPv6 server as the relay server.
IPv6 Router Advertisement Setting	
Enable Router Advertisement	Select this to enable this interface to send router advertisement messages periodically. See IPv6 Router Advertisement on page 289 for more information.
Advertised Hosts Get Network Configuration From DHCPv6	Select this to have the Zyxel Device indicate to hosts to obtain network settings (such as prefix and DNS settings) through DHCPv6. Clear this to have the Zyxel Device indicate to hosts that DHCPv6 is not available and they should use the prefix in the router advertisement message.
Advertised Hosts Get Other Configuration From DHCPv6	Select this to have the Zyxel Device indicate to hosts to obtain DNS information through DHCPv6. Clear this to have the Zyxel Device indicate to hosts that DNS information is not available in this network.
Router Preference	Select the router preference (Low, Medium or High) for the interface. The interface sends this preference in the router advertisements to tell hosts what preference they should use for the Zyxel Device. This helps hosts to choose their default router especially when there are multiple IPv6 router on the network. Note: Make sure the hosts also support router preference to make this function work.
MTU	The Maximum Transmission Unit. Enter the maximum size of each IPv6 data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device divides it into smaller fragments.
Hop Limit	Enter the maximum number of network segments that a packet can cross before reaching the destination. When forwarding an IPv6 packet, IPv6 routers are required to decrease the Hop Limit by 1 and to discard the IPv6 packet when the Hop Limit is 0.

Table 89 Configuration > Network > Interface > VLAN > Add / Edit (continued)

LABEL	DESCRIPTION
Advertised Prefix Table	Configure this table only if you want the Zyxel Device to advertise a fixed prefix to the network.
Add	Click this to create an IPv6 prefix address.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
IPv6 Address/ Prefix Length	Enter the IPv6 network prefix address and the prefix length. The prefix length indicates what the left-most part of the IP address is the same for all computers on the network, that is, the network address.
Advertised Prefix from DHCPv6 Prefix Delegation	Use this table to configure the network prefix if you want to use a delegated prefix as the beginning part of the network prefix.
Add	Click this to create an entry in this table.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
References	Select an entry and click References to open a screen that shows which settings use the entry. See Section 11.5.4 on page 314 for an example.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use for generating the network prefix for the network.
Suffix Address	Enter the ending part of the IPv6 network address plus a slash (/) and the prefix length. The Zyxel Device will append it to the selected delegated prefix. The combined address is the network prefix for the network. For example, you got a delegated prefix of 2003:1234:5678/48. You want to divide it into 2003:1234:5678:1111/64 for this interface and 2003:1234:5678:2222/64 for another interface. You can use ::1111/64 and ::2222/64 for the suffix address respectively. But if you do not want to divide the delegated prefix into subnetworks, enter ::0/48 here, which keeps the same prefix length (/48) as the delegated prefix.
Address	This is the final network prefix combined by the delegated prefix and the suffix. Note: This field displays the combined address after you click OK and reopen this screen.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Enter the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
Connectivity Check	The Zyxel Device can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often to check the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the Zyxel Device stops routing to the gateway. The Zyxel Device resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.

Table 89 Configuration > Network > Interface > VLAN > Add / Edit (continued)

LABEL	DESCRIPTION
Check Method	Select the method that the gateway allows. Select icmp to have the Zyxel Device regularly ping the gateway you specify to make sure it is still available. Select tcp to have the Zyxel Device regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the Zyxel Device stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the Check Method to tcp. Specify the port number to use for a TCP connectivity check.
Check these addresses	Enter one or two domain names or IP addresses for the connectivity check.
Probe Succeeds When	This field applies when you specify two domain names or IP addresses for the connectivity check. Select any one if you want the check to pass if at least one of the domain names or IP addresses responds. Select all if you want the check to pass only if both domain names or IP addresses respond.
DHCP Setting	The DHCP settings are available for the OPT, LAN and DMZ interfaces.
DHCP	Select what type of DHCP service the Zyxel Device provides to the network. Choices are: None - the Zyxel Device does not provide any DHCP services. There is already a DHCP server on the network. DHCP Relay - the Zyxel Device routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. DHCP Server - the Zyxel Device assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The Zyxel Device is the DHCP server for the network.
	These fields appear if the Zyxel Device is a DHCP Relay.
Relay Server 1	Enter the IP address of a DHCP server for the network.
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.
	These fields appear if the Zyxel Device is a DHCP Server.
IP Pool Start Address	Enter the IP address from which the Zyxel Device begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click Add Static DHCP. If this field is blank, the Pool Size must also be blank. In this case, the Zyxel Device can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.

Table 89 Configuration > Network > Interface > VLAN > Add / Edit (continued)

LABEL	DESCRIPTION
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's Subnet Mask. For example, if the Subnet Mask is 255.255.255.0 and IP Pool Start Address is 10.10.10.10, the Zyxel Device can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses. If this field is blank, the IP Pool Start Address must also be blank. In this case, the Zyxel Device can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
First DNS Server Second DNS Server Third DNS Server	Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. Custom Defined - enter a static IP address. From ISP - select the DNS server that another interface received from its DHCP server. Zyxel Device - the DHCP clients use the IP address of this interface and the Zyxel Device works as a DNS relay.
First WINS Server, Second WINS Server	Enter the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Default Router	If you set this interface to DHCP Server, you can select to use either the interface's IP address or another IP address as the default router. This default router will become the DHCP clients' default gateway. To use another IP address as the default router, select Custom Defined and enter the IP address.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: infinite - select this if IP addresses never expire days, hours, and minutes - select this to enter how long IP addresses are valid. The default is 2 days.
Extended Options	This table is available if you selected DHCP server. Configure this table if you want to send more information to DHCP clients through DHCP packets.
Add	Click this to create an entry in this table. See Section 11.5.6 on page 316.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
Name	This is the option's name.
Code	This is the option's code number.
Type	This is the option's type.
Value	This is the option's value.
Enable IP/MAC Binding	Select this option to have the Zyxel Device enforce links between specific IP addresses and specific MAC addresses for this VLAN. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.
Enable Logs for IP/MAC Binding Violation	Select this option to have the Zyxel Device generate a log if a device connected to this VLAN attempts to use an IP address that is bound to another device's MAC address.
Static DHCP Table	Configure a list of static IP addresses the Zyxel Device assigns to computers connected to the interface. Otherwise, the Zyxel Device assigns an IP address dynamically using the interface's IP Pool Start Address and Pool Size.

Table 89 Configuration > Network > Interface > VLAN > Add / Edit (continued)

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Import	Click this to import a previously saved file (.csv) to the Zyxel Device. The IP/MAC binding settings and description to identify these settings in the file will be applied to the Zyxel Device. The previously saved csv file may be a file you configured, or a file you exported at Monitor> System Status> DHCP Table if you want to recover settings configured before. Configure your csv file in the order of IP address, MAC address and description. Spaces are allowed. Separate each item with a comma, for example, 1.1.1.1,22:22:33:44:55:02,test. Press enter to configure the next group in a new line. Your currently configured IP/MAC binding settings and entries description will be overwritten once you import the file. Make sure to click Export to export your settings as a file for backup in Monitor> System Status> DHCP Table first.
File Path	Enter the file path and name of the DHCP settings file you want to import in the text box (or click Browse to find it on your computer) and then click Upload to transfer the file to the Zyxel Device.
#	This field is a sequential value, and it is not associated with a specific entry.
IP Address	Enter the IP address to assign to a device with this entry's MAC address.
MAC	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
RIP Setting	See Section 12.6 on page 399 for more information about RIP.
Enable RIP	Select this to enable RIP on this interface.
Direction	This field is effective when RIP is enabled. Select the RIP direction from the drop-down list box. BiDir - This interface sends and receives routing information. In-Only - This interface receives routing information. Out-Only - This interface sends routing information.
Send Version	This field is effective when RIP is enabled. Select the RIP version(s) used for sending RIP packets. Choices are 1, 2, and 1 and 2.
Receive Version	This field is effective when RIP is enabled. Select the RIP version(s) used for receiving RIP packets. Choices are 1, 2, and 1 and 2.
V2-Broadcast	This field is effective when RIP is enabled. Select this to send RIP-2 packets using subnet broadcasting; otherwise, the Zyxel Device uses multicasting.
OSPF Setting	See Section 12.7 on page 401 for more information about OSPF.
Area	Select the area in which this interface belongs. Select None to disable OSPF in this interface.
Priority	Enter the priority (between 0 and 255) of this interface when the area is looking for a Designated Router (DR) or Backup Designated Router (BDR). The highest-priority interface identifies the DR, and the second-highest-priority interface identifies the BDR. Set the priority to zero if the interface can not be the DR or BDR.
Link Cost	Enter the cost (between 1 and 65,535) to route packets through this interface.
Passive Interface	Select this to stop forwarding OSPF routing information from the selected interface. As a result, this interface only receives routing information.

Table 89 Configuration > Network > Interface > VLAN > Add / Edit (continued)

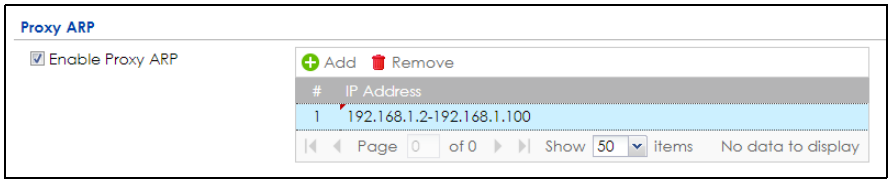
LABEL	DESCRIPTION
Authentication	Select an authentication method, or disable authentication. To exchange OSPF routing information with peer border routers, you must use the same authentication method that they use. Choices are: Same-as-Area - use the default authentication method in the area None - disable authentication Text - authenticate OSPF routing information using a plain-text password MD5 - authenticate OSPF routing information using MD5 encryption
Text Authentication Key	This field is available if the Authentication is Text. Enter the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MD5 Authentication ID	This field is available if the Authentication is MD5. Enter the ID for MD5 authentication. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the Authentication is MD5. Enter the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MAC Address Setting	This section appears when Interface Properties is External or General. Have the interface use either the factory assigned default MAC address, a manually specified MAC address, or clone the MAC address of another device or computer.
Use Default MAC Address	Select this option to have the interface use the factory assigned default MAC address. By default, the Zyxel Device uses the factory assigned MAC address to identify itself.
Overwrite Default MAC Address	Select this option to have the interface use a different MAC address. Either the MAC address in the field. Once it is successfully configured, the address will be copied to the configuration file. It will not change unless you change the setting or upload a different configuration file.
Proxy ARP	Proxy ARP is available for external or general interfaces on the Zyxel Device. See Section on page 303 for more information on Proxy ARP.
Enable Proxy ARP	Select this to allow the Zyxel Device to answer external interface ARP requests on behalf of a device on its internal interface. Interfaces supported are: • Ethernet • VLAN • Bridge See Section 11.5.2 on page 312 for more information.
Add	Click Add to create an IPv4 Address, an IPv4 CIDR (for example, 192.168.1.1/24) or an IPv4 Range (for example, 192.168.1.2-192.168.1.100) as the target IP address. The Zyxel Device answers external ARP requests only if they match one of these inputted target IP addresses. For example, if the IPv4 Address is 192.168.1.5, then the Zyxel Device will answer ARP requests coming from the WAN only if it contains 192.168.1.5 as the target IP address. Select an existing entry and click Remove to delete that entry. 
Related Setting	
Configure WAN TRUNK	Click WAN TRUNK to go to a screen where you can set this VLAN to be part of a WAN trunk for load balancing.
Configure Policy Route	Click Policy Route to go to the screen where you can manually configure a policy route to associate traffic with this VLAN.

Table 89 Configuration > Network > Interface > VLAN > Add / Edit (continued)

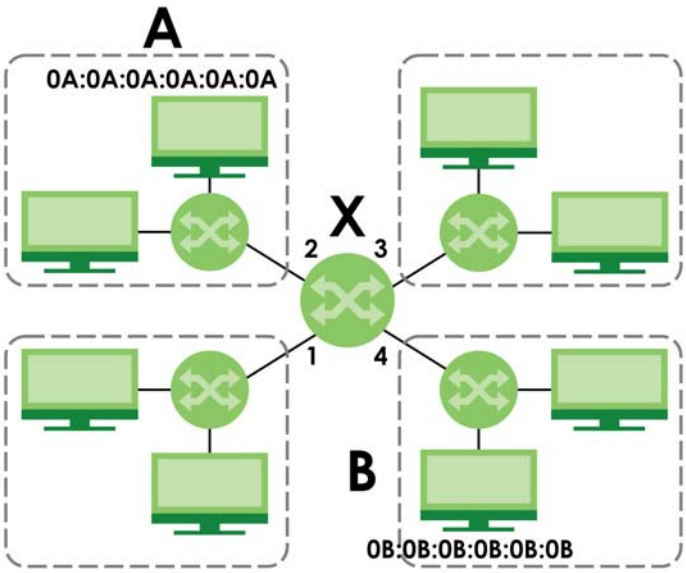
LABEL	DESCRIPTION
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

11.10 Bridge Interfaces

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

Bridge Overview

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



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

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

Table 90 Example: Bridge Table After Computer A Sends a Packet to Computer B

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

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

Table 91 Example: Bridge Table After Computer B Responds to Computer A

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

Bridge Interface Overview

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

Unlike the device-wide bridge mode in ZyNoS-based Zyxel Devices, this Zyxel Device can bridge traffic between some interfaces while it routes traffic for other interfaces. The bridge interfaces also support more functions, like interface bandwidth parameters, DHCP settings, and connectivity check. To use the whole Zyxel Device as a transparent bridge, add all of the Zyxel Device's interfaces to a bridge interface.

A bridge interface may consist of the following members:

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

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

Table 92 Example: Routing Table Before and After Bridge Interface br0 Is Created

IP ADDRESS(ES)	DESTINATION
210.210.210.0/24	lan1
210.211.1.0/24	lan1:1
221.221.221.0/24	vlan0
222.222.222.0/24	vlan1
230.230.230.192/26	wan2
241.241.241.241/32	dmz
242.242.242.242/32	dmz

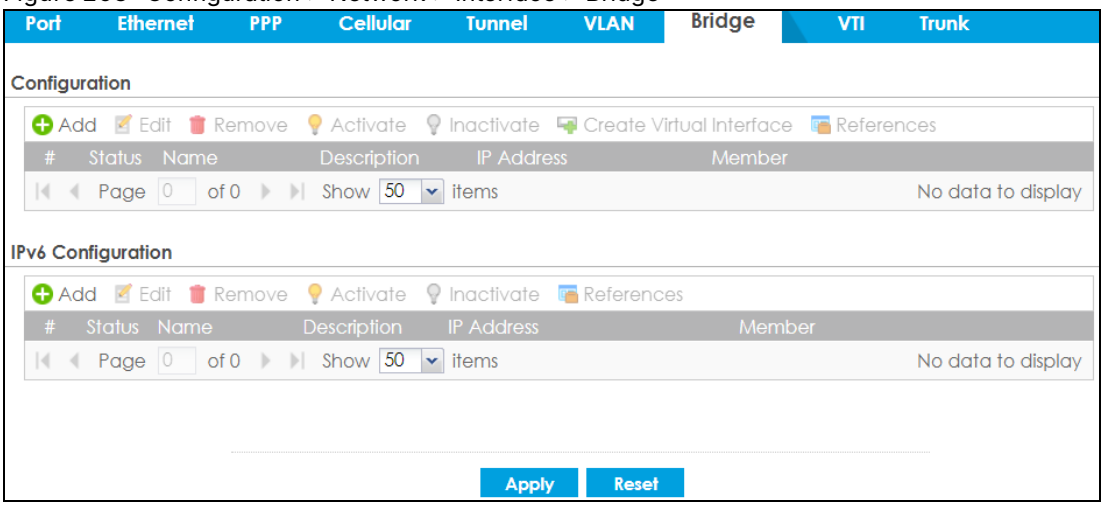
IP ADDRESS(ES)	DESTINATION
221.221.221.0/24	vlan0
230.230.230.192/26	wan2
241.241.241.241/32	dmz
242.242.242.242/32	dmz
250.250.250.0/23	br0

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

11.10.1 Bridge Summary

This screen lists every bridge interface and virtual interface created on top of bridge interfaces. If you enabled IPv6 on the Configuration > System > IPv6 screen, you can also configure bridge interfaces used for your IPv6 network on this screen. To access this screen, click Configuration > Network > Interface > Bridge.

Figure 263 Configuration > Network > Interface > Bridge



Each field is described in the following table.

Table 93 Configuration > Network > Interface > Bridge

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.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The 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.
Create Virtual Interface	To open the screen where you can create a virtual interface, select an 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 11.5.4 on page 314 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.
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet. This screen also shows whether the IP address is a static IP address (STATIC) or dynamically assigned (DHCP). IP addresses are always static in virtual interfaces.
Member	This field displays the Ethernet interfaces and VLAN interfaces in the bridge interface. It is blank for virtual interfaces.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

11.10.2 Bridge Add/Edit

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

Figure 264 Configuration > Network > Interface > Bridge > Add / Edit

Add Bridge

IPv4/IPv6 View ▼ Hide Advanced Settings Create New Object

General Settings

Enable Interface

General IPv6 Setting

Enable IPv6

Interface Properties

Interface Type: general

Interface Name: br

Zone: LAN1

Description: (Optional)

Member Configuration

Available	Member
sfp	
wan	
lan1	
lan2	
dmz	
opt	

IP Address Assignment

Get Automatically

Advance

DHCP Option 60: (Optional)

Use Fixed IP Address

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: (Optional)

Metric: 0 (0-15)

Enable IGMP Support

IGMP Upstream

IGMP Downstream

IPv6 Address Assignment

Enable Stateless Address Auto-configuration (SLAAC)

Link-Local Address: n/a

IPv6 Address/Prefix Length: (Optional)

Advance

Gateway: (Optional)

Metric: (0-15)

Address from DHCPv6 Prefix Delegation

Add Edit Remove References

#	Delegated Prefix	Suffix Address	Addr...

Page 0 of 0 Show 50 items No data to display

DHCPv6 Setting

DHCPv6: N/A

IPv6 Router Advertisement Setting

Enable Router Advertisement

Advance
- Advertised Hosts Get Network Configuration From DHCPv6
- Advertised Hosts Get Other Configuration From DHCPv6

Router Preference: Medium

Advance
MTU: 1480 (1280-1500)
Hop Limit: 64 (1-255)

Advertised Prefix Table
Add Edit Remove

#	IPv6 Address/Prefix Length
Page 0 of 0 Show 50 items	No data to display

Advance
Advertised Prefix from DHCPv6 Prefix Delegation
Add Edit Remove References

#	Delegated Prefix	Suffix Address	Addr...
Page 0 of 0 Show 50 items			No data to display

Advance

Interface Parameters
Egress Bandwidth: 1048576 Kbps
Ingress Bandwidth: 1048576 Kbps
MTU: 1500 Bytes

DHCP Setting
DHCP: None
- 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

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 0.0.0.0
- Check These Addresses (Domain Name or IP Address) (Optional)

Probe Succeeds When: any one respond(s)

Proxy ARP
- Enable Proxy ARP

Add Remove

#	IP Address
Page 0 of 0 Show 50 items	No data to display

Related Setting
Configure WAN_TRUNK
Configure Policy Route

OK Cancel

Each field is described in the table below.

Table 94 Configuration > Network > Interface > Bridge > Add / Edit

LABEL	DESCRIPTION
IPv4/IPv6 View / IPv4 View / IPv6 View	Use this button to display both IPv4 and IPv6, IPv4-only, or IPv6-only configuration fields.
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create New Object	Click this button to create a DHCPv6 lease or DHCPv6 request object that you may use for the DHCPv6 settings in this screen.
General Settings	
Enable Interface	Select this to enable this interface. Clear this to disable this interface.
General IPv6 Setting	
Enable IPv6	Select this to enable IPv6 on this interface. Otherwise, clear this to disable it.
Interface Properties	
Interface Type	Select one of the following option depending on the type of network to which the Zyxel Device is connected or if you want to additionally manually configure some related settings. internal is for connecting to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The Zyxel Device automatically adds default SNAT settings for traffic flowing from this interface to an external interface. external is for connecting to an external network (like the Internet). The Zyxel Device automatically adds this interface to the default WAN trunk. For general, the rest of the screen's options do not automatically adjust and you must manually configure a policy route to add routing and SNAT settings for the interface.
Interface Name	This field is read-only if you are editing the interface. Enter the name of the bridge interface. The format is br*x*, where *x* is 0 - 11. For example, br0, br3, and so on.
Zone	Select the zone to which the interface is to belong. You use zones to apply security settings such as security policy and remote management.
Description	Enter a description of this interface. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long. Spaces are allowed, but the string can't start with a space.
Member Configuration	
Available	This field displays Ethernet interfaces and VLAN interfaces that can become part of the bridge interface. An interface is not available in the following situations: • There is a virtual interface on top of it • It is already used in a different bridge interface Select one, and click the >> arrow to add it to the bridge interface. Each bridge interface can only have one VLAN interface.
Member	This field displays the interfaces that are part of the bridge interface. Select one, and click the << arrow to remove it from the bridge interface.
IP Address Assignment	
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address, subnet mask, and gateway automatically.

Table 94 Configuration > Network > Interface > Bridge > Add / Edit (continued)

LABEL	DESCRIPTION
DHCP Option 60	DHCP Option 60 is used by the Zyxel Device for identification to the DHCP server using the VCI (Vendor Class Identifier) on the DHCP server. The Zyxel Device adds it in the initial DHCP discovery message that a DHCP client broadcasts in search of an IP address. The DHCP server can assign different IP addresses or options to clients with the specific VCI or reject the request from clients without the specific VCI. Enter a string using up to 63 of these characters [a-zA-Z0-9!\"#$%&\'()*+,-./ :;<=>?@\[\\\]^_`{}] to identify this Zyxel Device to the DHCP server. For example, Zyxel-TW.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	This field is enabled if you select Use Fixed IP Address. Enter the IP address for this interface.
Subnet Mask	This field is enabled if you select Use Fixed IP Address. Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers on the network.
Gateway	This field is enabled if you select Use Fixed IP Address. Enter the IP address of the gateway. The Zyxel Device sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
Enable IGMP Support	Select this to allow the Zyxel Device to act as an IGMP proxy for hosts connected on the IGMP downstream interface.
IGMP Upstream	Enable IGMP Upstream on the interface which connects to a router running IGMP that is closer to the multicast server.
IGMP Downstream	Enable IGMP Downstream on the interface which connects to the multicast hosts.
IPv6 Address Assignment	These IP address fields configure an IPv6 IP address on the interface itself.
Enable Stateless Address Auto-configuration (SLAAC)	Select this to enable IPv6 stateless auto-configuration on this interface. The interface will generate an IPv6 IP address itself from a prefix obtained from an IPv6 router on the network.
Link-Local address	This displays the IPv6 link-local address and the network prefix that the Zyxel Device generates itself for the interface.
IPv6 Address/ Prefix Length	Enter the IPv6 address and the prefix length for this interface if you want to use a static IP address. This field is optional. The prefix length indicates what the left-most part of the IP address is the same for all computers on the network, that is, the network address.
Gateway	Enter the IPv6 address of the default outgoing gateway using colon (:) hexadecimal notation.
Metric	Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.

Table 94 Configuration > Network > Interface > Bridge > Add / Edit (continued)

LABEL	DESCRIPTION
Address from DHCPv6 Prefix Delegation	Use this table to have the Zyxel Device obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ. You have to also enter a suffix address which is appended to the delegated prefix to form an address for this interface. See Prefix Delegation on page 289 for more information. To use prefix delegation, you must: • Create at least one DHCPv6 request object before configuring this table. • The external interface must be a DHCPv6 client. You must configure the DHCPv6 request options using a DHCPv6 request object with the type of prefix-delegation. • Assign the prefix delegation to an internal interface and enable router advertisement on that interface.
Add	Click this to create an entry.
Edit	Select an entry and click this to change the settings.
Remove	Select an entry and click this to delete it from this table.
References	Select an entry and click References to open a screen that shows which settings use the entry. See Section 11.5.4 on page 314 for an example.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use from the drop-down list.
Suffix Address	Enter the ending part of the IPv6 address, a slash (/), and the prefix length. The Zyxel Device will append it to the delegated prefix. For example, you got a delegated prefix of 2003:1234:5678/48. You want to configure an IP address of 2003:1234:5678:1111:1/128 for this interface, then enter ::1111:0:0:0:1/128 in this field.
Address	This field displays the combined IPv6 IP address for this interface. Note: This field displays the combined address after you click OK and reopen this screen.
DHCPv6 Setting	
DHCPv6	Select N/A to not use DHCPv6. Select Client to set this interface to act as a DHCPv6 client. Select Server to set this interface to act as a DHCPv6 server which assigns IP addresses and provides subnet mask, gateway, and DNS server information to clients. Select Relay to set this interface to route DHCPv6 requests to the DHCPv6 relay server you specify. The DHCPv6 server(s) may be on another network.
DUID	This field displays the DHCP Unique IDentifier (DUID) of the interface, which is unique and used for identification purposes when the interface is exchanging DHCPv6 messages with others. See DHCPv6 on page 289 for more information.
DUID as MAC	Select this if you want the DUID is generated from the interface's default MAC address.
Customized DUID	If you want to use a customized DUID, enter it here for the interface.
Enable Rapid Commit	Select this to shorten the DHCPv6 message exchange process from four to two steps. This function helps reduce heavy network traffic load. Note: Make sure you also enable this option in the DHCPv6 clients to make rapid commit work.
Information Refresh Time	Enter the number of seconds a DHCPv6 client should wait before refreshing information retrieved from DHCPv6.
Request Address	This field is available if you set this interface to DHCPv6 Client. Select this to get an IPv6 IP address for this interface from the DHCP server. Clear this to not get any IP address information through DHCPv6.

Table 94 Configuration > Network > Interface > Bridge > Add / Edit (continued)

LABEL	DESCRIPTION
DHCPv6 Request Options / DHCPv6 Lease Options	If this interface is a DHCPv6 client, use this section to configure DHCPv6 request settings that determine what additional information to get from the DHCPv6 server. If the interface is a DHCPv6 server, use this section to configure DHCPv6 lease settings that determine what to offer to the DHCPv6 clients.
Add	Click this to create an entry in this table. See Section 11.5.5 on page 315 for more information.
Edit	Select an entry and click this to change the settings.
Remove	Select an entry and click this to delete it from this table.
References	Select an entry and click References to open a screen that shows which settings use the entry. See Section 11.5.4 on page 314 for an example.
#	This field is a sequential value, and it is not associated with any entry.
Name	This field displays the name of the DHCPv6 request or lease object.
Type	This field displays the type of the object.
Value	This field displays the IPv6 prefix that the Zyxel Device obtained from an uplink router (Server is selected) or will advertise to its clients (Client is selected).
Interface	When Relay is selected, select this checkbox and an interface from the drop-down list if you want to use it as the relay server.
Relay Server	When Relay is selected, select this checkbox and enter the IP address of a DHCPv6 server as the relay server.
IPv6 Router Advertisement Setting	
Enable Router Advertisement	Select this to enable this interface to send router advertisement messages periodically. See IPv6 Router Advertisement on page 289 for more information.
Advertised Hosts Get Network Configuration From DHCPv6	Select this to have the Zyxel Device indicate to hosts to obtain network settings (such as prefix and DNS settings) through DHCPv6. Clear this to have the Zyxel Device indicate to hosts that DHCPv6 is not available and they should use the prefix in the router advertisement message.
Advertised Hosts Get Other Configuration From DHCPv6	Select this to have the Zyxel Device indicate to hosts to obtain DNS information through DHCPv6. Clear this to have the Zyxel Device indicate to hosts that DNS information is not available in this network.
Router Preference	Select the router preference (Low, Medium or High) for the interface. The interface sends this preference in the router advertisements to tell hosts what preference they should use for the Zyxel Device. This helps hosts to choose their default router especially when there are multiple IPv6 router on the network. Note: Make sure the hosts also support router preference to make this function work.
MTU	The Maximum Transmission Unit. Enter the maximum size of each IPv6 data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device divides it into smaller fragments.
Hop Limit	Enter the maximum number of network segments that a packet can cross before reaching the destination. When forwarding an IPv6 packet, IPv6 routers are required to decrease the Hop Limit by 1 and to discard the IPv6 packet when the Hop Limit is 0.
Advertised Prefix Table	Configure this table only if you want the Zyxel Device to advertise a fixed prefix to the network.
Add	Click this to create an IPv6 prefix address.
Edit	Select an entry in this table and click this to modify it.

Table 94 Configuration > Network > Interface > Bridge > Add / Edit (continued)

LABEL	DESCRIPTION
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
IPv6 Address/ Prefix Length	Enter the IPv6 network prefix address and the prefix length. The prefix length indicates what the left-most part of the IP address is the same for all computers on the network, that is, the network address.
Advertised Prefix from DHCPv6 Prefix Delegation	Use this table to configure the network prefix if you want to use a delegated prefix as the beginning part of the network prefix.
Add	Click this to create an entry in this table.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
References	Select an entry and click References to open a screen that shows which settings use the entry. See Section 11.5.4 on page 314 for an example.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use for generating the network prefix for the network.
Suffix Address	Enter the ending part of the IPv6 network address plus a slash (/) and the prefix length. The Zyxel Device will append it to the selected delegated prefix. The combined address is the network prefix for the network. For example, you got a delegated prefix of 2003:1234:5678/48. You want to divide it into 2003:1234:5678:1111/64 for this interface and 2003:1234:5678:2222/64 for another interface. You can use ::1111/64 and ::2222/64 for the suffix address respectively. But if you do not want to divide the delegated prefix into subnetworks, enter ::0/48 here, which keeps the same prefix length (/48) as the delegated prefix.
Address	This is the final network prefix combined by the selected delegated prefix and the suffix. Note: This field displays the combined address after you click OK and reopen this screen.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Enter the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
DHCP Setting	
DHCP	Select what type of DHCP service the Zyxel Device provides to the network. Choices are: None - the Zyxel Device does not provide any DHCP services. There is already a DHCP server on the network. DHCP Relay - the Zyxel Device routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. DHCP Server - the Zyxel Device assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The Zyxel Device is the DHCP server for the network.
	These fields appear if the Zyxel Device is a DHCP Relay.
Relay Server 1	Enter the IP address of a DHCP server for the network.

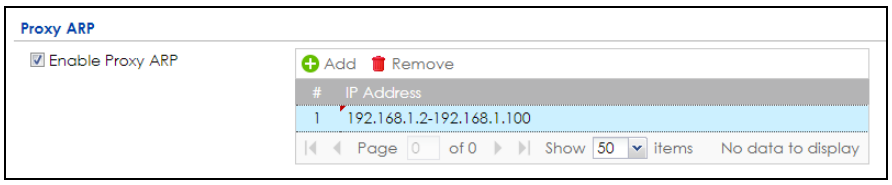
Table 94 Configuration > Network > Interface > Bridge > Add / Edit (continued)

LABEL	DESCRIPTION
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.
	These fields appear if the Zyxel Device is a DHCP Server.
IP Pool Start Address	Enter the IP address from which the Zyxel Device begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click Add Static DHCP. If this field is blank, the Pool Size must also be blank. In this case, the Zyxel Device can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's Subnet Mask. For example, if the Subnet Mask is 255.255.255.0 and IP Pool Start Address is 10.10.10.10, the Zyxel Device can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses. If this field is blank, the IP Pool Start Address must also be blank. In this case, the Zyxel Device can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
First DNS Server Second DNS Server Third DNS Server	Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. Custom Defined - enter a static IP address. From ISP - select the DNS server that another interface received from its DHCP server. Zyxel Device - the DHCP clients use the IP address of this interface and the Zyxel Device works as a DNS relay.
First WINS Server, Second WINS Server	Enter the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Default Router	If you set this interface to DHCP Server, you can select to use either the interface's IP address or another IP address as the default router. This default router will become the DHCP clients' default gateway. To use another IP address as the default router, select Custom Defined and enter the IP address.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: infinite - select this if IP addresses never expire days, hours, and minutes - select this to enter how long IP addresses are valid.
Extended Options	This table is available if you selected DHCP server. Configure this table if you want to send more information to DHCP clients through DHCP packets.
Add	Click this to create an entry in this table. See Section 11.5.6 on page 316.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
Name	This is the option's name.
Code	This is the option's code number.
Type	This is the option's type.
Value	This is the option's value.

Table 94 Configuration > Network > Interface > Bridge > Add / Edit (continued)

LABEL	DESCRIPTION
PXE Server	PXE (Preboot eXecution Environment) allows a client computer to use the network to boot up and install an operating system through a PXE-capable Network Interface Card (NIC). PXE is available for computers on internal interfaces to allow them to boot up using boot software on a PXE server. The Zyxel Device acts as an intermediary between the PXE server and the computers that need boot software. The PXE server must have a public IPv4 address. You must enable DHCP Server on the Zyxel Device so that it can receive information from the PXE server.
PXE Boot Loader File	A boot loader is a computer program that loads the operating system for the computer. Enter the exact file name of the boot loader software file, including filename extension, that is on the PXE server. If the wrong filename is entered, then the client computers cannot boot.
Enable IP/MAC Binding	Select this option to have this interface enforce links between specific IP addresses and specific MAC addresses. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.
Enable Logs for IP/MAC Binding Violation	Select this option to have the Zyxel Device generate a log if a device connected to this interface attempts to use an IP address that is bound to another device's MAC address.
Static DHCP Table	Configure a list of static IP addresses the Zyxel Device assigns to computers connected to the interface. Otherwise, the Zyxel Device assigns an IP address dynamically using the interface's IP Pool Start Address and Pool Size.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific entry.
IP Address	Enter the IP address to assign to a device with this entry's MAC address.
MAC Address	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
Connectivity Check	The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the Zyxel Device stops routing to the gateway. The Zyxel Device resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select icmp to have the Zyxel Device regularly ping the gateway you specify to make sure it is still available. Select tcp to have the Zyxel Device regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the Zyxel Device stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.

Table 94 Configuration > Network > Interface > Bridge > Add / Edit (continued)

LABEL	DESCRIPTION
Check Port	This field only displays when you set the Check Method to tcp. Specify the port number to use for a TCP connectivity check.
Check these addresses	Enter one or two domain names or IP addresses for the connectivity check.
Probe Succeeds When	This field applies when you specify two domain names or IP addresses for the connectivity check. Select any one if you want the check to pass if at least one of the domain names or IP addresses responds. Select all if you want the check to pass only if both domain names or IP addresses respond.
Proxy ARP	Proxy ARP is available for external or general interfaces on the Zyxel Device. See Section on page 303 for more information on Proxy ARP.
Enable Proxy ARP	Select this to allow the Zyxel Device to answer external interface ARP requests on behalf of a device on its internal interface. Interfaces supported are: • Ethernet • VLAN • Bridge See Section 11.5.2 on page 312 for more information.
Add	Click Add to create an IPv4 Address, an IPv4 CIDR (for example, 192.168.1.1/24) or an IPv4 Range (for example, 192.168.1.2-192.168.1.100) as the target IP address. The Zyxel Device answers external ARP requests only if they match one of these inputted target IP addresses. For example, if the IPv4 Address is 192.168.1.5, then the Zyxel Device will answer ARP requests coming from the WAN only if it contains 192.168.1.5 as the target IP address. Select an existing entry and click Remove to delete that entry. 
Related Setting	
Configure WAN TRUNK	Click WAN TRUNK to go to a screen where you can configure the interface as part of a WAN trunk for load balancing.
Configure Policy Route	Click Policy Route to go to the screen where you can manually configure a policy route to associate traffic with this bridge interface.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

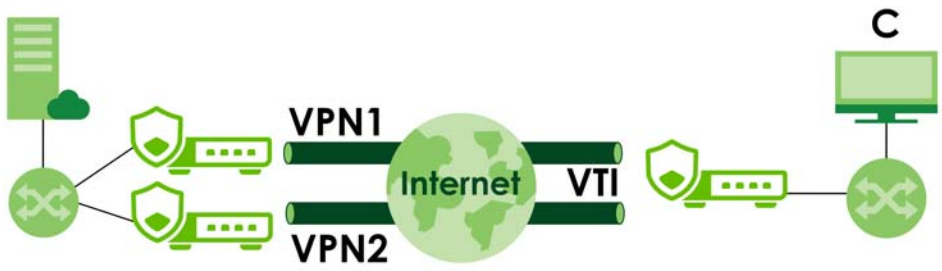
11.11 VTI

IPSec VPN Tunnel Interface (VTI) encrypts or decrypts IPv4 traffic from or to the interface according to the IP routing table.

VTI allows static routes to send traffic over the VPN. The IPSec tunnel endpoint is associated with an actual (virtual) interface. Therefore many interface capabilities such as Policy Route, Static Route, Trunk, and BWM can be applied to the IPSec tunnel as soon as the tunnel is active

IPSec VTI simplifies network management and load balancing. Create a trunk using VPN tunnel interfaces for load balancing. In the following example configure VPN tunnels with static IP addresses or DNS on both Zyxel Devices (or IPSec routers at the end of the tunnel). Also configure VTI and a trunk on both Zyxel Devices.

Figure 265 VTI and Trunk for VPN Load Balancing



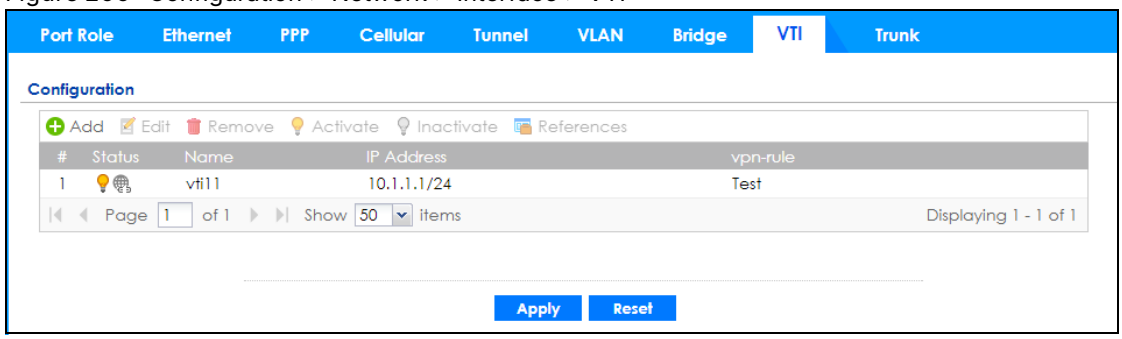
11.11.1 Restrictions for IPSec Virtual Tunnel Interface

- IPv4 traffic only
- IPSec tunnel mode only. A shared keyword must not be configured when using tunnel mode.
- With a VTI VPN you do not add local or remote LANs to your VPN configuration.
- For a VTI VPN you should only have one local and one remote WAN.
- A dynamic peer is not supported
- The IPSec VTI is limited to IP unicast and multicast traffic only.

11.11.2 VTI Screen

To access this screen, click Configuration > Network > Interface > VTI.

Figure 266 Configuration > Network > Interface > VTI



The following table describes the fields in this screen.

Table 95 Configuration > Network > Interface > VTI

LABEL	DESCRIPTION
Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.

Table 95 Configuration > Network > Interface > VTI (continued)

LABEL	DESCRIPTION
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.
References	Select an entry and click References to open a screen that shows which settings use the entry.
#	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 VTI interface.
IP Address	This field displays the current IP address of the virtual interface and subnet mask in bits. If the IP address is 0.0.0.0, the interface does not have an IP address yet.
vpn-rule	This shows the name of the associated IPSec VPN rule with VPN Tunnel Interface application scenario.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

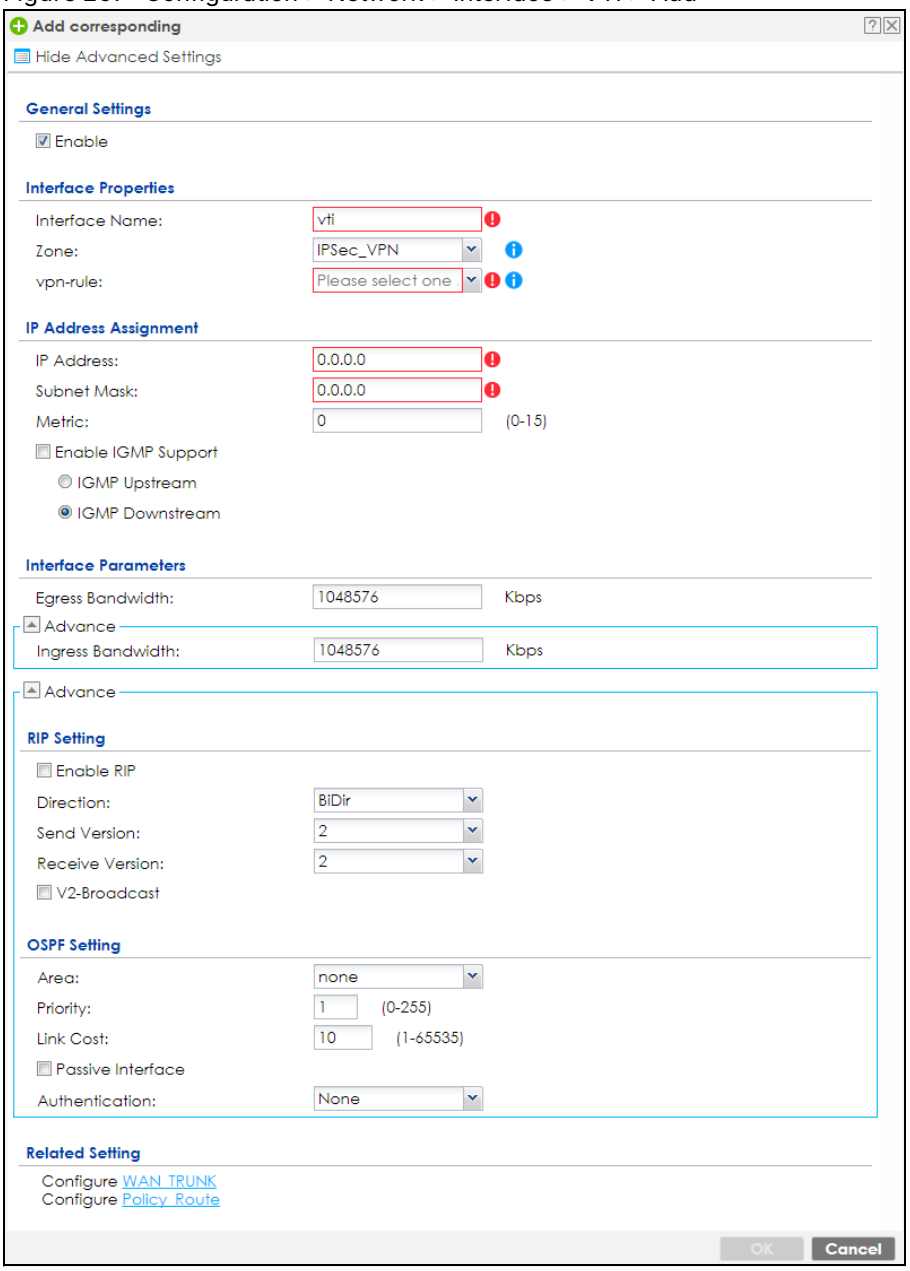
11.11.3 VTI Add/Edit

This screen lets you configure IP address assignment and interface parameters for VTI.

Note: You should have created a VPN tunnel for a VPN Tunnel Interface scenario first.

To access this screen, click the Add or Edit icon in Network > Interface > VTI. The following screen appears.

Figure 267 Configuration > Network > Interface > VTI > Add



Each field is described in the table below.

Table 96 Configuration > Network > Interface > VTI > Add

LABEL	DESCRIPTION
General Settings	
Enable	Select this to enable VTI. Clear this to disable it.
Interface Properties	
Interface Name	This field is read-only if you are editing an existing VPN tunnel interface. For a new VPN tunnel interface, enter the name of the VPN tunnel interface in vtix format, where x is a number from 0 to the maximum number of VPN connections allowed for this model. For example, enter vti10.

Table 96 Configuration > Network > Interface > VTI > Add (continued)

LABEL	DESCRIPTION
Zone	Select a zone. Make sure that the zone you select does not have traffic blocked by a security feature such as a security policy.
vpn-rule	You should have created a VPN tunnel first for a VPN Tunnel Interface scenario. Select one of the VPN Tunnel Interface scenario rules that you created.
IP Address Assignment	
IP Address	Enter the IP address for this interface. Please note that the IP address cannot conflict with any IP addresses that are already used.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers on the network. Please note that the subnet mask cannot conflict with any subnet masks that are already used.
Metric	Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
Enable IGMP Support	Select this to allow the Zyxel Device to act as an IGMP proxy for hosts connected on the IGMP downstream interface.
IGMP Upstream	Enable IGMP Upstream on the interface which connects to a router running IGMP that is closer to the multicast server.
IGMP Downstream	Enable IGMP Downstream on the interface which connects to the multicast hosts.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can receive from the network through the interface. Allowed values are 0 - 1048576.
Connectivity Check	These fields appear when you select a vpn-rule. The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the Zyxel Device stops routing to the gateway. The Zyxel Device resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select icmp to have the Zyxel Device regularly ping the gateway you specify to make sure it is still available. Select tcp to have the Zyxel Device regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the Zyxel Device stops routing through the gateway.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the Check Method to tcp. Specify the port number to use for a TCP connectivity check.

Table 96 Configuration > Network > Interface > VTI > Add (continued)

LABEL	DESCRIPTION
RIP Setting	See Section 12.6 on page 399 for more information about RIP.
Enable RIP	Select this to enable RIP in this interface.
Direction	This field is effective when RIP is enabled. Select the RIP direction from the drop-down list box. BiDir - This interface sends and receives routing information. In-Only - This interface receives routing information. Out-Only - This interface sends routing information.
Send Version	This field is effective when RIP is enabled. Select the RIP version(s) used for sending RIP packets. Choices are 1, 2, and 1 and 2.
Receive Version	This field is effective when RIP is enabled. Select the RIP version(s) used for receiving RIP packets. Choices are 1, 2, and 1 and 2.
V2-Broadcast	This field is effective when RIP is enabled. Select this to send RIP-2 packets using subnet broadcasting; otherwise, the Zyxel Device uses multicasting.
OSPF Setting	See Section 12.7 on page 401 for more information about OSPF.
Area	Select the area in which this interface belongs. Select None to disable OSPF in this interface.
Priority	Enter the priority (between 0 and 255) of this interface when the area is looking for a Designated Router (DR) or Backup Designated Router (BDR). The highest-priority interface identifies the DR, and the second-highest-priority interface identifies the BDR. Set the priority to zero if the interface can not be the DR or BDR.
Link Cost	Enter the cost (between 1 and 65,535) to route packets through this interface.
Passive Interface	Select this to stop forwarding OSPF routing information from the selected interface. As a result, this interface only receives routing information.
Authentication	Select an authentication method, or disable authentication. To exchange OSPF routing information with peer border routers, you must use the same authentication method that they use. Choices are: Same-as-Area - use the default authentication method in the area None - disable authentication Text - authenticate OSPF routing information using a plain-text password MD5 - authenticate OSPF routing information using MD5 encryption
Text Authentication Key	This field is available if the Authentication is Text. Enter the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MD5 Authentication ID	This field is available if the Authentication is MD5. Enter the ID for MD5 authentication. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the Authentication is MD5. Enter the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
Related Setting	
Configure WAN TRUNK	Click WAN TRUNK to go to a screen where you can configure the interface as part of a WAN trunk for load balancing.
Configure Policy Route	Click Policy Route to go to the screen where you can manually configure a policy route to associate traffic with this bridge interface.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

11.12 Trunk Overview

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

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

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

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

- Use the Trunk summary screen (Section 11.13 on page 376) to view the list of configured trunks and which load balancing algorithm each trunk uses.
- Use the Add Trunk screen (Section 11.13.1 on page 377) to configure the member interfaces for a trunk and the load balancing algorithm the trunk uses.
- Use the Add System Default screen (Section 11.13.2 on page 379) to configure the load balancing algorithm for the system default trunk.

11.12.1 What You Need to Know

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

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

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

1. LAN user A logs into server B on the Internet. The Zyxel Device uses wan1 to send the request to server B.
2. The Zyxel Device is using active/active load balancing. So when LAN user A tries to access something on the server, the request goes out through wan2.
3. The server finds that the request comes from wan2's IP address instead of wan1's IP address and rejects the request.

If link sticking had been configured, the Zyxel Device would have still used wan1 to send LAN user A's request to the server and server would have given the user A access.

Load Balancing Algorithms

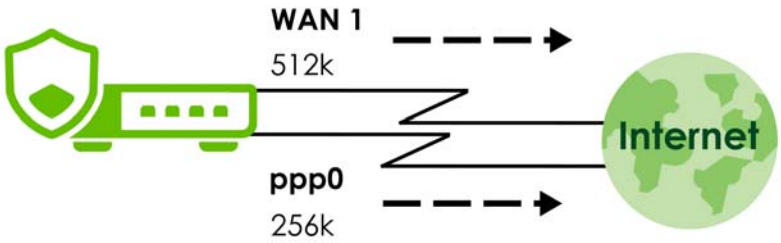
The following sections describe the load balancing algorithms the Zyxel Device can use to decide which interface the traffic (from the LAN) should use for a session. In the load balancing section, a session may refer to normal connection-oriented, UDP or SNMP2 traffic. The available bandwidth you configure on the Zyxel Device refers to the actual bandwidth provided by the ISP and the measured bandwidth refers to the bandwidth an interface is currently using.

Least Load First

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

Here the Zyxel Device has two WAN interfaces connected to the Internet. The configured available outbound bandwidths for WAN 1 and WAN 2 are 512K and 256K respectively.

Figure 268 Load Balancing Least Load First Example



The outbound bandwidth utilization is used as the load balancing index. In this example, the measured (current) outbound throughput of WAN 1 is 412K and WAN 2 is 198K. The Zyxel Device calculates the load balancing index as shown in the table below.

Since WAN 2 has a smaller load balancing index (meaning that it is less utilized than WAN 1), the Zyxel Device will send the subsequent new session traffic through WAN 2.

Table 97 Least Load First Example

INTERFACE	OUTBOUND		LOAD BALANCING INDEX (M/A)
	AVAILABLE (A)	MEASURED (M)	
WAN 1	512 K	412 K	0.8
WAN 2	256 K	198 K	0.77

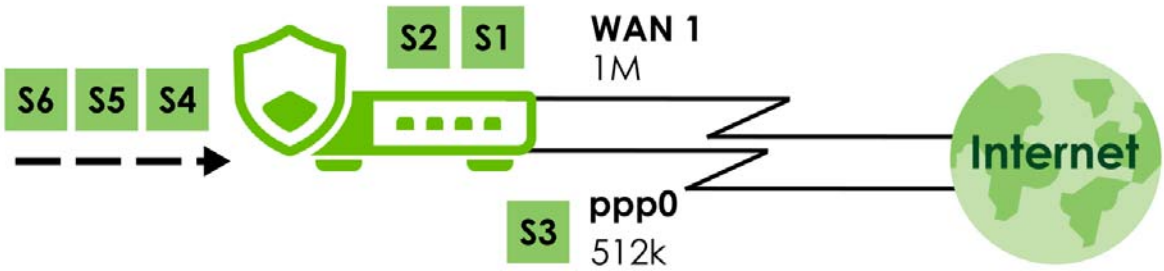
Weighted Round Robin

Round Robin scheduling services queues on a rotating basis and is activated only when an interface has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that interface. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

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

For example, in the figure below, the configured available bandwidth of WAN1 is 1M and WAN2 is 512K. You can set the Zyxel Device to distribute the network traffic between the two interfaces by setting the weight of wan1 and wan2 to 2 and 1 respectively. The Zyxel Device assigns the traffic of two sessions to wan1 and one session's traffic to wan2 in each round of 3 new sessions.

Figure 269 Weighted Robin Algorithm Example



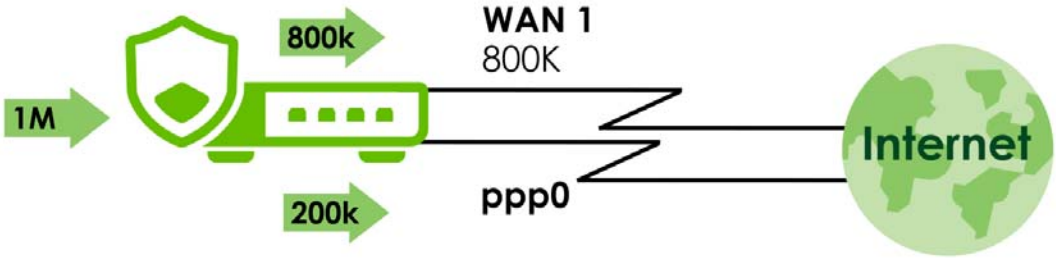
Spillover

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

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

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

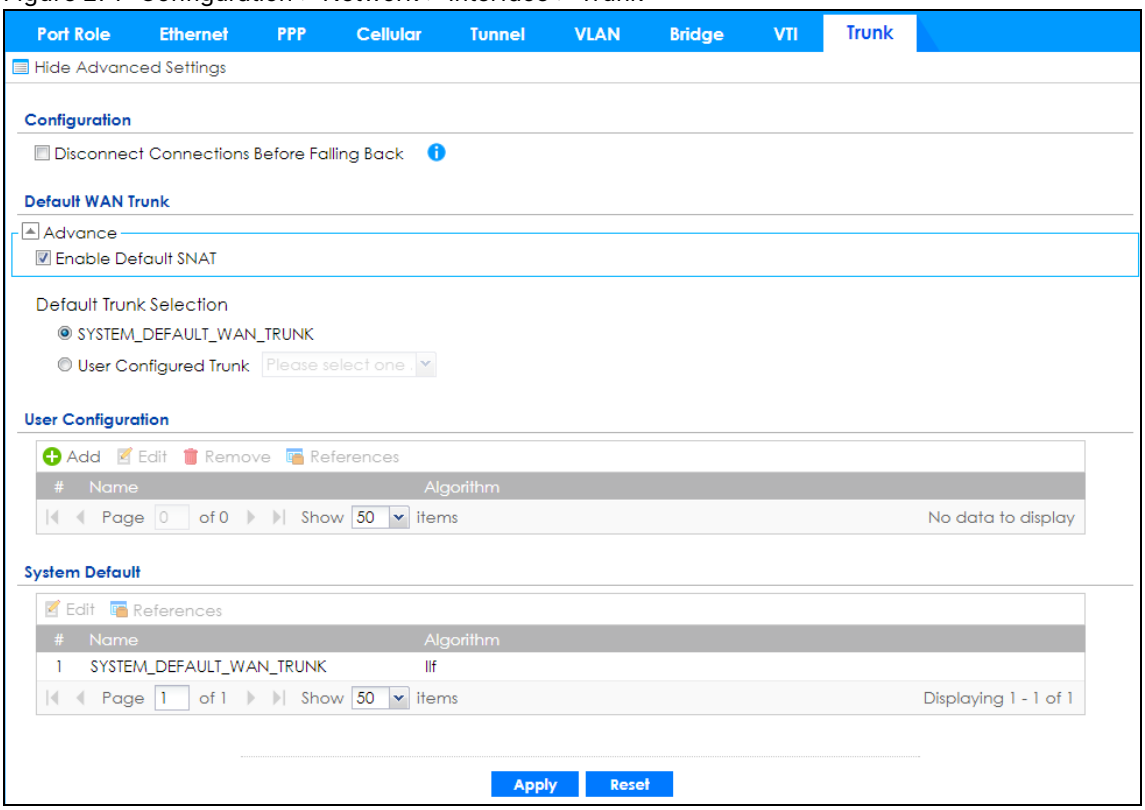
Figure 270 Spillover Algorithm Example



11.13 The Trunk Summary Screen

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

Figure 271 Configuration > Network > Interface > Trunk



The following table describes the items in this screen.

Table 98 Configuration > Network > Interface > Trunk

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

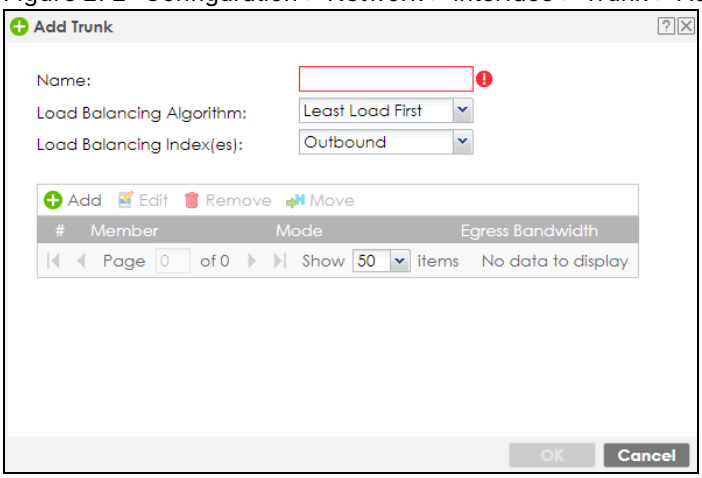
Table 98 Configuration > Network > Interface > Trunk (continued)

LABEL	DESCRIPTION
User Configuration / System Default	The Zyxel Device automatically adds all external interfaces into the pre-configured system default SYSTEM_DEFAULT_WAN_TRUNK. You cannot delete it. You can create your own User Configuration trunks and customize the algorithm, member interfaces and the active/passive mode.
Add	Click this to create a new user-configured trunk.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove a user-configured trunk, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click References to open a screen that shows which settings use the entry. See Section 11.5.4 on page 314 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Name	This field displays the label that you specified to identify the trunk.
Algorithm	This field displays the load balancing method the trunk is set to use.
Apply	Click this button to save your changes to the Zyxel Device.
Reset	Click this button to return the screen to its last-saved settings.

11.13.1 Configuring a User-Defined Trunk

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

Figure 272 Configuration > Network > Interface > Trunk > Add (or Edit)



Each field is described in the table below.

Table 99 Configuration > Network > Interface > Trunk > Add (or Edit)

LABEL	DESCRIPTION
Name	This is read-only if you are editing an existing trunk. When adding a new trunk, enter a descriptive name for this trunk. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Load Balancing Algorithm	Select a load balancing method to use from the drop-down list box. Select Weighted Round Robin to balance the traffic load between interfaces based on their respective weights. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight. For example, if the weight ratio of wan1 and wan2 interfaces is 2:1, the Zyxel Device chooses wan1 for 2 sessions' traffic and wan2 for 1 session's traffic in each round of 3 new sessions. Select Least Load First to send new session traffic through the least utilized trunk member. Select Spillover to send network traffic through the first interface in the group member list until there is enough traffic that the second interface needs to be used (and so on).
Load Balancing Index(es)	This field is available if you selected to use the Least Load First or Spillover method. Select Outbound, Inbound, or Outbound + Inbound to set the traffic to which the Zyxel Device applies the load balancing method. Outbound means the traffic traveling from an internal interface (ex. LAN) to an external interface (ex. WAN). Inbound means the opposite.
	The table lists the trunk's member interfaces. You can add, edit, remove, or move entries for user configured trunks.
Add	Click this to add a member interface to the trunk. Select an interface and click Add to add a new member interface after the selected member interface.
Edit	Select an entry and click Edit to modify the entry's settings.
Remove	To remove a member interface, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
Move	To move an interface to a different number in the list, click the Move icon. In the field that appears, specify the number to which you want to move the interface.
#	This column displays the priorities of the group's interfaces. The order of the interfaces in the list is important since they are used in the order they are listed.
Member	Click this table cell and select an interface to be a group member. If you select an interface that is part of another Ethernet interface, the Zyxel Device does not send traffic through the interface as part of the trunk. For example, if you have physical port 5 in the ge2 representative interface, you must select interface ge2 in order to send traffic through port 5 as part of the trunk. If you select interface ge5 as a member here, the Zyxel Device will not send traffic through port 5 as part of the trunk.
Mode	Click this table cell and select Active to have the Zyxel Device always attempt to use this connection. Select Passive to have the Zyxel Device only use this connection when all of the connections set to active are down. You can only set one of a group's interfaces to passive mode.
Weight	This field displays with the weighted round robin load balancing algorithm. Specify the weight (1~10) for the interface. The weights of the different member interfaces form a ratio. This ratio determines how much traffic the Zyxel Device assigns to each member interface. The higher an interface's weight is (relative to the weights of the interfaces), the more sessions that interface should handle.

Table 99 Configuration > Network > Interface > Trunk > Add (or Edit) (continued)

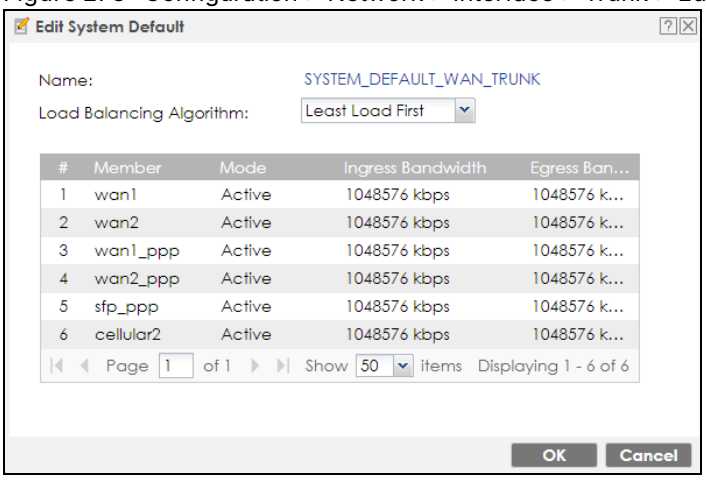
LABEL	DESCRIPTION
Ingress Bandwidth	This is reserved for future use. This field displays with the least load first load balancing algorithm. It displays the maximum number of kilobits of data the Zyxel Device is to allow to come in through the interface per second. Note: You can configure the bandwidth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

11.13.2 Configuring the System Default Trunk

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

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

Figure 273 Configuration > Network > Interface > Trunk > Edit (System Default)



Each field is described in the table below.

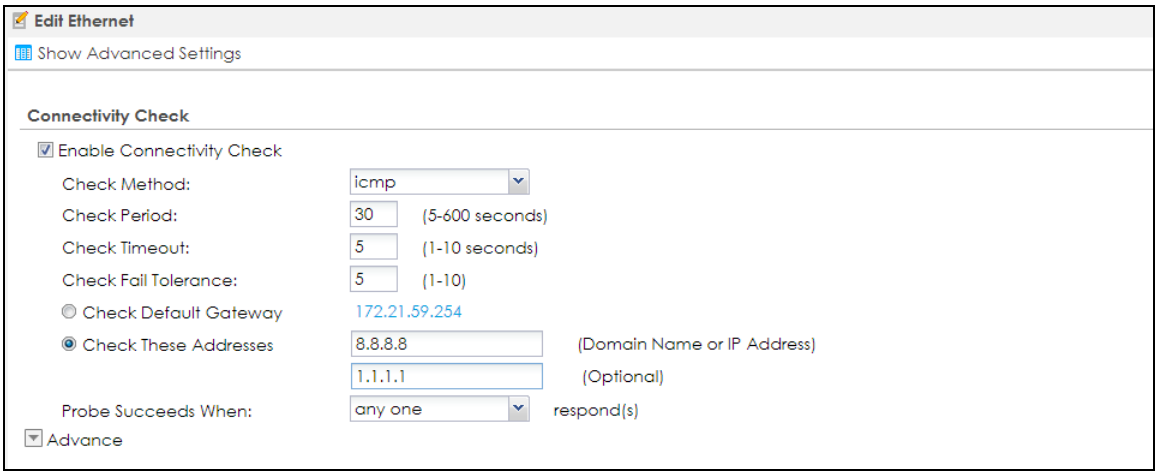
Table 100 Configuration > Network > Interface > Trunk > Edit (System Default)

LABEL	DESCRIPTION
Name	This field displays the name of the selected system default trunk.
Load Balancing Algorithm	Select the load balancing method to use for the trunk. Select Weighted Round Robin to balance the traffic load between interfaces based on their respective weights. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight. For example, if the weight ratio of wan1 and wan2 interfaces is 2:1, the Zyxel Device chooses wan1 for 2 sessions' traffic and wan2 for 1 session's traffic in each round of 3 new sessions. Select Least Load First to send new session traffic through the least utilized trunk member. Select Spillover to send network traffic through the first interface in the group member list until there is enough traffic that the second interface needs to be used (and so on).
	The table lists the trunk's member interfaces. This table is read-only.
#	This column displays the priorities of the group's interfaces. The order of the interfaces in the list is important since they are used in the order they are listed.
Member	This column displays the name of the member interfaces.
Mode	This field displays Active if the Zyxel Device always attempt to use this connection. This field displays Passive if the Zyxel Device only use this connection when all of the connections set to active are down. Only one of a group's interfaces can be set to passive mode.
Weight	This field displays with the weighted round robin load balancing algorithm. Specify the weight (1~10) for the interface. The weights of the different member interfaces form a ratio. s
Ingress Bandwidth	This is reserved for future use. This field displays with the least load first load balancing algorithm. It displays the maximum number of kilobits of data the Zyxel Device is to allow to come in through the interface per second.
Egress Bandwidth	This field displays with the least load first or spillover load balancing algorithm. It displays the maximum number of kilobits of data the Zyxel Device is to send out through the interface per second.
Spillover	This field displays with the spillover load balancing algorithm. Specify the maximum bandwidth of traffic in kilobits per second (1~1048576) to send out through the interface before using another interface. When this spillover bandwidth limit is exceeded, the Zyxel Device sends new session traffic through the next interface. The traffic of existing sessions still goes through the interface on which they started. The Zyxel Device uses the group member interfaces in the order that they are listed.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

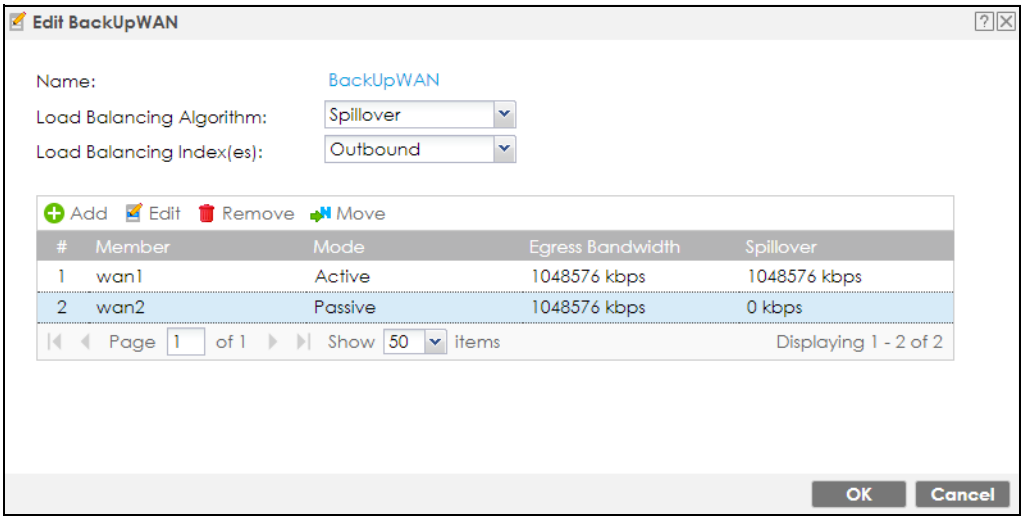
11.14 Example: WAN Trunk Failover

In this example, you have two WAN connections: one fiber which is always active, and one DSL which becomes active only if the fiber WAN1 connection fails.

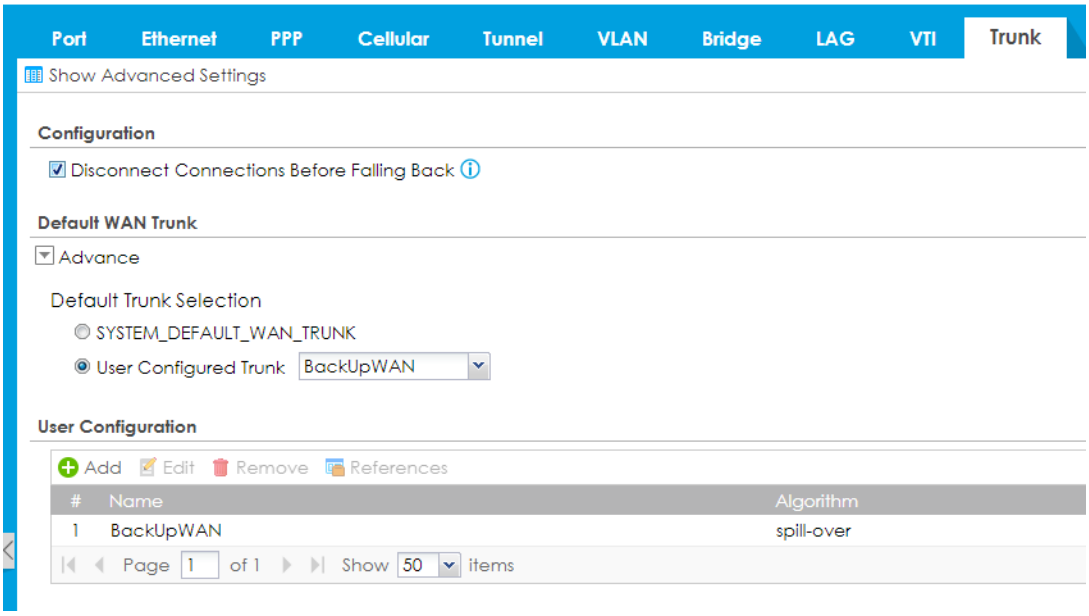
1 First arrange a connectivity check for WAN1 (fiber). Set up the ICMP connectivity check (ping) in Configuration > Network > Interface > Ethernet > WAN1 > Edit.



2 Then go to Configuration > Network > Interface > Trunk > User Configuration > Add to configure your own trunk connection. Add the WAN ports with one as Passive, then select Spillover in Load Balancing Algorithm, Outbound for the Load Balancing Index.



If WAN1 fails, then the Zyxel Device automatically uses the WAN2 connection and an alert report will be sent to the administer. When WAN1 is available again, the Zyxel Device returns to using WAN1.



11.15 Example: Trunk Tagged VLAN Traffic to a Switch

Configure VLAN on the Zyxel Device and the connected VLAN switch so as a computer can access VLAN10 as shown in the following example:

Zyxel Device

- LAN1 192.168.1.1/24
- VLAN10, ge3/10,192.168.10.1/24
- VLAN20, ge3/20, 192.168.20.2/24

Switch

- port 1 Tx VLAN10, VLAN20 PVID1 -> connect this port to Zyxel Device interface ge3
- port 2 Ux VLAN10 -> connect this port to a computer

11.16 Interface Technical Reference

Here is more detailed information about interfaces on the Zyxel Device.

IP Address Assignment

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

Figure 274 Example: Entry in the Routing Table Derived from Interfaces

Table 101 Example: Routing Table Entries for Interfaces

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

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

In most interfaces, you can enter the IP address and subnet mask manually. In PPPoE/PPTP/L2TP interfaces, however, the subnet mask is always 255.255.255.255 because it is a point-to-point interface. For these interfaces, you can only enter the IP address.

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

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

In the example above, if the Zyxel Device gets a packet with a destination address of 5.5.5.5, it might not find any entries in the routing table. In this case, the packet is dropped. However, if there is a default router to which the Zyxel Device should send this packet, you can specify it as a gateway in one of the interfaces. For example, if there is a default router at 200.200.200.100, you can create a gateway at 200.200.200.100 on ge2. In this case, the Zyxel Device creates the following entry in the routing table.

Table 102 Example: Routing Table Entry for a Gateway

IP ADDRESS(ES)	DESTINATION
0.0.0.0/0	200.200.200.100

The gateway is an optional setting for each interface. If there is more than one gateway, the Zyxel Device uses the gateway with the lowest metric, or cost. If two or more gateways have the same metric, the Zyxel Device uses the one that was set up first (the first entry in the routing table). In PPPoE/PPTP/L2TP interfaces, the other computer is the gateway for the interface by default. In this case, you should specify the metric.

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

Interface Parameters

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

- Egress bandwidth sets the amount of traffic the Zyxel Device sends out through the interface to the network.
- Ingress bandwidth sets the amount of traffic the Zyxel Device allows in through the interface from the network.At the time of writing, the Zyxel Device does not support ingress bandwidth management.

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

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

DHCP Settings

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

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

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

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

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

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

Table 103 Example: Assigning IP Addresses from a Pool

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

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

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

- Subnet mask - The interface provides the same subnet mask you specify for the interface. See IP Address Assignment on page 382.
- Gateway - The interface provides the same gateway you specify for the interface. See IP Address Assignment on page 382.
- DNS servers - The interface provides IP addresses for up to three DNS servers that provide DNS services for DHCP clients. You can specify each IP address manually (for example, a company's own DNS server), or you can refer to DNS servers that other interfaces received from DHCP servers (for example, a DNS server at an ISP). These other interfaces have to be DHCP clients.

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

WINS

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

PPPoE/PPTP/L2TP Overview

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

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

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

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

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

Layer 2 Tunneling Protocol (L2TP) was taken from PPTP of Microsoft and Cisco's L2F (Layer 2 Forwarding technology), so LT2P combines PPTP's control and runs over a faster transport protocol, UDP, although it may be a bit more complicated to set up.

It supports up to 256 bit session keys using the IPSec protocol. When security is a priority, L2TP is a good option as it requires certificates unlike PPTP.

It uses the following ports: UDP 500, Protocol 50, UDP 1701 and UDP 4500.

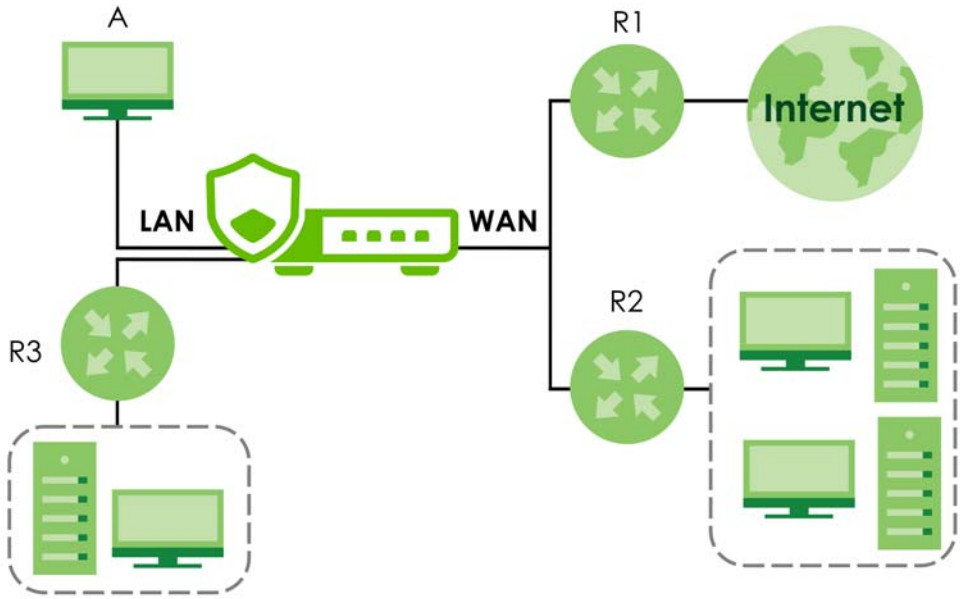
CHAPTER 12
Routing

12.1 Policy and Static Routes Overview

Use policy routes and static routes to override the Zyxel Device's default routing behavior in order to send packets through the appropriate interface or VPN tunnel.

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

Figure 275 Example of Policy Routing Topology



Note: You can generally just use policy routes. You only need to use static routes if you have a large network with multiple routers where you use RIP or OSPF to propagate routing information to other routers.

12.1.1 What You Can Do in this Chapter

- Use the Policy Route screens (see Section 12.2 on page 389) to list and configure policy routes.
- Use the Static Route screens (see Section 12.3 on page 396) to list and configure static routes.

12.1.2 What You Need to Know

Policy Routing

Traditionally, routing is based on the destination address only and the Zyxel Device takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

How You Can Use Policy Routing

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Bandwidth Shaping – You can allocate bandwidth to traffic that matches routing policies and prioritize traffic. You can also use policy routes to manage other types of traffic (like ICMP traffic) and send traffic through VPN tunnels.
- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.
- NAT - The Zyxel Device performs NAT by default for traffic going to or from the WAN interfaces. A routing policy's SNAT allows network administrators to have traffic received on a specified interface use a specified IP address as the source IP address.

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

Static Routes

The Zyxel Device usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the Zyxel Device send data to devices not reachable through the default gateway, use static routes. Configure static routes if you need to use RIP or OSPF to propagate the routing information to other routers. See Chapter 12 on page 398 for more on RIP and OSPF.

Policy Routes Versus Static Routes

- Policy routes are more flexible than static routes. You can select more criteria for the traffic to match and can also use schedules, NAT, and bandwidth management.
- Policy routes are only used within the Zyxel Device itself. Static routes can be propagated to other routers using RIP or OSPF.
- Policy routes take priority over static routes. If you need to use a routing policy on the Zyxel Device and propagate it to other routers, you could configure a policy route and an equivalent static route.

DiffServ

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

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the

application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP Marking and Per-Hop Behavior

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

DSCP (6 bits)	Unused (2 bits)

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

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

12.2 Policy Route Screen

Click Configuration > Network > Routing to open the Policy Route screen. Use this screen to see the configured policy routes and turn policy routing based bandwidth management on or off.

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

The actions that can be taken include:

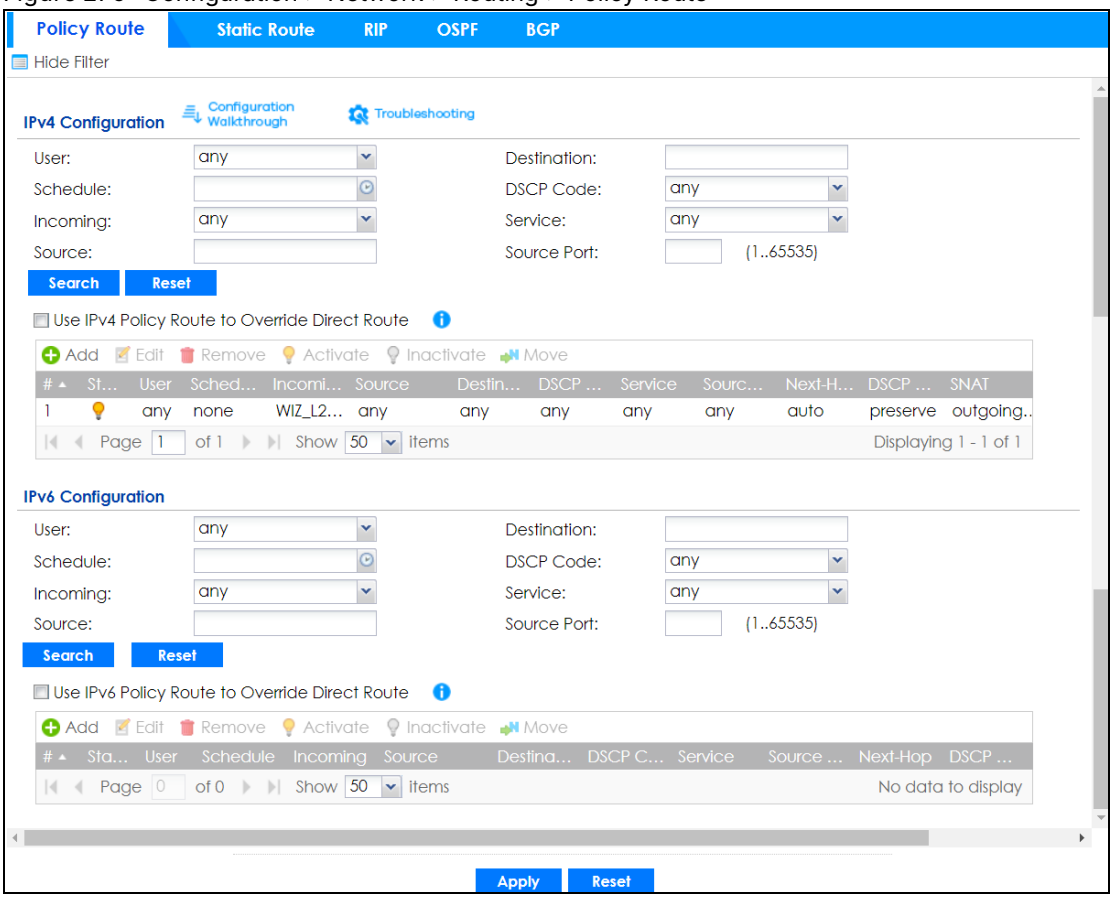
- Routing the packet to a different gateway, outgoing interface, VPN tunnel, or trunk.
- Limiting the amount of bandwidth available and setting a priority for traffic.

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

If you enabled IPv6 in the Configuration > System > IPv6 screen, you can also configure policy routes used for your IPv6 networks on this screen.

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

Figure 276 Configuration > Network > Routing > Policy Route



The following table describes the labels in this screen.

Table 104 Configuration > Network > Routing > Policy Route

LABEL	DESCRIPTION
Show Filter / Hide Filter	Click this button to display a greater or lesser number of configuration fields.
IPv4 Configuration / IPv6 Configuration	Use the IPv4 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.
Use IPv4/IPv6 Policy Route to Override Direct Route	Select this to have the Zyxel Device forward packets that match a policy route according to the policy route instead of sending the packets directly to a connected network.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The 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.
Move	To change a rule's position in the numbered list, select the rule and click Move to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.

Table 104 Configuration > Network > Routing > Policy Route (continued)

LABEL	DESCRIPTION
#	This is the number of an individual policy route.
Status	This icon is lit when the entry is active, red when the next hop's connection is down, and dimmed when the entry is inactive.
User	This is the name of the user (group) object from which the packets are sent. any means all users.
Schedule	This is the name of the schedule object. none means the route is active at all times if enabled.
Incoming	This is the interface on which the packets are received.
Source	This is the name of the source IP address (group) object, including geographic address and FQDN (group) objects. any means all IP addresses.
Destination	This is the name of the destination IP address (group) object, including geographic and FQDN (group) address objects. any means all IP addresses.
DSCP Code	This is the DSCP value of incoming packets to which this policy route applies. any means all DSCP values or no DSCP marker. default means traffic with a DSCP value of 0. This is usually best effort traffic. The "af" entries stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ for more details.
Service	This is the name of the service object. any means all services.
Source Port	This is the name of a service object. The Zyxel Device applies the policy route to the packets sent from the corresponding service port. any means all service ports.
Next-Hop	This is the next hop to which packets are directed. It helps forward packets to their destinations and can be a router, VPN tunnel, outgoing interface or trunk.
DSCP Marking	This is how the Zyxel Device handles the DSCP value of the outgoing packets that match this route. If this field displays a DSCP value, the Zyxel Device applies that DSCP value to the route's outgoing packets. preserve means the Zyxel Device does not modify the DSCP value of the route's outgoing packets. default means the Zyxel Device sets the DSCP value of the route's outgoing packets to 0. The "af" choices stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ for more details.
SNAT	This is the source IP address that the route uses. It displays none if the Zyxel Device does not perform NAT for this route.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

12.2.1 Policy Route Edit Screen

Click Configuration > Network > Routing to open the Policy Route screen. Then click the Add or Edit icon in the IPv4 Configuration or IPv6 Configuration section. The Add Policy Route or Policy Route Edit screen opens. Use this screen to configure or edit a policy route. Both IPv4 and IPv6 policy route have similar settings except the Address Translation (SNAT) settings.

Figure 277 Configuration > Network > Routing > Policy Route > Add/Edit (IPv4 Configuration)

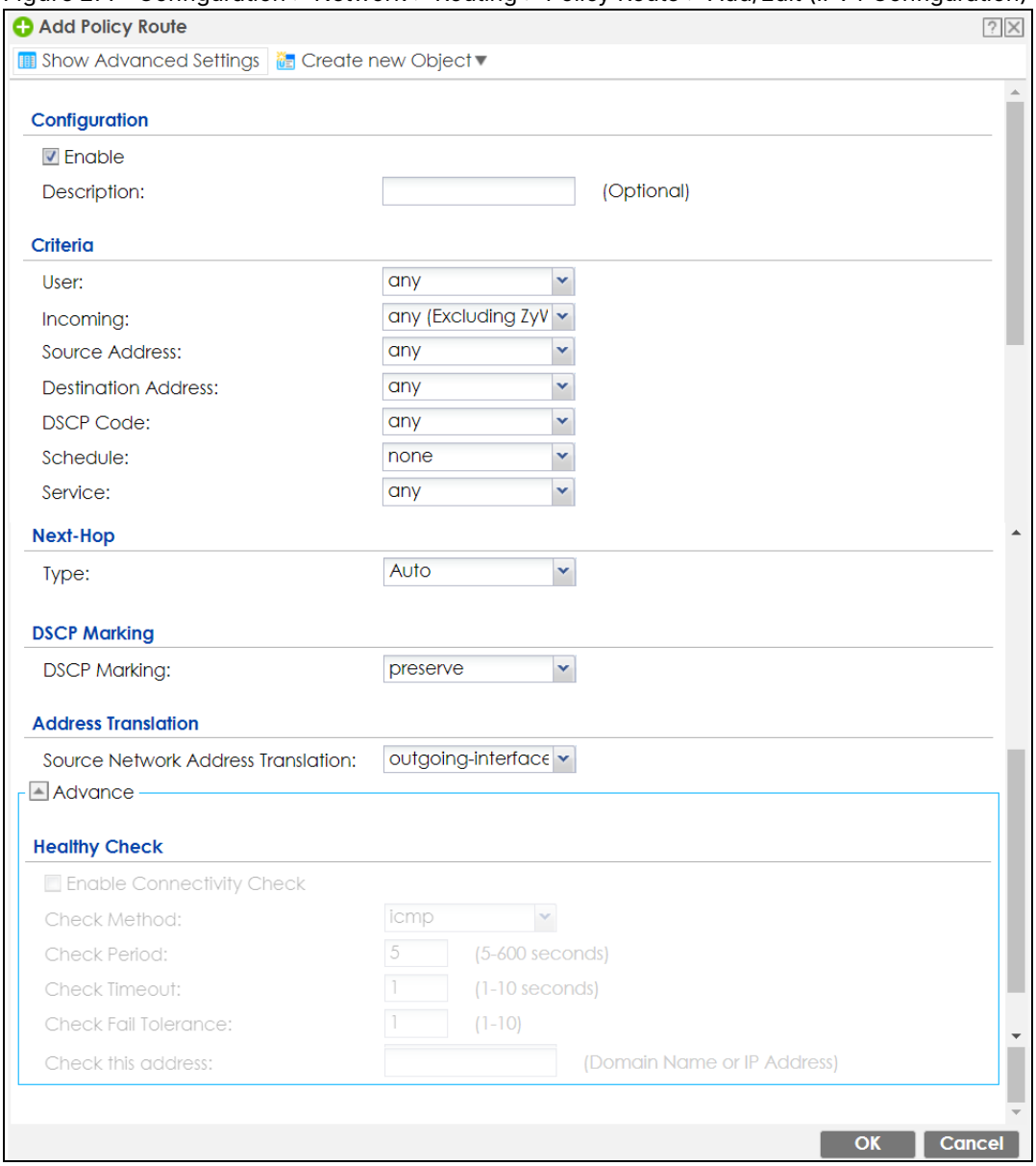
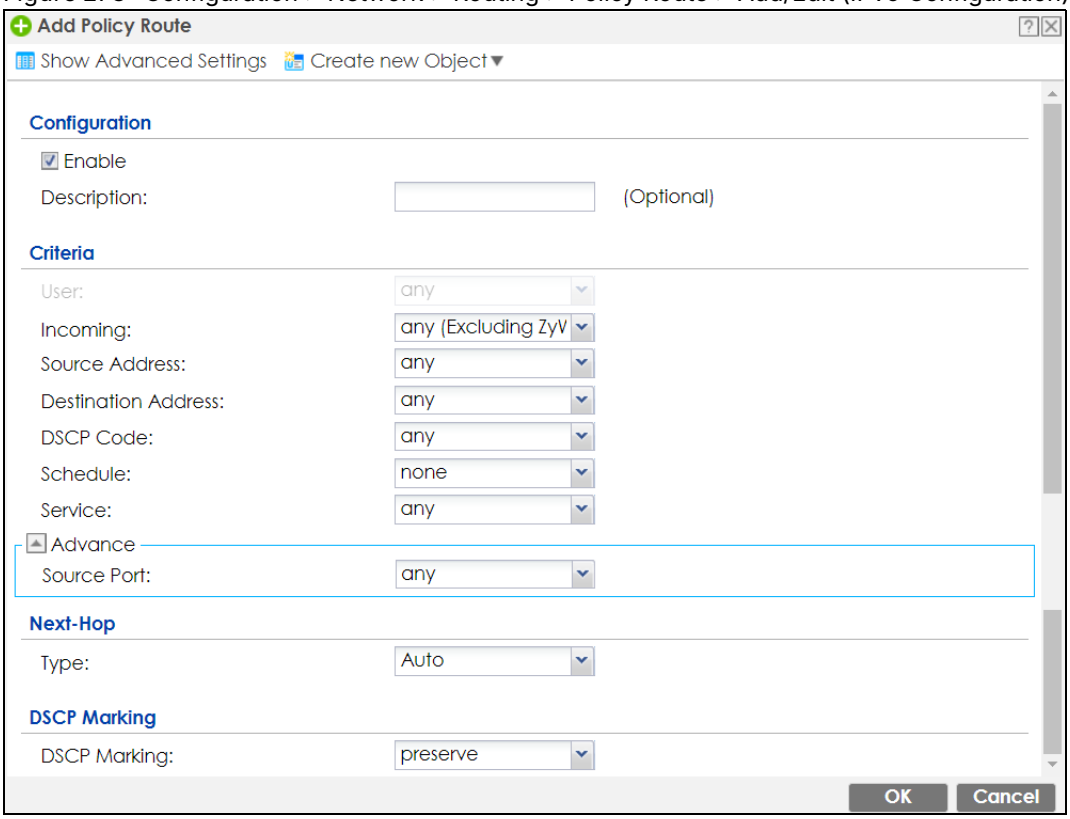


Figure 278 Configuration > Network > Routing > Policy Route > Add/Edit (IPv6 Configuration)



The following table describes the labels in this screen.

Table 105 Configuration > Network > Routing > Policy Route > Add/Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Configuration	
Enable	Select this to activate the policy.
Description	Enter a descriptive name consists of 1 to 60 single-byte characters, including a-zA-Z0-9!"#$%'()*+,-/;:=?@_&[.]<>\^'{|} are not allowed.
Criteria	
User	Select a user name or user group from which the packets are sent.
Incoming	Select where the packets are coming from; any, an interface, a tunnel, an SSL VPN, or the Zyxel Device itself. For an interface, a tunnel, or an SSL VPN, you also need to select the individual interface, VPN tunnel, or SSL VPN connection.
Source Address	Select a source IP address object, including geographic address and FQDN (group) objects, from which the packets are sent.
Destination Address	Select a destination IP address object, including geographic address and FQDN (group) objects, to which the traffic is being sent. If the next hop is a dynamic VPN tunnel and you enable Auto Destination Address, the Zyxel Device uses the local network of the peer router that initiated an incoming dynamic IPSec tunnel as the destination address of the policy instead of your configuration here.

Table 105 Configuration > Network > Routing > Policy Route > Add/Edit (continued)

LABEL	DESCRIPTION
DSCP Code	Select a DSCP code point value of incoming packets to which this policy route applies or select User Define to specify another DSCP code point. The lower the number the higher the priority with the exception of 0 which is usually given only best-effort treatment. any means all DSCP value or no DSCP marker. default means traffic with a DSCP value of 0. This is usually best effort traffic The “af” choices stand for Assured Forwarding. The number following the “af” identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ for more details.
User-Defined DSCP Code	Use this field to specify a custom DSCP code point when you select User Define in the previous field.
Schedule	Select a schedule to control when the policy route is active. none means the route is active at all times if enabled.
Service	Select a service or service group to identify the type of traffic to which this policy route applies.
Source Port	Select a service or service group to identify the source port of packets to which the policy route applies.
Next-Hop	
Type	Select Auto to have the Zyxel Device use the routing table to find a next-hop and forward the matched packets automatically. Select Gateway to route the matched packets to the next-hop router or switch you specified in the Gateway field. You have to set up the next-hop router or switch as a HOST address object first. Select VPN Tunnel to route the matched packets through the specified VPN tunnel. Select Trunk to route the matched packets through the interfaces in the trunk group based on the load balancing algorithm. Select Interface to route the matched packets through the specified outgoing interface to a gateway (which is connected to the interface).
Gateway	This field displays when you select Gateway in the Type field. Select a HOST address object. The gateway is an immediate neighbor of your Zyxel Device that will forward the packet to the destination. The gateway must be a router or switch on the same segment as your Zyxel Device's interface(s).
VPN Tunnel	This field displays when you select VPN Tunnel in the Type field. Select a VPN tunnel through which the packets are sent to the remote network that is connected to the Zyxel Device directly.
Auto Destination Address	This field displays when you select VPN Tunnel in the Type field. Select this to have the Zyxel Device use the local network of the peer router that initiated an incoming dynamic IPSec tunnel as the destination address of the policy. Leave this cleared if you want to manually specify the destination address.
Trunk	This field displays when you select Trunk in the Type field. Select a trunk group to have the Zyxel Device send the packets through the interfaces in the group.
Interface	This field displays when you select Interface in the Type field. Select an interface to have the Zyxel Device send traffic that matches the policy route through the specified interface.

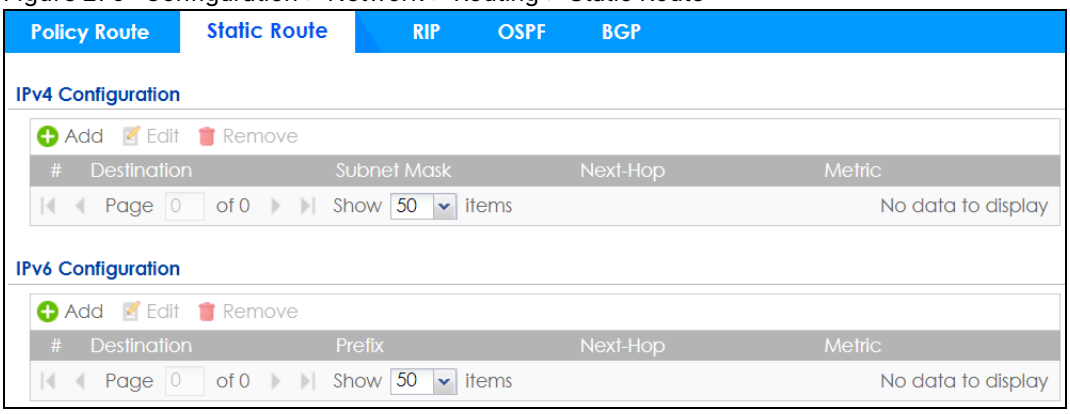
Table 105 Configuration > Network > Routing > Policy Route > Add/Edit (continued)

LABEL	DESCRIPTION
DSCP Marking	Set how the Zyxel Device handles the DSCP value of the outgoing packets that match this route. Select one of the pre-defined DSCP values to apply or select User Define to specify another DSCP value. The "af" choices stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ for more details. Select preserve to have the Zyxel Device keep the packets' original DSCP value. Select default to have the Zyxel Device set the DSCP value of the packets to 0.
User-Defined DSCP Marking	Use this field to specify a custom DSCP value.
Address Translation	Use this section to configure NAT for the policy route. This section does not apply to policy routes that use a VPN tunnel as the next hop.
Source Network Address Translation	Select none to not use NAT for the route. Select outgoing-interface to use the IP address of the outgoing interface as the source IP address of the packets that matches this route. To use SNAT for a virtual interface that is in the same WAN trunk as the physical interface to which the virtual interface is bound, the virtual interface and physical interface must be in different subnets. Otherwise, select a pre-defined address (group) to use as the source IP address(es) of the packets that match this route. Use Create new Object if you need to configure a new address (group) to use as the source IP address(es) of the packets that match this route.
Healthy Check	Use this part of the screen to configure a route connectivity check and disable the policy if the interface is down.
Disable policy route automatically while Interface link down	Select this to disable the policy if the interface is down or disabled. This is available for Interface and Trunk in the Type field above.
Enable Connectivity Check	Select this to turn on the connection check. This is available for Interface and Gateway in the Type field above.
Check Method:	Select the method that the gateway allows. Select icmp to have the Zyxel Device regularly ping the gateway you specify to make sure it is still available. Select tcp to have the Zyxel Device regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period:	Enter the number of seconds between connection check attempts (5-600 seconds).
Check Timeout:	Enter the number of seconds to wait for a response before the attempt is a failure (1-10 seconds).
Check Fail Tolerance:	Enter the number of consecutive failures before the Zyxel Device stops routing using this policy (1-10).
Check Port:	This field only displays when you set the Check Method to tcp. Specify the port number to use for a TCP connectivity check (1-65535).
Check this address:	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

12.3 IP Static Route Screen

Click Configuration > Network > Routing > Static Route to open the Static Route screen. This screen displays the configured static routes. Configure static routes to be able to use RIP or OSPF to propagate the routing information to other routers. If you enabled IPv6 in the Configuration > System > IPv6 screen, you can also configure static routes used for your IPv6 networks on this screen.

Figure 279 Configuration > Network > Routing > Static Route



The following table describes the labels in this screen.

Table 106 Configuration > Network > Routing > Static Route

LABEL	DESCRIPTION
IPv4 Configuration / IPv6 Configuration	Use the IPv4 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.
Add	Click this to create a new static route.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
#	This is the number of an individual static route.
Destination	This is the destination IP address.
Subnet Mask	This is the IP subnet mask.
Prefix	This is the IPv6 prefix for the destination IP address.
Next-Hop	This is the IP address of the next-hop gateway or the interface through which the traffic is routed. The gateway is a router or switch on the same segment as your Zyxel Device's interface(s). The gateway helps forward packets to their destinations.
Metric	This is the route's priority among the Zyxel Device's routes. The smaller the number, the higher priority the route has.

12.3.1 Static Route Add/Edit Screen

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

Figure 280 Configuration > Network > Routing > Static Route > Add (IPv4 Configuration)

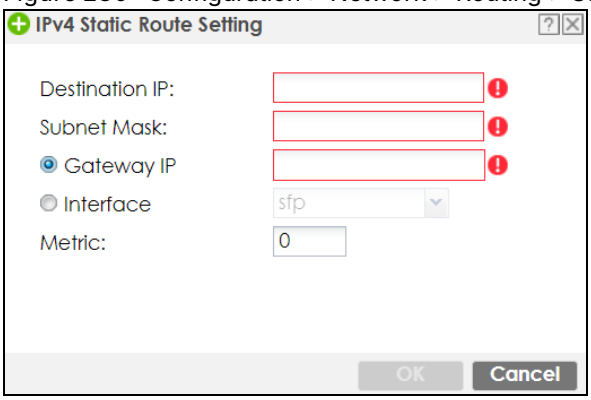
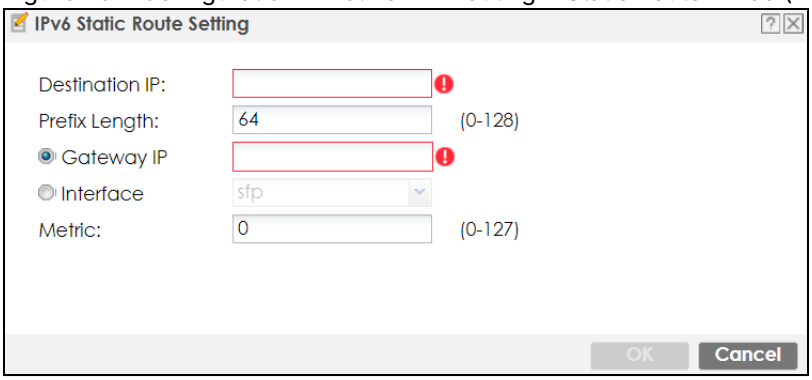


Figure 281 Configuration > Network > Routing > Static Route > Add (IPv6 Configuration)



The following table describes the labels in this screen.

Table 107 Configuration > Network > Routing > Static Route > Add

LABEL	DESCRIPTION
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, enter the specific IP address here and use a subnet mask of 255.255.255.255 (for IPv4) in the Subnet Mask field or a prefix of 128 (for IPv6) in the Prefix Length field to force the network number to be identical to the host ID. For IPv6, if you want to send all traffic to the gateway or interface specified in the Gateway IP or Interface field, enter :: in this field and 0 in the Prefix Length field.
Subnet Mask	Enter the IP subnet mask here.
Prefix Length	Enter the number of left-most digits in the destination IP address, which indicates the network prefix. Enter :: in the Destination IP field and 0 in this field if you want to send all traffic to the gateway or interface specified in the Gateway IP or Interface field.
Gateway IP	Select the radio button and enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your Zyxel Device's interface(s). The gateway helps forward packets to their destinations.
Interface	Select the radio button and a predefined interface through which the traffic is sent.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be 0~127. In practice, 2 or 3 is usually a good number.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

12.4 Policy Routing Technical Reference

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

NAT and SNAT

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

Assured Forwarding (AF) PHB for DiffServ

Assured Forwarding (AF) behavior is defined in RFC 2597. The AF behavior group defines four AF classes. Inside each class, packets are given a high, medium or low drop precedence. The drop precedence determines the probability that routers on the network will drop packets when congestion occurs. If congestion occurs between classes, the traffic in the higher class (smaller numbered class) is generally given priority. Combining the classes and drop precedence produces the following twelve DSCP encodings from AF11 through AF43. The decimal equivalent is listed in brackets.

Table 108 Assured Forwarding (AF) Behavior Group

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

Maximize Bandwidth Usage

The maximize bandwidth usage option allows the Zyxel Device to divide up any available bandwidth on the interface (including unallocated bandwidth and any allocated bandwidth that a policy route is not using) among the policy routes that require more bandwidth.

When you enable maximize bandwidth usage, the Zyxel Device first makes sure that each policy route gets up to its bandwidth allotment. Next, the Zyxel Device divides up an interface’s available bandwidth (bandwidth that is unbudgeted or unused by the policy routes) depending on how many policy routes require more bandwidth and on their priority levels. When only one policy route requires more bandwidth, the Zyxel Device gives the extra bandwidth to that policy route.

When multiple policy routes require more bandwidth, the Zyxel Device gives the highest priority policy routes the available bandwidth first (as much as they require, if there is enough available bandwidth), and then to lower priority policy routes if there is still bandwidth available. The Zyxel Device distributes the available bandwidth equally among policy routes with the same priority level.

12.5 Routing Protocols Overview

Routing protocols give the Zyxel Device routing information about the network from other routers. The Zyxel Device stores this routing information in the routing table it uses to make routing decisions. In turn, the Zyxel Device can also use routing protocols to propagate routing information to other routers.

Routing protocols are usually only used in networks using multiple routers like campuses or large enterprises.

- Use the RIP screen (see Section 12.6 on page 399) to configure the Zyxel Device to use RIP to receive and/or send routing information.
- Use the OSPF screen (see Section 12.7 on page 401) to configure general OSPF settings and manage OSPF areas.
- Use the OSPF Area Add/Edit screen (see Section 12.7.2 on page 405) to create or edit an OSPF area.
- Use the BGP screen (see Section 12.8 on page 408) to configure eBGP (exterior Border Gate Protocol).

12.5.1 What You Need to Know

The Zyxel Device supports two standards, RIP and OSPF, for routing protocols. RIP and OSPF are compared here and discussed further in the rest of the chapter.

Table 109 RIP vs. OSPF

	RIP	OSPF
Network Size	Small (with up to 15 routers)	Large
Metric	Hop count	Bandwidth, hop count, throughput, round trip time and reliability.
Convergence	Slow	Fast

12.6 The RIP Screen

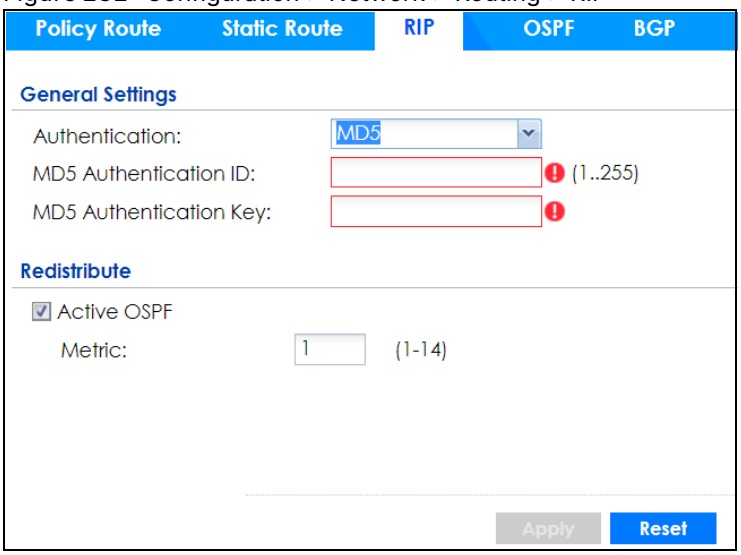
RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a device to exchange routing information with other routers. RIP is a vector-space routing protocol, and, like most such protocols, it uses hop count to decide which route is the shortest. Unfortunately, it also broadcasts its routes asynchronously to the network and converges slowly. Therefore, RIP is more suitable for small networks (up to 15 routers).

- In the Zyxel Device, you can configure two sets of RIP settings before you can use it in an interface.
- First, the Authentication field specifies how to verify that the routing information that is received is the same routing information that is sent.
- Second, the Zyxel Device can also redistribute routing information from non-RIP networks, specifically OSPF networks and static routes, to the RIP network. Costs might be calculated differently, however, so you use the Metric field to specify the cost in RIP terms.
- RIP uses UDP port 520.

Use the RIP screen to specify the authentication method and maintain the policies for redistribution.

Click Configuration > Network > Routing > RIP to open the following screen.

Figure 282 Configuration > Network > Routing > RIP



The following table describes the labels in this screen.

Table 110 Configuration > Network > Routing Protocol > RIP

LABEL	DESCRIPTION
Authentication	The transmitting and receiving routers must have the same key. For RIP, authentication is not available in RIP version 1. In RIP version 2, you can only select one authentication type for all interfaces.
Authentication	Select the authentication method used in the RIP network. This authentication protects the integrity, but not the confidentiality, of routing updates. • None uses no authentication. • Text uses a plain text password that is sent over the network (not very secure). • MD5 uses an MD5 password and authentication ID (most secure).
Text Authentication Key	This field is available if the Authentication is Text. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MD5 Authentication ID	This field is available if the Authentication is MD5. Type the ID for MD5 authentication. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the Authentication is MD5. Type the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
Redistribute	
Active OSPF	Select this to use RIP to advertise routes that were learned through OSPF.
Metric	Type the cost for routes provided by OSPF. The metric represents the “cost” of transmission for routing purposes. RIP routing uses hop count as the measurement of cost, with 1 usually used for directly connected networks. The number does not have to be precise, but it must be between 0 and 16. In practice, 2 or 3 is usually used.
Apply	Click this button to save your changes to the Zyxel Device.
Reset	Click this button to return the screen to its last-saved settings.

12.7 The OSPF Screen

OSPF (Open Shortest Path First, RFC 2328) is a link-state protocol designed to distribute routing information within a group of networks, called an Autonomous System (AS). OSPF offers some advantages over vector-space routing protocols like RIP.

- OSPF supports variable-length subnet masks, which can be set up to use available IP addresses more efficiently.
- OSPF filters and summarizes routing information, which reduces the size of routing tables throughout the network.
- OSPF responds to changes on the network, such as the loss of a router, more quickly.
- OSPF considers several factors, including bandwidth, hop count, throughput, round trip time, and reliability, when it calculates the shortest path.
- OSPF converges more quickly than RIP.

Naturally, OSPF is also more complicated than RIP, so OSPF is usually more suitable for large networks.

OSPF uses IP protocol 89.

OSPF Areas

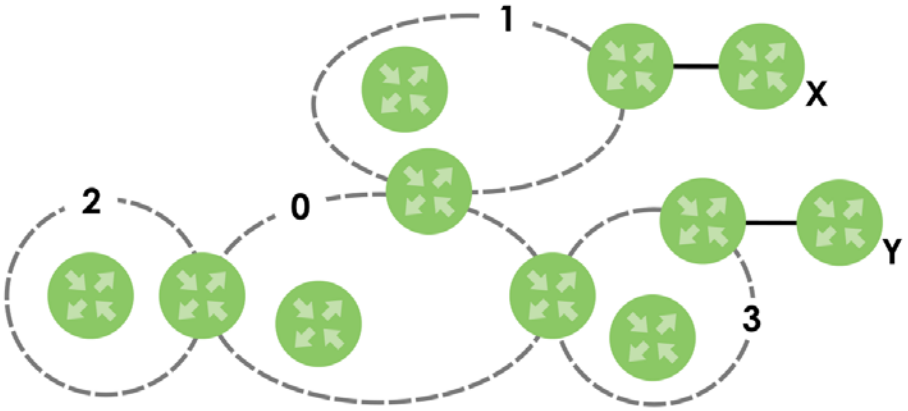
An OSPF Autonomous System (AS) is divided into one or more areas. Each area represents a group of adjacent networks and is identified by a 32-bit ID. In OSPF, this number may be expressed as an integer or as an IP address.

There are several types of areas.

- The backbone is the transit area that routes packets between other areas. All other areas are connected to the backbone.
- A normal area is a group of adjacent networks. A normal area has routing information about the OSPF AS, any networks outside the OSPF AS to which it is directly connected, and any networks outside the OSPF AS that provide routing information to any area in the OSPF AS.
- A stub area has routing information about the OSPF AS. It does not have any routing information about any networks outside the OSPF AS, including networks to which it is directly connected. It relies on a default route to send information outside the OSPF AS.
- A Not So Stubby Area (NSSA, RFC 1587) has routing information about the OSPF AS and networks outside the OSPF AS to which the NSSA is directly connected. It does not have any routing information about other networks outside the OSPF AS.

Each type of area is illustrated in the following figure.

Figure 283 OSPF: Types of Areas



This OSPF AS consists of four areas, areas 0-3. Area 0 is always the backbone. In this example, areas 1, 2, and 3 are all connected to it. Area 1 is a normal area. It has routing information about the OSPF AS and networks X and Y. Area 2 is a stub area. It has routing information about the OSPF AS, but it depends on a default route to send information to networks X and Y. Area 3 is a NSSA. It has routing information about the OSPF AS and network Y but not about network X.

OSPF Routers

Every router in the same area has the same routing information. They do this by exchanging Hello messages to confirm which neighbor (layer-3) devices exist, and then they exchange database descriptions (DDs) to create a synchronized link-state database. The link-state database contains records of router IDs, their associated links and path costs. The link-state database is then constantly updated through Link State Advertisements (LSA). Each router uses the link state database and the Dijkstra algorithm to compute the least cost paths to network destinations.

Like areas, each router has a unique 32-bit ID in the OSPF AS, and there are several types of routers. Each type is really just a different role, and it is possible for one router to play multiple roles at one time.

- An internal router (IR) only exchanges routing information with other routers in the same area.
- An Area Border Router (ABR) connects two or more areas. It is a member of all the areas to which it is connected, and it filters, summarizes, and exchanges routing information between them.
- An Autonomous System Boundary Router (ASBR) exchanges routing information with routers in networks outside the OSPF AS. This is called redistribution in OSPF.

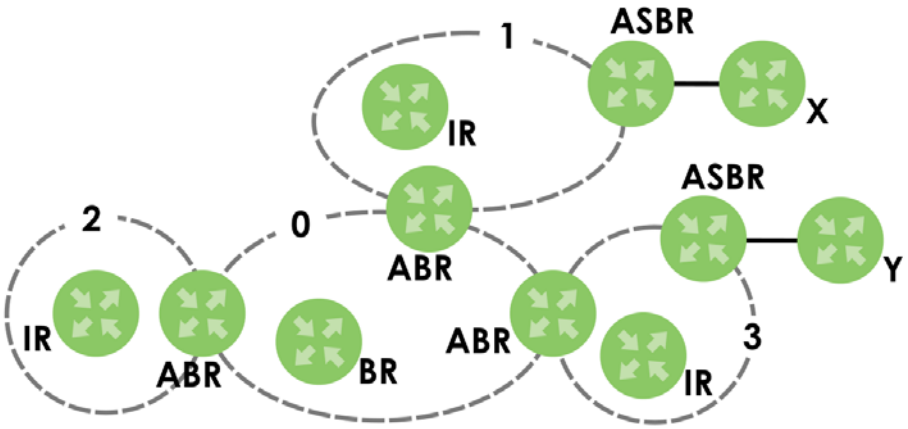
Table 111 OSPF: Redistribution from Other Sources to Each Type of Area

SOURCE \ TYPE OF AREA	NORMAL	NSSA	STUB
Static routes	Yes	Yes	No
RIP	Yes	Yes	Yes

- A backbone router (BR) has at least one interface with area 0. By default, every router in area 0 is a backbone router, and so is every ABR.

Each type of router is illustrated in the following example.

Figure 284 OSPF: Types of Routers



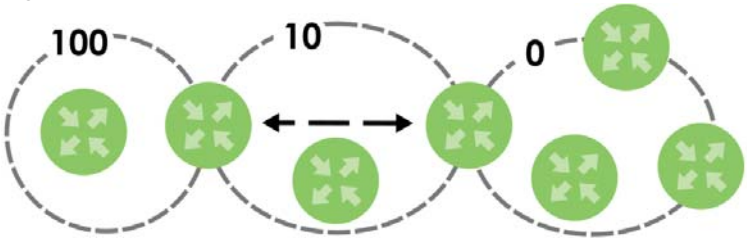
In order to reduce the amount of traffic between routers, a group of routers that are directly connected to each other selects a designated router (DR) and a backup designated router (BDR). All of the routers only exchange information with the DR and the BDR, instead of exchanging information with all of the other routers in the group. The DR and BDR are selected by priority; if two routers have the same priority, the highest router ID is used.

The DR and BDR are selected in each group of routers that are directly connected to each other. If a router is directly connected to several groups, it might be a DR in one group, a BDR in another group, and neither in a third group all at the same time.

Virtual Links

In some OSPF AS, it is not possible for an area to be directly connected to the backbone. In this case, you can create a virtual link through an intermediate area to logically connect the area to the backbone. This is illustrated in the following example.

Figure 285 OSPF: Virtual Link



In this example, area 100 does not have a direct connection to the backbone. As a result, you should set up a virtual link on both ABR in area 10. The virtual link becomes the connection between area 100 and the backbone.

You cannot create a virtual link to a router in a different area.

OSPF Configuration

Follow these steps when you configure OSPF on the Zyxel Device.

1 Enable OSPF.

2 Set up the OSPF areas.

3 Configure the appropriate interfaces. See Section 11.5.1 on page 296.

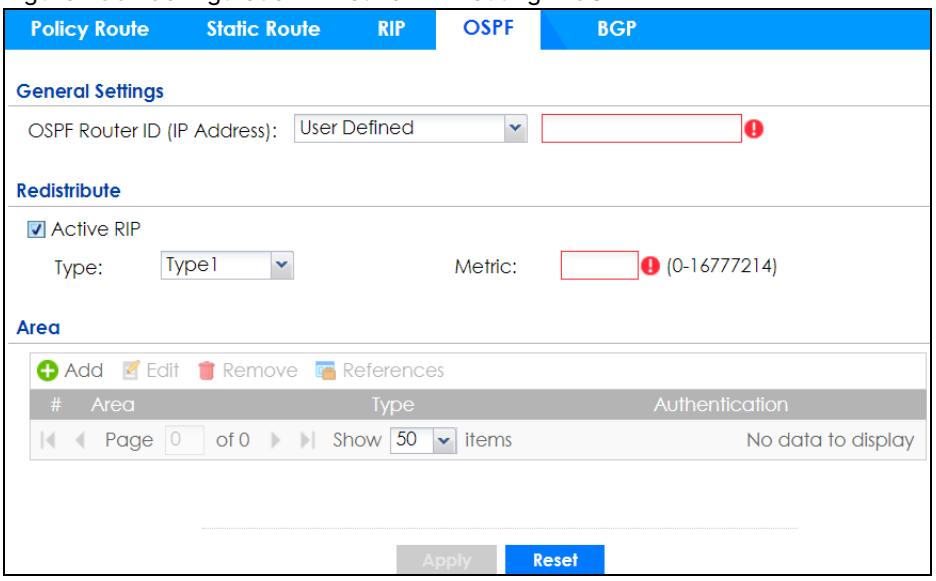
4 Set up virtual links, as needed.

12.7.1 Configuring the OSPF Screen

Use the first OSPF screen to specify the OSPF router the Zyxel Device uses in the OSPF AS and maintain the policies for redistribution. In addition, it provides a summary of OSPF areas, allows you to remove them, and opens the OSPF Add/Edit screen to add or edit them.

Click Configuration > Network > Routing > OSPF to open the following screen.

Figure 286 Configuration > Network > Routing > OSPF



The following table describes the labels in this screen. See Section 12.7.2 on page 405 for more information as well.

Table 112 Configuration > Network > Routing Protocol > OSPF

LABEL	DESCRIPTION
OSPF Router ID	Select the 32-bit ID the Zyxel Device uses in the OSPF AS. Default - the first available interface IP address is the Zyxel Device's ID. User Defined - enter the ID (in IP address format) in the field that appears when you select User Define.
Redistribute	
Active RIP	Select this to advertise routes that were learned from RIP. The Zyxel Device advertises routes learned from RIP to Normal and NSSA areas but not to Stub areas.
Type	Select how OSPF calculates the cost associated with routing information from RIP. Choices are: Type 1 and Type 2. Type 1 - cost = OSPF AS cost + external cost (Metric) Type 2 - cost = external cost (Metric); the OSPF AS cost is ignored.
Metric	Type the external cost for routes provided by RIP. The metric represents the "cost" of transmission for routing purposes. The way this is used depends on the Type field. This value is usually the average cost in the OSPF AS, and it can be between 1 and 16777214.

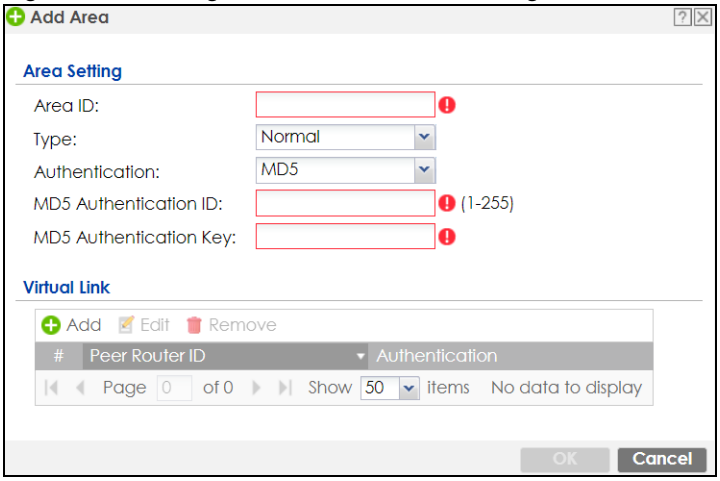
Table 112 Configuration > Network > Routing Protocol > OSPF (continued)

LABEL	DESCRIPTION
Area	This section displays information about OSPF areas in the Zyxel Device.
Add	Click this to create a new OSPF area.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click References to open a screen that shows which settings use the entry. Click Refresh to update information on this screen.
#	This field is a sequential value, and it is not associated with a specific area.
Area	This field displays the 32-bit ID for each area in IP address format.
Type	This field displays the type of area. This type is different from the Type field above.
Authentication	This field displays the default authentication method in the area.
Apply	Click this button to save your changes to the Zyxel Device.
Reset	Click this button to return the screen to its last-saved settings.

12.7.2 OSPF Area Add/Edit Screen

The OSPF Area Add/Edit screen allows you to create a new area or edit an existing one. To access this screen, go to the OSPF summary screen (see Section 12.7 on page 401), and click either the Add icon or an Edit icon.

Figure 287 Configuration > Network > Routing > OSPF > Add



The following table describes the labels in this screen.

Table 113 Configuration > Network > Routing > OSPF > Add

LABEL	DESCRIPTION
Area ID	Type the unique, 32-bit identifier for the area in IP address format.
Type	Select the type of OSPF area. Normal - This area is a normal area. It has routing information about the OSPF AS and about networks outside the OSPF AS. Stub - This area is an stub area. It has routing information about the OSPF AS but not about networks outside the OSPF AS. It depends on a default route to send information outside the OSPF AS. NSSA - This area is a Not So Stubby Area (NSSA), per RFC 1587. It has routing information about the OSPF AS and networks that are outside the OSPF AS and are directly connected to the NSSA. It does not have information about other networks outside the OSPF AS.
Authentication	Select the default authentication method used in the area. This authentication protects the integrity, but not the confidentiality, of routing updates. None uses no authentication. Text uses a plain text password that is sent over the network (not very secure). MD5 uses an MD5 password and authentication ID (most secure).
Text Authentication Key	This field is available if the Authentication is Text. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MD5 Authentication ID	This field is available if the Authentication is MD5. Type the default ID for MD5 authentication in the area. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the Authentication is MD5. Type the default password for MD5 authentication in the area. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
Virtual Link	This section is displayed if the Type is Normal. Create a virtual link if you want to connect a different area (that does not have a direct connection to the backbone) to the backbone. You should set up the virtual link on the ABR that is connected to the other area and on the ABR that is connected to the backbone.
Add	Click this to create a new virtual link.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific area.
Peer Router ID	This is the 32-bit ID (in IP address format) of the other ABR in the virtual link.

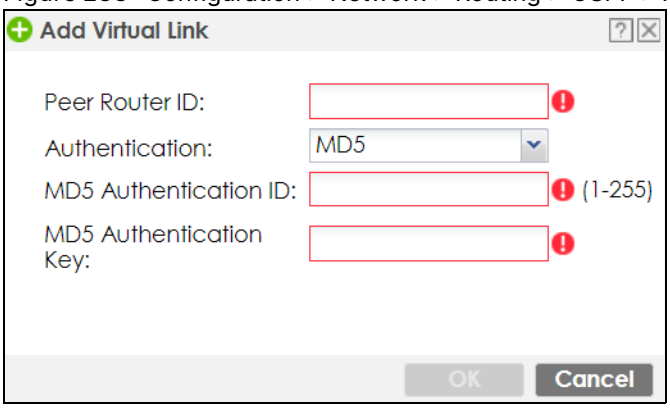
Table 113 Configuration > Network > Routing > OSPF > Add (continued)

LABEL	DESCRIPTION
Authentication	This is the authentication method the virtual link uses. This authentication protects the integrity, but not the confidentiality, of routing updates. For OSPF, the Zyxel Device supports a default authentication type by area. If you want to use this default in an interface or virtual link, you set the associated Authentication Type field to Same as Area. As a result, you only have to update the authentication information for the area to update the authentication type used by these interfaces and virtual links. Alternatively, you can override the default in any interface or virtual link by selecting a specific authentication method. Please see the respective interface sections for more information. None uses no authentication. Text uses a plain text password that is sent over the network (not very secure). Hover your cursor over this label to display the password. MD5 uses an MD5 password and authentication ID (most secure). Hover your cursor over this label to display the authentication ID and key. Same as Area has the virtual link also use the Authentication settings above.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

12.7.3 Virtual Link Add/Edit Screen

The Virtual Link Add/Edit screen allows you to create a new virtual link or edit an existing one. When the OSPF add or edit screen (see Section 12.7.2 on page 405) has the Type set to Normal, a Virtual Link table displays. Click either the Add icon or an entry and the Edit icon to display a screen like the following.

Figure 288 Configuration > Network > Routing > OSPF > Add > Add



The following table describes the labels in this screen.

Table 114 Configuration > Network > Routing > OSPF > Add > Add

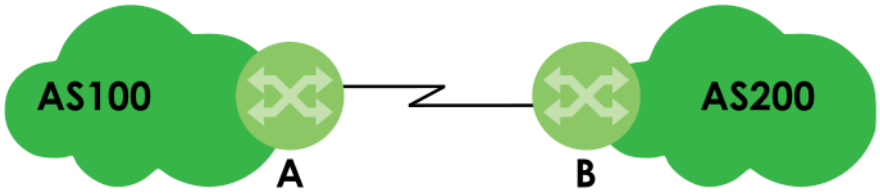
LABEL	DESCRIPTION
Peer Router ID	Enter the 32-bit ID (in IP address format) of the other ABR in the virtual link.
Authentication	Select the authentication method the virtual link uses. This authentication protects the integrity, but not the confidentiality, of routing updates. For OSPF, the Zyxel Device supports a default authentication type by area. If you want to use this default in an interface or virtual link, you set the associated Authentication Type field to Same as Area. As a result, you only have to update the authentication information for the area to update the authentication type used by these interfaces and virtual links. Alternatively, you can override the default in any interface or virtual link by selecting a specific authentication method. Please see the respective interface sections for more information. None uses no authentication. Text uses a plain text password that is sent over the network (not very secure). MD5 uses an MD5 password and authentication ID (most secure). Same as Area has the virtual link also use the Authentication settings above.
Text Authentication Key	This field is available if the Authentication is Text. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MD5 Authentication ID	This field is available if the Authentication is MD5. Type the default ID for MD5 authentication in the area. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the Authentication is MD5. Type the default password for MD5 authentication in the area. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

12.8 BGP (Border Gateway Protocol)

The Zyxel Device supports eBGP (exterior Border Gate Protocol) to route IPv4 traffic between routers in different Autonomous Systems (AS). An AS number is a number from 1 to 4294967295), that identifies an autonomous system. 4200000000 – 4294967294 are private AS numbers.

See Section 12.7 on page 401 for more information on autonomous systems.

Figure 289 eBGP Concept



12.8.1 Allow BGP Packets to Enter the Zyxel Device

You must first allow BGP packets to enter the Zyxel Device from the WAN.

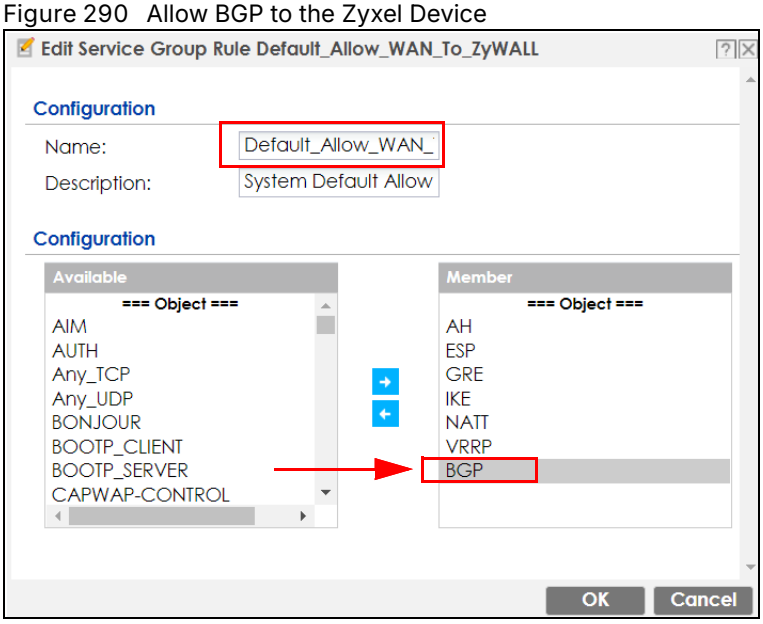
1 Go to Configuration > Object > Service > Service Group

2 Select the Default_Allow_WAN_To_ZyWALL rule and click Edit.

3 Move BGP from Available to Member.

4 Click OK.

Figure 290 Allow BGP to the Zyxel Device

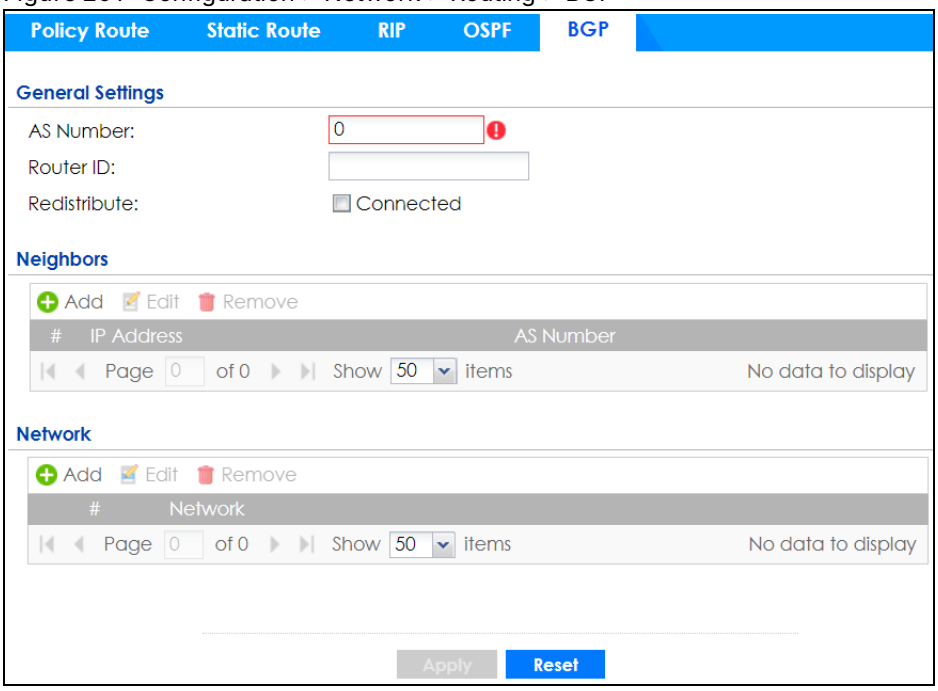


12.8.2 Configuring the BGP Screen

Use this screen to configure BGP information about the Zyxel Device and its peer BGP routers.

Click Configuration > Network > Routing > BGP to open the following screen.

Figure 291 Configuration > Network > Routing > BGP



The following table describes the labels in this screen.

Table 115 Configuration > Network > Routing Protocol > BGP

LABEL	DESCRIPTION
AS Number	Type a number from 1 to 4294967295 in this field. Note: The Zyxel Device can only belong to one AS at a time.
Router ID	Type the IP address of the interface on the Zyxel Device. This field is optional.
Redistribute	Select Connected to redistribute routes of directly attached devices to the Zyxel Device into the BGP Routing Information Base (RIB).
Neighbors	This section displays information about peer BGP routers in neighboring AS'. Note: The maximum number of neighboring BGP routers supported by the Zyxel Device is 5.
Add	Click this to configure BGP criteria for a new peer BGP router.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific area.
IP Address	This displays the IPv4 address of the peer BGP router in a neighboring AS.
AS Number	This displays the AS Number of the peer BGP router in a neighboring AS.
Network	Use this section to add routes that will be announced to all BGP neighbors. Note: You may configure up to 16 network routes.
Add	Click this to configure network information for a new route.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.

Table 115 Configuration > Network > Routing Protocol > BGP (continued)

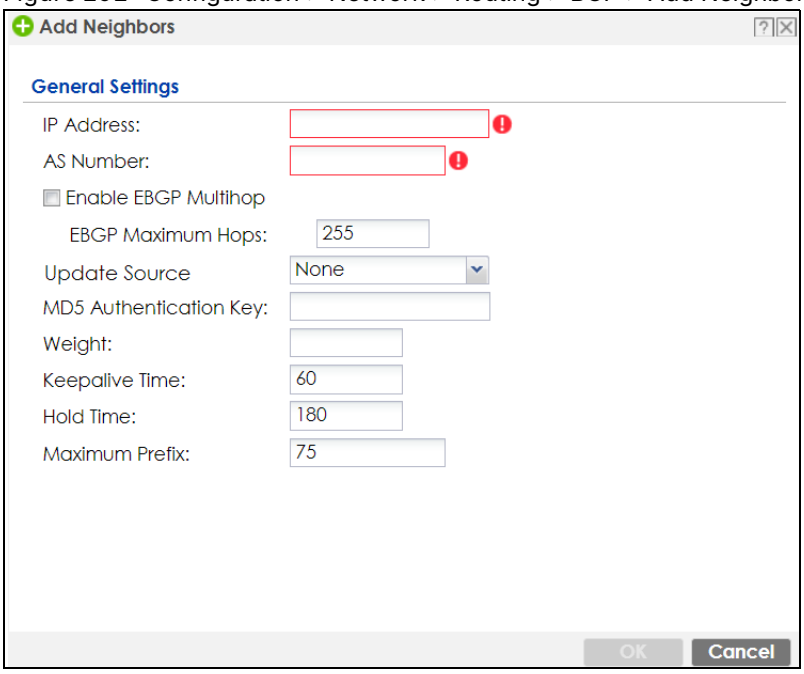
LABEL	DESCRIPTION
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific area.
Network	This displays the IP address and the number of subnet mask bits for the peer BGP route.
Apply	Click this button to save your changes to the Zyxel Device.
Reset	Click this button to return the screen to its last-saved settings.

12.8.3 The BGP Neighbors Screen

Use this screen to configure BGP information about a peer BGP router.

Click Configuration > Network > Routing > BGP > Add Neighbors to open the following screen.

Figure 292 Configuration > Network > Routing > BGP > Add Neighbors



The following table describes the labels in this screen.

Table 116 Configuration > Network > Routing Protocol > BGP

LABEL	DESCRIPTION
IP Address	Type the IP address of the interface on the peer BGP router.
AS Number	Type a number from 1 to 4294967295 in this field. Get the number from your service provider.
Enable EBGP Multihop	Select this to allow the Zyxel Device to attempt BGP connections to external peers on indirectly connected networks. eBGP neighbors must also perform multihop. Multihop is not established if the only route to the multihop peer is a default route. This avoids loop formation.
EBGP Maximum Hops	Enter a maximum hop count from <1-255>. The default is 255.

Table 116 Configuration > Network > Routing Protocol > BGP (continued)

LABEL	DESCRIPTION
Update Source	Use this to allow BGP sessions use the selected interface for TCP connections. • Choose Gateway and then enter the gateway IP address • Choose Interface and then select a Zyxel Device interface. • Choose None to use the closest interface.
MD5 authentication key	Type the default password for MD5 authentication of communication between the Zyxel Device and the peer BGP router. The password can consist of alphanumeric characters and the underscore, and it can be up to 63 characters long.
Weight	Specify a weight value for all routes learned from this peer BGP router in the specified network. The route with the highest weight gets preference.
Keepalive Time	Keepalive messages are sent by the Zyxel Device to a peer BGP router to inform it that the BGP connection between the two is still active. The Keepalive Time is the interval between each Keepalive message sent by the Zyxel Device. We recommend Keepalive Time is 1/3 of the Hold Time time.
Hold Time	This is the maximum time the Zyxel Device waits to receive a Keepalive message from a peer BGP router before it declares that the peer BGP router is dead. Hold Time must be greater than the Keepalive Time.
Maximum Prefix	A prefix is a network address (IP/subnet mask) that a BGP router can reach and that it shares with its neighbors. Set the maximum number, from 1 to 4294967295, of prefixes that can be received from a neighbor. This limits the number of prefixes that the Zyxel Device is allowed to receive from a neighbor. If extra prefixes are received, the Zyxel Device ends the connection with the peer BGP router. You need to edit the peer BGP router configuration to bring the connection back.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

12.8.4 Example Scenario

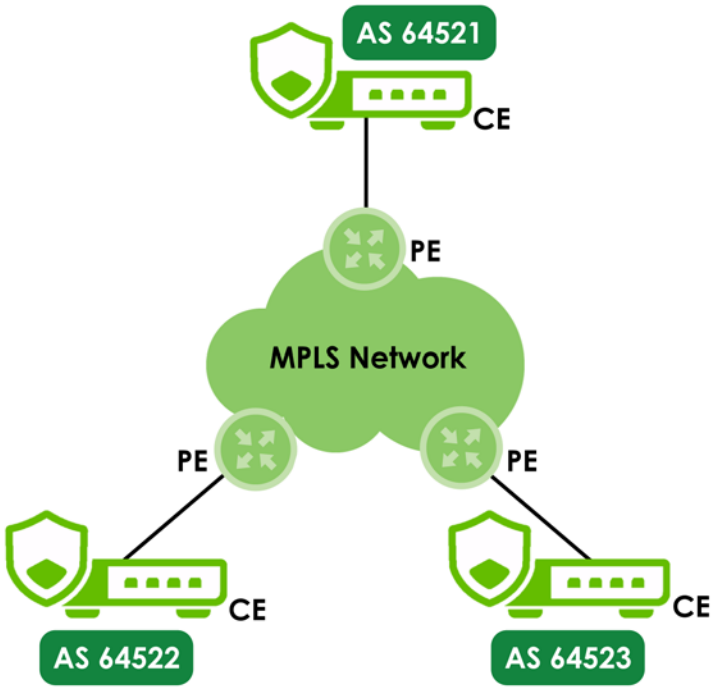
This is an example scenario for using BGP on the Zyxel Device.

12.8.4.1 Scenario: CE - PE (MLPS)

In this scenario, you want to transmit BGP packets from a CE router (Zyxel Device) to a peer BGP PE router in an MPLS network.

- CE: The Zyxel Device is the customer edge router located on the customer premises and connects to a PE router in the service provider MPLS network.
- PE: The provider edge router is located at the edge of the service provider MPLS network.
- MPLS: MultiProtocol Label Switching (MPLS) forwards data from one network node to the next based on path labels rather than network addresses.

Figure 293 Scenario 1: CE Router - to - MPLS



12.8.4.2 CE - PE Configuration Process

The process for configuring BGP in this scenario is:

1. Configure the AS number for BGP on the Zyxel Device (CE) in Configuration > Network > Routing > BGP.

   Note: The Zyxel Device can only belong to one AS at a time.

2. Configure the AS number and BGP criteria of the peer BGP routers (PE) in the neighboring AS in Configuration > Network > Routing > BGP > Add Neighbors.

   Note: The maximum number of neighboring BGP routers supported by the Zyxel Device is 5.

3. Configure the network for BGP routes in the neighboring AS.

   Note: You may configure up to 16 network routes.

CHAPTER 13
DDNS

13.1 DDNS Overview

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

13.1.1 What You Can Do in this Chapter

- Use the DDNS screen (see Section 13.2 on page 415) to view a list of the configured DDNS domain names and their details.
- Use the DDNS Add/Edit screen (see Section 13.2.1 on page 416) to add a domain name to the Zyxel Device or to edit the configuration of an existing domain name.

13.1.2 What You Need to Know

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

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

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

Table 117 DDNS Service Providers

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

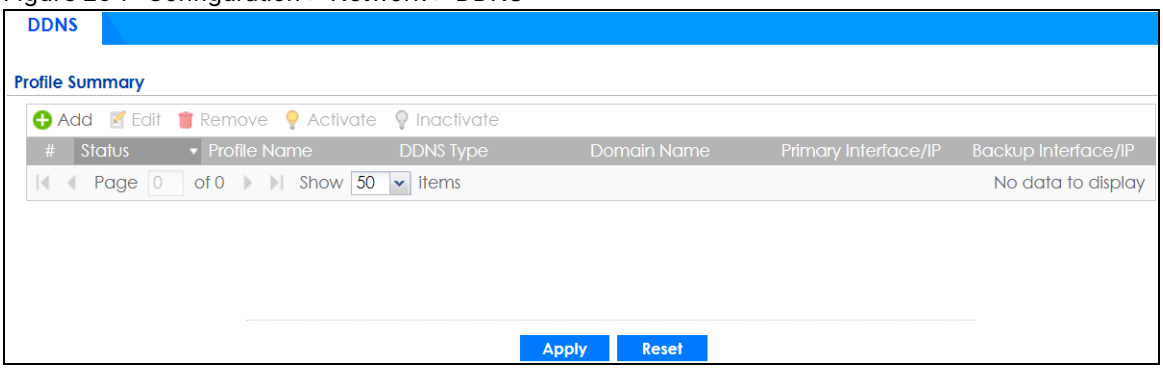
Note: Record your DDNS account's user name, password, and domain name to use to configure the Zyxel Device.

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

13.2 The DDNS Screen

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

Figure 294 Configuration > Network > DDNS



The following table describes the labels in this screen.

Table 118 Configuration > Network > DDNS

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

Table 118 Configuration > Network > DDNS (continued)

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

13.2.1 The Dynamic DNS Add/Edit Screen

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

Figure 295 Configuration > Network > DDNS > Add

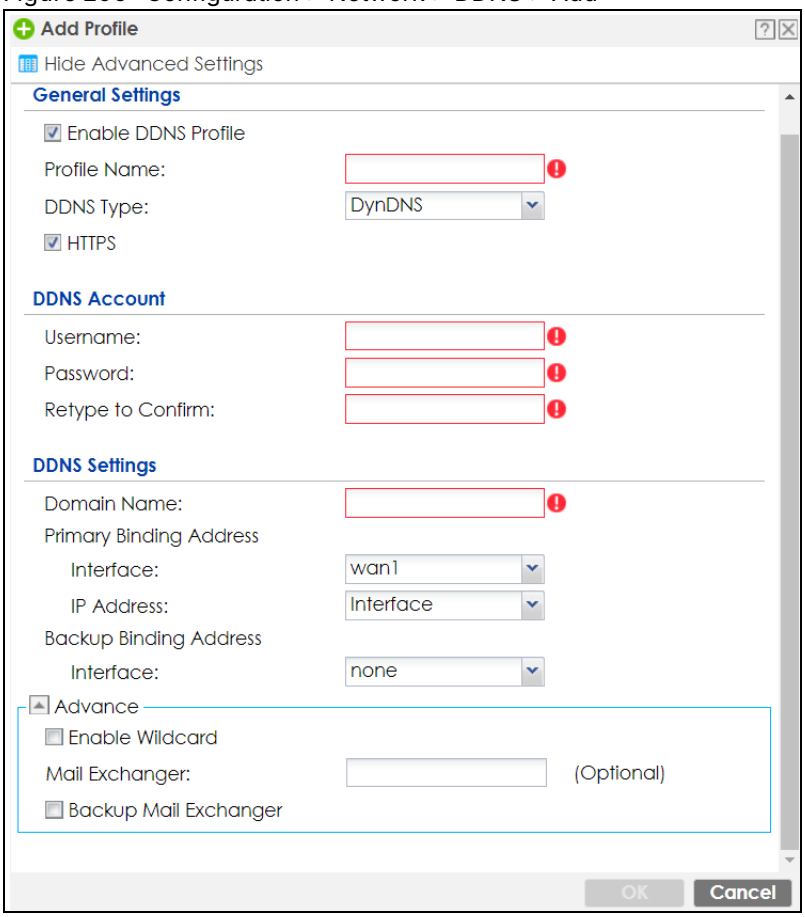
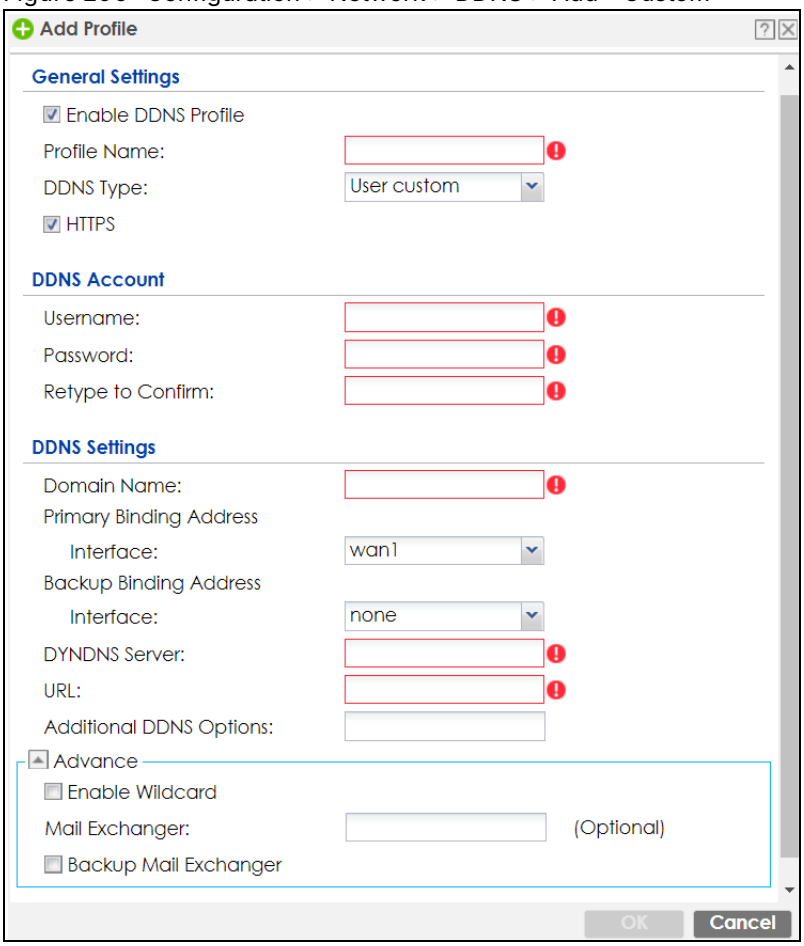


Figure 296 Configuration > Network > DDNS > Add - Custom



The following table describes the labels in this screen.

Table 119 Configuration > Network > DDNS > Add

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Enable DDNS Profile	Select this checkbox to use this DDNS entry.
Profile Name	When you are adding a DDNS entry, type a descriptive name for this DDNS entry in the Zyxel Device. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. This field is read-only when you are editing an entry.
DDNS Type	Select the type of DDNS service you are using. Select User custom to create your own DDNS service and configure the DYNDNS Server, URL, and Additional DDNS Options fields below.
HTTPS	Select this to encrypt traffic using SSL (port 443), including traffic with username and password, to the DDNS server. Not all DDNS providers support this option.
Username	Type the user name used when you registered your domain name. You can use up to 31 alphanumeric characters and the underscore. Spaces are not allowed. For a Dynu DDNS entry, this user name is the one you use for logging into the service, not the name recorded in your personal information in the Dynu website.

Table 119 Configuration > Network > DDNS > Add (continued)

LABEL	DESCRIPTION
Password	Type the password provided by the DDNS provider. You can use up to 64 alphanumeric characters and the underscore. Spaces are not allowed. Your password will be encrypted when you configure this field.
Retype to Confirm	Type the password again to confirm it.
DDNS Settings	
Domain name	Type the domain name you registered. You can use up to 255 characters.
Primary Binding Address	Use these fields to set how the Zyxel Device determines the IP address that is mapped to your domain name in the DDNS server. The Zyxel Device uses the Backup Binding Address if the interface specified by these settings is not available.
Interface	Select the interface to use for updating the IP address mapped to the domain name. Select Any to let the domain name be used with any interface.
IP Address	The options available in this field vary by DDNS provider. Interface -The Zyxel Device uses the IP address of the specified interface. This option appears when you select a specific interface in the Primary Binding Address Interface field. Auto - If the interface has a dynamic IP address, the DDNS server checks the source IP address of the packets from the Zyxel Device for the IP address to use for the domain name. You may want to use this if there are one or more NAT routers between the Zyxel Device and the DDNS server. Note: The Zyxel Device may not determine the proper IP address if there is an HTTP proxy server between the Zyxel Device and the DDNS server. Custom - If you have a static IP address, you can select this to use it for the domain name. The Zyxel Device still sends the static IP address to the DDNS server.
Custom IP	This field is only available when the IP Address is Custom. Type the IP address to use for the domain name.
Backup Binding Address	Use these fields to set an alternate interface to map the domain name to when the interface specified by the Primary Binding Interface settings is not available.
Interface	Select the interface to use for updating the IP address mapped to the domain name. Select Any to let the domain name be used with any interface. Select None to not use a backup address.
IP Address	The options available in this field vary by DDNS provider. Interface -The Zyxel Device uses the IP address of the specified interface. This option appears when you select a specific interface in the Backup Binding Address Interface field. Auto -The DDNS server checks the source IP address of the packets from the Zyxel Device for the IP address to use for the domain name. You may want to use this if there are one or more NAT routers between the Zyxel Device and the DDNS server. Note: The Zyxel Device may not determine the proper IP address if there is an HTTP proxy server between the Zyxel Device and the DDNS server. Custom - If you have a static IP address, you can select this to use it for the domain name. The Zyxel Device still sends the static IP address to the DDNS server.
Custom IP	This field is only available when the IP Address is Custom. Type the IP address to use for the domain name.
Enable Wildcard	This option is only available with a DynDNS account. Enable the wildcard feature to alias subdomains to be aliased to the same IP address as your (dynamic) domain name. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

Table 119 Configuration > Network > DDNS > Add (continued)

LABEL	DESCRIPTION
Mail Exchanger	This option is only available with a DynDNS account. DynDNS can route email for your domain name to a mail server (called a mail exchanger). For example, DynDNS routes email for john-doe@yourhost.dyndns.org to the host record specified as the mail exchanger. If you are using this service, type the host record of your mail server here. Otherwise leave the field blank. See www.dyndns.org for more information about mail exchangers.
Backup Mail Exchanger	This option is only available with a DynDNS account. Select this checkbox if you are using DynDNS's backup service for email. With this service, DynDNS holds onto your email if your mail server is not available. Once your mail server is available again, the DynDNS server delivers the mail to you. See www.dyndns.org for more information about this service.
DYNDNS Server	This field displays when you select User custom from the DDNS Type field above. Type the IP address of the server that will host the DDSN service.
URL	This field displays when you select User custom from the DDNS Type field above. Type the URL that can be used to access the server that will host the DDSN service.
Additional DDNS Options	This field displays when you select User custom from the DDNS Type field above. These are the options supported at the time of writing: • dyndns_system to specify the DYNDNS Server type - for example, dyndns@dyndns.org • ip_server_name which should be the URL to get the server's public IP address - for example, http://myip.easylife.tw/
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

CHAPTER 14
NAT

14.1 Overview

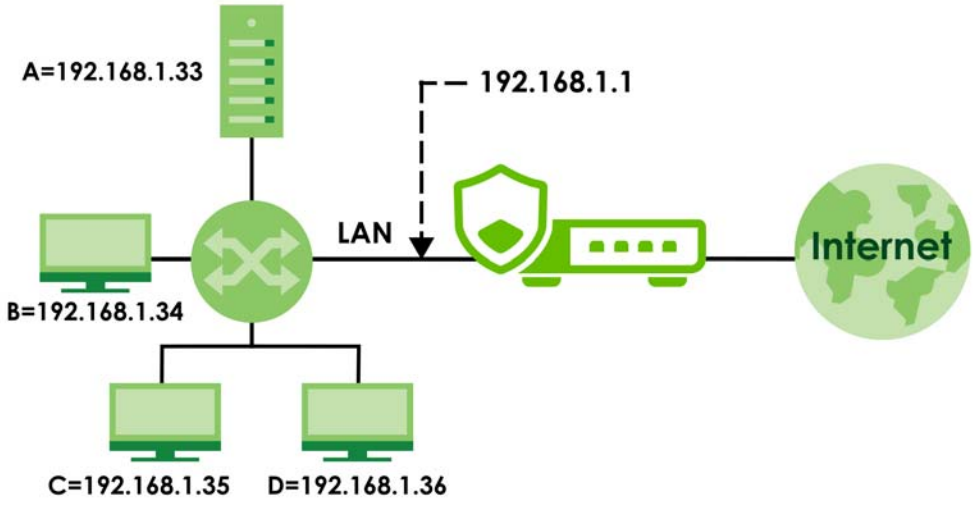
- Use the Network > NAT screen (Section 14.2 on page 420) to enable and configure network address translation.

14.2 NAT Overview

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

Suppose you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), port 80 to another (B in the example) and assign a default server IP address of 192.168.1.35 to a third (C in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 297 Multiple Servers Behind NAT Example



14.2.1 What You Can Do in this Chapter

Use the NAT screens (see Section 14.3 on page 422) to view and manage the list of NAT rules and see their configuration details. You can also create new NAT rules and edit or delete existing ones.

14.2.2 What You Need to Know

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

Well-known Ports

Port numbers range from 0 to 65535, but only port numbers 0 to 1023 are reserved for privileged services and designated as well-known ports. The following list specifies the ports used by the server process as its contact ports. See Section 30.5 on page 716 (Configuration > Object > Service) for more information about service objects.

- Well-known ports range from 0 to 1023.
- Registered ports range from 1024 to 49151.
- Dynamic ports (also called private ports) range from 49152 to 65535.

Table 120 Well-known Ports

PORT	TCP/UDP	DESCRIPTION
1	TCP	TCP Port Service Multiplexer (TCPMUX)
20	TCP	FTP - Data
21	TCP	FTP - Control
22	TCP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol (SMTP)
42	UDP	Host Name Server (Nameserv)
43	TCP	WhoIs
53	TCP/UDP	Domain Name System (DNS)
67	UDP	BOOTP/DHCP server
68	UDP	BOOTP/DHCP client
69	UDP	Trivial File Transfer Protocol (TFTP)
79	TCP	Finger
80	TCP	HTTP
110	TCP	POP3
119	TCP	Newsgroup (NNTP)
123	UDP	Network Time Protocol (NTP)
135	TCP/UDP	RPC Locator service
137	TCP/UDP	NetBIOS Name Service
138	UDP	NetBIOS Datagram Service
139	TCP	NetBIOS Datagram Service
143	TCP	Interim Mail Access Protocol (IMAP)
161	UDP	SNMP
179	TCP	Border Gateway Protocol (BGP)
389	TCP/UDP	Lightweight Directory Access Protocol (LDAP)
443	TCP	HTTPS
445	TCP	Microsoft - DS
636	TCP	LDAP over TLS/SSL (LDAPS)
953	TCP	BIND DNS

Table 120 Well-known Ports

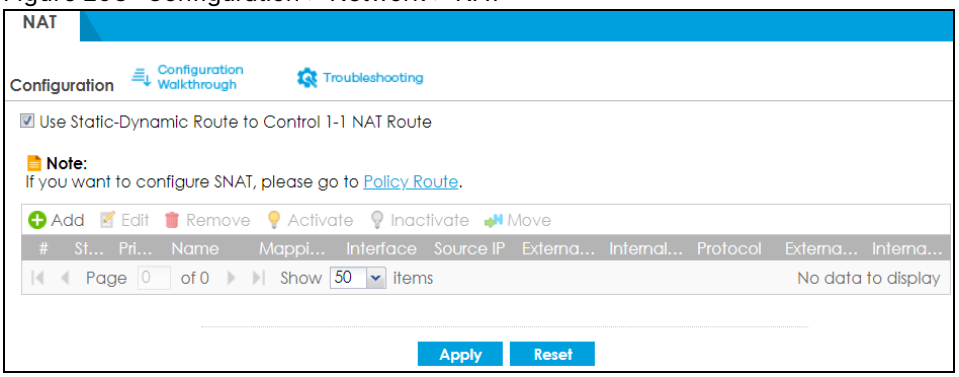
PORT	TCP/UDP	DESCRIPTION
990	TCP	FTP over TLS/SSL (FTPS)
995	TCP	POP3 over TLS/SSL (POP3S)

14.3 The NAT Screen

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

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

Figure 298 Configuration > Network > NAT



The following table describes the labels in this screen.

Table 121 Configuration > Network > NAT

LABEL	DESCRIPTION
Use Static-Dynamic Route to Control 1-1 NAT Route	If you are using SiteToSite VPN and 1-1 SNAT, it's recommended that you select this checkbox. Otherwise, you'll need to create policy route rules for VPN and Destination NAT traffic. Note that the selection of this checkbox will change the priority of the routing flow (SiteToSite VPN, Static-Dynamic Route, and 1-1 SNAT). See Packet Flow Explore for more information about the routing flow.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The 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.
Move	To change a rule's position in the numbered list, select the rule and click Move to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.

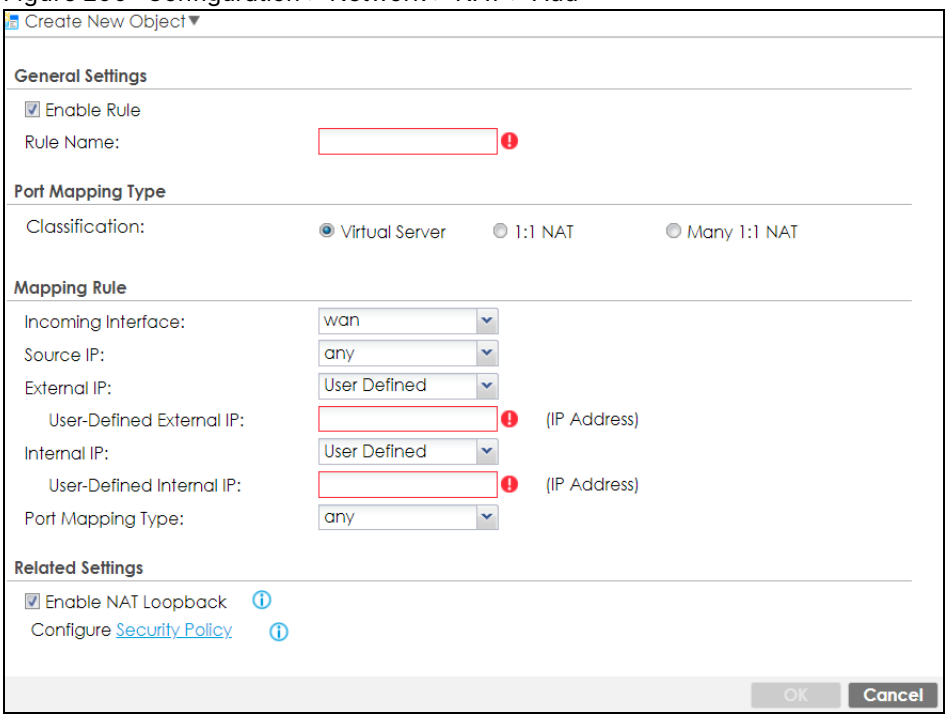
Table 121 Configuration > Network > NAT (continued)

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Priority	This field displays the priority for the entry. The smaller the number, the higher the priority.
Name	This field displays the name of the entry.
Mapping Type	This field displays what kind of NAT this entry performs: Virtual Server, 1:1 NAT, or Many 1:1 NAT.
Interface	This field displays the interface on which packets for the NAT entry are received.
Source IP	This field displays the source IP address (or address object) of traffic that matches this NAT entry. It displays any if there is no restriction on the source IP address.
External IP	This field displays the original destination IP address (or address object) of traffic that matches this NAT entry. It displays any if there is no restriction on the original destination IP address.
Internal IP	This field displays the new destination IP address for the packet.
Protocol	This field displays the service used by the packets for this NAT entry. It displays any if there is no restriction on the services.
External Port	This field displays the original destination port(s) of packets for the NAT entry. This field is blank if there is no restriction on the original destination port.
Internal Port	This field displays the new destination port(s) for the packet. This field is blank if there is no restriction on the original destination port.
Apply	Click this button to save your changes to the Zyxel Device.
Reset	Click this button to return the screen to its last-saved settings.

14.3.1 The NAT Add/Edit Screen

The NAT Add/Edit screen lets you create new NAT rules and edit existing ones. To open this window, open the NAT summary screen. (See Section 14.3 on page 422.) Then, click on an Add icon or Edit icon to open the following screen.

Figure 299 Configuration > Network > NAT > Add



The following table describes the labels in this screen.

Table 122 Configuration > Network > NAT > Add

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable Rule	Use this option to turn the NAT rule on or off.
Rule Name	Type in the name of the NAT rule. The name is used to refer to the NAT rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Classification	Select what kind of NAT this rule is to perform. Virtual Server - This makes computers on a private network behind the Zyxel Device available to a public network outside the Zyxel Device (like the Internet). 1:1 NAT - If the private network server will initiate sessions to the outside clients, select this to have the Zyxel Device translate the source IP address of the server's outgoing traffic to the same public IP address that the outside clients use to access the server. Many 1:1 NAT - If you have a range of private network servers that will initiate sessions to the outside clients and a range of public IP addresses, select this to have the Zyxel Device translate the source IP address of each server's outgoing traffic to the same one of the public IP addresses that the outside clients use to access the server. The private and public ranges must have the same number of IP addresses. One many 1:1 NAT rule works like multiple 1:1 NAT rules, but it eases configuration effort since you only create one rule.
Incoming Interface	Select the interface on which packets for the NAT rule must be received. It can be an Ethernet, VLAN, bridge, or PPPoE/PPTP interface.

Table 122 Configuration > Network > NAT > Add (continued)

LABEL	DESCRIPTION
Source IP	Specify the source IP address of the packets received by this NAT rule's specified incoming interface. any - Select this to use all of the incoming interface's IP addresses including dynamic addresses or those of any virtual interfaces built upon the selected incoming interface. User Defined - Select this to manually enter an IP address in the User Defined field. For example, you could enter a static IP address. Host address - select a address object to use the IP address it specifies.
External IP	Specify the destination IP address of the packets received by this NAT rule's specified incoming interface. The specified IP address will be translated to the Internal IP address. any - Select this to use all of the incoming interface's IP addresses including dynamic addresses or those of any virtual interfaces built upon the selected incoming interface. User Defined - Select this to manually enter an IP address in the User Defined field. For example, you could enter a static public IP assigned by the ISP without having to create a virtual interface for it. Host address - select a host address object to use the IP address it specifies. The list also includes address objects based on interface IPs. So for example you could select an address object based on a WAN interface even if it has a dynamic IP address.
User Defined External IP	This field is available if External IP is User Defined. Type the destination IP address that this NAT rule supports.
External IP Subnet/ Range	This field displays for Many 1:1 NAT. Select the destination IP address subnet or IP address range that this NAT rule supports. The original and mapped IP address subnets or ranges must have the same number of IP addresses.
Internal IP	Select to which translated destination IP address this NAT rule forwards packets. User Defined - this NAT rule supports a specific IP address, specified in the User Defined field. HOST address - the drop-down box lists all the HOST address objects in the Zyxel Device. If you select one of them, this NAT rule supports the IP address specified by the address object.
User Defined Internal IP	This field is available if Internal IP is User Defined. Type the translated destination IP address that this NAT rule supports.
Internal IP Subnet/ Range	This field displays for Many 1:1 NAT. Select to which translated destination IP address subnet or IP address range this NAT rule forwards packets. The original and mapped IP address subnets or ranges must have the same number of IP addresses.
Port Mapping Type	Use the drop-down list box to select how many original destination ports this NAT rule supports for the selected destination IP address (Original IP). Choices are: Any - this NAT rule supports all the destination ports. Port - this NAT rule supports one destination port. Ports - this NAT rule supports a range of destination ports. You might use a range of destination ports for unknown services or when one server supports more than one service. Service - this NAT rule supports a service such as FTP (see Object > Service > Service) Service-Group - this NAT rule supports a group of services such as all service objects related to DNS (see Object > Service > Service Group)
Protocol Type	This field is available if Mapping Type is Port or Ports. Select the protocol (TCP, UDP, or Any) used by the service requesting the connection.
External Port	This field is available if Mapping Type is Port. Enter the external destination port this NAT rule supports.

Table 122 Configuration > Network > NAT > Add (continued)

LABEL	DESCRIPTION
Internal Port	This field is available if Mapping Type is Port. Enter the translated destination port if this NAT rule forwards the packet.
External Start Port	This field is available if Mapping Type is Ports. Enter the beginning of the range of original destination ports this NAT rule supports.
External End Port	This field is available if Mapping Type is Ports. Enter the end of the range of original destination ports this NAT rule supports.
Internal Start Port	This field is available if Mapping Type is Ports. Enter the beginning of the range of translated destination ports if this NAT rule forwards the packet.
Internal End Port	This field is available if Mapping Type is Ports. Enter the end of the range of translated destination ports if this NAT rule forwards the packet. The original port range and the mapped port range must be the same size.
Enable NAT Loopback	Enable NAT loopback to allow users connected to any interface (instead of just the specified Incoming Interface) to use the NAT rule's specified External IP address to access the Internal IP device. For users connected to the same interface as the Internal IP device, the Zyxel Device uses that interface's IP address as the source address for the traffic it sends from the users to the Internal IP device. For example, if you configure a NAT rule to forward traffic from the WAN to a LAN server, enabling NAT loopback allows users connected to other interfaces to also access the server. For LAN users, the Zyxel Device uses the LAN interface's IP address as the source address for the traffic it sends to the LAN server. See NAT Loopback on page 427 for more details. If you do not enable NAT loopback, this NAT rule only applies to packets received on the rule's specified incoming interface.
Security Policy	By default the security policy blocks incoming connections from external addresses. After you configure your NAT rule settings, click the Security Policy link to configure a security policy to allow the NAT rule's traffic to come in. The Zyxel Device checks NAT rules before it applies To-Zyxel Device security policies, so To-Zyxel Device security policies, do not apply to traffic that is forwarded by NAT rules. The Zyxel Device still checks other security policies, according to the source IP address and mapped IP address.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to return to the NAT summary screen without creating the NAT rule (if it is new) or saving any changes (if it already exists).

Note: If you set the User-Defined External IP to the IP address of the web configurator and set the External Port to 80 or 443, this rule will conflict with the Zyxel Device's default HTTP server port.

A warning message will pop out when you click OK. If you click No in the warning message, the rule will apply to the Zyxel Device. You will not be able to access the web configurator through this interface.

14.4 NAT Technical Reference

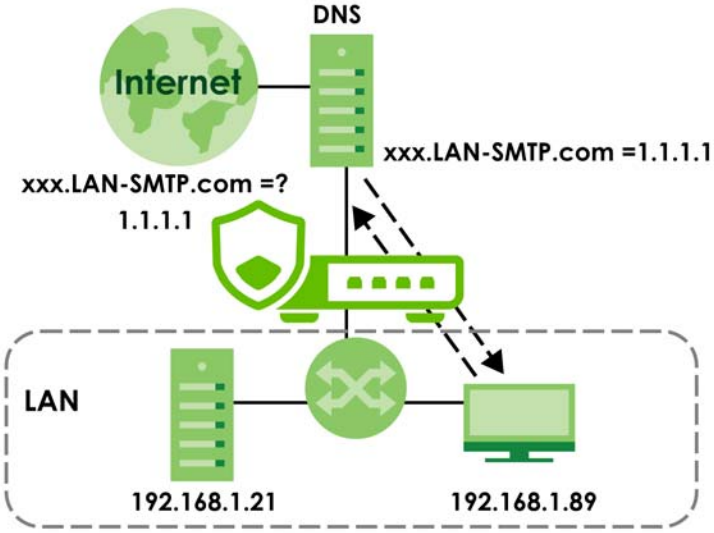
Here is more detailed information about NAT on the Zyxel Device.

NAT Loopback

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

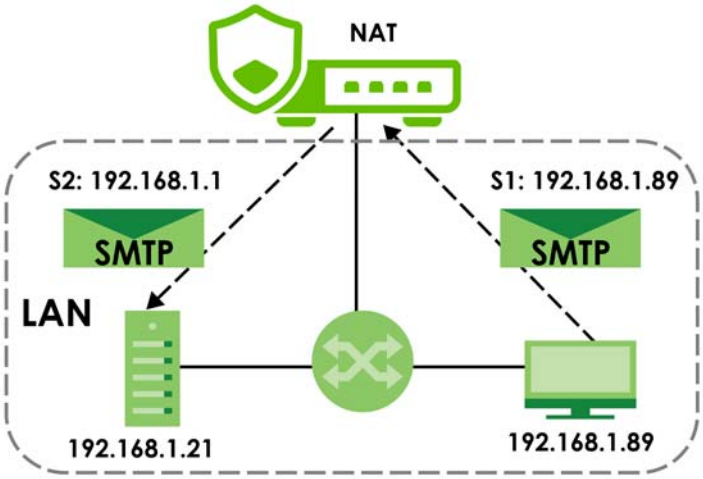
For example, a LAN user's computer at IP address 192.168.1.89 queries a public DNS server to resolve the SMTP server's domain name (xxx.LAN-SMTP.com in this example) and gets the SMTP server's mapped public IP address of 1.1.1.1.

Figure 300 LAN Computer Queries a Public DNS Server



The LAN user's computer then sends traffic to IP address 1.1.1.1. NAT loopback uses the IP address of the Zyxel Device's LAN interface (S2: 192.168.1.1) as the source address of the traffic going from the LAN users to the LAN SMTP server.

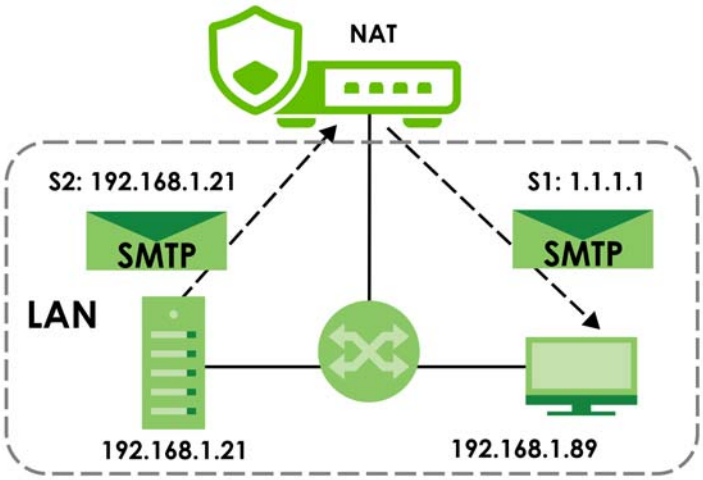
Figure 301 LAN to LAN Traffic



The LAN SMTP server replies to the Zyxel Device's LAN IP address and the Zyxel Device changes the source address to 1.1.1.1 before sending it to the LAN user. The return traffic's source matches the original destination address (S1: 1.1.1.1). If the SMTP server replied directly to the LAN user without the traffic

going through NAT, the source would not match the original destination address which would cause the LAN user's computer to shut down the session.

Figure 302 LAN to LAN Return Traffic



CHAPTER 15
Redirect Service

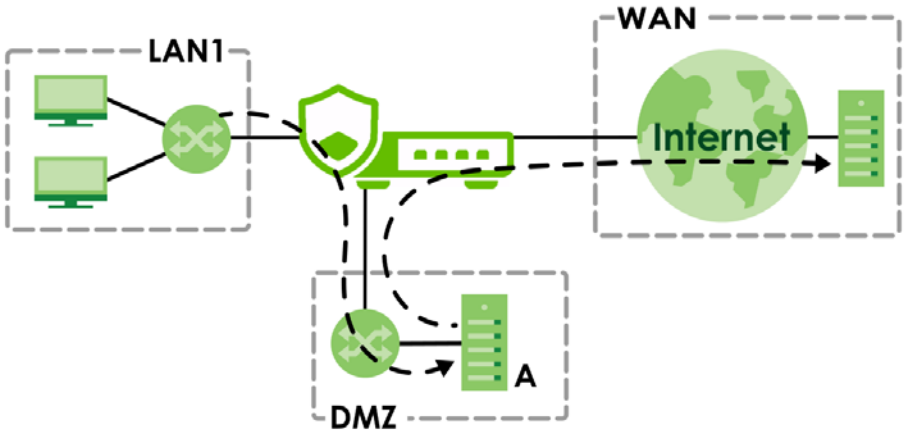
15.1 Overview

Redirect Service redirects HTTP and SMTP traffic.

15.1.1 HTTP Redirect

HTTP redirect forwards the client's HTTP request (except HTTP traffic destined for the Zyxel Device) to a web proxy server. In the following example, proxy server A is connected to the DMZ interface. When a client connected to the LAN1 zone wants to open a web page, its HTTP request is redirected to proxy server A first. If proxy server A cannot find the web page in its cache, a policy route allows it to access the Internet to get them from a server. Proxy server A then forwards the response to the client.

Figure 303 HTTP Redirect Example

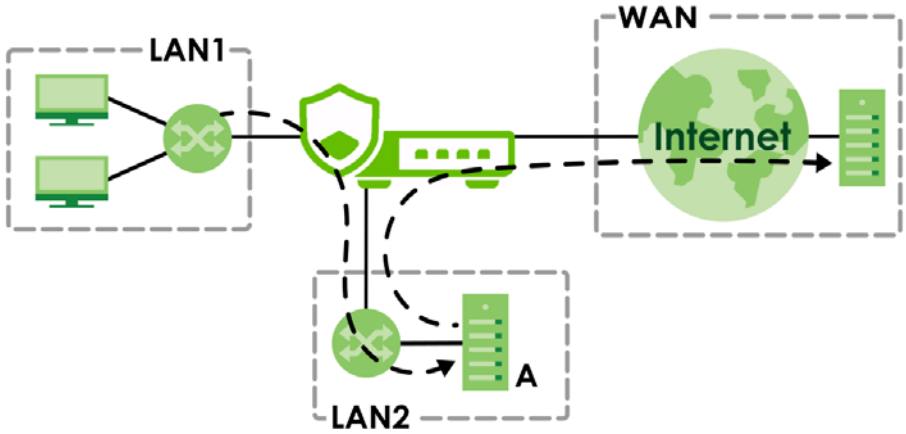


15.1.2 SMTP Redirect

SMTP redirect forwards the authenticated client's SMTP message to a SMTP server, that handles all outgoing email messages. In the following example, SMTP server A is connected to the lan2 interface in the LAN2 zone. When a client connected to the lan1 interface in the LAN1 zone logs into the Zyxel Device and wants to send an email, its SMTP message is redirected to SMTP server A. SMTP server A then sends it to a mail server, where the message will be delivered to the recipient.

The Zyxel Device forwards SMTP traffic using TCP port 25.

Figure 304 SMTP Redirect Example



15.1.3 What You Can Do in this Chapter

Use the Redirect Service screens (see Section 15.2 on page 432) to display and edit the HTTP and SMTP redirect rules.

15.1.4 What You Need to Know

Web Proxy Server

A proxy server helps client devices make indirect requests to access the Internet or outside network resources/services. A proxy server can act as a security policy or an ALG (application layer gateway) between the private network and the Internet or other networks. It also keeps hackers from knowing internal IP addresses.

A client connects to a web proxy server each time he/she wants to access the Internet. The web proxy provides caching service to allow quick access and reduce network usage. The proxy checks its local cache for the requested web resource first. If it is not found, the proxy gets it from the specified server and forwards the response to the client.

HTTP Redirect, Security Policy and Policy Route

With HTTP redirect, the relevant packet flow for HTTP traffic is:

1. Security Policy
2. HTTP Redirect
3. Policy Route

Even if you set a policy route to the same incoming interface and service as a HTTP redirect rule, the Zyxel Device checks the HTTP redirect rules first and forwards HTTP traffic to a proxy server if matched. You need to make sure there is no security policy blocking the HTTP requests from the client to the proxy server.

You also need to manually configure a policy route to forward the HTTP traffic from the proxy server to the Internet. To make the example in Figure 303 on page 429 work, make sure you have the following settings.

For HTTP traffic between lan1 and dmz:

- a from LAN1 to DMZ security policy (default) to allow HTTP requests from lan1 to dmz. Responses to this request are allowed automatically.
- a HTTP redirect rule to forward HTTP traffic from lan1 to proxy server A.

For HTTP traffic between dmz and wan1:

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

SMTP

Simple Mail Transfer Protocol (SMTP) is the Internet's message transport standard. It controls the sending of email messages between servers. Email clients (also called email applications) then use mail server protocols such as POP (Post Office Protocol) or IMAP (Internet Message Access Protocol) to retrieve email. Email clients also generally use SMTP to send messages to a mail server. The older POP2 requires SMTP for sending messages while the newer POP3 can be used with or without it. This is why many email applications require you to specify both the SMTP server and the POP or IMAP server (even though they may actually be the same server).

SMTP Redirect, Firewall and Policy Route

With SMTP redirect, the relevant packet flow for SMTP traffic is:

1. Firewall
2. SMTP Redirect
3. Policy Route

Even if you set a policy route to the same incoming interface and service as a SMTP redirect rule, the Zyxel Device checks the SMTP redirect rules first and forwards SMTP traffic to a SMTP server if matched. You need to make sure there is no firewall rule(s) blocking the SMTP traffic from the client to the SMTP server.

You also need to manually configure a policy route to forward the SMTP traffic from the SMTP server to the Internet. To make the example in Figure 304 on page 430 work, make sure you have the following settings.

For SMTP traffic between lan1 and lan2:

- a from LAN1 to LAN2 firewall rule to allow SMTP messages from lan1 to lan2. Responses to this request are allowed automatically.
- a SMTP redirect rule to forward SMTP traffic from lan1 to SMTP server A.

For SMTP traffic between lan2 and wan1:

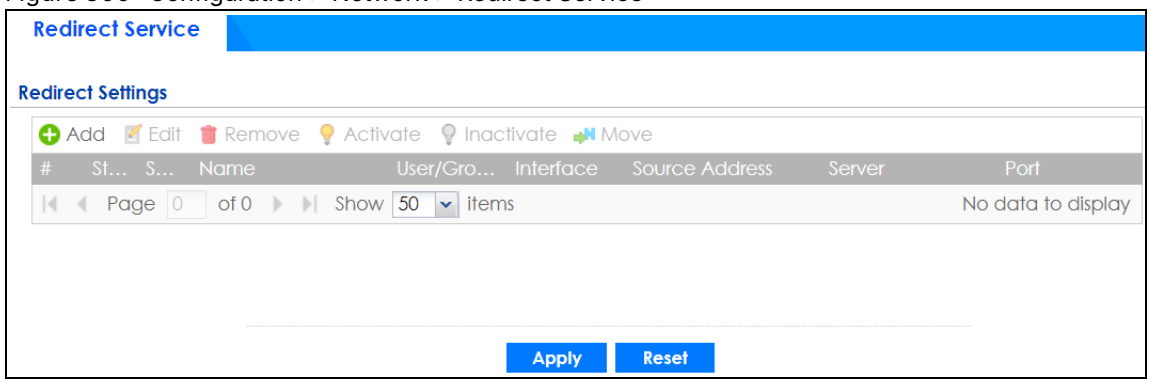
- a from LAN2 to WAN firewall rule (default) to allow SMTP messages from lan2 to wan1. Responses to these requests are allowed automatically.
- a policy route to forward SMTP messages from SMTP server A to the Internet.

15.2 The Redirect Service Screen

To configure redirection of a HTTP or SMTP request, click Configuration > Network > HTTP Redirect. This screen displays the summary of the redirect rules.

Note: You can configure up to one HTTP redirect rule and one SMTP redirect rule for each (incoming) interface.

Figure 305 Configuration > Network > Redirect Service



The following table describes the labels in this screen.

Table 123 Configuration > Network > Redirect Service

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The 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.
Move	To change a rule's position in the numbered list, select the rule and click Move to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
#	This field is a sequential value, and it is not associated with a specific entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Service	This is the name of the service: HTTP or SMTP.
Name	This is the descriptive name of a rule.
User/Group	This is the user account or user group name to which this rule is applied.
Interface	This is the interface on which the request must be received.
Source Address	This is the name of the source IP address object from which the traffic should be sent. If any displays, the rule is effective for every source.

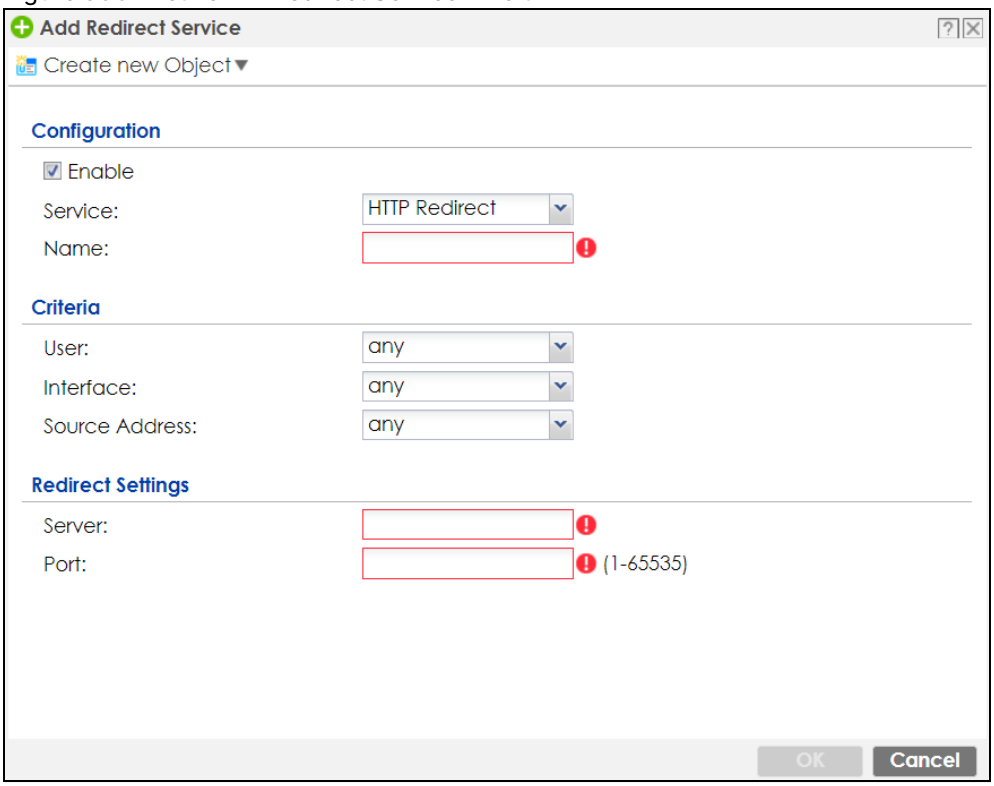
Table 123 Configuration > Network > Redirect Service (continued)

LABEL	DESCRIPTION
Server	This is the IP address of the HTTP proxy server or the SMTP server to which the matched traffic is forwarded.
Port	This is the service port number used by the HTTP proxy server or SMTP server.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

15.2.1 The Redirect Service Edit Screen

Click Network > Redirect Service to open the Redirect Service screen. Then click the Add or Edit icon to open the Redirect Service Edit screen where you can configure the rule.

Figure 306 Network > Redirect Service > Edit



The following table describes the labels in this screen.

Table 124 Network > Redirect Service > Edit

LABEL	DESCRIPTION
Enable	Use this option to turn the Redirect Service rule on or off.
Service	Select the service to be redirected: HTTP Redirect or SMTP redirect.
Name	Enter a name to identify this rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Criteria	
User	Select the user account or user group name to which this rule is applied.

Table 124 Network > Redirect Service > Edit (continued)

LABEL	DESCRIPTION
Interface	Select the interface on which the request must be received for the Zyxel Device to forward it to the specified server.
Source Address	Select the name of the source IP address object from which the traffic should be sent. Select any for the rule to be effective for every source.
Redirect Settings	
Server	Enter the IP address of the HTTP proxy or SMTP server.
Port	Enter the port number that the HTTP proxy or SMTP server uses.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

CHAPTER 16
ALG

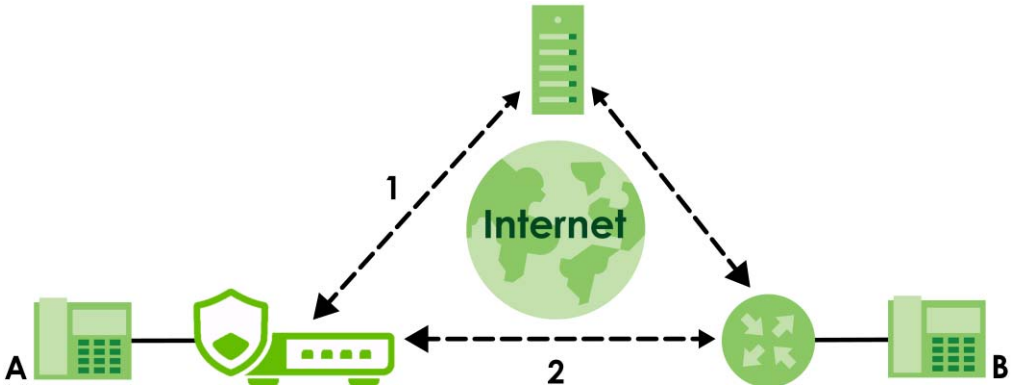
16.1 ALG Overview

Application Layer Gateway (ALG) allows the following applications to operate properly through the Zyxel Device's NAT.

- SIP - Session Initiation Protocol (SIP) - An application-layer protocol that can be used to create voice and multimedia sessions over Internet.
- H.323 - A teleconferencing protocol suite that provides audio, data and video conferencing.
- FTP - File Transfer Protocol - an Internet file transfer service.

The following example shows SIP signaling (1) and audio (2) sessions between SIP clients A and B and the SIP server.

Figure 307 SIP ALG Example



The ALG feature is only needed for traffic that goes through the Zyxel Device's NAT.

16.1.1 What You Need to Know

Application Layer Gateway (ALG), NAT and Security Policy

The Zyxel Device can function as an Application Layer Gateway (ALG) to allow certain NAT un-friendly applications (such as SIP) to operate properly through the Zyxel Device's NAT and security policy. The Zyxel Device dynamically creates an implicit NAT session and security policy session for the application's traffic from the WAN to the LAN. The ALG on the Zyxel Device supports all of the Zyxel Device's NAT mapping types.

FTP ALG

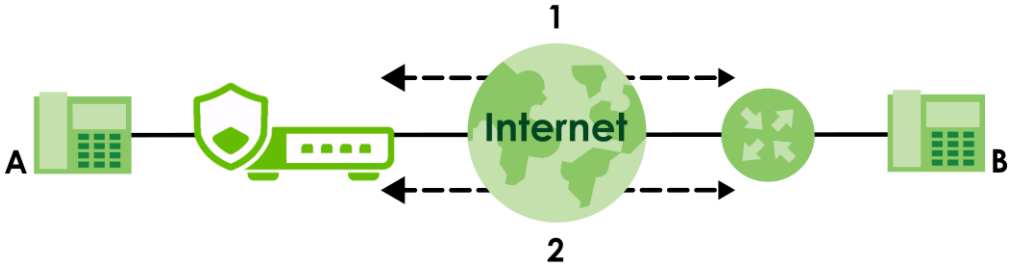
The FTP ALG allows TCP packets with a specified port destination to pass through. If the FTP server is located on the LAN, you must also configure NAT (port forwarding) and security policies if you want to allow access to the server from the WAN. Bandwidth management can be applied to FTP ALG traffic.

H.323 ALG

- The H.323 ALG supports peer-to-peer H.323 calls.
- The H.323 ALG handles H.323 calls that go through NAT or that the Zyxel Device routes. You can also make other H.323 calls that do not go through NAT or routing. Examples would be calls between LAN IP addresses that are on the same subnet.
- The H.323 ALG allows calls to go out through NAT. For example, you could make a call from a private IP address on the LAN to a peer device on the WAN.
- The H.323 ALG operates on TCP packets with a specified port destination.
- Bandwidth management can be applied to H.323 ALG traffic.
- The Zyxel Device allows H.323 audio connections.
- The Zyxel Device can also apply bandwidth management to traffic that goes through the H.323 ALG.

The following example shows H.323 signaling (1) and audio (2) sessions between H.323 devices A and B.

Figure 308 H.323 ALG Example



SIP ALG

- SIP phones can be in any zone (including LAN, DMZ, WAN), and the SIP server and SIP clients can be in the same network or different networks. The SIP server cannot be on the LAN. It must be on the WAN or the DMZ.
- There should be only one SIP server (total) on the Zyxel Device's private networks. Any other SIP servers must be on the WAN. So for example you could have a Back-to-Back User Agent such as the IPPBX x6004 or an asterisk PBX on the DMZ or on the LAN but not on both.
- Using the SIP ALG allows you to use bandwidth management on SIP traffic. Bandwidth management can be applied to FTP ALG traffic. Use the option in the Configuration > BWM screen to configure the highest bandwidth available for SIP traffic.
- The SIP ALG handles SIP calls that go through NAT or that the Zyxel Device routes. You can also make other SIP calls that do not go through NAT or routing. Examples would be calls between LAN IP addresses that are on the same subnet.
- The SIP ALG supports peer-to-peer SIP calls. The security policy (by default) allows peer to peer calls from the LAN zone to go to the WAN zone and blocks peer to peer calls from the WAN zone to the LAN zone.
- The SIP ALG allows UDP packets with a specified port destination to pass through.
- The Zyxel Device allows SIP audio connections.

- You do not need to use TURN (Traversal Using Relay NAT) for VoIP devices behind the Zyxel Device when you enable the SIP ALG.

Peer-to-Peer Calls and the Zyxel Device

The Zyxel Device ALG can allow peer-to-peer VoIP calls for both H.323 and SIP. You must configure the security policy and NAT (port forwarding) to allow incoming (peer-to-peer) calls from the WAN to a private IP address on the LAN (or DMZ).

VoIP Calls from the WAN with Multiple Outgoing Calls

When you configure the security policy and NAT (port forwarding) to allow calls from the WAN to a specific IP address on the LAN, you can also use policy routing to have H.323 (or SIP) calls from other LAN or DMZ IP addresses go out through a different WAN IP address. The policy routing lets the Zyxel Device correctly forward the return traffic for the calls initiated from the LAN IP addresses.

For example, you configure the security policy and NAT to allow LAN IP address A to receive calls from the Internet through WAN IP address 1. You also use a policy route to have LAN IP address A make calls out through WAN IP address 1. Configure another policy route to have H.323 (or SIP) calls from LAN IP addresses B and C go out through WAN IP address 2. Even though only LAN IP address A can receive incoming calls from the Internet, LAN IP addresses B and C can still make calls out to the Internet.

Figure 309 VoIP Calls from the WAN with Multiple Outgoing Calls

VoIP with Multiple WAN IP Addresses

With multiple WAN IP addresses on the Zyxel Device, you can configure different security policy and NAT (port forwarding) rules to allow incoming calls from each WAN IP address to go to a specific IP address on the LAN (or DMZ). Use policy routing to have the H.323 (or SIP) calls from each of those LAN or DMZ IP addresses go out through the same WAN IP address that calls come in on. The policy routing lets the Zyxel Device correctly forward the return traffic for the calls initiated from the LAN IP addresses.

For example, you configure security policy and NAT rules to allow LAN IP address A to receive calls through public WAN IP address 1. You configure different security policy and port forwarding rules to allow LAN IP address B to receive calls through public WAN IP address 2. You configure corresponding policy routes to have calls from LAN IP address A go out through WAN IP address **1** and calls from LAN IP address B go out through WAN IP address 2.

Figure 310 VoIP with Multiple WAN IP Addresses

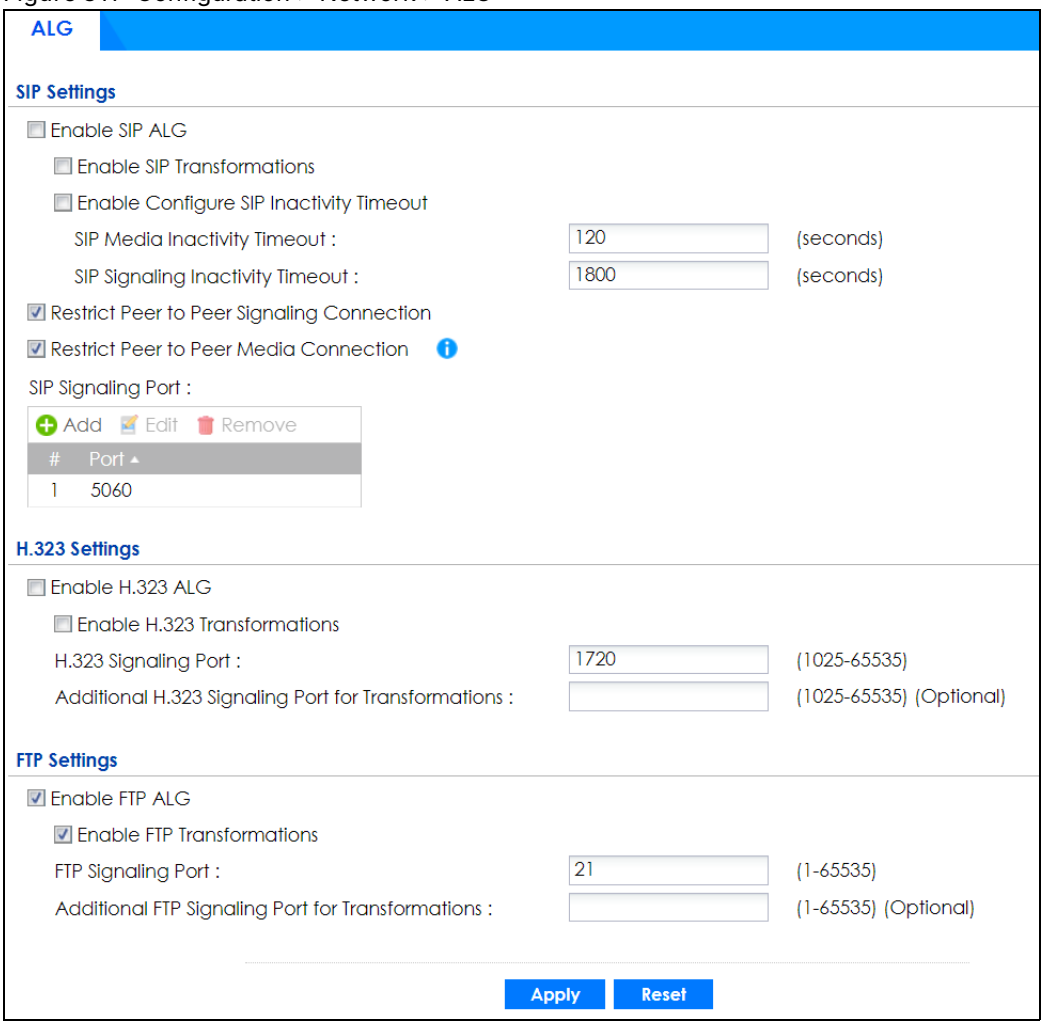
16.1.2 Before You Begin

You must also configure the security policy and enable NAT in the Zyxel Device to allow sessions initiated from the WAN.

16.2 The ALG Screen

Click Configuration > Network > ALG to open the ALG screen. Use this screen to turn ALGs off or on, configure the port numbers to which they apply, and configure SIP ALG time outs.

Figure 311 Configuration > Network > ALG



The following table describes the labels in this screen.

Table 125 Configuration > Network > ALG

LABEL	DESCRIPTION
Enable SIP ALG	Turn on the SIP ALG to detect SIP traffic and help build SIP sessions through the Zyxel Device's NAT.
Enable SIP Transformations	Select this to have the Zyxel Device modify IP addresses and port numbers embedded in the SIP data payload. You do not need to use this if you have a SIP device or server that will modify IP addresses and port numbers embedded in the SIP data payload.
Enable Configure SIP Inactivity Timeout	Select this option to have the Zyxel Device apply SIP media and signaling inactivity time out limits. These timeouts will take priority over the SIP session time out "Expires" value in a SIP registration response packet.
SIP Media Inactivity Timeout	Use this field to set how many seconds (1~86400) the Zyxel Device will allow a SIP session to remain idle (without voice traffic) before dropping it. If no voice packets go through the SIP ALG before the timeout period expires, the Zyxel Device deletes the audio session. You cannot hear anything and you will need to make a new call to continue your conversation.

Table 125 Configuration > Network > ALG (continued)

LABEL	DESCRIPTION
SIP Signaling Inactivity Timeout	Most SIP clients have an “expire” mechanism indicating the lifetime of signaling sessions. The SIP user agent sends registration packets to the SIP server periodically and keeps the session alive in the Zyxel Device. If the SIP client does not have this mechanism and makes no calls during the Zyxel Device SIP timeout, the Zyxel Device deletes the signaling session after the timeout period. Enter the SIP signaling session timeout value (1~86400).
Restrict Peer to Peer Signaling Connection	A signaling connection is used to set up the SIP connection. Enable this if you want signaling connections to only arrive from the IP address(es) you registered with. Signaling connections from other IP addresses will be dropped.
Restrict Peer to Peer Media Connection	A media connection is the audio transfer in a SIP connection. Enable this if you want media connections to only arrive from the IP address(es) you registered with. Media connections from other IP addresses will be dropped. You should disable this if have registered for cloud VoIP services.
SIP Signaling Port	If you are using a custom UDP port number (not 5060) for SIP traffic, enter it here. Use the Add icon to add fields if you are also using SIP on additional UDP port numbers.
Enable H.323 ALG	Turn on the H.323 ALG to detect H.323 traffic (used for audio communications) and help build H.323 sessions through the Zyxel Device’s NAT.
Enable H.323 Transformations	Select this to have the Zyxel Device modify IP addresses and port numbers embedded in the H.323 data payload. You do not need to use this if you have a H.323 device or server that will modify IP addresses and port numbers embedded in the H.323 data payload.
H.323 Signaling Port	If you are using a custom TCP port number (not 1720) for H.323 traffic, enter it here.
Additional H.323 Signaling Port for Transformations	If you are also using H.323 on an additional TCP port number, enter it here.
Enable FTP ALG	Turn on the FTP ALG to detect FTP (File Transfer Program) traffic and help build FTP sessions through the Zyxel Device’s NAT.
Enable FTP Transformations	Select this option to have the Zyxel Device modify IP addresses and port numbers embedded in the FTP data payload to match the Zyxel Device’s NAT environment. Clear this option if you have an FTP device or server that will modify IP addresses and port numbers embedded in the FTP data payload to match the Zyxel Device’s NAT environment.
FTP Signaling Port	If you are using a custom TCP port number (not 21) for FTP traffic, enter it here.
Additional FTP Signaling Port for Transformations	If you are also using FTP on an additional TCP port number, enter it here.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

16.3 ALG Technical Reference

Here is more detailed information about the Application Layer Gateway.

ALG

Some applications cannot operate through NAT (are NAT unfriendly) because they embed IP addresses and port numbers in their packets' data payload. The Zyxel Device examines and uses IP address and port number information embedded in the VoIP traffic's data stream. When a device behind the Zyxel Device uses an application for which the Zyxel Device has VoIP pass through enabled, the Zyxel Device translates the device's private IP address inside the data stream to a public IP address. It also records session port numbers and allows the related sessions to go through the security policy so the application's traffic can come in from the WAN to the LAN.

ALG and Trunks

If you send your ALG-managed traffic through an interface trunk and all of the interfaces are set to active, you can configure routing policies to specify which interface the ALG-managed traffic uses.

You could also have a trunk with one interface set to active and a second interface set to passive. The Zyxel Device does not automatically change ALG-managed connections to the second (passive) interface when the active interface's connection goes down. When the active interface's connection fails, the client needs to re-initialize the connection through the second interface (that was set to passive) in order to have the connection go through the second interface. VoIP clients usually re-register automatically at set intervals or the users can manually force them to re-register.

FTP

File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files.

H.323

H.323 is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. NetMeeting uses H.323.

SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is used in VoIP (Voice over IP), the sending of voice signals over the Internet Protocol.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

RTP

When you make a VoIP call using H.323 or SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

CHAPTER 17
UPnP

17.1 UPnP and NAT-PMP Overview

The Zyxel Device supports both UPnP and NAT-PMP to permit networking devices to discover each other and connect seamlessly.

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use. A gateway that supports UPnP is called Internet Gateway Device (IGD). The standardized Device Control Protocol (DCP) is defined by the UPnP Forum for IGDs to configure port mapping automatically.

NAT Port Mapping Protocol (NAT-PMP), introduced by Apple and implemented in current Apple products, is used as an alternative NAT traversal solution to the UPnP IGD protocol. NAT-PMP runs over UDP port 5351. NAT-PMP is much simpler than UPnP IGD and mainly designed for small home networks. It allows a client behind a NAT router to retrieve the router's public IP address and port number and make them known to the peer device with which it wants to communicate. The client can automatically configure the NAT router to create a port mapping to allow the peer to contact it.

17.2 What You Need to Know

UPnP hardware is identified as an icon on the network folder (Windows 7). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

17.2.1 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence on the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

17.2.2 Cautions with UPnP and NAT-PMP

The automated nature of NAT traversal applications in establishing their own services and opening security policy ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP or NAT-PMP device joins a network, it announces its presence with a multicast message. For security reasons, the Zyxel Device allows multicast messages on the LAN only.

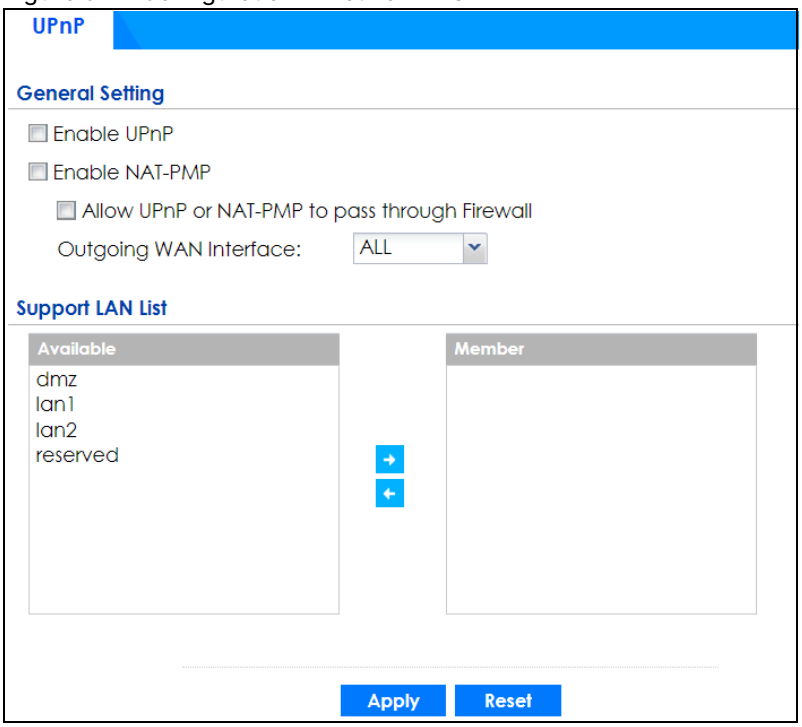
All UPnP-enabled or NAT-PMP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP or NAT-PMP if this is not your intention.

17.3 UPnP Screen

Use this screen to enable UPnP and NAT-PMP on your Zyxel Device.

Click Configuration > Network > UPnP to display the screen shown next.

Figure 312 Configuration > Network > UPnP



The following table describes the fields in this screen.

Table 126 Configuration > Network > UPnP

LABEL	DESCRIPTION
Enable UPnP	Select this checkbox to activate UPnP on the Zyxel Device. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the Zyxel Device's IP address (although you must still enter the password to access the web configurator).
Enable NAT-PMP	NAT Port Mapping Protocol (NAT-PMP) automates port forwarding to allow a computer in a private network (behind the Zyxel Device) to automatically configure the Zyxel Device to allow computers outside the private network to contact it. Select this checkbox to activate NAT-PMP on the Zyxel Device. Be aware that anyone could use a NAT-PMP application to open the web configurator's login screen without entering the Zyxel Device's IP address (although you must still enter the password to access the web configurator).
Allow UPnP or NAT-PMP to pass through Firewall	Select this checkbox to allow traffic from UPnP-enabled or NAT-PMP-enabled applications to bypass the security policy. Clear this checkbox to have the security policy block all UPnP or NAT-PMP application packets (for example, MSN packets).
Outgoing WAN Interface	Select through which WAN interface(s) you want to send out traffic from UPnP-enabled or NAT-PMP-enabled applications. If the WAN interface you select loses its connection, the Zyxel Device attempts to use the other WAN interface. If the other WAN interface also does not work, the Zyxel Device drops outgoing packets from UPnP-enabled or NAT-PMP-enabled applications.
Support LAN List	The Available list displays the name(s) of the internal interface(s) on which the Zyxel Device supports UPnP and/or NAT-PMP. To enable UPnP and/or NAT-PMP on an interface, you can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and click the right arrow button to add to the Member list. To remove an interface, select the name(s) in the Member list and click the left arrow button.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

17.4 Technical Reference

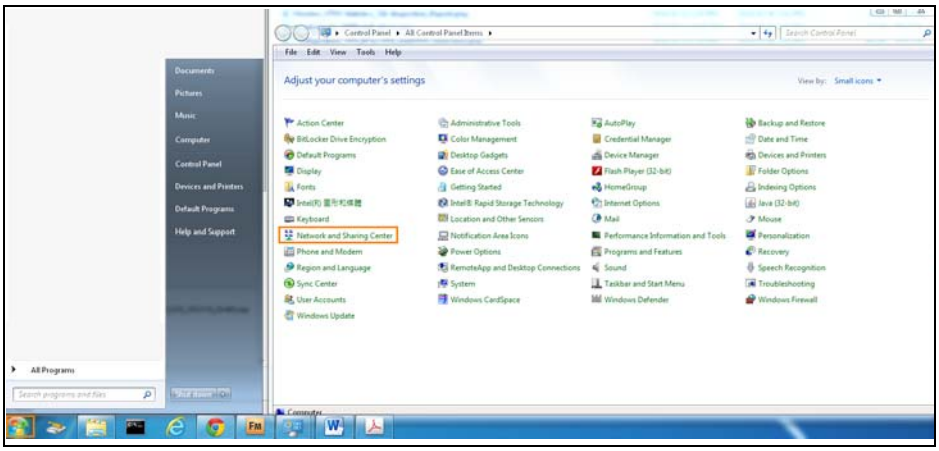
The sections show examples of using UPnP.

17.4.1 Turning on UPnP in Windows 7 Example

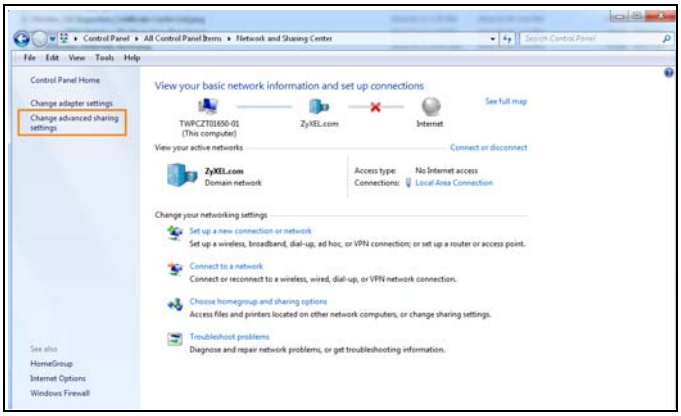
This section shows you how to use the UPnP feature in Windows 7. UPnP server is installed in Windows 7. Activate UPnP on the Zyxel Device.

Make sure the computer is connected to a LAN port of the Zyxel Device. Turn on your computer and the Zyxel Device.

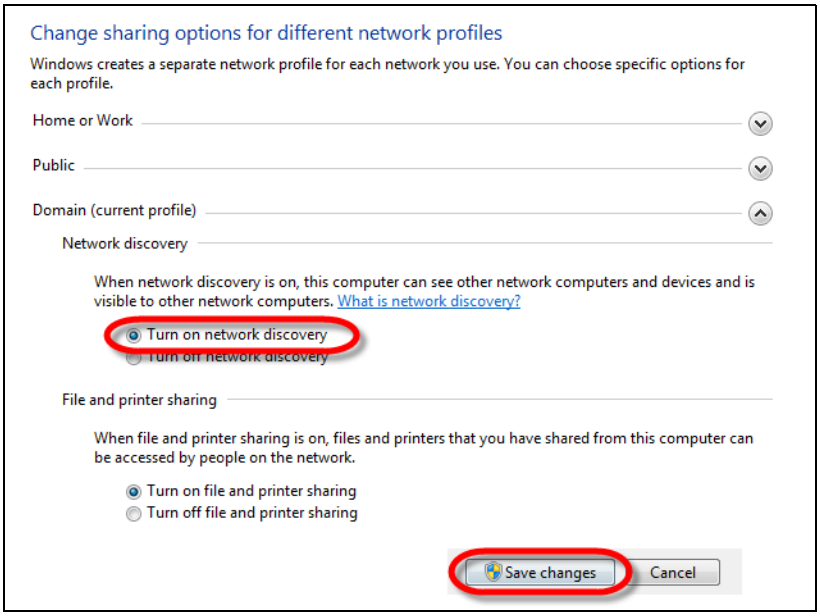
1 Click the start icon, Control Panel and then the Network and Sharing Center.



2 Click Change Advanced Sharing Settings.



3 Select Turn on network discovery and click Save Changes. Network discovery allows your computer to find other computers and devices on the network and other computers on the network to find your computer. This makes it easier to share files and printers.



17.4.1.1 Auto-discover Your UPnP-enabled Network Device

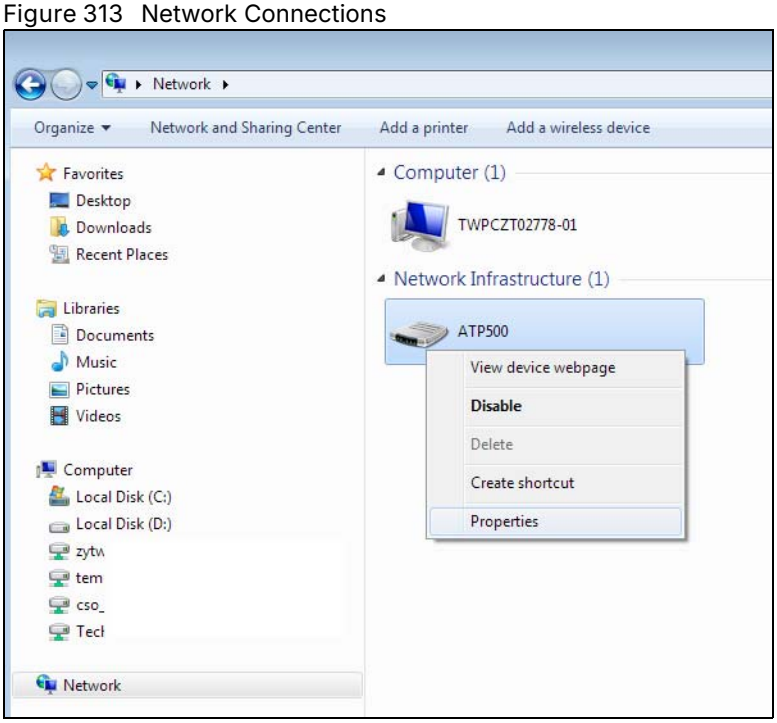
Before you follow these steps, make sure you already have UPnP activated on the Zyxel Device and in your computer.

Make sure your computer is connected to a LAN port of the Zyxel Device.

1 Open the Windows Explorer and click Network.

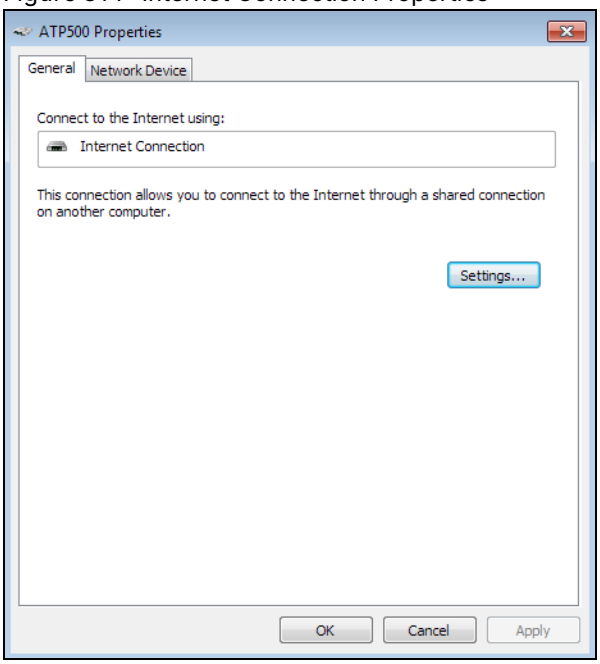
2 Right-click the device icon and select Properties.

Figure 313 Network Connections



3 In the Internet Connection Properties window, click Settings to see port mappings.

Figure 314 Internet Connection Properties



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

Figure 315 Internet Connection Properties: Advanced Settings

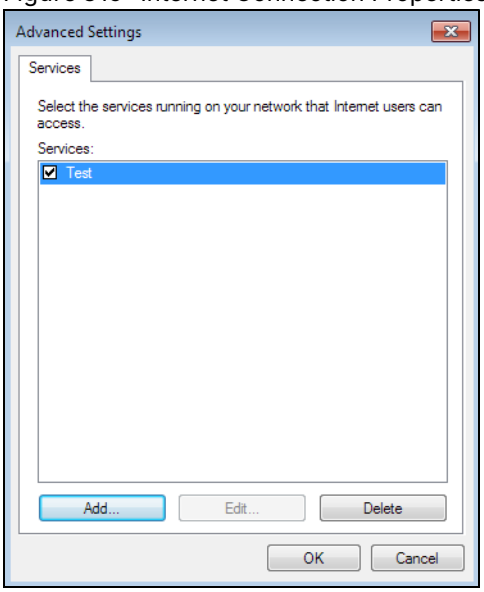
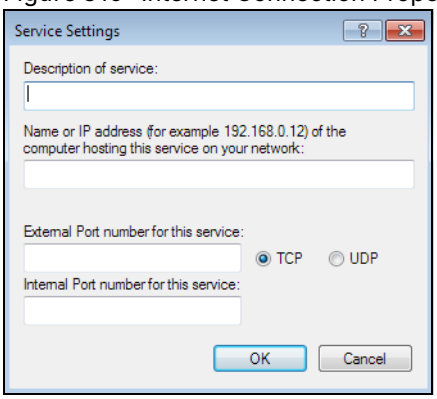


Figure 316 Internet Connection Properties: Advanced Settings: Add



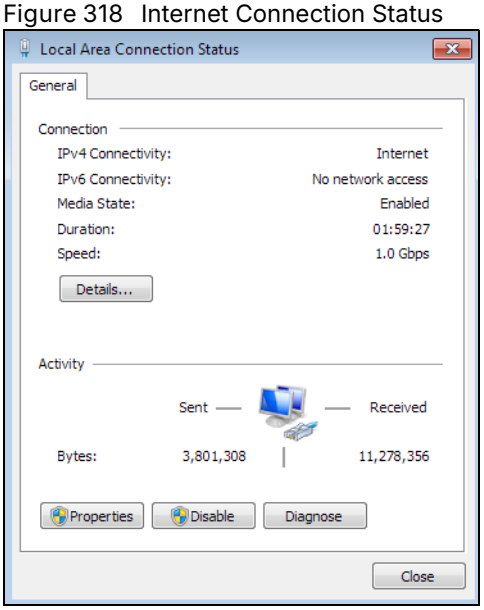
Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

5 Click OK. Check the network icon on the system tray to see your Internet connection status.

Figure 317 System Tray Icon

6 To see more details about your current Internet connection status, right click on the network icon in the system tray and click Open Network and Sharing Center. Click Local Area Network.

Figure 318 Internet Connection Status

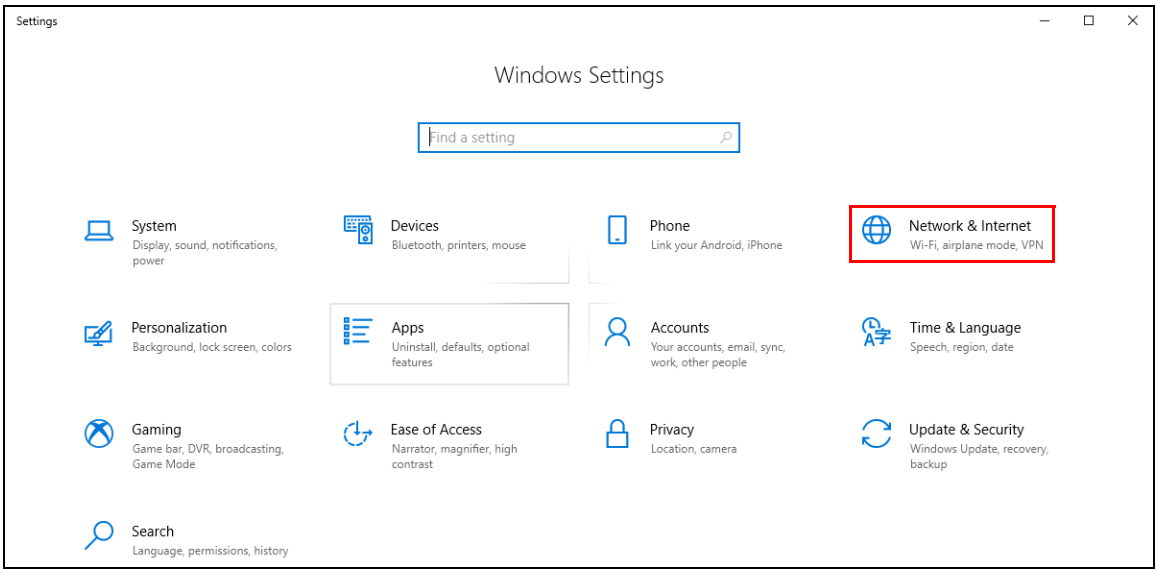


17.4.2 Turn on UPnP in Windows 10 Example

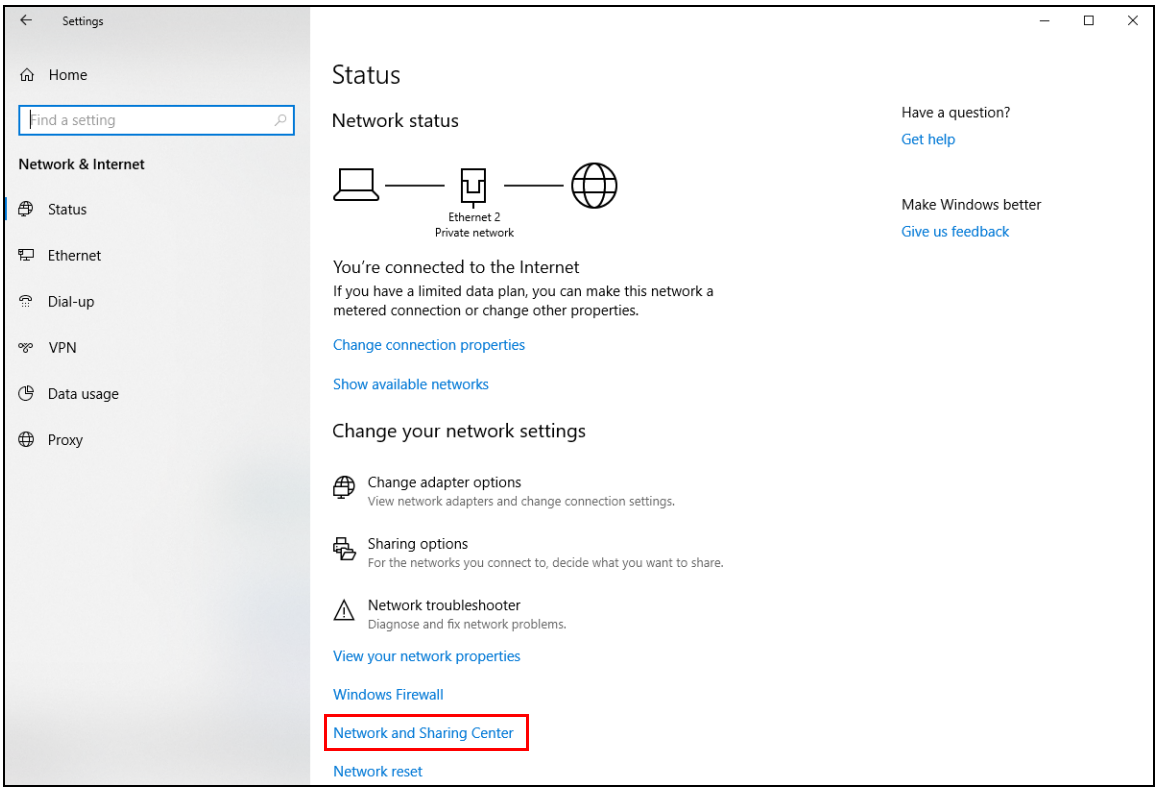
This section shows you how to use the UPnP feature in Windows 10. UPnP server is installed in Windows 10. Activate UPnP on the Zyxel Device by clicking Network Setting > Home Networking > UPnP.

Make sure the computer is connected to the LAN port of the Zyxel Device. Turn on your computer and the Zyxel Device.

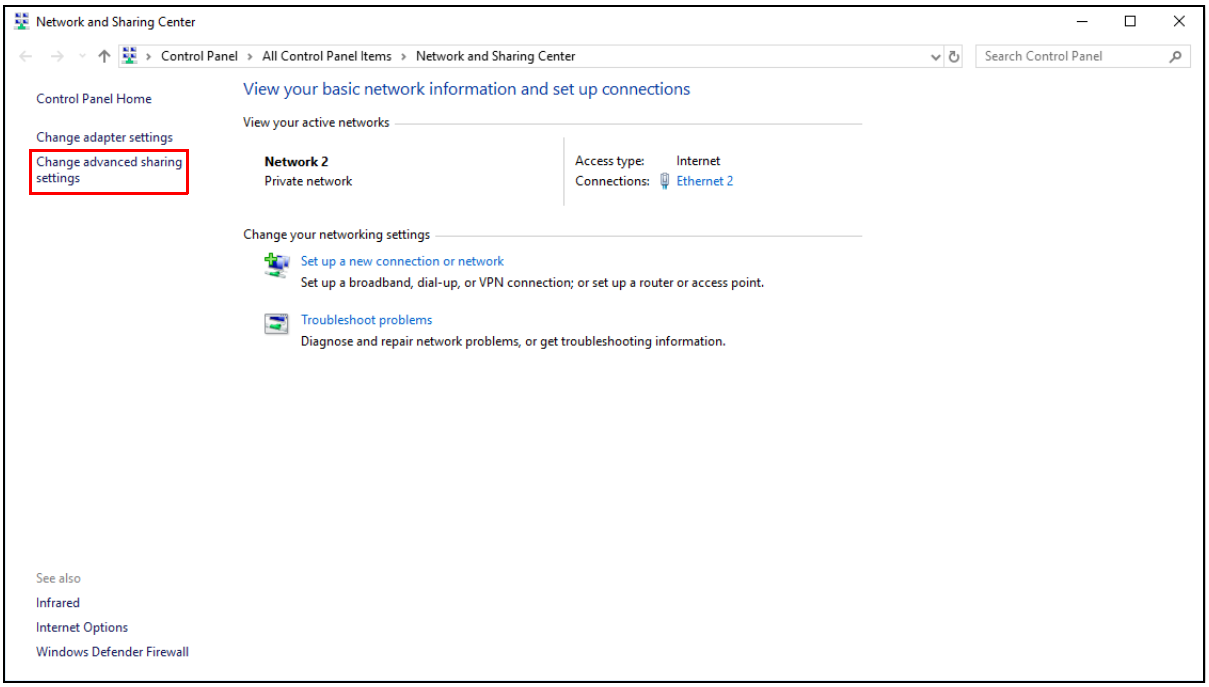
1 Click the start icon, Settings and then Network & Internet.



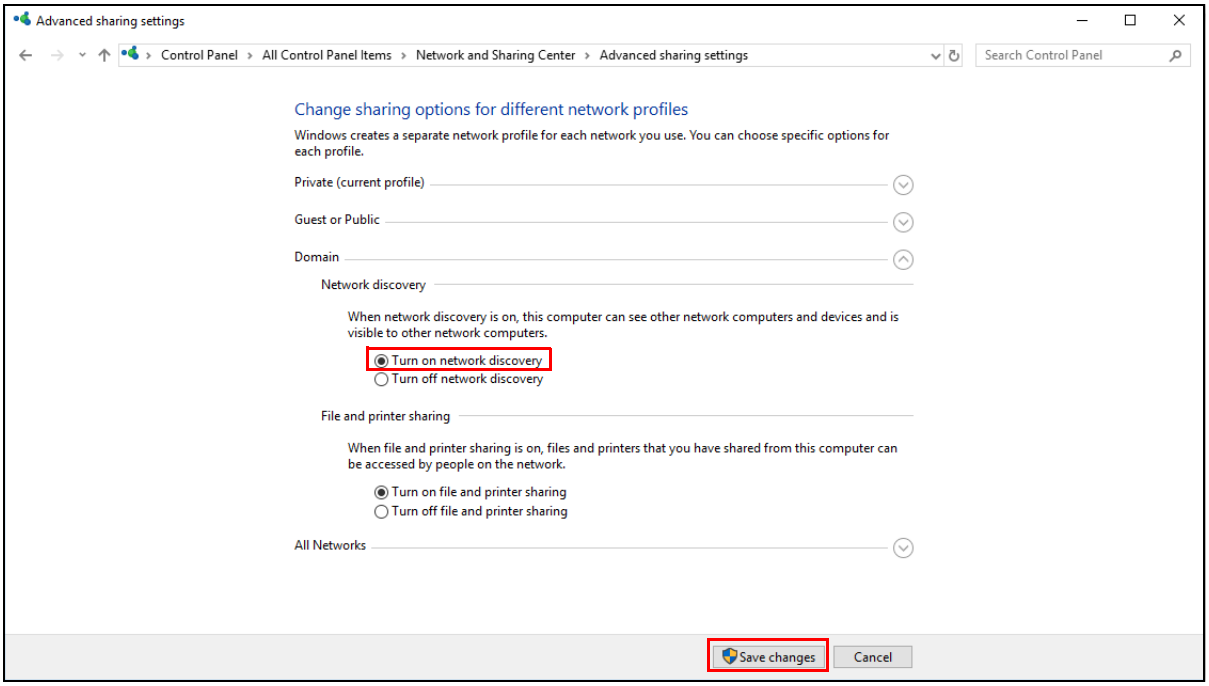
2 Click Network and Sharing Center.



3 Click Change advanced sharing settings.



4 Under Domain, select Turn on network discovery and click Save Changes. Network discovery allows your computer to find other computers and devices on the network and other computers on the network to find your computer. This makes it easier to share files and printers.



17.4.3 Auto-discover Your UPnP-enabled Network Device

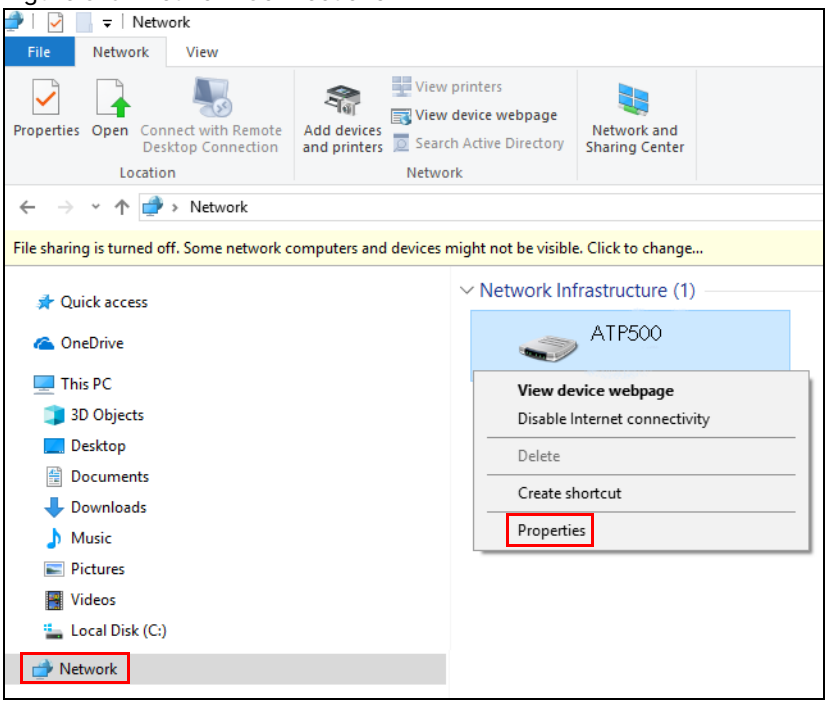
Before you follow these steps, make sure you already have UPnP activated on the Zyxel Device and in your computer.

Make sure your computer is connected to the LAN port of the Zyxel Device.

1 Open File Explorer and click Network.

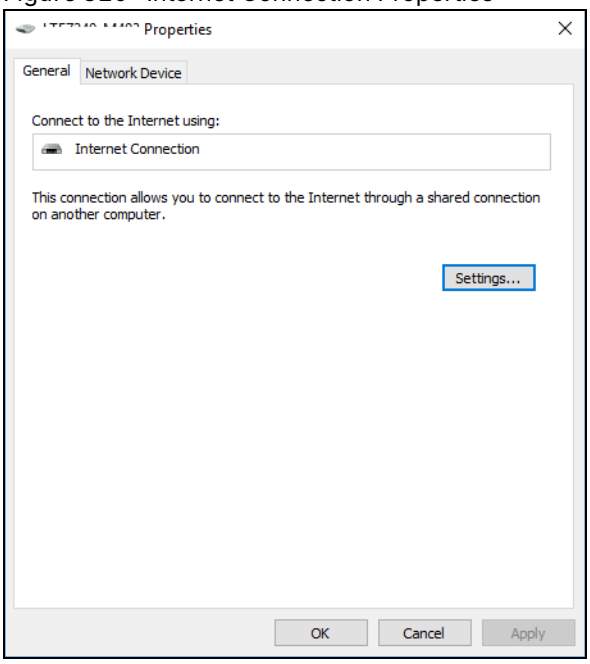
2 Right-click the Zyxel Device icon and select Properties.

Figure 319 Network Connections



3 In the Internet Connection Properties window, click Settings to see port mappings.

Figure 320 Internet Connection Properties



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

Figure 321 Internet Connection Properties: Advanced Settings

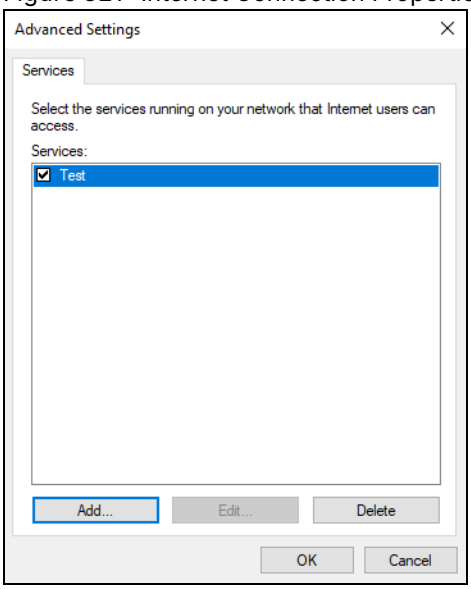
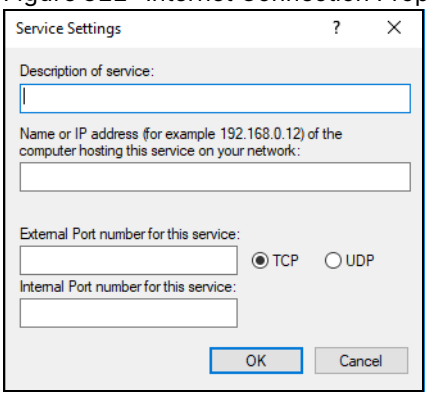


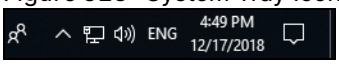
Figure 322 Internet Connection Properties: Advanced Settings: Add



Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

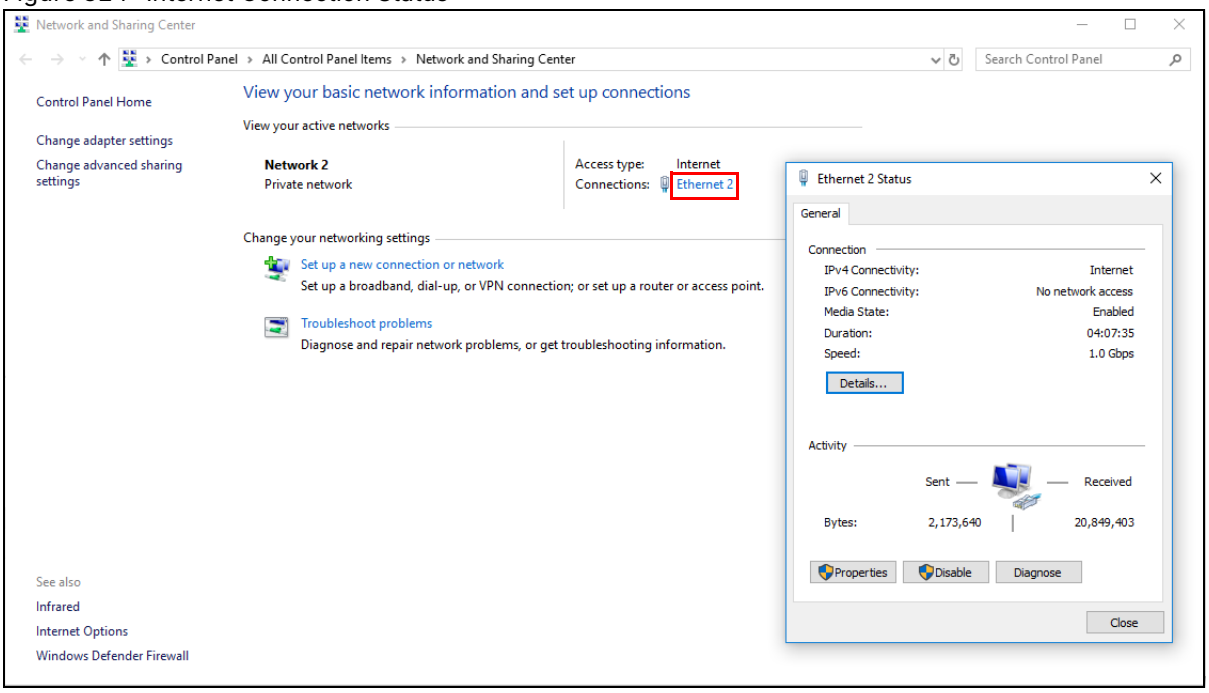
5 Click OK. Check the network icon on the system tray to see your Internet connection status.

Figure 323 System Tray Icon



6 To see more details about your current Internet connection status, right click the network icon in the system tray and click Open Network & Internet settings. Click Network and Sharing Center and click the Connections.

Figure 324 Internet Connection Status



17.4.4 Web Configurator Easy Access in Windows 7

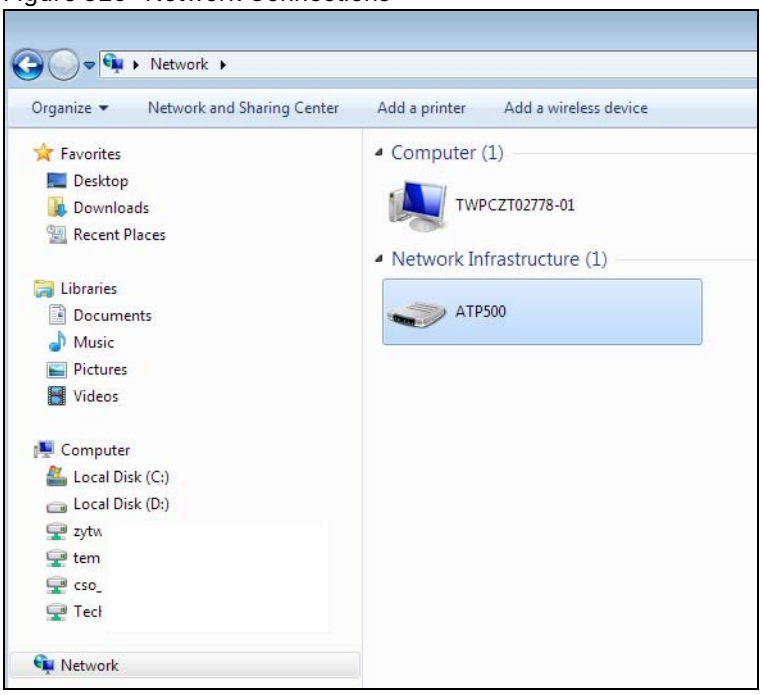
With UPnP, you can access the web-based configurator on the Zyxel Device without finding out the IP address of the Zyxel Device first. This comes helpful if you do not know the IP address of the Zyxel Device.

Follow the steps below to access the web configurator.

1 Open Windows Explorer.

2 Click Network.

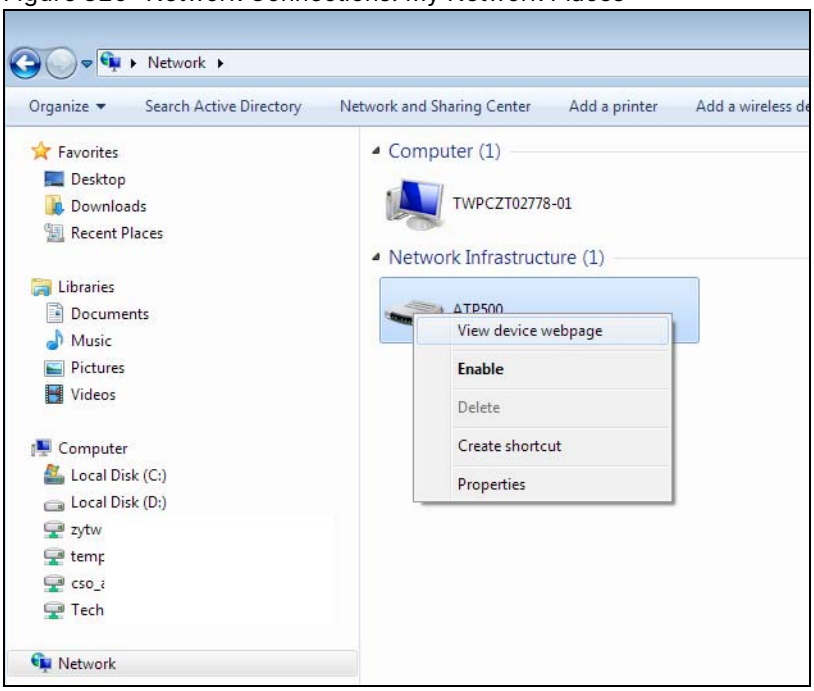
Figure 325 Network Connections



3 An icon with the description for each UPnP-enabled device displays under Network Infrastructure.

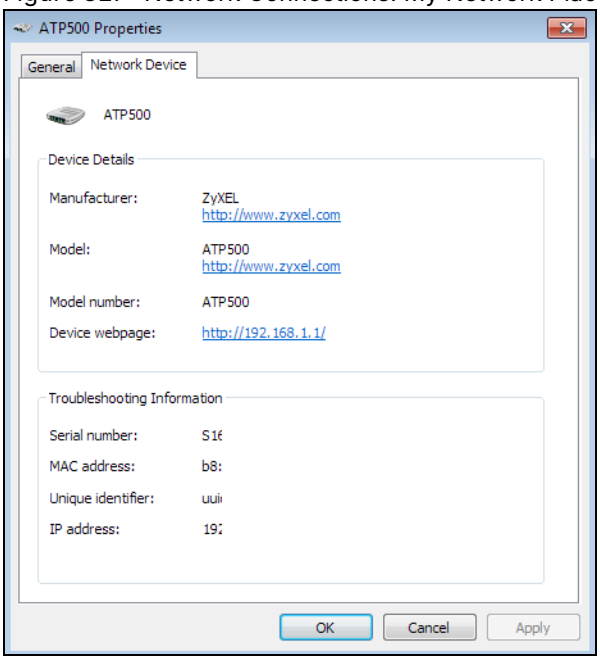
4 Right-click on the icon for your Zyxel Device and select View device webpage. The web configurator login screen displays.

Figure 326 Network Connections: My Network Places



5 Right-click on the icon for your Zyxel Device and select Properties. Click the Network Device tab. A window displays with information about the Zyxel Device.

Figure 327 Network Connections: My Network Places: Properties: Example



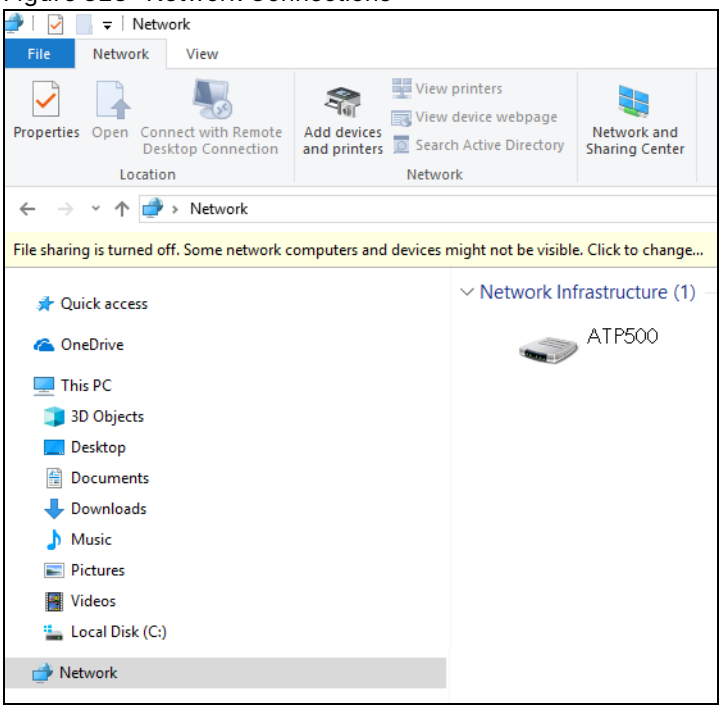
17.4.5 Web Configurator Easy Access in Windows 10

Follow the steps below to access the Web Configurator.

1 Open File Explorer.

2 Click Network.

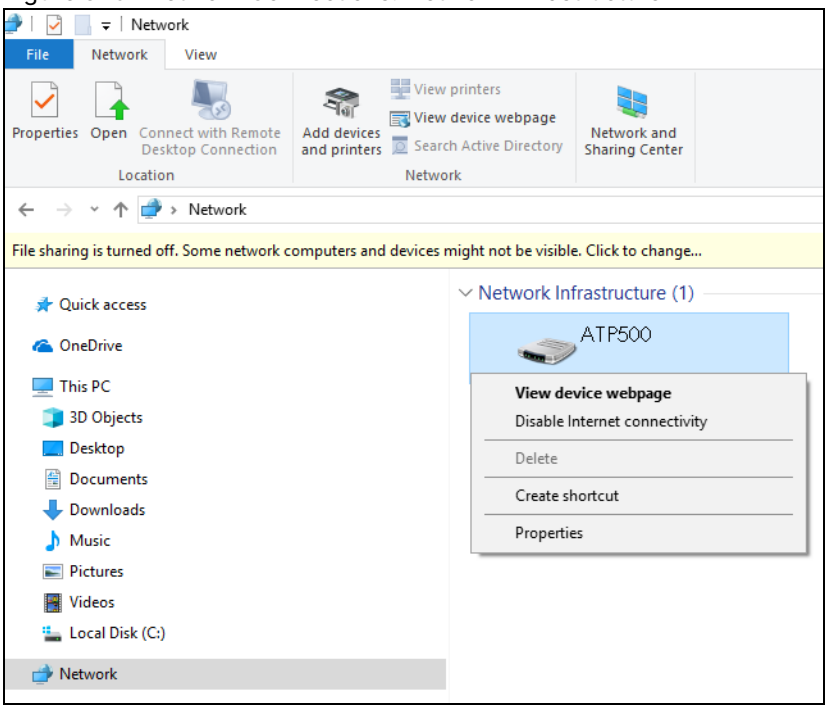
Figure 328 Network Connections



3 An icon with the description for each UPnP-enabled device displays under Network Infrastructure.

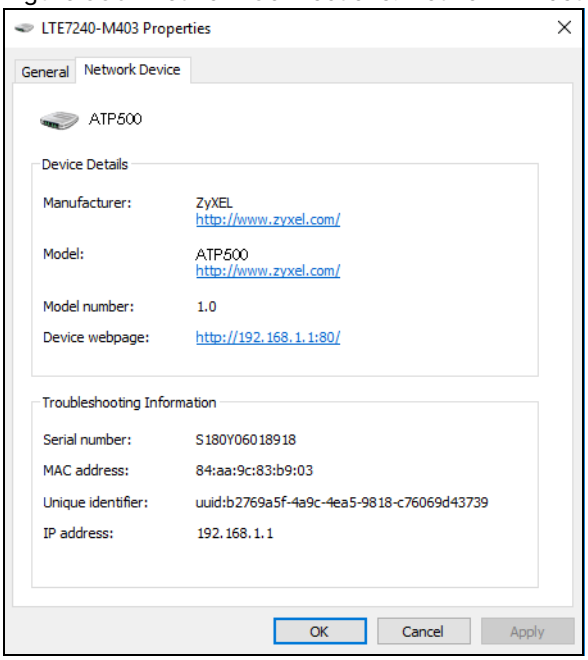
4 Right-click the icon for your Zyxel Device and select View device webpage. The Web Configurator login screen displays.

Figure 329 Network Connections: Network Infrastructure



5 Right-click the icon for your Zyxel Device and select Properties. Click the Network Device tab. A window displays information about the Zyxel Device.

Figure 330 Network Connections: Network Infrastructure: Properties: Example



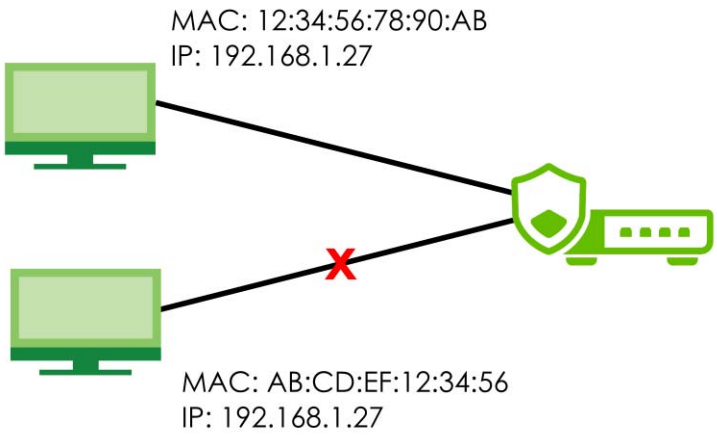
CHAPTER 18
IP/MAC Binding

18.1 IP/MAC Binding Overview

IP address to MAC address binding helps ensure that only the intended devices get to use privileged IP addresses. The Zyxel Device uses DHCP to assign IP addresses and records the MAC address it assigned to each IP address. The Zyxel Device then checks incoming connection attempts against this list. A user cannot manually assign another IP to his computer and use it to connect to the Zyxel Device.

Suppose you configure access privileges for IP address 192.168.1.27 and use static DHCP to assign it to Tim's computer's MAC address of 12:34:56:78:90:AB. IP/MAC binding drops traffic from any computer trying to use IP address 192.168.1.27 with another MAC address.

Figure 331 IP/MAC Binding Example



18.1.1 What You Can Do in this Chapter

- Use the Summary and Edit screens (Section 18.2 on page 459) to bind IP addresses to MAC addresses.
- Use the Exempt List screen (Section 18.3 on page 462) to configure ranges of IP addresses to which the Zyxel Device does not apply IP/MAC binding.

18.1.2 What You Need to Know

DHCP

IP/MAC address bindings are based on the Zyxel Device's dynamic and static DHCP entries.

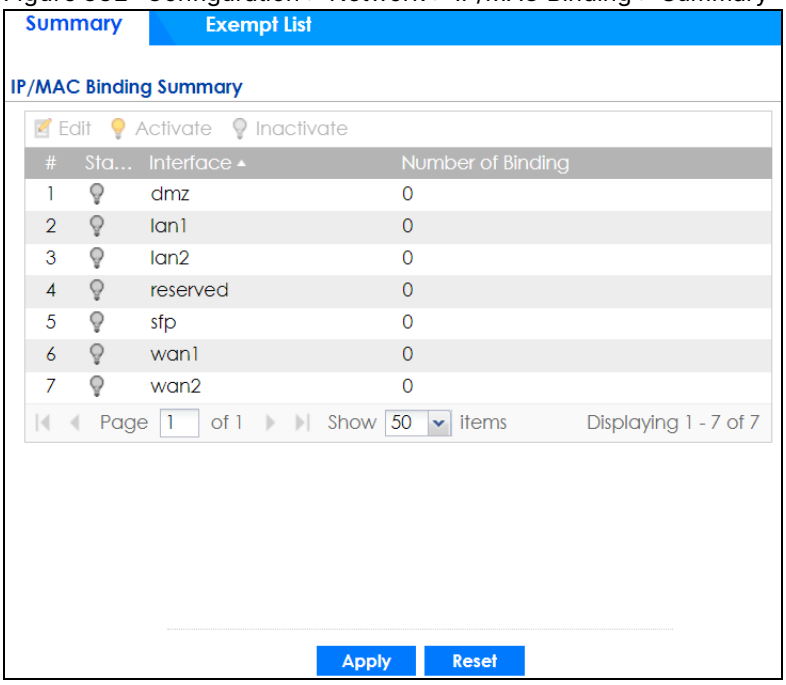
Interfaces Used With IP/MAC Binding

IP/MAC address bindings are grouped by interface. You can use IP/MAC binding with Ethernet, bridge, VLAN, and WLAN interfaces. You can also enable or disable IP/MAC binding and logging in an interface's configuration screen.

18.2 IP/MAC Binding Summary

Click Configuration > Network > IP/MAC Binding to open the IP/MAC Binding Summary screen. This screen lists the total number of IP to MAC address bindings for devices connected to each supported interface.

Figure 332 Configuration > Network > IP/MAC Binding > Summary



The following table describes the labels in this screen.

Table 127 Configuration > Network > IP/MAC Binding > Summary

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
#	This field is a sequential value, and it is not associated with a specific entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Interface	This is the name of an interface that supports IP/MAC binding.
Number of Binding	This field displays the interface's total number of IP/MAC bindings and IP addresses that the interface has assigned by DHCP.

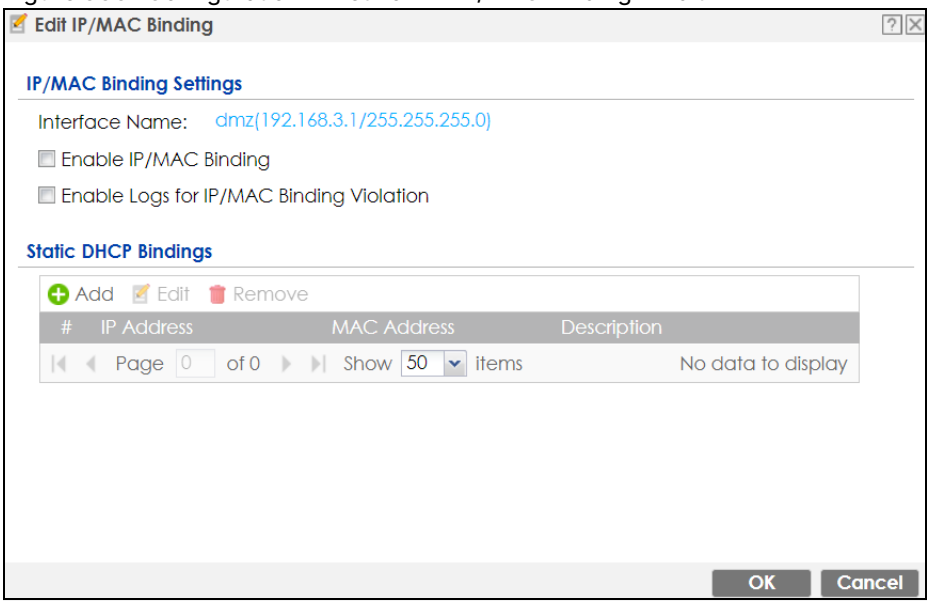
Table 127 Configuration > Network > IP/MAC Binding > Summary (continued)

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.

18.2.1 IP/MAC Binding Edit

Click Configuration > Network > IP/MAC Binding > Edit to open the IP/MAC Binding Edit screen. Use this screen to configure an interface's IP to MAC address binding settings.

Figure 333 Configuration > Network > IP/MAC Binding > Edit



The following table describes the labels in this screen.

Table 128 Configuration > Network > IP/MAC Binding > Edit

LABEL	DESCRIPTION
IP/MAC Binding Settings	
Interface Name	This field displays the name of the interface within the Zyxel Device and the interface's IP address and subnet mask.
Enable IP/MAC Binding	Select this option to have this interface enforce links between specific IP addresses and specific MAC addresses. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.
Enable Logs for IP/MAC Binding Violation	Select this option to have the Zyxel Device generate a log if a device connected to this interface attempts to use an IP address not assigned by the Zyxel Device.
Static DHCP Bindings	This table lists the bound IP and MAC addresses. The Zyxel Device checks this table when it assigns IP addresses. If the computer's MAC address is in the table, the Zyxel Device assigns the corresponding IP address. You can also access this table from the interface's edit screen.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.

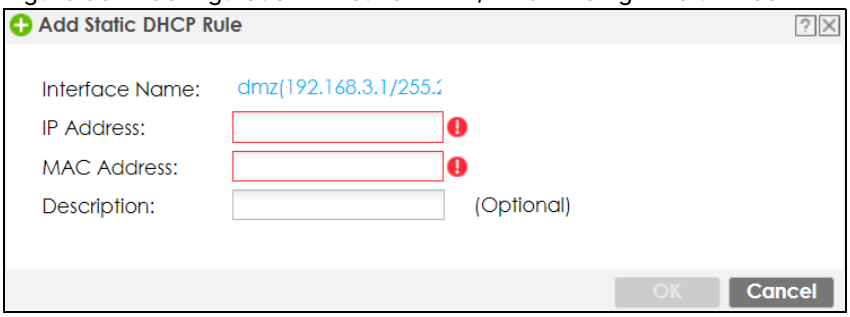
Table 128 Configuration > Network > IP/MAC Binding > Edit (continued)

LABEL	DESCRIPTION
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
#	This is the index number of the static DHCP entry.
IP Address	This is the IP address that the Zyxel Device assigns to a device with the entry's MAC address.
MAC Address	This is the MAC address of the device to which the Zyxel Device assigns the entry's IP address.
Description	This helps identify the entry.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

18.2.2 Static DHCP Edit

Click Configuration > Network > IP/MAC Binding > Edit to open the IP/MAC Binding Edit screen. Click the Add or Edit icon to open the following screen. Use this screen to configure an interface's IP to MAC address binding settings.

Figure 334 Configuration > Network > IP/MAC Binding > Edit > Add



The following table describes the labels in this screen.

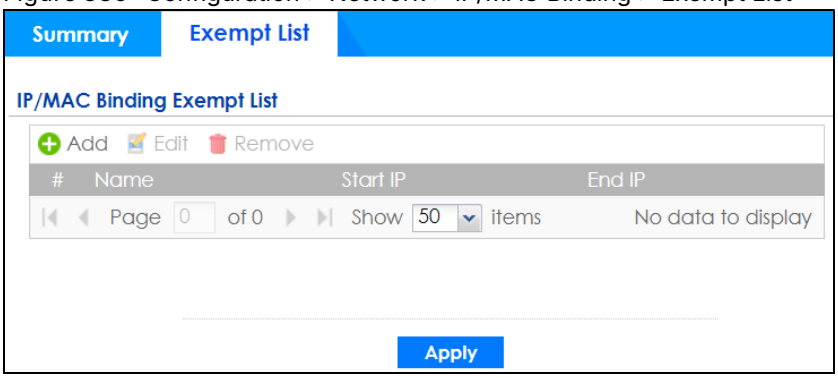
Table 129 Configuration > Network > IP/MAC Binding > Edit > Add

LABEL	DESCRIPTION
Interface Name	This field displays the name of the interface within the Zyxel Device and the interface's IP address and subnet mask.
IP Address	Enter the IP address that the Zyxel Device is to assign to a device with the entry's MAC address.
MAC Address	Enter the MAC address of the device to which the Zyxel Device assigns the entry's IP address.
Description	Enter a descriptive name consists of 1 to 60 single-byte characters, including a-zA-Z0-9!"#$%'()*+,-/;:=?@_ &[.]<>\^'{|} are not allowed.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

18.3 IP/MAC Binding Exempt List

Click Configuration > Network > IP/MAC Binding > Exempt List to open the IP/MAC Binding Exempt List screen. Use this screen to configure ranges of IP addresses to which the Zyxel Device does not apply IP/MAC binding.

Figure 335 Configuration > Network > IP/MAC Binding > Exempt List



The following table describes the labels in this screen.

Table 130 Configuration > Network > IP/MAC Binding > Exempt List

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Click an entry or select it and click Edit to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
#	This is the index number of the IP/MAC binding list entry.
Name	Enter a name to help identify this entry.
Start IP	Enter the first IP address in a range of IP addresses for which the Zyxel Device does not apply IP/MAC binding.
End IP	Enter the last IP address in a range of IP addresses for which the Zyxel Device does not apply IP/MAC binding.
Add icon	Click the Add icon to add a new entry. Click the Remove icon to delete an entry. A window displays asking you to confirm that you want to delete it.
Apply	Click Apply to save your changes back to the Zyxel Device.

CHAPTER 19
Layer 2 Isolation

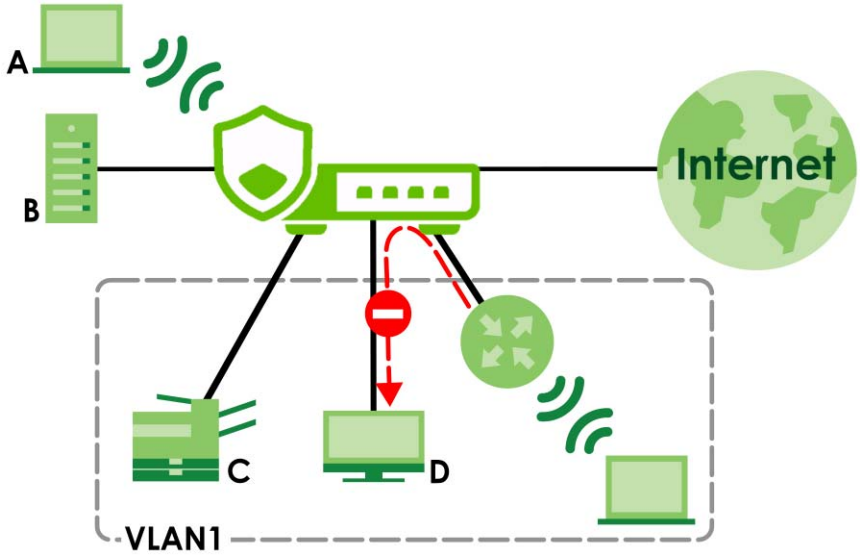
19.1 Overview

Layer-2 isolation is used to prevent connected devices from communicating with each other in the Zyxel Device's local network(s), except for the devices in the white list, when layer-2 isolation is enabled on the Zyxel Device and the local interface(s).

Note: The security policy control must be enabled before you can use layer-2 isolation.

In the following example, layer-2 isolation is enabled on the Zyxel Device's interface Vlan1. A printer, PC and AP are in the Vlan1. The IP address of network printer (C) is added to the white list. With this setting, the connected AP then cannot communicate with the PC (D), but can access the network printer (C), server (B), wireless client (A) and the Internet.

Figure 336 Layer-2 Isolation Application



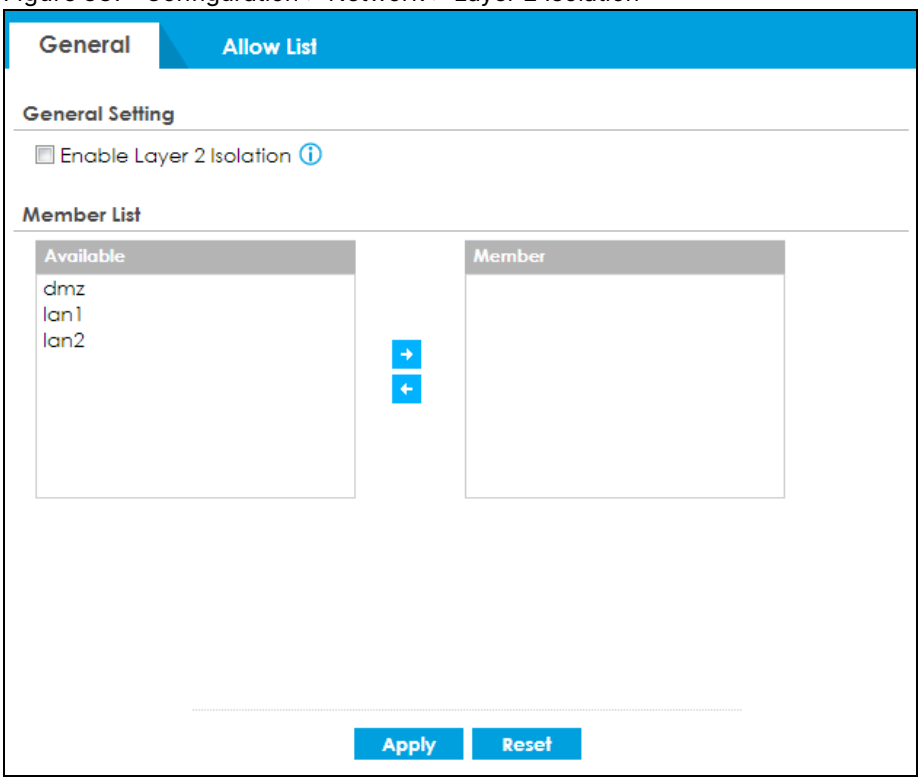
19.1.1 What You Can Do in this Chapter

- Use the General screen (Section 19.2 on page 464) to enable layer-2 isolation on the Zyxel Device and the internal interface(s).
- Use the Allow List screen (Section 19.3 on page 465) to enable and configures the allow list.

19.2 Layer-2 Isolation General Screen

This screen allows you to enable Layer-2 isolation on the Zyxel Device and specific internal interface(s). To access this screen click Configuration > Network > Layer 2 Isolation.

Figure 337 Configuration > Network > Layer 2 Isolation



The following table describes the labels in this screen.

Table 131 Configuration > Network > Layer 2 Isolation

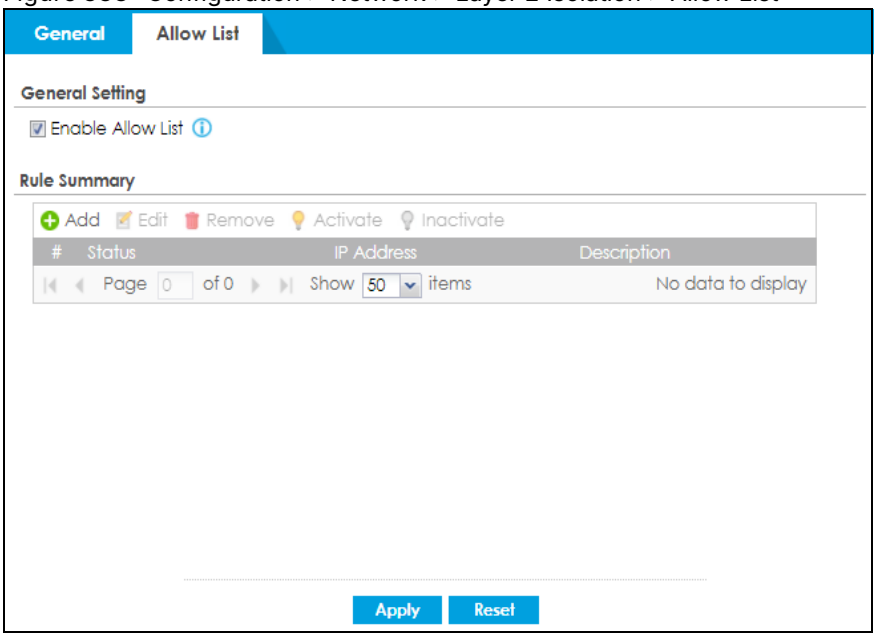
LABEL	DESCRIPTION
Enable Layer2 Isolation	Select this option to turn on the layer-2 isolation feature on the Zyxel Device. Note: You can enable this feature only when the security policy is enabled.
Member List	The Available list displays the name(s) of the internal interface(s) on which you can enable layer-2 isolation. To enable layer-2 isolation on an interface, you can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and click the right arrow button to add to the Member list. To remove an interface, select the name(s) in the Member list and click the left arrow button.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

19.3 Allow List Screen

IP addresses that are not listed in the allow list are blocked from communicating with other devices in the layer-2-isolation-enabled internal interface(s) except for broadcast packets.

To access this screen click Configuration > Network > Layer 2 Isolation > Allow List.

Figure 338 Configuration > Network > Layer 2 Isolation > Allow List



The following table describes the labels in this screen.

Table 132 Configuration > Network > Layer 2 Isolation > Allow List

LABEL	DESCRIPTION
Enable Allow List	Select this option to turn on the white list on the Zyxel Device. Note: You can enable this feature only when the security policy is enabled.
Add	Click this to add a new rule.
Edit	Click this to edit the selected rule.
Remove	Click this to remove the selected rule.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
#	This field is a sequential value, and it is not associated with a specific rule.
Status	This icon is lit when the rule is active and dimmed when the rule is inactive.
IP Address	This field displays the IP address of device that can be accessed by the devices connected to an internal interface on which layer-2 isolation is enabled.
Description	This field displays the description for the IP address in this rule.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

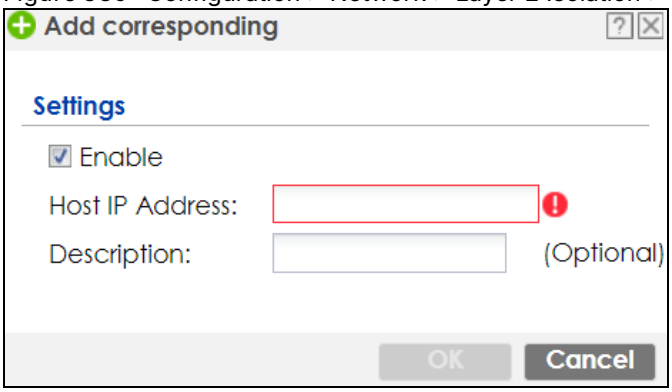
19.3.1 Add/Edit Allow List Rule

This screen allows you to create a new rule in the allow list or edit an existing one. To access this screen, click the Add button or select an entry from the list and click the Edit button.

Note: You can configure up to 100 allow list rules on the Zyxel Device.

Note: You need to know the IP address of each connected device that you want to allow to be accessed by other devices when layer-2 isolation is enabled.

Figure 339 Configuration > Network > Layer 2 Isolation > White List > Add/Edit



The following table describes the labels in this screen.

Table 133 Configuration > Network > Layer 2 Isolation > Allow List > Add/Edit

LABEL	DESCRIPTION
Enable	Select this option to turn on the rule.
Host IP Address	Enter an IPv4 address associated with this rule.
Description	Specify a description for the IP address associated with this rule. Enter up to 60 characters, spaces and underscores allowed.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving your changes.

CHAPTER 20
DNS Inbound LB

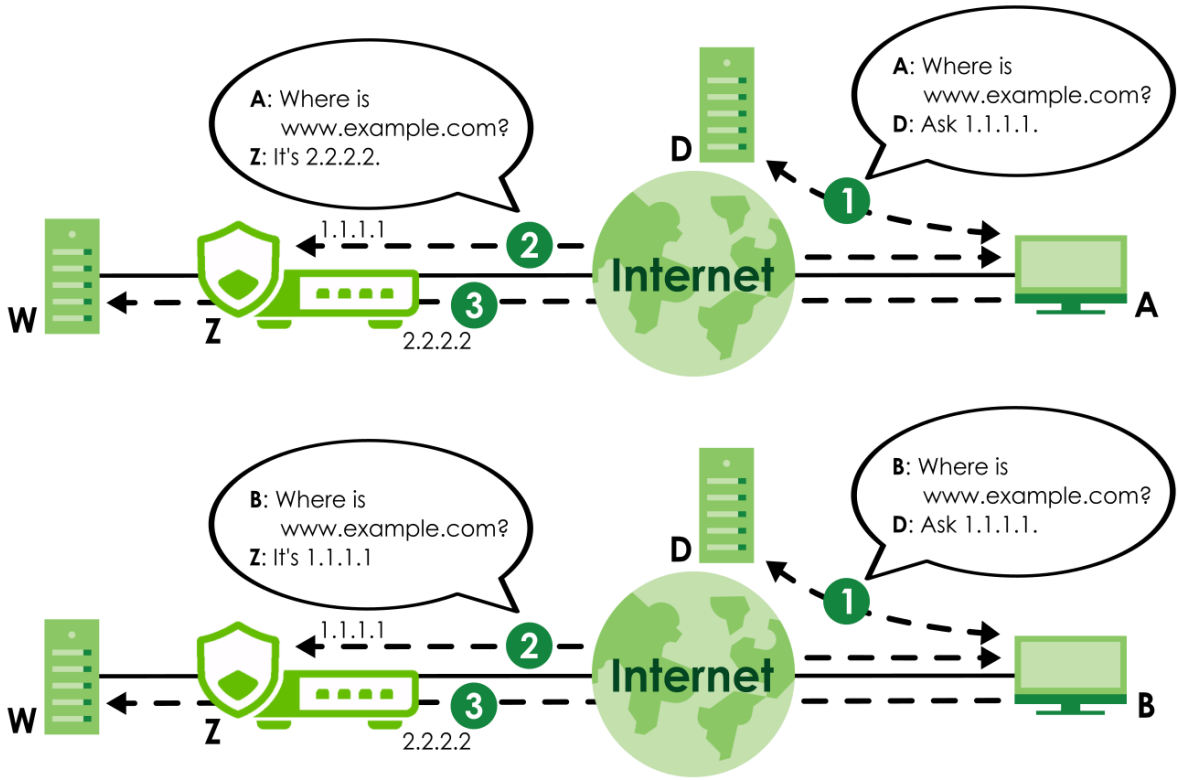
20.1 DNS Inbound Load Balancing Overview

Inbound load balancing enables the Zyxel Device to respond to a DNS query message with a different IP address for DNS name resolution. The Zyxel Device checks which member interface has the least load and responds to the DNS query message with the interface's IP address.

In the following figure, an Internet host (A) sends a DNS query message to the DNS server (D) in order to resolve a domain name of www.example.com. DNS server D redirects it to the Zyxel Device (Z)'s WAN1 with an IP address of 1.1.1.1. The Zyxel Device receives the DNS query message and responds to it with the WAN2's IP address, 2.2.2.2, because the WAN2 has the least load at that moment.

Another Internet host (B) also sends a DNS query message to ask where www.example.com is. The Zyxel Device responds to it with the WAN1's IP address, 1.1.1.1, since WAN1 has the least load this time.

Figure 340 DNS Load Balancing Example



20.1.1 What You Can Do in this Chapter

- Use the Inbound LB screen (see Section 20.2 on page 468) to view a list of the configured DNS load balancing rules.

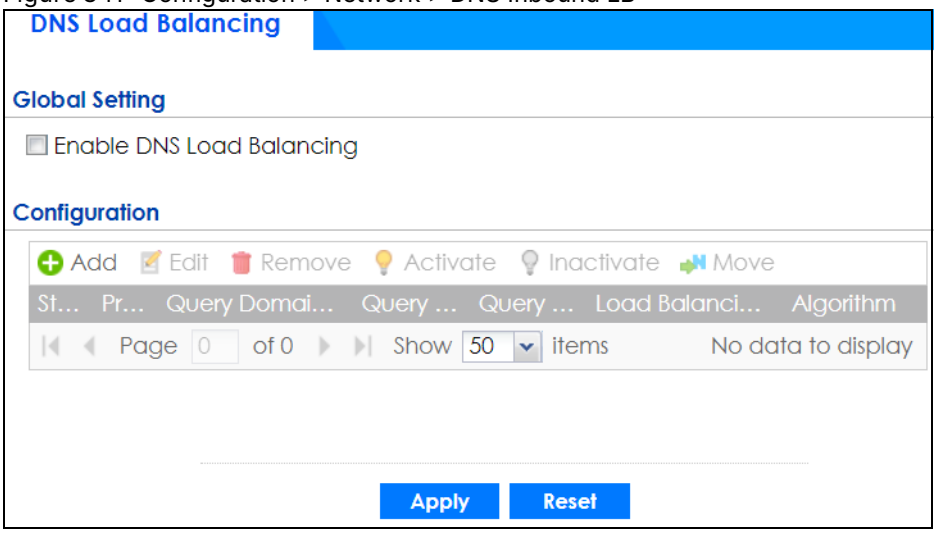
- Use the Inbound LB Add/Edit screen (see Section 20.2.1 on page 469) to add or edit a DNS load balancing rule.

20.2 The DNS Inbound LB Screen

The Inbound LB screen provides a summary of all DNS load balancing rules and the details. You can also use this screen to add, edit, or remove the rules. Click Configuration > Network > Inbound LB to open the following screen.

Note: After you finish the inbound load balancing settings, go to security policy and NAT screens to configure the corresponding rule and virtual server to allow the Internet users to access your internal servers.

Figure 341 Configuration > Network > DNS Inbound LB



The following table describes the labels in this screen.

Table 134 Configuration > Network > DNS Inbound LB

LABEL	DESCRIPTION
Global Setting	
Enable DNS Load Balancing	Select this to enable DNS load balancing.
Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The 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.
Move	To move an entry to a different number in the list, click the Move icon. In the field that appears, specify the number to which you want to move the entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.

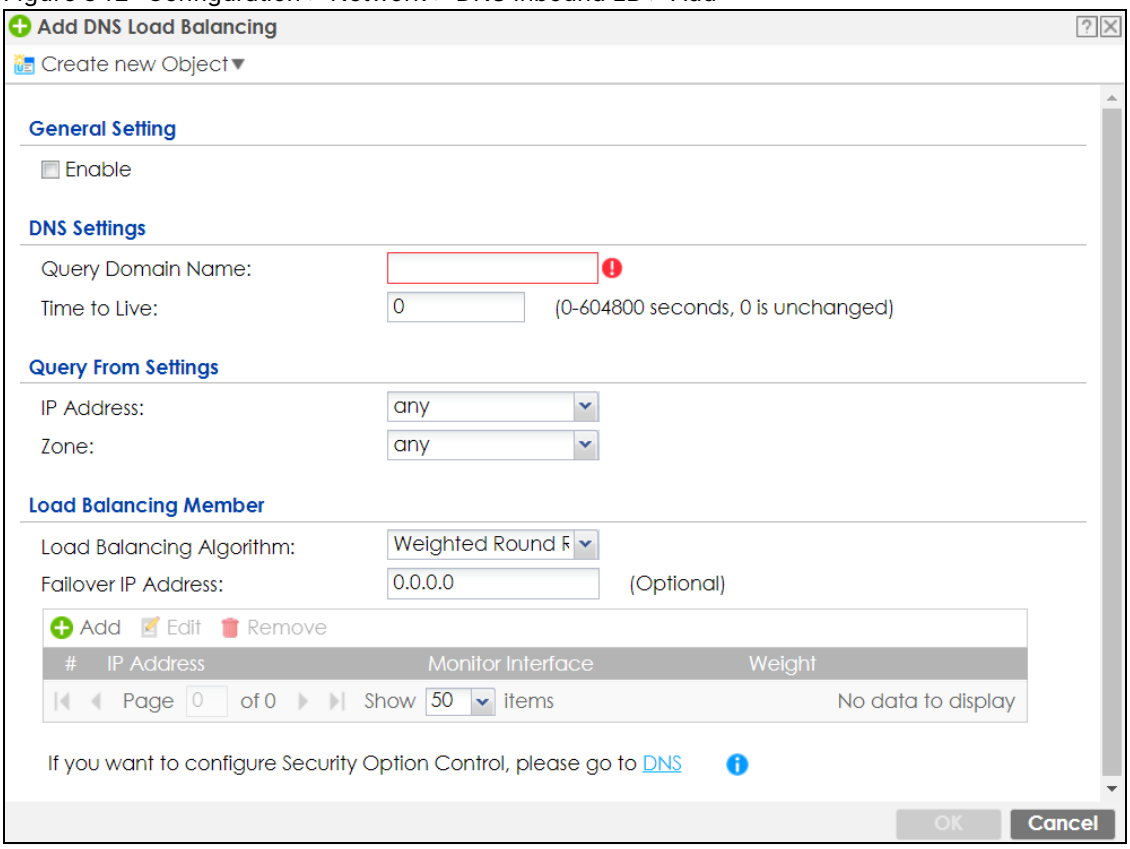
Table 134 Configuration > Network > DNS Inbound LB (continued)

LABEL	DESCRIPTION
Priority	This field displays the order in which the Zyxel Device checks the member interfaces of this DNS load balancing rule.
Query Domain Name	This field displays the domain name for which the Zyxel Device manages load balancing between the specified interfaces.
Query From Address	This field displays the source IP address of the DNS query messages to which the Zyxel Device applies the DNS load balancing rule.
Query From Zone	The Zyxel Device applies the DNS load balancing rule to the query messages received from this zone.
Load Balancing Member	This field displays the member interfaces which the Zyxel Device manages for load balancing.
Algorithm	This field displays the load balancing method the Zyxel Device uses for this DNS load balancing rule. Weighted Round Robin - Each member interface is assigned a weight. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight. For example, if the weight ratio of wan1 and wan2 interfaces is 2:1, the Zyxel Device chooses wan1 for 2 sessions' traffic and wan2 for 1 session's traffic in each round of 3 new sessions. Least Connection - The Zyxel Device chooses choose a member interface which is handling the least number of sessions. Least Load - Outbound - The Zyxel Device chooses a member interface which is handling the least amount of outgoing traffic. Least Load - Inbound - The Zyxel Device chooses a member interface which is handling the least amount of incoming traffic. Least Load - Total - The Zyxel Device chooses a member interface which is handling the least amount of outgoing and incoming traffic.
Apply	Click this button to save your changes to the Zyxel Device.
Reset	Click this button to return the screen to its last-saved settings.

20.2.1 The DNS Inbound LB Add/Edit Screen

The Add DNS Load Balancing screen allows you to add a domain name for which the Zyxel Device manages load balancing between the specified interfaces. You can configure the Zyxel Device to apply DNS load balancing to some specific hosts only by configuring the Query From settings. Click Configuration > Network > Inbound LB and then the Add or Edit icon to open this screen.

Figure 342 Configuration > Network > DNS Inbound LB > Add



The following table describes the labels in this screen.

Table 135 Configuration > Network > DNS Inbound LB > Add/Edit

LABEL	DESCRIPTION
Create New Object	Use this to configure any new setting objects that you need to use in this screen.
General Settings	
Enable	Select this to enable this DNS load balancing rule.
DNS Settings	
Query Domain Name	Type up to 255 characters for a domain name for which you want the Zyxel Device to manage DNS load balancing. You can use a wildcard (*) to let multiple domains match the name. For example, use *.example.com to specify any domain name that ends with "example.com" would match.
Time to Live	Enter the number of seconds the Zyxel Device recommends DNS request hosts to keep the DNS entry in their caches before removing it. Enter 0 to have the Zyxel Device not recommend this so the DNS request hosts will follow their DNS server's TTL setting.
Query From Setting	
IP Address	Select the name of an P address object, including geographic address object, of a computer or a DNS server which makes the DNS queries upon which to apply this rule. DNS servers process client queries using recursion or iteration: • In recursion, DNS servers make recursive queries on behalf of clients. So you have to configure this field to the DNS server's IP address when recursion is used. • In iteration, a client asks the DNS server and expects the best and immediate answer without the DNS server contacting other DNS servers. If the primary DNS server cannot provide the best answer, the client makes iteration queries to other configured DNS servers to resolve the name. You have to configure this field to the client's IP address when iteration is used.

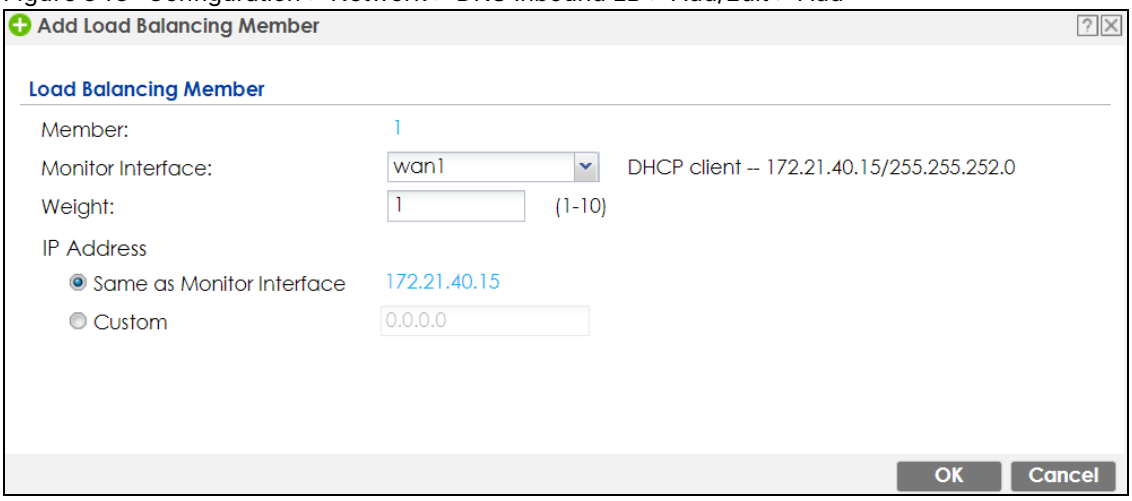
Table 135 Configuration > Network > DNS Inbound LB > Add/Edit (continued)

LABEL	DESCRIPTION
Zone	Select the zone of DNS query messages upon which to apply this rule.
Load Balancing Member	
Load Balancing Algorithm	Select a load balancing method to use from the drop-down list box. Select Weighted Round Robin to balance the traffic load between interfaces based on their respective weights. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight. For example, if the weight ratio of wan1 and wan2 interfaces is 2:1, the Zyxel Device chooses wan1 for 2 sessions' traffic and wan2 for every session's traffic in each round of 3 new sessions. Select Least Connection to have the Zyxel Device choose the member interface which is handling the least number of sessions. Select Least Load - Outbound to have the Zyxel Device choose the member interface which is handling the least amount of outgoing traffic. Select Least Load - Inbound to have the Zyxel Device choose the member interface which is handling the least amount of incoming traffic. Select Least Load - Total to have the Zyxel Device choose the member interface which is handling the least amount of outgoing and incoming traffic.
Failover IP Address	Enter an alternate IP address with which the Zyxel Device will respond to a DNS query message when the load balancing algorithm cannot find any available interface.
Add	Click this to create a new member interface for this rule.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
#	This field displays the order in which the Zyxel Device checks this rule's member interfaces.
IP Address	This field displays the IP address of the member interface.
Monitor Interface	This field displays the name of the member interface. The Zyxel Device manages load balancing between the member interfaces.
Weight	This field is available if you selected Weighted Round Robin as the load balancing algorithm. This field displays the weight of the member interface. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

20.2.2 The DNS Inbound LB Add/Edit Member Screen

The Add Load Balancing Member screen allows you to add a member interface for the DNS load balancing rule. Click Configuration > Network > DNS Inbound LB > Add or Edit and then an Add or Edit icon to open this screen.

Figure 343 Configuration > Network > DNS Inbound LB > Add/Edit > Add



The following table describes the labels in this screen.

Table 136 Configuration > Network > DNS Inbound LB > Add/Edit > Add/Edit

LABEL	DESCRIPTION
Member	The Zyxel Device checks each member interface's loading in the order displayed here.
Monitor Interface	Select an interface to associate it with the DNS load balancing rule. This field also displays whether the IP address is a static IP address (Static), dynamically assigned (Dynamic) or obtained from a DHCP server (DHCP Client), as well as the IP address and subnet mask.
Weight	This field is available if you selected Weighted Round Robin for the load balancing algorithm. Specify the weight of the member interface. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight.
IP Address	
Same as Monitor Interface	Select this to send the IP address displayed in the Monitor Interface field to the DNS query senders.
Custom	Select this and enter another IP address to send to the DNS query senders.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

CHAPTER 21
IPSec VPN

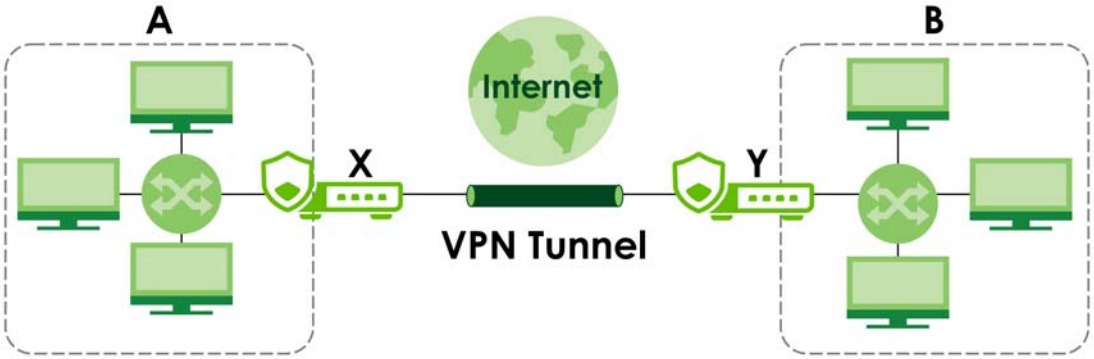
21.1 Virtual Private Networks (VPN) Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

IPSec VPN

Internet Protocol Security (IPSec) VPN connects IPSec routers or remote users using IPSec client software. This standards-based VPN offers flexible solutions for secure data communications across a public network. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer. The Zyxel Device can also combine multiple IPSec VPN connections into one secure network. Here local Zyxel Device X uses an IPSec VPN tunnel to remote (peer) Zyxel Device Y to connect the local (A) and remote (B) networks.

Figure 344 IPSec VPN Example



Internet Key Exchange (IKE): IKEv1 and IKEv2

The Zyxel Device supports IKEv1 and IKEv2 for IPv4 and IPv6 traffic. IKE (Internet Key Exchange) is a protocol used in setting up security associations that allows two parties 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. A security policy for each peer must be manually created.

IPSec VPN consists of two phases: Phase 1 and Phase 2. Phase 1's purpose is to establish a secure authenticated communication channel by using the Diffie–Hellman key exchange algorithm to generate a shared secret key to encrypt IKE communications. This negotiation results in one single bi-directional ISAKMP Security Association (SA). The authentication can be performed using either pre-shared key

(shared secret), signatures, or public key encryption. Phase 1 operates in either Main Mode or Aggressive Mode. Main Mode protects the identity of the peers, but Aggressive Mode does not.

During Phase 2, the remote IPSec routers use the secure channel established in Phase 1 to negotiate Security Associations for IPSec. The negotiation results in a minimum of two unidirectional security associations (one inbound and one outbound). Phase 2 uses Quick Mode (only). Quick mode occurs after IKE has established the secure tunnel in Phase 1. It negotiates a shared IPSec policy, derives shared secret keys used for the IPSec security algorithms, and establishes IPSec SAs. Quick mode is also used to renegotiate a new IPSec SA when the IPSec SA lifetime expires.

In the Zyxel Device, use the VPN Connection tab to set up Phase 2 and the VPN Gateway tab to set up Phase 1.

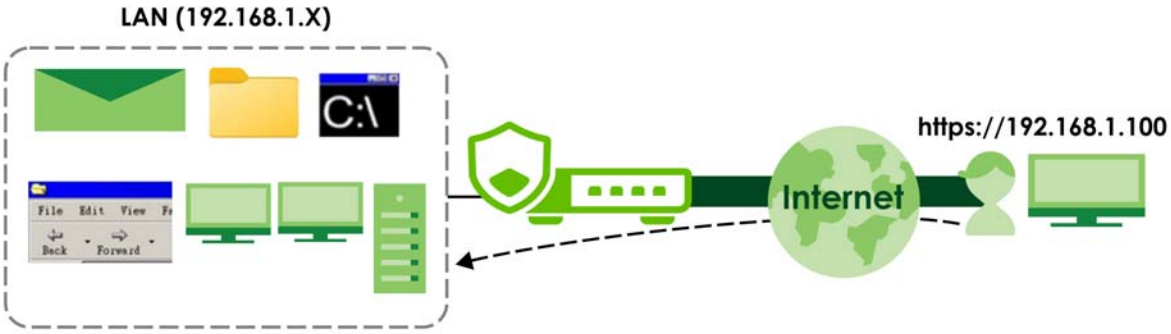
Some differences between IKEv1 and IKEv2 include:

- IKEv2 uses less bandwidth than IKEv1. IKEv2 uses one exchange procedure with 4 messages. IKEv1 uses two phases with Main Mode (9 messages) or Aggressive Mode (6 messages) in phase 1.
- IKEv2 supports Extended Authentication Protocol (EAP) authentication, and IKEv1 supports X-Auth. EAP is important when connecting to existing enterprise authentication systems.
- IKEv2 always uses NAT traversal and Dead Peer Detection (DPD), but they can be disabled in IKEv1 using Zyxel Device firmware (the default is on).
- Configuration payload (includes the IP address pool in the VPN setup data) is supported in IKEv2 (off by default), but not in IKEv1.
- Narrowed is supported in IKEv2, but not in IKEv1. Narrowed has the SA apply only to IP addresses in common between the Zyxel Device and the remote IPSec router.
- The IKEv2 protocol supports connectivity checks which is used to detect whether the tunnel is still up or not. If the check fails (the tunnel is down), IKEv2 can re-establish the connection automatically. The Zyxel Device uses firmware to perform connectivity checks when using IKEv1.

SSL VPN

SSL VPN uses remote users' web browsers to provide the easiest-to-use of the Zyxel Device's VPN solutions. 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. Remote users do not need to configure security settings. Here a user uses his browser to securely connect to network resources in the same way as if he were part of the internal network. See Chapter 22 on page 511 for more on SSL VPN.

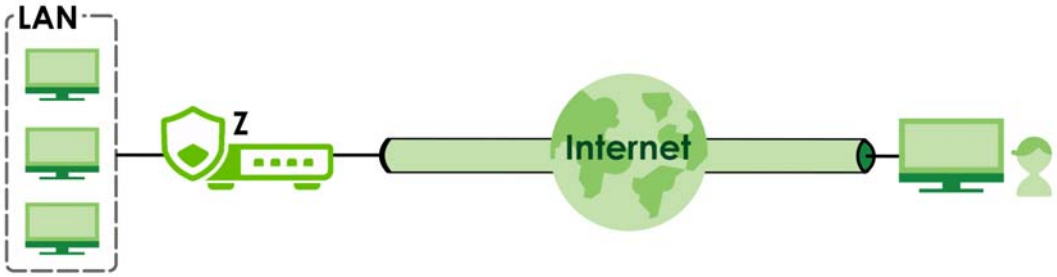
Figure 345 SSL VPN



L2TP VPN

L2TP VPN uses the L2TP and IPSec client software included in remote users' Android, iOS, or Windows operating systems for secure connections to the network behind the Zyxel Device. The remote users do not need their own IPSec gateways or third-party VPN client software. For example, configure sales representatives' laptops, tablets, or smartphones to securely connect to the Zyxel Device's network. See Chapter 23 on page 517 for more on L2TP over IPSec.

Figure 346 L2TP VPN



21.1.1 What You Can Do in this Chapter

- Use the VPN Connection screens (see Section 21.2 on page 478) to specify which IPSec VPN gateway an IPSec VPN connection policy uses, which devices behind the IPSec routers can use the VPN tunnel, and the IPSec SA settings (phase 2 settings). You can also activate or deactivate and connect or disconnect each VPN connection (each IPSec SA).
- Use the VPN Gateway screens (see Section 21.2.1 on page 480) to manage the Zyxel Device's VPN gateways. A VPN gateway specifies the IPSec routers at either end of a VPN tunnel and the IKE SA settings (phase 1 settings). You can also activate and deactivate each VPN gateway.
- Use the VPN Concentrator screens (see Section 21.4 on page 495) to combine several IPSec VPN connections into a single secure network.
- Use the Configuration Provisioning screen (see Section 21.5 on page 497) to set who can retrieve VPN rule settings from the Zyxel Device using the Zyxel Device IPSec VPN Client.

21.1.2 What You Need to Know

An IPSec VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the Zyxel Device and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the Zyxel Device and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the Zyxel Device and remote IPSec router can send data between computers on the local network and remote network. This is illustrated in the following figure.

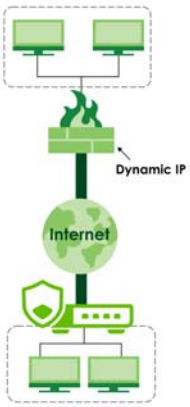
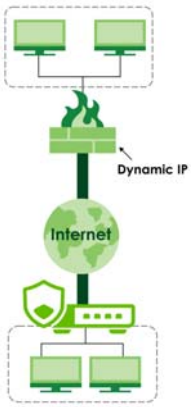
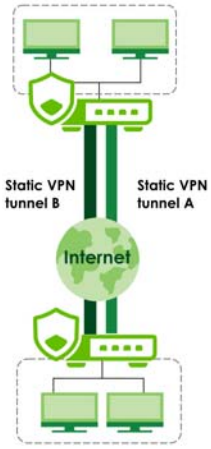
Figure 347 VPN: IKE SA and IPSec SA

In this example, a computer in network A is exchanging data with a computer in network B. Inside networks A and B, the data is transmitted the same way data is normally transmitted in the networks. Between routers X and Y, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is secure because routers X and Y established the IKE SA first.

Application Scenarios

The Zyxel Device's application scenarios make it easier to configure your VPN connection settings.

Table 137 IPSec VPN Application Scenarios

SITE-TO-SITE	SITE-TO-SITE WITH DYNAMIC PEER	REMOTE ACCESS (SERVER ROLE)	REMOTE ACCESS (CLIENT ROLE)	VPN TUNNEL INTERFACE
				
Choose this if the remote IPSec router has a static IP address or a domain name. This Zyxel Device can initiate the VPN tunnel. The remote IPSec router can also initiate the VPN tunnel if this Zyxel Device has a static IP address or a domain name.	Choose this if the remote IPSec router has a dynamic IP address. You don't specify the remote IPSec router's address, but you specify the remote policy (the addresses of the devices behind the remote IPSec router). This Zyxel Device must have a static IP address or a domain name. Only the remote IPSec router can initiate the VPN tunnel.	Choose this to allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. You don't specify the addresses of the client IPSec routers or the remote policy. This creates a dynamic IPSec VPN rule that can let multiple clients connect. Only the clients can initiate the VPN tunnel.	Choose this to connect to an IPSec server. This Zyxel Device is the client (dial-in user). Client role Zyxel Devices initiate IPSec VPN connections to a server role Zyxel Device. This Zyxel Device can have a dynamic IP address. The IPSec server doesn't configure this Zyxel Device's IP address or the addresses of the devices behind it. Only this Zyxel Device can initiate the VPN tunnel.	Choose this to set up a VPN tunnel interface to bind with a VPN connection. The Zyxel Device can use the interface to do load balancing using a specific Trunk. The remote IPSec router should have a static IP address or a domain name.

Finding Out More

- See Section 21.7 on page 500 for IPSec VPN background information.
- See the help in the IPSec VPN quick setup wizard screens.

21.1.3 Before You Begin

This section briefly explains the relationship between VPN tunnels and other features. It also gives some basic suggestions for troubleshooting.

You should set up the following features before you set up the VPN tunnel.

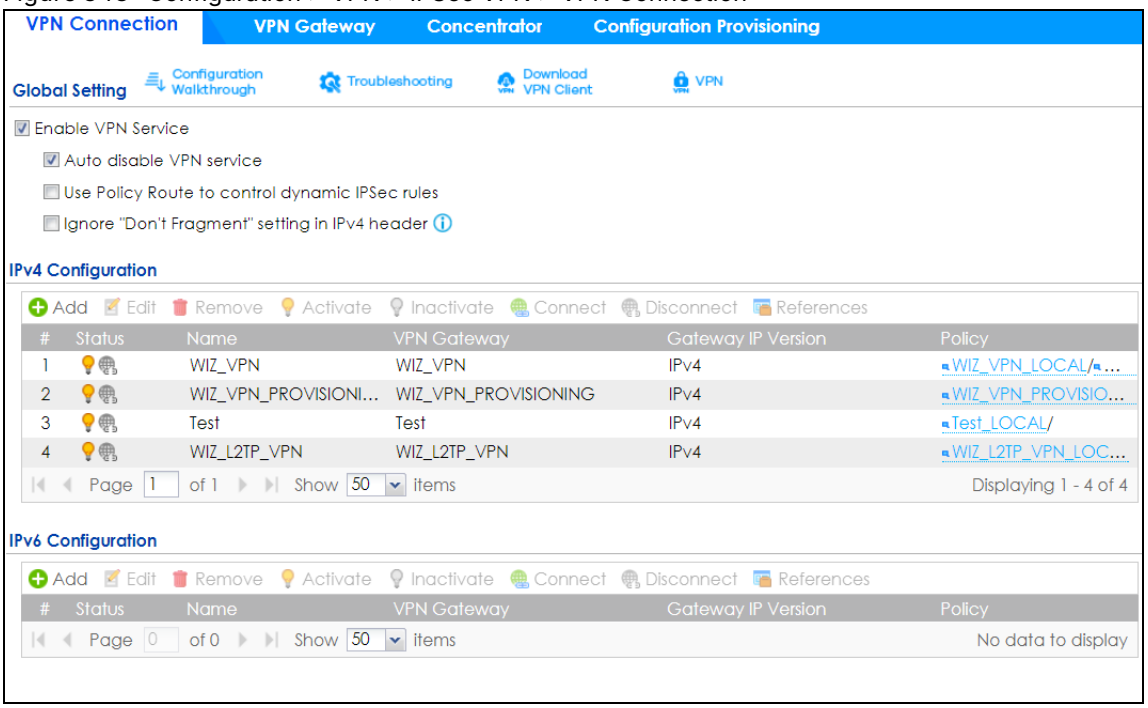
- In any VPN connection, you have to select address objects to specify the local policy and remote policy. You should set up the address objects first.
- In a VPN gateway, you can select an Ethernet interface, virtual Ethernet interface, VLAN interface, or virtual VLAN interface to specify what address the Zyxel Device uses as its IP address when it establishes the IKE SA. You should set up the interface first.
- In a VPN gateway, you can enable extended authentication. If the Zyxel Device is in server mode, you should set up the authentication method (AAA server) first. The authentication method specifies how the Zyxel Device authenticates the remote IPSec router.
- In a VPN gateway, the Zyxel Device and remote IPSec router can use certificates to authenticate each other. Make sure the Zyxel Device and the remote IPSec router will trust each other's certificates.

21.2 The VPN Connection Screen

Click Configuration > VPN > IPSec VPN to open the VPN Connection screen. The VPN Connection screen lists the VPN connection policies and their associated VPN gateway(s), and various settings. In addition, it also lets you activate or deactivate and connect or disconnect each VPN connection (each IPSec SA). Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

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

Figure 348 Configuration > VPN > IPSec VPN > VPN Connection



Each field is discussed in the following table.

Table 138 Configuration > VPN > IPSec VPN > VPN Connection

LABEL	DESCRIPTION
Enable VPN Service	Select this to enable IPSec VPN on the Zyxel Device.
Auto disable VPN service	Select this to disable UDP ports 500 and 4500 when no IPSec VPN rules are configured on the Zyxel Device. Use this to prevent hackers from attacking the Zyxel Device through UDP 500 and 4500 when you're not using IPSec VPN.
Use Policy Route to control dynamic IPSec rules	Select this to be able to use policy routes to manually specify the destination addresses of dynamic IPSec rules. You must manually create these policy routes. The Zyxel Device automatically obtains source and destination addresses for dynamic IPSec rules that do not match any of the policy routes. Clear this to have the Zyxel Device automatically obtain source and destination addresses for all dynamic IPSec rules.
Ignore "Don't Fragment" setting in packet header	Select this to fragment packets larger than the MTU (Maximum Transmission Unit) that have the "Don't Fragment" bit in the IP header turned on. When you clear this the Zyxel Device drops packets larger than the MTU that have the "Don't Fragment" bit in the header turned on.
IPv4 / IPv6 Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The 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.

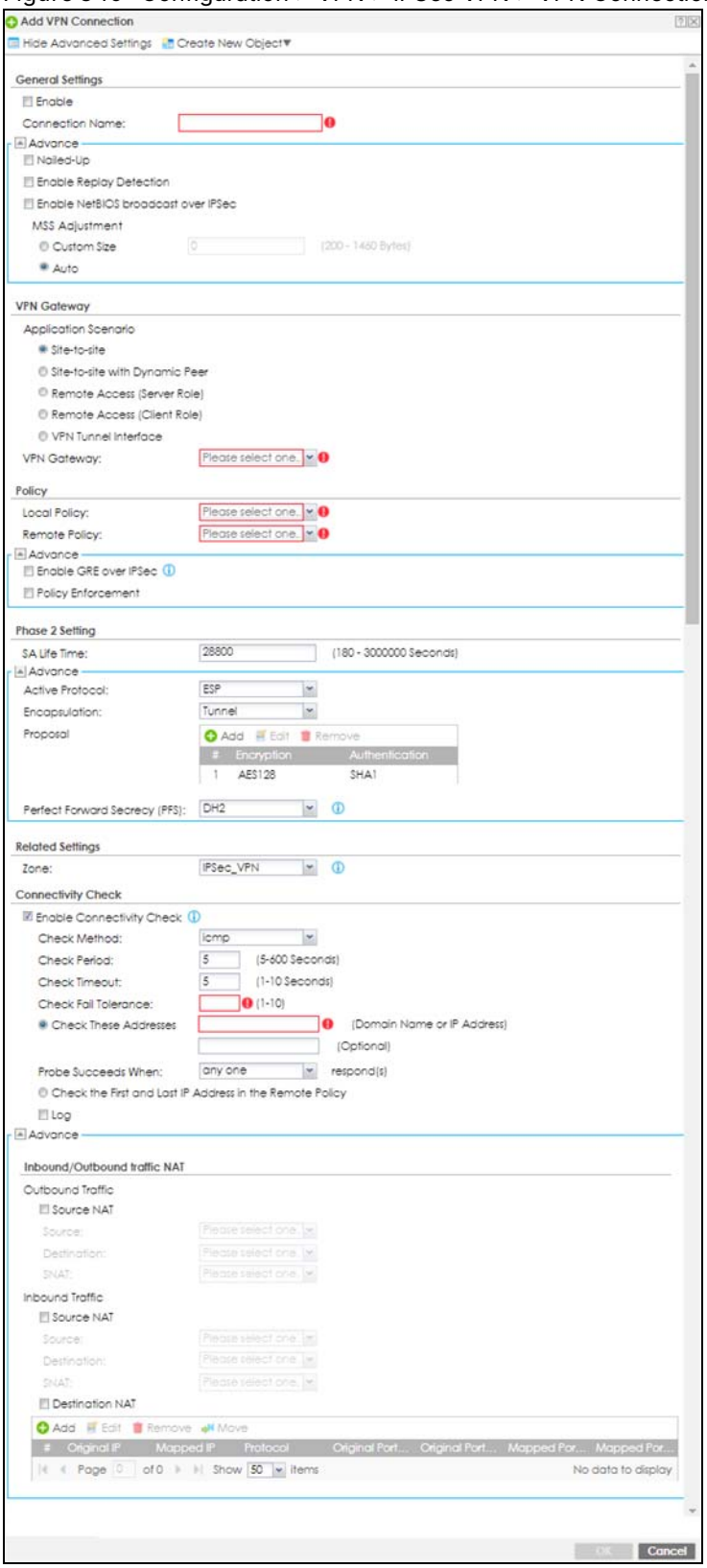
Table 138 Configuration > VPN > IPSec VPN > VPN Connection (continued)

LABEL	DESCRIPTION
Connect	To connect an IPSec SA, select it and click Connect.
Disconnect	To disconnect an IPSec SA, select it and click Disconnect.
References	Select an entry and click References to open a screen that shows which settings use the entry. See Section 11.5.4 on page 314 for an example.
#	This field is a sequential value, and it is not associated with a specific connection.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The connect icon is lit when the interface is connected and dimmed when it is disconnected.
Name	This field displays the name of the IPSec SA.
VPN Gateway	This field displays the VPN gateway in use for this VPN connection.
Gateway IP Version	This field displays what IP version the associated VPN gateway(s) is using. An IPv4 gateway may use an IKEv1 or IKEv2 SA. An IPv6 gateway may use IKEv2 only.
Policy	This field displays the local policy and the remote policy, respectively.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

21.2.1 The VPN Connection Add/Edit Screen

The VPN Connection Add/Edit Gateway screen allows you to create a new VPN connection policy or edit an existing one. To access this screen, go to the Configuration > VPN Connection screen (see Section 21.2 on page 478), and click either the Add icon or an Edit icon.

Figure 349 Configuration > VPN > IPSec VPN > VPN Connection > Add/Edit



Each field is described in the following table.

Table 139 Configuration > VPN > IPSec VPN > VPN Connection > Add/Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create new Object	Use to configure any new settings objects that you need to use in this screen.
General Settings	
Enable	Select this checkbox to activate this VPN connection.
Connection Name	Type the name used to identify this IPSec SA. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Nailed-Up	Select this if you want the Zyxel Device to automatically renegotiate the IPSec SA when the SA life time expires.
Enable Replay Detection	Select this checkbox to detect and reject old or duplicate packets to protect against Denial-of-Service attacks.
Enable NetBIOS Broadcast over IPSec	Select this checkbox if you the Zyxel Device to send NetBIOS (Network Basic Input/Output System) packets through the IPSec SA. NetBIOS packets are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. It may sometimes be necessary to allow NetBIOS packets to pass through IPSec SAs in order to allow local computers to find computers on the remote network and vice versa.
MSS Adjustment	Select Custom Size to set a specific number of bytes for the Maximum Segment Size (MSS) meaning the largest amount of data in a single TCP segment or IP datagram for this VPN connection. Some VPN clients may not be able to use a custom MSS size if it is set too small. In that case those VPN clients will ignore the size set here and use the minimum size that they can use. Select Auto to have the Zyxel Device automatically set the MSS for this VPN connection.
Narrowed	This is visible when you select any options in the VPN Gateway section except for VPN Tunnel Interface. If the IP range on the Zyxel Device (local policy) and the local IP range on the remote IPSec router overlap in an IKEv2 SA, then you may select Narrowed to have the SA only apply to the IP addresses in common. Here are some examples. Zyxel Device (local policy) Remote IPSec router IKEv2 SA-1 192.168.20.0/24 192.168.20.1 ~ 192.168.20.20 Narrowed 192.168.20.1 ~ 192.168.20.20 IKEv2 SA- 2 192.168.30.50 ~ 192.168.30.70 192.168.30.60 ~ 192.168.30.80 Narrowed 192.168.30.60 ~ 192.168.30.70
VPN Gateway	

Table 139 Configuration > VPN > IPSec VPN > VPN Connection > Add/Edit (continued)

LABEL	DESCRIPTION
Application Scenario	Select the scenario that best describes your intended VPN connection. Site-to-site - Choose this if the remote IPSec router has a static IP address or a domain name. This Zyxel Device can initiate the VPN tunnel. Site-to-site with Dynamic Peer - Choose this if the remote IPSec router has a dynamic IP address. Only the remote IPSec router can initiate the VPN tunnel. Remote Access (Server Role) - Choose this to 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) - Choose this to connect to an IPSec server. This Zyxel Device is the client (dial-in user) and can initiate the VPN tunnel. VPN Tunnel Interface - Choose this to set up a VPN tunnel interface to bind with a VPN connection. The Zyxel Device can use the interface to do load balancing using a specific Trunk. The remote IPSec router should have a static IP address or a domain name. See Configuration > Network > Interface > VTI.
VPN Gateway	Select the VPN gateway this VPN connection is to use or select Create Object to add another VPN gateway for this VPN connection to use.
Policy	
Local Policy	Select the address corresponding to the local network. Use Create new Object if you need to configure a new one.
Remote Policy	Select the address corresponding to the remote network. Use Create new Object if you need to configure a new one.
Enable GRE over IPSec	Select this to allow traffic using the Generic Routing Encapsulation (GRE) tunneling protocol through an IPSec tunnel.
Policy Enforcement	Clear this to allow traffic with source and destination IP addresses that do not match the local and remote policy to use the VPN tunnel. Leave this cleared for free access between the local and remote networks. Selecting this restricts who can use the VPN tunnel. The Zyxel Device drops traffic with source and destination IP addresses that do not match the local and remote policy.
Mode Config	This is visible when you select Remote Access (Server Role) and a VPN Gateway.
Enable Mode Config	Select this to have the IPSec VPN client receive an IP address, DNS and WINS information from the Zyxel Device.
IP Address Pool	Select an address object from the drop-down list box.
First DNS Server (Optional)	The Domain Name System (DNS) maps a domain name to an IP address and vice versa. The Zyxel Device uses these (in the order you specify here) to resolve domain names for VPN. Enter a DNS server's IP address.
Second DNS Server (Optional)	Enter a secondary DNS server's IP address that is checked if the first one is unavailable.
First WINS Server (Optional)	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Second WINS Server (Optional)	Enter a secondary WINS server's IP address that is checked if the first one is unavailable.
Configuration Payload	This is only available when you have created an IKEv2 Gateway and are using Remote Access (Server Role).
Enable Configuration Payload	Select this to have at least have the IP address pool included in the VPN setup data.
IP Address Pool:	Select an address object from the drop-down list box.

Table 139 Configuration > VPN > IPSec VPN > VPN Connection > Add/Edit (continued)

LABEL	DESCRIPTION
First DNS Server (optional)	The Domain Name System (DNS) maps a domain name to an IP address and vice versa. The Zyxel Device uses these (in the order you specify here) to resolve domain names for VPN. Enter a DNS server's IP address.
Second DNS Server (Optional)	Enter a secondary DNS server's IP address that is checked if the first one is unavailable.
First WINS Server (Optional)	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Second WINS Server (Optional)	Enter a secondary WINS server's IP address that is checked if the first one is unavailable.
Phase 2 Settings	
SA Life Time	Type the maximum number of seconds the IPSec SA can last. Shorter life times provide better security. The Zyxel Device automatically negotiates a new IPSec SA before the current one expires, if there are users who are accessing remote resources.
Active Protocol	Select which protocol you want to use in the IPSec SA. Choices are: AH (RFC 2402) - provides integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not encryption. If you select AH, you must select an Authentication algorithm. ESP (RFC 2406) - provides encryption and the same services offered by AH, but its authentication is weaker. If you select ESP, you must select an Encryption algorithm and Authentication algorithm. Both AH and ESP increase processing requirements and latency (delay). The Zyxel Device and remote IPSec router must use the same active protocol.
Encapsulation	Select which type of encapsulation the IPSec SA uses. Choices are Tunnel - this mode encrypts the IP header information and the data. Transport - this mode only encrypts the data. The Zyxel Device and remote IPSec router must use the same encapsulation.
Proposal	Use this section to manage the encryption algorithm and authentication algorithm pairs the Zyxel Device accepts from the remote IPSec router for negotiating the IPSec SA.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific proposal. The sequence of proposals should not affect performance significantly.

Table 139 Configuration > VPN > IPSec VPN > VPN Connection > Add/Edit (continued)

LABEL	DESCRIPTION
Encryption	This field is applicable when the Active Protocol is ESP. Select which key size and encryption algorithm to use in the IPSec SA. Choices are: NULL - no encryption key or algorithm DES - a 56-bit key with the DES encryption algorithm 3DES - a 168-bit key with the DES encryption algorithm AES128 - a 128-bit key with the AES encryption algorithm AES192 - a 192-bit key with the AES encryption algorithm AES256 - a 256-bit key with the AES encryption algorithm The Zyxel Device and the remote IPSec router must both have at least one proposal that uses use the same encryption and the same key. Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput.
Authentication	Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are SHA1, SHA256, SHA512 and MD5. SHA is generally considered stronger than MD5, but it is also slower. The Zyxel Device and the remote IPSec router must both have a proposal that uses the same authentication algorithm.
Perfect Forward Secrecy (PFS)	Select whether or not you want to enable Perfect Forward Secrecy (PFS) and, if you do, which Diffie-Hellman key group to use for encryption. Choices are: none - disable PFS DH1 - enable PFS and use a 768-bit random number DH2 - enable PFS and use a 1024-bit random number DH5 - enable PFS and use a 1536-bit random number DH14 - enable PFS and use a 2048 bit random number PFS changes the root key that is used to generate encryption keys for each IPSec SA. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group. PFS is ignored in initial IKEv2 authentication but is used when re-authenticating.
Related Settings	
Zone	Select the security zone into which to add this VPN connection policy. Any security rules or settings configured for the selected zone apply to this VPN connection policy.
Connectivity Check	The Zyxel Device can regularly check the VPN connection to the gateway you specified to make sure it is still available.
Enable Connectivity Check	Select this to turn on the VPN connection check.
Check Method	Select how the Zyxel Device checks the connection. The peer must be configured to respond to the method you select. Select icmp to have the Zyxel Device regularly ping the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to respond to pings. Select tcp to have the Zyxel Device regularly perform a TCP handshake with the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to accept the TCP connection.
Check Port	This field displays when you set the Check Method to tcp. Specify the port number to use for a TCP connectivity check.

Table 139 Configuration > VPN > IPSec VPN > VPN Connection > Add/Edit (continued)

LABEL	DESCRIPTION
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures allowed before the Zyxel Device disconnects the VPN tunnel. The Zyxel Device resumes using the first peer gateway address when the VPN connection passes the connectivity check.
Check These Addresses	Type one or two domain names or IPv4 addresses for the connectivity check. You can type an IPv4 address in one field and a domain name in the other. For example, type “192.168.1.2” in the top field and “www.zyxel.com” in the bottom field.
Probe Succeeds When	This field applies when you specify two domain names or IP addresses for the connectivity check. Select any one if you want the check to pass if at least one of the domain names or IP addresses responds. Select all if you want the check to pass only if both domain names or IP addresses respond.
Check the First and Last IP Address in the Remote Policy	Select this to have the Zyxel Device check the connection to the first and last IP addresses in the connection’s remote policy. Make sure one of these is the peer gateway’s LAN IP address.
Log	Select this to have the Zyxel Device generate a log every time it checks this VPN connection.
Inbound/Outbound traffic NAT	
Outbound Traffic	
Source NAT	This translation hides the source address of computers in the local network. It may also be necessary if you want the Zyxel Device to route packets from computers outside the local network through the IPSec SA.
Source	Select the address object that represents the original source address (or select Create Object to configure a new one). This is the address object for the computer or network outside the local network.
Destination	Select the address object that represents the original destination address (or select Create Object to configure a new one). This is the address object for the remote network.
SNAT	Select the address object that represents the translated source address (or select Create Object to configure a new one). This is the address object for the local network. The size of the original source address range (Source) must be equal to the size of the translated source address range (SNAT).
Inbound Traffic	
Source NAT	This translation hides the source address of computers in the remote network.
Source	Select the address object that represents the original source address (or select Create Object to configure a new one). This is the address object for the remote network. The size of the original source address range (Source) must be equal to the size of the translated source address range (SNAT).
Destination	Select the address object that represents the original destination address (or select Create Object to configure a new one). This is the address object for the local network.
SNAT	Select the address object that represents the translated source address (or select Create Object to configure a new one). This is the address that hides the original source address. The size of the original source address range (Source) must be equal to the size of the translated source address range (SNAT).
Destination NAT	This translation forwards packets (for example, mail) from the remote network to a specific computer (for example, the mail server) in the local network.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.

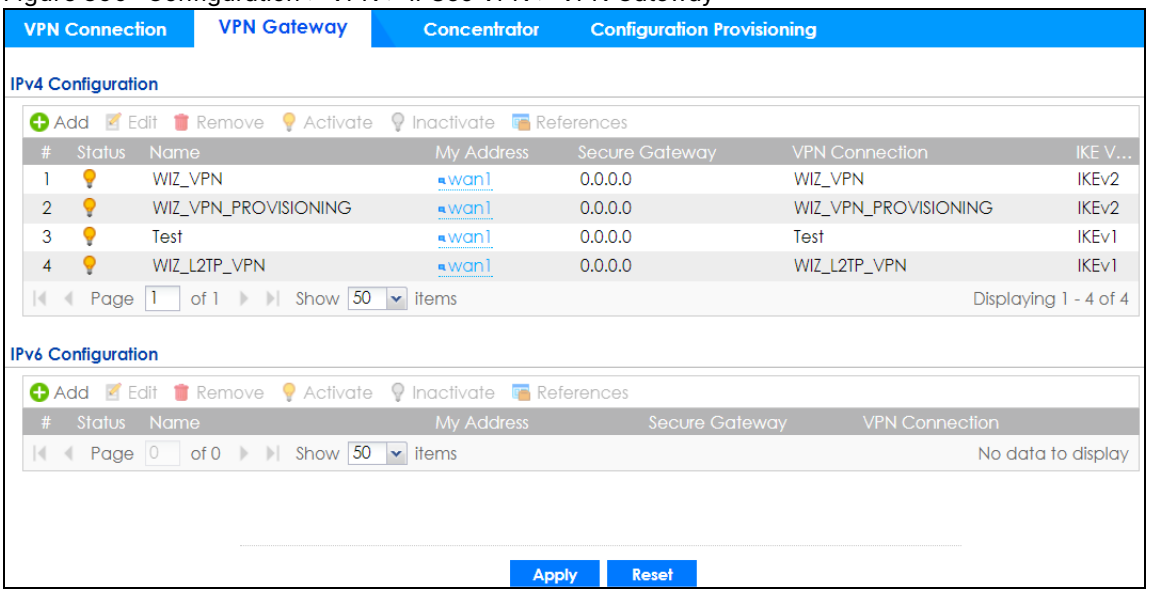
Table 139 Configuration > VPN > IPSec VPN > VPN Connection > Add/Edit (continued)

LABEL	DESCRIPTION
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Move	To change an entry's position in the numbered list, select it and click Move to display a field to type a number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed.
#	This field is a sequential value, and it is not associated with a specific NAT record. However, the order of records is the sequence in which conditions are checked and executed.
Original IP	Select the address object that represents the original destination address. This is the address object for the remote network.
Mapped IP	Select the address object that represents the desired destination address. For example, this is the address object for the mail server.
Protocol	Select the protocol required to use this translation. Choices are: TCP, UDP, or All.
Original Port Start / Original Port End	These fields are available if the protocol is TCP or UDP. Enter the original destination port or range of original destination ports. The size of the original port range must be the same size as the size of the mapped port range.
Mapped Port Start / Mapped Port End	These fields are available if the protocol is TCP or UDP. Enter the translated destination port or range of translated destination ports. The size of the original port range must be the same size as the size of the mapped port range.
OK	Click OK to save the changes.
Cancel	Click Cancel to discard all changes and return to the main VPN screen.

21.3 The VPN Gateway Screen

The VPN Gateway summary screen displays the IPSec VPN gateway policies in the Zyxel Device, as well as the Zyxel Device's address, remote IPSec router's address, and associated VPN connections for each one. In addition, it also lets you activate and deactivate each VPN gateway. To access this screen, click Configuration > VPN > Network > IPSec VPN > VPN Gateway. The following screen appears.

Figure 350 Configuration > VPN > IPSec VPN > VPN Gateway



Each field is discussed in the following table. See Section 21.3.1 on page 488 for more information.

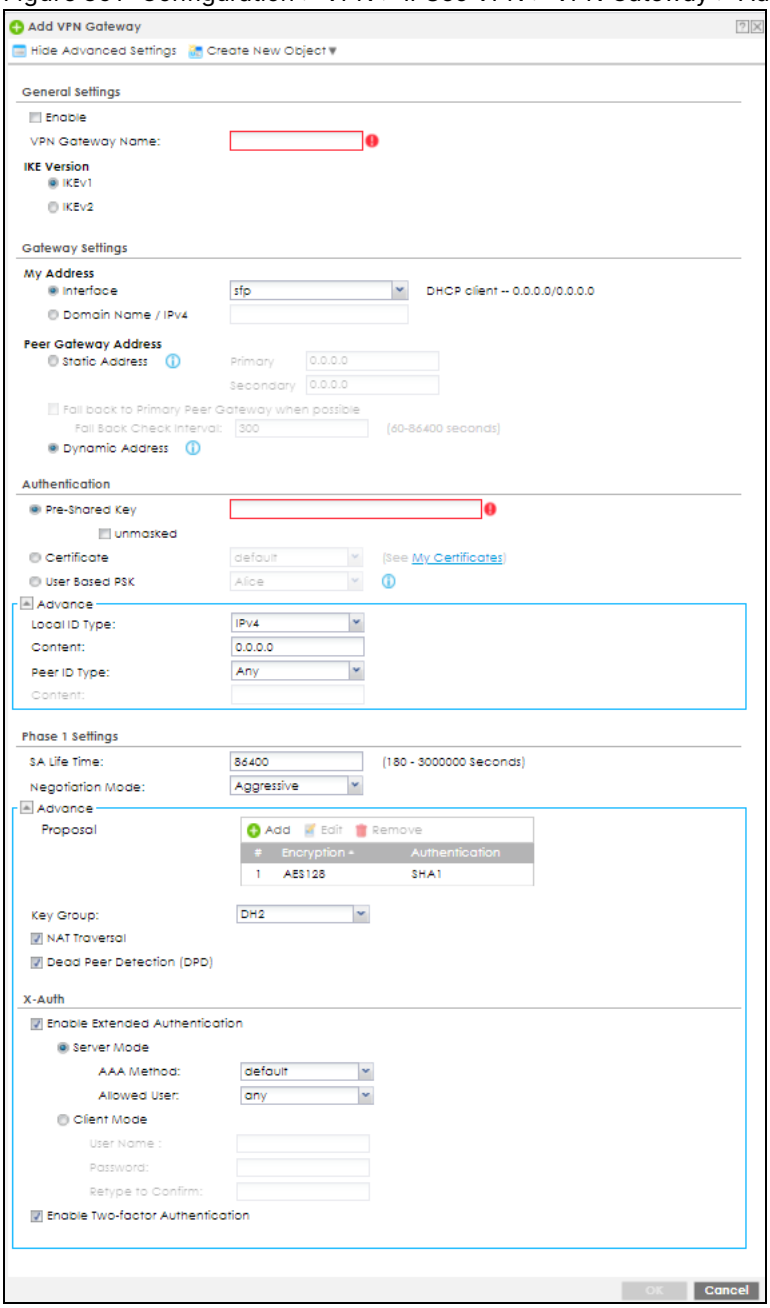
Table 140 Configuration > VPN > IPSec VPN > VPN Gateway

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The 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.
References	Select an entry and click References to open a screen that shows which settings use the entry. See Section 11.5.4 on page 314 for an example.
#	This field is a sequential value, and it is not associated with a specific VPN gateway.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the VPN gateway
My address	This field displays the interface or a domain name the Zyxel Device uses for the VPN gateway.
Secure Gateway	This field displays the IP address(es) of the remote IPSec routers.
VPN Connection	This field displays VPN connections that use this VPN gateway.
IKE Version	This field displays whether the gateway is using IKEv1 or IKEv2. IKEv1 applies to IPv4 traffic only. IKEv2 applies to both IPv4 and IPv6 traffic. IKE (Internet Key Exchange) is a protocol used in setting up security associations that allows two parties to send data securely. See Section 21.1 on page 473 for more information on IKEv1 and IKEv2.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

21.3.1 The VPN Gateway Add/Edit Screen

The VPN Gateway Add/Edit screen allows you to create a new VPN gateway policy or edit an existing one. To access this screen, go to the VPN Gateway summary screen (see Section 21.3 on page 487), and click either the Add icon or an Edit icon.

Figure 351 Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit



Each field is described in the following table.

Table 141 Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create New Object	Use to configure any new settings objects that you need to use in this screen.
General Settings	
Enable	Select this to activate the VPN Gateway policy.

Table 141 Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit (continued)

LABEL	DESCRIPTION
VPN Gateway Name	Type the name used to identify this VPN gateway. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
IKE Version	
IKEv1 / IKEv2	Select IKEv1 or IKEv2. IKEv1 applies to IPv4 traffic only. IKEv2 applies to both IPv4 and IPv6 traffic. IKE (Internet Key Exchange) is a protocol used in setting up security associations that allows two parties to send data securely. See Section 21.1 on page 473 for more information on IKEv1 and IKEv2.
Gateway Settings	
My Address	Select how the IP address of the Zyxel Device in the IKE SA is defined. If you select Interface, select the Ethernet interface, VLAN interface, virtual Ethernet interface, virtual VLAN interface or PPPoE/PPTP interface. The IP address of the Zyxel Device in the IKE SA is the IP address of the interface. If you select Domain Name / IP, enter the domain name or the IP address of the Zyxel Device. The IP address of the Zyxel Device in the IKE SA is the specified IP address or the IP address corresponding to the domain name. 0.0.0.0 is not generally recommended as it has the Zyxel Device accept IPSec requests destined for any interface address on the Zyxel Device.
Peer Gateway Address	Select how the IP address of the remote IPSec router in the IKE SA is defined. Select Static Address to enter the domain name or the IP address of the remote IPSec router. You can provide a second IP address or domain name for the Zyxel Device to try if it cannot establish an IKE SA with the first one. Fall back to Primary Peer Gateway when possible: When you select this, if the connection to the primary address goes down and the Zyxel Device changes to using the secondary connection, the Zyxel Device will reconnect to the primary address when it becomes available again and stop using the secondary connection. Users will lose their VPN connection briefly while the Zyxel Device changes back to the primary connection. To use this, the peer device at the secondary address cannot be set to use a nailed-up VPN connection. In the Fallback Check Interval field, set how often to check if the primary address is available. Select Dynamic Address if the remote IPSec router has a dynamic IP address (and does not use DDNS).
Authentication	Note: The Zyxel Device and remote IPSec router must use the same authentication method to establish the IKE SA.
Pre-Shared Key	Select this to have the Zyxel Device and remote IPSec router use a pre-shared key (password) of up to 128 characters to identify each other when they negotiate the IKE SA. Type the pre-shared key in the field to the right. The pre-shared key can be: • 8 to 128 single-byte characters, including a-zA-Z0-9,;.|`~!?@#$%^&*()_^+\{}':./<>= -"[] are not allowed. • pairs of hexadecimal (a-zA-Z0-9) characters, preceded by “0x”. Type “0x” at the beginning of a hexadecimal key. For example, "0x0123456789ABCDEF" is in hexadecimal format; “0123456789ABCDEF” is in ASCII format. If you use hexadecimal, you must enter twice as many characters since you need to enter pairs. The Zyxel Device and remote IPSec router must use the same pre-shared key. Select unmasked to see the pre-shared key in readable plain text.

Table 141 Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit (continued)

LABEL	DESCRIPTION
Certificate	Select this to have the Zyxel Device and remote IPSec router use certificates to authenticate each other when they negotiate the IKE SA. Then select the certificate the Zyxel Device uses to identify itself to the remote IPSec router. This certificate is one of the certificates in My Certificates. If this certificate is self-signed, import it into the remote IPSec router. If this certificate is signed by a CA, the remote IPSec router must trust that CA. Note: The IPSec routers must trust each other's certificates. The Zyxel Device uses one of its Trusted Certificates to authenticate the remote IPSec router's certificate. The trusted certificate can be a self-signed certificate or that of a trusted CA that signed the remote IPSec router's certificate.
User-based PSK	User-based PSK (IKEv1 only) generates and manages separate pre-shared keys for every user. This enables multiple users, each with a unique key, to access the same VPN gateway policy with one-to-one authentication and strong encryption. Access can be denied on a per-user basis thus allowing VPN SA user-based policies. Click User-Based PSK then select a user or group object who is allowed VPN SA access using this VPN gateway policy. This is for IKEv1 only.
Local ID Type	This field is read-only if the Zyxel Device and remote IPSec router use certificates to identify each other. Select which type of identification is used to identify the Zyxel Device during authentication. Choices are: IPv4 or IPv6 - the Zyxel Device is identified by an IP address DNS - the Zyxel Device is identified by a domain name E-mail - the Zyxel Device is identified by the string specified in this field
Content	This field is read-only if the Zyxel Device and remote IPSec router use certificates to identify each other. Type the identity of the Zyxel Device during authentication. The identity depends on the Local ID Type. IP - type an IP address; if you type 0.0.0.0, the Zyxel Device uses the IP address specified in the My Address field. This is not recommended in the following situations: • There is a NAT router between the Zyxel Device and remote IPSec router. • You want the remote IPSec router to be able to distinguish between IPSec SA requests that come from IPSec routers with dynamic WAN IP addresses. • In these situations, use a different IP address, or use a different Local ID Type. • DNS - type the fully qualified domain name (FQDN). This value is only used for identification and can be any string that matches the peer ID string. • E-mail - the Zyxel Device is identified by the string you specify here; you can use 1 to 63 single-byte characters, including a-zA-Z0-9_.- • !"#$%&'()*+,/;:<=>?[\]^'{|} are not allowed. This value is only used for identification and can be any string.
Peer ID Type	Select which type of identification is used to identify the remote IPSec router during authentication. Choices are: IP - the remote IPSec router is identified by an IP address DNS - the remote IPSec router is identified by a domain name E-mail - the remote IPSec router is identified by the string specified in this field Any - the Zyxel Device does not check the identity of the remote IPSec router If the Zyxel Device and remote IPSec router use certificates, there is one more choice. Subject Name - the remote IPSec router is identified by the subject name in the certificate

Table 141 Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit (continued)

LABEL	DESCRIPTION
Content	This field is disabled if the Peer ID Type is Any. Type the identity of the remote IPSec router during authentication. The identity depends on the Peer ID Type. If the Zyxel Device and remote IPSec router do not use certificates, IP - type an IP address; see the note at the end of this description. DNS - type the fully qualified domain name (FQDN). This value is only used for identification and can be any string that matches the peer ID string. E-mail - the remote IPSec router is identified by the string you specify here; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string. If the Zyxel Device and remote IPSec router use certificates, type the following fields from the certificate used by the remote IPSec router. IP - subject alternative name field; see the note at the end of this description. DNS - subject alternative name field E-mail - subject alternative name field. Subject Name - subject name (maximum 255 ASCII characters, including spaces) Note: If Peer ID Type is IP, please read the rest of this section. If you type 0.0.0.0, the Zyxel Device uses the IP address specified in the Secure Gateway Address field. This is not recommended in the following situations: • There is a NAT router between the Zyxel Device and remote IPSec router. • You want the remote IPSec router to be able to distinguish between IPSec SA requests that come from IPSec routers with dynamic WAN IP addresses. In these situations, use a different IP address, or use a different Peer ID Type.
Phase 1 Settings	
SA Life Time (Seconds)	Type the maximum number of seconds the IKE SA can last. When this time has passed, the Zyxel Device and remote IPSec router have to update the encryption and authentication keys and re-negotiate the IKE SA. This does not affect any existing IPSec SAs, however.
Negotiation Mode	Select the negotiation mode to use to negotiate the IKE SA. Choices are Main - this encrypts the Zyxel Device's and remote IPSec router's identities but takes more time to establish the IKE SA Aggressive - this is faster but does not encrypt the identities The Zyxel Device and the remote IPSec router must use the same negotiation mode.
Proposal	Use this section to manage the encryption algorithm and authentication algorithm pairs the Zyxel Device accepts from the remote IPSec router for negotiating the IKE SA.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific proposal. The sequence of proposals should not affect performance significantly.

Table 141 Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit (continued)

LABEL	DESCRIPTION
Encryption	Select which key size and encryption algorithm to use in the IKE SA. Choices are: DES - a 56-bit key with the DES encryption algorithm 3DES - a 168-bit key with the DES encryption algorithm AES128 - a 128-bit key with the AES encryption algorithm AES192 - a 192-bit key with the AES encryption algorithm AES256 - a 256-bit key with the AES encryption algorithm The Zyxel Device and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication	Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are SHA1, SHA256, SHA512 and MD5. SHA is generally considered stronger than MD5, but it is also slower. The remote IPSec router must use the same authentication algorithm.
Key Group	Select which Diffie-Hellman key group (DH*x*) you want to use to create encryption keys. See Diffie-Hellman (DH) Key Exchange for more information on which to select.
NAT Traversal	Select this if any of these conditions are satisfied. • This IKE SA might be used to negotiate IPSec SAs that use ESP as the active protocol. • There are one or more NAT routers between the Zyxel Device and remote IPSec router, and these routers do not support IPSec pass-thru or a similar feature. The remote IPSec router must also enable NAT traversal, and the NAT routers have to forward packets with UDP port 500 and UDP 4500 headers unchanged. This field applies for IKEv1 only. NAT Traversal is always performed when you use IKEv2.
Dead Peer Detection (DPD)	Select this checkbox if you want the Zyxel Device to make sure the remote IPSec router is there before it transmits data through the IKE SA. The remote IPSec router must support DPD. If there has been no traffic for at least 15 seconds, the Zyxel Device sends a message to the remote IPSec router. If the remote IPSec router responds, the Zyxel Device transmits the data. If the remote IPSec router does not respond, the Zyxel Device shuts down the IKE SA. If the remote IPSec router does not support DPD, see if you can use the VPN connection connectivity check (see Section 21.2.1 on page 480). This field applies for IKEv1 only. Dead Peer Detection (DPD) is always performed when you use IKEv2.
X Auth / Extended Authentication Protocol	This part of the screen displays X-Auth when using IKEv1 and Extended Authentication Protocol when using IKEv2.
X-Auth	This displays when using IKEv1. When different users use the same VPN tunnel to connect to the Zyxel Device (telecommuters sharing a tunnel for example), use X-auth to enforce a user name and password check. This way even though telecommuters all know the VPN tunnel's security settings, each still has to provide a unique user name and password.
Enable Extended Authentication	Select this if one of the routers (the Zyxel Device or the remote IPSec router) verifies a user name and password from the other router using the local user database and/or an external server.
Server Mode	Select this if the Zyxel Device authenticates the user name and password from the remote IPSec router. You also have to select the authentication method, which specifies how the Zyxel Device authenticates this information.
AAA Method	Select the authentication method, which specifies how the Zyxel Device authenticates this information.
Allowed User	Extended authentication now supports an allowed user. Select what users should be authenticated.

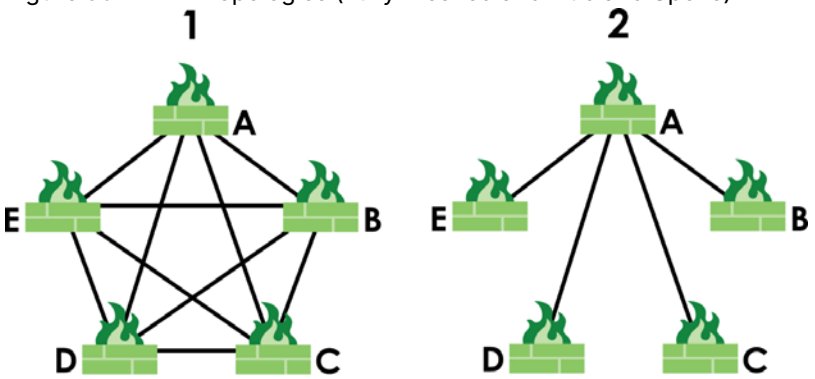
Table 141 Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit (continued)

LABEL	DESCRIPTION
Client Mode	Select this radio button if the Zyxel Device provides a username and password to the remote IPSec router for authentication. You also have to provide the User Name and the Password.
User Name	This field is required if the Zyxel Device is in Client Mode for extended authentication. Type the user name the Zyxel Device sends to the remote IPSec router. This is case-sensitive. Enter 1-31 single-byte characters, including a-zA-Z.- 0-9!"#$%&'()*+/:;<>?[\]^'{|} and spaces are not allowed.
Password	This field is required if the Zyxel Device is in Client Mode for extended authentication. Type the password the Zyxel Device sends to the remote IPSec router. Enter 1 to 63 single-byte characters, including 0-9a-zA-Z!"#$%&'()*+,-./:;<=>@\^_'{|} ?[] and spaces are not allowed.
Retype to Confirm	Type the exact same password again here to make sure an error was not made when typing it originally.
Extended Authentication Protocol	This displays when using IKEv2. EAP uses a certificate for authentication.
Enable Extended Authentication Protocol	Select this if one of the routers (the Zyxel Device or the remote IPSec router) verifies a user name and password from the other router using the local user database and/or an external server or a certificate.
Allowed Auth Method	This field displays the authentication method that is used to authenticate the users.
Server Mode	Select this if the Zyxel Device authenticates the user name and password from the remote IPSec router. You also have to select an AAA method, which specifies how the Zyxel Device authenticates this information and who may be authenticated (Allowed User).
Client Mode	Select this radio button if the Zyxel Device provides a username and password to the remote IPSec router for authentication. You also have to provide the User Name and the Password.
User Name	This field is required if the Zyxel Device is in Client Mode for extended authentication. Type the user name the Zyxel Device sends to the remote IPSec router. The user name can be 1-31 ASCII characters. It is case-sensitive, but spaces are not allowed.
Password	This field is required if the Zyxel Device is in Client Mode for extended authentication. Type the password the Zyxel Device sends to the remote IPSec router. The password can be 1-31 ASCII characters. It is case-sensitive, but spaces are not allowed.
Retype to Confirm	Type the exact same password again here to make sure an error was not made when typing it originally.
Enable Two-Factor Authentication	Select this to enable two-factor authentication for this VPN gateway policy. Make sure to enable two-factor authentication in Object > Auth. Method > Two-factor Authentication > VPN Access. You will also need to do one of the following: • Click Show Advanced Settings. If you select IKEv1 in IKE Version, enable X-Auth in IPSec VPN > Add VPN Gateway. Enable Mode Config in IPSec VPN > Add VPN Connection. • Click Show Advanced Settings. If you select IKEv2 in IKE Version, enable Extended Authentication Protocol in IPSec VPN > Add VPN Gateway. Enable Configuration Payload in IPSec VPN > Add VPN Connection. • Enable L2TP over IPSec VPN in Configuration > VPN > L2TP VPN. See Section 30.8.4 on page 738 for more information on two-factor authentication.
OK	Click OK to save your settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

21.4 VPN Concentrator

A VPN concentrator combines several IPSec VPN connections into one secure network.

Figure 352 VPN Topologies (Fully Meshed and Hub and Spoke)



In a fully-meshed VPN topology (1 in the figure), there is a VPN connection between every pair of routers. In a hub-and-spoke VPN topology (2 in the figure), there is a VPN connection between each spoke router (B, C, D, and E) and the hub router (A), which uses the VPN concentrator. The VPN concentrator routes VPN traffic between the spoke routers and itself.

A VPN concentrator reduces the number of VPN connections that you have to set up and maintain on the network. You might also be able to consolidate the policy routes in each spoke router, depending on the IP addresses and subnets of each spoke.

However a VPN concentrator is not for every situation. The hub router is a single failure point, so a VPN concentrator is not as appropriate if the connection between spoke routers cannot be down occasionally (maintenance, for example). There is also more burden on the hub router. It receives VPN traffic from one spoke, decrypts it, inspects it to find out to which spoke to route it, encrypts it, and sends it to the appropriate spoke. Therefore, a VPN concentrator is more suitable when there is a minimum amount of traffic between spoke routers.

21.4.1 VPN Concentrator Requirements and Suggestions

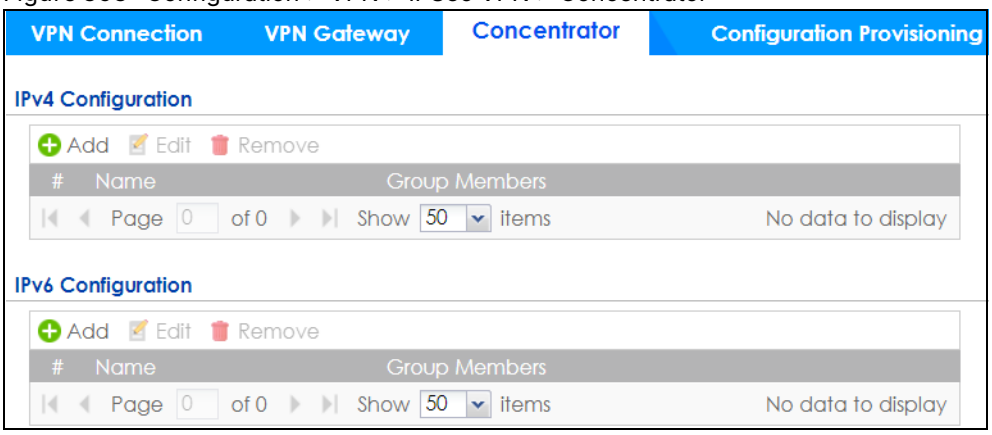
Consider the following when using the VPN concentrator.

- The local IP addresses configured in the VPN rules should not overlap.
- The concentrator must have at least one separate VPN rule for each spoke. In the local policy, specify the IP addresses of the networks with which the spoke is to be able to have a VPN tunnel. This may require you to use more than one VPN rule for each spoke.
- To have all Internet access from the spoke routers go through the VPN tunnel, set the VPN rules in the spoke routers to use 0.0.0.0 (any) as the remote IP address.
- Your security policies can still block VPN packets.

21.4.2 VPN Concentrator Screen

The VPN Concentrator summary screen displays the VPN concentrators in the Zyxel Device. To access this screen, click Configuration > VPN > IPSec VPN > Concentrator.

Figure 353 Configuration > VPN > IPSec VPN > Concentrator



Each field is discussed in the following table. See Section 21.4.3 on page 496 for more information.

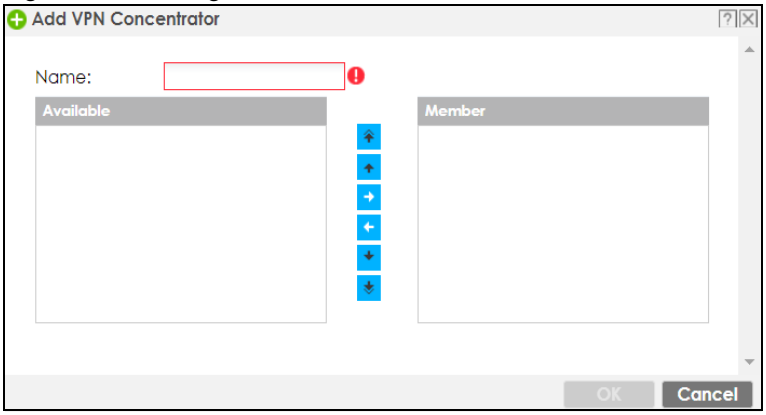
Table 142 Configuration > VPN > IPSec VPN > Concentrator

LABEL	DESCRIPTION
IPv4/IPv6 Configuration	Choose to configure for IPv4 or IPv6 traffic.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific concentrator.
Name	This field displays the name of the VPN concentrator.
Group Members	These are the VPN connection policies that are part of the VPN concentrator.

21.4.3 The VPN Concentrator Add/Edit Screen

Use the VPN Concentrator Add/Edit screen to create or edit a VPN concentrator. To access this screen, go to the VPN Concentrator summary screen (see Section 21.4 on page 495), and click either the Add icon or an Edit icon.

Figure 354 Configuration > VPN > IPSec VPN > Concentrator > Add/Edit



Each field is described in the following table.

Table 143 VPN > IPSec VPN > Concentrator > Add/Edit

LABEL	DESCRIPTION
Name	Enter the name of the concentrator. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Member	Select the concentrator's IPSec VPN connection policies. Note: You must disable policy enforcement in each member. See Section 21.2.1 on page 480. IPSec VPN connection policies that do not belong to a VPN concentrator appear under Available. Select any VPN connection policies that you want to add to the VPN concentrator and click the right arrow button to add them. The VPN concentrator's member VPN connections appear under Member. Select any VPN connections that you want to remove from the VPN concentrator, and click the left arrow button to remove them.
OK	Click OK to save your changes in the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

21.5 Zyxel Device IPSec VPN Client Configuration Provisioning

Use the Configuration > VPN > IPSec VPN > Configuration Provisioning screen to configure who can retrieve VPN rule settings from the Zyxel Device using the Zyxel Device IPSec VPN Client. In the Zyxel Device IPSec VPN Client, you just need to enter the IP address of the Zyxel Device to get all the VPN rule settings automatically. You do not need to manually configure all rule settings in 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

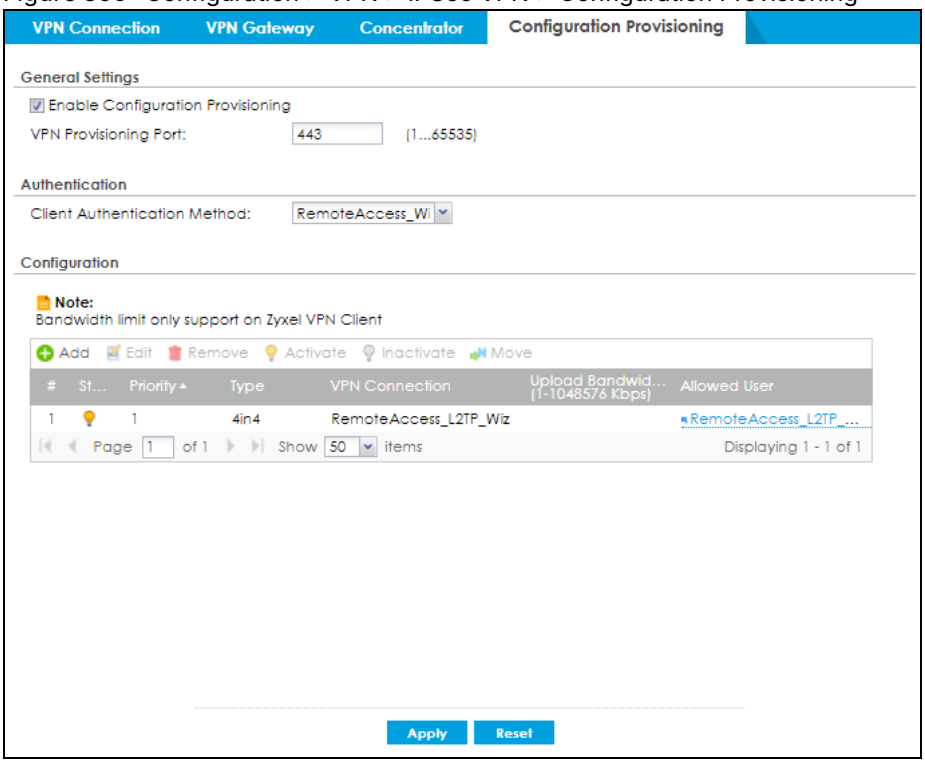
The following VPN Gateway rules configured on the Zyxel Device cannot be provisioned to the IPSec VPN Client:

- IPv4 rules with IKEv2 version
- IPv4 rules with User-based PSK authentication

Note: You must enable IPv6 in System > IPv6 to activate IPv6 VPN tunneling rules.

In the Zyxel Device Quick Setup wizard, you can use the VPN Settings for Configuration Provisioning wizard to create a VPN rule that will not violate these restrictions.

Figure 355 Configuration > VPN > IPSec VPN > Configuration Provisioning



Each field is discussed in the following table.

Table 144 Configuration > VPN > IPSec VPN > Configuration Provisioning

LABEL	DESCRIPTION
Enable Configuration Provisioning	Select this for users to be able to retrieve VPN rule settings using the Zyxel Device IPSec VPN client.
VPN Provisioning Port	Change the default port that IPSec VPN clients use to retrieve VPN rule settings from the Zyxel Device. The default is 443 which is already in use for remote management by default. If you change the default IPSec VPN port on the Zyxel Device, make sure to make the same change to the Zyxel IPSec VPN client. See Section 26.3.2 on page 576 for more information. Configure a new port between 1024 to 65535 that is not in use by other services.
Client Authentication Method	Choose how users should be authenticated. They can be authenticated using the local database on the Zyxel Device or an external authentication database such as LDAP, Active Directory or RADIUS. default is a method you configured in Object > Auth Method. You may configure multiple methods there. If you choose the local database on the Zyxel Device, then configure users using the Object > User/Group screen. If you choose LDAP, Active Directory or RADIUS authentication servers, then configure users on the respective server.
Configuration	When you add or edit a configuration provisioning entry, you are allowed to set the VPN Connection and Allowed User fields. Duplicate entries are not allowed. You cannot select the same VPN Connection and Allowed User pair in a new entry if the same pair exists in a previous entry. You can bind different rules to the same user, but the Zyxel Device will only allow VPN rule setting retrieval for the first match found.

Table 144 Configuration > VPN > IPSec VPN > Configuration Provisioning (continued)

LABEL	DESCRIPTION
Add	Click Add to bind a configured VPN rule to a user or group. Only that user or group may then retrieve the specified VPN rule settings. If you click Add without selecting an entry in advance then the new entry appears as the first entry. Entry order is important as the Zyxel Device searches entries in the order listed here to find a match. After a match is found, the Zyxel Device stops searching. If you want to add an entry as number three for example, then first select entry 2 and click Add. To reorder an entry, use Move.
Edit	Select an existing entry and click Edit to change its settings.
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. Make sure that Enable Configuration Provisioning is also selected.
Inactivate	To turn off an entry, select it and click Inactivate.
Move	Use Move to reorder a selected entry. Select an entry, click Move, type the number where the entry should be moved, press <ENTER>, then click Apply.
Status	This icon shows if the entry is active (yellow) or not (gray). VPN rule settings can only be retrieved when the entry is activated (and Enable Configuration Provisioning is also selected).
Priority	Priority shows the order of the entry in the list. Entry order is important as the Zyxel Device searches entries in the order listed here to find a match. After a match is found the Zyxel Device stops searching.
VPN Connection	This field shows all configured VPN rules that match the rule criteria for the Zyxel Device IPSec VPN client. Select a rule to bind to the associated user or group.
Upload Bandwidth Limit	Upload Bandwidth Limit is only available for Zyxel subscription-based SecuExtender IPSec VPN clients. Windows VPN clients support Zyxel SecuExtender versions 5.6.80.007 or later. macOS VPN clients support Zyxel SecuExtender versions 1.2.0.7 or later. Use Upload Bandwidth Limit to set the maximum bandwidth for uploading traffic from Zyxel IPSec VPN clients over IPSec VPN tunnels.
Allowed User	Select which user or group of users is allowed to retrieve the associated VPN rule settings using the Zyxel Device IPSec VPN client. A user may belong to a number of groups. If entries are configured for different groups, the Zyxel Device will allow VPN rule setting retrieval based on the first match found. Users of type admin or limited-admin are not allowed.
Type	This field shows how traffic is tunneled from the Zyxel Device to the Zyxel VPN client: • 6in4 (tunnel IPv6 traffic from the Zyxel Device to the Zyxel client in an IPv4 network); • 4in6 (tunnel IPv4 traffic from the Zyxel Device to the Zyxel VPN client in an IPv6 network); • 4in4 (tunnel IPv4 traffic from the Zyxel Device to the Zyxel VPN client in an IPv4 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.

21.6 Example: IPSec VPN with IKEv2 on a Mobile Phone

This section shows you how to connect your mobile phone to the Zyxel Device using IPSec VPN with and a pre-shared key.

21.6.1 Configuration on Android

This example uses Android software version 13.

1 Go to Settings, search for “VPN”, open the VPN settings screen, and then tap Add.

2 Enter a name for the VPN rule in the Name field.

3 Select IKEv2 as Type.

4 Enter the WAN IP address your Zyxel Device is currently using in the Server address field.

5 Enter the IPSec identifier. By default, it is 0.0.0.0.

6 Enter the pre-shared key in the IPSec pre-shared key field. You can find the pre-shared key on the VPN Gateway screen in the Web Configurator.

7 Tap Save to create the VPN rule.

8 Select the VPN rule you created and tap Connect.

9 To check the connection status, go to Configuration > VPN > IPSec VPN in the Web Configurator.

21.6.2 Configuration on iOS

This example uses iOS software version 17.

1 Go to Settings, search for “VPN”, open the VPN & Device Management screen, and then tap Add VPN Configuration.

2 Select IKEv2 as Type.

3 Enter a name for the VPN rule in the Name field.

4 Enter the WAN IP address your Zyxel Device is currently using in the Server field.

5 Enter the Remote ID. By default, it is 0.0.0.0.

6 Select None as User Authentication.

7 Disable Use Certificate.

8 Enter the pre-shared key in the Password field. You can find the pre-shared key on the VPN Gateway screen in the Web Configurator.

9 Tap Done to create the VPN rule.

10 Select the VPN rule you created and tap Connect.

11 To check the connection status, go to Configuration > VPN > IPSec VPN in the Web Configurator.

21.7 IPSec VPN Background Information

Here is some more detailed IPSec VPN background information.

IKE SA Overview

The IKE SA provides a secure connection between the Zyxel Device and remote IPSec router.

It takes several steps to establish an IKE SA. The negotiation mode determines how many. There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Note: Both routers must use the same negotiation mode.

These modes are discussed in more detail in Negotiation Mode. Main mode is used in various examples in the rest of this section.

The Zyxel Device supports IKEv1 and IKEv2. See Section 21.1 on page 473 for more information.

IP Addresses of the Zyxel Device and Remote IPSec Router

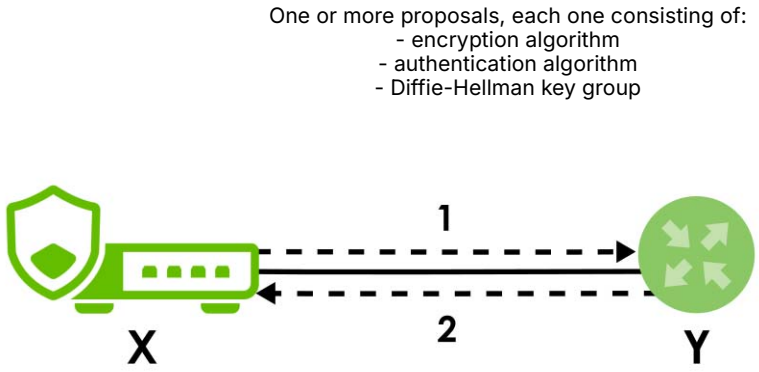
To set up an IKE SA, you have to specify the IP addresses of the Zyxel Device and remote IPSec router. You can usually enter a static IP address or a domain name for either or both IP addresses. Sometimes, your Zyxel Device might offer another alternative, such as using the IP address of a port or interface,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

You can also specify the IP address of the remote IPSec router as 0.0.0.0. This means that the remote IPSec router can have any IP address. In this case, only the remote IPSec router can initiate an IKE SA because the Zyxel Device does not know the IP address of the remote IPSec router. This is often used for telecommuters.

IKE SA Proposal

The IKE SA proposal is used to identify the encryption algorithm, authentication algorithm, and Diffie-Hellman (DH) key group that the Zyxel Device and remote IPSec router use in the IKE SA. In main mode, this is done in steps 1 and 2, as illustrated next.

Figure 356 IKE SA: Main Negotiation Mode, Steps 1 - 2: IKE SA Proposal



The Zyxel Device sends one or more proposals to the remote IPSec router. (In some devices, you can only set up one proposal.) Each proposal consists of an encryption algorithm, authentication algorithm, and DH key group that the Zyxel Device wants to use in the IKE SA. The remote IPSec router selects an acceptable proposal and sends the accepted proposal back to the Zyxel Device. If the remote IPSec router rejects all of the proposals, the Zyxel Device and remote IPSec router cannot establish an IKE SA.

Note: Both routers must use the same encryption algorithm, authentication algorithm, and DH key group.

In most Zyxel Devices, you can select one of the following encryption algorithms for each proposal. The algorithms are listed in order from weakest to strongest.

- Data Encryption Standard (DES) is a widely used method of data encryption. It applies a 56-bit key to each 64-bit block of data.
- Triple DES (3DES) is a variant of DES. It iterates three times with three separate keys, effectively tripling the strength of DES.
- Advanced Encryption Standard (AES) is a newer method of data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data. It is faster than 3DES.

Some Zyxel Devices also offer stronger forms of AES that apply 192-bit or 256-bit keys to 128-bit blocks of data.

In most Zyxel Devices, you can select one of the following authentication algorithms for each proposal. The algorithms are listed in order from weakest to strongest.

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

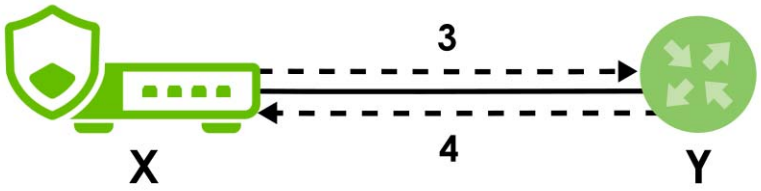
See Diffie-Hellman (DH) Key Exchange on page 502 for more information about DH key groups.

Diffie-Hellman (DH) Key Exchange

The Zyxel Device and the remote IPSec router use DH public-key cryptography to establish a shared secret. The shared secret is then used to generate encryption keys for the IKE SA and IPSec SA. In main mode, this is done in steps 3 and 4, as illustrated next.

Figure 357 IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange

Diffie-Hellman key exchange



DH public-key cryptography is based on DH key groups. Each key group is a fixed number of bits long. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. For example, DH2 keys (1024 bits) are more secure than DH1 keys (768 bits), but DH2 keys take longer to encrypt and decrypt.

Note: Ensure both The Zyxel Device and the remote IPSec router use the same DH key group.

The available DHx options on the Zyxel Device are:

- DH1 - uses a 768-bit random number to create an encryption key.
- DH2 - uses a 1024-bit random number to create an encryption key.
- DH5 - uses a 1536-bit random number to create an encryption key.
- DH14 - uses a 2048-bit random number to create an encryption key.
- DH15 - uses a 3072-bit random number to create an encryption key.
- DH16 - uses a 4096-bit random number to create an encryption key.
- DH17 - uses a 6144-bit random number to create an encryption key.
- DH18 - uses a 8192-bit random number to create an encryption key.
- DH19 - uses a 256-bit elliptic curve to create an encryption key, offering stronger security than the random number-based method.
- DH20 - uses a 384-bit elliptic curve to create an encryption key, offering stronger security than the random number-based method.
- DH21 - uses a 521-bit elliptic curve to create an encryption key, offering stronger security than the random number-based method.

Elliptic Curve Diffie-Hellman provides a higher level of protection using elliptic curve mathematical principles (recommeded).

Different operating systems may support different DH key groups. Check your operating system documentation.

- For Windows VPN clients, Zyxel SecuExtender perpetual VPN clients versions 3.8.203.61.32 and earlier support DH1 to DH14.
- For macOS VPN clients, Zyxel SecuExtender subscription VPN clients versions 1.2.0.7 and later support DH14 to DH21. For Windows VPN clients, Zyxel SecuExtender subscription VPN clients versions 5.6.80.007 and later support DH14 to DH21.
- Windows versions 7, 10, 11 built-in IKEv2 VPN clients support DH2 by default.
- macOS versions 14.2 and later built-in IKEv2 VPN clients support DH14 by default.
- iOS versions 10.15 and later built-in IKEv2 VPN clients support DH14 by default.

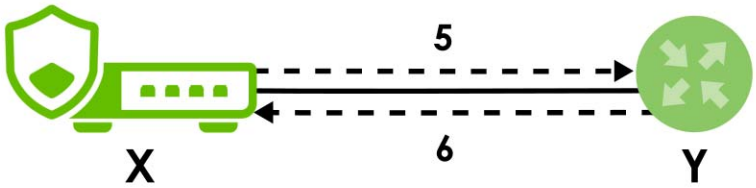
Authentication

Before the Zyxel Device and remote IPSec router establish an IKE SA, they have to verify each other’s identity. This process is based on pre-shared keys and router identities.

In main mode, the Zyxel Device and remote IPSec router authenticate each other in steps 5 and 6, as illustrated below. The identities are also encrypted using the encryption algorithm and encryption key the Zyxel Device and remote IPSec router selected in previous steps.

Figure 358 IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication (continued)

Step 5:
pre-shared key
Zyxel Device identity, consisting of
- ID type
- content
Step 6:
pre-shared key
Remote IPSec router identity, consisting of
- ID type
- content



You have to create (and distribute) a pre-shared key. The Zyxel Device and remote IPSec router use it in the authentication process, though it is not actually transmitted or exchanged.

Note: The Zyxel Device and the remote IPSec router must use the same pre-shared key.

Router identity consists of ID type and content. The ID type can be domain name, IP address, or email address, and the content is a (properly-formatted) domain name, IP address, or email address. The content is only used for identification. Any domain name or email address that you enter does not have to actually exist. Similarly, any domain name or IP address that you enter does not have to correspond to the Zyxel Device's or remote IPSec router's properties.

The Zyxel Device and the remote IPSec router have their own identities, so both of them must store two sets of information, one for themselves and one for the other router. Local ID type and content refers to the ID type and content that applies to the router itself, and peer ID type and content refers to the ID type and content that applies to the other router.

Note: The Zyxel Device's local and peer ID type and content must match the remote IPSec router's peer and local ID type and content, respectively.

For example, in the next table, the Zyxel Device and the remote IPSec router authenticate each other successfully. In contrast, in the following table, the Zyxel Device and the remote IPSec router cannot authenticate each other and, therefore, cannot establish an IKE SA.

Table 145 VPN Example: Matching ID Type and Content

ZYXEL DEVICE	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

Table 146 VPN Example: Mismatching ID Type and Content

ZYXEL DEVICE	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.20	Peer ID content: tom@yourcompany.com

It is also possible to configure the Zyxel Device to ignore the identity of the remote IPSec router. In this case, you usually set the peer ID type to Any. This is less secure, so you should only use this if your Zyxel Device provides another way to check the identity of the remote IPSec router (for example, extended authentication) or if you are troubleshooting a VPN tunnel.

Additional Topics for IKE SA

This section provides more information about IKE SA.

Negotiation Mode

There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Main mode takes six steps to establish an IKE SA.

Steps 1 - 2: The Zyxel Device sends its proposals to the remote IPSec router. The remote IPSec router selects an acceptable proposal and sends it back to the Zyxel Device.

Steps 3 - 4: The Zyxel Device and the remote IPSec router exchange pre-shared keys for authentication and participate in a Diffie-Hellman key exchange, based on the accepted DH key group, to establish a shared secret.

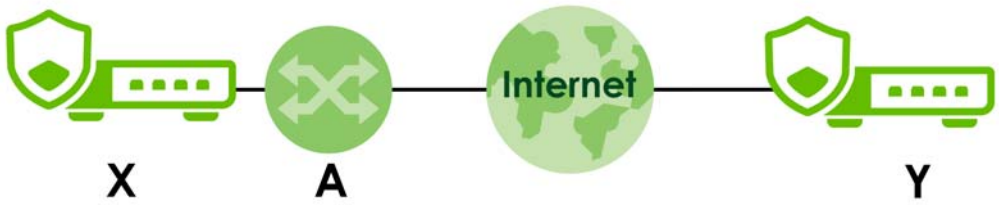
Steps 5 - 6: Finally, the Zyxel Device and the remote IPSec router generate an encryption key (from the shared secret), encrypt their identities, and exchange their encrypted identity information for authentication.

In contrast, aggressive mode only takes three steps to establish an IKE SA. Aggressive mode does not provide as much security because the identity of the Zyxel Device and the identity of the remote IPSec router are not encrypted. It is usually used in remote-access situations, where the address of the initiator is not known by the responder and both parties want to use pre-shared keys for authentication. For example, the remote IPSec router may be a telecommuter who does not have a static IP address.

VPN, NAT, and NAT Traversal

In the following example, there is another router (A) between router X and router Y.

Figure 359 VPN/NAT Example



If router A does NAT, it might change the IP addresses, port numbers, or both. If router X and router Y try to establish a VPN tunnel, the authentication fails because it depends on this information. The routers cannot establish a VPN tunnel.

Most routers like router A now have an IPSec pass-thru feature. This feature helps router A recognize VPN packets and route them appropriately. If router A has this feature, router X and router Y can establish a VPN tunnel as long as the active protocol is ESP. (See Active Protocol on page 507 for more information about active protocols.)

If router A does not have an IPSec pass-thru or if the active protocol is AH, you can solve this problem by enabling NAT traversal. In NAT traversal, router X and router Y add an extra header to the IKE SA and IPSec SA packets. If you configure router A to forward these packets unchanged, router X and router Y can establish a VPN tunnel.

You have to do the following things to set up NAT traversal.

- Enable NAT traversal on the Zyxel Device and remote IPSec router.
- Configure the NAT router to forward packets with the extra header unchanged. (See the field description for detailed information about the extra header.)

The extra header may be UDP port 500 or UDP port 4500, depending on the standard(s) the Zyxel Device and remote IPSec router support.

X-Auth / Extended Authentication

X-Auth / Extended authentication is often used when multiple IPSec routers use the same VPN tunnel to connect to a single IPSec router. For example, this might be used with telecommuters.

In extended authentication, one of the routers (the Zyxel Device or the remote IPSec router) provides a user name and password to the other router, which uses a local user database and/or an external server to verify the user name and password. If the user name or password is wrong, the routers do not establish an IKE SA.

You can set up the Zyxel Device to provide a user name and password to the remote IPSec router, or you can set up the Zyxel Device to check a user name and password that is provided by the remote IPSec router.

If you use extended authentication, it takes four more steps to establish an IKE SA. These steps occur at the end, regardless of the negotiation mode (steps 7-10 in main mode, steps 4-7 in aggressive mode).

Certificates

It is possible for the Zyxel Device and remote IPSec router to authenticate each other with certificates. In this case, you do not have to set up the pre-shared key, local identity, or remote identity because the certificates provide this information instead.

- Instead of using the pre-shared key, the Zyxel Device and remote IPSec router check the signatures on each other's certificates. Unlike pre-shared keys, the signatures do not have to match.
- The local and peer ID type and content come from the certificates.

Note: You must set up the certificates for the Zyxel Device and remote IPSec router first.

IPSec SA Overview

Once the Zyxel Device and remote IPSec router have established the IKE SA, they can securely negotiate an IPSec SA through which to send data between computers on the networks.

Note: The IPSec SA stays connected even if the underlying IKE SA is not available anymore.

This section introduces the key components of an IPSec SA.

Local Network and Remote Network

In an IPSec SA, the local network, the one(s) connected to the Zyxel Device, may be called the local policy. Similarly, the remote network, the one(s) connected to the remote IPSec router, may be called the remote policy.

Active Protocol

The active protocol controls the format of each packet. It also specifies how much of each packet is protected by the encryption and authentication algorithms. IPSec VPN includes two active protocols, AH (Authentication Header, RFC 2402) and ESP (Encapsulating Security Payload, RFC 2406).

Note: The Zyxel Device and remote IPSec router must use the same active protocol.

Usually, you should select ESP. AH does not support encryption, and ESP is more suitable with NAT.

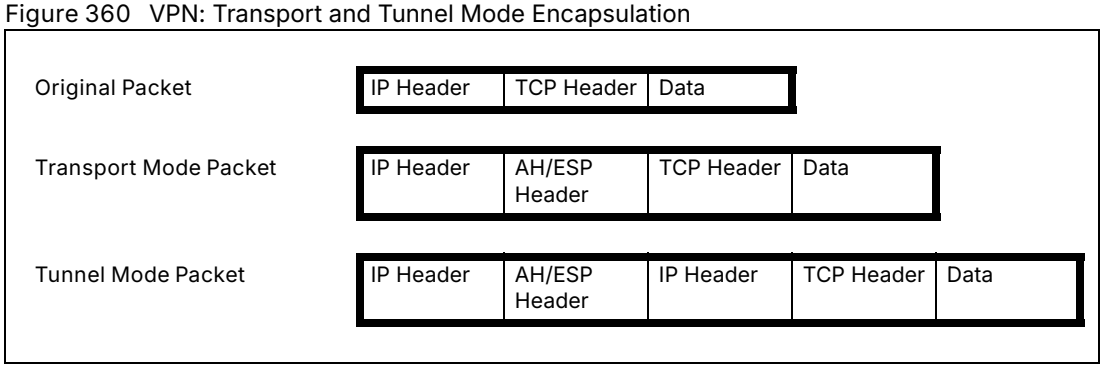
Encapsulation

There are two ways to encapsulate packets. Usually, you should use tunnel mode because it is more secure. Transport mode is only used when the IPSec SA is used for communication between the Zyxel Device and remote IPSec router (for example, for remote management), not between computers on the local and remote networks.

Note: The Zyxel Device and remote IPSec router must use the same encapsulation.

These modes are illustrated below.

Figure 360 VPN: Transport and Tunnel Mode Encapsulation



In tunnel mode, the Zyxel Device uses the active protocol to encapsulate the entire IP packet. As a result, there are two IP headers:

- Outside header: The outside IP header contains the IP address of the Zyxel Device or remote IPSec router, whichever is the destination.
- Inside header: The inside IP header contains the IP address of the computer behind the Zyxel Device or remote IPSec router. The header for the active protocol (AH or ESP) appears between the IP headers.

In transport mode, the encapsulation depends on the active protocol. With AH, the Zyxel Device includes part of the original IP header when it encapsulates the packet. With ESP, however, the Zyxel Device does not include the IP header when it encapsulates the packet, so it is not possible to verify the integrity of the source IP address.

IPSec SA Proposal and Perfect Forward Secrecy

An IPSec SA proposal is similar to an IKE SA proposal (see IKE SA Proposal), except that you also have the choice whether or not the Zyxel Device and remote IPSec router perform a new DH key exchange every time an IPSec SA is established. This is called Perfect Forward Secrecy (PFS).

If you enable PFS, the Zyxel Device and remote IPSec router perform a DH key exchange every time an IPSec SA is established, changing the root key from which encryption keys are generated. As a result, if one encryption key is compromised, other encryption keys remain secure.

If you do not enable PFS, the Zyxel Device and remote IPSec router use the same root key that was generated when the IKE SA was established to generate encryption keys.

The DH key exchange is time-consuming and may be unnecessary for data that does not require such security.

PFS is ignored in initial IKEv2 authentication but is used when re-authenticating.

Additional Topics for IPSec SA

This section provides more information about IPSec SA in your Zyxel Device.

Authentication and the Security Parameter Index (SPI)

For authentication, the Zyxel Device and remote IPSec router use the SPI, instead of pre-shared keys, ID type and content. The SPI is an identification number.

Note: The Zyxel Device and remote IPSec router must use the same SPI.

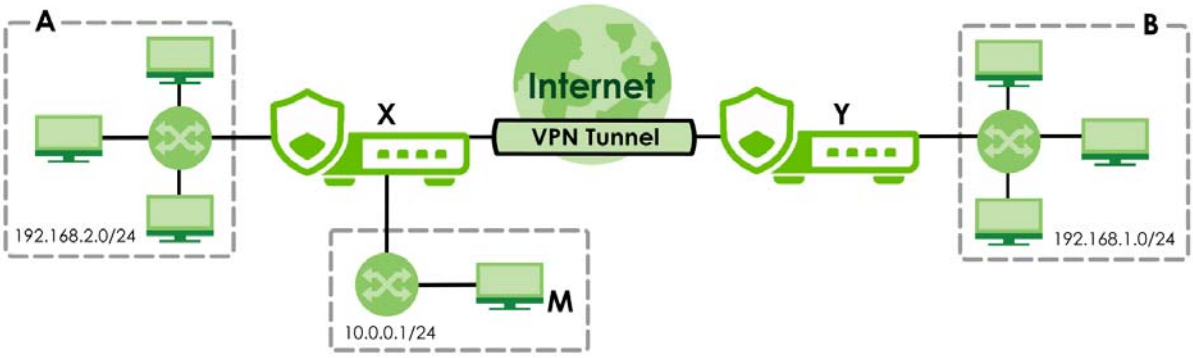
NAT for Inbound and Outbound Traffic

The Zyxel Device can translate the following types of network addresses in IPSec SA.

- Source address in outbound packets - this translation is necessary if you want the Zyxel Device to route packets from computers outside the local network through the IPSec SA.
- Source address in inbound packets - this translation hides the source address of computers in the remote network.
- Destination address in inbound packets - this translation is used if you want to forward packets (for example, mail) from the remote network to a specific computer (like the mail server) in the local network.

Each kind of translation is explained below. The following example is used to help explain each one.

Figure 361 VPN Example: NAT for Inbound and Outbound Traffic



Source Address in Outbound Packets (Outbound Traffic, Source NAT)

This translation lets the Zyxel Device route packets from computers that are not part of the specified local network (local policy) through the IPSec SA. For example, in Figure 361 on page 508, you have to configure this kind of translation if you want computer M to establish a connection with any computer in the remote network (B). If you do not configure it, the remote IPSec router may not route messages for computer M through the IPSec SA because computer M's IP address is not part of its local policy.

To set up this NAT, you have to specify the following information:

- Source - the original source address; most likely, computer M's network.
- Destination - the original destination address; the remote network (B).
- SNAT - the translated source address; the local network (A).

Source Address in Inbound Packets (Inbound Traffic, Source NAT)

You can set up this translation if you want to change the source address of computers in the remote network. To set up this NAT, you have to specify the following information:

- Source - the original source address; the remote network (B).
- Destination - the original destination address; the local network (A).
- SNAT - the translated source address; a different IP address (range of addresses) to hide the original source address.

Destination Address in Inbound Packets (Inbound Traffic, Destination NAT)

You can set up this translation if you want the Zyxel Device to forward some packets from the remote network to a specific computer in the local network. For example, in Figure 361 on page 508, you can configure this kind of translation if you want to forward mail from the remote network to the mail server in the local network (A).

You have to specify one or more rules when you set up this kind of NAT. The Zyxel Device checks these rules similar to the way it checks rules for a security policy. The first part of these rules define the conditions in which the rule apply.

- Original IP - the original destination address; the remote network (B).
- Protocol - the protocol [TCP, UDP, or both] used by the service requesting the connection.
- Original Port - the original destination port or range of destination ports; in Figure 361 on page 508, it might be port 25 for SMTP.

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

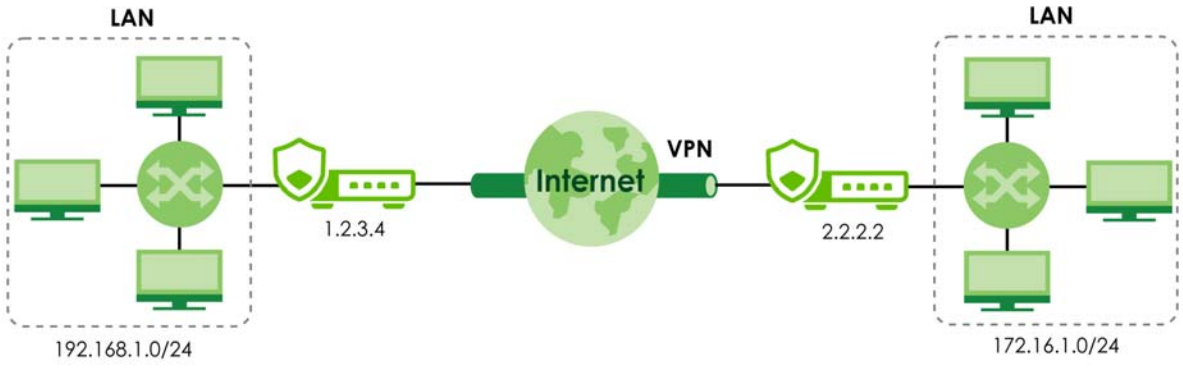
- Mapped IP - the translated destination address; in Figure 361 on page 508, the IP address of the mail server in the local network (A).
- Mapped Port - the translated destination port or range of destination ports.

The original port range and the mapped port range must be the same size.

IPSec VPN Example Scenario

Here is an example site-to-site IPSec VPN scenario.

Figure 362 Site-to-site IPSec VPN Example



CHAPTER 22
SSL VPN

22.1 Overview

Use SSL VPN to allow users to use a web browser for secure remote user login. The remote users do not need a VPN router or VPN client software.

22.1.1 What You Can Do in this Chapter

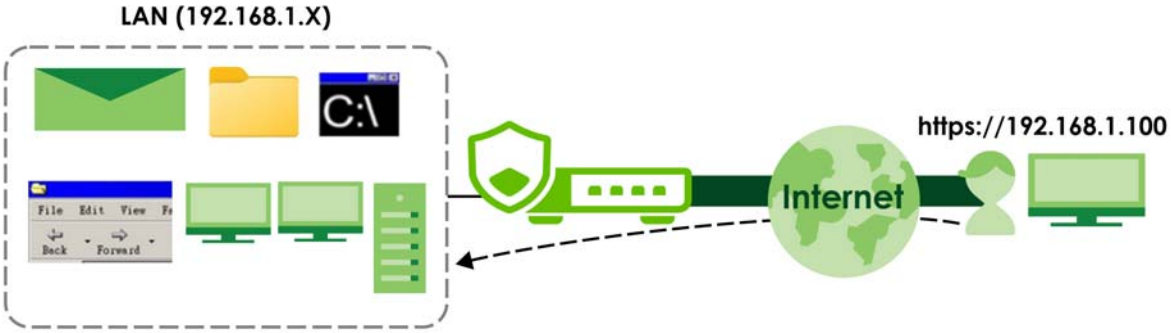
- Use the VPN > SSL VPN > Access Privilege screens (see Section 22.2 on page 512) to configure SSL access policies.
- Use the Click VPN > SSL VPN > Global Setting screen (see Section 22.3 on page 516) to set the IP address of the Zyxel Device (or a gateway device) on your network for full tunnel mode access, enter access messages or upload a custom logo to be displayed on the remote user screen.

22.1.2 What You Need to Know

Full Tunnel Mode

In full tunnel mode, a virtual connection is created for remote users with private IP addresses in the same subnet as the local network. This allows them to access network resources in the same way as if they were part of the internal network.

Figure 363 Network Access Mode: Full Tunnel Mode



SSL Access Policy

An SSL access policy allows the Zyxel Device to perform the following tasks:

- limit user access to specific applications or file sharing server on the network.
- allow user access to specific networks.
- assign private IP addresses and provide DNS/WINS server information to remote users to access internal networks.

SSL Access Policy Objects

The SSL access policies reference the following objects. If you update this information, in response to changes, the Zyxel Device automatically propagates the changes through the SSL policies that use the object(s). When you delete an SSL policy, the objects are not removed.

Table 147 Objects

OBJECT TYPE	OBJECT SCREEN	DESCRIPTION
User Accounts	User Account/ User Group	Configure a user account or user group to which you want to apply this SSL access policy.
Application	SSL Application	Configure an SSL application object to specify the type of application and the address of the local computer, server, or web site SSL users are to be able to access.
IP Pool	Address	Configure an address object that defines a range of private IP addresses to assign to user computers so they can access the internal network through a VPN connection.
Server Addresses	Address	Configure address objects for the IP addresses of the DNS and WINS servers that the Zyxel Device sends to the VPN connection users.
VPN Network	Address	Configure an address object to specify which network segment users are allowed to access through a VPN connection.

You cannot delete an object that is referenced by an SSL access policy. To delete the object, you must first unassociate the object from the SSL access policy.

Multiple WAN Connections

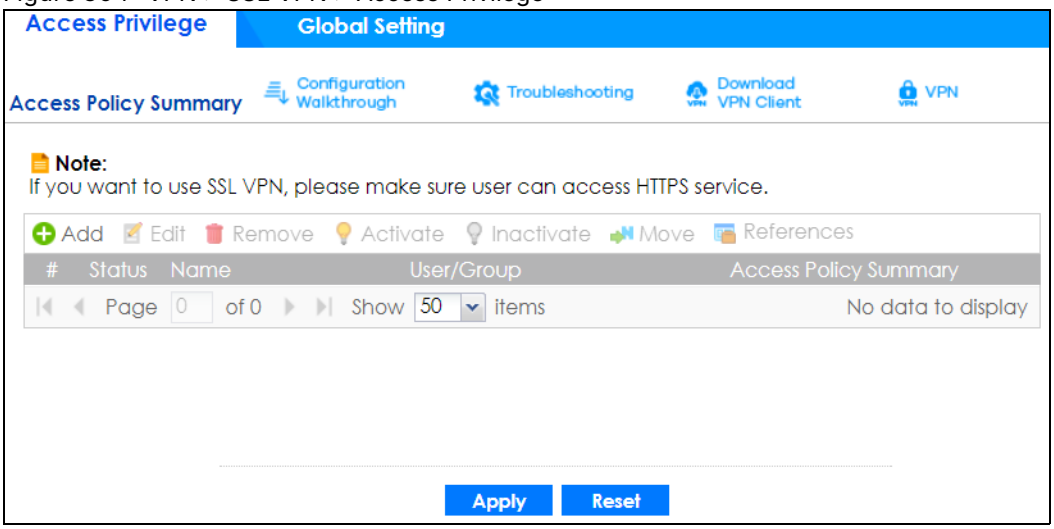
You can connect VPN for different ports (wan1, wan2) after you enable SSL VPN.

22.2 The SSL Access Privilege Screen

Click VPN > SSL VPN to open the Access Privilege screen. This screen lists the configured SSL access policies.

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

Figure 364 VPN > SSL VPN > Access Privilege



The following table describes the labels in this screen.

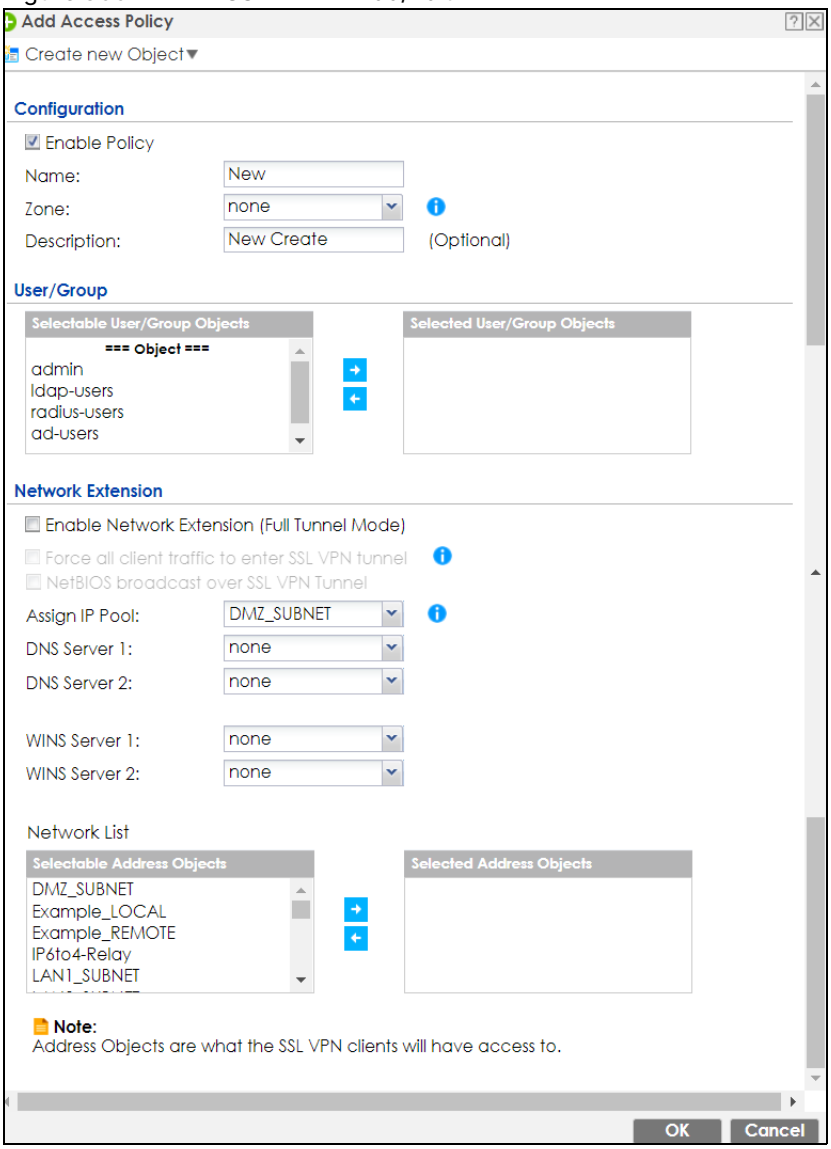
Table 148 VPN > SSL VPN > Access Privilege

LABEL	DESCRIPTION
Access Policy Summary	This screen shows a summary of SSL VPN policies created. Click on the VPN icon to go to the Zyxel VPN Client product page at the Zyxel website.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The 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.
Move	To move an entry to a different number in the list, click the Move icon. In the field that appears, specify the number to which you want to move the interface.
References	Select an entry and click References to open a screen that shows which settings use the entry. Click Refresh to update information on this screen.
#	This field displays the index number of the entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the descriptive name of the SSL access policy for identification purposes.
User/Group	This field displays the user account or user group name(s) associated to an SSL access policy. This field displays up to three names.
Access Policy Summary	This field displays details about the SSL application object this policy uses including its name, type, and address.
Apply	Click Apply to save the settings.
Reset	Click Reset to discard all changes.

22.2.1 The SSL Access Privilege Policy Add/Edit Screen

To create a new or edit an existing SSL access policy, click the Add or Edit icon in the Access Privilege screen.

Figure 365 VPN > SSL VPN > Add/Edit



The following table describes the labels in this screen.

Table 149 VPN > SSL VPN > Access Privilege > Add/Edit

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Configuration	
Enable Policy	Select this option to activate this SSL access policy.
Name	Enter a descriptive name to identify this policy. You can enter up to 31 characters (“a-z”, A-Z”, “0-9”) with no spaces allowed.

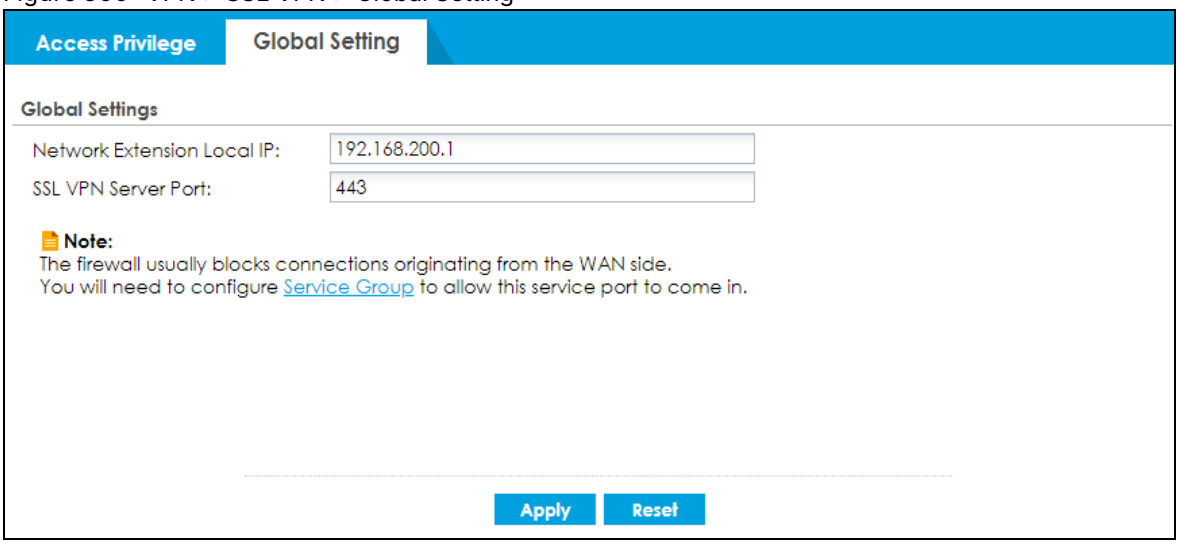
Table 149 VPN > SSL VPN > Access Privilege > Add/Edit (continued)

LABEL	DESCRIPTION
Zone	Select the zone to which to add this SSL access policy. You use zones to apply security settings such as security policy and remote management.
Description	Enter additional information about this SSL access policy. You can enter up to 60 characters ("0-9", "a-z", "A-Z", "-" and "_").
User/Group	The Selectable User/Group Objects list displays the name(s) of the user account and/or user group(s) to which you have not applied an SSL access policy yet. To associate a user or user group to this SSL access policy, select a user account or user group and click the right arrow button to add to the Selected User/Group Objects list. You can select more than one name. To remove a user or user group, select the name(s) in the Selected User/Group Objects list and click the left arrow button. Note: Although you can select admin and limited-admin accounts in this screen, they are reserved for device configuration only. You cannot use them to access the SSL VPN portal.
Network Extension (Optional)	
Enable Network Extension	Select this option to create a VPN tunnel between the authenticated users and the internal network. This allows the users to access the resources on the network as if they were on the same local network. This includes access to resources not supported by SSL application objects. For example this lets users Telnet to the internal network even though the Zyxel Device does not have SSL application objects for Telnet. Clear this option to disable this feature. Users can only access the applications as defined by the VPN tunnel's selected SSL application settings and the remote user computers are not made to be a part of the local network.
Force all client traffic to SSL VPN tunnel	Select this to send all traffic from the SSL VPN clients through the SSL VPN tunnel. This replaces the default gateway of the SSL VPN clients with the SSL VPN gateway.
NetBIOS broadcast over SSL VPN Tunnel	Select this to search for a remote computer and access its applications as if it was in a Local Area Network. The user can find a computer not only by its IP address but also by computer name.
Assign IP Pool	Define a separate pool of IP addresses to assign to the SSL users. Select it here. The SSL VPN IP pool should not overlap with IP addresses on the Zyxel Device's local networks (LAN and DMZ for example), the SSL user's network, or the networks you specify in the SSL VPN Network List.
DNS/WINS Server 1..2	Select the name of the DNS or WINS server whose information the Zyxel Device sends to the remote users. This allows them to access devices on the local network using domain names instead of IP addresses.
Network List	To allow user access to local network(s), select a network name in the Selectable Address Objects list and click the right arrow button to add to the Selected Address Objects list. You can select more than one network. To block access to a network, select the network name in the Selected Address Objects list and click the left arrow button.
OK	Click OK to save the changes and return to the main Access Privilege screen.
Cancel	Click Cancel to discard all changes and return to the main Access Privilege screen.

22.3 The SSL Global Setting Screen

Click VPN > SSL VPN and click the Global Setting tab to display the following screen. Use this screen to set the IP address of the Zyxel Device (or a gateway device) on your network for full tunnel mode access.

Figure 366 VPN > SSL VPN > Global Setting



The following table describes the labels in this screen.

Table 150 VPN > SSL VPN > Global Setting

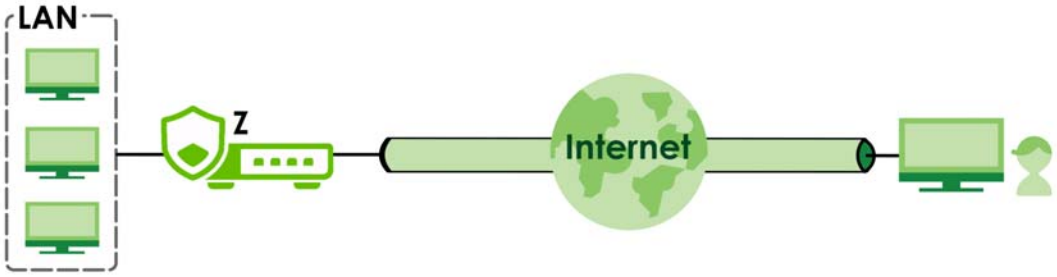
LABEL	DESCRIPTION
Global Setting	
Network Extension Local IP	Specify the IP address of the Zyxel Device (or a gateway device) for full tunnel mode SSL VPN access. Leave this field to the default settings unless it conflicts with another interface.
SSL VPN Server Port	Specify the SSL VPN server port of the Zyxel Device for full tunnel mode SLL VPN access. Leave this field to default settings unless it conflicts with another interface.
Apply	Click Apply to save the changes and/or start the logo file upload process.
Reset	Click Reset to return the screen to its last-saved settings.

CHAPTER 23
L2TP VPN

23.1 Overview

L2TP VPN uses the L2TP and IPSec client software included in remote users' Android, iOS, Windows or Mac OS X operating systems for secure connections to the network behind the Zyxel Device. The remote users do not need their own IPSec gateways or third-party VPN client software.

Figure 367 L2TP VPN Overview



23.1.1 What You Can Do in this Chapter

- Use the L2TP VPN screen (see Section 23.2 on page 518) to configure the Zyxel Device's L2TP VPN settings.
- Use the VPN Setup Wizard screen in Quick Setup (Chapter 6 on page 158) to configure the Zyxel Device's L2TP VPN settings.

23.1.2 What You Need to Know

The Layer 2 Tunneling Protocol (L2TP) works at layer 2 (the data link layer) to tunnel network traffic between two peers over another network (like the Internet). In L2TP VPN, an IPSec VPN tunnel is established first and then an L2TP tunnel is built inside it. See Chapter 21 on page 473 for information on IPSec VPN.

IPSec Configuration Required for L2TP VPN

You must configure an IPSec VPN connection prior to proper L2TP VPN usage(see Chapter 23 on page 517 for details). The IPSec VPN connection must meet the following requirements:

- VPN Connection is enabled.
- VPN Gateway is enabled.
- Set VPN Connection > VPN Gateway to Remote Access (Server Role).
- Set VPN Connection > Encapsulation to Transport mode.
- Configuration Payload is disabled in the VPN Gateway settings.
- X-Auth is disabled in the VPN Gateway settings.

- VPN Gateway authentication method is using Pre-Shared Key.

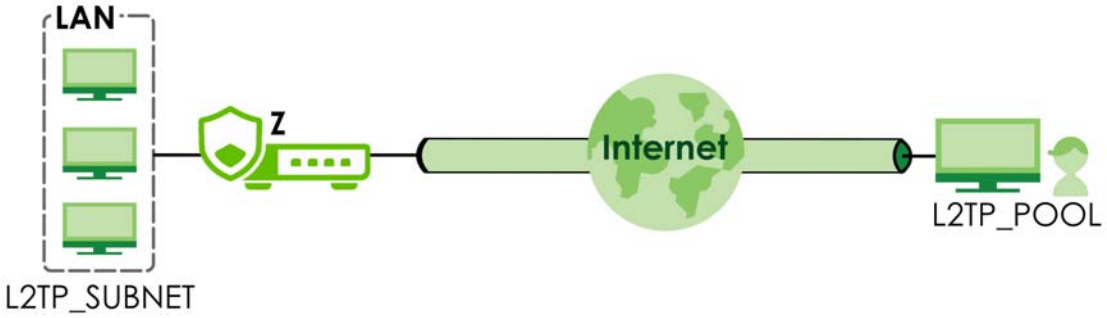
Using the Quick Setup VPN Setup Wizard

The VPN Setup Wizard is an easy and convenient way to configure the L2TP VPN settings. Click Configuration > Quick Setup > VPN Setup > VPN Settings for L2TP VPN Settings to get started.

Policy Route

The Policy Route for return traffic (from LAN to L2TP clients) is automatically created when Zyxel Device adds a new L2TP connection, allowing users access the resources on a network without additional configuration. However, if some of the traffic from the L2TP clients needs to go to the Internet, you will need to create a policy route to send that traffic from the L2TP tunnels out through a WAN trunk. This task can be easily performed by clicking the Allow L2TP traffic through WAN checkbox at Quick Setup > VPN Setup > Allow L2TP traffic through WAN.

Figure 368 Policy Route for L2TP VPN



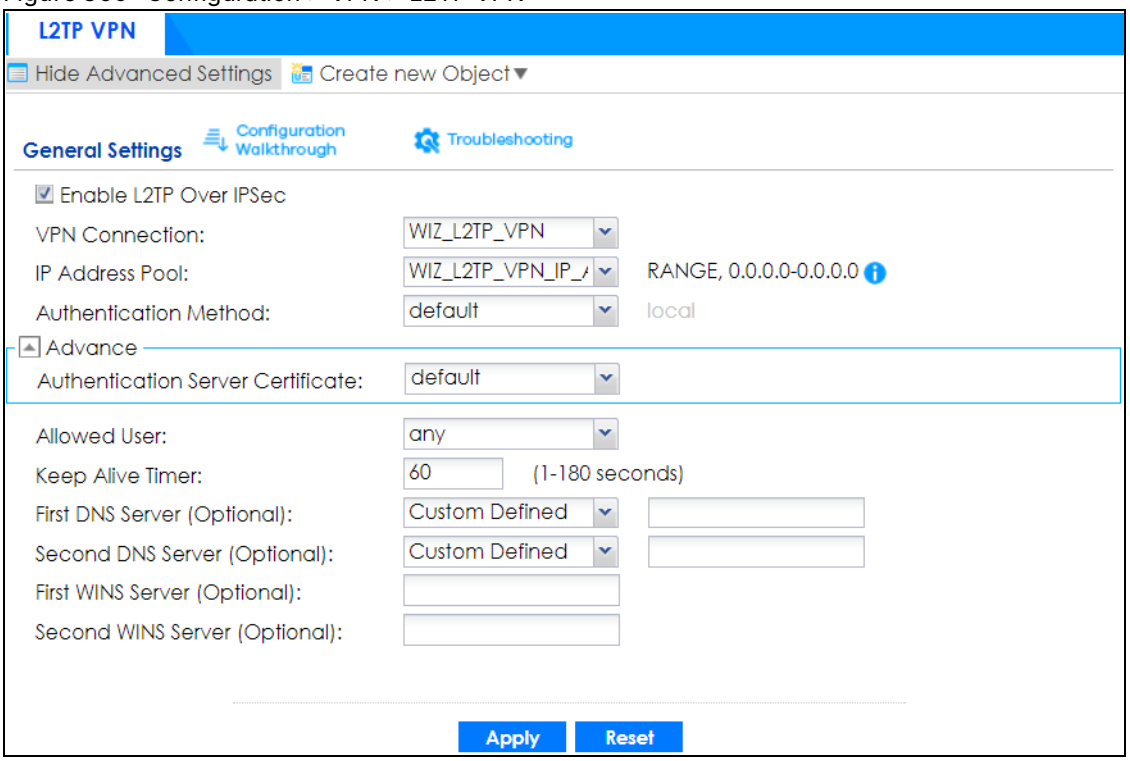
23.2 L2TP VPN Screen

Click Configuration > VPN > L2TP VPN to open the following screen. Use this screen to configure the Zyxel Device's L2TP VPN settings.

Note: Disconnect any existing L2TP VPN sessions before modifying L2TP VPN settings. The remote users must make any needed matching configuration changes and re-establish the sessions using the new settings.

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

Figure 369 Configuration > VPN > L2TP VPN



The following table describes the fields in this screen.

Table 151 Configuration > VPN > L2TP VPN

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable L2TP Over IPSec	Use this field to turn the Zyxel Device's L2TP VPN function on or off.
VPN Connection	Select the IPSec VPN connection the Zyxel Device uses for L2TP VPN. Only the configured VPN connections in Configuration > VPN > IPSec VPN > VPN Connection that meet the following requirements are displayed here. • Remote Access (Server Role) • Use transport mode • Configuration Payload is disabled • X-Auth is disabled Your VPN settings must also meet the requirements listed in IPSec Configuration Required for L2TP VPN. Note: Selecting a different VPN connection (or modifying the VPN gateway that it uses) disconnects any existing L2TP VPN sessions.
IP Address Pool	Select the pool of IP addresses that the Zyxel Device uses to assign to the L2TP VPN clients. Use Create new Object if you need to configure a new pool of IP addresses. This should not conflict with any WAN, LAN, DMZ or WLAN subnet even if they are not in use.

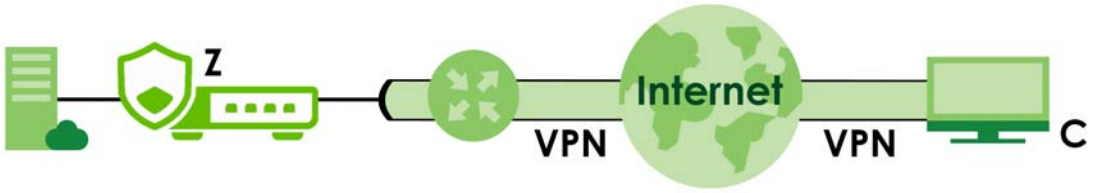
Table 151 Configuration > VPN > L2TP VPN (continued)

LABEL	DESCRIPTION
Authentication Method	Select how the Zyxel Device authenticates a remote user before allowing access to the L2TP VPN tunnel. The authentication method has the Zyxel Device check a user's user name and password against the Zyxel Device's local database, a remote LDAP, RADIUS, a Active Directory server, or more than one of these.
Authentication Server Certificate	Select the certificate to use to identify the Zyxel Device for L2TP VPN connections. You must have certificates already configured in the My Certificates screen. The certificate is used with the EAP, PEAP, and MSCHAPv2 authentication protocols.
Allowed User	The remote user must log into the Zyxel Device to use the L2TP VPN tunnel. Select a user or user group that can use the L2TP VPN tunnel. Use Create new Object if you need to configure a new user account. Otherwise, select any to allow any user with a valid account and password on the Zyxel Device to log in.
Keep Alive Timer	The Zyxel Device sends a Hello message after waiting this long without receiving any traffic from the remote user. The Zyxel Device disconnects the VPN tunnel if the remote user does not respond.
First DNS Server, Second DNS Server	Specify the IP addresses of DNS servers to assign to the remote users. You can specify these IP addresses two ways. Custom Defined - enter a static IP address. From ISP - use the IP address of a DNS server that another interface received from its DHCP server.
First WINS Server, Second WINS Server	The WINS (Windows Internet Naming Service) server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. Type the IP addresses of up to two WINS servers to assign to the remote users. You can specify these IP addresses two ways.
Apply	Click Apply to save your changes in the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

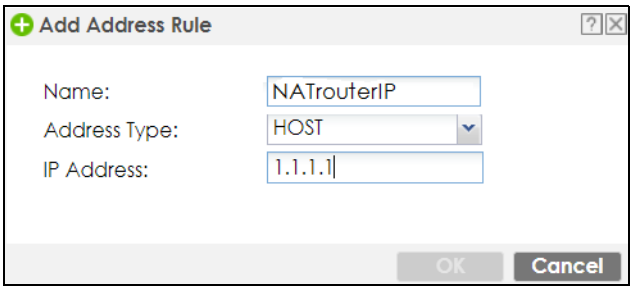
23.2.1 Example: L2TP and Zyxel Device Behind a NAT Router

If the Zyxel Device (Z) is behind a NAT router (N), then do the following for remote clients (C) to access the network behind the Zyxel Device (Z) using L2TP over IPv4.

Figure 370 L2TP and Zyxel Device Behind a NAT Router



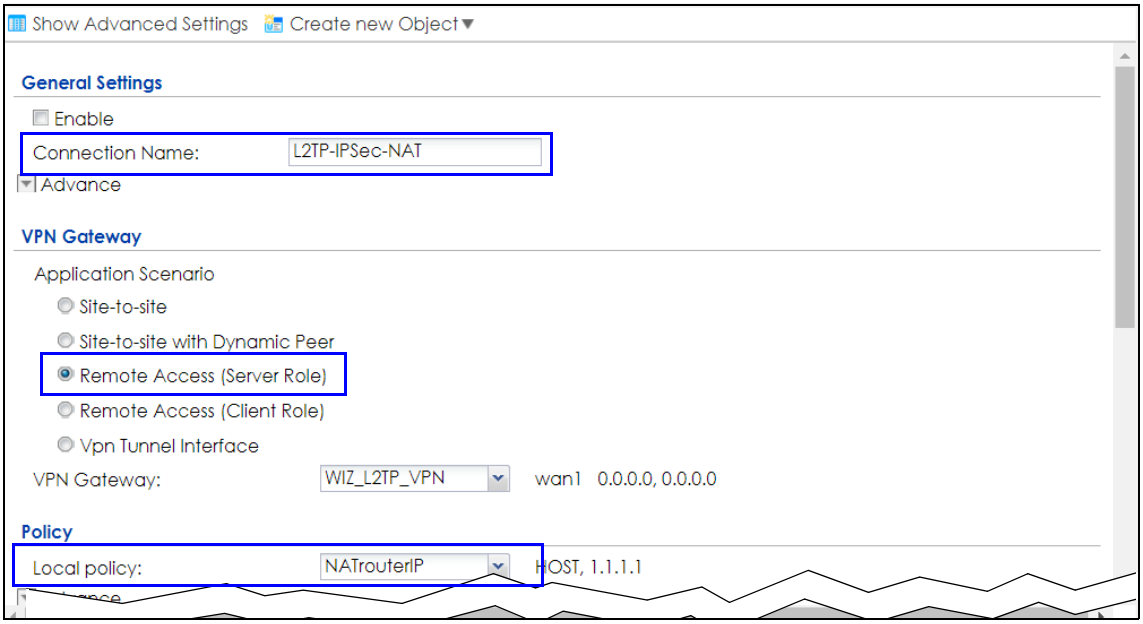
1 Create an address object in Configuration > Object > Address/GEO IP > Address for the WAN IP address of the NAT router.



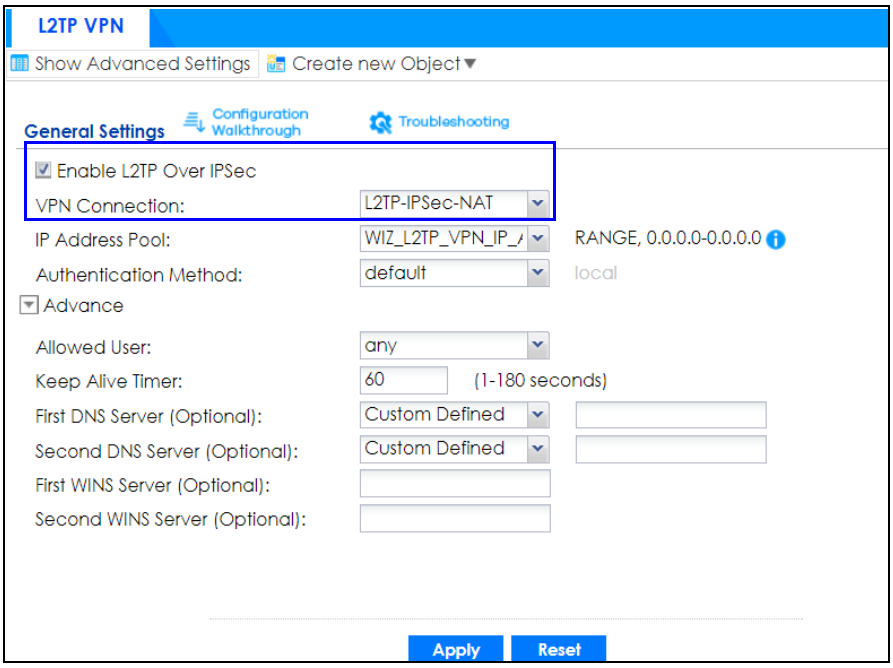
2 Go to Configuration > VPN > IPSec VPN > VPN Connection and click Add for IPv4 Configuration to create a new VPN connection.

3 Select Remote Access (Server Role) as the VPN scenario for the remote client.

4 Select the NAT router WAN IP address object as the Local Policy.



5 Go to Configuration > VPN > L2TP VPN and select the VPN Connection just configured.


L2TP VPN
Show Advanced Settings
Create new Object
General Settings
Configuration Walkthrough
Troubleshooting
Enable L2TP Over IPSec
VPN Connection:
L2TP-IPSec-NAT
IP Address Pool:
WIZ_L2TP_VPN_IP_
RANGE, 0.0.0.0-0.0.0.0
Authentication Method:
default
local
Advance
Allowed User:
any
Keep Alive Timer:
60
(1-180 seconds)
First DNS Server (Optional):
Custom Defined
Second DNS Server (Optional):
Custom Defined
First WINS Server (Optional):
Second WINS Server (Optional):
Apply
Reset

CHAPTER 24
BWM (Bandwidth Management)

24.1 Overview

Bandwidth management provides a convenient way to manage the use of various services on the network. It manages general protocols (for example, HTTP and FTP) and applies traffic prioritization to enhance the performance of delay-sensitive applications like voice and video.

24.1.1 What You Can Do in this Chapter

Use the BWM screens (see Section 24.2 on page 527) to control bandwidth for services passing through the Zyxel Device, and to identify the conditions that define the bandwidth control.

24.1.2 What You Need to Know

When you allow a service, you can restrict the bandwidth it uses. It controls TCP and UDP traffic. Use policy routes to manage other types of traffic (like ICMP).

Note: Bandwidth management in policy routes has priority over TCP and UDP traffic policies.

If you want to use a service, make sure both the security policy allow the service's packets to go through the Zyxel Device.

Note: The Zyxel Device checks security policies before it checks bandwidth management rules for traffic going through the Zyxel Device.

Bandwidth management examines every TCP and UDP connection passing through the Zyxel Device. Then, you can specify, by port, whether or not the Zyxel Device continues to route the connection.

BWM Type

The Zyxel Device supports three types of bandwidth management: Shared, Per user and Per-Source-IP.

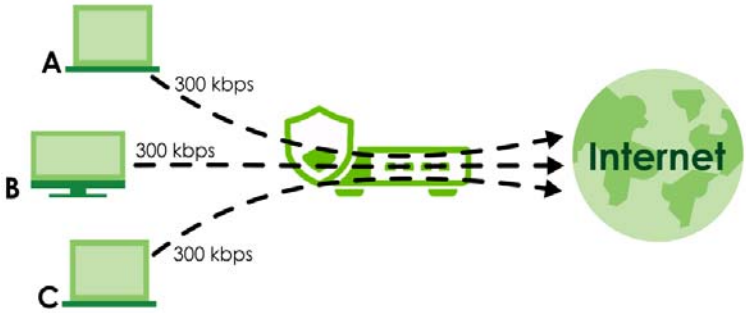
The Shared BWM type is selected by default in a bandwidth management rule. All matched traffic shares the bandwidth configured in the rule.

If the BWM type is set to Per user in a rule, each user that matches the rule can use up to the configured bandwidth by his/her own.

Select the Per-Source-IP type when you want to set the maximum bandwidth for traffic from an individual source IP address.

In the following example, you configure a Per user bandwidth management rule for radius-users to limit outgoing traffic to 300 kbs. Then all radius-users (A, B and C) can send 300 kbps of traffic.

Figure 371 Bandwidth Management Per User Type



DiffServ and DSCP Marking

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

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

Connection and Packet Directions

Bandwidth management looks at the connection direction, that is, from which interface the connection was initiated and to which interface the connection is going.

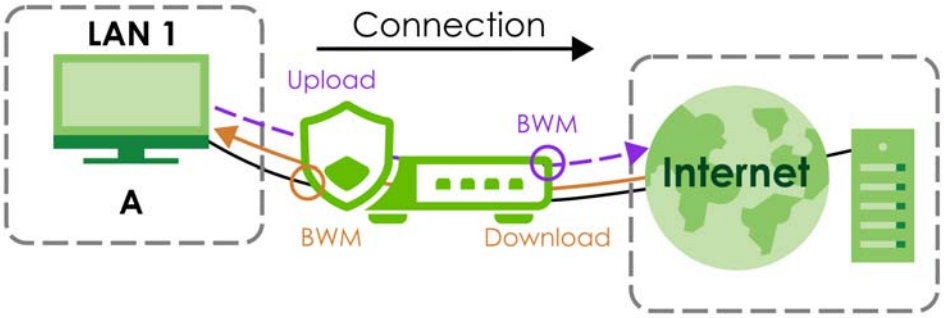
A connection has outbound and inbound packet flows. The Zyxel Device controls the bandwidth of traffic of each flow as it is going out through an interface or VPN tunnel.

- The outbound traffic flows from the connection initiator to the connection responder.
- The inbound traffic flows from the connection responder to the connection initiator.

For example, a LAN1 to WAN connection is initiated from LAN1 and goes to the WAN.

- Outbound traffic goes from a LAN1 device to a WAN device. Bandwidth management is applied before sending the packets out a WAN interface on the Zyxel Device.
- Inbound traffic comes back from the WAN device to the LAN1 device. Bandwidth management is applied before sending the traffic out a LAN1 interface.

Figure 372 LAN1 to WAN Connection and Packet Directions

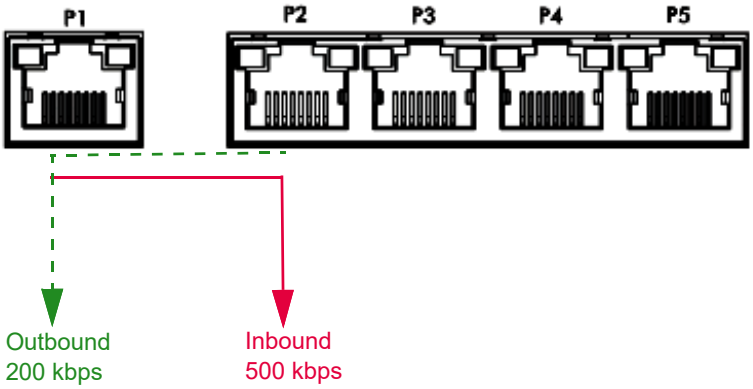


Outbound and Inbound Bandwidth Limits

You can limit an application's outbound or inbound bandwidth. This limit keeps the traffic from using up too much of the out-going interface's bandwidth. This way you can make sure there is bandwidth for other applications. When you apply a bandwidth limit to outbound or inbound traffic, each member of the out-going zone can send up to the limit. Take a LAN1 to WAN policy for example.

- Outbound traffic is limited to 200 kbps. The connection initiator is on the LAN1 so outbound means the traffic traveling from the LAN1 to the WAN. Each of the WAN zone's two interfaces can send the limit of 200 kbps of traffic.
- Inbound traffic is limited to 500 kbs. The connection initiator is on the LAN1 so inbound means the traffic traveling from the WAN to the LAN1.

Figure 373 LAN1 to WAN, Outbound 200 kbps, Inbound 500 kbps



Bandwidth Management Priority

- The Zyxel Device gives bandwidth to higher-priority traffic first, until it reaches its configured bandwidth rate.
- Then lower-priority traffic gets bandwidth.
- The Zyxel Device uses a fairness-based (round-robin) scheduler to divide bandwidth among traffic flows with the same priority.
- The Zyxel Device automatically treats traffic with bandwidth management disabled as priority 7 (the lowest priority).

Maximize Bandwidth Usage

Maximize bandwidth usage allows applications with maximize bandwidth usage enabled to “borrow” any unused bandwidth on the out-going interface.

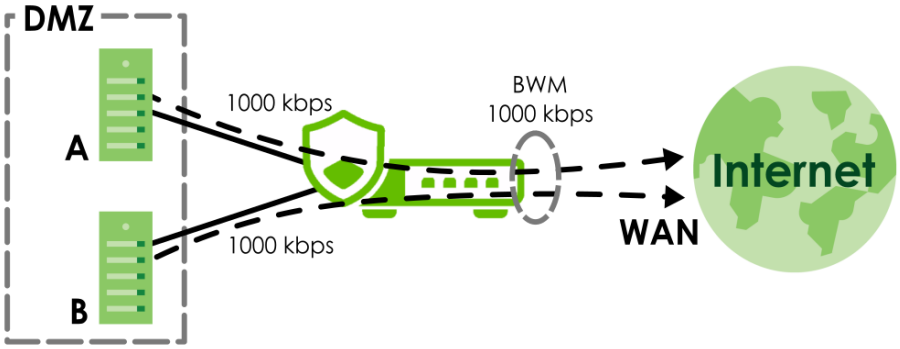
After each application gets its configured bandwidth rate, the Zyxel Device uses the fairness- based scheduler to divide any unused bandwidth on the out-going interface amongst applications that need more bandwidth and have maximize bandwidth usage enabled.

Unused bandwidth is divided equally. Higher priority traffic does not get a larger portion of the unused bandwidth.

Bandwidth Management Behavior

The following sections show how bandwidth management behaves with various settings. For example, you configure DMZ to WAN policies for FTP servers A and B. Each server tries to send 1000 kbps, but the WAN is set to a maximum outgoing speed of 1000 kbps. You configure policy A for server A’s traffic and policy B for server B’s traffic.

Figure 374 Bandwidth Management Behavior



Configured Rate Effect

In the following table the configured rates total less than the available bandwidth and maximize bandwidth usage is disabled, both servers get their configured rate.

Table 152 Configured Rate Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	300 kbps	No	1	300 kbps
B	200 kbps	No	1	200 kbps

Priority Effect

Here the configured rates total more than the available bandwidth. Because server A has higher priority, it gets up to it’s configured rate (800 kbps), leaving only 200 kbps for server B.

Table 153 Priority Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	800 kbps	Yes	1	800 kbps
B	1000 kbps	Yes	2	200 kbps

Maximize Bandwidth Usage Effect

With maximize bandwidth usage enabled, after each server gets its configured rate, the rest of the available bandwidth is divided equally between the two. So server A gets its configured rate of 300 kbps and server B gets its configured rate of 200 kbps. Then the Zyxel Device divides the remaining bandwidth (1000 - 500 = 500) equally between the two (500 / 2 = 250 kbps for each). The priority has no effect on how much of the unused bandwidth each server gets.

So server A gets its configured rate of 300 kbps plus 250 kbps for a total of 550 kbps. Server B gets its configured rate of 200 kbps plus 250 kbps for a total of 450 kbps.

Table 154 Maximize Bandwidth Usage Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	300 kbps	Yes	1	550 kbps
B	200 kbps	Yes	2	450 kbps

Priority and Over Allotment of Bandwidth Effect

Server A has a configured rate that equals the total amount of available bandwidth and a higher priority. You should regard extreme over allotment of traffic with different priorities (as shown here) as a configuration error. Even though the Zyxel Device still attempts to let all traffic get through and not be lost, regardless of its priority, server B gets almost no bandwidth with this configuration.

Table 155 Priority and Over Allotment of Bandwidth Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	1000 kbps	Yes	1	999 kbps
B	1000 kbps	Yes	2	1 kbps

Limit the Bandwidth for a Specific VLAN

If you want to limit the bandwidth for a specific VLAN, set the VLAN as the incoming interface and VPN as the outgoing interface. Then, set the bandwidth limit for this BWM rule.

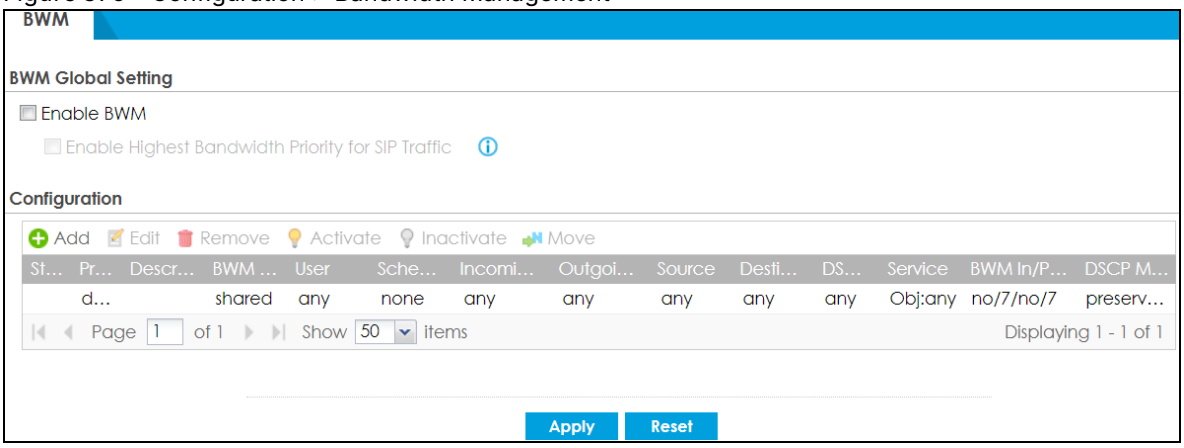
24.2 The Bandwidth Management Configuration

The Bandwidth management screens control the bandwidth allocation for TCP and UDP traffic. You can use source interface, destination interface, destination port, schedule, user, source, destination information, DSCP code and service type as criteria to create a sequence of specific conditions, similar to the sequence of rules used by firewalls, to specify how the Zyxel Device handles the DSCP value and allocate bandwidth for the matching packets.

Click Configuration > BWM to open the following screen. This screen allows you to enable/disable bandwidth management and add, edit, and remove user-defined bandwidth management policies.

The default bandwidth management policy is the one with the priority of “default”. It is the last policy the Zyxel Device checks if traffic does not match any other bandwidth management policies you have configured. You cannot remove, activate, deactivate or move the default bandwidth management policy.

Figure 375 Configuration > Bandwidth Management



The following table describes the labels in this screen. See Section 24.2.1 on page 530 for more information as well.

Table 156 Configuration > Bandwidth Management

LABEL	DESCRIPTION
Enable BWM	Select this checkbox to activate management bandwidth.
Enable Highest Bandwidth Priority for SIP Traffic	Select this to maximize the throughput of SIP traffic to improve SIP-based VoIP call sound quality. This has the Zyxel Device immediately send SIP traffic upon identifying it.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Move	To change an entry's position in the numbered list, select it and click Move to display a field to type a number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The status icon is not available for the default bandwidth management policy.
Priority	This field displays a sequential value for each bandwidth management policy and it is not associated with a specific setting. This field displays default for the default bandwidth management policy.
Description	This field displays additional information about this policy.
BWM Type	This field displays the below types of BWM: • Shared, when the policy is set for all matched traffic • Per User, when the policy is set for an individual user or a user group • Per-Source-IP, when the policy is set for a source IP
User	This is the type of user account to which the policy applies. If any displays, the policy applies to all user accounts.
Schedule	This is the schedule that defines when the policy applies. none means the policy always applies.
Incoming Interface	This is the source interface of the traffic to which this policy applies.
Outgoing Interface	This is the destination interface of the traffic to which this policy applies.

Table 156 Configuration > Bandwidth Management

LABEL	DESCRIPTION
Source	This is the source address or address group, including geographic address and FQDN (group) objects, for whom this policy applies. If any displays, the policy is effective for every source.
Destination	This is the destination address or address group, including geographic address and FQDN (group) objects, for whom this policy applies. If any displays, the policy is effective for every destination.
DSCP Code	These are the DSCP code point values of incoming and outgoing packets to which this policy applies. The lower the number the higher the priority with the exception of 0 which is usually given only best-effort treatment. any means all DSCP value or no DSCP marker. default means traffic with a DSCP value of 0. This is usually best effort traffic The “af” options stand for Assured Forwarding. The number following the “af” identifies one of four classes and one of three drop preferences.
Service	App and the service name displays if you selected Application Object for the service type. An Application Object is a pre-defined service. Obj and the service name displays if you selected Service Object for the service type. A Service Object is a customized pre-defined service or another service. Mouse over the service object name to view the corresponding IP protocol number.
BWM In/Pri/Out/Pri	This field shows the inbound/outbound bandwidth and traffic priority. In - This is how much inbound bandwidth, in kilobits per second, this policy allows the matching traffic to use. Inbound refers to the traffic that the Zyxel Device sends to a connection’s initiator. If no displays here, this policy does not apply bandwidth management for the inbound traffic. Out - This is how much outbound bandwidth, in kilobits per second, this policy allows the matching traffic to use. Outbound refers to the traffic the Zyxel Device sends out from a connection’s initiator. If no displays here, this policy does not apply bandwidth management for the outbound traffic. Pri - This is the priority for the inbound (the first Pri value) or outbound (the second Pri value) traffic that matches this policy. The smaller the number, the higher the priority. Traffic with a higher priority is given bandwidth before traffic with a lower priority. If the inbound or outbound limit is set to 0, the traffic is assigned to the lowest priority (7) regardless of this field’s configuration.
DSCP Marking	This is how the Zyxel Device handles the DSCP value of the incoming and outgoing packets that match this policy. In - Inbound, the traffic the Zyxel Device sends to a connection’s initiator. Out - Outbound, the traffic the Zyxel Device sends out from a connection’s initiator. If this field displays a DSCP value, the Zyxel Device applies that DSCP value to the route’s outgoing packets. preserve means the Zyxel Device does not modify the DSCP value of the route’s outgoing packets. default means the Zyxel Device sets the DSCP value of the route’s outgoing packets to 0. The “af” choices stand for Assured Forwarding. The number following the “af” identifies one of four classes and one of three drop preferences.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

24.2.1 The Bandwidth Management Add/Edit Screen

The Configuration > Bandwidth Management Add/Edit screen allows you to create a new condition or edit an existing one.

802.1P Marking

Use 802.1P to prioritize outgoing traffic from a VLAN interface. The Priority Code is a 3-bit field within a 802.1Q VLAN tag that's used to prioritize associated outgoing VLAN traffic. "0" is the lowest priority level and "7" is the highest.

Table 157 Single Tagged 802.1Q Frame Format

			DA	SA	TPID	Priority	VID	Len/Etype	Data	FCS	IEEE 802.1Q customer tagged frame

Table 158 802.1Q Frame

DA	Destination Address	Priority	802.1p Priority
SA	Source Address	Len/Etype	Length and type of Ethernet frame
TPID	Tag Protocol IDentifier	Data	Frame data
VID	VLAN ID	FCS	Frame Check Sequence

The following table is a guide to types of traffic for the priority code.

Table 159 Priority Code and Types of Traffic

PRIORITY	TRAFFIC TYPES
0 (lowest)	Background
1	Best Effort
2	Excellent Effort
3	Critical Applications
4	Video, less than 100 ms latency and jitter
5	Voice, less than 10 ms latency and jitter
6	Internetwork Control
7 (highest)	Network Control

To access this screen, go to the Configuration > Bandwidth Management screen (see Section 24.2 on page 527), and click either the Add icon or an Edit icon.

Figure 376 Configuration > Bandwidth Management > Edit (For the Default Policy)

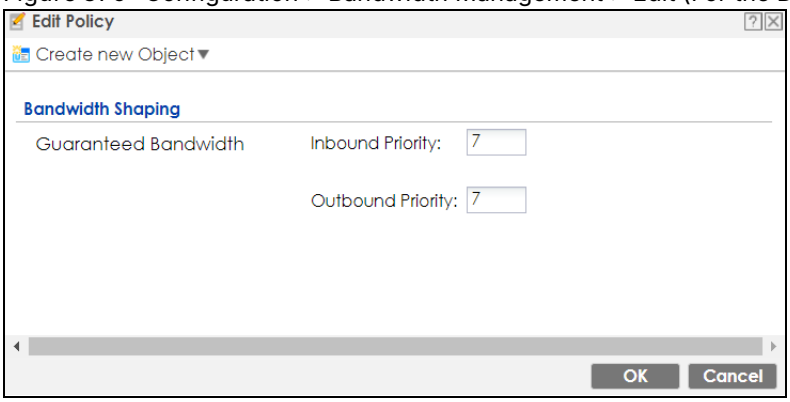
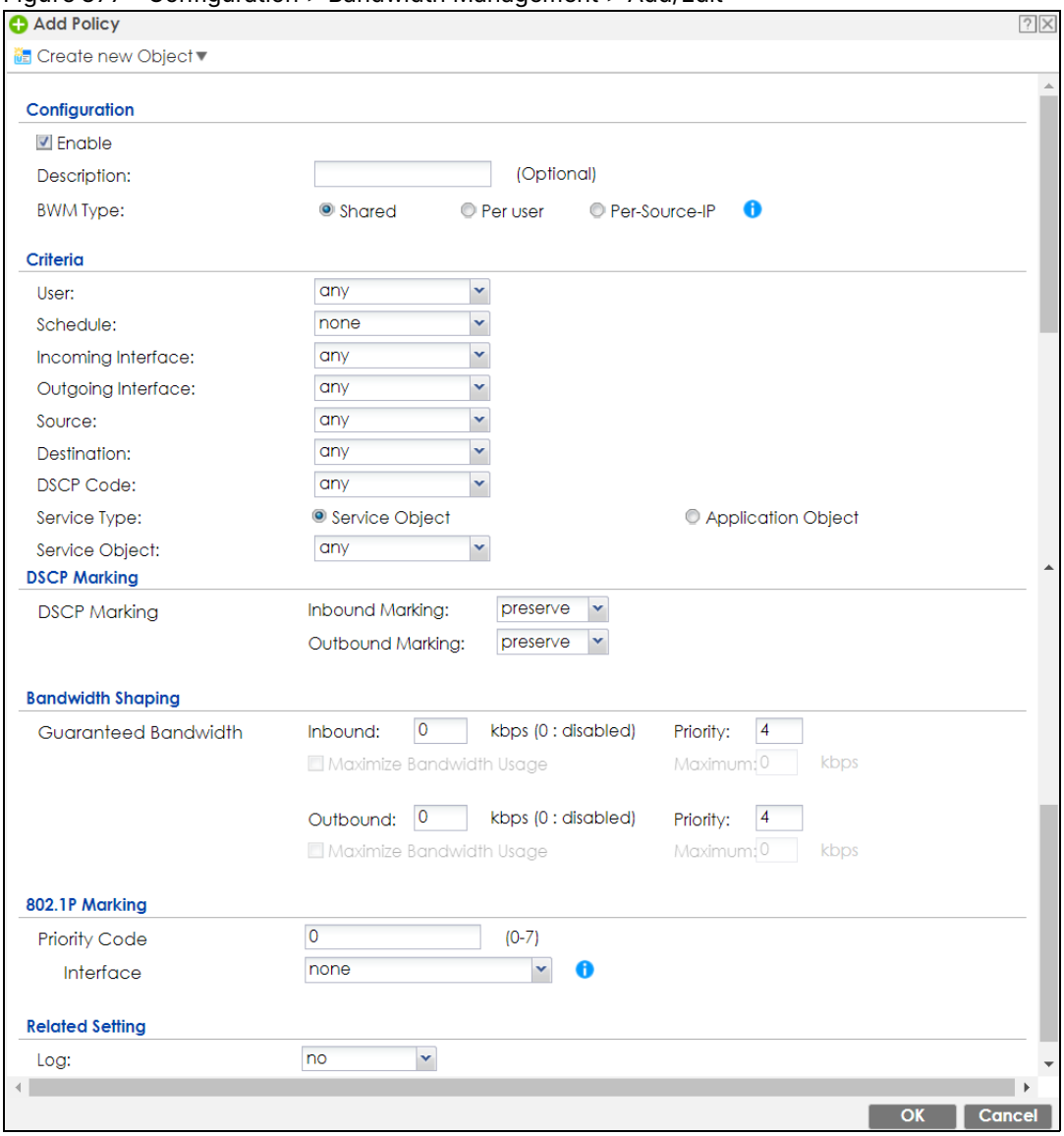


Figure 377 Configuration > Bandwidth Management > Add/Edit



The following table describes the labels in this screen.

Table 160 Configuration > Bandwidth Management > Add/Edit

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Configuration	
Enable	Select this checkbox to turn on this policy.
Description	Enter a description of this policy. It is not used elsewhere. You can use alphanumeric and ()+/:+?!*#@$_%- characters, and it can be up to 60 characters long.
Criteria	Use this section to configure the conditions of traffic to which this policy applies.
BWM Type	This field displays the below types of BWM rule: • Shared, when the policy is set for all users • Per User, when the policy is set for an individual user or a user group • Per Source IP, when the policy is set for a source IP
User	Select a user name or user group to which to apply the policy. Use Create new Object if you need to configure a new user account. Select any to apply the policy for every user.
Schedule	Select a schedule that defines when the policy applies or select Create Object to configure a new one. Otherwise, select none to make the policy always effective.
Incoming Interface	Select the source interface of the traffic to which this policy applies.
Outgoing Interface	Select the destination interface of the traffic to which this policy applies.
Source	Select a source address or address group, including geographic address and FQDN (group) objects, for whom this policy applies. Use Create new Object if you need to configure a new one. Select any if the policy is effective for every source.
Destination	Select a destination address or address group, including geographic address and FQDN (group) objects, for whom this policy applies. Use Create new Object if you need to configure a new one. Select any if the policy is effective for every destination.
DSCP Code	Select a DSCP code point value of incoming packets to which this policy route applies or select User Defined to specify another DSCP code point. The lower the number the higher the priority with the exception of 0 which is usually given only best-effort treatment. any means all DSCP value or no DSCP marker. default means traffic with a DSCP value of 0. This is usually best effort traffic The “af” choices stand for Assured Forwarding. The number following the “af” identifies one of four classes and one of three drop preferences.
User-Defined DSCP Code	Use this field to specify a custom DSCP code point.
Service Type	Select Service Object or Application Object if you want a specific service (defined in a service object) to which the policy applies.
Service Object	This field is available if you selected Service Object as the service type. Select a service or service group to identify the type of traffic to which this policy applies. any means all services.

Table 160 Configuration > Bandwidth Management > Add/Edit

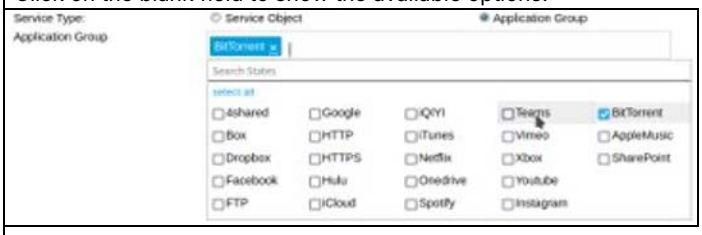
LABEL	DESCRIPTION
Application Object	This field is available if you selected Application Object as the service type. Click on the blank field to show the available options.  Select application patrol services to identify the specific traffic to which this policy applies. If you select BitTorrent, it includes the services listed below at the time of writing: • BitTorrent • BitTorrent_FileTransfer • BitTorrent_Application • BitTorrent_Bundle
DSCP Marking	Set how the Zyxel Device handles the DSCP value of the incoming and outgoing packets that match this policy. Inbound refers to the traffic the Zyxel Device sends to a connection's initiator. Outbound refers to the traffic the Zyxel Device sends out from a connection's initiator. Select one of the pre-defined DSCP values to apply or select User Defined to specify another DSCP value. The "af" choices stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. Select preserve to have the Zyxel Device keep the packets' original DSCP value. Select default to have the Zyxel Device set the DSCP value of the packets to 0.
Bandwidth Shaping	Configure these fields to set the amount of bandwidth the matching traffic can use.
Inbound kbps	Type how much inbound bandwidth, in kilobits per second, this policy allows the traffic to use. Inbound refers to the traffic the Zyxel Device sends to a connection's initiator. If you enter 0 here, this policy does not apply bandwidth management for the matching traffic that the Zyxel Device sends to the initiator. Traffic with bandwidth management disabled (inbound and outbound are both set to 0) is automatically treated as the lowest priority (7). If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.
Outbound kbps	Type how much outbound bandwidth, in kilobits per second, this policy allows the traffic to use. Outbound refers to the traffic the Zyxel Device sends out from a connection's initiator. If you enter 0 here, this policy does not apply bandwidth management for the matching traffic that the Zyxel Device sends out from the initiator. Traffic with bandwidth management disabled (inbound and outbound are both set to 0) is automatically treated as the lowest priority (7). If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.

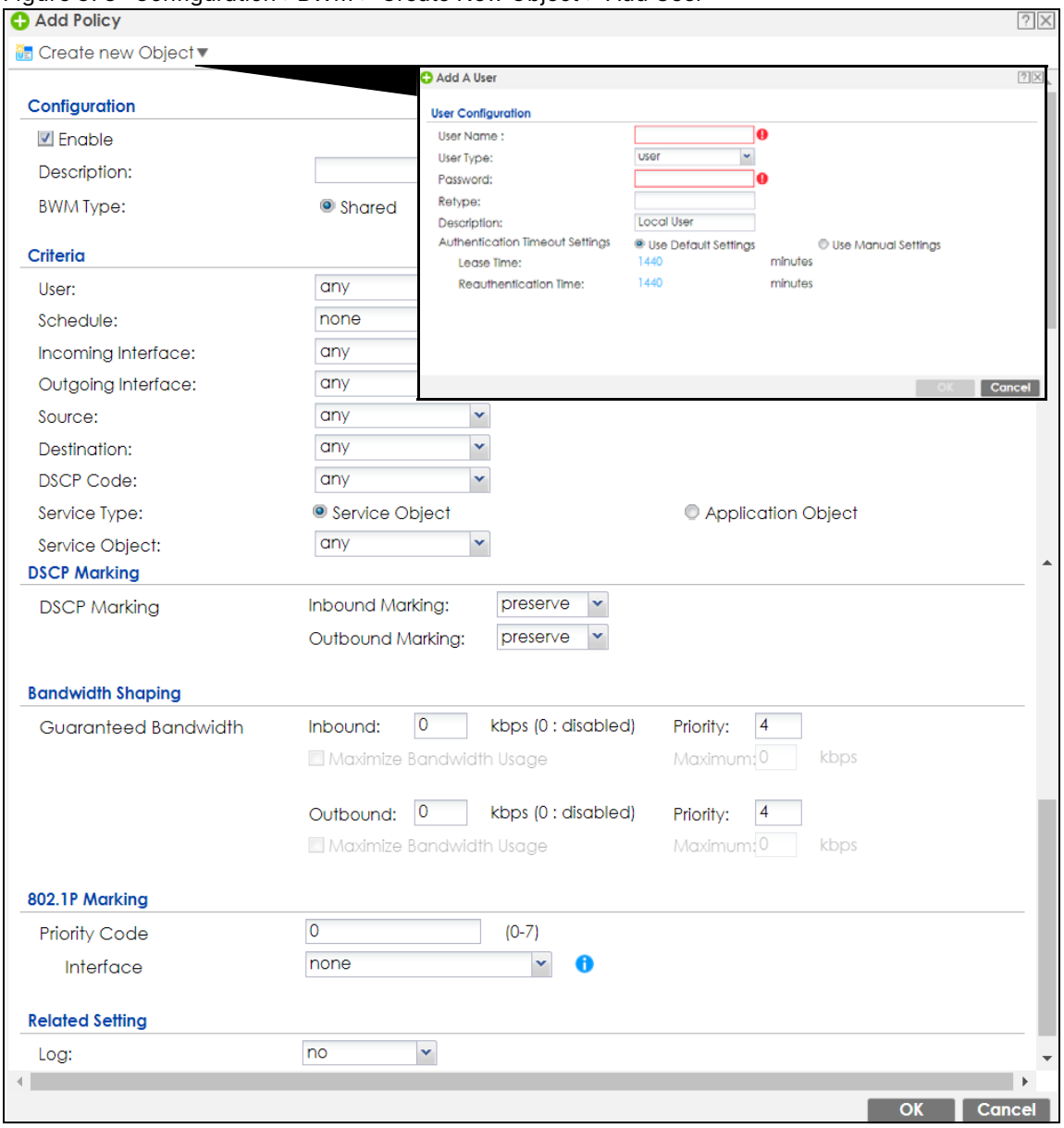
Table 160 Configuration > Bandwidth Management > Add/Edit

LABEL	DESCRIPTION
Priority	This field displays when the inbound or outbound bandwidth management is not set to 0. Enter a number between 1 and 7 to set the priority for traffic that matches this policy. The smaller the number, the higher the priority. Traffic with a higher priority is given bandwidth before traffic with a lower priority. When traffic with higher priority has reached the full bandwidth, the traffic with lower priority can use the remaining bandwidth. The Zyxel Device uses a fairness-based (round-robin) scheduler to divide bandwidth between traffic flows with the same priority. If the inbound or outbound limit is set to 0, the traffic is assigned to the lowest priority (7) regardless of this field's configuration.
Maximize Bandwidth Usage	This field displays when the inbound or outbound bandwidth management is not set to 0 and the BWM Type is set to Shared. Enable maximize bandwidth usage to let the traffic matching this policy "borrow" all unused bandwidth on the out-going interface. After each application or type of traffic gets its configured bandwidth rate, the Zyxel Device uses the fairness-based scheduler to divide any unused bandwidth on the out-going interface among applications and traffic types that need more bandwidth and have maximize bandwidth usage enabled.
Maximum	If you did not enable Maximize Bandwidth Usage, then type the maximum unused bandwidth that traffic matching this policy is allowed to "borrow" on the out-going interface (in Kbps), here.
802.1P Marking	Use 802.1P to prioritize outgoing traffic from a VLAN interface.
Priority Code	This is a 3-bit field within a 802.1Q VLAN tag that's used to prioritize associated outgoing VLAN traffic. "0" is the lowest priority level and "7" is the highest. See Table 159 on page 530. The setting configured here overwrites existing priority settings.
Interface	Choose a VLAN interface to which to apply the priority level for matching frames.
Related Setting	
Log	Select whether to have the Zyxel Device generate a log (log), log and alert (log alert) or neither (no) when any traffic matches this policy.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving your changes.

24.2.1.1 Adding Objects for the BWM Policy

Objects are parameters to which the Policy rules are built upon. There are three kinds of objects you can add/edit for the BWM policy, they are User, Schedule and Address objects. Click Configuration > BWM > Add > Create New Object > Add User to see the following screen.

Figure 378 Configuration >BWM > Create New Object > Add User



The following table describes the fields in the above screen.

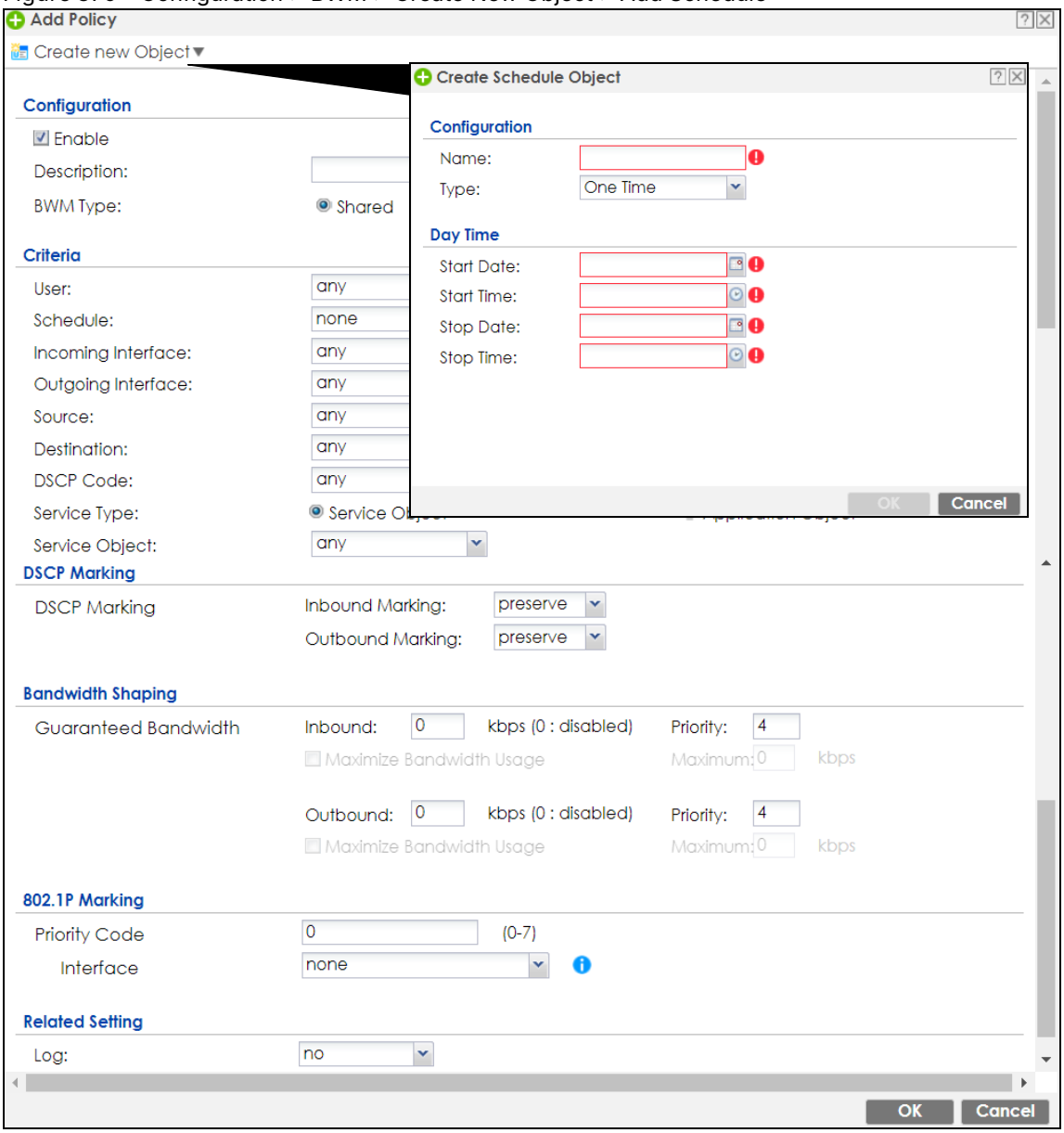
Table 161 Configuration > BWM > Create New Object > Add User

LABEL	DESCRIPTION
User Name	Type a user or user group object name of the rule.
User Type	Select a user type from the drop down menu. The user types are Admin, Limited admin, User, Guest, Ext-user, Ext-group-user.
Password	Type a password for the user object. The password can consist of alphanumeric characters, the underscore, and some punctuation marks (+-/*= :; .! @$&%#~ ' \ ()), and it can be up to eight characters long.
Retype	Retype the password to confirm.
Description	Enter a description of this policy. It is not used elsewhere. You can use alphanumeric and ()+/:+?!*#@$_%- characters, and it can be up to 60 characters long.

Table 161 Configuration > BWM > Create New Object > Add User

LABEL	DESCRIPTION
Authentication Timeout Settings	Choose either Use Default setting option, which shows the default Lease Time of 1,440 minutes and Reauthentication Time of 1,440 minutes or you can enter them manually by choosing Use Manual Settings option.
Lease Time	This shows the Lease Time setting for the user, by default it is 1,440 minutes.
Reauthentication Time	This shows the Reauthentication Time for the user, by default it is 1,440 minutes.
OK	Click OK to save the setting.
Cancel	Click Cancel to abandon this screen.

Figure 379 Configuration > BWM > Create New Object > Add Schedule

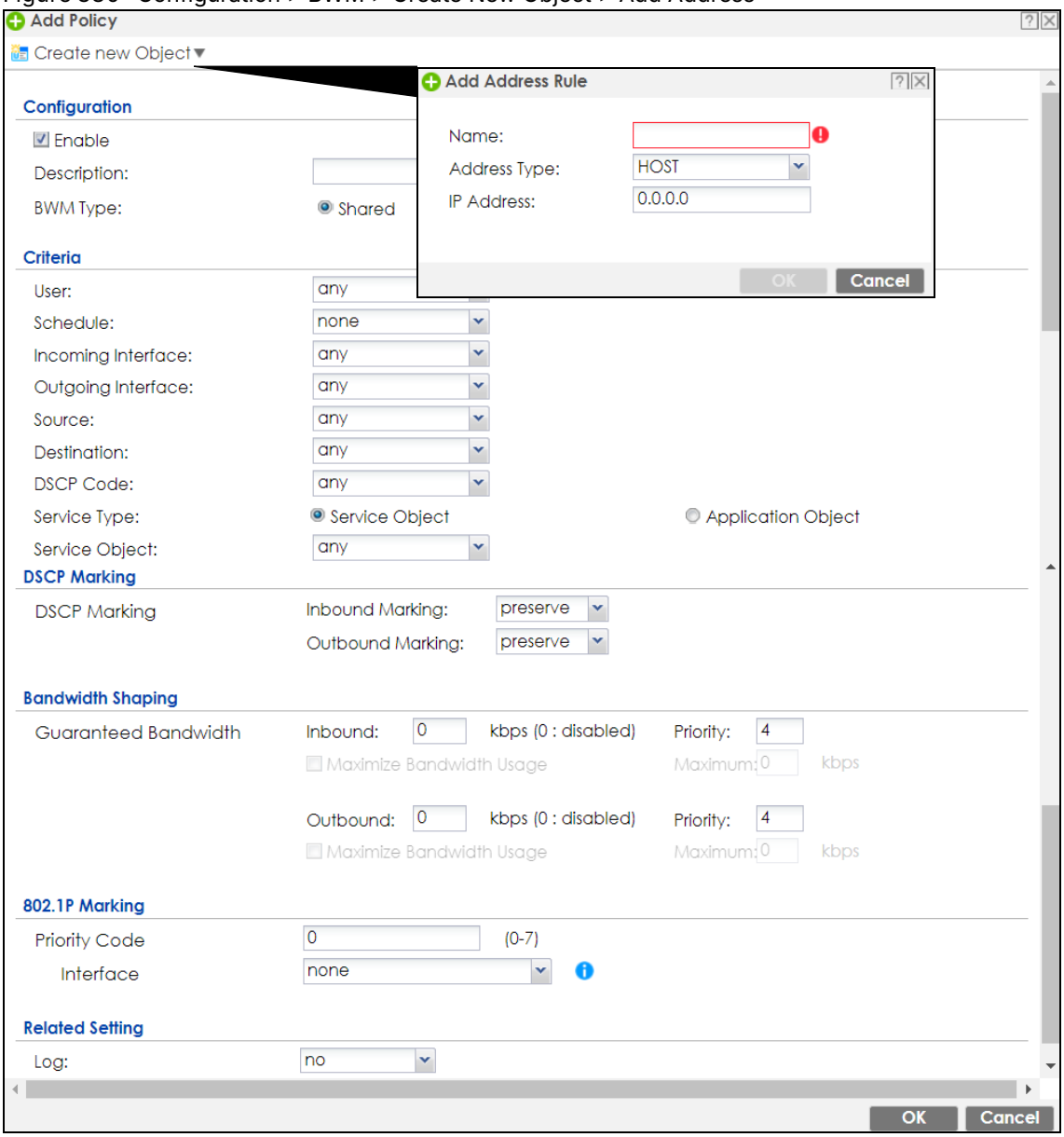


The following table describes the fields in the above screen.

Table 162 Configuration > BWM > Create New Object > Add Schedule

LABEL	DESCRIPTION
Name	Enter a name for the schedule object of the rule.
Type	Select an option from the drop down menu for the schedule object. It will show One Time or Recurring.
Start Date	Click the icon menu on the right to choose a Start Date for the schedule object.
Start Time	Click the icon menu on the right to choose a Start Time for the schedule object.
Stop Date	Click the icon menu on the right to choose a Stop Date for schedule object.
Stop Time	Click the icon menu on the right to choose a Stop Time for the schedule object.

Figure 380 Configuration > BWM > Create New Object > Add Address



The following table describes the fields in the above screen.

Table 163 Configuration > BWM > Create New Object > Add Address

LABEL	DESCRIPTION
Name	Enter a name for the Address object of the rule.
Address Type	Select an Address Type from the drop down menu on the right. The Address Types are Host, Range, Subnet, Interface IP, Interface Subnet, and Interface Gateway.
IP Address	Enter an IP address for the Address object.
OK	Click OK to save the setting.
Cancel	Click Cancel to abandon the setting.

24.3 Example: Prioritize a Specific Application

You are a client on the Zyxel Device LAN1. You use Teams to communicate with your colleagues and have video meetings often at work. You want to create a bandwidth management rule to prioritize traffic for Teams so that you can always use Teams without any delay.

Set the BWM Type to Shared to apply the BWM rule to all matched traffic.

This example uses the parameters given below.

Table 164 BWM Example

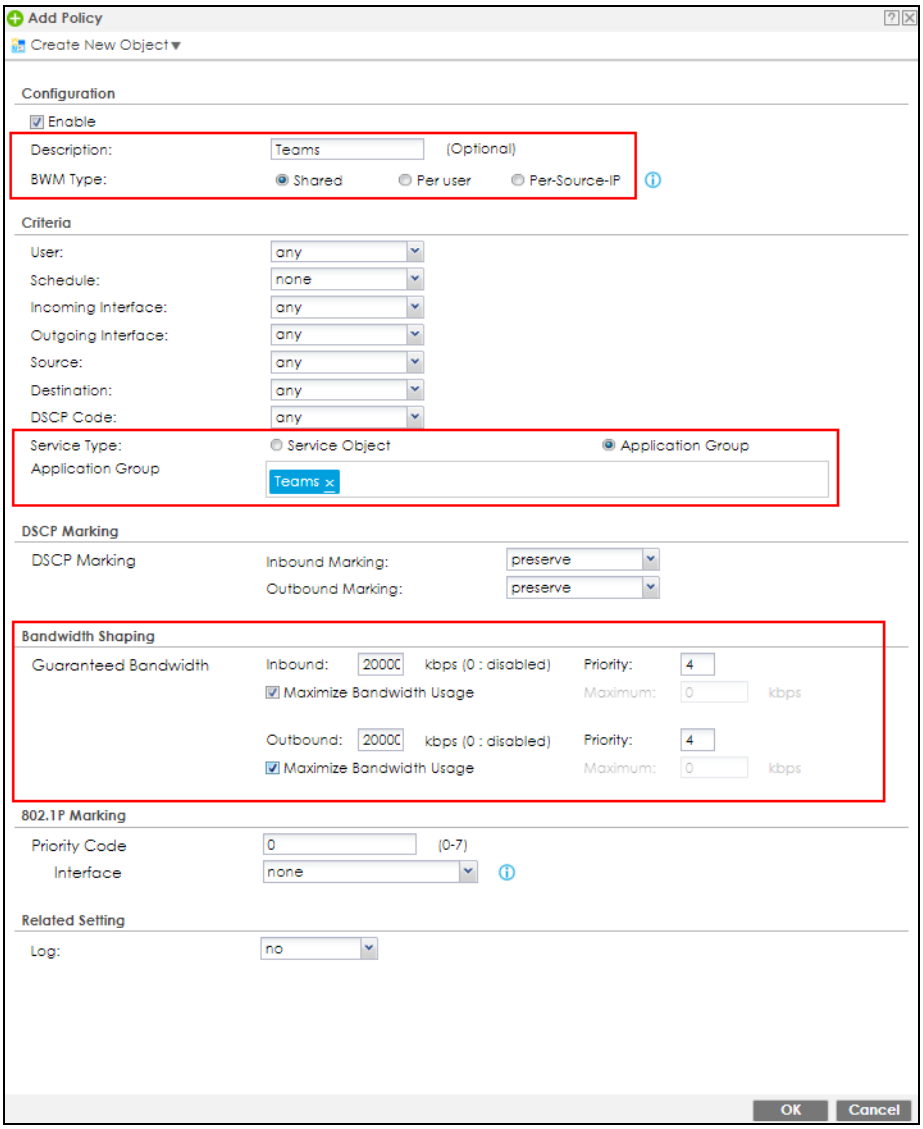
DESCRIPTION	BWM TYPE	SERVICE TYPE	SERVICE OBJECT	GUARANTEED BANDWIDTH
Teams	Shared	Service Object	Teams	Inbound: 20000 kbps/ Priority: 1 Outbound: 20000 kbps/ Priority: 1

1 Go to Configuration > BWM. Click Add to create a bandwidth management rule using the parameters given in Table 164 on page 538.

2 Select Maximize Bandwidth Usage to allow the traffic that matches this rule borrow all unused bandwidth on the outgoing interface.

3 Select Teams under Application Group.

4 Click OK to save your changes.



5 The traffic for Teams is now at the highest priority to use the Zyxel Device bandwidth.

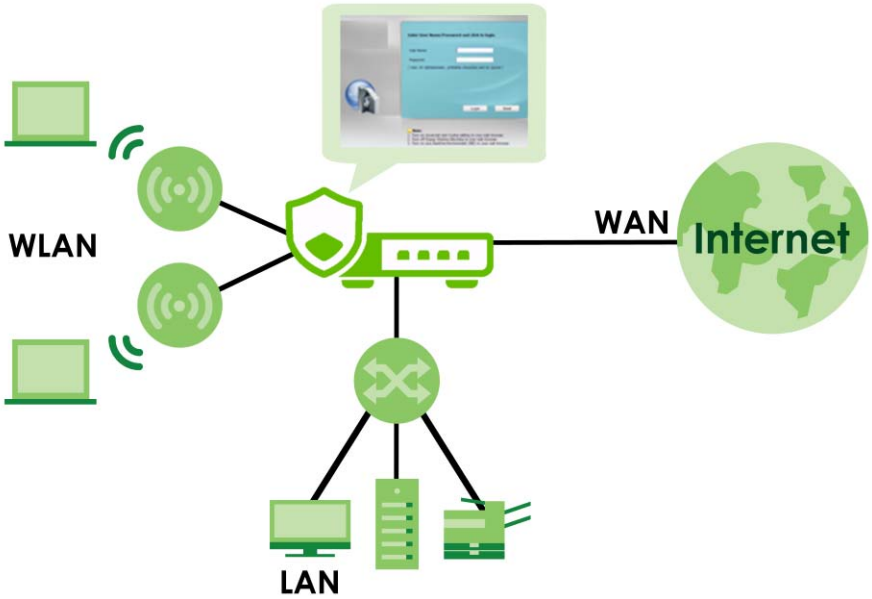
CHAPTER 25
Web Authentication

25.1 Web Auth Overview

Web authentication can intercept network traffic, according to the authentication policies, until the user authenticates his or her connection, usually through a specifically designated login web page. This means all web page requests can initially be redirected to a special web page that requires users to authenticate their sessions. Once authentication is successful, they can then connect to the rest of the network or Internet.

As soon as a user attempt to open a web page, the Zyxel Device reroutes his/her browser to a web portal page that prompts him/her to log in.

Figure 381 Web Authentication Example



The web authentication page only appears once per authentication session. Unless a user session times out or he/she closes the connection, he or she generally will not see it again during the same session.

25.1.1 What You Can Do in this Chapter

- Use the Configuration > Web Authentication screens (Section 25.2 on page 542) to create and manage web authentication policies.
- Use the Configuration > Web Authentication > SSO screen (Section 25.3 on page 558) to configure how the Zyxel Device communicates with a Single Sign-On agent.

25.1.2 What You Need to Know

Single Sign-On

A SSO (Single Sign On) agent integrates Domain Controller and Zyxel Device authentication mechanisms, so that users just need to log in once (single) to get access to permitted resources.

Forced User Authentication

Instead of making users for which User-Authentication policies have been configured go to the Zyxel Device Login screen manually, you can configure the Zyxel Device to display the Login screen automatically whenever it routes HTTP traffic for anyone who has not logged in yet.

Note: This works with HTTP traffic only. The Zyxel Device does not display the Login screen when users attempt to send other kinds of traffic.

The Zyxel Device does not automatically route the request that prompted the login, however, so users have to make this request again.

Google Authentication

Please see authentication method objects in Section 30.8.3 on page 736.

Summary of User Authentication Methods

The following table summarizes how users authenticate with the Zyxel Device when web authentication is enabled.

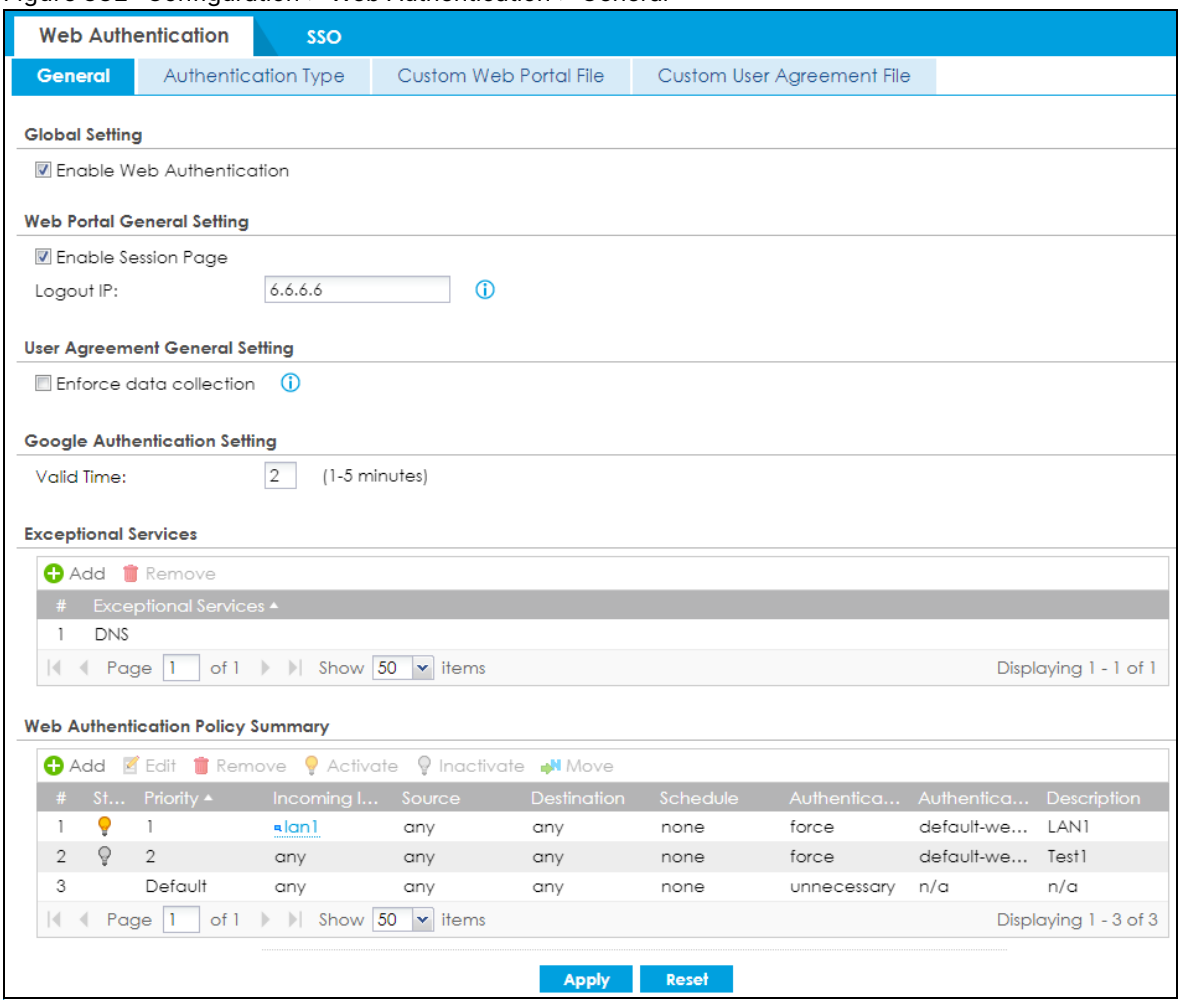
Table 165 User Authentication Methods

CLIENT	GOOGLE AUTHENTICATOR	USER AUTHENTICATION STEPS
802.1X	No	1. 802.1X - Username/password 2. Web Authentication Portal - Username/password
	Yes	1. 802.1X - Username/password 2. Web Authentication Portal - Username/password 3. Web Authentication Portal - Google Authenticator code
	No	1. 802.1X - Username/password
	Yes	1. 802.1X - Username/password 2. Web Authentication Portal - Google Authenticator code
Non-802.1X	No	1. Web Authentication Portal - Username/password
	Yes	1. Web Authentication Portal - Username/password 2. Web Authentication Portal - Google Authenticator code
	No	None needed (if user is using Windows)
	Yes	None needed (if user is using Windows)

25.2 Web Authentication General Screen

The Web Authentication General screen displays the general web portal settings and web authentication policies you have configured on the Zyxel Device. Use this screen to enable web authentication on the Zyxel Device.

Figure 382 Configuration > Web Authentication > General



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

Table 166 Configuration > Web Authentication > General

LABEL	DESCRIPTION
Global Setting	
Enable Web Authentication	Select the checkbox to turn on the web authentication feature. Otherwise, clear the checkbox to turn it off. Once enabled, all network traffic is blocked until a client authenticates with the Zyxel Device through the specifically designated web portal or user agreement page.
Web Portal General Setting	
Enable Session Page	Select this to display a page showing information on the user session after s/he logs in. It displays remaining time with an option to renew or log out immediately.

Table 166 Configuration > Web Authentication > General (continued)

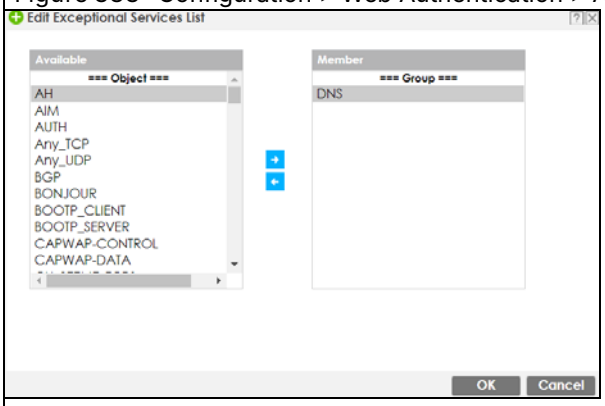
LABEL	DESCRIPTION
Logout IP	Specify an IP address that users can use to terminate their sessions manually by entering the IP address in the address bar of the web browser.
User Agreement General Setting	
Enforce data collection	Select this to require users to fill in their registration information (name, telephone number, address and email address) on the User Agreement (PC or mobile) page.
Google Authentication Setting	Web authentication supports two-factor authentication using Google Authenticator. When enabled, the web authentication page first prompts the user to enter their username and password (factor 1), and then prompts them to enter a time-limited code from the Google Authenticator app (factor 2). It is also possible to configure two-factor authentication for VPN and admin users. The admin two-factor authentication settings override the web authentication two-factor authentication settings if both are configured.
Valid Time	Enter the time limit (1-5 minutes) for the code from the Google Authenticator app to be used for login.
Exceptional Services	Use this table to list services that users can access without logging in. Click Add to change the list's membership. A screen appears. Available services appear on the left. Select any services you want users to be able to access without logging in and click the right arrow button to add them. The member services are on the right. Select any service that you want to remove from the member list, and click the left arrow button to remove them. Keeping DNS as a member allows users' computers to resolve domain names into IP addresses. Figure 383 Configuration > Web Authentication > Add Exceptional Service  In the table, select one or more entries and click Remove to delete it or them.
Web Authentication Policy Summary	Use this table to manage the Zyxel Device's list of web authentication policies.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The 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.
Move	To move an entry to a different number in the list, click the Move icon. In the field that appears, specify the number to which you want to move the interface.

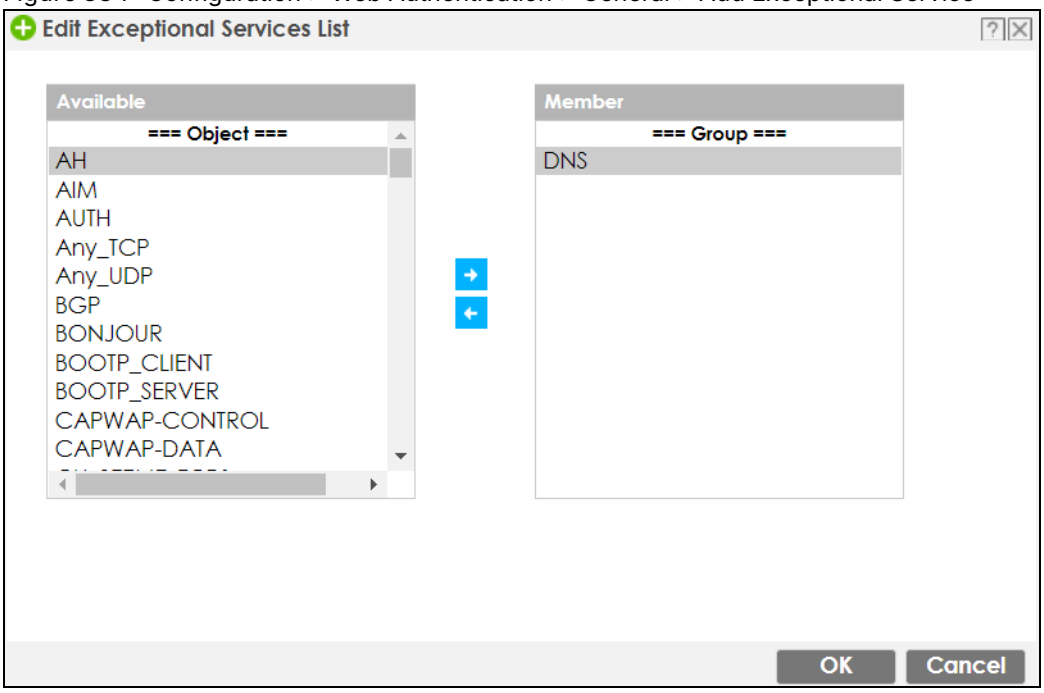
Table 166 Configuration > Web Authentication > General (continued)

LABEL	DESCRIPTION
#	This field is a sequential value showing the number of the profile. The profile order is not important.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Priority	This is the position of the authentication policy in the list. The priority is important as the policies are applied in order of priority. Default displays for the default authentication policy that the Zyxel Device uses on traffic that does not match any exceptional service or other authentication policy. You can edit the default rule but not delete it.
Incoming Interface	This field displays the interface on which packets for this policy are received.
Source	This displays the source address object, including geographic address and FQDN (group) objects, to which this policy applies.
Destination	This displays the destination address object, including geographic address and FQDN (group) objects, to which this policy applies.
Schedule	This field displays the schedule object that dictates when the policy applies. none means the policy is active at all times if enabled.
Authentication	This field displays the authentication requirement for users when their traffic matches this policy. unnecessary - Users do not need to be authenticated. required - Users need to be authenticated. They must manually go to the login screen or user agreement page. The Zyxel Device will not redirect them to the login screen. force - Users need to be authenticated. The Zyxel Device automatically displays the login screen or user agreement page whenever it routes HTTP traffic for users who have not logged in yet.
Authentication Type	This field displays the name of the authentication type profile used in this policy to define how users authenticate their sessions. It shows n/a if Authentication is set to unnecessary.
Description	If the entry has a description configured, it displays here. This is n/a for the default policy.
Apply	Click this button to save your changes to the Zyxel Device.
Reset	Click this button to return the screen to its last-saved settings.

Creating Exceptional Services

This screen lists services that users can access without logging in. Click Add under Exceptional Services in the previous screen to display this screen. You can change the list's membership here. Available services appear on the left. Select any services you want users to be able to access without logging in and click the right arrow button -> to add them. The member services are on the right. Select any service that you want to remove from the member list, and click the left arrow <- button to remove them. Then click OK to apply the changes and return to the main Web Authentication screen. Alternatively, click Cancel to discard the changes and return to the main Web Authentication screen.

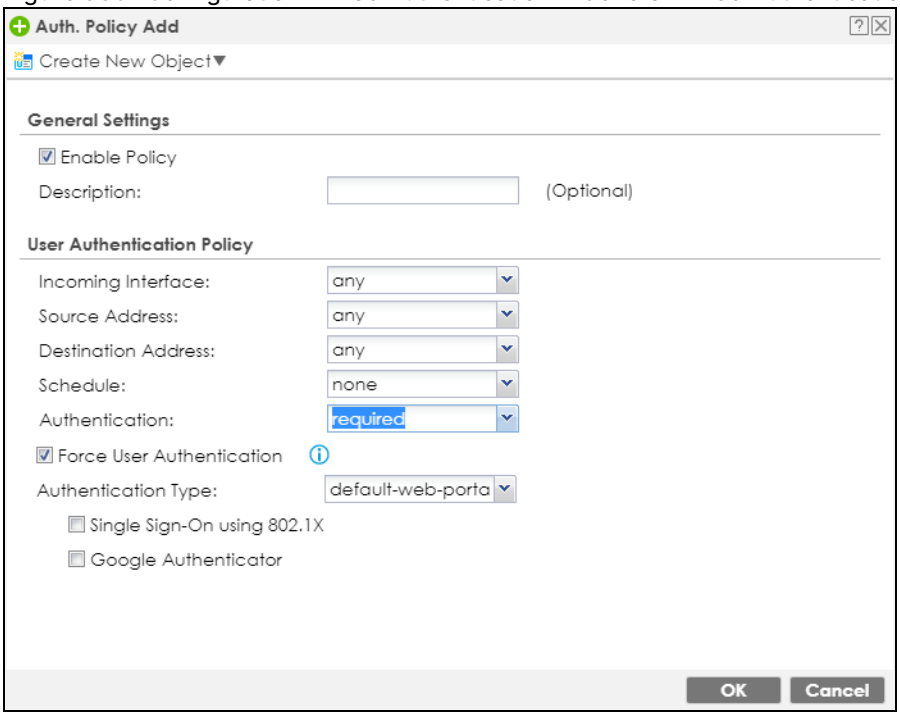
Figure 384 Configuration > Web Authentication > General > Add Exceptional Service



Creating/Editing an Authentication Policy

Open the Configuration > Web Authentication > General screen, then click the Add icon or select an entry and click the Edit icon in the Web Authentication Policy Summary section to open the Auth. Policy Add/Edit screen. Use this screen to configure an authentication policy.

Figure 385 Configuration > Web Authentication > General > Add Authentication Policy



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

Table 167 Configuration > Web Authentication > General > Add Authentication Policy

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen. Select Address or Schedule.
Enable Policy	Select this checkbox to activate the authentication policy. This field is available for user-configured policies.
Description	Enter a descriptive name with 1 to 63 single-byte characters, including a-zA-Z0-9!"#$%&'()*+,-/:;=?@_ and spaces. .<>[\]^'{|} are not allowed. This field is available for user-configured policies.
User Authentication Policy	Use this section of the screen to determine which traffic requires (or does not require) the senders to be authenticated in order to be routed.
Incoming Interface	Select the interface on which packets for this policy are received.
Source Address	Select a source address or address group, including geographic address and FQDN (group) objects, for whom this policy applies. Select any if the policy is effective for every source. This is any and not configurable for the default policy.
Destination Address	Select a destination address or address group, including geographic address and FQDN (group) objects, for whom this policy applies. Select any if the policy is effective for every destination. This is any and not configurable for the default policy.
Schedule	Select a schedule that defines when the policy applies. Otherwise, select none and the rule is always effective. This is none and not configurable for the default policy.
Authentication	Select the authentication requirement for users when their traffic matches this policy. unnecessary - Users do not need to be authenticated. required - Users need to be authenticated. If Force User Authentication is selected, all HTTP traffic from unauthenticated users is redirected to a default or user-defined login page. Otherwise, they must manually go to the login screen. The Zyxel Device will not redirect them to the login screen.
Force User Authentication	This field is available for user-configured policies that require authentication. Select this to have the Zyxel Device automatically display the login screen when users who have not logged in yet try to send HTTP traffic.
Authentication Type	Select an authentication method. default-web-portal: the default login page built into the Zyxel Device. default-user-agreement: the default user agreement page built into the Zyxel Device.
Single Sign-On using 802.1X	802.1X Single Sign-On allows the Zyxel Device to use the same username and password for 802.1X WiFi authentication and web authentication. When enabled, a user logs into a WiFi network on the Zyxel Device that has 802.1X (WPA Enterprise) enabled. The Zyxel Device then reuses the 802.1X username and password for web authentication, preventing the user from having to log in twice. Active Directory Single Sign-On takes priority over 802.1X Single Sign-On, if both are enabled.
Google Authenticator	Select Google Authenticator to first prompt a user to enter their username and password (factor 1), and then prompt the user to enter a time-limited code from the Google Authenticator app (factor 2).
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

25.2.1 User-Authentication Access Control Example

You can configure many policies and security settings for specific users or groups of users. Users can be authenticated locally by the Zyxel Device or by an external (RADIUS) authentication server.

In this example the users are authenticated by an external RADIUS server at 172.16.1.200. First, set up the user accounts and user groups in the Zyxel Device. Then, set up user authentication using the RADIUS server. Finally, set up the policies in the table above.

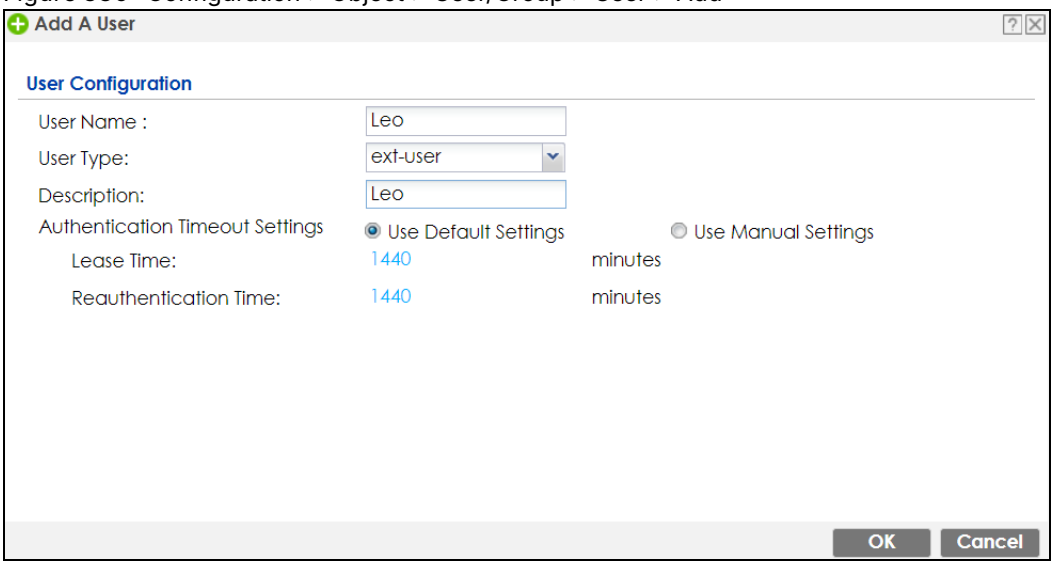
25.2.1.1 Set Up User Accounts

Set up user accounts in the RADIUS server. This example uses the Web Configurator. If you can export user names from the RADIUS server to a text file, then you might configure a script to create the user accounts instead.

1 Click Configuration > Object > User/Group > User. Click the Add icon.

2 Enter the same user name that is used in the RADIUS server, and set the User Type to ext-user because this user account is authenticated by an external server. Click OK.

Figure 386 Configuration > Object > User/Group > User > Add



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

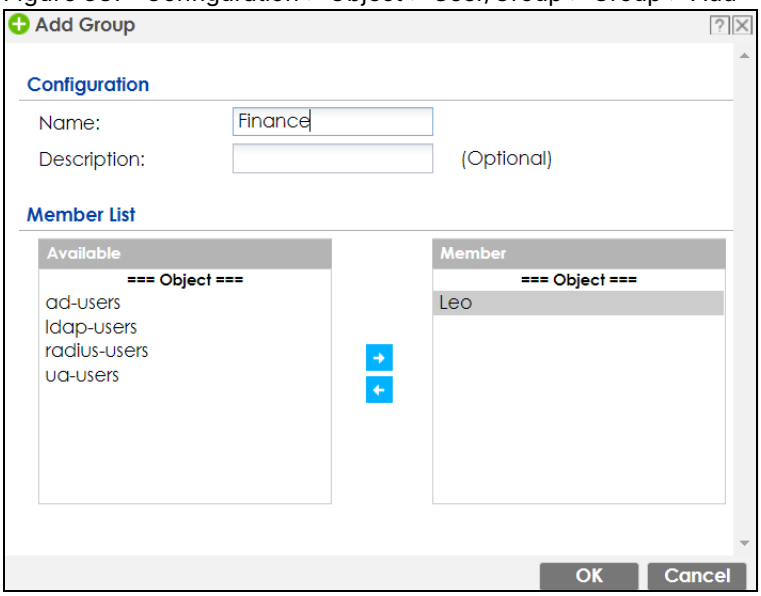
25.2.1.2 Set Up User Groups

Set up the user groups and assign the users to the user groups.

1 Click Configuration > Object > User/Group > Group. Click the Add icon.

2 Enter the name of the group. In this example, it is “Finance”. Then, select Object/Leo and click the right arrow to move him to the Member list. This example only has one member in this group, so click OK. Of course you could add more members later.

Figure 387 Configuration > Object > User/Group > Group > Add



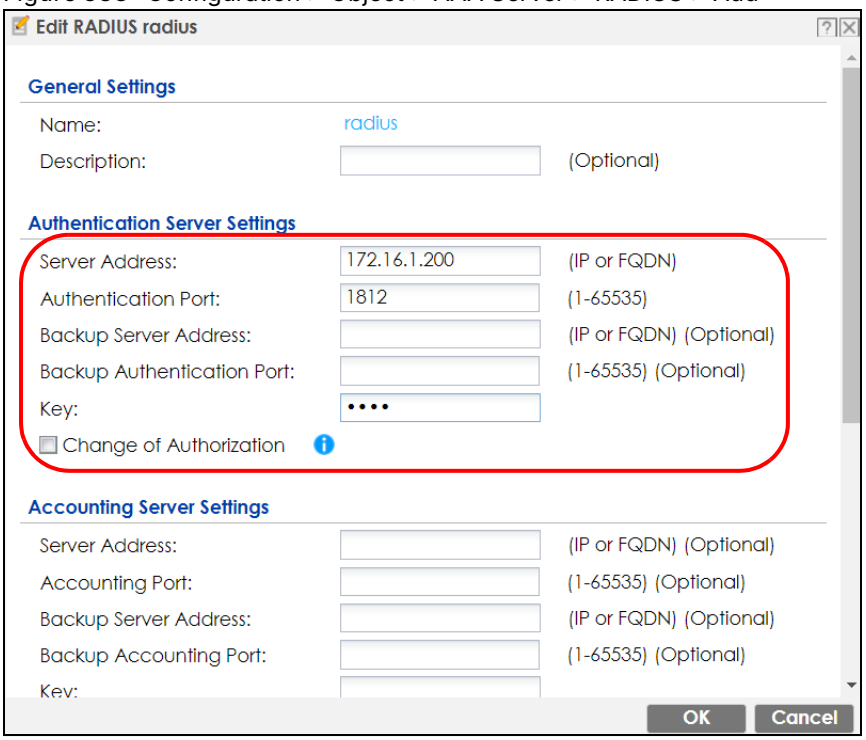
3 Repeat this process to set up the remaining user groups.

25.2.1.3 Set Up User Authentication Using the RADIUS Server

This step sets up user authentication using the RADIUS server. First, configure the settings for the RADIUS server. Then, set up the authentication method, and configure the Zyxel Device to use the authentication method. Finally, force users to log into the Zyxel Device before it routes traffic for them.

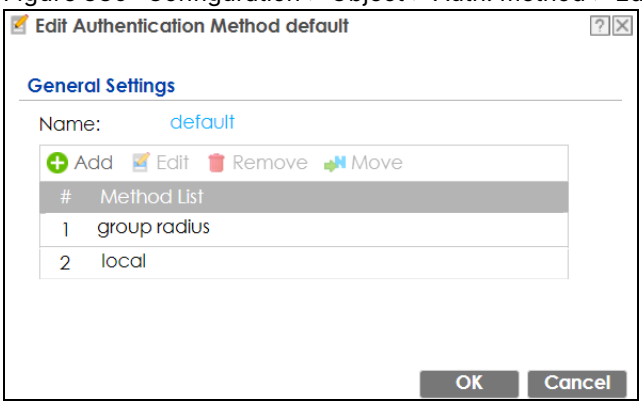
1 Click Configuration > Object > AAA Server > RADIUS. Double-click the radius entry. Configure the RADIUS server's address, authentication port (1812 if you were not told otherwise), and key. Click OK.

Figure 388 Configuration > Object > AAA Server > RADIUS > Add



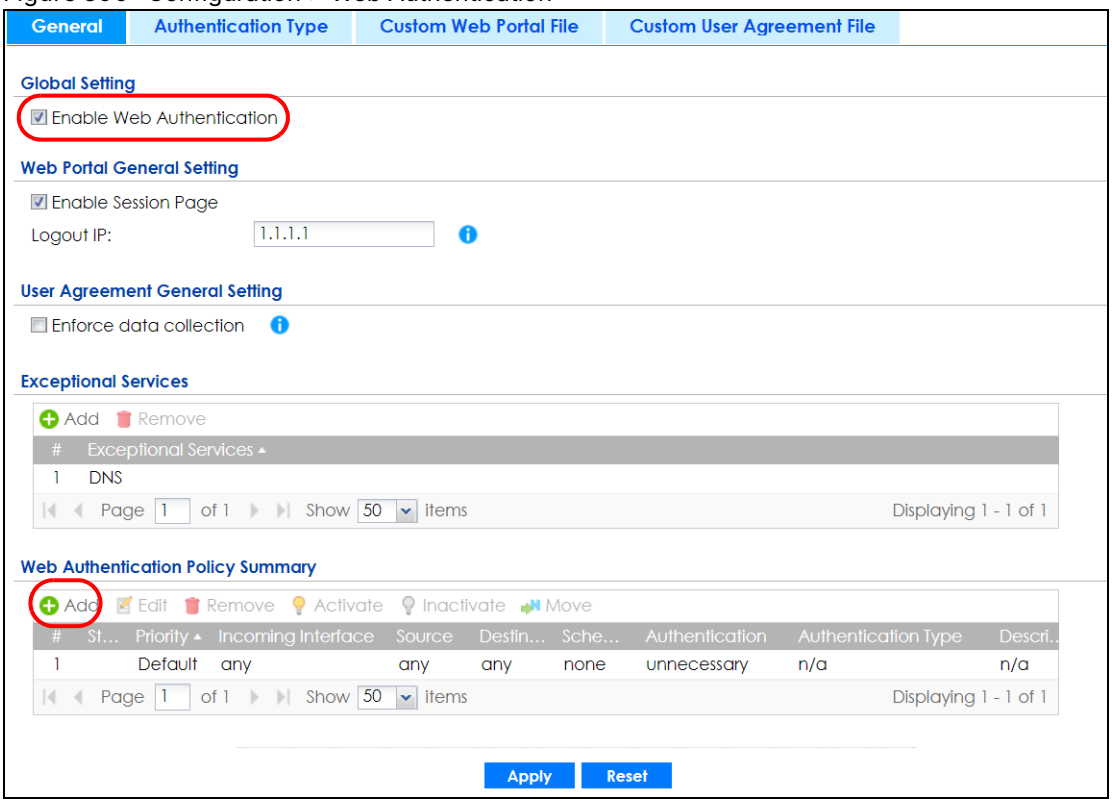
2 Click Configuration > Object > Auth. Method. Double-click the default entry. Click the Add icon. Select group radius because the Zyxel Device should use the specified RADIUS server for authentication. Click OK.

Figure 389 Configuration > Object > Auth. method > Edit



3 Click Configuration > Web Authentication. In the Web Authentication > General screen, select Enable Web Authentication to turn on the web authentication feature and click Apply.

Figure 390 Configuration > Web Authentication

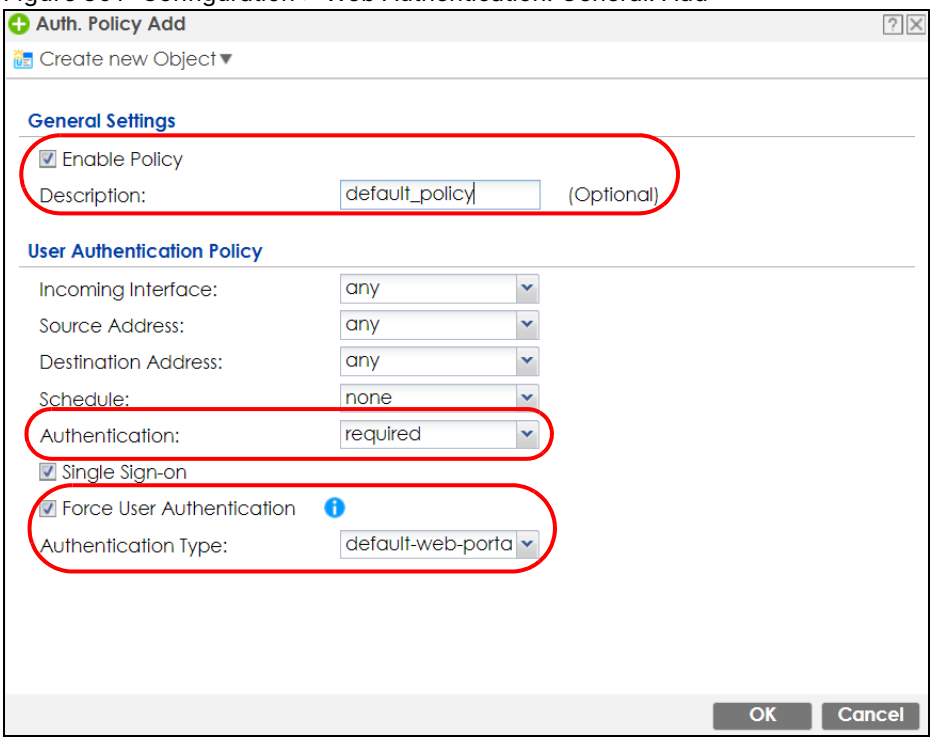


4 In the Web Authentication Policy Summary section, click the Add icon to set up a default policy that has priority over other policies and forces every user to log into the Zyxel Device before the Zyxel Device routes traffic for them.

5 Select Enable Policy. Enter a descriptive name, “default_policy” for example. Set the Authentication field to required, and make sure Force User Authentication is selected. Select an authentication type profile (“default-web-portal” in this example). Keep the rest of the default settings, and click OK.

Note: The users must log in at the Web Configurator login screen before they can use HTTP or MSN.

Figure 391 Configuration > Web Authentication: General: Add



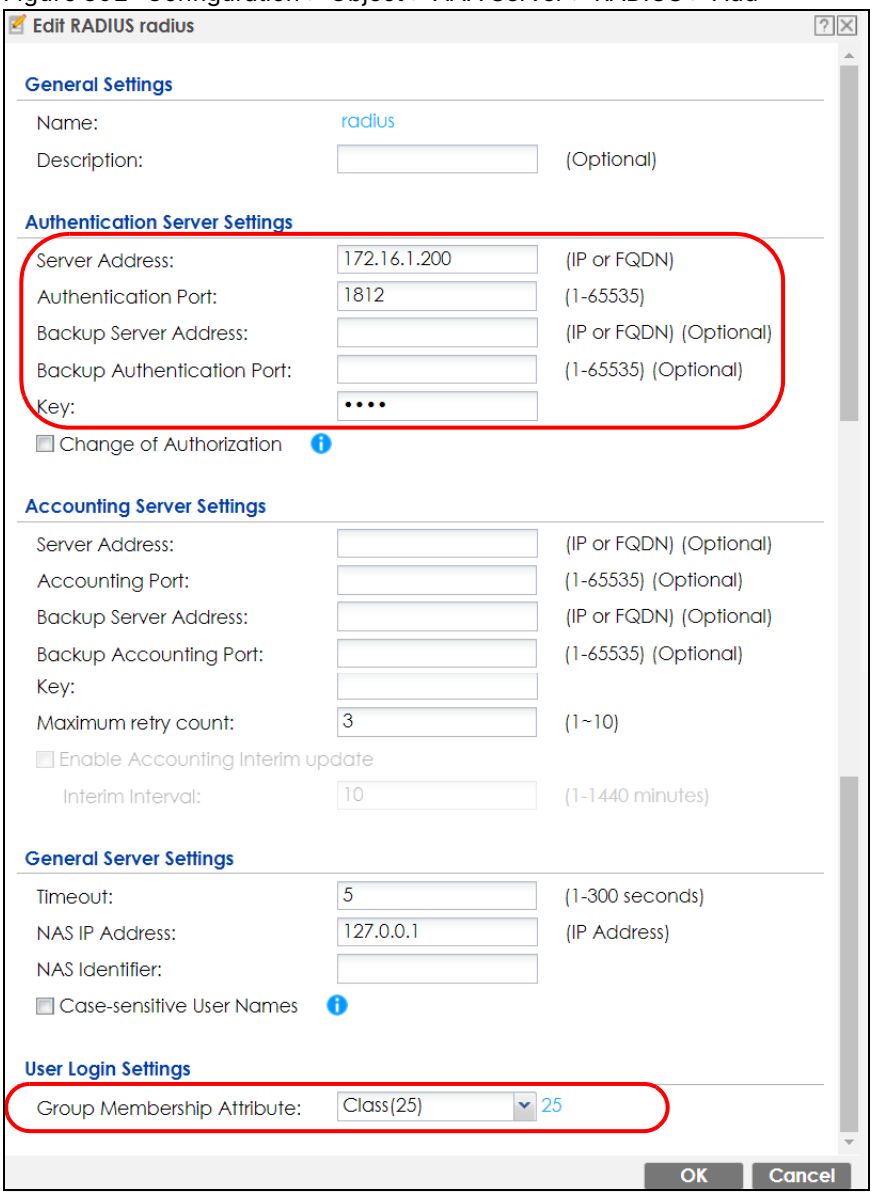
When the users try to browse the web (or use any HTTP application), the login screen appears. They have to log in using the user name and password in the RADIUS server.

25.2.1.4 User Group Authentication Using the RADIUS Server

The previous example showed how to have a RADIUS server authenticate individual user accounts. If the RADIUS server has different user groups distinguished by the value of a specific attribute, you can make a couple of slight changes in the configuration to have the RADIUS server authenticate groups of user accounts defined in the RADIUS server.

1 Click Configuration > Object > AAA Server > RADIUS. Double-click the radius entry. Besides configuring the RADIUS server's address, authentication port, and key; set the Group Membership Attribute field to the attribute that the Zyxel Device is to check to determine to which group a user belongs. This example uses Class. This attribute's value is called a group identifier; it determines to which group a user belongs. In this example the values are Finance, Engineer, Sales, and Boss.

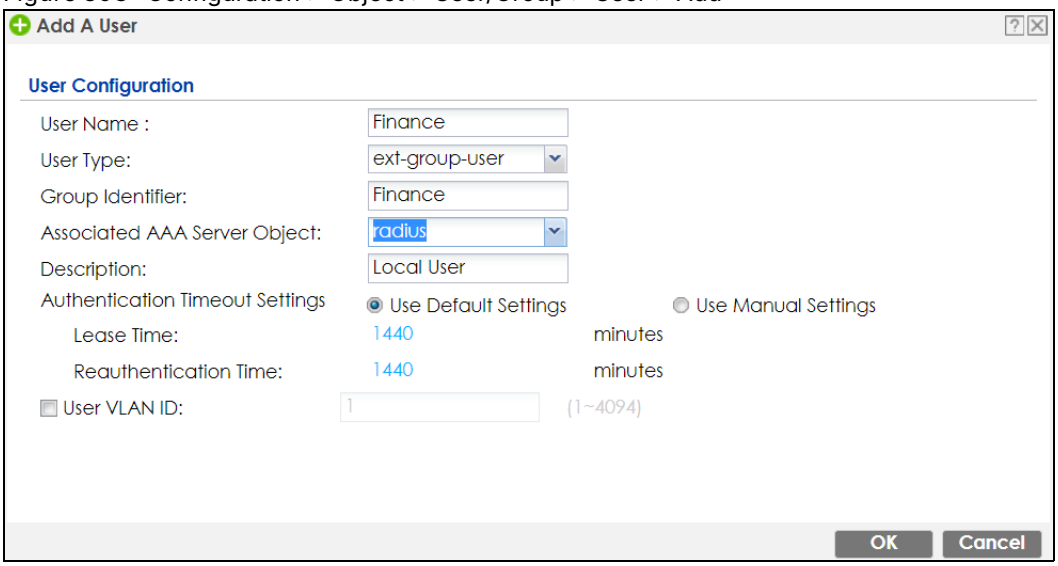
Figure 392 Configuration > Object > AAA Server > RADIUS > Add



2 Now you add ext-group-user objects to identify groups based on the group identifier values. Set up one user account for each group of user accounts in the RADIUS server. Click Configuration > Object > User/Group > User. Click the Add icon.

3 Enter a user name and set the User Type to ext-group-user. In the Group Identifier field, enter Finance, Engineer, Sales, or Boss and set the Associated AAA Server Object to radius.

Figure 393 Configuration > Object > User/Group > User > Add

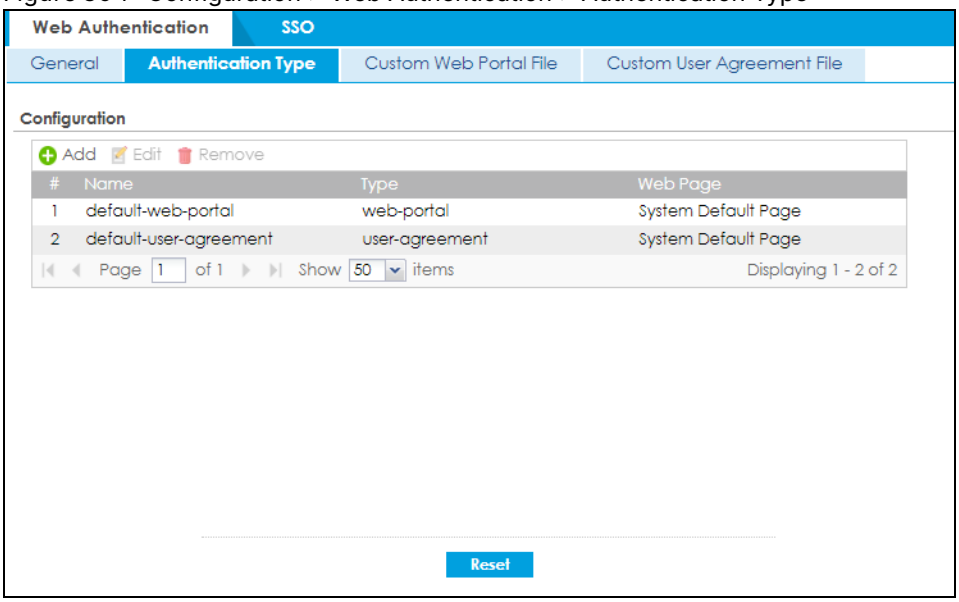


4 Repeat this process to set up the remaining groups of user accounts.

25.2.2 Authentication Type Screen

Use this screen to view, create and manage the authentication type profiles on the Zyxel Device. An authentication type profile decides which type of web authentication pages to be used for user authentication. Go to Configuration > Web Authentication and then select the Authentication Type tab to display the screen.

Figure 394 Configuration > Web Authentication > Authentication Type



The following table describes the labels in this screen.

Table 168 Configuration > Web Authentication > Authentication Type

LABEL	DESCRIPTION
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Name	This field displays the name of the profile. default-web-portal: the default login page built into the Zyxel Device. Note: You can also customize the default login page built into the Zyxel Device in the System > WWW > Login Page screen. default-user-agreement: the default user agreement page built into the Zyxel Device.
Type	This field displays the type of the web authentication page used by this profile.
Web Page	This field displays whether this profile uses the default web authentication page built into the Zyxel Device (System Default Page) or custom web authentication pages from an external web server (External Page).
Reset	Click Reset to return the screen to its last-saved settings.

Add/Edit an Authentication Type Profile

Click the Add icon or select an entry in the Web Authentication > Authentication Type screen and click the Edit icon to display the screen. The screen differs depending on what you select in the Type field.

Figure 395 Configuration > Web Authentication > Authentication Type: Add/Edit (Web Portal)

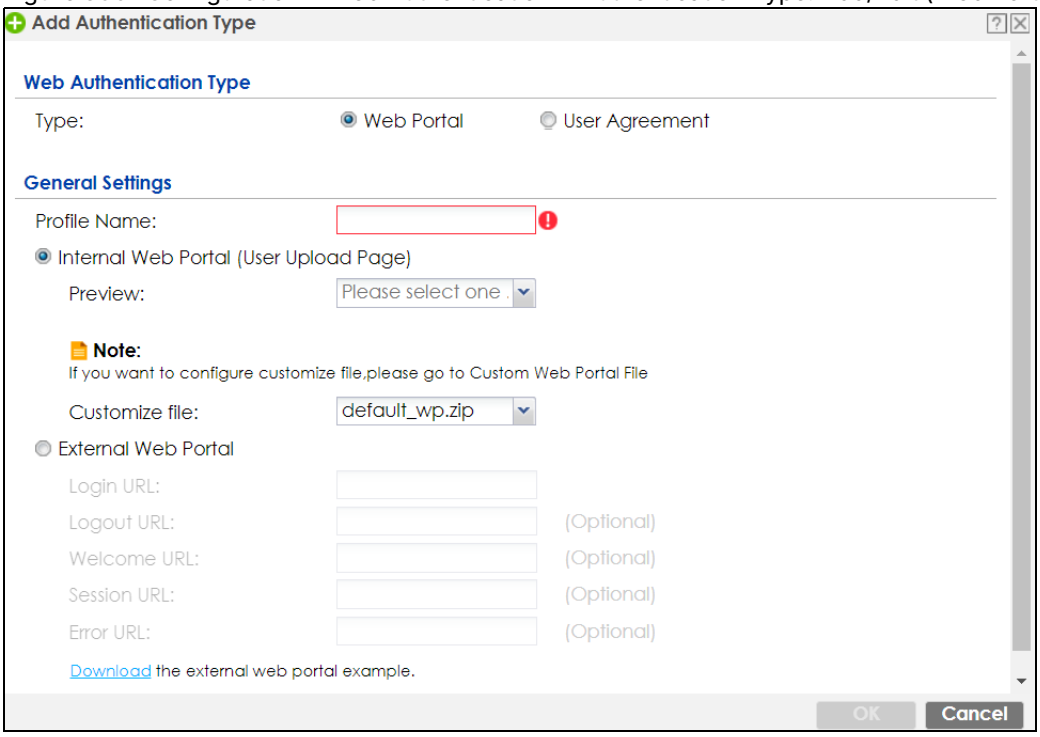
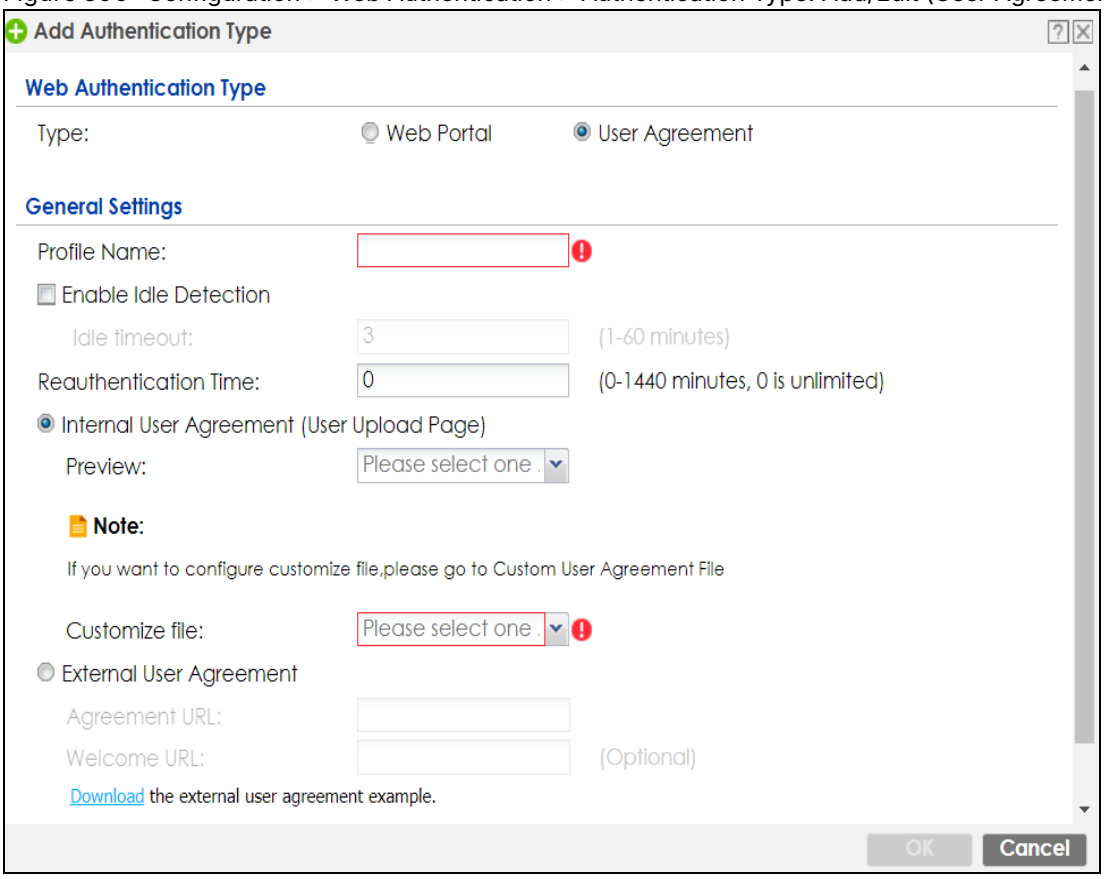


Figure 396 Configuration > Web Authentication > Authentication Type: Add/Edit (User Agreement)



The following table describes the labels in this screen.

Table 169 Configuration > Web Authentication > Authentication Type: Add/Edit

LABEL	DESCRIPTION
Type	Select the type of the web authentication page through which users authenticate their connections. If you select User Agreement, by agreeing to the policy of user agreement, users can access the Internet without a guest account.
Profile Name	Enter a name for the profile. You can use up to 31 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). Spaces are not allowed. The first character must be a letter.
The following fields are available if you set Type to Web Portal.	
Internal Web Portal	Select this to use the web portal pages uploaded to the Zyxel Device. The login page appears whenever the web portal intercepts network traffic, preventing unauthorized users from gaining access to the network.
Preview	Select to display the page you uploaded to the Zyxel Device in a new frame. Note: You must select a custom file uploaded to the Zyxel Device before you can preview the pages.
Customize file	Select the file name of the web portal file in the Zyxel Device. Note: You can upload zipped custom web portal files to the Zyxel Device using the Configuration > Web Authentication > Web Portal Customize File screen.

Table 169 Configuration > Web Authentication > Authentication Type: Add/Edit (continued)

LABEL	DESCRIPTION
External Web Portal	Select this to use a custom login page from an external web portal instead of the one uploaded to the Zyxel Device. You can configure the look and feel of the web portal page.
Login URL	Specify the login page's URL; for example, http://IIS server IP Address/login.html. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Logout URL	Specify the logout page's URL; for example, http://IIS server IP Address/logout.html. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Welcome URL	Specify the welcome page's URL; for example, http://IIS server IP Address/welcome.html. Users will be redirected to the welcome page after authentication. This field is optional. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Session URL	Specify the session page's URL; for example, http://IIS server IP Address/session.html. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Error URL	Specify the error page's URL; for example, http://IIS server IP Address/error.html. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Download	Click this to download an example external web portal file for your reference.
The following fields are available if you set Type to User Agreement.	
Enable Idle Detection	This is applicable for access users. Select this checkbox if you want the Zyxel Device to monitor how long each access user is logged in and idle (in other words, there is no traffic for this access user). The Zyxel Device automatically logs out the access user once the Idle timeout has been reached.
Idle timeout	This is applicable for access users. This field is effective when Enable Idle Detection is checked. Type the number of minutes each access user can be logged in and idle before the Zyxel Device automatically logs out the access user.
Reauthentication Time	Enter the number of minutes the user can be logged into the Zyxel Device in one session before having to log in again.
Internal User Agreement	Select this to use the user agreement pages in the Zyxel Device. The user agreement page appears whenever the Zyxel Device intercepts network traffic, preventing unauthorized users from gaining access to the network.
Preview	Select to display the page you uploaded to the Zyxel Device in a new frame. Note: You must select a custom file uploaded to the Zyxel Device before you can preview the pages.
Customize file	Select the file name of the user agreement file in the Zyxel Device. Note: You can upload zipped custom user agreement files to the Zyxel Device using the Configuration > Web Authentication > User Agreement Customize File screen.
External User Agreement	Select this to use custom user agreement pages from an external web server instead of the default one built into the Zyxel Device. You can configure the look and feel of the user agreement page.
Agreement URL	Specify the user agreement page's URL; for example, http://IIS server IP Address/logout.html. The Internet Information Server (IIS) is the web server on which the user agreement files are installed.

Table 169 Configuration > Web Authentication > Authentication Type: Add/Edit (continued)

LABEL	DESCRIPTION
Welcome URL	Specify the welcome page's URL; for example, http://IIS server IP Address/welcome.html. The Internet Information Server (IIS) is the web server on which the user agreement files are installed. If you leave this field blank, the Zyxel Device will use the welcome page of internal user agreement file.
Download	Click this to download an example external user agreement file for your reference.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving.

25.2.3 Custom Web Portal / User Agreement File Screen

Use this screen to upload the zipped custom web portal or user agreement files to the Zyxel Device. You can also download the custom files to your computer.

Click Configuration > Web Authentication and then select the Custom Web Portal File or Custom User Agreement File tab to display the screen.

Figure 397 Configuration > Web Authentication > Custom Web Portal File

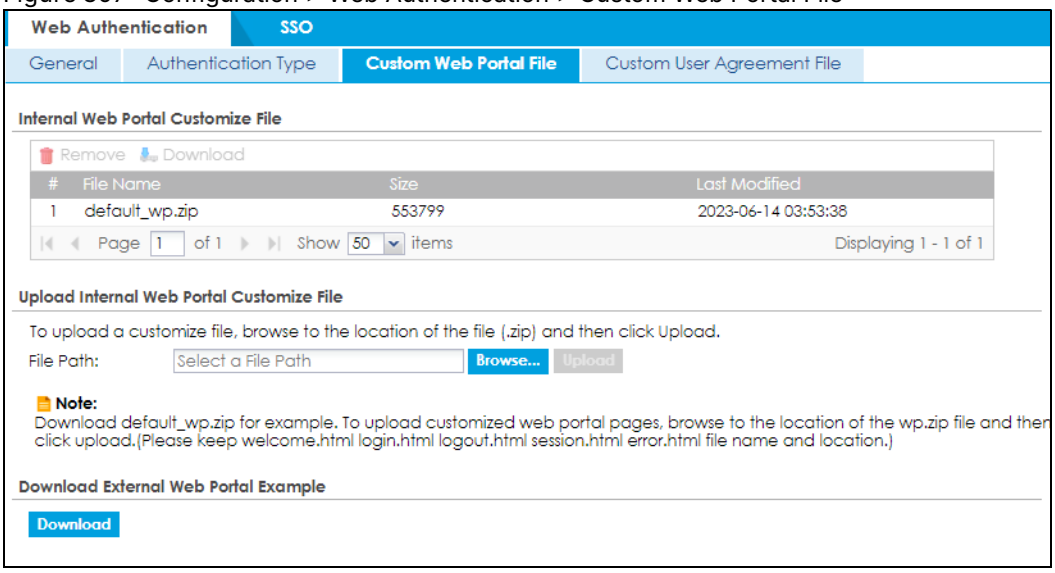
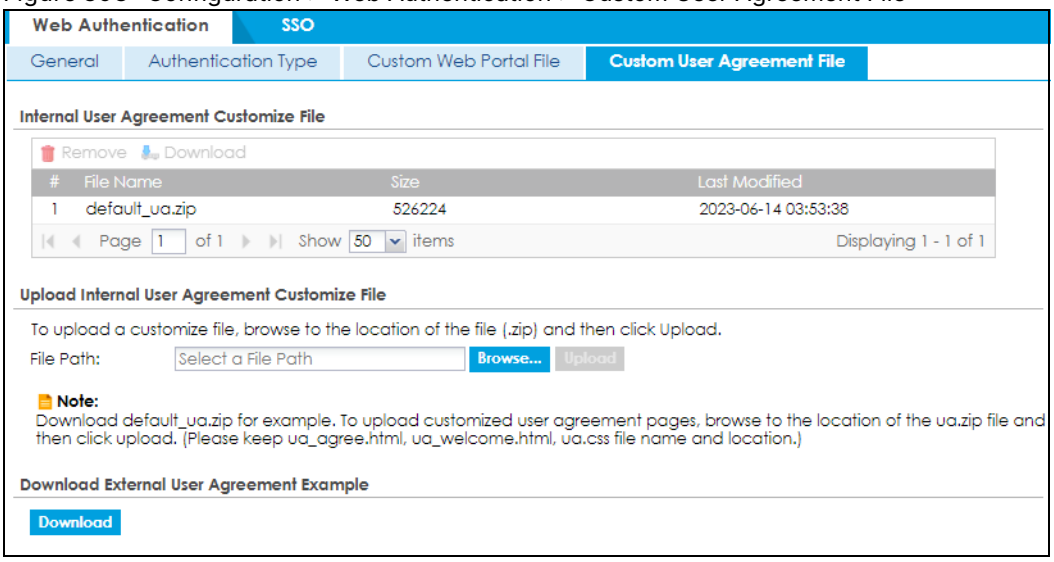


Figure 398 Configuration > Web Authentication > Custom User Agreement File



The following table describes the labels in this screen.

Table 170 Configuration > Web Authentication > Custom Web Portal / User Agreement File

LABEL	DESCRIPTION
Remove	Click a file's row to select it and click Remove to delete it from the Zyxel Device.
Download	Click a file's row to select it and click Download to save the zipped file to your computer.
#	This column displays the index number for each file entry. This field is a sequential value, and it is not associated with a specific entry.
File Name	This column displays the label that identifies a web portal or user agreement file.
Size	This column displays the size (in KB) of a file.
Last Modified	This column displays the date and time that the individual files were last changed or saved.
Browse / Upload	Click Browse... to find the zipped file you want to upload, then click the Upload button to put it on the Zyxel Device.
Download	Click this to download an example external web portal or user agreement file for your reference.

25.3 SSO Overview

The SSO (Single Sign-On) function integrates Domain Controller and Zyxel Device authentication mechanisms, so that users just need to log in once (single login) to get access to permitted resources.

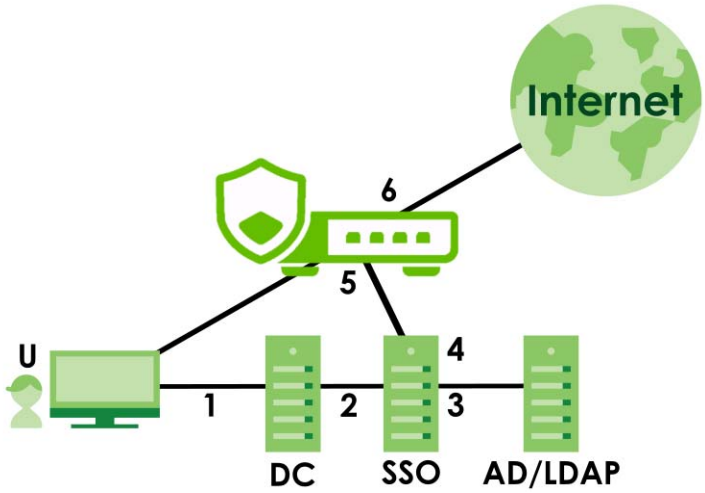
In the following figure, U user logs into a Domain Controller (DC) which passes the user's login credentials to the SSO agent. The SSO agent checks that these credentials are correct with the AD server, and if the AD server confirms so, the SSO then notifies the Zyxel Device to allow access for the user to the permitted resource (Internet access, for example).

Note: The Zyxel Device, the DC, the SSO agent and the AD server must all be in the same domain and be able to communicate with each other.

SSO does not support IPv6, LDAP or RADIUS; you must use it in an IPv4 network environment with Windows AD (Active Directory) authentication database.

You must enable Web Authentication in the Configuration > Web Authentication screen.

Figure 399 SSO Overview



U	User
DC	Domain Controller
SSO	Single Sign-On agent
AD	Active Directory

Install the SSO Agent on one of the following platforms:

- Windows 7 Professional (32-bit and 64-bit)
- Windows Server 2008 Enterprise (32-bit and 64-bit)
- Windows 2008 R2 (64-bit)
- Windows Server 2012 (64-bit)

25.4 SSO - Zyxel Device Configuration

This section shows what you have to do on the Zyxel Device in order to use SSO.

Table 171 Zyxel Device - SSO Agent Field Mapping

ZYXEL DEVICE		SSO	
SCREEN	FIELD	SCREEN	FIELD
Web Authentication > SSO	Listen Port	Agent Configuration Page > Gateway Setting	Gateway Port
Web Authentication > SSO	Primary Agent Port	Agent Configuration Page	Agent Listening Port
Object > User/Group > User > Add	Group Identifier	Agent Configuration Page > Configure LDAP/AD Server	Group Membership
Object > AAA Server > Active Directory > Add	Base DN	Agent Configuration Page > Configure LDAP/AD Server	Base DN
Object > AAA Server > Active Directory > Add	Bind DN	Agent Configuration Page > Configure LDAP/AD Server	Bind DN
Object > User/Group > User > Add	User Name	Agent Configuration Page > Configure LDAP/AD Server	Login Name Attribute
Object > AAA Server > Active Directory > Add	Server Address	Agent Configuration Page > Configure LDAP/AD Server	Server Address
Network > Interface > Ethernet > wan (IPv4)	IP address	Agent Configuration Page > Gateway Setting	Gateway IP

25.4.1 Configuration Overview

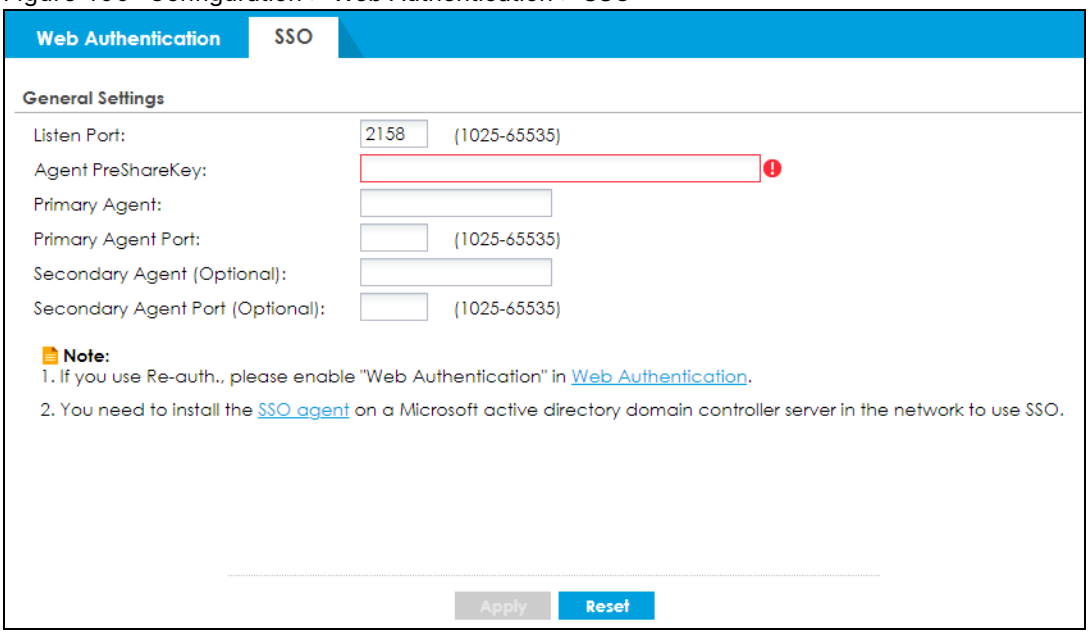
These are the screens you need to configure:

- Configure the Zyxel Device to Communicate with SSO on page 560
- Enable Web Authentication on page 561
- Create a Security Policy on page 563
- Configure User Information on page 564
- Configure an Authentication Method on page 564
- Configure Active Directory on page 565

25.4.2 Configure the Zyxel Device to Communicate with SSO

Use Configuration > Web Authentication > SSO to configure how the Zyxel Device communicates with the Single Sign-On (SSO) agent.

Figure 400 Configuration > Web Authentication > SSO



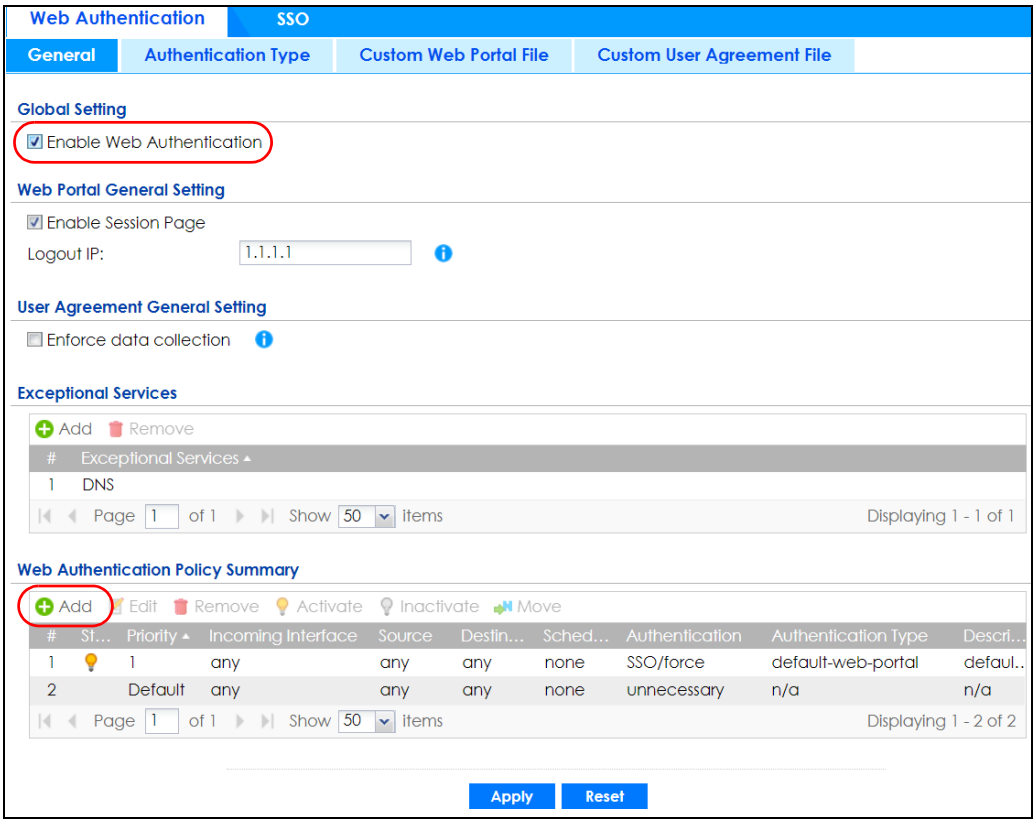
The following table gives an overview of the objects you can configure.

Table 172 Configuration > Web Authentication > SSO

LABEL	DESCRIPTION
Listen Port	The default agent listening port is 2158. If you change it on the Zyxel Device, then change it to the same number in the Gateway Port field on the SSO agent too. Type a number ranging from 1025 to 65535.
Agent PreShareKey	Type 8-32 single-byte characters, including 0-9a-zA_Z!"#$%&'()*+,-./:;<=>?@\^_' [] are not allowed. The Agent PreShareKey is used to encrypt communications between the Zyxel Device and the SSO agent.
Primary Agent	Type the IPv4 address of the SSO agent. The Zyxel Device and the SSO agent must be in the same domain and be able to communicate with each other.
Primary Agent Port	Type the same port number here as in the Agent Listening Port field on the SSO agent. Type a number ranging from 1025 to 65535.
Secondary Agent Address (Optional)	Type the IPv4 address of the backup SSO agent if there is one. The Zyxel Device and the backup SSO agent must be in the same domain and be able to communicate with each other.
Secondary Agent Port (Optional)	Type the same port number here as in the Agent Listening Port field on the backup SSO agent if there is one. Type a number ranging from 1025 to 65535.
Apply	Click this button to save your changes to the Zyxel Device.
Reset	Click this button to return the screen to its last-saved settings

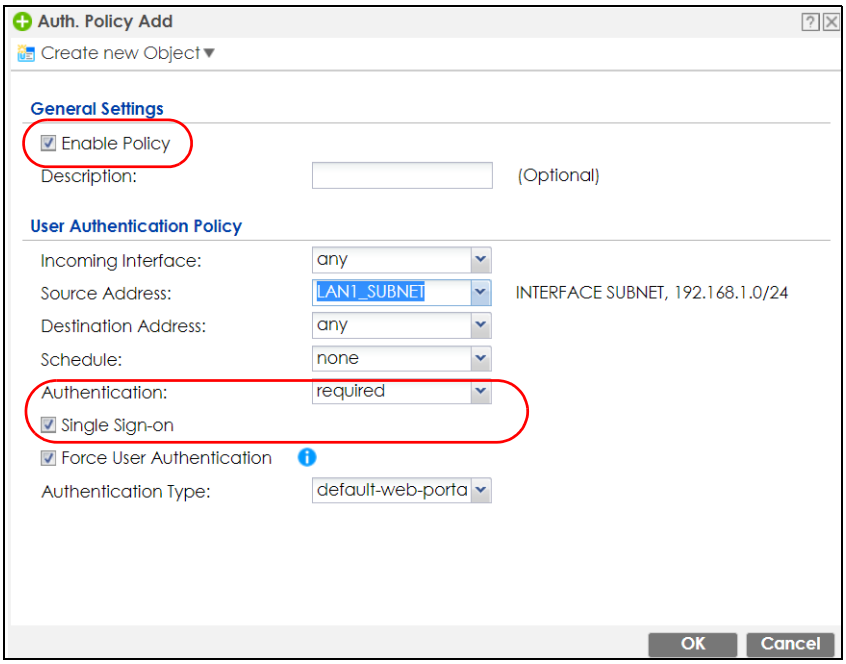
25.4.3 Enable Web Authentication

Enable Web Authentication and add a web authentication policy.



Make sure you select Enable Policy, Single Sign-On and choose required in Authentication.

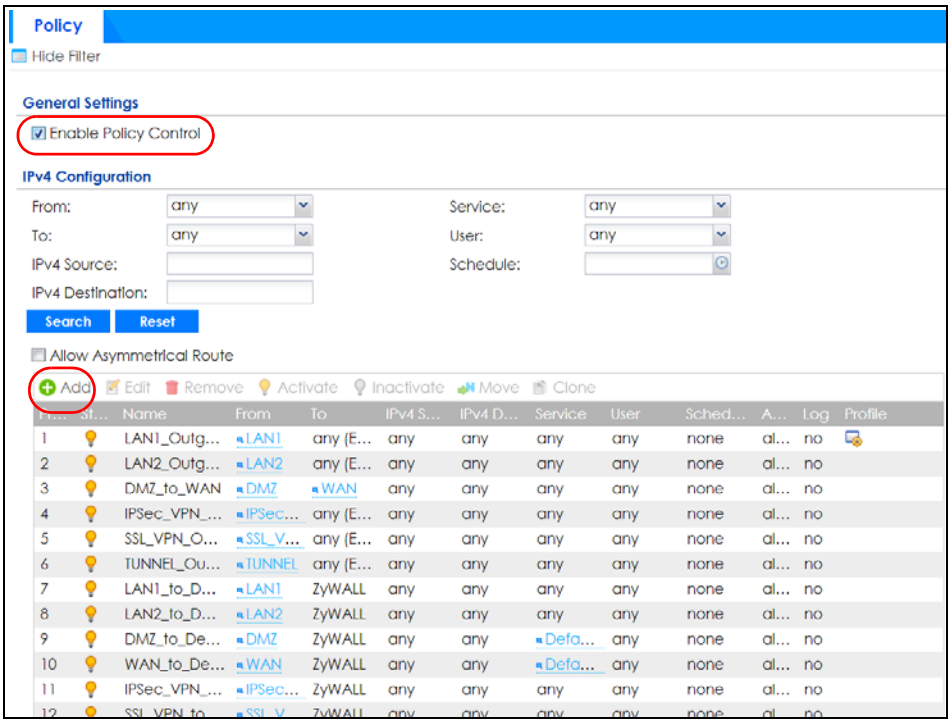
Do NoT select any as the source address unless you want all incoming connections to be authenticated!



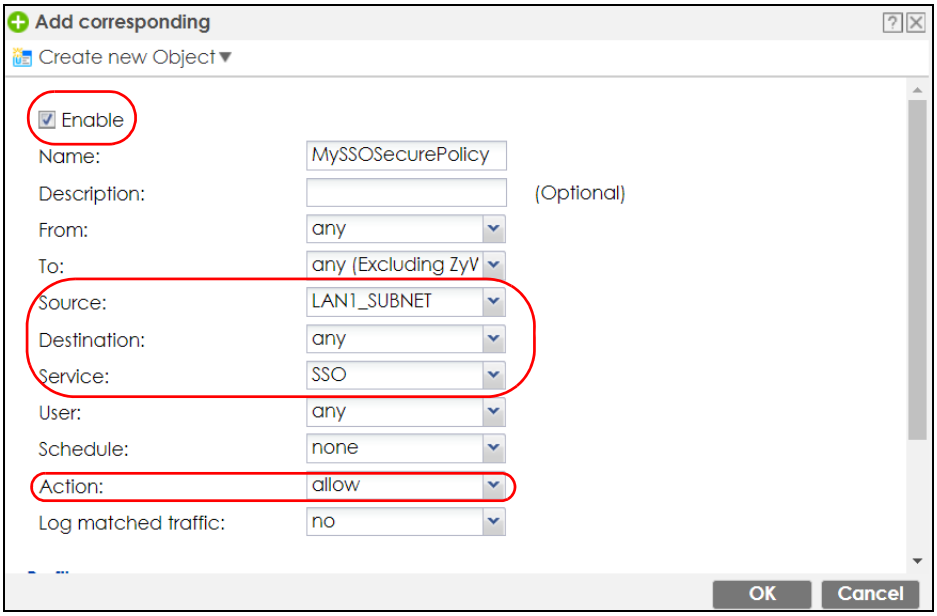
See Table 166 on page 542 and Table 167 on page 546 for more information on configuring these screens.

25.4.4 Create a Security Policy

Configure a Security Policy for SSO traffic source and destination direction in order to prevent the security policy from blocking this traffic. Go to Configuration > Security Policy > Policy Control and add a new policy if a default one does not cover the SSO web authentication traffic direction.

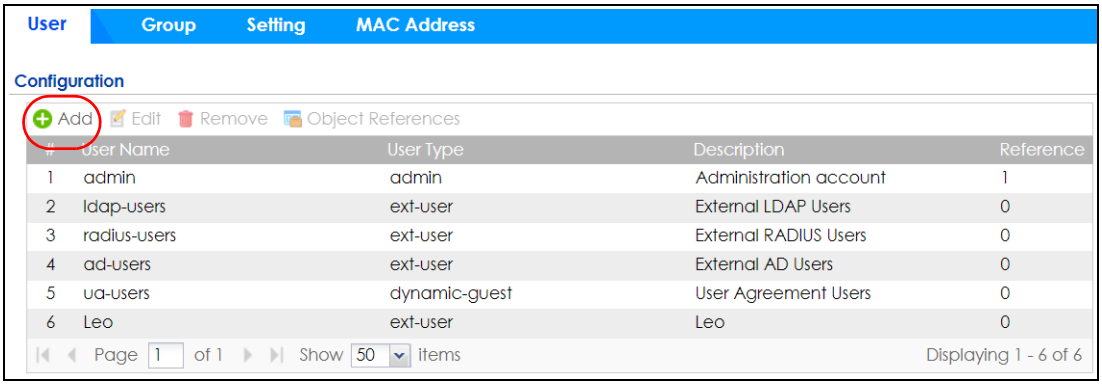


Configure the fields as shown in the following screen. Configure the source and destination addresses according to the SSO web authentication traffic in your network.

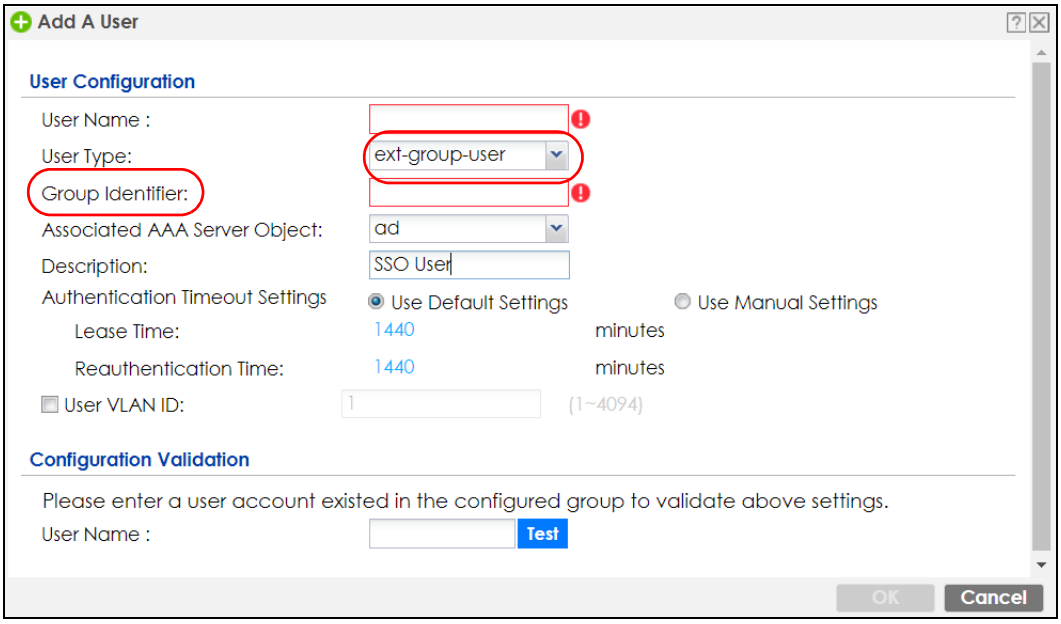


25.4.5 Configure User Information

Configure a User account of the ext-group-user type.

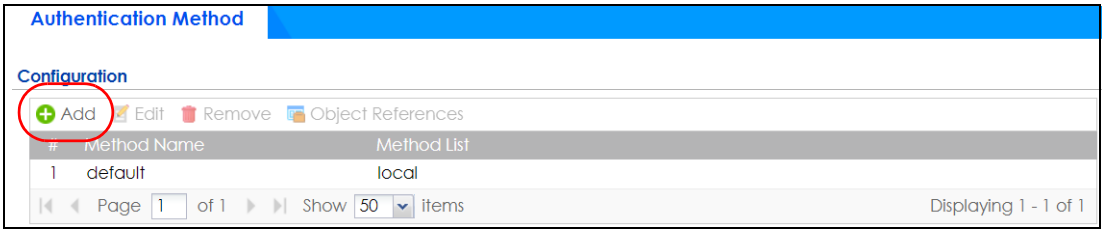


Configure Group Identifier to be the same as Group Membership on the SSO agent.

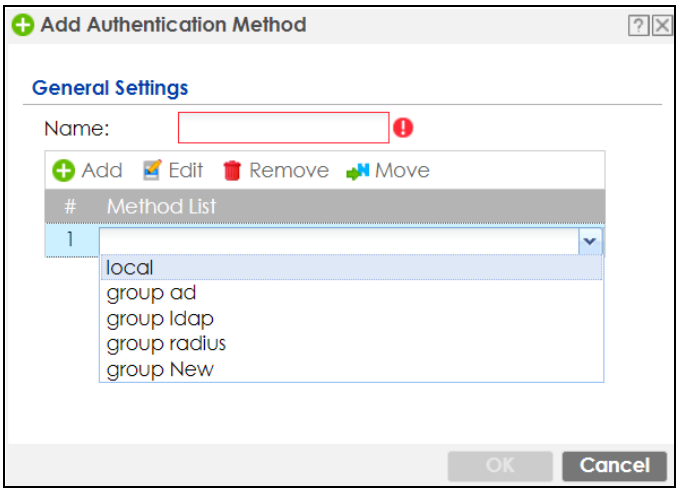


25.4.6 Configure an Authentication Method

Configure Active Directory (AD) for authentication with SSO.

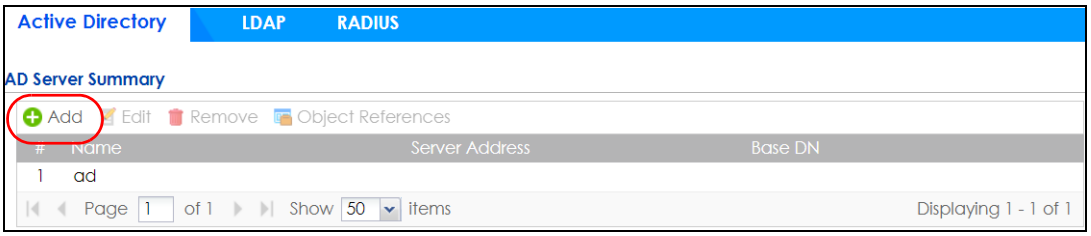


Choose group ad as the authentication server for SSO.

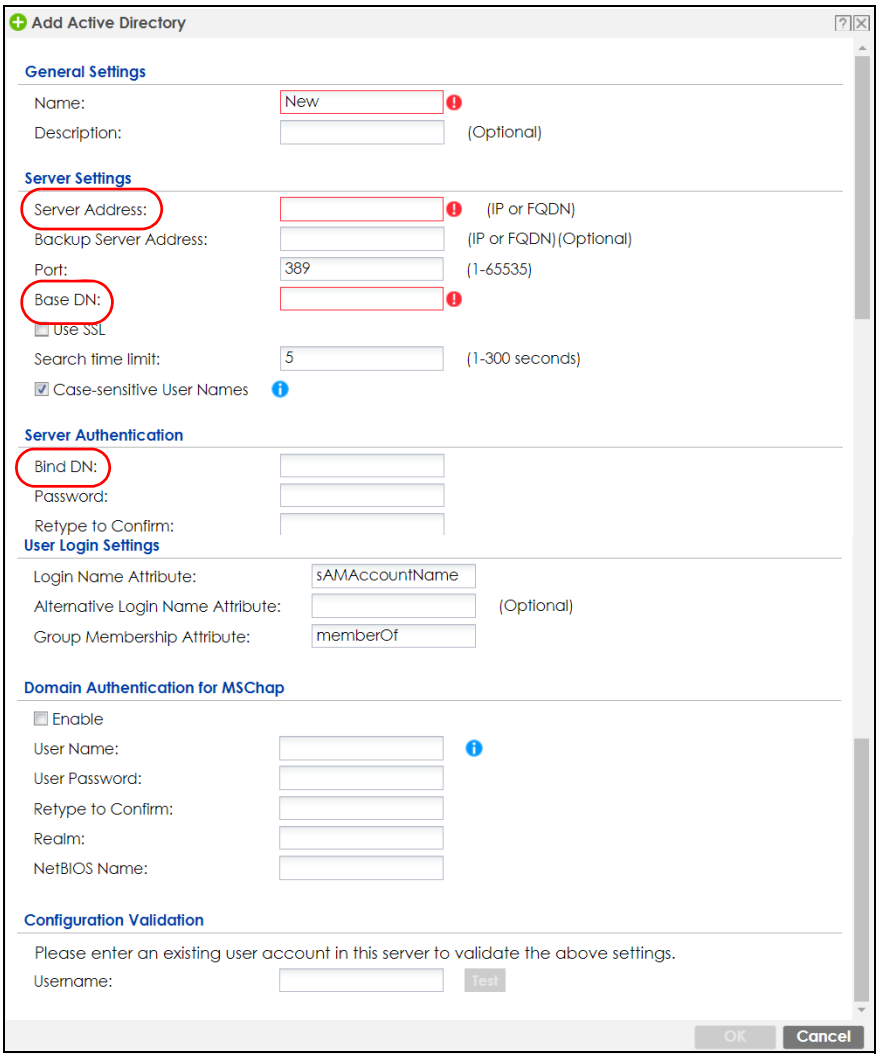


25.4.7 Configure Active Directory

You must configure an Active Directory (AD) server in AAA Setup to be the same as AD configured on the SSO agent.



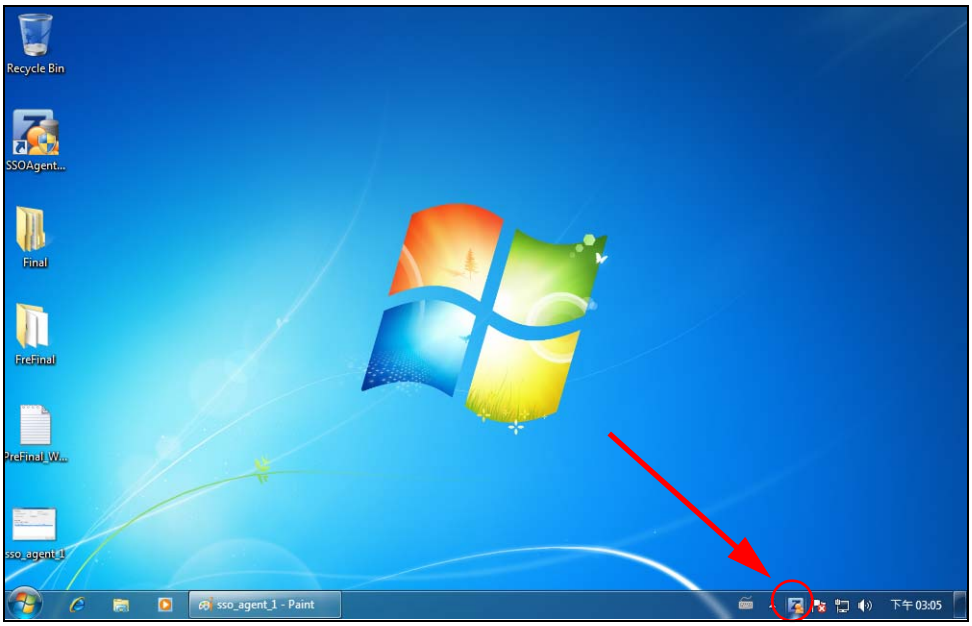
The default AD server port is 389. If you change this, make sure you make the same changes on the SSO. Configure the Base DN exactly the same as on the Domain Controller and SSO. Bind DN is a user name and password that allows the Zyxel Device to join the domain with administrative privileges. It is a required field.



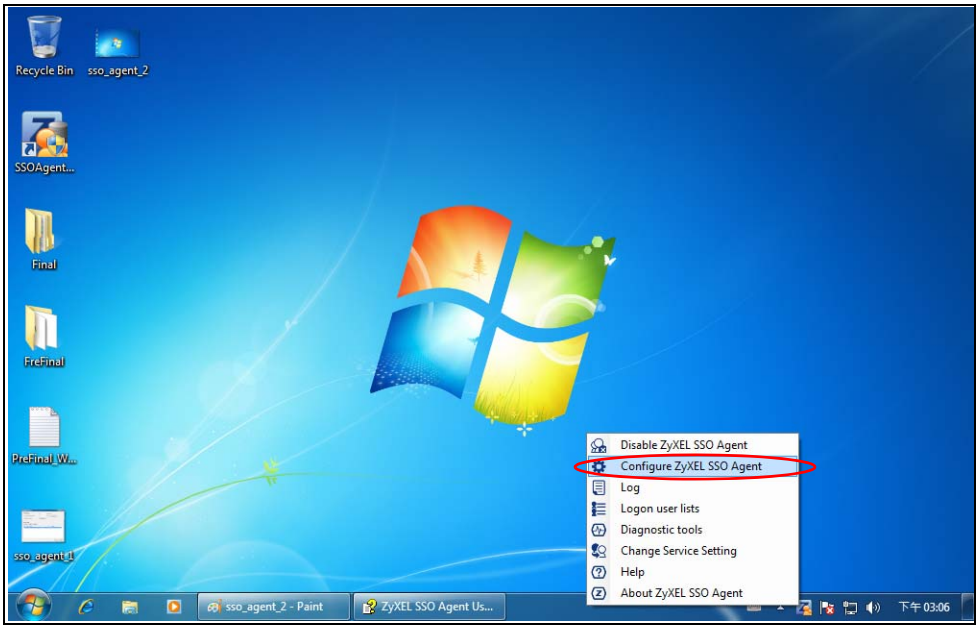
25.5 SSO Agent Configuration

This section shows what you have to do on the SSO agent in order to work with the Zyxel Device.

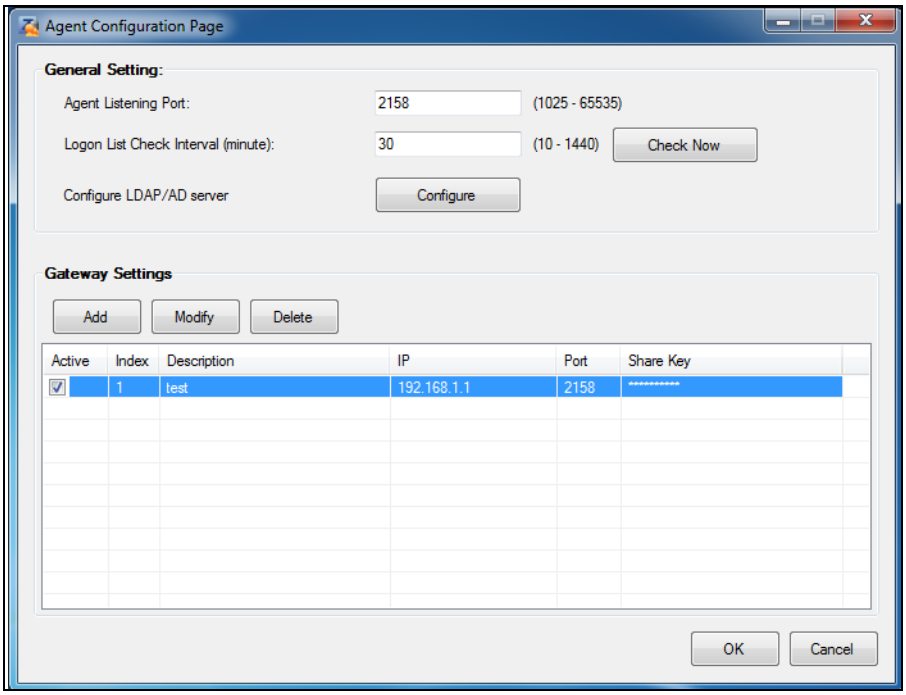
After you install the SSO agent, you will see an icon in the system tray (bottom right of the screen)



Right-click the SSO icon and select Configure Zyxel SSO Agent.

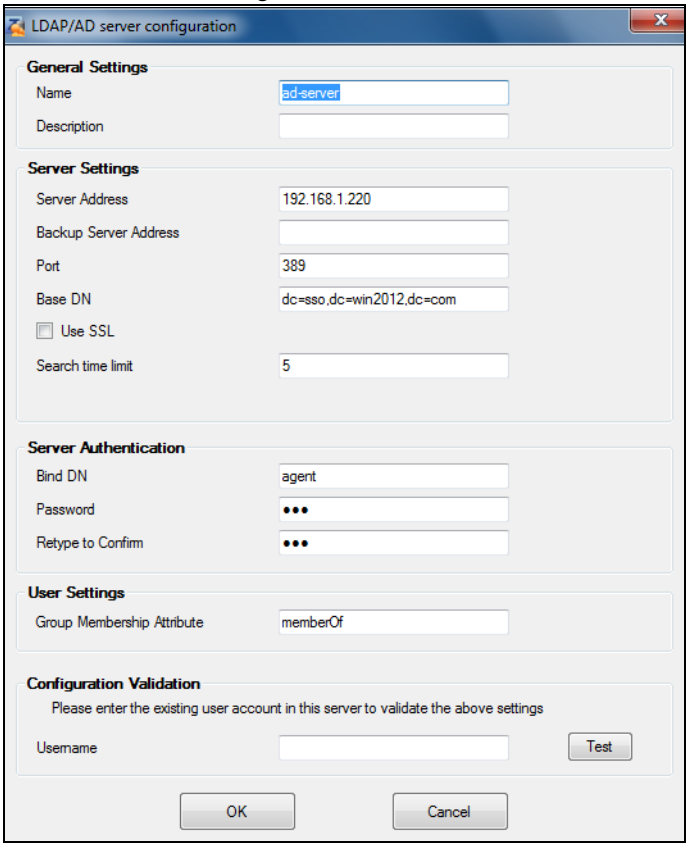


Configure the Agent Listening Port, AD server exactly as you have done on the Zyxel Device. Add the Zyxel Device IP address as the Gateway. Make sure the Zyxel Device and SSO agent are able to communicate with each other.

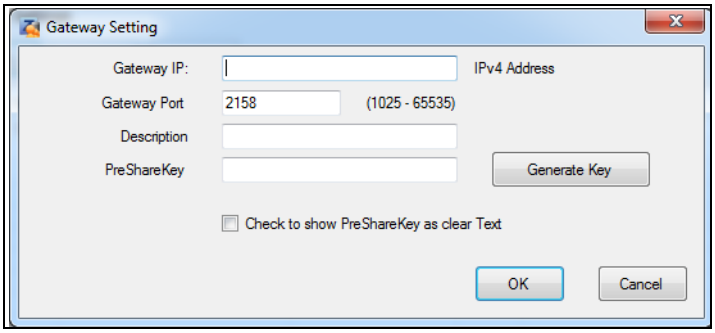


Configure the Server Address, Port, Base DN, Bind DN, Login Name Attribute and Group Membership for the AD server settings exactly as you have done on the Zyxel Device. Group Membership is called Group Identifier on the Zyxel Device.

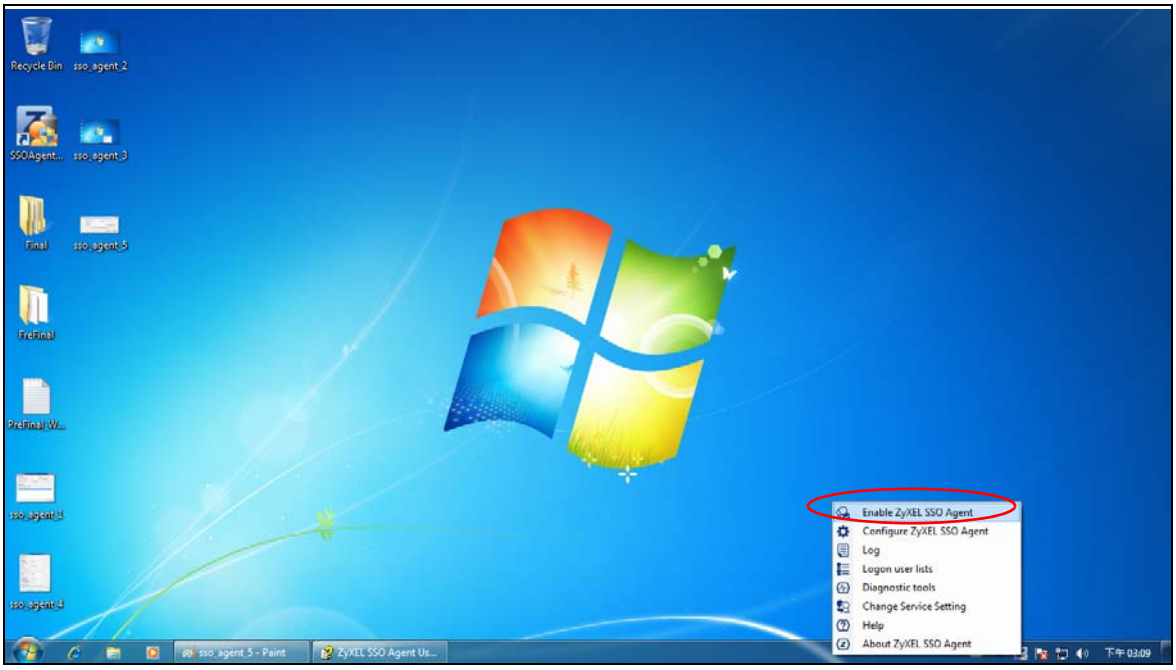
LDAP/AD Server Configuration



Configure the Gateway IP address, Gateway Port and PreShareKey exactly as you have done in the Zyxel Device Configuration > Web Authentication > SSO screen. If you want to use Generate Key to have the SSO create a random password, select Check to show PreShareKey as clear Text so as to see the password, then copy and paste it to the Zyxel Device.



After all SSO agent configurations are done, right-click the SSO icon in the system tray and select Enable Zyxel SSO Agent.



CHAPTER 26
Security Policy

26.1 Overview

A security policy is a template of security settings that can be applied to specific traffic at specific times. The policy can be applied:

- to a specific direction of travel of packets (from / to)
- to a specific source and destination address objects
- to a specific type of traffic (services)
- to a specific user or group of users
- at a specific schedule

Note: Make sure to choose the correct direction of traffic for the security policy.

The policy can be configured:

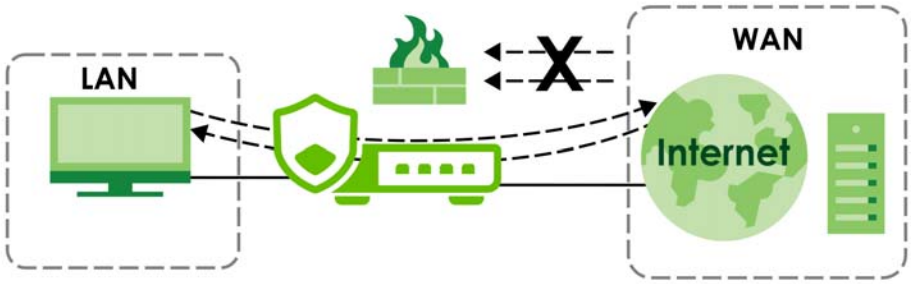
- to allow or deny traffic that matches the criteria above
- send a log or alert for traffic that matches the criteria above
- to apply the actions configured in the profiles to traffic that matches the criteria above

Note: Security policies can be applied to both IPv4 and IPv6 traffic.

The security policies can also limit the number of user sessions.

The following example shows the Zyxel Device's default security policies behavior for a specific direction of travel of packets. WAN to LAN traffic and how stateful inspection works. A LAN user can initiate a Telnet session from within the LAN zone and the Zyxel Device allows the response. However, the Zyxel Device blocks incoming Telnet traffic initiated from the WAN zone and destined for the LAN zone.

Figure 401 Default Directional Security Policy Example



26.2 What You Can Do in this Chapter

- Use the Security Policy Control screens (Section 26.3 on page 572) to enable or disable policies, asymmetrical routes, and manage and configure policies.
- Use the Anomaly Detection and Prevention (ADP) screens (Section 26.4 on page 587) to detect traffic with protocol anomalies and take appropriate action.
- Use the Session Control screens (see Section 26.5 on page 596) to limit the number of concurrent NAT/security policies traffic sessions a client can use.

26.2.1 What You Need to Know

Stateful Inspection

The Zyxel Device uses stateful inspection in its security policies. The Zyxel Device restricts access by screening data packets against defined access rules. It also inspects sessions. For example, traffic from one zone is not allowed unless it is initiated by a computer in another zone first.

Zones

A zone is a group of interfaces. Group the Zyxel Device's interfaces into different zones based on your needs. You can configure security policies for data passing between zones or even between interfaces.

Default Directional Security Policy Behavior

Security Policies can be grouped based on the direction of travel of packets to which they apply. Here is the The Zyxel Device has default Security Policy behavior for traffic going through the Zyxel Device in various directions.

Table 173 Directional Security Policy Behavior

FROM ZONE TO ZONE	BEHAVIOR
From any to Device	DHCP traffic from any interface to the Zyxel Device is allowed.
From LAN1 to any (other than the Zyxel Device)	Traffic from the LAN1 to any of the networks connected to the Zyxel Device is allowed.
From LAN2 to any (other than the Zyxel Device)	Traffic from the LAN2 to any of the networks connected to the Zyxel Device is allowed.
From LAN1 to Device	Traffic from the LAN1 to the Zyxel Device itself is allowed.
From LAN2 to Device	Traffic from the LAN2 to the Zyxel Device itself is allowed.
From WAN to Device	The default services listed in To-Device Policies are allowed from the WAN to the Zyxel Device itself. All other WAN to Zyxel Device traffic is dropped.
From any to any	Traffic that does not match any Security policy is dropped. This includes traffic from the WAN to any of the networks behind the Zyxel Device. This also includes traffic to or from interfaces that are not assigned to a zone (extra-zone traffic).

To-Device Policies

Policies with Device as the To Zone apply to traffic going to the Zyxel Device itself. By default:

- The Security Policy allows only LAN, or WAN computers to access or manage the Zyxel Device.

- The Zyxel Device allows DHCP traffic from any interface to the Zyxel Device.
- The Zyxel Device drops most packets from the WAN zone to the Zyxel Device itself and generates a log except for AH, ESP, GRE, HTTPS, IKE, NATT.

When you configure a Security Policy rule for packets destined for the Zyxel Device itself, make sure it does not conflict with your service control rule. The Zyxel Device checks the security policy before the service control rules for traffic destined for the Zyxel Device.

A From Any To Device direction policy applies to traffic from an interface which is not in a zone.

Global Security Policies

Security Policies with from any and/or to any as the packet direction are called global Security Policies. The global Security Policies are the only Security Policies that apply to an interface that is not included in a zone. The from any policies apply to traffic coming from the interface and the to any policies apply to traffic going to the interface.

Security Policy Rule Criteria

The Zyxel Device checks the schedule, user name (user's login name on the Zyxel Device), source IP address and object, destination IP address and object, IP protocol type of network traffic (service) and Security Service profile criteria against the Security Policies (in the order you list them). When the traffic matches a policy, the Zyxel Device takes the action specified in the policy.

User Specific Security Policies

You can specify users or user groups in Security Policies. For example, to allow a specific user from any computer to access a zone by logging in to the Zyxel Device, you can set up a policy based on the user name only. If you also apply a schedule to the Security Policy, the user can only access the network at the scheduled time. A user-authentication Security Policy is activated whenever the user logs in to the Zyxel Device and will be disabled after the user logs out of the Zyxel Device.

Session Limits

Accessing the Zyxel Device or network resources through the Zyxel Device requires a NAT session and corresponding Security Policy session. Peer to peer applications, such as file sharing applications, may use a large number of NAT sessions. A single client could use all of the available NAT sessions and prevent others from connecting to or through the Zyxel Device. The Zyxel Device lets you limit the number of concurrent NAT/Security Policy sessions a client can use.

26.3 The Security Policy Screen

Asymmetrical Routes

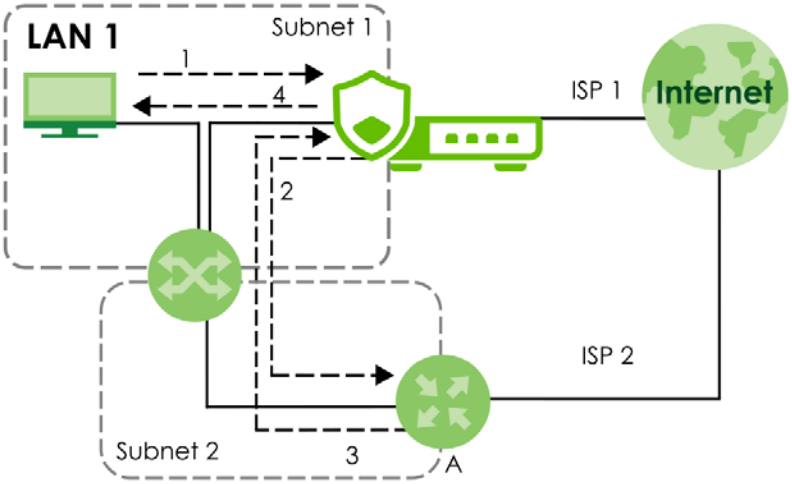
If an alternate gateway on the LAN has an IP address in the same subnet as the Zyxel Device's LAN IP address, return traffic may not go through the Zyxel Device. This is called an asymmetrical or "triangle" route. This causes the Zyxel Device to reset the connection, as the connection has not been acknowledged.

You can have the Zyxel Device permit the use of asymmetrical route topology on the network (not reset the connection). However, allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the Zyxel Device. A better solution is to use virtual interfaces to put the Zyxel Device and the backup gateway on separate subnets. Virtual interfaces allow you to partition your network into logical sections over the same interface. See the chapter about interfaces for more information.

By putting LAN 1 and the alternate gateway (A in the figure) in different subnets, all returning network traffic must pass through the Zyxel Device to the LAN. The following steps and figure describe such a scenario.

1. A computer on the LAN1 initiates a connection by sending a SYN packet to a receiving server on the WAN.
2. The Zyxel Device reroutes the packet to gateway A, which is in Subnet 2.
3. The reply from the WAN goes to the Zyxel Device.
4. The Zyxel Device then sends it to the computer on the LAN1 in Subnet 1.

Figure 402 Using Virtual Interfaces to Avoid Asymmetrical Routes



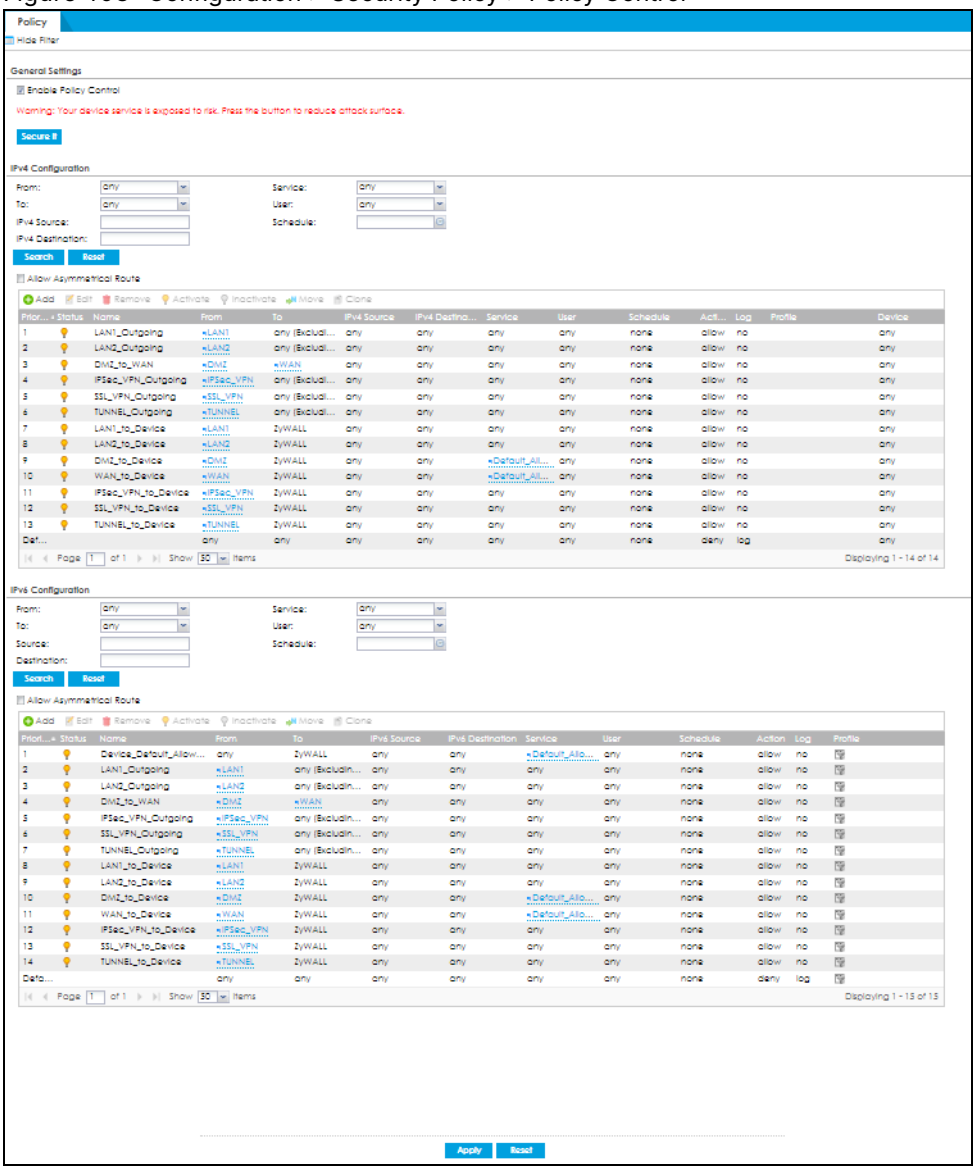
26.3.1 Configuring the Security Policy Control Screen

Click Configuration > Security Policy > Policy Control to open the Security Policy screen. Use this screen to enable or disable the Security Policy and asymmetrical routes, set a maximum number of sessions per host, and display the configured Security Policies. Specify from which zone packets come and to which zone packets travel to display only the policies specific to the selected direction. Note the following.

- Besides configuring the Security Policy, you also need to configure NAT rules to allow computers on the WAN to access LAN devices.
- The Zyxel Device applies NAT (Destination NAT) settings before applying the Security Policies. So for example, if you configure a NAT entry that sends WAN traffic to a LAN IP address, when you configure a corresponding Security Policy to allow the traffic, you need to set the LAN IP address as the destination.
- The ordering of your policies is very important as policies are applied in sequence.

The following screen shows the Security Policy summary screen.

Figure 403 Configuration > Security Policy > Policy Control



The following table describes the labels in this screen.

Table 174 Configuration > Security Policy > Policy Control

LABEL	DESCRIPTION
Show Filter/Hide Filter	Click Show Filter to display IPv4 and IPv6 (if enabled) security policy search filters.
General Settings	Enable or disable the Security Policy feature on the Zyxel Device.
Enable Policy Control	Select this to activate Security Policy on the Zyxel Device to perform access control.
Secure it	You have a WAN_to_Device rule that allows traffic such as HTTP, HTTPS, SSL and so on to access to your Zyxel Device from any IPv4 source on the WAN. Click this button to secure WAN_to_Device traffic. See Section 26.3.2 on page 576 for more information.
IPv4 / IPv6 Configuration	Use IPv4 / IPv6 search filters to find specific IPv4 and IPv6 (if enabled) security policies based on direction, application, user, source, destination and/or schedule.

Table 174 Configuration > Security Policy > Policy Control (continued)

LABEL	DESCRIPTION
From / To	Select a zone to view all security policies from a particular zone and/or to a particular zone. any means all zones.
IPv4 / IPv6 Source	Type an IPv4 or IPv6 IP address to view all security policies based on the IPv4 / IPv6 source address object used. • An IPv4 IP address is written as four integer blocks separated by periods. This is an example IPv4 address: 172.16.6.7. • 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.
IPv4 / IPv6 Destination	Type an IPv4 or IPv6 IP address to view all security policies based on the IPv4 / IPv6 destination address object used. • An IPv4 IP address is written as four integer blocks separated by periods. This is an example IPv4 address: 172.16.6.7. • 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.
Service	View all security policies based the service object used.
User	View all security policies based on user or user group object used.
Schedule	View all security policies based on the schedule object used.
IPv4/IPv6 Policy Management	Use the following items to manage IPv4 and IPv6 policies.
Allow Asymmetrical Route	If an alternate gateway on the LAN has an IP address in the same subnet as the Zyxel Device's LAN IP address, return traffic may not go through the Zyxel Device. This is called an asymmetrical or "triangle" route. This causes the Zyxel Device to reset the connection, as the connection has not been acknowledged. Select this checkbox to have the Zyxel Device permit the use of asymmetrical route topology on the network (not reset the connection). Note: Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the Zyxel Device. A better solution is to use virtual interfaces to put the Zyxel Device and the backup gateway on separate subnets.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The 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.
Move	To change a policy's position in the numbered list, select the policy and click Move to display a field to type a number for where you want to put that policy and press [ENTER] to move the policy to the number that you typed. The ordering of your policies is important as they are applied in order of their numbering.
Clone	Use Clone to create a new entry by modifying an existing one. • Select an existing entry. • Click Clone, type a number where the new entry should go and then press [ENTER]. • A configuration copy of the selected entry pops up. You must at least change the name as duplicate entry names are not allowed.
The following read-only fields summarize the policies you have created that apply to traffic traveling in the selected packet direction.	

Table 174 Configuration > Security Policy > Policy Control (continued)

LABEL	DESCRIPTION
Priority	This is the position of your Security Policy in the global policy list (including all through-Zyxel Device and to-Zyxel Device policies). The ordering of your policies is important as policies are applied in sequence. Default displays for the default Security Policy behavior that the Zyxel Device performs on traffic that does not match any other Security Policy.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This is the name of the Security policy.
From / To	This is the direction of travel of packets. Select from which zone the packets come and to which zone they go. Security Policies are grouped based on the direction of travel of packets to which they apply. For example, from LAN to LAN means packets traveling from a computer or subnet on the LAN to either another computer or subnet on the LAN. From any displays all the Security Policies for traffic going to the selected To Zone. To any displays all the Security Policies for traffic coming from the selected From Zone. From any to any displays all of the Security Policies. To ZyWALL policies are for traffic that is destined for the Zyxel Device and control which computers can manage the Zyxel Device.
IPv4 / IPv6 Source	This displays the IPv4 / IPv6 source address object, including geographic address and FQDN (group) objects, to which this Security Policy applies.
IPv4 / IPv6 Destination	This displays the IPv4 / IPv6 destination address object, including geographic address and FQDN (group) objects, to which this Security Policy applies.
Service	This displays the service object to which this Security Policy applies.
User	This is the user name or user group name to which this Security Policy applies.
Schedule	This field tells you the schedule object that the policy uses. none means the policy is active at all times if enabled.
Action	This field displays whether the Security Policy silently discards packets without notification (deny), permits the passage of packets (allow) or drops packets with notification (reject)
Log	Select whether to have the Zyxel Device generate a log (log), log and alert (log alert) or not (no) when the policy is matched to the criteria listed above.
Profile	This field shows you which Security Service profiles (content filter, anti-spam) apply to this Security policy. Click an applied Security Service profile icon to edit the profile directly.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

26.3.2 The Security Check for Web Interface Screen

Use this screen to configure settings to secure your Zyxel Device. You can configure:

- Secure SSL access from the Internet to the Zyxel Device.
- Secure SSL access from the Internet to the network behind the Zyxel Device.
- The default port that IPSec VPN clients use to retrieve VPN rule settings from the Zyxel Device.
- The default port for two-factor authentication for VPN clients to access the network behind the Zyxel Device.

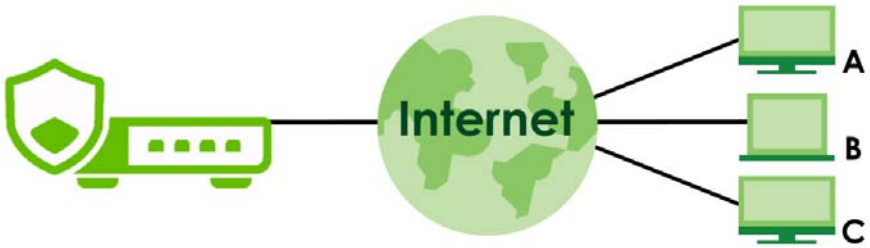
Secure SSL Access from the Internet to the Zyxel Device

You can configure up to 3 trusted computers to access the Zyxel Device using secure SSL. The default HTTPS SSL port is 443. If you change this, remote connections from the Internet must use this port. For example, if you change this to port 8800 and the Zyxel Device is using IP address 1.1.1.1, then remote users must use https://1.1.1.1:8800.

The following figure shows that A, B and C can connect to the Zyxel Device to access the Zyxel Device web configurator for remote management.

Configure a new port between 1024 to 65535 that is not in use by other services.

Figure 404 Secure SSL Access Example

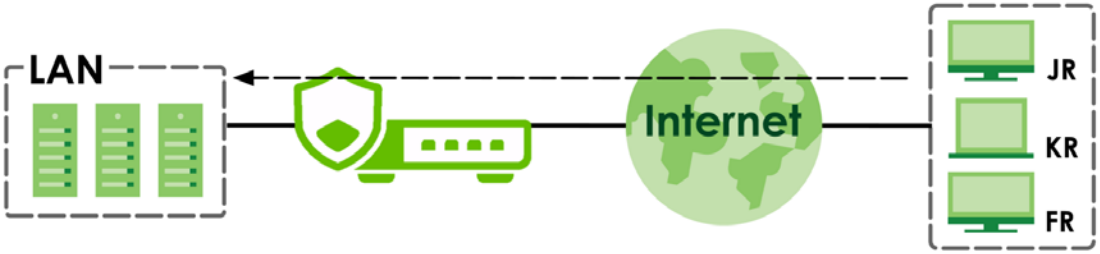


Secure SSL VPN Access from the Internet to the Network Behind the Zyxel Device

The default SSL VPN port is 443. If you change the default SSL VPN port on the Zyxel Device, make sure to make the same change to SecuExtender, the SSL VPN client software. Configure a new port between 1024 to 65535 that is not in use by other services.

You can also restrict SSL VPN access to up to 3 locations on the Internet.

Figure 405 Secure SSL VPN Access Example



The table below describes the abbreviations used in the figure.

Table 175 Countries Abbreviations

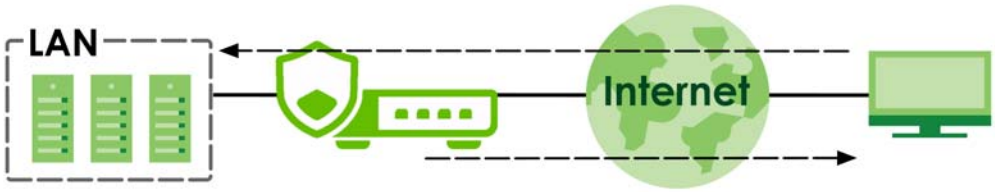
ABBREVIATION	COUNTRY
JP	Japan
KR	Korea
FR	France

Change the Default IPSec VPN Provisioning Port

Change the default port that IPSec VPN clients use to retrieve VPN rule settings from the Zyxel Device. The default is 443 which is already in use for remote management by default. If you change the default IPSec VPN port on the Zyxel Device, make sure to make the same change to the Zyxel IPSec VPN client.

Configure a new port between 1024 to 65535 that is not in use by other services.

Figure 406 IPSec VPN Provisioning Example



Note: The remote management port, the SSL VPN port and the IPSec VPN port all use 443 by default. If you do not change the default ports, then only 3 connections of the remote management and SSL VPN will be allowed at one time.

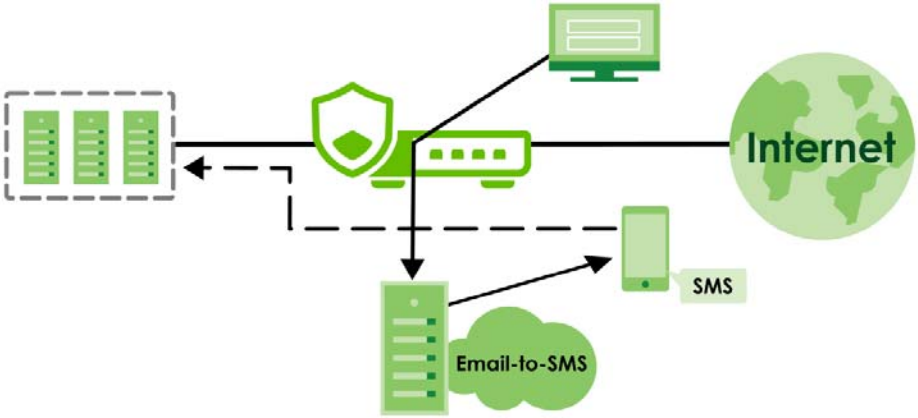
Change the Default Port for Two-Factor VPN Access Authentication

Change the default port for two-factor authentication for VPN clients to access the network behind the Zyxel Device. VPN clients do not need to change the port number on their devices, because the link to access the network behind the Zyxel Devices will contain the new port number. For example, if you change this to port 8008 and the link is using a.b.c.d, then VPN clients will see this link in their email or SMS to retrieve settings: https://a.b.c.d:8008.

You can also change this port in Object > Auth. Method > Two-factor Authentication > VPN Access. See Section 30.8.4 on page 738 for more information on two-factor authentication.

Configure a new port between 1024 to 65535 that is not in use by other services.

Figure 407 Two-Factor Authentication Example



Overall Port Configuration Example

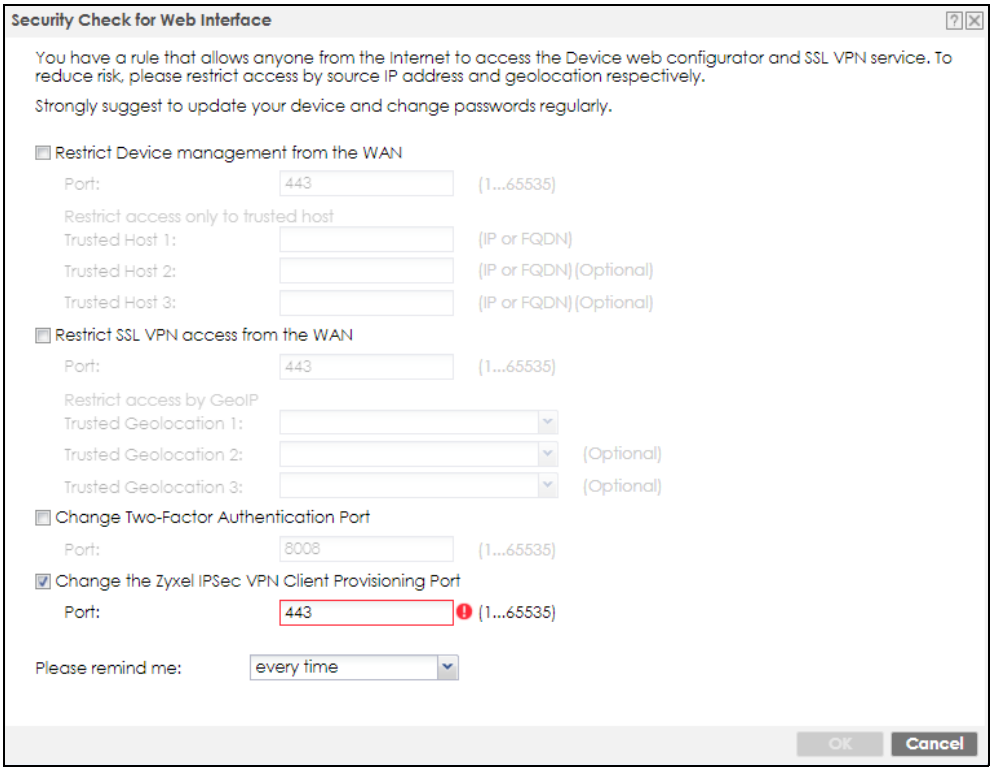
Below is an example of configuring these ports to avoid port conflict.

Table 176 Port Configuration Example

REMOTE MANAGEMENT	SSL VPN	IPSEC VPN PROVISIONING	TWO-FACTOR VPN ACCESS AUTHENTICATION
8800	8080	443 (default)	8008

Click the Secure It button to show the following screen.

Figure 408 Configuration > Security Policy > Policy Control > Secure It > Security Check for Web Interface



The following table describes the labels in this screen.

Table 177 Security Check for Web Interface

LABEL	DESCRIPTION
Allow secure remote management from WAN	Select this to allow access to the Zyxel Device remotely only from specified IP addresses or Fully Qualified Domain Names (FQDNs), such as 1.1.1.1 or www.zyxel.com. See Section on page 577 for more information.
Port	Configure a new port between 1024 to 65535 to use it to access the web configurator. Do not use a port number that has been used. For example, use https://1.1.1.1:8800 if you changed the default HTTPS port to 8800.
Trusted Host 1-3	Configure the IP addresses or FQDNs that are allowed to access the Zyxel Device.

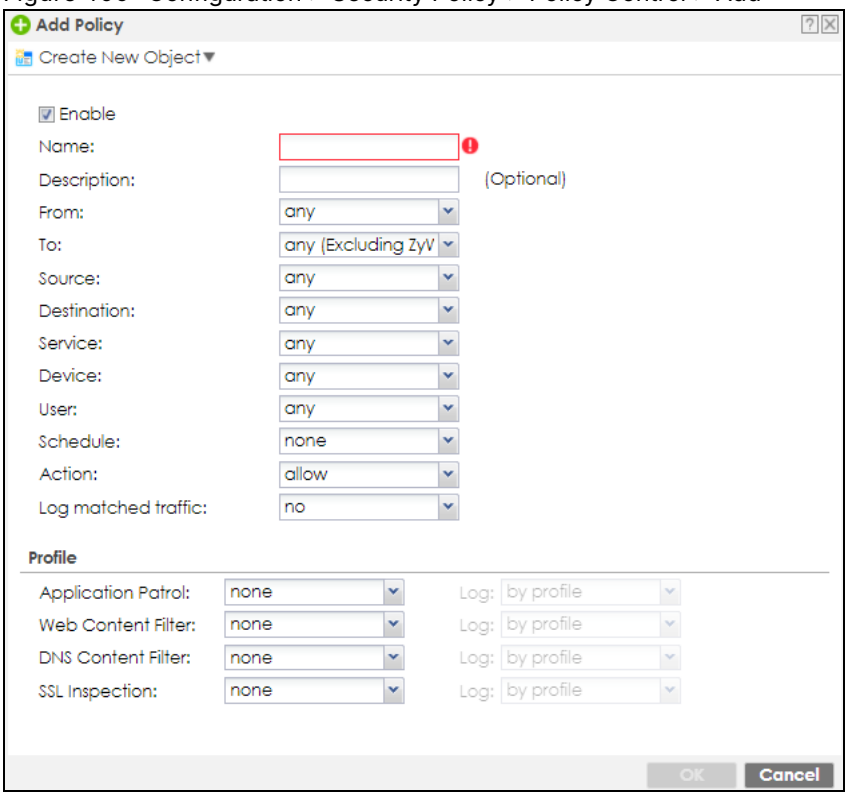
Table 177 Security Check for Web Interface (continued)

LABEL	DESCRIPTION
Allow SSL VPN access from WAN	Select this to allow SSL VPN clients to access the Zyxel Device only from specified regions. See Section on page 577 for more information.
Port	Configure a new port between 1024 to 65535 to use it to access the web configurator using SSL VPN. Do not use a port number that has been used. The port you configure here must be the same as the port you use in SecuExtender. See Section on page 577 for more information on SecuExtender.
Trusted Geolocation 1-3	Select the regions that are allowed to access the Zyxel Device from the drop-down list box.
Change Two-Factor Authentication Port	Select this to change the port VPN clients use to access the Zyxel Device LAN with two-factor authentication. See Section on page 578 for more information. Configure a new port between 1024 to 65535. Do not use a port number that has been used.
Change Zyxel IPSec VPN Client Provisioning Port	Select this to change the port IPSec VPN clients use to retrieve VPN rule settings from the Zyxel Device. See Section on page 578 for more information. Configure a new port between 1024 to 65535. Do not use a port number that has been used. The port you configure here must be the same as the port you use when logging in as a Zyxel IPSec VPN client.
Please remind me	Select how often to display the screen from the drop-down list box.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving your changes.

26.3.3 The Security Policy Control Add/Edit Screen

In the Security Policy Control screen, click the Edit or Add icon to display the Security Policy Edit or Add screen.

Figure 409 Configuration > Security Policy > Policy Control > Add



The following table describes the labels in this screen.

Table 178 Configuration > Security Policy > Policy Control > Add

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable	Select this checkbox to activate the Security policy.
Name	Type a name with 1 to 30 single-byte characters to identify the policy, including a-zA-Z. 0-9!"#$%&'()*+,-./:;<=>?@[\]^_'{|} and spaces are not allowed.
Description	Enter a descriptive name of 1 to 63 single-byte characters for the Policy, including spaces and 0-9a-zA-Z!"#$%()*+,-/:;=?@_ &.<>[\]^'{|} are not allowed.
From To	For through-Zyxel Device policies, select the direction of travel of packets to which the policy applies. any means all interfaces. Device means packets destined for the Zyxel Device itself.
Source	Select an IPv4 / IPv6 address or address group object, including geographic address and FQDN (group) objects, to apply the policy to traffic coming from it. Select any to apply the policy to all traffic coming from IPv4 / IPv6 addresses.
Destination	Select an IPv4 / IPv6 address or address group, including geographic address and FQDN (group) objects, to apply the policy to traffic going to it. Select any to apply the policy to all traffic going to IPv4 / IPv6 addresses.
Service	Select a service or service group from the drop-down list box.

Table 178 Configuration > Security Policy > Policy Control > Add (continued)

LABEL	DESCRIPTION
Device	Select a profile you created in Configuration > Object > Device Insight to apply the policy to clients specified in the Device Insight profile from the drop-down list box. Select any to apply the policy to all clients.
User	This field is not available when you are configuring a to-Zyxel Device policy. Select a user name or user group to which to apply the policy. The Security Policy is activated only when the specified user logs into the system and the policy will be disabled when the user logs out. Otherwise, select any and there is no need for user logging. Note: If you specified a source IP address (group) instead of any in the field below, the user's IP address should be within the IP address range.
Schedule	Select a schedule that defines when the policy applies. Otherwise, select none and the policy is always effective.
Action	Use the drop-down list box to select what the Security Policy is to do with packets that match this policy. Select deny to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select reject to discard the packets and send a TCP reset packet or an ICMP destination-unreachable message to the sender. Select allow to permit the passage of the packets.
Log matched traffic	Select whether to have the Zyxel Device generate a log (log), log and alert (log alert) or not (no) when the policy is matched to the criteria listed above.
Profile	Use this section to apply anti- x profiles (created in the Configuration > Security Service screens) to traffic that matches the criteria above. You must have created a profile first; otherwise none displays. Use Log to generate a log (log), log and alert (log alert) or not (no) for all traffic that matches criteria in the profile.
Content Filter	Select a Content Filter profile from the list box; none displays if no profiles have been created in the Configuration > Security Service > Content Filter screen.
SSL Inspection	Select an SSL Inspection profile from the list box; none displays if no profiles have been created in the Configuration > Security Service > SSL Inspection screen.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

26.3.4 Example: Allow a Server to Ping the Zyxel Device Without Creating Logs

A server on the LAN pings the Zyxel Device every 15 seconds to check if the Zyxel Device is connected to the Internet. The Zyxel Device creates a log every time the server pings it. You want to allow the server to ping the Zyxel Device without creating so many logs.

This example uses the parameters given below.

Table 179 Address Object Configuration Example

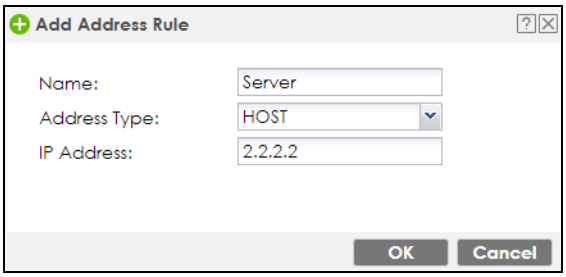
NAME	ADDRESS TYPE	IP ADDRESS
Server	Host	2.2.2.2

Table 180 Security Policy Configuration Example

NAME	SOURCE	SERVICE	ACTION	LOG
LAN1_to_Device	Server	Ping	Allow	No
LAN2_to_Device	Server	Ping	Allow	No

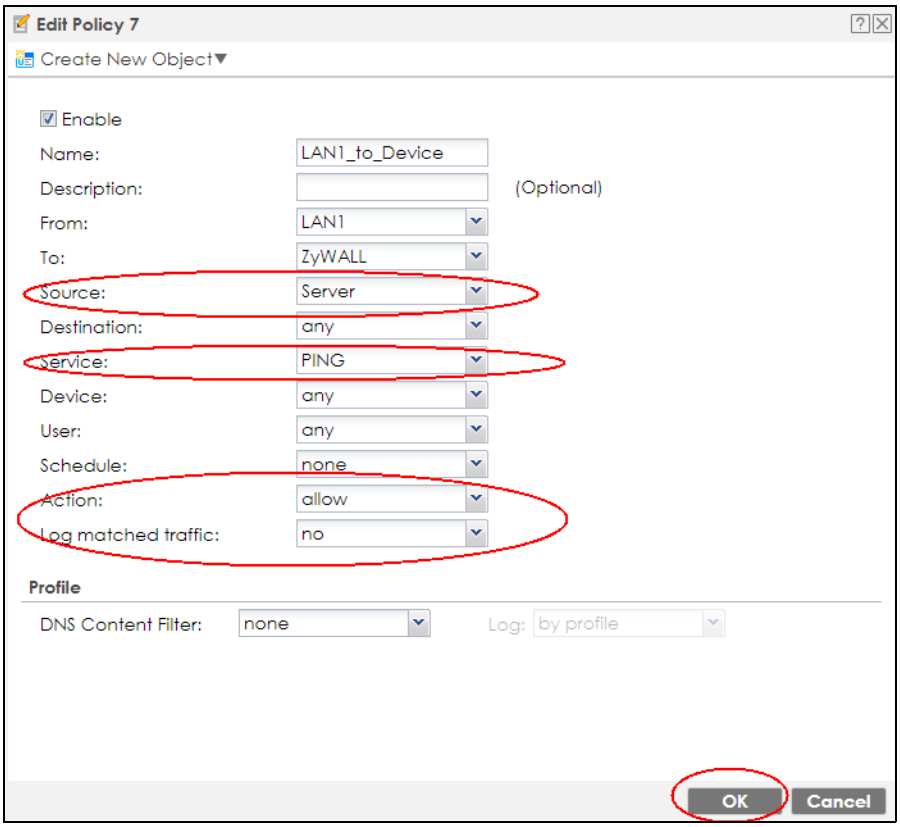
1 Go to Configuration > Object > Address/Geo IP > Address and click Add.

2 Configure the settings using the parameters given in Table 179 on page 582. Click OK to save your changes.



3 Go to Configuration > Security Policy > Policy Control. Select LAN1_to_Device then click Edit.

4 Configure the settings using the parameters given in Table 180 on page 583. Set Log to no so when the server pings the Zyxel Device, the Zyxel Device will not create logs. Click OK to save your changes.



5 Repeat Step 3 and Step 4 to configure the LAN2_to_Device policy so that when the sever pings the Zyxel Device, the Zyxel Device will not create logs.

26.3.5 Example: Create a Guest Network with Internet Access Only

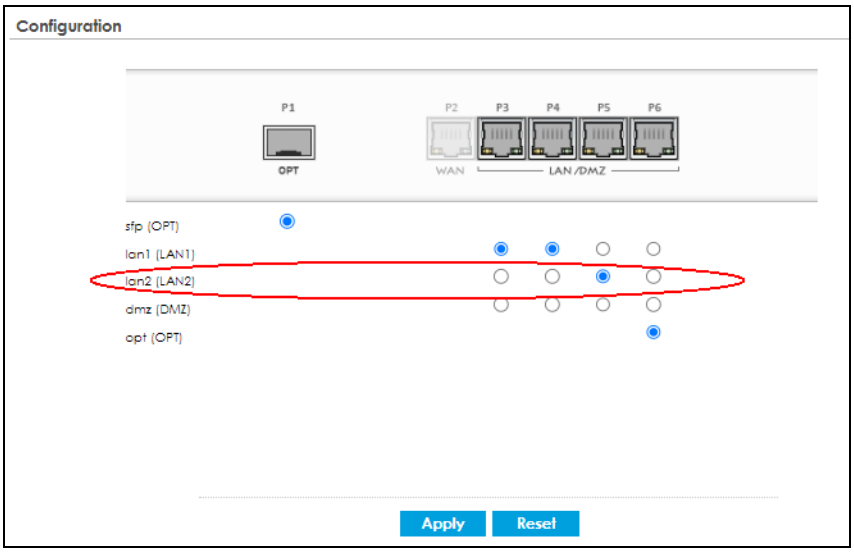
The Zyxel Device LAN1 is your private network. LAN1 clients have access to all resources in the network, such as private servers, as well as access to the Internet. You want to create a guest network on LAN2 where clients can connect to only the Internet through the Zyxel Device. Clients on LAN2 cannot access your private network on LAN1.

This example uses the parameters given below.

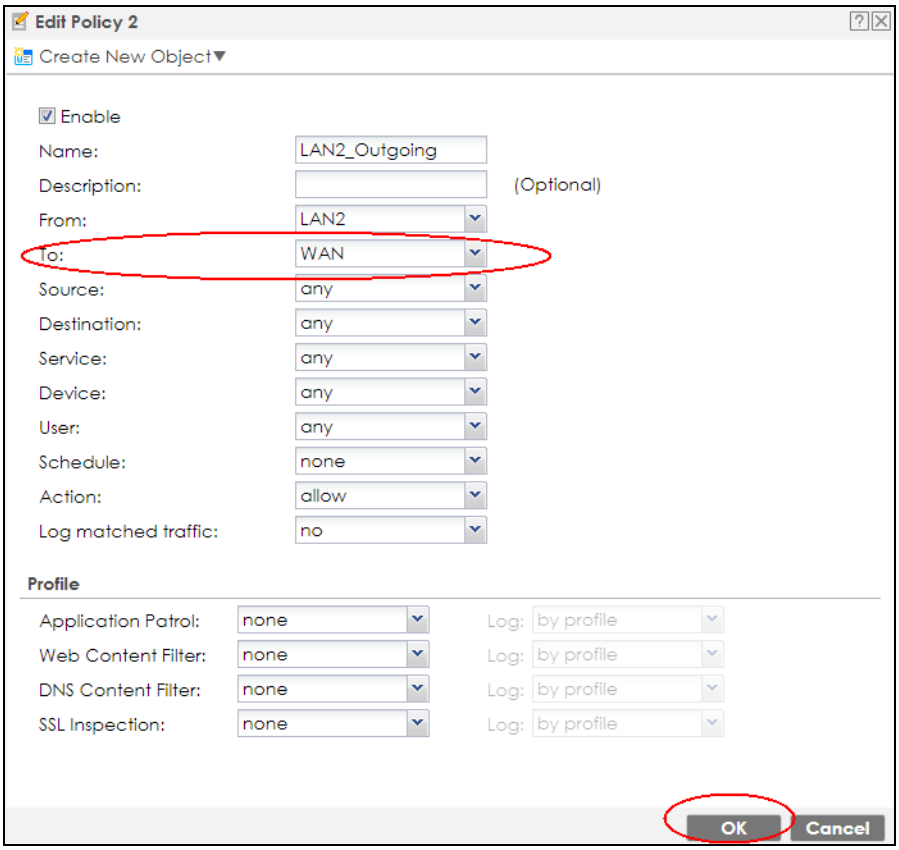
Table 181 Guest Network Policy Example

NAME	FROM	TO	ACTION
LAN2_To_LAN1	ALN2	LAN1	reject

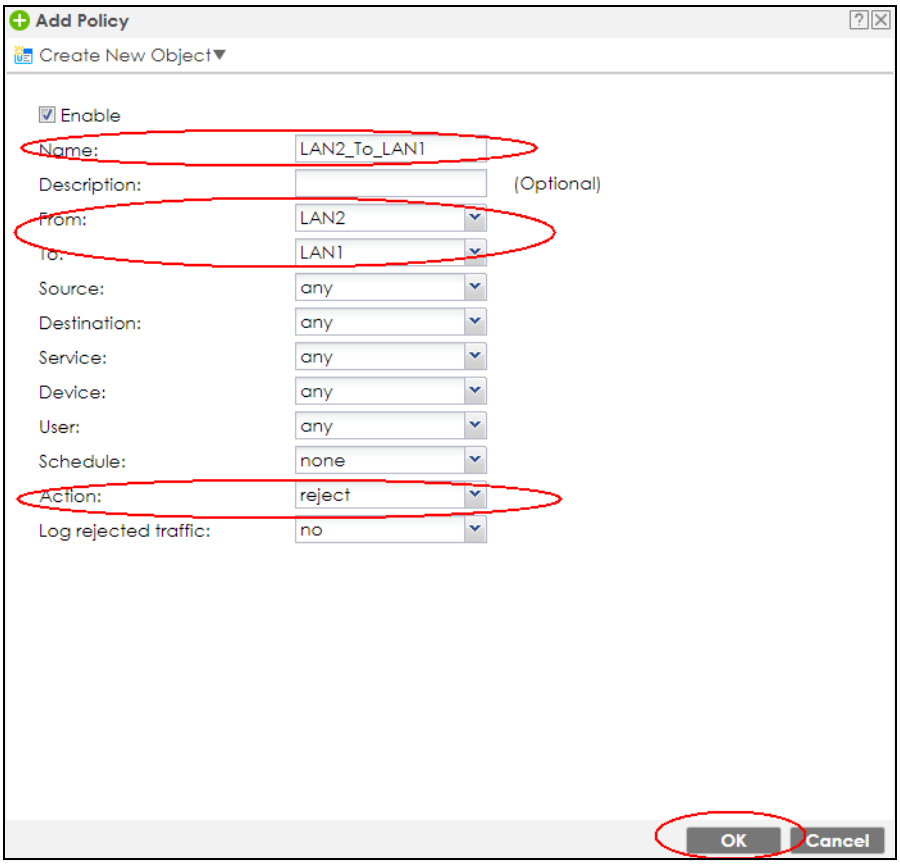
1 Go to Configuration > Network > Interface > Port > Port Role. Set lan2 (LAN2) to use P5. Click Apply to save your changes. Connect LAN1 clients to P3 and guest clients to P5.



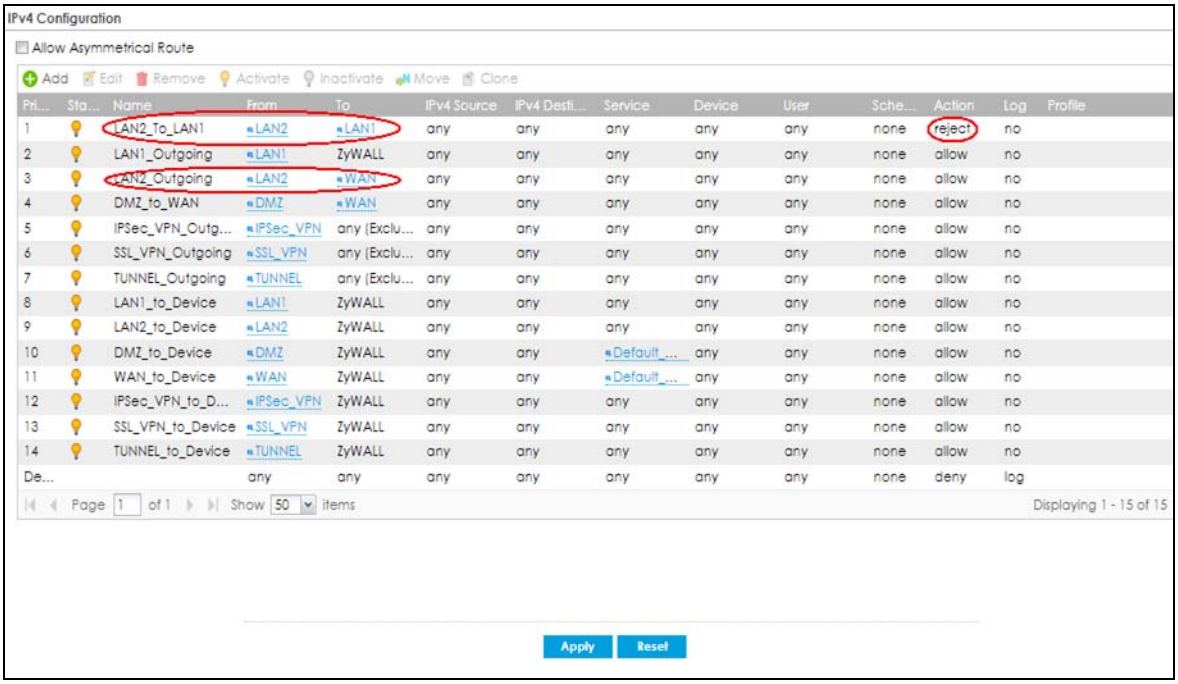
2 In Configuration > Security Policy > Policy Control, select LAN2_Outgoing and click Edit. Set To to WAN to allow LAN2 clients to access the Internet. Click OK to save your changes.



3 In Configuration > Security Policy > Policy Control, click Add to add a new rule. Configure the settings using the parameters given in Table 181 on page 584 to block LAN2 clients from accessing LAN1 and it resources. Click OK to save your changes.



4 You can check the result in the Policy Control screen. Clients on LAN2 can now access the Internet through the Zyxel Device without accessing the private network on LAN1.



26.4 Anomaly Detection and Prevention Overview

Anomaly Detection and Prevention (ADP) protects against anomalies based on violations of protocol standards (RFCs – Requests for Comments) and abnormal flows such as port scans. This section introduces ADP, anomaly profiles and applying an ADP profile to a traffic direction.

Traffic Anomalies

Traffic anomaly policies look for abnormal behavior or events such as port scanning, sweeping or network flooding. They operate at OSI layer-2 and layer-3. Traffic anomaly policies may be updated when you upload new firmware.

Protocol Anomalies

Protocol anomalies are packets that do not comply with the relevant RFC (Request For Comments). Protocol anomaly detection includes:

- TCP Decoder
- UDP Decoder
- ICMP Decoder

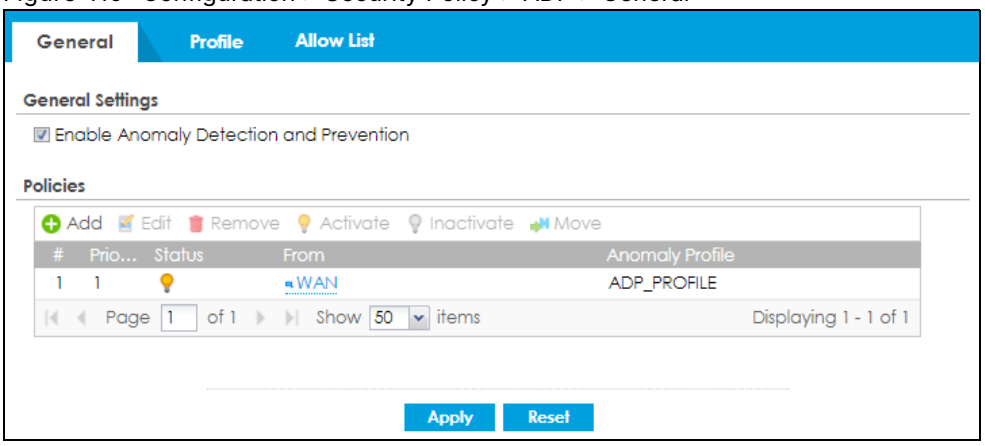
Protocol anomaly policies may be updated when you upload new firmware.

Note: First, create an ADP profile in the In the Configuration > Security Policy > ADP > Profile screen. Then, apply the profile to traffic originating from a specific zone in the Configuration > Security Policy > ADP > General screen.

26.4.1 The Anomaly Detection and Prevention General Screen

Click Configuration > Security Policy > ADP > General to display the next screen.

Figure 410 Configuration > Security Policy > ADP > General



The following table describes the labels in this screen.

Table 182 Configuration > Security Policy > ADP > General

LABEL	DESCRIPTION
General Settings	
Enable Anomaly Detection and Prevention	Select this to enable traffic anomaly and protocol anomaly detection and prevention.
Add	Select an entry and click Add to append a new row beneath the one selected. ADP policies are applied in order (Priority) shown in this screen
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Move	To change an entry's position in the numbered list, select it and click Move to display a field to type a number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed.
#	This is the entry's index number in the list.
Priority	This is the rank in the list of anomaly profile policies. The list is applied in order of priority.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
From	This is the direction of travel of packets to which an anomaly profile is bound. Traffic direction is defined by the zone the traffic is coming from. Use the From field to specify the zone from which the traffic is coming. Select ZyWALL to specify traffic coming from the Zyxel Device itself. From LAN means packets traveling from a computer on one LAN subnet to a computer on another subnet through the Zyxel Device's LAN1 zone interfaces. The Zyxel Device does not check packets traveling from a LAN computer to another LAN computer on the same subnet. From WAN means packets that come in from the WAN zone and the Zyxel Device routes back out through the WAN zone. Note: Depending on your network topology and traffic load, applying every packet direction to an anomaly profile may affect the Zyxel Device's performance.
Anomaly Profile	An anomaly profile is a set of anomaly policies with configured activation, log and action settings. This field shows which anomaly profile is bound to which traffic direction. Select an ADP profile to apply to the entry's traffic direction. Configure the ADP profiles in the ADP profile screens.

26.4.2 Creating New ADP Profiles

Create new ADP profiles in the Configuration > Security Policy > ADP > Profile screens.

When creating ADP profiles. you may find that certain policies are triggering too many false positives or false negatives. A false positive is when valid traffic is flagged as an attack. A false negative is when invalid traffic is wrongly allowed to pass through the Zyxel Device. As each network is different, false positives and false negatives are common on initial ADP deployment.

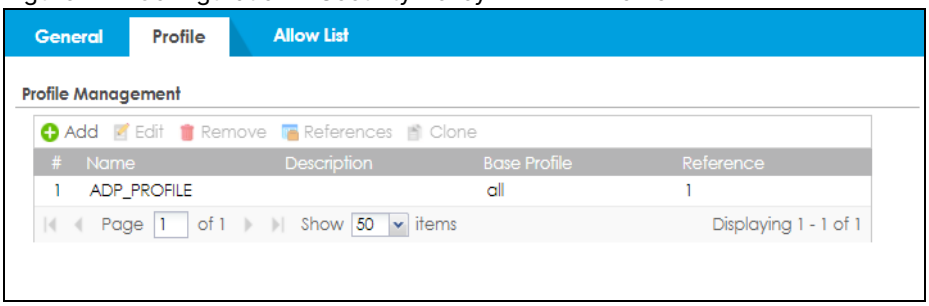
To counter this, you could create a 'monitor profile' that creates logs, but all actions are disabled. Observe the logs over time and try to eliminate the causes of the false alarms. When you're satisfied that they have

been reduced to an acceptable level, you could then create an 'in-line profile' whereby you configure appropriate actions to be taken when a packet matches a policy.

ADP profiles consist of traffic anomaly profiles and protocol anomaly profiles. To create a new profile, select a base profile and then click OK to go to the profile details screen. Type a new profile name, enable or disable individual policies and then edit the default log options and actions.

Click Configuration > Security Policy > ADP > Profile to view the following screen.

Figure 411 Configuration > Security Policy > ADP > Profile



The following table describes the labels in this screen.

Table 183 Configuration > Security Policy > ADP > Profile

LABEL	DESCRIPTION
Profile Management	Create ADP profiles here and then apply them in the Configuration > Security Policy > ADP > Profile screen.
Add	Click Add and first choose a none or all Base Profile. • none base profile sets all ADP entries to have Log set to no and Action set to none by default. • all base profile sets all ADP entries to have Log set to log and Action set to block by default.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
References	Select an entry and click References to open a screen that shows which settings use the entry. Click Refresh to update information on this screen.
Clone	Use Clone to create a new entry by modifying an existing one. • Select an existing entry. • Click Clone. • A configuration copy of the selected entry pops up. You must at least change the name as duplicate entry names are not allowed.
#	This is the entry's index number in the list.
Name	This is the name of the profile you created.
Description	This is the description of the profile you created.
Base Profile	This is the name of the base profile used to create this profile.
Reference	This is the number of object references used to create this profile.

26.4.3 Traffic Anomaly Profiles

Traffic anomaly detection looks for abnormal behavior such as scan or flooding attempts. In the

Table 184 Configuration > Security Policy > ADP > Profile > Add-Traffic-Anomaly

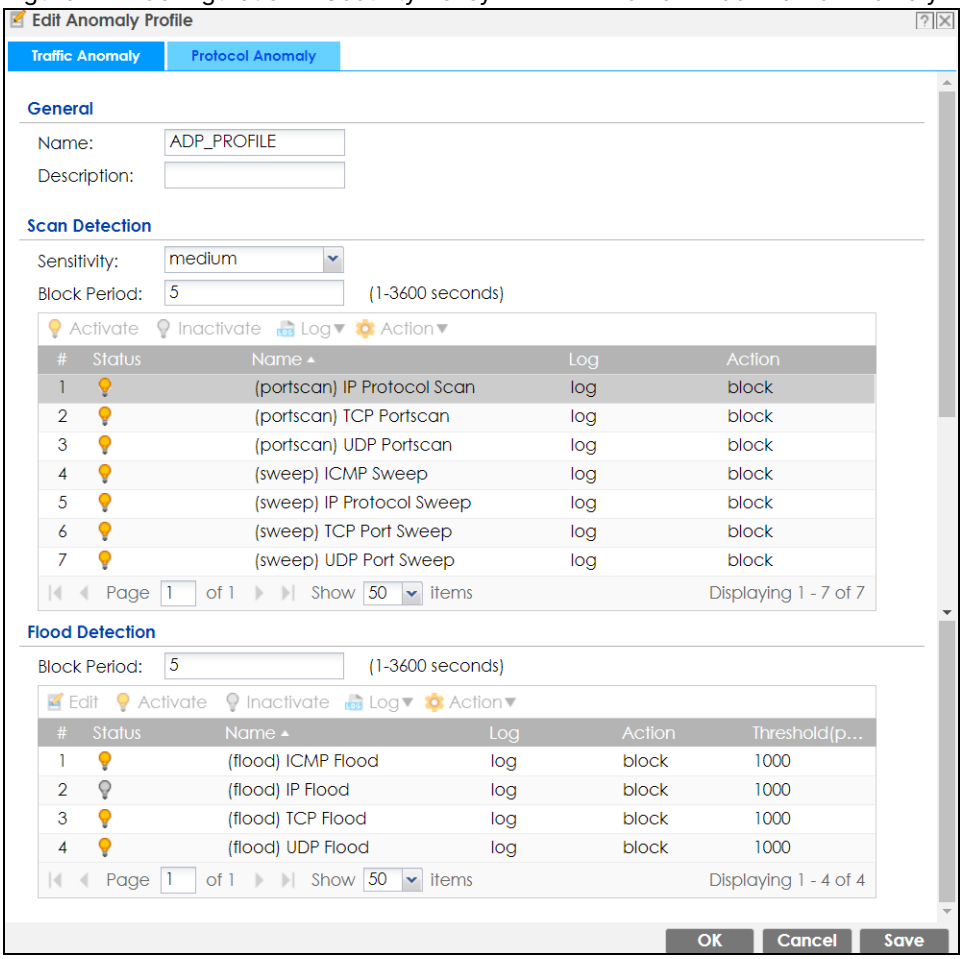
LABEL	DESCRIPTION
Name	A name is automatically generated that you can edit. The name must be the same in the Traffic Anomaly and Protocol Anomaly screens for the same ADP profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. These are valid, unique profile names: • MyProfile • mYProfile • Mymy12_3-4 These are invalid profile names: • 1mYProfile • My Profile • MyProfile? • Whatalongprofilename123456789012
Description	In addition to the name, type additional information to help you identify this ADP profile.
Scan/Flood Detection	Scan detection, such as port scanning, tries to find attacks where an attacker scans device(s) to determine what types of network protocols or services a device supports. Flood detection tries to find attacks that saturate a network with useless data, use up all available bandwidth, and so aim to make communications on the network impossible.
Sensitivity	(Scan detection only.) Select a sensitivity level so as to reduce false positives in your network. If you choose low sensitivity, then scan thresholds and sample times are set low, so you will have fewer logs and false positives; however some traffic anomaly attacks may not be detected. If you choose high sensitivity, then scan thresholds and sample times are set high, so most traffic anomaly attacks will be detected; however you will have more logs and false positives.
Block Period	Specify for how many seconds the Zyxel Device blocks all packets from being sent to the victim (destination) of a detected anomaly attack. Flood Detection applies blocking to the destination IP address and Scan Detection applies blocking to the source IP address.
Edit (Flood Detection only)	Select an entry and click this to be able to modify it.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Log	To edit an item's log option, select it and use the Log icon. Select whether to have the Zyxel Device generate a log (log), log and alert (log alert) or neither (no) when traffic matches this anomaly policy.
Action	To edit what action the Zyxel Device takes when a packet matches a policy, select the policy and use the Action icon. none: The Zyxel Device takes no action when a packet matches the policy. block: The Zyxel Device silently drops packets that matches the policy. Neither sender nor receiver are notified.
#	This is the entry's index number in the list.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.

Table 184 Configuration > Security Policy > ADP > Profile > Add-Traffic-Anomaly (continued)

LABEL	DESCRIPTION
Name	This is the name of the anomaly policy. Click the Name column heading to sort in ascending or descending order according to the protocol anomaly policy name.
Log	These are the log options. To edit this, select an item and use the Log icon.
Action	This is the action the Zyxel Device should take when a packet matches a policy. To edit this, select an item and use the Action icon.
Threshold (pkt/sec)	(Flood detection only.) Select a suitable threshold level (the number of packets per second that match the flood detection criteria) for your network. If you choose a low threshold, most traffic anomaly attacks will be detected, but you may have more logs and false positives. If you choose a high threshold, some traffic anomaly attacks may not be detected, but you will have fewer logs and false positives.
OK	Click OK to save your settings to the Zyxel Device, complete the profile and return to the profile summary page.
Cancel	Click Cancel to return to the profile summary page without saving any changes.
Save	Click Save to save the configuration to the Zyxel Device but remain in the same page. You may then go to the another profile screen (tab) in order to complete the profile. Click OK in the final profile screen to complete the profile.

Configuration > Security Policy > ADP > Profile screen, click the Edit or Add icon and choose a base profile. Traffic Anomaly is the first tab in the profile.

Figure 412 Configuration > Security Policy > ADP > Profile > Add-Traffic-Anomaly



The following table describes the labels in this screen.

26.4.4 Protocol Anomaly Profiles

Protocol anomalies are packets that do not comply with the relevant RFC (Request For Comments). Protocol anomaly detection includes:

- TCP Decoder
- UDP Decoder
- ICMP Decoder
- IP Decoder

Teardrop

When an IP packet is larger than the Maximum Transmission Unit (MTU) configured in the Zyxel Device, it is fragmented using the TCP or ICMP protocol.

A Teardrop attack falsifies the offset which defines the size of the fragment and the original packet. A series of IP fragments with overlapping offset fields can cause some systems to crash, hang, or reboot when fragment reassembling is attempted at the destination.

IP Spoofing

IP Spoofing is used to gain unauthorized access to network devices by modifying packet headers so that it appears that the packets originate from a host within a trusted network.

- In an IP Spoof from the WAN, the source address appears to be in the same subnet as a Zyxel Device LAN interface.
- In an IP Spoof from a LAN interface, the source address appears to be in a different subnet from that Zyxel Device LAN interface.

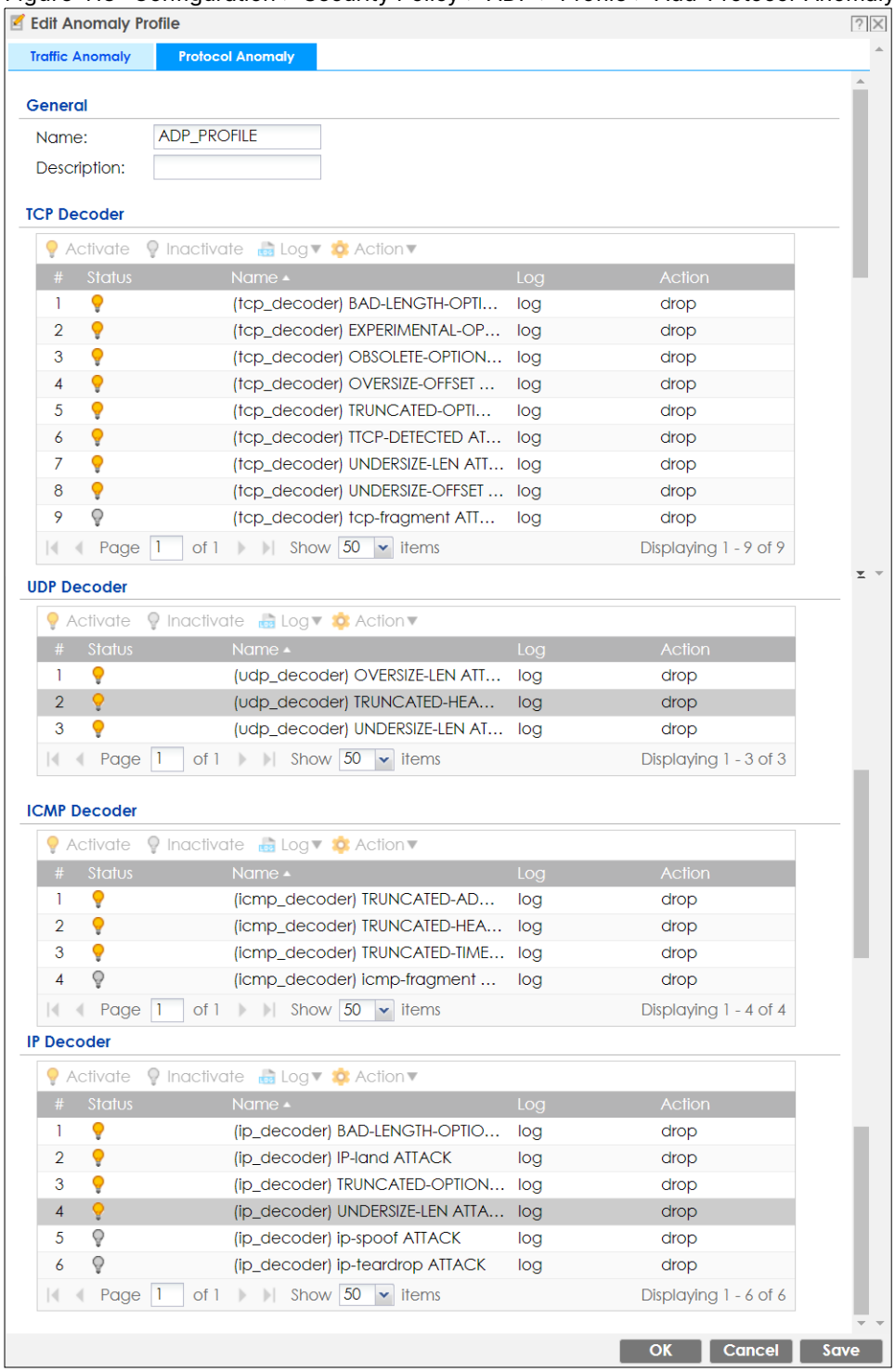
Table 185 Configuration > Security Policy > ADP > Profile > Add-Protocol-Anomaly

LABEL	DESCIRPTION
Name	A name is automatically generated that you can edit. The name must be the same in the Traffic Anomaly and Protocol Anomaly screens for the same ADP profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. These are valid, unique profile names: • MyProfile • mYProfile • Mymy12_3-4 • These are invalid profile names: • 1mYProfile • My Profile • MyProfile? • Whatalongprofilename123456789012
Description	In addition to the name, type additional information to help you identify this ADP profile.
TCP Decoder/UDP Decoder/ ICMP Decoder/IP Decoder	Perform the following actions for each type of encoder.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.

Table 185 Configuration > Security Policy > ADP > Profile > Add-Protocol-Anomaly (continued)

LABEL	DESCIRPTION
Log	To edit an item's log option, select it and use the Log icon. Select whether to have the Zyxel Device generate a log (log), log and alert (log alert) or neither (no) when traffic matches this anomaly policy.
Action	To edit what action the Zyxel Device takes when a packet matches a policy, select the policy and use the Action icon. original setting: Select this action to return each rule in a service group to its previously saved configuration. none: Select this action to have the Zyxel Device take no action when a packet matches a policy. drop: Select this action to have the Zyxel Device silently drop a packet that matches a policy. Neither sender nor receiver are notified. reject-sender: Select this action to have the Zyxel Device send a reset to the sender when a packet matches the policy. If it is a TCP attack packet, the Zyxel Device will send a packet with a 'RST' flag. If it is an ICMP or UDP attack packet, the Zyxel Device will send an ICMP unreachable packet. reject-receiver: Select this action to have the Zyxel Device send a reset to the receiver when a packet matches the policy. If it is a TCP attack packet, the Zyxel Device will send a packet with an a 'RST' flag. If it is an ICMP or UDP attack packet, the Zyxel Device will do nothing. reject-both: Select this action to have the Zyxel Device send a reset to both the sender and receiver when a packet matches the policy. If it is a TCP attack packet, the Zyxel Device will send a packet with a 'RST' flag to the receiver and sender. If it is an ICMP or UDP attack packet, the Zyxel Device will send an ICMP unreachable packet.
#	This is the entry's index number in the list.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This is the name of the anomaly policy. Click the Name column heading to sort in ascending or descending order according to the protocol anomaly policy name.
Log	These are the log options. To edit this, select an item and use the Log icon.
Action	This is the action the Zyxel Device should take when a packet matches a policy. To edit this, select an item and use the Action icon.
OK	Click OK to save your settings to the Zyxel Device, complete the profile and return to the profile summary page.
Cancel	Click Cancel to return to the profile summary page without saving any changes.
Save	Click Save to save the configuration to the Zyxel Device but remain in the same page. You may then go to the another profile screen (tab) in order to complete the profile. Click OK in the final profile screen to complete the profile.

Figure 413 Configuration > Security Policy > ADP > Profile > Add-Protocol-Anomaly

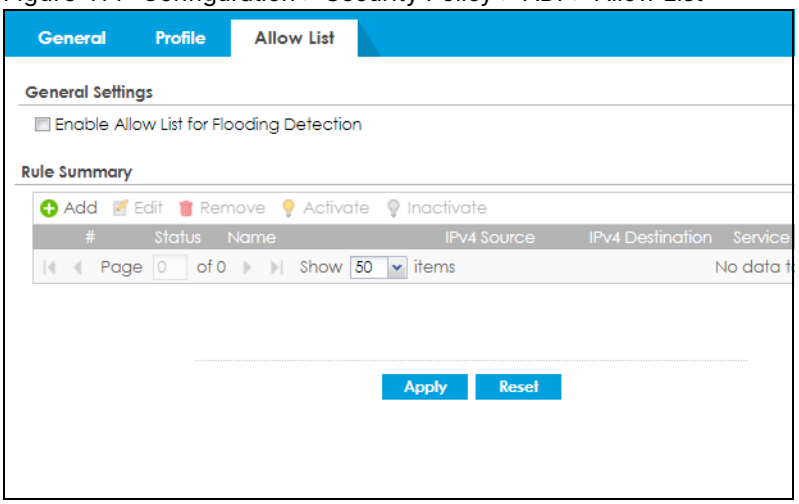


The following table describes the labels in this screen.

26.4.5 The ADP Allow List Screen

Click Configuration> Security Policy> ADP> Allow List to display the following screen. Use this screen to configure allow list rules to let certain IP addresses or services bypass port scanning, port sweeping and flood detection.

Figure 414 Configuration > Security Policy > ADP> Allow List



The following table describes the labels in this screen.

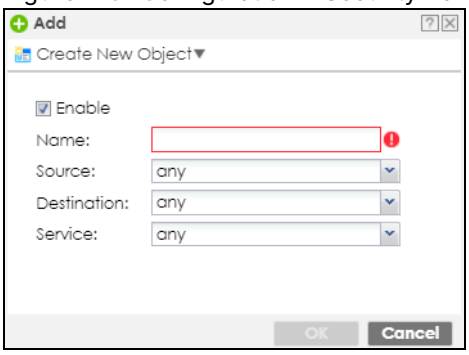
Table 186 Configuration > Security Policy > ADP > Allow List

LABEL	DESCRIPTION
General Settings	
Enable allow list for all traffic anomaly detection	Select this to allow certain IP addresses or services bypass port scanning, port sweeping and flood detection.
Rule Summary	
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The 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.
#	This field is a sequential value showing the number of the profile. The profile order is not important.
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 rule.
IPv4 Source	This field displays the IPv4 source address object to which the ADP white list rule applies.
IPv4 Destination	This field displays the IPv4 destination address object to which the ADP white list rule applies.
Service	This displays the service object to which the ADP white list rule applies.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

26.4.6 Creating New ADP Allow List Rule

Create new ADP allow list rules in this screen. Click Configuration > Security Policy > ADP > Allow List to view the following screen.

Figure 415 Configuration > Security Policy > ADP > Allow List



The following table describes the labels in this screen.

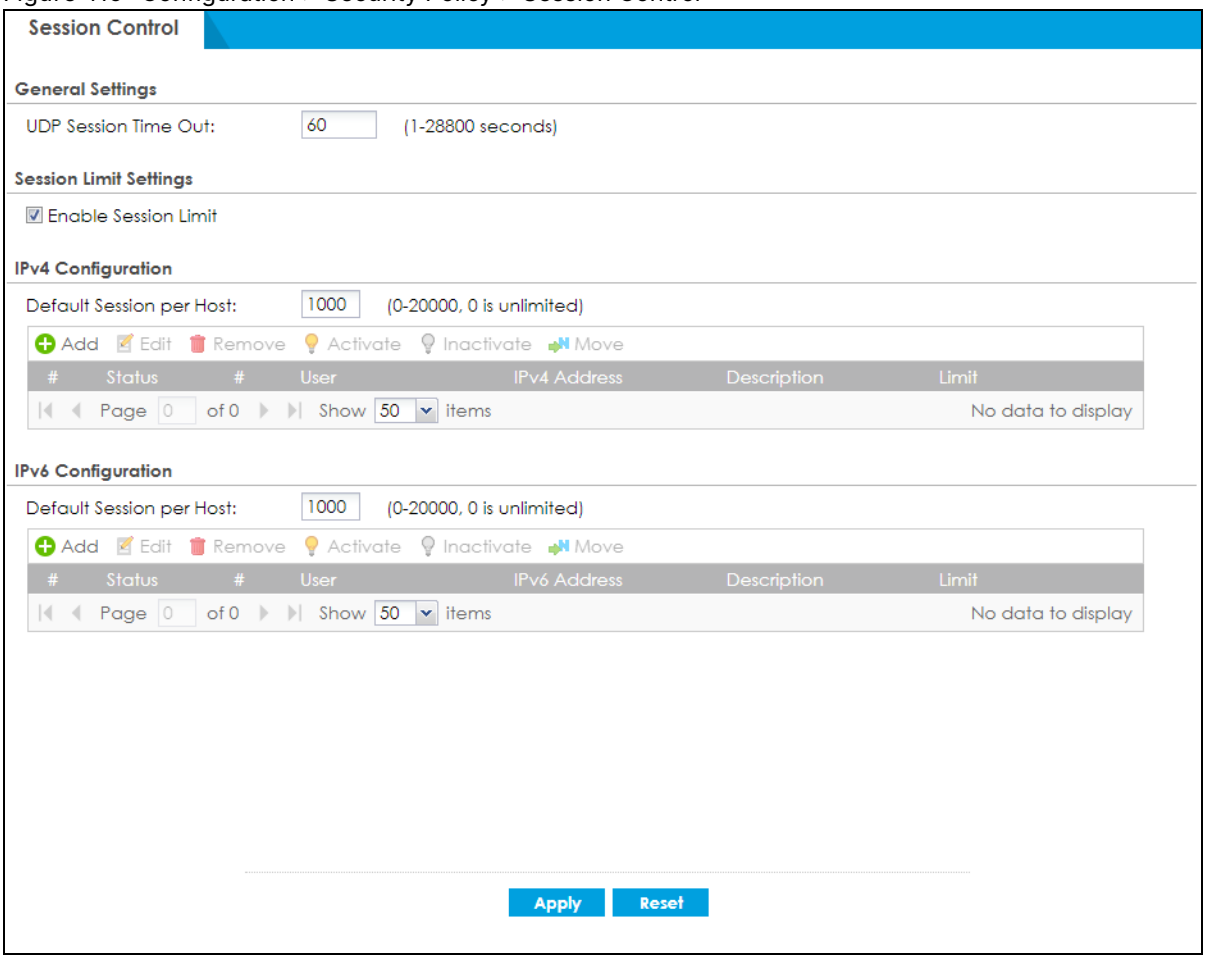
Table 187 Configuration > Security Policy > ADP > Allow List > Add

LABEL	DESCRIPTION
Enable	Select this to enable this allow list rule.
Name	Enter a name to help you identify this rule. Use up to 60 printable ASCII characters. Spaces are allowed.
Source	Select a source address or address group, including geographic address and FQDN (group) objects, to which this rule applies. Select any to make the rule apply to every source address.
Destination	Select a destination address or address group, including geographic address and FQDN (group) objects, for whom this rule applies. Select any to make the rule apply to every destination address.
Service	Select the service or service group to which this rule applies. Select any to white list all traffic between the source and destination addresses.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

26.5 The Session Control Screen

Click Configuration > Security Policy > Session Control to display the Security Policy Session Control screen. Use this screen to limit the number of concurrent NAT/Security Policy sessions a client can use. You can apply a default limit for all users and individual limits for specific users, addresses, or both. The individual limit takes priority if you apply both.

Figure 416 Configuration > Security Policy > Session Control



The following table describes the labels in this screen.

Table 188 Configuration > Security Policy > Session Control

LABEL	DESCRIPTION
General Settings	
UDP Session Time Out	Set how many seconds the Zyxel Device will allow a UDP session to remain idle (without UDP traffic) before closing it.
Session Limit Settings	
Enable Session limit	Select this checkbox to control the number of concurrent sessions hosts can have.
IPv4 / IPv6 Configuration	This table lists the rules for limiting the number of concurrent sessions hosts can have.
Default Session per Host	This field is configurable only when you enable session limit. Use this field to set a common limit to the number of concurrent NAT/Security Policy sessions each client computer can have. If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions. Create rules below to apply other limits for specific users or addresses.

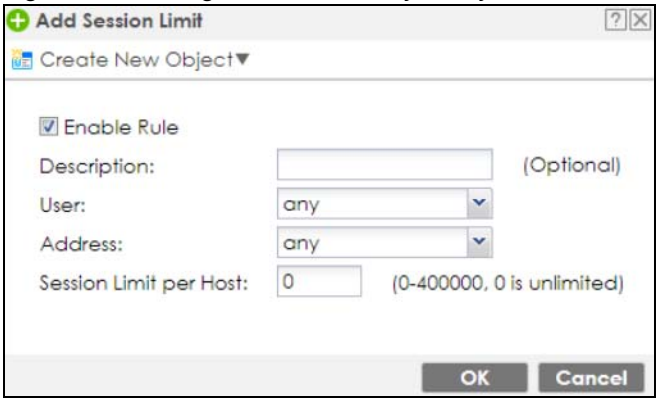
Table 188 Configuration > Security Policy > Session Control (continued)

LABEL	DESCRIPTION
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The 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.
Move	To change a rule's position in the numbered list, select the rule and click Move to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
#	This field is a sequential value showing the number of the profile. The profile order is not important.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
#	This is the index number of a session limit rule. It is not associated with a specific rule.
User	This is the user name or user group name to which this session limit rule applies.
IPv4 / IPv6 Address	This is the IPv4 / IPv6 address object, including geographic address (group) objects to which this session limit rule applies.
Description	This is the information configured to help you identify the rule.
Limit	This is how many concurrent sessions this user or address is allowed to have.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

26.5.1 The Session Control Add/Edit Screen

Click Configuration > Security Policy > Session Control and the Add or Edit icon to display the Add or Edit screen. Use this screen to configure rules that define a session limit for specific users or addresses.

Figure 417 Configuration > Security Policy > Session Control > Edit



The following table describes the labels in this screen.

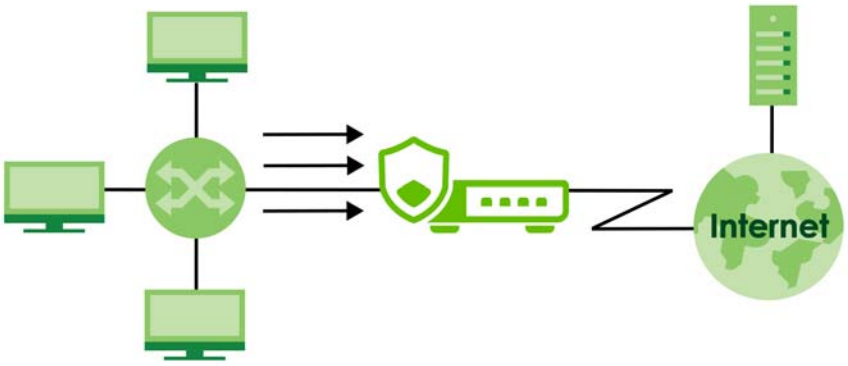
Table 189 Configuration > Security Policy > Session Control > Add / Edit

LABEL	DESCRIPTION
Create new Object	Use to configure new settings for User or Address objects that you need to use in this screen.Click on the down arrow to see the menu.
Enable Rule	Select this checkbox to turn on this session limit rule.
Description	Enter information to help you identify this rule. Use up to 60 printable ASCII characters. Spaces are allowed.
User	Select a user name or user group to which to apply the rule. The rule is activated only when the specified user logs into the system and the rule will be disabled when the user logs out. Otherwise, select any and there is no need for user logging. Note: If you specified an IP address (or address group) instead of any in the field below, the user's IP address should be within the IP address range.
Address	Select the IPv4 source address or address group, including geographic address (group) object, to which this rule applies. Select any to apply the rule to all IPv4 source addresses.
IPv6 Address	Select the IPv6 source address or address group, including geographic address (group) object, to which this rule applies. Select any to apply the rule to all IPv6 source addresses.
Session Limit per Host	Use this field to set a limit to the number of concurrent NAT/Security Policy sessions this rule's users or addresses can have. For this rule's users and addresses, this setting overrides the Default Session per Host setting in the general Security Policy Session Control screen.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

26.6 Security Policy Example Applications

Suppose you decide to block LAN users from using IRC (Internet Relay Chat) through the Internet. To do this, you would configure a LAN to WAN Security Policy that blocks IRC traffic from any source IP address from going to any destination address. You do not need to specify a schedule since you need the Security Policy to always be in effect. The following figure shows the results of this policy.

Figure 418 Blocking All LAN to WAN IRC Traffic Example



Your Security Policy would have the following settings.

Table 190 Blocking All LAN to WAN IRC Traffic Example

#	USER	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	Any	Any	Any	Any	IRC	Deny
2	Any	Any	Any	Any	Any	Allow

- The first row blocks LAN access to the IRC service on the WAN.
- The second row is the Security Policy's default policy that allows all LAN1 to WAN traffic.

The Zyxel Device applies the security policies in order. So for this example, when the Zyxel Device receives traffic from the LAN, it checks it against the first policy. If the traffic matches (if it is IRC traffic) the security policy takes the action in the policy (drop) and stops checking the subsequent security policies. Any traffic that does not match the first security policy will match the second security policy and the Zyxel Device forwards it.

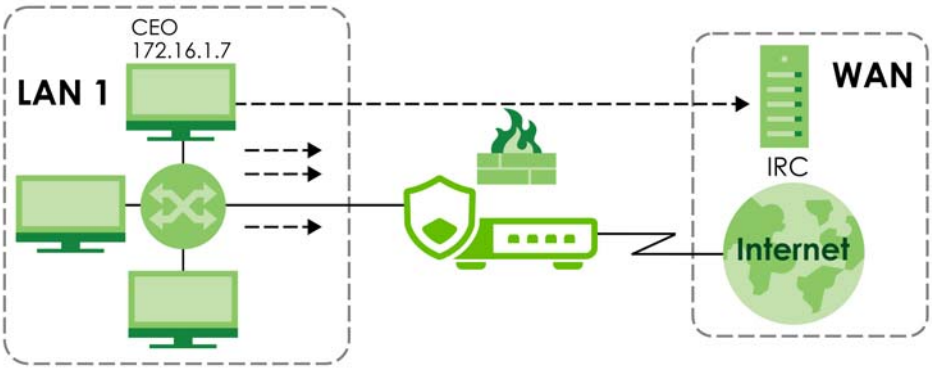
Now suppose you need to let the CEO use IRC. You configure a LAN1 to WAN security policy that allows IRC traffic from the IP address of the CEO's computer. You can also configure a LAN to WAN policy that allows IRC traffic from any computer through which the CEO logs into the Zyxel Device with his/her user name. In order to make sure that the CEO's computer always uses the same IP address, make sure it either:

- Has a static IP address,

  or
- You configure a static DHCP entry for it so the Zyxel Device always assigns it the same IP address.

Now you configure a LAN1 to WAN security policy that allows IRC traffic from the IP address of the CEO's computer (172.16.1.7 for example) to go to any destination address. You do not need to specify a schedule since you want the security policy to always be in effect. The following figure shows the results of your two custom policies.

Figure 419 Limited LAN to WAN IRC Traffic Example



Your security policy would have the following configuration.

Table 191 Limited LAN1 to WAN IRC Traffic Example 1

#	USER	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	Any	172.16.1.7	Any	Any	IRC	Allow
2	Any	Any	Any	Any	IRC	Deny
3	Any	Any	Any	Any	Any	Allow

- The first row allows the LAN1 computer at IP address 172.16.1.7 to access the IRC service on the WAN.
- The second row blocks LAN1 access to the IRC service on the WAN.
- The third row is the default policy of allowing all traffic from the LAN1 to go to the WAN.

Alternatively, you configure a LAN1 to WAN policy with the CEO's user name (say CEO) to allow IRC traffic from any source IP address to go to any destination address.

Your Security Policy would have the following settings.

Table 192 Limited LAN1 to WAN IRC Traffic Example 2

#	USER	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	CEO	Any	Any	Any	IRC	Allow
2	Any	Any	Any	Any	IRC	Deny
3	Any	Any	Any	Any	Any	Allow

- The first row allows any LAN1 computer to access the IRC service on the WAN by logging into the Zyxel Device with the CEO's user name.
- The second row blocks LAN1 access to the IRC service on the WAN.
- The third row is the default policy of allowing allows all traffic from the LAN1 to go to the WAN.

The policy for the CEO must come before the policy that blocks all LAN1 to WAN IRC traffic. If the policy that blocks all LAN1 to WAN IRC traffic came first, the CEO's IRC traffic would match that policy and the Zyxel Device would drop it and not check any other security policies.

CHAPTER 27
Content Filter

27.1 Overview

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

27.1.1 What You Can Do in this Chapter

- Use the Web Content Filter General screens (Section 27.2 on page 605) to set up web content filtering profiles.
- Use the Web Content Filter Trusted Web Sites screens (Section 27.3 on page 625) to create a common list of good (allowed) web site addresses.
- Use the Web Content Filter Forbidden Web Sites screens (Section 27.4 on page 626) to create a common list of bad (blocked) web site addresses.
- Use the DNS Content Filter General screens (Section 27.5 on page 627) to set up DNS content filtering profiles.
- Use the DNS Content Filter Allow List screen (Section 27.6 on page 642) to create a list of good (allowed) web site addresses.
- Use the DNS Content Filter Block List screen (Section 27.7 on page 643) to create a list of bad (blocked) web site addresses.

27.1.2 What You Need to Know

Web Content Filter

The Web Content Filter allows the Zyxel Device to block specific web features, such as cookies or ActiveX, by inspecting the web pages that users are visiting. The Zyxel Device can also block access to specific websites, by inspecting the URL or Server Name Indication (SNI) that the user's web browser sends to the web server.

Web Content Filtering Process

1. A user enters a URL into their web browser.
2. The user's computer sends a DNS query for the URL.
3. The DNS server returns an IP address for the URL.
4. The user's web browser connects to the IP address.
5. The Web Content Filter detects an HTTP connection, and inspects the website send using Server Name Indication (SNI).

6 If the website contains prohibited material, the HTTP request is redirected to a block page.

Note: If the user's web browser is using encryption, then you must enable SSL Inspection for Web Content Filter to work.

If the user's web browser is using Encrypted Server Name Indication (ESNI), DNS Content Filter will not work.

Web Content Filtering Policies

A web content filtering policy allows you to do the following.

- Use schedule objects to define when to apply a content filter profile.
- Use address and/or user/group objects to define to whose web access to apply the content filter profile.
- Apply a content filter profile that you have custom-tailored.

Web Content Filtering Profiles

A web content filtering profile conveniently stores your custom settings for the following features.

- Category-based Blocking

  The Zyxel Device can block access to particular categories of web site content, such as pornography or racial intolerance.
- Restrict Web Features

  The Zyxel Device can disable web proxies and block web features such as ActiveX controls, Java applets and cookies.
- Customize Web Site Access

  You can specify URLs to which the Zyxel Device blocks access. You can alternatively block access to all URLs except ones that you specify. You can also have the Zyxel Device block access to URLs that contain particular keywords.

Web Content Filtering Configuration Guidelines

When the Zyxel Device receives an HTTP request, the content filter searches for a policy that matches the source address and time (schedule). The content filter checks the policies in order (based on the policy numbers). When a matching policy is found, the content filter allows or blocks the request depending on the settings of the filtering profile specified by the policy. Some requests may not match any policy. The Zyxel Device allows the request if the default policy is not set to block. The Zyxel Device blocks the request if the default policy is set to block.

External Web Filtering Service

When you register for and enable the external web filtering service, your Zyxel Device accesses an external database that has millions of web sites categorized based on content. You can have the Zyxel Device block, block and/or log access to web sites based on these categories.

HTTPS Domain Filter

HTTPS Domain Filter works with the Content Filter category feature to identify HTTPS traffic and take appropriate action. SSL Inspection identifies HTTPS traffic for all Security Service traffic and has higher priority than HTTPS Domain Filter. HTTPS Domain Filter only identifies keywords in the domain name of an URL and matches it to a category. For example, if the keyword is 'picture' and the URL is http://www.google.com/picture/index.htm, then HTTPS Domain Filter cannot identify 'picture' because that keyword in not in the domain name 'www.google.com'. However, SSL Inspection can identify 'picture' in the URL http://www.google.com/picture/index.htm.

Keyword Blocking URL Checking

The Zyxel Device checks the URL's domain name (or IP address) and file path separately when performing keyword blocking.

The URL's domain name or IP address is the characters that come before the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the domain name is www.zyxel.com.tw.

The file path is the characters that come after the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the file path is news/pressroom.php.

Since the Zyxel Device checks the URL's domain name (or IP address) and file path separately, it will not find items that go across the two. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the Zyxel Device would find "tw" in the domain name (www.zyxel.com.tw). It would also find "news" in the file path (news/pressroom.php) but it would not find "tw/news".

DNS Content Filter

The DNS Content Filter allows the Zyxel Device to block access to specific websites by inspecting DNS queries made by users on your network. If the website in the DNS query contains prohibited material, then the Zyxel Device replies to the DNS query with a IP address that points to the block page. Unlike the Web Content Filter, the DNS Content Filter works if the user is using TLS 1.3 with ESNI.

DNS Content Filter Process

1. A user enters a URL into their web browser.
2. The user's computer sends a DNS query for the URL.
3. The DNS Content Filter inspects the website in the DNS query packet.
4. If the website contains prohibited material, the DNS reply is redirected to a block page.

Finding Out More

- See Section 27.9 on page 645 for content filtering background/technical information.

27.1.3 Before You Begin

- You must configure an address object, a schedule object and a filtering profile before you can set up a content security policy.

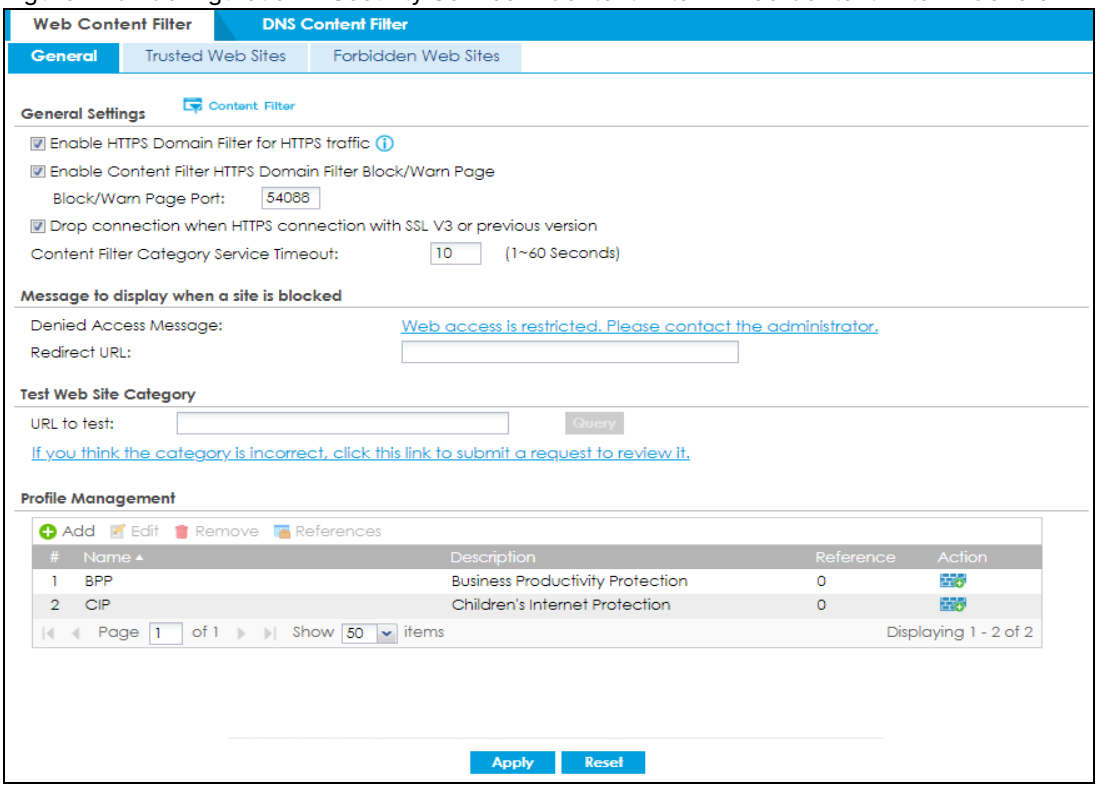
- You must have Content Filtering license in order to use the function. Subscribe to use the external database content filtering (see the Licensing > Registration screens).

27.2 Web Content Filter General Screen

Click Configuration > Security Service> Content Filter > Web Content Filter > General to open the Web Content Filter General screen. Use this screen to enable content filtering, view and order your list of content filter policies, create a denial of access message or specify a redirect URL and check your external web filtering service registration status.

Click the Content Filter icon for more information on the Zyxel Device's security features.

Figure 420 Configuration > Security Service > Content Filter > Web Content Filter > General



The following table describes the labels in this screen.

Table 193 Configuration > Security Service > Content Filter > Web Content Filter > General

LABEL	DESCRIPTION
General Settings	
Enable HTTPS Domain Filter for HTTPS traffic	Select this checkbox to have the Zyxel Device block HTTPS web pages using the cloud category service. In an HTTPS connection, the Zyxel Device can extract the Server Name Indication (SNI) from a client request, check if it matches a category in the cloud content filter and then take appropriate action. The keyword match is for the domain name only.
Enable Content Filter HTTPS Domain Filter Block/Warn Page	Use this field to have the Zyxel Device display a warning page instead of a blank page when an HTPPS connection is redirected.

Table 193 Configuration > Security Service > Content Filter > Web Content Filter > General (continued)

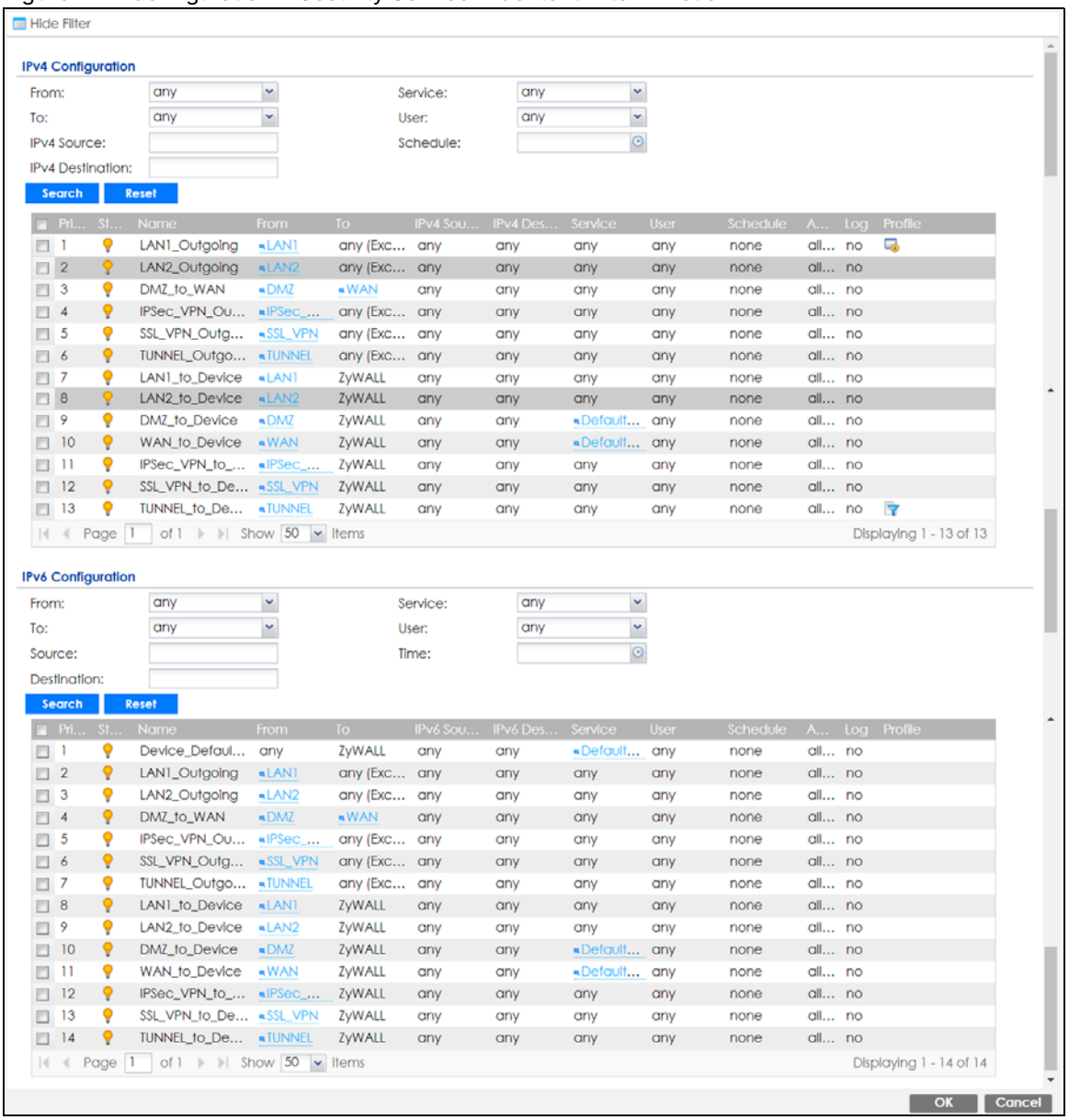
LABEL	DESCRIPTION
Block/Warn Page Port	Use the default port number as displayed for the warning page. If you change it, the new port number should be unique.
Drop connection when HTTPS connection with SSL V3 or previous version	Select this checkbox to have the Zyxel Device block HTTPS web pages using SSL V3 or a previous version.
Content Filter Category Service Timeout	Specify the allowable time period in seconds for accessing the external web filtering service's server.
Denied Access Message	Enter a message to be displayed when content filter blocks access to a web page. Use up to 127 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator". It is also possible to leave this field blank if you have a URL specified in the Redirect URL field. In this case if the content filter blocks access to a web page, the Zyxel Device just opens the web page you specified without showing a denied access message.
Redirect URL	Enter the URL of the web page to which you want to send users when their web access is blocked by content filter. The web page you specify here opens in a new frame below the denied access message. Use "http://" or "https://" followed by up to 255 characters (0-9a-zA-Z;/?:@&=+$.-_!~*'()%). For example, http://192.168.1.17/blocked access.
Test Web Site Category	
URL to test	You can check which category a web page belongs to. Enter a web site URL in the text box. When the content filter is active, you should see the web page's category. The query fails if the content filter is not active. Content Filtering can query a category by full URL string (for example, http://www.google.com/picture/index.htm), but HTTPS Domain Filter can only query a category by domain name ('www.google.com'), so the category may be different in the query result. URL to test displays both results in the test.
If you think the category is incorrect, click this link to submit a request to review it	Click this link to see the category recorded in the Zyxel Device's content filtering database for the web page you specified (if the database has an entry for it).
Profile Management	
Add	Click Add to create a new content filter rule.
Edit	Click Edit to make changes to a content filter rule.
Remove	Click Remove the delete a content filter rule.
References	Select an entry and click References to open a screen that shows which settings use the entry. . Click Refresh to update information on this screen.
#	This column lists the index numbers of the content filter profile.
Name	This column lists the names of the content filter profile rule.
Description	This column lists the description of the content filter profile rule.
Reference	This displays the number of times an Object Reference is used in a rule.
Action	Click this icon to apply the content filter profile with a security policy. Go to the Configuration > Security Policy > Policy Control screen to check the result.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

27.2.1 Apply to a Security Policy

Click the icon in the Action field to apply the entry to a security policy.

Go to the Configuration > Security Policy > Policy Control screen to check the result.

Figure 421 Configuration > Security Service > Content Filter > Action



The following table describes the labels in this screen.

Table 194 Configuration > Security Service > Content Filter > Action

LABEL	DESCRIPTION
Show Filter/Hide Filter	Click Show Filter to display IPv4 and IPv6 (if enabled) security policy search filters.
IPv4 / IPv6 Configuration	Use IPv4 / IPv6 search filters to find specific IPv4 and IPv6 (if enabled) security policies based on direction, application, user, source, destination and/or schedule.

Table 194 Configuration > Security Service > Content Filter > Action

LABEL	DESCRIPTION
From / To	Select a zone to view all security policies from a particular zone and/or to a particular zone. any means all zones.
IPv4 / IPv6 Source	Type an IPv4 or IPv6 IP address to view all security policies based on the IPv4 / IPv6 source address object used. • An IPv4 IP address is written as four integer blocks separated by periods. This is an example IPv4 address: 172.16.6.7. • 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.
IPv4 / IPv6 Destination	Type an IPv4 or IPv6 IP address to view all security policies based on the IPv4 / IPv6 destination address object used. • An IPv4 IP address is written as four integer blocks separated by periods. This is an example IPv4 address: 172.16.6.7. • 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.
Service	View all security policies based the service object used.
User	View all security policies based on user or user group object used.
Schedule	View all security policies based on the schedule object used.
Priority	This is the position of your Security Policy in the global policy list (including all through-Zyxel Device and to-Zyxel Device policies). The ordering of your policies is important as policies are applied in sequence. Default displays for the default Security Policy behavior that the Zyxel Device performs on traffic that does not match any other Security Policy.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This is the name of the Security policy.
From / To	This is the direction of travel of packets. Select from which zone the packets come and to which zone they go. Security Policies are grouped based on the direction of travel of packets to which they apply. For example, from LAN to LAN means packets traveling from a computer or subnet on the LAN to either another computer or subnet on the LAN. From any displays all the Security Policies for traffic going to the selected To Zone. To any displays all the Security Policies for traffic coming from the selected From Zone. From any to any displays all of the Security Policies. To ZyWALL policies are for traffic that is destined for the Zyxel Device and control which computers can manage the Zyxel Device.
IPv4 / IPv6 Source	This displays the IPv4 / IPv6 source address object, including geographic address and FQDN (group) objects, to which this Security Policy applies.
IPv4 / IPv6 Destination	This displays the IPv4 / IPv6 destination address object, including geographic address and FQDN (group) objects, to which this Security Policy applies.
Service	This displays the service object to which this Security Policy applies.
User	This is the user name or user group name to which this Security Policy applies.
Schedule	This field tells you the schedule object that the policy uses. none means the policy is active at all times if enabled.
Action	This field displays whether the Security Policy silently discards packets without notification (deny), permits the passage of packets (allow) or drops packets with notification (reject)
Log	Select whether to have the Zyxel Device generate a log (log), log and alert (log alert) or not (no) when the policy is matched to the criteria listed above.

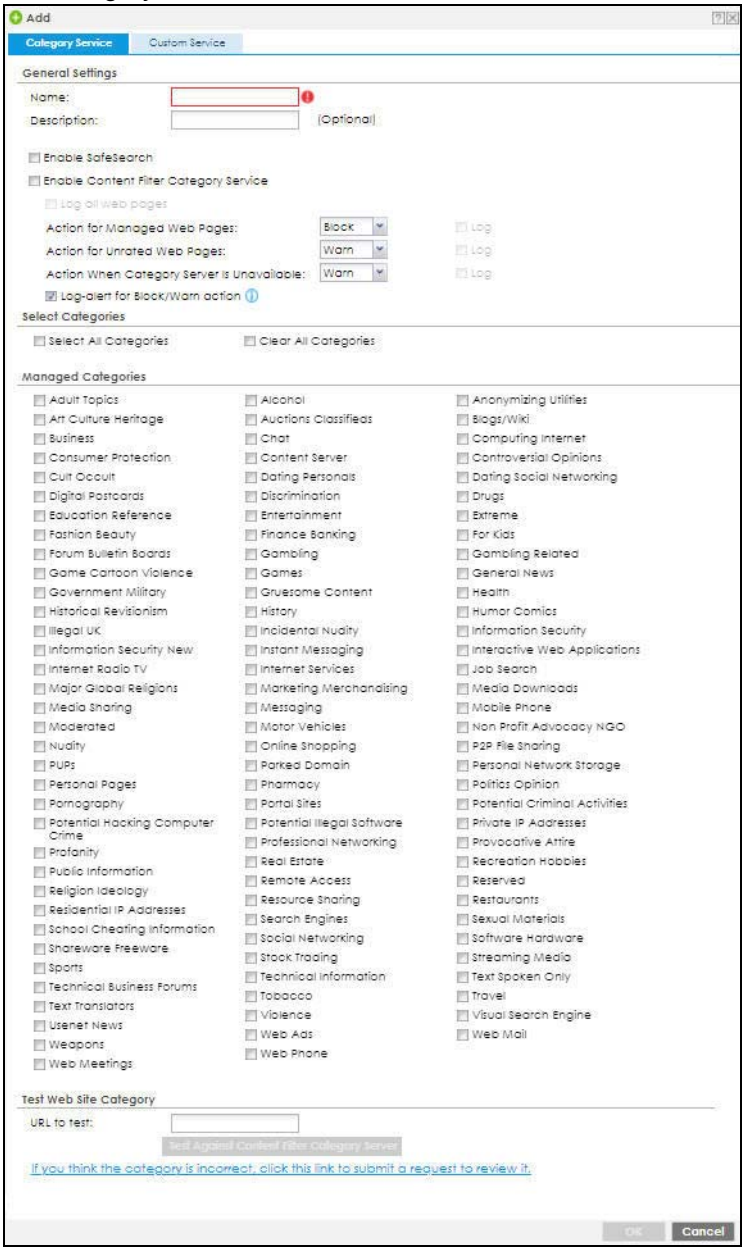
Table 194 Configuration > Security Service > Content Filter > Action

LABEL	DESCRIPTION
Profile	This field shows you which Security Service profiles apply to this security policy. Click an applied Security Service profile icon to edit the profile directly.
OK	Click OK to save your changes back to the Zyxel Device.

27.2.2 Web Content Filter Add Category Service

Click Configuration > Security Service > Content Filter > Web Content Filter > General > Add or Edit to open the Add screen.

Figure 422 Configuration > Security Service > Content Filter > Web Content Filter > General > Add > Category Service



The following table describes the labels in this screen.

Table 195 Configuration > Security Service > Content Filter > Web Content Filter > General > Add > Category Service

LABEL	DESCRIPTION
Name	Enter a descriptive name for this content filtering profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description for the content filtering profile rule to help identify the purpose of rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. This field is optional.
Enable SafeSearch	SafeSearch is a search engine that can automatically filter sexually explicit videos and images from the search result without overloading the Zyxel Device. Supported search engines at the time of writing are: Yahoo, Google, MSN Live Bing, Yandex
Enable Content Filter Category Service	Enable external database content filtering to have the Zyxel Device check an external database to find to which category a requested web page belongs. The Zyxel Device then blocks or forwards access to the web page depending on the configuration of the rest of this page.
Log all web pages	Select this to record attempts to access web pages when: • They match the other categories that you select below. • They are not categorized. • The external content filtering database is unavailable.
Action for Managed Web Pages	Select Pass to allow users to access web pages that match the other categories that you select below. Select Block to prevent users from accessing web pages that match the other categories that you select below. When external database content filtering blocks access to a web page, it displays the denied access message that you configured in the Content Filter General screen along with the category of the blocked web page. If a web page matches multiple categories, and at least one of those categories is blocked, that web page will be blocked. If a web page matches multiple categories, and at least one of those categories is blocked, that web page will be blocked. If a web page matches multiple categories, and at least one of those categories is blocked, that web page will be blocked. Select Log to record attempts to access web pages that match the other categories that you select below.
Action for Unrated Web Pages	Select Pass to allow users to access web pages that the external web filtering service has not categorized. Select Block to prevent users from accessing web pages that the external web filtering service has not categorized. When the external database content filtering blocks access to a web page, it displays the denied access message that you configured in the Content Filter General screen along with the category of the blocked web page. Select Warn to display a warning message before allowing users to access web pages that the external web filtering service has not categorized. Select Log to record attempts to access web pages that are not categorized.

Table 195 Configuration > Security Service > Content Filter > Web Content Filter > General > Add > Category Service (continued)

LABEL	DESCRIPTION
Action When Category Server Is Unavailable	Select Pass to allow users to access any requested web page if the external content filtering database is unavailable. Select Block to block access to any requested web page if the external content filtering database is unavailable. Select Warn to display a warning message before allowing users to access any requested web page if the external content filtering database is unavailable. The following are possible causes for the external content filtering server not being available: • There is no response from the external content filtering server within the time period specified in the Content Filter Server Unavailable Timeout field. • The Zyxel Device is not able to resolve the domain name of the external content filtering database. • There is an error response from the external content filtering database. This can be caused by an expired content filtering registration (External content filtering's license key is invalid"). Select Log to record attempts to access web pages that occur when the external content filtering database is unavailable.
Log-alert for Block/Warn action	A log at the alert level is a log for serious events that may need more immediate attention. For example, you may want to know right away if there are clients in your networks that try to access adult topics or drugs related web pages. Set the action to Block or Warn and select Log for Action for Managed Web Pages, Action for Unrated Web Pages or Action When Category Server is Unavailable. Then enable this to have the Zyxel Device generate logs at the alert level instead of the info level. You can check the priority of log messages in Monitor > Log > View Log > Priority.
Select Categories	
Select All Categories	Select this checkbox to restrict access to all site categories listed below.
Clear All Categories	Select this checkbox to clear the selected categories below.
Managed Categories	These are categories of web pages based on their content. Select categories in this section to control access to specific types of Internet content. You must have the Category Service content filtering license to filter these categories. See the next table for category details.
Test Web Site Category	
URL to test	You can check which category a web page belongs to. Enter a web site URL in the text box. When the content filter is active, you should see the web page's category. The query fails if the content filter is not active. Content Filtering can query a category by full URL string (for example, http://www.google.com/picture/index.htm), but HTTPS Domain Filter can only query a category by domain name ('www.google.com'), so the category may be different in the query result. URL to test displays both results in the test.
If you think the category is incorrect	Click this link to see the category recorded in the Zyxel Device's content filtering database for the web page you specified (if the database has an entry for it).
Test Against Content Filter Category Server	Click this button to see the category recorded in the external content filter server's database for the web page you specified.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving your changes.

The following table describes the managed categories.

Table 196 Managed Category Descriptions

CATEGORY	DESCRIPTION
Adult Topics	Web pages that contain content or themes that are generally considered unsuitable for children.
Alcohol	Web pages that mainly sell, promote, or advocate the use of alcohol, such as beer, wine, and liquor. This category also includes cocktail recipes and home-brewing instructions.
Anonymizing Utilities	Web pages that result in anonymous web browsing without the explicit intent to provide such a service. This category includes URL translators, web-page caching, and other utilities that might function as anonymizers, but without the express purpose of bypassing filtering software. This category does not include text translation.
Art Culture Heritage	Web pages that contain virtual art galleries, artist sites (including sculpture and photography), museums, ethnic customs, and country customs. This category does not include online photograph albums.
Auctions Classifieds	Web pages that provide online bidding and selling of items or services. This category includes web pages that focus on bidding and sales. This category does not include classified advertisements such as real estate postings, personal ads, or companies marketing their auctions.
Blogs/Wiki	Web pages containing dynamic content, which often changes because users can post or edit content at any time. This category covers the risks with dynamic content that might range from harmless to offensive.
Business	Web pages that provide business-related information, such as corporate overviews or business planning and strategies. This category also includes information, services, or products that help other businesses plan, manage, and market their enterprises, and multi-level marketing. This category does not include personal pages and web-hosting web pages.
Chat	Web pages that provide web-based, real-time social messaging in public and private chat rooms. This category includes IRC. This category does not include instant messaging.
Computing Internet	Web pages containing reviews, information, buyer's guides of computers, computer parts and accessories, computer software and internet companies, industry news and magazines, and pay-to-surf sites.
Consumer Protection	Websites that try to rob or cheat consumers. Some examples of their activities include selling counterfeit products, selling products that were originally provided for free, or improperly using the brand of another company. This category also includes sites where many consumers reported being cheated or not receiving services. This category does not include phishing, which tries to perpetrate fraud or theft by stealing account information. To check for phishing, go to Security Service > Reputation Filter > IP Reputation and select Phishing.

Table 196 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Content Server	URLs for servers that host images, media files, or JavaScript for one or more sites and are intended to speed up content retrieval for existing web servers, such as Apache. This category includes domain-level and sub-domain-level URLs that function as content servers. This category does not include: • Web pages for businesses that provide the content servers • Web pages that allow users to browse photographs. See the Media Sharing category. • URLs for servers that serve only advertisements. See the Web Ads category.
Controversial Opinions	Web pages that contain opinions that are likely to offend political or social sensibilities and incite controversy. Much of this content is at the extremes of public opinion. This category does not include opinion or language clearly intended to promote hate or discrimination.
Cult Occult	Sites relating to non-traditional religious practices considered to be false, unorthodox, extremist, or coercive.
Dating Personals	Web pages that provide networking for online dating, matchmaking, escort services, or introductions to potential spouses. This category does not include sites that provide social networking that might include dating, but are not specific to dating.
Dating Social Networking	Web pages that focus on social interaction such as online dating, friendship, school reunions, pen-pals, escort services, or introductions to potential spouses. This category does not include wedding-related content, dating tips, or related marketing.
Digital Postcards	Web pages that allow people to send and receive digital postcards and greeting cards through the Internet.
Discrimination	Web pages, which provide information that explicitly encourages the oppression or discrimination of a specific group of individuals. This category does not include jokes and humor, unless the focus of the entire site is considered discriminatory.
Drugs	Websites that provide information on the purchase, manufacture, and use of illegal or recreational drugs. This category does not include sites with exclusive health or political themes.
Education Reference	Web pages devoted to academic-related content such as academic subjects (mathematics, history), school or university web pages, and education administration pages (school boards, teacher curriculum).
Entertainment	Web pages that provide information about cinema, theater, music, television, infotainment, entertainment industry gossip-news, and sites about celebrities such as actors and musicians. This category also includes sites where the content is devoted to providing entertainment on the web, such as horoscopes or fan clubs.
Extreme	Web pages that provide content considered gory, perverse, or horrific.
Fashion Beauty	Web pages that market clothing, cosmetics, jewelry, and other fashion-oriented products, accessories, or services. This category also includes product reviews, comparisons, and general consumer information, and services such as hair salons, tanning salons, tattoo studios, and body-piercing studios. This category does not include fashion-related content such as modeling or celebrity fashion unless the site focuses on marketing the product line.

Table 196 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Finance Banking	Web pages that provide financial information or access to online financial accounts. This category includes stock information (but not stock trading), home finance, and government-related financial information.
For Kids	Web pages that are family-safe, specifically for children of approximate ages ten and under. This category can also be used as an exception to allow web pages that do not pose a risk to children, or to access sites that have a primary educational or recreational focus for children, but are in other categories such as Games, Humor/Comics, Recreation/Hobbies, or Entertainment.
Forum Bulletin Boards	Web pages that provide access (http://) to Usenet newsgroups or hold discussions and post user-generated content, such as real-time message posting for an interest group. This category also includes archives of files uploaded to newsgroups. This category does not include message forums with a business or technical support focus.
Gambling	Web pages that allow users to wager or place bets online, or provide gambling software that allows online betting, such as casino games, betting pools, sports betting, and lotteries. This category does not include web pages related to gambling that do not allow betting online.
Gambling Related	Web pages that offer information about gambling, without providing the means to gamble. This category includes casino-related web pages that do not offer online gambling, gambling links, tips, sports picks, lottery results, and horse, car, or boat racing.
Game Cartoon Violence	Web pages that provide fantasy or fictitious representations of violence within the context of games, comics, cartoons, or graphic novels. This category includes images and textual descriptions of physical assaults or hand-to-hand combat, and grave injury and destruction caused by weapons or explosives.
Games	Web pages that offer online games and related information such as cheats, codes, demos, emulators, online contests or role-playing games, gaming clans, game manufacturer sites, fantasy or virtual sports leagues, and other gaming sites without chances of profit. This category includes gaming consoles.
General News	Web pages that provide online news media, such as international or regional news broadcasting and publication. This category includes portal sites that provide news content.
Government Military	Web pages that contain content maintained by governmental or military organizations, such as government branches or agencies, police departments, fire departments, civil defense, counter-terrorism organizations, or supranational organizations, such as the United Nations or the European Union. This category includes military and veterans' medical facilities.
Gruesome Content	Web pages with content that can be considered tasteless, gross, shocking, or gruesome. This category does not include web pages with content pertaining to physical assault.
Health	Web pages that cover all health-related information and health care services. This category does not include cosmetic surgery, marketing/selling pharmaceuticals, or animal-related medical services.

Table 196 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Historical Revisionism	Web pages that denounce, or offer different interpretations of, significant historical facts, such as holocaust denial. This category does not include all re-examination of historical facts, only historical events that are highly sensitive.
History	Web pages that provide content about historical facts. This category includes content suitable for higher education, but the Education category includes content for primary education. For example, a site with Holocaust photographs might be offensive, but have academic value.
Humor Comics	Web pages that provide comical or funny content. This category includes sites with jokes, sketches, comics, and satire pages. This category might also include graphic novel content, which is often associated with comics.
Illegal UK	Web pages that contain child sexual abuse content hosted anywhere in the world, and criminally obscene and incitement to racial hatred content hosted in the UK.
Incidental Nudity	Web pages that contain non-pornographic images of the bare human body like those in classic sculpture and paintings, or medical images. This category enables you to allow or block sites in order to address cultural or geographic differences in opinion about nudity. For example, you can use this category to block access to nudity, but allow access when nudity is not the primary focus of a site, such as news sites or major portals.
Information Security	Web pages that legitimately provide information about data protection. This category includes detailed information for safeguarding business or personal data, intellectual property, privacy, and infrastructure on the Internet, private networks, or in other bandwidth services such as telecommunications. This category does not include: • Legitimate information security companies and security software providers, such as virus protection companies. • Sites that intend to exploit security or teach how to bypass security.
Information Security New	Web pages that legitimately provide information about data protection. This category includes detailed information for safeguarding business or personal data, intellectual property, privacy, and infrastructure on the Internet, private networks, or in other bandwidth services such as telecommunications. This category does not include: • Legitimate information security companies and security software providers, such as virus protection companies. • Sites that intend to exploit security or teach how to bypass security.
Instant Messaging	Web pages that provide software for real-time communication over a network exclusively for users who joined a member's contact list or an instant-messaging session. Most instant-messaging software includes features such as file transfer, PC-to-PC phone calls, and can track when other people log on and off.
Interactive Web Applications	Web pages that provide access to live or interactive web applications, such as browser-based office suites and groupware. This category includes sites with business, academic, or individual focus. This category does not include sites providing access to interactive web applications that do not take critical user data or offer security risks, such as Google Maps.

Table 196 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Internet Radio TV	Web pages that provide software or access to continuous audio or video broadcasting, such as Internet radio, TV programming, or podcasting. Quick downloads and shorter streams that consume less bandwidth are in the Streaming Media or Media Downloads categories.
Internet Services	Web pages that provide services for publication and maintenance of Internet sites such as web design, domain registration, Internet Service Providers, and broadband and telecommunications companies that provide web services. This category includes web utilities such as statistics and access logs, and web graphics like clip art.
Job Search	Web pages related to a job search including sites concerned with resume writing, interviewing, changing careers, classified advertising, and large job databases. This category also includes corporate web pages that list job openings, salary comparison sites, temporary employment, and company job-posting sites. This category does not include make-money-at-home sites.
Major Global Religions	Web pages with content about religious topics and information related to major religions. This category includes sites that cover religious content such as discussion, beliefs, non-controversial commentary, articles, and information for local congregations such as a church or synagogue homepage. The religions in this category are Baha'i, Buddhism, Chinese Traditional, Christianity, Hinduism, Islam, Jainism, Judaism, Shinto, Sikhism, Tenrikyo, Zoroastrianism.
Marketing Merchandising	Web pages that promote individual or business products or services on the web, but do not sell their products or services online. This category includes websites that are generally a company overview, describing services or products that cannot be purchased directly from these sites. Examples include automobile manufacturer sites, wedding photography services, or graphic design services. This category does not include: • Other categories that imply marketing such as Alcohol, Auctions/Classifieds, Drugs, Finance/Banking, Mobile Phone, Online Shopping, Real Estate, School Cheating Information, Software/Hardware, Stock Trading, Tobacco, Travel, and Weapons. • Sites that market their services only to other businesses. See the Business category. • Sites that rob or cheat consumers. See the Consumer Protection category.
Media Downloads	Web pages that provide audio or video files for download such as MP3, WAV, AVI, and MPEG formats. The files are saved to, and played from, the user's computer. This category does not include audio or video files that are played directly through a browser window. See the Streaming Media category.
Media Sharing	Web pages that allow users to upload, search for, and share media files and photographs, such as online photograph albums.
Messaging	Examples include text messaging to mobile phones, PDAs, fax machines, and internal website user-to-user messaging or site-to-site messaging. This category does not include real-time chat or instant messaging, or message posts that can be viewed by anyone but the intended recipient.
Mobile Phone	Web pages that sell media, software, or utilities for mobile phones that can be downloaded and delivered to mobile phones. Examples include ringtones, logos/skins, games, screen-savers, text-based tunes, and software for SMS, MMS, WAP, and other mobile phone protocols.

Table 196 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Moderated	Bulletin boards, chat rooms, search engines, or web mail sites that are monitored by an individual or group who has the authority to block messages or content considered inappropriate. This category does not include sites with posted rules against offensive content. See the Forum/Bulletin Boards category.
Motor Vehicles	Websites for manufacturers and dealerships of consumer transportation vehicles, such as cars, vans, trucks, SUVs, motorcycles, and scooters. This category also includes sites that provide product marketing, reviews, comparisons, pricing information, auto fairs, auto expos, and general consumer information about motor vehicles. This category does not include automotive accessories, mechanics, auto-body shops, and recreational hobby pages. This category does not include sites that provide business-to-business-only content regarding motor vehicles.
Non Profit Advocacy NGO	Web pages from charitable or educational groups that fulfill a stated mission, benefiting the larger community, such as clubs, lobbies, communities, non-profit organizations, labor unions, and advocacy groups. Examples are Masons, Elks, Boy and Girl Scouts, or Big Brothers.
Nudity	Web pages that have non-pornographic images of the bare human body. This category includes classic sculpture and paintings, artistic nude photographs, some naturism pictures, and detailed medical illustrations. This category does not include high-profile sites where nudity is not a concern for visitors. See the Incidental Nudity category.
Online Shopping	Web pages that sell products or services online. Web pages selling a broad range of products might pose a risk to users by offering access to items that are normally in other categories such as Pornography, Weapons, Nudity, or Violence. Web pages selling such content exclusively are in their respective categories.
P2P File Sharing	Web pages that allow the exchange of files between computers and users for business or personal use, such as downloadable music. P2P clients allow users to search for and exchange files from a peer-user network. They often include spyware or real-time chat capabilities. This category includes BitTorrent web pages.
Parked Domain	Web pages that once served content, but their domains have been sold or abandoned and are no longer registered. Parked domains do not host their own content, but usually redirect users to a generic page that states the domain name is for sale, or redirect users to a generic search engine and portal page, some of which provide valid search engine results.
Personal Network Storage	Web pages that allow users to upload folders and files to an online network server in order to backup, share, edit, or retrieve files or folders from any web browser.
Personal Pages	Personal home pages that share a common domain such as those hosted by ISPs, university/education servers, or free web page hosts. This category also includes unique domains that contain personal information, such as a personal home page. This category does not include home pages of public figures.
Pharmacy	Web pages that provide reviews, descriptions, and market or sell prescription-based drugs, over-the-counter drugs, birth control, or dietary supplements.
Politics Opinion	Web pages covering political parties, individuals in political life, and opinion on various topics. This category might also cover laws and political opinion about drugs. This category includes URLs for political parties, political campaigning, and opinions on various topics, including political debates.

Table 196 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Pornography	Web pages that contain materials intended to be sexually arousing or erotic. This category includes fetish pages, animation, cartoons, stories, and illegal pornography.
Portal Sites	Web pages that serve as major gateways or directories to content on the web. Many portal sites also provide a variety of internal site features or services such as search engines, email, news, and entertainment. Mailing list sites with a variety of content are in this category. This category does not include sites with topic-specific content.
Potential Criminal Activities	Web pages that provide instructions to commit illegal or criminal activities. Instructions include committing murder or suicide, sabotage, bomb-making, lock-picking, service theft, evading law enforcement, or spoofing drug tests. This category might also include information on how to distribute illegal content, perpetrate fraud, or consumer scams. This category does not include computer-related fraud.
Potential Hacking Computer Crime	Web pages that provide instructions, or otherwise enable, fraud, crime, or malicious activity that is computer-oriented. This category includes web pages related to computer crime include malicious hacking information or tools that help individuals gain unauthorized access to computers and networks (root kits, kiddy scripts). This category also includes other areas of electronic fraud such as dialer scams and illegal manipulation of electronic devices. This category does not include illegal software.
Potential Illegal Software	Web pages, which the filter believes offer information to potentially ‘pirated’ or illegally distribute software or electronic media, such as copyrighted music or film, distribution of illegal license key generators, software cracks, and serial numbers. This category does not include peer-to-peer web pages.
Private IP Addresses	Sites that are private IP addresses as defined in RFC 1918, that is, hosts that do not require access to hosts in other enterprises (or require just limited access) and whose IP address may be ambiguous between enterprises but are well defined within a certain enterprise.
Profanity	Web pages that contain crude, vulgar, or obscene language or gestures.
Professional Networking	Web pages that provide social networking exclusively for professional or business purposes. This category includes sites that provide personal or group profiles, and enable their members to interact through real-time communication, message posting, public bulletins, and media sharing. This category also contains alumni sites that have a networking function. This category does not include social networking sites where the focus might vary, but include friendship, dating, or professional focuses.
Provocative Attire	Web pages with pictures that include alluring or revealing attire, lingerie and swimsuits, or supermodel or celebrity photograph collections, but do not involve nudity. This category does not include sites with swimwear or similar attire that is not intended to be provocative. For example, Olympic swimming sites are not in this category.
Public Information	Web pages that provide general reference information such as public service providers, regional information, transportation schedules, maps, or weather reports.

Table 196 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
PUPs	Web pages that contain Potentially Unwanted Programs (PUPs). PUPs are often made for a beneficial purpose but they alter the security of a computer or the computer user's privacy. Computer users who are concerned about security or privacy might want to be informed about this software, and in some cases, they might want to remove this software from their computers.
Real Estate	Web pages that provide commercial or residential real estate services and information. Service and information includes sales and rental of living space or retail space and guides for apartments, housing, and property, and information on appraisal and brokerage. This category includes sites that allow you to browse model homes. This category does not include content related to personal finance, such as credit applications.
Recreation Hobbies	Web pages for recreational organizations and facilities that include content devoted to recreational activities and hobbies. This category includes information about public swimming pools, zoos, fairs, festivals, amusement parks, recreation guides, hiking, fishing, bird watching, or stamp collecting. This category does not include activities that need no active participation, such as watching a movie or reading celebrity gossip.
Religion Ideology	Web pages with content related to religious topics and beliefs in human spirituality that are not within the major religions. This category includes religious discussion, beliefs, articles, and information for local congregations or groups such as a church homepage, unless the site is already in the Major Global Religions category. This category also includes comparative religion, or sites that include religions and ideologies. This category does not include astrology and horoscope sites
Remote Access	Web pages that provide remote access to a program, online service, or an entire computer system. Although remote access is often used legitimately to run a computer from a remote location, it creates a security risk, such as backdoor access. Backdoor access, written by the original programmer, allows the system to be controlled by another party without the user's knowledge.
Reserved	This category is reserved for future use.
Residential IP Addresses	IP addresses (and any domains associated with them) that access the Internet by DSL modems or cable modems. Because this content is not generally intended for Internet access through HTTP, access to the Internet through these IP addresses can indicate suspicious behavior. This behavior might be related to malware located on the home computer or homegrown gateways set up to allow anonymous Internet access.
Resource Sharing	Web pages that harness idle or unused computer resources to focus on a common task. The task can be on a company or an international basis. Well known examples are the SETI program and the Human Genome Project, which use the idle time of thousands of volunteered computers to analyze data.

Table 196 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Restaurants	Web pages that provide information about restaurants, bars, catering, take-out and delivery, including online ordering. This category includes sites that provide information about location, hours, prices, menus and related dietary information. This category also includes restaurant guides and reviews, and cafes and coffee shops. This category does not include groceries, wholesale food, non-profit and charitable food organizations, or bars that do not focus on serving food.
School Cheating Information	Web pages that promote plagiarism or cheating by providing free or fee-based term papers, written essays, or exam answers. This category does not include sites that offer student help, discuss literature, films, or books, or other content that is often the subject of research papers.
Search Engines	Web pages that provide search results that enable users to find information on the Internet based on key words. This category does not include site-specific search engines.
Sexual Materials	Web pages that describe or depict sexual acts, but are not intended to be arousing or erotic. Examples of sexual materials include sex education, sexual innuendo, humor, or sex related merchandise. This category does not include web pages with content intended to arouse.
Shareware Freeware	Web pages that are repositories of downloadable copies of shareware and freeware. This category does not include subscription-based software.
Social Networking	Web pages that enable social networking for a variety of purposes, such as friendship, dating, professional, or topics of interest. These sites provide personal or group profiles and enable interaction among their members through real-time communication, message posting, public bulletins, and media sharing. This category does not include sites that are exclusive to dating, matchmaking, or a specific professional networking focus.
Software Hardware	Web pages related to computing software and hardware, including vendors, product marketing and reviews, deployment and maintenance of software and hardware, and software updates and add-ons such as scripts, plug-ins, or drivers. Hardware includes computer parts, accessories, and electronic equipment used with computers and networks. This category includes the marketing of software and hardware, and magazines focused on software or hardware product reviews or industry trends.
Sports	Web pages related to professional or organized recreational sports. This category includes sporting news, events, and information such as playing tips, strategies, game scores, or player trades. This category does not include fantasy leagues, sports centers, athletic clubs, fitness or martial arts clubs, and non-league billiards, darts, or other such activities.
Stock Trading	Web pages that offer purchasing, selling, or trading of shares online. This category also includes ticker-tape information that enables viewing of real-time stock prices and financial spread betting in the stock market. Other betting is in the Gambling category. This category does not include sites that offer information about stocks, but do not offer purchasing, selling, or trading of shares.

Table 196 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Streaming Media	Web pages that provide streaming media, or contain software plug-ins for displaying audio and visual data before the entire file has been transmitted. This category does not include audio or video files that are downloaded to a user's computer before being played.
Technical Business Forums	Web pages with a technical or business focus that provide online message posting or real-time chatting, such as technical support or interactive business communication. Although users can post any type of content, these forums tend to present less risk of containing offensive content. Sites that offer a variety of forums with themes, including technical and business content, are only in the categories of Forum/Bulletin Boards or Chat.
Technical Information	Web pages that provide computing information with an educational focus in areas such as Information Technology, computer programming, and certification. Examples include Linux user groups, UNIX commands, software tutorials, or dictionaries of technical terms. Most sites in this category might be subdirectories of larger domains. For example, a software site with a tutorial page is in this category only at the tutorial page URL. This category does not include content about information security.
Text Spoken Only	Content that is text or audio only, and does not contain pictures. This category can be used as an exception to allow explicit text and recorded material to be accessed when you want pictures blocked using the Pornography, Violence, or Sexual Materials categories. Libraries or universities can use this category to prevent the display of offensive graphics in their public facilities.
Text Translators	Web pages that allow users to type phrases or a block of text to translate it from one language into another. This category also includes language identifier web pages. URL translation is in the Anonymizing Utilities category.
Tobacco	Web pages that sell, promote, or advocate the use of tobacco products, tobacco paraphernalia, including cigarettes, cigars, pipes, snuff and chewing tobacco.
Travel	Web pages that promote personal or business travel, such as hotels, resorts, airlines, ground transportation, car rentals, travel agencies, and general tourist and travel information. This category also includes sites for buying tickets or accommodation. This category does not include personal vacation photographs.
Usenet News	Web pages that provide access (http://) to Usenet newsgroups and archives of files uploaded to newsgroups. This category also includes online groups that offer similar community-oriented content posting.
Violence	Web pages that contain real or lifelike images or text that portray, describe, or advocate physical assaults against people, animals, or institutions, such as depictions of war, suicide, mutilation, or dismemberment.
Visual Search Engine	Web pages that provide image-specific search results such as thumbnail pictures. This category does not include sites that offer site-specific visual search engines.

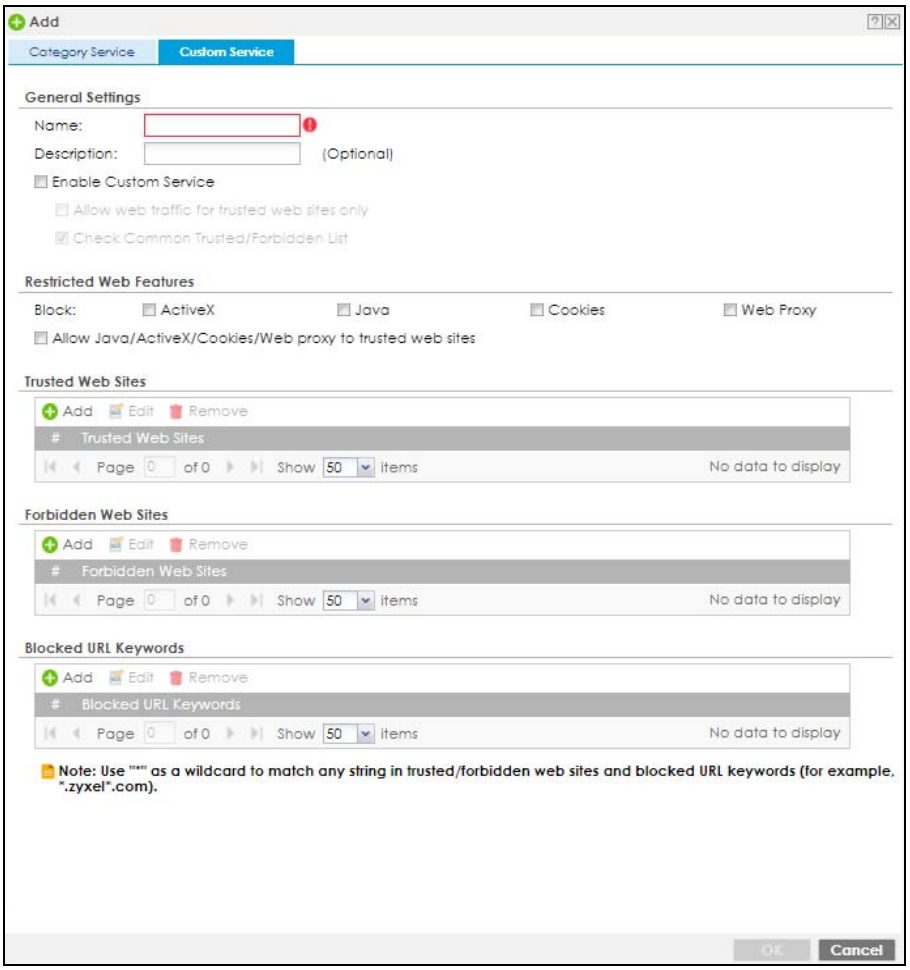
Table 196 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Weapons	Web pages that provide information about buying, making, modifying, or using weapons, such as guns, knives, swords, paintball guns, and ammunition, explosives, and weapon accessories. This category also includes sites that contain content for: weapons for personal or military use, homemade weapons, non-lethal weapons such as mace, pepper spray, or Taser guns, weapons facilities, such as shooting ranges, and government or military oriented weapons. This category does not include political action groups, such as the NRA.
Web Ads	Web pages that provide advertisement-hosting or programs that create advertisements. Examples include links, source code or applets for banners, popups, and other kinds of static or dynamically generated advertisements that appear on web pages. This category is intended to block advertisements on web pages, not the companies that provide the advertisements or advertising services. This category does not include aggressive advertising adware. See the Spyware/Adware category.
Web Mail	Web pages that enable users to send or receive email through the Internet.
Web Meetings	Web pages that host live meetings, video conferences, and interactive presentations mainly for businesses. Web meetings generally include streaming audio and video, and allow data transfer or office-oriented application sharing, such as online presentations.
Web Phone	Web pages that enable users to make telephone calls through the Internet or obtain information or software for this purpose. Web Phone service is also called Internet Telephony, or VoIP. Web phone service includes PC-to-PC, PC-to-phone, and phone-to-phone services connecting through TCP/IP networks.

27.2.3 Content Filter Add Filter Profile Custom Service

Click Configuration > Security Service > Content Filter > Web Content Filter > General > Add or Edit > Custom Service to open the Custom Service screen. You can create a list of good (allowed) web site addresses and a list of bad (blocked) web site addresses. You can also block web sites based on whether the web site's address contains a keyword. Use this screen to add or remove specific sites or keywords from the filter list.

Figure 423 Configuration > Security Service > Content Filter > Web Content Filter > General > Custom Service



The following table describes the labels in this screen.

Table 197 Configuration > Security Service > Content Filter > Web Content Filter > General > Custom Service

LABEL	DESCRIPTION
Name	Enter a descriptive name for this content filtering profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description for the content filtering profile rule to help identify the purpose of rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. This field is optional.
Enable Custom Service	Select this checkbox to allow trusted web sites and block forbidden web sites. Content filter list customization may be enabled and disabled without re-entering these site names.
Allow Web traffic for trusted web sites only	When this box is selected, the Zyxel Device blocks Web access to sites that are not on the Trusted Web Sites list. If they are chosen carefully, this is the most effective way to block objectionable material.
Check Common Trusted/ Forbidden List	Select this checkbox to check the common trusted and forbidden web sites lists. See Section 27.3 on page 625 and Section 27.4 on page 626 for information on configuring these lists.

Table 197 Configuration > Security Service > Content Filter > Web Content Filter > General > Custom Service (continued)

LABEL	DESCRIPTION
Restricted Web Features	Select the checkbox(es) to restrict a feature. Select the checkbox(es) to restrict a feature. • When you download a page containing ActiveX or Java, that part of the web page will be blocked with an X. • When you download a page coming from a Web Proxy, the whole web page will be blocked. • When you download a page containing cookies, the cookies will be removed, but the page will not be blocked.
Block ActiveX	ActiveX is a tool for building dynamic and active web pages and distributed object applications. When you visit an ActiveX web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	Java is a programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Cookies are files stored on a computer's hard drive. Some web servers use them to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Allow Java/ActiveX/Cookies/ Web proxy to trusted web sites	When this box is selected, the Zyxel Device will permit Java, ActiveX and Cookies from sites on the Trusted Web Sites list to the LAN. In certain cases, it may be desirable to allow Java, ActiveX or Cookies from sites that are known and trusted.
Trusted Web Sites	These are sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This displays the index number of the trusted web sites.
Trusted Web Site	This column displays the trusted web sites already added. Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are allowed. For example, entering "*.zyxel.com" also allows "www.zyxel.com", "partner.zyxel.com", "press.zyxel.com", and so on. You can also enter just a top level domain. For example, enter "*.com" to allow all .com domains. Use up to 127 characters (0-9a-z-). The casing does not matter. "*" can be used as a wildcard to match any string. The entry must contain at least one "." or it will be invalid.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This displays the index number of the forbidden web sites.

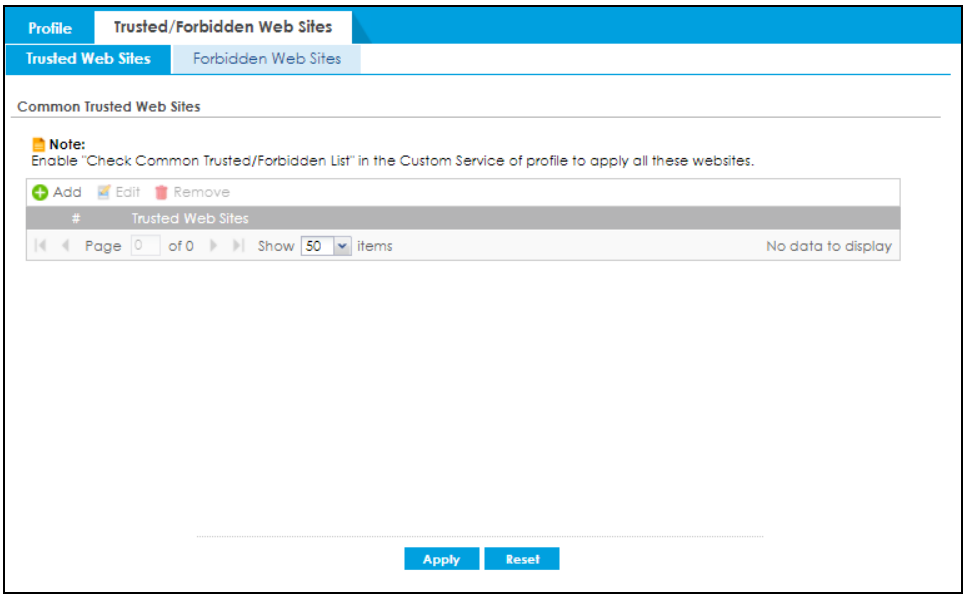
Table 197 Configuration > Security Service > Content Filter > Web Content Filter > General > Custom Service (continued)

LABEL	DESCRIPTION
Forbidden Web Sites	This list displays the forbidden web sites already added. Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include “http://”. All subdomains are also blocked. For example, entering “*bad-site.com” also blocks “www.bad-site.com”, “partner.bad-site.com”, “press.bad-site.com”, and do on. You can also enter just a top level domain. For example, enter “*.com” to block all .com domains. Use up to 127 characters (0-9a-z-). The casing does not matter. “*” can be used as a wildcard to match any string. The entry must contain at least one “.” or it will be invalid.
Blocked URL Keywords	This section allows you to block Web sites with URLs that contain certain keywords in the domain name or IP address.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This displays the index number of the blocked URL keywords.
Blocked URL Keywords	This list displays the keywords already added. Enter a keyword or a numerical IP address to block. You can also enter a numerical IP address. Use up to 127 case-insensitive characters (0-9a-zA-Z;/?:@&=+$\.-_!~*()%). “*” can be used as a wildcard to match any string. Use “|*” to indicate a single wildcard character. For example enter *Bad_Site* to block access to any web page that includes the exact phrase Bad_Site. This does not block access to web pages that only include part of the phrase (such as Bad for example).
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving your changes.

27.3 Web Content Filter Trusted Web Sites Screen

Click Configuration > Security Service > Content Filter > Web Content Filter > Trusted/Forbidden Web Sites> Trusted Web Sites to open the Trusted Web Sites screen. You can create a common list of good (allowed) web site addresses. When you configure Web Content Filter Profiles, you can select the option to check the Common Trusted Web Sites list. Use this screen to add or remove specific sites from the filter list.

Figure 424 Configuration > Security Service > Content Filter > Web Content Filter > Trusted/Forbidden Web Sites> Trusted Web Sites



The following table describes the labels in this screen.

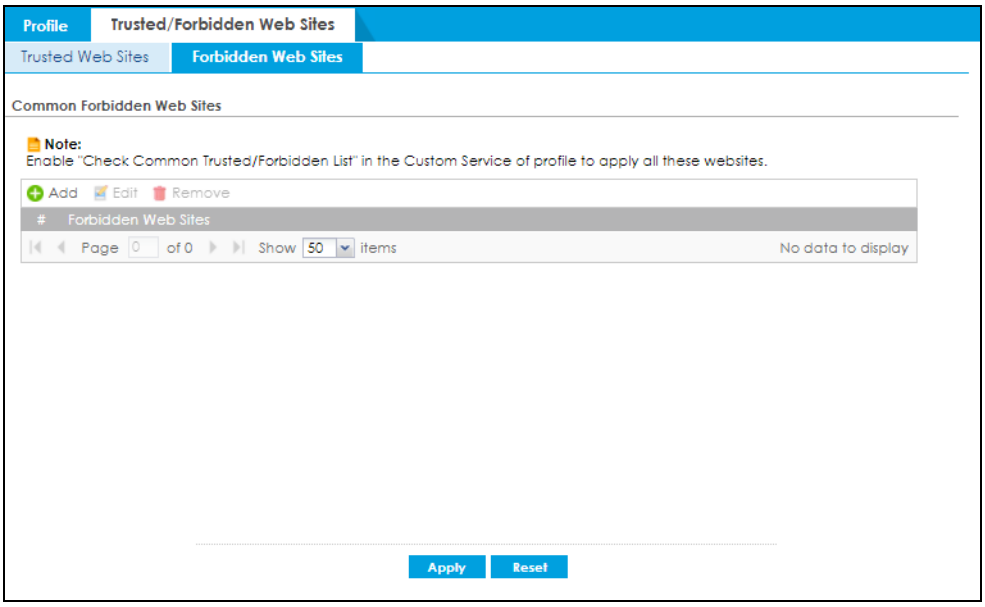
Table 198 Configuration > Security Service > Content Filter > Web Content Filter > Trusted/Forbidden Web Sites> Trusted Web Sites

LABEL	DESCRIPTION
Common Trusted Web Sites	These are sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This displays the index number of the trusted web sites.
Trusted Web Site	This column displays the trusted web sites already added. Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include “http://”. All subdomains are allowed. For example, entering “*.zyxel.com” also allows “www.zyxel.com”, “partner.zyxel.com”, “press.zyxel.com”, and so on. You can also enter just a top level domain. For example, enter .com to allow all .com domains. Use up to 127 characters (0-9a-z-). The casing does not matter.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

27.4 Web Content Filter Forbidden Web Sites Screen

Click Configuration > Security Service > Content Filter > Web Content Filter > Trusted/Forbidden Web Sites> Forbidden Web Sites to open the Forbidden Web Sites screen. You can create a common list of bad (blocked) web site addresses. When you configure Filter Profiles, you can select the option to check the Common Forbidden Web Sites list. Use this screen to add or remove specific sites from the filter list.

Figure 425 Configuration > Security Service > Content Filter > Web Content Filter > Trusted/Forbidden Web Sites> Forbidden Web Sites



The following table describes the labels in this screen.

Table 199 Configuration > Security Service > Content Filter > Web Content Filter > Trusted/Forbidden Web Sites> Forbidden Web Sites

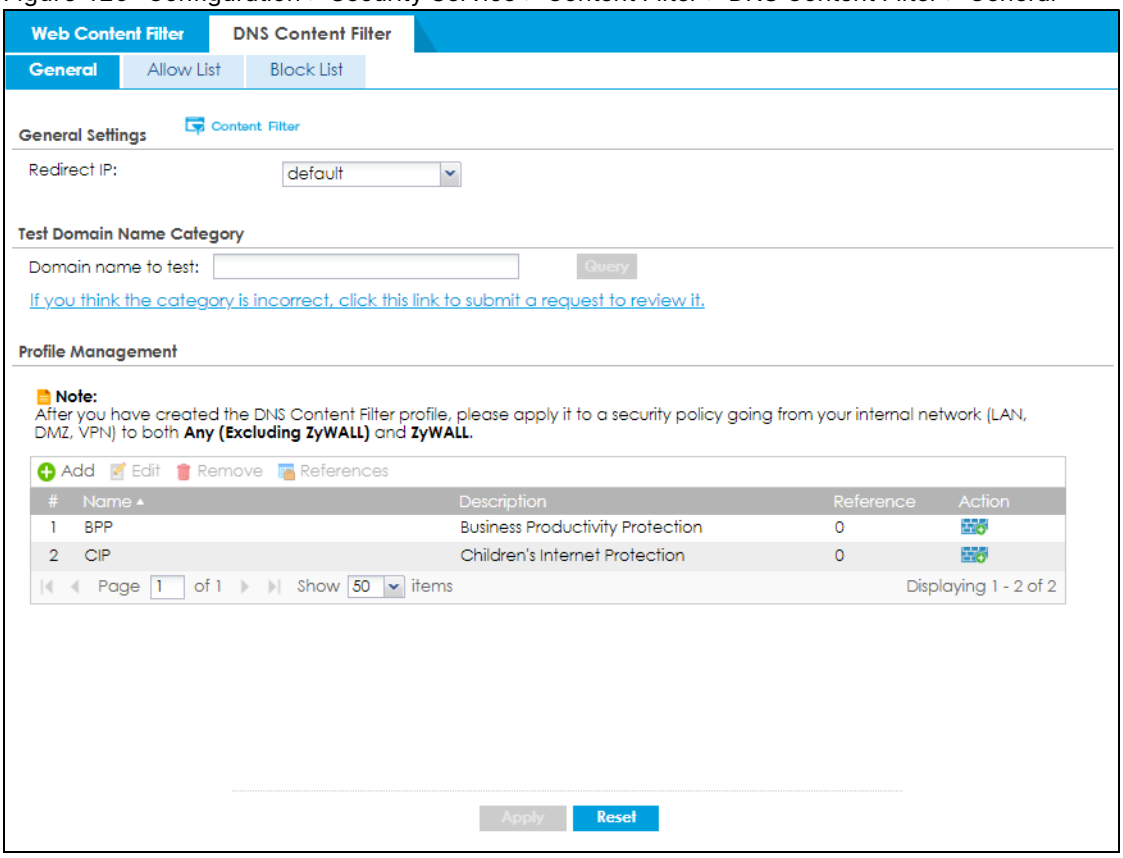
LABEL	DESCRIPTION
Forbidden Web Site List	Sites that you want to block access to, regardless of their content rating, can be allowed by adding them to this list.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This displays the index number of the forbidden web sites.
Forbidden Web Sites	This list displays the forbidden web sites already added. Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are also blocked. For example, entering "bad-site.com" also blocks "www.bad-site.com", "partner.bad-site.com", "press.bad-site.com", and do on. You can also enter just a top level domain. For example, enter .com to block all .com domains. Use up to 127 characters (0-9a-z-). The casing does not matter.
Apply	Click Apply to save your changes back to the Zyxel Device.
Cancel	Click Reset to return the screen to its last-saved settings.

27.5 DNS Content Filter General Screen

Click Configuration > Security Service> Content Filter > DNS Content Filter > General to open the DNS Content Filter General screen.Use this screen to view and order your list of DNS content filter policies, specify a redirect URL and check your external web filtering service registration status. See Section 27.1.2 on page 602 for more information on DNS content filter.

Click the Content Filter icon for more information on the Zyxel Device's security features.

Figure 426 Configuration > Security Service > Content Filter > DNS Content Filter > General



The following table describes the labels in this screen.

Table 200

LABEL	DESCRIPTION
General Settings	
Redirect IP	The URL of the web page to which you want to send users when their web access is blocked by DNS content filtering. The web page you specify here opens in a new frame below the denied access message. Select default to send users to the default web page when their web access is blocked by DNS content filter. Select custom defined to send users to the web page you set when their web access is blocked by DNS content filter. Use "http://" followed by up to 255 characters (0-9 a-z A-Z;/?:@&=+$\.-_!~*'()%) in quotes. For example, "http://192.168.2.17/blocked access". IPv6 format support: http://[2001::1]/blocked_access
Test Web Site Category	

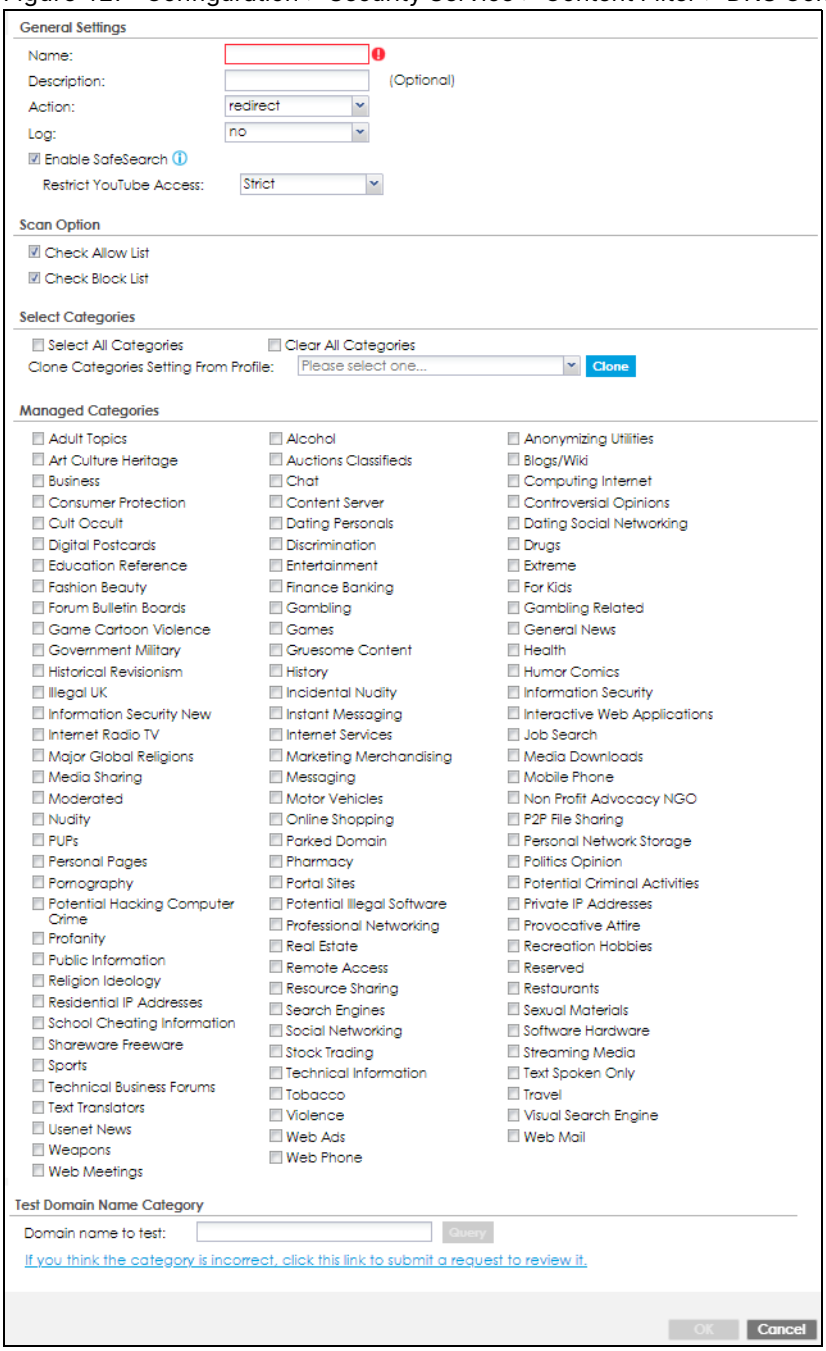
Table 200

LABEL	DESCRIPTION
URL to test	You can check which category a web page belongs to. Enter a web site URL in the text box. When the content filter is active, you should see the web page's category. The query fails if the content filter is not active. Content Filtering can query a category by full URL string (for example, http://www.google.com/picture/index.htm), but HTTPS Domain Filter can only query a category by domain name ('www.google.com'), so the category may be different in the query result. URL to test displays both results in the test.
If you think the category is incorrect, click this link to submit a request to review it	Click this link to see the category recorded in the Zyxel Device's content filtering database for the web page you specified (if the database has an entry for it).
Profile Management	
Add	Click Add to create a new content filter profile.
Edit	Click Edit to make changes to a content filter profile.
Remove	Click Remove the delete a content filter profile.
References	Select an entry and click References to open a screen that shows which settings use the entry. . Click Refresh to update information on this screen.
#	This column lists the index numbers of the content filter profile.
Name	This column lists the names of the content filter profile.
Description	This column lists the description of the content filter profile.
Reference	This displays the number of times an Object Reference is used in a rule.
Action	Click this icon to apply the content filter profile with a security policy. Go to the Configuration > Security Policy > Policy Control screen to check the result.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

27.5.1 DNS Content Filter Add Profile

Click Configuration > Security Service > Content Filter > DNS Content Filter > General > Add or Edit to open the Add screen.

Figure 427 Configuration > Security Service > Content Filter > DNS Content Filter > General > Add



The following table describes the labels in this screen.

Table 201

LABEL	DESCRIPTION
Name	Enter a descriptive name for this content filtering profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description for the content filtering profile rule to help identify the purpose of rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. This field is optional.
Action	Select pass to allow users to access web pages that match the other categories that you select below. Select redirect to send users to the default redirect web page or the web page you set
Log	Select log if you want the Zyxel Deviceto create a log recording the attempts to access web pages that match the categories you select below. Select alert if you want the Zyxel Device to create an alert log recording the attempts to access web pages that match the categories you select below. Select none if you don't want the Zyxel Device to create a log.
Enable SafeSearch	SafeSearch is a search engine that can automatically filter sexually explicit videos and images from the search result without overloading the Zyxel Device. Supported search engines at the time of writing are: • YouTube • Google • MSN Live Bing
Restrict YouTube Access	Select Strict to better protect the Zyxel Device clients from seeing pornography, potentially offensive and inappropriate videos. Select Moderate to allow YouTube to display more videos in the search result.
Scan Option	
Check White List	Select this to check if the IP addresses of the web pages users try to access are listed in the DNS content filter white list.
Check Black List	Select this to check if the IP addresses of the web pages users try to access are listed in the DNS content filter black list.
Select Categories	
Select All Categories	Select this checkbox to restrict access to all site categories listed below.
Clear All Categories	Select this checkbox to clear the selected categories below.
Clone Categories Setting From Profile	Choose an existing profile from the drop down list if you want the profile you are currently configuring to use the same categories setting as one of the existing profile.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving your changes.

The following table describes the managed categories.

Table 202 Managed Category Descriptions

CATEGORY	DESCRIPTION
Adult Topics	Web pages that contain content or themes that are generally considered unsuitable for children.
Alcohol	Web pages that mainly sell, promote, or advocate the use of alcohol, such as beer, wine, and liquor. This category also includes cocktail recipes and home-brewing instructions.
Anonymizing Utilities	Web pages that result in anonymous web browsing without the explicit intent to provide such a service. This category includes URL translators, web-page caching, and other utilities that might function as anonymizers, but without the express purpose of bypassing filtering software. This category does not include text translation.
Art Culture Heritage	Web pages that contain virtual art galleries, artist sites (including sculpture and photography), museums, ethnic customs, and country customs. This category does not include online photograph albums.
Auctions Classifieds	Web pages that provide online bidding and selling of items or services. This category includes web pages that focus on bidding and sales. This category does not include classified advertisements such as real estate postings, personal ads, or companies marketing their auctions.
Blogs/Wiki	Web pages containing dynamic content, which often changes because users can post or edit content at any time. This category covers the risks with dynamic content that might range from harmless to offensive.
Business	Web pages that provide business-related information, such as corporate overviews or business planning and strategies. This category also includes information, services, or products that help other businesses plan, manage, and market their enterprises, and multi-level marketing. This category does not include personal pages and web-hosting web pages.
Chat	Web pages that provide web-based, real-time social messaging in public and private chat rooms. This category includes IRC. This category does not include instant messaging.
Computing Internet	Web pages containing reviews, information, buyer's guides of computers, computer parts and accessories, computer software and internet companies, industry news and magazines, and pay-to-surf sites.
Consumer Protection	Websites that try to rob or cheat consumers. Some examples of their activities include selling counterfeit products, selling products that were originally provided for free, or improperly using the brand of another company. This category also includes sites where many consumers reported being cheated or not receiving services. This category does not include phishing, which tries to perpetrate fraud or theft by stealing account information. To check for phishing, go to Security Service > Reputation Filter > IP Reputation and select Phishing.

Table 202 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Content Server	URLs for servers that host images, media files, or JavaScript for one or more sites and are intended to speed up content retrieval for existing web servers, such as Apache. This category includes domain-level and sub-domain-level URLs that function as content servers. This category does not include: • Web pages for businesses that provide the content servers • Web pages that allow users to browse photographs. See the Media Sharing category. • URLs for servers that serve only advertisements. See the Web Ads category.
Controversial Opinions	Web pages that contain opinions that are likely to offend political or social sensibilities and incite controversy. Much of this content is at the extremes of public opinion. This category does not include opinion or language clearly intended to promote hate or discrimination.
Cult Occult	Sites relating to non-traditional religious practices considered to be false, unorthodox, extremist, or coercive.
Dating Personals	Web pages that provide networking for online dating, matchmaking, escort services, or introductions to potential spouses. This category does not include sites that provide social networking that might include dating, but are not specific to dating.
Dating Social Networking	Web pages that focus on social interaction such as online dating, friendship, school reunions, pen-pals, escort services, or introductions to potential spouses. This category does not include wedding-related content, dating tips, or related marketing.
Digital Postcards	Web pages that allow people to send and receive digital postcards and greeting cards through the Internet.
Discrimination	Web pages, which provide information that explicitly encourages the oppression or discrimination of a specific group of individuals. This category does not include jokes and humor, unless the focus of the entire site is considered discriminatory.
Drugs	Websites that provide information on the purchase, manufacture, and use of illegal or recreational drugs. This category does not include sites with exclusive health or political themes.
Education Reference	Web pages devoted to academic-related content such as academic subjects (mathematics, history), school or university web pages, and education administration pages (school boards, teacher curriculum).
Entertainment	Web pages that provide information about cinema, theater, music, television, infotainment, entertainment industry gossip-news, and sites about celebrities such as actors and musicians. This category also includes sites where the content is devoted to providing entertainment on the web, such as horoscopes or fan clubs.
Extreme	Web pages that provide content considered gory, perverse, or horrific.
Fashion Beauty	Web pages that market clothing, cosmetics, jewelry, and other fashion-oriented products, accessories, or services. This category also includes product reviews, comparisons, and general consumer information, and services such as hair salons, tanning salons, tattoo studios, and body-piercing studios. This category does not include fashion-related content such as modeling or celebrity fashion unless the site focuses on marketing the product line.

Table 202 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Finance Banking	Web pages that provide financial information or access to online financial accounts. This category includes stock information (but not stock trading), home finance, and government-related financial information.
For Kids	Web pages that are family-safe, specifically for children of approximate ages ten and under. This category can also be used as an exception to allow web pages that do not pose a risk to children, or to access sites that have a primary educational or recreational focus for children, but are in other categories such as Games, Humor/Comics, Recreation/Hobbies, or Entertainment.
Forum Bulletin Boards	Web pages that provide access (http://) to Usenet newsgroups or hold discussions and post user-generated content, such as real-time message posting for an interest group. This category also includes archives of files uploaded to newsgroups. This category does not include message forums with a business or technical support focus.
Gambling	Web pages that allow users to wager or place bets online, or provide gambling software that allows online betting, such as casino games, betting pools, sports betting, and lotteries. This category does not include web pages related to gambling that do not allow betting online.
Gambling Related	Web pages that offer information about gambling, without providing the means to gamble. This category includes casino-related web pages that do not offer online gambling, gambling links, tips, sports picks, lottery results, and horse, car, or boat racing.
Game Cartoon Violence	Web pages that provide fantasy or fictitious representations of violence within the context of games, comics, cartoons, or graphic novels. This category includes images and textual descriptions of physical assaults or hand-to-hand combat, and grave injury and destruction caused by weapons or explosives.
Games	Web pages that offer online games and related information such as cheats, codes, demos, emulators, online contests or role-playing games, gaming clans, game manufacturer sites, fantasy or virtual sports leagues, and other gaming sites without chances of profit. This category includes gaming consoles.
General News	Web pages that provide online news media, such as international or regional news broadcasting and publication. This category includes portal sites that provide news content.
Government Military	Web pages that contain content maintained by governmental or military organizations, such as government branches or agencies, police departments, fire departments, civil defense, counter-terrorism organizations, or supranational organizations, such as the United Nations or the European Union. This category includes military and veterans' medical facilities.
Gruesome Content	Web pages with content that can be considered tasteless, gross, shocking, or gruesome. This category does not include web pages with content pertaining to physical assault.
Health	Web pages that cover all health-related information and health care services. This category does not include cosmetic surgery, marketing/selling pharmaceuticals, or animal-related medical services.

Table 202 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Historical Revisionism	Web pages that denounce, or offer different interpretations of, significant historical facts, such as holocaust denial. This category does not include all re-examination of historical facts, only historical events that are highly sensitive.
History	Web pages that provide content about historical facts. This category includes content suitable for higher education, but the Education category includes content for primary education. For example, a site with Holocaust photographs might be offensive, but have academic value.
Humor Comics	Web pages that provide comical or funny content. This category includes sites with jokes, sketches, comics, and satire pages. This category might also include graphic novel content, which is often associated with comics.
Illegal UK	Web pages that contain child sexual abuse content hosted anywhere in the world, and criminally obscene and incitement to racial hatred content hosted in the UK.
Incidental Nudity	Web pages that contain non-pornographic images of the bare human body like those in classic sculpture and paintings, or medical images. This category enables you to allow or block sites in order to address cultural or geographic differences in opinion about nudity. For example, you can use this category to block access to nudity, but allow access when nudity is not the primary focus of a site, such as news sites or major portals.
Information Security	Web pages that legitimately provide information about data protection. This category includes detailed information for safeguarding business or personal data, intellectual property, privacy, and infrastructure on the Internet, private networks, or in other bandwidth services such as telecommunications. This category does not include: • Legitimate information security companies and security software providers, such as virus protection companies. • Sites that intend to exploit security or teach how to bypass security.
Information Security New	Web pages that legitimately provide information about data protection. This category includes detailed information for safeguarding business or personal data, intellectual property, privacy, and infrastructure on the Internet, private networks, or in other bandwidth services such as telecommunications. This category does not include: • Legitimate information security companies and security software providers, such as virus protection companies. • Sites that intend to exploit security or teach how to bypass security.
Instant Messaging	Web pages that provide software for real-time communication over a network exclusively for users who joined a member's contact list or an instant-messaging session. Most instant-messaging software includes features such as file transfer, PC-to-PC phone calls, and can track when other people log on and off.
Interactive Web Applications	Web pages that provide access to live or interactive web applications, such as browser-based office suites and groupware. This category includes sites with business, academic, or individual focus. This category does not include sites providing access to interactive web applications that do not take critical user data or offer security risks, such as Google Maps.

Table 202 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Internet Radio TV	Web pages that provide software or access to continuous audio or video broadcasting, such as Internet radio, TV programming, or podcasting. Quick downloads and shorter streams that consume less bandwidth are in the Streaming Media or Media Downloads categories.
Internet Services	Web pages that provide services for publication and maintenance of Internet sites such as web design, domain registration, Internet Service Providers, and broadband and telecommunications companies that provide web services. This category includes web utilities such as statistics and access logs, and web graphics like clip art.
Job Search	Web pages related to a job search including sites concerned with resume writing, interviewing, changing careers, classified advertising, and large job databases. This category also includes corporate web pages that list job openings, salary comparison sites, temporary employment, and company job-posting sites. This category does not include make-money-at-home sites.
Major Global Religions	Web pages with content about religious topics and information related to major religions. This category includes sites that cover religious content such as discussion, beliefs, non-controversial commentary, articles, and information for local congregations such as a church or synagogue homepage. The religions in this category are Baha'i, Buddhism, Chinese Traditional, Christianity, Hinduism, Islam, Jainism, Judaism, Shinto, Sikhism, Tenrikyo, Zoroastrianism.
Marketing Merchandising	Web pages that promote individual or business products or services on the web, but do not sell their products or services online. This category includes websites that are generally a company overview, describing services or products that cannot be purchased directly from these sites. Examples include automobile manufacturer sites, wedding photography services, or graphic design services. This category does not include: • Other categories that imply marketing such as Alcohol, Auctions/Classifieds, Drugs, Finance/Banking, Mobile Phone, Online Shopping, Real Estate, School Cheating Information, Software/Hardware, Stock Trading, Tobacco, Travel, and Weapons. • Sites that market their services only to other businesses. See the Business category. • Sites that rob or cheat consumers. See the Consumer Protection category.
Media Downloads	Web pages that provide audio or video files for download such as MP3, WAV, AVI, and MPEG formats. The files are saved to, and played from, the user's computer. This category does not include audio or video files that are played directly through a browser window. See the Streaming Media category.
Media Sharing	Web pages that allow users to upload, search for, and share media files and photographs, such as online photograph albums.
Messaging	Examples include text messaging to mobile phones, PDAs, fax machines, and internal website user-to-user messaging or site-to-site messaging. This category does not include real-time chat or instant messaging, or message posts that can be viewed by anyone but the intended recipient.
Mobile Phone	Web pages that sell media, software, or utilities for mobile phones that can be downloaded and delivered to mobile phones. Examples include ringtones, logos/skins, games, screen-savers, text-based tunes, and software for SMS, MMS, WAP, and other mobile phone protocols.

Table 202 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Moderated	Bulletin boards, chat rooms, search engines, or web mail sites that are monitored by an individual or group who has the authority to block messages or content considered inappropriate. This category does not include sites with posted rules against offensive content. See the Forum/Bulletin Boards category.
Motor Vehicles	Websites for manufacturers and dealerships of consumer transportation vehicles, such as cars, vans, trucks, SUVs, motorcycles, and scooters. This category also includes sites that provide product marketing, reviews, comparisons, pricing information, auto fairs, auto expos, and general consumer information about motor vehicles. This category does not include automotive accessories, mechanics, auto-body shops, and recreational hobby pages. This category does not include sites that provide business-to-business-only content regarding motor vehicles.
Non Profit Advocacy NGO	Web pages from charitable or educational groups that fulfill a stated mission, benefiting the larger community, such as clubs, lobbies, communities, non-profit organizations, labor unions, and advocacy groups. Examples are Masons, Elks, Boy and Girl Scouts, or Big Brothers.
Nudity	Web pages that have non-pornographic images of the bare human body. This category includes classic sculpture and paintings, artistic nude photographs, some naturism pictures, and detailed medical illustrations. This category does not include high-profile sites where nudity is not a concern for visitors. See the Incidental Nudity category.
Online Shopping	Web pages that sell products or services online. Web pages selling a broad range of products might pose a risk to users by offering access to items that are normally in other categories such as Pornography, Weapons, Nudity, or Violence. Web pages selling such content exclusively are in their respective categories.
P2P File Sharing	Web pages that allow the exchange of files between computers and users for business or personal use, such as downloadable music. P2P clients allow users to search for and exchange files from a peer-user network. They often include spyware or real-time chat capabilities. This category includes BitTorrent web pages.
Parked Domain	Web pages that once served content, but their domains have been sold or abandoned and are no longer registered. Parked domains do not host their own content, but usually redirect users to a generic page that states the domain name is for sale, or redirect users to a generic search engine and portal page, some of which provide valid search engine results.
Personal Network Storage	Web pages that allow users to upload folders and files to an online network server in order to backup, share, edit, or retrieve files or folders from any web browser.
Personal Pages	Personal home pages that share a common domain such as those hosted by ISPs, university/education servers, or free web page hosts. This category also includes unique domains that contain personal information, such as a personal home page. This category does not include home pages of public figures.
Pharmacy	Web pages that provide reviews, descriptions, and market or sell prescription-based drugs, over-the-counter drugs, birth control, or dietary supplements.
Politics Opinion	Web pages covering political parties, individuals in political life, and opinion on various topics. This category might also cover laws and political opinion about drugs. This category includes URLs for political parties, political campaigning, and opinions on various topics, including political debates.

Table 202 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Pornography	Web pages that contain materials intended to be sexually arousing or erotic. This category includes fetish pages, animation, cartoons, stories, and illegal pornography.
Portal Sites	Web pages that serve as major gateways or directories to content on the web. Many portal sites also provide a variety of internal site features or services such as search engines, email, news, and entertainment. Mailing list sites with a variety of content are in this category. This category does not include sites with topic-specific content.
Potential Criminal Activities	Web pages that provide instructions to commit illegal or criminal activities. Instructions include committing murder or suicide, sabotage, bomb-making, lock-picking, service theft, evading law enforcement, or spoofing drug tests. This category might also include information on how to distribute illegal content, perpetrate fraud, or consumer scams. This category does not include computer-related fraud.
Potential Hacking Computer Crime	Web pages that provide instructions, or otherwise enable, fraud, crime, or malicious activity that is computer-oriented. This category includes web pages related to computer crime include malicious hacking information or tools that help individuals gain unauthorized access to computers and networks (root kits, kiddy scripts). This category also includes other areas of electronic fraud such as dialer scams and illegal manipulation of electronic devices. This category does not include illegal software.
Potential Illegal Software	Web pages, which the filter believes offer information to potentially ‘pirated’ or illegally distribute software or electronic media, such as copyrighted music or film, distribution of illegal license key generators, software cracks, and serial numbers. This category does not include peer-to-peer web pages.
Private IP Addresses	Sites that are private IP addresses as defined in RFC 1918, that is, hosts that do not require access to hosts in other enterprises (or require just limited access) and whose IP address may be ambiguous between enterprises but are well defined within a certain enterprise.
Profanity	Web pages that contain crude, vulgar, or obscene language or gestures.
Professional Networking	Web pages that provide social networking exclusively for professional or business purposes. This category includes sites that provide personal or group profiles, and enable their members to interact through real-time communication, message posting, public bulletins, and media sharing. This category also contains alumni sites that have a networking function. This category does not include social networking sites where the focus might vary, but include friendship, dating, or professional focuses.
Provocative Attire	Web pages with pictures that include alluring or revealing attire, lingerie and swimsuits, or supermodel or celebrity photograph collections, but do not involve nudity. This category does not include sites with swimwear or similar attire that is not intended to be provocative. For example, Olympic swimming sites are not in this category.
Public Information	Web pages that provide general reference information such as public service providers, regional information, transportation schedules, maps, or weather reports.

Table 202 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
PUPs	Web pages that contain Potentially Unwanted Programs (PUPs). PUPs are often made for a beneficial purpose but they alter the security of a computer or the computer user's privacy. Computer users who are concerned about security or privacy might want to be informed about this software, and in some cases, they might want to remove this software from their computers.
Real Estate	Web pages that provide commercial or residential real estate services and information. Service and information includes sales and rental of living space or retail space and guides for apartments, housing, and property, and information on appraisal and brokerage. This category includes sites that allow you to browse model homes. This category does not include content related to personal finance, such as credit applications.
Recreation Hobbies	Web pages for recreational organizations and facilities that include content devoted to recreational activities and hobbies. This category includes information about public swimming pools, zoos, fairs, festivals, amusement parks, recreation guides, hiking, fishing, bird watching, or stamp collecting. This category does not include activities that need no active participation, such as watching a movie or reading celebrity gossip.
Religion Ideology	Web pages with content related to religious topics and beliefs in human spirituality that are not within the major religions. This category includes religious discussion, beliefs, articles, and information for local congregations or groups such as a church homepage, unless the site is already in the Major Global Religions category. This category also includes comparative religion, or sites that include religions and ideologies. This category does not include astrology and horoscope sites
Remote Access	Web pages that provide remote access to a program, online service, or an entire computer system. Although remote access is often used legitimately to run a computer from a remote location, it creates a security risk, such as backdoor access. Backdoor access, written by the original programmer, allows the system to be controlled by another party without the user's knowledge.
Reserved	This category is reserved for future use.
Residential IP Addresses	IP addresses (and any domains associated with them) that access the Internet by DSL modems or cable modems. Because this content is not generally intended for Internet access through HTTP, access to the Internet through these IP addresses can indicate suspicious behavior. This behavior might be related to malware located on the home computer or homegrown gateways set up to allow anonymous Internet access.
Resource Sharing	Web pages that harness idle or unused computer resources to focus on a common task. The task can be on a company or an international basis. Well known examples are the SETI program and the Human Genome Project, which use the idle time of thousands of volunteered computers to analyze data.

Table 202 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Restaurants	Web pages that provide information about restaurants, bars, catering, take-out and delivery, including online ordering. This category includes sites that provide information about location, hours, prices, menus and related dietary information. This category also includes restaurant guides and reviews, and cafes and coffee shops. This category does not include groceries, wholesale food, non-profit and charitable food organizations, or bars that do not focus on serving food.
School Cheating Information	Web pages that promote plagiarism or cheating by providing free or fee-based term papers, written essays, or exam answers. This category does not include sites that offer student help, discuss literature, films, or books, or other content that is often the subject of research papers.
Search Engines	Web pages that provide search results that enable users to find information on the Internet based on key words. This category does not include site-specific search engines.
Sexual Materials	Web pages that describe or depict sexual acts, but are not intended to be arousing or erotic. Examples of sexual materials include sex education, sexual innuendo, humor, or sex related merchandise. This category does not include web pages with content intended to arouse.
Shareware Freeware	Web pages that are repositories of downloadable copies of shareware and freeware. This category does not include subscription-based software.
Social Networking	Web pages that enable social networking for a variety of purposes, such as friendship, dating, professional, or topics of interest. These sites provide personal or group profiles and enable interaction among their members through real-time communication, message posting, public bulletins, and media sharing. This category does not include sites that are exclusive to dating, matchmaking, or a specific professional networking focus.
Software Hardware	Web pages related to computing software and hardware, including vendors, product marketing and reviews, deployment and maintenance of software and hardware, and software updates and add-ons such as scripts, plug-ins, or drivers. Hardware includes computer parts, accessories, and electronic equipment used with computers and networks. This category includes the marketing of software and hardware, and magazines focused on software or hardware product reviews or industry trends.
Sports	Web pages related to professional or organized recreational sports. This category includes sporting news, events, and information such as playing tips, strategies, game scores, or player trades. This category does not include fantasy leagues, sports centers, athletic clubs, fitness or martial arts clubs, and non-league billiards, darts, or other such activities.
Stock Trading	Web pages that offer purchasing, selling, or trading of shares online. This category also includes ticker-tape information that enables viewing of real-time stock prices and financial spread betting in the stock market. Other betting is in the Gambling category. This category does not include sites that offer information about stocks, but do not offer purchasing, selling, or trading of shares.

Table 202 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Streaming Media	Web pages that provide streaming media, or contain software plug-ins for displaying audio and visual data before the entire file has been transmitted. This category does not include audio or video files that are downloaded to a user's computer before being played.
Technical Business Forums	Web pages with a technical or business focus that provide online message posting or real-time chatting, such as technical support or interactive business communication. Although users can post any type of content, these forums tend to present less risk of containing offensive content. Sites that offer a variety of forums with themes, including technical and business content, are only in the categories of Forum/Bulletin Boards or Chat.
Technical Information	Web pages that provide computing information with an educational focus in areas such as Information Technology, computer programming, and certification. Examples include Linux user groups, UNIX commands, software tutorials, or dictionaries of technical terms. Most sites in this category might be subdirectories of larger domains. For example, a software site with a tutorial page is in this category only at the tutorial page URL. This category does not include content about information security.
Text Spoken Only	Content that is text or audio only, and does not contain pictures. This category can be used as an exception to allow explicit text and recorded material to be accessed when you want pictures blocked using the Pornography, Violence, or Sexual Materials categories. Libraries or universities can use this category to prevent the display of offensive graphics in their public facilities.
Text Translators	Web pages that allow users to type phrases or a block of text to translate it from one language into another. This category also includes language identifier web pages. URL translation is in the Anonymizing Utilities category.
Tobacco	Web pages that sell, promote, or advocate the use of tobacco products, tobacco paraphernalia, including cigarettes, cigars, pipes, snuff and chewing tobacco.
Travel	Web pages that promote personal or business travel, such as hotels, resorts, airlines, ground transportation, car rentals, travel agencies, and general tourist and travel information. This category also includes sites for buying tickets or accommodation. This category does not include personal vacation photographs.
Usenet News	Web pages that provide access (http://) to Usenet newsgroups and archives of files uploaded to newsgroups. This category also includes online groups that offer similar community-oriented content posting.
Violence	Web pages that contain real or lifelike images or text that portray, describe, or advocate physical assaults against people, animals, or institutions, such as depictions of war, suicide, mutilation, or dismemberment.
Visual Search Engine	Web pages that provide image-specific search results such as thumbnail pictures. This category does not include sites that offer site-specific visual search engines.

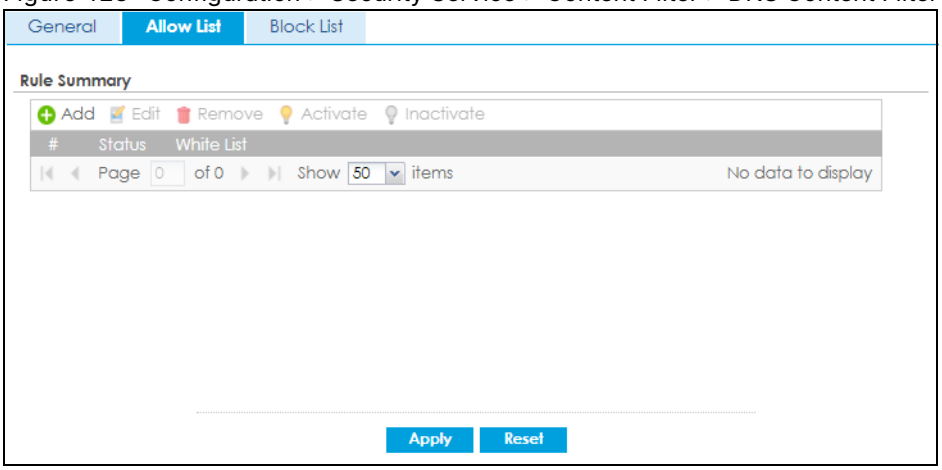
Table 202 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Weapons	Web pages that provide information about buying, making, modifying, or using weapons, such as guns, knives, swords, paintball guns, and ammunition, explosives, and weapon accessories. This category also includes sites that contain content for: weapons for personal or military use, homemade weapons, non-lethal weapons such as mace, pepper spray, or Taser guns, weapons facilities, such as shooting ranges, and government or military oriented weapons. This category does not include political action groups, such as the NRA.
Web Ads	Web pages that provide advertisement-hosting or programs that create advertisements. Examples include links, source code or applets for banners, popups, and other kinds of static or dynamically generated advertisements that appear on web pages. This category is intended to block advertisements on web pages, not the companies that provide the advertisements or advertising services. This category does not include aggressive advertising adware. See the Spyware/Adware category.
Web Mail	Web pages that enable users to send or receive email through the Internet.
Web Meetings	Web pages that host live meetings, video conferences, and interactive presentations mainly for businesses. Web meetings generally include streaming audio and video, and allow data transfer or office-oriented application sharing, such as online presentations.
Web Phone	Web pages that enable users to make telephone calls through the Internet or obtain information or software for this purpose. Web Phone service is also called Internet Telephony, or VoIP. Web phone service includes PC-to-PC, PC-to-phone, and phone-to-phone services connecting through TCP/IP networks.

27.6 DNS Content Filter Allow List Screen

Click Configuration > Security Service > Content Filter > DNS Content Filter > Allow List to open the Allow List screen. You can create a list of good (allowed) web site addresses. When you configure DNS Content Filter Profiles, you can select the option to check the allow list. Use this screen to add or remove specific sites from the allow list.

Figure 428 Configuration > Security Service > Content Filter > DNS Content Filter > Allow List



The following table describes the labels in this screen.

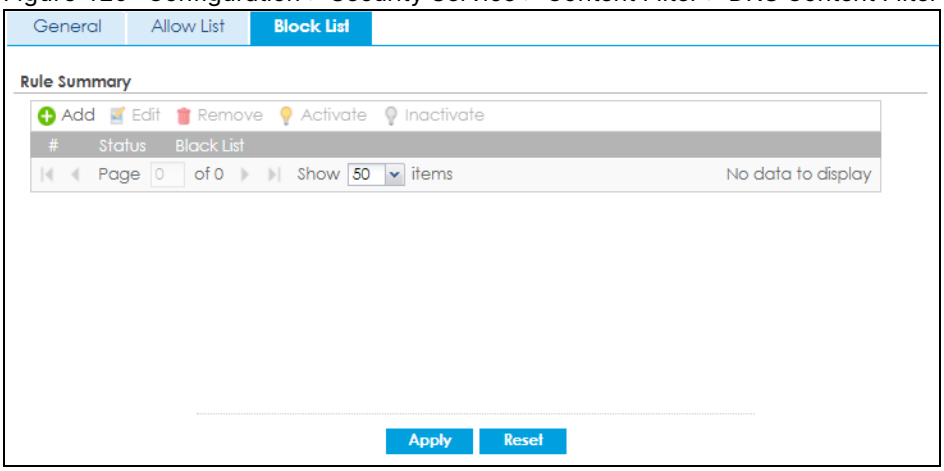
Table 203

LABEL	DESCRIPTION
Add	Click this to add a new rule. Enter an IPv4 address associated with this rule.
Edit	Click this to edit the selected rule.
Remove	Click this to remove the selected rule.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
#	This field is a sequential value, and it is not associated with a specific rule.
Status	This icon is lit when the rule is active and dimmed when the rule inactive
White List	This field displays the IP address associated with this rule.

27.7 DNS Content Filter Block List Screen

Click Configuration > Security Service > Content Filter > DNS Content Filter > Block List to open the Block List screen.You can create a list of bad (blocked) web site addresses. When you configure DNS Content Filter Profiles, you can select the option to check the block list. Use this screen to add or remove specific sites from the block list.

Figure 429 Configuration > Security Service > Content Filter > DNS Content Filter > Block List



The following table describes the labels in this screen.

Table 204

LABEL	DESCRIPTION
Add	Click this to add a new rule. Enter an IPv4 address associated with this rule.
Edit	Click this to edit the selected rule.
Remove	Click this to remove the selected rule.
Activate	To turn on an entry, select it and click Activate. The Zyxel Device treats all FQDNs in the blacklist as prohibited, and applies DNS Content Filter rules when they are queried.
Inactivate	To turn off an entry, select it and click Inactivate.
#	This field is a sequential value, and it is not associated with a specific rule.
Status	This icon is lit when the rule is active and dimmed when the rule inactive
White List	This field displays the IP address associated with this rule.

27.8 Content Filter Technical Reference

This section provides content filtering background information.

External Content Filter Server Lookup Procedure

The content filter lookup process is described below.

Figure 430 Content Filter Lookup Procedure

1 A computer behind the Zyxel Device tries to access a web site.

2 The Zyxel Device looks up the web site in its cache. If an attempt to access the web site was made in the past, a record of that web site's category will be in the Zyxel Device's cache. The Zyxel Device blocks, blocks and logs or just logs the request based on your configuration.

3 Use the Content Filter Cache screen to configure how long a web site address remains in the cache as well as view those web site addresses. All of the web site address records are also cleared from the local cache when the Zyxel Device restarts.

4 If the Zyxel Device has no record of the web site, it queries the external content filter database and simultaneously sends the request to the web server.

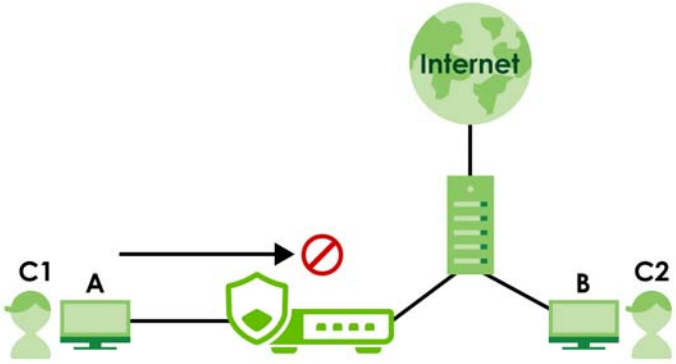
5 The external content filter server sends the category information back to the Zyxel Device, which then blocks and/or logs access to the web site based on the settings in the content filter profile. The web site's address and category are then stored in the Zyxel Device's content filter cache.

27.9 Example: Block LAN Users From Using a Remote WAN Application

This example shows you how to block LAN users from using a remote WAN application such as TeamViewer.

Client C1 on the Zyxel Device LAN uses computer A. Client C2 on the WAN uses computer B. Computer A and computer B are connected to the TeamViewer server (S). Client C1 could access computer B using TeamViewer. Client C2 could access computer A using TeamViewer. TeamViewer only works if computer A and computer B are both connected to the TeamViewer server (S).

Figure 431 Content Filter Tutorial Example



You want to block all LAN clients from using TeamViewer. Create a Content Filtering profile that includes the remote access category. Create a Forbidden Web Sites rule with TeamViewer as the keyword. Then apply the profile to the LAN_Outgoing security policy.

All LAN clients are now blocked from using TeamViewer.

This example uses the parameters listed below.

Table 205 Content Filtering Profile Configuration Example

PROFILE NAME	ENABLE CONTENT FILTER CATEGORY SERVICE	ACTION	LOG	MANAGED CATEGORIES	LOG-ALERT FOR BLOCK/WARN ACTION
NoRemoteAccess	Enabled	Block	Log	Remote Access	Enabled

Table 206 Forbidden Web Sites Configuration Example

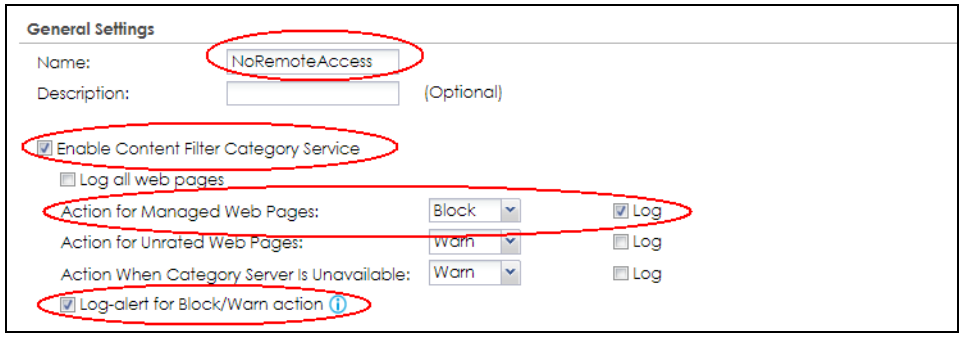
ENABLE CUSTOM SERVICE	FORBIDDEN WEB SITES KEYWORD
Enabled	*.*teamviewer*.*

Table 207 Security Policy Configuration Example

TO	FROM	LOG	CONTENT FILTERING PROFILE
WAN	LAN1/LAN2	By Profile	NoRemoteAccess

1 Go to Configuration > Security Service > Content Filter > Web Content Filter > General and click Add.

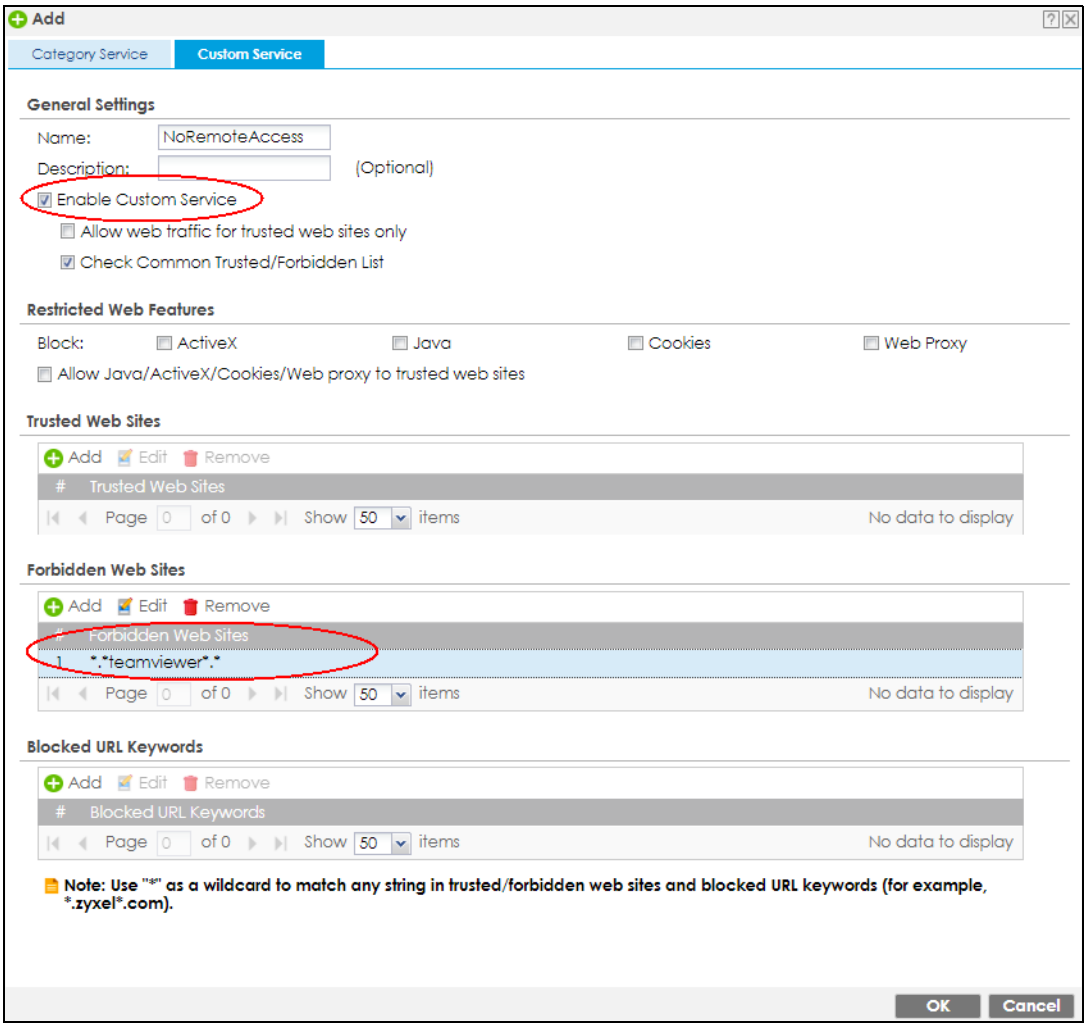
2 Configure the profile settings using the parameters given in Table 205 on page 646.



3 Select the Remote Access checkbox under Managed Categories.

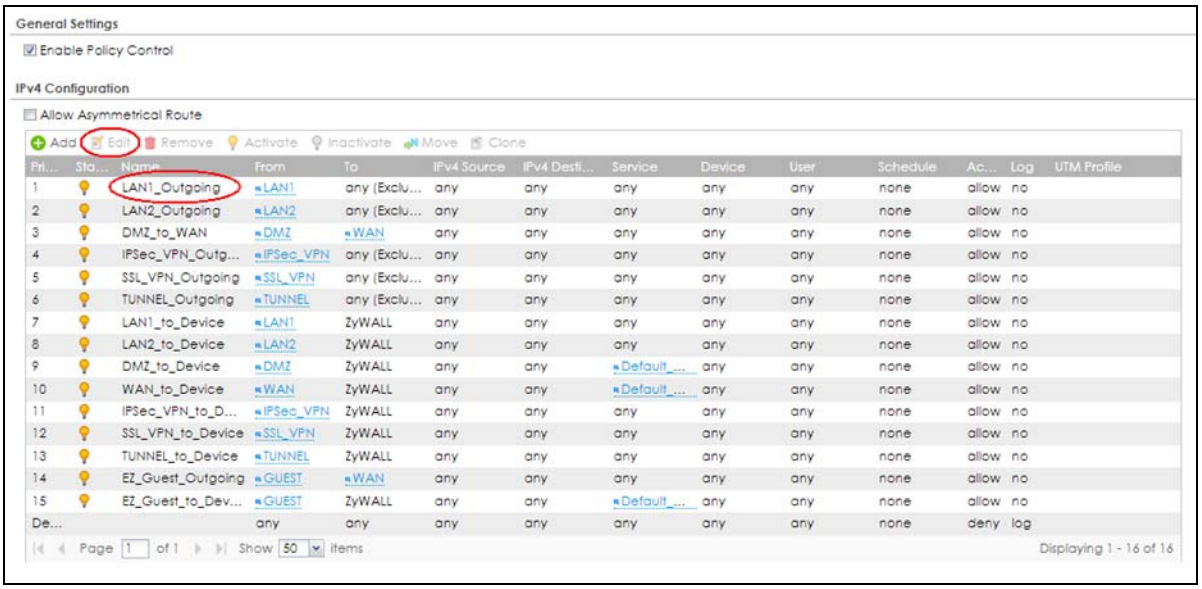
4 Go to Custom Service. Select Enable Custom Service.

5 Click Add under Forbidden Web Sites to add a rule using the parameters given in Table 206 on page 646.

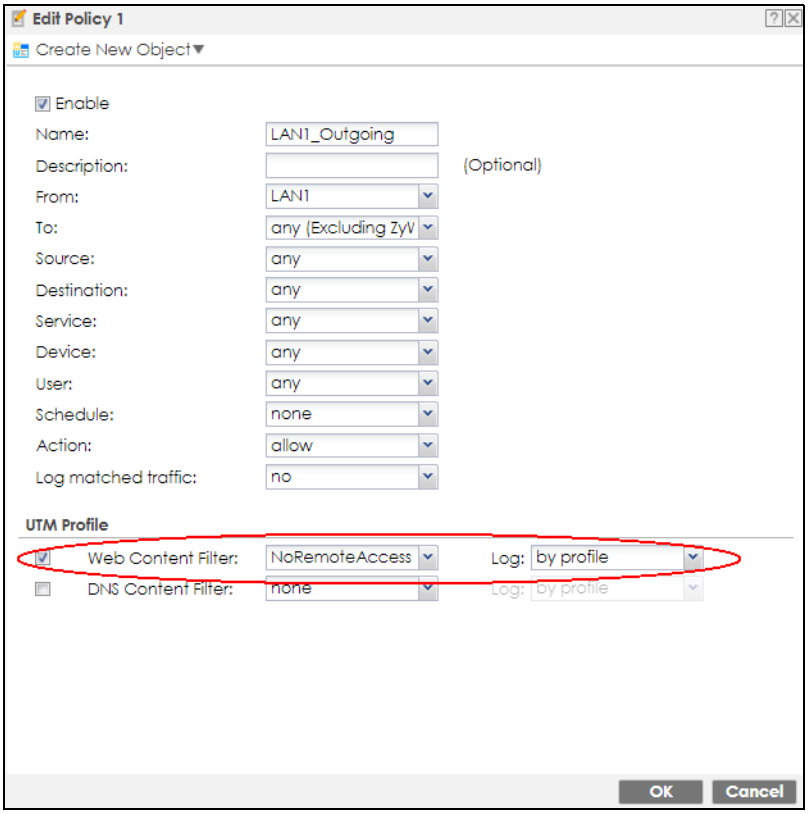


6 Click OK to save your changes.

7 Go to Configuration > Security Policy > Policy Control. Select LAN1_Outgoing then click Edit.

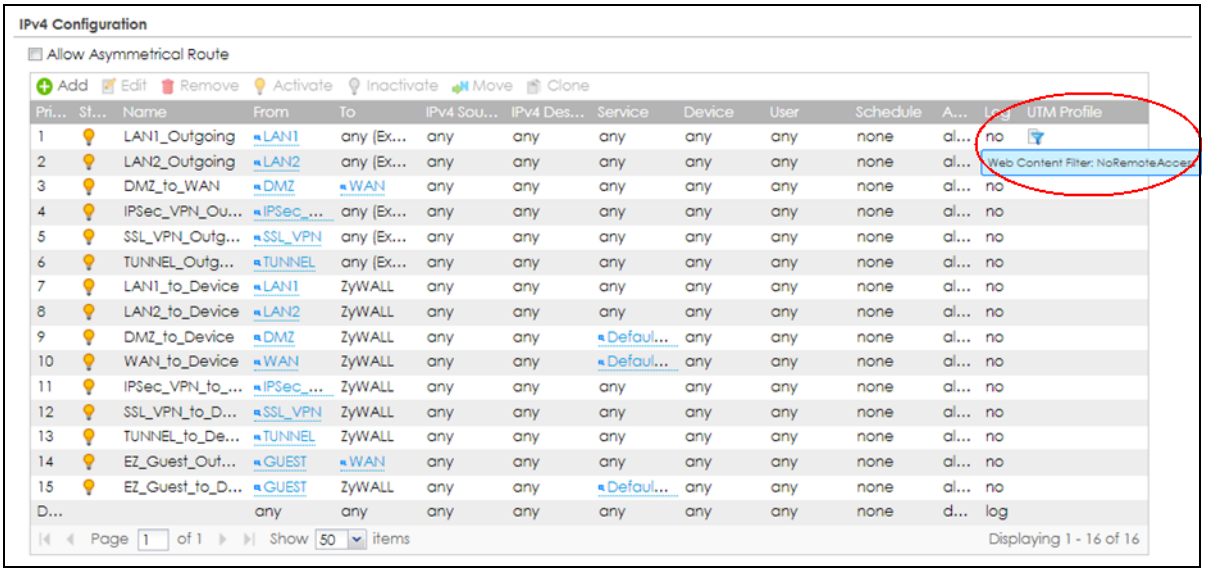


8 Set Web Content Filter to NoRemoteAccess and Log to by profile. Click OK to save your changes.



9 Repeat Step 7 and Step 8 to apply the NoRemoteAccess web content filter profile to LAN2_Outgoing.

10 You can check the result in the Policy Control screen. Mouse-over the icon under the UTM Profile column to check that the NoRemoteAccess profile has been applied to the LAN1_Outgoing and LAN2_Outgoing security policies. You can also check the logs in Monitor > Log > View Log. The Zyxel Device will create logs if the clients on the Zyxel Device LAN try to access TeamViewer.



CHAPTER 28
Anti-Spam

28.1 Overview

The anti-spam feature can mark or discard spam (unsolicited commercial or junk e-mail). Use the Allow List to identify legitimate e-mail. Use the Block List to identify spam e-mail. The Zyxel Device can also check e-mail against a DNS black list (DNSBL) of IP addresses of servers that are suspected of being used by spammers.

28.1.1 What You Can Do in this Chapter

- Use the General Profilescreens (Section 28.3 on page 653) to turn anti-spam on or off and manage anti-spam policies.
- Use the Mail Scan screen (Section 28.4 on page 656) to enable and configure the mail scan functions.
- Use the Block/Allow List screens (Section 28.5 on page 657) to set up a block list to identify spam and an allow list to identify legitimate e-mail.
- Use the DNSBL screens (Section 28.7 on page 662) to have the Zyxel Device check e-mail against DNS Black Lists.

28.1.2 What You Need to Know

Allow List

Configure allow list entries to identify legitimate e-mail. The allow list entries have the Zyxel Device classify any e-mail that is from a specified sender or uses a specified header field and header value as being legitimate (see E-mail Headers for more on mail headers). The anti-spam feature checks an e-mail against the allow list entries before doing any other anti-spam checking. If the e-mail matches an allow list entry, the Zyxel Device classifies the e-mail as legitimate and does not perform any more anti-spam checking on that individual e-mail. A properly configured allow list helps keep important e-mail from being incorrectly classified as spam. The allow list can also increases the Zyxel Device's anti-spam speed and efficiency by not having the Zyxel Device perform the full anti-spam checking process on legitimate e-mail.

Block List

Configure block list entries to identify spam. The block list entries have the Zyxel Device classify any e-mail that is from or forwarded by a specified IP address or uses a specified header field and header value as being spam. If an e-mail does not match any of the allow list entries, the Zyxel Device checks it against the block list entries. The Zyxel Device classifies an e-mail that matches a block list entry as spam and immediately takes the configured action for dealing with spam. If an e-mail matches a block list entry, the Zyxel Device does not perform any more anti-spam checking on that individual e-mail. A properly configured block list helps catch spam e-mail and increases the Zyxel Device's anti-spam speed and efficiency.

SMTP and POP3

Simple Mail Transfer Protocol (SMTP) is the Internet's message transport standard. It controls the sending of e-mail messages between servers. E-mail clients (also called e-mail applications) then use mail server protocols such as POP (Post Office Protocol) or IMAP (Internet Message Access Protocol) to retrieve e-mail. E-mail clients also generally use SMTP to send messages to a mail server. The older POP2 requires SMTP for sending messages while the newer POP3 can be used with or without it. This is why many e-mail applications require you to specify both the SMTP server and the POP or IMAP server (even though they may actually be the same server).

The Zyxel Device's anti-spam feature checks SMTP (TCP port 25) and POP3 (TCP port 110) e-mails by default. You can also specify custom SMTP and POP3 ports for the Zyxel Device to check.

E-mail Headers

Every email has a header and a body. The header is structured into fields and includes the addresses of the recipient and sender, the subject, and other information about the e-mail and its journey. The body is the actual message text and any attachments. You can have the Zyxel Device check for specific header fields with specific values.

E-mail programs usually only show you the To:, From:, Subject:, and Date: header fields but there are others such as Received: and Content-Type:. To see all of an e-mail's header, you can select an e-mail in your e-mail program and look at its properties or details. For example, in Microsoft's Outlook Express, select a mail and click File > Properties > Details. This displays the e-mail's header. Click Message Source to see the source for the entire mail including both the header and the body.

E-mail Header Buffer Size

The Zyxel Device has a 5 K buffer for an individual e-mail header. If an e-mail's header is longer than 5 K, the Zyxel Device only checks up to the first 5 K.

DNSBL

A DNS Black List (DNSBL) is a server that hosts a list of IP addresses known or suspected of having sent or forwarded spam. A DNSBL is also known as a DNS spam blocking list. The Zyxel Device can check the routing addresses of e-mail against DNSBLs and classify an e-mail as spam if it was sent or forwarded by a computer with an IP address in the DNSBL.

Finding Out More

See Section 28.8 on page 663 for more background information on anti-spam.

28.2 Before You Begin

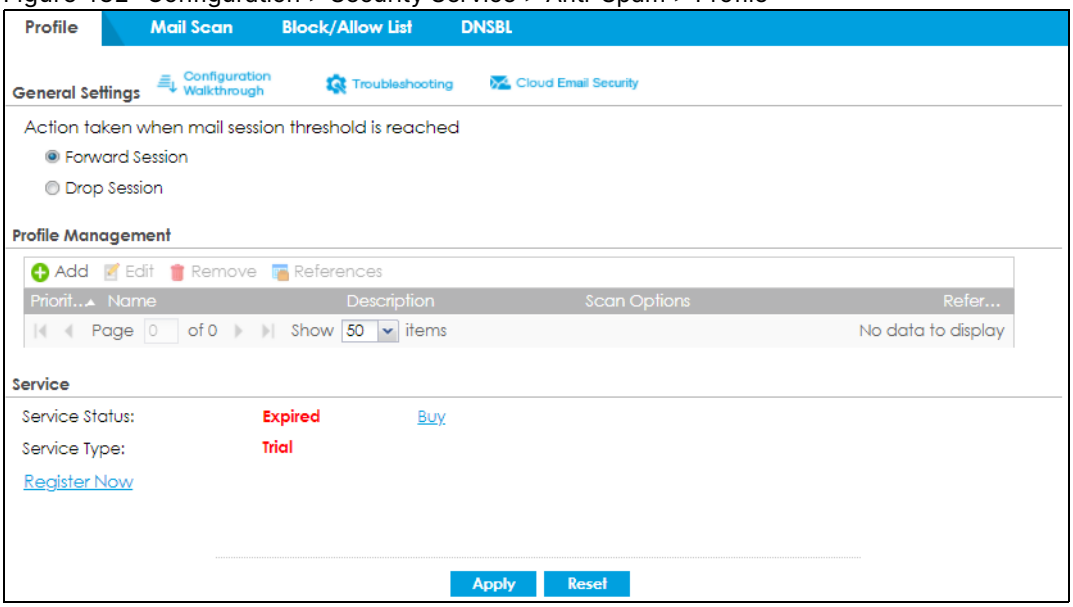
- Before using the Anti-Spam features (IP Reputation, Mail Content Analysis and Virus Outbreak Detection) you must activate your Anti-Spam Service license.
- Configure your zones before you configure anti-spam.

28.3 The Anti-Spam Profile Screen

Click Configuration > Security Service > Anti-Spam to open the Anti-Spam Profile screen. Use this screen to turn the anti-spam feature on or off and manage anti-spam policies. You can also select the action the Zyxel Device takes when the mail sessions threshold is reached.

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

Figure 432 Configuration > Security Service > Anti-Spam > Profile



The following table describes the labels in this screen.

Table 208 Configuration > Security Service > Anti-Spam > Profile

LABEL	DESCRIPTION
General Settings	
Action taken when mail sessions threshold is reached	An e-mail session is when an e-mail client and e-mail server (or two e-mail servers) connect through the Zyxel Device. Select how to handle concurrent e-mail sessions that exceed the maximum number of concurrent e-mail sessions that the anti-spam feature can handle. See the chapter of product specifications for the threshold. Select Forward Session to have the Zyxel Device allow the excess e-mail sessions without any spam filtering. Select Drop Session to have the Zyxel Device drop mail connections to stop the excess e-mail sessions. The e-mail client or server will have to re-attempt to send or receive e-mail later when the number of e-mail sessions is under the threshold.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
References	Select an entry and click References to open a screen that shows which settings use the entry. Click Refresh to update information in this screen.
Priority	This is the index number of the anti-spam rule. Antis-spam rules are applied in turn.
Name	The name identifies the anti-spam rule.

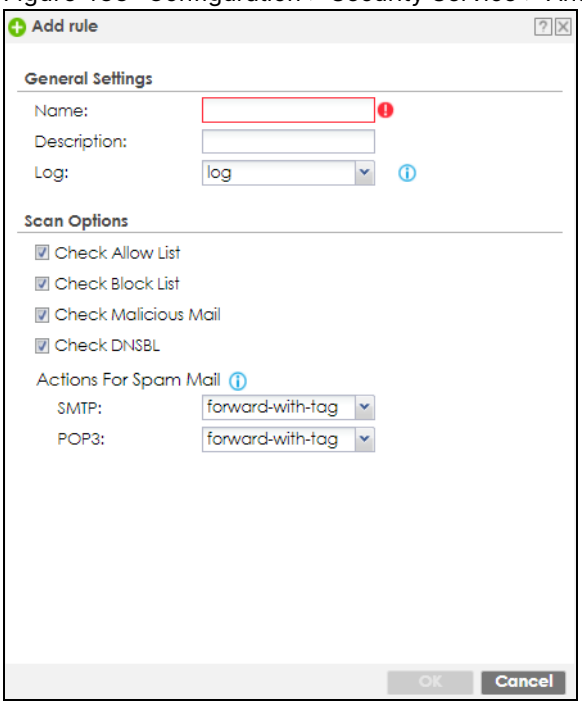
Table 208 Configuration > Security Service > Anti-Spam > Profile

LABEL	DESCRIPTION
Description	This is some optional extra information on the rule.
Scan Options	This shows which types (protocols) of traffic to scan for spam.
Reference	This shows how many objects are referenced in the rule.
Service	
Service 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. 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 Type	This read-only field displays what kind of service registration you have for the anti-spam scanning. None displays if you have not successfully registered and activated the service. Standard displays if you have successfully registered the Zyxel Device and activated the service with your iCard's PIN number. Trial displays if you have successfully registered the Zyxel Device and activated the trial service subscription.
Expiration Date	This field displays the date your service license expires.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

28.3.1 The Anti-Spam Profile Add or Edit Screen

Click the Add or Edit icon in the Configuration > Security Service > Anti-Spam > Profile screen to display the configuration screen as shown next. Use this screen to configure an anti-spam policy that controls scan options, and the action to take on spam traffic.

Figure 433 Configuration > Security Service > Anti-Spam > Profile > Add



The following table describes the labels in this screen.

Table 209 Configuration > Security Service > Anti-Spam > Profile > Add

LABEL	DESCRIPTION
General Settings	
Name	Enter a descriptive name for this anti-spam rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description for the anti-spam rule to help identify the purpose of rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. This field is optional.
Log	Select how the Zyxel Device is to log the event when the DNSBL times out or an e-mail matches the allow list, block list, or DNSBL. no: Do not create a log. log: Create a log on the Zyxel Device. log alert: An alert is an e-mailed log for more serious events that may need more immediate attention. Select this option to have the Zyxel Device send an alert.
Scan Options	
Check Allow List	Select this checkbox to check e-mail against the allow list. The Zyxel Device classifies e-mail that matches an allow list entry as legitimate (not spam).
Check Block List	Select this checkbox to check e-mail against the block list. The Zyxel Device classifies e-mail that matches a block list entry as spam.
Check Malicious Mail	
Check DNSBL	Select this checkbox to check e-mail against the Zyxel Device's configured DNSBL domains. The Zyxel Device classifies e-mail that matches a DNS black list as spam.

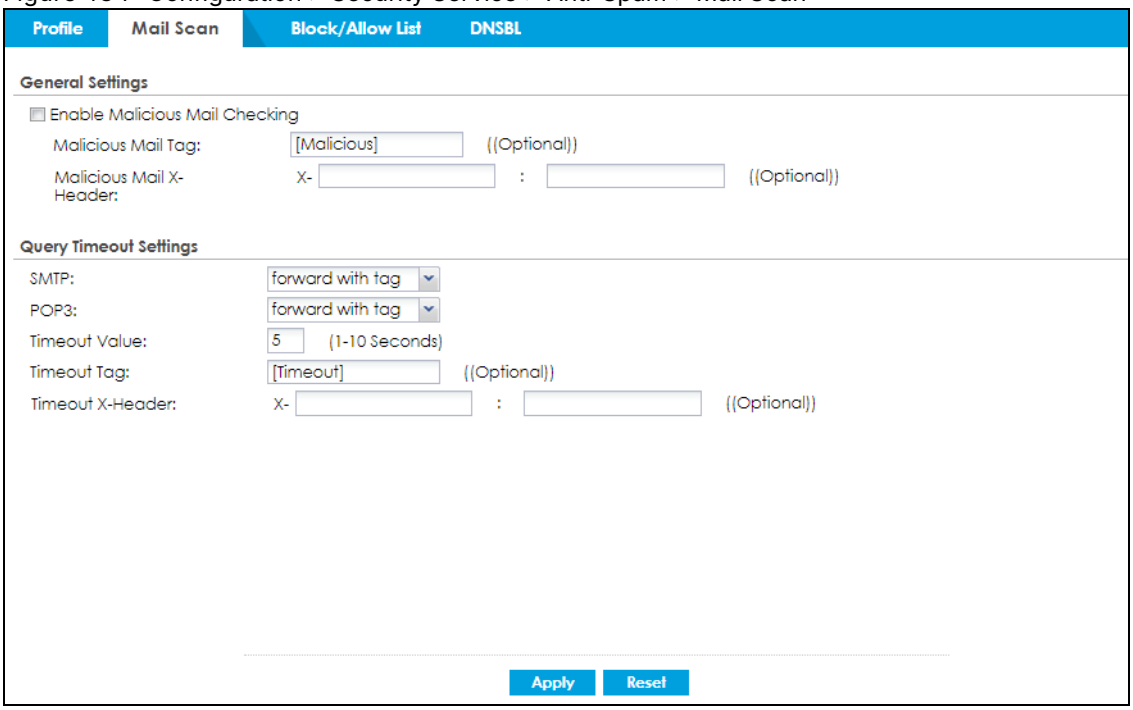
Table 209 Configuration > Security Service > Anti-Spam > Profile > Add (continued)

LABEL	DESCRIPTION
Actions for Spam Mail	Use this section to set how the Zyxel Device is to handle spam mail.
SMTP	Select how the Zyxel Device is to handle spam SMTP mail. Select drop to discard spam SMTP mail. Select forward to allow spam SMTP mail to go through. Select forward with tag to add a spam tag to an SMTP spam mail's mail subject and send it on to the destination.
POP3	Select how the Zyxel Device is to handle spam POP3 mail. Select forward to allow spam POP3 mail to go through. Select forward with tag to add a spam tag to an POP3 spam mail's mail subject and send it on to the destination.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving your changes.

28.4 The Mail Scan Screen

Click Configuration > Security Service > Anti-Spam > Mail Scan to open the Mail Scan screen. Use this screen to enable and configure the Mail Scan functions. You must first enable the mail scan functions on this screen before selecting them in the Configuration > Security Service > Anti-Spam > Profile > Add/Edit screen.

Figure 434 Configuration > Security Service > Anti-Spam > Mail Scan



The following table describes the labels in this screen.

Table 210 Configuration > Security Service > Anti-Spam > Mail Scan

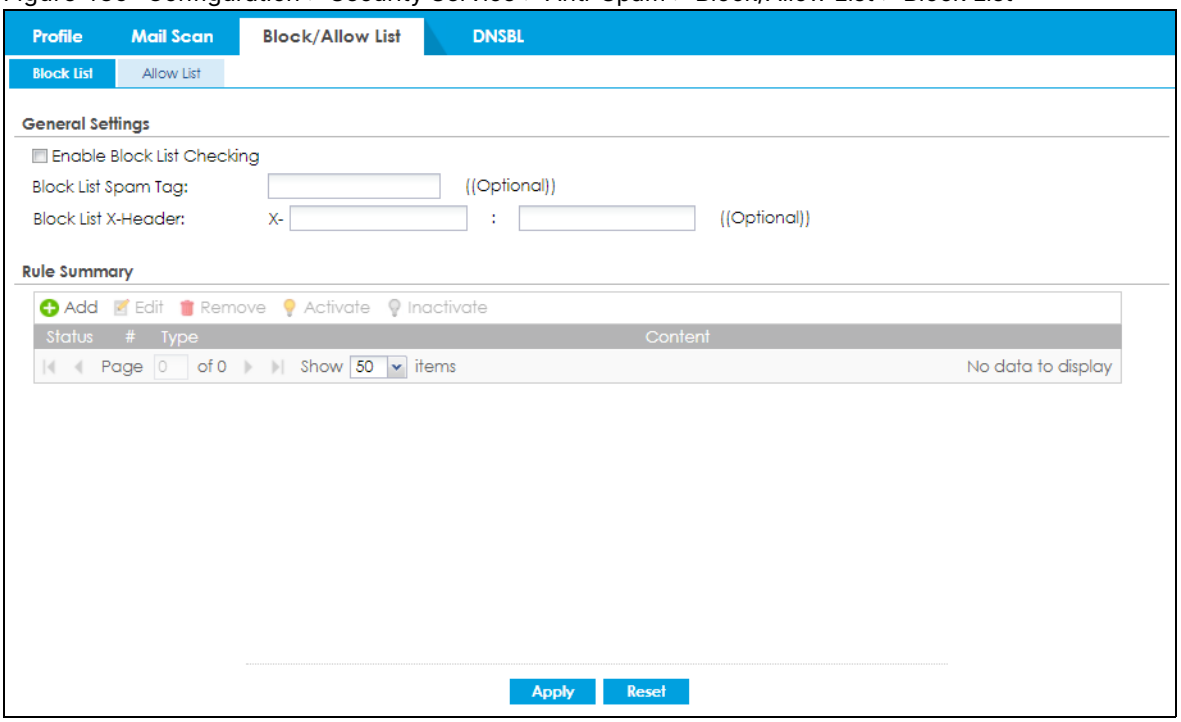
LABEL	DESCRIPTION
General Settings	
Enable Malicious Mail Checking	Select this to identify spam email by content, such as malicious content.
Malicious Mail Tag	Enter a message or label (up to 15 ASCII characters) to add to the beginning of the mail subject of emails that are determined to spam based on the mail content analysis. This tag is only added if the email security policy is configured to forward spam mail with a spam tag.
Malicious X-Header	Specify the name and value for the X-Header to be added to e-mails that are determined as spam email.
Query Timeout Settings	
SMTP	Select how the Zyxel Device is to handle SMTP mail query timeout. Select drop to discard SMTP mail. Select forward to allow SMTP mail to go through. Select forward with tag to add a tag to an SMTP query timeout mail's mail subject and send it on to the destination.
POP3	Select how the Zyxel Device is to handle POP3 mail query timeout. Select forward to allow POP3 mail to go through. Select forward with tag to add a tag to an POP3 query timeout mail's mail subject and send it on to the destination.
Timeout Value	Set how long the Zyxel Device waits for a reply from the mail scan server. If there is no reply before this time period expires, the Zyxel Device takes the action defined in the relevant Actions when Query Timeout field.
Timeout Tag	Enter a message or label (up to 15 ASCII characters) to add to the mail subject of e-mails that the Zyxel Device forwards if queries to the mail scan servers time out.
Timeout X-Header	Specify the name and value for the X-Header to be added when queries to the mail scan servers time out.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

28.5 The Anti-Spam Block List Screen

Click Configuration > Security Service > Anti-Spam > Block/Allow List to display the Anti-Spam Block List screen.

Configure the block list to identify spam e-mail. You can create block list entries based on the sender's or relay server's IP address or e-mail address. You can also create entries that check for particular e-mail header fields with specific values or specific subject text. 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 435 Configuration > Security Service > Anti-Spam > Block/Allow List > Block List



The following table describes the labels in this screen.

Table 211 Configuration > Security Service > Anti-Spam > Block/Allow List > Block List

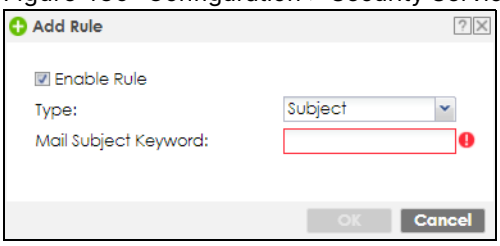
LABEL	DESCRIPTION
General Settings	
Enable Block List Checking	Select this checkbox to have the Zyxel Device treat e-mail that matches (an active) block list entry as spam.
Block List Spam Tag	Enter a message or label (up to 15 ASCII characters) to add to the mail subject of e-mails that match the Zyxel Device's spam black list.
Block List X-Header	Specify the name and value for the X-Header to be added to e-mails that match the Zyxel Device's spam black list.
Rule Summary	
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
#	This is the entry's index number in the list.
Type	This field displays whether the entry is based on the e-mail's subject, source or relay IP address, source e-mail address, or header.
Content	This field displays the subject content, source or relay IP address, source e-mail address, or header value for which the entry checks.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

28.5.1 The Anti-Spam Block or Allow List Add/Edit Screen

In the anti-spam Block List or Allow List screen, click the Add icon or an Edit icon to display the following screen.

Use this screen to configure an anti-spam block list entry to identify spam e-mail. You can create entries based on specific subject text, or the sender's or relay's IP address or e-mail address. You can also create entries that check for particular header fields and values.

Figure 436 Configuration > Security Service > Anti-Spam > Block/Allow List > Block/Allow List > Add



The following table describes the labels in this screen.

Table 212 Configuration > Security Service > Anti-Spam > Block/Allow List > Block/Allow List > Add

LABEL	DESCRIPTION
Enable Rule	Select this to have the Zyxel Device use this entry as part of the block or allow list. To actually use the entry, you must also turn on the use of the list in the corresponding list screen, enable the anti-spam feature in the anti-spam general screen, and configure an anti-spam policy to use the list.
Type	Use this field to base the entry on the e-mail's subject, source or relay IP address, source e-mail address, or header. Select Subject to have the Zyxel Device check e-mail for specific content in the subject line. Select IP Address to have the Zyxel Device check e-mail for a specific source or relay IP address. Select IPv6 Address to have the Zyxel Device check e-mail for a specific source or relay IPv6 address. Select E-Mail Address to have the Zyxel Device check e-mail for a specific source e-mail address or domain name. Select Mail Header to have the Zyxel Device check e-mail for specific header fields and values. Configure block list header entries to check for e-mail from bulk mail programs or with content commonly used in spam. Configure allow list header entries to allow certain header values that identify the e-mail as being from a trusted source.
Mail Subject Keyword	This field displays when you select the Subject type. Enter up to 63 ASCII characters of text to check for in e-mail headers. Spaces are not allowed, although you could substitute a question mark (?). See Section 28.5.2 on page 660 for more details.
Sender or Mail Relay IP Address	This field displays when you select the IP Address type. Enter an IP address in dotted decimal notation.
Sender or Mail Relay IPv6 Address	This field displays when you select the IPv6 Address type. Enter an IPv6 address with prefix.
Netmask	This field displays when you select the IP type. Enter the subnet mask here, if applicable.
Sender E-Mail Address	This field displays when you select the E-Mail type. Enter a keyword (up to 63 ASCII characters). See Section 28.5.2 on page 660 for more details.

Table 212 Configuration > Security Service > Anti-Spam > Block/Allow List > Block/Allow List > Add

LABEL	DESCRIPTION
Mail Header Field Name	This field displays when you select the Mail Header type. Type the name part of an e-mail header (the part that comes before the colon). Use up to 63 ASCII characters. For example, if you want the entry to check the “Received:” header for a specific mail server’s domain, enter “Received” here.
Field Value Keyword	This field displays when you select the Mail Header type. Type the value part of an e-mail header (the part that comes after the colon). Use up to 63 ASCII characters. For example, if you want the entry to check the “Received:” header for a specific mail server’s domain, enter the mail server’s domain here. See Section 28.5.2 on page 660 for more details.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving your changes.

28.5.2 Regular Expressions in Block or Allow List Entries

The following applies for a block or allow list entry based on an e-mail subject, e-mail address, or e-mail header value.

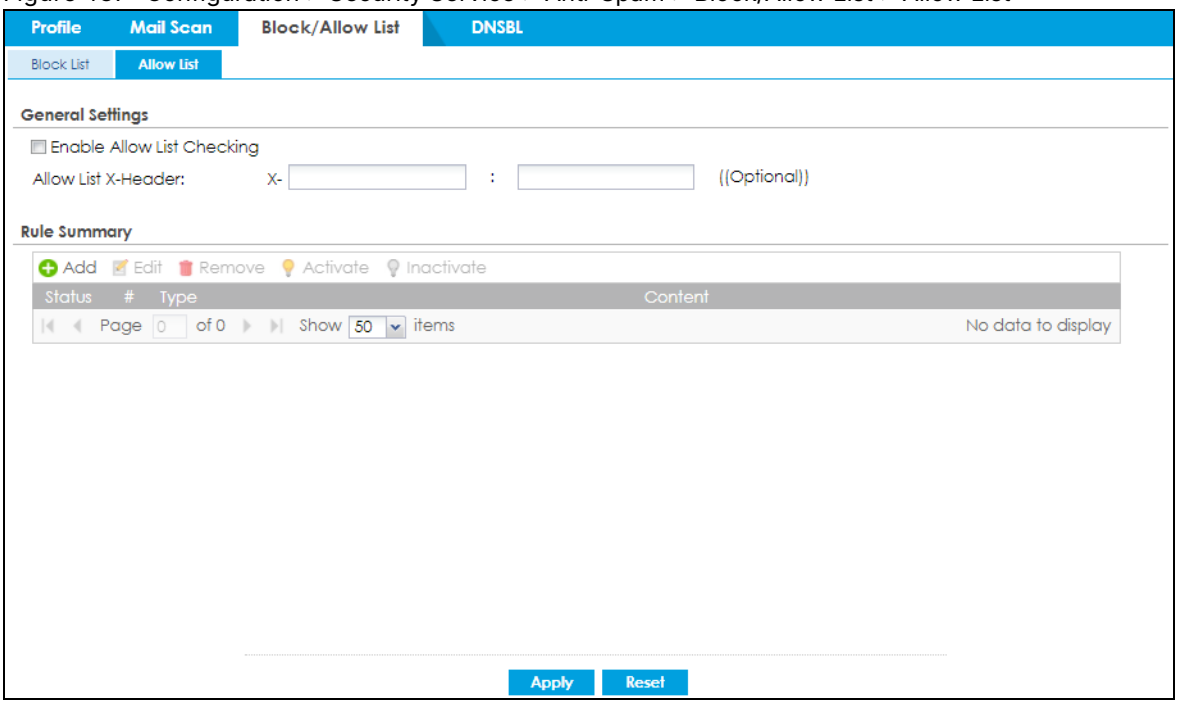
- Use a question mark (?) to let a single character vary. For example, use “a?c” (without the quotation marks) to specify abc, acc and so on.
- You can also use a wildcard (*). For example, if you configure *def.com, any e-mail address that ends in def.com matches. So “mail.def.com” matches.
- The wildcard can be anywhere in the text string and you can use more than one wildcard. You cannot use two wildcards side by side, there must be other characters between them.
- The Zyxel Device checks the first header with the name you specified in the entry. So if the e-mail has more than one “Received” header, the Zyxel Device checks the first one.

28.6 The Anti-Spam Allow List Screen

Click Configuration > Security Service > Anti-Spam > Block/Allow List and then the Allow List tab to display the Anti-Spam Allow List screen.

Configure the allow list to identify legitimate e-mail. You can create allow list entries based on the sender’s or relay’s IP address or e-mail address. You can also create entries that check for particular header fields and values or specific subject text.

Figure 437 Configuration > Security Service > Anti-Spam > Block/Allow List > Allow List



The following table describes the labels in this screen.

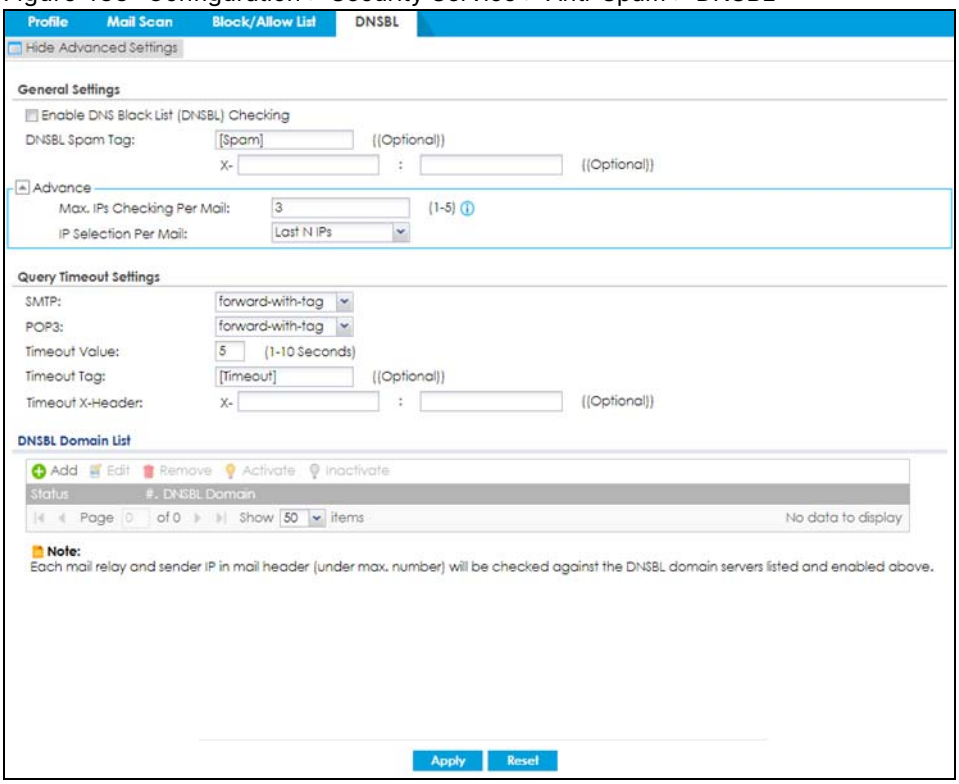
Table 213 Configuration > Security Service > Anti-Spam > Block/Allow List > Allow List

LABEL	DESCRIPTION
General Settings	
Enable Allow List Checking	Select this checkbox to have the Zyxel Device forward e-mail that matches (an active) allow list entry without doing any more anti-spam checking on that individual e-mail.
Allow List X-Header	Specify the name and value for the X-Header to be added to e-mails that match the Zyxel Device's spam allow list.
Rule Summary	
Add	Click this to create a new entry. See Section 28.5.1 on page 659 for details.
Edit	Select an entry and click this to be able to modify it. See Section 28.5.1 on page 659 for details.
Remove	Select an entry and click this to delete it.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
#	This is the entry's index number in the list.
Type	This field displays whether the entry is based on the e-mail's subject, source or relay IP address, source e-mail address, or a header.
Content	This field displays the subject content, source or relay IP address, source e-mail address, or header value for which the entry checks.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

28.7 The DNSBL Screen

Click Configuration > Security Service > Anti-Spam > DNSBL to display the anti-spam DNSBL screen. Use this screen to configure the Zyxel Device to check the sender and relay IP addresses in e-mail headers against DNS (Domain Name Service)-based spam Black Lists (DNSBLs).

Figure 438 Configuration > Security Service > Anti-Spam > DNSBL



The following table describes the labels in this screen.

Table 214 Configuration > Security Service > Anti-Spam > DNSBL

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Enable DNS Black List (DNSBL) Checking	Select this to have the Zyxel Device check the sender and relay IP addresses in e-mail headers against the DNSBL servers maintained by the DNSBL domains listed in the Zyxel Device.
DNSBL Spam Tag	Enter a message or label (up to 15 ASCII characters) to add to the beginning of the mail subject of e-mails that have a sender or relay IP address in the header that matches a block list maintained by one of the DNSBL domains listed in the Zyxel Device. This tag is only added if the anti-spam policy is configured to forward spam mail with a spam tag.
Max. IPs Checking Per Mail	Set the maximum number of sender and relay server IP addresses in the mail header to check against the DNSBL domain servers.
IP Selection Per Mail	Select first N IPs to have the Zyxel Device start checking from the first IP address in the mail header. This is the IP of the sender or the first server that forwarded the mail. Select last N IPs to have the Zyxel Device start checking from the last IP address in the mail header. This is the IP of the last server that forwarded the mail.

Table 214 Configuration > Security Service > Anti-Spam > DNSBL (continued)

LABEL	DESCRIPTION
Query Timeout Setting	
SMTP	Select how the Zyxel Device is to handle SMTP mail (mail) going to an e-mail server) if the queries to the DNSBL domains time out. Select drop to discard SMTP mail. Select forward to allow SMTP mail to go through. Select forward with tag to add a DNSBL timeout tag to the mail subject of an SMTP mail and send it.
POP3	Select how the Zyxel Device is to handle POP3 mail (mail coming to an e-mail client) if the queries to the DNSBL domains time out. Select forward to allow POP3 mail to go through. Select forward with tag to add a DNSBL timeout tag to the mail subject of an POP3 mail and send it.
Timeout Value	Set how long the Zyxel Device waits for a reply from the DNSBL domains listed below. If there is no reply before this time period expires, the Zyxel Device takes the action defined in the relevant Actions when Query Timeout field.
Timeout Tag	Enter a message or label (up to 15 ASCII characters) to add to the mail subject of e-mails that the Zyxel Device forwards if queries to the DNSBL domains time out.
Timeout X-Header	Specify the name and value for the X-Header to be added to e-mails that the Zyxel Device forwards if queries to the DNSBL domains time out.
DNSBL Domain List	
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
#	This is the entry's index number in the list.
DNSBL Domain	This is the name of a domain that maintains DNSBL servers. Enter the domain that is maintaining a DNSBL.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

28.8 Anti-Spam Technical Reference

Here is more detailed anti-spam information.

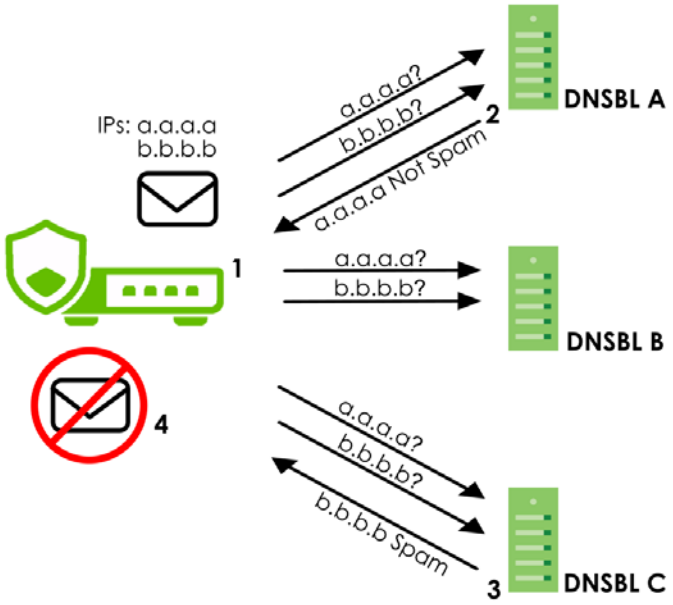
DNSBL

- The Zyxel Device checks only public sender and relay IP addresses, it does not check private IP addresses.
- The Zyxel Device sends a separate query (DNS lookup) for each sender or relay IP address in the e-mail's header to each of the Zyxel Device's DNSBL domains at the same time.

- The DNSBL servers send replies as to whether or not each IP address matches an entry in their list. Each IP address has a separate reply.
- As long as the replies are indicating the IP addresses do not match entries on the DNSBL lists, the Zyxel Device waits until it receives at least one reply for each IP address.
- If the Zyxel Device receives a DNSBL reply that one of the IP addresses is in the DNSBL list, the Zyxel Device immediately classifies the e-mail as spam and takes the anti-spam policy's configured action for spam. The Zyxel Device does not wait for any more DNSBL replies.
- If the Zyxel Device receives at least one non-spam reply for each of an e-mail's routing IP addresses, the Zyxel Device immediately classifies the e-mail as legitimate and forwards it.
- Any further DNSBL replies that come after the Zyxel Device classifies an e-mail as spam or legitimate have no effect.
- The Zyxel Device records DNSBL responses for IP addresses in a cache for up to 72 hours. The Zyxel Device checks an e-mail's sender and relay IP addresses against the cache first and only sends DNSBL queries for IP addresses that are not in the cache.

Here is an example of an e-mail classified as spam based on DNSBL replies.

Figure 439 DNSBL Spam Detection Example



1 The Zyxel Device receives an e-mail that was sent from IP address a.a.a.a and relayed by an e-mail server at IP address b.b.b.b. The Zyxel Device sends a separate query to each of its DNSBL domains for IP address a.a.a.a. The Zyxel Device sends another separate query to each of its DNSBL domains for IP address b.b.b.b.

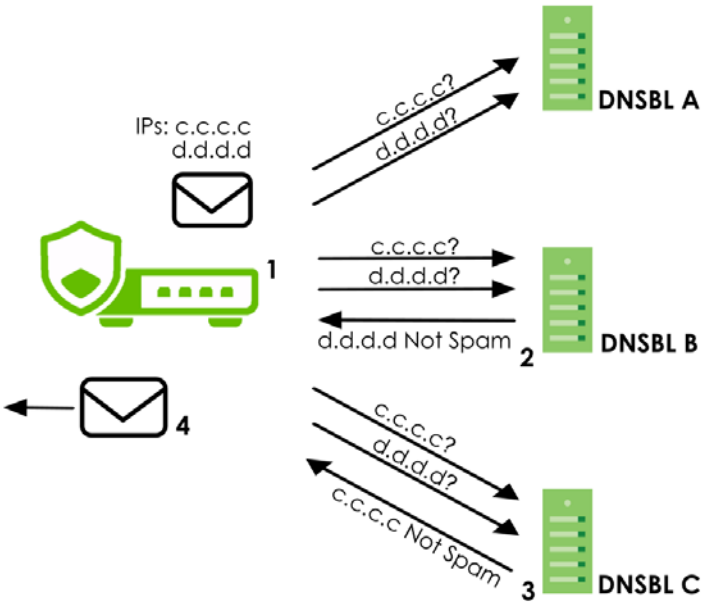
2 DNSBL A replies that IP address a.a.a.a does not match any entries in its list (not spam).

3 DNSBL C replies that IP address b.b.b.b matches an entry in its list.

4 The Zyxel Device immediately classifies the e-mail as spam and takes the action for spam that you defined in the anti-spam policy. In this example it was an SMTP mail and the defined action was to drop the mail. The Zyxel Device does not wait for any more DNSBL replies.

Here is an example of an e-mail classified as legitimate based on DNSBL replies.

Figure 440 DNSBL Legitimate E-mail Detection Example



1 The Zyxel Device receives an e-mail that was sent from IP address c.c.c.c and relayed by an e-mail server at IP address d.d.d.d. The Zyxel Device sends a separate query to each of its DNSBL domains for IP address c.c.c.c. The Zyxel Device sends another separate query to each of its DNSBL domains for IP address d.d.d.d.

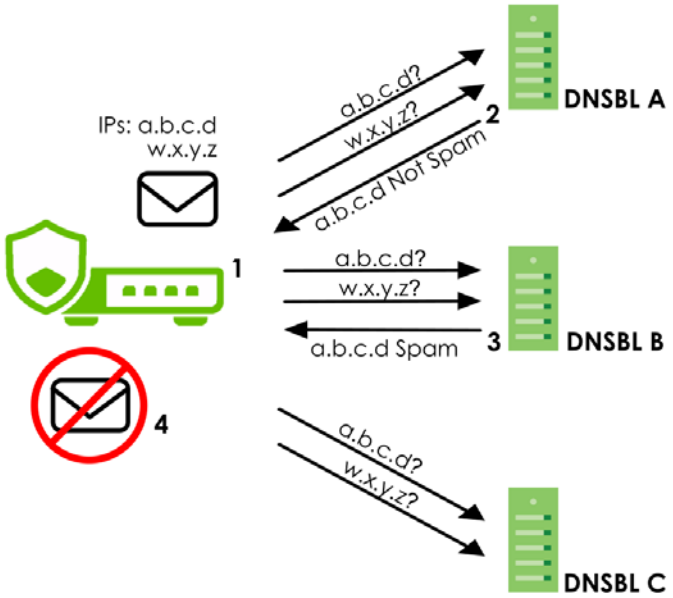
2 DNSBL B replies that IP address d.d.d.d does not match any entries in its list (not spam).

3 DNSBL C replies that IP address c.c.c.c does not match any entries in its list (not spam).

4 Now that the Zyxel Device has received at least one non-spam reply for each of the e-mail's routing IP addresses, the Zyxel Device immediately classifies the e-mail as legitimate and forwards it. The Zyxel Device does not wait for any more DNSBL replies.

If the Zyxel Device receives conflicting DNSBL replies for an e-mail routing IP address, the Zyxel Device classifies the e-mail as spam. Here is an example.

Figure 441 Conflicting DNSBL Replies Example



1 The Zyxel Device receives an e-mail that was sent from IP address a.b.c.d and relayed by an e-mail server at IP address w.x.y.z. The Zyxel Device sends a separate query to each of its DNSBL domains for IP address a.b.c.d. The Zyxel Device sends another separate query to each of its DNSBL domains for IP address w.x.y.z.

2 DNSBL A replies that IP address a.b.c.d does not match any entries in its list (not spam).

3 While waiting for a DNSBL reply about IP address w.x.y.z, the Zyxel Device receives a reply from DNSBL B saying IP address a.b.c.d is in its list.

4 The Zyxel Device immediately classifies the e-mail as spam and takes the action for spam that you defined in the anti-spam policy. In this example it was an SMTP mail and the defined action was to drop the mail. The Zyxel Device does not wait for any more DNSBL replies.

CHAPTER 29
Astra Cloud Security

29.1 Overview

The Astra web portal is a platform that provides security services to mobile devices. It is managed by an admin. You can configure security services such as content filter and URL blocking to protect mobile devices that install the Astra app.

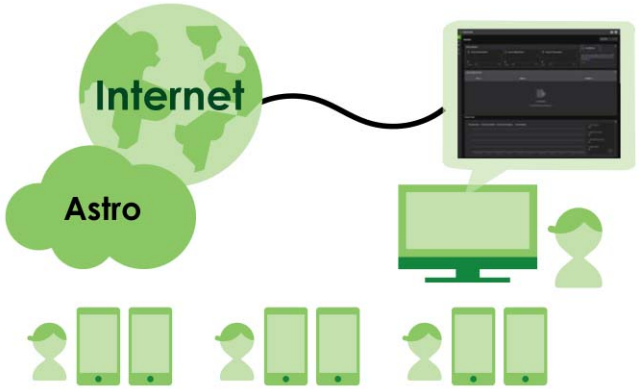
See the Astra web portal online help at *http://www.zyxel.com/web-help-compact/AstraPortal/index.html* for more information.

The Astra app protects traffic on the members mobile devices that install this app. A member is a person whose mobile device the admin wishes to protect. You can also enable email leakage detection to receive an email from the Astra app if your email address was illegally or unknowingly used to access certain websites.

Please note that only two mobile devices can use the same account to log into the Astra app at a time. You need to contact your admin to remove one of your device first if you wish to log into the Astra app on a third mobile device.

See the Astra app online help at *http://www.zyxel.com/web-help-app/Astra/index.html* for more information.

Figure 442 Astra Network Overview



29.2 Astra Cloud Security Screen

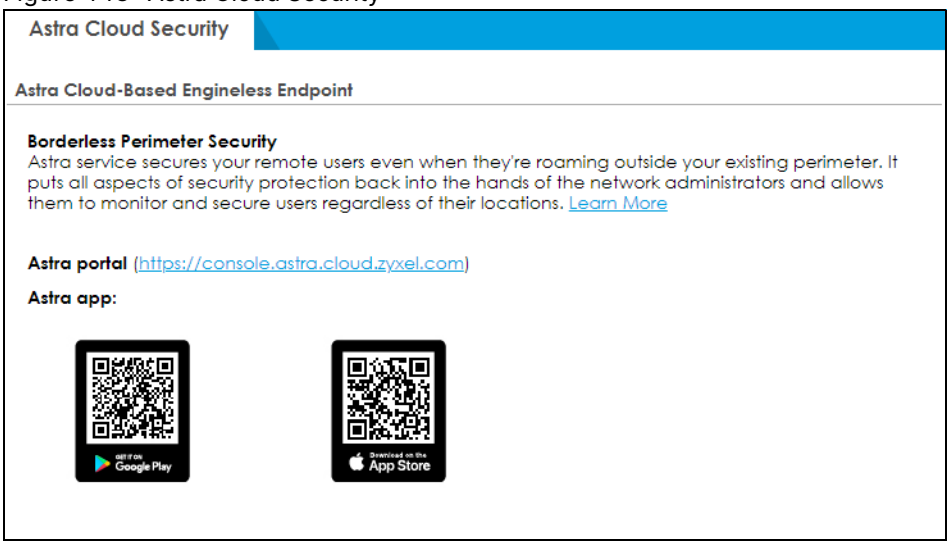
Click Security Service > Astra Cloud Security to open the following screen.

Click Learn More to go to the Astra product page.

If you are an admin, click *https://console.astra.cloud.zyxel.com* to go to the Astra web portal.

If you are a member, scan one of the QR codes to download the Astra app from Google Play (Android) or Apple App Store (iOS).

Figure 443 Astra Cloud Security



CHAPTER 30
Object

30.1 The Device Insight Screen

Use this screen to configure profiles to block specified clients from accessing the Internet or the Zyxel Device in Configuration > Security Policy > Policy Control. Configure profiles for WiFi and wired clients connected to the Zyxel Device according to the types of devices they use or operating systems their devices use.

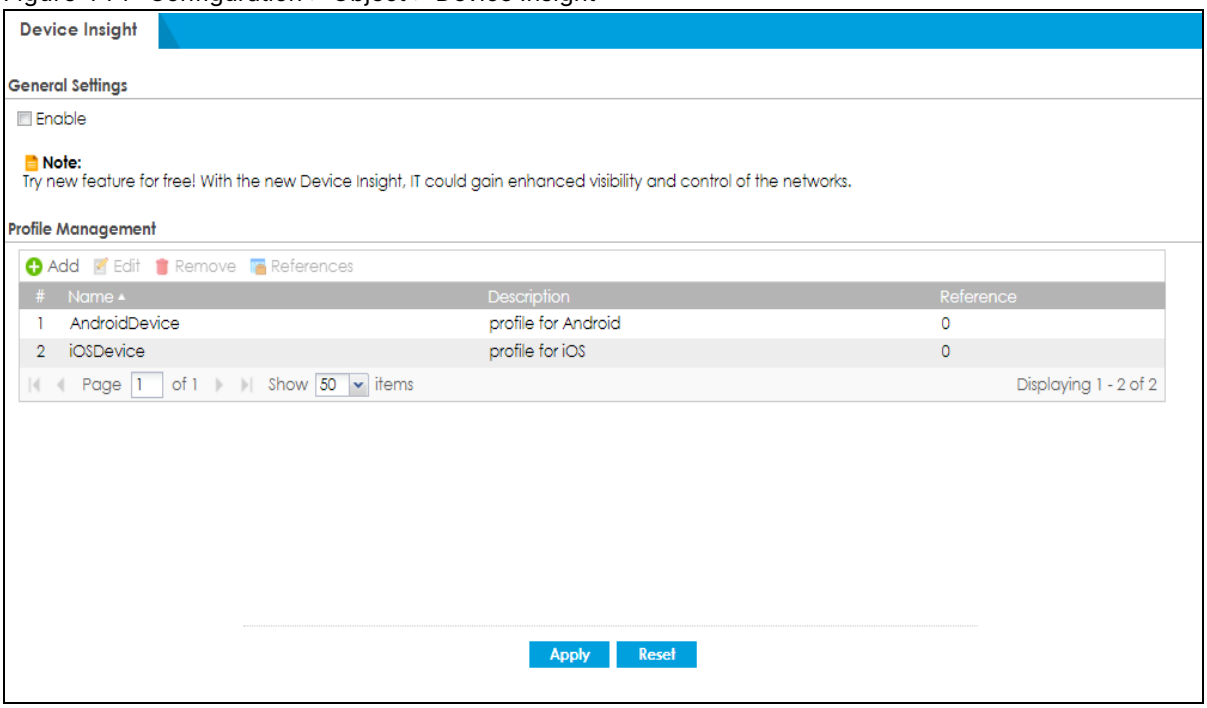
Note: To collect clients' information using Device Insight, the clients must be in the same IP subnet in the LAN/VLAN/DMZ networks behind the Zyxel Device. Information from clients that are in different IP subnets in the LAN/VLAN/DMZ networks might not be collected correctly as traffic must pass through another router or a layer-2 switch to the Zyxel Device.

Here's the process for the Zyxel Device to block a profile in this screen:

1. Create a profile in the Device Insight screen to block specific clients.
2. Add the created device insight profile to one of the rules in Policy Control.
3. The Zyxel Device will block clients if they match the settings you configure in the Device Insight profile.

To access this screen, go to Configuration > Object > Device Insight.

Figure 444 Configuration > Object > Device Insight



The following table describes the labels in this screen.

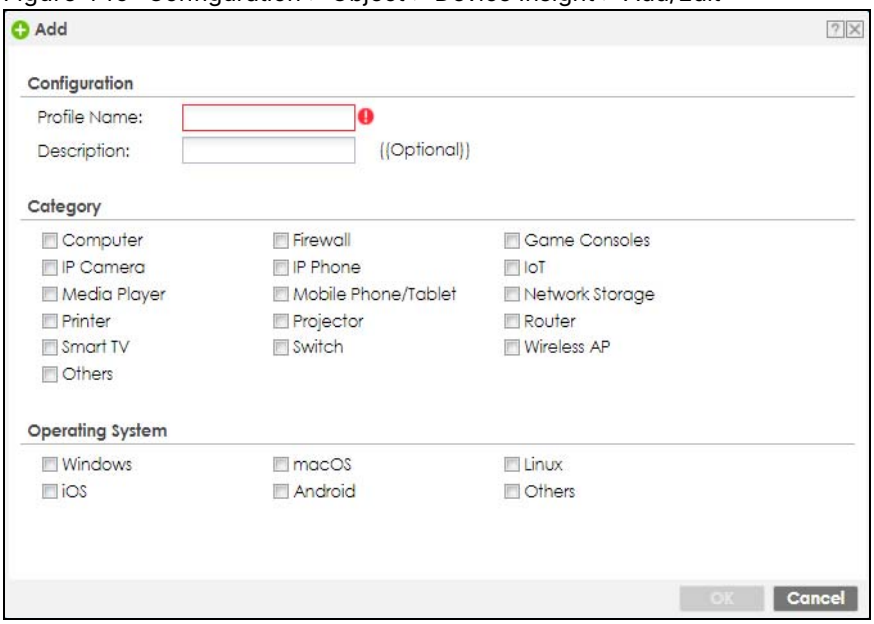
Table 215 Configuration > Object > Device Insight

LABEL	DESCRIPTION
General Settings	
Enable	Select this to enable device insight. Clear this to disable it.
Add	Click this to create a new, user-configured zone.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove a user-configured trunk, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click References to open a screen that shows which settings use the entry. Click Refresh to update information in this screen.
#	This field is a sequential value, and it is not associated with any interface.
Name	This field displays the name of the device.
Description	If the device insight profile has a description configured, it displays here.
Reference	This field displays the number of times an Object Reference is used in a policy.

30.1.1 Device Insight Add/Edit Screen

The Device Insight Add/Edit screen allows you to add a new device insight profile or edit and existing one. To access this screen, go to Configuration > Object > Device Insight > Add/Edit.

Figure 445 Configuration > Object > Device Insight > Add/Edit



The following table describes the labels in this screen.

Table 216 Configuration > Object > Device Insight > Add/Edit

LABEL	DESCRIPTION
Profile Name	Type a name for this device insight profile. You may use 1-31 alphanumeric character, underscores (_), or dashes (-), but the first character cannot be a number. Spaces and duplicate names are not allowed. This value is case-sensitive.
Description	Enter the description of each device insight profile. You can use 1 to 63 single-byte characters, including 0-9a-zA-Z!"#$%'()*+,-/:;=?@_ &.<>[\]^'{|} are not allowed.
Category	Select the type of device used by the connected client for this profile. IoT (Internet of Things) is a device with sensors and software that collects and analyzes data. It exchanges the data it collects with other devices over the Internet. IoT is used in many places, such as home assistant, personal care or toys. For example, a smart watch that your grandparents wear is an IoT. It can detects the heart rate and blood pressure of the person wearing it. It sends out warning to other devices, such as your parents phones, if it detects something wrong.
Operating System	Select the device operating system used by the connected client for this profile.
OK	Click this button to save your changes to the Zyxel Device and return to the summary screen.
Cancel	Click this button to return to the summary screen without saving any changes.

30.1.2 Example: Block a Profile

In this example, company A on the Zyxel Device LAN1 wants to block its subsidiary employees on LAN2 from accessing the company A local networks with their mobile phones. Company A can create a profile that includes all operating systems mobile phones, and then apply it to the LAN2_To_LAN1 policy you created. Clients using mobile phones on the Zyxel Device LAN2 will be blocked from accessing the Zyxel Device LAN1.

Here's the process to use a Device Insight profile in a Zyxel Device security policy. The example below uses the parameters in this table.

Table 217 Device Insight Profile Configurations Example

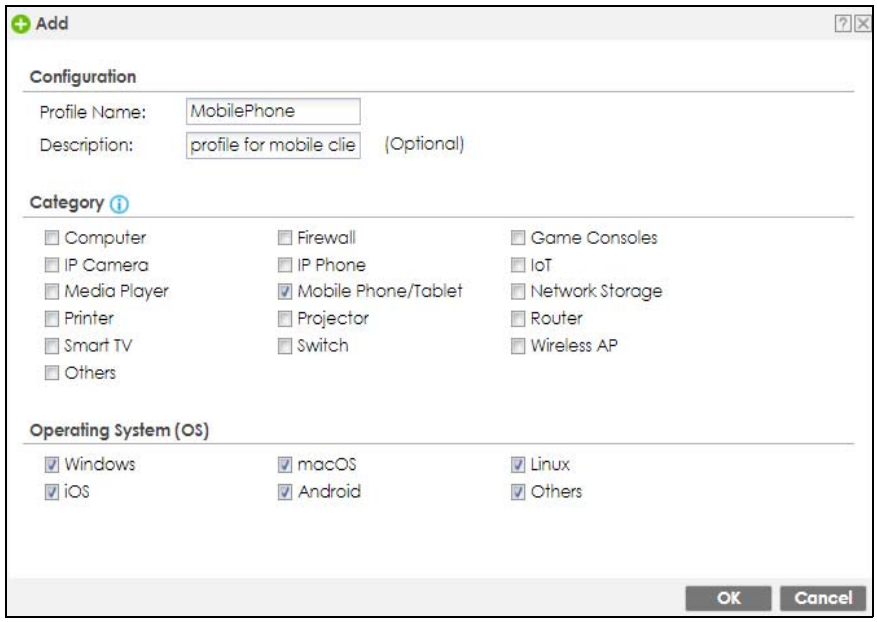
PROFILE NAME	DESCRIPTION	CATEGORY	OPERATING SYSTEM	APPLIED POLICY
MobilePhone	profile for mobile clients	Mobile Phone/Tablet	• Windows • macOS • Linux • OS • Android • Others	LAN2_To_LAN1

The security policy LAN2_To_LAN1 uses the parameters in this table

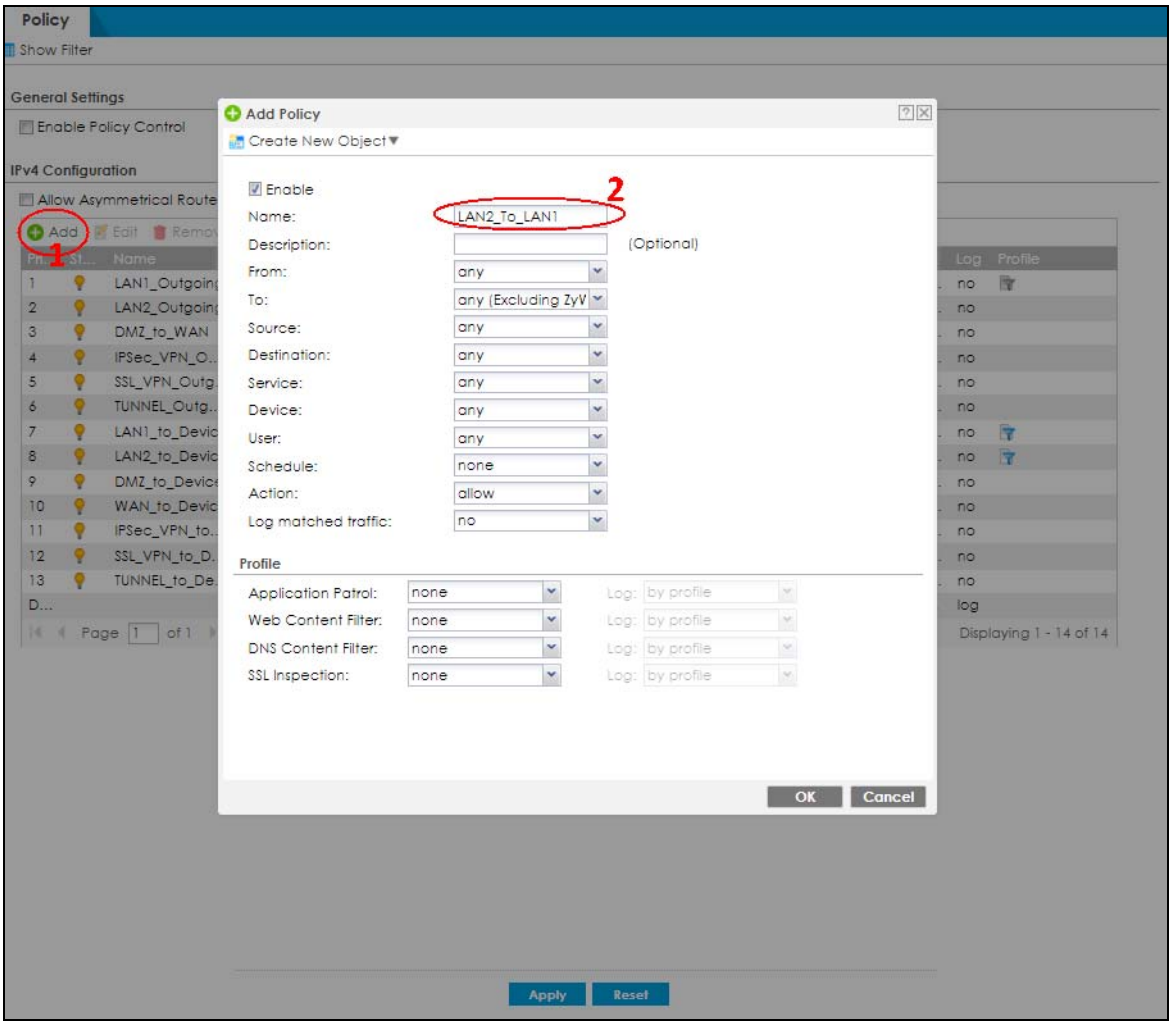
Table 218 Device Insight Profile Configurations Example

TO	FROM	ACTION	DEVICE INSIGHT PROFILE
LAN1	LAN2	deny	MobilePhone

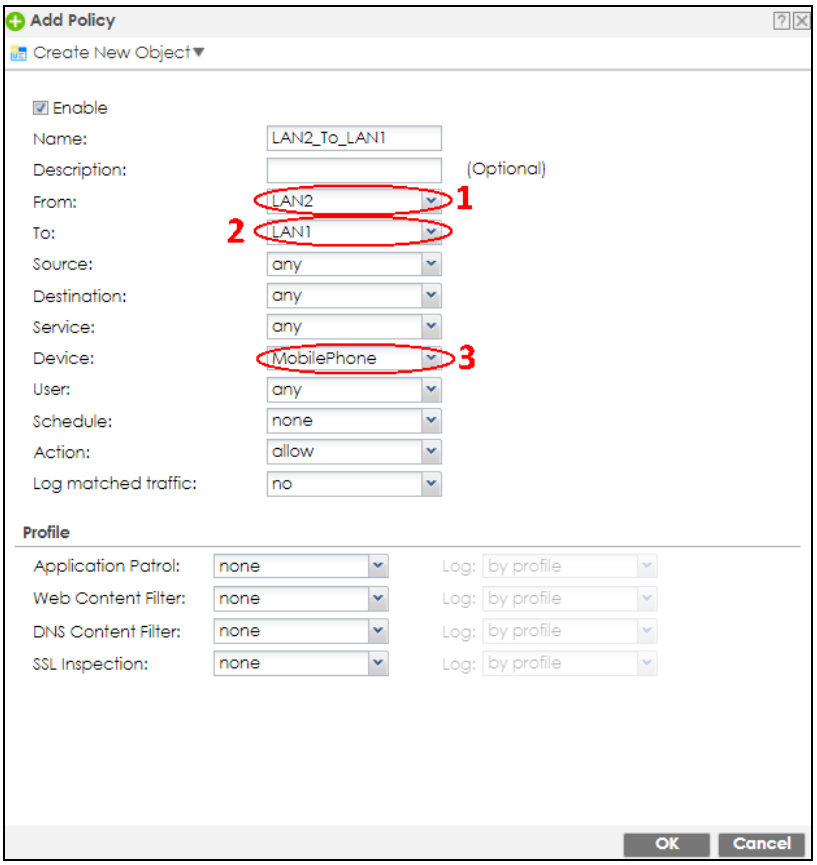
1 Go to Object > Device Insight and click Add. Follow the parameters in the table above to configure a profile for clients using mobile phones. Click OK to save your changes.



2 Go to Configuration > Security Policy > Policy Control. Click Add to create a rule and name it as LAN2_To_LAN1.

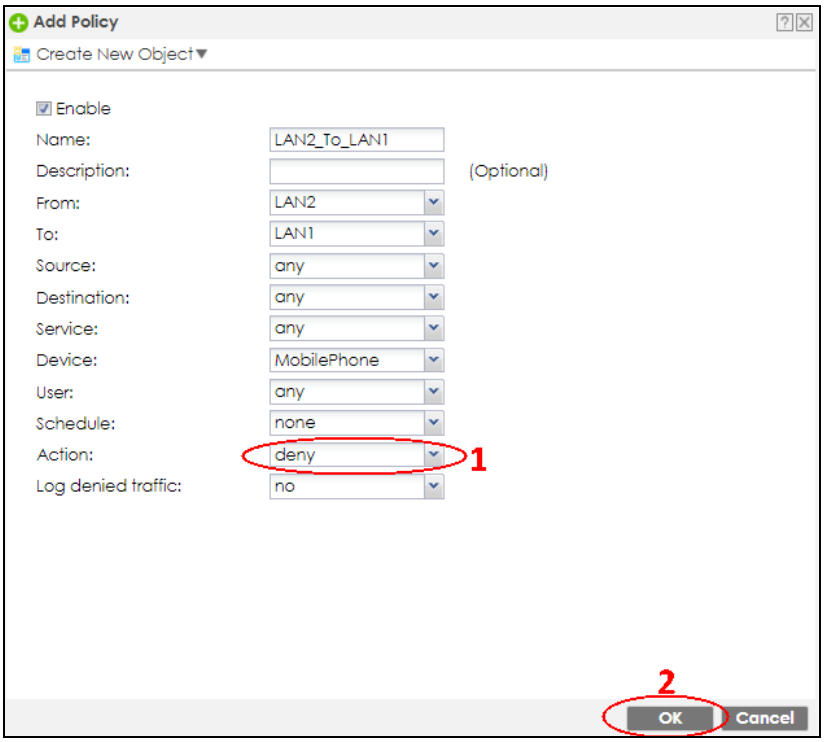


3 In the Add Policy screen, set From to LAN2 and To to LAN1 to configure the traffic direction for the security policy. Add the created Device Insight (MobilePhone) profile to the security policy.



4 Set the Action to deny then click OK to save your changes. Check that the Device Insight profile name (MobilePhone) shows under the Device column to make sure clients using mobile phones are blocked from accessing the Zyxel Device LAN1 from LAN2.

Note: Make sure to configure a security policy to ensure your access to the Zyxel Device before blocking a Device Insight profile. Reset the Zyxel Device if you're blocked from accessing the Zyxel Device.

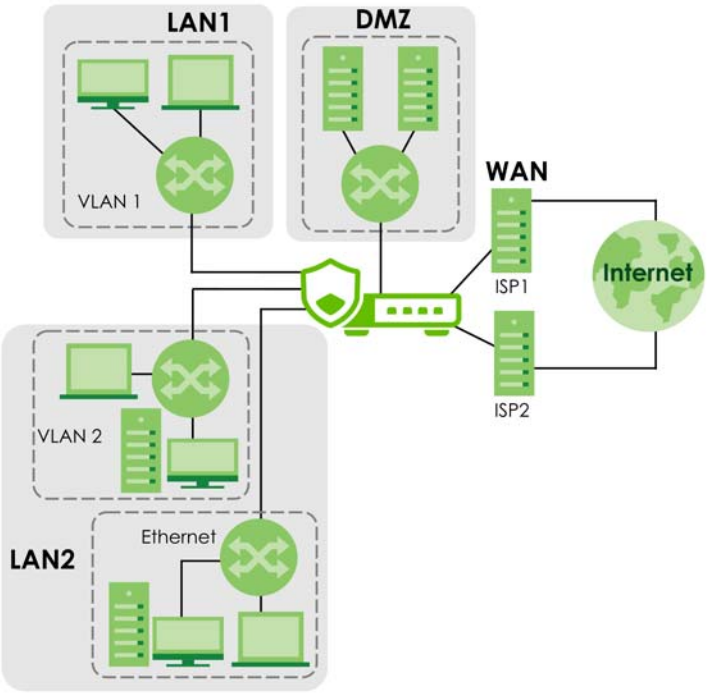


30.2 Zones Overview

Set up zones to configure network security and network policies in the Zyxel Device. A zone is a group of interfaces and/or VPN tunnels. The Zyxel Device uses zones instead of interfaces in many security and policy settings, such as Secure Policies rules, Security Service, and remote management.

Zones cannot overlap. Each Ethernet interface, VLAN interface, bridge interface, PPPoE/PPTP interface and VPN tunnel can be assigned to at most one zone. Virtual interfaces are automatically assigned to the same zone as the interface on which they run.

Figure 446 Example: Zones



Use the Zone screens (see Section 30.6.2 on page 721) to manage the Zyxel Device's zones.

30.2.1 What You Need to Know

Zones effectively divide traffic into three types--intra-zone traffic, inter-zone traffic, and extra-zone traffic.

Intra-zone Traffic

- Intra-zone traffic is traffic between interfaces or VPN tunnels in the same zone. For example, in Figure 446 on page 676, traffic between VLAN 2 and the Ethernet is intra-zone traffic.

Inter-zone Traffic

Inter-zone traffic is traffic between interfaces or VPN tunnels in different zones. For example, in Figure 446 on page 676, traffic between VLAN 1 and the Internet is inter-zone traffic. This is the normal case when zone-based security and policy settings apply.

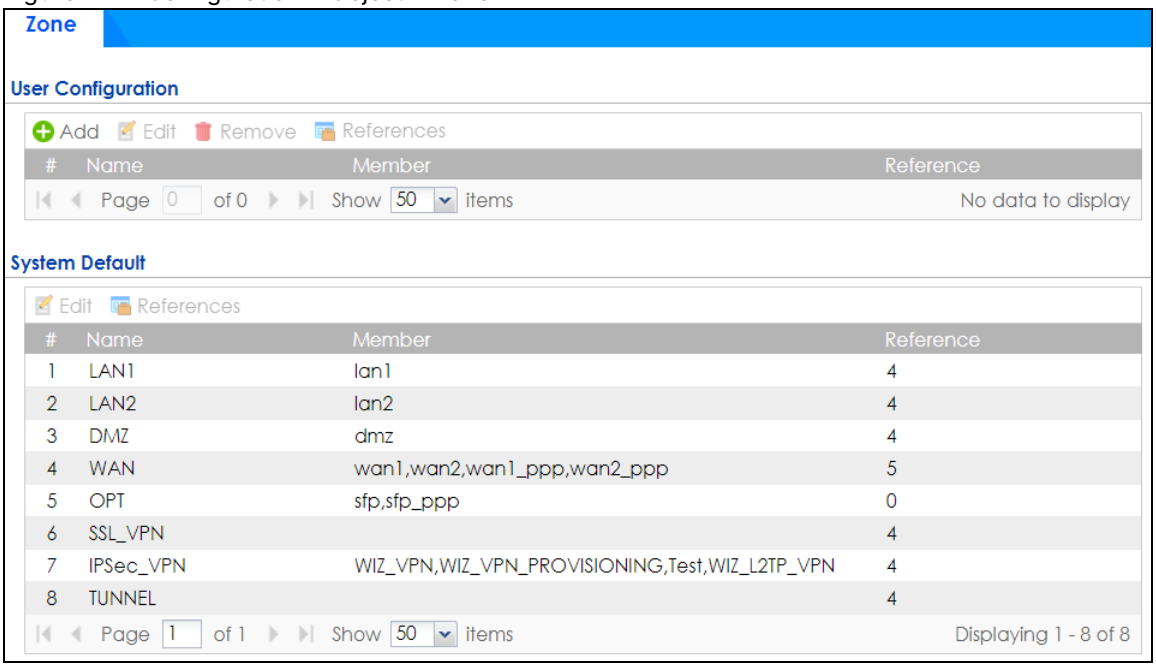
Extra-zone Traffic

- Extra-zone traffic is traffic to or from any interface or VPN tunnel that is not assigned to a zone. For example, in Figure 446 on page 676, traffic to or from computer C is extra-zone traffic.
- Some zone-based security and policy settings may apply to extra-zone traffic, especially if you can set the zone attribute in them to Any or All. See the specific feature for more information.

30.2.2 The Zone Screen

The Zone screen provides a summary of all zones. In addition, this screen allows you to add, edit, and remove zones. To access this screen, click Configuration > Object > Zone.

Figure 447 Configuration > Object > Zone



The following table describes the labels in this screen.

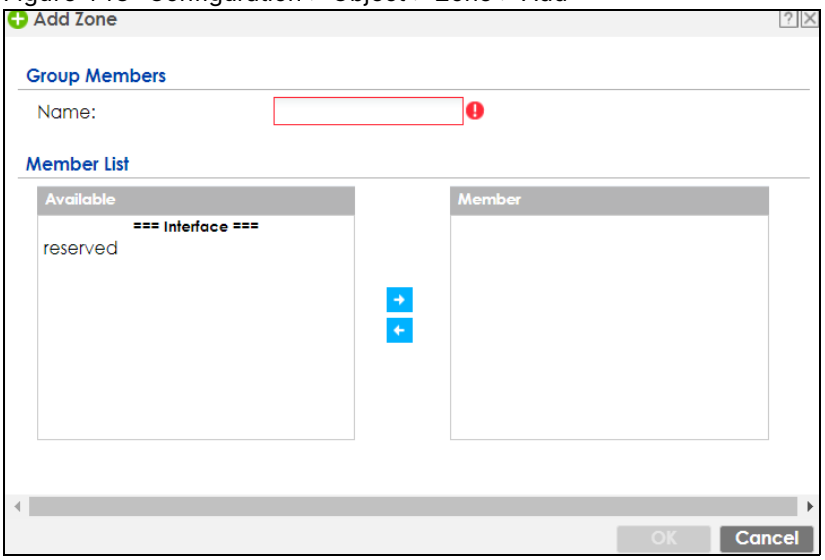
Table 219 Configuration > Object > Zone

LABEL	DESCRIPTION
User Configuration / System Default	The Zyxel Device comes with pre-configured System Default zones that you cannot delete. You can create your own User Configuration zones
Add	Click this to create a new, user-configured zone.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove a user-configured trunk, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click References to open a screen that shows which settings use the entry. Click Refresh to update information in this screen.
#	This field is a sequential value, and it is not associated with any interface.
Name	This field displays the name of the zone.
Member	This field displays the names of the interfaces that belong to each zone.
Reference	This field displays the number of times an Object Reference is used in a policy.

30.2.2.1 Zone Edit

The Zone Edit screen allows you to add or edit a zone. To access this screen, go to the Zone screen (see Section 30.6.2 on page 721), and click the Add icon or an Edit icon.

Figure 448 Configuration > Object > Zone > Add



The following table describes the labels in this screen.

Table 220 Configuration > Object > Zone > Add/Edit

LABEL	DESCRIPTION
Name	For a system default zone, the name is read only. For a user-configured zone, type the name used to refer to the zone. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Member List	Available lists the interfaces and VPN tunnels that do not belong to any zone. Select the interfaces and VPN tunnels that you want to add to the zone you are editing, and click the right arrow button to add them. Member lists the interfaces and VPN tunnels that belong to the zone. Select any interfaces that you want to remove from the zone, and click the left arrow button to remove them.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

30.3 User/Group Overview

This section describes how to set up user accounts, user groups, and user settings for the Zyxel Device. You can also set up rules that control when users have to log in to the Zyxel Device before the Zyxel Device routes traffic for them.

- The User screen (see Section 30.3.2 on page 681) provides a summary of all user accounts.
- The Group screen (see Section 30.3.5 on page 697) provides a summary of all user groups. In addition, this screen allows you to add, edit, and remove user groups. User groups may consist of access users and other user groups. You cannot put admin users in user groups.
- The Setting screen (see Section 30.3.6 on page 699) controls default settings, login settings, lockout settings, and other user settings for the Zyxel Device. You can also use this screen to specify when users must log in to the Zyxel Device before it routes traffic for them.

- The MAC Address screen (see Section 30.3.7 on page 703) allows you to configure the MAC addresses or OUI (Organizationally Unique Identifier) of wireless clients for MAC authentication using the local user database. The OUI is the first three octets in a MAC address and uniquely identifies the manufacturer of a network device.

30.3.1 What You Need To Know

User Account

A user account defines the privileges of a user logged into the Zyxel Device. User accounts are used in security policies, in addition to controlling access to configuration and services in the Zyxel Device.

User Types

These are the types of user accounts the Zyxel Device uses.

Table 221 Types of User Accounts

TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
admin	Change Zyxel Device configuration (web, CLI)	WWW, TELNET, SSH, FTP, Console
Access Users		
limited-admin	Look at Zyxel Device configuration (web, CLI) Perform basic diagnostics (CLI) Cannot execute commands such as 'show running-config'	WWW, TELNET, SSH, Console
user	Access network services Browse user-mode commands (CLI)	WWW, TELNET, SSH
guest	Access network services	WWW
ext-user	External user account	WWW
ext-group-user	External group user account	WWW
guest-manager	Create dynamic guest accounts	WWW
dynamic-guest	Access network services	Hotspot Portal

Note: The default admin account is always authenticated locally, regardless of the authentication method setting. (See Chapter 30 on page 735 for more information about authentication methods.)

Ext-User Accounts

Set up an ext-user account if the user is authenticated by an external server and you want to set up specific policies for this user in the Zyxel Device. If you do not want to set up policies for this user, you do not have to set up an ext-user account.

All ext-user users should be authenticated by an external server, such as AD, LDAP or RADIUS. If the Zyxel Device tries to use the local database to authenticate an ext-user, the authentication attempt always fails. (This is related to AAA servers and authentication methods, which are discussed in those chapters in this guide.)

Note: If the Zyxel Device tries to authenticate an ext-user using the local database, the attempt always fails.

Once an ext-user user has been authenticated, the Zyxel Device tries to get the user type (see Table 221 on page 679) from the external server. If the external server does not have the information, the Zyxel Device sets the user type for this session to User.

For the rest of the user attributes, such as reauthentication time, the Zyxel Device checks the following places, in order.

1. User account in the remote server.
2. User account (Ext-User) in the Zyxel Device.
3. Default user account for AD users (ad-users), LDAP users (ldap-users) or RADIUS users (radius-users) in the Zyxel Device.

See Setting up User Attributes in an External Server for a list of attributes and how to set up the attributes in an external server.

Ext-Group-User Accounts

Ext-Group-User accounts work are similar to ext-user accounts but allow you to group users by the value of the group membership attribute configured for the AD or LDAP server. See Section 30.7.5.1 on page 730 for more on the group membership attribute.

Dynamic-Guest Accounts

Dynamic guest accounts are guest accounts, but are created dynamically and stored in the Zyxel Device's local user database. A dynamic guest account has a dynamically-created user name and password. A dynamic guest account user can access the Zyxel Device's services only within a given period of time and will become invalid after the expiration date/time.

There are three types of dynamic guest accounts depending on how they are created or authenticated: billing-users, ua-users and trial-users.

billing-users are guest account created with the guest manager account or an external printer and paid by cash or created and paid through the on-line payment service. ua-users are users that log in from the user agreement page. trial-users are free guest accounts that are created with the Free Time function.

User Groups

User groups may consist of user accounts or other user groups. Use user groups when you want to create the same rule for several user accounts, instead of creating separate rules for each one.

Note: You cannot put access users and admin users in the same user group.

Note: You cannot put the default admin account into any user group.

The sequence of members in a user group is not important.

User Awareness

By default, users do not have to log into the Zyxel Device to use the network services it provides. The Zyxel Device automatically routes packets for everyone. If you want to restrict network services that certain users can use through the Zyxel Device, you can require them to log in to the Zyxel Device first. The Zyxel Device is then 'aware' of the user who is logged in and you can create 'user-aware policies' that define what services they can use. See Section 30.3.8 on page 705 for a user-aware login example.

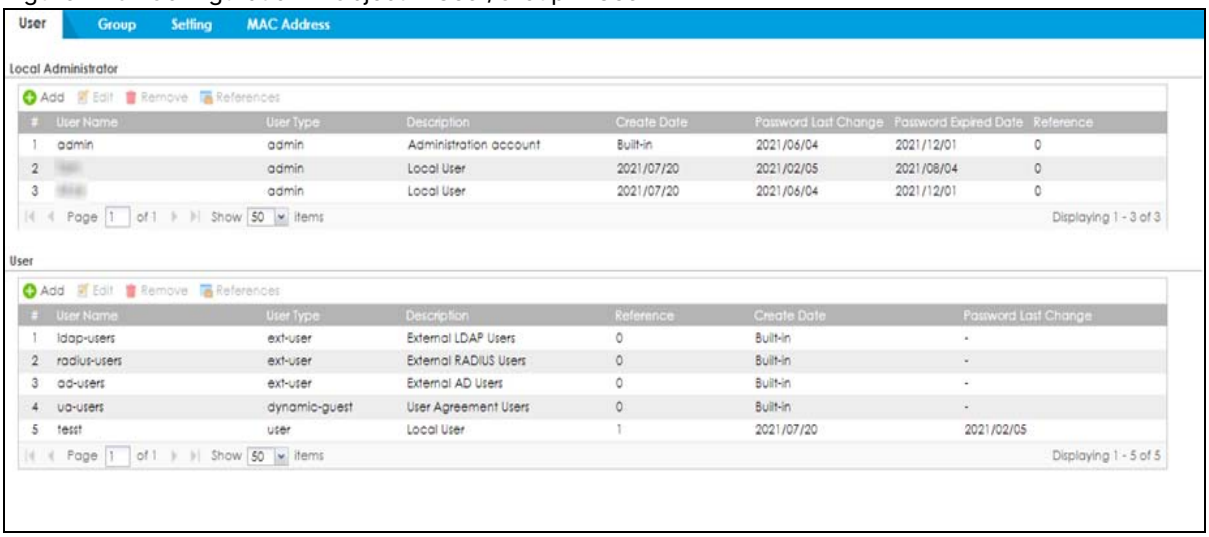
Finding Out More

- See Section 30.3.8 on page 705 for some information on users who use an external authentication server in order to log in.
- The Zyxel Device supports TTLS using PAP so you can use the Zyxel Device's local user database to authenticate users with WPA or WPA2 instead of needing an external RADIUS server.

30.3.2 User/Group User Summary Screen

The User screen provides a summary of all user accounts. To access this screen, login to the Web Configurator, and click Configuration > Object > User/Group.

Figure 449 Configuration > Object > User/Group > User



The following table describes the labels in this screen.

Table 222 Configuration > Object > User/Group > User

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click References to open a screen that shows which settings use the entry.
Local Administrator	Use this table to view and configure the Zyxel Device admin accounts.
#	This field is a sequential value, and it is not associated with a specific user.

Table 222 Configuration > Object > User/Group > User (continued)

LABEL	DESCRIPTION
User Name	This field displays the user name of each user.
User Type	This field displays the admin accounts the Zyxel Device uses. Admin accounts are users that can look at and change the configuration of the Zyxel Device
Description	This field displays the description for each user.
Created Date	This field displays the date the account is created. This field displays - if the account is created before the Zyxel Device upgrades firmware to version 5.10 or later.
Password Last Change	This field displays the last time the user changed the account password.
Password Expired Date	This field displays the account password expiry date. The user should change the password before it expires.
Reference	This displays the number of times an object reference is used in a profile.
User	Use this table to configure the Zyxel Device: • Limited-admin accounts. • User accounts. • Guest accounts. • Ext-user accounts. • Ext-group-user accounts.
#	This field is a sequential value, and it is not associated with a specific user.
User Name	This field displays the user name of each user.
User Type	This field displays the types of user accounts the Zyxel Device uses: • limited-admin - this user can look at the configuration of the Zyxel Device but not to change it • dynamic-guest - this user has access to the Zyxel Device's services but cannot look at the configuration. • user - this user has access to the Zyxel Device's services and can also browse user-mode commands (CLI). • guest - this user has access to the Zyxel Device's services but cannot look at the configuration • ext-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 679 for more information about this type. • ext-group-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 680 for more information about this type. • guest-manager - this user can log in through the web configurator login screen and create dynamic guest accounts using the Account Generator screen that pops up.
Description	This field displays the description for each user.
Create Date	This field displays the date the account is created.
Password Last Change	This field displays the last time the user changes the account password.
Reference	This displays the number of times an object reference is used in a profile.

30.3.3 User Add/Edit General Screen

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

30.3.3.1 Rules for User Names

Enter a user name from 1 to 31 characters.

The user name can only contain the following characters:

- Alphanumeric A-z 0-9 (there is no unicode support)
- _ [underscores]
- - [dashes]

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

- User names are case-sensitive. If you enter a user 'bob' but use 'BOB' when connecting through CIFS or FTP, it will use the account settings used for 'BOB' not 'bob'.
- User names have to be different than user group names.
- Here are the reserved user names:

  - adm
  - admin
  - any
  - bin
  - daemon
  - debug
  - devicehaecived
  - ftp
  - games
  - halt
  - ldap-users
  - lp
  - mail
  - news
  - nobody
  - operator
  - radius-users
  - root
  - shutdown
  - sshd
  - sync
  - uucp
  - zyxel

To access this screen, go to the User screen (see Section 30.3.2 on page 681), and click either the Add icon or an Edit icon.

Figure 450 Configuration > Object > User/Group > User > Add/Edit_General (Local Administrator)

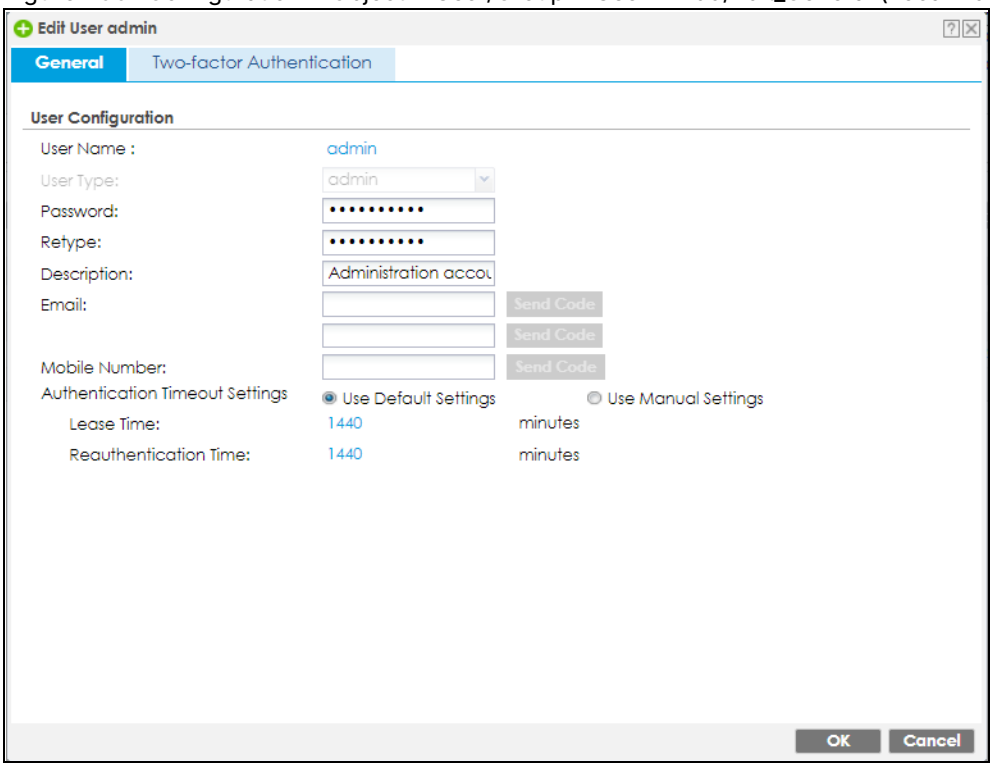
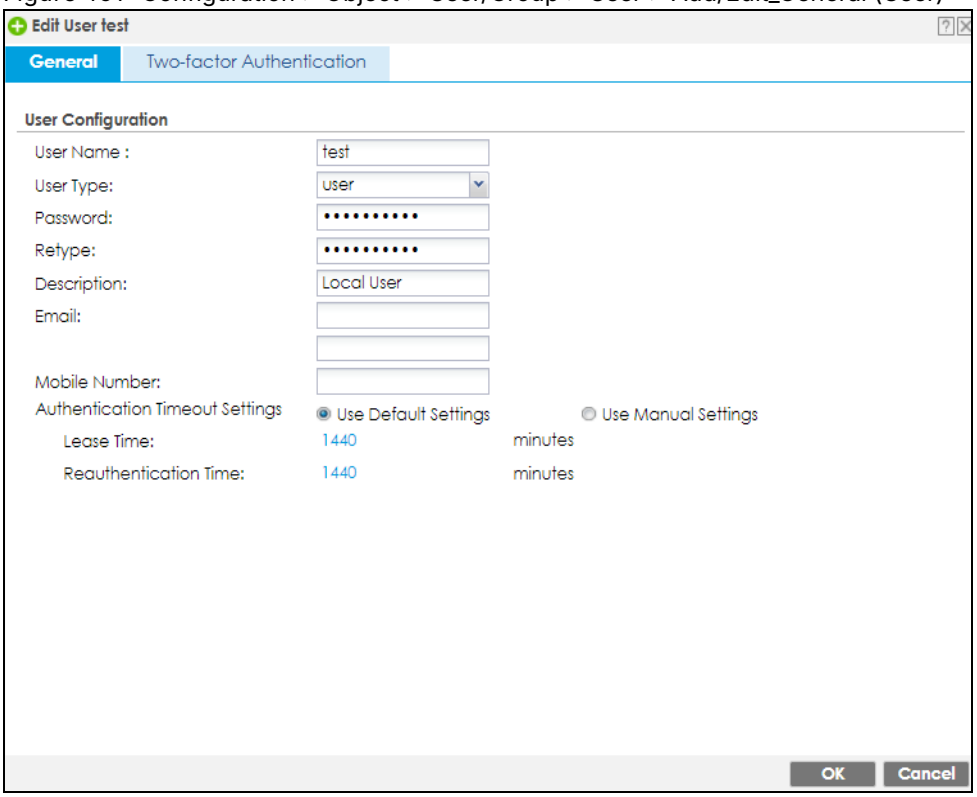


Figure 451 Configuration > Object > User/Group > User > Add/Edit_General (User)



The following table describes the labels in this screen.

Table 223 Configuration > Object > User/Group > User > Add/Edit_General

LABEL	DESCRIPTION
User Name	Type the user name for this user account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User names have to be different than user group names, and some words are reserved. See Section 30.3.3.1 on page 682.
User Type	This field is not available if you're adding an account to the Local Administrator table. Select the types of user accounts the Zyxel Device uses from the drop-down list box: • limited-admin - this user can look at the configuration of the Zyxel Device but not to change it • user - this user has access to the Zyxel Device's services and can also browse user-mode commands (CLI). • guest - this user has access to the Zyxel Device's services but cannot look at the configuration. • ext-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 679 for more information about this type. • ext-group-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 680 for more information about this type.
Password	This field is not available if you select the ext-user or ext-group-user type. Enter a password of from 1 to 64 characters for this user account. If you selected Enable Password Complexity in Configuration > Object > User/Group > Setting, it must consist of at least 8 characters and at most 64. 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 !@#$%^&*()_+. Note: After the first login, you are not allowed to set the password to 1234.

Table 223 Configuration > Object > User/Group > User > Add/Edit_General (continued)

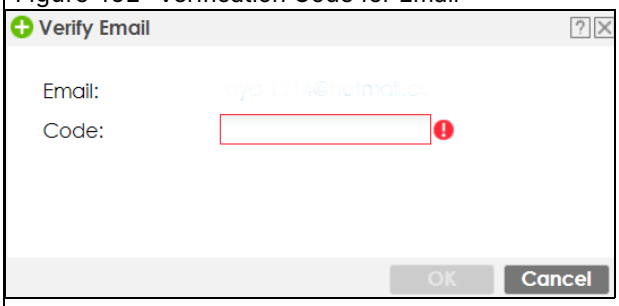
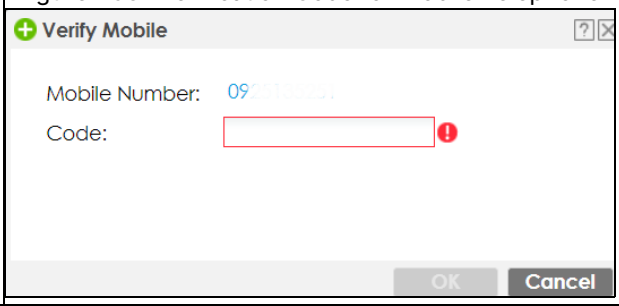
LABEL	DESCRIPTION
Retype	This field is not available if you select the ext-user or ext-group-user type.
Group Identifier	This field is available for a ext-group-user type user account. Specify the value of the AD or LDAP server's Group Membership Attribute that identifies the group to which this user belongs.
Associated AAA Server Object	This field is available for a ext-group-user type user account. Select the AAA server to use to authenticate this account's users.
Description	Enter the description of each user, if any. You can use 1 to 63 single-byte characters, including 0-9a-zA-Z!"#$%'()*+,-/:;=?@_ &.<>[\]{|}^'are not allowed. Default descriptions are provided.
Email	Type one or more valid email addresses for this user so that email messages can be sent to this user if required. A valid email address must contain the @ character. For example, this is a valid email address: abc@example.com.
Mobile Number	Type a valid mobile telephone number for this user so that SMS messages can be sent to this user if required. A valid mobile telephone number can be up to 20 characters in length, including the numbers 1~9 and the following characters in the square brackets [+*#()-].
Send Code	This button is available when the user type is admin or limited-admin. Click this and an authorization email or SMS message with a code of six digits will be sent to the email addresses or mobile telephone number you put in. Enter the verification code to verify your email addresses or mobile telephone number. Figure 452 Verification Code for Email  Figure 453 Verification Code for Mobile Telephone Number 
Authentication Timeout Settings	If you want the system to use default settings, select Use Default Settings. If you want to set authentication timeout to a value other than the default settings, select Use Manual Settings then fill your preferred values in the fields that follow.

Table 223 Configuration > Object > User/Group > User > Add/Edit_General (continued)

LABEL	DESCRIPTION
Lease Time	If you select Use Default Settings in the Authentication Timeout Settings field, the default lease time is shown. If you select Use Manual Settings, you need to enter the number of minutes this user has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the Renew button on their screen. If you allow access users to renew time automatically (see Section 30.3.6 on page 699), the users can select this checkbox on their screen as well. In this case, the session is automatically renewed before the lease time expires.
Reauthentication Time	If you select Use Default Settings in the Authentication Timeout Settings field, the default reauthentication time is shown. If you select Use Manual Settings, you need to type the number of minutes this user can be logged into the Zyxel Device in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike Lease Time, the user has no opportunity to renew the session without logging out.
User VLAN ID	This field is available for a ext-group-user type user account. Select this option to enable dynamic VLAN assignment on the Zyxel Device. When a user is authenticated successfully, all data traffic from this user is tagged with the VLAN ID number you specify here. This allows you to assign a user of the ext-group-user type to a specific VLAN based on the user credentials instead of using an AAA server.
Configuration Validation	Use a user account from the group specified above to test if the configuration is correct. Enter the account's user name in the User Name field and click Test.
OK	Click OK to save your changes back to the Zyxel Device and close the screen.
Cancel	Click Cancel to exit this screen without saving your changes.
Save	This button is only available when adding a new user. Click Save to save your changes back to the Zyxel Device and then go to the Two-factor Authentication screen.

30.3.4 User Add/Edit Two-factor Authentication Screen

The User Add/Edit Two-factor Authentication screen allows you to create two-factor security for VPN access or admin access for this user to the Zyxel Device.

Two-factor authentication adds an extra layer of security for users logging into the Zyxel Device. When two-factor authentication is enabled, a user has to first enter their username and password, and then click on a temporary link or enter a one-time password when logging in.

You can enable two-factor authentication for users who are logging into the Zyxel Device to create a VPN tunnel (VPN access), and for administrator and limited admin users who are logging into the Web Configurator or CLI (admin access) to configure the Zyxel Device.

Table 224 Two Factor Authentication Methods

ACCESS TYPE	TWO-FACTOR AUTHENTICATION METHODS	FACTOR 2 PASSWORD
VPN	SMS	Code
VPN	Email	Link
VPN	Google Authenticator app	Code
Admin	SMS	Code

Table 224 Two Factor Authentication Methods (continued)

ACCESS TYPE	TWO-FACTOR AUTHENTICATION METHODS	FACTOR 2 PASSWORD
Admin	Email	Link
Admin	Google Authenticator app	Code

You must first enable two-factor authentication on the Zyxel Device in Object > Auth. Method > Two-factor Authentication > VPN Access and Object > Auth. Method > Two-factor Authentication > Admin Access. See Section 30.8.4 on page 738 and Section 30.8.6 on page 743 for more prerequisites and other information.

In Object > User/Group > User, click Add to create a new entry or select an entry and click Edit to modify the entry. You must create a user account first before you can edit the two-factor authentication settings.

You can configure two-factor authentication for non-VPN and non-admin users in web authentication.

Note: The admin two-factor authentication settings override the web authentication two-factor authentication settings.

Figure 454 Configuration > Object > User/Group > User > Add/Edit_Two-factor Authentication

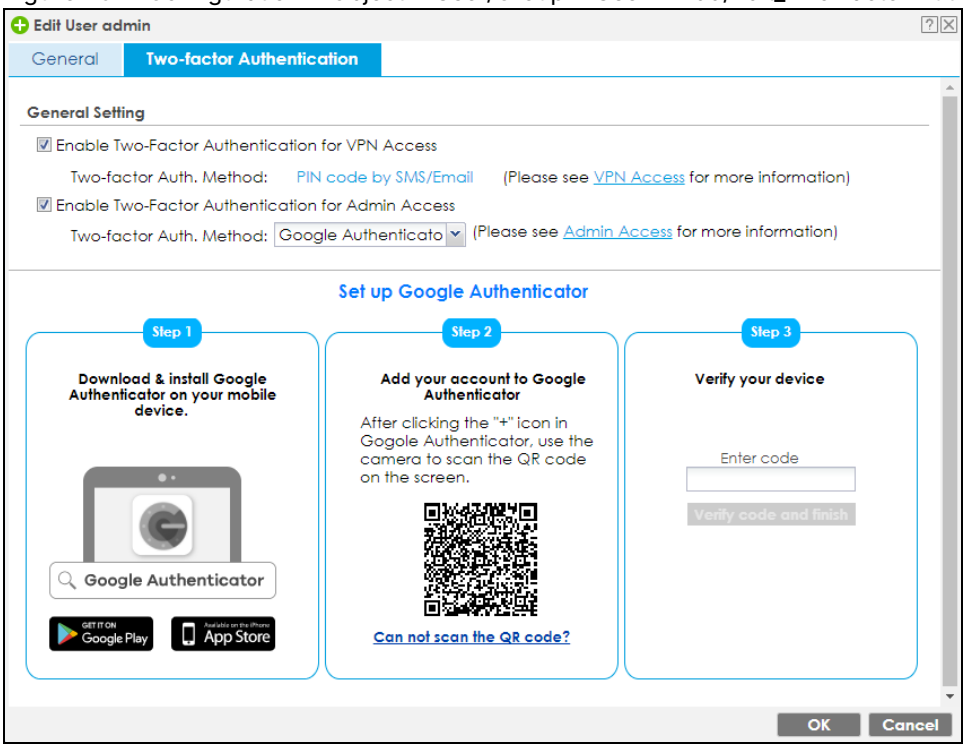
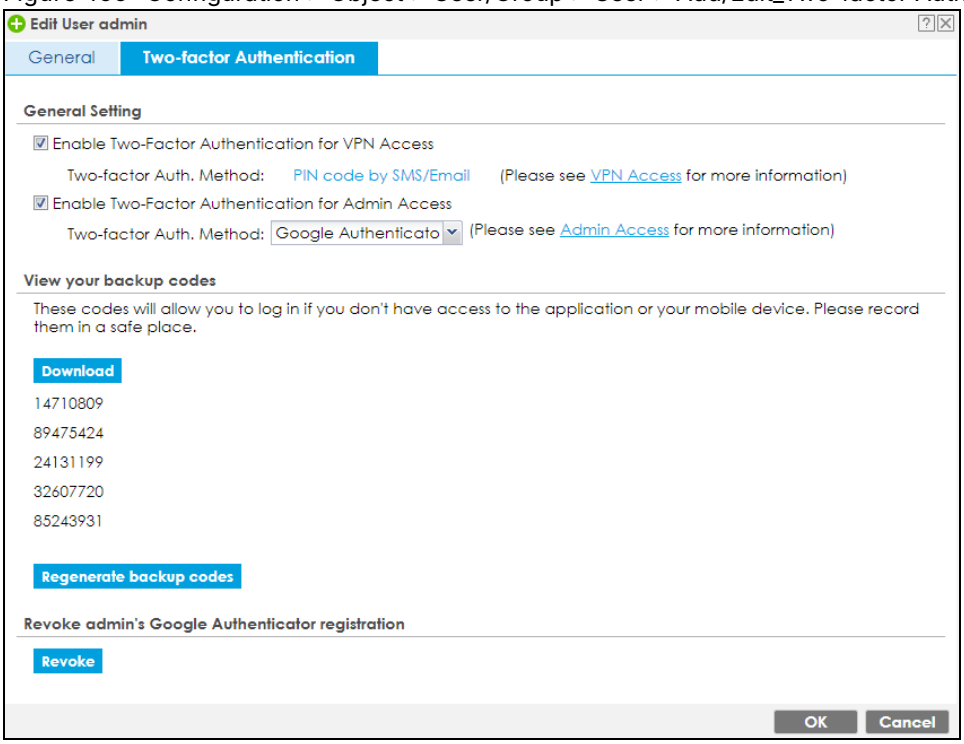


Figure 455 Configuration > Object > User/Group > User > Add/Edit_Two-factor Authentication_Verified



The following table describes the labels in this screen.

Table 225 Configuration > Object > User/Group > User > Add_Two-factor Authentication

LABEL	DESCRIPTION
Enable Two-factor Authentication for VPN Access	Select this to require two-factor authentication for this user to use a pre-configured VPN tunnel for secure access to a network behind the Zyxel Device. Select the types of VPN allowed in Object > Auth. Method > Two-factor Authentication > VPN Access. You may choose from: • SSL VPN Access • IPSec VPN Access • L2TP/IPSec VPN Access
Enable Two-factor Authentication for Admin Access	Select this to require two-factor authentication for an admin user to access the Zyxel Device. Select the types of access allowed in Object > Auth. Method > Two-factor Authentication > Admin Access. You may choose from: • Web • SSH • TELNET
Two-factor Auth. Method	Select Default or User Defined and select from PIN code by SMS/Email or Google Authenticator
Set up Google Authenticator	If you chose Google Authenticator for offline two-factor authentication, on your mobile device, go to an app store to download Google Authenticator. To add your account to Google Authenticator, press the plus (+) icon, select Scan Barcode, then use your mobile device's camera to scan the barcode. Finally enter the verification code you receive on your mobile device in Verify your device.
View your backup codes	You see this after successful Google authentication. In the event that you do not have access to email or your mobile device, click Download to create backup codes as second-factor authentication. Make sure to put them in a safe place.

Table 225 Configuration > Object > User/Group > User > Add_Two-factor Authentication (continued)

LABEL	DESCRIPTION
Verify your device	In the event that you do not have access to email or your mobile device, enter a backup code here as second factor authentication. You can use each code only once. If you generate a new set of backup codes (Regenerate backup codes), the old set become obsolete.
Revoke	Click this to cancel Google authentication as second-factor authentication for Admin Access. You must then use a PIN code by SMS or email as second-factor authentication instead.
OK	Click OK to save your changes back to the Zyxel Device and close the screen.
Cancel	Click Cancel to exit this screen without saving your changes.

30.3.4.1 Google Two-Factor Authentication Setup Example

You can use two-factor authentication through SMS, email or Google Authenticator (more secure). Google Authenticator is more secure as it generates a new code every 30 seconds, and each code expires in 30 seconds.

Two-Factor with Google Authenticator Overview

1 Enable Google Authentication for a User

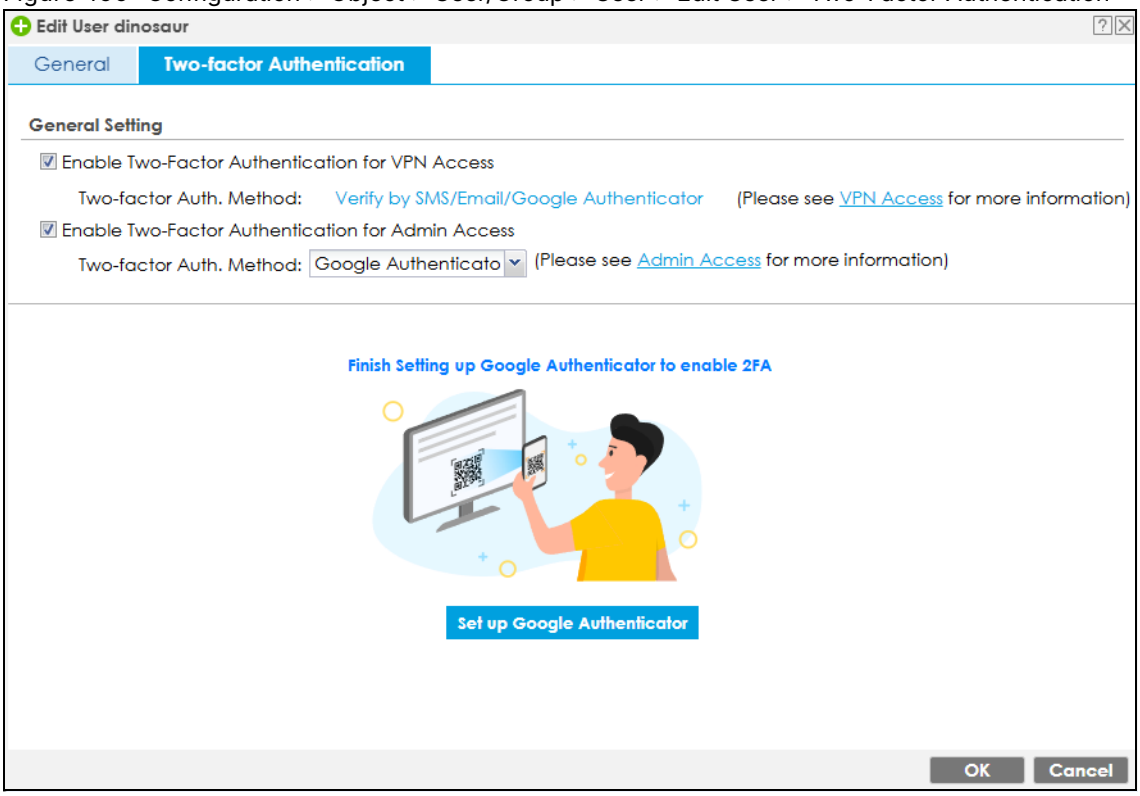
2 Set Up Google Authenticator

3 Configure Two-Factor Authentication for a Remote VPN User

Enable Google Authentication for a User

Go to Configuration > Object > User/Group > User , select a user, and click Edit. The following screen appears. Click Set up Google Authenticator.

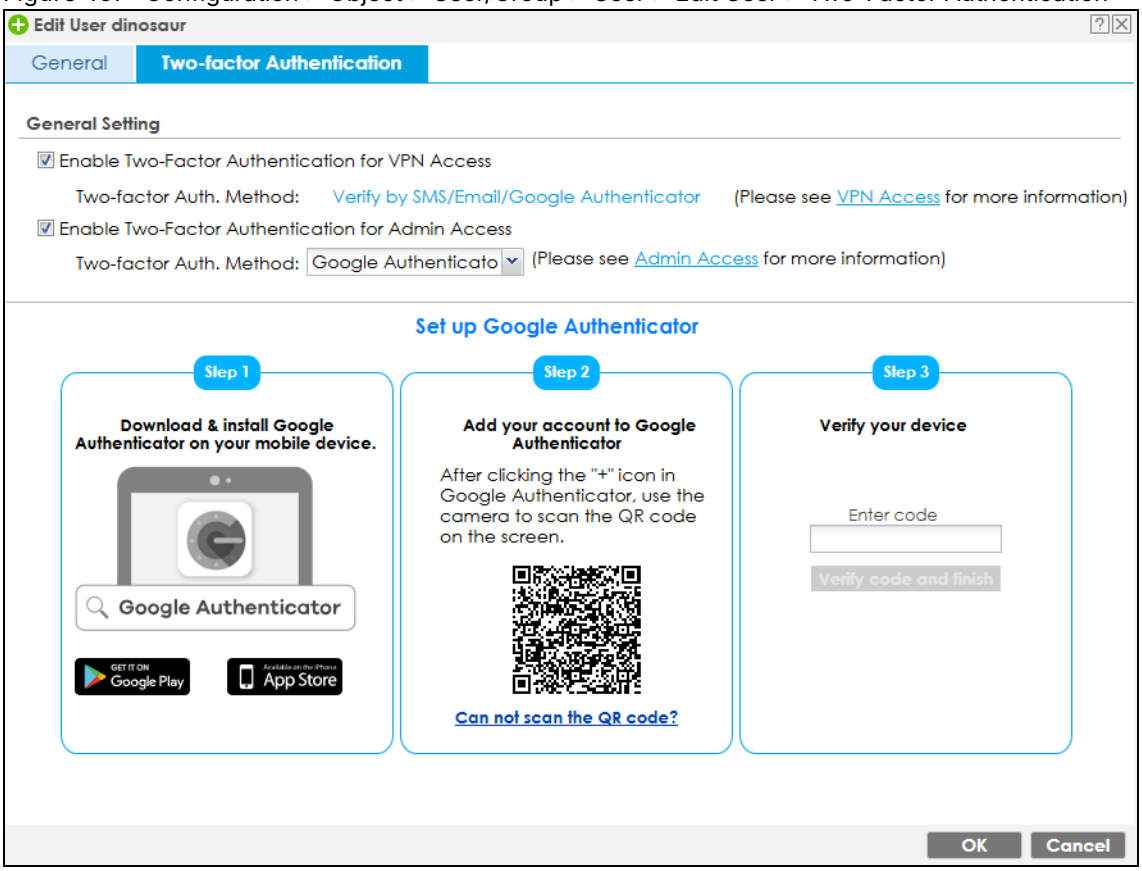
Figure 456 Configuration > Object > User/Group > User > Edit User > Two-Factor Authentication



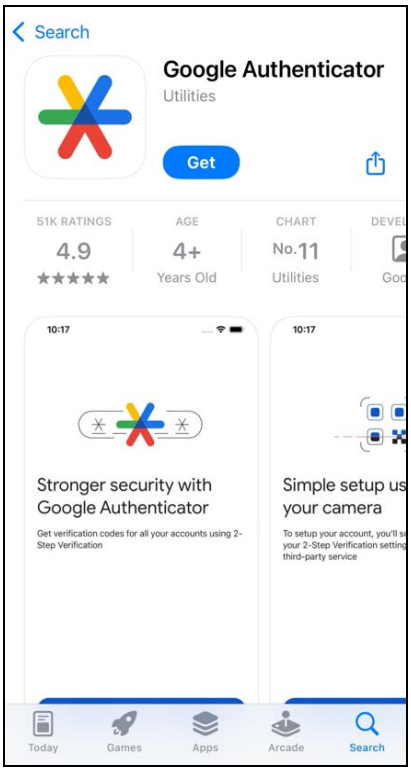
Set Up Google Authenticator

Follow the instructions on the Configuration > Object > User/Group > User > Edit User > Two-Factor Authentication screen to set up Google Authenticator.

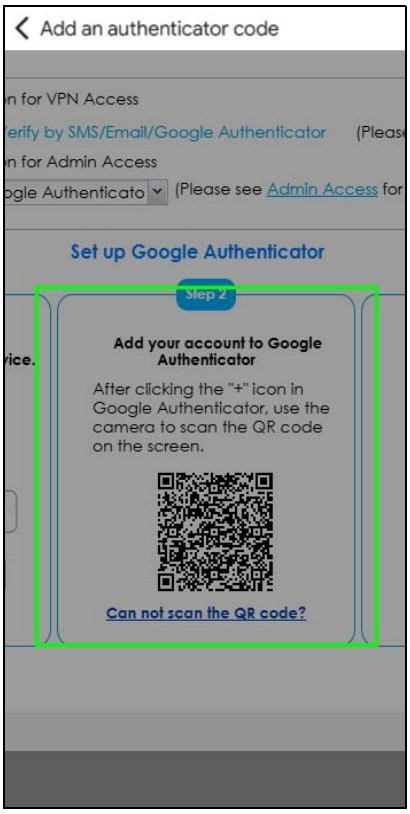
Figure 457 Configuration > Object > User/Group > User > Edit User > Two-Factor Authentication



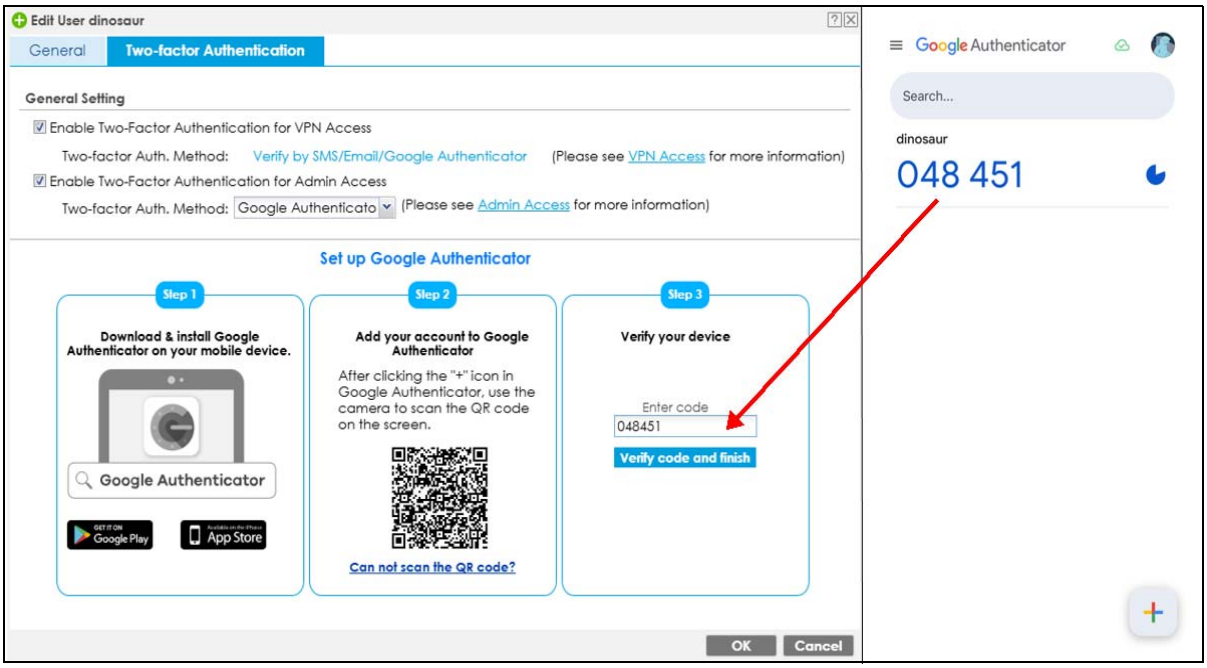
1 Download and install Google Authenticator from Google Play or the App Store on your mobile device.



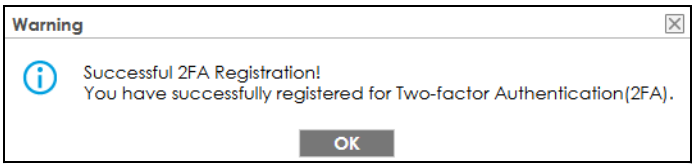
2 Open the Google Authenticator app and scan the QR code on the screen.



3 Enter the code displayed in Google Authenticator from Step 3 in the Web Configurator, then click Verify Code and finish to complete the verification.

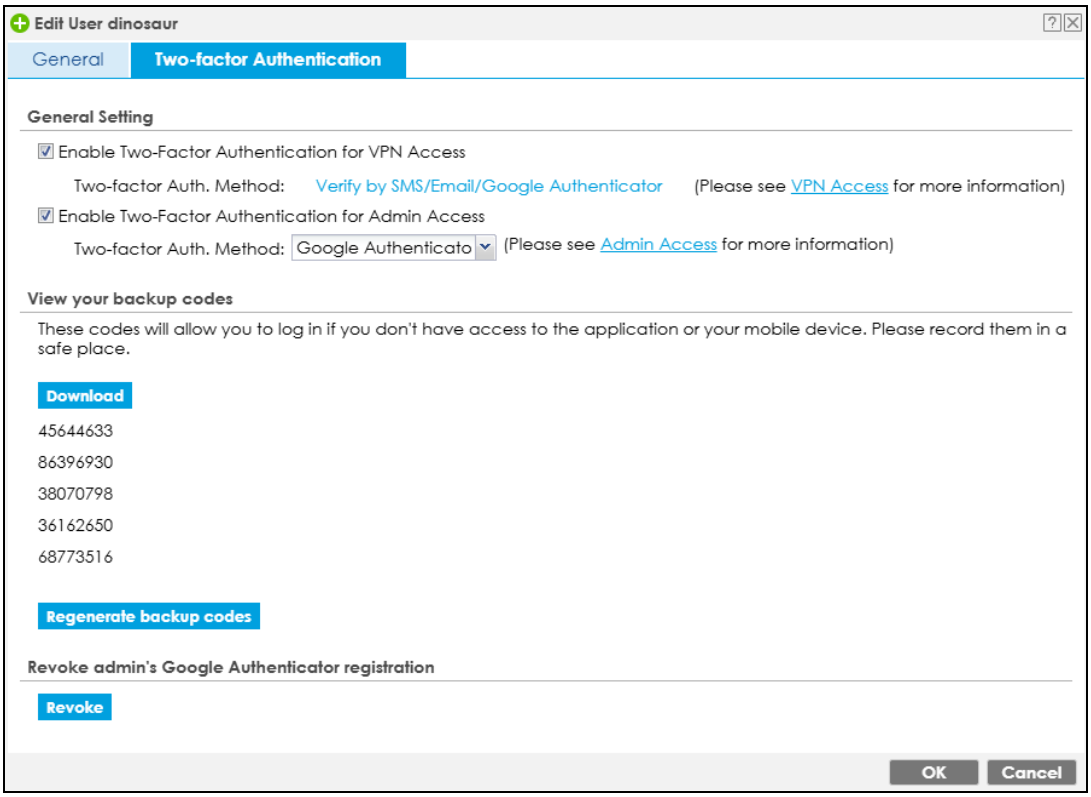


4 If two-factor verification is successful, the following message appears. If it fails, an error message will be displayed. Try again when the next code appears and ensure you enter the correct code within the time limit.



5 After 2FA registration is successfully set up, backup codes will be available in Configuration > Object > User/Group > User > Edit User > Two-Factor Authentication. These codes can be used for device login if you don't have access to the application on your mobile device. Download the backup codes and store them in a safe place.

Note: If you click Regenerate backup codes or revoke the Google Authenticator registration and re-register, the backup codes will change.

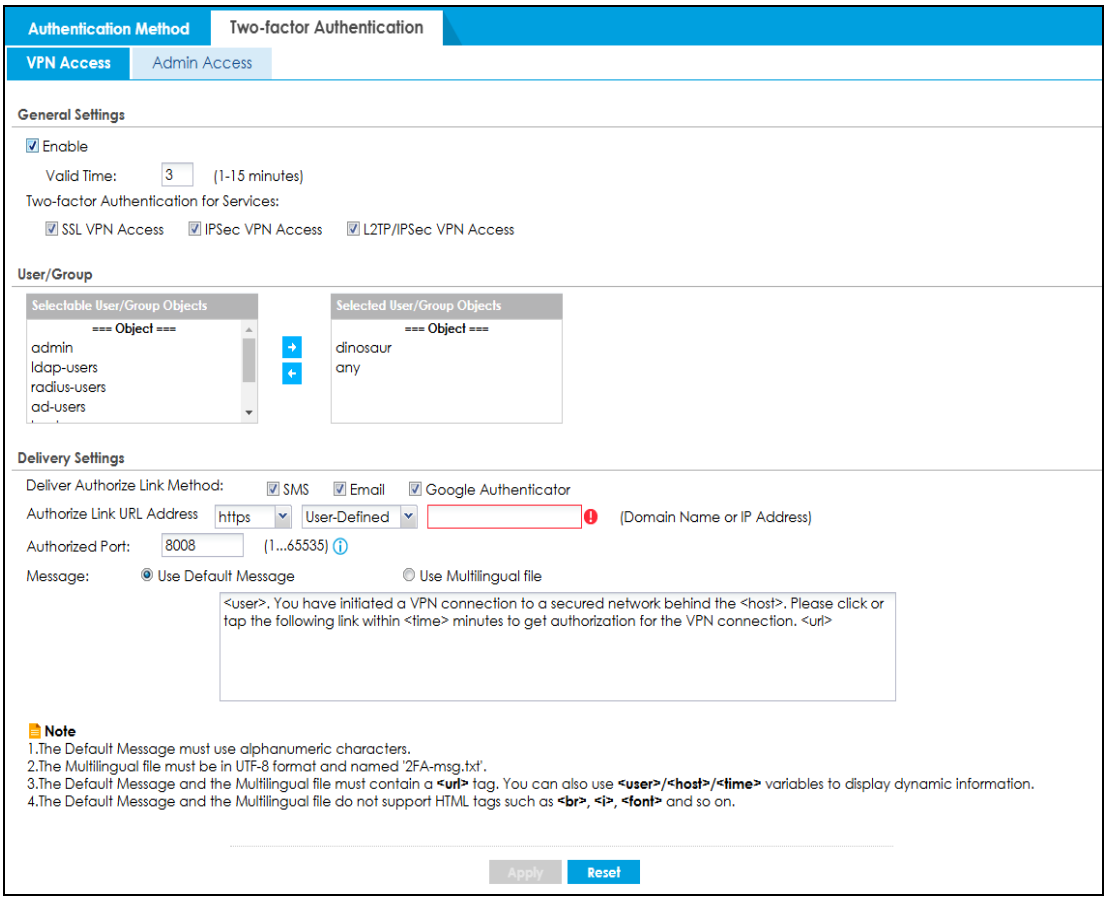


Configure Two-Factor Authentication for a Remote VPN User

Follow these steps to set a valid time and allowed login method for a remote user who connects securely to the network behind the Zyxel Device through a Virtual Private Network (VPN):

1 Go to Configuration > Object > Auth. Method > Two-factor Authentication > VPN Access and configure the following fields:

- Valid time (optional): Enter the maximum time (in minutes) that you must enter the code in Google Authenticator in order to get authorization for the VPN connection.
- Two-factor Authentication for Services: Select which kinds of VPN tunnels require Two-Factor Authentication. You should have configured the VPN tunnel first.
- Deliver Authorize Link Method: Select Google Authenticator. You will receive an authentication code in Google Authenticator. Log in to the Zyxel Device by entering the authentication code from Google Authenticator.
- Authorized Port: Configure a new port between 1024 to 65535 that is not in use by other services. Use this port for two-factor authentication of VPN clients to access the network behind the Zyxel Device. VPN clients do not need to change the port number on their devices, because the link to access the network behind the Zyxel Device will contain the new port number.

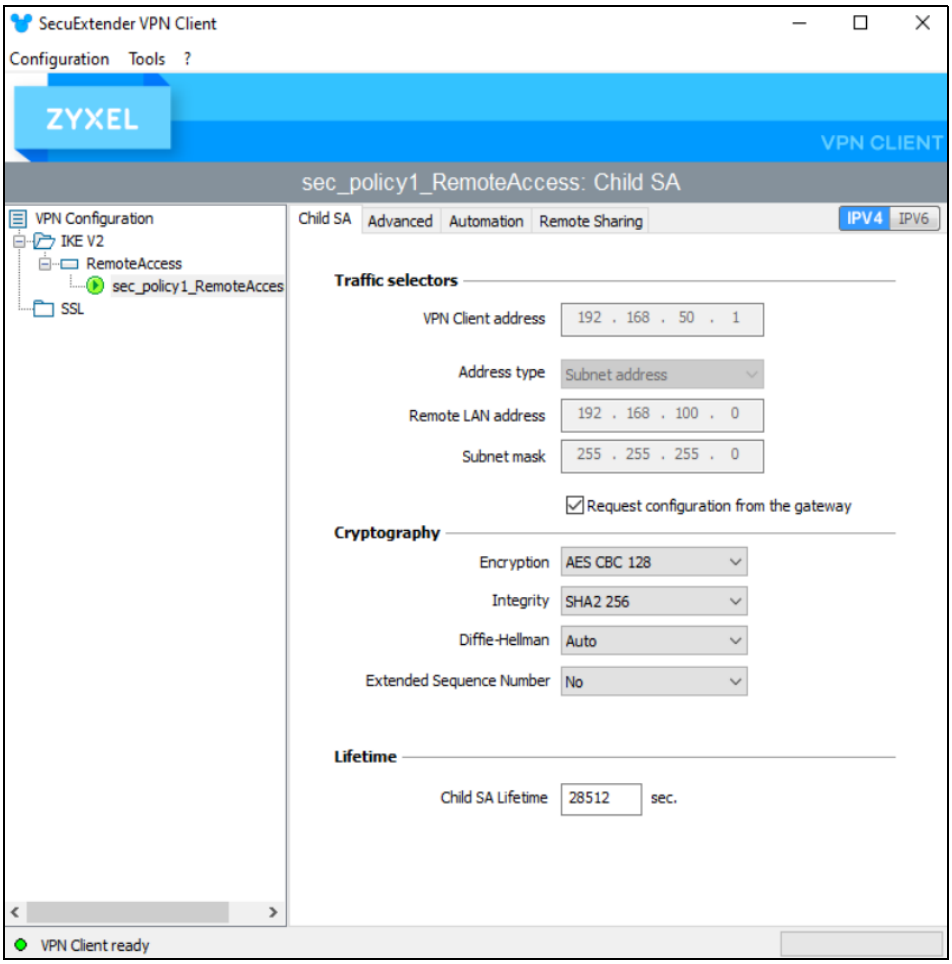


2 Click Apply to save the changes to the Zyxel Device.

Test the Remote VPN Two-Factor Authentication

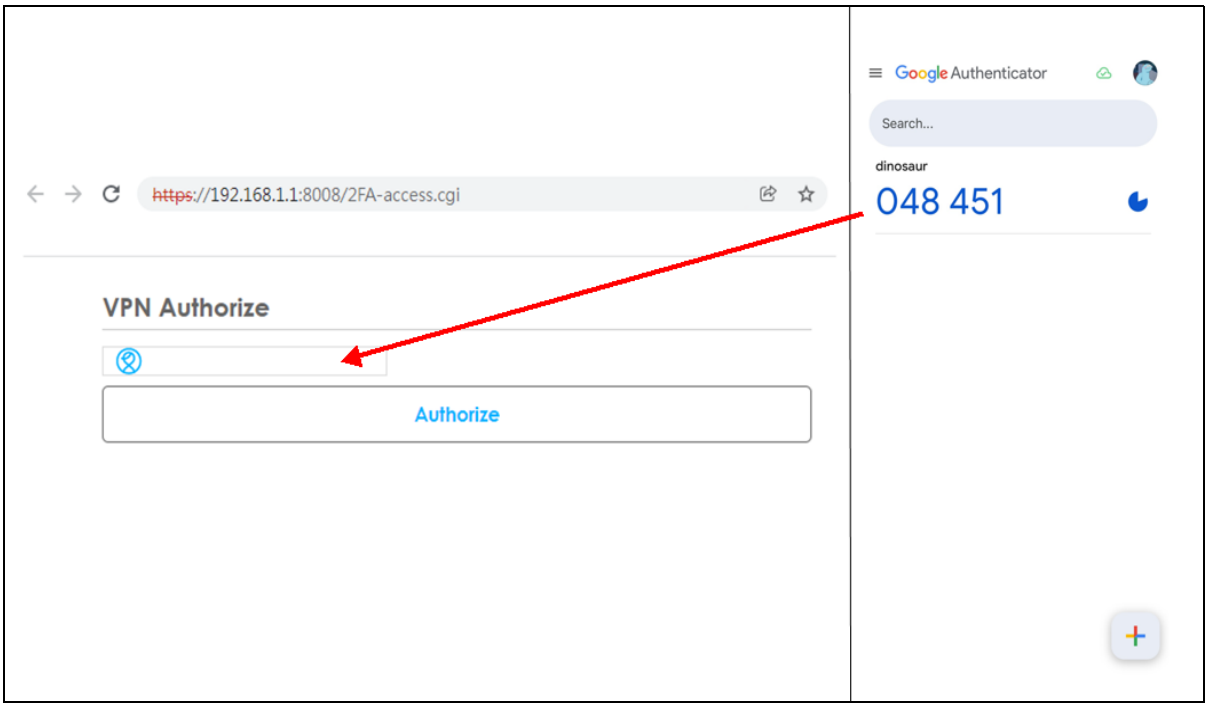
To verify whether the remote VPN user can successfully use two-factor authentication to access the Zyxel Device, follow these steps:

1 The remote user should establish a VPN connection using a VPN client application. See Section 21.2 on page 478 for more information about establishing a VPN connection.



2 The Web Configurator displays the following screen. Enter the code shown in Google Authenticator and click Authorize.

Note: If you don't have a mobile device on hand, you can find a backup code in Configuration > Object > User/Group > User > Edit User > Two-Factor Authentication and enter it.

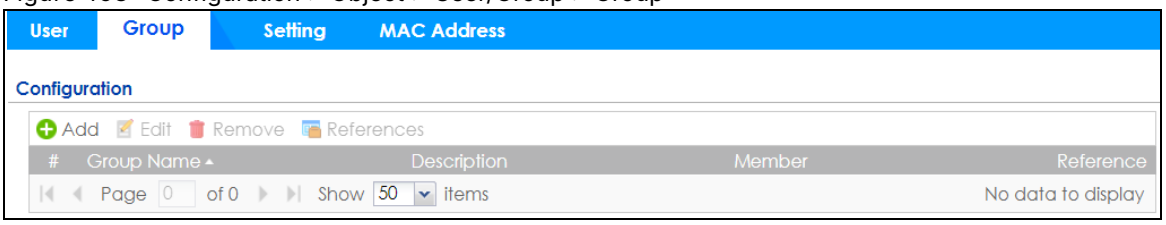


3 The remote VPN user can now access the Zyxel Device.

30.3.5 User/Group Group Summary Screen

User groups consist of access users and other user groups. You cannot put admin users in user groups. The Group screen provides a summary of all user groups. In addition, this screen allows you to add, edit, and remove user groups. To access this screen, login to the Web Configurator, and click Configuration > Object > User/Group > Group.

Figure 458 Configuration > Object > User/Group > Group



The following table describes the labels in this screen. See Section 30.3.5.1 on page 698 for more information as well.

Table 226 Configuration > Object > User/Group > Group

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so. Removing a group does not remove the user accounts in the group.
References	Select an entry and click References to open a screen that shows which settings use the entry.

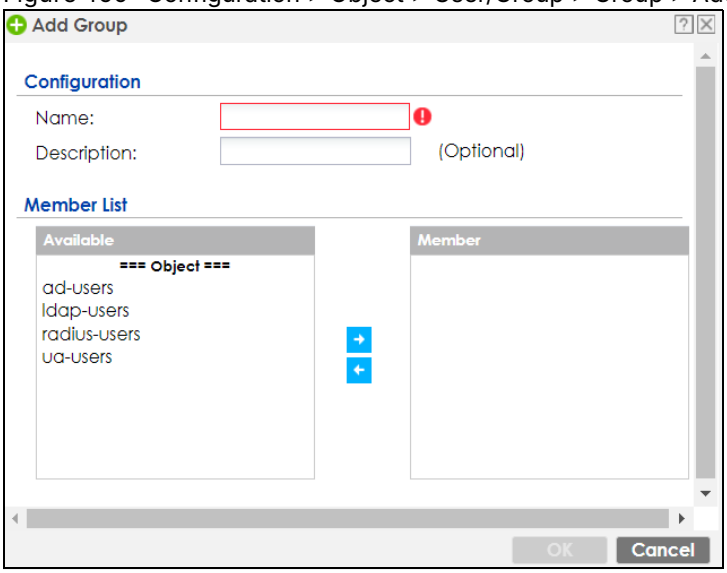
Table 226 Configuration > Object > User/Group > Group (continued)

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific user group.
Group Name	This field displays the name of each user group.
Description	This field displays the description for each user group.
Member	This field lists the members in the user group. Each member is separated by a comma.
Reference	This displays the number of times an object reference is used in a profile.

30.3.5.1 Group Add/Edit Screen

The Group Add/Edit screen allows you to create a new user group or edit an existing one. To access this screen, go to the Group screen (see Section 30.3.5 on page 697), and click either the Add icon or an Edit icon.

Figure 459 Configuration > Object > User/Group > Group > Add



The following table describes the labels in this screen.

Table 227 Configuration > Object > User/Group > Group > Add

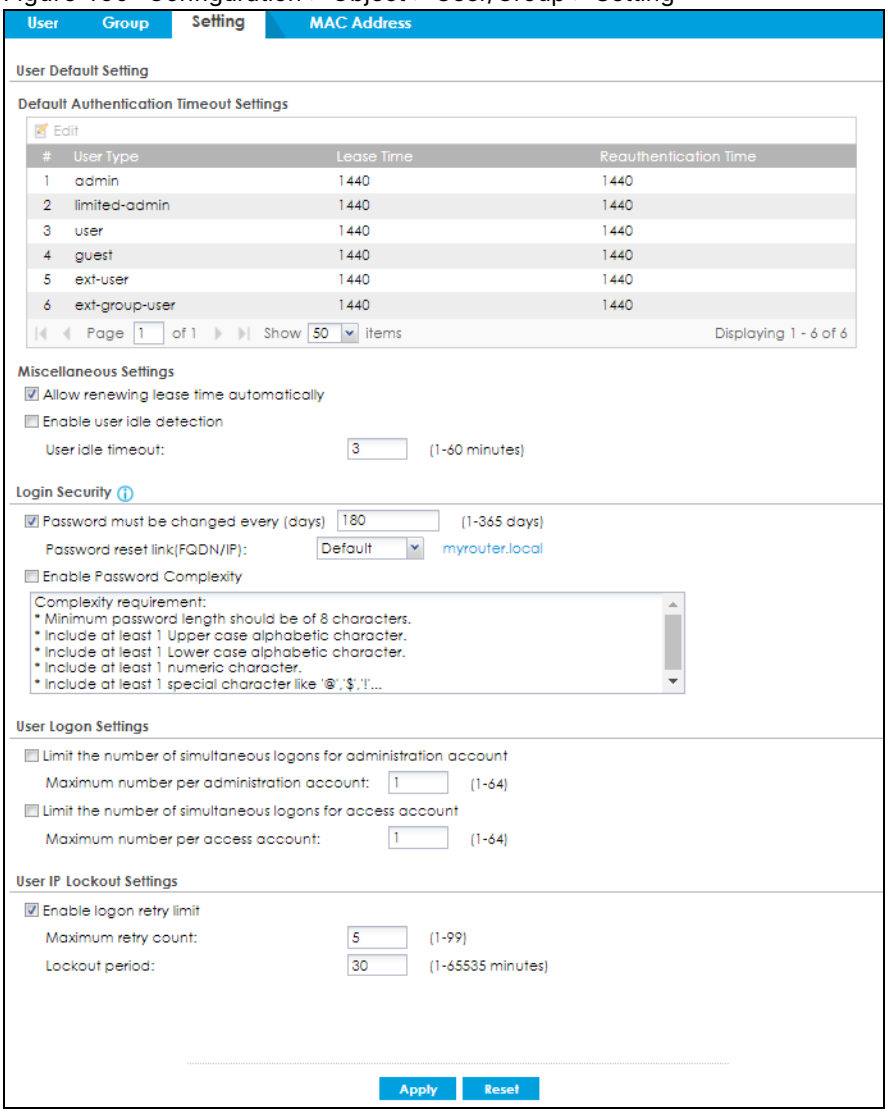
LABEL	DESCRIPTION
Name	Type the name for this user group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User group names have to be different than user names.
Description	Enter the description of the user group, if any. You can use up to 60 characters, punctuation marks, and spaces.
Member List	The Member list displays the names of the users and user groups that have been added to the user group. The order of members is not important. Select users and groups from the Available list that you want to be members of this group and move them to the Member list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Move any members you do not want included to the Available list.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving your changes.

30.3.6 User/Group Setting Screen

The Setting screen controls default settings, login settings, lockout settings, and other user settings for the Zyxel Device. You can also use this screen to specify when users must log in to the Zyxel Device before it routes traffic for them.

To access this screen, login to the Web Configurator, and click Configuration > Object > User/Group > Setting.

Figure 460 Configuration > Object > User/Group > Setting



The following table describes the labels in this screen.

Table 228 Configuration > Object > User/Group > Setting

LABEL	DESCRIPTION
User Authentication Timeout Settings	
Default Authentication Timeout Settings	These authentication timeout settings are used by default when you create a new user account. They also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentication timeout settings.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
#	This field is a sequential value, and it is not associated with a specific entry.
User Type	These are the kinds of user account the Zyxel Device supports. • admin - this user can look at and change the configuration of the Zyxel Device • limited-admin - this user can look at the configuration of the Zyxel Device but not to change it • user - this user has access to the Zyxel Device's services but cannot look at the configuration • guest - this user has access to the Zyxel Device's services but cannot look at the configuration • ext-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 679 for more information about this type. • ext-group-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 680 for more information about this type.
Lease Time	This is the default lease time in minutes for each type of user account. It defines the number of minutes the user has to renew the current session before the user is logged out. Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the Renew button on their screen. If you allow access users to renew time automatically (see Section 30.3.6 on page 699), the users can select this checkbox on their screen as well. In this case, the session is automatically renewed before the lease time expires.
Reauthentication Time	This is the default reauthentication time in minutes for each type of user account. It defines the number of minutes the user can be logged into the Zyxel Device in one session before having to log in again. Unlike Lease Time, the user has no opportunity to renew the session without logging out.
Miscellaneous Settings	
Allow renewing lease time automatically	Select this checkbox if access users can renew lease time automatically, as well as manually, simply by selecting the Updating lease time automatically checkbox on their screen.
Enable user idle detection	This is applicable for access users. Select this checkbox if you want the Zyxel Device to monitor how long each access user is logged in and idle (in other words, there is no traffic for this access user). The Zyxel Device automatically logs out the access user once the User idle timeout has been reached.
User idle timeout	This is applicable for access users. This field is effective when Enable user idle detection is checked. Type the number of minutes each access user can be logged in and idle before the Zyxel Device automatically logs out the access user.
Login Security	
Password must changed every (days):	Enter how often local users of User Type 'admin' must change their login passwords. You can choose from once a day to once a year.

Table 228 Configuration > Object > User/Group > Setting (continued)

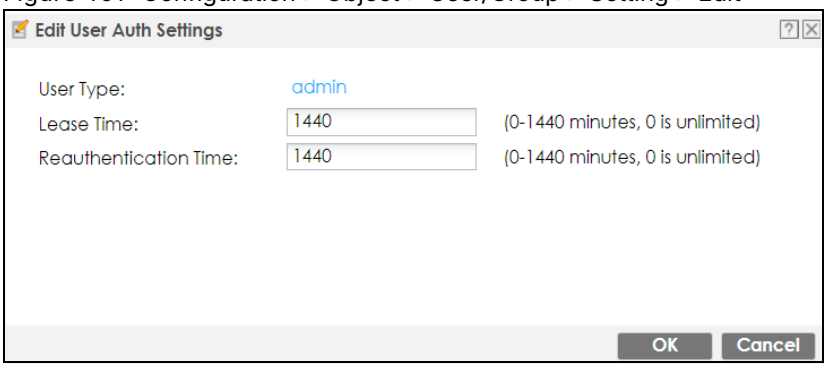
LABEL	DESCRIPTION
Password reset link (FQDN/IP):	Associate the password expiration to a specific Zyxel Device. Default is this Zyxel Device (myrouter) or select Custom and enter the IP address or Fully Qualified Domain Name (FQDN).
Enable Password Complexity	Select this to enforce the following conditions in a user password. Requiring a strong password is good for security. The conditions are that the password must consist of at least 8 characters and at most 64. 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 !@#$%^&*()_+.
User Logon Settings	
Limit the number of simultaneous logons for administration account	Select this checkbox if you want to set a limit on the number of simultaneous logins by admin users. If you do not select this, admin users can login as many times as they want at the same time using the same or different IP addresses.
Maximum number per administration account	This field is effective when Limit ... for administration account is checked. Type the maximum number of simultaneous logins by each admin user.
Limit the number of simultaneous logons for access account	Select this checkbox if you want to set a limit on the number of simultaneous logins by non-admin users. If you do not select this, access users can login as many times as they want as long as they use different IP addresses.
Maximum number per access account	This field is effective when Limit ... for access account is checked. Type the maximum number of simultaneous logins by each access user.
User IP Lockout Settings	
Enable logon retry limit	Select this checkbox to set a limit on the number of times each user can login unsuccessfully (for example, wrong password) before the IP address is locked out for a specified amount of time.
Maximum retry count	This field is effective when Enable logon retry limit is checked. Type the maximum number of times each user can login unsuccessfully before the IP address is locked out for the specified lockout period. The number must be between 1 and 99.
Lockout period	This field is effective when Enable logon retry limit is checked. Type the number of minutes the user must wait to try to login again, if logon retry limit is enabled and the maximum retry count is reached. This number must be between 1 and 65,535 (about 45.5 days).
Apply	Click Apply to save the changes.
Reset	Click Reset to return the screen to its last-saved settings.

30.3.6.1 Default User Authentication Timeout Settings Edit Screens

The Default Authentication Timeout Settings Edit screen allows you to set the default authentication timeout settings for the selected type of user account. These default authentication timeout settings also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentication timeout settings.

To access this screen, go to the Configuration > Object > User/Group > Setting screen (see Section 30.3.6 on page 699), and click one of the Default Authentication Timeout Settings section's Edit icons.

Figure 461 Configuration > Object > User/Group > Setting > Edit



The following table describes the labels in this screen.

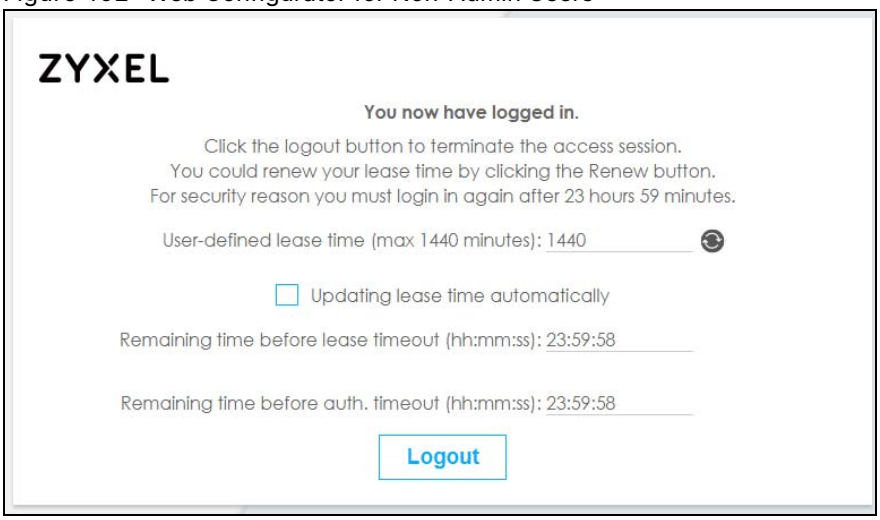
Table 229 Configuration > Object > User/Group > Setting > Edit

LABEL	DESCRIPTION
User Type	This read-only field identifies the type of user account for which you are configuring the default settings. • admin - this user can look at and change the configuration of the Zyxel Device • limited-admin - this user can look at the configuration of the Zyxel Device but not to change it. • dynamic-guest - this user has access to the Zyxel Device's services but cannot look at the configuration. • user - this user has access to the Zyxel Device's services but cannot look at the configuration. • guest - this user has access to the Zyxel Device's services but cannot look at the configuration. • ext-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 679 for more information about this type. • ext-group-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 680 for more information about this type. • guest-manager - this user can log in through the web configurator login screen and create dynamic guest accounts using the Account Generator screen that pops up.
Lease Time	Enter the number of minutes this type of user account has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the Renew button on their screen. If you allow access users to renew time automatically (see Section 30.3.6 on page 699), the users can select this checkbox on their screen as well. In this case, the session is automatically renewed before the lease time expires.
Reauthentication Time	Type the number of minutes this type of user account can be logged into the Zyxel Device in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike Lease Time, the user has no opportunity to renew the session without logging out.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving your changes.

30.3.6.2 User Aware Login Example

Access users cannot use the Web Configurator to browse the configuration of the Zyxel Device. Instead, after access users log into the Zyxel Device, the following screen appears.

Figure 462 Web Configurator for Non-Admin Users



The following table describes the labels in this screen.

Table 230 Web Configurator for Non-Admin Users

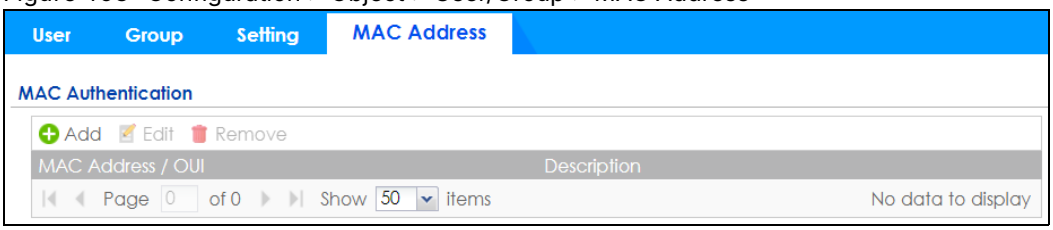
LABEL	DESCRIPTION
User-defined lease time (max ... minutes)	Access users can specify a lease time shorter than or equal to the one that you specified. The default value is the lease time that you specified.
Renew	Access users can click this button to reset the lease time, the amount of time remaining before the Zyxel Device automatically logs them out. The Zyxel Device sets this amount of time according to the: • User-defined lease time field in this screen • Lease time field in the User Add/Edit screen (see Section 30.3.3 on page 682) • Lease time field in the Setting screen (see Section 30.3.6 on page 699).
Updating lease time automatically	This box appears if you checked the Allow renewing lease time automatically box in the Setting screen. (See Section 30.3.6 on page 699.) Access users can select this checkbox to reset the lease time automatically 30 seconds before it expires. Otherwise, access users have to click the Renew button to reset the lease time.
Remaining time before lease timeout	This field displays the amount of lease time that remains, though the user might be able to reset it.
Remaining time before auth. timeout	This field displays the amount of time that remains before the Zyxel Device automatically logs the access user out, regardless of the lease time.

30.3.7 User/Group MAC Address Summary Screen

This screen shows the MAC addresses of wireless clients, which can be authenticated by their MAC addresses using the local user database. Click Configuration > Object > User/Group > MAC Address to open this screen.

Note: You need to configure an SSID security profile's MAC authentication settings to have the AP use the Zyxel Device's local database to authenticate wireless clients by their MAC addresses.

Figure 463 Configuration > Object > User/Group > MAC Address



The following table describes the labels in this screen.

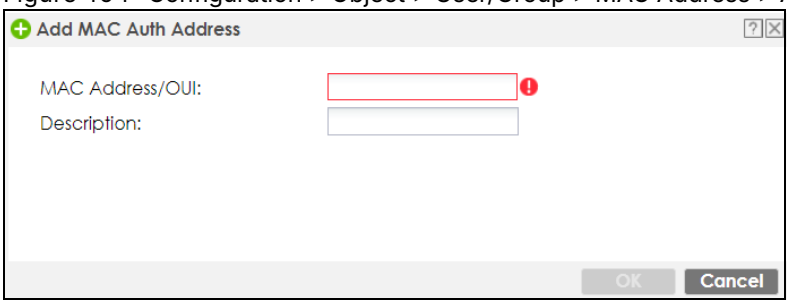
Table 231 Configuration > Object > User/Group > MAC Address

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
MAC Address/ OUI	This field displays the MAC address or OUI (Organizationally Unique Identifier of computer hardware manufacturers) of wireless clients using MAC authentication with the Zyxel Device local user database.
Description	This field displays a description of the device identified by the MAC address or OUI.

30.3.7.1 MAC Address Add/Edit Screen

This screen allows you to create a new allowed device or edit an existing one. To access this screen, go to the MAC Address screen (see Section 30.3.7 on page 703), and click either the Add icon or an Edit icon.

Figure 464 Configuration > Object > User/Group > MAC Address > Add



The following table describes the labels in this screen.

Table 232 Configuration > Object > User/Group > MAC Address > Add

LABEL	DESCRIPTION
MAC Address/ OUI	Type the MAC address (six hexadecimal number pairs separated by colons or hyphens) or OUI (three hexadecimal number pairs separated by colons or hyphens) to identify specific wireless clients for MAC authentication using the Zyxel Device local user database. The OUI is the first three octets in a MAC address and uniquely identifies the manufacturer of a network device.
Description	Enter an optional description of the wireless device(s) identified by the MAC or OUI. You can use up to 60 characters, punctuation marks, and spaces.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving your changes.

30.3.8 User /Group Technical Reference

This section provides some information on users who use an external authentication server in order to log in.

Setting up User Attributes in an External Server

To set up user attributes, such as reauthentication time, in LDAP or RADIUS servers, use the following keywords in the user configuration file.

Table 233 LDAP/RADIUS: Keywords for User Attributes

KEYWORD	CORRESPONDING ATTRIBUTE IN WEB CONFIGURATOR
type	User Type. Possible Values: admin, limited-admin, dynamic-guest, user, guest.
leaseTime	Lease Time. Possible Values: 1-1440 (minutes).
reauthTime	Reauthentication Time. Possible Values: 1-1440 (minutes).

The following examples show you how you might set up user attributes in LDAP and RADIUS servers.

Figure 465 LDAP Example: Keywords for User Attributes

```
type: admin
leaseTime: 99
reauthTime: 199
```

Figure 466 RADIUS Example: Keywords for User Attributes

```
type=user;leaseTime=222;reauthTime=222
```

Creating a Large Number of Ext-User Accounts

If you plan to create a large number of Ext-User accounts, you might use CLI commands, instead of the Web Configurator, to create the accounts. Extract the user names from the LDAP or RADIUS server, and create a shell script that creates the user accounts.

Built-in System Accounts

The following built-in system accounts are disabled by default.

Table 234 Built-in System Accounts

ACCOUNT NAME	ACTIVATION	PURPOSE	SUPPORTED MODELS	USER NAME / PASSWORD
debug	The Zyxel Device owner must create an account with admin privileges to allow access to the Zyxel Device using CLI remotely (Telnet or SSH). The debug account cannot be used to log into the Zyxel Device using WWW or FTP.	RD can use this account to collect information for troubleshooting.	ZyWALL ATP, USG Flex (On-Premise / On-Cloud mode), VPN (standalone and Nebula Orchestrator managed)	debug / Authentication Phrase The Authentication Phrase is generated internally in Zyxel. It must be used within 10 minutes of being generated. Each generated Authentication Phrase can be used just once.
devicehaecived	This account is activated when Device HA is enabled. This account cannot be used to log into the Zyxel Device using WWW, SSH, or FTP.	The Zyxel Device can use this account to synchronize configuration, firmware and licenses on a backup Device HA Zyxel Device.	ZyWALL ATP, USG Flex (On-Premise mode), and VPN models that support Device HA.	devicehaecived / Zyxel Device HA Pro Password The Device HA password is configured in the Web Configurator (Configuration > Device HA> Device HA Pro > Password) or CLI (`device-ha2 sync password <password>`).
support	This account is activated when you configure a Zyxel Device from factory default using Nebula Cloud Center ZTP.	An administrator can use this account to access a managed Zyxel Device using WWW, SSH or FTP for troubleshooting.	ZyWALL USG Flex (On-Cloud mode)	support / Zyxel Device serial number The default password (serial number) is automatically changed when the Zyxel Device is managed by Nebula Control Center (NCC). You can change the password using NCC.
sdwan	This account is activated when the Zyxel Device is managed by Nebula Orchestrator.	An administrator can use this account to access a managed Zyxel Device using WWW, SSH or FTP for troubleshooting.	ZyWALL VPN (Nebula Orchestrator managed)	sdwan / Zyxel Device serial number You can change the password using Nebula Orchestrator.

30.4 Address/Geo IP Overview

Address objects can represent a single IP address or a range of IP addresses. Address groups are composed of address objects and other address groups.

- The Address screen (Section 30.4.2 on page 707) provides a summary of all addresses in the Zyxel Device. Use the Address Add/Edit screen to create a new address or edit an existing one.
- Use the Address Group summary screen (Section 30.4.3 on page 711) and the Address Group Add/Edit screen, to maintain address groups in the Zyxel Device.
- Use the Geo IP screen (Section 30.4.4 on page 713) to update the database of country-to-IP address mappings and to manually configure country-to-IP address mappings.

30.4.1 What You Need To Know

Address objects and address groups are used in dynamic routes, security policies, content filtering, and VPN connection policies. For example, addresses are used to specify where content restrictions apply in

content filtering. Please see the respective sections for more information about how address objects and address groups are used in each one.

Address groups are composed of address objects and address groups. The sequence of members in the address group is not important.

30.4.2 Address Summary Screen

The address screens are used to create, maintain, and remove addresses. There are the types of address objects:

- HOST - the object uses an IP Address to define a host address
- RANGE - the object uses a range address defined by a Starting IP Address and an Ending IP Address
- SUBNET - the object uses a network address defined by a Network IP address and Netmask subnet mask
- INTERFACE IP - the object uses the IP address of one of the Zyxel Device's interfaces
- INTERFACE SUBNET - the object uses the subnet mask of one of the Zyxel Device's interfaces
- INTERFACE GATEWAY - the object uses the gateway IP address of one of the Zyxel Device's interfaces
- GEOGRAPHY - the object uses the IP addresses of a country to represent a country

FQDN - the object uses a FQDN (Fully Qualified Domain Name). An FQDN consists of a host and domain name. For example, www.zyxel.com is a fully qualified domain name, where "www" is the host, "zyxel" is the second-level domain, and "com" is the top level domain. mail.myZyxel.com.tw is also an FQDN, where "mail" is the host, "myZyxel" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain.

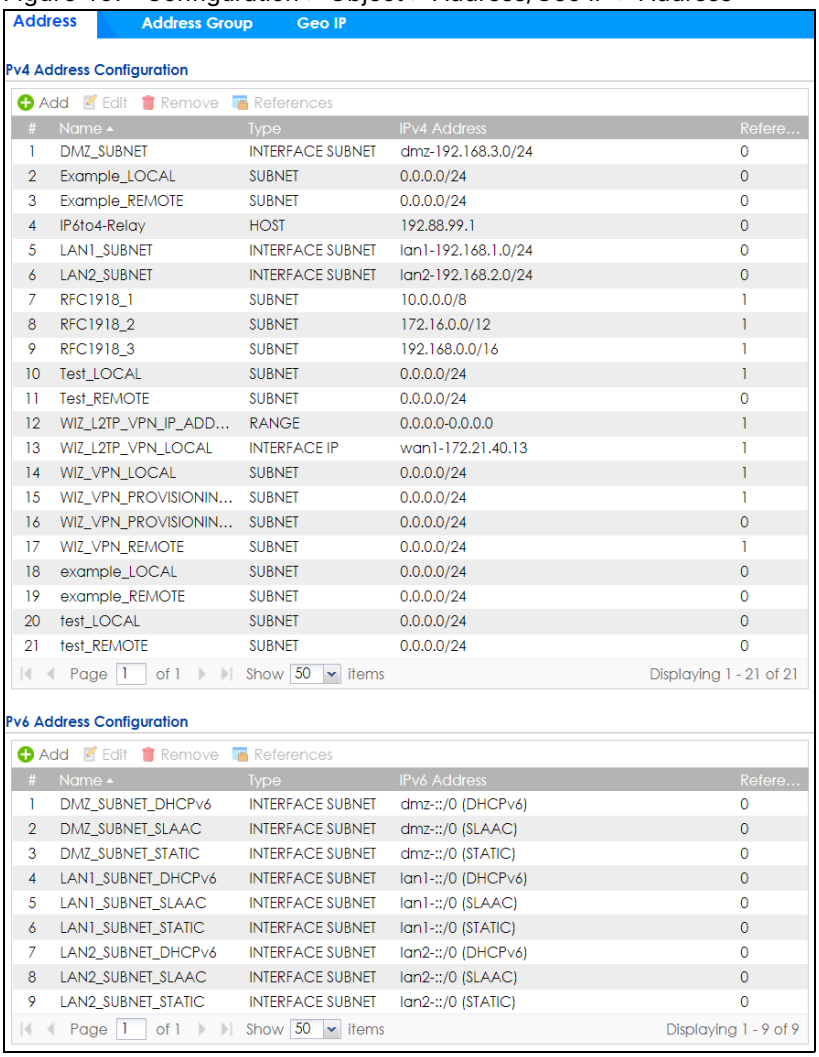
Table 235 FQDN Example

HTTP://	WWW.	ZYXEL.	COM
	host name	second-level domain name	top-level domain name
	FQDN		
Uniform Resource Locator (URL)			

In an address FQDN object, you can also use one wildcard. For example, *.zyxel.com. An FQDN is resolved to its IP address using the DNS server configured on the Zyxel Device.

The Address screen provides a summary of all addresses in the Zyxel Device. To access this screen, click Configuration > Object > Address > Address. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 467 Configuration > Object > Address/Geo IP > Address



The following table describes the labels in this screen. See Section 30.4.2.1 on page 709 for more information as well.

Table 236 Configuration > Object > Address/Geo IP > Address

LABEL	DESCRIPTION
IPv4 Address Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific address.
Name	This field displays the configured name of each address object.
Type	This field displays the type of each address object. "INTERFACE" means the object uses the settings of one of the Zyxel Device's interfaces.
IPv4 Address	This field displays the IPv4 addresses represented by each address object. If the object's settings are based on one of the Zyxel Device's interfaces, the name of the interface displays first followed by the object's current address settings.

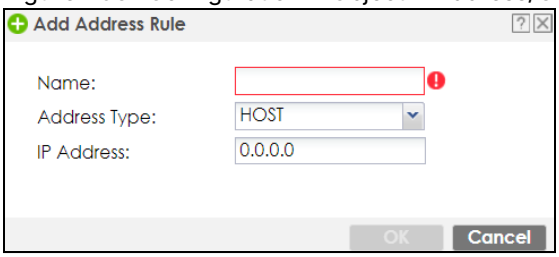
Table 236 Configuration > Object > Address/Geo IP > Address (continued)

LABEL	DESCRIPTION
Reference	This displays the number of times an object reference is used in a profile.
IPv6 Address Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific address.
Name	This field displays the configured name of each address object.
Type	This field displays the type of each address object. "INTERFACE" means the object uses the settings of one of the Zyxel Device's interfaces.
IPv6 Address	This field displays the IPv6 addresses represented by each address object. If the object's settings are based on one of the Zyxel Device's interfaces, the name of the interface displays first followed by the object's current address settings.
Reference	This displays the number of times an object reference is used in a profile.

30.4.2.1 IPv4 Address Add/Edit Screen

The Configuration > Object > Address/GeoIP > Address > Add/Edit (IPv4) screen allows you to create a new address or edit an existing one. To access this screen, go to the Address screen (see Section 30.4.2 on page 707), and click either the Add icon or an Edit icon in the IPv4 Address Configuration section.

Figure 468 Configuration > Object > Address/GeoIP > Address > Add/Edit (IPv4)



The following table describes the labels in this screen.

Table 237 Configuration > Object > Address/GeoIP > Address > Add/Edit (IPv4)

LABEL	DESCRIPTION
Name	Type the name used to refer to the address. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Address Type	Select the type of address you want to create. Note: The Zyxel Device automatically updates address objects that are based on an interface's IP address, subnet, or gateway if the interface's IP address settings change. For example, if you change 1's IP address, the Zyxel Device automatically updates the corresponding interface-based, LAN subnet address object.
IP Address	This field is only available if the Address Type is HOST. This field cannot be blank. Enter the IP address that this address object represents.
Starting IP Address	This field is only available if the Address Type is RANGE. This field cannot be blank. Enter the beginning of the range of IP addresses that this address object represents.

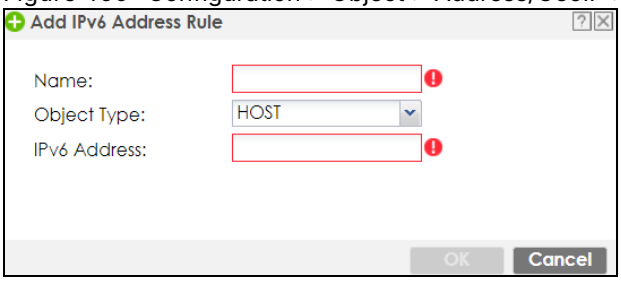
Table 237 Configuration > Object > Address/GeoIP > Address > Add/Edit (IPv4)

LABEL	DESCRIPTION
Ending IP Address	This field is only available if the Address Type is RANGE. This field cannot be blank. Enter the end of the range of IP address that this address object represents.
Network	This field is only available if the Address Type is SUBNET, in which case this field cannot be blank. Enter the IP address of the network that this address object represents.
Netmask	This field is only available if the Address Type is SUBNET, in which case this field cannot be blank. Enter the subnet mask of the network that this address object represents. Use dotted decimal format.
Interface	If you selected INTERFACE IP, INTERFACE SUBNET, or INTERFACE GATEWAY as the Address Type, use this field to select the interface of the network that this address object represents.
Region	If you selected GEOGRAPHY as the Address Type, use this field to select a country or continent. A GEOGRAPHY object uses the data from the country-to-IP/continent-to-IP address database. Go to the Configuration > Object > Address/Geo IP > Geo IP screen to configure the custom country-to-IP/continent-to-IP address mappings for a GEOGRAPHY object.
Country	If you selected Geography as the Address Type, use this field to select a country.
FQDN	If you selected FQDN as the Address Type, use this field to enter a fully qualified domain name.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving your changes.

30.4.2.2 IPv6 Address Add/Edit Screen

The Configuration > Object > Address/GeoIP > Address > Add/Edit (IPv6) screen allows you to create a new address or edit an existing one. To access this screen, go to the Address screen (see Section 30.4.2 on page 707), and click either the Add icon or an Edit icon in the IPv6 Address Configuration section.

Figure 469 Configuration > Object > Address/GeoIP > Address > Add/Edit (IPv6)



The following table describes the labels in this screen.

Table 238 Configuration > Object > Address/GeoIP > Address > Add/Edit (IPv6)

LABEL	DESCRIPTION
Name	Type the name used to refer to the address. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Object Type	Select the type of address you want to create. Note: The Zyxel Device automatically updates address objects that are based on an interface's IP address, subnet, or gateway if the interface's IP address settings change. For example, if you change 1's IP address, the Zyxel Device automatically updates the corresponding interface-based, LAN subnet address object.
IPv6 Address	This field is only available if the Address Type is HOST. This field cannot be blank. Enter the IP address that this address object represents.

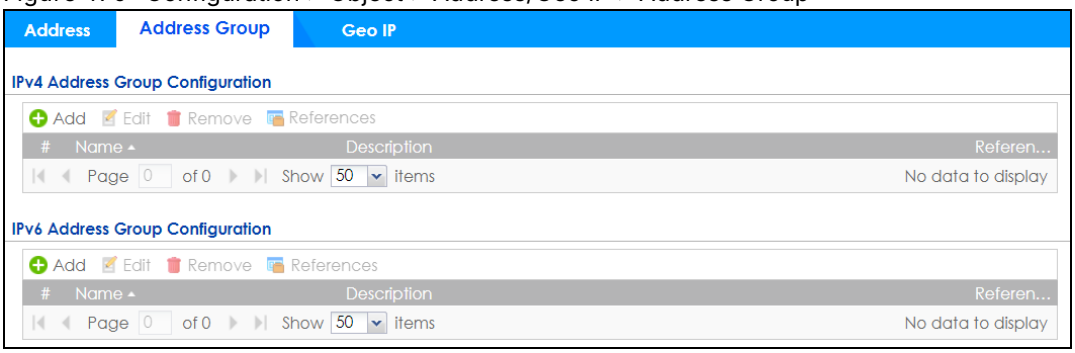
Table 238 Configuration > Object > Address/GeoIP > Address > Add/Edit (IPv6)

LABEL	DESCRIPTION
IPv6 Starting Address	This field is only available if the Address Type is RANGE. This field cannot be blank. Enter the beginning of the range of IP addresses that this address object represents.
IPv6 Ending Address	This field is only available if the Address Type is RANGE. This field cannot be blank. Enter the end of the range of IP address that this address object represents.
IPv6 Address Prefix	This field is only available if the Address Type is SUBNET. This field cannot be blank. Enter the IPv6 address prefix that the Zyxel Device uses for the LAN IPv6 address.
Interface	If you selected INTERFACE IP, INTERFACE SUBNET, or INTERFACE GATEWAY as the Address Type, use this field to select the interface of the network that this address object represents.
IPv6 Address Type	Select whether the IPv6 address is a link-local IP address (LINK LOCAL), static IP address (STATIC), an IPv6 StateLess Address Auto Configuration IP address (SLAAC), or is obtained from a DHCPv6 server (DHCPv6).
Region	If you selected Geography as the Address Type, use this field to select a country or continent.
FQDN	If you selected FQDN as the Address Type, use this field to enter a fully qualified domain name.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving your changes.

30.4.3 Address Group Summary Screen

The Address Group screen provides a summary of all address groups. To access this screen, click Configuration > Object > Address/Geo IP > Address Group. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 470 Configuration > Object > Address/Geo IP > Address Group



The following table describes the labels in this screen. See Section 30.4.3.1 on page 712 for more information as well.

Table 239 Configuration > Object > Address/Geo IP > Address Group

LABEL	DESCRIPTION
IPv4 Address Group Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific address group.
Name	This field displays the name of each address group.

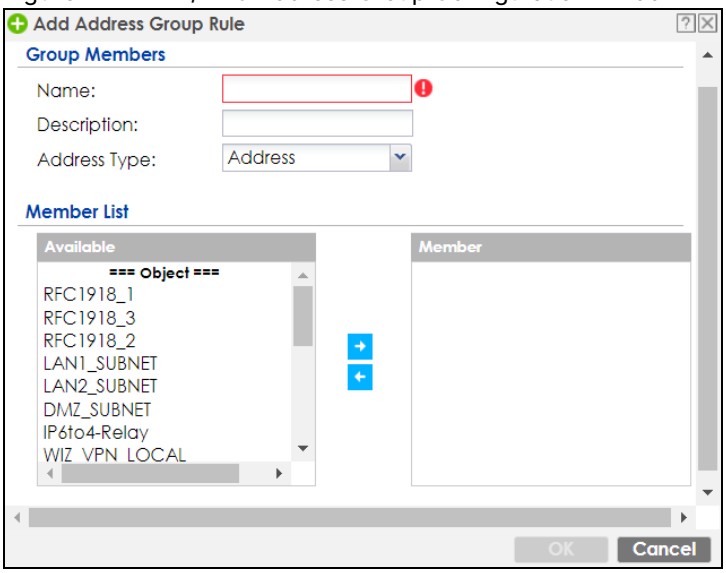
Table 239 Configuration > Object > Address/Geo IP > Address Group (continued)

LABEL	DESCRIPTION
Description	This field displays the description of each address group, if any.
Reference	This displays the number of times an object reference is used in a profile.
IPv6 Address Group Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific address group.
Name	This field displays the name of each address group.
Description	This field displays the description of each address group, if any.
Reference	This displays the number of times an object reference is used in a profile.

30.4.3.1 Address Group Add/Edit Screen

The Address Group Add/Edit screen allows you to create a new address group or edit an existing one. To access this screen, go to the Address Group screen (see Section 30.4.3 on page 711), and click either the Add icon or an Edit icon in the IPv4 Address Group Configuration or IPv6 Address Group Configuration section.

Figure 471 IPv4/IPv6 Address Group Configuration > Add



The following table describes the labels in this screen.

Table 240 IPv4/IPv6 Address Group Configuration > Add

LABEL	DESCRIPTION
Name	Enter a name for the address group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	This field displays the description of each address group, if any. You can use up to 60 characters, punctuation marks, and spaces.

Table 240 IPv4/IPv6 Address Group Configuration > Add (continued)

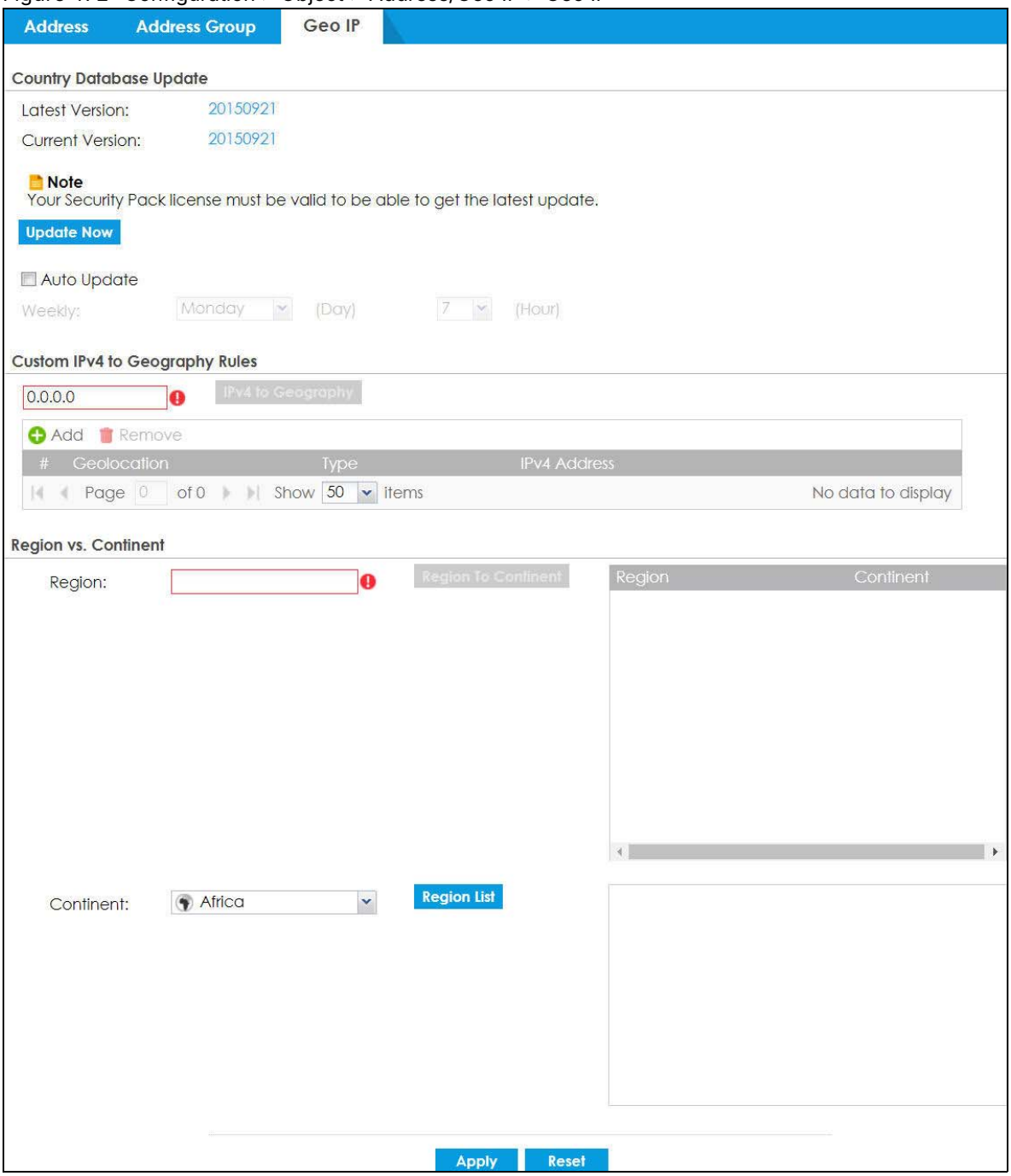
LABEL	DESCRIPTION
Address Type	Select the type of address you want to create. Note: The Zyxel Device automatically updates address objects that are based on an interface's IP address, subnet, or gateway if the interface's IP address settings change. For example, if you change 1's IP address, the Zyxel Device automatically updates the corresponding interface-based, LAN subnet address object.
Member List	The Member list displays the names of the address and address group objects that have been added to the address group. The order of members is not important. Select items from the Available list that you want to be members and move them to the Member list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Move any members you do not want included to the Available list. Note: Only objects of the same address type can be added to a address group.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving your changes.

30.4.4 Geo IP Summary Screen

Use this screen to update the database of country-to-IP and continent-to-IP address mappings and manually configure custom country-to-IP and continent-to-IP address mappings in geographic address objects. You can then use geographic address objects in security policies to forward or deny traffic to whole countries or regions.

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 472 Configuration > Object > Address/Geo IP > Geo IP



The following table describes the labels in this screen.

Table 241 Configuration > Object > Address/Geo IP > Geo IP

LABEL	DESCRIPTION
Country Database Update	
Latest Version	This is the latest country-to-IP address database version on myZyxel.
Current Version	This is the country-to-IP address database version currently on the Zyxel Device.

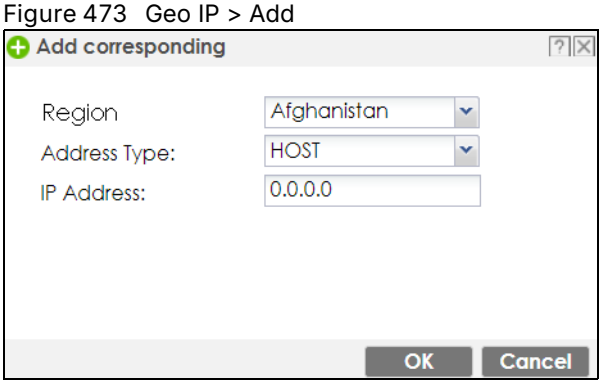
Table 241 Configuration > Object > Address/Geo IP > Geo IP (continued)

LABEL	DESCRIPTION
Update Now	Click this to check for the latest country-to-IP address database version on myZyxel. The latest version is downloaded to the Zyxel Device and replaces the current version if it is newer. There are logs to show the update status.
Auto Update	If you want the Zyxel Device to check weekly for the latest country-to-IP address database version on myZyxel, select the checkbox, choose a day and time each week and then click Apply. The default day and time displayed is the Zyxel Device current day and time.
Custom IPv4/IPv6 to Geography Rules	
IPv4/IPv6 to Geography	Enter an IP address, then click this button to query which country this IP address belongs to.
Add	Click this to create a new entry.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific entry.
Geolocation	This field displays the name of the country or region that is associated with this IP address.
Type	This field displays whether this address object is HOST, RANGE or SUBNET.
IPv4/IPv6 Address	This field displays the IPv4/IPv6 addresses represented by the type of address object.
Region vs. Continent	
Region	Enter a country name, then click the Region to Continent button to query which continent this country belongs to.
Continent	Select a continent, then click the Region List button to query which countries belong to the continent.
Apply	Click Apply to save the changes.
Reset	Click Reset to return the screen to its last-saved settings.

30.4.4.1 Add Custom IPv4/IPv6 Address to Geography Screen

This screen allows you to create a new geography-to-IP address mapping. To access this screen, go to the Geo IP screen (see Section 30.4.4 on page 713), and click the Add icon in the Custom IPv4 to Geography Rules or Custom IPv6 to Geography Rules section.

Figure 473 Geo IP > Add



The following table describes the labels in this screen.

Table 242 Geo IP > Add

LABEL	DESCRIPTION
Region	Select the country or continent that maps to this IP address.
Address Type	Select the type of address you want to create. Choices are: HOST, RANGE, SUBNET.
IP Address	This field is only available if the Address Type is HOST. This field cannot be blank. Enter the IP address that this address object represents.
IP Starting Address	This field is only available if the Address Type is RANGE. This field cannot be blank. Enter the beginning of the range of IP addresses that this address object represents.
IP Ending Address	This field is only available if the Address Type is RANGE. This field cannot be blank. Enter the end of the range of IP address that this address object represents.
Network / Netmask	These fields are only available if the IPv4 Address Type is SUBNET. They cannot be blank. Enter the network IP and subnet mask that defines the IPv4 subnet.
IPv6 Address Prefix	This field is only available if the IPv6 Address Type is SUBNET. This field cannot be blank. Enter the IPv6 address prefix that the Zyxel Device uses for the LAN IPv6 address.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving your changes.

30.5 Service Overview

Use service objects to define TCP applications, UDP applications, and ICMP messages. You can also create service groups to refer to multiple service objects in other features.

- Use the Service screens (Section 30.5.2 on page 717) to view and configure the Zyxel Device's list of services and their definitions.
- Use the Service Group screens (Section 30.5.2 on page 717) to view and configure the Zyxel Device's list of service groups.

30.5.1 What You Need to Know

IP Protocols

IP protocols are based on the eight-bit protocol field in the IP header. This field represents the next-level protocol that is sent in this packet. This section discusses three of the most common IP protocols.

Computers use Transmission Control Protocol (TCP, IP protocol 6) and User Datagram Protocol (UDP, IP protocol 17) to exchange data with each other. TCP guarantees reliable delivery but is slower and more complex. Some uses are FTP, HTTP, SMTP, and TELNET. UDP is simpler and faster but is less reliable. Some uses are DHCP, DNS, RIP, and SNMP.

TCP creates connections between computers to exchange data. Once the connection is established, the computers exchange data. If data arrives out of sequence or is missing, TCP puts it in sequence or waits for the data to be re-transmitted. Then, the connection is terminated.

In contrast, computers use UDP to send short messages to each other. There is no guarantee that the messages arrive in sequence or that the messages arrive at all.

Both TCP and UDP use ports to identify the source and destination. Each port is a 16-bit number. Some port numbers have been standardized and are used by low-level system processes; many others have no particular meaning.

Unlike TCP and UDP, Internet Control Message Protocol (ICMP, IP protocol 1) is mainly used to send error messages or to investigate problems. For example, ICMP is used to send the response if a computer cannot be reached. Another use is ping. ICMP does not guarantee delivery, but networks often treat ICMP messages differently, sometimes looking at the message itself to decide where to send it.

Service Objects and Service Groups

Use service objects to define IP protocols.

- TCP applications
- UDP applications
- ICMP messages
- user-defined services (for other types of IP protocols)

These objects are used in policy routes and security policies.

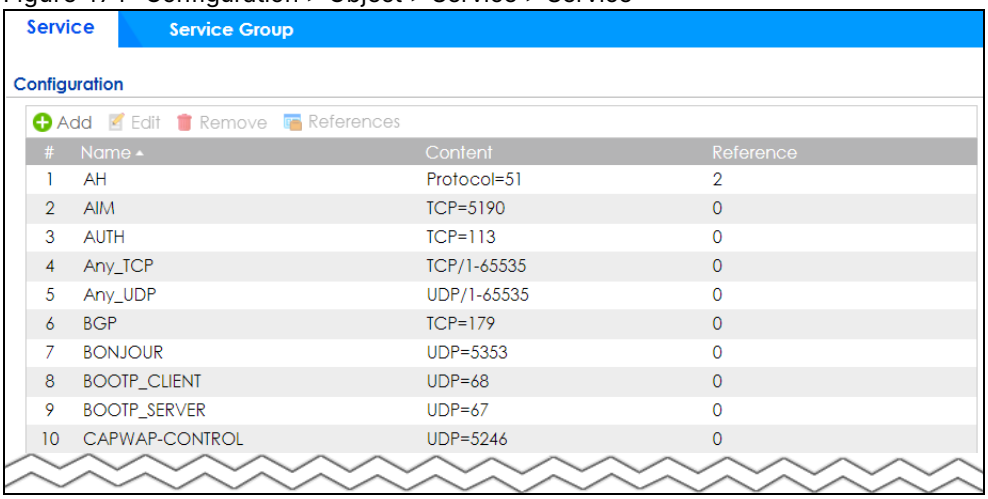
Use service groups when you want to create the same rule for several services, instead of creating separate rules for each service. Service groups may consist of services and other service groups. The sequence of members in the service group is not important.

30.5.2 The Service Summary Screen

The Service summary screen provides a summary of all services and their definitions. In addition, this screen allows you to add, edit, and remove services.

To access this screen, log in to the Web Configurator, and click Configuration > Object > Service > Service. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 474 Configuration > Object > Service > Service



#	Name	Content	Reference
1	AH	Protocol=51	2
2	AIM	TCP=5190	0
3	AUTH	TCP=113	0
4	Any_TCP	TCP/1-65535	0
5	Any_UDP	UDP/1-65535	0
6	BGP	TCP=179	0
7	BONJOUR	UDP=5353	0
8	BOOTP_CLIENT	UDP=68	0
9	BOOTP_SERVER	UDP=67	0
10	CAPWAP-CONTROL	UDP=5246	0

The following table describes the labels in this screen.

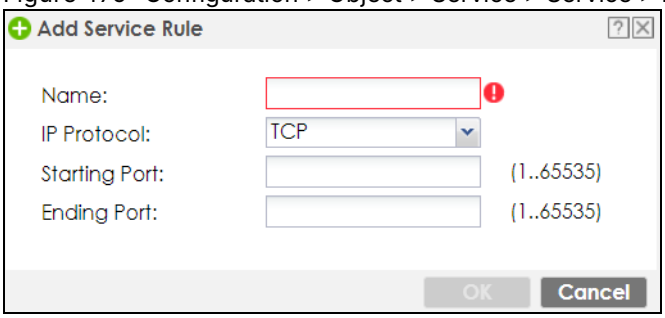
Table 243 Configuration > Object > Service > Service

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific service.
Name	This field displays the name of each service.
Content	This field displays a description of each service.
Reference	This displays the number of times an object reference is used in a profile.

30.5.2.1 The Service Add/Edit Screen

The Service Add/Edit screen allows you to create a new service or edit an existing one. To access this screen, go to the Service screen (see Section 30.5.2 on page 717), and click either the Add icon or an Edit icon.

Figure 475 Configuration > Object > Service > Service > Edit



The following table describes the labels in this screen.

Table 244 Configuration > Object > Service > Service > Edit

LABEL	DESCRIPTION
Name	Type the name used to refer to the service. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
IP Protocol	Select the protocol the service uses. Choices are: TCP, UDP, ICMP, ICMPv6, and User Defined.
Starting Port Ending Port	This field appears if the IP Protocol is TCP or UDP. Specify the port number(s) used by this service. If you fill in one of these fields, the service uses that port. If you fill in both fields, the service uses the range of ports.
ICMP Type	This field appears if the IP Protocol is ICMP or ICMPv6. Select the ICMP message used by this service. This field displays the message text, not the message number.
IP Protocol Number	This field appears if the IP Protocol is User Defined. Enter the number of the next-level protocol (IP protocol). Allowed values are 1 - 255.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving your changes.

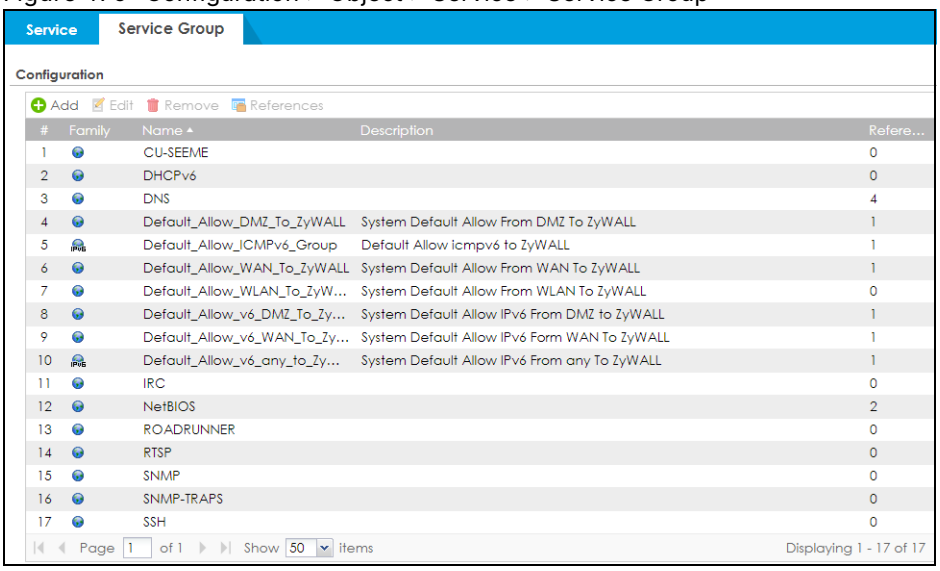
30.5.3 The Service Group Summary Screen

The Service Group summary screen provides a summary of all service groups. In addition, this screen allows you to add, edit, and remove service groups.

Note: If you want to access the Zyxel Device using HTTP, HTTPS, SSH, and/or, TELNET, you must add them in the Object > Service > Service Group > Default_Allow_WAN_To_ZyWALL service group, which is used in the WAN_to_Device security policy.

To access this screen, log in to the Web Configurator, and click Configuration > Object > Service > Service Group.

Figure 476 Configuration > Object > Service > Service Group



The following table describes the labels in this screen. See Section 30.5.3.1 on page 720 for more information as well.

Table 245 Configuration > Object > Service > Service Group

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific service group.
Family	This field displays the Server Group supported type, which is according to your configurations in the Service Group Add/Edit screen. There are 3 types of families: • : Supports IPv4 only • : Supports IPv6 only • : Supports both IPv4 and IPv6

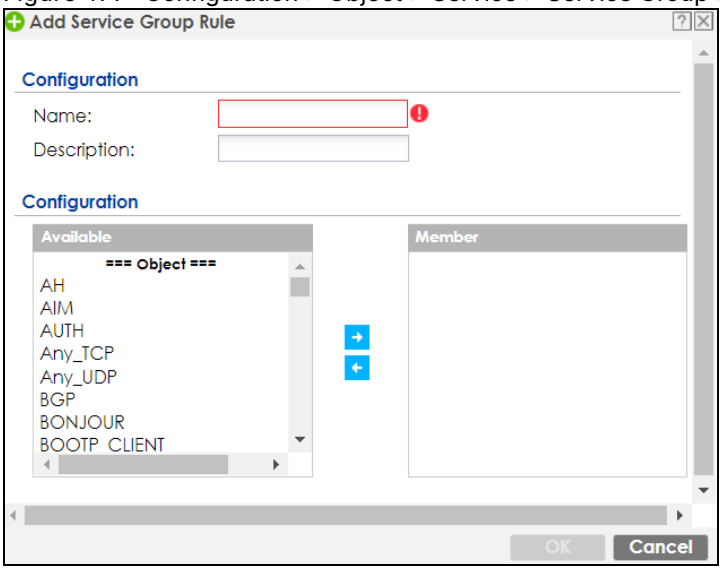
Table 245 Configuration > Object > Service > Service Group (continued)

LABEL	DESCRIPTION
Name	This field displays the name of each service group. By default, the Zyxel Device uses services starting with “Default_Allow_” in the security policies to allow certain services to connect to the Zyxel Device.
Description	This field displays the description of each service group, if any.
Reference	This displays the number of times an object reference is used in a profile.

30.5.3.1 The Service Group Add/Edit Screen

The Service Group Add/Edit screen allows you to create a new service group or edit an existing one. To access this screen, go to the Service Group screen (see Section 30.5.3 on page 719), and click either the Add icon or an Edit icon.

Figure 477 Configuration > Object > Service > Service Group > Edit



The following table describes the labels in this screen.

Table 246 Configuration > Object > Service > Service Group > Edit

LABEL	DESCRIPTION
Name	Enter the name of the service group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description of the service group, if any. You can use 1 to 60 single-byte characters, including 0-9a-zA-Z!"#$%'()*+,-/:;=?@_ &.<>[\]^'{|} are not allowed.
Configuration	The Member list displays the names of the service and service group objects that have been added to the service group. The order of members is not important. Select items from the Available list that you want to be members and move them to the Member list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Move any members you do not want included to the Available list.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving your changes.

30.6 Schedule Overview

Use schedules to set up one-time and recurring schedules for policy routes, security policies, and content filtering. The Zyxel Device supports one-time and recurring schedules. One-time schedules are effective only once, while recurring schedules usually repeat. Both types of schedules are based on the current date and time in the Zyxel Device.

Note: Schedules are based on the Zyxel Device's current date and time.

- Use the Schedule summary screen (Section 30.6.2 on page 721) to see a list of all schedules in the Zyxel Device.
- Use the One-Time Schedule Add/Edit screen (Section 30.6.2.1 on page 722) to create or edit a one-time schedule.
- Use the Recurring Schedule Add/Edit screen (Section 30.6.2.2 on page 723) to create or edit a recurring schedule.
- Use the Schedule Group screen (Section 30.6.3 on page 724) to merge individual schedule objects as one object.

30.6.1 What You Need to Know

One-time Schedules

One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods.

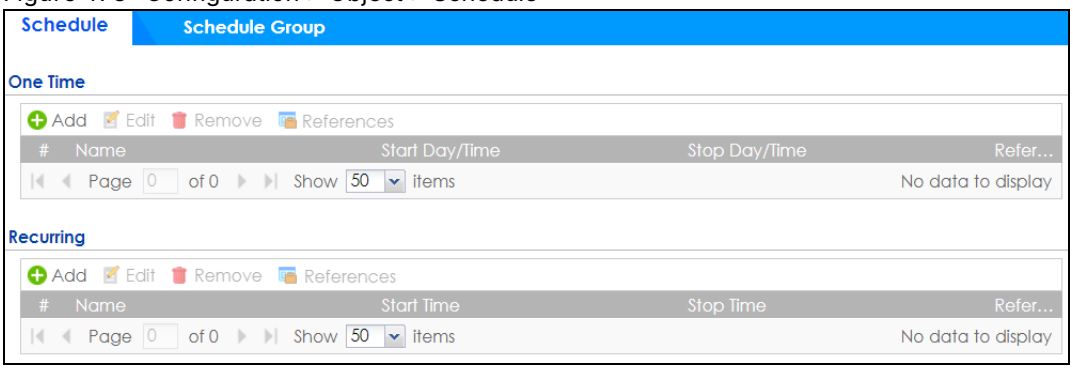
Recurring Schedules

Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring schedules always begin and end in the same day. Recurring schedules are useful for defining the workday and off-work hours.

30.6.2 The Schedule Screen

The Schedule screen provides a summary of all schedules in the Zyxel Device. To access this screen, click Configuration > Object > Schedule.

Figure 478 Configuration > Object > Schedule



The following table describes the labels in this screen. See Section 30.6.2.1 on page 722 and Section 30.6.2.2 on page 723 for more information as well.

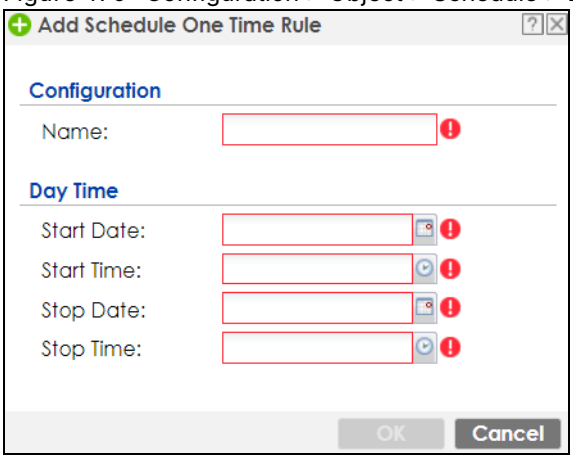
Table 247 Configuration > Object > Schedule

LABEL	DESCRIPTION
One Time	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific schedule.
Name	This field displays the name of the schedule, which is used to refer to the schedule.
Start Day / Time	This field displays the date and time at which the schedule begins.
Stop Day / Time	This field displays the date and time at which the schedule ends.
Reference	This displays the number of times an object reference is used in a profile.
Recurring	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific schedule.
Name	This field displays the name of the schedule, which is used to refer to the schedule.
Start Time	This field displays the time at which the schedule begins.
Stop Time	This field displays the time at which the schedule ends.
Reference	This displays the number of times an object reference is used in a profile.

30.6.2.1 The One-Time Schedule Add/Edit Screen

The One-Time Schedule Add/Edit screen allows you to define a one-time schedule or edit an existing one. To access this screen, go to the Schedule screen (see Section 30.6.2 on page 721), and click either the Add icon or an Edit icon in the One Time section.

Figure 479 Configuration > Object > Schedule > Edit (One Time)



The following table describes the labels in this screen.

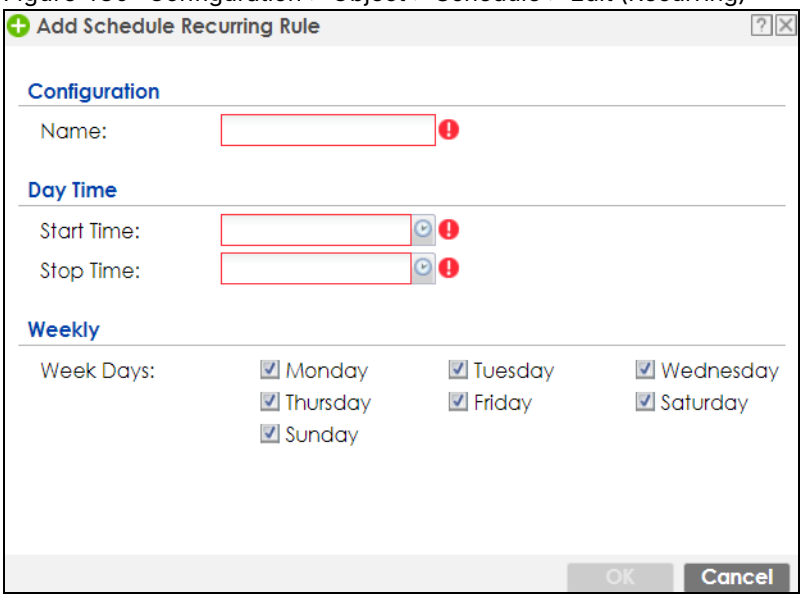
Table 248 Configuration > Object > Schedule > Edit (One Time)

LABEL	DESCRIPTION
Configuration	
Name	Type the name used to refer to the one-time schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Day Time	
StartDate	Specify the year, month, and day when the schedule begins. • Year - 1900 - 2999 • Month - 1 - 12 • Day - 1 - 31 (it is not possible to specify illegal dates, such as February 31.)
StartTime	Specify the hour and minute when the schedule begins. • Hour - 0 - 23 • Minute - 0 - 59
StopDate	Specify the year, month, and day when the schedule ends. • Year - 1900 - 2999 • Month - 1 - 12 • Day - 1 - 31 (it is not possible to specify illegal dates, such as February 31.)
StopTime	Specify the hour and minute when the schedule ends. • Hour - 0 - 23 • Minute - 0 - 59
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving your changes.

30.6.2.2 The Recurring Schedule Add/Edit Screen

The Recurring Schedule Add/Edit screen allows you to define a recurring schedule or edit an existing one. To access this screen, go to the Schedule screen (see Section 30.6.2 on page 721), and click either the Add icon or an Edit icon in the Recurring section.

Figure 480 Configuration > Object > Schedule > Edit (Recurring)



The Year, Month, and Day columns are not used in recurring schedules and are disabled in this screen. The following table describes the remaining labels in this screen.

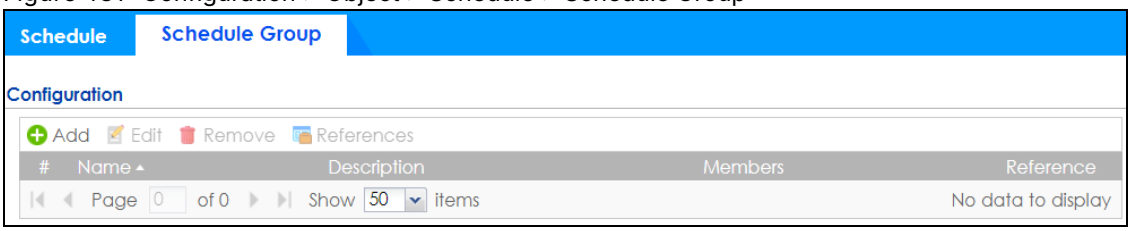
Table 249 Configuration > Object > Schedule > Edit (Recurring)

LABEL	DESCRIPTION
Configuration	
Name	Type the name used to refer to the recurring schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Date Time	
StartTime	Specify the hour and minute when the schedule begins each day. • Hour - 0 - 23 • Minute - 0 - 59
StopTime	Specify the hour and minute when the schedule ends each day. • Hour - 0 - 23 • Minute - 0 - 59
Weekly	
Week Days	Select each day of the week the recurring schedule is effective.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving your changes.

30.6.3 The Schedule Group Screen

The Schedule Group screen provides a summary of all groups of schedules in the Zyxel Device. To access this screen, click Configuration > Object > Schedule > Group.

Figure 481 Configuration > Object > Schedule > Schedule Group



The following table describes the fields in the above screen.

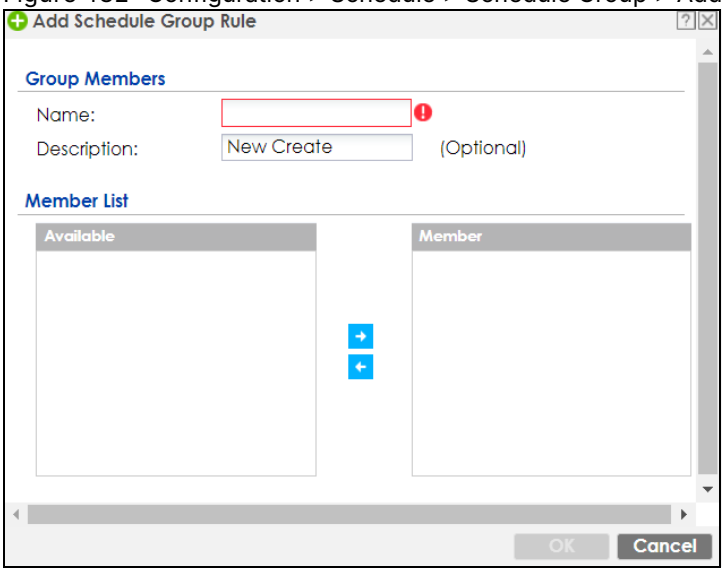
Table 250 Configuration > Object > Schedule > Schedule Group

LABEL	DESCRIPTION
Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific schedule.
Name	This field displays the name of the schedule group, which is used to refer to the schedule.
Description	This field displays the description of the schedule group.
Members	This field lists the members in the schedule group. Each member is separated by a comma.
Reference	This displays the number of times an object reference is used in a profile.

30.6.3.1 The Schedule Group Add/Edit Screen

The Schedule Group Add/Edit screen allows you to define a schedule group or edit an existing one. To access this screen, go to the Schedule screen (see Section 30.6.2 on page 721), and click either the Add icon or an Edit icon in the Schedule Group section.

Figure 482 Configuration > Schedule > Schedule Group > Add



The following table describes the fields in the above screen.

Table 251 Configuration > Object > Schedule > Schedule Group > Add

LABEL	DESCRIPTION
Group Members	
Name	Type the name used to refer to the recurring schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description of the service group, if any. You can use 1 to 60 single-byte characters, including 0-9a-zA-Z!"#$%'()*+,-/:;=?@_ &.<>[\]^'{|} are not allowed.
Member List	The Member list displays the names of the service and service group objects that have been added to the service group. The order of members is not important. Select items from the Available list that you want to be members and move them to the Member list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Move any members you do not want included to the Available list.
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to exit this screen without saving your changes.

30.7 AAA Server Overview

You can use a AAA (Authentication, Authorization, Accounting) server to provide access control to your network. The AAA server can be a Active Directory, LDAP, or RADIUS server. Use the AAA Server screens to create and manage objects that contain settings for using AAA servers. You use AAA server objects in configuring ext-group-user user objects and authentication method objects (see Chapter 30 on page 735).

30.7.1 Directory Service (AD/LDAP)

LDAP/AD allows a client (the Zyxel Device) to connect to a server to retrieve information from a directory. A network example is shown next.

Figure 483 Example: Directory Service Client and Server

The following describes the user authentication procedure through an LDAP/AD server.

1 A user logs in with a user name and password pair.

2 The Zyxel Device tries to bind (or log in) to the LDAP/AD server.

3 When the binding process is successful, the Zyxel Device checks the user information in the directory against the user name and password pair.

4 If it matches, the user is allowed access. Otherwise, access is blocked.

30.7.2 RADIUS Server

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate a large number of users from a central location.

Figure 484 RADIUS Server Network Example

30.7.3 ASAS

ASAS (Authenex Strong Authentication System) is a RADIUS server that works with the One-Time Password (OTP) feature. Purchase a Zyxel Device OTP package in order to use this feature. The package contains server software and physical OTP tokens (PIN generators). Do the following to use OTP. See the documentation included on the ASAS' CD for details.

1 Install the ASAS server software on a computer.

2 Create user accounts on the Zyxel Device and in the ASAS server.

3 Import each token's database file (located on the included CD) into the server.

4 Assign users to OTP tokens (on the ASAS server).

5 Configure the ASAS as a RADIUS server in the Zyxel Device's Configuration > Object > AAA Server screens.

6 Give the OTP tokens to (local or remote) users.

- Use the Configuration > Object > AAA Server > Active Directory (or LDAP) screens (Section 30.7.5 on page 729) to configure Active Directory or LDAP server objects.
- Use the Configuration > Object > AAA Server > RADIUS screen (Section 30.7.2 on page 727) to configure the default external RADIUS server to use for user authentication.

30.7.4 What You Need To Know

AAA Servers Supported by the Zyxel Device

The following lists the types of authentication server the Zyxel Device supports.

- Local user database

  The Zyxel Device uses the built-in local user database to authenticate administrative users logging into the Zyxel Device's Web Configurator or network access users logging into the network through the Zyxel Device. You can also use the local user database to authenticate VPN users.

- Directory Service (LDAP/AD)

  LDAP (Lightweight Directory Access Protocol)/AD (Active Directory) is a directory service that is both a directory and a protocol for controlling access to a network. The directory consists of a database specialized for fast information retrieval and filtering activities. You create and store user profile and login information on the external server.

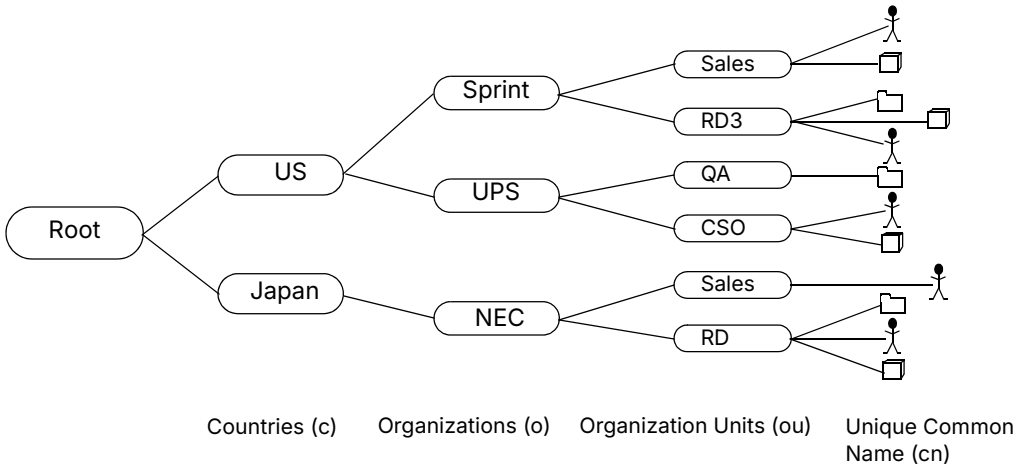
- RADIUS

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

Directory Structure

The directory entries are arranged in a hierarchical order much like a tree structure. Normally, the directory structure reflects the geographical or organizational boundaries. The following figure shows a basic directory structure branching from countries to organizations to organizational units to individuals.

Figure 485 Basic Directory Structure



Distinguished Name (DN)

A DN uniquely identifies an entry in a directory. A DN consists of attribute-value pairs separated by commas. The leftmost attribute is the Relative Distinguished Name (RDN). This provides a unique name for

entries that have the same “parent DN” (“`cn=domain1.com`, `ou=Sales, o=MyCompany`” in the following examples).

```
cn=domain1.com, ou = Sales, o=MyCompany, c=US
cn=domain1.com, ou = Sales, o=MyCompany, c=JP
```

Base DN

A base DN specifies a directory. A base DN usually contains information such as the name of an organization, a domain name and/or country. For example, `o=MyCompany`, `c=UK` where o means organization and c means country.

Bind DN

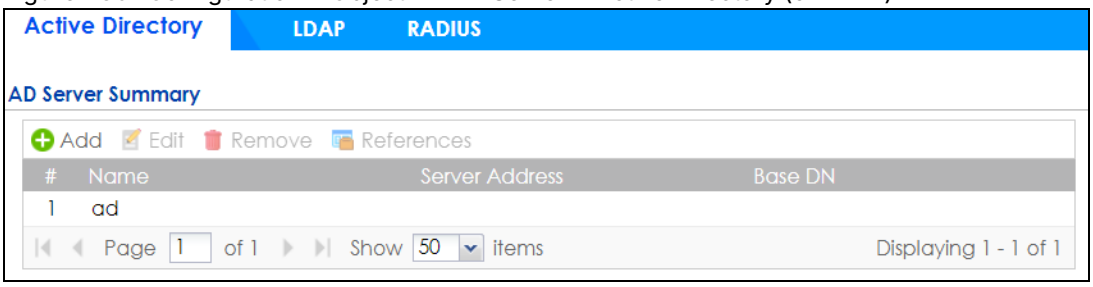
A bind DN is used to authenticate with an LDAP/AD server. For example a bind DN of `cn=zywallAdmin` allows the Zyxel Device to log into the LDAP/AD server using the user name of `zywallAdmin`. The bind DN is used in conjunction with a bind password. When a bind DN is not specified, the Zyxel Device will try to log in as an anonymous user. If the bind password is incorrect, the login will fail.

30.7.5 Active Directory or LDAP Server Summary

Use the Active Directory or LDAP screen to manage the list of AD or LDAP servers the Zyxel Device can use in authenticating users.

Click Configuration > Object > AAA Server > Active Directory (or LDAP) to display the Active Directory (or LDAP) screen.

Figure 486 Configuration > Object > AAA Server > Active Directory (or LDAP)



The following table describes the labels in this screen.

Table 252 Configuration > Object > AAA Server > Active Directory (or LDAP)

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry’s settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific AD or LDAP server.
Name	This field displays the name of the Active Directory.

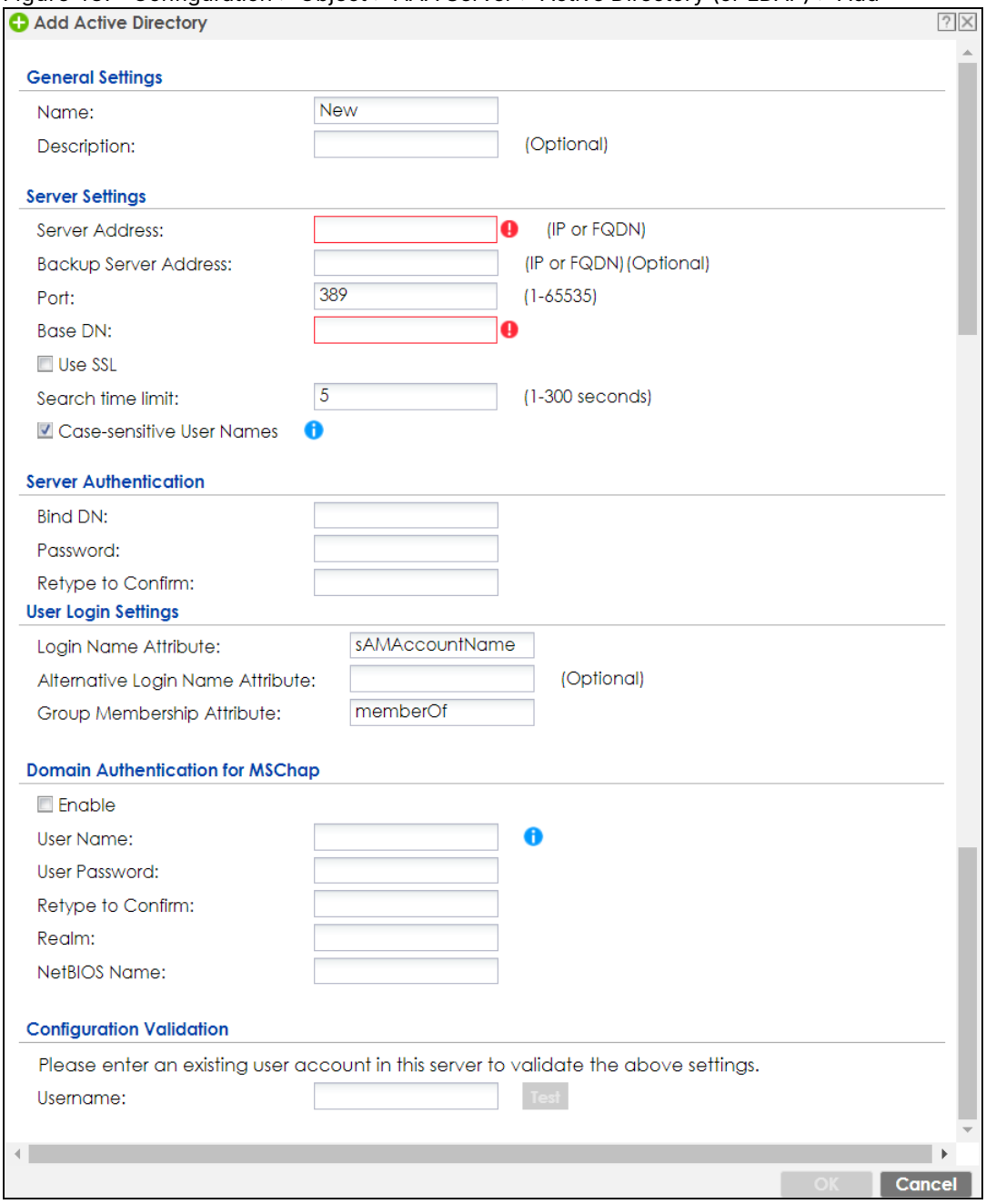
Table 252 Configuration > Object > AAA Server > Active Directory (or LDAP) (continued)

LABEL	DESCRIPTION
Server Address	This is the address of the AD or LDAP server.
Base DN	This specifies a directory. For example, `o=Zyxel, c=US`.

30.7.5.1 Adding an Active Directory or LDAP Server

Click Object > AAA Server > Active Directory (or LDAP) to display the Active Directory (or LDAP) screen. Click the Add icon or an Edit icon to display the following screen. Use this screen to create a new AD or LDAP entry or edit an existing one.

Figure 487 Configuration > Object > AAA Server > Active Directory (or LDAP) > Add



The following table describes the labels in this screen.

Table 253 Configuration > Object > AAA Server > Active Directory (or LDAP) > Add

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 63 alphanumerical characters) for identification purposes.
Description	Enter the description of each server, if any. ou can use 1 to 60 single-byte characters, including 0-9a-zA-Z!"#$%'()*+,-/:;=?@_ &.<>[\]^'{|} are not allowed.
Server Address	Enter the address of the AD or LDAP server.
Backup Server Address	If the AD or LDAP server has a backup server, enter its address here.
Port	Specify the port number on the AD or LDAP server to which the Zyxel Device sends authentication requests. Enter a number between 1 and 65535. This port number should be the same on all AD or LDAP server(s) in this group.
Base DN	Specify the directory (up to 127 alphanumerical characters). For example, `o=Zyxel, c=US`. This is only for LDAP.
Use SSL	Select Use SSL to establish a secure connection to the AD or LDAP server(s).
Search time limit	Specify the timeout period (between 1 and 300 seconds) before the Zyxel Device disconnects from the AD or LDAP server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the AD or LDAP server(s) or the AD or LDAP server(s) is down.
Case-sensitive User Names	Select this if the server checks the case of the usernames.
Bind DN	Specify the bind DN for logging into the AD or LDAP server. Enter up to 127 alphanumerical characters. For example, `cn=zywallAdmin` specifies `zywallAdmin` as the user name.
Password	If required, enter the password (up to 15 alphanumerical characters) for the Zyxel Device to bind (or log in) to the AD or LDAP server. Your password will be encrypted when you configure this field.
Retype to Confirm	Retype your new password for confirmation.
Login Name Attribute	Enter the type of identifier the users are to use to log in. For example “name” or “email address”.
Alternative Login Name Attribute	If there is a second type of identifier that the users can use to log in, enter it here. For example “name” or “email address”.
Group Membership Attribute	An AD or LDAP server defines attributes for its accounts. Enter the name of the attribute that the Zyxel Device is to check to determine to which group a user belongs. The value for this attribute is called a group identifier; it determines to which group a user belongs. You can add ext-group-user user objects to identify groups based on these group identifier values. For example you could have an attribute named “memberOf” with values like “sales”, “RD”, and “management”. Then you could also create a ext-group-user user object for each group. One with “sales” as the group identifier, another for “RD” and a third for “management”.
Domain Authentication for MSChap	Select the Enable checkbox to enable domain authentication for MSChap. This is only for Active Directory.
User Name	Enter the user name for the user who has rights to add a machine to the domain. This is only for Active Directory.
User Password	Enter the password for the associated user name. This is only for Active Directory.

Table 253 Configuration > Object > AAA Server > Active Directory (or LDAP) > Add (continued)

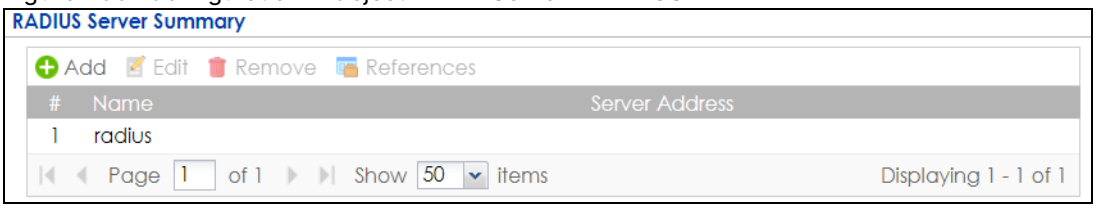
LABEL	DESCRIPTION
Retype to Confirm	Retype your new password for confirmation. This is only for Active Directory.
Realm	Enter the realm FQDN. This is only for Active Directory.
NetBIOS Name	Type the NetBIOS name. This field is optional. NetBIOS packets are TCP or UDP packets that enable a computer to connect to and communicate with a LAN which allows local computers to find computers on the remote network and vice versa.
Configuration Validation	Use a user account from the server specified above to test if the configuration is correct. Enter the account's user name in the Username field and click Test.
OK	Click OK to save the changes.
Cancel	Click Cancel to discard the changes.

30.7.6 RADIUS Server Summary

Use the RADIUS screen to manage the list of RADIUS servers the Zyxel Device can use in authenticating users.

Click Configuration > Object > AAA Server > RADIUS to display the RADIUS screen.

Figure 488 Configuration > Object > AAA Server > RADIUS



The following table describes the labels in this screen.

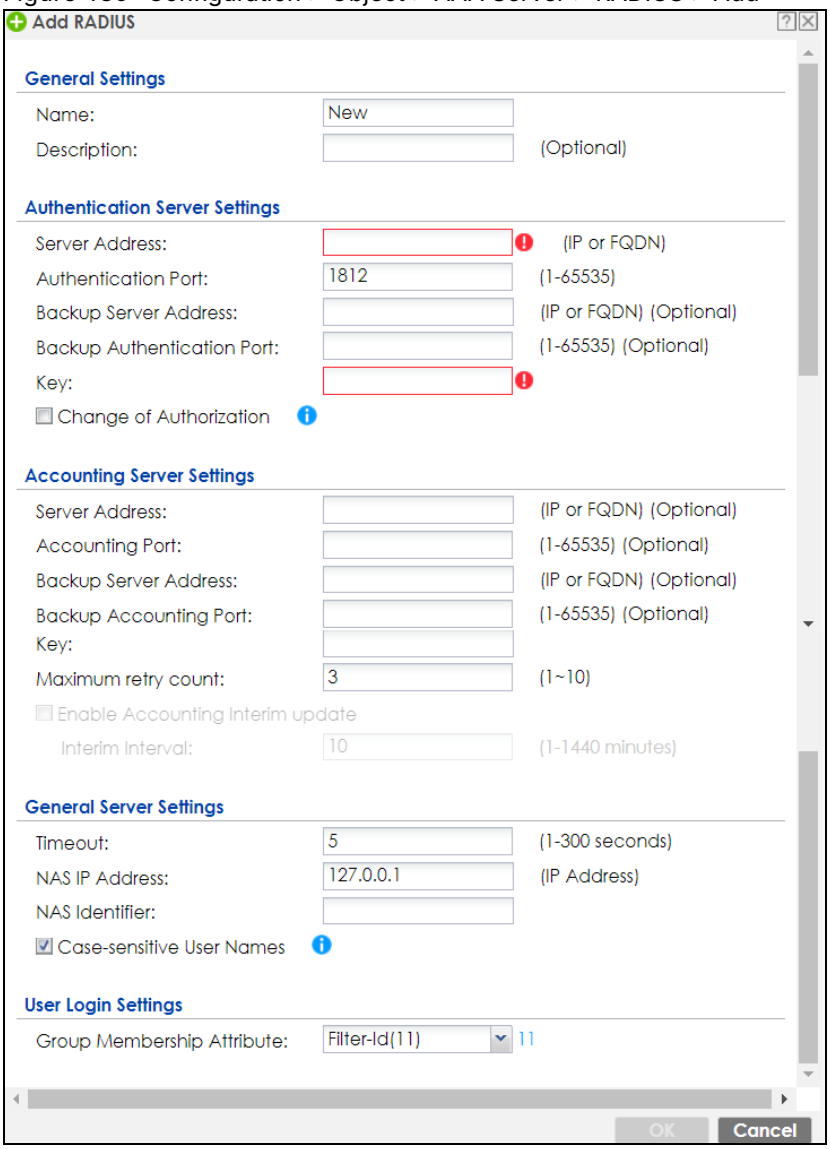
Table 254 Configuration > Object > AAA Server > RADIUS

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click References to open a screen that shows which settings use the entry.
#	This field displays the index number.
Name	This is the name of the RADIUS server entry.
Server Address	This is the address of the AD or LDAP server.

30.7.6.1 Adding a RADIUS Server

Click Configuration > Object > AAA Server > RADIUS to display the RADIUS screen. Click the Add icon or an Edit icon to display the following screen. Use this screen to create a new AD or LDAP entry or edit an existing one.

Figure 489 Configuration > Object > AAA Server > RADIUS > Add



The following table describes the labels in this screen.

Table 255 Configuration > Object > AAA Server > RADIUS > Add

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 63 alphanumerical characters) for identification purposes.
Description	Enter the description of each server, if any. ou can use 1 to 60 single-byte characters, including 0-9a-zA-Z!"#$%'()*+,-/:;=?@_ &.<>[\]^'{|} are not allowed.
Server Address	Enter the address of the RADIUS server.
Authentication Port	Specify the port number on the RADIUS server to which the Zyxel Device sends authentication requests. Enter a number between 1 and 65535.
Backup Server Address	If the RADIUS server has a backup server, enter its address here.

Table 255 Configuration > Object > AAA Server > RADIUS > Add (continued)

LABEL	DESCRIPTION
Backup Authentication Port	Specify the port number on the RADIUS server to which the Zyxel Device sends authentication requests. Enter a number between 1 and 65535.
Key	Enter a password (up to 15 alphanumeric characters) as the key to be shared between the external authentication server and the Zyxel Device. Your password will be encrypted when you configure this field. The key is not sent over the network. This key must be the same on the external authentication server and the Zyxel Device.
Change of Authorization	The external RADIUS server can change its authentication policy and send CoA (Change of Authorization) or RADIUS Disconnect messages in order to terminate the subscriber's service. Select this option to allow the Zyxel Device to disconnect wireless clients based on the information (such as client's user name and MAC address) specified in CoA or RADIUS Disconnect messages sent by the RADIUS server.
Server Address	Enter the IP address or Fully-Qualified Domain Name (FQDN) of the RADIUS accounting server.
Accounting Port	Specify the port number on the RADIUS server to which the Zyxel Device sends accounting information. Enter a number between 1 and 65535.
Backup Server Address	If the RADIUS server has a backup accounting server, enter its address here.
Backup Accounting Port	Specify the port number on the RADIUS server to which the Zyxel Device sends accounting information. Enter a number between 1 and 65535.
Key	Enter a password (up to 15 alphanumeric characters) as the key to be shared between the external authentication server and the Zyxel Device. The key is not sent over the network. This key must be the same on the external authentication server and the Zyxel Device.
Maximum Retry Count	At times the Zyxel Device may not be able to use the primary RADIUS accounting server. Specify the number of times the Zyxel Device should reattempt to use the primary RADIUS server before attempting to use the secondary RADIUS server. This also sets how many times the Zyxel Device will attempt to use the secondary RADIUS server. For example, you set this field to 3. If the Zyxel Device does not get a response from the primary RADIUS server, it tries again up to three times. If there is no response, the Zyxel Device tries the secondary RADIUS server up to three times. If there is also no response from the secondary RADIUS server, the Zyxel Device stops attempting to authenticate the subscriber. The subscriber will see a message that says the RADIUS server was not found.
Enable Accounting Interim Update	This field is configurable only after you configure a RADIUS accounting server address. Select this to have the Zyxel Device send subscriber status updates to the RADIUS server at the interval you specify.
Interim Interval	Specify the time interval for how often the Zyxel Device is to send a subscriber status update to the RADIUS server.
Timeout	Specify the timeout period (between 1 and 300 seconds) before the Zyxel Device disconnects from the RADIUS server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the RADIUS server or the RADIUS server is down.
NAS IP Address	Type the IP address of the NAS (Network Access Server).
NAS Identifier	If the RADIUS server requires the Zyxel Device to provide the Network Access Server identifier attribute with a specific value, enter it here.
Case-sensitive User Names	Select this if you want configure your username as case-sensitive.

Table 255 Configuration > Object > AAA Server > RADIUS > Add (continued)

LABEL	DESCRIPTION
Group Membership Attribute	A RADIUS server defines attributes for its accounts. Select the name and number of the attribute that the Zyxel Device is to check to determine to which group a user belongs. If it does not display, select user-defined and specify the attribute's number. This attribute's value is called a group identifier; it determines to which group a user belongs. You can add ext-group-user user objects to identify groups based on these group identifier values. For example you could have an attribute named "memberOf" with values like "sales", "RD", and "management". Then you could also create a ext-group-user user object for each group. One with "sales" as the group identifier, another for "RD" and a third for "management".
OK	Click OK to save the changes.
Cancel	Click Cancel to discard the changes.

30.8 Auth. Method Overview

Authentication method objects set how the Zyxel Device authenticates wireless, HTTP/HTTPS clients, and peer IPSec routers (extended authentication) clients. Configure authentication method objects to have the Zyxel Device use the local user database, and/or the authentication servers and authentication server groups specified by AAA server objects. By default, user accounts created and stored on the Zyxel Device are authenticated locally.

- Use the Configuration > Object > Auth. Method screens (Section 30.8.3 on page 736) to create and manage authentication method objects.
- Use the Configuration > Object > Auth. Method > Two-Factor Authentication screen (Section 30.8.4 on page 738) to configure double-layer security to access the Zyxel Device through a VPN tunnel, or access the Zyxel Device using Web Configurator, SSH, or Telnet.

30.8.1 Before You Begin

Configure AAA server objects before you configure authentication method objects.

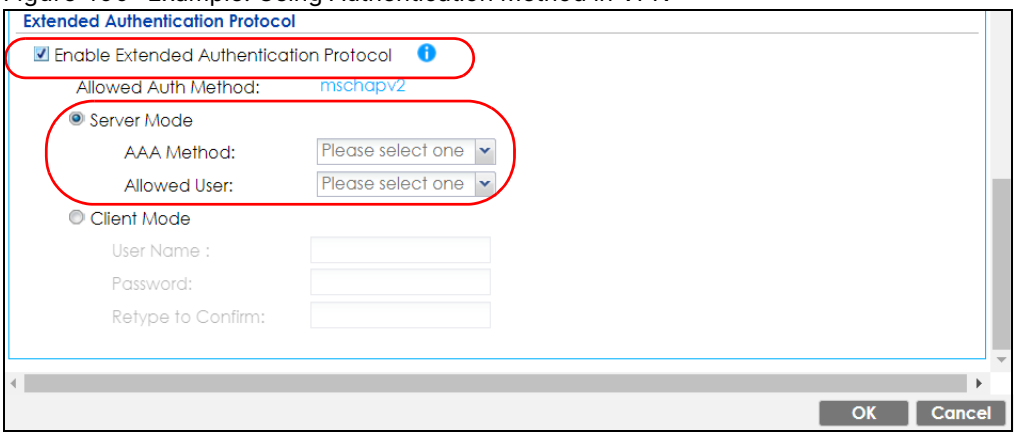
30.8.2 Example: Selecting a VPN Authentication Method

After you set up an authentication method object in the Auth. Method screens, you can use it in the VPN Gateway screen to authenticate VPN users for establishing a VPN connection. Refer to the chapter on VPN for more information.

Follow the steps below to specify the authentication method for a VPN connection.

1. Access the Configuration > VPN > IPSec VPN > VPN Gateway > Edit screen.
2. Click Show Advance Setting and select Enable Extended Authentication.
3. Select Server Mode and select an authentication method object from the drop-down list box.
4. Click OK to save the settings.

Figure 490 Example: Using Authentication Method in VPN

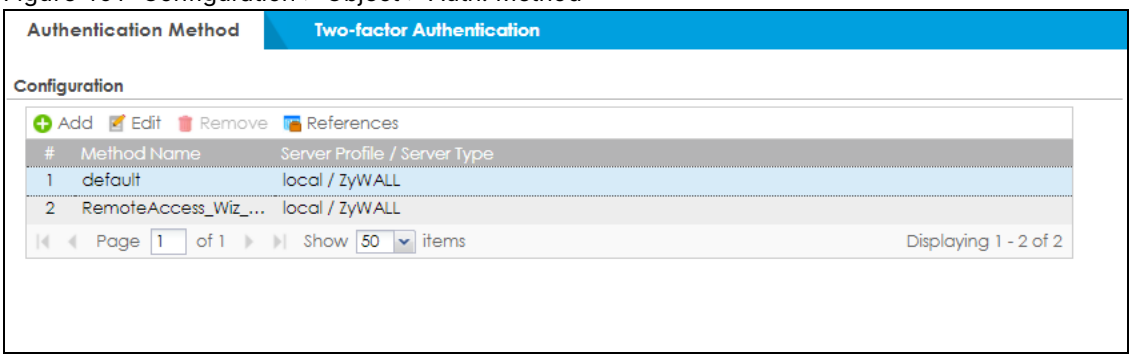


30.8.3 Authentication Method Objects

Click Configuration > Object > Auth. Method to display the screen as shown.

Note: You can create up to 16 authentication method objects.

Figure 491 Configuration > Object > Auth. Method



The following table describes the labels in this screen.

Table 256 Configuration > Object > Auth. Method

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click References to open a screen that shows which settings use the entry.
#	This field displays the index number.
Method Name	This field displays a descriptive name for identification purposes.
Server Profile/ Server Type	This field displays the authentication method(s) for this entry.

30.8.3.1 Creating an Authentication Method Object

Follow the steps below to create an authentication method object.

1 Click Configuration > Object > Auth. Method.

2 Click Add.

3 Specify a descriptive name for identification purposes in the Name field. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. For example, “My_Device”.

4 Click Add to insert an authentication method in the table.

5 Select a server object from the Method List drop-down list box.

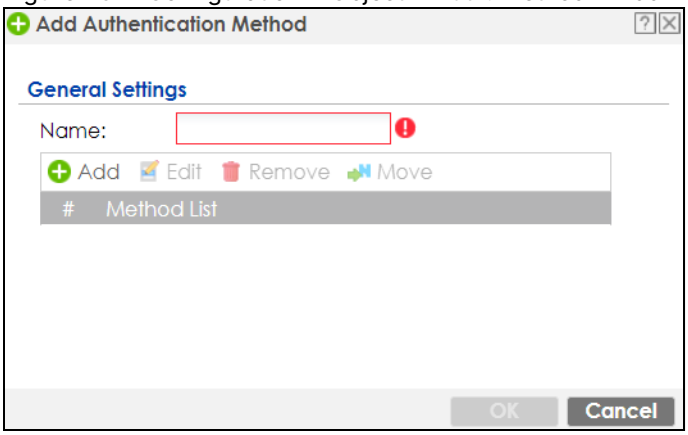
6 You can add up to four server objects to the table. The ordering of the Method List column is important. The Zyxel Device authenticates the users using the databases (in the local user database or the external authentication server) in the order they appear in this screen.

If two accounts with the same username exist on two authentication servers you specify, the Zyxel Device does not continue the search on the second authentication server when you enter the username and password that doesn’t match the one on the first authentication server.

Note: You can NoT select two server objects of the same type.

7 Click OK to save the settings or click Cancel to discard all changes and return to the previous screen.

Figure 492 Configuration > Object > Auth. Method > Add



The following table describes the labels in this screen.

Table 257 Configuration > Object > Auth. Method > Add

LABEL	DESCRIPTION
Name	Specify a descriptive name for identification purposes. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. For example, “My_Device”.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry’s settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.

Table 257 Configuration > Object > Auth. Method > Add (continued)

LABEL	DESCRIPTION
Move	To change a method's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed. The ordering of your methods is important as Zyxel Device authenticates the users using the authentication methods in the order they appear in this screen.
#	This field displays the index number.
Method List	Select a server object from the drop-down list box. You can create a server object in the AAA Server screen. The Zyxel Device authenticates the users using the databases (in the local user database or the external authentication server) in the order they appear in this screen. If two accounts with the same username exist on two authentication servers you specify, the Zyxel Device does not continue the search on the second authentication server when you enter the username and password that doesn't match the one on the first authentication server.
OK	Click OK to save the changes.
Cancel	Click Cancel to discard the changes.

30.8.4 Two-Factor Authentication

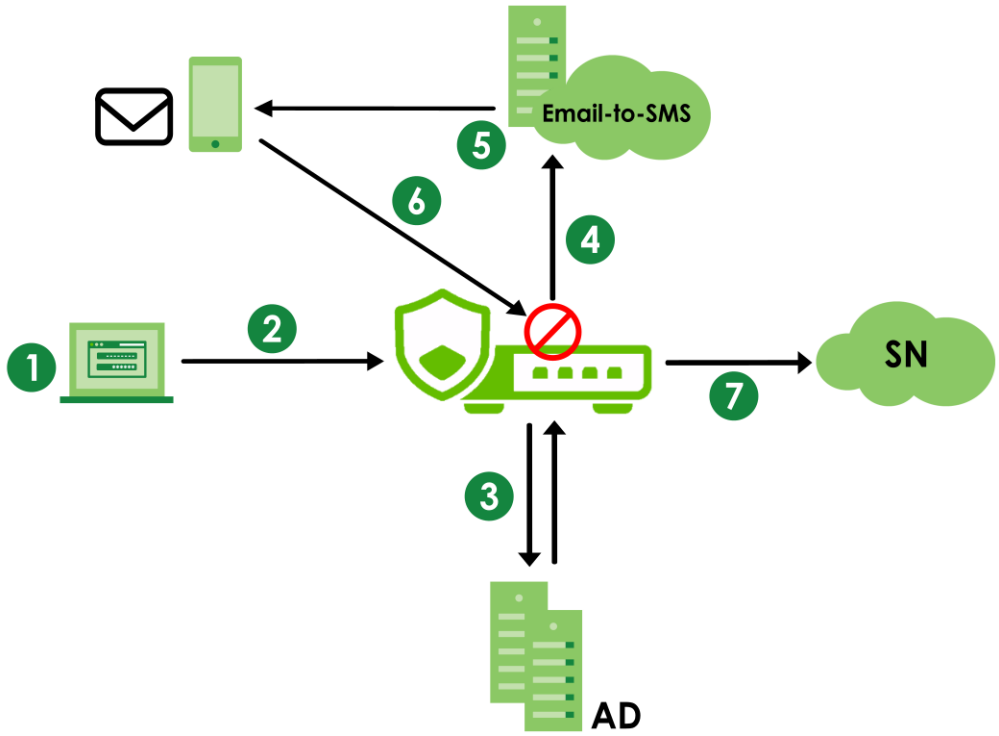
Use two-factor authentication to have double-layer security to access the Zyxel Device through a VPN tunnel, Web Configurator, SSH, or Telnet.

The first layer is the VPN client/Zyxel Device's login user name / password and the second layer is an authorized SMS (through mobile phone number) or email address.

30.8.4.1 Overview

This section introduces how two-factor authentication works.

Figure 493 Two-Factor Authentication



VPN Access Through a VPN Tunnel

1 A user runs a VPN client and logs in with the user name and password for this VPN tunnel.

2 The VPN client connects to the Zyxel Device and authenticates using the specified username and password.

3 The Zyxel Device requests the user's user-name, password and mobile phone number or email address from the Active Directory (AD), RADIUS server or local Zyxel Device database in order to authenticate this user (factor 1). If they are not found, then the Zyxel Device terminates the connection.

4 If all correct credentials are found, then the Zyxel Device performs one of the following actions:

- Emails an authorization link to the admin user
- Requests that the Email-to-SMS cloud system send an SMS with the authorization link

5 The client must open the authorization link or enter the authorization code within a specified deadline (Valid Time).

6 If the authorization is correct and received on time, then the client can access the secured network (SN) through the VPN tunnel. If the authorization deadline has expired, then the client has to log into the Zyxel Device again. If authorization credentials are incorrect or if the SMS/email was not received, then the client should contact the network administrator.

Admin Access Through the Web Configurator, SSH, or Telnet

1 An admin user connects to the Zyxel Device through the Web Configurator, SSH, or Telnet.

2 The Zyxel Device requests the admin user's user-name, password and mobile phone number or email address from the Active Directory (AD), RADIUS server or local Zyxel Device database in order to authenticate this admin user.

3 If all correct credentials are found, then the Zyxel Device performs one of the following actions:
   - Requests the Google Authenticator code
   - Emails an authorization link or code to the admin user
   - Requests that the Email-to-SMS cloud system send an SMS with an authorization link or code

4 The admin user must open the authorization link or enter the authorization code within a specified deadline (Valid Time).

5 If the authorization is correct and received on time, then the admin user can log into Zyxel Device. If the authorization deadline has expired, then the admin user has to log in again. If authorization credentials are incorrect code was received, then the admin user should contact the network administrator.

30.8.4.2 Pre-configuration

Before configuration, you must:

- Set up the user's user-name, password and email address or mobile number in the Active Directory, RADIUS server or local Zyxel Device database
- Enable Two-factor Authentication in Object > User/Group > User > Edit > Two-factor Authentication for a specific user
- Enable Two-factor Authentication in Object > Auth. Method > Two-factor Authentication for the Zyxel Device
- Enable HTTP and/or HTTPS in System > WWW > Service Control
- Enable SSH and/or Telnet in System > SSH and/or System > TELNET
- Add HTTP, HTTPS, SSH, and/or, TELNET in the Object > Service > Service Group > Default_Allow_WAN_To_ZyWALL service group. This service group defines the default services allowed in the WAN_to_Device security policy.
- For VPN access, configure the VPN tunnel for this user on the Zyxel Device

Email Authentication

- Configure Mail Server in System > Notification > Mail Server.

SMS Authentication

- Configure Mail Server in System > Notification > Mail Server.
- Configure SMS in System > Notification > SMS.
- Have an account with an Email-to-SMS cloud provider to be able to send SMS authorization requests

Google Authentication

- Install Google Authenticator

Two-Factor authentication will fail under the following conditions:

- You omit any of the pre-configuration items. Make sure to perform all pre-configuration items.

- The user cannot receive the authorization SMS or email. Make sure the mobile telephone number or email address of the user in the Active Directory, RADIUS Server or local Zyxel Device database is configured correctly.
- Email-to-SMS cloud system authentication fails. Make sure that SMS is enabled and credentials are correct in System > Notification > SMS.
- Mail server authentication fails. Make sure the System > Notification > Mail Server settings are correct.
- Authorization times out. Extend the Valid Time in Configuration > Object > Auth. Method > Two-factor Authentication > VPN Access.
- You are unable to access Google Authenticator (you lost your phone or uninstalled the app). Log in using one of the backup codes.
- You get a Google Authenticator verification error. You must enter the code within the time displayed in Google Authenticator. The time on your cellphone and the time on the Zyxel Device must be the same.

Google Authenticator Settings

The following is a list of specifications and limitations on using Google Authenticator for two-factor authentication.

- Ext-users (authenticated by external servers) are not supported.
- A user must setup Google Authenticator on their mobile device before they can successfully authenticate with the Zyxel Device.
- Verification code length: 6 digits.
- Maximum verification code failed attempts: 3
- Backup code length: 8 digits
- Google authenticator is supported in device High Availability (HA) mode. The secret keys are synchronized between all Zyxel Devices.

You can configure two-factor authentication for non-VPN and non-admin users in web authentication.

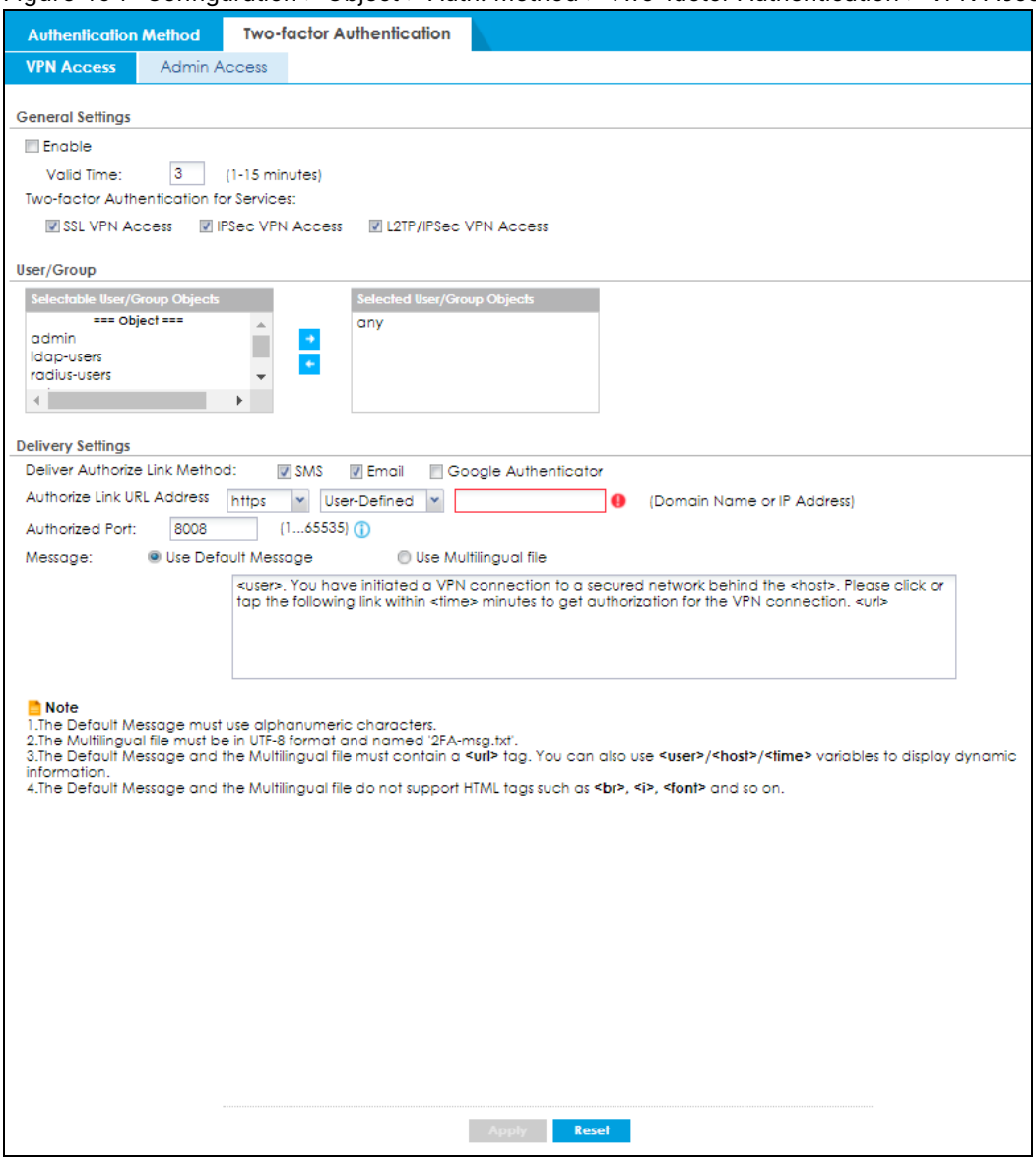
Note: The admin two-factor authentication settings override the web authentication two-factor authentication settings if both are configured.

30.8.5 Two-Factor Authentication VPN Access

Use this screen to select the users and VPN services that requires two-factor authentication.

Go to Configuration > Object > Auth. Method > Two-factor Authentication > VPN Access and configure the following screen as shown.

Figure 494 Configuration > Object > Auth. Method > Two-factor Authentication > VPN Access



The following table describes the labels in this screen.

Table 258 Configuration > Object > Auth. Method > Two-factor Authentication > VPN Access

LABEL	DESCRIPTION
General Settings	
Enable	Select the checkbox to require double-layer security to access the Zyxel Device through a VPN tunnel.
Valid Time	Enter the maximum time (in minutes) that the user must tap or click the authorization link in the SMS or email in order to get authorization for the VPN connection.
Two-factor Authentication for Services:	Select which kinds of VPN tunnels require Two-Factor Authentication. You should have configured the VPN tunnel first. • SSL VPN Access • IPSec VPN Access • L2TP/IPSec VPN Access

Table 258 Configuration > Object > Auth. Method > Two-factor Authentication > VPN (continued)Access

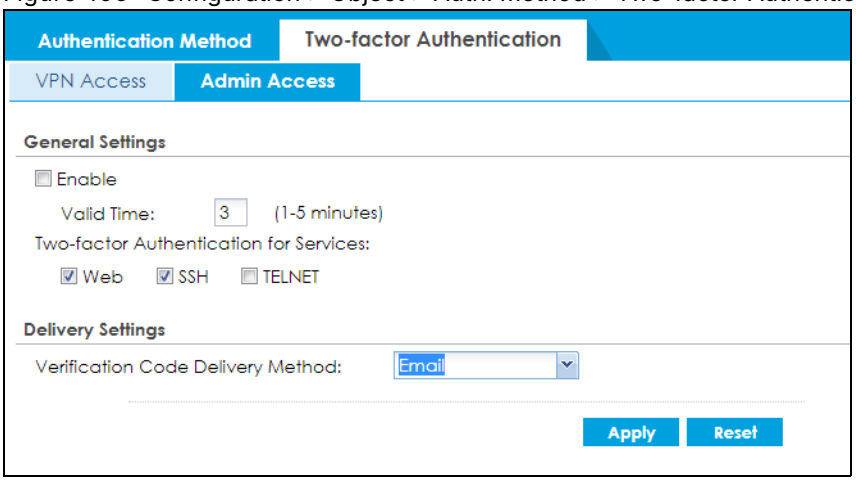
LABEL	DESCRIPTION
User/Group	This list displays the names of the users and user groups that can be selected for two-factor authentication. The order of members is not important. Select users and groups from the Selectable User/Group Objects list that require two-factor authentication for VPN access to a secured network behind the Zyxel Device and move them to the Selected User/Group Objects list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Similarly, move user/groups that do not you do not require two-factor authentication back to the Selectable User/Group Objects list.
Delivery Settings	Use this section to configure how to send an SMS or email for authorization.
Deliver Authorize Link Method:	The second factor authentication is done by sending a URL link by text (SMS) or email, or using Google Authenticator. Select one or up to three methods. You will get a URL link by text and email, and a authentication code for Google Authenticator if you select all three methods. Log in to the Zyxel Device by either clicking the URL in the text or email you received, or enter the authentication code in Google Authenticator. • SMS: Object > User/Group > User must contain a valid mobile telephone number. A valid mobile telephone number can be up to 20 characters in length, including the numbers 1~9 and the following characters in the square brackets [+*#()-]. • Email: Object > User/Group > User must contain a valid email address. A valid email address must contain the @ character. For example, this is a valid email address: abc@example.com • Google Authenticator: You must first set up your Zyxel Device on the Google Authenticator app in Configuration > Object > User/Group > User > Add > Two-factor Authentication; see Section 30.3.4 on page 686 for more information. Then enter a time-limited code from the Google Authenticator app.
Authorize Link URL Address:	Configure the link that the user will receive in the SMS or email. The user must be able to access the link. • http/https: you must enable HTTP or HTTPS in System > WWW > Service Control • From Interface/User-Defined: select the Zyxel Device WAN interface (wan1/2) or select User-Defined and then enter an IP address.
Authorized Port	Configure a new port between 1024 to 65535 that is not in use by other services. Use this port for two-factor authentication of VPN clients to access the network behind the Zyxel Device. VPN clients do not need to change the port number on their devices, because the link to access the network behind the Zyxel Devices will contain the new port number. For example, if you change this to port 8008 and the link is using a.b.c.d, then VPN clients will see this link in their email or SMS to retrieve settings: https://a.b.c.d:8008.
Message	You can either create a default message in the text box or upload a message file (Use Multilingual file) from your computer. The message file must be named '2FA-msg.txt' and be in UTF-8 format. To create the file, click Download the default 2FA-msg.txt example and edit the file for your needs. (If you make a mistake, use Restore Customized File to Default to restore your customized file to the default.) Use Select a File Path to locate the final file on your computer and then click Upload to transfer it to the Zyxel Device. The message in either the text box or the file must contain the <url> variable within angle brackets, while the <user>, <host>, and <time> variables are optional.
Apply	Click Apply to save the changes.
Reset	Click Reset to return the screen to its last-saved settings.

30.8.6 Two-Factor Authentication Admin Access

Use this screen to select the service (Web, SSH, and TELNET) that requires two-factor authentication for the admin user.

Go to Configuration > Object > Auth. Method > Two-factor Authentication > Admin Access and configure the following screen as shown.

Figure 495 Configuration > Object > Auth. Method > Two-factor Authentication > Admin Access



The following table describes the labels in this screen.

Table 259 Configuration > Object > Auth. Method > Two-factor Authentication > Admin Access

LABEL	DESCRIPTION
General Settings	
Enable	Select the checkbox to require double-layer security to access the Zyxel Device through the Web Configurator, SSH, or Telnet.
Valid Time	Enter the maximum time (in minutes) that the user must click or tap the authorization link in the SMS or email in order to get authorization for logins through the Web Configurator, SSH, or Telnet.
Two-factor Authentication for Services:	Select which services require Two-Factor Authentication for the admin user. • Web • SSH • TELNET
Delivery Settings	Use this section to configure how to send an SMS or email for authorization.
Verification Code Delivery Method	Select one or both (All) methods: • SMS: Object > User/Group > User must contain a valid mobile telephone number. A valid mobile telephone number can be up to 20 characters in length, including the numbers 1~9 and the following characters in the square brackets [+*#()-]. • Email: Object > User/Group > User must contain a valid email address. A valid email address must contain the @ character. For example, this is a valid email address: abc@example.com
Apply	Click Apply to save the changes.
Reset	Click Reset to return the screen to its last-saved settings.

30.8.7 Example: Admin Login with Two-factor Authentication by SMS

Email-to-SMS service allows you to convert an email to a SMS message with an authentication code that is used for two-factor authentication login to the Zyxel Device. The user can receive an SMS message even if he has no Internet connection.

1 First subscribe for an Email-to-SMS service. Enter the email address which will send email to the Email-to-SMS service.

2 Then, in the Zyxel Device web configurator, go to CONFIGURATION > System > Notification > SMS and enter the SMS Provider Email server domain name in Provider Domain, and the sender's email address in Mail From.

3 Next, go to CONFIGURATION > System > Notification > Mail to set up the following fields for the mail server:

- Mail server
- Mail server ports
- Mail From
- SMTP Authentication

4 Then go to Configuration > Object > User/Group > User > Add to create an admin type user. Enter the phone number for this user to receive SMS messages.

5 Next, set up two-factor authentication for this user in CONFIGURATION > Object > Auth Method > Two-Factor Authentication > Admin Access. Select which services, HTTPS (web), SSH and/or Telnet which requires Two-Factor authentication, and the user. Select SMS to send the verification code by SMS.

When this user logs into the Zyxel Device he will be asked to enter the verification code that was sent by SMS to his mobile phone.

30.9 Certificate Overview

The Zyxel Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

- Use the My Certificates screens (see Section 30.9.3 on page 748 to Section 30.9.3.3 on page 756) to generate and export self-signed certificates or certification requests and import the CA-signed certificates.
- Use the Trusted Certificates screens (see Section 30.9.4 on page 757 to Section 30.9.4.2 on page 761) to save CA certificates and trusted remote host certificates to the Zyxel Device. The Zyxel Device trusts any valid certificate that you have imported as a trusted certificate. It also trusts any valid certificate signed by any of the certificates that you have imported as a trusted certificate.

30.9.1 What You Need to Know

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available. The other key is private and must be kept secure.

These keys work like a handwritten signature (in fact, certificates are often referred to as "digital signatures"). Only you can write your signature exactly as it should look. When people know what your signature looks like, they can verify whether something was signed by you, or by someone else. In the same way, your private key "writes" your digital signature and your public key allows people to verify whether data was signed by you, or by someone else. This process works as follows.

1 Tim wants to send a message to Jenny. He needs her to be sure that it comes from him, and that the message content has not been altered by anyone else along the way. Tim generates a public key pair (one public key and one private key).

2 Tim keeps the private key and makes the public key openly available. This means that anyone who receives a message seeming to come from Tim can read it and verify whether it is really from him or not.

3 Tim uses his private key to sign the message and sends it to Jenny.

4 Jenny receives the message and uses Tim's public key to verify it. Jenny knows that the message is from Tim, and that although other people may have been able to read the message, no-one can have altered it (because they cannot re-sign the message with Tim's private key).

5 Additionally, Jenny uses her own private key to sign a message and Tim uses Jenny's public key to verify the message.

The Zyxel Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The Zyxel Device does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The Zyxel Device can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

Advantages of Certificates

Certificates offer the following benefits.

- The Zyxel Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

Self-signed Certificates

You can have the Zyxel Device act as a certification authority and sign its own certificates.

Factory Default Certificate

The Zyxel Device generates its own unique self-signed certificate when you first turn it on. This certificate is referred to in the GUI as the factory default certificate.

Certificate File Formats

Any certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.

- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The Zyxel Device currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.
- Binary PKCS#12: This is a format for transferring public key and private key certificates. The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the Zyxel Device.

Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

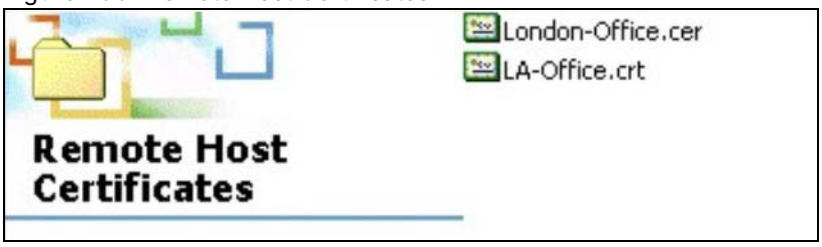
30.9.2 Verifying a Certificate

Before you import a trusted certificate into the Zyxel Device, you should verify that you have the correct certificate. You can do this using the certificate's fingerprint. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithm. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

1 Browse to where you have the certificate saved on your computer.

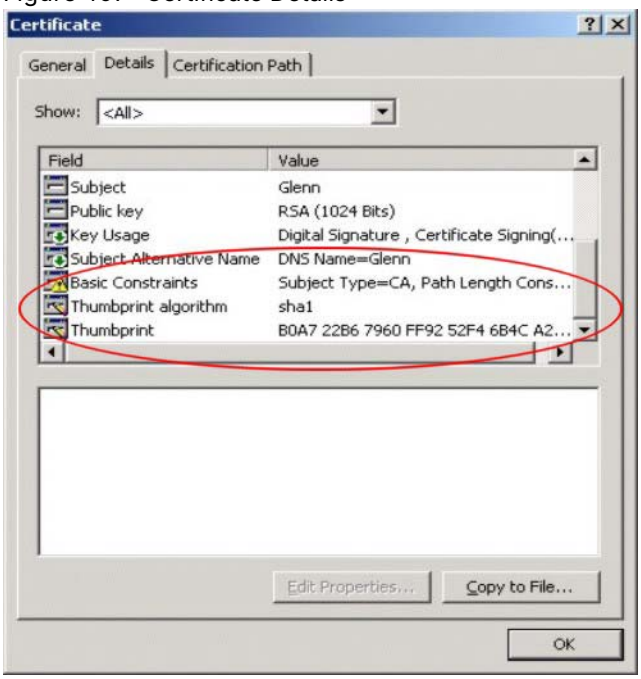
2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 496 Remote Host Certificates



3 Double-click the certificate's icon to open the Certificate window. Click the Details tab and scroll down to the Thumbprint Algorithm and Thumbprint fields.

Figure 497 Certificate Details

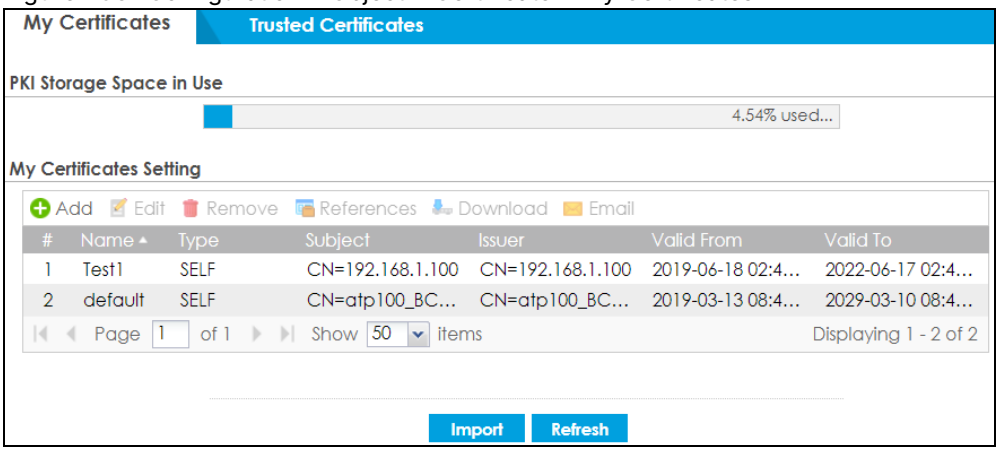


4 Use a secure method to verify that the certificate owner has the same information in the Thumbprint Algorithm and Thumbprint fields. The secure method may very based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

30.9.3 The My Certificates Screen

Click Configuration > Object > Certificate > My Certificates to open the My Certificates screen. This is the Zyxel Device's summary list of certificates and certification requests.

Figure 498 Configuration > Object > Certificate > My Certificates



The following table describes the labels in this screen.

Table 260 Configuration > Object > Certificate > My Certificates

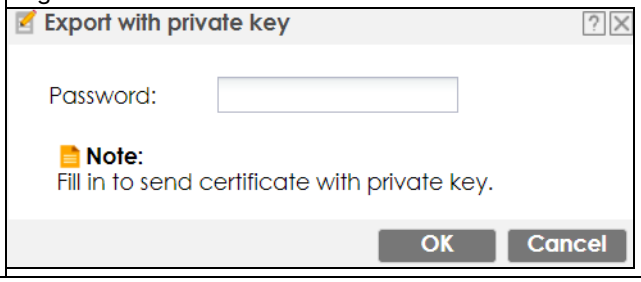
LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the Zyxel Device's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Add	Click this to go to the screen where you can have the Zyxel Device generate a certificate or a certification request.
Edit	Double-click an entry or select it and click Edit to open a screen with an in-depth list of information about the certificate.
Remove	The Zyxel Device keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so. Subsequent certificates move up by one when you take this action.
References	You cannot delete certificates that any of the Zyxel Device's features are configured to use. Select an entry and click References to open a screen that shows which settings use the entry.
Download	Click this and the following screen will appear. Type the selected certificate's password and save the selected certificate to your computer. Figure 499 Download a Certificate 

Table 260 Configuration > Object > Certificate > My Certificates (continued)

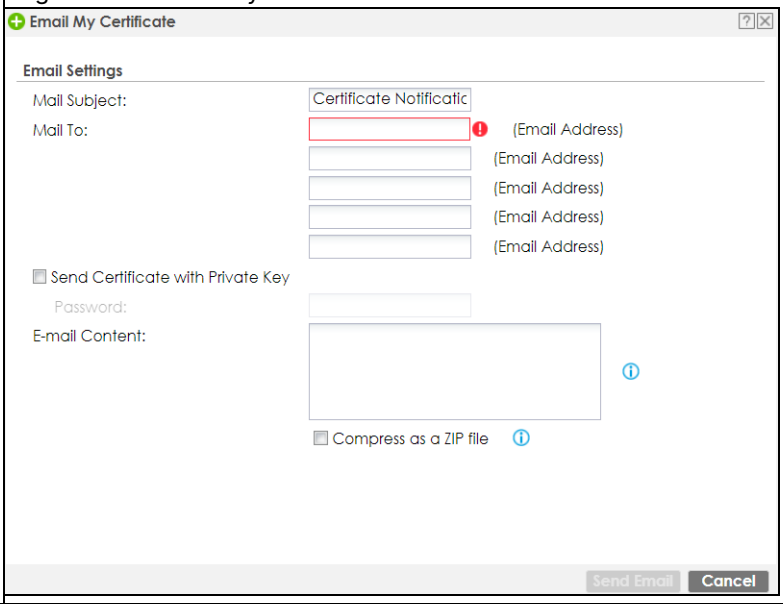
LABEL	DESCRIPTION
Email	Click this to email the selected certificate to the configured email address(es) for SSL connection establishment. This enables you to establish an SSL connection on your laptops, tablets, or smartphones. Click this and the following screen will appear. Here are the field descriptions: • Mail Subject: Type the subject line for outgoing email from the Zyxel Device. • Mail To: Type the email address (or addresses) to which the outgoing email is delivered. • Send Certificate with Private Key: Select the checkbox to send the selected certificate with a private key. • Password: Enter a private key of up to 31 keyboard characters for the certificate. The special characters listed in the brackets [;|`~!@#$%^&*()_+\\{}':,./<>=-"] are allowed. • E-mail Content: Create the email content in English, and use up to 250 keyboard characters. The special characters listed in the brackets [;\|`~!@#$%^&*()_+\\{}':,./<>=-"] are allowed. • Compress as a ZIP File: Select the checkbox to compress the selected certificate. Make sure the endpoint devices can decompress ZIP files before sending the compressed certificate. It's recommended to compress the certificate with a private key. Some email servers block PKCS #12 files. • Send Email: Click this to send the selected certificate. • Cancel: Click this to return to the previous screen without saving your changes. Figure 500 Email My Certificate 
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.

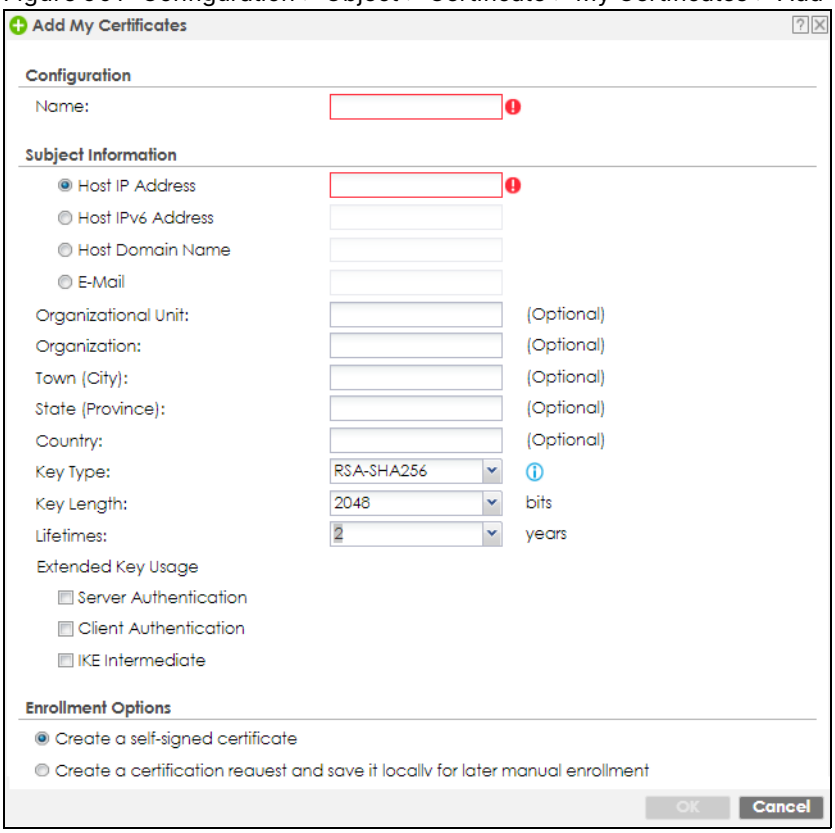
Table 260 Configuration > Object > Certificate > My Certificates (continued)

LABEL	DESCRIPTION
Type	This field displays what kind of certificate this is. REQ represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the My Certificate Import screen to import the certificate and replace the request. SELF represents a self-signed certificate. CERT represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Import	Click Import to open a screen where you can save a certificate to the Zyxel Device.
Refresh	Click Refresh to display the current validity status of the certificates.

30.9.3.1 The My Certificates Add Screen

Click Configuration > Object > Certificate > My Certificates and then the Add icon to open the My Certificates Add screen. Use this screen to have the Zyxel Device create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request.

Figure 501 Configuration > Object > Certificate > My Certificates > Add



The following table describes the labels in this screen.

Table 261 Configuration > Object > Certificate > My Certificates > Add

LABEL	DESCRIPTION
Name	Type a name to identify this certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although you must specify a Host IP Address, Host IPv6 Address, Host Domain Name, or E-Mail. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information. Select a radio button to identify the certificate's owner by IP address, domain name or email address. Type the IP address (in dotted decimal notation), domain name or email address in the field provided. The domain name or email address is for identification purposes only and can be any string. A domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods. An email address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore.
Organizational Unit	Identify the organizational unit or department to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Organization	Identify the company or group to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Town (City)	Identify the town or city where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.

Table 261 Configuration > Object > Certificate > My Certificates > Add (continued)

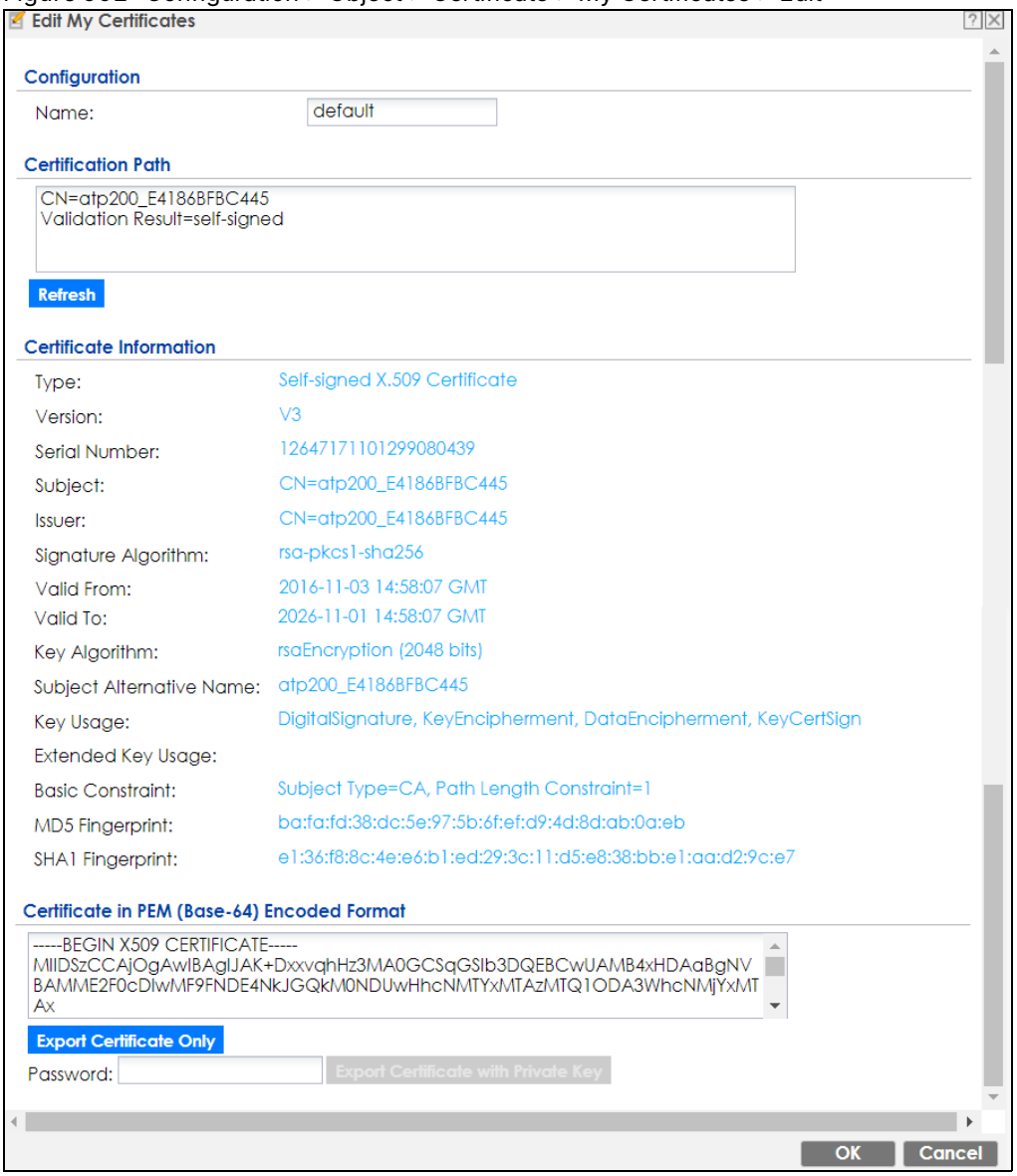
LABEL	DESCRIPTION
State, (Province)	Identify the state or province where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Country	Enter a two-letter country code to Identify the nation where the certificate owner is located.
Key Type	This sets the certificate's encryption algorithm and signature hash algorithm. Encryption algorithms: • RSA: Rivest, Shamir and Adleman public-key algorithm. • DSA: Digital Signature Algorithm public-key algorithm. • ECDSA: Elliptic Curve Digital Signature Algorithm. Signature hash algorithms: • SHA256 • SHA384 • SHA512 RSA and SHA256 are less secure but more compatible with different clients and applications. ECDSA and SHA512 are the more secure but less compatible.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (1024 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space. ECDSA keys are significant shorter than RSA and DSA keys, while offering equal or higher security.
LifeTimes	Select how long the certificate is valid. It can be valid from 2 to 10 years.
Extended Key Usage	
Server Authentication	Select this to have Zyxel Device generate and store a request for server authentication certificate.
Client Authentication	Select this to have Zyxel Device generate and store a request for client authentication certificate.
IKE Intermediate	Select this to have Zyxel Device generate and store a request for IKE Intermediate authentication certificate.
Create a self-signed certificate	Select this to have the Zyxel Device generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select this to have the Zyxel Device generate and store a request for a certificate. Use the My Certificate Details screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the My Certificate Details screen (see Section 30.9.3.2 on page 753) and then send it to the certification authority.
OK	Click OK to begin certificate or certification request generation.
Cancel	Click Cancel to quit and return to the My Certificates screen.

If you configured the My Certificate Create screen to have the Zyxel Device enroll a certificate and the certificate enrollment is not successful, you see a screen with a Return button that takes you back to the My Certificate Create screen. Click Return and check your information in the My Certificate Create screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the Zyxel Device to enroll a certificate online.

30.9.3.2 The My Certificates Edit Screen

Click Configuration > Object > Certificate > My Certificates and then the Edit icon to open the My Certificate Edit screen. You can use this screen to view in-depth certificate information and change the certificate's name.

Figure 502 Configuration > Object > Certificate > My Certificates > Edit



The following table describes the labels in this screen.

Table 262 Configuration > Object > Certificate > My Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
Certification Path	This field displays for a certificate, not a certification request. Click the Refresh button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The Zyxel Device does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click Refresh to display the certification path.

Table 262 Configuration > Object > Certificate > My Certificates > Edit (continued)

LABEL	DESCRIPTION
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the Zyxel Device.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O), State (ST), and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the Subject Name field. "none" displays for a certification request.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The Zyxel Device uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. "none" displays for a certification request.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired. "none" displays for a certification request.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the Zyxel Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or email address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Extended Key Usage	This field displays how the Zyxel Device generates and stores a request for server authentication, client authentication, or IKE Intermediate authentication certificate.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path. This field does not display for a certification request.
MD5 Fingerprint	This is the certificate's message digest that the Zyxel Device calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the Zyxel Device calculated using the SHA1 algorithm.

Table 262 Configuration > Object > Certificate > My Certificates > Edit (continued)

LABEL	DESCRIPTION
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form. You can copy and paste a certification request into a certification authority's web page, an email that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an email to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (through external storage device for example).
Export Certificate Only	Use this button to save a copy of the certificate without its private key. Click this button and then Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save.
Password	If you want to export the certificate with its private key, create a password and type it here. Make sure you keep this password in a safe place. You will need to use it if you import the certificate to another device.
Export Certificate with Private Key	Use this button to save a copy of the certificate with its private key. Type the certificate's password and click this button. Click Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save.
OK	Click OK to save your changes back to the Zyxel Device. You can only change the name.
Cancel	Click Cancel to quit and return to the My Certificates screen.

30.9.3.3 The My Certificates Import Screen

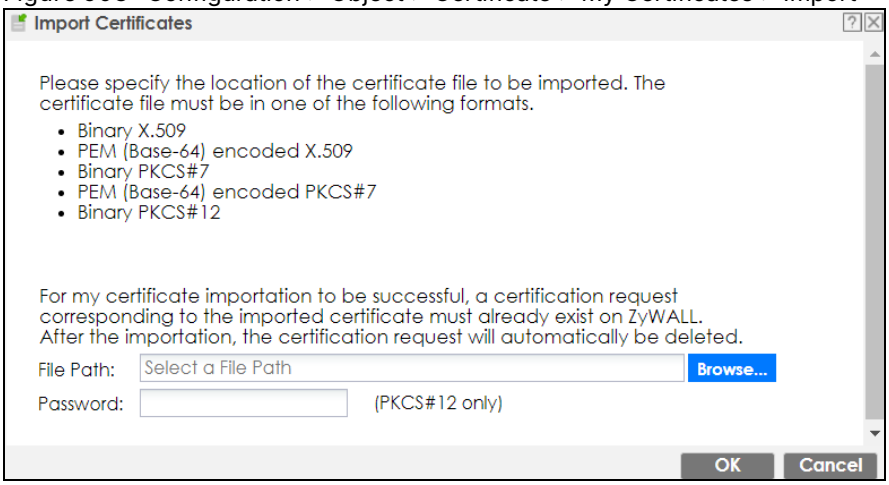
Click Configuration > Object > Certificate > My Certificates > Import to open the My Certificate Import screen. Follow the instructions in this screen to save an existing certificate to the Zyxel Device.

Note: You can import a certificate that matches a corresponding certification request that was generated by the Zyxel Device. You can also import a certificate in PKCS#12 format, including the certificate's public and private keys.

The certificate you import replaces the corresponding request in the My Certificates screen.

You must remove any spaces from the certificate's filename before you can import it.

Figure 503 Configuration > Object > Certificate > My Certificates > Import



The following table describes the labels in this screen.

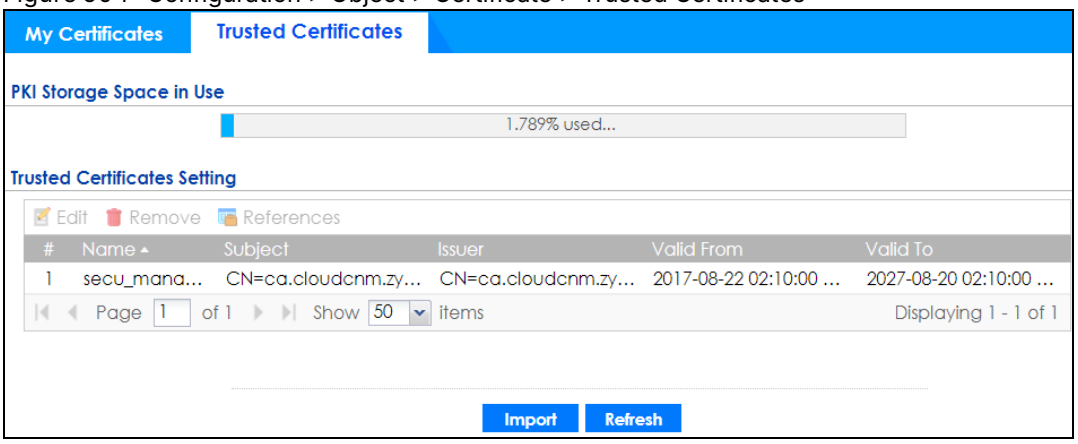
Table 263 Configuration > Object > Certificate > My Certificates > Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it. You cannot import a certificate with the same name as a certificate that is already in the Zyxel Device.
Browse	Click Browse to find the certificate file you want to upload.
Password	This field only applies when you import a binary PKCS#12 format file. Type the file's password that was created when the PKCS #12 file was exported.
OK	Click OK to save the certificate on the Zyxel Device.
Cancel	Click Cancel to quit and return to the My Certificates screen.

30.9.4 The Trusted Certificates Screen

Click Configuration > Object > Certificate > Trusted Certificates to open the Trusted Certificates screen. This screen displays a summary list of certificates that you have set the Zyxel Device to accept as trusted. The Zyxel Device also accepts any valid certificate signed by a certificate on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certificates.

Figure 504 Configuration > Object > Certificate > Trusted Certificates



The following table describes the labels in this screen.

Table 264 Configuration > Object > Certificate > Trusted Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the Zyxel Device's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Edit	Double-click an entry or select it and click Edit to open a screen with an in-depth list of information about the certificate.
Remove	The Zyxel Device keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so. Subsequent certificates move up by one when you take this action.
References	You cannot delete certificates that any of the Zyxel Device's features are configured to use. Select an entry and click References to open a screen that shows which settings use the entry.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.

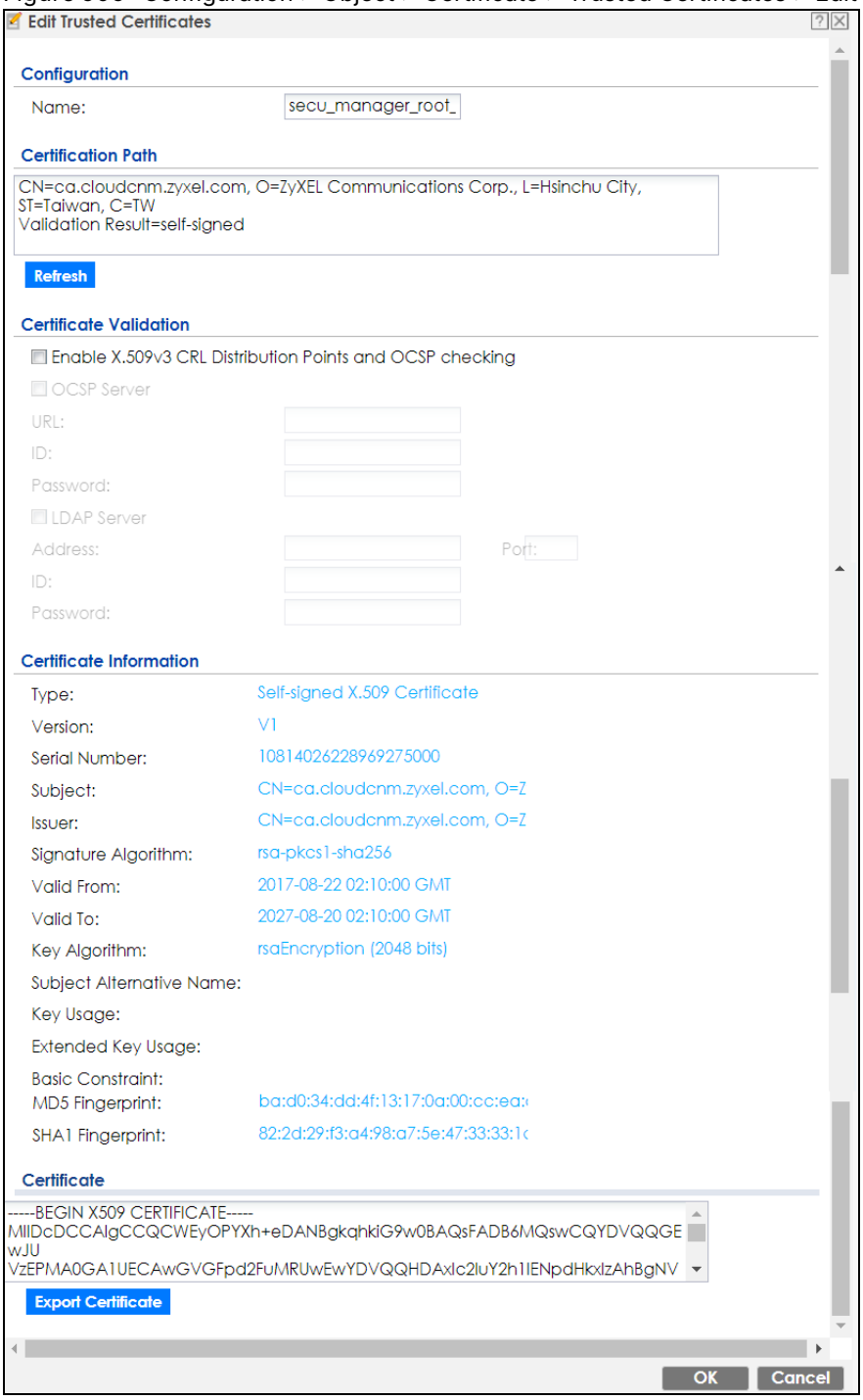
Table 264 Configuration > Object > Certificate > Trusted Certificates (continued)

LABEL	DESCRIPTION
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Import	Click Import to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the Zyxel Device.
Refresh	Click this button to display the current validity status of the certificates.

30.9.4.1 The Trusted Certificates Edit Screen

Click Configuration > Object > Certificate > Trusted Certificates and then a certificate's Edit icon to open the Trusted Certificates Edit screen. Use this screen to view in-depth information about the certificate, change the certificate's name and set whether or not you want the Zyxel Device to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Figure 505 Configuration > Object > Certificate > Trusted Certificates > Edit



The following table describes the labels in this screen.

Table 265 Configuration > Object > Certificate > Trusted Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can change the name. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
Certification Path	Click the Refresh button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certificate, it may be the only certification authority in the list (along with the end entity's own certificate). The Zyxel Device does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click Refresh to display the certification path.
Enable X.509v3 CRL Distribution Points and OCSP checking	Select this checkbox to turn on/off certificate revocation. When it is turned on, the Zyxel Device validates a certificate by getting Certificate Revocation List (CRL) through HTTP or LDAP (can be configured after selecting the LDAP Server checkbox) and online responder (can be configured after selecting the OCSP Server checkbox).
OCSP Server	Select this checkbox if the directory server uses OCSP (Online Certificate Status Protocol).
URL	Type the protocol, IP address and path name of the OCSP server.
ID	The Zyxel Device may need to authenticate itself in order to assess the OCSP server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the OCSP server (usually a certification authority).
LDAP Server	Select this checkbox if the directory server uses LDAP (Lightweight Directory Access Protocol). LDAP is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates.
Address	Type the IP address (in dotted decimal notation) of the directory server.
Port	Use this field to specify the LDAP server port number. You must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.
ID	The Zyxel Device may need to authenticate itself in order to assess the CRL directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the CRL directory server (usually a certification authority).
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the Subject Name field.

Table 265 Configuration > Object > Certificate > Trusted Certificates > Edit (continued)

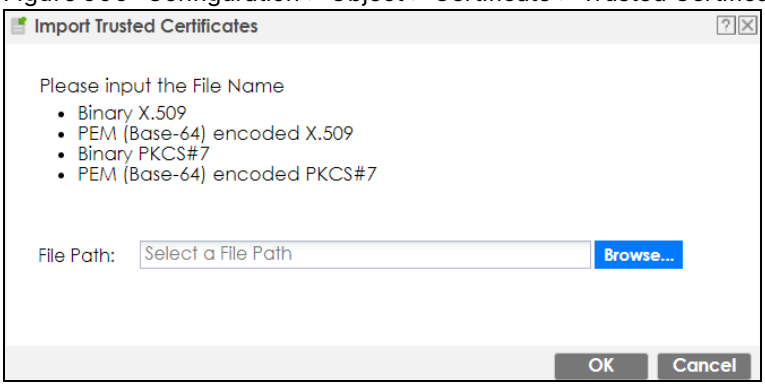
LABEL	DESCRIPTION
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the Zyxel Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or email address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Extended Key Usage	This field displays the method that the Zyxel Device generates and stores a request for server authentication, client authentication, or IKE Intermediate authentication certificate.Zyxel Device
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the Zyxel Device calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the Zyxel Device calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form. You can copy and paste the certificate into an email to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (through external storage device for example).
Export Certificate	Click this button and then Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save.
OK	Click OK to save your changes back to the Zyxel Device. You can only change the name.
Cancel	Click Cancel to quit and return to the Trusted Certificates screen.

30.9.4.2 The Trusted Certificates Import Screen

Click Configuration > Object > Certificate > Trusted Certificates > Import to open the Trusted Certificates Import screen. Follow the instructions in this screen to save a trusted certificate to the Zyxel Device.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 506 Configuration > Object > Certificate > Trusted Certificates > Import



The following table describes the labels in this screen.

Table 266 Configuration > Object > Certificate > Trusted Certificates > Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it. You cannot import a certificate with the same name as a certificate that is already in the Zyxel Device.
Browse	Click Browse to find the certificate file you want to upload.
OK	Click OK to save the certificate on the Zyxel Device.
Cancel	Click Cancel to quit and return to the previous screen.

30.9.5 Certificates Technical Reference

OCSP

OCSP (Online Certificate Status Protocol) allows an application or device to check whether a certificate is valid. With OCSP the Zyxel Device checks the status of individual certificates instead of downloading a Certificate Revocation List (CRL). OCSP has two main advantages over a CRL. The first is real-time status information. The second is a reduction in network traffic since the Zyxel Device only gets information on the certificates that it needs to verify, not a huge list. When the Zyxel Device requests certificate status information, the OCSP server returns a “expired”, “current” or “unknown” response.

30.10 ISP Account Overview

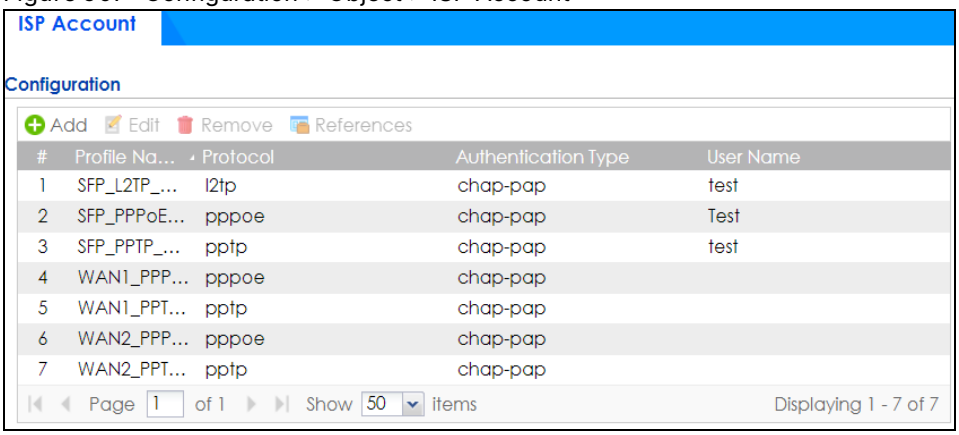
Use ISP accounts to manage Internet Service Provider (ISP) account information for PPPoE/PPTP/L2TP interfaces. An ISP account is a profile of settings for Internet access using PPPoE, PPTP or L2TP.

Use the Object > ISP Account screens (Section 30.10.1 on page 762) to create and manage ISP accounts in the Zyxel Device.

30.10.1 ISP Account Summary

This screen provides a summary of ISP accounts in the Zyxel Device. To access this screen, click Configuration > Object > ISP Account.

Figure 507 Configuration > Object > ISP Account



The following table describes the labels in this screen. See the ISP Account Add/Edit section below for more information as well.

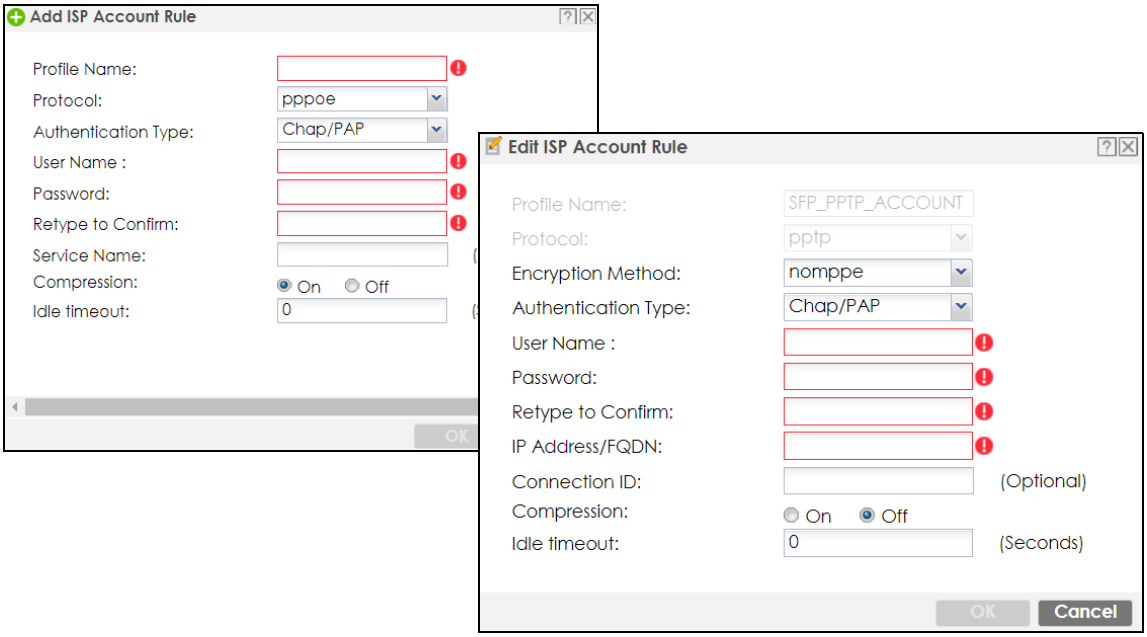
Table 267 Configuration > Object > ISP Account

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific entry.
Profile Name	This field displays the profile name of the ISP account. This name is used to identify the ISP account.
Protocol	This field displays the protocol used by the ISP account.
Authentication Type	This field displays the authentication type used by the ISP account.
User Name	This field displays the user name of the ISP account.

30.10.1.1 ISP Account Add/Edit

The ISP Account Add/Edit screen lets you add information about new accounts and edit information about existing accounts. To open this window, open the ISP Account screen. (See Section 30.10.1 on page 762.) Then, click on an Add icon or Edit icon to open the ISP Account Edit screen below.

Figure 508 Configuration > Object > ISP Account > Edit



The following table describes the labels in this screen.

Table 268 Configuration > Object > ISP Account > Edit

LABEL	DESCRIPTION
Profile Name	This field is read-only if you are editing an existing account. Type in the profile name of the ISP account. The profile name is used to refer to the ISP account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Protocol	This field is read-only if you are editing an existing account. Select the protocol used by the ISP account. Your ISP will provide you with a related username, password and IP (server) information. Options are: pppoe - This ISP account uses the PPPoE protocol. pptp - This ISP account uses the PPTP protocol. l2tp - This ISP account uses the L2TP protocol.
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.
Encryption Method	This field is available if this ISP account uses the PPTP protocol. Use the drop-down list box to select the type of Microsoft Point-to-Point Encryption (MPPE). Options are: nomppe - This ISP account does not use MPPE. mppe-40 - This ISP account uses 40-bit MPPE. mppe-128 - This ISP account uses 128-bit MMPE.
User Name	Type the user name given to you by your ISP.

Table 268 Configuration > Object > ISP Account > Edit (continued)

LABEL	DESCRIPTION
Password	Type the password associated with the user name above. The password can only consist of alphanumeric characters (A-Z, a-z, 0-9). This field can be blank. Your password will be encrypted when you configure this field.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
IP Address/FQDN	Enter the IP address or Fully-Qualified Domain Name (FQDN) of the PPTP or L2TP server.
Connection ID	This field is available if this ISP account uses the PPTP protocol. Type your identification name for the PPTP server. This field can be blank.
Service Name	If this ISP account uses the PPPoE protocol, type the PPPoE service name to access. PPPoE uses the specified service name to identify and reach the PPPoE server. This field can be blank. If this ISP account uses the PPTP protocol, this field is not displayed.
Compression	Select On button to turn on stac compression, and select Off to turn off stac compression. Stac compression is a data compression technique capable of compressing data by a factor of about four.
Idle Timeout	This value specifies the number of seconds that must elapse without outbound traffic before the Zyxel Device automatically disconnects from the PPPoE/PPTP server. This value must be an integer between 0 and 360. If this value is zero, this timeout is disabled.
OK	Click OK to save your changes back to the Zyxel Device. If there are no errors, the program returns to the ISP Account screen. If there are errors, a message box explains the error, and the program stays in the ISP Account Edit screen.
Cancel	Click Cancel to return to the ISP Account screen without creating the profile (if it is new) or saving any changes to the profile (if it already exists).

CHAPTER 31
Mgmt. & Analytics

31.1 Mgmt. & Analytics Overview

You need licenses to use Cloud CNM SecuManager You need the SecuManager license to get a CNM ID with which you can access the SecuManager server. It is independent from the Zyxel Devices.

Follow the instructions on the Nebula screen to pass your Zyxel Device management to Nebula. The screen you see may vary depending on the device you're using or the WAN settings you configured.

31.1.1 What You Can Do in this Chapter

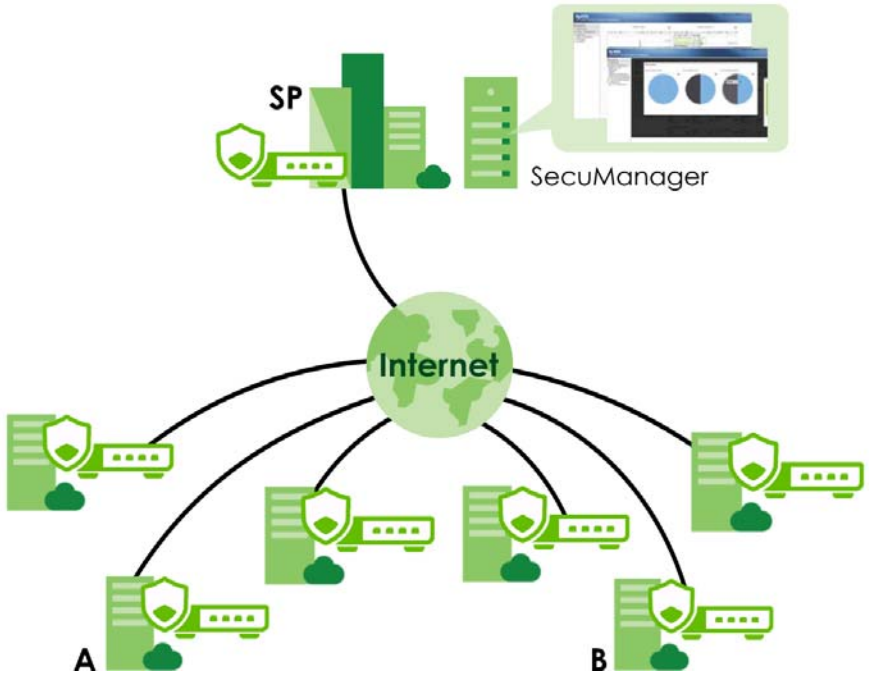
- Use the Mgmt. & Analytics > SecuManager screen (Section 31.2 on page 766) to enable and configure management of the Zyxel Device by a Central Network Management system.
- Use the Mgmt. & Analytics > SecuReporter screen (Section 31.3 on page 769) to enable SecuReporter logging on your Zyxel Device, see license status, type, expiration date and access a link to the SecuReporter web portal. The SecuReporter web portal collects and analyzes logs from your Zyxel Device in order to identify anomalies, alert on potential internal / external threats, and report on network usage.
- Use Mgmt. & Analytics > Nebula screen (Section 31.4 on page 773)to let Nebula manage your Zyxel Device remotely.

31.2 Cloud CNM SecuManager

Cloud CNM SecuManager is a Virtual Machine-based (VM) management system that uses the TR-069 protocol to encapsulate commands to the Zyxel Device devices for management and monitoring; these devices must have firmware that supports the TR-069 protocol.

In the following figure, SP is the management service provider, while A and B are sites with devices being managed by SP.

Figure 509 Cloud CNM SecuManager Example Network Topology



Cloud CNM SecuManager features include:

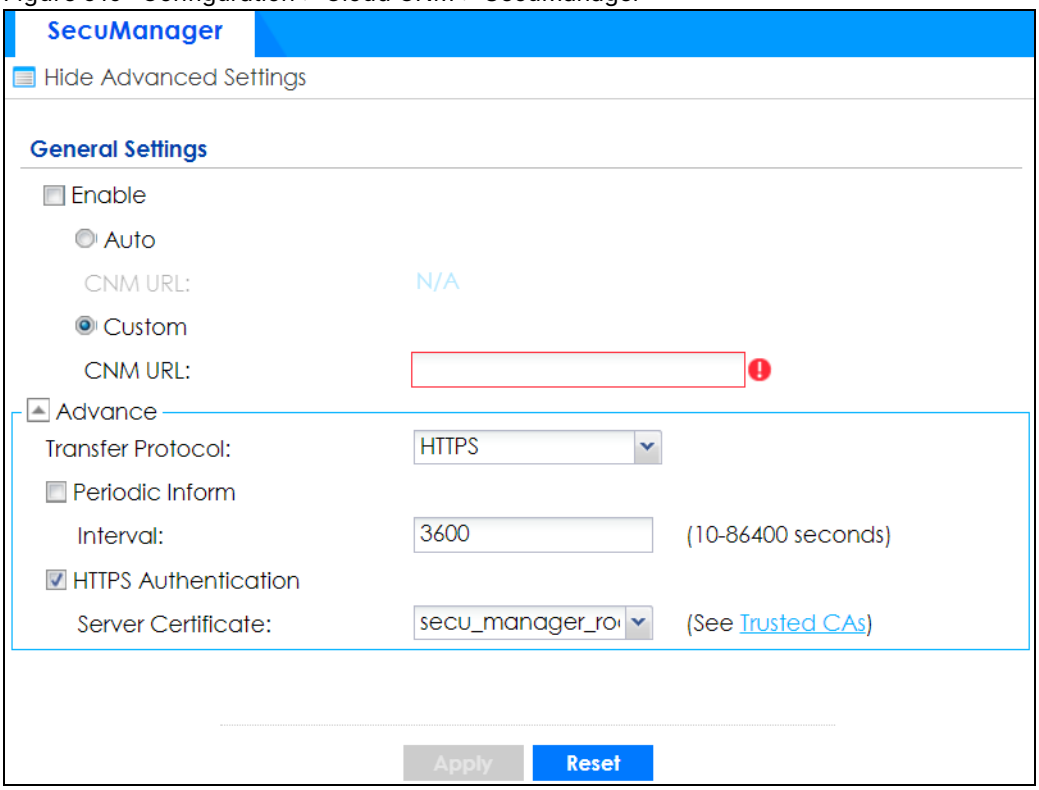
- Batch import of managed Zyxel Devices at one time using one CSV file
- See an overview of all managed Zyxel Devices and system information in one place
- Monitor and manage Zyxel Devices
- Install firmware to multiple Zyxel Devices of the same model at one time
- Backup and restore Zyxel Device configuration
- View the location of managed devices on a map

To allow Cloud CNM SecuManager management of your Zyxel Device:

- You must have a Cloud CNM SecuManager license with CNM ID number or a Cloud CNM SecuManager server URL.
- The Zyxel Device must be able to communicate with the Cloud CNM SecuManager server.

You must configure Configuration > Cloud CNM > SecuManager to allow the Zyxel Device to find the Cloud CNM SecuManager server.

Figure 510 Configuration > Cloud CNM > SecuManager



The following table describes the labels in this screen.

Table 269 Configuration > Cloud CNM > SecuManager

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Enable	Select this to allow management of the Zyxel Device by Cloud CNM SecuManager.
Auto	Select this if your Cloud CNM SecuManager server can access myZyxel to automatically get the VM server URL from myZyxel. You also need CNM ID from the Cloud CNM SecuManager license.
CNM URL	myZyxel associates the CNM ID with the CNM URL which identifies the server on which Cloud CNM SecuManager is installed. Therefore you don't need to enter the CNM URL when you select Auto.
Custom	Select this if your Cloud CNM SecuManager server cannot access myZyxel.
CNM URL	Select this if your VM server or Zyxel Device are in a private network, or if the VM server is behind a NAT router. You then need to manually enter the VM server URL into the Zyxel Device. Enter the IPv4 IP address of the Cloud CNM SecuManager server followed by the port number (default 7547 for HTTPS or 7549 for HTPP) followed by the CNM ID from the license in CNM URL. For example, if you installed Cloud CNM SecuManager on a server with IP address 1.1.1.1 and CNM ID V6ABQNTPYGD, then type `1.1.1.1:7547/V6ABQNTPYG` or `1.1.1.1:7549/V6ABQNTPYG` as the CNM URL.
Transfer Protocol	Choose the CNM URL protocol: HTTP or HTTPS. If you enter 1.1.1.1:7547 as the CNM URL, you must choose HTTPS as the Transfer Protocol, and then the whole CNM URL is https://1.1.1.1:7547. If you enter 1.1.1.1:7549 as the CNM URL, you must choose HTTP as the Transfer Protocol, and then the whole CNM URL is http://1.1.1.1:7549.
Periodic Inform	Enable this to have the Zyxel Device inform the Cloud CNM SecuManager server of its presence at regular intervals.

Table 269 Configuration > Cloud CNM > SecuManager (continued)

LABEL	DESCRIPTION
Interval	Type how often the Zyxel Device should inform Cloud CNM SecuManager server of its presence.
HTTPS Authentication	Select the checkbox if you have a HTTPS server certificate.
Server Certificate	Select a certificate the HTTPS server (the Zyxel Device) uses to authenticate itself to the HTTPS client.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

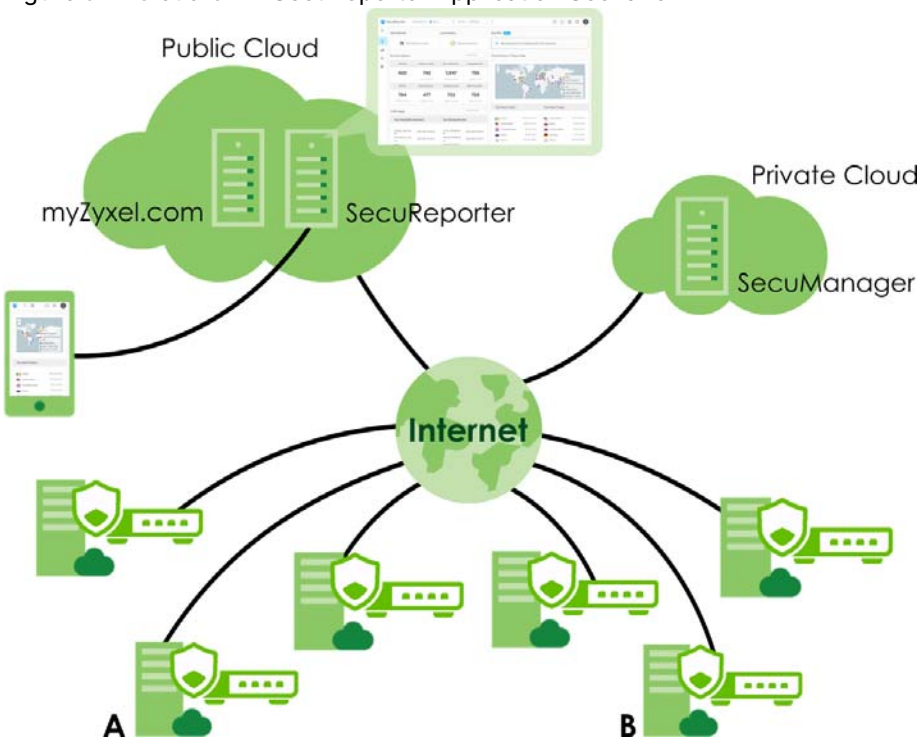
Note: See the Cloud CNM SecuManager User's Guide for more information on Cloud CNM SecuManager.

31.3 Cloud CNM SecuReporter

Cloud CNM SecuReporter is a security analytics portal that collects and analyzes logs from SecuReporter-licensed Zyxel Devices in order to identify anomalies, alert on potential internal / external threats, and report on network usage. You need to buy a license for SecuReporter for your Zyxel Device and register it at myZyxel. You must be a registered user at myZyxel.

You can access the portal from a web browser and also get notifications sent to an app on your mobile phone.

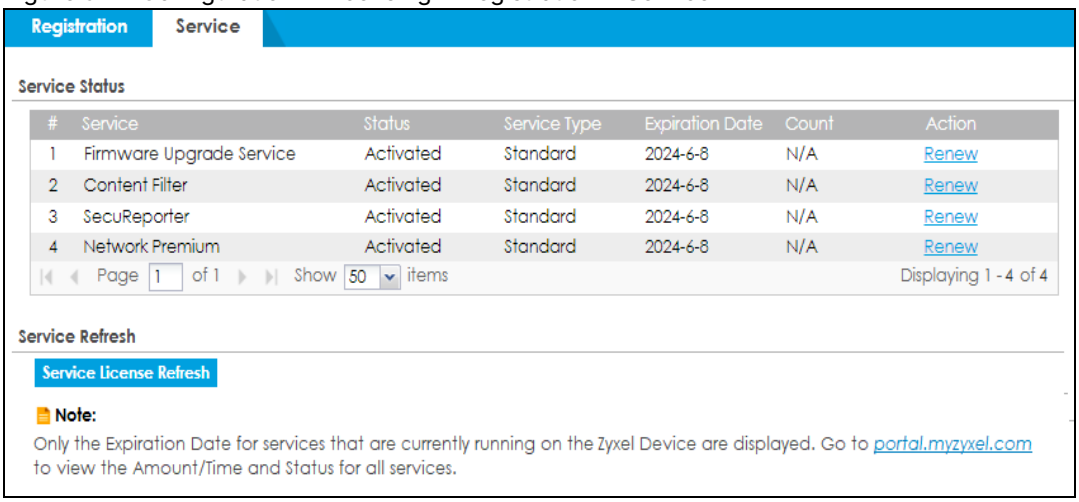
Figure 511 Cloud CNM SecuReporter Application Scenario



How to activate and enable SecuReporter

1 Does Service Status displays Activated in the Configuration > Cloud CNM > SecuReporter screen? If not, you have to log in to myZyxel.com and activate the SecuReporter license for this Zyxel Device. The Zyxel Device must be able to communicate with the myZyxel server.
Your SecuReporter license displays in Configuration > Licensing > Registration > Service after you activate the SecuReporter license at myZyxel.

Figure 512 Configuration > Licensing > Registration > Service



2 After the SecuReporter license is activated, go back to the Configuration > Cloud CNM > SecuReporter screen, and select the categories of logs that you want this Zyxel Device to send to the SecuReporter portal.

3 Select Enable SecuReporter. Do not go to the SecuReporter portal until after you have enabled SecuReporter on this Zyxel Device and applied the settings. You can also see license status, type, expiration date.

4 Click Apply and wait.

How to add this Zyxel Device to SecuReporter

1 Log in to the SecuReporter portal.

2 Go to Settings > Organization & Devices > Add to create an organization.

3 Add this Zyxel Device to an Organization using the hyper link under Unclaimed Device.

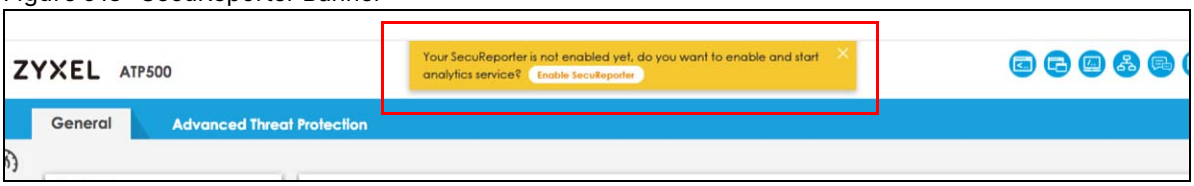
SecuReporter Banner

The SecuReporter banner appears when:

1 SecuReporter hasn't been enabled before.

2 The Zyxel Device is not added to an organization yet.

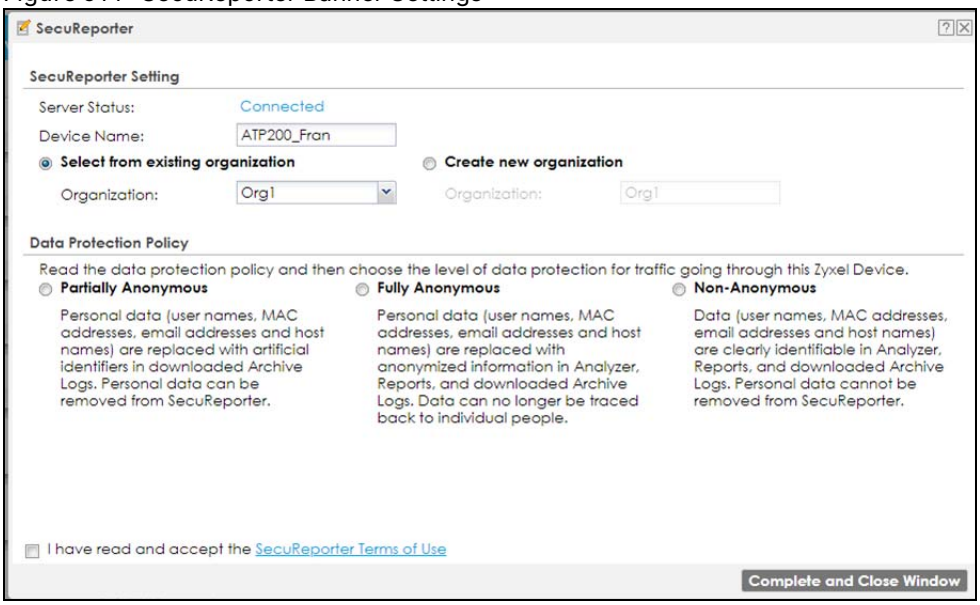
Figure 513 SecuReporter Banner



Click the Continue button in the SecuReporter banner to configure the SecuReporter settings.

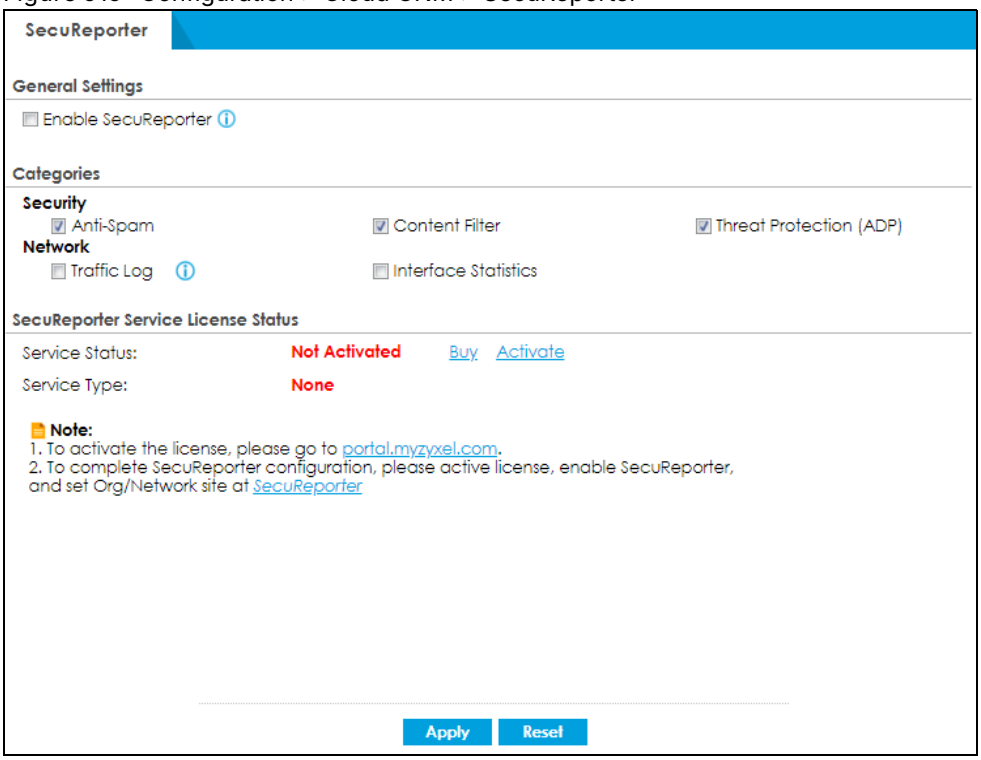
- Server Status: This is the connection status between the Zyxel Device and the SecuReporter server. This field shows Connected when the Zyxel Device can synchronize with the SecuReporter server. This field shows Timeout when the Zyxel Device can't synchronize with the SecuReporter server. This field 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 514 SecuReporter Banner Settings



Click Configuration > Cloud CNM > SecuReporter to open the following screen.

Figure 515 Configuration > Cloud CNM > SecuReporter



The following table describes the labels in this screen.

Table 270 Configuration > Cloud CNM > SecuReporter

LABEL	DESCRIPTION
Enable SecuReporter	Security-related logs are sent to the SecuReporter portal. Click the General Data Protection Regulation (GDPR) privacy link below to see the Zyxel privacy policy. This must be selected to have SecuReporter collect and analyze logs from this Zyxel Device. • It's selected by default if you have activated a SecuReporter Standard license, • You need to select this if you have a SecuReporter Trial license. • This field is not available if you do not have a SecuReporter license.
Categories	Select the categories of logs that you want this Zyxel Device to send to SecuReporter for analysis and trend spotting.
SecuReporter Service License Status	
Service 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.
Service Type	This field displays whether you applied for a trial application (Trial) or registered this service with your iCard's PIN number (Standard). This field is blank when the service is not activated.
Expiration Date	This field displays the date your service expires.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

31.4 Nebula

Select Cloud Monitoring Mode to monitor your Zyxel Device using Nebula Control Center (NCC) but configure your Zyxel Device in On Premises Mode using the web configurator/CLI at the same time. You can allow remote access to the web configurator remotely using reverse SSH or HTTPS tunnel.

Note: You cannot set the Zyxel Device to Cloud Monitoring Mode if Device HA is enabled on the Zyxel Device.

Select Cloud Mode to manage your Zyxel Device using Nebula only. Use this mode to manage your Zyxel Device with accounts at different privilege levels. You can also manage your Zyxel Device licenses and check status through Nebula.

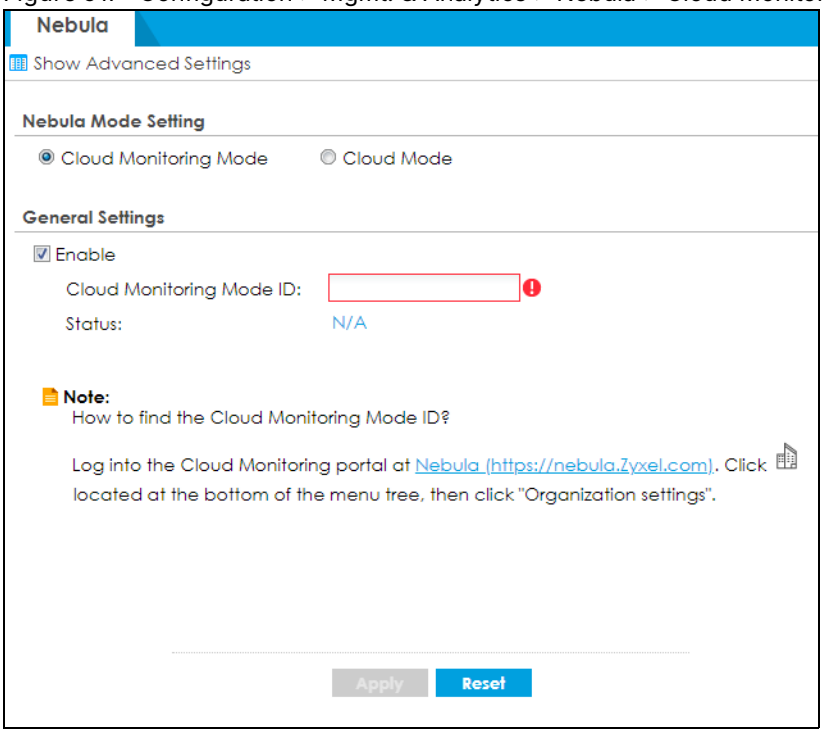
Your Zyxel Device uses Native Mode to register with Nebula. See Section 31.4.2 on page 775 for more information on registering your Zyxel Device with Nebula using Native Mode.

31.4.1 Cloud Monitoring Mode

You must have created an organization and a site on Nebula first. Follow the steps below to set the Zyxel Device to Cloud Monitoring Mode.

Figure 516 Cloud Monitoring Mode Example

Figure 517 Configuration > Mgmt. & Analytics > Nebula > Cloud Monitoring Mode



On Premises Mode to Cloud Monitoring Mode

1 Back up the Zyxel Device configurations.

2 Select Cloud Monitoring Mode in Configuration > Mgmt. & Analytics > Nebula, then select Enable.

3 Enter the Monitor mode ID of an organization you created on Nebula. See the organization Monitor mode ID on Nebula in Organization-wide > Organization-wide manage > Organization settings.

4 Click Apply. Check the result in the Status field.

The following table explains the possible results that might display in the Status field.

Table 271 Cloud Monitoring Mode Status

N/A	You've not entered a Monitor mode ID on the Zyxel Device.
Connected	The Zyxel Device is connected to Nebula. Check the Zyxel Device Device Type on Nebula in Organization-wide > License & inventory.
Disconnected - Server is not reachable	The Zyxel Device cannot connect to Nebula. Please make sure the Zyxel Device can access Nebula at *.nebula.zyxel.com and ports 443, 4335 and 6667 are enabled.
Disconnected - Connection failure	The Zyxel Device failed to connect to Nebula. Make sure the Zyxel Device settings match the Nebula settings.
Disconnected - Registration failure	The email registered on myZyxel and the email registered on the Nebula organization to which you want to add the Zyxel Device are different.
Disconnected - Operation modes mismatch	Remove the Zyxel Device from the Nebula organization and site.

Nebula Mode to Cloud Monitoring Mode

1 Remove the Zyxel Device from the organization and site.

2 If the Zyxel Device is connected to Nebula, the Zyxel Device will automatically reset after you remove the Zyxel Device from the organization and site. If the Zyxel Device is not connected to Nebula, press the reset button.

3 After the PWR LED turns steady green, log into the Zyxel Device, select On Premises Mode, go to Configuration > Mgmt. & Analytics > Nebula, select Cloud Monitoring Mode and then follow the screen prompts.

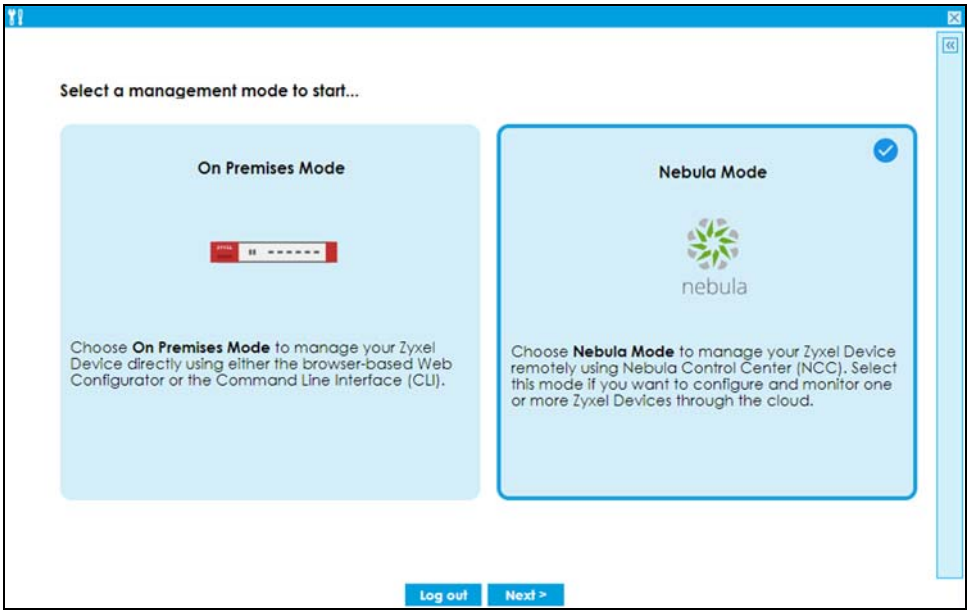
Cloud Monitoring Mode to Nebula Mode

1 Remove the Zyxel Device in cloud monitoring mode from the organization and site.

2 Back up your current configuration in Maintenance > File Manager > Configuration File.

3 Reset the Zyxel Device to the factory default by pushing the Reset button until the port connection LEDs turn off (after about 5 seconds). Your Zyxel Device will reboot to the factory defaults.

4 Log into the Zyxel Device. Run the wizard and choose Nebula Mode.



31.4.2 Cloud Management Scenario A - Native Mode

You will see the following screen if:

- Your Zyxel Device supports Native Mode and you can connect to Nebula with your current WAN settings.

If the Zyxel Device meets these criteria, Nebula can use the Zyxel Device's current WAN settings. Other settings are reset to factory defaults.

Please note that only the WAN settings that meet the criteria below will show in the Nebula Internet Access table:

- External interface - Interface that connects to an external network, such as the Internet or PPPoE. The Zyxel Device automatically adds this interface to the default WAN trunk.
- Base port - Ethernet interface on which the VLAN interface runs.
- Ethernet, VLAN or Ethernet/VLAN interface on which PPPoE interface runs.

Follow the steps below to let Nebula manage your Zyxel Device:

1. You cans select up to two WAN interfaces on the physical ports, but you cannot select two interfaces on the same port. Nebula will use one of the WAN interfaces you selected to connect to your Zyxel Device.

2. Click Test to test the connections to make sure you can access Nebula through these ports.

   Note: If you cannot access Nebula through the ports after you click Apply & Go To Nebula, you will need to access the local GUI with your support account by connecting to the LAN.

3. Click Apply & Go to Nebula. The Zyxel Device will:
   - Back up its current configuration (for future reference).
   - Reset its configuration to factory defaults except for the WAN configuration.
   - Automatically restart.

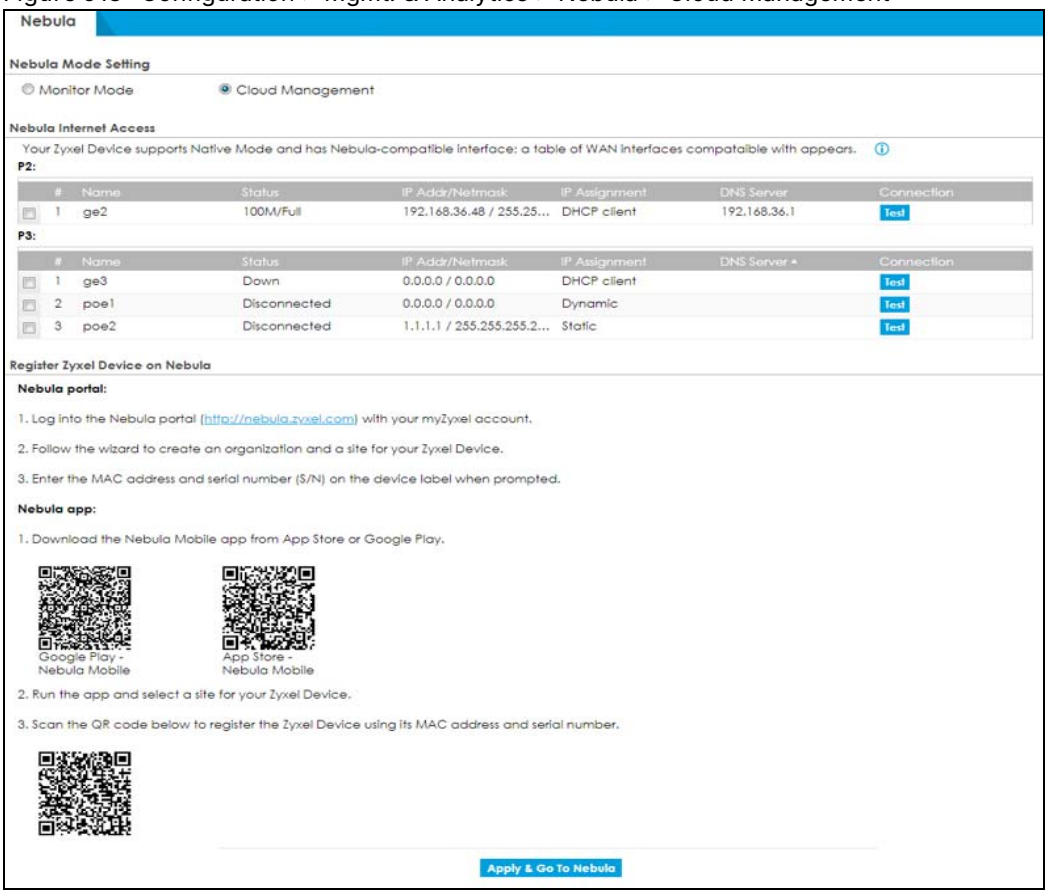
   Note: You will no longer be able to access the Zyxel Device through the WAN. You must use Nebula to manage it.

4. Use the Nebula web portal or the Nebula app to create an organization and site, then add the Zyxel Device to it.

   Note: You will not see Nebula app in Register Zyxel Device on Nebula if you log into the Zyxel Device as a limited admin.

Click Configuration > Mgmt. & Analytics > Nebula to open the following screen.

Figure 518 Configuration > Mgmt. & Analytics > Nebula > Cloud Management



The following table describes the labels in this screen.

Table 272 Configuration > Mgmt. & Analytics > Nebula > Cloud Management

LABEL	DESCRIPTION
	Select the WAN interfaces for Nebula to connect to your Zyxel Device. You can select up to two physical ports, but you cannot select two interfaces on the same port. For example, P2 and P3 stand for Port 2 and Port 3 on your Zyxel Device. You can only select one interface for each port. Nebula will use one of the WAN interfaces you selected to connect to your Zyxel Device. The settings of the WAN interfaces, including IP addresses, IP assignment and DNS servers, will be kept on Nebula.
#	This field is a sequential value.
Name	This field displays the name of the interface.

Table 272 Configuration > Mgmt. & Analytics > Nebula > Cloud Management (continued)

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 VLAN interfaces: • Up - The VLAN interface is enabled. • Down - The VLAN interface is disabled. For PPPoE interfaces: • Connected - The PPPoE interface is connected. • Disconnected - The PPPoE interface is disconnected.
IP Addr/Netmask	This field displays the current IP address and subnet mask assigned to the interface. 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). Note: If you set an interface static IP to 0.0.0.0, the interface will not show in the table.
IP Assignment	This field displays how the interface gets its IP address. • Static- This interface has a static IP address. • Dynamic- This interface has a dynamic IP address. • DHCP Client- This interface gets its IP address from a DHCP server.
DNS Server	The field displays the Domain Name System (DNS) server IP address. The DNS server maps a domain name to an IP address and vice versa. The DNS server is important because without it, you must know the IP address of a computer before you can access it.
Connection	Click Test to check if the interface you select can access Nebula.
Apply & Go to Nebula	Click this button to pass your Zyxel Device management to Nebula. Your Zyxel Device will automatically reset to factory defaults (except for the WAN settings) and restart.

CHAPTER 32
System

32.1 Overview

Use the system screens to configure general Zyxel Device settings.

32.1.1 What You Can Do in this Chapter

- Use the System > Host Name screen (see Section 32.2 on page 780) to configure a unique name for the Zyxel Device in your network.
- Use the System > USB Storage screen (see Section 32.3 on page 780) to configure the settings for the connected USB devices.
- Use the System > Date/Time screen (see Section 32.4 on page 782) to configure the date and time for the Zyxel Device.
- Use the System > Console Speed screen (see Section 32.5 on page 786) to configure the console port speed when you connect to the Zyxel Device through the console port using a terminal emulation program.
- Use the System > DNS screen (see Section 32.6 on page 787) to configure the DNS (Domain Name System) server used for mapping a domain name to its corresponding IP address and vice versa.
- Use the System > WWW screens (see Section 32.7 on page 796) to configure settings for HTTP or HTTPS access to the Zyxel Device and how the login and access user screens look.
- Use the System > SSH screen (see Section 32.8 on page 814) to configure SSH (Secure SHell) used to securely access the Zyxel Device's command line interface. You can specify which zones allow SSH access and from which IP address the access can come.
- Use the System > TELNET screen (see Section 32.9 on page 818) to configure Telnet to access the Zyxel Device's command line interface. Specify which zones allow Telnet access and from which IP address the access can come.
- Use the System > FTP screen (see Section 32.10 on page 820) to specify from which zones FTP can be used to access the Zyxel Device. You can also specify from which IP addresses the access can come. You can upload and download the Zyxel Device's firmware and configuration files using FTP.
- Your Zyxel Device can act as an SNMP agent, which allows a manager station to manage and monitor the Zyxel Device through the network. Use the System > SNMP screen (see Section 32.11 on page 822) to configure SNMP settings, including from which zones SNMP can be used to access the Zyxel Device. You can also specify from which IP addresses the access can come.
- Use the Auth. Server screen (Section 32.12 on page 828) to configure the Zyxel Device to operate as a RADIUS server.
- Use the Notification > Mail Server screen (Section 32.13 on page 831) to configure the Zyxel Device to operate as a RADIUS server.
- Use the Notification > SMS screen (Section 32.14 on page 832) to turn on the SMS service on the Zyxel Device in order to send dynamic guest account information in text messages and authorization for VPN tunnel access to a secured network.
- Use the Notification > Response Message screen (Section 32.15 on page 833) to create a web page when access to a website is restricted due to a security service.

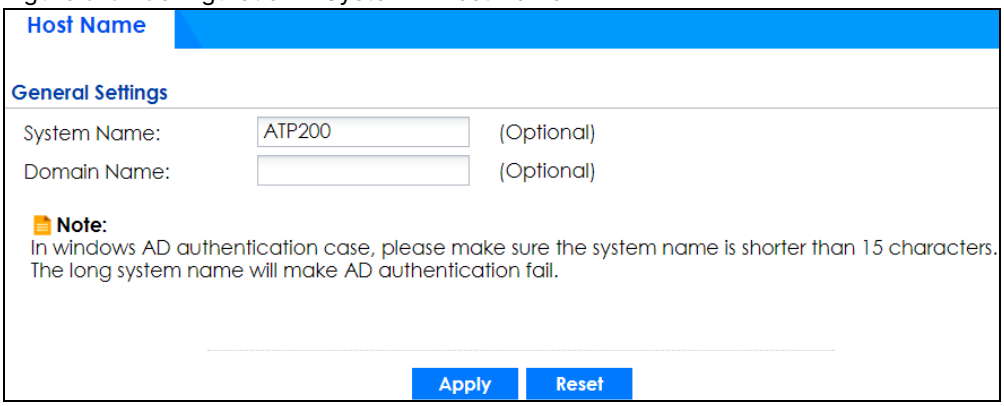
- Use the System > Language screen (see Section 32.16 on page 834) to set a language for the Zyxel Device's Web Configurator screens.
- Use the System > IPv6 screen (see Section 32.17 on page 835) to enable or disable IPv6 support on the Zyxel Device.
- Use the System > ZON screen (see Section 32.18 on page 836) to enable or disable the Zyxel One Network (ZON) utility that uses Zyxel Discovery Protocol (ZDP) for discovering and configuring ZDP-aware Zyxel devices in the same network as the computer on which ZON is installed.
- Use the System > Advanced screen (see Section 32.19 on page 841) to enable or disable the Fast Forwarding feature for your Zyxel Device.

Note: See each section for related background information and term definitions.

32.2 Host Name

A host name is the unique name by which a device is known on a network. Click Configuration > System > Host Name to open the Host Name screen.

Figure 519 Configuration > System > Host Name



The following table describes the labels in this screen.

Table 273 Configuration > System > Host Name

LABEL	DESCRIPTION
System Name	Enter a descriptive name to identify your Zyxel Device device. This name can be up to 64 alphanumeric characters long. Spaces are not allowed, but dashes (-) underscores (_) and periods (.) are accepted.
Domain Name	Enter the domain name (if you know it) here. This name is propagated to DHCP clients connected to interfaces with the DHCP server enabled. This name can be up to 254 alphanumeric characters long. Spaces are not allowed, but dashes "-" are accepted.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

32.3 USB Storage

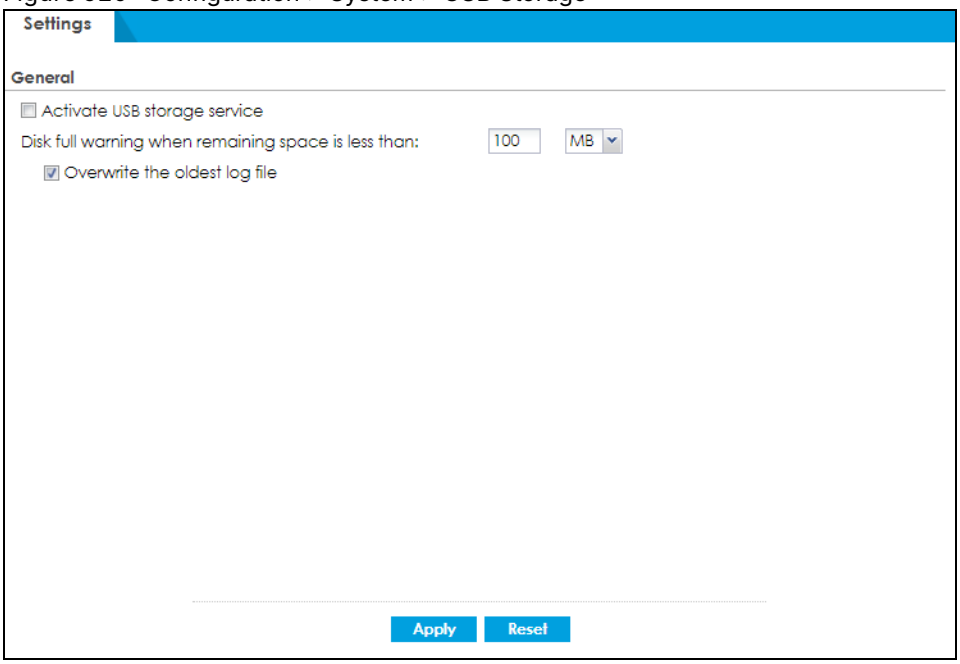
The Zyxel Device can use a connected USB device to store the system log and other diagnostic information. Use this screen to turn on this feature and set a disk full warning limit.

Note: Only connect one USB device. It must allow writing (it cannot be read-only) and use the FAT16, FAT32, EXT2, or EXT3 file system.

Note: The USB device must use MBR mode (Master Boot Record). It cannot have multiple partitions (GUID Partition Table).

Click Configuration > System > USB Storage to open the screen as shown next.

Figure 520 Configuration > System > USB Storage



The following table describes the labels in this screen.

Table 274 Configuration > System > USB Storage

LABEL	DESCRIPTION
Activate USB storage service	Select this if you want to use the connected USB device(s).
Disk full warning when remaining space is less than	Set a number and select a unit (MB or %) to have the Zyxel Device generate a log at the alert level when the remaining USB storage space is less than the value you set here.
Overwrite the oldest log file	Select this to have the Zyxel Device overwrite the oldest log file when the remaining USB storage space is less than the value you set above. Note: Make sure to save the log files to your computer.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

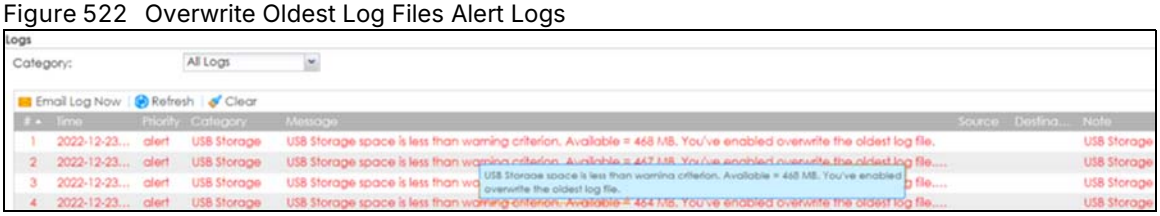
The Zyxel Device will generate logs at the alert level when:

- The remaining USB storage space is less the values you set.
- The Zyxel Device overwrites the oldest log files in your USB device.

A log at the alert level is a log for serious events that may need more immediate attention. You can check the priority of log messages in Monitor > Log > View Log > Priority.

Figure 521 USB Storage Space Alert Logs

Figure 522 Overwrite Oldest Log Files Alert Logs

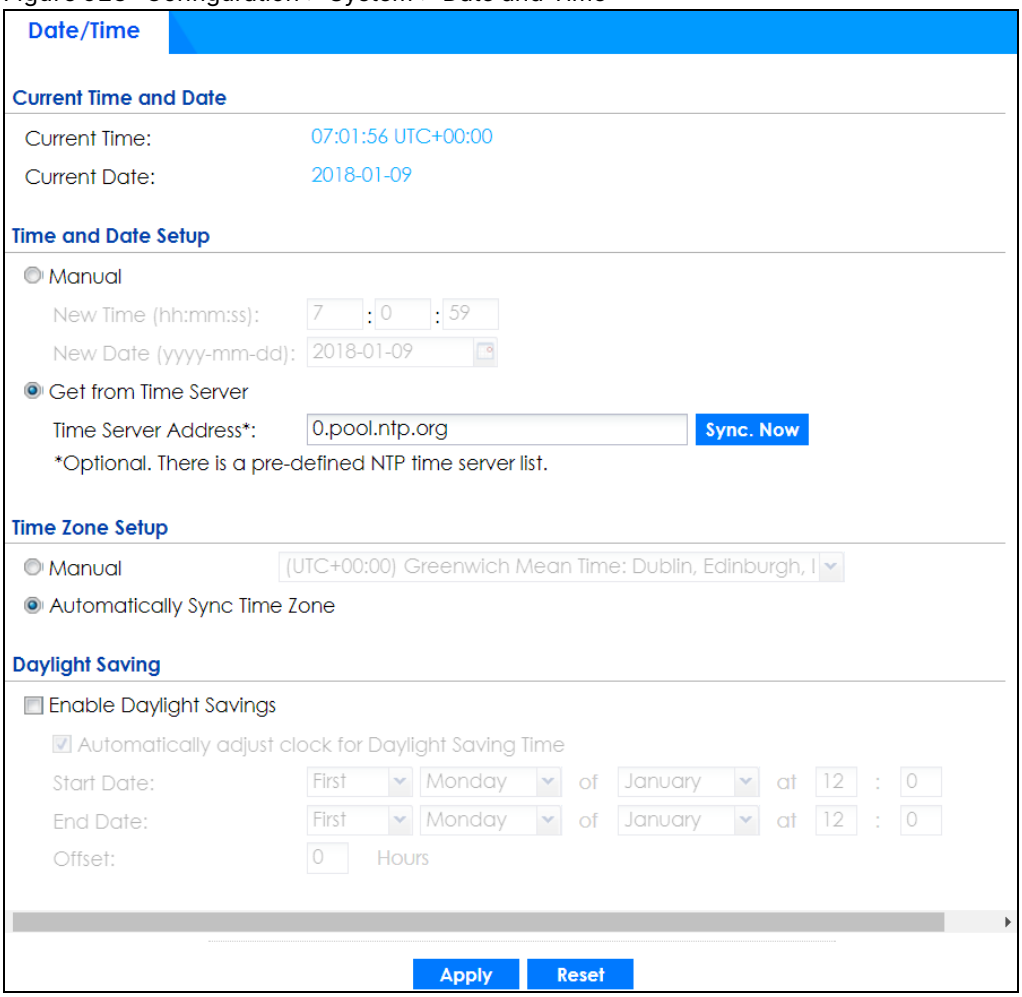


32.4 Date and Time

For effective scheduling and logging, the Zyxel Device system time must be accurate. The Zyxel Device's Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server.

To change your Zyxel Device's time based on your local time zone and date, click Configuration > System > Date/Time. The screen displays as shown. You can manually set the Zyxel Device's time and date or have the Zyxel Device get the date and time from a time server.

Figure 523 Configuration > System > Date and Time



The following table describes the labels in this screen.

Table 275 Configuration > System > Date and Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the present time of your Zyxel Device.
Current Date	This field displays the present date of your Zyxel Device.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, time zone and daylight saving at the same time, the time zone and daylight saving will affect the new time and date you entered. When you enter the time settings manually, the Zyxel Device uses the new setting once you click Apply.
New Time (hh-mm-ss)	This field displays the last updated time from the time server or the last time configured manually. When you set Time and Date Setup to Manual, enter the new time in this field and then click Apply.
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server or the last date configured manually. When you set Time and Date Setup to Manual, enter the new date in this field and then click Apply.

Table 275 Configuration > System > Date and Time (continued)

LABEL	DESCRIPTION
Get from Time Server	Select this radio button to have the Zyxel Device get the time and date from the time server you specify below. The Zyxel Device requests time and date settings from the time server under the following circumstances. • When the Zyxel Device starts up. • When you click Apply or Synchronize Now in this screen. • 24-hour intervals after starting up.
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Sync. Now	Click this button to have the Zyxel Device get the time and date from a time server (see the Time Server Address field). This also saves your changes (except the daylight saving settings).
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Automatically Sync Time Zone	Select this for the Zyxel Device to automatically get its time zone.
Daylight Saving	
Enable Daylight Savings	Daylight savings is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Automatically adjust clock for Daylight Saving Time	Select this for the Zyxel Device to automatically adjust the time if daylight savings is implemented in its time zone.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected Enable Daylight Saving. The at field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Second, Sunday, March and type 2 in the at field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, March. The time you type in the at field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected Enable Daylight Saving. The at field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select First, Sunday, November and type 2 in the at field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, October. The time you type in the at field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Offset	Specify how much the clock changes when daylight saving begins and ends. Enter a number from 1 to 5.5 (by 0.5 increments). For example, if you set this field to 3.5, a log occurred at 6 P.M. in local official time will appear as if it had occurred at 10:30 P.M.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

32.4.1 Pre-defined NTP Time Servers List

When you turn on the Zyxel Device for the first time, the date and time start at 2003-01-01 00:00:00. The Zyxel Device then attempts to synchronize with one of the following pre-defined list of Network Time Protocol (NTP) time servers.

The Zyxel Device continues to use the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

Table 276 Default Time Servers

0.pool.ntp.org
1.pool.ntp.org
2.pool.ntp.org

When the Zyxel Device uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the Zyxel Device goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

32.4.2 Time Server Synchronization

Click the Synchronize Now button to get the time and date from the time server you specified in the Time Server Address field.

When the Loading screen appears, you may have to wait up to one minute.

Figure 524 Synchronization in Process

The Current Time and Current Date fields will display the appropriate settings if the synchronization is successful.

If the synchronization was not successful, a log displays in the View Log screen. Try re-configuring the Date/Time screen.

To manually set the Zyxel Device date and time.

1 Click System > Date/Time.

2 Select Manual under Time and Date Setup.

3 Enter the Zyxel Device's time in the New Time field.

4 Enter the Zyxel Device's date in the New Date field.

5 Under Time Zone Setup, select your Time Zone from the list.

6 As an option you can select the Enable Daylight Saving checkbox to adjust the Zyxel Device clock for daylight savings.

7 Click Apply.

To get the Zyxel Device date and time from a time server

1 Click System > Date/Time.

2 Select Get from Time Server under Time and Date Setup.

3 Under Time Zone Setup, select your Time Zone from the list.

4 As an option you can select the Enable Daylight Saving checkbox to adjust the Zyxel Device clock for daylight savings.

5 Under Time and Date Setup, enter a Time Server Address (Table 276 on page 785).

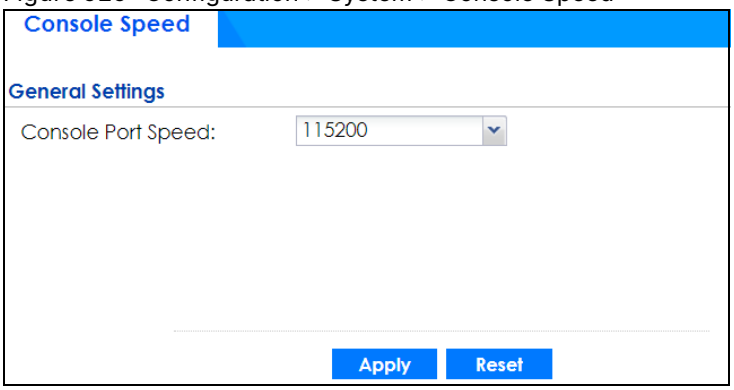
6 Click Apply.

32.5 Console Port Speed

This section shows you how to set the console port speed when you connect to the Zyxel Device through the console port using a terminal emulation program.

Click Configuration > System > Console Speed to open the Console Speed screen.

Figure 525 Configuration > System > Console Speed



The following table describes the labels in this screen.

Table 277 Configuration > System > Console Speed

LABEL	DESCRIPTION
Console Port Speed	Use the drop-down list box to change the speed of the console port. Your Zyxel Device supports 9600, 19200, 38400, 57600, and 115200 bps (default) for the console port. The Console Port Speed applies to a console port connection using terminal emulation software and NoT the Console in the Zyxel Device Web Configurator Status screen.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

32.6 DNS Overview

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

32.6.1 DNS Server Address Assignment

The Zyxel Device can get the DNS server addresses in the following ways.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
- If your ISP dynamically assigns the DNS server IP addresses (along with the Zyxel Device's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.
- You can manually enter the IP addresses of other DNS servers.

32.6.2 Configuring the DNS Screen

Click Configuration > System > DNS to change your Zyxel Device's DNS settings. Use the DNS screen to configure the Zyxel Device to use a DNS server to resolve domain names for Zyxel Device system features like VPN, DDNS and the time server. You can also configure the Zyxel Device to accept or discard DNS queries. Use the Network > Interface screens to configure the DNS server information that the Zyxel Device sends to the specified DHCP client devices.

A name query begins at a client computer and is passed to a resolver, a DNS client service, for resolution. The Zyxel Device can be a DNS client service. The Zyxel Device can resolve a DNS query locally using cached Resource Records (RR) obtained from a previous query (and kept for a period of time). If the Zyxel Device does not have the requested information, it can forward the request to DNS servers. This is known as recursion.

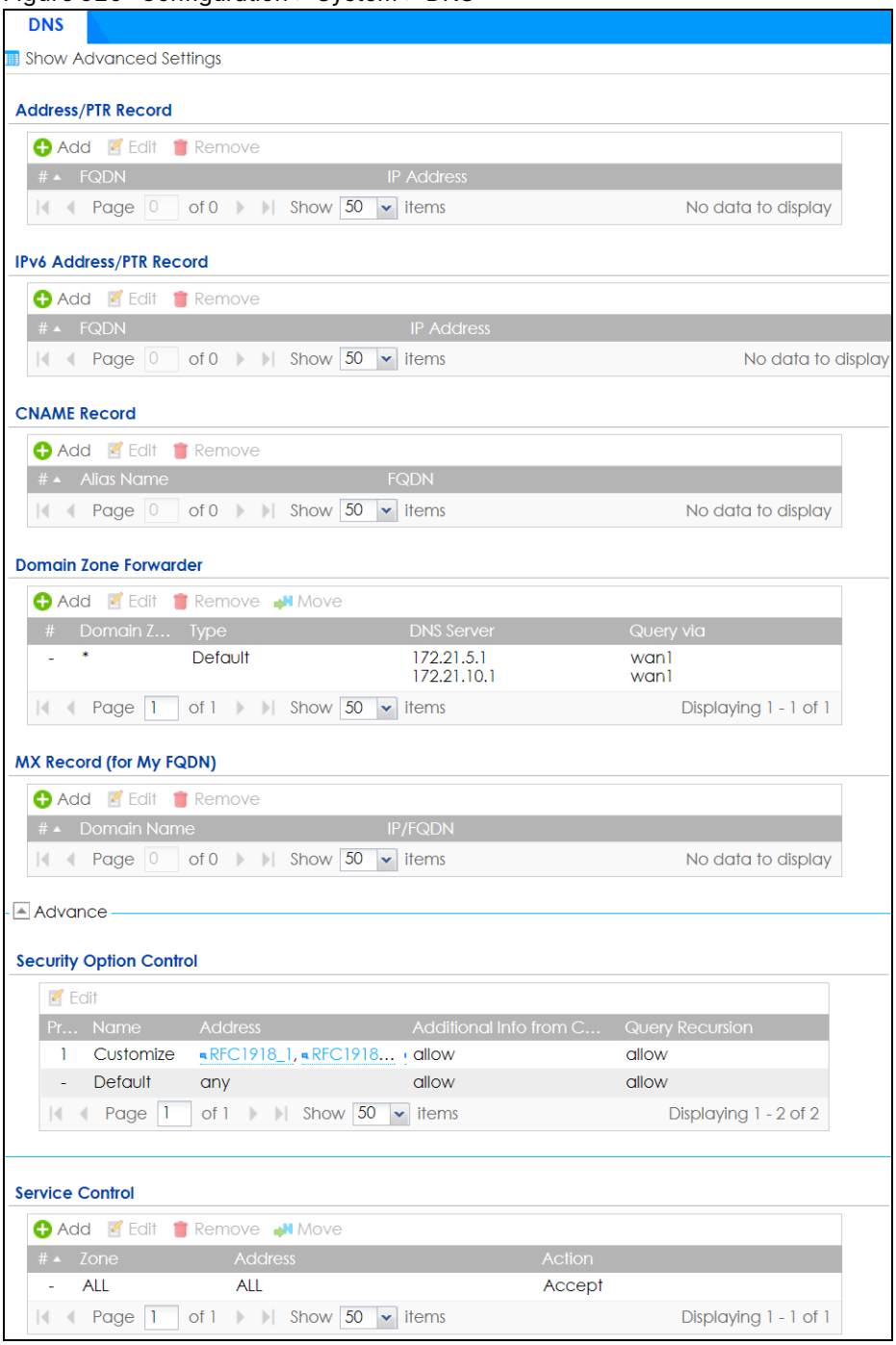
The Zyxel Device can ask a DNS server to use recursion to resolve its DNS client requests. If recursion on the Zyxel Device or a DNS server is disabled, they cannot forward DNS requests for resolution.

A Domain Name Server (DNS) amplification attack is a kind of Distributed Denial of Service (DDoS) attack that uses publicly accessible open DNS servers to flood a victim with DNS response traffic. An open DNS server is a DNS server which is willing to resolve recursive DNS queries from anyone on the Internet.

In a DNS amplification attack, an attacker sends a DNS name lookup request to an open DNS server with the source address spoofed as the victim's address. When the DNS server sends the DNS record response, it is sent to the victim. Attackers can request as much information as possible to maximize the amplification effect.

Configure the Security Option Control section in the Configuration > System > DNS screen (click Show Advanced Settings to display it) if you suspect the Zyxel Device is being used (either by hackers or by a corrupted open DNS server) in a DNS amplification attack.

Figure 526 Configuration > System > DNS



The following table describes the labels in this screen.

Table 278 Configuration > System > DNS

LABEL	DESCRIPTION
Address/PTR Record	This record specifies the mapping of a Fully-Qualified Domain Name (FQDN) to an IP address. An FQDN consists of a host and domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the third-level domain, “com” is the second-level domain, and “tw” is the top level domain.
Add	Click this to create a new entry.

Table 278 Configuration > System > DNS (continued)

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
#	This is the index number of the address/PTR record.
FQDN	This is a host's fully qualified domain name.
IP Address	This is the IP address of a host.
CNAME Record	This record specifies an alias for a FQDN. Use this record to bind all subdomains with the same IP address as the FQDN without having to update each one individually, which increases chance for errors. See CNAME Record (Section 32.6.6 on page 791) for more details.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
#	This is the index number of the domain zone forwarder record. The ordering of your rules is important as rules are applied in sequence. A hyphen (-) displays for the default domain zone forwarder record. The default record is not configurable. The Zyxel Device uses this default record if the domain zone that needs to be resolved does not match any of the other domain zone forwarder records.
Alias Name	Enter an Alias name. Use "*." as prefix for a wildcard domain name. For example, *.example.com.
FQDN	Enter the Fully Qualified Domain Name (FQDN).
Domain Zone Forwarder	This specifies a DNS server's IP address. The Zyxel Device can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. When the Zyxel Device needs to resolve a domain zone, it checks it against the domain zone forwarder entries in the order that they appear in this list.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This is the index number of the domain zone forwarder record. The ordering of your rules is important as rules are applied in sequence. A hyphen (-) displays for the default domain zone forwarder record. The default record is not configurable. The Zyxel Device uses this default record if the domain zone that needs to be resolved does not match any of the other domain zone forwarder records.
Domain Zone	A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. A "*" means all domain zones.
Type	This displays whether the DNS server IP address is assigned by the ISP dynamically through a specified interface or configured manually (User-Defined).
DNS Server	This is the IP address of a DNS server. This field displays N/A if you have the Zyxel Device get a DNS server IP address from the ISP dynamically but the specified interface is not active.
Query Via	This is the interface through which the Zyxel Device sends DNS queries to the entry's DNS server. If the Zyxel Device connects through a VPN tunnel, tunnel displays.

Table 278 Configuration > System > DNS (continued)

LABEL	DESCRIPTION
MX Record (for My FQDN)	A MX (Mail eXchange) record identifies a mail server that handles the mail for a particular domain.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
#	This is the index number of the MX record.
Domain Name	This is the domain name where the mail is destined for.
IP/FQDN	This is the IP address or Fully-Qualified Domain Name (FQDN) of a mail server that handles the mail for the domain specified in the field above.
Security Option Control	Click Show Advanced Settings to display this part of the screen. There are two control policies: Default and Customize.
Edit	Click either control policy and then click this button to change allow or deny actions for Query Recursion and Additional Info from Cache.
Priority	The Customize control policy is checked first and if an address object match is not found, the Default control policy is checked.
Name	You may change the name of the Customize control policy.
Address	These are the object addresses used in the control policy. RFC1918 refers to private IP address ranges. It can be modified in Object > Address.
Additional Info from Cache	This displays if the Zyxel Device is allowed or denied to cache Resource Records (RR) obtained from previous DNS queries.
Query Recursion	This displays if the Zyxel Device is allowed or denied to forward DNS client requests to DNS servers for resolution.
Service Control	This specifies from which computers and zones you can send DNS queries to the Zyxel Device.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule. The ordering of your rules is important as rules are applied in sequence. The entry with a hyphen (-) instead of a number is the Zyxel Device's (non-configurable) default policy. The Zyxel Device applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the Zyxel Device will not have to use the default policy.
Zone	This is the zone on the Zyxel Device the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to send DNS queries.
Action	This displays whether the Zyxel Device accepts DNS queries from the computer with the IP address specified above through the specified zone (Accept) or discards them (Deny).

32.6.3 (IPv6) Address Record

An address record contains the mapping of a Fully-Qualified Domain Name (FQDN) to an IP address.

The Zyxel Device allows you to configure address records about the Zyxel Device itself or another device. This way you can keep a record of DNS names and addresses that people on your network may use frequently. If the Zyxel Device receives a DNS query for an FQDN for which the Zyxel Device has an address record, the Zyxel Device can send the IP address in a DNS response without having to query a DNS name server.

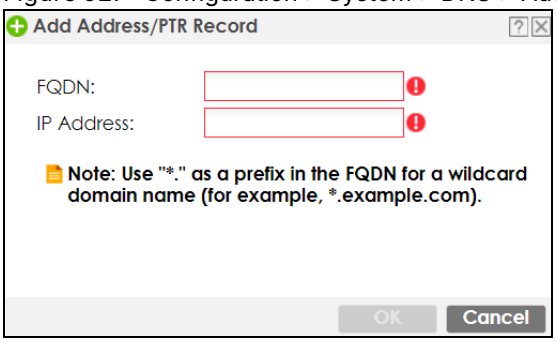
32.6.4 PTR Record

A PTR (pointer) record is also called a reverse record or a reverse lookup record. It is a mapping of an IP address to a domain name.

32.6.5 Adding an (IPv6) Address/PTR Record

Click the Add icon in the Address/PTR Record or IPv6 Address/PTR Record table to add an IPv4 or IPv6 address/PTR record.

Figure 527 Configuration > System > DNS > Address/PTR Record Edit



The following table describes the labels in this screen.

Table 279 Configuration > System > DNS > (IPv6) Address/PTR Record Edit

LABEL	DESCRIPTION
FQDN	Type a Fully-Qualified Domain Name (FQDN) of a server. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the third-level domain, “com” is the second-level domain, and “tw” is the top level domain. Underscores are not allowed. Use "*." as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).
IP Address	Enter the IP address of the host in dotted decimal notation.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

32.6.6 CNAME Record

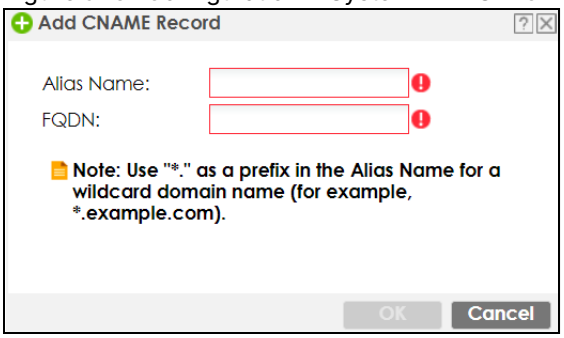
A Canonical Name Record or CNAME record is a type of resource record in the Domain Name System (DNS) that specifies that the domain name is an alias of another, canonical domain name. This allows users to set up a record for a domain name which translates to an IP address, in other words, the domain name is an alias of another. This record also binds all the subdomains to the same IP address without having to create a record for each, so when the IP address is changed, all subdomain’s IP address is updated as well, with one edit to the record.

For example, the domain name zyxel.com is hooked up to a record named A which translates it to 11.22.33.44. You also have several subdomains, like mail.zyxel.com, ftp.zyxel.com and you want this subdomain to point to your main domain zyxel.com. Edit the IP Address in record A and all subdomains will follow automatically. This eliminates chances for errors and increases efficiency in DNS management.

32.6.7 Adding a CNAME Record

Click the Add icon in the CNAME Record table to add a record. Use “*.” as a prefix for a wildcard domain name. For example *.zyxel.com.

Figure 528 Configuration > System > DNS > CNAME Record > Add



The following table describes the labels in this screen.

Table 280 Configuration > System > DNS > CNAME Record > Add

LABEL	DESCRIPTION
Alias name	Enter an Alias Name. Use "*." as a prefix in the Alias name for a wildcard domain name (for example, *.example.com).
FQDN	Type a Fully-Qualified Domain Name (FQDN) of a server. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the third-level domain, “com” is the second-level domain, and “tw” is the top level domain. Underscores are not allowed. Use "*." as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

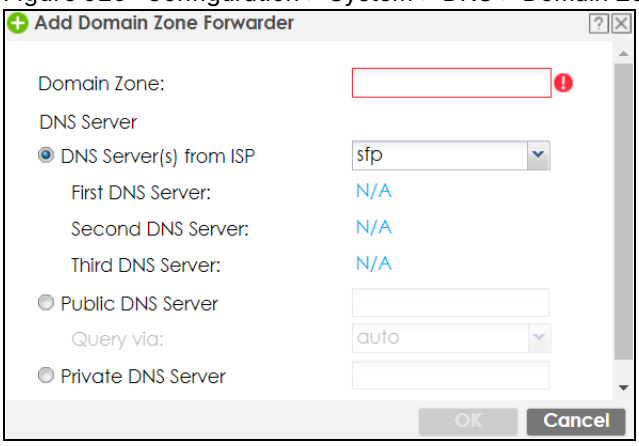
32.6.8 Domain Zone Forwarder

A domain zone forwarder contains a DNS server’s IP address. The Zyxel Device can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.

32.6.9 Adding a Domain Zone Forwarder

Click the Add icon in the Domain Zone Forwarder table to add a domain zone forwarder record.

Figure 529 Configuration > System > DNS > Domain Zone Forwarder Add



The following table describes the labels in this screen.

Table 281 Configuration > System > DNS > Domain Zone Forwarder Add

LABEL	DESCRIPTION
Domain Zone	A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. For example, whenever the Zyxel Device receives needs to resolve a zyxel.com.tw domain name, it can send a query to the recorded name server IP address. Enter * if all domain zones are served by the specified DNS server(s).
DNS Server	Select DNS Server(s) from ISP if your ISP dynamically assigns DNS server information. You also need to select an interface through which the ISP provides the DNS server IP address(es). The interface should be activated and set to be a DHCP client. The fields below display the (read-only) DNS server IP address(es) that the ISP assigns. N/A displays for any DNS server IP address fields for which the ISP does not assign an IP address. Select Public DNS Server if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. The Zyxel Device must be able to connect to the DNS server without using a VPN tunnel. The DNS server could be on the Internet or one of the Zyxel Device's local networks. You cannot use 0.0.0.0. Use the Query via field to select the interface through which the Zyxel Device sends DNS queries to a DNS server. Select Private DNS Server if you have the IP address of a DNS server to which the Zyxel Device connects through a VPN tunnel. Enter the DNS server's IP address in the field to the right. You cannot use 0.0.0.0.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

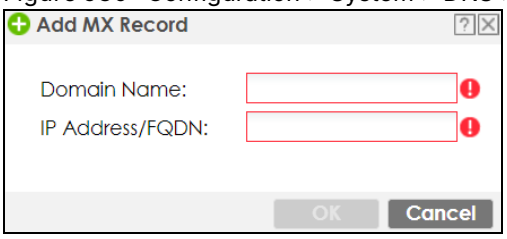
32.6.10 MX Record

A MX (Mail eXchange) record indicates which host is responsible for the mail for a particular domain, that is, controls where mail is sent for that domain. If you do not configure proper MX records for your domain or other domain, external email from other mail servers will not be able to be delivered to your mail server and vice versa. Each host or domain can have only one MX record, that is, one domain is mapping to one host.

32.6.11 Adding a MX Record

Click the Add icon in the MX Record table to add a MX record.

Figure 530 Configuration > System > DNS > MX Record Add



The following table describes the labels in this screen.

Table 282 Configuration > System > DNS > MX Record Add

LABEL	DESCRIPTION
Domain Name	Enter the domain name where the mail is destined for.
IP Address/FQDN	Enter the IP address or Fully-Qualified Domain Name (FQDN) of a mail server that handles the mail for the domain specified in the field above.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

32.6.12 Security Option Control

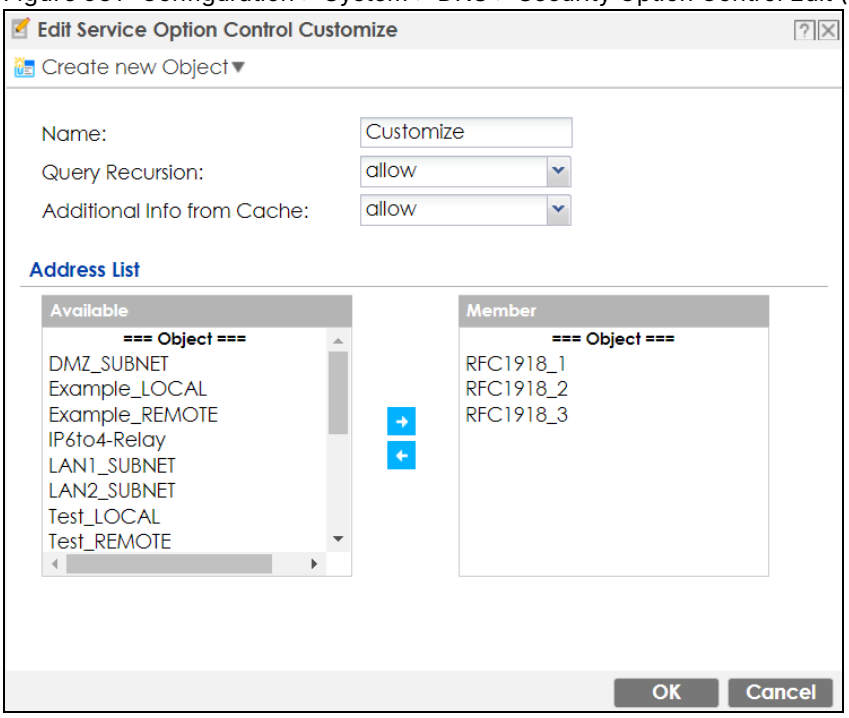
Configure the Security Option Control section in the Configuration > System > DNS screen (click Show Advanced Settings to display it) if you suspect the Zyxel Device is being used by hackers in a DNS amplification attack.

One possible strategy would be to deny Query Recursion and Additional Info from Cache in the default policy and allow Query Recursion and Additional Info from Cache only from trusted DNS servers identified by address objects and added as members in the customized policy.

32.6.13 Editing a Security Option Control

Click a control policy and then click Edit to change allow or deny actions for Query Recursion and Additional Info from Cache.

Figure 531 Configuration > System > DNS > Security Option Control Edit (Customize)



The following table describes the labels in this screen.

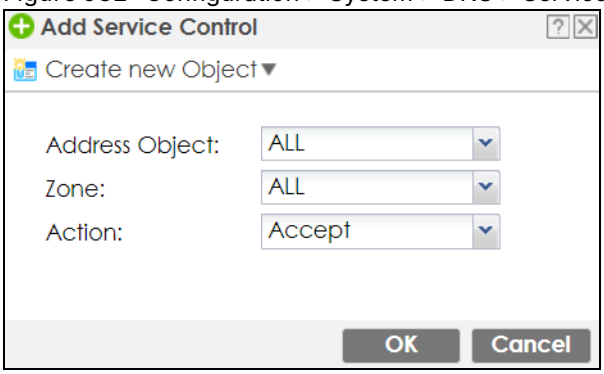
Table 283 Configuration > System > DNS > Security Option Control Edit (Customize)

LABEL	DESCRIPTION
Name	You may change the name for the customized security option control policy. The customized security option control policy is checked first and if an address object match is not found, the Default control policy is checked.
Query Recursion	Choose if the Zyxel Device is allowed or denied to forward DNS client requests to DNS servers for resolution. This can apply to specific open DNS servers using the address objects in a customized rule.
Additional Info from Cache	Choose if the Zyxel Device is allowed or denied to cache Resource Records (RR) obtained from previous DNS queries.
Address List	Specifying address objects is not available in the default policy as all addresses are included.
Available	This box displays address objects created in Object > Address. Select one (or more), and click the > arrow to have it (them) join the Member list of address objects that will apply to this rule. For example, you could specify an open DNS server suspect of sending compromised resource records by adding an address object for that server to the member list.
Member	This box displays address objects that will apply to this rule.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

32.6.14 Adding a DNS Service Control Rule

Click the Add icon in the Service Control table to add a service control rule.

Figure 532 Configuration > System > DNS > Service Control Rule Add



The following table describes the labels in this screen.

Table 284 Configuration > System > DNS > Service Control Rule Add

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Address Object	Select ALL to allow or deny any computer to send DNS queries to the Zyxel Device. Select a predefined address object to just allow or deny the computer with the IP address that you specified to send DNS queries to the Zyxel Device.
Zone	Select ALL to allow or prevent DNS queries through any zones. Select a predefined zone on which a DNS query to the Zyxel Device is allowed or denied.
Action	Select Accept to have the Zyxel Device allow the DNS queries from the specified computer. Select Deny to have the Zyxel Device reject the DNS queries from the specified computer.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

32.7 WWW Overview

The following figure shows secure and insecure management of the Zyxel Device coming in from the WAN. HTTPS and SSH access are secure. HTTP and Telnet access are not secure.

Note: To allow the Zyxel Device to be accessed from a specified computer using a service, make sure you do not have a service control rule or to-Zyxel Device security policy rule to block that traffic.

To stop a service from accessing the Zyxel Device, clear Enable in the corresponding service screen.

32.7.1 Service Access Limitations

A service cannot be used to access the Zyxel Device when:

1 You have disabled that service in the corresponding screen.

2 The allowed IP address (address object) in the Service Control table does not match the client IP address (the Zyxel Device disallows the session).

3 The IP address (address object) in the Service Control table is not in the allowed zone or the action is set to Deny.

4 There is a security policy rule that blocks it.

32.7.2 System Timeout

There is a lease timeout for administrators. The Zyxel Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

Each user is also forced to log in the Zyxel Device for authentication again when the reauthentication time expires.

You can change the timeout settings in the User/Group screens.

32.7.3 HTTPS

You can set the Zyxel Device to use HTTP or HTTPS (HTTPS adds security) for Web Configurator sessions. Specify which zones allow Web Configurator access and from which IP address the access can come.

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys.

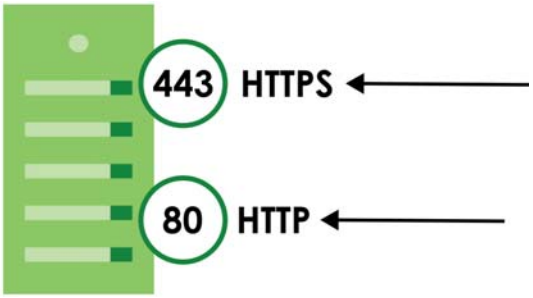
HTTPS on the Zyxel Device is used so that you can securely access the Zyxel Device using the Web Configurator. The SSL protocol specifies that the HTTPS server (the Zyxel Device) must always authenticate itself to the HTTPS client (the computer which requests the HTTPS connection with the Zyxel Device), whereas the HTTPS client only should authenticate itself when the HTTPS server requires it to do so (select Authenticate Client Certificates in the WWW screen). Authenticate Client Certificates is optional and if selected means the HTTPS client must send the Zyxel Device a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the Zyxel Device.

Please refer to the following figure.

1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the Zyxel Device’s web server.

2 HTTP connection requests from a web browser go to port 80 (by default) on the Zyxel Device’s web server.

Figure 533 HTTP/HTTPS Implementation



Note: If you disable HTTP in the WWW screen, then the Zyxel Device blocks all HTTP connection attempts.

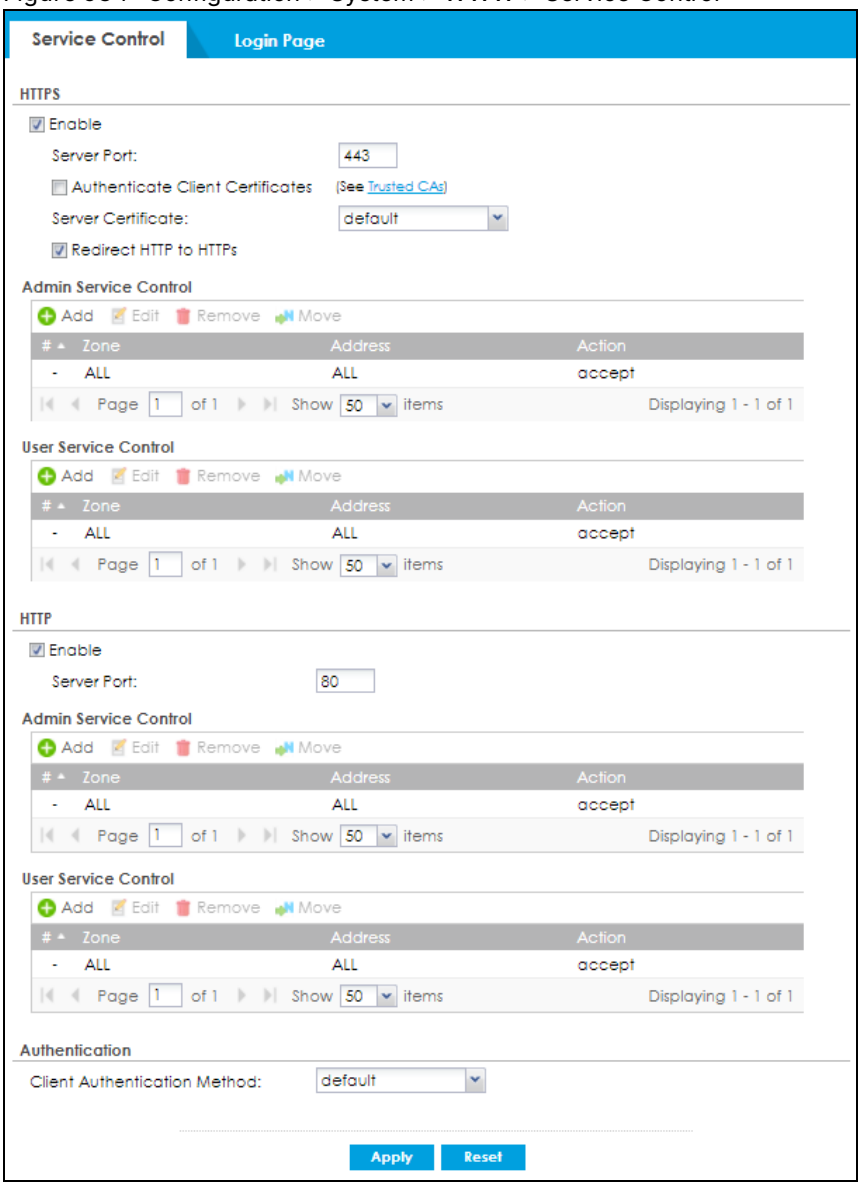
32.7.4 Configuring WWW Service Control

Click Configuration > System > WWW to open the WWW screen. Use this screen to specify from which zones you can access the Zyxel Device using HTTP or HTTPS. You can also specify which IP addresses the access can come from.

Admin Service Control deals with management access (to the Web Configurator). User Service Control deals with user access to the Zyxel Device.

Note: You can specify the IP address a user can use to access the Zyxel Device using HTTPS or the network behind the Zyxel Device using SSL VPN if the SSL VPN port and the HTTPS port are the same in System > WWW > Service Control > HTTPS > User Service. Please note that if you change the SSL VPN port in VPN > SSL VPN > Global Setting to a port different from the HTTPS port, the settings you configure in HTTPS User Service Control can only be used for users that access the Zyxel Device using HTTPS.

Figure 534 Configuration > System > WWW > Service Control



The following table describes the labels in this screen.

Table 285 Configuration > System > WWW > Service Control

LABEL	DESCRIPTION
HTTPS	
Enable	Select the checkbox to allow or disallow the computer with the IP address that matches the IP address(es) in the HTTPS Admin Service Control and User Service Control table to access the Zyxel Device Web Configurator using secure HTTPS connections.
Server Port	The HTTPS server listens on port 443 by default. If you change the HTTPS server port to a different number on the Zyxel Device, for example 8443, then you must notify people who need to access the Zyxel Device Web Configurator to use “https://Zyxel Device IP Address:8443” as the URL.

Table 285 Configuration > System > WWW > Service Control (continued)

LABEL	DESCRIPTION

Authenticate Client Certificates	Select Authenticate Client Certificates (optional) to require the SSL client to authenticate itself to the Zyxel Device by sending the Zyxel Device a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the Zyxel Device(see Section 32.7.7.5 on page 809 on importing certificates for details).
	
	If you enabled Authenticate Client Certificates, but you do not have a trusted certificate, then the client device will not be able to access the Zyxel Device web configurator. To disable Authenticate Client Certificates, log in through the console port and use the following commands to disable Authenticate Client Certificates.
	
	`Router > configure terminal`
	`Router(config)# no ip http secure-server auth-client`
	`Router(config)# write`
	`Router(config)# exit`

Server Certificate	Select a certificate the HTTPS server (the Zyxel Device) uses to authenticate itself to the HTTPS client. You must have certificates already configured in the My Certificates screen.
Redirect HTTP to HTTPS	To allow only secure Web Configurator access, select this to redirect all HTTP connection requests to the HTTPS server.
Admin/User Service Control	Admin Service Control specifies from which zones an administrator can use HTTPS to manage the Zyxel Device (using the Web Configurator). You can also specify the IP addresses from which the administrators can manage the Zyxel Device. User Service Control specifies from which zones a user can use HTTPS to log into the Zyxel Device. You can also specify the IP addresses from which the users can access the Zyxel Device.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This is the index number of the service control rule. The entry with a hyphen (-) instead of a number is the Zyxel Device's (non-configurable) default policy. The Zyxel Device applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the Zyxel Device will not have to use the default policy.
Zone	This is the zone on the Zyxel Device the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the Zyxel Device zone(s) configured in the Zone field (Accept) or not (Deny).
HTTP	
Enable	Select the checkbox to allow or disallow the computer with the IP address that matches the IP address(es) in the HTTP Admin Service Control and User Service Control table to access the Zyxel Device Web Configurator using HTTP connections.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service to access the Zyxel Device.

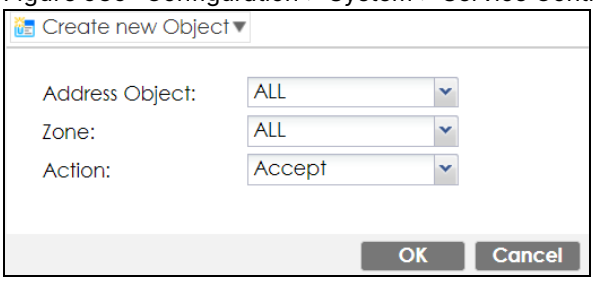
Table 285 Configuration > System > WWW > Service Control (continued)

LABEL	DESCRIPTION
Admin/User Service Control	Admin Service Control specifies from which zones an administrator can use HTTP to manage the Zyxel Device (using the Web Configurator). You can also specify the IP addresses from which the administrators can manage the Zyxel Device. User Service Control specifies from which zones a user can use HTTP to log into the Zyxel Device. You can also specify the IP addresses from which the users can access the Zyxel Device. Please note that if you want to access the Zyxel Device through SSL VPN using the same port as the HTTP port, the SSL VPN port and the HTTP port have to be the same.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This is the index number of the service control rule. The entry with a hyphen (-) instead of a number is the Zyxel Device's (non-configurable) default policy. The Zyxel Device applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the Zyxel Device will not have to use the default policy.
Zone	This is the zone on the Zyxel Device the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the Zyxel Device zone(s) configured in the Zone field (Accept) or not (Deny).
Authentication	
Client Authentication Method	Select a method the HTTPS or HTTP server uses to authenticate a client. You must have configured the authentication methods in the Object > Auth. method screen.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

32.7.5 Service Control Rules

Click Add or Edit in the Service Control table in a WWW, SSH, Telnet, FTP or SNMP screen to add a service control rule.

Figure 535 Configuration > System > Service Control Rule > Edit



The following table describes the labels in this screen.

Table 286 Configuration > System > Service Control Rule > Edit

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Address Object	Select ALL to allow or deny any computer to communicate with the Zyxel Device using this service. Select a predefined address object to just allow or deny the computer with the IP address that you specified to access the Zyxel Device using this service.
Zone	Select ALL to allow or prevent any Zyxel Device zones from being accessed using this service. Select a predefined Zyxel Device zone on which a incoming service is allowed or denied.
Action	Select Accept to allow the user to access the Zyxel Device from the specified computers. Select Deny to block the user's access to the Zyxel Device from the specified computers.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

32.7.6 Customizing the WWW Login Page

Click Configuration > System > WWW > Login Page to open the Login Page screen. Use this screen to customize the Web Configurator login screen. You can also customize the page that displays after an access user logs into the Web Configurator to access network services like the Internet.

Figure 536 Configuration > System > WWW > Login Page (Desktop View)

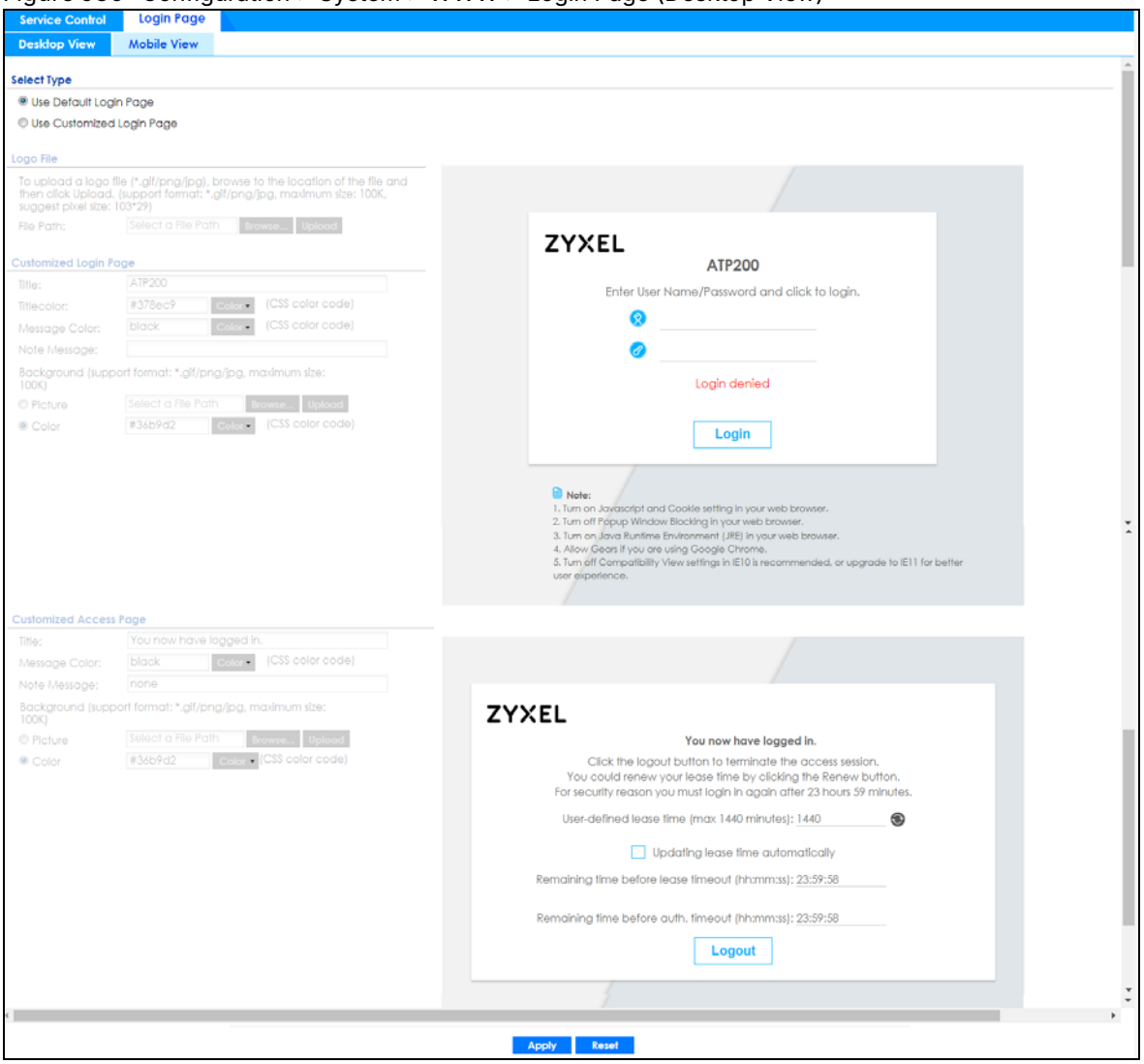
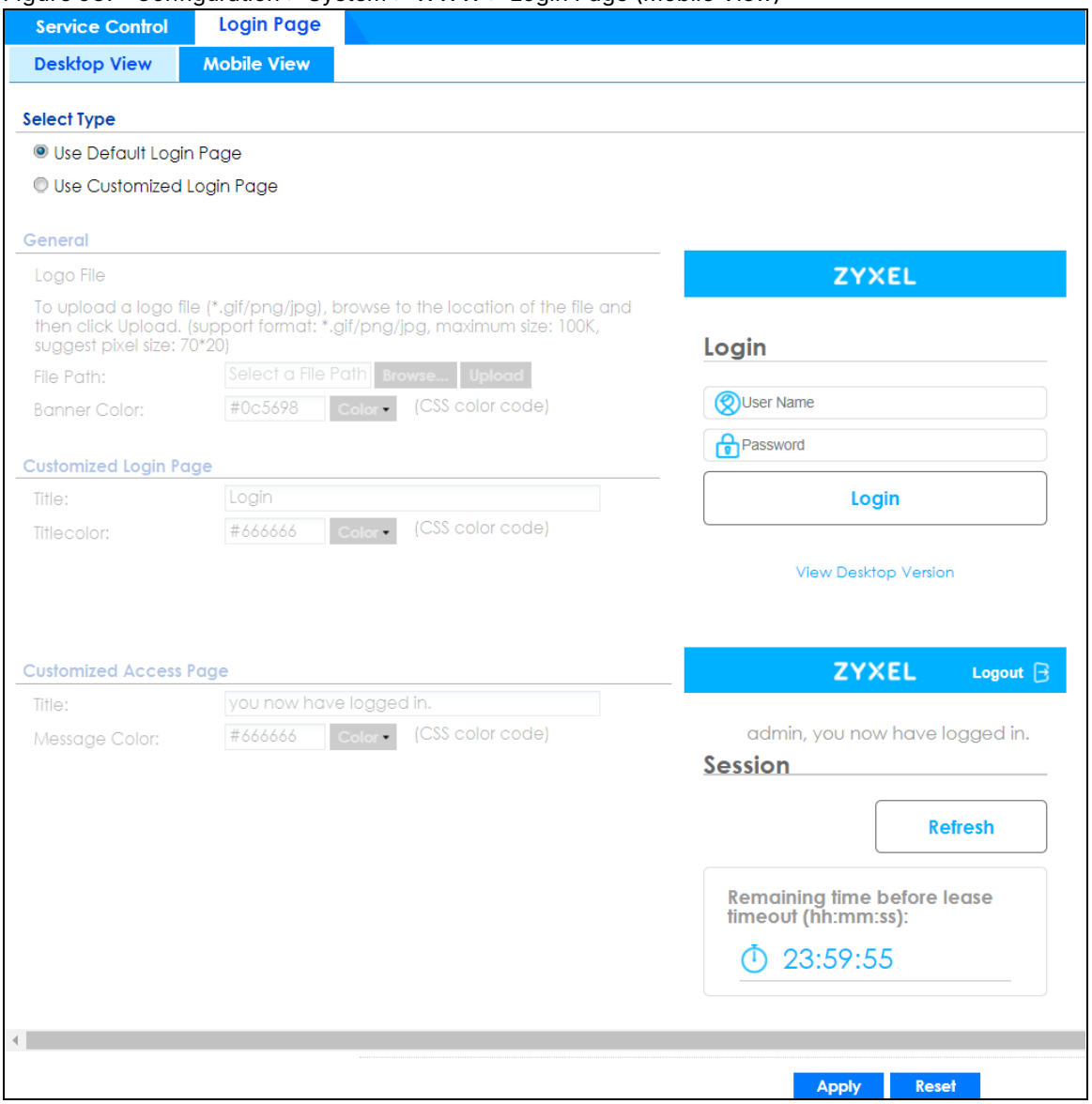


Figure 537 Configuration > System > WWW > Login Page (Mobile View)



The following figures identify the parts you can customize in the login and access pages.

Figure 538 Login Page Customization

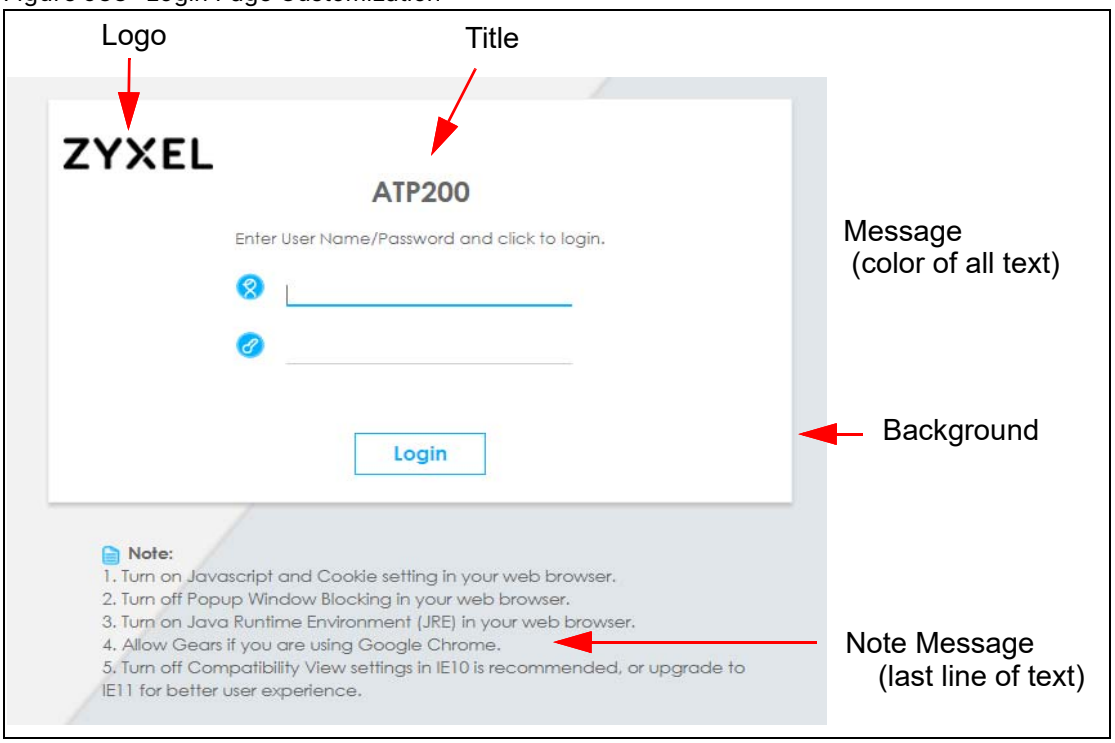
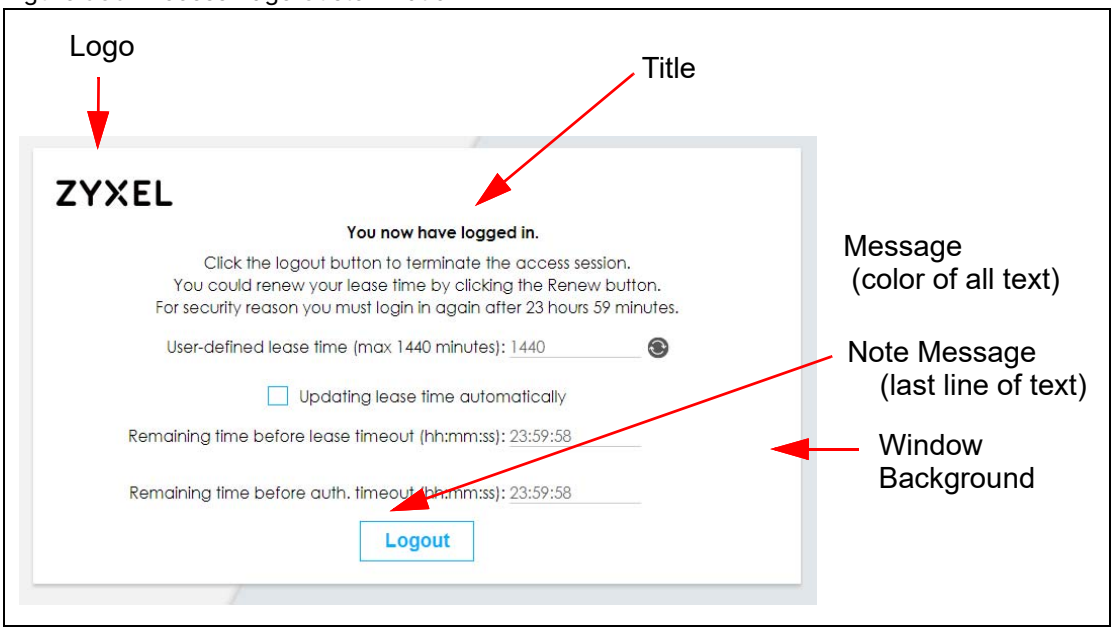


Figure 539 Access Page Customization



You can specify colors in one of the following ways:

- Click Color to display a screen of web-safe colors from which to choose.
- Enter the name of the desired color.
- Enter a pound sign (#) followed by the six-digit hexadecimal number that represents the desired color. For example, use “#000000” for black.
- Enter “rgb” followed by red, green, and blue values in parenthesis and separate by commas. For example, use “rgb(0,0,0)” for black.

Your desired color should display in the preview screen on the right after you click in another field, click Apply, or press [ENTER]. If your desired color does not display, your browser may not support it. Try selecting another color.

The following table describes the labels on the screen.

Table 287 Configuration > System > WWW > Login Page

LABEL	DESCRIPTION
Select Type	Select whether the Web Configurator uses the default login screen or one that you customize in the rest of this screen.
Logo File	You can upload a graphic logo to be displayed on the upper left corner of the Web Configurator login screen and access page. Specify the location and file name of the logo graphic or click Browse to locate it. Note: Use a GIF, JPG, or PNG of 100 kilobytes or less. Click Upload to transfer the specified graphic file from your computer to the Zyxel Device.
Customized Login Page	Use this section to set how the Web Configurator login screen looks.
Title	Enter the title for the top of the screen. Use 1 to 64 single-byte characters, including 0-9a-zA-Z!"#$%&'()*+,-./:;=?@[\]^_'. Spaces are allowed. <> are not allowed.
Title Color	Specify the color of the screen's title text.
Message Color	Specify the color of the screen's text.
Note Message	Enter a note to display at the bottom of the screen. Use up to 64 single-byte characters, including0-9a-zA-Z!"#$%'()+,-./:;<=>?@[\]^_'{|}. Spaces are allowed.
Background	Set how the screen background looks. To use a graphic, select Picture and upload a graphic. Specify the location and file name of the logo graphic or click Browse to locate it. The picture's size cannot be over 438 x 337 pixels. Note: Use a GIF, JPG, or PNG of 100 kilobytes or less. To use a color, select Color and specify the color.
Customized Access Page	Use this section to customize the page that displays after an access user logs into the Web Configurator to access network services like the Internet.
Title	Enter the title for the top of the screen. Use up to 64 printable ASCII characters. Spaces are allowed.
Message Color	Specify the color of the screen's text.
Note Message	Enter a note to display below the title. Use up to 64 printable ASCII characters. Spaces are allowed.
Background	Set how the window's background looks. To use a graphic, select Picture and upload a graphic. Specify the location and file name of the logo graphic or click Browse to locate it. The picture's size cannot be over 438 x 337 pixels. Note: Use a GIF, JPG, or PNG of 100 kilobytes or less. To use a color, select Color and specify the color.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

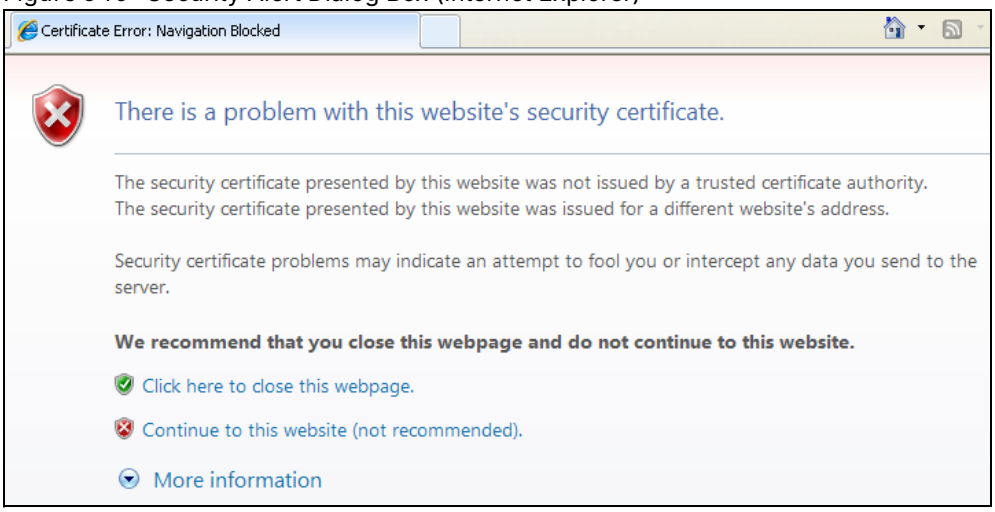
32.7.7 HTTPS Example

If you haven't changed the default HTTPS port on the Zyxel Device, then in your browser enter "https://Zyxel Device IP Address/" as the web site address where "Zyxel Device IP Address" is the IP address or domain name of the Zyxel Device you wish to access.

32.7.7.1 Internet Explorer Warning Messages

When you attempt to access the Zyxel Device HTTPS server, you will see the error message shown in the following screen.

Figure 540 Security Alert Dialog Box (Internet Explorer)



Select Continue to this website to proceed to the Web Configurator login screen. Otherwise, select Click here to close this web page to block the access.

32.7.7.2 Mozilla Firefox Warning Messages

When you attempt to access the Zyxel Device HTTPS server, a The Connection is Untrusted screen appears as shown in the following screen. Click Technical Details if you want to verify more information about the certificate from the Zyxel Device.

Select I Understand the Risks and then click Add Exception to add the Zyxel Device to the security exception list. Click Confirm Security Exception.

Figure 541 Security Certificate 1 (Firefox)

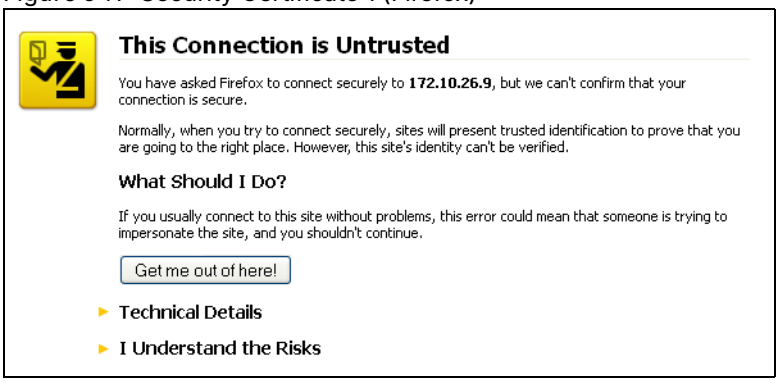
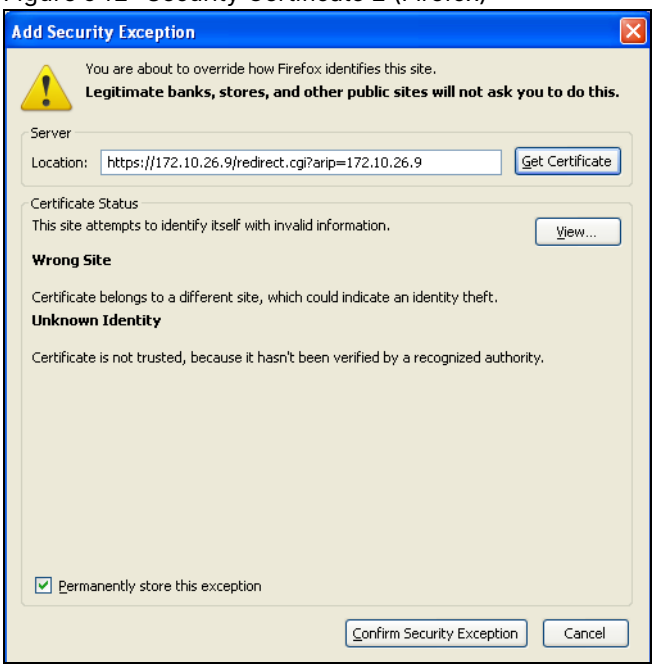


Figure 542 Security Certificate 2 (Firefox)



32.7.7.3 Avoiding Browser Warning Messages

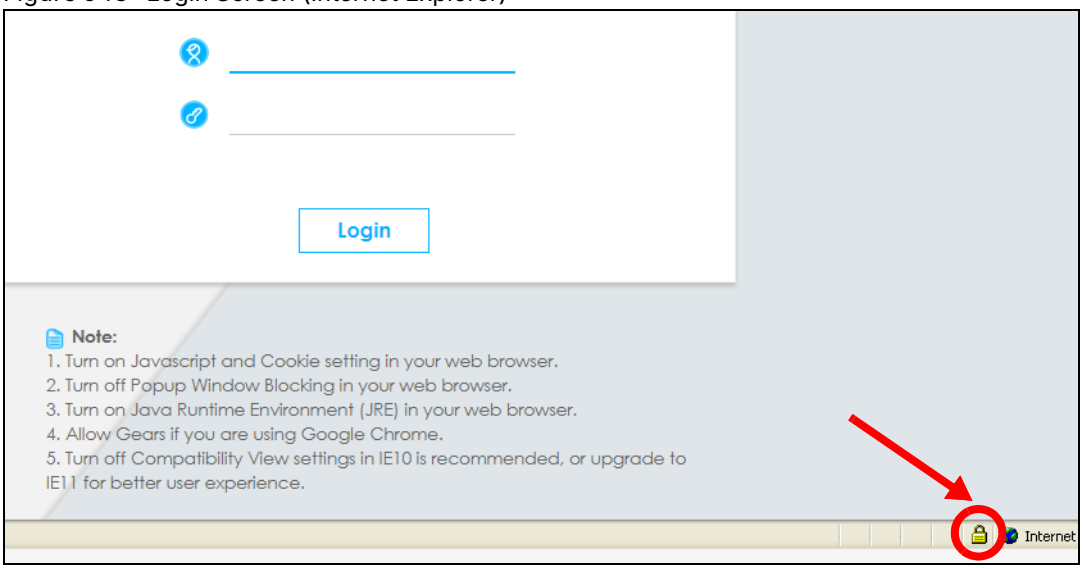
Here are the main reasons your browser displays warnings about the Zyxel Device's HTTPS server certificate and what you can do to avoid seeing the warnings:

- The issuing certificate authority of the Zyxel Device's HTTPS server certificate is not one of the browser's trusted certificate authorities. The issuing certificate authority of the Zyxel Device's factory default certificate is the Zyxel Device itself since the certificate is a self-signed certificate.
- For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.
- To have the browser trust the certificates issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certificate.

32.7.7.4 Login Screen

After you accept the certificate, the Zyxel Device login screen appears. The lock displayed in the bottom of the browser status bar denotes a secure connection.

Figure 543 Login Screen (Internet Explorer)



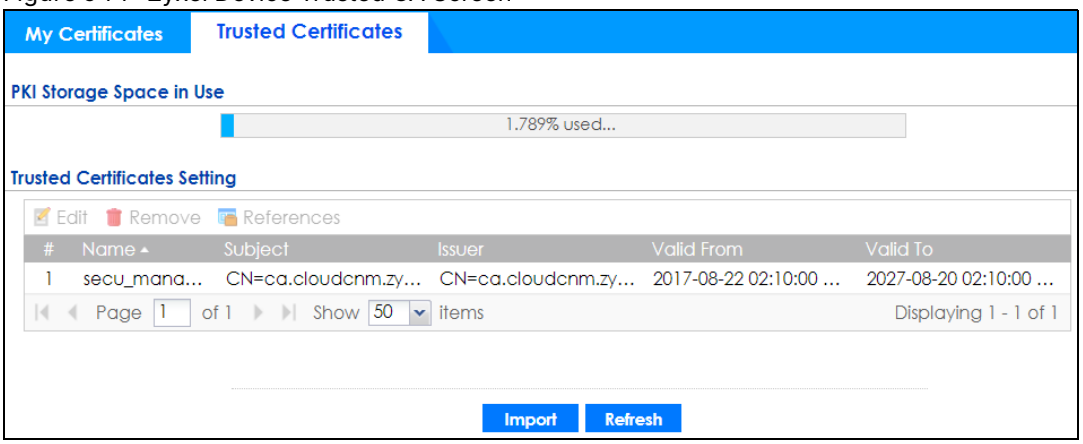
32.7.7.5 Enrolling and Importing SSL Client Certificates

The SSL client needs a certificate if Authenticate Client Certificates is selected on the Zyxel Device.

You must have imported at least one trusted CA to the Zyxel Device in order for the Authenticate Client Certificates to be active (see the Certificates chapter for details).

Apply for a certificate from a Certification Authority (CA) that is trusted by the Zyxel Device (see the Zyxel Device's Trusted CA Web Configurator screen).

Figure 544 Zyxel Device Trusted CA Screen

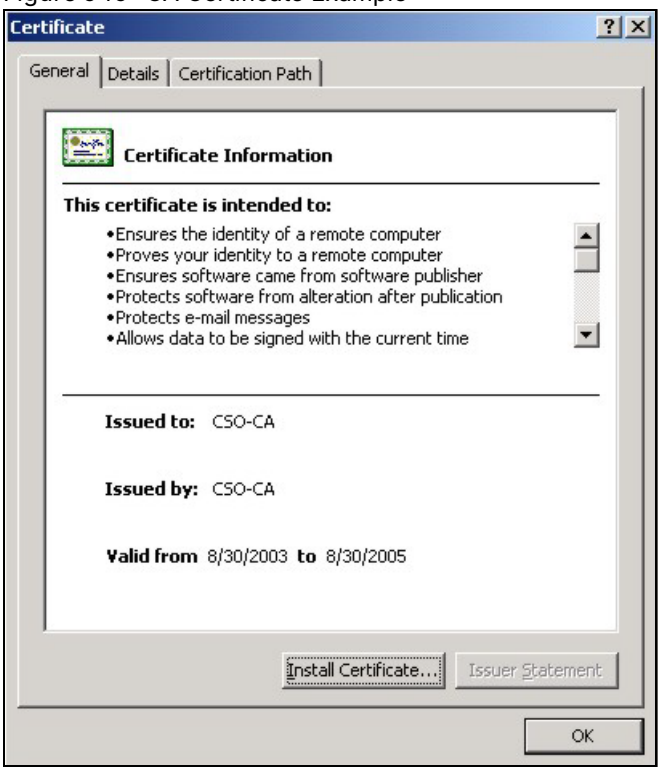


The CA sends you a package containing the CA's trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

32.7.7.5.1 Installing the CA's Certificate

1 Double click the CA's trusted certificate to produce a screen similar to the one shown next.

Figure 545 CA Certificate Example



2 Click Install Certificate and follow the wizard as shown earlier in this appendix.

32.7.7.5.2 Installing Your Personal Certificate(s)

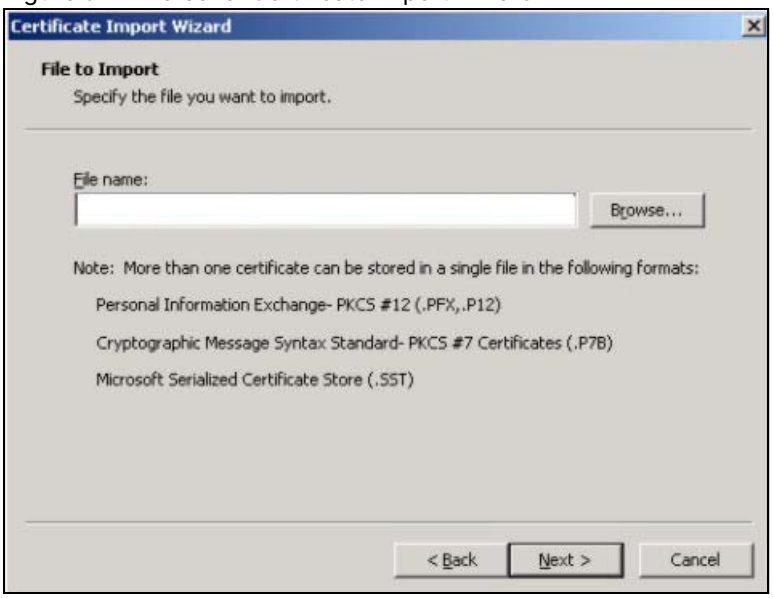
You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next

1 Click Next to begin the wizard.

Figure 546 Personal Certificate Import Wizard 1

2 The file name and path of the certificate you double-clicked should automatically appear in the File name text box. Click Browse if you wish to import a different certificate.

Figure 547 Personal Certificate Import Wizard 2

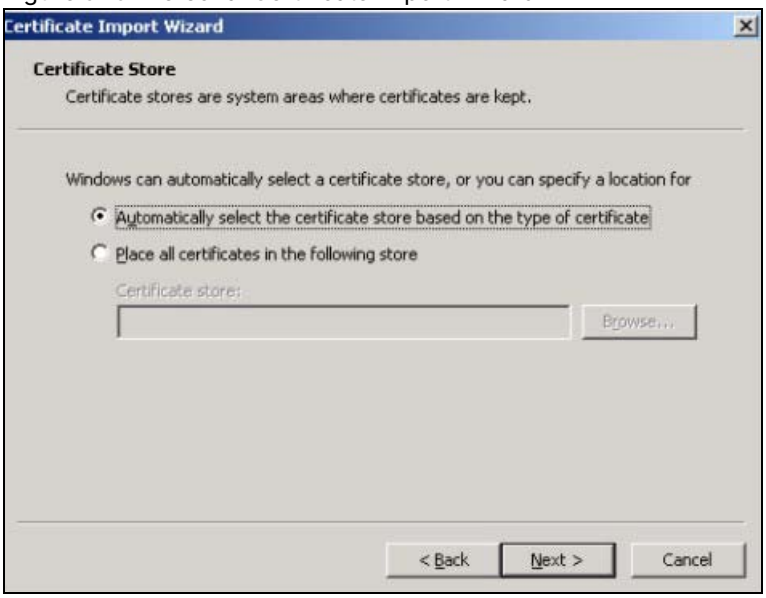


3 Enter the password given to you by the CA.

Figure 548 Personal Certificate Import Wizard 3

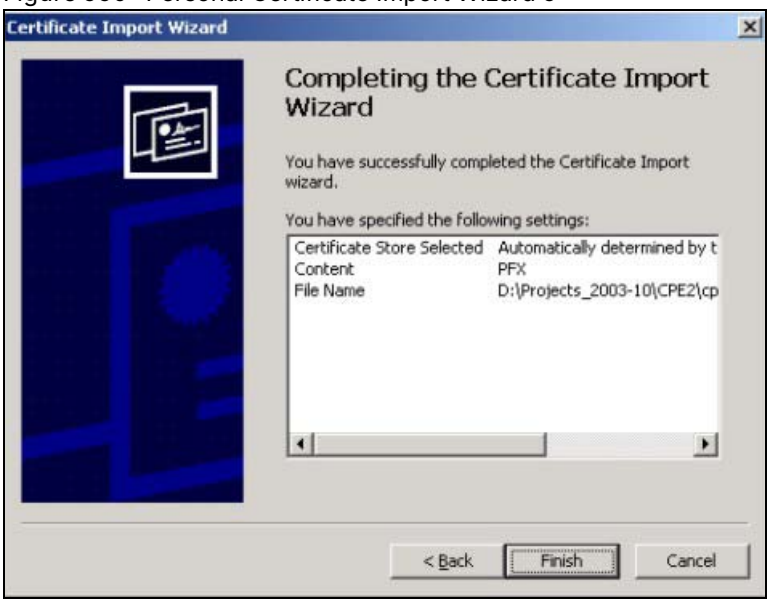
4 Have the wizard determine where the certificate should be saved on your computer or select Place all certificates in the following store and choose a different location.

Figure 549 Personal Certificate Import Wizard 4



5 Click Finish to complete the wizard and begin the import process.

Figure 550 Personal Certificate Import Wizard 5



6 You should see the following screen when the certificate is correctly installed on your computer.

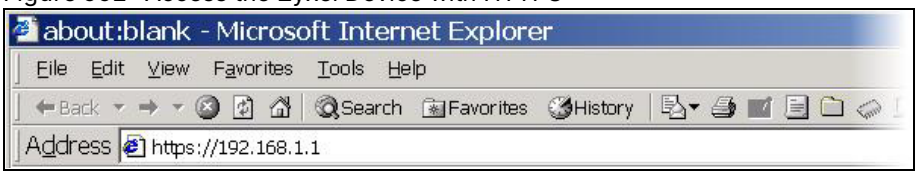
Figure 551 Personal Certificate Import Wizard 6

32.7.7.6 Using a Certificate When Accessing the Zyxel Device Example

Use the following procedure to access the Zyxel Device with HTTPS.

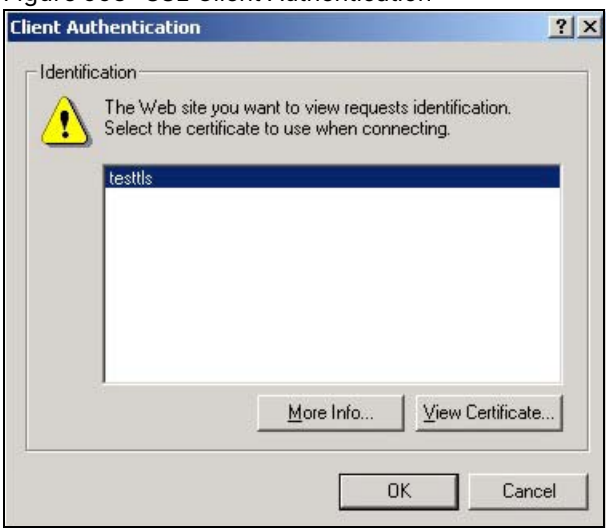
1 Enter ‘https://Zyxel Device IP Address/ in your browser’s web address field.

Figure 552 Access the Zyxel Device with HTTPS



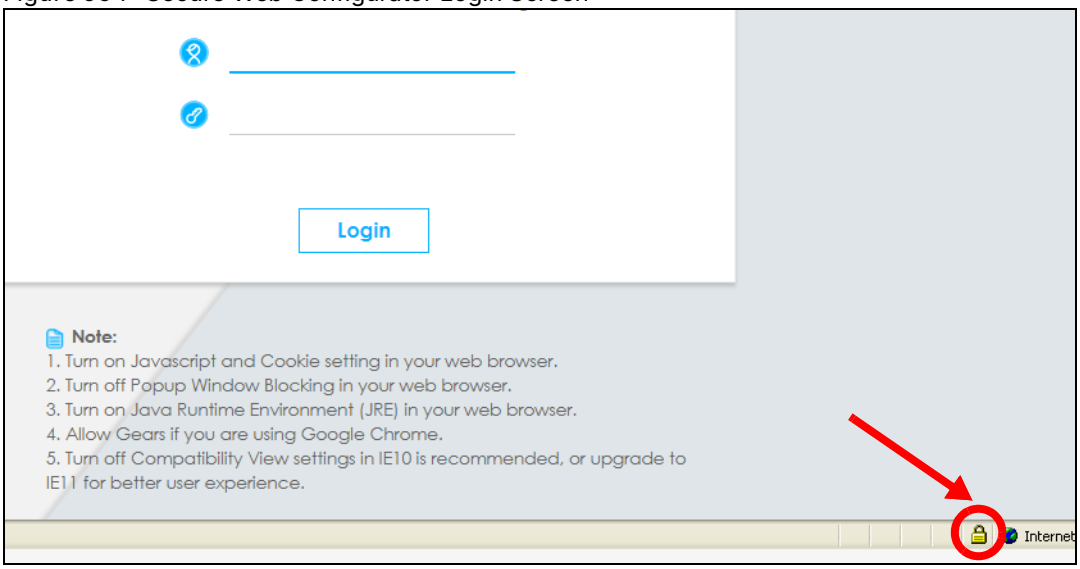
2 When Authenticate Client Certificates is selected on the Zyxel Device, the following screen asks you to select a personal certificate to send to the Zyxel Device. This screen displays even if you only have a single certificate as in the example.

Figure 553 SSL Client Authentication



3 You next see the Web Configurator login screen.

Figure 554 Secure Web Configurator Login Screen



32.8 SSH

You can use SSH (Secure SHell) to securely access the Zyxel Device's command line interface. Specify which zones allow SSH access and from which IP address the access can come.

SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. In the following figure, computer A on the Internet uses SSH to securely connect (SC) to the WAN port of the Zyxel Device for a management session.

Note: To allow an SSH connection to the Zyxel Device, add SSH in the Object > Service > Service Group > Default_Allow_WAN_To_ZyWALL service group which defines the default services allowed in the WAN_to_Device security policy.

Figure 555 SSH Communication Over the WAN Example

32.8.1 SSH Implementation on the Zyxel Device

Your Zyxel Device supports SSH version 2 using RSA authentication and four encryption methods (AES, 3DES, Archfour, and Blowfish). The SSH server is implemented on the Zyxel Device for management using port 22 (by default).

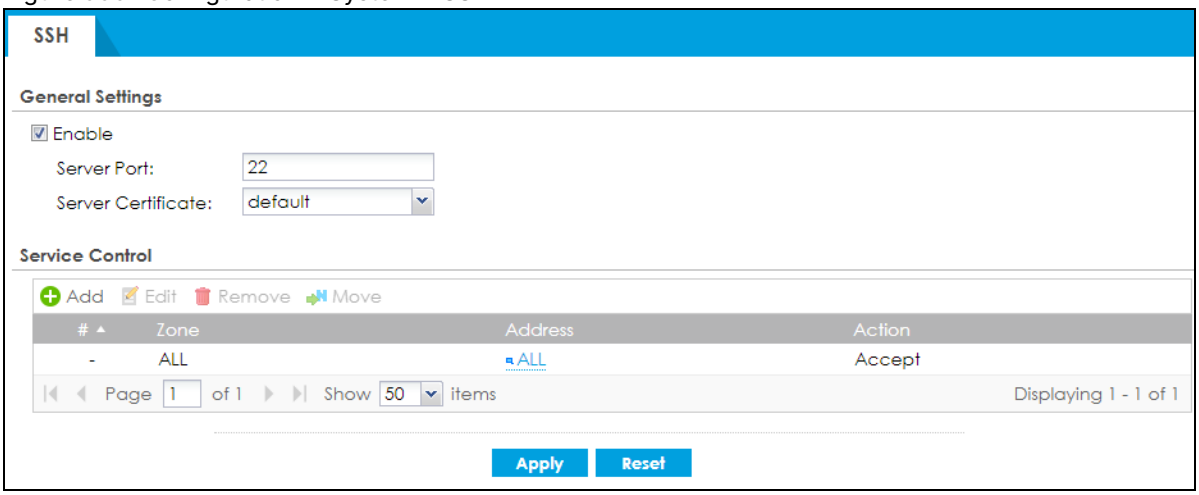
32.8.2 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the Zyxel Device over SSH.

32.8.3 Configuring SSH

Click Configuration > System > SSH to change your Zyxel Device's Secure Shell settings. Use this screen to specify from which zones SSH can be used to manage the Zyxel Device. You can also specify from which IP addresses the access can come.

Figure 556 Configuration > System > SSH



The following table describes the labels in this screen.

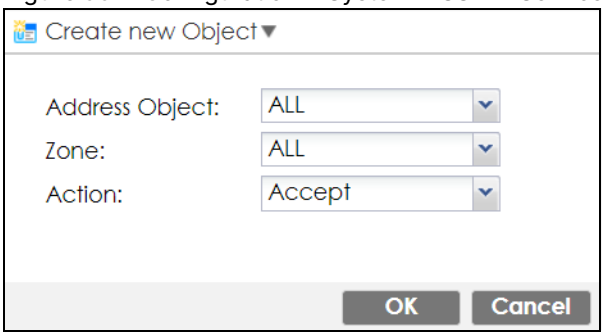
Table 288 Configuration > System > SSH

LABEL	DESCRIPTION
Enable	Select the checkbox to allow or disallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the Zyxel Device CLI using this service.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the Zyxel Device for SSH connections. You must have certificates already configured in the My Certificates screen.
Service Control	This specifies from which computers you can access which Zyxel Device zones.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry. Refer to Table 286 on page 802 for details on the screen that opens.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule.
Zone	This is the zone on the Zyxel Device the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the Zyxel Device zone(s) configured in the Zone field (Accept) or not (Deny).
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

32.8.4 Service Control Rules

Click the Add or Edit icon in the Service Control table to add a service control rule.

Figure 557 Configuration > System > SSH > Service Control Rule Add/Edit



The following table describes the labels in this screen.

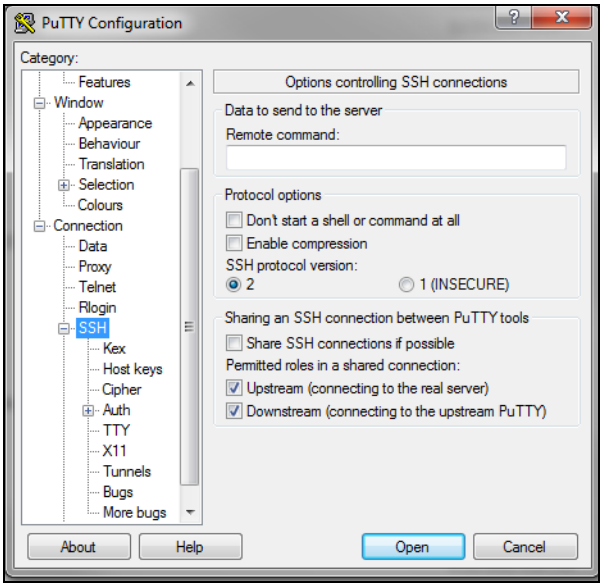
Table 289 Configuration > System > SSH > Service Control Rule Add/Edit

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Address Object	Select ALL to allow or deny any computer to communicate with the Zyxel Device using SSH. Select a predefined address object to just allow or deny the computer with the IP address that you specified to access the Zyxel Device using SSH.
Zone	Select ALL to allow or prevent any Zyxel Device zones from being accessed using SSH. Select a predefined Zyxel Device zone on which a incoming service is allowed or denied.
Action	Select Accept to allow the user to access the Zyxel Device from the specified computers. Select Deny to block the user's access to the Zyxel Device from the specified computers.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

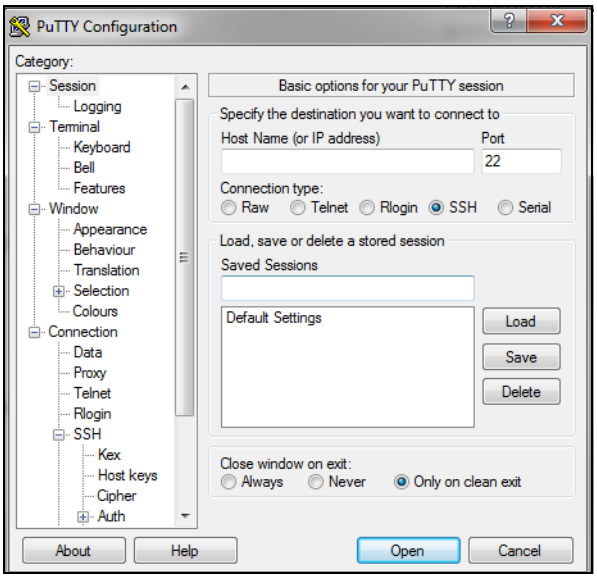
32.8.5 SSH Example

This section shows using a PuTTY SSH client to remotely access the Zyxel Device. The configuration and connection steps are similar for most SSH client programs. Refer to your SSH client program user's guide.

1 Launch the SSH client and configure the SSH client to use SSH version 2.



2 Specify the connection information (IP address, port number) for the Zyxel Device.



3 A command window displays. Enter the password to log in to the Zyxel Device.

```
login as: admin
Using keyboard-interactive authentication.
Password:
% session is not found
Bad terminal type: "xterm". Will assume vt100.
Router> enable
Router#
```

32.9 Telnet

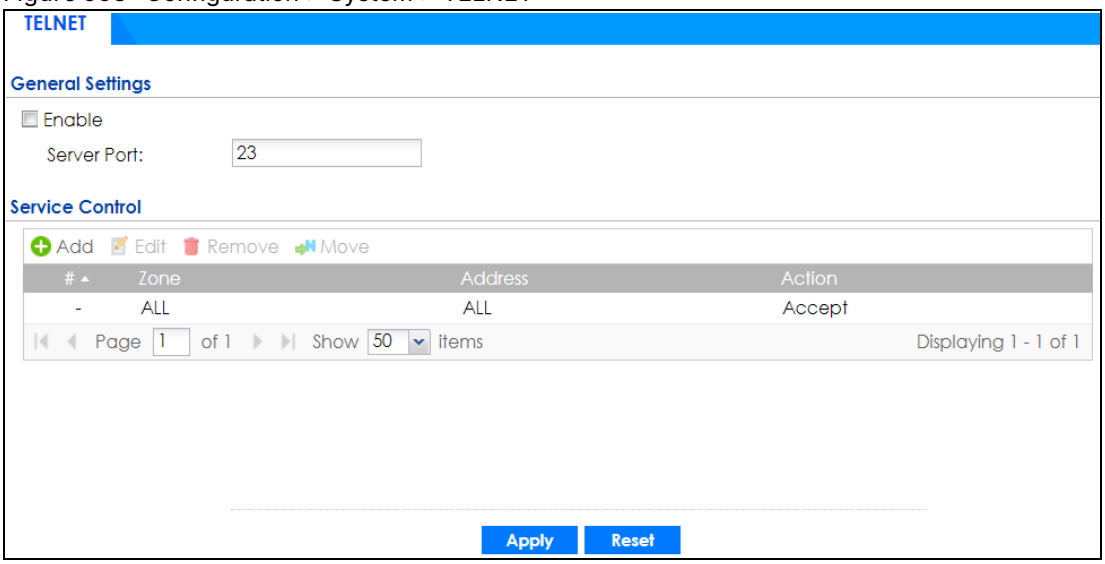
You can use Telnet to access the Zyxel Device's command line interface. Specify which zones allow Telnet access and from which IP address the access can come.

32.9.1 Configuring Telnet

Click Configuration > System > TELNET to configure your Zyxel Device for remote Telnet access. Use this screen to specify from which zones Telnet can be used to manage the Zyxel Device. You can also specify from which IP addresses the access can come.

Note: To allow a Telnet connection to the Zyxel Device, add Telnet in the Object > Service > Service Group > Default_Allow_WAN_To_ZyWALL service group which defines the default services allowed in the WAN_to_Device security policy.

Figure 558 Configuration > System > TELNET



The following table describes the labels in this screen.

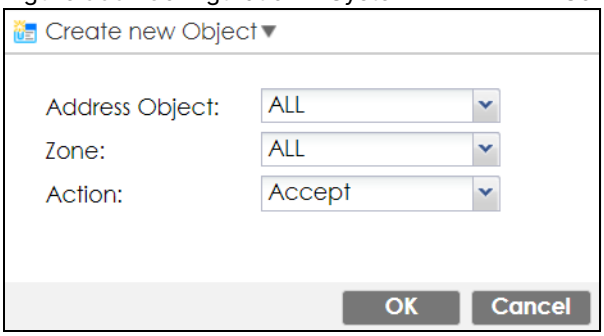
Table 290 Configuration > System > TELNET

LABEL	DESCRIPTION
Enable	Select the checkbox to allow or disallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the Zyxel Device CLI using this service.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Service Control	This specifies from which computers you can access which Zyxel Device zones.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry. Refer to Table 286 on page 802 for details on the screen that opens.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule. The entry with a hyphen (-) instead of a number is the Zyxel Device's (non-configurable) default policy. The Zyxel Device applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the Zyxel Device will not have to use the default policy.
Zone	This is the zone on the Zyxel Device the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the Zyxel Device zone(s) configured in the Zone field (Accept) or not (Deny).
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

32.9.2 Service Control Rules

Click the Add or Edit icon in the Service Control table to add a service control rule.

Figure 559 Configuration > System > TELNET > Service Control Rule Add/Edit



The following table describes the labels in this screen.

Table 291 Configuration > System > TELNET > Service Control Rule Add/Edit

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Address Object	Select ALL to allow or deny any computer to communicate with the Zyxel Device using Telnet. Select a predefined address object to just allow or deny the computer with the IP address that you specified to access the Zyxel Device using Telnet.
Zone	Select ALL to allow or prevent any Zyxel Device zones from being accessed using Telnet. Select a predefined Zyxel Device zone on which a incoming service is allowed or denied.
Action	Select Accept to allow the user to access the Zyxel Device from the specified computers. Select Deny to block the user's access to the Zyxel Device from the specified computers.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

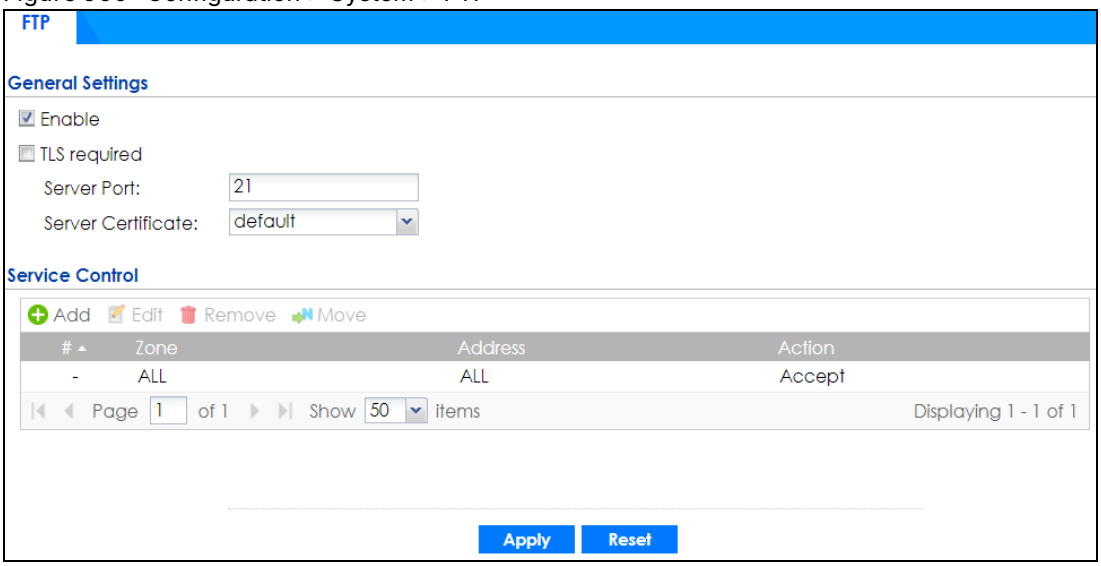
32.10 FTP

You can upload and download the Zyxel Device's firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

32.10.1 Configuring FTP

To change your Zyxel Device's FTP settings, click Configuration > System > FTP tab. The screen appears as shown. Use this screen to specify from which zones FTP can be used to access the Zyxel Device. You can also specify from which IP addresses the access can come.

Figure 560 Configuration > System > FTP



The following table describes the labels in this screen.

Table 292 Configuration > System > FTP

LABEL	DESCRIPTION
Enable	Select the checkbox to allow or disallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the Zyxel Device using this service.
TLS required	Select the checkbox to use FTP over TLS (Transport Layer Security) to encrypt communication. This implements TLS as a security mechanism to secure FTP clients and/or servers.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the Zyxel Device for FTP connections. You must have certificates already configured in the My Certificates screen.
Service Control	This specifies from which computers you can access which Zyxel Device zones.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry. Refer to Table 286 on page 802 for details on the screen that opens.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule. The entry with a hyphen (-) instead of a number is the Zyxel Device's (non-configurable) default policy. The Zyxel Device applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the Zyxel Device will not have to use the default policy.
Zone	This is the zone on the Zyxel Device the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the Zyxel Device zone(s) configured in the Zone field (Accept) or not (Deny).

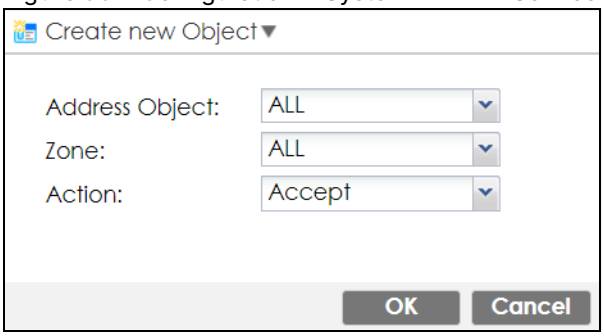
Table 292 Configuration > System > FTP (continued)

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.

32.10.2 Service Control Rules

Click the Add or Edit icon in the Service Control table to add a service control rule.

Figure 561 Configuration > System > FTP > Service Control Rule Add/Edit



The following table describes the labels in this screen.

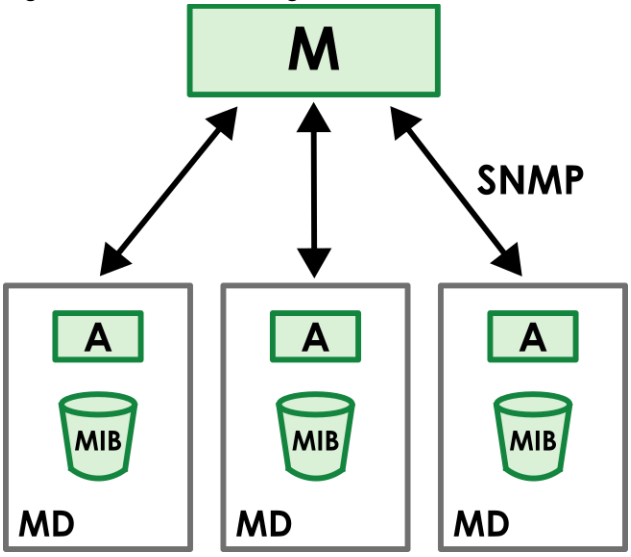
Table 293 Configuration > System > FTP > Service Control Rule Add/Edit

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Address Object	Select ALL to allow or deny any computer to communicate with the Zyxel Device using FTP. Select a predefined address object to just allow or deny the computer with the IP address that you specified to access the Zyxel Device using FTP.
Zone	Select ALL to allow or prevent any Zyxel Device zones from being accessed using FTP. Select a predefined Zyxel Device zone on which a incoming service is allowed or denied.
Action	Select Accept to allow the user to access the Zyxel Device from the specified computers. Select Deny to block the user's access to the Zyxel Device from the specified computers.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

32.11 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your Zyxel Device supports SNMP agent functionality, which allows a manager station to manage and monitor the Zyxel Device through the network. The Zyxel Device supports SNMP version one (SNMPv1), version two (SNMPv2c) and version 3 (SNMPv3). The next figure illustrates an SNMP management operation.

Figure 562 SNMP Management Model



An SNMP managed network consists of two main types of component: agents (A) and a manager (M).

An agent is a management software module that resides in a managed device (MD, the Zyxel Device). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

32.11.1 SNMPv3 and Security

SNMPv3 enhances security for SNMP management using authentication and encryption. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

32.11.2 Supported MIBs

The Zyxel Device supports MIB II that is defined in RFC-1213 and RFC-1215. The Zyxel Device also supports private MIBs to collect information about CPU and memory usage and VPN total throughput. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance. You can download the Zyxel Device's MIBs from www.zyxel.com.

32.11.3 SNMP Traps

The Zyxel Device will send traps to the SNMP manager when any one of the following events occurs.

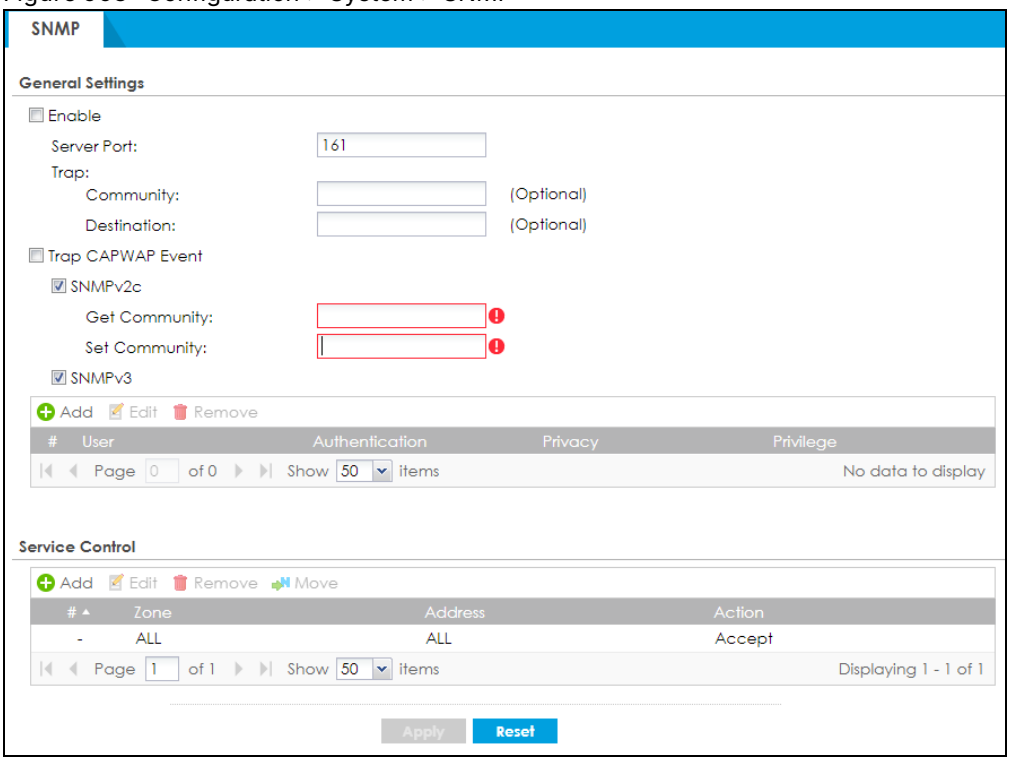
Table 294 SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the Zyxel Device is turned on or an agent restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.
vpnTunnelDisconnected	1.3.6.1.4.1.890.1.6.22.2.3	This trap is sent when an IPSec VPN tunnel is disconnected.
vpnTunnelName	1.3.6.1.4.1.890.1.6.22.2.2.1.1	This trap is sent along with the vpnTunnelDisconnected trap. This trap carries the disconnected tunnel's IPSec SA name.
vpnIKEName	1.3.6.1.4.1.890.1.6.22.2.2.1.2	This trap is sent along with the vpnTunnelDisconnected trap. This trap carries the disconnected tunnel's IKE SA name.
vpnTunnelSPI	1.3.6.1.4.1.890.1.6.22.2.2.1.3	This trap is sent along with the vpnTunnelDisconnected trap. This trap carries the security parameter index (SPI) of the disconnected VPN tunnel.

32.11.4 Configuring SNMP

To change your Zyxel Device's SNMP settings, click Configuration > System > SNMP tab. The screen appears as shown. Use this screen to configure your SNMP settings, including from which zones SNMP can be used to access the Zyxel Device. You can also specify from which IP addresses the access can come.

Figure 563 Configuration > System > SNMP



The following table describes the labels in this screen.

Table 295 Configuration > System > SNMP

LABEL	DESCRIPTION
Enable	Select the checkbox to allow or disallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the Zyxel Device using this service.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests. You can use up to 64 single-byte characters, including 0-9a-zA-Z_.-. The first character cannot be a period (.).
Destination	Type the IP address of the station to send your SNMP traps to.
Trap CAPWAP Event	Select this option to have the Zyxel Device send a trap to the SNMP manager when a managed AP is connected to or disconnected from the Zyxel Device.
SNMPv2c	Select the SNMP version for the Zyxel Device. The SNMP version on the Zyxel Device must match the version on the SNMP manager.
Get Community	Enter the Get Community, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests. You can use up to 64 single-byte characters, including 0-9a-zA-Z_.-. The first character cannot be a period (.).
Set Community	Enter the Set community, which is the password for incoming Set requests from the management station. The default is private and allows all requests.

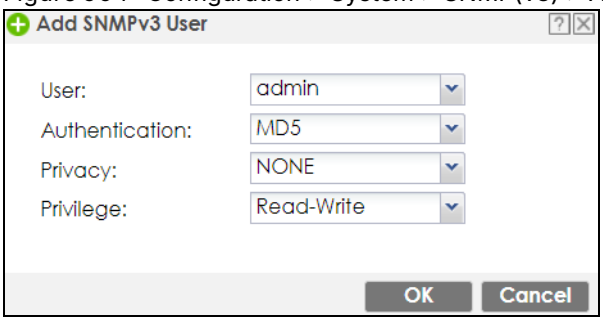
Table 295 Configuration > System > SNMP (continued)

LABEL	DESCRIPTION
SNMPv3	Select the SNMP version for the Zyxel Device. The SNMP version on the Zyxel Device must match the version on the SNMP manager. SNMPv3 (RFCs 3413 to 3415) provides secure access by authenticating and encrypting data packets over the network. The Zyxel Device uses your login password as the SNMPv3 authentication and encryption passphrase. Note: Your login password must consist of at least 8 printable characters for SNMPv3. An error message will display if your login password has fewer characters.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
#	This is the index number of the entry.
User	This displays the name of the user object to be sent to the SNMP manager along with the SNMP v3 trap.
Authentication	This displays the authentication algorithm used for this entry. MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.
Privacy	This displays the encryption method for SNMP communication from this user. Methods available are: • DES - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. • AES - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.
Privilege	This displays the access rights to MIBs. • Read-Write - The associated user can create and edit the MIBs on the Zyxel Device, except the user account. • Read-Only - The associated user can only collect information from the Zyxel Device MIBs.
Service Control	This specifies from which computers you can access which Zyxel Device zones.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry. Refer to Table 286 on page 802 for details on the screen that opens.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Move	To change an entry's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed.
#	This the index number of the service control rule. The entry with a hyphen (-) instead of a number is the Zyxel Device's (non-configurable) default policy. The Zyxel Device applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the Zyxel Device will not have to use the default policy.
Zone	This is the zone on the Zyxel Device the user is allowed or denied to access.
Address	This is the object name of the IP address(es) with which the computer is allowed or denied to access.
Action	This displays whether the computer with the IP address specified above can access the Zyxel Device zone(s) configured in the Zone field (Accept) or not (Deny).
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

32.11.5 Add SNMPv3 User

Click Add under SNMPv3 in Configuration > System > SNMP to create an SNMPv3 user for authentication with managers using SNMP v3. Use the username and password of the login accounts you specify in this screen to create accounts on the SNMP v3 manager.

Figure 564 Configuration > System > SNMP(v3) > Add



The following table describes the labels in this screen.

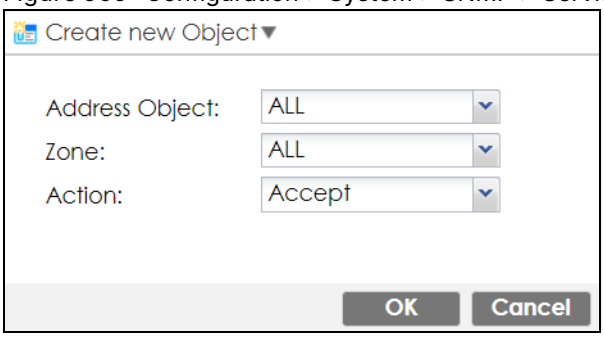
Table 296 Configuration > System > SNMP(v3) > Add

LABEL	DESCRIPTION
User	Specify the username of a login account on the Zyxel Device. The associated password is used in authentication algorithms and encryption methods.
Authentication	Select an authentication algorithm. MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.
Privacy	Specify the encryption method for SNMP communication from this user. You can choose one of the following: • DES - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. • AES - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.
Privilege	Select the access rights to MIBs. • Read-Write - The associated user can create and edit the MIBs on the Zyxel Device, except the user account. • Read-Only - The associated user can only collect information from the Zyxel Device MIBs.
OK	Click OK to save the changes.
Cancel	Click Cancel to begin configuring this screen afresh.

32.11.6 Service Control Rules

Click the Add or Edit icon in the Service Control table to add a service control rule.

Figure 565 Configuration > System > SNMP > Service Control Rule Add/Edit



The following table describes the labels in this screen.

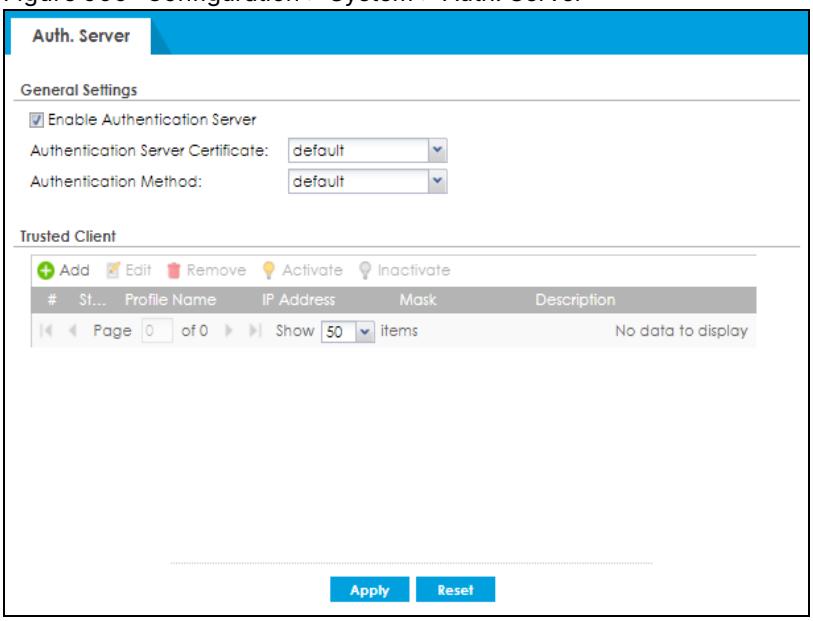
Table 297 Configuration > System > SNMP > Service Control Rule Add/Edit

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Address Object	Select ALL to allow or deny any computer to communicate with the Zyxel Device using SNMP. Select a predefined address object to just allow or deny the computer with the IP address that you specified to access the Zyxel Device using SNMP.
Zone	Select ALL to allow or prevent any Zyxel Device zones from being accessed using SNMP. Select a predefined Zyxel Device zone on which a incoming service is allowed or denied.
Action	Select Accept to allow the user to access the Zyxel Device from the specified computers. Select Deny to block the user's access to the Zyxel Device from the specified computers.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

32.12 Authentication Server

You can set the Zyxel Device to work as a RADIUS server to exchange messages with a RADIUS client, such as an AP for user authentication and authorization. Click Configuration > System > Auth. Server tab. The screen appears as shown. Use this screen to enable the authentication server feature of the Zyxel Device and specify the RADIUS client's IP address.

Figure 566 Configuration > System > Auth. Server



The following table describes the labels in this screen.

Table 298 Configuration > System > Auth. Server

LABEL	DESCRIPTION
Enable Authentication Server	Select the checkbox to have the Zyxel Device act as a RADIUS server.
Authentication Server Certificate	Select the certificate whose corresponding private key is to be used to identify the Zyxel Device to the RADIUS client. You must have certificates already configured in the My Certificates screen.
Authentication Method	Select an authentication method if you have created any in the Configuration > Object > Auth. Method screen.
Trusted Client	Use this section to configure trusted clients in the Zyxel Device RADIUS server database.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
#	This is the index number of the entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Profile Name	This field indicates the name assigned to the profile.
IP Address	This is the IP address of the RADIUS client that is allowed to exchange messages with the Zyxel Device.
Netmask	This is the subnet mask of the RADIUS client.
Secret	Enter a shared key used to authenticate the managed AP. The key is encrypted before being saved to the Zyxel Device. You can use the following characters: 0-9a-zA-Z`~!@#$%^&*()_\-+={}\\|\\;:'<,>\?.\ for your password.

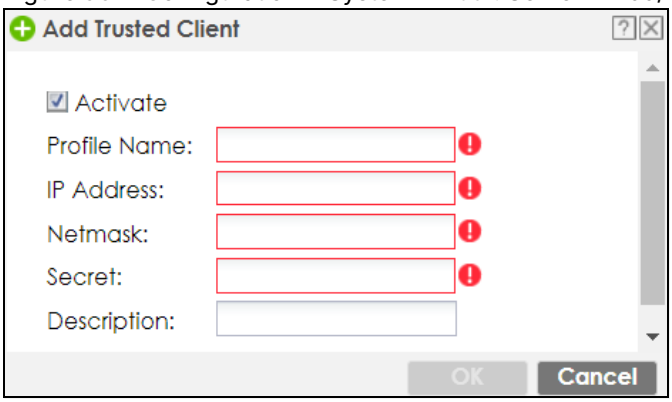
Table 298 Configuration > System > Auth. Server (continued)

LABEL	DESCRIPTION
Description	This is the description of the RADIUS client.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

32.12.1 Add/Edit Trusted RADIUS Client

Click Configuration > System > Auth. Server to display the Auth. Server screen. Click the Add icon or an Edit icon to display the following screen. Use this screen to create a new entry or edit an existing one.

Figure 567 Configuration > System > Auth. Server > Add/Edit



The following table describes the labels in this screen.

Table 299 Configuration > System > Auth. Server > Add/Edit

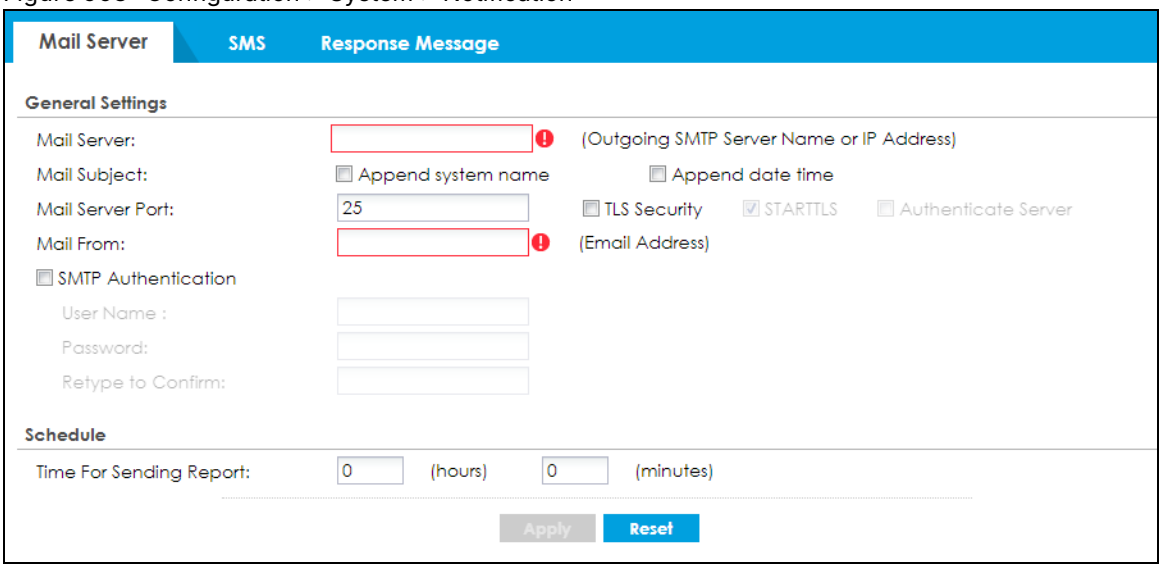
LABEL	DESCRIPTION
Activate	Select this checkbox to make this profile active.
Profile Name	Enter a descriptive name (up to 31 alphanumerical characters) for identification purposes.
IP Address	Enter the IP address of the RADIUS client that is allowed to exchange messages with the Zyxel Device.
Netmask	Enter the subnet mask of the RADIUS client.
Secret	Enter a password (up to 64 alphanumeric characters) as the key to be shared between the Zyxel Device and the RADIUS client. The key is not sent over the network. This key must be the same on the external authentication server and the Zyxel Device.
Description	Enter the description of each server, if any. You can use 1 to 60 single-byte characters, including 0-9a-zA-Z!"#$%'()*+,-/:;=?@_ &.<>[\]^'{|} are not allowed.
OK	Click OK to save the changes.
Cancel	Click Cancel to discard the changes.

32.13 Notification > Mail Server

Use this screen to configure a mail server so you can receive reports and notification emails such as when your password is about to expire. After you configure the screen, you can test the settings in Maintenance > Diagnostics > Network Tool and then select Test Email Server. See Configuration > Log & Report > Email Daily Report to configure what reports to send and to whom.

Click Configuration > System > Notification to display the Mail Server screen.

Figure 568 Configuration > System > Notification



The following table describes the labels in this screen.

Table 300 Configuration > System > Notification

LABEL	DESCRIPTION
Mail Server	Type the name or IP address of the outgoing SMTP server.
Mail Subject	Go to Configuration > Log & Report > Email Daily Report to type a subject line for outgoing email from the Zyxel Device.
Append system name	Select Append system name to add the Zyxel Device's system name to the subject.
Append date time	Select Append date time to add the Zyxel Device's system date and time to the subject.
Mail Server Port	Enter the same port number here as is on the mail server for mail traffic.
TLS Security	Select this option if the mail server uses Transport Layer Security (TLS) for encrypted communications between the mail server and the Zyxel Device.
STARTTLS	Select this option if the mail server uses SSL or TLS for encrypted communications between the mail server and the Zyxel Device.
Authenticate Server	Select this if the Zyxel Device authenticates the mail server in the TLS handshake.
Mail From	Type the email address from which the outgoing email is delivered. This address is used in replies.
SMTP Authentication	Select this checkbox if it is necessary to provide a user name and password to the SMTP server.

Table 300 Configuration > System > Notification (continued)

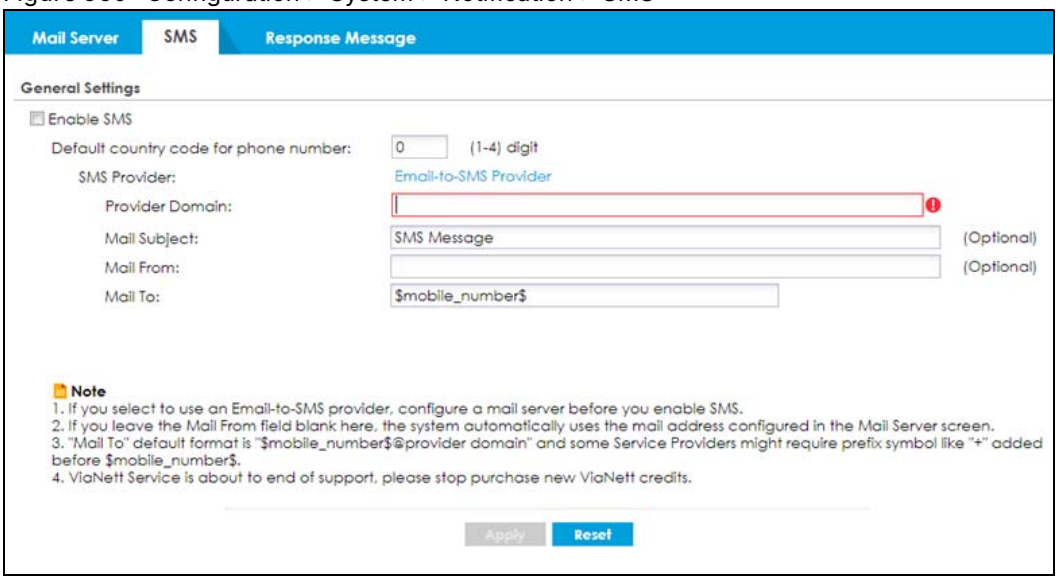
LABEL	DESCRIPTION
User Name	This box is effective when you select the SMTP Authentication checkbox. Type the user name to provide to the SMTP server when the log is emailed. Note: Make sure this User Name and Mail From email addressess are the same.
Password	This box is effective when you select the SMTP Authentication checkbox. Type a password to provide to the SMTP server when the log is emailed. Use up to 63 characters, including 0-9a-zA-Z'~!@#$%^&*()_+={}|\;:"<>'./
Retype to Confirm	Type the password again to make sure that you have entered is correctly.
Time for sending report	Select the time of day (hours and minutes) when the log is emailed. Use 24-hour 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.

32.14 Notification > SMS

The Zyxel Device supports Short Message Service (SMS) to send short text messages to mobile phone devices.

Click Configuration > System > Notification > SMS to open the following screen.

Figure 569 Configuration > System > Notification > SMS



The following table describes the labels in this screen.

Table 301 Configuration > System > Notification > SMS

LABEL	DESCRIPTION
General Settings	
Enable SMS	Select the checkbox to turn on the SMS service.

Table 301 Configuration > System > Notification > SMS (continued)

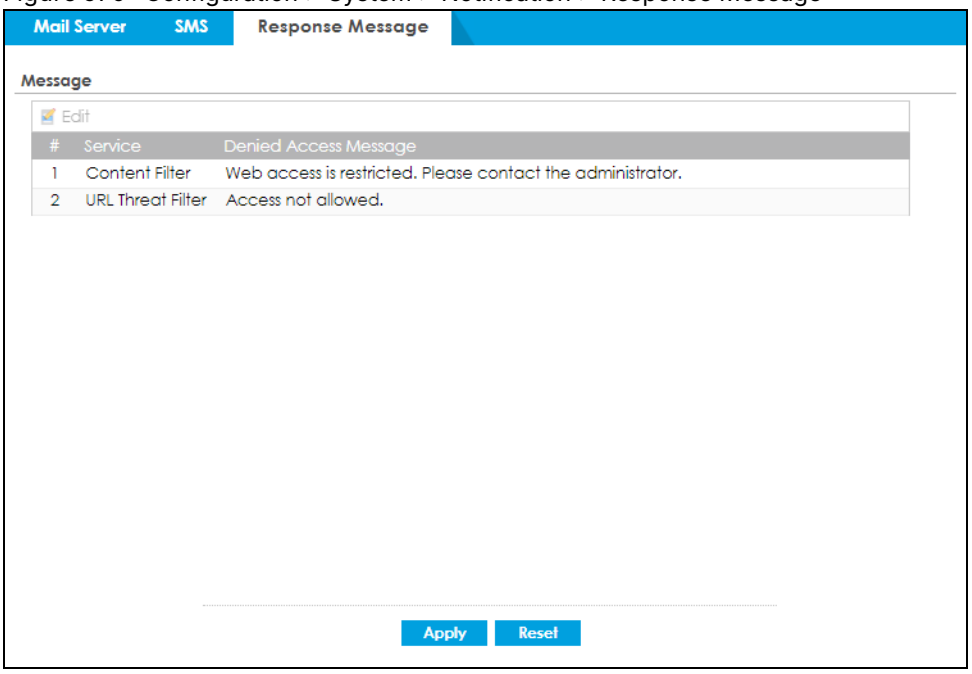
LABEL	DESCRIPTION
Default country code for phone number	Enter the default country code for the mobile phone number to which you want to send SMS messages.
SMS Provider	The Zyxel Device uses Email-to-SMS Provider to forward SMS messages. Note: Go to the Configuration > System > Notification > Mail Server screen to configure a mail server to allow the Zyxel Device to send SMS messages to the SMS service provider using emails.
Provider Domain	Enter the domain name of your SMS service provider. The domain name can be of up to 252 characters. Select auto append to "Mail to" to add the domain name of your SMS service provider after the mobile phone number in the Mail To field.
Mail Subject	Type the subject line of up to 128 characters for outgoing e-mail from the Zyxel Device.
Mail From	Enter the sender's email address of up to 64 characters. This email address needs to be in your SMS provider's allowed sender address list. If you leave this field blank, the Zyxel Device will use the IP address or domain name of the Mail Server field in the Configuration > System > Notification > Mail Server screen.
Mail To	Enter the mobile phone number of up to 80 characters. You can only have one receiver. Use this variable in brackets [$mobile_number$], and the Zyxel Device will use the mobile phone number of the user logging in. Go to the Configuration > Object > User/Group > User screen to add a valid mobile telephone number for a user.
Apply	Click this button to save your changes to the Zyxel Device.
Reset	Click this button to return the screen to its last-saved settings.

32.15 Notification > Response Message

Use this screen to create a web page when access to a website is restricted due to a security service.

Click Configuration > System > Notification > Response Message to open the following screen.

Figure 570 Configuration > System > Notification > Response Message



The following table describes the labels in this screen.

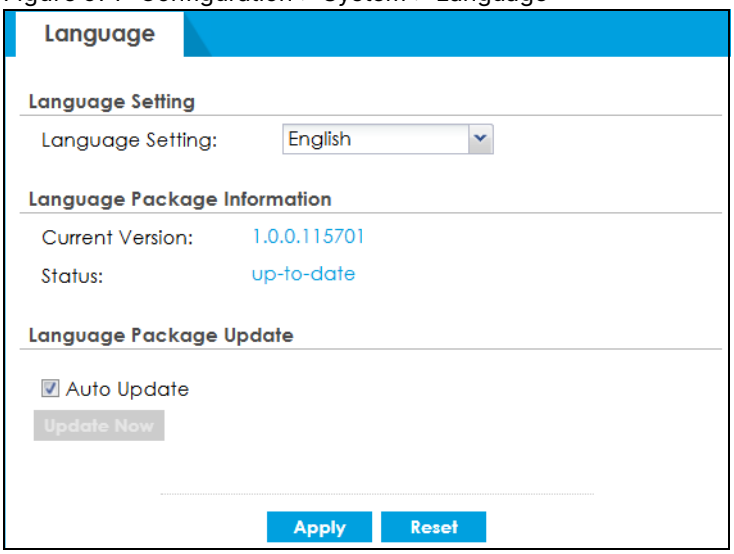
Table 302 Configuration > System > Notification > Response Message

LABEL	DESCRIPTION
Message	Use this part of the screen to create a message to display when access to a website is blocked due to a security service.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
#	This is the index number of the entry.
Service	This is the security service that may restrict access to a website.
Denied Access Message	Type a message to display when access to a website is blocked due to this security service. You may type up to 127 characters.
Apply	Click this button to save your changes to the Zyxel Device.
Reset	Click this button to return the screen to its last-saved settings.

32.16 Language Screen

Click Configuration > System > Language to open the following screen. Use this screen to select a display language for the Zyxel Device's Web Configurator screens.

Figure 571 Configuration > System > Language



The following table describes the labels in this screen.

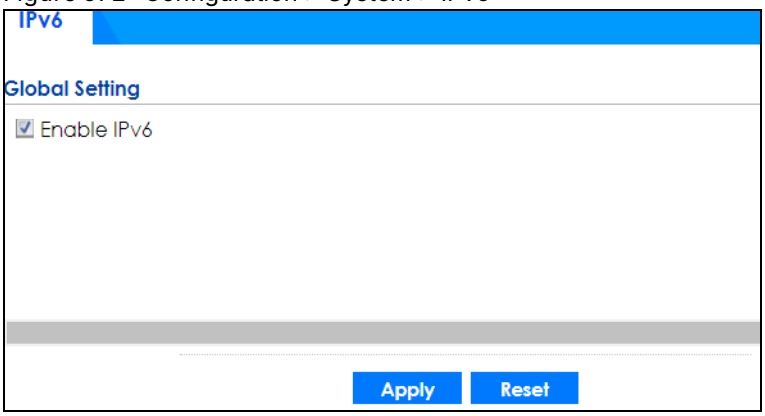
Table 303 Configuration > System > Language

LABEL	DESCRIPTION
Language Setting	Select a display language for the Zyxel Device's Web Configurator screens. You also need to open a new browser session to display the screens in the new language.
Current Version	This shows the current language package version of the Zyxel Device.
Status	This shows whether the language package of the Zyxel Device is up-to-date or not.
Auto Update	Select this to have the Zyxel Device regularly check for and download the latest language package.
Update Now	If the Status of the Language Package Information is not up-to-date, click this button to download the latest language package.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

32.17 IPv6 Screen

Click Configuration > System > IPv6 to open the following screen. Use this screen to enable IPv6 support for the Zyxel Device's Web Configurator screens.

Figure 572 Configuration > System > IPv6



The following table describes the labels in this screen.

Table 304 Configuration > System > IPv6

LABEL	DESCRIPTION
Enable IPv6	Select this to have the Zyxel Device support IPv6 and make IPv6 settings be available on the screens that the functions support, such as the Configuration > Network > Interface > Ethernet, VLAN, and Bridge screens. The Zyxel Device discards all IPv6 packets if you clear this checkbox.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

32.18 Zyxel One Network (ZON) Utility

The Zyxel One Network (ZON) utility uses the Zyxel Discovery Protocol (ZDP) for discovering and configuring ZDP-aware Zyxel devices in the same broadcast domain as the computer on which ZON is installed.

The ZON Utility issues requests through ZDP and in response to the query, the Zyxel device responds with basic information including IP address, firmware version, location, system and model name. The information is then displayed in the ZON Utility screen and you can perform tasks like basic configuration of the devices and batch firmware upgrade in it. You can download the ZON Utility at www.zyxel.com and install it on a computer.

32.18.1 Requirements

Before installing the ZON Utility on your computer, please make sure it meets the requirements listed below.

Operating System

At the time of writing, the ZON Utility is compatible with:

- Windows 7 (both 32-bit / 64-bit versions)
- Windows 8 (both 32-bit / 64-bit versions)
- Windows 8.1 (both 32-bit / 64-bit versions)

- Window 10 (both 32-bit / 64-bit versions)

Note: To check for your Windows operating system version, right-click on My Computer > Properties. You should see this information in the General tab.

Hardware

Here are the minimum hardware requirements to use the ZON Utility on your computer.

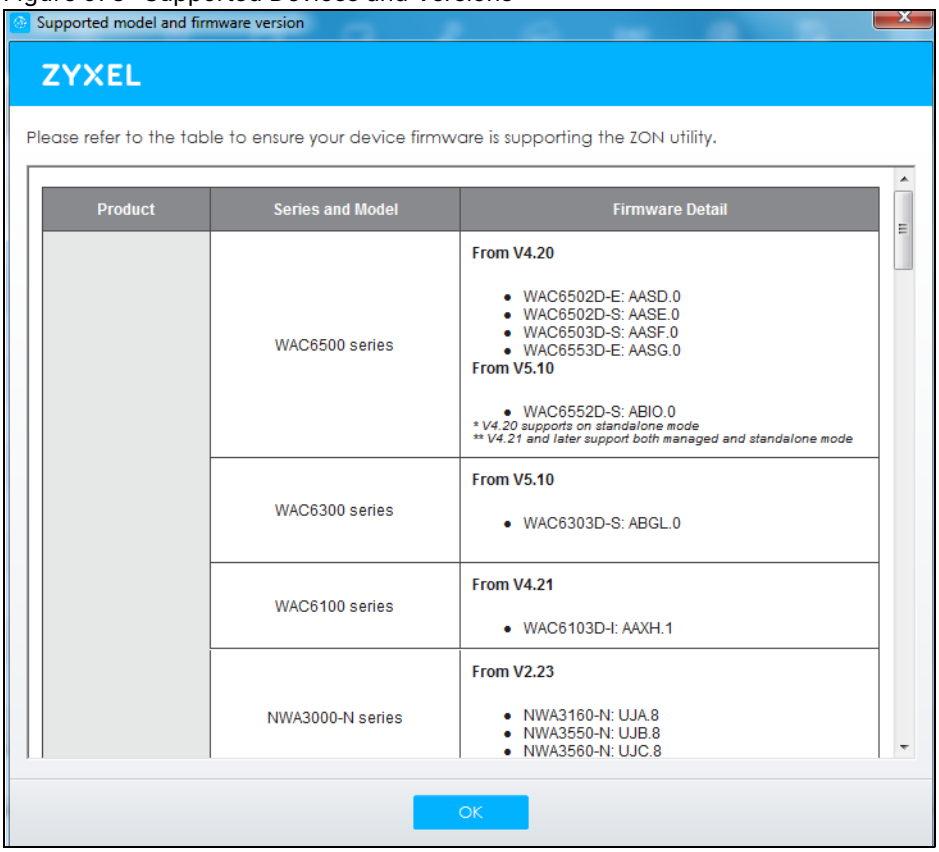
- Core i3 processor
- 2GB RAM
- 100MB free hard disk
- WXGA (Wide XGA 1280x800)

32.18.2 Run the ZON Utility

1 Double-click the ZON Utility to run it.

2 The first time you run the ZON Utility you will see if your Zyxel Device and firmware version support the ZON Utility. Click the OK button to close this screen.

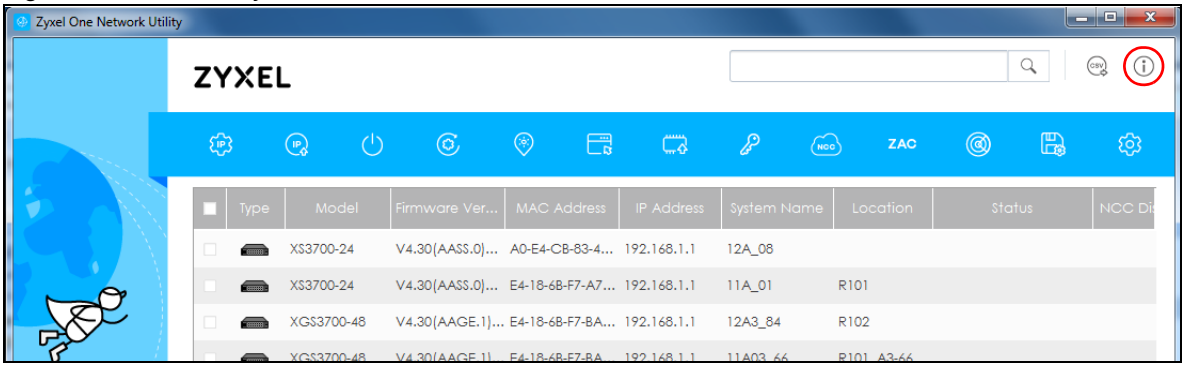
Figure 573 Supported Devices and Versions



If you want to check the supported models and firmware versions later, you can click the Show information about ZON icon in the upper right hand corner of the screen. Then select the Supported

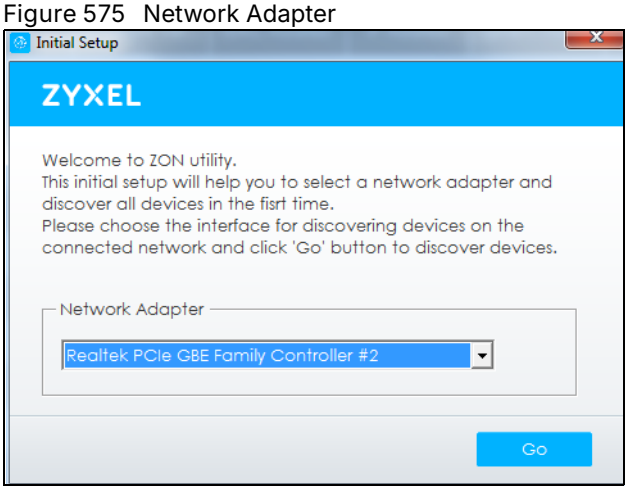
model and firmware version link. If your device is not listed here, see the device release notes for ZON utility support. The release notes are in the firmware zip file on the Zyxel web site.

Figure 574 ZON Utility Screen



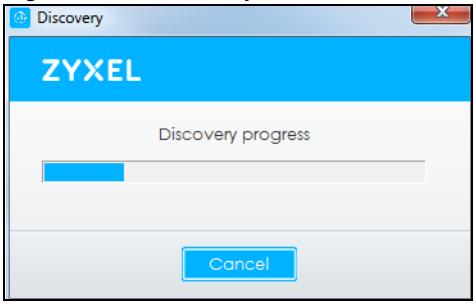
3 Select a network adapter to which your supported devices are connected.

Figure 575 Network Adapter



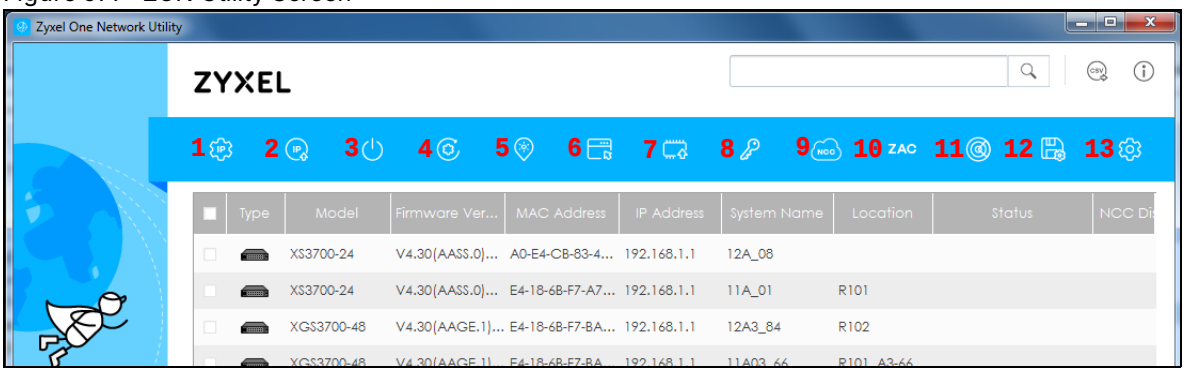
4 Click the Go button for the ZON Utility to discover all supported devices in your network.

Figure 576 Discovery



5 The ZON Utility screen shows the devices discovered.

Figure 577 ZON Utility Screen



6 Select a device and then use the icons to perform actions. Some functions may not be available for your devices.

The following table describes the icons numbered from left to right in the ZON Utility screen.

Table 305 ZON Utility Icons

ICON	DESCRIPTION
1 IP configuration	Change the selected device's IP address.
2 Renew IP Address	Update a DHCP-assigned dynamic IP address.
3 Reboot Device	Use this icon to restart the selected device(s). This may be useful when troubleshooting or upgrading new firmware.
4 Reset Configuration to Default	If you forget your password or cannot access the Web Configurator, you can use this icon to reload the factory-default configuration file. This means that you will lose all configurations that you had previously.
5 Locator LED	Use this icon to locate the selected device by causing its Locator LED to blink.
6 Web GUI	Use this to access the selected device web configurator from your browser. You will need a username and password to log in.
7 Firmware Upgrade	Use this icon to upgrade new firmware to selected device(s) of the same model. Make sure you have downloaded the firmware from the Zyxel website to your computer and unzipped it in advance. If your Zyxel Device supports dual firmware images, the standby image will be upgraded. After the new firmware is uploaded, you Zyxel Device will reboot, and the new firmware will be the running firmware.
8 Change Password	Use this icon to change the admin password of the selected device. You must know the current admin password before changing to a new one.
9 Configure NCC Discovery	You must have Internet access to use this feature. Use this icon to enable or disable the Nebula Control Center (NCC) discovery feature on the selected device. If it's enabled, the selected device will try to connect to the NCC. Once the selected device is connected to and has registered in the NCC, it'll go into the cloud management mode.
10 ZAC	Use this icon to run the Zyxel AP Configurator of the selected AP.
11 Clear and Rescan	Use this icon to clear the list and discover all devices on the connected network again.
12 Save Configuration	Use this icon to save configuration changes to permanent memory on a selected device.
13 Settings	Use this icon to select a network adaptor for the computer on which the ZON utility is installed, and the utility language.

The following table describes the fields in the ZON Utility main screen.

Table 306 ZON Utility Fields

LABEL	DESCRIPTION
Type	This field displays an icon of the kind of device discovered.
Model	This field displays the model name of the discovered device.
Firmware Version	This field displays the firmware version of the discovered device.
MAC Address	This field displays the MAC address of the discovered device.
IP Address	This field displays the IP address of an internal interface on the discovered device that first received an ZDP discovery request from the ZON utility.
System Name	This field displays the system name of the discovered device.
Location	This field displays where the discovered device is.
Status	This field displays whether changes to the discovered device have been done successfully. As the Zyxel Device does not support IP Configuration, Renew IP address and Flash Locator LED, this field displays “Update failed”, “Not support Renew IP address” and “Not support Flash Locator LED” respectively.
NCC Discovery	This field displays if the discovered device supports the Nebula Control Center (NCC) discovery feature. If it’s enabled, the selected device will try to connect to the NCC. Once the selected device is connected to and has registered in the NCC, it’ll go into the cloud management mode.
Serial Number	Enter the admin password of the discovered device to display its serial number.
Hardware Version	This field displays the hardware version of the discovered device.

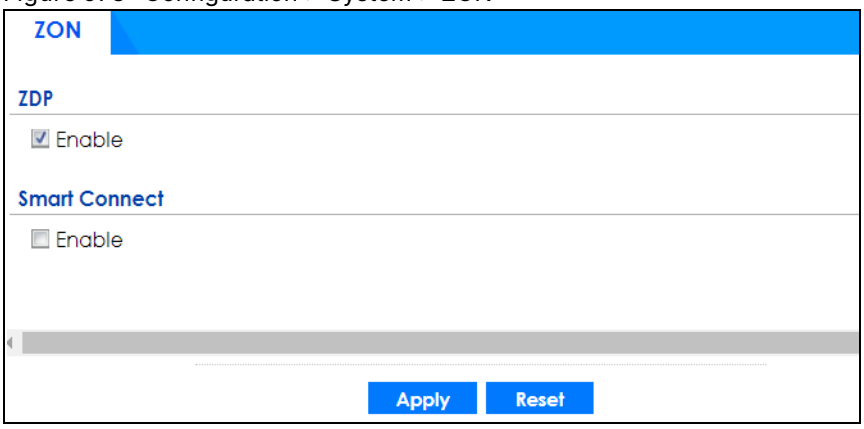
32.18.3 Zyxel One Network (ZON) System Screen

Enable ZDP (ZON) and Smart Connect (Ethernet Neighbor) in the System > ZON screen.

See Monitor > System Status > Ethernet Neighbor for information on using Smart Connect (Link Layer Discovery Protocol (LLDP)) for discovering and configuring LLDP-aware devices in the same broadcast domain as the Zyxel Device that you’re logged into using the web configurator.

The following figure shows the System > ZON screen.

Figure 578 Configuration > System > ZON



The following table describes the labels in this screen.

Table 307 Configuration > System > ZON

LABEL	DESCRIPTION
ZDP	Zyxel Discovery Protocol (ZDP) is the protocol that the Zyxel One Network (ZON) utility uses for discovering and configuring ZDP-aware Zyxel devices in the same broadcast domain as the computer on which ZON is installed.
Enable	Select to activate ZDP discovery on the Zyxel Device.
Smart Connect	Smart Connect uses 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.
Enable	Select to activate LLDP discovery on the Zyxel Device. See also Monitor > System Status > Ethernet Discovery.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

32.19 Advanced Screen

Use this screen to maximize the network performance of the Zyxel Device.

Fast Forwarding maximizes the network performance of the Zyxel Device by enabling a faster packet switching method which uses a trie (prefix tree).

When Fast Forwarding is enabled, essential network services such as NAT, routing, firewall, and VPN work as expected. However, security and logging services such as UTM, web authentication, MAC address binding, BWM, and traffic statistics are bypassed. This means traffic passes through the Zyxel Device unchecked and unlogged.

Note: Enabling Fast Forwarding might expose your network to security threat. We recommend enabling Fast Forwarding temporarily and only when it is needed.

32.19.1 Fast Forwarding Technical Reference

When switching a packet, a network device examines the packet's destination and then searches its local route cache to determine the output interface and then next hop to the destination. The route cached must be periodically cleared of old and invalid entries, to prevent the cached from consuming too much memory.

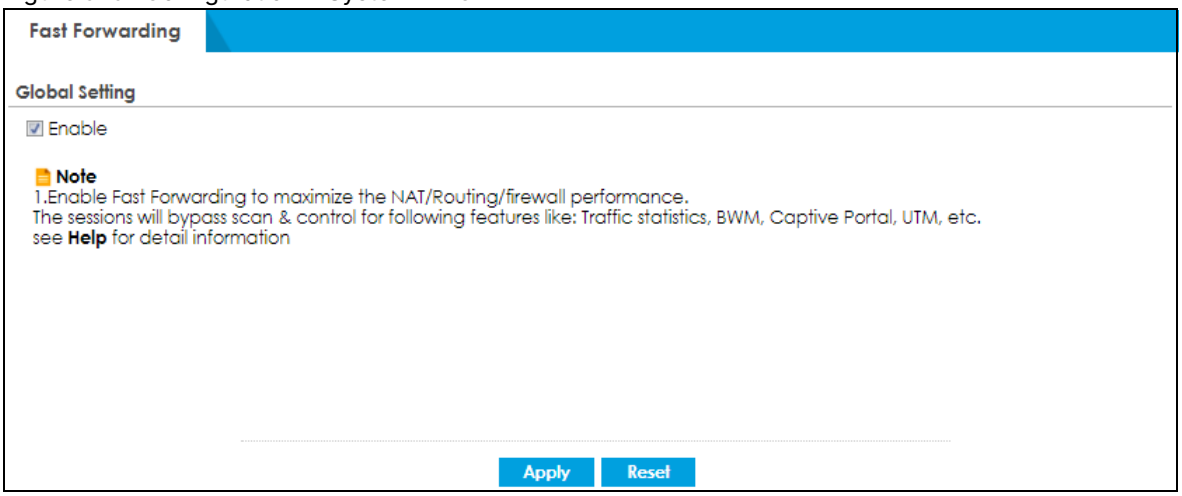
Fast Forwarding improves route cached performance by using a trie (prefix tree). A trie is a 256-way binary tree that does not store any data. Instead, each leaf in the tree contains a pointer to data in a separate adjacency table. The routing cached stores destination information in the search tree, and information about how to reach each destination in the adjacency table. separating the routing cached into two data structures offers several advantages:

- The search tree and adjacency table can be created and recreated separately
- Modifying entries in the adjacency table does not invalidate entries int eh search tree
- Entries in the adjacency table can point to each other, speeding up recursive routing. Recursive routing is where a device looks up a packet's next hop in the routing cached bu does not know how to reach the next hop, requiring another lookup

- The adjacency table can be updated directly from the device's ARP cache and routing table. This eliminates the need to periodically clear old and invalid entires from the cache

Click System > Advanced to open the following screen.

Figure 579 Configuration > System > ZON



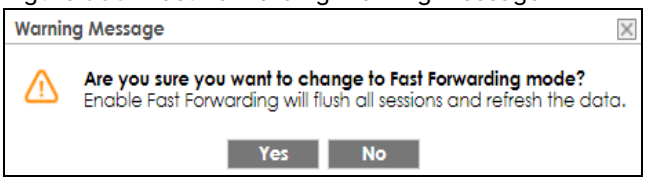
The following table describes the labels in this screen.

Table 308 Configuration > System > ZON

LABEL	DESCRIPTION
Enable	Select to activate fast forwarding on the Zyxel Device.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

A warning message will pop out when you select Enable. An icon will show at the Title Bar when fast forwarding is enabled.

Figure 580 Fast Forwarding Warning Message



CHAPTER 33
Log and Report

33.1 Overview

Use these screens to configure daily reporting and log settings.

33.1.1 What You Can Do In this Chapter

- Use the Email Daily Report screen (Section 33.2 on page 843) to configure where and how to send daily reports and what reports to send.
- Use the Log Setting screens (Section 33.3 on page 845) to specify settings for recording log messages and alerts, e-mailing them, storing them on a connected USB storage device, and sending them to remote syslog servers.

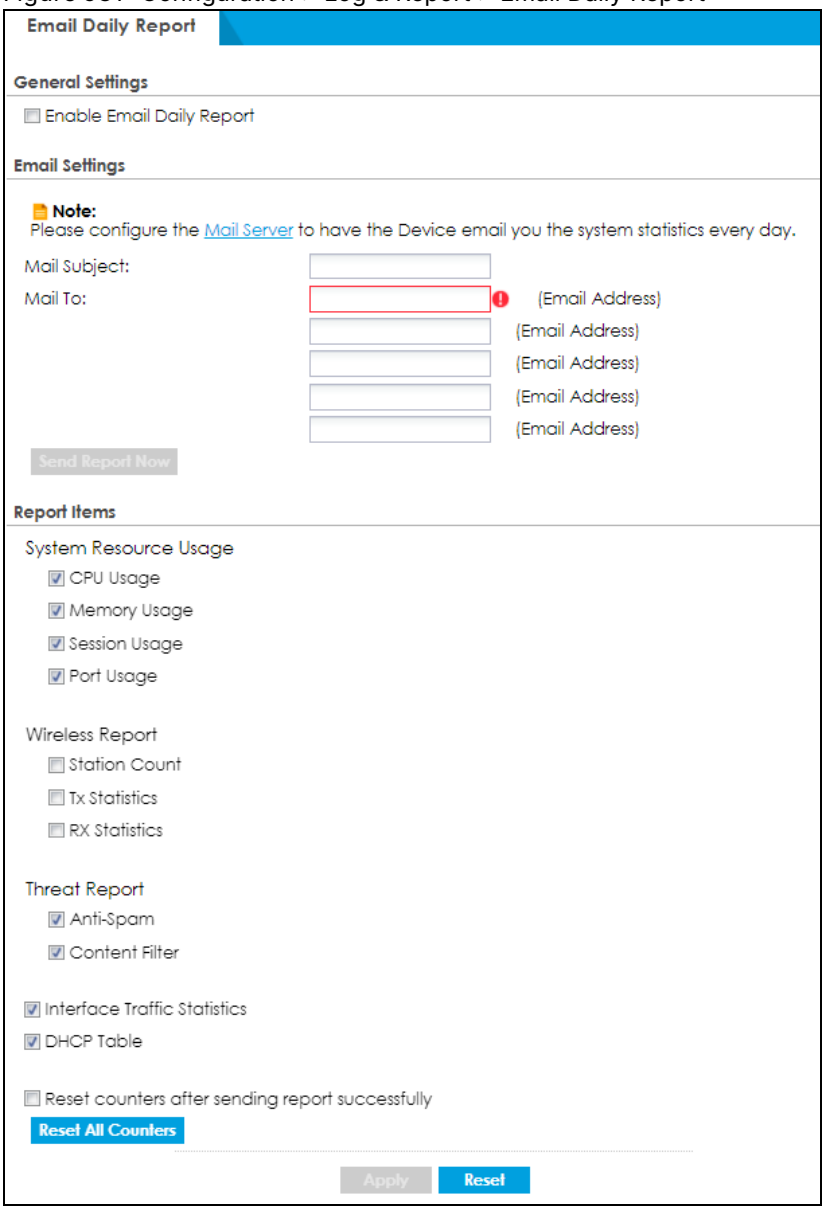
33.2 Email Daily Report

Use the Email Daily Report screen to start or stop data collection and view various statistics about traffic passing through your Zyxel Device. Click the Mail Server link under Note to set up the mail server in the Notification screen.

Note: Data collection may decrease the Zyxel Device's traffic throughput rate.

Click Configuration > Log & Report > Email Daily Report to display the following screen. Configure this screen to have the Zyxel Device email you system statistics every day.

Figure 581 Configuration > Log & Report > Email Daily Report



The following table describes the labels in this screen.

Table 309 Configuration > Log & Report > Email Daily Report

LABEL	DESCRIPTION
Enable Email Daily Report	Select this to send reports by email every day.
Mail Subject	Type the subject line for outgoing email from the Zyxel Device. Type a string using up to 60 of these characters [a-zA-Z0-9'()+,./:=?;!#@$_%-].
Mail To	Type the email address (or addresses) to which the outgoing email is delivered.
Send Report Now	Click this button to have the Zyxel Device send the daily email report immediately.

Table 309 Configuration > Log & Report > Email Daily Report (continued)

LABEL	DESCRIPTION
Report Items	Select the information to include in the report. Types of information include System Resource Usage, Wireless Report, Security Service, Interface Traffic Statistics and DHCP Table. Select Reset counters after sending report successfully if you only want to see statistics for a 24 hour period.
Reset All Counters	Click this to discard all report data and start all of the counters over at zero.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

33.3 Log Setting Screens

The Log Setting screens control log messages and alerts. A log message stores the information for viewing or regular emailing later, and an alert is emailed immediately. Usually, alerts are used for events that require more serious attention, such as system errors and attacks.

The Zyxel Device provides a system log and supports email profiles and remote syslog servers. View the system log in the MONITOR > Log screen. Use the email profiles to mail log messages to the specific destinations. You can also have the Zyxel Device store system logs on a connected USB storage device. The other four logs are stored on specified syslog servers.

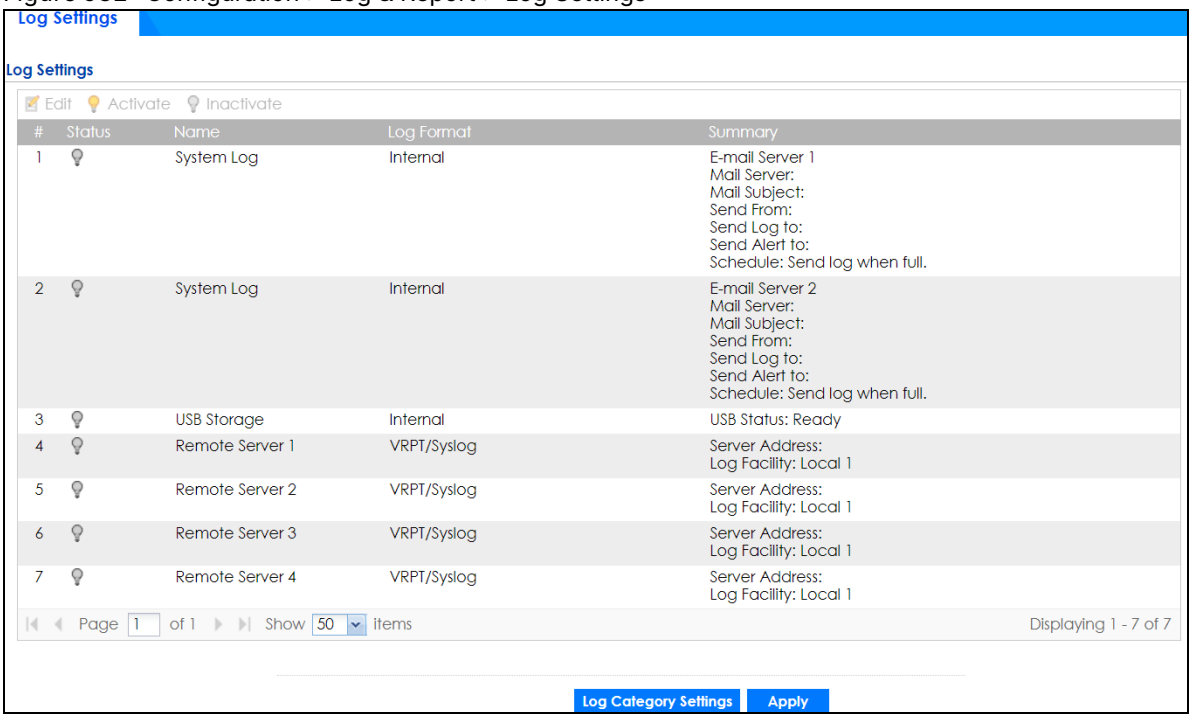
The Log Setting screens control what information the Zyxel Device saves in each log. You can also specify which log messages to email for the system log, and where and how often to email them. These screens also set for which events to generate alerts and where to email the alerts.

The first Log Setting screen provides a settings summary. Use the Edit screens to configure settings such as log categories, email addresses, and server names for any log. Use the Log Category Settings screen to edit what information is included in the system log, USB storage, email profiles, and remote servers.

33.3.1 Log Setting Summary

To access this screen, click Configuration > Log & Report > Log Settings.

Figure 582 Configuration > Log & Report > Log Settings



The following table describes the labels in this screen.

Table 310 Configuration > Log & Report > Log Settings

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify it.
Activate	To turn on an entry, select it and click Activate.
Inactivate	To turn off an entry, select it and click Inactivate.
#	This field is a sequential value, and it is not associated with a specific log.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the type of log setting entry (system log, logs stored on a USB storage device connected to the Zyxel Device, or one of the remote servers).
Log Format	This field displays the format of the log. Internal - System logs only; VRPT - Syslog-compatible format. CEF/Syslog - Common Event Format, syslog-compatible format. The CEF log format is as follows: Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension Features that use the CEF log format at the time of writing are: • ADP • Security Policy • Content Filter • Traffic Log • System Monitoring • User • DHCP (Your model may not support all features.)

Table 310 Configuration > Log & Report > Log Settings (continued)

LABEL	DESCRIPTION
Summary	This field is a summary of the settings for each log. Please see Section 33.3.2 on page 847 for more information.
Log Category Settings	Click this button to open the Log Category Settings Edit screen.
Apply	Click this button to save your changes (activate and deactivate logs) and make them take effect.

33.3.2 Edit System Log Settings

The Log Settings Edit screen controls the detailed settings for each log in the system log (which includes the email profiles). Go to the Log Settings Summary screen (see Section 33.3.1 on page 845), and click the system log Edit icon.

Figure 583 Configuration > Log & Report > Log Setting > Edit (System Log - E-mail Servers)

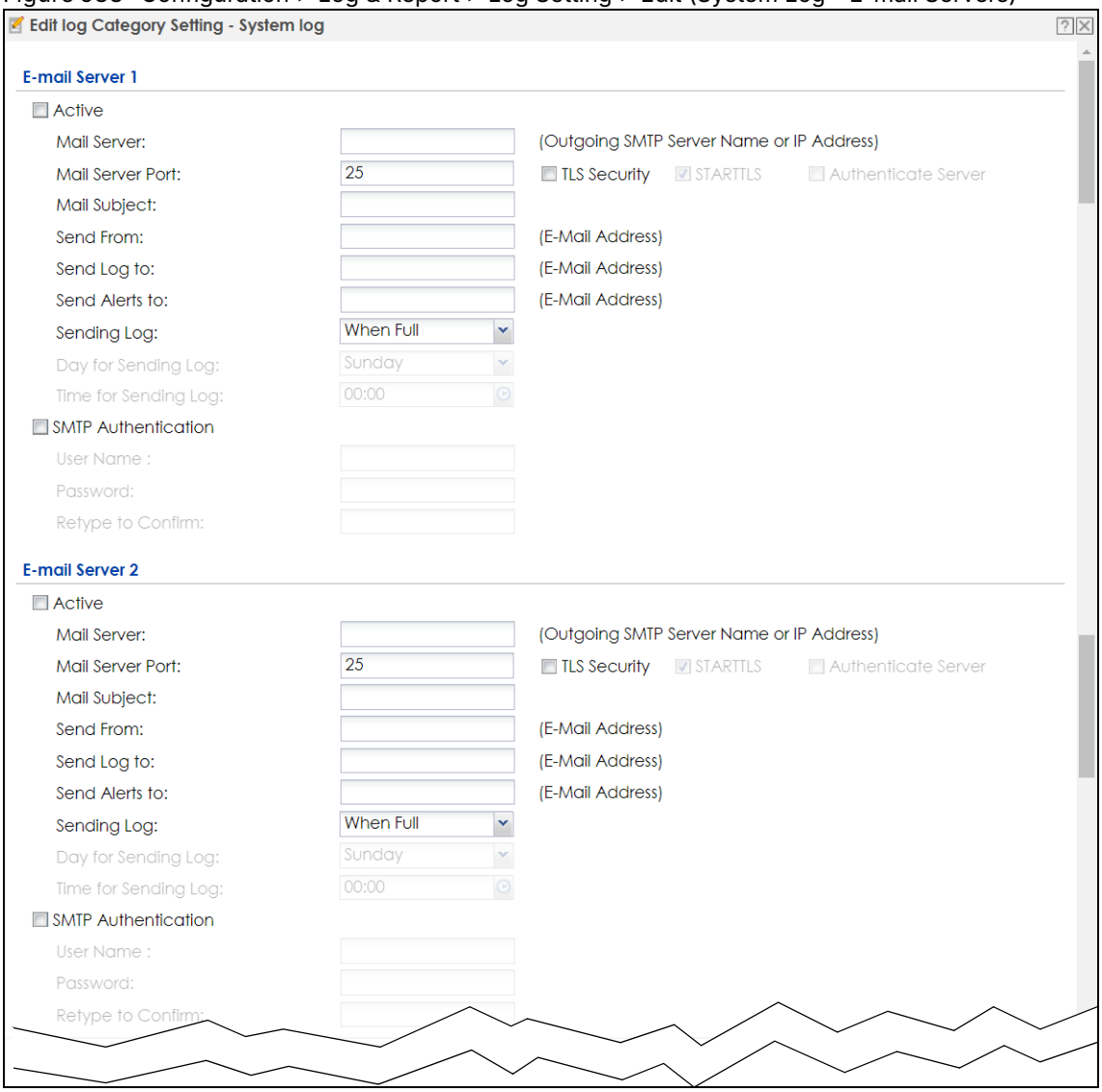


Figure 584 Configuration > Log & Report > Log Setting > Edit (System Log)

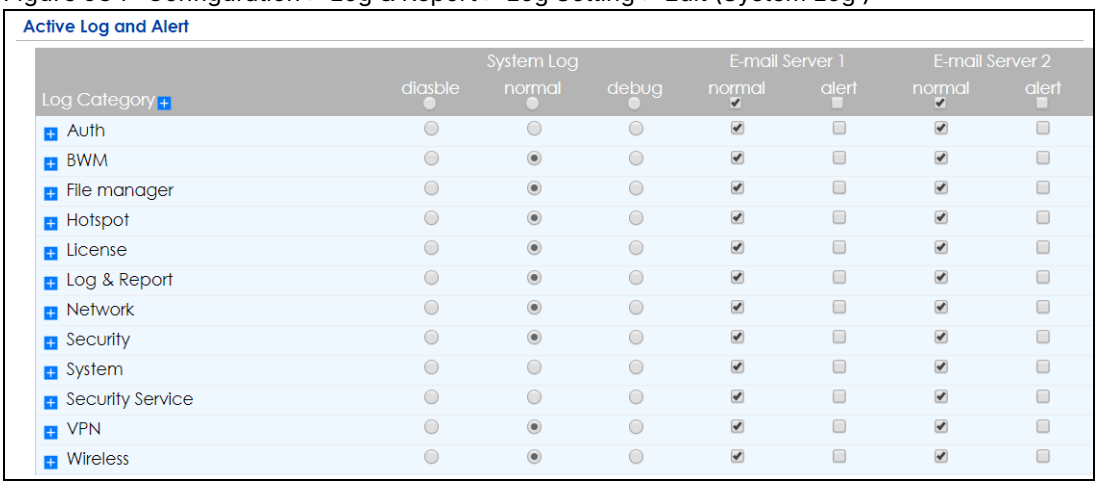
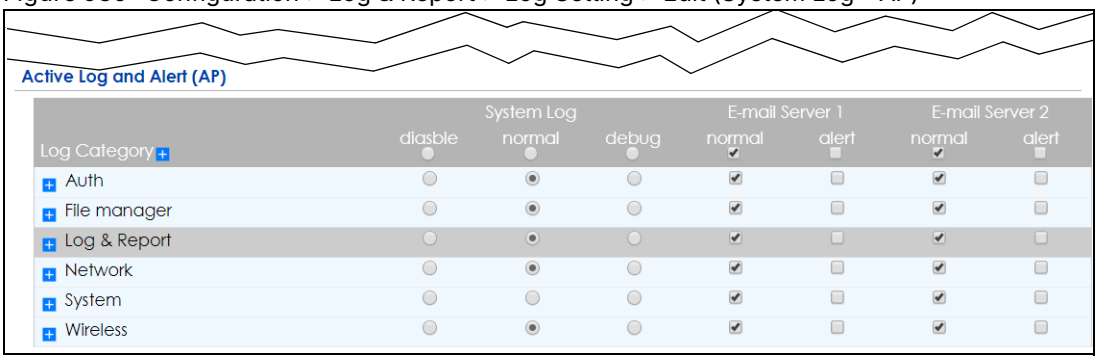


Figure 585 Configuration > Log & Report > Log Setting > Edit (System Log - AP)



The following table describes the labels in this screen.

Table 311 Configuration > Log & Report > Log Setting > Edit (System Log)

LABEL	DESCRIPTION
E-Mail Server 1/2	
Active	Select this to send log messages and alerts according to the information in this section. You specify what kinds of log messages are included in log information and what kinds of log messages are included in alerts in the Active Log and Alert section.
Mail Server	Type the name or IP address of the outgoing SMTP server.
Mail Server Port	Enter the same port number here as is on the mail server for mail traffic.
Mail Subject	Type the subject line for the outgoing email.
Send From	Type the email address from which the outgoing email is delivered. This address is used in replies.
Send Log To	Type the email address to which the outgoing email is delivered.
Send Alerts To	Type the email address to which alerts are delivered.
Sending Log	Select how often log information is emailed. Choices are: When Full, Hourly and When Full, Daily and When Full, and Weekly and When Full.
Day for Sending Log	This field is available if the log is emailed weekly. Select the day of the week the log is emailed.
Time for Sending Log	This field is available if the log is emailed weekly or daily. Select the time of day (hours and minutes) when the log is emailed. Use 24-hour notation.
SMTP Authentication	Select this checkbox if it is necessary to provide a user name and password to the SMTP server.

Table 311 Configuration > Log & Report > Log Setting > Edit (System Log) (continued)

LABEL	DESCRIPTION
User Name	This box is effective when you select the SMTP Authentication checkbox. Type the user name to provide to the SMTP server when the log is emailed.
Password	This box is effective when you select the SMTP Authentication checkbox. Type the password of up to 63 characters to provide to the SMTP server when the log is emailed.
Retype to Confirm	Type the password again to make sure that you have entered is correctly.
Active Log and Alert	
System Log	Use the System Log drop-down list to change the log settings for all of the log categories. disable all logs (red X) - do not log any information for any category for the system log or email any logs to email server 1 or 2. enable normal logs (green check mark) - create log messages and alerts for all categories for the system log. If email server 1 or 2 also has normal logs enabled, the Zyxel Device will email logs to them. enable normal logs and debug logs (yellow check mark) - create log messages, alerts, and debugging information for all categories. The Zyxel Device does not email debugging information, even if this setting is selected.
E-mail Server 1	Use the E-Mail Server 1 drop-down list to change the settings for emailing logs to email server 1 for all log categories. Using the System Log drop-down list to disable all logs overrides your email server 1 settings. enable normal logs (green check mark) - email log messages for all categories to email server 1. enable alert logs (red exclamation point) - email alerts for all categories to email server 1.
E-mail Server 2	Use the E-Mail Server 2 drop-down list to change the settings for emailing logs to email server 2 for all log categories. Using the System Log drop-down list to disable all logs overrides your email server 2 settings. enable normal logs (green check mark) - email log messages for all categories to email server 2. enable alert logs (red exclamation point) - email alerts for all categories to email server 2.
Log Category	This field displays each category of messages. It is the same value used in the Display and Category fields in the View Log tab. The Default category includes debugging messages generated by open source software.
System log	Select which events you want to log by Log Category. There are three choices: disable all logs (red X) - do not log any information from this category enable normal logs (green check mark) - create log messages and alerts from this category enable normal logs and debug logs (yellow check mark) - create log messages, alerts, and debugging information from this category; the Zyxel Device does not email debugging information, however, even if this setting is selected.
E-mail Server 1	Select whether each category of events should be included in the log messages when it is emailed (green check mark) and/or in alerts (red exclamation point) for the email settings specified in E-Mail Server 1. The Zyxel Device does not email debugging information, even if it is recorded in the System log.
E-mail Server 2	Select whether each category of events should be included in log messages when it is emailed (green check mark) and/or in alerts (red exclamation point) for the email settings specified in E-Mail Server 2. The Zyxel Device does not email debugging information, even if it is recorded in the System log.
Log Consolidation	

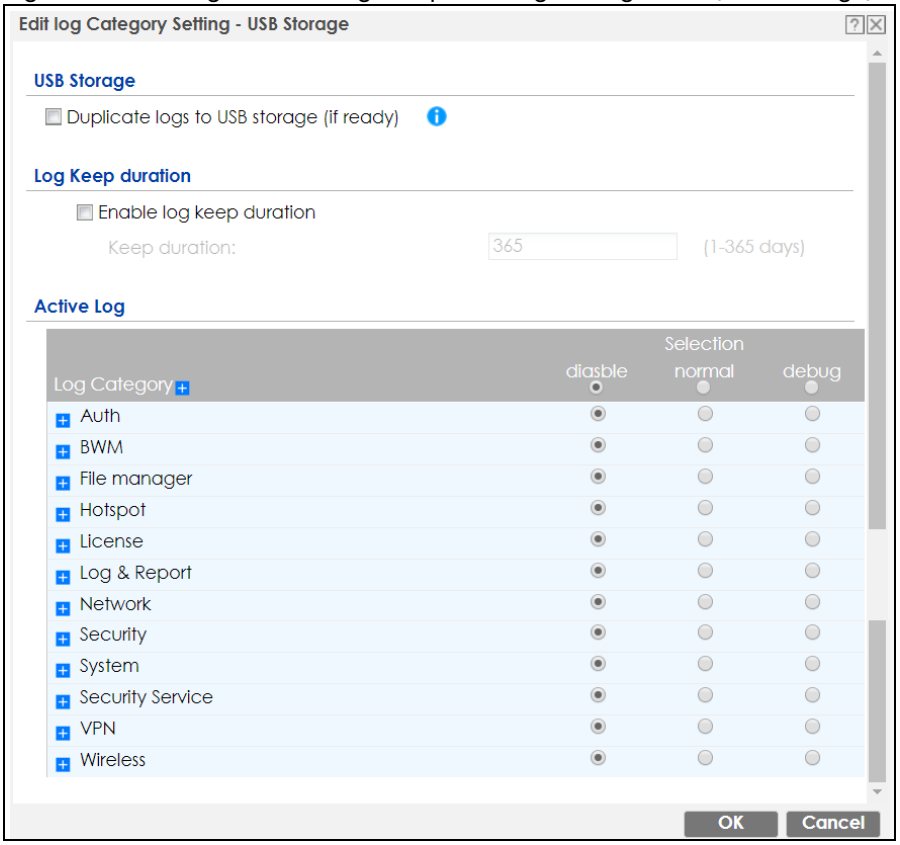
Table 311 Configuration > Log & Report > Log Setting > Edit (System Log) (continued)

LABEL	DESCRIPTION
Active	Select this to activate log consolidation. Log consolidation aggregates multiple log messages that arrive within the specified Log Consolidation Interval. In the View Log tab, the text "[count=*x*]", where *x* is the number of original log messages, is appended at the end of the Message field, when multiple log messages were aggregated.
Log Consolidation Interval	Type how often, in seconds, to consolidate log information. If the same log message appears multiple times, it is aggregated into one log message with the text "[count=*x*]", where *x* is the number of original log messages, appended at the end of the Message field.
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

33.3.3 Edit Log on USB Storage Setting

The Edit Log on USB Storage Setting screen controls the detailed settings for saving logs to a connected USB storage device. Go to the Log Setting Summary screen (see Section 33.3.1 on page 845), and click the USB storage Edit icon.

Figure 586 Configuration > Log & Report > Log Setting > Edit (USB Storage)



The following table describes the labels in this screen.

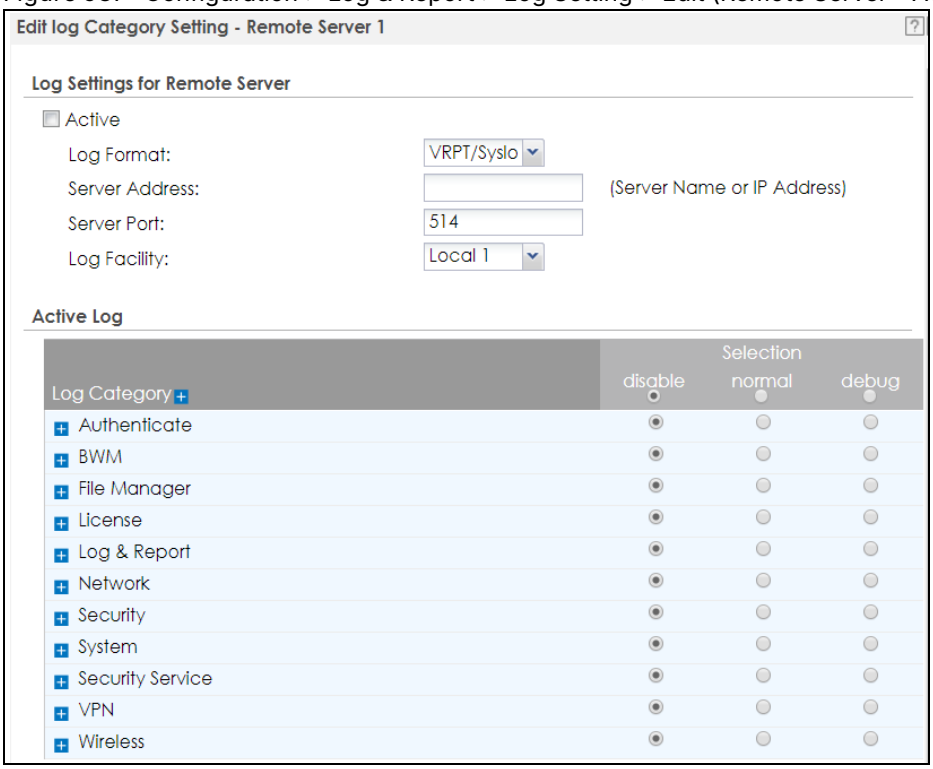
Table 312 Configuration > Log & Report > Log Setting > Edit (USB Storage)

LABEL	DESCRIPTION
Duplicate logs to USB storage (if ready)	Select this to have the Zyxel Device save a copy of its system logs to a connected USB storage device. Use the Active Log section to specify what kinds of messages to include.
Enable log keep duration	Select this checkbox to enter a value in the Keep Duration field.
Keep Duration	Enter a number of days that the Zyxel Device keeps this log.
Active Log	
Selection	Use the Selection drop-down list to change the log settings for all of the log categories. disable all logs (red X) - do not send the remote server logs for any log category. enable normal logs (green check mark) - send the remote server log messages and alerts for all log categories. enable normal logs and debug logs (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
Log Category	This field displays each category of messages. The Default category includes debugging messages generated by open source software.
Selection	Select what information you want to log from each Log Category (except All Logs; see below). Choices are: disable all logs (red X) - do not log any information from this category enable normal logs (green check mark) - log regular information and alerts from this category enable normal logs and debug logs (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

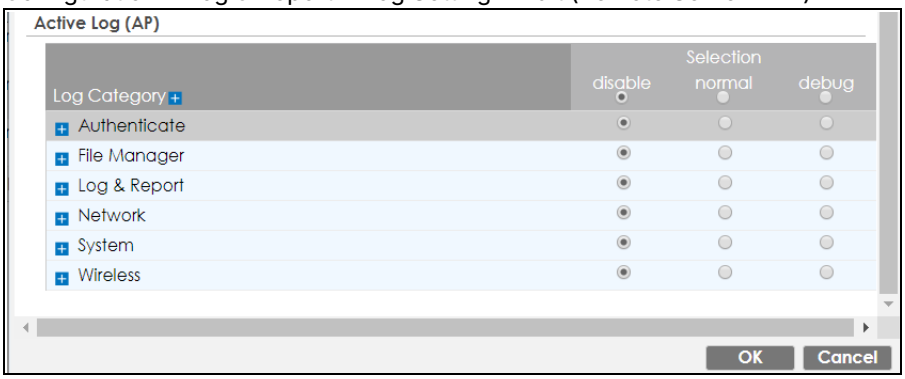
33.3.4 Edit Remote Server Log Settings

The Log Settings Edit screen controls the detailed settings for each log in the remote server (syslog). Go to the Log Settings Summary screen (see Section 33.3.1 on page 845), and click a remote server Edit icon.

Figure 587 Configuration > Log & Report > Log Setting > Edit (Remote Server - AC)



Configuration > Log & Report > Log Setting > Edit (Remote Server - AP)



The following table describes the labels in this screen.

Table 313 Configuration > Log & Report > Log Setting > Edit (Remote Server)

LABEL	DESCRIPTION
Log Settings for Remote Server	
Active	Select this checkbox to send log information according to the information in this section. You specify what kinds of messages are included in log information in the Active Log section.
Log Format	This field displays the format of the log information. It is read-only. VRPT/Syslog - Zyxel's Vantage Report, syslog-compatible format. CEF/Syslog - Common Event Format, syslog-compatible format.
Server Address	Type the server name or the IP address of the syslog server to which to send log information.

Table 313 Configuration > Log & Report > Log Setting > Edit (Remote Server) (continued)

LABEL	DESCRIPTION
Server Port	Type the service port number used by the remote server.
Log Facility	Select a log facility. The log facility allows you to log the messages to different files in the syslog server. Please see the documentation for your syslog program for more information.
Active Log	
Selection	Use the Selection drop-down list to change the log settings for all of the log categories. disable all logs (red X) - do not send the remote server logs for any log category. enable normal logs (green check mark) - send the remote server log messages and alerts for all log categories. enable normal logs and debug logs (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
Log Category	This field displays each category of messages. It is the same value used in the Display and Category fields in the View Log tab. The Default category includes debugging messages generated by open source software.
Selection	Select what information you want to log from each Log Category (except All Logs; see below). Choices are: disable all logs (red X) - do not log any information from this category enable normal logs (green check mark) - log regular information and alerts from this category enable normal logs and debug logs (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

33.3.5 Log Category Settings Screen

The Log Category Settings screen allows you to view and to edit what information is included in the system log, USB storage, email profiles, and remote servers at the same time. It does not let you change other log settings (for example, where and how often log information is emailed or remote server names). To access this screen, go to the Log Settings Summary screen (see Section 33.3.1 on page 845), and click the Log Category Settings button.

Figure 588 Log Category Settings AC

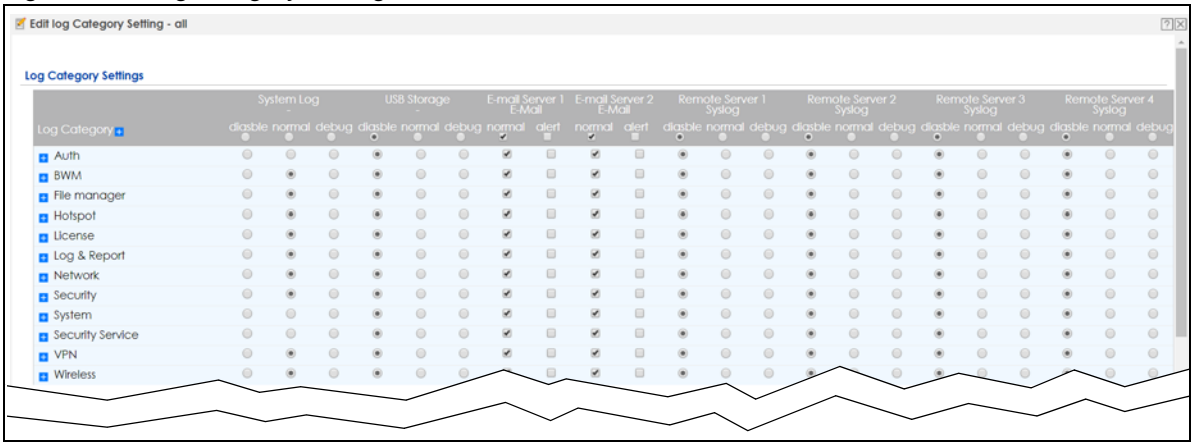
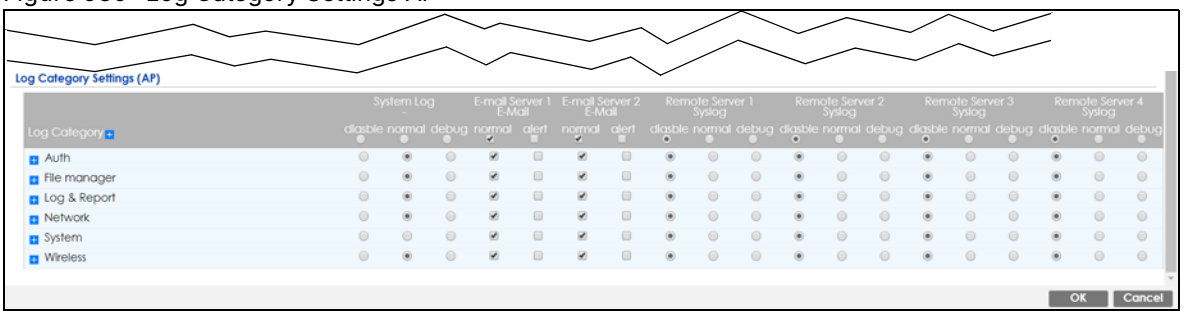


Figure 589 Log Category Settings AP



This screen provides a different view and a different way of indicating which messages are included in each log and each alert. Please see Section 33.3.2 on page 847, where this process is discussed. (The Default category includes debugging messages generated by open source software.)

The following table describes the fields in this screen.

Table 314 Configuration > Log & Report > Log Setting > Log Category Settings

LABEL	DESCRIPTION
System Log	Use the System Log drop-down list to change the log settings for all of the log categories. disable all logs (red X) - do not log any information for any category for the system log or email any logs to email server 1 or 2. enable normal logs (green check mark) - create log messages and alerts for all categories for the system log. If email server 1 or 2 also has normal logs enabled, the Zyxel Device will email logs to them. enable normal logs and debug logs (yellow check mark) - create log messages, alerts, and debugging information for all categories. The Zyxel Device does not email debugging information, even if this setting is selected.
USB Storage	Use the USB Storage drop-down list to change the log settings for saving logs to a connected USB storage device. disable all logs (red X) - do not log any information for any category to a connected USB storage device. enable normal logs (green check mark) - create log messages and alerts for all categories and save them to a connected USB storage device. enable normal logs and debug logs (yellow check mark) - create log messages, alerts, and debugging information for all categories and save them to a connected USB storage device.
E-mail Server 1 E-mail	Use the E-Mail Server 1 drop-down list to change the settings for emailing logs to email server 1 for all log categories. Using the System Log drop-down list to disable all logs overrides your email server 1 settings. enable normal logs (green check mark) - email log messages for all categories to email server 1. enable alert logs (red exclamation point) - email alerts for all categories to email server 1.
E-mail Server 2 E-mail	Use the E-Mail Server 2 drop-down list to change the settings for emailing logs to email server 2 for all log categories. Using the System Log drop-down list to disable all logs overrides your email server 2 settings. enable normal logs (green check mark) - email log messages for all categories to email server 2. enable alert logs (red exclamation point) - email alerts for all categories to email server 2.

Table 314 Configuration > Log & Report > Log Setting > Log Category Settings (continued)

LABEL	DESCRIPTION
Remote Server 1~4 Syslog	For each remote server, use the Selection drop-down list to change the log settings for all of the log categories. disable all logs (red X) - do not send the remote server logs for any log category. enable normal logs (green check mark) - send the remote server log messages and alerts for all log categories. enable normal logs and debug logs (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
Log Category	This field displays each category of messages. It is the same value used in the Display and Category fields in the View Log tab. The Default category includes debugging messages generated by open source software.
System Log	Select which events you want to log by Log Category. There are three choices: disable all logs (red X) - do not log any information from this category enable normal logs (green check mark) - create log messages and alerts from this category enable normal logs and debug logs (yellow check mark) - create log messages, alerts, and debugging information from this category; the Zyxel Device does not email debugging information, however, even if this setting is selected.
USB Storage	Select which event log categories to save to a connected USB storage device. There are three choices: disable all logs (red X) - do not log any information from this category enable normal logs (green check mark) - save log messages and alerts from this category enable normal logs and debug logs (yellow check mark) - save log messages, alerts, and debugging information from this category.
E-mail Server 1 E-mail	Select whether each category of events should be included in the log messages when it is emailed (green check mark) and/or in alerts (red exclamation point) for the email settings specified in E-Mail Server 1. The Zyxel Device does not email debugging information, even if it is recorded in the System log.
E-mail Server 2 E-mail	Select whether each category of events should be included in log messages when it is emailed (green check mark) and/or in alerts (red exclamation point) for the email settings specified in E-Mail Server 2. The Zyxel Device does not email debugging information, even if it is recorded in the System log.
Remote Server 1~4 Syslog	For each remote server, select what information you want to log from each Log Category (except All Logs; see below). Choices are: disable all logs (red X) - do not log any information from this category enable normal logs (green check mark) - log regular information and alerts from this category enable normal logs and debug logs (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

CHAPTER 34
File Manager

34.1 Overview

Configuration files define the Zyxel Device's settings. Shell scripts are files of commands that you can store on the Zyxel Device and run when you need them. You can apply a configuration file or run a shell script without the Zyxel Device restarting. You can store multiple configuration files and shell script files on the Zyxel Device. You can edit configuration files or shell scripts in a text editor and upload them to the Zyxel Device. Configuration files use a .conf extension and shell scripts use a .zysh extension.

34.1.1 What You Can Do in this Chapter

- Use the Configuration File screen (see Section 34.2 on page 860) to store and name configuration files. You can also download configuration files from the Zyxel Device to your computer and upload configuration files from your computer to the Zyxel Device.
- Use the Firmware Package screen (see Section 34.3 on page 866) to check your current firmware version and upload firmware to the Zyxel Device.
- Use the Shell Script screen (see Section 34.4 on page 873) to store, name, download, upload and run shell script files.

34.1.2 What you Need to Know

Configuration Files and Shell Scripts

When you apply a configuration file, the Zyxel Device uses the factory default settings for any features that the configuration file does not include. When you run a shell script, the Zyxel Device only applies the commands that it contains. Other settings do not change.

These files have the same syntax, which is also identical to the way you run CLI commands manually. An example is shown below.

Figure 590 Configuration File / Shell Script: Example

```
# enter configuration mode
configure terminal
# change administrator password
username admin password 4321 user-type admin
# configure ge3
interface ge3
ip address 172.23.37.240 255.255.255.0
ip gateway 172.23.37.254 metric 1
exit
# create address objects for remote management / to-ZyWALL firewall rules
# use the address group in case we want to open up remote management later
address-object TW_SUBNET 172.23.37.0/24
object-group address TW_TEAM
address-object TW_SUBNET
exit
# enable Telnet access (not enabled by default, unlike other services)
ip telnet server
# open WAN-to-ZyWALL firewall for TW_TEAM for remote management
firewall WAN ZyWALL insert 4
sourceip TW_TEAM
service TELNET
action allow
exit
write
```

While configuration files and shell scripts have the same syntax, the Zyxel Device applies configuration files differently than it runs shell scripts. This is explained below.

Table 315 Configuration Files and Shell Scripts in the Zyxel Device

Configuration Files (.conf)	Shell Scripts (.zysh)
• Resets to default configuration. • Goes into CLI Configuration mode. • Runs the commands in the configuration file.	• Goes into CLI Privilege mode. • Runs the commands in the shell script.

You have to run the example in Figure 590 on page 857 as a shell script because the first command is run in Privilege mode. If you remove the first command, you have to run the example as a configuration file because the rest of the commands are executed in Configuration mode.

Comments in Configuration Files or Shell Scripts

In a configuration file or shell script, use “#” or “!” as the first character of a command line to have the Zyxel Device treat the line as a comment.

Your configuration files or shell scripts can use “exit” or a command line consisting of a single “!” to have the Zyxel Device exit sub command mode.

Note: “exit” or “!” must follow sub commands if it is to make the Zyxel Device exit sub command mode.

Line 3 in the following example exits sub command mode.

```
interface ge1
ip address dhcp
!
```

Lines 1 and 3 in the following example are comments and line 4 exits sub command mode.

```
!
interface ge1
# this interface is a DHCP client
!
```

Lines 1 and 2 are comments. Line 5 exits sub command mode.

```
! this is from Joe
# on 2008/04/05
interface ge1
ip address dhcp
!
```

Errors in Configuration Files or Shell Scripts

When you apply a configuration file or run a shell script, the Zyxel Device processes the file line-by-line. The Zyxel Device checks the first line and applies the line if no errors are detected. Then it continues with the next line. If the Zyxel Device finds an error, it stops applying the configuration file or shell script and generates a log.

You can change the way a configuration file or shell script is applied. Include `setenv stop-on-error off` in the configuration file or shell script. The Zyxel Device ignores any errors in the configuration file or shell script and applies all of the valid commands. The Zyxel Device still generates a log for any errors.

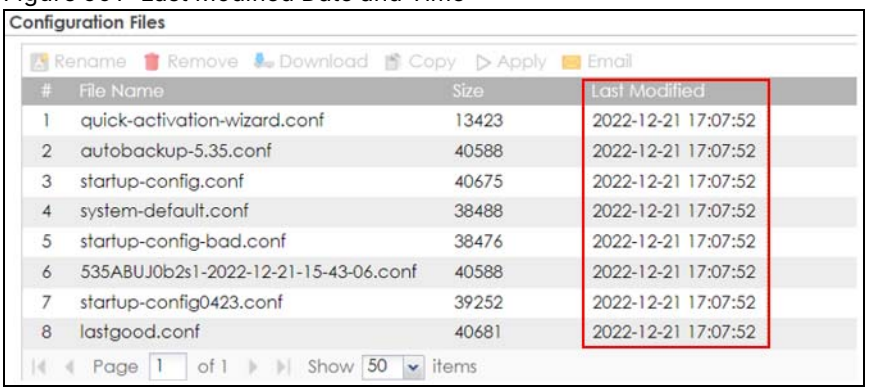
Sensitive Data Protection

The Zyxel Device by default encrypts local admin and user account passwords for web configurator and CLI.

Enable Sensitive Data Protection to better protect local admin and user account passwords for web configurator and CLI.

When you change the private key, the date and time shown in Maintenance > File Manager > Configuration File > Configuration > Last Modified for all configuration files will change to the date and time you changed the private key.

Figure 591 Last Modified Date and Time



#	File Name	Size	Last Modified
1	quick-activation-wizard.conf	13423	2022-12-21 17:07:52
2	autobackup-5.35.conf	40588	2022-12-21 17:07:52
3	startup-config.conf	40675	2022-12-21 17:07:52
4	system-default.conf	38488	2022-12-21 17:07:52
5	startup-config-bad.conf	38476	2022-12-21 17:07:52
6	535ABUJ0b2s1-2022-12-21-15-43-06.conf	40588	2022-12-21 17:07:52
7	startup-config0423.conf	39252	2022-12-21 17:07:52
8	lastgood.conf	40681	2022-12-21 17:07:52

Note: You can only upload configuration files using FTP that are using the current private key of the Zyxel Device.

The following examples describe the situations you might come across using Sensitive Data Protection.

Example 1:

1 Download a configuration file (file1).

2 Enable Sensitive Data Protection.

3 Create a private key (key1).

4 When you upload file1 to the Zyxel Device through the Zyxel Device web configurator, you do not need to enter the private key (key1). Configuration file1 is not encrypted by the private key (key1).

Example 2:

1 Enable Sensitive Data Protection.

2 Create a private key (key1).

3 Download a configuration file (file2).

4 You must use key1 to upload file2 to the Zyxel Device because file2 is encrypted by key1.

Example 3:

1 Change the private key from key1 to key2.

2 Download another configuration file (file3).

3 You must use key2 to upload file3 to the Zyxel Device.

Note: You must still use key1 to upload file2 to the Zyxel Device. Make a note of the key to use when you change the private key and then download a configuration file.

Example 4:

1. Enable Sensitive Data Protection on Zyxel Device1 and create a private key.
2. Download a configuration file from Zyxel Device1.
3. You must upload this configuration file using the private key you created on Zyxel Device1 to Zyxel Device2 even if Sensitive Data Protection is not enabled on Zyxel Device2.

34.2 The Configuration Screen

Click Maintenance > File Manager > Configuration File > Configuration to open the Configuration screen. Use the Configuration screen to store, run, and name configuration files. You can also download configuration files from the Zyxel Device to your computer and upload configuration files from your computer to the Zyxel Device.

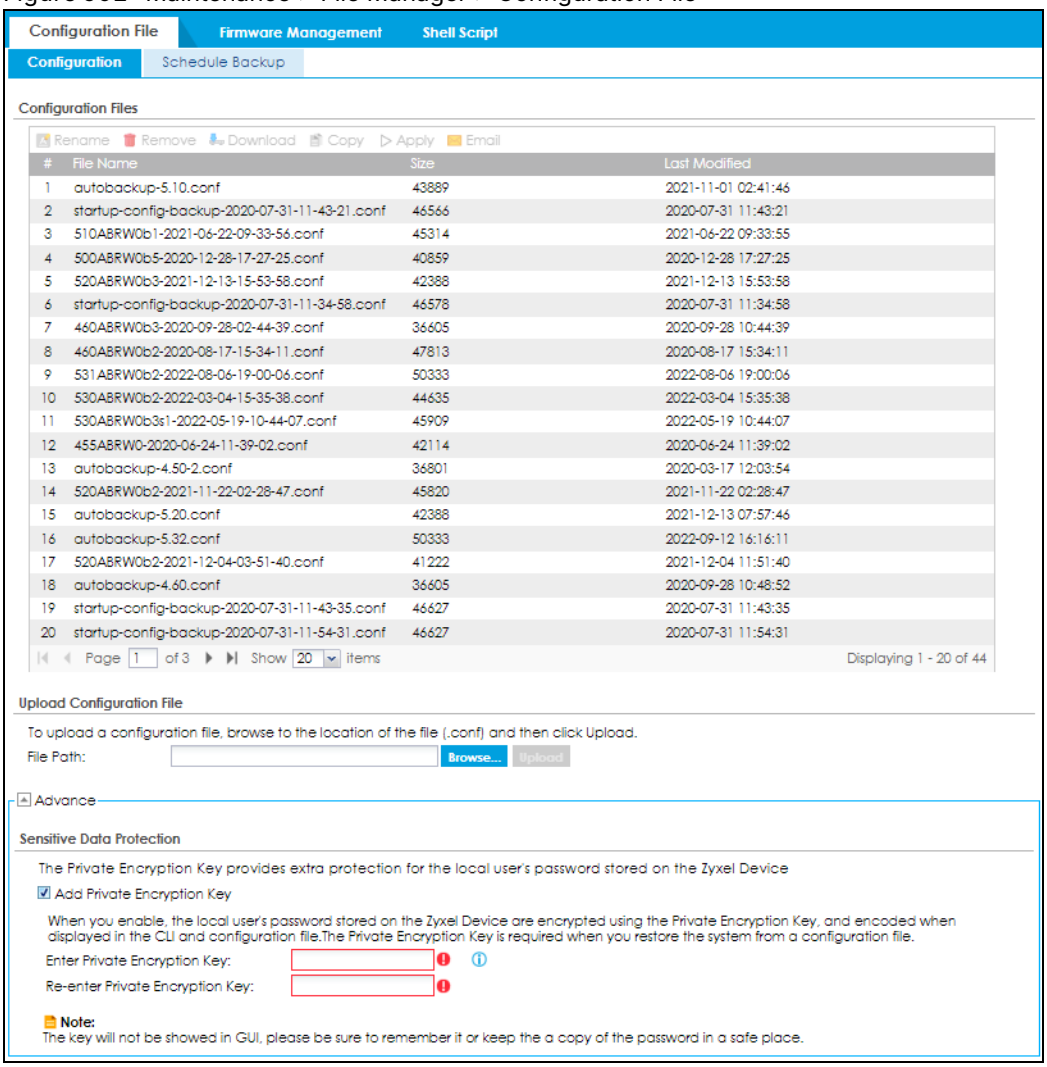
Once your Zyxel Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making further configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Filenames beginning with autoback are automatic configuration files created when new firmware is uploaded. backup-yyyy-mm-dd-hh-mm-ss.conf is the name of the automatic backup when a secure policy is added or changed. Select a configuration file, then click Apply to apply the file to the Zyxel Device .

Configuration File Flow at Restart

- If there is not a startup-config.conf when you restart the Zyxel Device (whether through a management interface or by physically turning the power off and back on), the Zyxel Device uses the system-default.conf configuration file with the Zyxel Device's default settings.
- If there is a startup-config.conf, the Zyxel Device checks it for errors and applies it. If there are no errors, the Zyxel Device uses it and copies it to the lastgood.conf configuration file as a back up file. If there is an error, the Zyxel Device generates a log and copies the startup-config.conf configuration file to the startup-config-bad.conf configuration file and tries the existing lastgood.conf configuration file. If there isn't a lastgood.conf configuration file or it also has an error, the Zyxel Device applies the system-default.conf configuration file.
- You can change the way the startup-config.conf file is applied. Include the `setenv-startup stop-on-error off` command. The Zyxel Device ignores any errors in the startup-config.conf file and applies all of the valid commands. The Zyxel Device still generates a log for any errors.

Figure 592 Maintenance > File Manager > Configuration File



Do not turn off the Zyxel Device while configuration file upload is in progress.

The following table describes the labels in this screen.

Table 316 Maintenance > File Manager > Configuration File

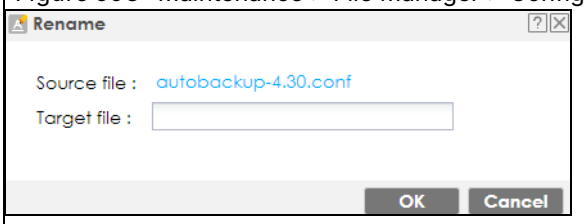
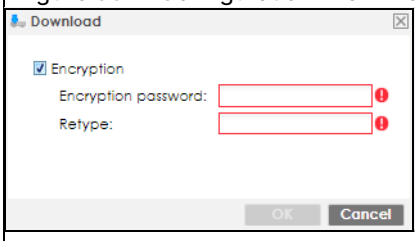
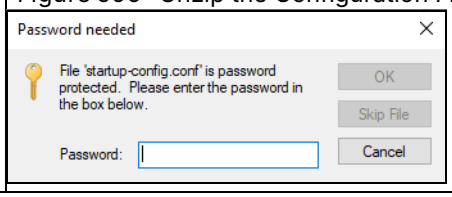
LABEL	DESCRIPTION
Rename	Use this button to change the label of a configuration file on the Zyxel Device. You can only rename manually saved configuration files. You cannot rename the lastgood.conf, system-default.conf and startup-config.conf files. You cannot rename a configuration file to the name of another configuration file in the Zyxel Device. Click a configuration file's row to select it and click Rename to open the Rename File screen. Figure 593 Maintenance > File Manager > Configuration File > Rename  Specify the new name for the configuration file. Use up to 63 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click OK to save the duplicate or click Cancel to close the screen without saving a duplicate of the configuration file.
Remove	Click a configuration file's row to select it and click Remove to delete it from the Zyxel Device. You can only delete manually saved configuration files. You cannot delete the system-default.conf, startup-config.conf and lastgood.conf files. A pop-up window asks you to confirm that you want to delete the configuration file. Click OK to delete the configuration file or click Cancel to close the screen without deleting the configuration file.
Download	Click a configuration file's row to select it and click Download to save the configuration to your computer. Select Encryption if you want to add an encryption password to the downloaded zipped configuration file. Enter a password consists of 1 to 31 single-bye characters, with the following special characters !"#$%&'()*+,-./;:<=>@\^_'{|}~ This field is case sensitive. []?and spaces are not allowed. You or another admin must use the same password to unzip the file. Figure 594 Configuration File > Download > Encryption  Figure 595 Unzip the Configuration File Password 

Table 316 Maintenance > File Manager > Configuration File (continued)

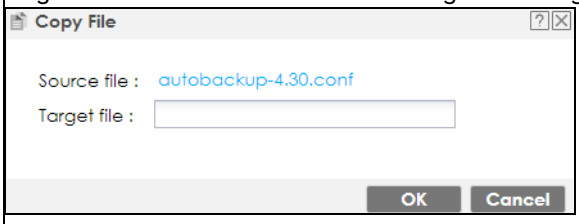
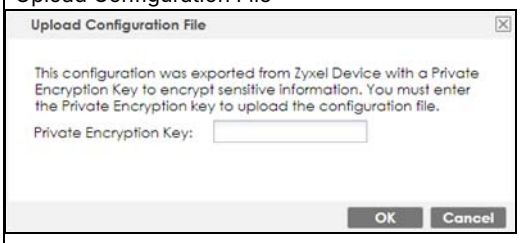
LABEL	DESCRIPTION
Copy	Use this button to save a duplicate of a configuration file on the Zyxel Device. Click a configuration file's row to select it and click Copy to open the Copy File screen. Figure 596 Maintenance > File Manager > Configuration File > Copy  Specify a name for the duplicate configuration file. Use up to 63 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click OK to save the duplicate or click Cancel to close the screen without saving a duplicate of the configuration file.
Apply	Use this button to have the Zyxel Device use a specific configuration file. Click a configuration file's row to select it and click Apply to have the Zyxel Device use that configuration file. The Zyxel Device does not have to restart in order to use a different configuration file, although you will need to wait for a few minutes while the system reconfigures. The following screen gives you option for what the Zyxel Device is to do if it encounters an error in the configuration file. Immediately stop applying the configuration file- this is not recommended because it would leave the rest of the configuration blank. If the interfaces were not configured before the first error, the console port may be the only way to access the device. Immediately stop applying the configuration file and roll back to the previous configuration - this gets the Zyxel Device started with a fully valid configuration file as quickly as possible. Ignore errors and finish applying the configuration file - this applies the valid parts of the configuration file and generates error logs for all of the configuration file's errors. This lets the Zyxel Device apply most of your configuration and you can refer to the logs for what to fix. Ignore errors and finish applying the configuration file and then roll back to the previous configuration - this applies the valid parts of the configuration file, generates error logs for all of the configuration file's errors, and starts the Zyxel Device with a fully valid configuration file. Click OK to have the Zyxel Device start applying the configuration file or click Cancel to close the screen
#	This column displays the number for each configuration file entry. This field is a sequential value, and it is not associated with a specific address. The total number of configuration files that you can save depends on the sizes of the configuration files and the available flash storage space.

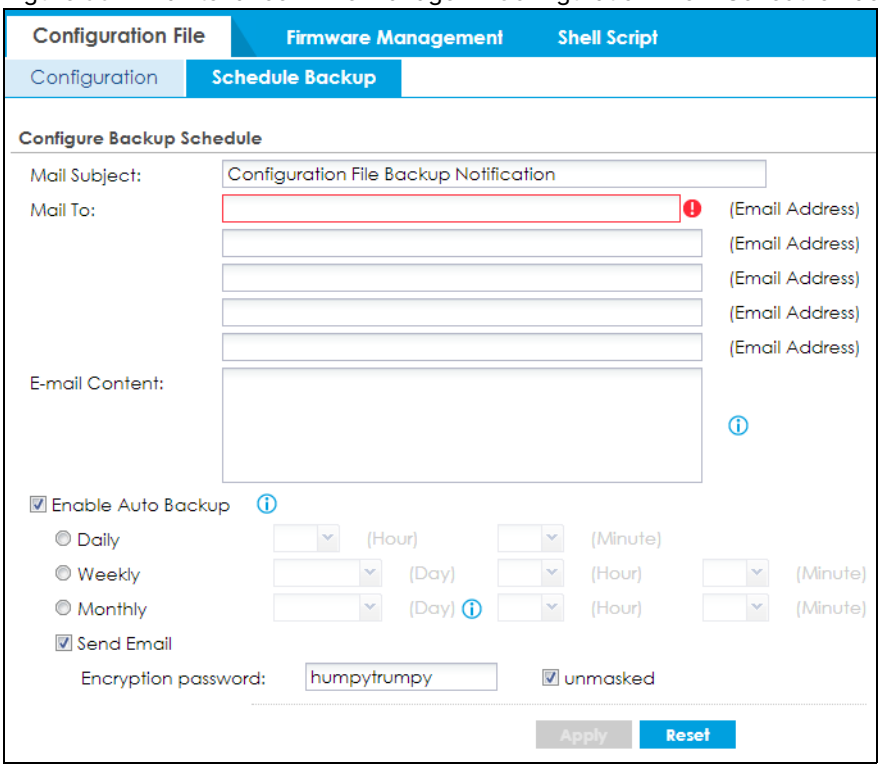
Table 316 Maintenance > File Manager > Configuration File (continued)

LABEL	DESCRIPTION
File Name	This column displays the label that identifies a configuration file. You cannot delete the following configuration files or change their file names. The system-default.conf file contains the Zyxel Device's default settings. Select this file and click Apply to reset all of the Zyxel Device settings to the factory defaults. This configuration file is included when you upload a firmware package. The startup-config.conf file is the configuration file that the Zyxel Device is currently using. If you make and save changes during your management session, the changes are applied to this configuration file. The Zyxel Device applies configuration changes made in the Web Configurator to the configuration file when you click Apply or OK. It applies configuration changes made through commands when you use the `write` command. The lastgood.conf is the most recently used (valid) configuration file that was saved when the device last restarted. If you upload and apply a configuration file with an error, you can apply lastgood.conf to return to a valid configuration.
Size	This column displays the size (in KB) of a configuration file.
Last Modified	This column displays the date and time that the individual configuration files were last changed or saved.
Upload Configuration File	The bottom part of the screen allows you to upload a new or previously saved configuration file from your computer to your Zyxel Device You cannot upload a configuration file named system-default.conf or lastgood.conf. If you upload startup-config.conf, it will replace the current configuration and immediately apply the new settings.
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click Browse... to find the .conf file you want to upload. The configuration file must use a ".conf" filename extension. You will receive an error message if you try to upload a fie of a different format. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click Upload to begin the upload process. This process may take up to two minutes.
Advance	
Add Private Encryption Key	Select the checkbox to enable Sensitive Data Protection; see Section 34.1.2 on page 856 for more information. You need this key to upload configuration files. Write down the key you set and keep it in a safe place. Upload Configuration File  Clear the checkbox to disable Sensitive Data Encryption.
Enter Private Encryption Key	Enter the encryption key in this field. The encryption key should be 4 to 8 single-byte printable characters, including 0-9a-zA-Z'~!@#$%^&*()_\-=+{}|;:'<,>./"
Re-enter Private Encryption Key	Enter the encryption key again in this field.

34.2.1 The Configuration Schedule Backup Screen

Use the Schedule Backup screen to automatically back up the current Zyxel Device configuration file according to a schedule, and then send it to the configured email addresses.

Figure 597 Maintenance > File Manager > Configuration File > Schedule Backup



The following table describes the labels in this screen.

Table 317 Maintenance > File Manager > Configuration File > Schedule Backup

LABEL	DESCRIPTION
Configure Backup Schedule	
Mail Subject	Enter a email subject text with 1-60 characters. It may consist of letters, numbers, and the following special characters: '()+,./:=?;!*#@$%-
Mail To	Enter the receiving email address. You and send the configuration file to a maximum of five email addresses.
E-mail Content	Enter the backup email body text using 1 to 251 single-byte characters, including 0-9a-zA-Z!"#$%&'()*+,-./:;<=>@[\]^_'{|} and spaces are allowed. ? is not allowed.
Enable Auto Backup	Select the checkbox to back up the configuration file at a user defined schedule. Note: After the first backup, the back up only occurs if the configuration file is different from the previous backed up configuration file.
Daily	Set the Zyxel Device to back up its configuration file once a day at the specified hour and minute.
Weekly	Set the Zyxel Device to back up its configuration file once a week on the specified day, at the specified hour and minute.

Table 317 Maintenance > File Manager > Configuration File > Schedule Backup (continued)

LABEL	DESCRIPTION
Monthly	Set the Zyxel Device to back up its configuration file once a month on the specified day, at the a specified hour and minute. Note: If the date you select is greater than the number of days in a month, the Zyxel Device automatically backs up its configuration file on the last day of the month. For example, if you select 31 and the month is February, the Zyxel Device backs up its configuration file on day 28 or 29.
Send Email	Select the checkbox to have the Zyxel Device sends the current configuration file to the configured email addresses.
Encryption password	Enter a password consists of 1 to 31 single-byte characters, with the following special characters !"#$%&'()*+,-./;:<=>@\^_'{|}~ This field is case sensitive. []?and spaces are not allowed.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

34.3 Firmware Management

Use the Firmware Management screen to check your current firmware version and upload firmware to the Zyxel Device. You can upload firmware to be the Running firmware or Standby firmware.

Note: The Web Configurator is the recommended method for uploading firmware. You only need to use the command line interface if you need to recover the firmware. See the CLI Reference Guide for how to determine if you need to recover the firmware and how to recover it.

Find the firmware file in a folder that (usually) uses the system model name with the model code and a bin extension. For example, a firmware for ZyWALL VPN100 is "430ABFV0b2s1.bin".

The firmware update can take up to five minutes. Do not turn off or reset the Zyxel Device while the firmware update is in progress!

If your Zyxel Device has two firmware images installed, and one fails to boot (kernel crash, kernel panic, out-of-memory etc.), then the Zyxel Device will automatically use the (good) backup image to boot.

34.3.1 Cloud Helper

Cloud Helper lets you know if there is a later firmware available on the Cloud Helper server and lets you download it if there is.

Note: Go to myZyxel, create an account and register your Zyxel Device first. Then you will be able to see notification for new firmware available when you log into the 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. The license does not expire if you have firmware version 4.32 patch 1 and later.

The following table explains the Upgrade icons in the web configurator.

Table 318 Cloud Helper Firmware Icons

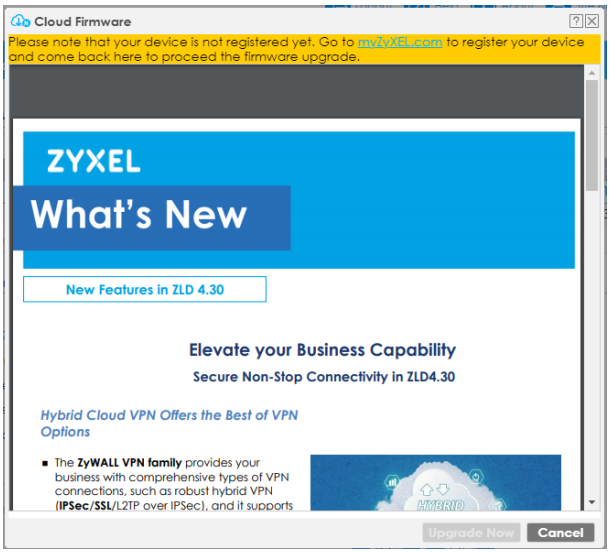
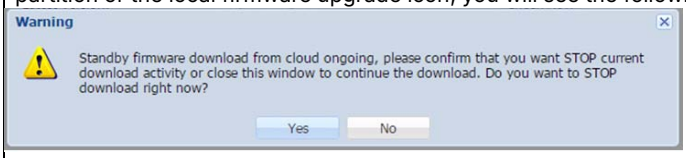
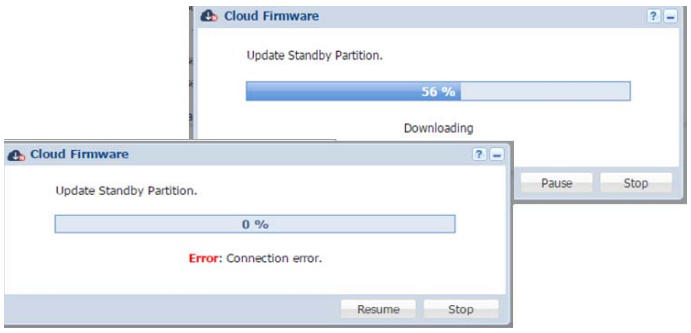
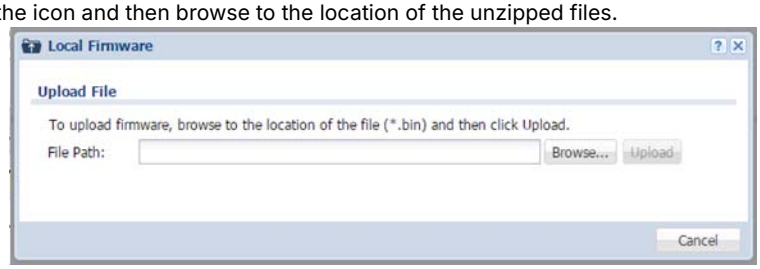
Cloud Helper New	A later firmware is available on the Cloud Helper Server. Click this icon to display a What's New pop-up screen. You need a Firmware Upgrade license to upgrade the firmware. If you do not have a license, Upgrade Now is grayed out. If you have a license, click Upgrade Now to directly upgrade firmware to the standby partition and have the Zyxel Device reboot automatically so that the new standby firmware becomes the running firmware. The previous running firmware becomes the standby firmware. If you haven't registered the Zyxel Device, a message will appear and remind you to register it. Also, Upgrade Now is grayed out. 

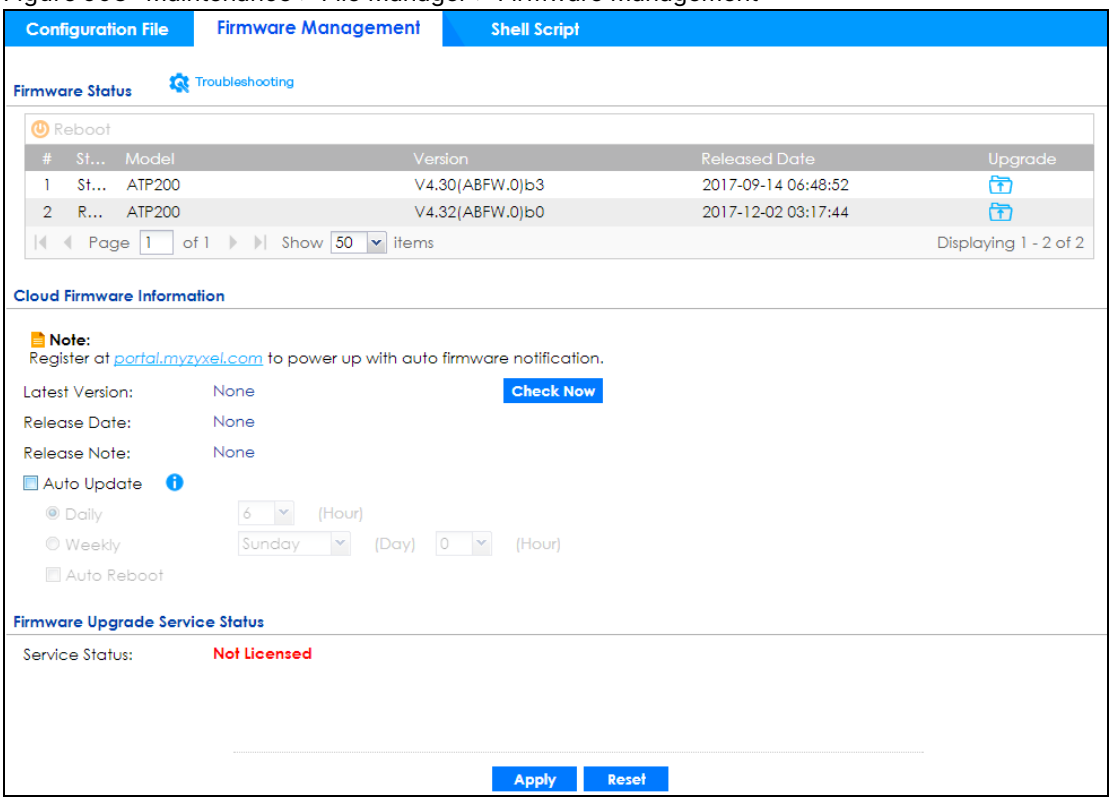
Table 318 Cloud Helper Firmware Icons

Cloud Helper Downloading	Cloud firmware is being downloaded from the Cloud Helper Server. If you select another partition or the local firmware upgrade icon, you will see the following warning message.  When firmware is downloading, you can pause, resume, stop or retry the firmware download. 
Local Firmware	Use this if you have already downloaded the latest firmware from the Zyxel website to your computer and unzipped it. Click the icon and then browse to the location of the unzipped files.  If you upload the latest firmware to the running partition, the Zyxel Device will reboot automatically when it finishes uploading. If you upload the latest firmware to the standby partition, a message will appear to ask if you want to reboot the Zyxel Device.

34.3.2 The Firmware Management Screen

Click Maintenance > File Manager > Firmware Management to open the Firmware Management screen.

Figure 598 Maintenance > File Manager > Firmware Management



The following table describes the labels in this screen.

Table 319 Maintenance > File Manager > Firmware Management

LABEL	DESCRIPTION
Firmware Status	
Reboot	Click the Reboot icon to restart the Zyxel Device. If you applied changes in the web configurator, these were saved automatically and do not change when you reboot. If you made changes in the CLI, however, you have to use the `write` command to save the configuration before you reboot. Otherwise, the changes are lost when you reboot. If you want the Standby firmware to be the Running firmware, then select the Standby firmware row and click Reboot. Wait a few minutes until the login screen appears. If the login screen does not appear, clear your browser cache and refresh the screen or type the IP address of the Zyxel Device in your web browser again. You can also use the CLI command `reboot` to restart the Zyxel Device.
#	This displays the system space (partition) index number where the firmware is located. The firmware can be either Standby or Running; only one firmware can be running at any one time.
Status	This indicates whether the firmware is Running, or not running but already uploaded to the Zyxel Device and is on Standby. It displays N/A if there is no firmware uploaded to that system space.
Model	This is the model name of the device which the firmware is running on.
Version	This is the firmware version and the date created.
Released Date	This is the date that the version of the firmware was created.

Table 319 Maintenance > File Manager > Firmware Management (continued)

LABEL	DESCRIPTION
Upgrade	A cloud helper icon displays if there is a later firmware on the Cloud Server than the firmware in the partition. Click the cloud helper icon to download a later firmware from the Cloud Helper Server. Use the local firmware icon if you have already downloaded the latest firmware from the Zyxel website to your computer and unzipped it.
Cloud Firmware Information	You must register your Zyxel Device at myZyxel first to use cloud firmware.
Latest Version	This displays the latest firmware version at the Cloud Helper Server. Click Check Now to see if there is a later firmware at the Cloud Server.
Release Date	This displays the date the latest firmware version was made available.
Release Note	The release note contains details of latest firmware version such as new features and bug fixes.
Auto Update	Select this checkbox to have the Zyxel Device automatically check for and download new firmware to the standby partition at the time and day specified. You should select a time when your network is not busy for minimal interruption. The firmware will upgrade within an hour from the time you selected. Note: You cannot enable Auto Update in File Manager > Firmware Management and Schedule Reboot in Maintenance > Shutdown-Reboot at the same time.
Daily	Select this option to have the Zyxel Device check for new firmware every day at the specified time. The time format is the 24 hour clock, so '0' means midnight for example.
Weekly	Select this option to have the Zyxel Device check for new firmware once a week on the day and at the time specified.
Auto Reboot	Select this to have the newly downloaded firmware in the standby partition become the running firmware after the Zyxel Device automatically restarts.
Firmware Upgrade Service Status	
Service Status	This field displays whether the firmware license service is activated at myZyxel (Activated) or not (Not Activated).

Click Yes to upload the firmware as the running firmware after the Zyxel Device reboots. Your current configuration settings will be saved and applied after reboot.

The following steps describe procedures to upload firmware and reboot the Zyxel Device.

1. Upload firmware to the standby partition.
2. Click Yes to reboot the Zyxel Device.
3. The firmware you uploaded is copied from the standby partition to the running partition.
4. Your current configuration settings are saved.
5. The Zyxel Device reboots. The firmware you uploaded becomes the running firmware. Your current configuration settings are applied.

   Click No to upload the firmware and current configuration settings to the standby partition. If you reboot the Zyxel Device later, the standby firmware and standby configuration will become the running firmware and new configuration.

Please note that configurations made after you upload the firmware will not be saved to the standby partition. These configurations will be lost after you reboot the Zyxel Device. You should back up your current configuration before you reboot the Zyxel Device.

The following steps describe the procedures to upload firmware without rebooting the Zyxel Device.

1 Upload firmware to the standby partition.

2 Click No to have the Zyxel Device upload firmware without rebooting.

3 Your current configuration settings are saved.

The following steps describe the procedures if you decide to reboot the Zyxel Device later.

1 Back up your current configuration settings.

2 Go to Maintenance > File Manager > Firmware Management. Click the Standby firmware then click Reboot.

3 The firmware in the standby partition is copied to the running partition.

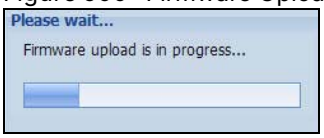
4 The Zyxel Device reboots.

5 The Standby firmware becomes the Running firmware. The configuration settings saved at the time you uploaded the firmware will be applied.

6 If you want to apply the configuration settings you saved at step1, go to Maintenance > File Manager > Configuration File > Configuration > Upload Configuration File to upload the configuration settings file you just saved.

After you see the Firmware Upload in Process screen, wait a few minutes before logging into the Zyxel Device again.

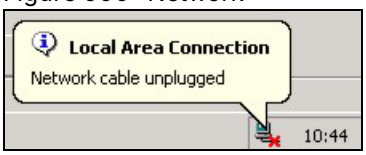
Figure 599 Firmware Upload In Process



Note: The Zyxel Device automatically reboots after a successful upload.

The Zyxel Device automatically restarts causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

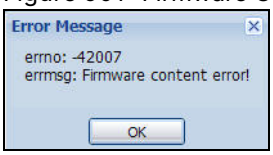
Figure 600 Network



After five minutes, log in again and check your new firmware version in the Dashboard screen.

If the upload was not successful, the following message appears in the status bar at the bottom of the screen.

Figure 601 Firmware Upload Error



34.3.3 Firmware Upgrade through USB Stick

In addition to uploading firmware through the web configurator or console port (see the CLI Reference Guide), you can also upload firmware directly from a USB stick connected to the Zyxel Device.

1. Create a folder on the USB stick called '/[ProductName_dir]/firmware'. For example, if your Zyxel Device is USG110, then create a '/usg110_dir/firmware/' folder on the stick.
2. Put one firmware 'bin' file into the firmware folder. Make sure the firmware ID and version number are correct for your model (the firmware ID is in brackets after the firmware version number - for USG100 it is AAPH).

   Note: Do not put more than one firmware 'bin' file into the firmware folder.

   The firmware version in the USB stick must be different to the currently running firmware. If the firmware on the USB stick is older, then the Zyxel Device will 'upgrade' to the older version. It is recommended that the firmware on the USB stick be the latest firmware version.
3. Insert the USB stick into the Zyxel Device. The firmware uploads to the standby system space.
4. The SYS LED blinks when the Zyxel Device automatically reboots making the upgraded firmware in standby become the running firmware.

   Note: If the startup-config.conf configuration file has problems and you are upgrading to 4.25 or later firmware, then the Zyxel Device will revert (failover) to the previously running firmware.

   If the startup-config.conf configuration file has problems and you are upgrading to earlier than 4.25 firmware, then the Zyxel Device uses the new earlier firmware, but generates a log and tries the existing lastgood.conf configuration file. If there isn't a lastgood.conf configuration file or it also has an error, the Zyxel Device applies the system-default.conf configuration file.

34.3.4 Firmware Integrity Check

The Zyxel Device will conduct a firmware integrity check every time you restart the Zyxel Device.

A firmware integrity check is a feature to check if the firmware currently running on the Zyxel Device is verified. A verified firmware is a firmware that has integrity and is genuine.

- To have integrity, the firmware certificate must pass the digital signature verification.
- To be genuine, the firmware must be officially released by Zyxel and signed by the Zyxel firmware release server.

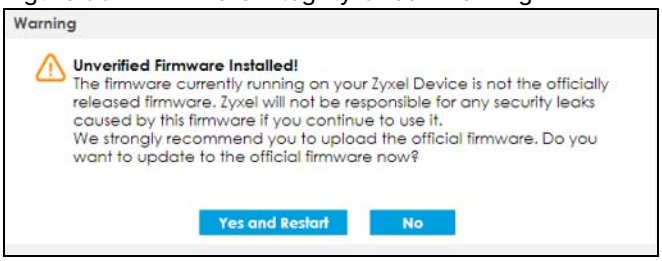
A firmware may have one of the following status:

- The firmware has integrity and is genuine.
- The firmware certificate has expired, but it is genuine.
- The firmware has integrity, but it is not genuine.
- The firmware has no integrity.

At the time of writing, a firmware that has no integrity or is not genuine is considered unverified.

Using an unverified firmware may cause security leaks. Click Yes and Restart to upload the latest official firmware available on the Cloud Helper Server to your Zyxel Device.

Figure 602 Firmware Integrity Check Warning



If you click No, the Zyxel Device will continue to use the unverified firmware, but Zyxel will not be responsible for any security leaks caused by this firmware. A warning icon ( ) will also show in Dashboard > General > Device Information and Maintenance > Firmware Management > Firmware Status.

34.4 The Shell Script Screen

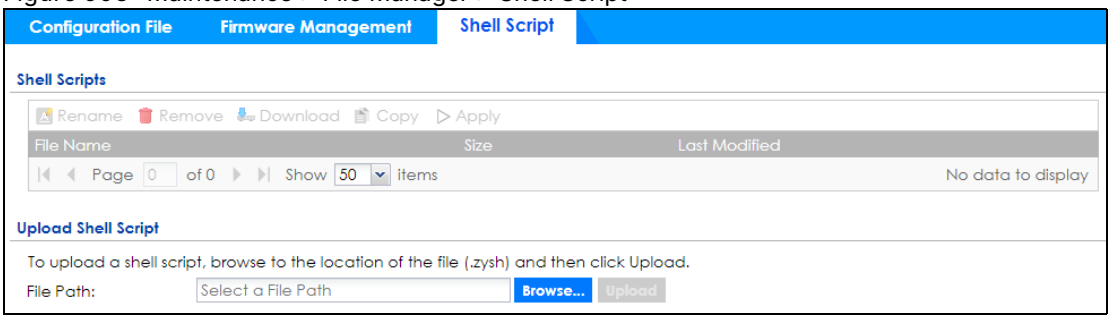
Use shell script files to have the Zyxel Device execute commands that you specify. Use a text editor to create the shell script files. They must use a ".zysh" filename extension.

Click Maintenance > File Manager > Shell Script to open the Shell Script screen. Use the Shell Script screen to store, name, download, upload and run shell script files. You can store multiple shell script files on the Zyxel Device at the same time.

Note: You should include `write` commands in your scripts. If you do not use the `write` command, the changes will be lost when the Zyxel Device restarts. You could use multiple `write` commands in a long script.

See Section 35.2.1 on page 876 for more information on scripts.

Figure 603 Maintenance > File Manager > Shell Script



Each field is described in the following table.

Table 320 Maintenance > File Manager > Shell Script

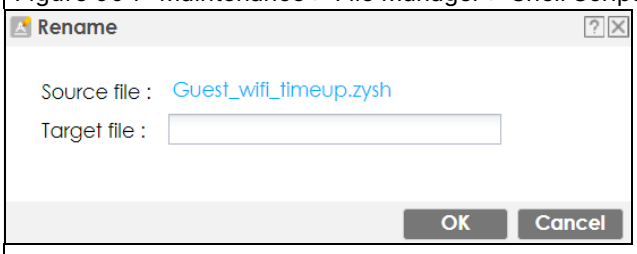
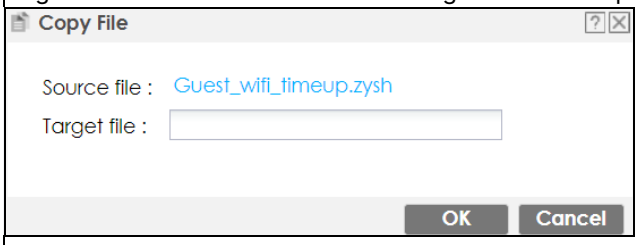
LABEL	DESCRIPTION
Rename	Use this button to change the label of a shell script file on the Zyxel Device. You cannot rename a shell script to the name of another shell script in the Zyxel Device. Click a shell script's row to select it and click Rename to open the Rename File screen. Figure 604 Maintenance > File Manager > Shell Script > Rename  Specify the new name for the shell script file. Use up to 63 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click OK to save the duplicate or click Cancel to close the screen without saving a duplicate of the configuration file.
Remove	Click a shell script file's row to select it and click Remove to delete the shell script file from the Zyxel Device. A pop-up window asks you to confirm that you want to delete the shell script file. Click OK to delete the shell script file or click Cancel to close the screen without deleting the shell script file.
Download	Click a shell script file's row to select it and click Download to save the configuration to your computer.
Copy	Use this button to save a duplicate of a shell script file on the Zyxel Device. Click a shell script file's row to select it and click Copy to open the Copy File screen. Figure 605 Maintenance > File Manager > Shell Script > Copy  Specify a name for the duplicate file. Use up to 63 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click OK to save the duplicate or click Cancel to close the screen without saving a duplicate of the configuration file.
Apply	Use this button to have the Zyxel Device use a specific shell script file. Click a shell script file's row to select it and click Apply to have the Zyxel Device use that shell script file. You may need to wait awhile for the Zyxel Device to finish applying the commands.
File Name	This column displays the label that identifies a shell script file.
Size	This column displays the size (in KB) of a shell script file.
Last Modified	This column displays the date and time that the individual shell script files were last changed or saved.
Upload Shell Script	The bottom part of the screen allows you to upload a new or previously saved shell script file from your computer to your Zyxel Device.

Table 320 Maintenance > File Manager > Shell Script (continued)

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click Browse... to find the .zysh file you want to upload.
Upload	Click Upload to begin the upload process. This process may take up to several minutes.

CHAPTER 35 Diagnostics

35.1 Overview

Use the diagnostics screens for troubleshooting.

35.1.1 What You Can Do in this Chapter

- Use the Diagnostics screens (see Section 35.2 on page 876) to generate a file containing the Zyxel Device's configuration and diagnostic information if you need to provide it to customer support during troubleshooting.
- Use the Packet Capture screens (see Section 35.3 on page 880) to capture packets going through the Zyxel Device.
- Use the CPU / Memory Status screens (see Section 35.4 on page 884) to view the CPU and memory performance of various applications on the Zyxel Device.
- Use the System Logs screen (see Section 35.5 on page 885) to see system logs stored on a connected USB storage device on the Zyxel Device.
- Use the Network Tool screen (see Section 35.6 on page 886) to ping an IP address or trace the route packets take to a host.
- Use the Routing Traces screens (see Section 35.7 on page 890) to configure traceroute to identify where packets are dropped for troubleshooting.
- Use the Wireless Frame Capture screens (see Section 35.8 on page 891) to capture network traffic going through the AP interfaces connected to your Zyxel Device.

35.2 The Diagnostics Screens

The Diagnostics screens provide an easy way for you to generate a file containing the Zyxel Device's configuration and diagnostic information. You may need to send this file to customer support for troubleshooting.

35.2.1 Scripts

Use scripts to gather information on the Zyxel Device or on external APs connected to the Zyxel Device.

Use a notepad editor that supports Unicode, such as Notepad to create a script. Each command in a script must be on its own line and the file must end with an empty line. The script must be saved in Unicode format (UTF-8).

This is an example of a script to display information about the Zyxel Device.

```
show service-register status all
show myzyxel-service get-cloud-timezone
show cloud-helper firmware
show cloud-helper remind
```

This is an example of a default script with interface diagnostic commands.

```
debug interface ifconfig
debug interface show event_sink
debug interface show interface_obj
debug switch table
debug switch port_groupping
show ping-check status
debug system netstat interface
show interface all
show port status
```

Script Name

The script name must use a “.zysh” filename extension with a file name of up to 25 characters (including a-z, A-Z, 0-9 and ;’~!@#$%^&()_+[]{}’,.=-). Spaces are allowed

Script Uploads to the Zyxel Device

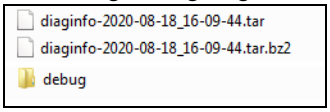
You can upload scripts in File Manager > Shell Script to run commands on the Zyxel Device. You can also copy, and download scripts here.

Upload a script in Diagnostics > Controller to generate information about the Zyxel Device own configuration and diagnostics.

Upload a script in Diagnostics > AP to generate information about the selected managed AP in Diagnostics > AP.

Script Output

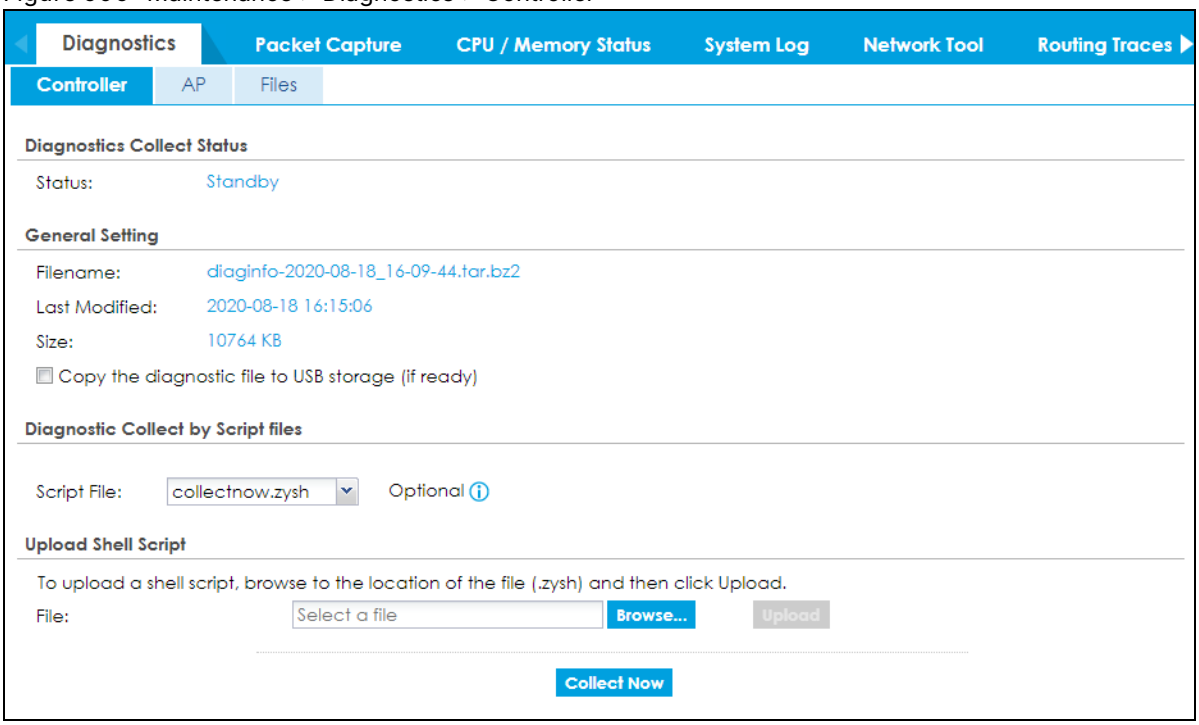
The results of generating a script are shown in Diagnostics > Files in bz2 format. You need to decompress the bz2 file to tar, and then unwrap the tar file to display a debug folder that contains other folders containing debug dbg text files. Customer support may request the bz2 file for troubleshooting.



35.2.2 The Diagnostics Controller Screen

Click Maintenance > Diagnostics > Controller to open the following screen. When you click Collect Now, a series of commands are run to display information about the Zyxel Device.

Figure 606 Maintenance > Diagnostics > Controller

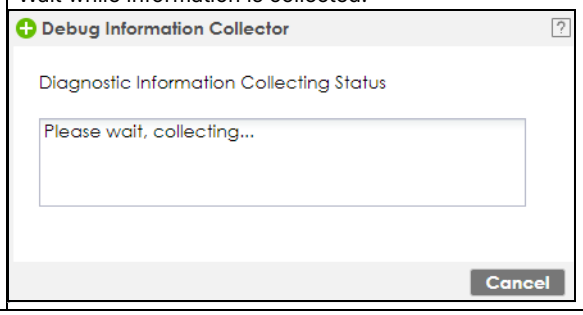


The following table describes the labels in this screen.

Table 321 Maintenance > Diagnostics > Controller

LABEL	DESCRIPTION
Diagnostics Collect Status	
Status	This field displays the following states the Zyxel Device is in when collecting diagnostic data. • Standby: The Zyxel Device is ready to generate a diagnostic file or has just finished generating a diagnostic file. • Busy on AP: The Zyxel Device is generating a diagnostic file for the selected managed AP in Diagnostics > AP. • Busy on ZyWall: The Zyxel Device is generating a diagnostic file containing its own configuration and diagnostic information.
General Setting	
Filename	This is the name of the most recently created diagnostic file.
Last modified	This is the date and time that the last diagnostic file was created. The format is yyyy-mm-dd hh:mm:ss.
Size	This is the size of the most recently created diagnostic file.
Copy the diagnostic file to USB storage (if ready)	Select this to have the Zyxel Device create an extra copy of the diagnostic file to a connected USB storage device.
Diagnostic Collect by Script files	
Script File	Select a script here to generate information about configuration and diagnostics of managed APs. See Section 35.2.1 on page 876 for more information on scripts.
Upload Shell Script	

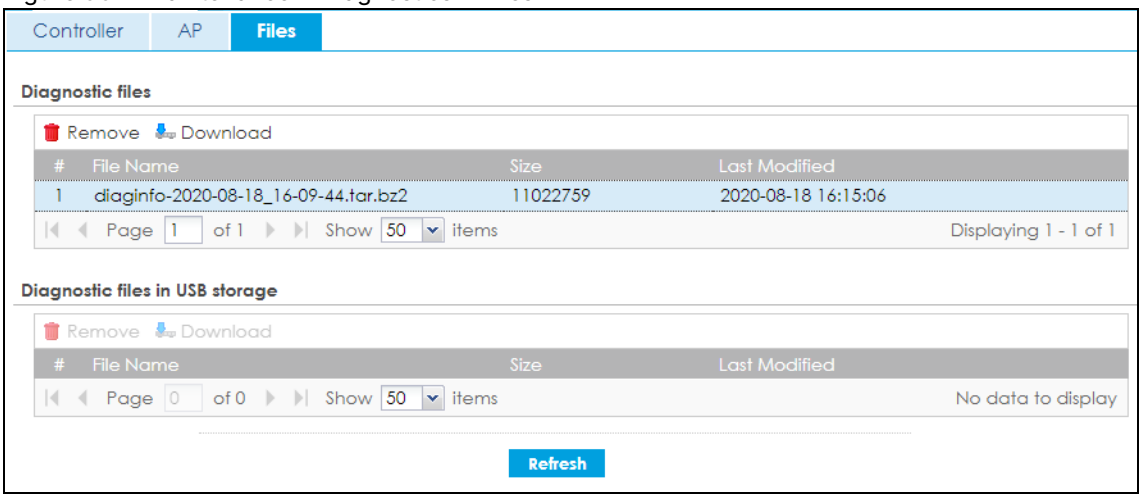
Table 321 Maintenance > Diagnostics > Controller (continued)

LABEL	DESCRIPTION
File	Upload a script here to generate information about the Zyxel Device's own configuration and diagnostics. Click Browse to find the location of the file you want to upload in this field. Click Upload to begin the upload process. This process may take a few minutes.
Collect Now	Click this to have the Zyxel Device run the uploaded script and create a new diagnostic file. Wait while information is collected. 

35.2.3 The Diagnostics Files Screen

Click Maintenance > Diagnostics > Files to open the diagnostic files screen. This screen lists the files of diagnostic information the Zyxel Device has collected and stored on the Zyxel Device or in a connected USB storage device. You may need to send these files to customer support for troubleshooting.

Figure 607 Maintenance > Diagnostics > Files



The following table describes the labels in this screen.

Table 322 Maintenance > Diagnostics > Files

LABEL	DESCRIPTION
Diagnostic files	This lists the files of generated diagnostic information stored on the Zyxel Device.
Diagnostic files in USB storage	This lists the files of generated diagnostic information stored in a connected USB storage device.

Table 322 Maintenance > Diagnostics > Files (continued)

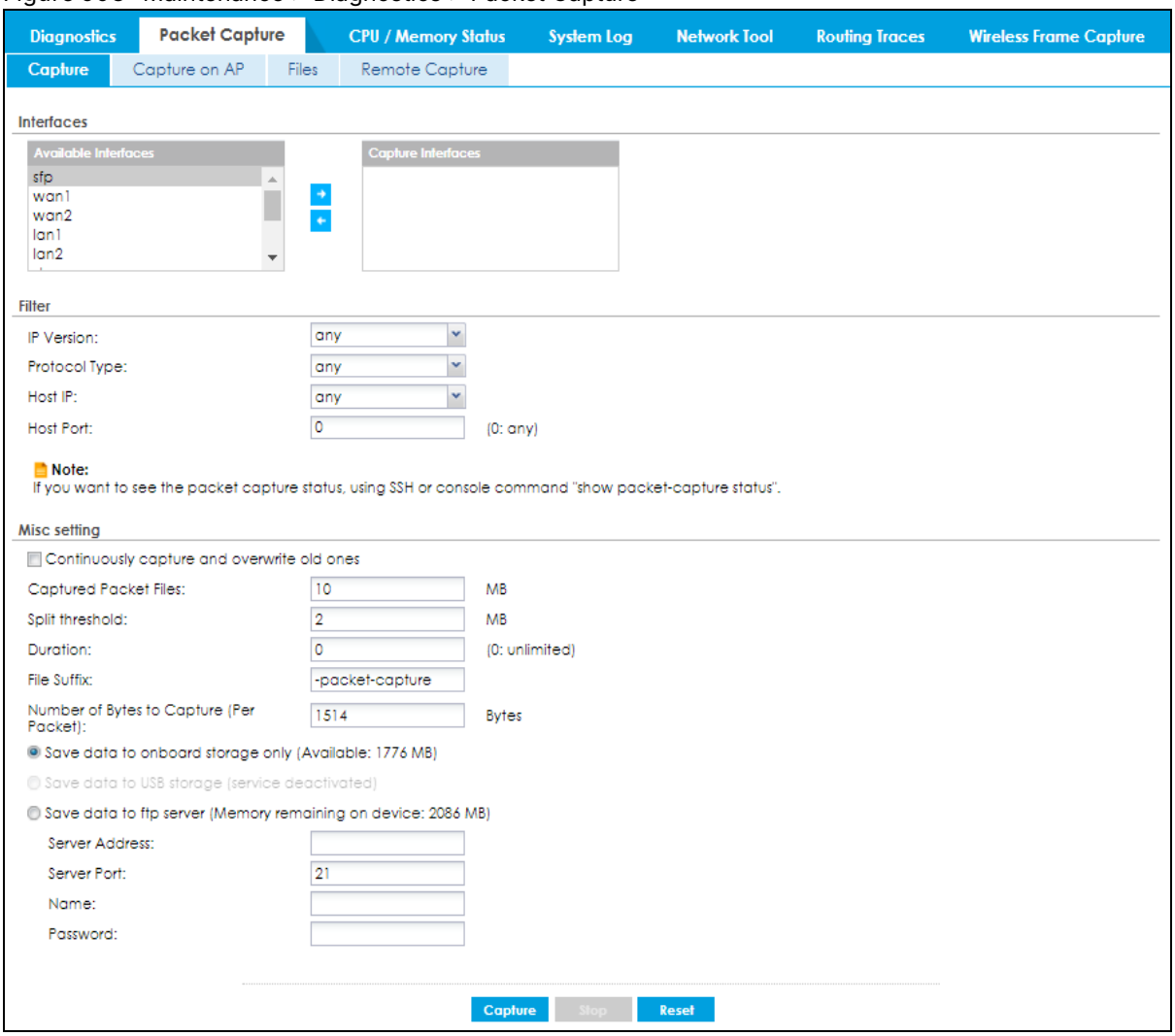
LABEL	DESCRIPTION
Remove	Select files and click Remove to delete them from the Zyxel Device or the USB storage device. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click Download to save it to your computer.
#	This column displays the number for each file entry. The total number of files that you can save depends on the file sizes and the available storage space.
File Name	This column displays the label that identifies the file.
Size	This column displays the size (in bytes) of a file.
Last Modified	This column displays the date and time that the individual files were saved.

35.3 The Packet Capture Screen

Use this screen to capture network traffic going through the Zyxel Device's interfaces. Studying these packet captures may help you identify network problems. Click Maintenance > Diagnostics > Packet Capture to open the packet capture screen.

Note: New capture files overwrite existing files of the same name. Change the File Suffix field's setting to avoid this.

Figure 608 Maintenance > Diagnostics > Packet Capture



The following table describes the labels in this screen.

Table 323 Maintenance > Diagnostics > Packet Capture

LABEL	DESCRIPTION
Interfaces	Enabled interfaces (except for virtual interfaces) appear under Available Interfaces. Select interfaces for which to capture packets and click the right arrow button to move them to the Capture Interfaces list. Use the [Shift] and/or [Ctrl] key to select multiple objects.
IP Version	Select the version of IP for which to capture packets. Select any to capture packets for all IP versions.
Protocol Type	Select the protocol of traffic for which to capture packets. Select any to capture packets for all types of traffic.
Host IP	Select a host IP address object for which to capture packets. Select any to capture packets for all hosts. Select User Defined to be able to enter an IP address.
Host Port	This field is configurable when you set the IP Type to any, tcp, or udp. Specify the port number of traffic to capture.
Continuously capture and overwrite old ones	Select this to have the Zyxel Device keep capturing traffic and overwriting old packet capture entries when the available storage space runs out.

Table 323 Maintenance > Diagnostics > Packet Capture (continued)

LABEL	DESCRIPTION
Captured Packet Files	When saving packet captures only to the Zyxel Device's on board storage, specify a maximum limit in megabytes for the total combined size of all the capture files on the Zyxel Device. When saving packet captures to a connected USB storage device, specify a maximum limit in megabytes for each capture file. Note: If you have existing capture files and have not selected the Continuously capture and overwrite old ones option, you may need to set this size larger or delete existing capture files. The valid range depends on the available on board/USB storage size. The Zyxel Device stops the capture and generates the capture file when either the file reaches this size or the time period specified in the Duration field expires.
Split threshold	Specify a maximum size limit in megabytes for individual packet capture files. After a packet capture file reaches this size, the Zyxel Device starts another packet capture file.
Duration	Set a time limit in seconds for the capture. The Zyxel Device stops the capture and generates the capture file when either this period of time has passed or the file reaches the size specified in the File Size field. 0 means there is no time limit.
File Suffix	Specify text to add to the end of the file name (before the dot and filename extension) to help you identify the packet capture files. Modifying the file suffix also avoids making new capture files that overwrite existing files of the same name. The file name format is "interface name-file suffix.cap", for example "vlan2-packet-capture.cap".
Number Of Bytes To Capture (Per Packet)	Specify the maximum number of bytes to capture per packet. The Zyxel Device automatically truncates packets that exceed this size. As a result, when you view the packet capture files in a packet analyzer, the actual size of the packets may be larger than the size of captured packets.
Save data to onboard storage only	Select this to have the Zyxel Device only store packet capture entries on the Zyxel Device. The available storage size is displayed as well. Note: The Zyxel Device reserves some on board storage space as a buffer.
Save data to USB storage	Select this to have the Zyxel Device store packet capture entries only on a USB storage device connected to the Zyxel Device if the Zyxel Device allows this. Status: 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. none - no USB storage device is connected. service deactivated - USB storage feature is disabled (in Configuration > System > USB Storage), so the Zyxel Device cannot use a connected USB device to store system logs and other diagnostic information. available - you can have the Zyxel Device use the USB storage device. The available storage capacity also displays. Note: The Zyxel Device reserves some USB storage space as a buffer.
Save data to ftp server (available: xx MB)	Select this to have the Zyxel Device store packet capture entries on the defined FTP site. The available storage size is displayed as well.
Server Address	Type the IP address of the FTP server.
Server Port	Type the port this server uses for FTP traffic. The default FTP port is 21.
Name	Type the login username to access the FTP server.
Password	Type the associated login password to access the FTP server.

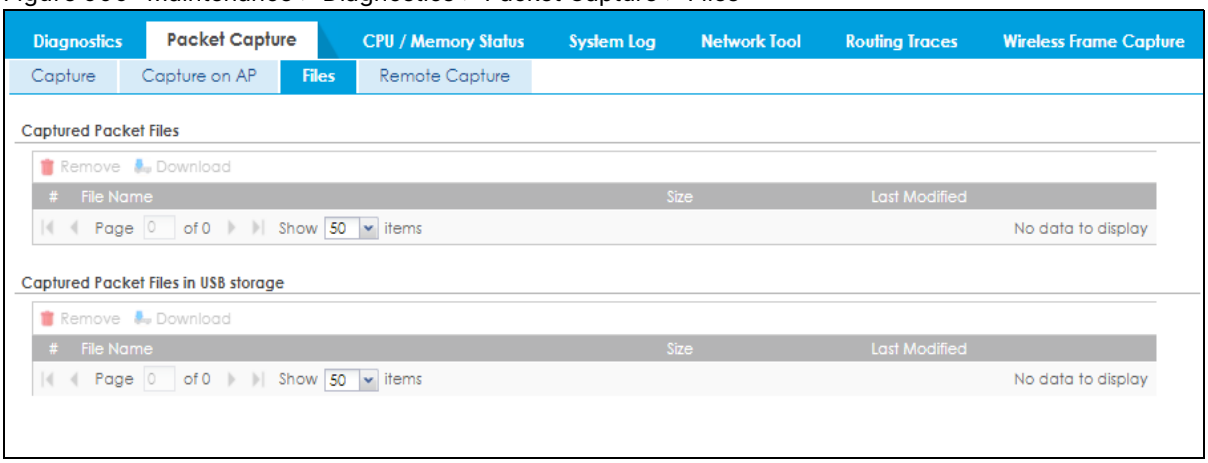
Table 323 Maintenance > Diagnostics > Packet Capture (continued)

LABEL	DESCRIPTION
Capture	Click this button to have the Zyxel Device capture packets according to the settings configured in this screen. You can configure the Zyxel Device while a packet capture is in progress although you cannot modify the packet capture settings. The Zyxel Device's throughput or performance may be affected while a packet capture is in progress. After the Zyxel Device finishes the capture it saves a separate capture file for each selected interface. The total number of packet capture files that you can save depends on the file sizes and the available flash storage space. Once the flash storage space is full, adding more packet captures will fail.
Stop	Click this button to stop a currently running packet capture and generate a separate capture file for each selected interface.
Reset	Click this button to return the screen to its last-saved settings.

35.3.1 The Packet Capture Files Screen

Click Maintenance > Diagnostics > Packet Capture > Files to open the packet capture files screen. This screen lists the files of packet captures stored on the Zyxel Device or a connected USB storage device. You can download the files to your computer where you can study them using a packet analyzer (also known as a network or protocol analyzer) such as Wireshark.

Figure 609 Maintenance > Diagnostics > Packet Capture > Files



The following table describes the labels in this screen.

Table 324 Maintenance > Diagnostics > Packet Capture > Files

LABEL	DESCRIPTION
Remove	Select files and click Remove to delete them from the Zyxel Device or the connected USB storage device. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click Download to save it to your computer.
#	This column displays the number for each packet capture file entry. The total number of packet capture files that you can save depends on the file sizes and the available flash storage space.
File Name	This column displays the label that identifies the file. The file name format is interface name-file suffix.cap.

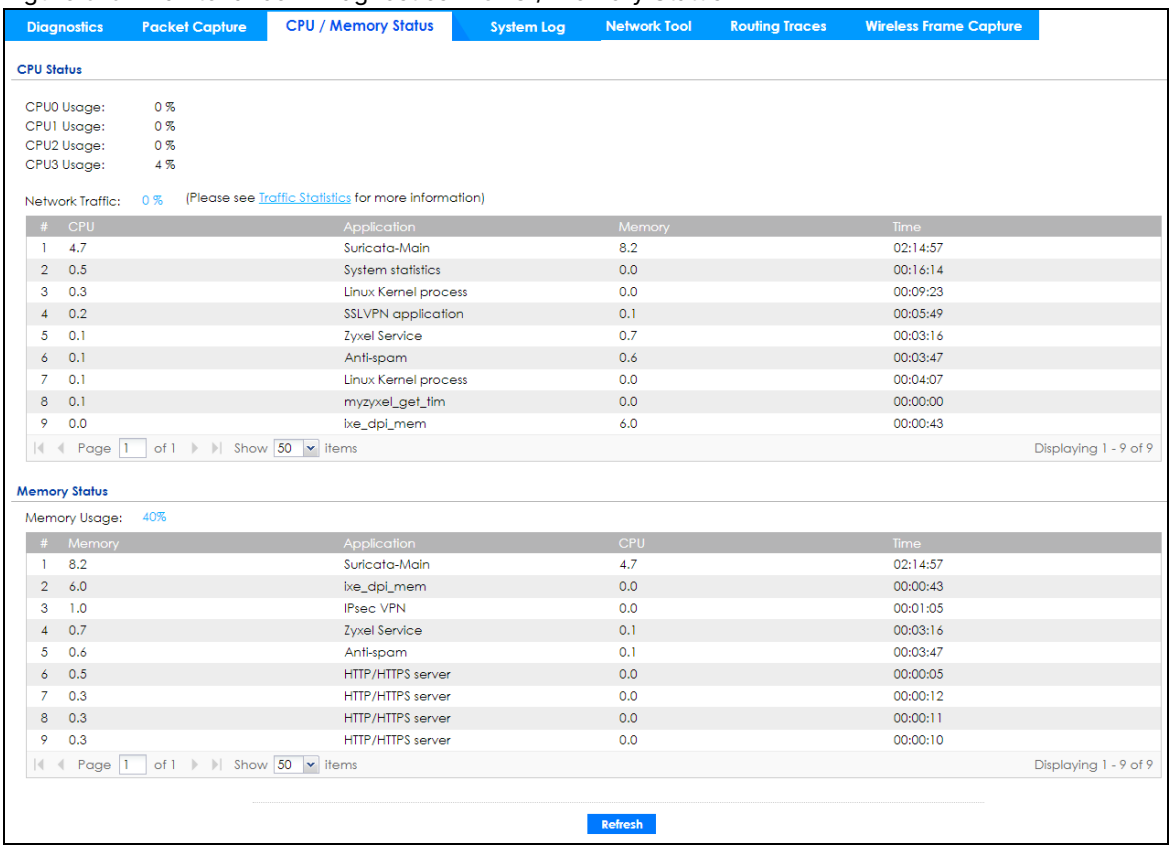
Table 324 Maintenance > Diagnostics > Packet Capture > Files (continued)

LABEL	DESCRIPTION
Size	This column displays the size (in bytes) of a configuration file.
Last Modified	This column displays the date and time that the individual files were saved.

35.4 The CPU / Memory Status Screen

Click Maintenance > Diagnostics > CPU / Memory Status to open the CPU/Memory Status screen. Use this screen to view the CPU and memory performance of various applications on the Zyxel Device.

Figure 610 Maintenance > Diagnostics > CPU / Memory Status



The following table describes the labels in this screen.

Table 325 Maintenance > Diagnostics > CPU / Memory Status

LABEL	DESCRIPTION
CPU Status This table displays the applications that use the most Zyxel Device CPU processing.	
CPUn Usage	CPU usage shows how much processing power the Zyxel Device is using. This field displays the current percentage usage of a CPU (where n is the number of the CPU) as a percentage of total processing power.
Network Traffic	This field displays the current percentage of network traffic through the Zyxel Device.
#	This field is a sequential value, and it is not associated with any entry.

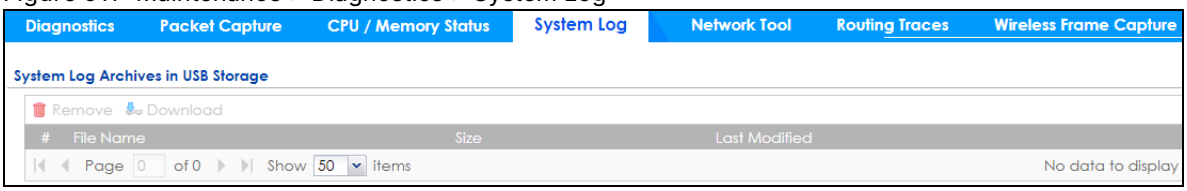
Table 325 Maintenance > Diagnostics > CPU / Memory Status

LABEL	DESCRIPTION
CPU	This field displays the current CPU utilization percentage for each application used on the Zyxel Device.
Application	This field displays the name of the application consuming the related processing power on the Zyxel Device.
Memory	This field displays the current DRAM memory utilization percentage for each application used on the Zyxel Device.
Time	This field displays each application's running time in hours - minutes - seconds.
Memory Status This table displays the applications that use the most Zyxel Device DRAM memory.	
Memory Usage	Memory usage shows how much DRAM memory the Zyxel Device is using. This field displays the current percentage of memory utilization.
#	This field is a sequential value, and it is not associated with any entry.
Memory	This field displays the current DRAM memory utilization percentage for each application used on the Zyxel Device.
Application	This field displays the name of the application consuming the related memory on the Zyxel Device.
CPU	This field displays the current CPU utilization percentage for each application used on the Zyxel Device.
Time	This field displays each application's running time.
Refresh	Click this to update the information in this screen.

35.5 The System Log Screen

Click Maintenance > Diagnostics > System Log to open the System Log screen. This screen lists the files of Zyxel Device system logs stored on a connected USB storage device. The files are in comma separated value (csv) format. You can download them to your computer and open them in a tool like Microsoft's Excel.

Figure 611 Maintenance > Diagnostics > System Log



The following table describes the labels in this screen.

Table 326 Maintenance > Diagnostics > System Log

LABEL	DESCRIPTION
Remove	Select files and click Remove to delete them from the Zyxel Device. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click Download to save it to your computer.
#	This column displays the number for each file entry. The total number of files that you can save depends on the file sizes and the available storage space.
File Name	This column displays the label that identifies the file.

Table 326 Maintenance > Diagnostics > System Log

LABEL	DESCRIPTION
Size	This column displays the size (in bytes) of a file.
Last Modified	This column displays the date and time that the individual files were saved.

35.6 The Network Tool Screen

Use this screen to perform various network tests.

Click Maintenance > Diagnostics > Network Tool to display this screen.

Figure 612 Maintenance > Diagnostics > Network Tool

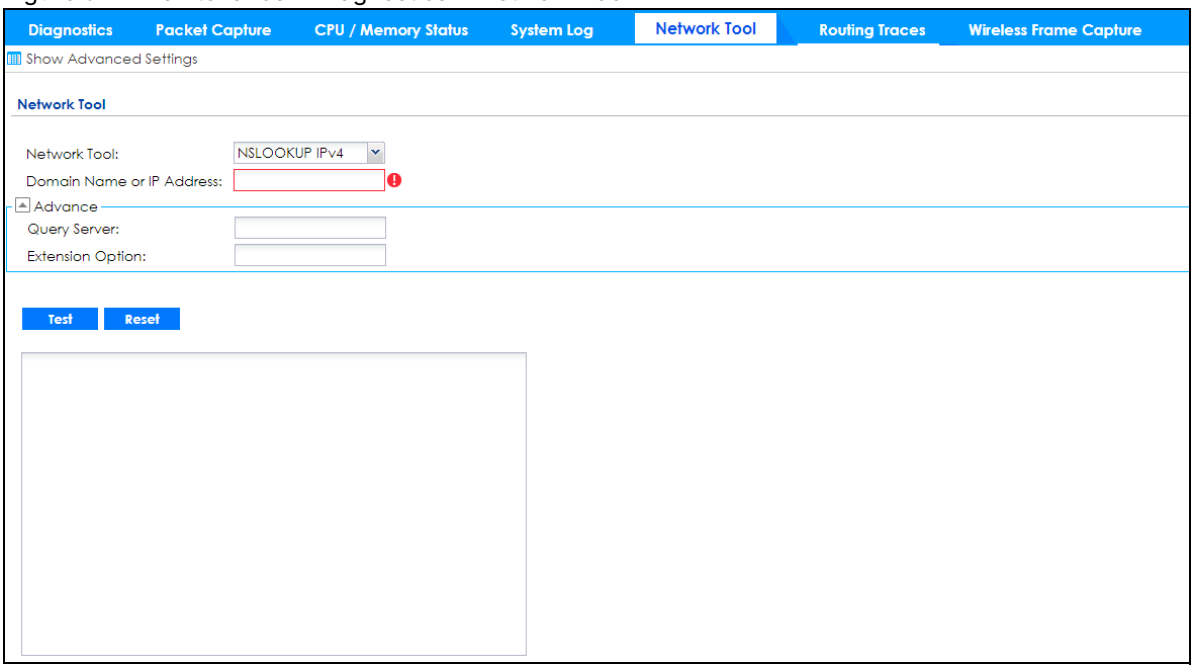


Figure 613 Maintenance > Diagnostics > Network Tool - Test Email Server

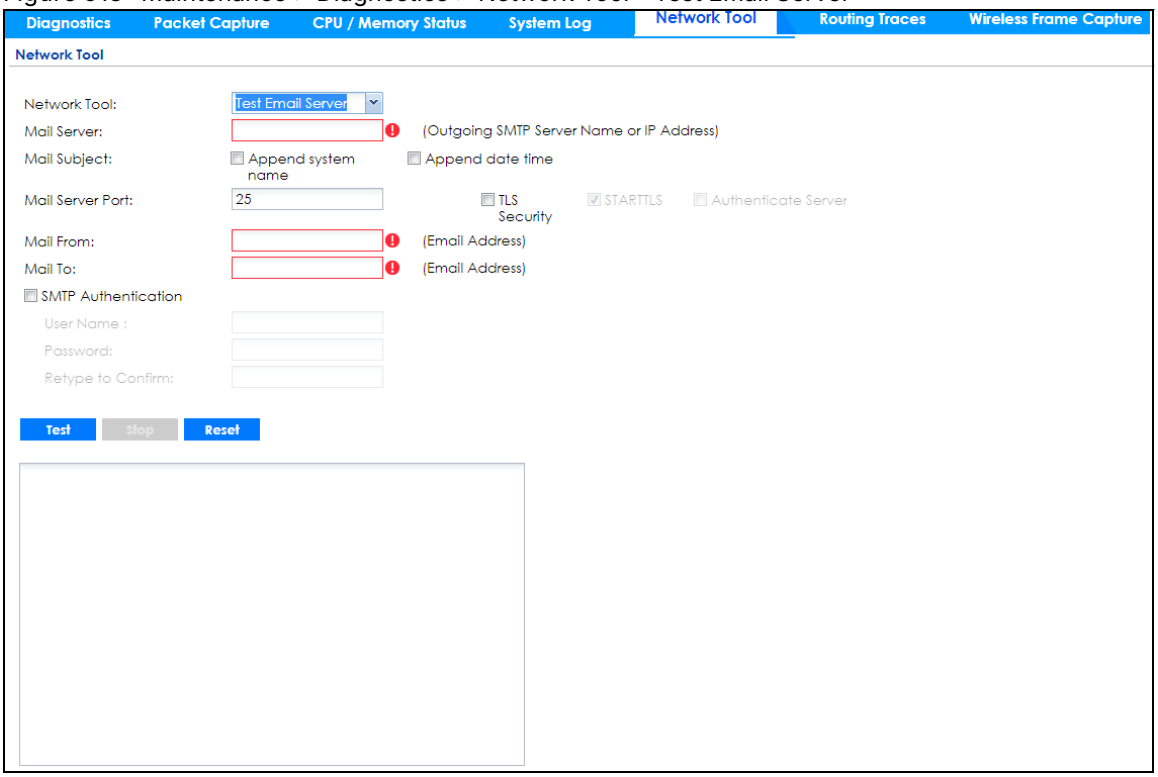
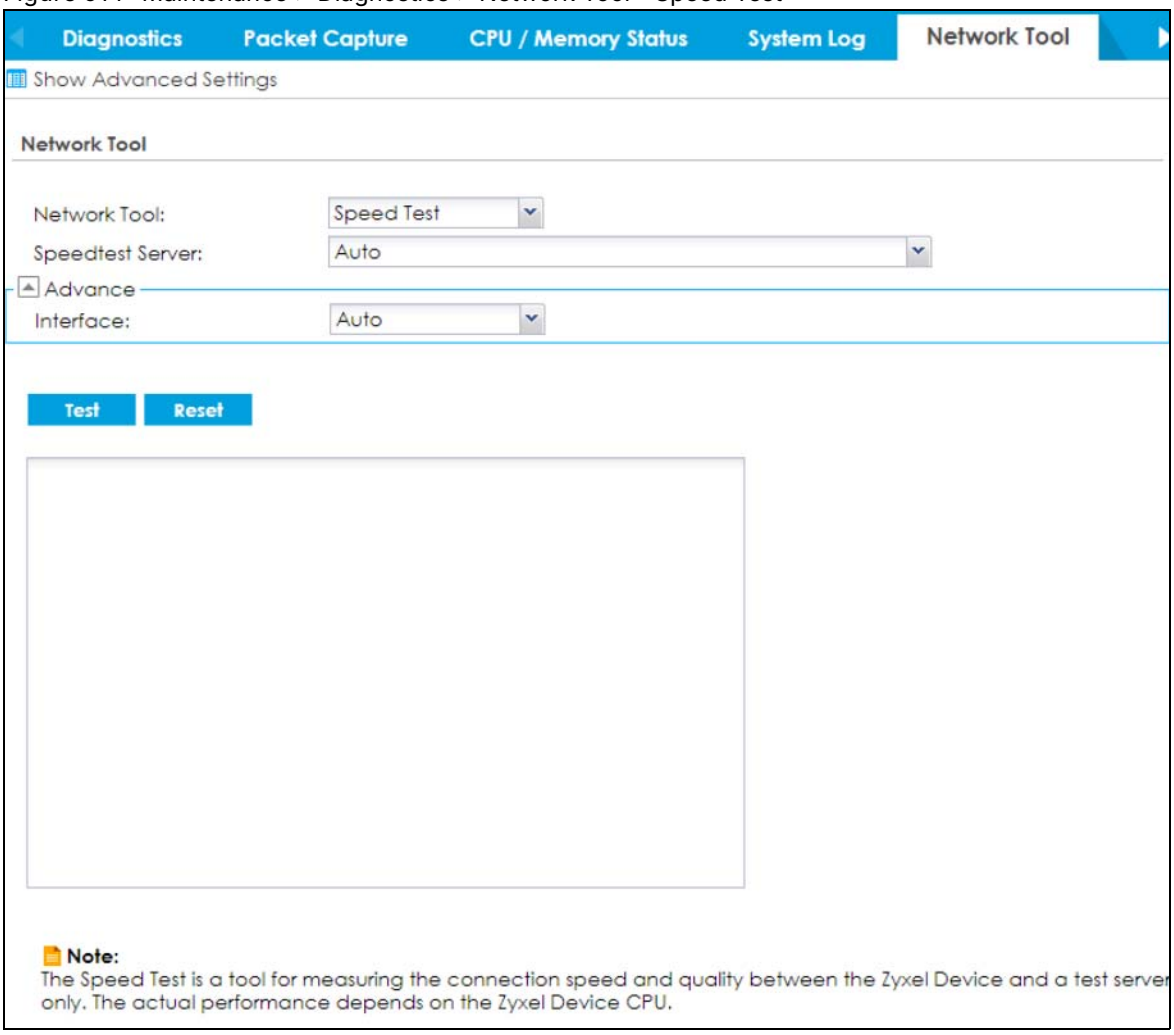


Figure 614 Maintenance > Diagnostics > Network Tool - Speed Test



The following table describes the labels in this screen.

Table 327 Maintenance > Diagnostics > Network Tool

LABEL	DESCRIPTION
Network Tool	Select a network tool: • Select NSLOOKUP IPv4 or NSLOOKUP IPv6 to perform name server lookup for querying the Domain Name System (DNS) to get the domain name or IP address mapping. • Select PING IPv4 or PING IPv6 to ping the IP address that you entered. • Select TRACEROUTE IPv4 or TRACEROUTE IPv6 to run the traceroute function. This determines the path a packet takes to the specified computer. • Select Test Email Server to test access to an SMTP email server. • Select Speed Test to test the connection speed and quality between the Zyxel Device and a test server on the Internet.
Domain Name or IP Address	Type the IP address that you want to use to for the selected network tool.
Advance Click this to display the following fields.	
Query Server	Enter the IP address of a server to which the Zyxel Device sends queries for NSLOOKUP.

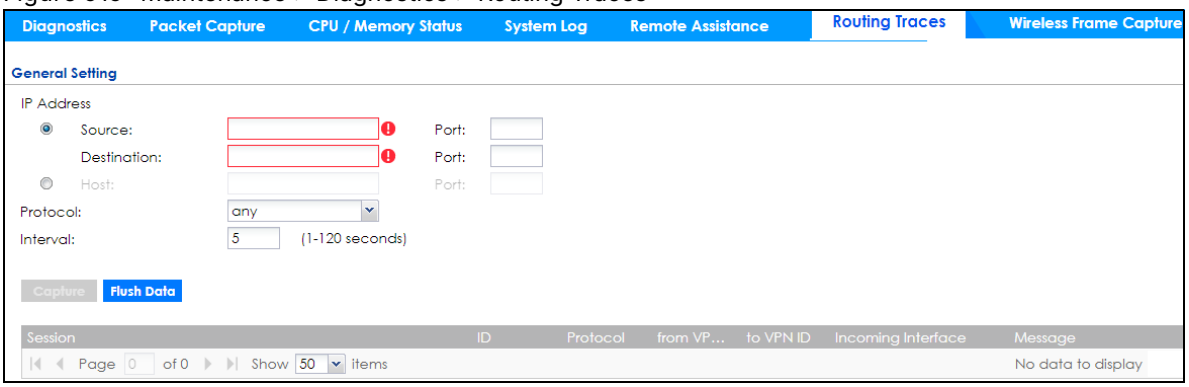
Table 327 Maintenance > Diagnostics > Network Tool (continued)

LABEL	DESCRIPTION
Interface	Select the interface through which the Zyxel Device sends queries for PING or TRACEROUTE.
Extension Option	Enter the extended option if you want to use an extended ping or traceroute command. For example, enter "`-c count`" (where `count` is the number of ping requests) to set how many times the Zyxel Device pings the destination IP address, or enter "`-w waittime`" (where `waittime` is a time period in seconds) to set how long the Zyxel Device waits for a response to a probe before running another traceroute.
The following fields display when you select Test Email Server in Network Tool.	
Mail Server	Type the name or IP address of the outgoing SMTP server.
Mail Subject	Type the subject line for the outgoing email. • Select Append system name to add the Zyxel Device system name to the subject. • Select Append date time to add the Zyxel Device date and time to the subject.
Mail Server Port	Enter the same port number here as is on the mail server for mail traffic.
TLS Security	Select this option if the mail server uses Transport Layer Security (TLS) for encrypted communications between the mail server and the Zyxel Device.
STARTTLS	Select this option if the mail server uses SSL or TLS for encrypted communications between the mail server and the Zyxel Device.
Authenticate Server	Select this if the Zyxel Device authenticates the mail server in the TLS handshake.
Mail From	Type the email address from which the outgoing email is delivered. This address is used in replies.
Mail To	Type the email address to which the outgoing email is delivered.
SMTP Authentication	Select this checkbox if it is necessary to provide a user name and password to the SMTP server.
User Name	This box is effective when you select the SMTP Authentication checkbox. Type the user name to provide to the SMTP server when the log is emailed.
Password	This box is effective when you select the SMTP Authentication checkbox. Type a password of up to 63 characters to provide to the SMTP server when the log is emailed.
Retype to Confirm	Retype your new password for confirmation.
The following fields display when you select Speed Test in Network Tool.	
Speed Test Server	Select Auto to have the Zyxel Device test the connection speed and quality between the Zyxel Device and a server nearest to the on Zyxel Device the Internet. Select a specified test server to have the Zyxel Device test the connection speed and quality between the Zyxel Device and the server you selected. Please note that this field is read-only if you selected a specified interface in Interface.
Interface	Select Auto to have the Zyxel Device test the connection speed and quality on one of the interface in Configuration > Network > Interface > Trunk > System Default > SYSTEM_DEFAULT_WAN_TRUNK. Select WAN to have the Zyxel Device test the connection speed and quality on the WAN. Please note that this field is read-only if you selected a specified server in Speed Test Server.
Test	Click this button to start the test.
Stop	Click this button to stop the test.
Reset	Click this button to return the screen to its last-saved settings.

35.7 The Routing Traces Screen

Click Maintenance > Diagnostics > Routing Traces to display this screen. Use this screen to configure a traceroute to identify where packets are dropped for troubleshooting.

Figure 615 Maintenance > Diagnostics > Routing Traces



The following table describes the labels in this screen.

Table 328 Maintenance > Diagnostics > Routing Traces

LABEL	DESCRIPTION
IP Address	You can trace traffic through the Zyxel Device from a specific source-to-destination stream or just from/to a specific host (source or destination).
Source	Enter the source IP address of traffic that you want to trace.
Port	Enter the source port number of traffic that you want to trace.
Destination	Enter the destination IP address of traffic that you want to trace.
Port	Enter the destination port number of traffic that you want to trace.
Host	Enter the IP address of a specific source or destination host whose traffic you want to trace.
Port	Enter the port number for particular source traffic on the host that you want to trace.
Protocol	Select the protocol of traffic that you want to trace. any means any protocol.
Interval	Enter a time interval in seconds for renewing a route trace. The default time interval is 5 seconds.
Capture	Click this button to have the Zyxel Device capture frames according to the settings configured in this screen. You can configure the Zyxel Device while a frame capture is in progress although you cannot modify the frame capture settings.
Flush Data	Click this to clear all data on the screen.
Session	This field displays established sessions that passed through the Zyxel Device which matched the capture criteria.
ID	This field displays the packet ID for each active session.
Protocol	This field displays the protocol used in each active session.
from VPN ID	This field displays the identifier for incoming VPN connections on the Zyxel Device.
to VPN ID	This field displays the identifier for outgoing VPN connections on the Zyxel Device.
Incoming Interface	This is the source interface of packets to which this active session applies.
Message	This field displays traceroute information.

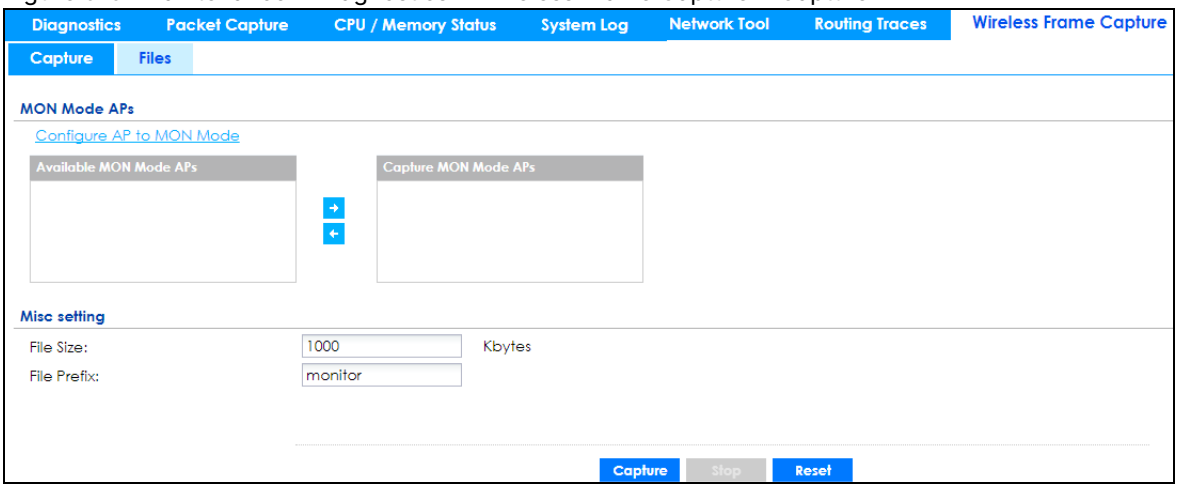
35.8 The Wireless Frame Capture Screen

Use this screen to capture wireless network traffic going through the AP interfaces connected to your Zyxel Device. Studying these frame captures may help you identify network problems.

Click Maintenance > Diagnostics > Wireless Frame Capture to display this screen.

Note: New capture files overwrite existing files of the same name. Change the File Prefix field's setting to avoid this.

Figure 616 Maintenance > Diagnostics > Wireless Frame Capture > Capture



The following table describes the labels in this screen.

Table 329 Maintenance > Diagnostics > Wireless Frame Capture > Capture

LABEL	DESCRIPTION
MON Mode APs	
Configure AP to MON Mode	Click this to go the Configuration > Wireless > AP Management screen, where you can set one or more APs to monitor mode.
Available MON Mode APs	This column displays which APs on your wireless network are currently configured for monitor mode. Use the arrow buttons to move APs off this list and onto the Captured MON Mode APs list.
Capture MON Mode APs	This column displays the monitor-mode configured APs selected to for wireless frame capture.
Misc Setting	
File Size	Specify a maximum size limit in kilobytes for the total combined size of all the capture files on the Zyxel Device, including any existing capture files and any new capture files you generate. Note: If you have existing capture files you may need to set this size larger or delete existing capture files. The valid range is 1 to 50000. The Zyxel Device stops the capture and generates the capture file when either the file reaches this size.

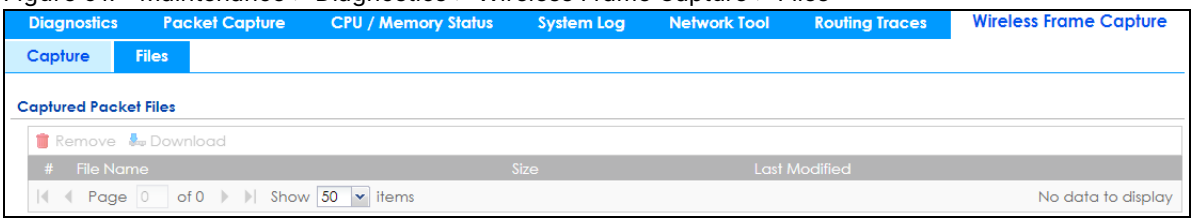
Table 329 Maintenance > Diagnostics > Wireless Frame Capture > Capture (continued)

LABEL	DESCRIPTION
File Prefix	Specify text to add to the front of the file name in order to help you identify frame capture files. You can modify the prefix to also create new frame capture files each time you perform a frame capture operation. Doing this does no overwrite existing frame capture files. The file format is: [file prefix].cap. For example, “monitor.cap”.
Capture	Click this button to have the Zyxel Device capture frames according to the settings configured in this screen. You can configure the Zyxel Device while a frame capture is in progress although you cannot modify the frame capture settings. The Zyxel Device’s throughput or performance may be affected while a frame capture is in progress. After the Zyxel Device finishes the capture it saves a combined capture file for all APs. The total number of frame capture files that you can save depends on the file sizes and the available flash storage space. Once the flash storage space is full, adding more frame captures will fail.
Stop	Click this button to stop a currently running frame capture and generate a combined capture file for all APs.
Reset	Click this button to return the screen to its last-saved settings.

35.8.1 The Wireless Frame Capture Files Screen

Click Maintenance > Diagnostics > Wireless Frame Capture > Files to open this screen. This screen lists the files of wireless frame captures the Zyxel Device has performed. You can download the files to your computer where you can study them using a packet analyzer (also known as a network or protocol analyzer) such as Wireshark.

Figure 617 Maintenance > Diagnostics > Wireless Frame Capture > Files



The following table describes the labels in this screen.

Table 330 Maintenance > Diagnostics > Wireless Frame Capture > Files

LABEL	DESCRIPTION
Remove	Select files and click Remove to delete them from the Zyxel Device. Use the [Shift] and/or [Ctrl] key to select multiple files. A pop-up window asks you to confirm that you want to delete.
Download	Click a file to select it and click Download to save it to your computer.
#	This column displays the number for each packet capture file entry. The total number of packet capture files that you can save depends on the file sizes and the available flash storage space.
File Name	This column displays the label that identifies the file. The file name format is interface name-file suffix.cap.
Size	This column displays the size (in bytes) of a configuration file.
Last Modified	This column displays the date and time that the individual files were saved.

CHAPTER 36
Packet Flow Explore

36.1 Overview

Use this to get a clear picture on how the Zyxel Device determines where to forward a packet and how to change the source IP address of the packet according to your current settings. This function provides you a summary of all your routing and SNAT settings and helps troubleshoot any related problems.

36.1.1 What You Can Do in this Chapter

- Use the Routing Status screen (see Section 36.2 on page 893) to view the overall routing flow and each routing function's settings.
- Use the SNAT Status screen (see Section 36.3 on page 897) to view the overall source IP address conversion (SNAT) flow and each SNAT function's settings.

36.2 Routing Status

The Routing Status screen allows you to view the current routing flow and quickly link to specific routing settings. Click a function box in the Routing Flow section, the related routes (activated) will display in the Routing Table section. To access this screen, click Maintenance > Packet Flow Explore > Routing Status.

The order of the routing flow may vary depending on whether you:

- Select use policy route to override direct route in the CONFIGURATION > Network > Routing > Policy Route screen.
- Use policy routes to control 1-1 NAT by using the `policy control-virtual-server-rules activate` command.
- Select use policy routes to control dynamic IPSec rules in the CONFIGURATION > VPN > IPSec VPN > VPN Connection screen.

Note: Once a packet matches the criteria of a routing rule, the Zyxel Device takes the corresponding action and does not perform any further flow checking.

Figure 618 Maintenance > Packet Flow Explore > Routing Status (Direct Route)

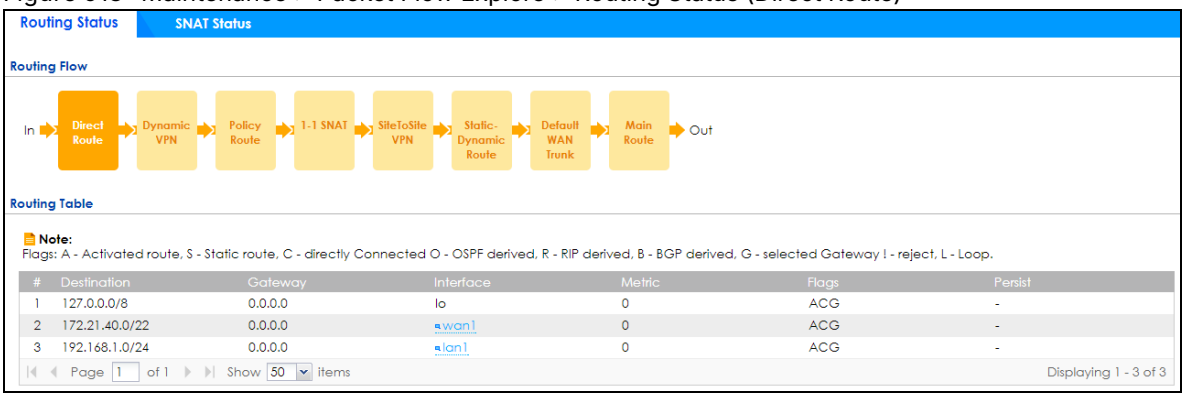


Figure 619 Maintenance > Packet Flow Explore > Routing Status (Dynamic VPN)

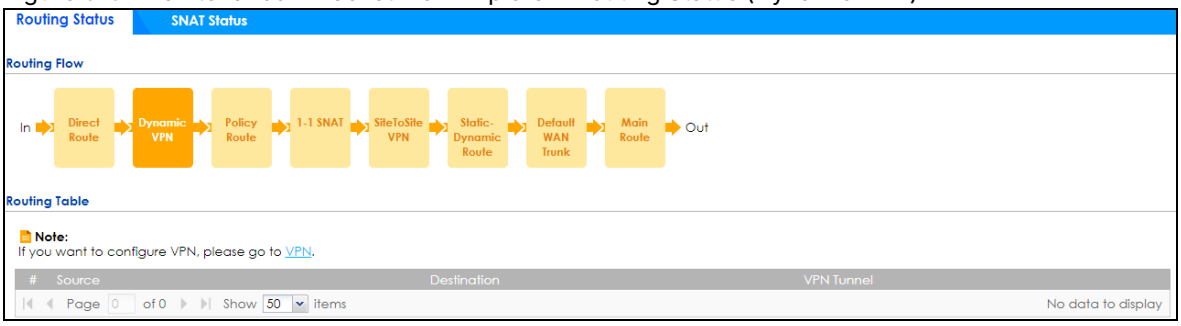


Figure 620 Maintenance > Packet Flow Explore > Routing Status (Policy Route)

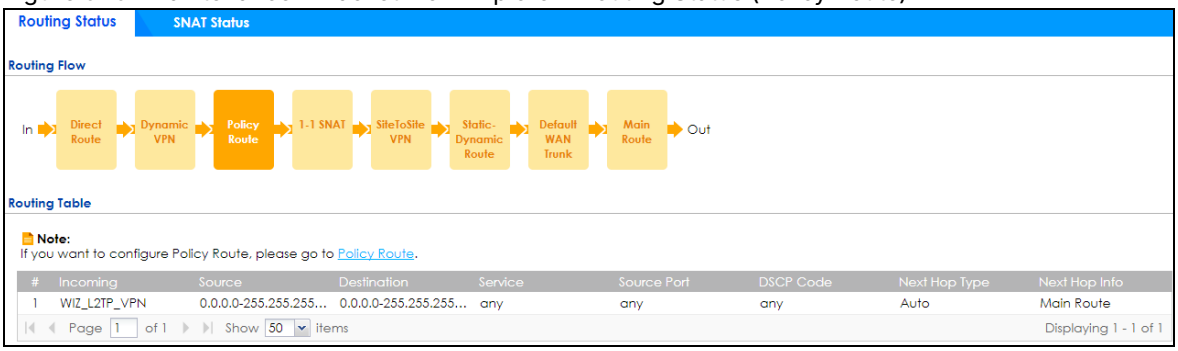


Figure 621 Maintenance > Packet Flow Explore > Routing Status (1-1 SNAT)

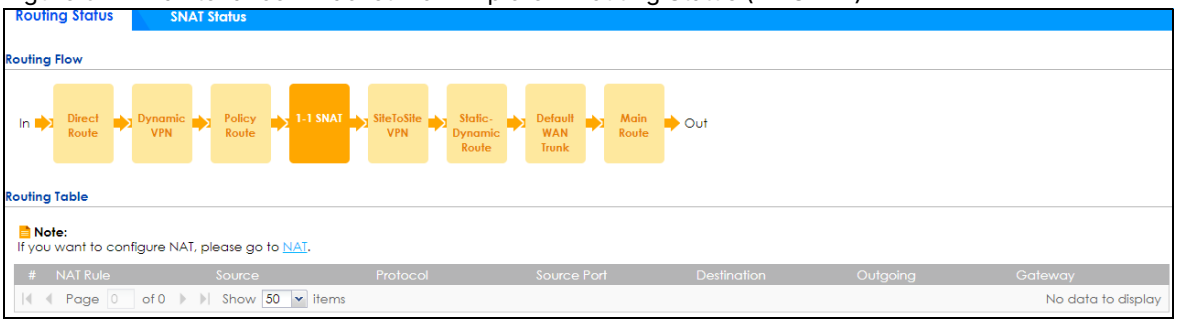


Figure 622 Maintenance > Packet Flow Explore > Routing Status (SiteToSite VPN)

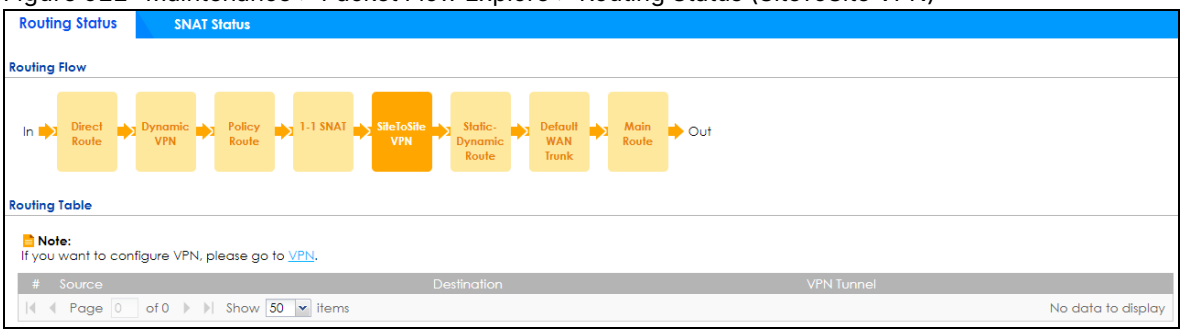


Figure 623 Maintenance > Packet Flow Explore > Routing Status (Static-Dynamic Route)

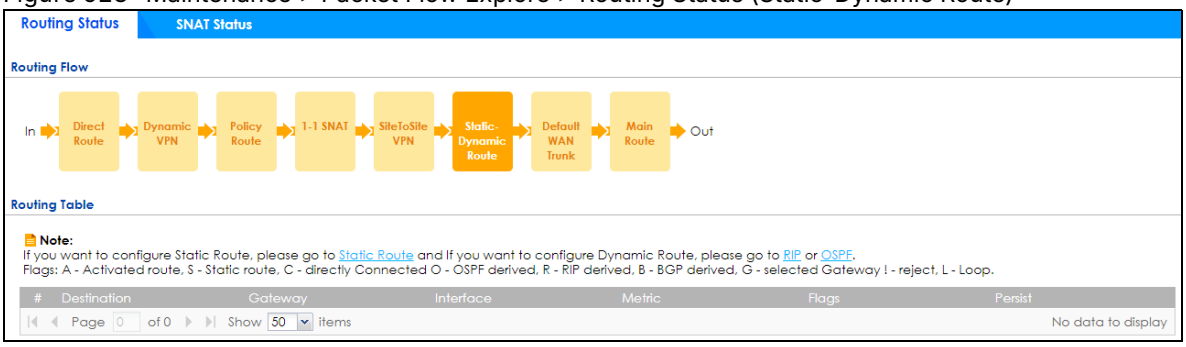


Figure 624 Maintenance > Packet Flow Explore > Routing Status (Default WAN Trunk)

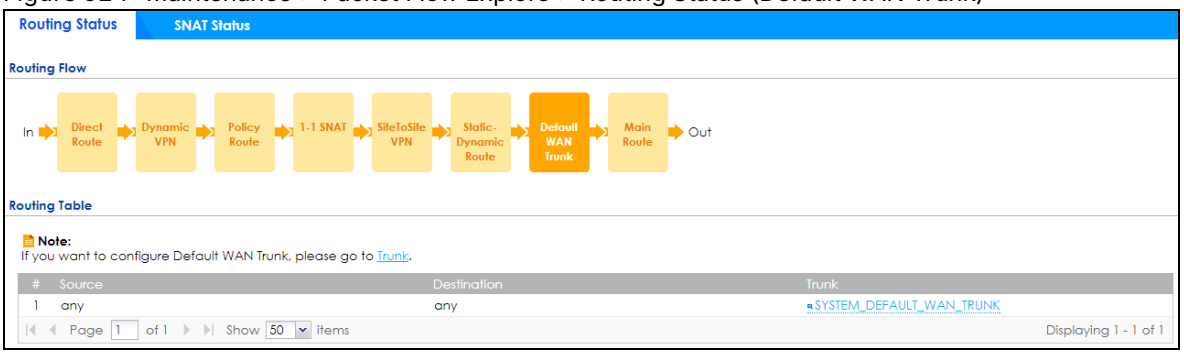
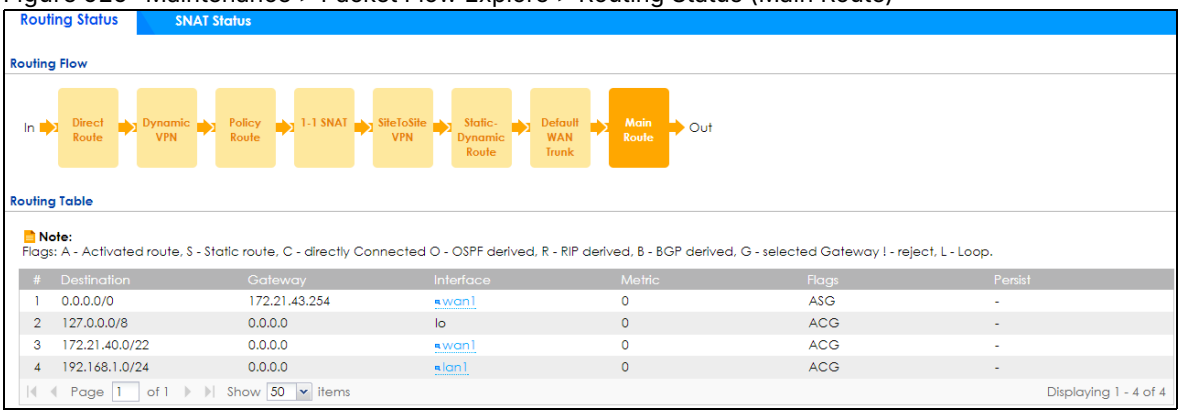


Figure 625 Maintenance > Packet Flow Explore > Routing Status (Main Route)



The following table describes the labels in this screen.

Table 331 Maintenance > Packet Flow Explore > Routing Status

LABEL	DESCRIPTION
Routing Flow	This section shows you the flow of how the Zyxel Device determines where to route a packet. Click a function box to display the related settings in the Routing Table section.
Routing Table	This section shows the corresponding settings according to the function box you click in the Routing Flow section.
The following fields are available if you click Direct Route, Static-Dynamic Route, or Main Route in the Routing Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
Destination	This is the destination IP address of a route.
Gateway	This is the IP address of the next-hop gateway or the interface through which the traffic is routed.
Interface	This is the name of an interface associated with the route.
Metric	This is the route's priority among the displayed routes.
Flags	This indicates additional information for the route. The possible flags are: • A - this route is currently activated. • S - this is a static route. • C - this is a direct connected route. • O - this is a dynamic route learned through OSPF. • R - this is a dynamic route learned through RIP. • B - this is a dynamic route learned through BGP. • G - the route is to a gateway (router) in the same network. • ! - this is a route which forces a route lookup to fail. • B - this is a route which discards packets. • L - this is a recursive route.
Persist	This is the remaining time of a dynamically learned route. The Zyxel Device removes the route after this time period is counted down to zero.
The following fields are available if you click Policy Route in the Routing Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
Incoming	This is the interface on which the packets are received.
Source	This is the source IP address(es) from which the packets are sent.
Destination	This is the destination IP address(es) to which the packets are transmitted.
Service	This is the name of the service object. any means all services.
Source Port	This is the source port(s) from which the packets are sent.
DSCP Code	This is the DSCP value of incoming packets to which this policy route applies. See Section 12.2 on page 389 for more information.
Next Hop Type	This is the type of the next hop to which packets are directed.
Next Hop Info	• This is the main route if the next hop type is Auto. • This is the interface name and gateway IP address if the next hop type is Interface /GW. • This is the tunnel name if the next hop type is VPN Tunnel. • This is the trunk name if the next hop type is Trunk.
The following fields are available if you click 1-1 SNAT in the Routing Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
NAT Rule	This is the name of an activated 1:1 or Many 1:1 NAT rule in the NAT table.
Source	This is the external source IP address(es).
Protocol	This is the transport layer protocol.
Source Port	This is the source port number.

Table 331 Maintenance > Packet Flow Explore > Routing Status (continued)

LABEL	DESCRIPTION
Destination	This is the external destination IP address(es).
Outgoing	This is the outgoing interface that the SNAT rule uses to transmit packets.
Gateway	This is the IP address of the gateway in the same network of the outgoing interface.
The following fields are available if you click Dynamic VPN or SiteToSite VPN in the Routing Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
Source	This is the IP address(es) of the local VPN network.
Destination	This is the IP address(es) for the remote VPN network.
VPN Tunnel	This is the name of the VPN tunnel.
The following fields are available if you click Default WAN Trunk in the Routing Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
Source	This is the source IP address(es) from which the packets are sent. any means any IP address.
Destination	This is the destination IP address(es) to which the packets are transmitted. any means any IP address.
Trunk	This is the name of the WAN trunk through which the matched packets are transmitted.

36.3 The SNAT Status Screen

The SNAT Status screen allows you to view and quickly link to specific source NAT (SNAT) settings. Click a function box in the SNAT Flow section, the related SNAT rules (activated) will display in the SNAT Table section. To access this screen, click Maintenance > Packet Flow Explore > SNAT Status.

The order of the SNAT flow may vary depending on whether you:

- select use default SNAT in the CONFIGURATION > Network > Interface > Trunk screen.
- use policy routes to control 1-1 NAT by using the `policy control-virtual-server-rules activate` command.

Note: Once a packet matches the criteria of an SNAT rule, the Zyxel Device takes the corresponding action and does not perform any further flow checking.

Figure 626 Maintenance > Packet Flow Explore > SNAT Status (Policy Route SNAT)

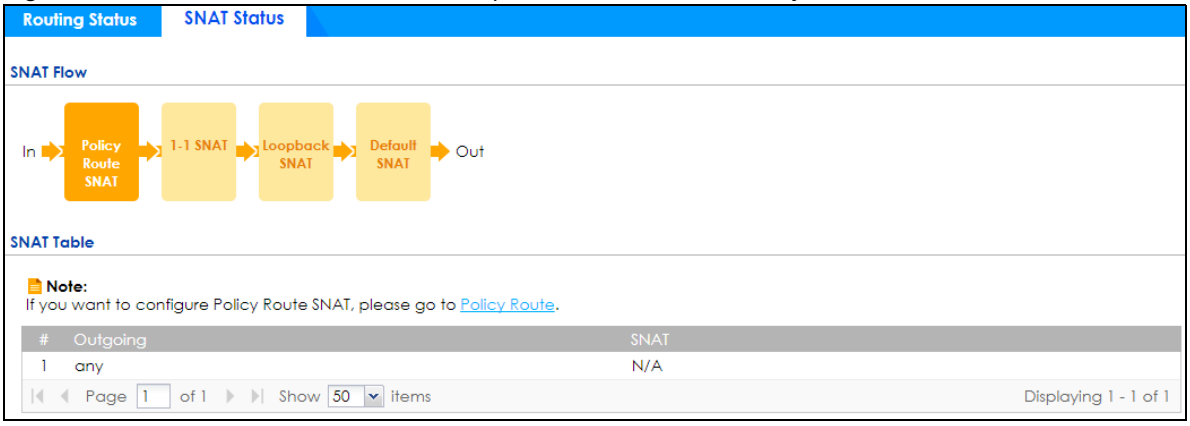


Figure 627 Maintenance > Packet Flow Explore > SNAT Status (1-1 SNAT)

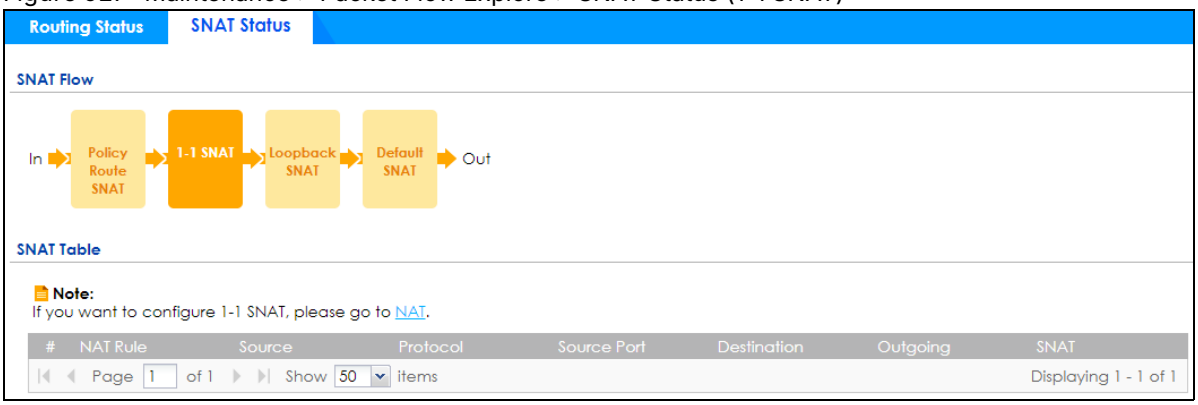


Figure 628 Maintenance > Packet Flow Explore > SNAT Status (Loopback SNAT)

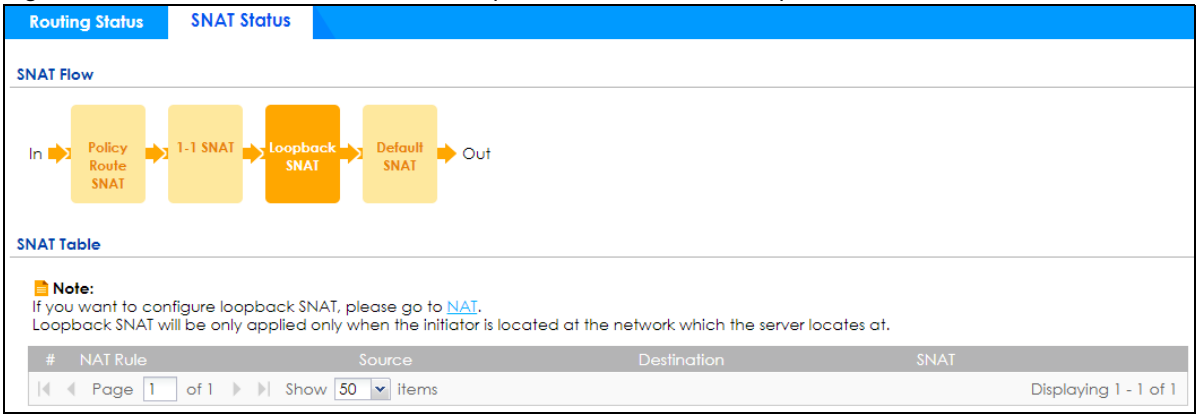
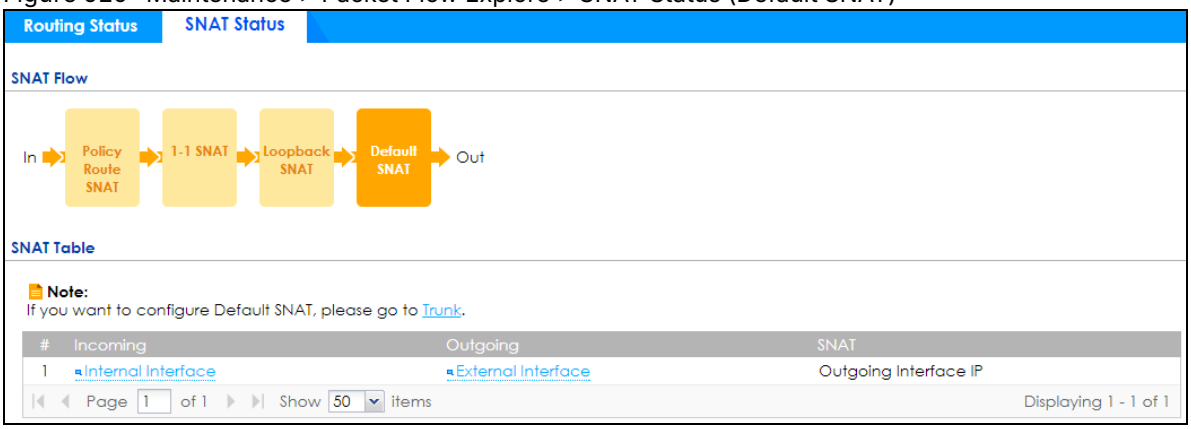


Figure 629 Maintenance > Packet Flow Explore > SNAT Status (Default SNAT)



The following table describes the labels in this screen.

Table 332 Maintenance > Packet Flow Explore > SNAT Status

LABEL	DESCRIPTION
SNAT Flow	This section shows you the flow of how the Zyxel Device changes the source IP address for a packet according to the rules you have configured in the Zyxel Device. Click a function box to display the related settings in the SNAT Table section.
SNAT Table	The table fields in this section vary depending on the function box you select in the SNAT Flow section.
The following fields are available if you click Policy Route SNAT in the SNAT Flow section.	
#	This field is a sequential value, and it is not associated with any entry.

Table 332 Maintenance > Packet Flow Explore > SNAT Status (continued)

LABEL	DESCRIPTION
Outgoing	This is the outgoing interface that the route uses to transmit packets.
SNAT	This is the source IP address(es) that the SNAT rule uses finally.
The following fields are available if you click 1-1 SNAT in the SNAT Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
NAT Rule	This is the name of an activated NAT rule which uses SNAT.
Source	This is the external source IP address(es).
Protocol	This is the transport layer protocol.
Source Port	This is the source port number.
Destination	This is the external destination IP address(es).
Outgoing	This is the outgoing interface that the SNAT rule uses to transmit packets.
SNAT	This is the source IP address(es) that the SNAT rule uses finally.
The following fields are available if you click Loopback SNAT in the SNAT Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
NAT Rule	This is the name of an activated NAT rule which uses SNAT and enables NAT loopback.
Source	This is the original source IP address(es). any means any IP address.
Destination	This is the original destination IP address(es). any means any IP address.
SNAT	This indicates which source IP address the SNAT rule uses finally. For example, Outgoing Interface IP means that the Zyxel Device uses the IP address of the outgoing interface as the source IP address for the matched packets it sends out through this rule.
The following fields are available if you click Default SNAT in the SNAT Flow section.	
#	This field is a sequential value, and it is not associated with any entry.
Incoming	This indicates internal interface(s) on which the packets are received.
Outgoing	This indicates external interface(s) from which the packets are transmitted.
SNAT	This indicates which source IP address the SNAT rule uses finally. For example, Outgoing Interface IP means that the Zyxel Device uses the IP address of the outgoing interface as the source IP address for the matched packets it sends out through this rule.

Chapter 37 Shutdown

37.1 Overview

Use this to shutdown the device in preparation for disconnecting the power.

Always use the Maintenance > Shutdown > Shutdown screen 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.

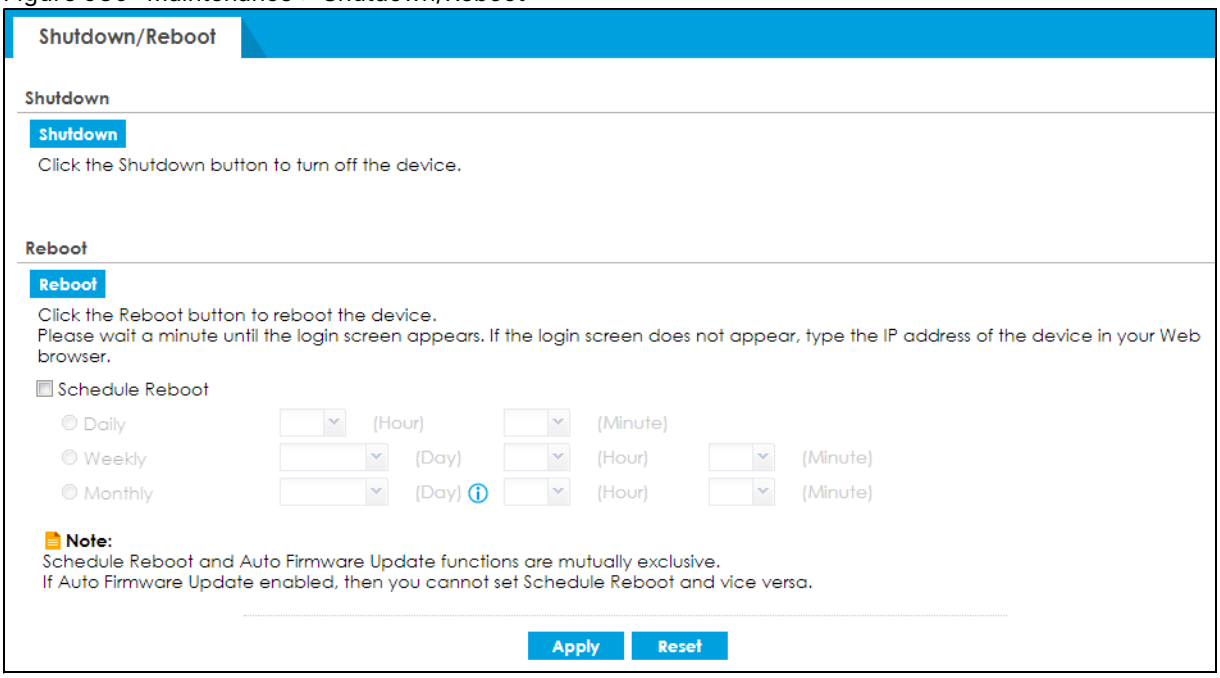
37.1.1 What You Need To Know

Shutdown writes all cached data to the local storage and stops the system processes.

37.2 The Shutdown / Reboot Screen

To access this screen, click Maintenance > Shutdown/Reboot.

Figure 630 Maintenance > Shutdown/Reboot



The following table describes the labels in this screen.

Table 333 Maintenance > Shutdown/Reboot

LABEL	DESCRIPTION
Shutdown	Click the Shutdown button to shut down the Zyxel Device. Wait for the device to shut down before you manually turn off or remove the power. It does not turn off the power.
Reboot	Click Reboot to reboot the Zyxel Device immediately without turning the power off.
Schedule Reboot	Select this checkbox to schedule a periodic reboot of the Zyxel Device. You should select a time when your network is not busy for minimal interruption. Note: You cannot enable Auto Update in File Manager > Firmware Management and Schedule Reboot in Maintenance > Shutdown-Reboot at the same time.
Daily	Set the Zyxel Device to reboot every day at the specified time. The time format is the 24 hour clock, so '0' means midnight for example.
Weekly	Set the Zyxel Device to reboot once a week on the day and at the time specified.
Monthly	Set the Zyxel Device to reboot once a month on the specified day, at the a specified hour and minute. If the date you select is greater than the number of days in a month, the Zyxel Device automatically reboots on the last day of the month. For example, if you select 31 and the month is February, the Zyxel Device reboots on day 28 or 29.
Apply	Click Apply to save your changes back to the Zyxel Device.
Reset	Click Reset to return the screen to its last-saved settings.

You can also use the CLI command `shutdown` to close down the Zyxel Device.

Part III
Appendices and Troubleshooting

CHAPTER 38
Troubleshooting

This chapter offers some suggestions to solve problems you might encounter.

- You can also refer to the logs (see Section 8.27 on page 263).
- For the order in which the Zyxel Device applies its features and checks, see Packet Flow Explore.

None of the LEDs turn on.

Make sure that you have the power cord connected to the Zyxel Device and plugged in to an appropriate power source. Make sure you have the Zyxel Device turned on. Check all cable connections.

If the LEDs still do not turn on, you may have a hardware problem. In this case, you should contact your local vendor.

I cannot finish Nebula registration because I did not connect a computer to the Zyxel Device LAN.

Follow the steps if you did not connect a computer to the LAN port of the Zyxel Device.

1. Connect a USB disk drive in FAT32 format to a USB port on your computer.
2. Go to your mailbox and find the email from Nebula. Save the JSON file in the email attachment to the root folder of the USB drive.
3. Connect the USB drive to the Zyxel Device. The SYS LED will blink. Please wait until the SYS LED is solid green again. The Nebula administrator should now check if the Zyxel Device is online indicating Nebula registration has succeeded.

Cannot access the Zyxel Device from the LAN.

- Check the cable connection between the Zyxel Device and your computer or switch.
- Ping the Zyxel Device from a LAN computer. Make sure your computer's Ethernet card is installed and functioning properly. Also make sure that its IP address is in the same subnet as the Zyxel Device's.
- In the computer, click Start, (All) Programs, Accessories and then Command Prompt. In the Command Prompt window, type "ping" followed by the Zyxel Device's LAN IP address (192.168.1.1 is the default) and then press [ENTER]. The Zyxel Device should reply.

- If you've forgotten the Zyxel Device's password, use the RESET button. Press the button in for about 5 seconds (or until the SYS LED starts to blink), then release it. It returns the Zyxel Device to the factory defaults (password is 1234, LAN IP address 192.168.1.1, etc).
- If you've forgotten the Zyxel Device's IP address, you can use the commands through the CONSOLE port to check it. Connect your computer to the CONSOLE port using a console cable. Your computer should have a terminal emulation communications program (such as Hyper Terminal) set to VT100 terminal emulation, no parity, 8 data bits, 1 stop bit, no flow control and 115200 bps port speed.

I cannot access the Internet.

- Check the Zyxel Device's connection to the Ethernet jack with Internet access. Make sure the Internet gateway device (such as a DSL modem) is working properly.
- Check the WAN interface's status in the Dashboard. Use the installation setup wizard again and make sure that you enter the correct settings. Use the same case as provided by your ISP.

I keep getting logged out of the Zyxel Device.

- Make sure the Internet connection is stable. Check the Zyxel Device's connection to the Ethernet jack with Internet access. Make sure the Internet gateway device (such as a DSL modem) is working properly.
- You will be automatically logged out after the configured Reauthentication Time. To change this:

1. Go to Configuration > User/Group > User, select your account and click Edit.
2. Select Use Manual Settings from the Authentication Timeout Settings.
3. Set a longer duration for the Reauthentication Time.

The content filter category service is not working.

- Make sure your Zyxel Device has the content filter category service registered and that the license is not expired. Purchase a new license if the license is expired.
- Make sure your Zyxel Device is connected to the Internet.
- Make sure you select Enable Content Filter Category Service when you add a filter profile in the Configuration > Security Service > Content Filter > Profile > Add or Edit screen.
- Block QUIC UDP ports 80 and 443. QUIC (Quick UDP Internet Connections) is a UDP protocol used by Google Chrome and Chromium web browsers.

I configured security settings but the Zyxel Device is not applying them for certain interfaces.

Many security settings are usually applied to zones. Make sure you assign the interfaces to the appropriate zones. When you create an interface, there is no security applied on it until you assign it to a zone.

The Zyxel Device is not applying the custom policy route I configured.

The Zyxel Device checks the policy routes in the order that they are listed. So make sure that your custom policy route comes before any other routes that the traffic would also match.

The Zyxel Device is not applying the custom security policy I configured.

The Zyxel Device checks the security policies in the order that they are listed. So make sure that your custom security policy comes before any other rules that the traffic would also match.

I cannot enter the interface name I want.

- The format of interface names other than the Ethernet interface names is very strict. Each name consists of 2-4 letters (interface type), followed by a number (x, limited by the maximum number of each type of interface). For example, VLAN interfaces are vlan0, vlan1, vlan2,...; and so on.
- The names of virtual interfaces are derived from the interfaces on which they are created. For example, virtual interfaces created on Ethernet interface wan1 are called wan1:1, wan1:2, and so on. Virtual interfaces created on VLAN interface vlan2 are called vlan2:1, vlan2:2, and so on. You cannot specify the number after the colon(:) in the Web Configurator; it is a sequential number. You can specify the number after the colon if you use the CLI to set up a virtual interface.

I cannot set up a PPP interface, virtual Ethernet interface or virtual VLAN interface on an Ethernet interface.

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

My rules and settings that apply to a particular interface no longer work.

The interface's IP address may have changed. To avoid this, create an IP address object based on the interface. This way the 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 LAN1's IP address, the Zyxel Device automatically updates the corresponding interface-based, LAN1 subnet address object.

I cannot set up a PPP interface.

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

The data rates through my cellular connection are no-where near the rates I expected.

The actual cellular data rate you obtain varies depending on the cellular device you use, the signal strength to the service provider's base station, and so on.

I created a cellular interface but cannot connect through it.

- Make sure you have a compatible mobile broadband device installed or connected. See www.zyxel.com for details.
- Make sure you have the cellular interface enabled.
- Make sure the cellular interface has the correct user name, password, and PIN code configured with the correct casing.
- If the Zyxel Device has multiple WAN interfaces, make sure their IP addresses are on different subnets.

Hackers have accessed my WEP-encrypted wireless LAN.

WEP is extremely insecure. Its encryption can be broken by an attacker, using widely-available software. It is strongly recommended that you use a more effective security mechanism. Use the strongest security mechanism that all the wireless devices in your network support. WPA2 or WPA2-PSK is recommended.

The wireless security is not following the re-authentication timer setting I specified.

If a RADIUS server authenticates wireless stations, the re-authentication timer on the RADIUS server has priority. Change the RADIUS server's configuration if you need to use a different re-authentication timer setting.

I cannot configure a particular VLAN interface on top of an Ethernet interface even though I have it configured it on top of another Ethernet interface.

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

The Zyxel Device is not applying an interface's configured ingress bandwidth limit.

At the time of writing, the Zyxel Device does not support ingress bandwidth management.

The Zyxel Device is not scanning some zipped files.

The Zyxel Device cannot unzip password protected ZIP files or a ZIP file within another ZIP file. There are also limits to the number of ZIP files that the Zyxel Device can concurrently unzip.

The Zyxel Device is deleting some zipped files.

The Zyxel Device cannot unzip password protected ZIP files or a ZIP file within another ZIP file. There are also limits to the number of ZIP files that the Zyxel Device can concurrently unzip.

The Zyxel Device's performance seems slower after configuring ADP.

Depending on your network topology and traffic load, applying an anomaly profile to each and every packet direction may affect the Zyxel Device's performance.

My Collaborative Detection& Response (CDR) is not working.

CDR signature are a subset of Web Filtering (ing), Anti-Malware (Anti-Virus) and IPS (IDP) license signatures. No checking for malicious traffic is done if these licenses have expired or are note active.

Make sure these licenses are activated and not expired. Purchase new licenses if the license are expired.

I cannot block traffic from an AP using CDR.

The Zyxel Device can only blocked traffic from Nebula-managed APs in your network using CDR.

Make sure:

- The AP is managed by the Zyxel Device.
- The AP must be in the Zyxel Device's supported list

The quarantined/blocked clients are released before I want them to.

Check if your CDR license is expired or disabled. Check if the Containment Period is expired in Configuration > Security Service > Collaborative Detection& Response screen.

The Zyxel Device routes and applies SNAT for traffic from some interfaces but not from others.

The Zyxel Device automatically uses SNAT for traffic it routes from internal interfaces to external interfaces. For example LAN to WAN traffic. You must manually configure a policy route to add routing and SNAT settings for an interface with the Interface Type set to General. You can also configure a policy route to override the default routing and SNAT behavior for an interface with the Interface Type set to Internal or External.

I cannot get Dynamic DNS to work.

- You must have a public WAN IP address to use Dynamic DNS.
- Make sure you recorded your DDNS account's user name, password, and domain name and have entered them properly in the Zyxel Device.
- You may need to configure the DDNS entry's IP Address setting to Auto if the interface has a dynamic IP address or there are one or more NAT routers between the Zyxel Device and the DDNS server.
- The Zyxel Device may not determine the proper IP address if there is an HTTP proxy server between the Zyxel Device and the DDNS server.

I cannot create a second HTTP redirect rule for an incoming interface.

You can configure up to one HTTP redirect rule for each (incoming) interface.

The Zyxel Device keeps resetting the connection.

If an alternate gateway on the LAN has an IP address in the same subnet as the Zyxel Device's LAN IP address, return traffic may not go through the Zyxel Device. This is called an asymmetrical or "triangle" route. This causes the Zyxel Device to reset the connection, as the connection has not been acknowledged.

You can set the Zyxel Device's security policy to permit the use of asymmetrical route topology on the network (so it does not reset the connection) although this is not recommended since allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the Zyxel Device. A better solution is to use virtual interfaces to put the Zyxel Device and the backup gateway on

separate subnets. See Asymmetrical Routes on page 572 and the chapter about interfaces for more information.

I cannot set up an IPSec VPN tunnel to another device.

If the IPSec tunnel does not build properly, the problem is likely a configuration error at one of the IPSec routers. Log into both Zyxel IPSec routers and check the settings in each field methodically and slowly. Make sure both the Zyxel Device and remote IPSec router have the same security settings for the VPN tunnel. It may help to display the settings for both routers side-by-side.

Here are some general suggestions. See also Chapter 21 on page 473.

- The system log can often help to identify a configuration problem.
- If you enable NAT traversal, the remote IPSec device must also have NAT traversal enabled.
- The Zyxel Device and remote IPSec router must use the same authentication method to establish the IKE SA.
- Both routers must use the same negotiation mode.
- Both routers must use the same encryption algorithm, authentication algorithm, and DH key group.
- When using pre-shared keys, the Zyxel Device and the remote IPSec router must use the same pre-shared key.
- The Zyxel Device's local and peer ID type and content must match the remote IPSec router's peer and local ID type and content, respectively.
- The Zyxel Device and remote IPSec router must use the same active protocol.
- The Zyxel Device and remote IPSec router must use the same encapsulation.
- The Zyxel Device and remote IPSec router must use the same SPI.
- If the sites are/were previously connected using a leased line or ISDN router, physically disconnect these devices from the network before testing your new VPN connection. The old route may have been learned by RIP and would take priority over the new VPN connection.
- To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other. Before doing so, ensure that both computers have Internet access (through the IPSec routers).
- It is also helpful to have a way to look at the packets that are being sent and received by the Zyxel Device and remote IPSec router (for example, by using a packet sniffer).

Check the configuration for the following Zyxel Device features.

- The Zyxel Device does not put IPSec SAs in the routing table. You must create a policy route for each VPN tunnel. See Routing.
- Make sure the To-Zyxel Device security policies allow IPSec VPN traffic to the Zyxel Device. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.
- The Zyxel Device supports UDP port 500 and UDP port 4500 for NAT traversal. If you enable this, make sure the To-Zyxel Device security policies allow UDP port 4500 too.
- Make sure regular security policies allow traffic between the VPN tunnel and the rest of the network. Regular security policies check packets the Zyxel Device sends before the Zyxel Device encrypts them and check packets the Zyxel Device receives after the Zyxel Device decrypts them. This depends on the zone to which you assign the VPN tunnel and the zone from which and to which traffic may be routed.

- If you set up a VPN tunnel across the Internet, make sure your ISP supports AH or ESP (whichever you are using).
- If you have the Zyxel Device and remote IPSec router use certificates to authenticate each other, You must set up the certificates for the Zyxel Device and remote IPSec router first and make sure they trust each other's certificates. If the Zyxel Device's certificate is self-signed, import it into the remote IPSec router. If it is signed by a CA, make sure the remote IPSec router trusts that CA. The Zyxel Device uses one of its Trusted Certificates to authenticate the remote IPSec router's certificate. The trusted certificate can be the remote IPSec router's self-signed certificate or that of a trusted CA that signed the remote IPSec router's certificate.
- Multiple SAs connecting through a secure gateway must have the same negotiation mode.

The VPN connection is up but VPN traffic cannot be transmitted through the VPN tunnel.

If you have the Configuration > VPN > IPSec VPN > VPN Connection screen's Use Policy Route to control dynamic IPSec rules option enabled, check the routing policies to see if they are sending traffic elsewhere instead of through the VPN tunnels.

I uploaded a logo to show in the SSL VPN user screens but it does not display properly.

The logo graphic must be GIF, JPG, or PNG format. The graphic should use a resolution of 103 x 29 pixels to avoid distortion when displayed. The Zyxel Device automatically resizes a graphic of a different resolution to 103 x 29 pixels. The file size must be 100 kilobytes or less. Transparent background is recommended.

I logged into the SSL VPN but cannot see some of the resource links.

Available resource links vary depending on the SSL application object's configuration.

I cannot set up a Remote AP VPN tunnel.

Check the settings in each field methodically and slowly.

Make sure:

- Your AP supports remote AP VPN. Check the AP Role Capability in the Mgnt. AP List screen.
- The Zyxel Device has 5.00 or later firmware and the managed AP has 6.20 or later firmware.
- Your Secure WiFi license is activated and not expired. Purchase a new license if the license is expired.
- You've selected the Remote AP checkbox in Configuration> Wireless> AP Management on the AP you want to set up as a remote AP.
- You've configured your AP using a Secure Tunnel SSID profile.

I changed the LAN IP address and can no longer access the Internet.

The Zyxel Device automatically updates address objects based on an interface's IP address, subnet, or gateway if the interface's IP address settings change. However, you need to manually edit any address objects for your LAN that are not based on the interface.

I configured policy routes to manage the bandwidth of TCP and UDP traffic but the bandwidth management is not being applied properly.

It is recommended to use application patrol instead of policy routes to manage the bandwidth of TCP and UDP traffic.

I cannot get the RADIUS server to authenticate the Zyxel Device's default admin account.

The default admin account is always authenticated locally, regardless of the authentication method setting.

The Zyxel Device fails to authentication the ext-user user accounts I configured.

An external server such as AD, LDAP or RADIUS must authenticate the ext-user accounts. If the Zyxel Device tries to use the local database to authenticate an ext-user, the authentication attempt will always fail. (This is related to AAA servers and authentication methods, which are discussed in other chapters in this guide.)

I cannot add the admin users to a user group with access users.

You cannot put access users and admin users in the same user group.

I cannot add the default admin account to a user group.

You cannot put the default admin account into any user group.

My two-factor authentication is not working.

Check that match the specifications and limitation in the following list:

- Ext-users (authenticated by external servers) are not supported.
- You must setup Google Authenticator on their mobile device before you can successfully authenticate with the Zyxel Device.
- Click or tap the authorization link in the SMS or email within the valid time. You can extend the time in Configuration > Object > Auth. Method > Two-factor Authentication > VPN Access.

I cannot receive the authorization SMS or email for two factor authentication.

- Make sure the mobile telephone number or email address of the user in the Active Directory, RADIUS Server or local Zyxel Device database is configured correctly.
- Email-to-SMS cloud system authentication fails. Make sure that SMS is enabled and credentials are correct in System > Notification > SMS.
- Mail server authentication fails. Make sure the System> Notification > Mail Server settings are correct if you’re using email for authentication.

I get a Google Authenticator verification error.

- Check that you enter the right verification code. The verification code should be 6 digits.
- You must enter the code within the time displayed in Google Authenticator.
- You’ve exceeded the maximum verification code failed attempts.

The schedule I configured is not being applied at the configured times.

Make sure the Zyxel Device’s current date and time are correct.

I cannot get a certificate to import into the Zyxel Device.

1. For My Certificates, you can import a certificate that matches a corresponding certification request that was generated by the Zyxel Device. You can also import a certificate in PKCS#12 format, including the certificate’s public and private keys.
2. You must remove any spaces from the certificate’s filename before you can import the certificate.
3. Any certificate that you want to import has to be in one of these file formats:
   - Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
   - PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.

- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The Zyxel Device currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.
- Binary PKCS#12: This is a format for transferring public key and private key certificates.The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the Zyxel Device.

Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

I cannot access the Zyxel Device from a computer connected to the Internet.

Check the service control rules and to-Zyxel Device security policies.

I uploaded a logo to display on the upper left corner of the Web Configurator login screen and access page but it does not display properly.

Make sure the logo file is a GIF, JPG, or PNG of 100 kilobytes or less.

I uploaded a logo to use as the screen or window background but it does not display properly.

Make sure the logo file is a GIF, JPG, or PNG of 100 kilobytes or less.

The Zyxel Device's traffic throughput rate decreased after I started collecting traffic statistics.

Data collection may decrease the Zyxel Device's traffic throughput rate.

I can only see newer logs. Older logs are missing.

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

The commands in my configuration file or shell script are not working properly.

- In a configuration file or shell script, use “#” or “!” as the first character of a command line to have the Zyxel Device treat the line as a comment.
- Your configuration files or shell scripts can use “exit” or a command line consisting of a single “!” to have the Zyxel Device exit sub command mode.
- Include `write` commands in your scripts. Otherwise the changes will be lost when the Zyxel Device restarts. You could use multiple `write` commands in a long script.

Note: “exit” or “!'” must follow sub commands if it is to make the Zyxel Device exit sub command mode.

See Chapter 34 on page 856 for more on configuration files and shell scripts.

I cannot get the firmware uploaded using the commands.

The Web Configurator is the recommended method for uploading firmware. You only need to use the command line interface if you need to recover the firmware. See the CLI Reference Guide for how to determine if you need to recover the firmware and how to recover it.

My packet capture captured less than I wanted or failed.

The packet capture screen’s File Size sets a maximum size limit for the total combined size of all the capture files on the Zyxel Device, including any existing capture files and any new capture files you generate. If you have existing capture files you may need to set this size larger or delete existing capture files.

The Zyxel Device stops the capture and generates the capture file when either the capture files reach the File Size or the time period specified in the Duration field expires.

My earlier packet capture files are missing.

New capture files overwrite existing files of the same name. Change the File Suffix field’s setting to avoid this.

The clients’ information I collected using device insight is not correct.

Make sure your clients are in the same IP subnet in the LAN/VLAN/DMZ networks behind the Zyxel Device. Information from clients that are in different IP subnets in the LAN/VLAN/DMZ networks might not be collected correctly.

To report on clients that are wrongly identified, go to Monitor > Network Status > Device Insight > Feedback.

I cannot remove a client in Monitor > Device Insight.

Clients that are blocked cannot be removed. Please make sure to unblock the client you want to remove first.

I cannot block clients using device insight profiles.

Make sure you select the correct device types and operating systems in device insight profiles.

Make sure you've applied the device insight profiles to the right policy in Security Policy and set the action to deny.

I cannot set the upload bandwidth limit for IPSec VPN configuration provisioning.

Upload bandwidth limit is only available for Zyxel subscription-based SecuExtender IPSec VPN clients for Windows and macOS clients. Make sure the VPN clients are using SecuExtender with supported operating system versions. See Section 21.5 on page 497 for more information.

I cannot access the Zyxel Device from the WAN after I configure settings in Security Check for Web Interface.

If you change the default HTTPS SSL port (443), make sure to use the new port to access the Zyxel Device.

Make sure to access the Zyxel Device from the specified IP address or FQDNs you set.

Reset the Zyxel Device if none of the above works.

I cannot access the Zyxel Device from the SSL VPN port after I configure settings in Security Check for Web Interface.

If you change the default SSL VPN port (443), make sure to use the new port to access the Zyxel Device. Make sure to make the same change to SecuExtender.

Make sure to access the Zyxel Device from the specified regions you set.

Reset the Zyxel Device if none of the above works.

I cannot retrieve VPN rule settings from the Zyxel Device after I configure settings in Security Check for Web Interface.

If you change the default port that IPSec VPN clients use to retrieve VPN rule settings from the Zyxel Device, make sure to make the same change to the Zyxel IPSec VPN clients.

Reset the Zyxel Device if none of the above works.

Someone attempted to log into my Zyxel Device Web Configurator.

An attacker may attempt to log in through the Web Configurator using brute force or password guessing. Use the following ways reduce the risk of login attempts from unknown sources.

- Limit Access to the Zyxel Device: If you set the allowed IP address to any, the Security Check for Web Interface screen pops up when you log in, enable Restrict Device management from the WAN and configure access to allow only trusted IP addresses or FQDNs.
- Enable Two-Factor Authentication: With two-factor authentication enabled, users must first enter their username and password, and then click on a temporary link or enter a one-time password when logging in. See Section 30.3.4 on page 686 for more information on setup instructions.

How can I see who is currently logged in and the login history?

- See users who are currently logged in to the Zyxel Device from the Current User List on the Monitor > Network Status > Login Users screen.
- See the login history from the logs. Go to Monitor > View Log. Select User from the Category drop-down list. Click Search.

How can I log a user out of the Zyxel Device?

If you notice an unknown user logged into your Zyxel Device, or if you want to log out your own account from another device, follow the steps below:

1. Go to Monitor > Network Status > Login Users.
2. Select the user you want to log out and click Force Logout.

My Zyxel Device CPU usage is too high.

The Zyxel Device may receive too many HTTPS connection requests when Web Authentication is enabled. Do the following to reduce the number of HTTPS connection requests:

- Go to Configuration > Object > User/Group > Setting and select Limit the number of simultaneous logons for administration account. Set a number in Maximum number per administration account to limit the number of simultaneous logins for each admin.
- Go to Configuration > Web Authentication > Exceptional Services to select services you want users to access without logging in.

I cannot see my WAN settings in Mgmt. & Analytics > Nebula.

Make sure your Zyxel Device supports Native Mode or you've managed your Zyxel Device with Nebula before.

Make sure you can connect to Nebula with your current WAN settings. See Section 31.4.2 on page 775 for more information.

I've passed the Zyxel Device management to Nebula, but I cannot access Nebula.

You can no longer access the Zyxel Device through the WAN after you let Nebula manage your Zyxel Device.

Connect your computer to the Zyxel Device LAN port to access the local GUI with your support account for troubleshooting. See the ZyWALL Series Local GUI User's Guide for more information.

My USB storage device is not compatible with the Zyxel Device.

The USB device must use MBR mode (Master Boot Record). It cannot have multiple partitions (GUID Partition Table).

The Zyxel Device supports USB file systems FAT16, FAT32, EXT3, and EXT4. To change the file system of your USB storage device by formatting it, follow these steps:

1. Insert your USB storage device into the computer. Be sure to back up your files before formatting your USB storage device.
2. Open File Explorer, right-click on the USB storage device and select Format.
3. In the Format window, select the desired file system:

   FAT16 supports Windows, macOS, and Linux. It can store files up to 2 GB.

   FAT32 supports Windows, macOS, and Linux. It can store files up to 4 GB.

   EXT3 supports Linux. It can store files up to 2 TB.

   EXT4 supports Linux. It can store files up to 16 TB.
4. Click Start to begin the formatting process.

38.1 Resetting the Zyxel Device

If you cannot access the Zyxel Device by any method, try restarting it by turning the power off and then on again. If you still cannot access the Zyxel Device by any method or you forget the administrator password(s), you can reset the Zyxel Device to its factory-default settings. Any configuration files or shell scripts that you saved on the Zyxel Device should still be available afterwards.

Use the following procedure to reset the Zyxel Device to its factory-default settings. This overwrites the settings in the startup-config.conf file with the settings in the system-default.conf file.

Note: This procedure removes the current configuration.

1. Make sure the SYS LED is on and not blinking.
2. Press the RESET button and hold it until the SYS LED begins to blink. (This usually takes about five seconds.)
3. Release the RESET button, and wait for the Zyxel Device to restart.

   You should be able to access the Zyxel Device using the default settings.

38.2 Getting More Troubleshooting Help

Search for support information for your model at www.zyxel.com for more troubleshooting suggestions.

Appendix A
Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

See *http://www.zyxel.com/homepage.shtml* and also *http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml* for the latest information.

Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- Zyxel Communications Corporation
- http://www.zyxel.com

Asia

China

- Zyxel Communications (Shanghai) Corp.
  Zyxel Communications (Beijing) Corp.
  Zyxel Communications (Tianjin) Corp.
- http://www.zyxel.cn

India

- Zyxel Technology India Pvt Ltd
- http://www.zyxel.in

Kazakhstan

- Zyxel Kazakhstan
- http://www.zyxel.kz

Korea

- Zyxel Korea Corp.
- http://www.zyxel.kr

Malaysia

- Zyxel Malaysia Sdn Bhd.
- http://www.zyxel.com.my

Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

Philippines

- Zyxel Philippines
- http://www.zyxel.com.ph

Singapore

- Zyxel Singapore Pte Ltd.
- http://www.zyxel.com.sg

Taiwan

- Zyxel Communications Corporation
- https://www.zyxel.com/tw/zh/

Thailand

- Zyxel Thailand Co., Ltd
- http://www.zyxel.co.th

Vietnam

- Zyxel Communications Corporation-Vietnam Office
- http://www.zyxel.com/vn/vi

Europe

Austria

- Zyxel Deutschland GmbH
- http://www.zyxel.de

Belarus

- Zyxel BY
- http://www.zyxel.by

Belgium

- Zyxel Communications B.V.
- http://www.zyxel.com/be/nl/
- http://www.zyxel.com/be/fr/

Bulgaria

- Zyxel България
- http://www.zyxel.com/bg/bg/

Czech Republic

- Zyxel Communications Czech s.r.o
- http://www.zyxel.cz

Denmark

- Zyxel Communications A/S
- http://www.zyxel.dk

Estonia

- Zyxel Estonia
- http://www.zyxel.com/ee/et/

Finland

- Zyxel Communications
- http://www.zyxel.fi

France

- Zyxel France
- http://www.zyxel.fr

Germany

- Zyxel Deutschland GmbH
- http://www.zyxel.de

Hungary

- Zyxel Hungary & SEE
- http://www.zyxel.hu

Italy

- Zyxel Communications Italy
- http://www.zyxel.it/

Latvia

- Zyxel Latvia
- http://www.zyxel.com/lv/lv/homepage.shtml

Lithuania

- Zyxel Lithuania
- http://www.zyxel.com/lt/lt/homepage.shtml

Netherlands

- Zyxel Benelux
- http://www.zyxel.nl

Norway

- Zyxel Communications
- http://www.zyxel.no

Poland

- Zyxel Communications Poland
- http://www.zyxel.pl

Romania

- Zyxel Romania
- http://www.zyxel.com/ro/ro

Russia

- Zyxel Russia
- http://www.zyxel.ru

Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- http://www.zyxel.sk

Spain

- Zyxel Communications ES Ltd
- http://www.zyxel.es

Sweden

- Zyxel Communications
- http://www.zyxel.se

Switzerland

- Studerus AG

- http://www.zyxel.ch/

Turkey

- Zyxel Turkey A.S.
- http://www.zyxel.com.tr

UK

- Zyxel Communications UK Ltd.
- http://www.zyxel.co.uk

Ukraine

- Zyxel Ukraine
- http://www.ua.zyxel.com

Latin America

Argentina

- Zyxel Communication Corporation
- http://www.zyxel.com/ec/es/

Brazil

- Zyxel Communications Brasil Ltda.
- https://www.zyxel.com/br/pt/

Ecuador

- Zyxel Communication Corporation
- http://www.zyxel.com/ec/es/

Middle East

Israel

- Zyxel Communication Corporation
- http://il.zyxel.com/homepage.shtml

Middle East

- Zyxel Communication Corporation
- http://www.zyxel.com/me/en/

North America

USA

- Zyxel Communications, Inc. - North America Headquarters
- http://www.zyxel.com/us/en/

Oceania

Australia

- Zyxel Communications Corporation
- http://www.zyxel.com/au/en/

Africa

South Africa

- Nology (Pty) Ltd.
- http://www.zyxel.co.za

APPENDIX B
Product Features

Please refer to the product datasheet for the latest product features.

Version	5.42	5.42	5.42
Model Name	USG FLEX 50 (USG20-VPN)	USG20W-VPN	USG FLEX 50AX
# of MAC Addresses	6	7	5
Interface			
VLAN	8	8	8
Virtual(alias) per interface	4	4	4
PPP (System Default)	2	2	2
PPP (User Created)	2	2	2
Bridge	2	2	2
Tunnel (GRE/IPv6 Transition)	4	4	4
Routing			
Static Route	64	64	64
Policy Route	100	100	100
Reserved Sessions For Managed Devices	500	500	500
Max OSPF areas	10	10	10
Max. BGP Neighbor	5	5	5
BGP Max. Network	16	16	16
Sessions			
Max. TCP Concurrent Sessions (Forwarding, NAT/Firewall)	100,000	100,000	100,000
Session Rate	2,000	2,000	2,000
NAT			
Max. Virtual Server Number	128	128	128
Firewall (Secure Policy)			
Max Firewall ACL Rule Number = Secure Policy Number	500	500	500
Max Session Limit per Host Rules	1000	1000	1000
ADP			
Max. ADP Profile Number	8	8	8
Max. ADP Rule Number	32	32	32
Application Patrol			
Max. App Patrol Profile	n/a	n/a	n/a
Max. Application Object In Each Profile (Object + Object Group)	n/a	n/a	n/a
User Profile			
Max. Local User	64	64	64
Max. Admin User	5	5	5
Max. User Group	16	16	16
Max User In One User Group	64	64	64
Default Concurrent Device Login	64	64	64
Max. Concurrent Device Upgrade (License)	64	64	64
On-Cloud Max. Concurrent Device Upgrade (License)	64	64	64
HTTPd			
Max HTTPd Number	128	128	128
Objects			

Address Object	300	300	300
Address Group	25	25	25
Max. Address Object In One Group	64	64	64
Service Object	200	200	200
Service Group	50	50	50
Max. Service Object In One Group	64	64	64
Schedule Object	32	32	32
Schedule Group	16	16	16
Max. Schedule Object In One Group	24	24	24
Application Object	n/a	n/a	n/a
Application Group	n/a	n/a	n/a
Max. Application Object In One Group	n/a	n/a	n/a
ISP Account	16 (PPP+3G)	16 (PPP+3G)	16 (PPP+3G)
Max. LDAP Server Object #	2	2	2
Max. RADIUS Server Object #	2	2	2
Max. Ad Server Object #	4	4	4
Max. auth. method #	4	4	4
Max. Zone Number (System Default)	8	8	8
Max. Zone Number (User Defined)	8	8	8
Trunk			
Max. Trunk Number (System Default)	1	1	1
Max. Trunk Number (User Defined)	4	4	4
Max. Member Number Per Trunk	2+8	2+8	2+8
VPN			
Max. VPN Tunnels Number	20	20	20
Max. VPN Concentrator Number	2	2	2
Max. VPN Configuration Provision Rule Number	20	20	20
Certificate			
Certificate Buffer Size	128k	128k	128k
Built-In Service			
A Record	32	32	32
NS Record (DNS Domain Zone Forward)	8	8	8
MX Record	4	4	4
Max Service Control Entries	16 per service	16 per service	16 per service
Max. DHCP Network Pool	15	15	15
Max. DHCP Host Pool (Static DHCP)	64	64	64
Max. DHCP Extended Options	10	10	10
Max DDNS Profiles	5	5	5
DHCP Relay	2 per interface	2 per interface	2 per interface
USB Storage			
Device Number	1	1	1
Centralized Log			
Log Entries	512	512	512
Debug Log Entries	1024	1024	1024
Admin E-Mail Address	2	2	2
Syslog Server	4	4	4
IDP			
Max. IDP Profile Number	n/a	n/a	n/a
Max. Custom Signatures	n/a	n/a	n/a

SSL Inspection			
Max. SSL Inspection Profile	n/a	n/a	n/a
Max. Exclude List	n/a	n/a	n/a
Content Filtering			
Max. Number Of Content Filter Policies	16	16	16
Forbidden Domain Entry Number	256 per profiles	256 per profiles	256 per profiles
Trusted Domain Entry Number	256 per profiles	256 per profiles	256 per profiles
Keyword Blocking Number	128 per profiles	128 per profiles	128 per profiles
Common Forbidden Domain Entry Number	1024	1024	1024
Common Trusted Domain Entry Number	1024	1024	1024
Anti-Spam			
Maximum AS Rule Number (Profile)	16	16	n/a
Maximum White List Rule Support	128	128	n/a
Maximum Black List Rule Support	128	128	n/a
Maximum DNSBL Domain Support	5	5	n/a
Concurrent Mail Session Scanning	200	200	n/a
Max. Statistics Number	500	500	n/a
Max. Statistics Ranking	10	10	n/a
Anti-Malware			
Max. AV Rule (Profile)	n/a	n/a	n/a
Max. Statistics Number	n/a	n/a	n/a
Max. Statistics Ranking	n/a	n/a	n/a
SSL VPN			
Default SSL VPN Connections	15	15	15
Maximum SSL VPN Connections	15	15	15
Max. SSL VPN Network List	8	8	8
SSL VPN Max Policy	32	32	32
AP Controller			
Default # Of Control AP	n/a	n/a	n/a
Max. # Of Control AP	n/a	n/a	n/a
AP Group	n/a	n/a	n/a
Max Radio Profile	n/a	16	16
Max SSID Profile	n/a	32	32
Max Security Profile	n/a	32	32
Max MAC Filter Profile	n/a	32	32
MAX MAC Entry Per MAC Filter Profile	n/a	512	512
MAX MAC Address for MAC Authentication	n/a	n/a	n/a
Zymesh	n/a	n/a	n/a
BWM			
Maximum BWM Rule Number	128	128	128
BWM Per Source IP (Max.)	256	256	256
SIP			
Maximum SIP Concurrent Call	50	50	50
Custom Web Portal Page			
Max Internal Web Portal Customize File	4	4	4
Upload Zip File Size	Up to 2MB	Up to 2MB	Up to 2MB
Unzip File Size	Up to 5MB	Up to 5MB	Up to 5MB
Hotspot Management			
Max Dynamic Account List	n/a	n/a	n/a

Max Free Time Account Limit	n/a	n/a	n/a
Hotspot Support	n/a	n/a	n/a
Walled Garden - URL Base	n/a	n/a	n/a
Walled Garden - Domain/IP Base	n/a	n/a	n/a
Advertisement	n/a	n/a	n/a
Ticket Printer Support	n/a	n/a	n/a

Appendix C
Legal Information

Copyright

Copyright © 2026 by Zyxel and/or its affiliates

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel and/ or its affiliates.

Published by Zyxel and/or its affiliates. All rights reserved.

Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement

Model List: USG FLEX 50, USG20-VPN, USG20W-VPN, USG FLEX 50AX

United States of America

The following information applies if you use the product within USA area.

Federal Communications Commission (FCC) EMC Statement

- The device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

  (1) This device may not cause harmful interference, and

  (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.
- This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna
  - Increase the separation between the equipment and receiver
  - Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
  - Consult the dealer or an experienced radio/TV technician for assistance

The following information applies to products with wireless functions.

- For 2.4G WLAN, only channels 1~11 are operational. Selection of other channels is not possible.
- Operation of this device is restricted to indoor use only, unless the relevant user's manual states that this device can be installed outdoors.

FCC Radiation Exposure Statement (For device with WiFi function)

- This device complies with FCC Radio Frequency (RF) radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.

Canada

The following information applies if you use the product within Canada area.

Innovation, Science and Economic Development Canada ICES statement

CAN ICES(B)/NMB(B)

Innovation, Science and Economic Development RSS-GEN & RSS-247 statement

The following information applies to products with wireless functions.

- For indoor use only. (For indoor devices only)
- This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions: (1) This device may not cause interference (2) This device must accept any interference, including interference that may cause undesired operation of the device.
- For 2.4 G WLAN, only channels 1-11 are operational. Selection of other channels is NoT possible.
- This radio transmitter 2468C-USG20WVPN and 9968A-AW7915NPD has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Antenna Information

Model Name	No.	Type	Gain (dBi)	Impedance
USG20W-VPN	1	Dipole	2 dBi (2.4G) 3 dBi (5G)	50 Ω
USG FLEX 50AX	1	Dipole	2.7 dBi (2400-2483.5 MHz) 3.86 dBi (5180-5250 MHz) 4.17 dBi (5745-5825 MHz)	50 Ω

If the product with 5G wireless function operating in 5150 – 5250 MHz and 5725 – 5850 MHz, the following attention must be paid,

- The device for operation in the band 5150 – 5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725 – 5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate; and
- Where applicable, antenna type(s), antenna models(s), and the worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2.3 of RSS 247 shall be clearly indicated.

If the product with 5G wireless function operating in 5250 – 5350 MHz and 5470 – 5725 MHz, the following attention must be paid.

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250 – 5350 MHz and 5470 – 5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit.

Innovation, Sciences et Développement économique Canada RSS-GEN & RSS-247

- Pour une utilisation en intérieur uniquement. (sauf modèle extérieur)
- L'émetterur/récepteur exempt de licence contenu dans le prés ent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio ex empts de licence. L'exploitation est autorisée aux deux condi tions suivantes: (1) L'appareil ne doit pas produire de brouillage (2)L'appareil doit accepter tout brouillage radioélectrique su bi, même si le brouillage est susc eptible d'en compromettre le fonctionnement.
- Pour le WLAN 2,4 G, seuls les canaux 1 à 11 sont opérationnels. La sélection d'autres canaux n'est PAS possible.
- Le présent émetteur radio 2468C-USG20WVPN et 9968A-AW7915NPD a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

informations antenne

Nom du Modèle	Nb.	Type	Gain (dBi)	Impédance
USG20W-VPN	1	Dipole	2 dBi (2.4G) 3 dBi (5G)	50 Ω
USG FLEX 50AX	1	Dipole	2.7 dBi (2400-2483.5 MHz) 3.86 dBi (5180-5250 MHz) 4.17 dBi (5745-5825 MHz)	50 Ω

Lorsque la fonction sans fil 5G fonctionnant en 5150-5250 MHz and 5725-5850 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes

- Les dispositifs fonctionnant dans la bande de 5 150 à 5 250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée, selon le cas;
- Lorsqu'il y a lieu, les types d'antennes (s'il y en a plusieurs), les numéros de modèle de l'antenne et les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, énoncée à la section 6.2.2.3 du CNR-247, doivent être clairement indiqués.

Lorsque la fonction sans fil 5G fonctionnant en 5250-5350 MHz et 5470-5725 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes.

- Pour les dispositifs munis d’antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

ISED Radio Frequency (RF) Exposure Statement (For device with WiFi function)

This equipment complies with ISED RF exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body. Refer to the list below for the models whose radiators require a minimum distance of over 20 cm from your body, along with the required distances.

- USG20W-VPN: 27 cm

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé en respectant une distance minimale de 20 cm entre le radiateur et votre corps. Veuillez vous référer à la liste ci-dessous pour connaître les modèles dont les radiateurs nécessitent une distance minimale de plus de 20 cm par rapport à votre corps, ainsi que les distances requises.

- USG20W-VPN: 27 cm

Europe and the United Kingdom

The following information applies if you use the product within the European Union or United Kingdom.

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED) and UK Radio Equipment Regulations 2017 (For device with WiFi function)

- Compliance information for wireless products relevant to the EU and other Countries following the EU Directive 2014/53/EU (RED) and UK regulation 2017 SI 2017-1206. And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) and the United Kingdom without any limitation except for the countries mentioned in the below table:
- In the majority of the EU and other European countries, the 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5GHz wireless LANs.
- If this device operates in the 5150-5350 MHz band, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20 cm between the radio equipment and your body.
- The maximum RF operating power for each band is as follows:

Frequency	Maximum Power
2,400 MHz to 2,483.5 MHz	< 100mW
5,150 MHz to 5,350 MHz	< 200mW
5,470 MHz to 5,725 MHz	< 1000mW
5,945 MHz to 6,425 MHz (For device with 6 GHz function)	< 200mW

Belgium (English) België (Flemish) Belgique (French)	National Restrictions • The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check *http://www.bipt.be* for more details. • Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie *http://www.bipt.be* voor meer gegevens. • Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez *http://www.ibpt.be* pour de plus amples détails.
Čeština (Czech)	Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.
Dansk (Danish)	Undertegnede Zyxel erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU.
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EU põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Zyxel ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/EU.
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Español (Spanish)	Por medio de la presente Zyxel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/UE.
Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/EU.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/EU.

Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/EU.
Italiano (Italian)	Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/EU. National Restrictions • This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a “general authorization.” Please check https://www.mise.gov.it/it/ for more details. • Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una “Autorizzazione Generale”. Consultare https://www.mise.gov.it/it/ per maggiori dettagli.
Latviešu valoda (Latvian)	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/EU būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/EU Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 2014/53/EU irányelv egyéb előírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/EU.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 2014/53/EU.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/EU.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/EU.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 2014/53/EU.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EU.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.
Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС.

Notes:

1. Not all European states that implement EU Directive 2014/53/EU are European Union (EU) members.
2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	No
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not put the device in a place that is humid, dusty, has extreme temperatures, or that blocks the device ventilation slots. These conditions may harm your device.
- Please refer to the device back label, datasheet, box specifications or catalog information for power rating of the device and operating temperature.
- There is a remote risk of electric shock from lightning: (1) Do not use the device outside, and make sure all the connections are indoors. (For indoor devices only) (2) Do not install or service this device during a thunderstorm.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Connect ONLY suitable accessories to the device.
- Do not open the device. Opening or removing the device covers can expose you to dangerous high voltage points or other risks.
- Only qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connected cables carefully so that no one will step on them or stumble over them.
- Disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NoT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect the power adaptor or cord to the right supply voltage (for example, 120V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove the damaged power adaptor or cord from the device and the power source. Do not try to repair the power adaptor or cord by yourself. Contact your local vendor to order a new one.
- CAUTION: There is a risk of explosion if you replace the device battery with an incorrect one. Dispose of used batteries according to the instructions. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device.
  - For a permanently connected device, a readily accessible method to disconnect the device shall be incorporated externally to the device;
  - For a pluggable device, the socket-outlet shall be installed near the device and shall be easily accessible.
- Caution - Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.
- Attention - L'utilisation des commandes ou reglages ou l'execution des procedures autres que celles specifiees dans les presents exigences peuvent etre la cause d'une exposition a un rayonnement dangereux)
- Do not leave a battery in an extremely high temperature environment or surroundings since it can result in an explosion or the leakage of flammable liquid or gas. (For devices with a battery)
- Do not subject a battery to extremely low air pressure since it may result in an explosion or the leakage of flammable liquid or gas. (For devices with a battery)
- Complies with 21 CFR 1040.10 and 1040.11 except for conformance with IEC 60825-1 Ed. 3., as described in Laser Notice No. 56, dated May 8, 2019. (For devices with fiber)
- Conforme à 21 CFR 1040.10 et 1040.11 sauf pour la conformité à la norme CEI 60825-1 Ed. 3., comme décrit dans la notice laser Numéro 56 du 8 mai 2019. (For devices with fiber)
- Ce produit laser est un produit laser de classe 1 conforme à la norme CEI 60825-1: 2014 (For devices with fiber)
- CLASS 1 CONSUMER LASER PRODUCT & “EN 50689:2021” (For devices with fiber)

Environment Statement

ErP (Energy-related Products)

Zyxel products put on the EU and United Kingdom markets comply with the requirement of the European Parliament and the Council published Directive 2009/125/EC and UK regulation establishing a framework for the setting of ecodesign requirements for energy-related products (recast), the so called "ErP Directive (Energy-related Products directive), as well as ecodesign requirements laid down in applicable implementation measures. Power consumption has satisfied the regulation requirements which are:

- Network standby power consumption < 8 W (watts), and/or
- Off mode power consumption < 0.5 W (watts), and/or
- Standby mode power consumption < 0.5 W (watts).

Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.

台灣

以下訊息僅適用於產品具有無線功能且銷售至台灣地區 (USG20W-VPN, USG FLEX 50AX)

- 取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
- 低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
- 使用無線產品時，應避免影響附近雷達系統之操作。
- 高增益指向性天線只得應用於固定式點對點系統。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

- 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

安全警告 - 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。

- 避免設備接觸：
  - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
  - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請使用隨貨提供或指定的連接線 / 電源線 / 電源變壓器，將其連接到合適的供應電壓 (如 ： 台灣供應電壓 110 伏特)。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  - 對永久連接之設備， 在設備外部須安裝可觸及之斷電裝置；
  - 對插接式之設備， 插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC is the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

Viewing Certifications

Go to *http://www.zyxel.com* to view this product's documentation and certifications.

Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at *https://www.zyxel.com/global/en/support/warranty-information*.

Open Source Licenses

This product may contain in part some free software distributed under GPL license terms and/or GPL like licenses.

To request the source code covered under these licenses, please go to: *https://www.zyxel.com/form/gpl_oss_software_notice.shtml*

Index

Symbols

Numbers

3322 Dynamic DNS 414
3DES 502
6in4 tunneling 334
6to4 tunneling 334

A

AAA
  Base DN 729
  Bind DN 729, 731
  directory structure 728
  Distinguished Name, see DN
  DN 728, 730, 731
  password 731
  port 731, 733, 734
  search time limit 731
  SSL 731
AAA server 726
  AD 728
  and users 679
  directory service 726
  LDAP 726, 728
  local user database 728
  RADIUS 727, 728, 732
  RADIUS group 732
  see also RADIUS
access 39
Access Point Name, see APN
Access Restricted Web Page
  Response Message 833
access users 679, 681
  custom page 802
  forcing login 541
  idle timeout 700
  logging in 541
  multiple logins 701
  see also users 679
  Web Configurator 702
access users, see also force user authentication policies
account
  user 678
accounting server 726
Active Directory, see AD
active protocol 507
  AH 507
  and encapsulation 507
  ESP 507
active sessions 209, 225
ActiveX 624
AD 726, 728, 729, 730, 731
  directory structure 728
  Distinguished Name, see DN
  password 731
  port 731, 733, 734
  search time limit 731
  SSL 731
address groups 706
  and content filtering 603
  and FTP 821
  and security policy 546
  and SNMP 826
  and SSH 816
  and Telnet 819
  and WWW 802
address objects 706
  and content filtering 603
  and FTP 821
  and NAT 395, 425
  and policy routes 394
  and security policy 546
  and SNMP 826
  and SSH 816
  and Telnet 819
  and VPN connections 478
  and WWW 802
  HOST 707

RANGE 707
SUBNET 707
types of 707, 713
address record 790
admin user
troubleshooting 911
admin users 679
multiple logins 701
see also users 679
ADP 587
false negatives 588
false positives 588
inline profile 589
monitor profile 588
Advanced Encryption Standard, see AES
AES 502
AF 398
AH 484, 507
and transport mode 507
alerts 848, 849, 851, 853, 854, 855
anti-spam 655
ALG 435, 441
and NAT 435, 437
and policy routes 437, 441
and security policy 435, 437
and trunks 441
FTP 435, 436
H.323 435, 436, 441
peer-to-peer calls 437
RTP 441
see also VoIP pass through 435
SIP 435, 436
Anomaly Detection and Prevention, see ADP
anti-spam 651, 655, 657
action for spam mails 656
alerts 655
black list 651, 655, 657
concurrent e-mail sessions 261, 653
DNSBL 652, 655, 662
e-mail header buffer 652
e-mail headers 652
excess e-mail sessions 653
general settings 653
identifying legitimate e-mail 651
identifying spam 651
log options 655
mail scan 656
mail sessions threshold 653
POP2 652
POP3 652
regular expressions 660
SMTP 652
white list 651, 655, 659, 660
anti-virus 154
virus 154
worm 154
APN 329
Application Layer Gateway, see ALG
application patrol
and HTTP redirect 430
ASAS (Authenex Strong Authentication System) 727
asymmetrical routes 573
allowing through the security policy 575
vs virtual interfaces 573
attacks
Denial of Service (DoS) 482
virus 154
Authenex Strong Authentication System (ASAS) 727
authentication
in IPSec 485
LDAP/AD 728
server 726
authentication algorithms 501, 502
and active protocol 501
MD5 502
SHA1 502
Authentication Header, see AH
authentication method objects 735
and users 679
and WWW 801
create 736
example 735
authentication policy
exceptional services 543
Authentication server
RADIUS client 830
authentication server 828, 831
authentication type 163, 764
Authentication, Authorization, Accounting servers, see AAA server
authorization server 726
Autonomous Systems (AS) 408
auxiliary interfaces 286

B

backing up configuration files 860
bandwidth
  egress 330, 339
  ingress 330, 339
bandwidth limit
  troubleshooting 907
bandwidth management
  maximize bandwidth usage 398, 527
Base DN 729
Batch import 767
BGP 413
Bind DN 729, 731
black list 655, 657
  anti-spam 651
bridge interfaces 286, 355
  and virtual interfaces of members 355
  basic characteristics 286
  effect on routing table 355
  member interfaces 355
  virtual 313
bridges 354

C

CA
  and certificates 746
CA (Certificate Authority), see certificates
Calling Station ID 275
capturing packets 880
card SIM 330
CEF (Common Event Format) 846, 852
cellular 324
  APN 329
  interfaces 286
  network types 239
  signal quality 239, 240
  SIM card 330
  SIM Card IMSI 240
  status 238, 241
  system 239, 240
  troubleshooting 906
certificate
  troubleshooting 912
Certificate Authority (CA)
  see certificates
Certificate Revocation List (CRL) 746
  vs OCSP 762
certificates 745
  advantages of 746
  and CA 746
  and FTP 821
  and HTTPS 797
  and IKE SA 506
  and SSH 816
  and VPN gateways 478
  and WWW 800
  certification path 746, 754, 760
  expired 746
  factory-default 746
  file formats 746
  fingerprints 755, 761
  importing 751
  in IPSec 491
  not used for encryption 746
  revoked 746
  self-signed 746, 753
  serial number 755, 760
  storage space 749, 757
  thumbprint algorithms 747
  thumbprints 747
  used for authentication 746
  verifying fingerprints 747
certification requests 753
certifications 933
  viewing 935
Challenge Handshake Authentication Protocol (CHAP) 764
CHAP (Challenge Handshake Authentication Protocol) 764
CHAP/PAP 764
CLI 37, 48
  button 48
  messages 48
  popup window 48
  Reference Guide 2
commands 37
  sent by Web Configurator 48
Common Event Format (CEF) 846, 852
compression (stac) 765
computer names 309, 351, 365, 385, 520
computer virus 154

see also virus
concurrent e-mail sessions 261, 653
configuration
information 876
configuration file
troubleshooting 913
configuration files 856
at restart 860
backing up 860
downloading 862, 892
downloading with FTP 820
editing 856
how applied 857
lastgood.conf 860, 864
managing 860
startup-config.conf 864
startup-config-bad.conf 860
syntax 857
system-default.conf 864
uploading 864
uploading with FTP 820
use without restart 856
connection
troubleshooting 908
connection monitor (in SSL) 255
connectivity check 307, 323, 330, 339, 349, 366, 371, 485
console port
speed 786
contact information 919, 925
content filter
troubleshooting 904
content filtering 602, 603
and address groups 603
and address objects 603
and schedules 603
and user groups 603
and users 603
by category 603, 611, 631
by keyword (in URL) 603, 604, 625
by URL 603, 624, 626, 627
by web feature 603, 624
categories 611, 631
category service 610
default policy 603
external web filtering service 610
filter list 603
managed web pages 610
policies 603
registration status 269
testing 611
uncategorized pages 610
URL for blocked access 606
cookies 39, 624
copyright 929
CPU usage 209
current date/time 207, 782
daylight savings 784
setting manually 785
time server 785
current user list 255
custom
access user page 802
login page 802
customer support 919, 925

D

Data Encryption Standard, see DES
date 782
daylight savings 784
DDNS 414
backup mail exchanger 419
mail exchanger 419
service providers 414
troubleshooting 908
Dead Peer Detection, see DPD
default
security policy behavior 571
Default_L2TP_VPN_GW 518
Denial of Service (Dos) attacks 482
DES 502
device access
troubleshooting 903
DHCP 384, 780
and DNS servers 385
and domain name 780
and interfaces 384
pool 385
static DHCP 385
DHCP Unique IDentifier 290
DHCPv6
DHCP Unique IDentifier 290

diagnostics 876
Diffie-Hellman key group 502
DiffServ 398
direct routes 390
directory 726
directory service 726
  file structure 728
disclaimer 929
Distinguished Name (DN) 728, 730, 731
DN 728, 730, 731
DNS 787
  address records 790
  domain name forwarders 792
  domain name to IP address 790
  IP address to domain name 791
  L2TP VPN 520
  Mail eXchange (MX) records 793
  pointer (PTR) records 791
DNS Blacklist see DNSBL 652
DNS inbound LB 467
DNS servers 164, 787, 792
  and interfaces 385
DNSBL 652, 655, 662
  see also anti-spam 652
domain name 780
Domain Name System, see DNS
DPD 493
DSCP 391, 394, 529, 896
DUID 290
Dynamic Domain Name System, see DDNS
dynamic guest account 680
Dynamic Host Configuration Protocol, see DHCP.
dynamic peers in IPSec 483
DynDNS 414
DynDNS see also DDNS 414
Dynu 414

E

eBGP (exterior Border Gate Protocol) 408
egress bandwidth 330, 339
e-mail 651
  daily statistics report 843
  header buffer 652
  headers 652
Encapsulating Security Payload, see ESP
encapsulation
  and active protocol 507
  IPSec 484
  transport mode 507
  tunnel mode 507
  VPN 507
encryption
  IPSec 485
  RSA 755
encryption algorithms 501, 502
  3DES 502
  AES 502
  and active protocol 501
  DES 502
encryption method 764
enforcing policies in IPSec 483
ESP 484, 507
  and transport mode 507
Ethernet interfaces 286
  and OSPF 296
  and RIP 296
  and routing protocols 294
  basic characteristics 286
  virtual 313
ethernet interfaces
  neighboring devices 242
exceptional services 543
extended authentication
  and VPN gateways 478
  IKE SA 506
ext-user
  troubleshooting 911

F

false negatives 588
false positives 588, 590, 591
fast forwarding 841
file extensions
  configuration files 856
  shell scripts 856
file manager 856
Firefox 39

firewall
and SMTP redirect 431
firmware
and restart 866
current version 207, 869
getting updated 866
uploading 868
uploading with FTP 820
firmware upload
troubleshooting 914
flash usage 209
forcing login 541
FQDN 790
FTP 820
additional signaling port 440
ALG 435
and address groups 821
and address objects 821
and certificates 821
and zones 821
signaling port 440
with Transport Layer Security (TLS) 821
full tunnel mode 511, 515
Fully-Qualified Domain Name, see FQDN

G

Generic Routing Encapsulation, see GRE.
global SSL setting 516
GRE 386
GSM 330
Guide
CLI Reference 2
Quick Start 2

H

H.323 441
additional signaling port 440
ALG 435, 441
and RTP 441
and security policy 436
signaling port 440
HSDPA 330
HTTP
over SSL, see HTTPS
redirect to HTTPS 800
vs HTTPS 797
HTTP redirect
and application patrol 430
and interfaces 434
and policy routes 430, 431
and security policy 430
packet flow 430
troubleshooting 908
HTTPS 797
and certificates 797
authenticating clients 797
avoiding warning messages 808
example 807
vs HTTP 797
with Internet Explorer 807
with Netscape Navigator 807
hub-and-spoke VPN, see VPN concentrator
HyperText Transfer Protocol over Secure Socket Layer, see HTTPS

I

ICMP 717
identifying
legitimate e-mail 651
spam 651
IDP
action 593
log options 591, 593
reject sender 593
reject-both 593
reject-receiver 593
IEEE 802.1q VLAN
IEEE 802.1q. See VLAN.
IKE SA
aggressive mode 501, 505
and certificates 506
and RADIUS 506
and to-ZyWALL security policy 909
authentication algorithms 501, 502
content 504
Dead Peer Detection (DPD) 493
Diffie-Hellman key group 502
encryption algorithms 501, 502

extended authentication 506
ID type 504
IP address, remote IPSec router 501
IP address, Zyxel device 501
local identity 504
main mode 501, 505
NAT traversal 505
negotiation mode 501
password 506
peer identity 504
pre-shared key 504
proposal 501
see also VPN
user name 506
IMAP 652
inbound LB algorithm
least connection 469
least load 469
weighted round robin 469
inbound load balancing 467
time to live 470
incoming bandwidth 330, 339
ingress bandwidth 330, 339
inline profile 589
interface
status 219
troubleshooting 905
interfaces 285
and DNS servers 385
and HTTP redirect 434
and layer-3 virtualization 286
and NAT 424
and physical ports 286
and policy routes 394
and static routes 397
and VPN gateways 478
and zones 286
as DHCP relays 384
as DHCP servers 384, 780
auxiliary, see also auxiliary interfaces.
backup, see trunks
bandwidth management 379, 380, 383
bridge, see also bridge interfaces.
cellular 286
DHCP clients 383
Ethernet, see also Ethernet interfaces.
gateway 383
general characteristics 286
IP address 382
metric 383
MTU 384
overlapping IP address and subnet mask 383
port groups, see also port groups.
PPPoE/PPTP, see also PPPoE/PPTP interfaces.
prerequisites 287
relationships between 287
static DHCP 385
subnet mask 382
trunks, see also trunks.
Tunnel, see also Tunnel interfaces.
types 286
virtual, see also virtual interfaces.
VLAN, see also VLAN interfaces.
WLAN, see also WLAN interfaces.
Internet access
troubleshooting 904, 911
Internet Control Message Protocol, see ICMP
Internet Explorer 39
Internet Message Access Protocol, see IMAP 652
Internet Protocol Security, see IPSec
Internet Protocol version 6, see IPv6
IP policy routing, see policy routes
IP pool 515
IP protocols 716
and service objects 717
ICMP, see ICMP
TCP, see TCP
UDP, see UDP
IP static routes, see static routes
IP/MAC binding 458
exempt list 462
monitor 235
static DHCP 461
IPSec 473
active protocol 484
AH 484
and certificates 478
authentication 485
basic troubleshooting 909
certificates 491
connections 478
connectivity check 485
Default_L2TP_VPN_GW 518
encapsulation 484
encryption 485
ESP 484

established in two phases 475
L2TP VPN 517
local network 473
local policy 483
NetBIOS 482
peer 473
Perfect Forward Secrecy 485
PFS 485
phase 2 settings 484
policy enforcement 483
remote access 483
remote IPSec router 473
remote network 473
remote policy 483
replay detection 482
SA life time 484
SA monitor 253
SA see also IPSec SA 506
see also VPN
site-to-site with dynamic peer 483
static site-to-site 483
transport encapsulation 484
tunnel encapsulation 484
VPN gateway 478
IPSec SA
active protocol 507
and security policy 909
and to-ZyWALL security policy 909
authentication algorithms 501, 502
destination NAT for inbound traffic 509
encapsulation 507
encryption algorithms 501, 502
local policy 506
NAT for inbound traffic 508
NAT for outbound traffic 508
Perfect Forward Secrecy (PFS) 507
proposal 507
remote policy 506
search by name 254
search by policy 254
Security Parameter Index (SPI) (manual keys) 508
see also IPSec
see also VPN
source NAT for inbound traffic 509
source NAT for outbound traffic 509
status 253
transport mode 507
tunnel mode 507
when IKE SA is disconnected 506
IPSec VPN
troubleshooting 909
IPv6 288
link-local address 289
prefix 288
prefix delegation 289
prefix length 288
stateless autoconfiguration 289
IPv6 tunnelings
6in4 tunneling 334
6to4 tunneling 334
IPv6-in-IPv4 tunneling 334
ISP account
CHAP 764
CHAP/PAP 764
MPPE 764
MSCHAP 764
MSCHAP-V2 764
PAP 764
ISP accounts 762
and PPPoE/PPTP interfaces 318, 762
authentication type 764
encryption method 764
stac compression 765

J

Java 624
permissions 39
JavaScripts 39

K

key pairs 745

L

L2TP VPN 517
Default_L2TP_VPN_GW 518
DNS 520
IPSec configuration 517
policy routes 518
session monitor 256

WINS 520
lastgood.conf 860, 864
Layer 2 Tunneling Protocol Virtual Private Network, see L2TP VPN 517
layer-2 isolation 463
example 463
IP 465
LDAP 726
and users 679
Base DN 729
Bind DN 729, 731
directory 726
directory structure 728
Distinguished Name, see DN
DN 728, 730, 731
password 731
port 731, 733, 734
search time limit 731
SSL 731
user attributes 705
least connection algorithm 469
least load algorithm 469
least load first load balancing 374
LED troubleshooting 903
legitimate e-mail 651
licensing 266
Lightweight Directory Access Protocol, see LDAP
Link Layer Discovery Protocol (LLDP) 242
LLDP (Link Layer Discovery Protocol) 242
load balancing 373
algorithms 374, 378, 380
DNS inbound 467
least load first 374
round robin 374
see also trunks 373
session-oriented 374
spillover 375
weighted round robin 375
local user database 728
log
troubleshooting 913
log messages
categories 849, 851, 853, 854, 855
debugging 263
regular 263
types of 263
log options 655
(IDP) 591, 593
login
custom page 802
logo
troubleshooting 913
logout
Web Configurator 45
logs
and security policy 582
e-mail profiles 845
e-mailing log messages 848
formats 846
log consolidation 849
settings 845
syslog servers 845
system 845
types of 845

M

MAC address 703
and VLAN 340
Ethernet interface 304
range 207
MAC authentication 275
Calling Station ID 275
case 275
delimiter 275
mac role 703
mail sessions threshold 653
managed web pages 610
management access
troubleshooting 913
Management Information Base (MIB) 823, 824
managing the device
using SNMP. See SNMP.
MD5 502
memory usage 209
Message Digest 5, see MD5
messages
CLI 48
metrics, see reports
Microsoft
Challenge-Handshake Authentication Protocol (MSCHAP) 764

Challenge-Handshake Authentication Protocol Version 2 (MSCHAP-V2) 764
Point-to-Point Encryption (MPPE) 764
mobile broadband see also cellular 324
Monitor 767
monitor 255
SA 253
sessions 225
monitor profile
ADP 588
mounting
rack 36, 90
wall 91
MPPE (Microsoft Point-to-Point Encryption) 764
MSCHAP (Microsoft Challenge-Handshake Authentication Protocol) 764
MSCHAP-V2 (Microsoft Challenge-Handshake Authentication Protocol Version 2) 764
MTU 330, 339
multicast 280
multicast rate 280
My Certificates, see also certificates 748
myZyXEL 32
accounts, creating 33
myZyxel.com
accounts, creating 155

N

NAT 398, 420
ALG, see ALG
and address objects 395
and address objects (HOST) 425
and ALG 435, 437
and interfaces 424
and policy routes 388, 395
and security policy 573
and to-ZyWALL security policy 426
and VoIP pass through 437
and VPN 505
loopback 427
port forwarding, see NAT
port translation, see NAT
traversal 505
NAT Port Mapping Protocol 442
NAT Traversal 442
NAT-PMP 442
NBNS 309, 351, 365, 385, 515
NetBIOS
Broadcast over IPSec 482
Name Server, see NBNS.
NetBIOS Name Server, see NBNS
NetMeeting 441
see also H.323
Netscape Navigator 39
network access mode 35
full tunnel 511
Network Address Translation, see NAT
network list, see SSL 515
Network Time Protocol (NTP) 785
No-IP 414
NSSA 401

O

objects 512
AAA server 726
addresses and address groups 706
authentication method 735
certificates 745
services and service groups 716
users, user groups 678
One-Time Password (OTP) 727
Online Certificate Status Protocol (OCSP) 762
vs CRL 762
Open Shortest Path First, see OSPF
OSPF 401
and Ethernet interfaces 296
and RIP 402
and static routes 402
and to-ZyWALL security policy 401
area 0 402
areas, see OSPF areas
authentication method 297
autonomous system (AS) 401
backbone 402
configuration steps 403
direction 297
link cost 297
priority 297
redistribute 402
redistribute type (cost) 404

routers, see OSPF routers
virtual links 403
vs RIP 399, 401
OSPF areas 401
and Ethernet interfaces 297
backbone 401
Not So Stubby Area (NSSA) 401
stub areas 401
types of 401
OSPF routers 402
area border (ABR) 402
autonomous system boundary (ASBR) 402
backbone (BR) 402
backup designated (BDR) 403
designated (DR) 403
internal (IR) 402
link state advertisements
priority 403
types of 402
OTP (One-Time Password) 727
outgoing bandwidth 330, 339

P

packet
statistics 216, 217
packet capture 880
files 879, 883, 884, 885
troubleshooting 914
packet captures
downloading files 880, 883, 885
packet statistics 216
PAP (Password Authentication Protocol) 764
Password Authentication Protocol (PAP) 764
Peanut Hull 414
Peer-to-peer (P2P)
calls 437
Perfect Forward Secrecy (PFS) 485
Diffie-Hellman key group 507
performance
troubleshooting 907
Personal Identification Number code, see PIN code
PFS (Perfect Forward Secrecy) 485, 507
physical ports
packet statistics 216, 217
PIN code 330
PIN generator 727
pointer record 791
policy enforcement in IPSec 483
policy routes 388
actions 389
and address objects 394
and ALG 437, 441
and HTTP redirect 430, 431
and interfaces 394
and NAT 388
and schedules 394, 528, 532
and service objects 717
and SMTP redirect 431
and trunks 373, 394
and user groups 393, 528, 532
and users 393, 528, 532
and VoIP pass through 437
and VPN connections 394, 909
benefits 388
criteria 389
L2TP VPN 518
overriding direct routes 390
troubleshooting 905, 911
POP
POP2 652
POP3 652
pop-up windows 39
port forwarding, see NAT
port groups 286
port roles 290, 291
and Ethernet interfaces 290, 291
and physical ports 290, 291
port translation, see NAT
Post Office Protocol, see POP 652
power off 900
PPP
troubleshooting 906
PPP interfaces
subnet mask 383
PPPoE 385
and RADIUS 385
TCP port 1723 386
PPPoE/PPTP interfaces 286, 317
and ISP accounts 318, 762
basic characteristics 286
gateway 318

subnet mask 318
PPTP
and GRE 386
as VPN 386
prefix delegation 289
proxy servers 430
web, see web proxy servers
PTR record 791
Public-Key Infrastructure (PKI) 746
public-private key pairs 745

Q

QoS 388, 524
Quick Start Guide 2

R

rack-mounting 36, 90
RADIUS 727, 728
advantages 727
and IKE SA 506
and PPPoE 385
and users 679
user attributes 705
RADIUS server 828, 831
troubleshooting 911
Real-time Transport Protocol, see RTP
Reference Guide, CLI 2
registration 266
reject (IDP)
both 593
receiver 593
sender 593
Relative Distinguished Name (RDN) 728, 730, 731
remote access IPSec 483
Remote Authentication Dial-In User Service, see RADIUS
remote management
FTP, see FTP
see also service control 796
Telnet 818
to-Device security policy 572
WWW, see WWW
remote network 473
replay detection 482
reports
collecting data 222
daily 843
daily e-mail 843
specifications 224
traffic statistics 222
reset 918
RESET button 918
Response Message 833
RFC
1058 (RIP) 399
1389 (RIP) 399
1587 (OSPF areas) 401
1631 (NAT) 398
1889 (RTP) 441
2131 (DHCP) 384
2132 (DHCP) 384
2328 (OSPF) 401
2402 (AH) 484, 507
2406 (ESP) 484, 507
2890 (GRE) 386
RIP 399
and Ethernet interfaces 296
and OSPF 399
and static routes 399
and to-ZyWALL security policyl 399
authentication 399
direction 296
redistribute 399
RIP-2 broadcasting methods 296
versions 296
vs OSPF 399
round robin 374
routing
troubleshooting 908
Routing Information Protocol, see RIP
routing protocols 398
and Ethernet interfaces 294
RSA 755, 761
RSSI threshold 280
RTP 441
see also ALG 441

S

schedule
  troubleshooting 912
schedules
  and content filtering 603
  and policy routes 394, 528, 532
  and security policy 528, 532, 546, 582
  one-time 721
  recurring 721
screen resolution 39
Secure Hash Algorithm, see SHA1
Secure Socket Layer, see SSL
security associations, see IPSec
security policy 571
  actions 582
  and address groups 546
  and address objects 546
  and ALG 435, 437
  and H.323 (ALG) 436
  and HTTP redirect 430
  and IPSec VPN 909
  and logs 582
  and NAT 573
  and schedules 528, 532, 546, 582
  and service groups 581
  and service objects 717
  and services 581
  and SIP (ALG) 436
  and user groups 582, 599
  and users 582, 599
  and VoIP pass through 437
  and zones 571, 576, 608
  asymmetrical routes 573, 575
  global rules 572
  priority 576, 608
  rule criteria 572
  see also to-Device security policy 571
  session limits 572, 596
  triangle routes 573, 575
  troubleshooting 905
security settings
  troubleshooting 904
sensitivity level 590
serial number 206
service control 796
  and to-ZyWALL security policy 796
  and users 797
  limitations 796
  timeouts 797
service groups 717
  and security policy 581
service objects 716
  and IP protocols 717
  and policy routes 717
  and security policy 717
service subscription status 269
services 716
  and security policy 581
Session Initiation Protocol 441
session limits 572, 596
session monitor (L2TP VPN) 256
sessions 225
sessions usage 209
SHA1 502
shell script
  troubleshooting 913
shell scripts 856
  and users 705
  downloading 874
  editing 873
  how applied 857
  managing 873
  syntax 857
  uploading 875
Short Message Service 832
shutdown 900
signal quality 239, 240
SIM card 330
Simple Mail Transfer Protocol, see SMTP 652
Simple Network Management Protocol, see SNMP
SIP 436, 441
  ALG 435
  and RTP 441
  and security policy 436
  media inactivity timeout 439
  signaling inactivity timeout 440
  signaling port 440
SMS 832
  Email-to-SMS 832
  send account information 832
SMS gateway 832
SMTP 652
SMTP redirect

and firewall 431
and policy routes 431
packet flow 431
SNAT 398
troubleshooting 908
SNMP 37, 822, 823
agents 823
and address groups 826
and address objects 826
and zones 826
authentication 827
Get 823
GetNext 823
Manager 823
managers 823
MIB 823, 824
network components 823
Set 823
Trap 823
traps 824
version 3 and security 823
versions 822
Source Network Address Translation, see SNAT
spam 651
spillover (for load balancing) 375
SSH 814
and address groups 816
and address objects 816
and certificates 816
and zones 816
client requirements 815
encryption methods 815
for secure Telnet 817
versions 815
SSL 511, 515, 797
access policy 511
and AAA 731
and AD 731
and LDAP 731
computer names 515
connection monitor 255
full tunnel mode 515
global setting 516
IP pool 515
network list 515
see also SSL VPN 511
troubleshooting 910
WINS 515
SSL policy
add 514
edit 514
objects used 512
SSL VPN 511
access policy 511
full tunnel mode 511
network access mode 35
see also SSL 511
troubleshooting 910
stac compression 765
startup-config.conf 864
if errors 860
missing at restart 860
present at restart 860
startup-config-bad.conf 860
static DHCP 461
static routes 388
and interfaces 397
and OSPF 402
and RIP 399
metric 397
statistics
daily e-mail report 843
traffic 222
status 204
stub area 401
subscription services
SSL VPN 155
SSL VPN, see also SSL VPN
status 269
supported browsers 39
syslog 852
syslog servers, see also logs
system log, see logs
system name 206, 780
system reports, see reports
system uptime 207
system-default.conf 864

T

TCP 716
attack packet 593
connections 716

port numbers 717
Telnet 818
and address groups 819
and address objects 819
and zones 819
with SSH 817
throughput rate
troubleshooting 913
time 782
time servers (default) 785
to-Device security policy
and remote management 572
global rules 571
see also security policy 571
token 727
to-ZyWALL security policy
and NAT 426
and NAT traversal (VPN) 909
and OSPF 401
and RIP 399
and service control 796
and VPN 909
TR-069 protocol 766
traffic statistics 222
Transmission Control Protocol, see TCP
transport encapsulation 484
Transport Layer Security (TLS) 821
triangle routes 573
allowing through the security policy 575
vs virtual interfaces 573
Triple Data Encryption Standard, see 3DES
troubleshooting 876, 903
admin user 911
bandwidth limit 907
cellular 906
certificate 912
configuration file 913
connection resets 908
content filter 904
DDNS 908
device access 903
ext-user 911
firmware upload 914
HTTP redirect 908
interface 905
Internet access 904, 911
IPSec VPN 909
LEDs 903
logo 913
logs 913
management access 913
packet capture 914
performance 907
policy routes 905, 911
PPP 906
problems 903
RADIUS server 911
routing 908
schedules 912
security policy 905
security settings 904
shell scripts 913
SNAT 908
SSL 910
SSL VPN 910
throughput rate 913
VLAN 906
VPN 910
WLAN 906
zipped files 907
trunks 286, 373
and ALG 441
and policy routes 373, 394
member interface mode 378, 380
member interfaces 378, 380
see also load balancing 373
Trusted Certificates, see also certificates 757
tunnel encapsulation 484
Tunnel interfaces 286

U

UDP 716
attack packet 593
messages 716
port numbers 717
Universal Plug and Play 144, 442
Application 442
security issues 443
unsolicited commercial e-mail 651
upgrading
firmware 868
uploading
configuration files 864

firmware 868
shell scripts 873
UPnP 442
UPnP-enabled Network Device
auto-discover 450
usage
CPU 209
flash 209
memory 209
onboard flash 209
sessions 209
user accounts
for WLAN 681
user authentication 679
external 679
local user database 728
user awareness 681
User Datagram Protocol, see UDP
user group objects 678
user groups 678, 680
and content filtering 603
and policy routes 393, 528, 532
and security policy 582, 599
user name
rules 682
user objects 678
user sessions, see sessions
user-authentication 547
users 678, 679
access, see also access users
admin (type) 679
admin, see also admin users
and AAA servers 679
and authentication method objects 679
and content filtering 603
and LDAP 679
and policy routes 393, 528, 532
and RADIUS 679
and security policy 582, 599
and service control 797
and shell scripts 705
attributes for Ext-User 680
attributes for LDAP 705
attributes for RADIUS 705
attributes in AAA servers 705
default lease time 700, 702
default reauthentication time 700, 702
default type for Ext-User 680
ext-group-user (type) 679
Ext-User (type) 679
ext-user (type) 679
groups, see user groups
Guest (type) 679
guest-manager (type) 679
lease time 686
limited-admin (type) 679
lockout 701
reauthentication time 686
types of 679
user (type) 679
user names 682

V

Vantage Report (VRPT) 852
virtual interfaces 286, 313
basic characteristics 286
not DHCP clients 383
types of 313
vs asymmetrical routes 573
vs triangle routes 573
Virtual Local Area Network, see VLAN.
Virtual Local Area Network. See VLAN.
Virtual Private Network, see VPN
virus
attack 154
VLAN 333, 340
advantages 340
and MAC address 340
ID 340
troubleshooting 906
VLAN interfaces 286, 341
and Ethernet interfaces 341, 906
basic characteristics 286
virtual 313
VoIP pass through 441
and NAT 437
and policy routes 437
and security policy 437
see also ALG 435
VPN 473
active protocol 507
and NAT 505
basic troubleshooting 909

hub-and-spoke, see VPN concentrator
IKE SA, see IKE SA
IPSec 473
IPSec SA
proposal 501
security associations (SA) 475
see also IKE SA
see also IPSec 473
see also IPSec SA
troubleshooting 910
VPN concentrator 495
advantages 495
and IPSec SA policy enforcement 497
disadvantages 495
VPN connections
and address objects 478
and policy routes 394, 909
VPN gateways
and certificates 478
and extended authentication 478
and interfaces 478
and to-ZyWALL security policy 909
VRPT (Vantage Report) 852

W

wall-mounting 91
warranty 935
note 935
Web Configurator 36
access 39
access users 702
requirements 39
supported browsers 39
web features
ActiveX 624
cookies 624
Java 624
web proxy servers 624
web proxy servers 430, 624
weighted round robin (for load balancing) 375
weighted round robin algorithm 469
white list (anti-spam) 651, 655, 659, 660
Windows Internet Naming Service, see WINS
Windows Internet Naming Service, see WINS.
WINS 309, 351, 365, 385, 515
in L2TP VPN 520
WINS server 309, 520
Wizard Setup 58, 158
WLAN
troubleshooting 906
user accounts 681
WLAN interfaces 286
worm 154
WWW 798
and address groups 802
and address objects 802
and authentication method objects 801
and certificates 800
and zones 802
see also HTTP, HTTPS 798

Z

zipped files
troubleshooting 907
ZON
utility 242, 836
zones 675
and FTP 821
and interfaces 675
and security policy 571, 576, 608
and SNMP 826
and SSH 816
and Telnet 819
and VPN 675
and WWW 802
extra-zone traffic 676
inter-zone traffic 676
intra-zone traffic 676
types of traffic 676
Zyxel One Network (ZON) 242