ZYXEL NETWORKS

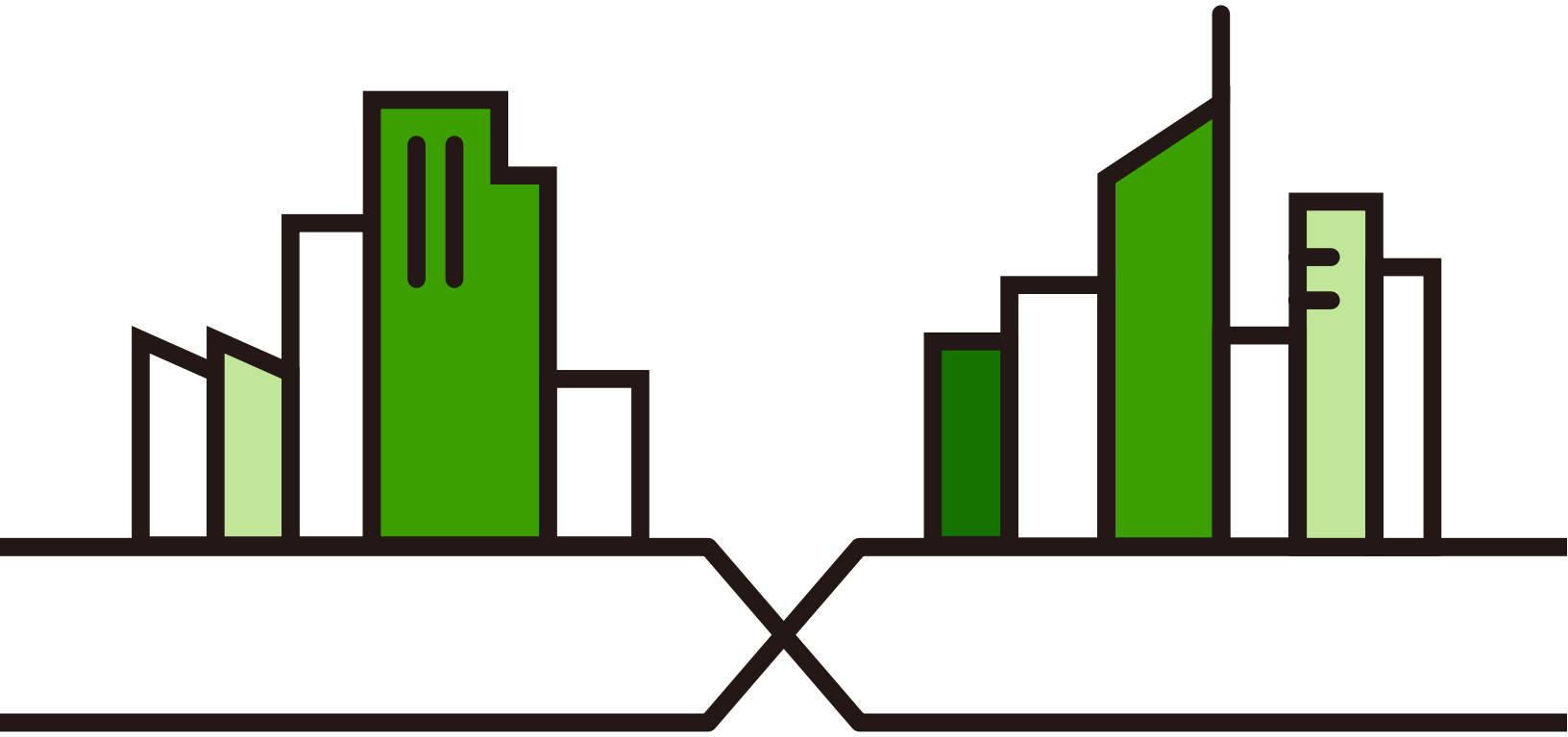
User's Guide

USG FLEX H Series

Default Login Details

Login IP Address	https://192.168.168.1
User Name	admin
Password	See Zyxel Device label or 1234
WAN	P1 or P2 (see Table 12 on page 59)
LAN	P3 or P4 (see Table 12 on page 59)

Version 1.39 Edition 1, 7/2026



Copyright © 2026 Zyxel and/or its affiliates. All Rights Reserved.

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.

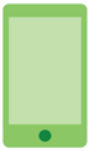
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

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, **Network > Interface > Ethernet** means you first click **Network**, then the **Interface** sub menu and finally the **Ethernet** tab to get to that screen.

Icons Used in Figures

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

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

Contents Overview

Introduction 19
Initial Setup Wizard 43
Hardware, Interfaces and Zones 58
Dashboard 74
Monitor 85
Licensing 123
Interfaces 130
Routing 179
NAT 190
BWM (Bandwidth Management) 198
ALG 211
Multicast 215
IPSec VPN 220
SSL VPN 268
Tailscale 277
Security Policy 287
Captive Portal 311
Object 324
Application Patrol 350
Content Filtering 361
Reputation Filter 391
Anti-Malware 411
Sandbox 422
IPS 426
IP Exception 438
SSL Inspection 443
External Block Lists 454
User & Authentication 459
Wireless 498
System 564
Log and Report 638
Firmware/File Manager 656
Diagnostics 672
AP Diagnostics 684
Packet Flow Explore 691
Reboot/Shutdown 705
Troubleshooting 708

Table of Contents

Document Conventions 2

Contents Overview 3

Table of Contents 4

Part I: User's Guide 18

Chapter 1
Introduction 19

1.1 Overview 19
1.1.1 Major Model Features 19
1.1.2 Fast-path Acceleration 20
1.2 Registration at Nebula Control Center (NCC) 20
1.3 Licenses 20
1.3.1 License Priority 21
1.3.2 Grace Period 21
1.4 Applications 21
1.4.1 Security Router 21
1.4.2 VPN Connectivity 22
1.4.3 User-Aware Access Control 22
1.4.4 Load Balancing 23
1.5 Management Overview 23
1.6 Web Configurator 25
1.6.1 Web Configurator Access 25
1.6.2 Security Best Practices 26
1.6.3 Remote Access to the Zyxel Device Networks 30
1.6.4 Web Configurator Screens Overview 30
1.6.5 Navigation Panel 33
1.6.6 Tables and Lists 40
1.6.7 Error /Warning Messages 41

Chapter 2
Initial Setup Wizard 43

2.1 Initial Setup Wizard Overview 43
2.1.1 Terms of Use/Privacy Policy/Firmware Upgrade Notification 43
2.2 Initial Configuration 44
2.2.1 Initial Configuration With Nebula 45

2.2.2 Initial Configuration With Web Configurator 45
2.3 Wizard - Connect to the Internet 47
2.3.1 Interface Type - DHCP 47
2.3.2 Interface Type - Static 48
2.3.3 Interface Type - PPPoE 49
2.4 Wizard - System Time 50
2.5 Wizard - Device Registration 51
2.5.1 Exit the Wizard 52
2.6 Wizard - License Summary 54
2.7 Wizard - Subnet Planning 54
2.8 Finish 56

Chapter 3
Hardware, Interfaces and Zones 58

3.1 Hardware Overview 58
3.1.1 Multi-Gigabit 58
3.1.2 Default Physical Port – Interface Mapping 59
3.1.3 PoE 59
3.1.4 Front Panels 61
3.1.5 Rear Panels 64
3.1.6 Console Port Pin Connectors 66
3.2 Installation Scenarios 67
3.2.1 Desktop Installation Procedure 67
3.2.2 Rack-mounting 68
3.2.3 Wall-mounting 69
3.3 Power Cord Lock 71
3.3.1 Procedure A 71
3.3.2 Procedure B 72

Chapter 4
Dashboard 74

4.1 Dashboard Overview 74
4.1.1 What You Can Do in this Chapter 74
4.2 The System Screen 74
4.2.1 System Information Screen 75
4.2.2 Port Status Screen 77
4.2.3 Resource Usage Screen 78
4.2.4 Bandwidth 80
4.2.5 Client Usage Screen 81
4.2.6 The Latest Logs Screen 81
4.3 The Security Screen 82

Part II: Technical Reference 84

Chapter 5
Monitor 85

5.1 Overview 85
5.1.1 What You Can Do in this Chapter 85
5.1.2 What You Need to Know 86
5.2 The Application Usage Screen 86
5.3 The Port Statistics Screen 88
5.4 The Interface Statistics Screen 89
5.5 The Session Monitor Screen 91
5.6 The Content Filter Screen 93
5.7 The Reputation Filter Screens 94
5.7.1 IP Reputation 95
5.7.2 DNS Threat Filter 96
5.7.3 URL Threat Filter 97
5.8 The IPS Screen 98
5.9 The Anti-Malware Screen 100
5.10 The Sandbox Screen 101
5.11 The SSL Inspection Screens 102
5.11.1 The Summary Screen 102
5.11.2 The Certificate Cache List Screen 104
5.12 The Interface Screen 104
5.13 The Device Insight Screen 106
5.14 The Login Users Screen 109
5.15 The Lockout IPs Screen 110
5.16 The DHCP Table Screen 111
5.17 The IPSec VPN Screen 114
5.17.1 The Site to Site VPN Screen 114
5.17.2 The Remote Access VPN Screen 115
5.18 The SSL VPN Screen 116
5.18.1 Regular Expressions in Searching IPSec Policies 117
5.19 The Tailscale Screen 117
5.20 The Access Points Screen 118
5.20.1 The Top N APs Screen 119
5.20.2 The Single AP Screen 120
5.21 The WLAN Clients Screen 121
5.21.1 The Top N Stations Screen 121
5.21.2 The Single Station Screen 121

Chapter 6
Licensing 123

6.1 Licensing Overview 123

6.1.1 What you Need to Know 123
6.1.2 The Licenses Screen 124
6.1.3 The Signature Update Screen 127
6.1.4 Signature Update 128
6.1.5 Auto Update 128

Chapter 7
Interfaces 130

7.1 Interface Overview 130
7.1.1 What You Can Do in this Chapter 130
7.1.2 What You Need to Know 131
7.2 Interface Screen 139
7.2.1 Interface Screen Warning Messages 139
7.3 External Interface 142
7.3.1 External Interface Add/Edit 142
7.4 Internal Interface 150
7.4.1 Internal Interface Add/Edit 150
7.5 General Interface 158
7.5.1 Add/Edit DHCP Extended Options 164
7.6 VTI Interface 166
7.6.1 Restrictions for IPSec Virtual Tunnel Interface 166
7.6.2 VTI Edit 167
7.7 Trunk Overview 169
7.7.1 What You Need to Know 172
7.8 The Trunk Summary Screen 173
7.8.1 Configuring a User-Defined Trunk 174
7.8.2 Configuring the System Default Trunk 175
7.9 Port 176

Chapter 8
Routing 179

8.1 Policy and Static Routes Overview 179
8.1.1 What You Can Do in this Chapter 179
8.1.2 What You Need to Know 179
8.2 Policy Route Screen 181
8.2.1 Policy Route Edit Screen 183
8.3 Static Route Screen 187
8.3.1 Static Route Add/Edit Screen 188

Chapter 9
NAT 190

9.1 NAT Overview 190
9.1.1 What You Can Do in this Chapter 190

9.1.2 What You Need to Know 190
9.2 The NAT Screen 193
9.2.1 The NAT Add/Edit Screen 194

Chapter 10
BWM (Bandwidth Management) 198

10.1 Overview 198
10.1.1 What You Can Do in this Chapter 198
10.1.2 What You Need to Know 198
10.2 The Bandwidth Management Configuration 201
10.2.1 The Bandwidth Management Add/Edit Screen 203
10.2.2 Adding Objects for the BWM Policy 206
10.3 Example: Prioritize a Specific Application 210

Chapter 11
ALG 211

11.1 ALG Overview 211
11.1.1 What You Need to Know 211
11.1.2 Before You Begin 212
11.2 The ALG Screen 212

Chapter 12
Multicast 215

12.1 Multicast Overview 215
12.1.1 What You Need to Know 215
12.2 The Multicast Screen 217

Chapter 13
IPSec VPN 220

13.1 Virtual Private Networks (VPN) Overview 220
13.2 IPSec VPN Background Information 221
13.2.1 IKE SA Overview 221
13.2.2 Additional Topics for IKE SA 226
13.2.3 Recommended VPN Algorithm Table 230
13.2.4 Additional Topics for IPSec SA 231
13.2.5 What You Can Do in this Chapter 231
13.2.6 What You Need to Know 231
13.3 The Site to Site VPN Screen 232
13.3.1 The Site to Site VPN Add/Edit Screen- Wizard 233
13.3.2 The Site to Site VPN Add/Edit Screen - Custom 238
13.4 The Remote Access VPN Screen 248
13.5 Remote Access VPN Setup Example 253
13.5.1 Zyxel Device Setup 254

13.5.2 Home User Setup 260
13.5.3 Test the VPN Connection 267

Chapter 14
SSL VPN 268

14.1 Overview 268
14.1.1 What You Can Do in this Chapter 268
14.1.2 What You Need to Know 268
14.2 The SSL VPN Screen 269
14.2.1 Add/Edit Client Profile 274

Chapter 15
Tailscale 277

15.1 Overview 277
15.1.1 What You Can Do in this Chapter 277
15.1.2 What You Need to Know 277
15.2 The Tailscale Screen 278
15.2.1 Set Up a Tailscale Network 279

Chapter 16
Security Policy 287

16.1 Overview 287
16.2 What You Can Do in this Chapter 287
16.2.1 What You Need to Know 288
16.3 The Security Policy Screen 289
16.3.1 Configuring the Security Policy Control Screen 290
16.3.2 The Policy Control Add/Edit Screen 293
16.3.3 Example: Allow a Server to Ping the Zyxel Device Without Creating Logs 294
16.4 DoS Prevention Overview 296
16.4.1 The DoS Prevention Policy Screen 297
16.4.2 The DoS Prevention Profile Screen 298
16.4.3 The Dos Prevention Profile Add/Edit Screen 299
16.5 IP Spoofing Prevention Overview 303
16.5.1 The IP Spoofing Prevention Screen 304
16.5.2 The Trusted IP Add / Edit Screen 305
16.6 The Session Control Screen 305
16.6.1 The Session Control Add/Edit Screen 307
16.7 Security Policy Example Applications 308

Chapter 17
Captive Portal 311

17.1 Overview 311
17.2 What You Can Do in This Chapter 311

17.2.1 What You Need to Know 311
17.3 Authentication Policy Overview 312
17.3.1 The Policy Screen 312
17.3.2 The Policy Add/Edit Screen 313
17.3.3 The Settings Screen 320
17.4 Captive Portal Client Sign-In Steps 321

Chapter 18
Object 324

18.1 Address/Geo IP Overview 324
18.1.1 What You Need To Know 324
18.1.2 Address Summary Screen 324
18.1.3 Address Group Summary Screen 327
18.1.4 Geo IP Summary Screen 330
18.2 Service Overview 333
18.2.1 What You Need to Know 333
18.2.2 The Service Summary Screen 335
18.2.3 The Service Group Summary Screen 338
18.3 Zone Overview 340
18.3.1 What You Need to Know 341
18.3.2 The Zone Screen 342
18.4 Schedule Overview 344
18.4.1 What You Need to Know 344
18.4.2 The Schedule Screen 344
18.4.3 The Schedule Group Screen 348

Chapter 19
Application Patrol 350

19.1 Overview 350
19.1.1 What You Can Do in this Chapter 350
19.1.2 What You Need to Know 350
19.2 Application Patrol Profile 351
19.2.1 Application Patrol Profile > Add/Edit - Application Management 353
19.3 Example: Block an Application 355

Chapter 20
Content Filtering 361

20.1 Overview 361
20.1.1 What You Can Do in this Chapter 361
20.1.2 What You Need to Know 361
20.2 Content Filtering General Screen 364
20.2.1 HSTS and QUIC 365
20.2.2 Content Filtering Add Profile 367

20.2.3 Content Filtering Profile (Allow List) 382
20.2.4 Content Filtering Profile (Block List) 383
20.2.5 Content Filtering Profile (Blocked URL Keywords) 384
20.2.6 Content Filtering Profile (Test Web Site Category) 385
20.3 Content Filtering Example: Block LAN Users 386

Chapter 21
Reputation Filter 391

21.1 Overview 391
21.1.1 What You Need to Know 391
21.1.2 What You Can Do in this Chapter 392
21.2 IP Reputation Screen 392
21.2.1 IP Reputation Allow List 395
21.2.2 IP Reputation Block List 396
21.2.3 IP Reputation SecuReporter Allow List 397
21.3 DNS Threat Filter Screen 399
21.3.1 DNS Threat Filter Allow List 402
21.3.2 DNS Threat Filter Block List 403
21.3.3 DNS Threat Filter SecuReporter Allow List 404
21.4 URL Threat Filter Screen 405
21.4.1 URL Threat Filter Allow List 407
21.4.2 URL Threat Filter Block List 408
21.4.3 URL Threat Filter SecuReporter Allow List 409

Chapter 22
Anti-Malware 411

22.1 Overview 411
22.1.1 What You Can Do in this Chapter 414
22.2 Anti-Malware Screen 414
22.3 The Allow List Screen 416
22.4 The Block List Screen 418
22.5 Anti-Malware Technical Reference 420

Chapter 23
Sandbox 422

23.1 Overview 422
23.1.1 What You Need to Know 422
23.2 Sandbox Screen 423

Chapter 24
IPS 426

24.1 Overview 426
24.1.1 What You Can Do in this Chapter 426

24.1.2 What You Need To Know 426
24.2 The IPS Screen 428
24.2.1 Query Example 434
24.3 The Allow List Screen 435
24.4 IPS Technical Reference 436

Chapter 25
IP Exception 438

25.1 Overview 438
25.2 The IP Exception Screen 439
25.2.1 The IP Exception Add/Edit Screen 440
25.3 Example: Bypass a Website 441

Chapter 26
SSL Inspection 443

26.1 Overview 443
26.1.1 What You Can Do in this Chapter 443
26.1.2 What You Need To Know 443
26.1.3 What You Can Do in this Chapter 444
26.1.4 Before You Begin 444
26.2 The SSL Inspection Profile Screen 444
26.2.1 Add/Edit SSL Inspection Profiles 446
26.3 Exclude List Screen 448
26.4 Certificate Update Screen 450
26.5 Install a CA Certificate in a Browser 451

Chapter 27
External Block Lists 454

27.1 Overview 454
27.1.1 IP Reputation External Block List Screen 454
27.1.2 DNS / URL Threat Filter External Block List Screen 456

Chapter 28
User & Authentication 459

28.1 User/Group Overview 459
28.1.1 What You Need To Know 459
28.1.2 NCAS 461
28.1.3 NID FS 462
28.1.4 User/Group User Summary Screen 463
28.1.5 User Add/Edit Screen 464
28.1.6 User/Group Group Summary Screen 471
28.1.7 User/Group Setting Screen 473
28.2 User Authentication Overview 477

28.2.1 What You Need To Know 478
28.3 AAA Server Overview 480
28.3.1 AAA Server Configuration 480
28.3.2 Add an AD Server 482
28.3.3 Join an AD Domain 484
28.3.4 Add an LDAP Server 485
28.3.5 Add an OIDC Server 487
28.3.6 Add a RADIUS Server 491
28.4 Two-Factor Authentication Overview 493
28.4.1 User Authentication Two-Factor Authentication 494
28.5 Advanced 496

Chapter 29
Wireless 498

29.1 Overview 498
29.1.1 What You Can Do in this Chapter 498
29.1.2 What You Need to Know 499
29.2 The AP Control Service Screen 509
29.3 The AP List Screen 510
29.3.1 The AP List > Managed AP Screen 511
29.3.2 The AP List > Unmanaged AP Screen 515
29.3.3 Edit AP List 515
29.4 The Policy Screen 521
29.5 The AP Firmware Screen 522
29.6 The Client List Screen 524
29.6.1 The WLAN Clients > Client List > All Clients Screen 524
29.6.2 The WLAN Clients > All Clients > Client List > Policy Screen 525
29.6.3 The WLAN Clients > Client List > All Clients > Add Policy Clients Screen 526
29.6.4 The WLAN Clients > Client List > Policy Clients Screen 528
29.6.5 The WLAN Clients > Client List > Policy Clients > Add Policy Screen 529
29.6.6 The WLAN Clients > Client List > Policy Clients > Add Policy Clients Screen 530
29.7 The WiFi Aid Screen 531
29.8 The Connection Log Screen 534
29.9 The SSID Settings Screen 535
29.9.1 The SSID Advanced Settings Screen 537
29.9.2 Edit SSID Advanced Settings 538
29.10 The Radio Settings Screen 543
29.10.1 The Wireless > WLAN Settings > Radio Settings > Edit Band Screen 548
29.11 The AP Settings Screen 551
29.11.1 The Wireless > WLAN Settings > AP Settings > Edit AP Screen 554
29.12 The AP Group Settings Screen 555
29.13 The Wireless Health Screen 556
29.14 The SSID Info Screen 557

29.15 The Rogue AP Detection Screen 558
29.16 Wireless Application Example 560
29.17 Wireless Technical Reference 562

Chapter 30
System 564

30.1 Overview 564
30.1.1 What You Can Do in this Chapter 564
30.2 Settings 564
30.2.1 System Settings 565
30.2.2 System Time 565
30.2.3 Administration Settings 565
30.2.4 Settings 567
30.3 Device HA (High Availability) 570
30.3.1 What You Can Do in These Screens 571
30.3.2 Heartbeat 571
30.3.3 GARP and Virtual IP / MAC Address 572
30.3.4 Preparing to Deploy Device HA 573
30.3.5 Using NCC To Manage Device HA 573
30.3.6 Deployment Overview 573
30.3.7 HA Status 574
30.3.8 HA Configuration 576
30.3.9 HA Log 578
30.3.10 Firmware Upgrade on Paired Zyxel Devices 580
30.3.11 Disabling Device HA 580
30.4 DNS & DDNS 581
30.4.1 DNS Server Address Assignment 582
30.4.2 The DNS Screen 582
30.4.3 Address/PTR Record 585
30.4.4 Adding an Address/PTR Record 585
30.4.5 CNAME Record 586
30.4.6 Adding a CNAME Record 586
30.4.7 MX Record 587
30.4.8 Adding a MX Record 587
30.4.9 Domain Zone Forwarder 587
30.4.10 Adding a Domain Zone Forwarder 587
30.4.11 Security Option Control 588
30.4.12 Editing a Security Option Control 588
30.4.13 The DDNS Screen 589
30.4.14 The DDNS Add/Edit Screen 591
30.5 SNMP 596
30.5.1 SNMPv3 and Security 597
30.5.2 Supported MIBs 597

30.5.3 SNMP Traps 597
30.5.4 Configuring SNMP 598
30.5.5 Add SNMP V3 User 600
30.6 Notification 601
30.6.1 The Mail Server Screen 601
30.6.2 The Alert Screen 606
30.7 Certificate Overview 609
30.7.1 What You Need to Know 610
30.7.2 Verifying a Certificate 611
30.8 My Certificates 612
30.8.1 The My Certificates Add Screen 614
30.8.2 The My Certificates Edit Screen 617
30.8.3 The My Certificates Import Screen 619
30.9 Trusted Certificates 621
30.9.1 The Trusted Certificates Edit Screen 622
30.9.2 The Trusted Certificates Import Screen 624
30.10 Let's Encrypt Certificate 625
30.10.1 The Let's Encrypt Certificate Add Screen 626
30.11 Advanced 629
30.11.1 SecuManager v3 630
30.11.2 Advanced System Screen 630
30.12 External Integrations 633
30.12.1 Avast 634
30.12.2 AnyInsight 636

Chapter 31
Log and Report 638

31.1 Overview 638
31.1.1 What You Can Do In this Chapter 638
31.2 Log/Events Screens 638
31.2.1 System Logs 638
31.2.2 Log Details 642
31.2.3 APC Logs 642
31.2.4 AP Logs 645
31.3 Log Settings Screen 647
31.4 SecuReporter 650
31.5 Email Daily Report 652
31.5.1 Example Reports 654

Chapter 32
Firmware/File Manager 656

32.1 Overview 656
32.1.1 What You Can Do in this Chapter 656

32.1.2 What you Need to Know 656
32.1.3 Configuration File Flow at Restart 656
32.2 The Configuration File Screen 657
32.2.1 Example: Back Up and Restore Zyxel Device Configuration 664
32.3 Firmware Management 666
32.3.1 Cloud Helper 666
32.3.2 The Firmware Management Screen 667
32.4 The CLI Script Screen 669
32.4.1 CLI Script File Command Rules and Examples 670

Chapter 33
Diagnostics 672

33.1 Overview 672
33.1.1 What You Can Do in this Chapter 672
33.2 The Diagnostics Screens 672
33.2.1 The Diagnostics Screen 672
33.3 The Packet Capture Screen 674
33.3.1 The Packet Capture Edit Screen 675
33.4 The CPU / Memory Status Screen 678
33.5 The System Log Screen 680
33.6 The Network Tool Screen 681

Chapter 34
AP Diagnostics 684

34.1 Overview 684
34.1.1 What You Can Do in this Chapter 684
34.2 Diagnostics Screen 684
34.3 Packet Capture Screen 685
34.3.1 Packet Capture Edit Screen 687
34.4 Remote Capture Screen 688

Chapter 35
Packet Flow Explore 691

35.1 Overview 691
35.1.1 What You Can Do in this Chapter 691
35.2 Routing Status 691
35.3 The SNAT Status Screen 698
35.4 Route Traces 702

Chapter 36
Reboot/Shutdown 705

36.1 Overview 705
36.2 The Reboot/Shutdown Screen 705

Part III: Appendices and Troubleshooting 707

Chapter 37
Troubleshooting 708

37.1 Reserved System Ports 724
37.2 Resetting the Zyxel Device 724
37.3 Restarting the Zyxel Device 726
37.4 Getting More Troubleshooting Help 726

Appendix A Zyxel Account Authentication 727

Appendix B Customer Support 755

Appendix C Product Features 760

Appendix D Legal Information 766

Index 775

PART I
User's Guide

CHAPTER 1
Introduction

1.1 Overview

Zyxel Device refers to these models as outlined below.

- USG FLEX 50H
- USG FLEX 100H
- USG FLEX 200H
- USG FLEX 500H
- USG FLEX 50HP
- USG FLEX 100HP
- USG FLEX 200HP
- USG FLEX 700H

1.1.1 Major Model Features

The following table lists the key features these models support:

Table 1 Zyxel Device Model Feature Comparison

FEATURE/ MODEL	USG FLEX 50H	USG FLEX 50HP	USG FLEX 100H	USG FLEX 100HP	USG FLEX 200H	USG FLEX 200HP	USG FLEX 500H	USG FLEX 700H
DoS Prevention	YES	YES	YES	YES	YES	YES	YES	YES
IPS	YES	YES	YES	YES	YES	YES	YES	YES
Anti-Malware	YES	YES	YES	YES	YES	YES	YES	YES
App Patrol	YES	YES	YES	YES	YES	YES	YES	YES
Content Filtering	YES	YES	YES	YES	YES	YES	YES	YES
SecuReporter	YES	YES	YES	YES	YES	YES	YES	YES
Reputation Filter	YES	YES	YES	YES	YES	YES	YES	YES
Sandboxing	YES	YES	YES	YES	YES	YES	YES	YES
Device Insight	YES	YES	YES	YES	YES	YES	YES	YES
IP Exception	YES	YES	YES	YES	YES	YES	YES	YES
SSL encrypted	YES	YES	YES	YES	YES	YES	YES	YES
Bundled Security Feature License	1 year	1 year	1 year	1 year	1 year	1 year	1 year	1 year
Management by Nebula Cloud Center	YES	YES	YES	YES	YES	YES	YES	YES
Device HA	NO	NO	NO	NO	YES	YES	YES	YES

- See Table 9 on page 58 for a comparison of hardware ports.
- See the Product Features appendix for a more detailed comparison of features.
- See the product's datasheet for detailed information on a specific model.

- For information on interface names by model, default port or interface name mapping, and default interface or zone mapping please see Section 3.1.2 on page 59.
- You can configure these features indirectly using the Nebula Control Center or directly using the Web Configurator.

1.1.2 Fast-path Acceleration

Fast-path Acceleration is a way to speed up certain traffic such as NAT, IPSec VPN, Security policies through the Zyxel Device by bypassing the kernel. SSL VPN traffic does not use fast-path acceleration.

1.2 Registration at Nebula Control Center (NCC)

Nebula Control Center (NCC) is an Internet portal that allows you to configure and monitor groups of Zyxel Devices in organizations. You must register your Zyxel Device at NCC to use security services and upgrade firmware. See **Licensing** > **Licenses** for security services available for your Zyxel Device.

Use NCC to monitor and manage your Zyxel Device. Use the web configurator to configure the Zyxel Device settings.

Run the initial setup wizard to register your Zyxel Device at NCC. Or you can follow the steps below to register your Zyxel Device at NCC.

1. Log into NCC (https://nebula.zyxel.com) with your Zyxel Account. If you do not have a Zyxel Account, you should click **Create an account** to create one.
2. After you log in, click **Go** under NCC 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 Zyxel Device MAC address and serial number 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.

   If you did not register your Zyxel Device at NCC, you will see a reminder to register every time you log into the Zyxel Device web configurator with an admin account.

1.3 Licenses

When you purchase a new Zyxel Device, it may comes with a Gold Security Pack (GSP) or an Entry Defense Pack (EDP) license. See **Licensing** > **Licenses** for the latest services available for your Zyxel Device.

An Entry Defense Pack license consists of the following services at the time of writing.

- Reputation Filter
- SecuReporter
- Nebula Professional Pack

A Gold Security Pack license consists of the following services at the time of writing.

- Anti -Malware
- Application Patrol
- Device Insight
- IPS (Intrusion Prevention System).
- Nebula Professional Pack
- Reputation Filter, including IP Reputation, URL Threat Filter, DNS Threat Filter services and External Blocking Lists (EBL) for these services
- Sandboxing
- Security Profile Sync - Use NCC to apply the same security settings to all Firewalls in the same organization
- SecuReporter
- Web Filtering (Content Filtering)

1.3.1 License Priority

New licenses queue until existing licenses expire. If you buy a new Gold Security Pack, these licenses will be used only after licenses in the existing Gold Security Pack expire.

When a service is included in multiple packs, Zyxel management system determines license activation priority by license type, and then by license scope.

1 **License Type:** Depending on how the license is obtained.

   Priority: Trial License > Bundled License > Purchased License

2 **License Scope:** The service from the license with the biggest pack is applied first.

   Priority: Big pack > Small pack > Individual Service License

1.3.2 Grace Period

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

Please note that a trial license does not have a grace period.

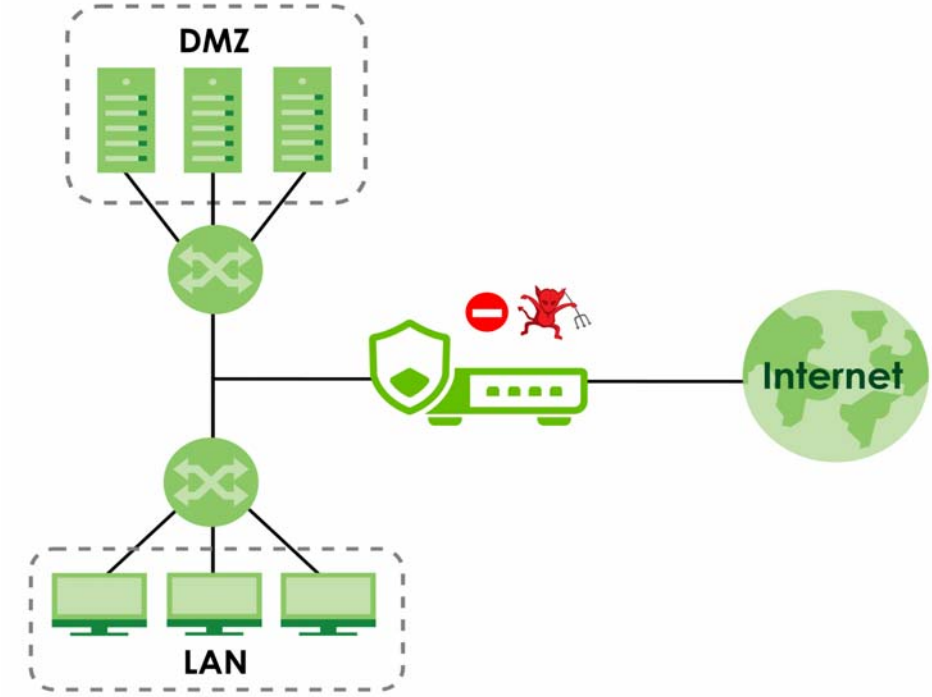
1.4 Applications

These are some Zyxel Device application scenarios.

1.4.1 Security Router

Security includes a Stateful Packet Inspection (SPI) firewall.

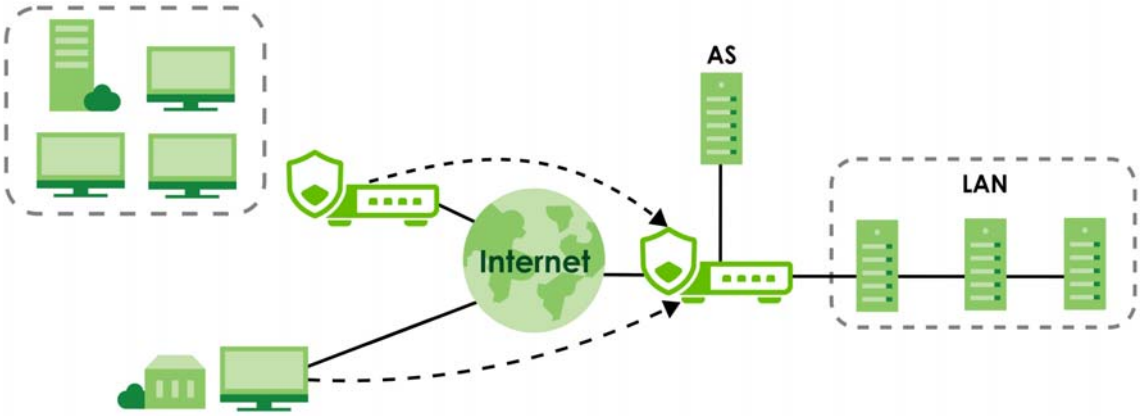
Figure 1 Applications: Security Router Applications: Security Router



1.4.2 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.

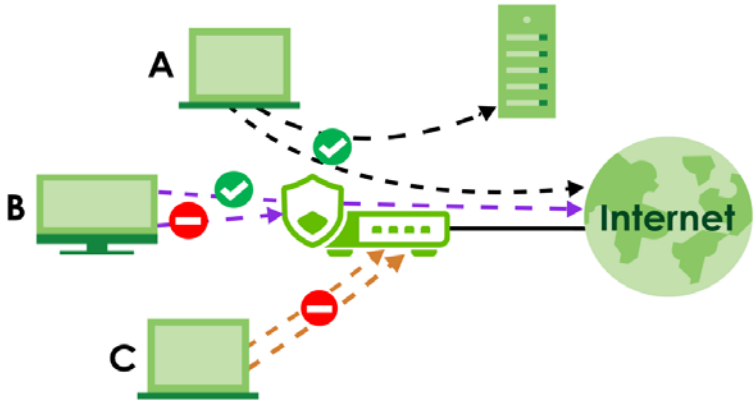
Figure 2 Applications: VPN Connectivity



1.4.3 User-Aware Access Control

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

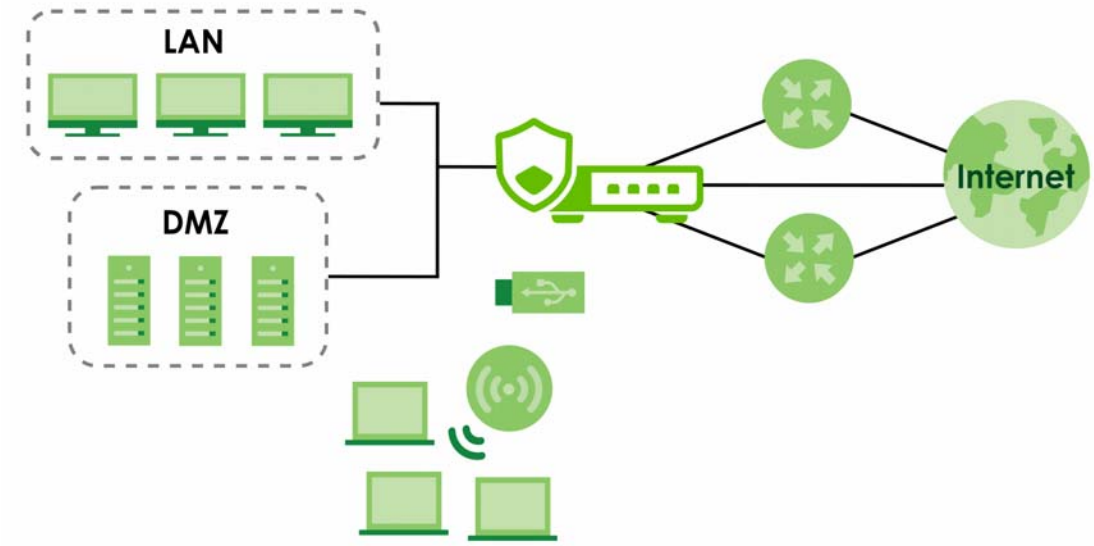
Figure 3 Applications: User-Aware Access Control



1.4.4 Load Balancing

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

Figure 4 Applications: Multiple WAN Interfaces



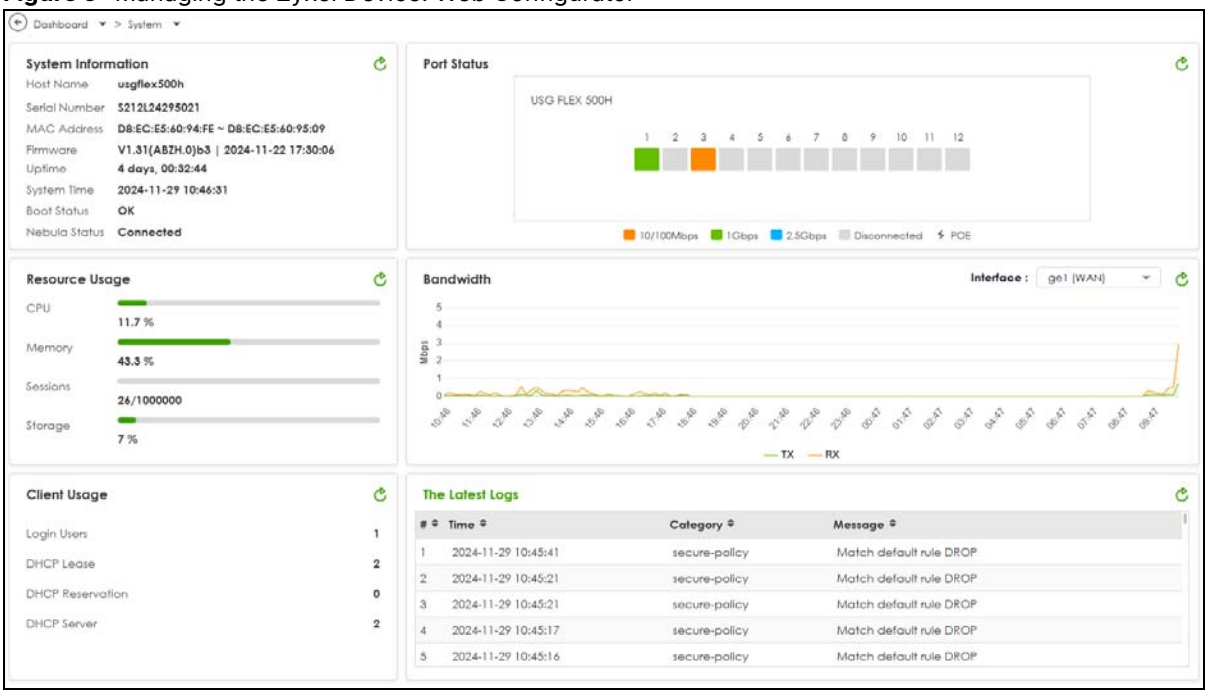
1.5 Management Overview

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 5 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 via the physical port. See the Command Reference Guide for CLI details. The default settings for the console port are:

Table 2 Console Port Default Settings

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

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 30.5 on page 596.

Management Authentication

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

- Local Zyxel Device authentication

- An external RADIUS server
- Certificates

1.6 Web Configurator

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).

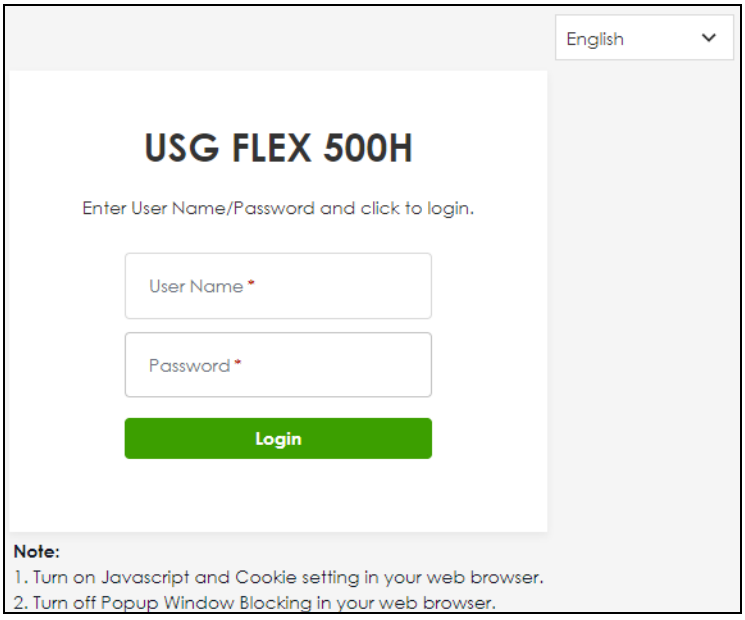
The recommended minimum screen resolution is 1366 x 768 pixels.

Note: Screenshots and graphics in this book may differ slightly from your product due to differences in product features.

1.6.1 Web Configurator Access

1 Make sure your Zyxel Device hardware is properly connected. See the Quick Start Guide.

2 In your browser go to *https://192.168.168.1*. By default, the Zyxel Device automatically routes this request to its HTTPS server, and it is recommended to keep this setting. The **Login** screen appears.



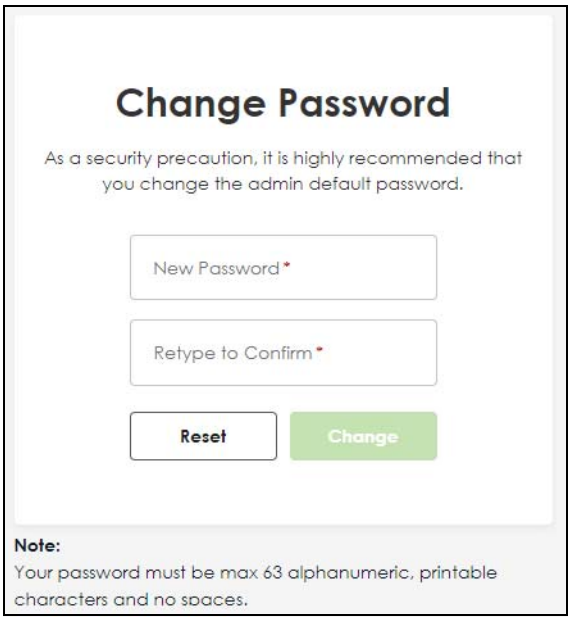
3 Select a display language for the Zyxel Device's web configurator screens in the upper right of the screen. The following are the languages supported at the time of writing.



4 Type the user name (default: “admin”) and password (default: “1234” or see the label on the back of the Zyxel Device).

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

Make a note of your new password, enter it in the following screen, then click **Apply**. The **Login** screen appears again. Log in with your new password.

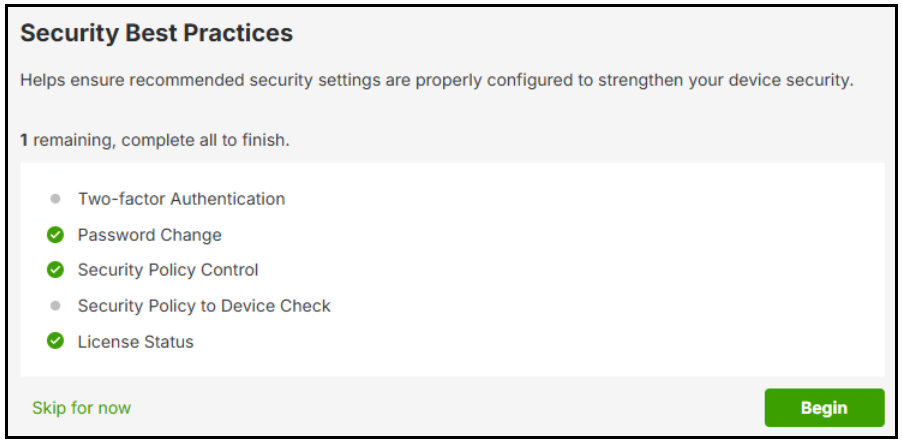


1.6.2 Security Best Practices

For a secure network, we recommend access to the Zyxel Device with two-factor authentication, regularly changing your password, enabling **Security Policy**, restricting access from WAN, and checking license status.

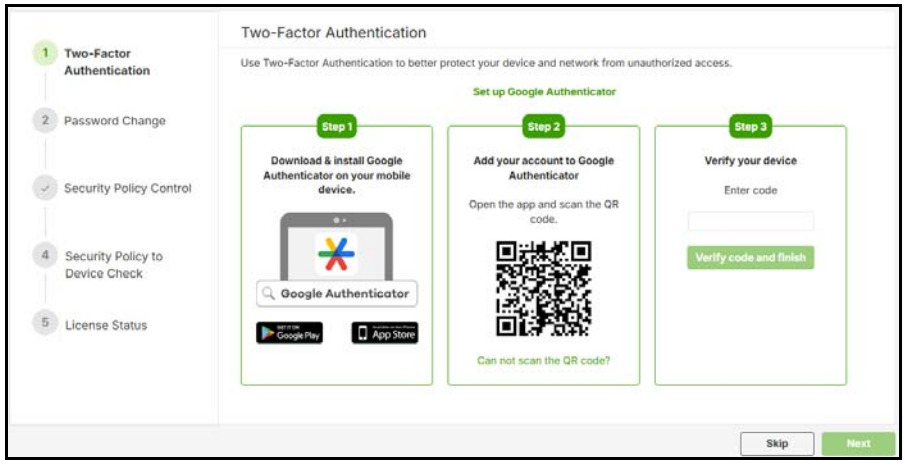
The **Security Best Practices** screen appears after each login to remind you of the recommended security settings. Click **Begin** to start the setup. A checkmark indicates that this check is not done as it's enabled by default (Security Policy) or the check was done before.

Note: If you do not want the **Security Best Practice** wizard to appear after each login, go to **System > Advanced** and disable the **Security Best Practice Wizard** under **Additional Features**.



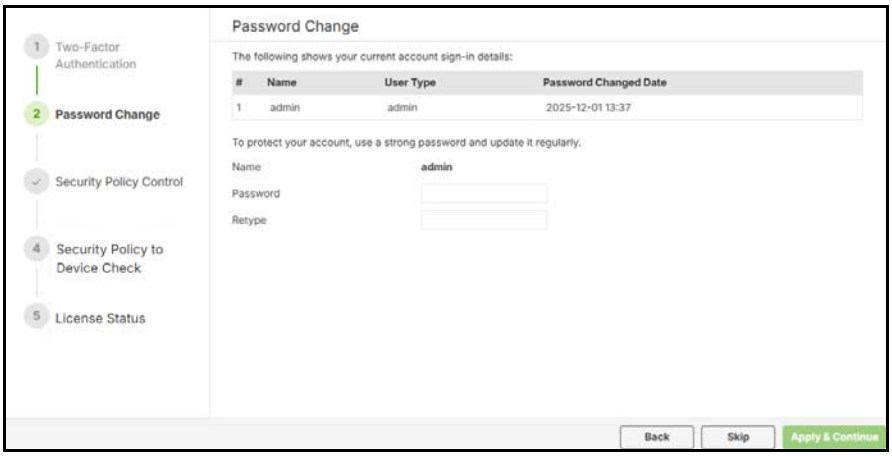
Two-Factor Authentication

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 Section 28.4 on page 493 for more information.



Password Change

Change your local administrator password every 60 days to enhance security and reduce the risk of unauthorized access.



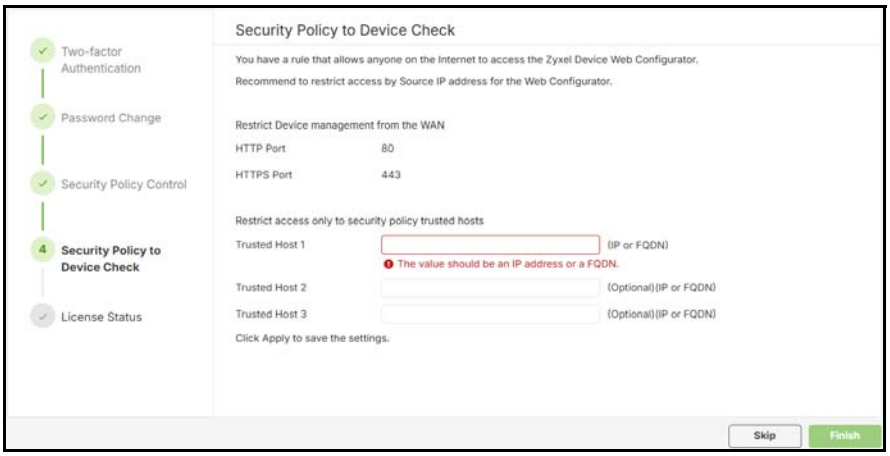
Security Policy Control

When the **General Settings** in **Security Policy > Policy Control** is disabled, the Zyxel Device operates without applying security policies. Click the switch to the right to enable the security policies configured in **Security Policy > Policy Control**. This is enabled by default, so appears checked after the first login.



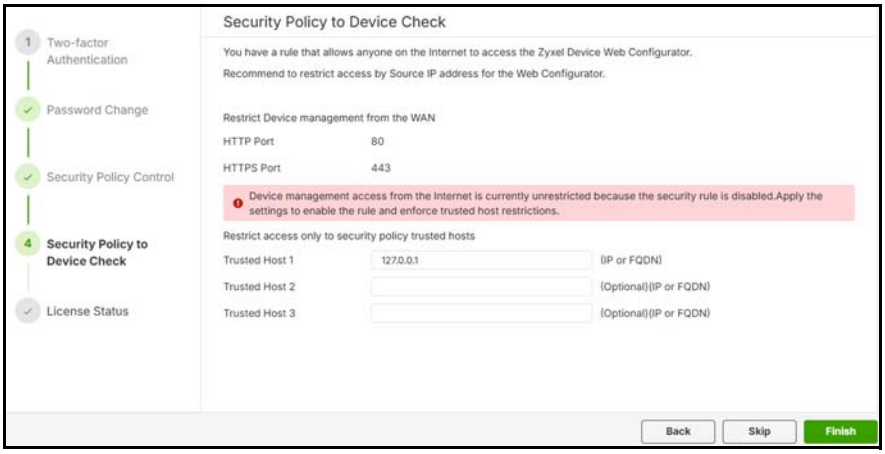
Security Policy to Device Check

This appears unchecked if the Zyxel Device detects a security policy rule that allows WAN access from any host using HTTP or HTTPS services. Use this screen to restrict access to trusted host(s) only.



The related service, address, and group objects are generated based on the HTTP and HTTPS ports for the configured trusted host(s). Two security policies, **Wiz_WAN_GUI_Allow** and **Wiz_WAN_GUI_Deny**, are also created with these objects included. You can view them in **Security Policy > Policy Control**. These policies block access for all hosts except the allowed ones.

If you configured this previously but disabled these two policies, this step is marked as incomplete, as shown below.



Note: The Zyxel Device checks security policy rules whenever any security policy configuration is changed. This step will be marked as unmarked the next time you log in and this wizard appears.

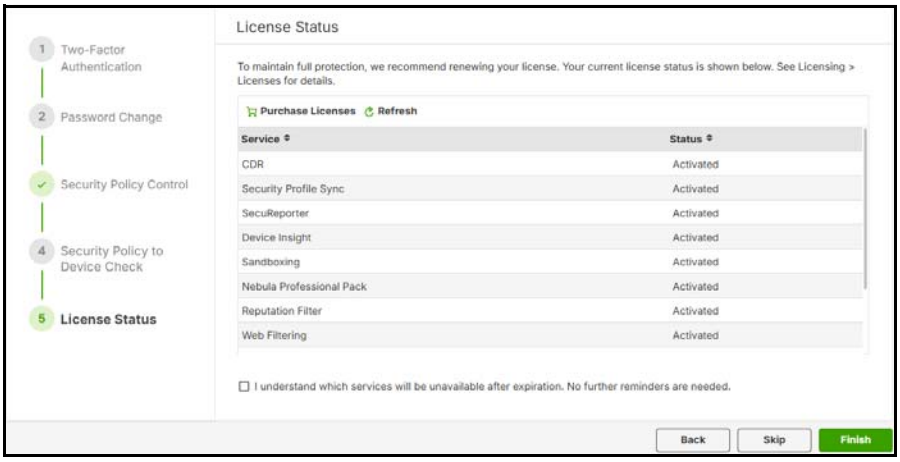
License Status

Keep licenses up to date to receive critical security enhancements, reduce security risks. Use this screen to check the license status. Click **Purchase Licenses** to go to Marketplace to renew Zyxel Device licenses.

This step is incomplete when:

- All services have expired (excluding Secure WiFi and Nebula Professional Packs).
- The Gold Pack license has expired, but the EDP Pack remains active. If you just have an EDP license and you don't want this item marked as incomplete, then select the checkmark to mark this step in the Security Best Practice wizard as completed.

For details on the services included in each pack, see Section 1.3 on page 20.



1.6.3 Remote Access to the Zyxel Device Networks

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

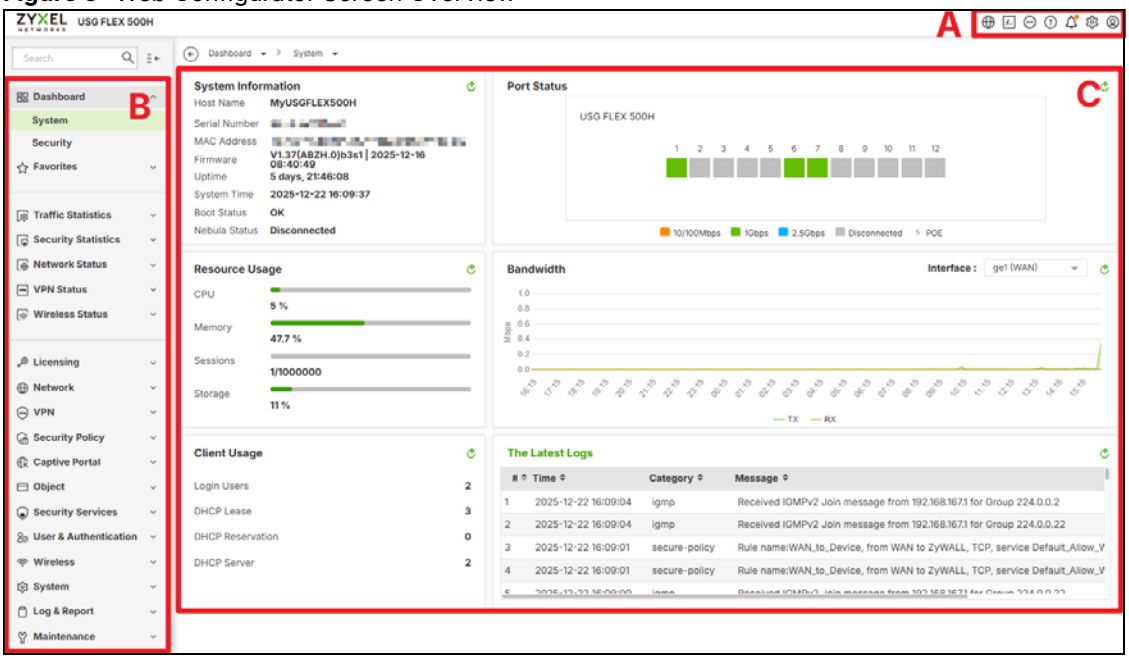
- Two-Factor Authentication: Use two-factor authentication to have double-layer security to access a secured network behind the Zyxel Device. The first layer is the VPN client/Zyxel Device's login user name / password. The second layer is an authorized SMS (via mobile phone number) or email address. See Section 28.4 on page 493 for more information on two-factor authentication.
- 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 13 on page 220 for more information on IPSec VPN.

1.6.4 Web Configurator Screens Overview

The Web Configurator screen is divided into these parts:

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

Figure 6 Web Configurator Screen Overview



Title Bar

Figure 7 Title Bar



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

Table 3 Title Bar: Web Configurator Icons

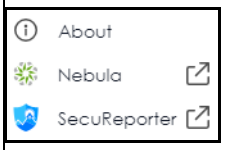
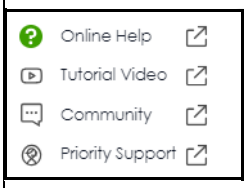
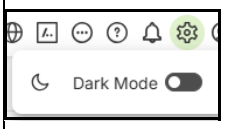
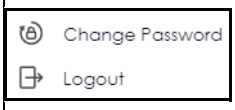
LABEL	DESCRIPTION
Language	Select a display language for the Zyxel Device's web configurator screens.
Web Console	Select this to display a Command Line Interface (CLI) in your browser. See the Command Line Interface Reference Guide for information on commands.
More	 **About:** Click this to display basic information about the Zyxel Device. **Nebula**: Click this to go to *https://nebula.zyxel.com/* to monitor or manage your Zyxel Device using Nebula. **SecuReporter**: Click this to go to *https://secureporter.cloudcnm.zyxel.com/* for security analytics.

Table 3 Title Bar: Web Configurator Icons (continued)

LABEL	DESCRIPTION
Help	 **Online Help**: Click this to open the help page for the current screen. **Tutorial Video**: Click this to go to YouTube to see related Zyxel Device configuration videos. **Community**: Click this to go to *https://community.zyxel.com/en/categories/security* for security product line discussions. **Priority Support:** The Nebula Pro license includes this to get direct assistance from the Nebula technical support team within 24 hours, and access to web chat during Taiwan office hours.
Notification	**What's New**: Click this to open a PDF file to display what's new in the Zyxel Device firmware. **License Expired**: Click this to go to **Licensing > License**. Update the expired license to keep your network fully protected.
Setting	 **Dark Mode**: The default mode of the Web Configurator uses a light background. Click the switch to the right to change the Web Configurator from a light to a dark background.
User	 **Change Password**: This is for an admin account type only. Click this to change the account password. You will need to log in again using the new password. **Logout**: Click this log out of the Web Configurator.

About

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

Figure 8 About



This table describes the fields in this screen.

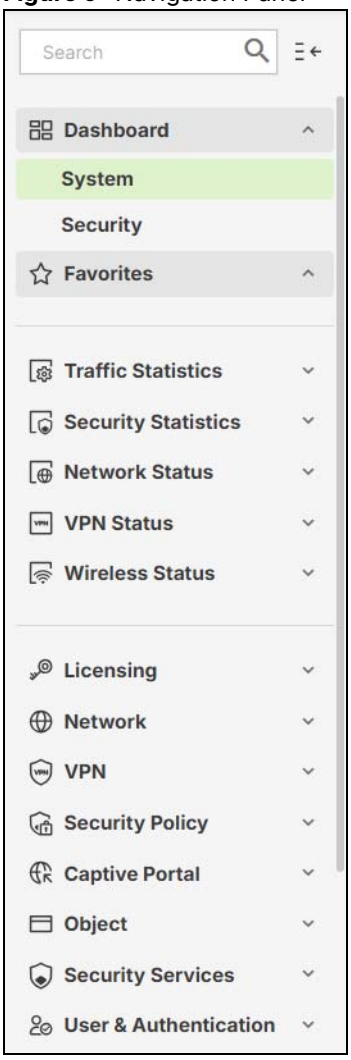
Table 4 About

LABEL	DESCRIPTION
Current Version	This shows the firmware version of the Zyxel Device.
Release Date	This shows the date (yyyy-mm-dd) and time (hh:mm:ss) when the firmware is released.
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.

1.6.5 Navigation Panel

Use the navigation panel menu items to open status and configuration screens. Click the arrow of the navigation panel to hide the panel. Type an entry in the Search box to find a menu item containing that entry. The following sections introduce the Zyxel Device's navigation panel menus and their screens.

Figure 9 Navigation Panel



Dashboard Screens

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.

Table 5 Dashboard Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
System		Collect and display the Zyxel Device system information, such as serial number, MAC address and CPU usage.
Security		Collect and display security event statistics.

Monitoring Screens

The monitoring screens display status and statistics information.

Table 6 Monitoring Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
Traffic Statistics		
Application Usage	Application Usage	Collect and display application statistics.
Port	Port	Collect and display port statistics.
Interface	Interface	Collect and display interface statistics.
Session Monitor	Session Monitor	Collect and display session statistics.
Security Statistics		
Content Filter	Content Filter	Collect and display content filter statistics
Reputation Filter	IP Reputation	Collect and display IP reputation statistics.
	DNS Threat Filter	Collect and display DNS threat filter statistics.
	URL Threat Filter	Collect and display URL threat filter statistics.
IPS	IPS	Collect and display statistics on the intrusions that the Zyxel Device has detected.
Anti-Malware	Anti-Malware	Collect and display anti-malware statistics.
Sandbox	Sandbox	Displays the sandbox statistics.
SSL Inspection	Summary	Collect and display SSL Inspection statistics.
	Certificate Cache List	Display traffic to destination servers using certificates.
Network Status		
Interface	Interface	Display the status of Zyxel Device interfaces.
Device Insight	Device Insight	Displays a list of WiFi and wired clients connected to the Zyxel Device local networks.
Login Users	Login Users	List the users currently logged into the Zyxel Device.
	Lockout IPs	View and unlock IP addresses blocked from logging in to the Zyxel Device.
DHCP Table	DHCP Table	Display a list of interfaces and their DHCP-assigned IP addresses.
VPN Status		
IPSec VPN	Site to Site VPN	Display and manage the Zyxel Device IPSec VPN connections with remote IPSec VPN routers that have static IP addresses or a domain names.
	Remote Access VPN	Display and manage IPSec VPN connections from external users who want to access the networks behind the Zyxel Device.
SSL VPN	Remote Access VPN	Display and manage SSL VPN connections from external users who want to access the networks behind the Zyxel Device.
Tailscale	Tailscale	Display Tailscale mesh VPN connections across different networks.
Wireless Status		
Access Points	Top N APs	View traffic usage of managed APs and details for the top 5 or 10 APs.
	Single AP	View traffic usage of a managed AP.
WLAN Clients	Top N Stations	View traffic usage of client devices and details for the top 5 or 10 client devices.
	Single Station	View traffic usage of a client device.

Configuration Screens

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

Table 7 Configuration Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
Licensing		
Licenses	Licenses	Displays if the Zyxel Device is registered and licenses purchased.
Signature Update	Signature Update	Use this screen to update signatures immediately or by a schedule.
Network		
Interface	Interface	Use this screen to: • Create and manage Ethernet interfaces. • Create and manage VLAN interfaces. • Create and manage bridge interfaces. • Configure IP address assignment and interface parameters for VTI (Virtual Tunnel Interface).
	Trunk	Create and manage trunks (groups of interfaces) for load balancing.
	Port	Use this screen to configure the Zyxel Device port settings.
Routing	Policy Route	Create and manage routing policies.
	Static Route	Create and manage IP static routing information.
NAT	NAT	Set up and manage port forwarding rules.
BWM	BWM	Control bandwidth for services passing through the Zyxel Device, and identify the conditions for bandwidth control.
ALG	ALG	Configure FTP pass-through settings.
Multicast	Multicast	Configure IGMP and mDNS Proxy settings.
VPN		
IPSec VPN	Site to Site VPN	Configure Zyxel Device IPSec VPN connections with remote IPSec VPN routers that have static IP addresses or a domain names.
	Remote Access VPN	Configure IPSec VPN connections for external users who want to access the networks behind the Zyxel Device.
SSL VPN	SSL VPN	Configure SSL VPN connections for external users who want to access the networks behind the Zyxel Device.
Tailscale	Tailscale	Configure the Zyxel Device in a Tailscale mesh VPN network.
Security Policy		
Policy Control	Policy Control	Create and manage level-3 traffic rules and apply Security Service profiles.
DoS Prevention	DoS Prevention Policy	Display and manage ADP bindings.
	Profile	Create and manage DoS prevention profiles.
IP Spoofing Prevention	IP Spoofing Prevention	Bind IP addresses to MAC addresses.
Session Control	Session Control	Limit the number of concurrent client NAT/security policy sessions.
Captive Portal		
Authentication Policy	Policy	Create client authentication profiles for network access through the Zyxel Device.
	Settings	Configure another server for clients to access the captive portal.
Object		

Table 7 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
Address	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.
Zone	Zone	Configure zone templates used to define various policies.
Schedule	Schedule	Create one-time and recurring schedules.
	Schedule Group	Create and manage groups of schedules to apply to policies as a single object.
Security Service		
App Patrol	App Patrol	Manage different types of traffic in this screen. Create App Patrol template(s) of settings to apply to a traffic flow using a security policy.
Content Filtering	Content Filtering	Use this screen to: • Create and manage the detailed filtering rules for HTTP(S) traffic scan and DNS domain scan. • Create a list of allowed web sites that bypass HTTP(S) traffic scan and DNS domain scan. • Create a list of web sites to block regardless of content filtering policies.
Reputation Filter	IP Reputation	Enable IP reputation and specify what action the Zyxel Device takes when any IP address with bad reputation is detected. You can also set up an allow list to identify which IPv4 addresses should be allowed, and a block list to identify which IPv4 addresses should be blocked.
	DNS Threat Filter	Enable DNS threat filtering and specify what action the Zyxel Device takes when a access attempt to a blocked Fully Qualified Domain Name (FQDN) is detected. You can also set up an allow list to identify which FQDNs should be allowed, and a block list to identify which FQDNs should be blocked.
	URL Threat Filter	Enable URL filtering and specify what action the Zyxel Device takes when a access attempt to a blocked website is detected. You can also set up an allow list to identify which IPv4 addresses and/or URLs should be allowed, and a block list to identify which IPv4 addresses and/or URLs should be blocked.
Anti-Malware	Anti-Malware	Enable, specify actions to take when encountering malware or compressed files, and set up a block list to identify files with malware file patterns and an allow list to identify files that should not be checked for malware.
Sandbox	Sandbox	Enable sandbox, and specify the actions the Zyxel Device takes when files with unknown or untrusted programs are detected.
IPS	IPS	Enable and configure IPS settings. Create, import, or export custom signatures.
	Allow List	Configure signatures that will be exempted from IPS inspection.

Table 7 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
IP Exception	IP Exception	Use this screen to view the IP exception list for the anti-malware, reputation filter and IPS (Intrusion Prevention System) features. The Zyxel Device will not intercept nor inspect the incoming packets that match the rules in the IP exception list for the anti-malware and/or IPS (Intrusion Prevention System) features.
SSL Inspection	Profile	Decrypt HTTPS traffic for Security Service inspection. Create SSL Inspection templates of settings to apply to a traffic flow using a security policy.
	Exclude List	Configure services to be excluded from SSL Inspection.
	Certificate Update	Use this screen to update the latest certificates of servers using SSL connections to the Zyxel Device network.
External Block List	IP Reputation	Set up an external block list which uses block list entries of IP addresses with bad reputations stored in a file on a web server that supports HTTP or HTTPS and is reachable from the Zyxel Device. The Zyxel Device will block incoming and outgoing packets from the black list entries in this file.
	DNS Threat Filter/ URL Threat Filter	Set up an external block list which uses block list entries of blocked Fully Qualified Domain Names (FQDN) or blocked URLs stored in a file on a web server that supports HTTP or HTTPS and is reachable from the Zyxel Device. The Zyxel Device will block incoming and outgoing packets from the black list entries in this file.
User & Authentication		
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.
User Authentication	AAA Server	Configure the default authentication server (AD/LDAP/OIDC/RADIUS) to use for user authentication.
	Two-factor Authentication	Configure Google Authenticator to access a secured network behind the Zyxel Device via the web configurator or SSH connection.
	Advanced	Configure an intermediary server for identification of remote users with an account on an AAA server.
Wireless		
AP Control Service	AP Control Service	Set the password for the admin accounts of APs connected to the Zyxel Device.
Access Points	AP List	Manage all of the APs connected to the Zyxel Device
	Policy	Configure the AP controller's IP address on the managed APs and determine the action the managed APs take if the current AP controller fails.
	AP Firmware	Check for and download new AP firmware when it becomes available on the firmware server.
WLAN Clients	All Clients	View a list of WiFi clients connected to APs.
	Policy Clients	Configure a policy to block a specific MAC address.
WLAN Settings	SSID Settings	Configure SSID profiles for each AP group.
	Radio Settings	Configure global radio settings for all managed APs.
	AP Settings	Configure general AP settings and enable or disable a port on the managed AP and configure the port's VLAN settings.
	AP Group Settings	Configure AP group settings and remove an AP group.

Table 7 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
Wireless Health	Wireless Health	Monitor the health of WiFi networks for your APs and connected WiFi clients.
SSID Info	SSID Info	Monitor the WiFi networks (SSIDs) currently in use and the client devices connected to them.
System		
Settings	Settings	Use this screen to configure: • The Zyxel Device host name. • System time settings. • Remote access to the Zyxel Device settings. • The web configurator language display settings.
Device HA	HA Status	See the license status for Device HA, and see the status of the active and passive devices.
	HA Configuration	Configure Device HA global settings, monitored interfaces and synchronization settings.
	HA Log	See logs of the active and passive devices.
DNS & DDNS	DNS	Configure the DNS server and address records for the Zyxel Device.
	DDNS	Define and manage the Zyxel Device's DDNS domain names.
SNMP	SNMP	Configure SNMP communities and services.
Notification	Mail Server	Configure a mail server with authentication to send reports and password expiration notification emails.
	Alert	Enable to have the Zyxel Device send events notification mails and alert logs.
Certificate	My Certificates	Create and manage the Zyxel Device's certificates.
	Trusted Certificates	Import and manage certificates from trusted sources.
Advanced	Advanced	Edit default Zyxel Device parameters such as UDP/ICMP timeout, ARP spoofing, device insight and LLDP.
External Integration	Endpoint	Integrate the Zyxel Device with other cloud-based security platforms such as the Avast Business Hub.
Log & Report		
Log / Events	System	View the Zyxel Device log messages.
	APC	View AP Controller (APC) related logs.
	AP	View connected AP related logs.
Log Setting	Log Setting	Configure the system log, email logs, and remote syslog servers.
SecuReporter	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.
Email Daily Report	Email Daily Report	Select statistics to email in a daily report.

Maintenance Screens

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

Table 8 Maintenance Menu Screens Summary

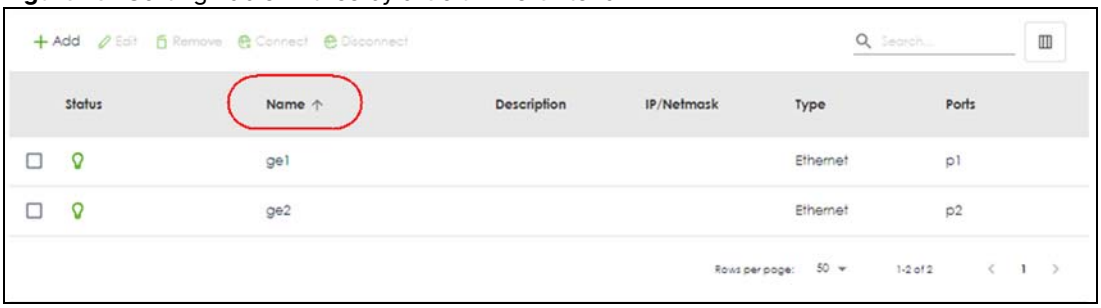
FOLDER OR LINK	TAB	FUNCTION
Maintenance		
Firmware/File Manager	Configuration File	Manage and upload configuration files for the Zyxel Device.
	Firmware Management	View the current firmware version and upload firmware.
Diagnostics	Diagnostics	Collect diagnostic information.
	Packet Capture	Capture packets for analysis.
	CPU/Memory Status	View CPU and memory usage statistics.
	System Log	View the files of diagnostic information the Zyxel Device has collected and stored on a connected USB storage device.
	Network Tool	Identify problems with the connections. You can use Ping or Traceroute to help you identify problems.
AP Diagnositcs	Diagnostics	Collect managed APs' diagnostic information
	Packet Captre	Capture packets of WiFi network (SSID) for analysis.
	Remote Capture	Capture wireless packets passing through a managed AP and output them to a packet analyzer.
Packet Flow Explore	Routing Status	Check how the Zyxel Device determines where to route a packet.
	SNAT Status	View the overall source IP address conversion (SNAT) flow and each SNAT function's settings.
	Route Traces	Configure traceroute to identify where packets are dropped for troubleshooting.
Reboot/ Shutdown	Reboot/Shutdown	Restart or turn off the Zyxel Device.

1.6.6 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 10 Sorting Table Entries by a Column's Criteria



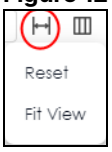
Click the Resize icon ( ) to adjust how to display column entries. If you manually adjusted the width of the columns, click **Reset** to return them to the original widths. If you have a big monitor and want to see

complete information in each column field, click **Fit Content.** If your monitor is not so big and you want to see all columns in the screen, click **Fit View.**

Figure 11 Fit Content

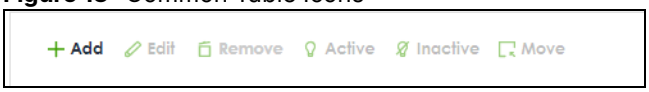


Figure 12 Fit View



Click the column icon ( ) for more options about how to display the entries. The options available vary depending on the type of fields in the column. You can select which columns to display by selecting or clearing the check box.The tables have icons for working with table entries.

Figure 13 Common Table Icons



1.6.7 Error /Warning Messages

The following are some error or warning messages that may appear on your Zyxel Device.

1.6.7.1 Parsing/Timeout Error

Some screens may display an error message if there is a parsing or time-out error. Use **Test** in **Maintenance > Firmware/File Manager > Configuration** to see if the currently running configuration file has an error.

Figure 14 Parsing Error

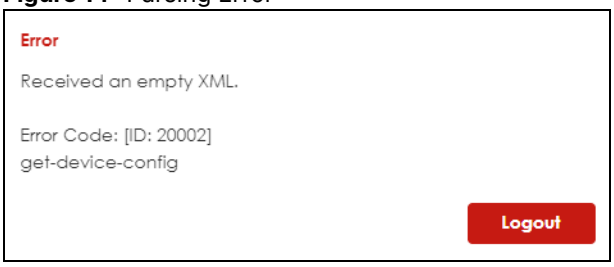


Figure 15 Timeout Error



1.6.7.2 Desynchronize from Nebula Security Profile Warning

Security profile sync in the Nebula Control Center (NCC) allows you to share the same Zyxel Device security service feature across multiple sites within an organization. If you enable **Security profile sync** in the NCC, and then add, edit or remove the security service feature in the web configurator, you will then see one of the following warnings.

Click **Cancel** to not apply or remove the security service feature and keep it synchronized with other sites on the NCC, or click **OK** to apply or remove the security service feature. The **Security profile sync** will then be disabled on the NCC.

Figure 16 Warning When Adding or Editing A Security Service Feature

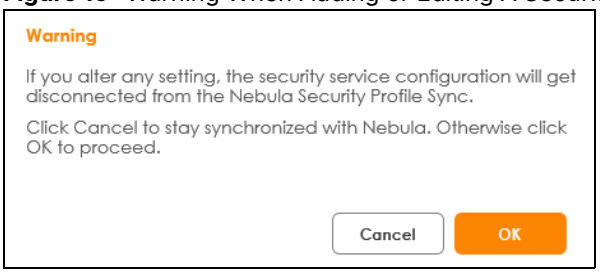
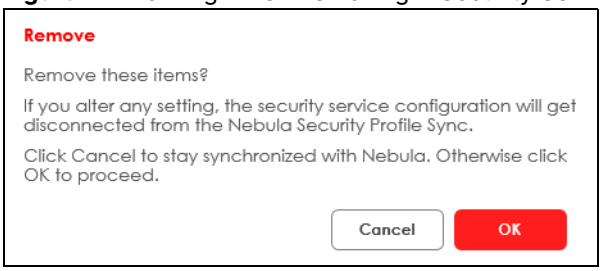


Figure 17 Warning When Removing A Security Service Feature



CHAPTER 2
Initial Setup Wizard

2.1 Initial Setup Wizard Overview

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

Nebula (NCC) is an Internet portal that allows you to monitor and manage groups of Zyxel Devices in organizations.

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.

You will be logged out of the Zyxel Device initial setup wizard after 1440 minutes. The settings you configured will be saved. Log into the Zyxel Device again if you have not finished configuring the initial setup wizard settings.

Click **Next** to continue the wizard. Click **Finish** at the end of the wizard to complete the wizard.

2.1.1 Terms of Use/Privacy Policy/Firmware Upgrade Notification

Click the links to see:

- What data Zyxel collects from you and how it is used
- Zyxel privacy policy.

Please also read the firmware upgrade notification carefully.

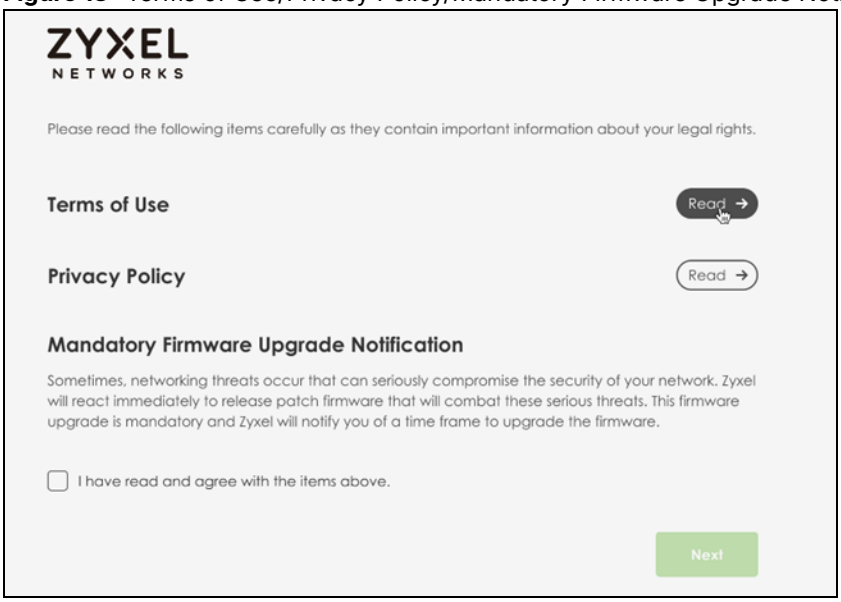
To use SecuReporter and sandbox, you need to allow Zyxel to collect data from you.

Select **I have read and agree with the items above**. SecuReporter and sandbox will be enabled automatically when you select the check box.

Click **Next** to configure the Zyxel Device settings with the initial setup wizard.

Note: You cannot proceed with the initial setup wizard if you do not select the check box.

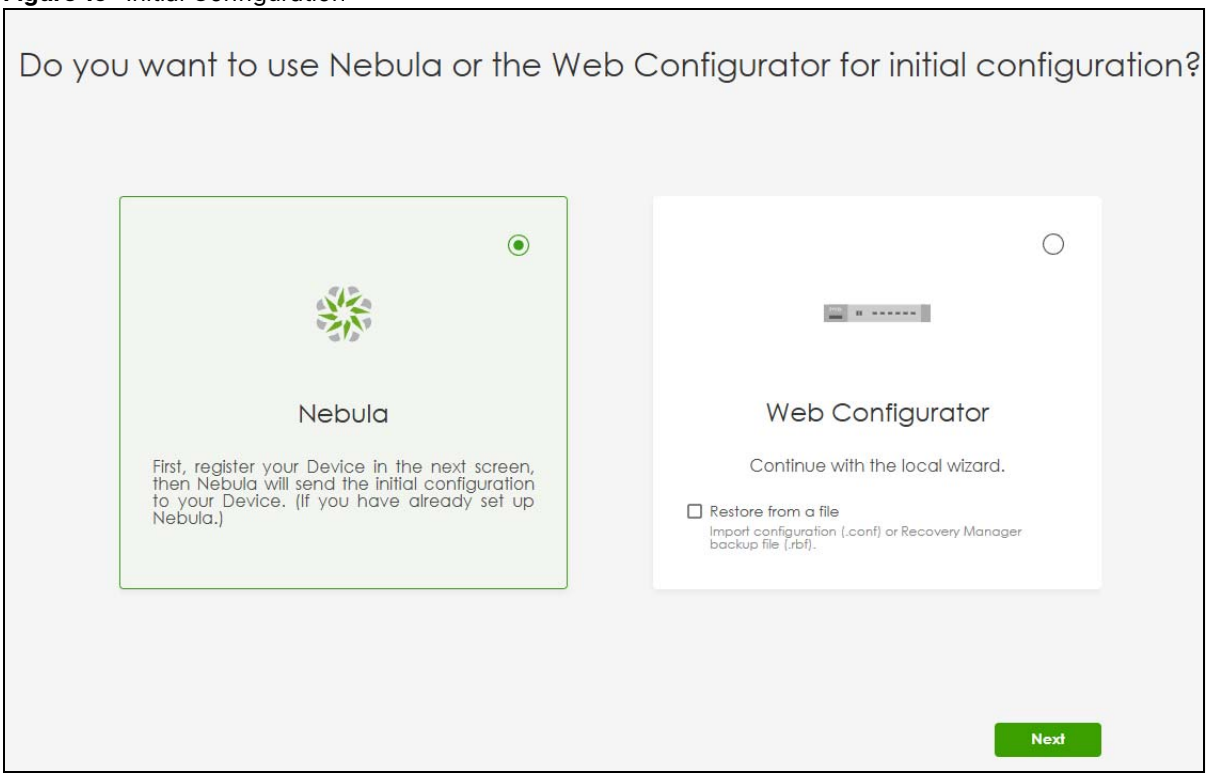
Figure 18 Terms of Use/Privacy Policy/Mandatory Firmware Upgrade Notification



2.2 Initial Configuration

You can configure the Zyxel Device using both Nebula (NCC) or the Web Configurator, but you must first decide which one you want to use for first-time configuration.

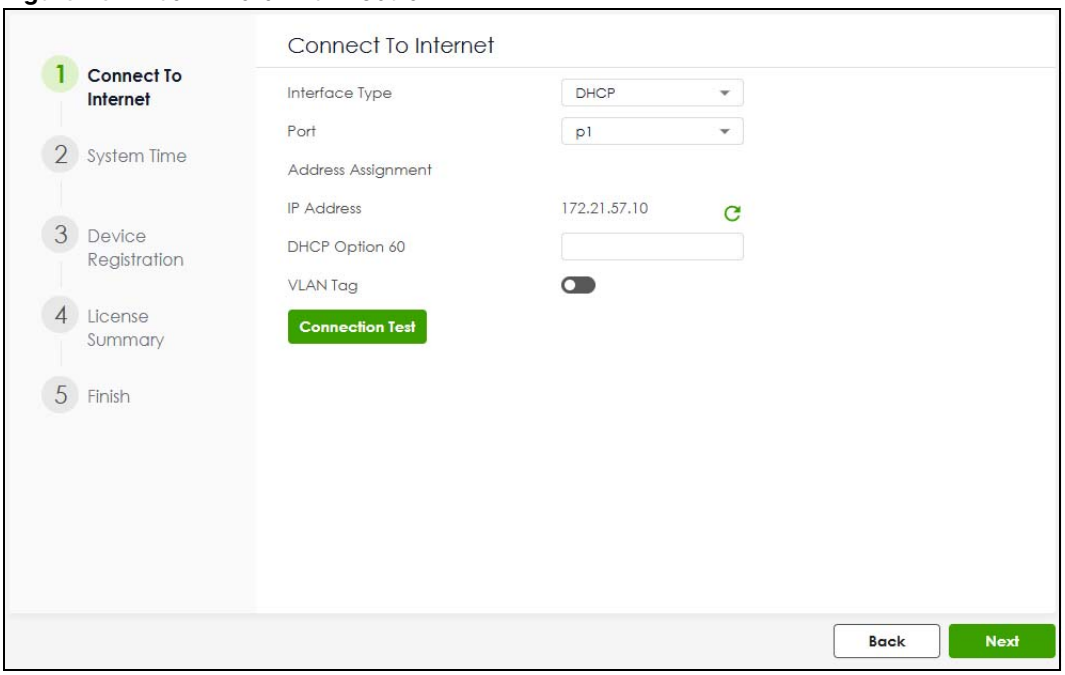
Figure 19 Initial Configuration



2.2.1 Initial Configuration With Nebula

If you already have a Nebula (NCC) account, and you have created an Organization and Site, choose **Nebula**, then click **Next**.

Figure 20 Initial Wizard With Nebula



- Complete each screen in the wizard, including registering your Zyxel Device in the Organization and Site you created at Nebula.
- After **Device Registration**, Nebula will send the initial configuration to your Zyxel Device. This may take up to 5 minutes to complete. Click **OK** to close the wizard and wait.

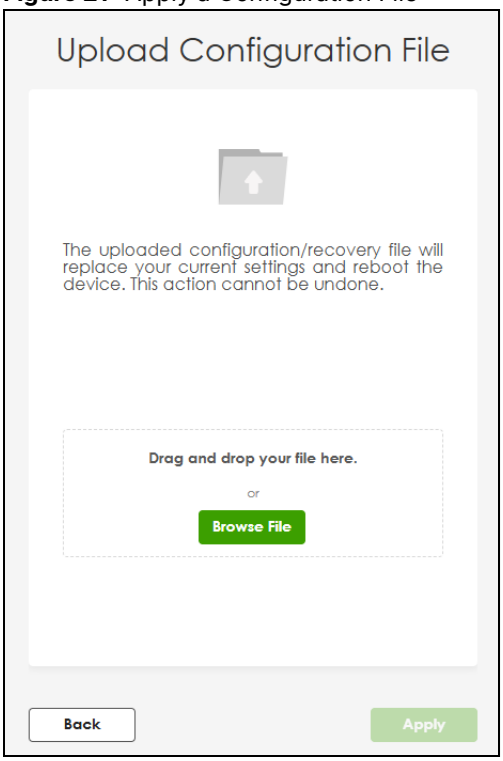
Note: Do not make any changes in the Web Configurator at this time. Log into Nebula to see the status of your Zyxel Device registration and make further configurations there.

2.2.2 Initial Configuration With Web Configurator

Choose **Web Configurator** if you do not already have a Nebula (NCC) account, or you prefer to directly configure your Zyxel Device initially with the Web Configurator.

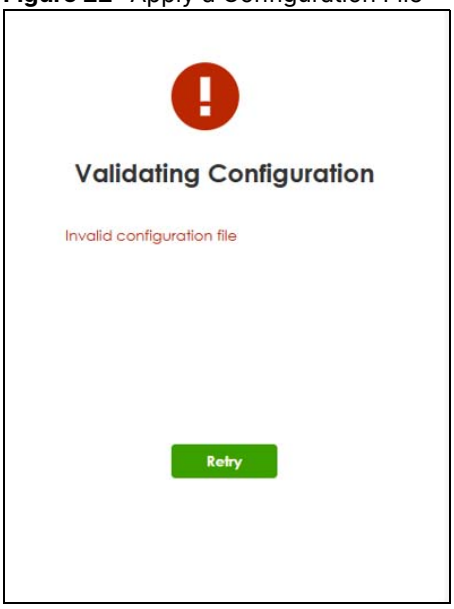
If you already have a configuration file (.conf) or a recovery file (.rbf) that you'd like to apply to the Zyxel Device, select **Restore from a file** under **Web Configurator**, and then click **Next**.

Figure 21 Apply a Configuration File



Select a file and then click **Apply**. The Wizard will check in advance if this is a valid file and prompt you to upload another one if it is not. Click **Retry** and select a valid configuration file.

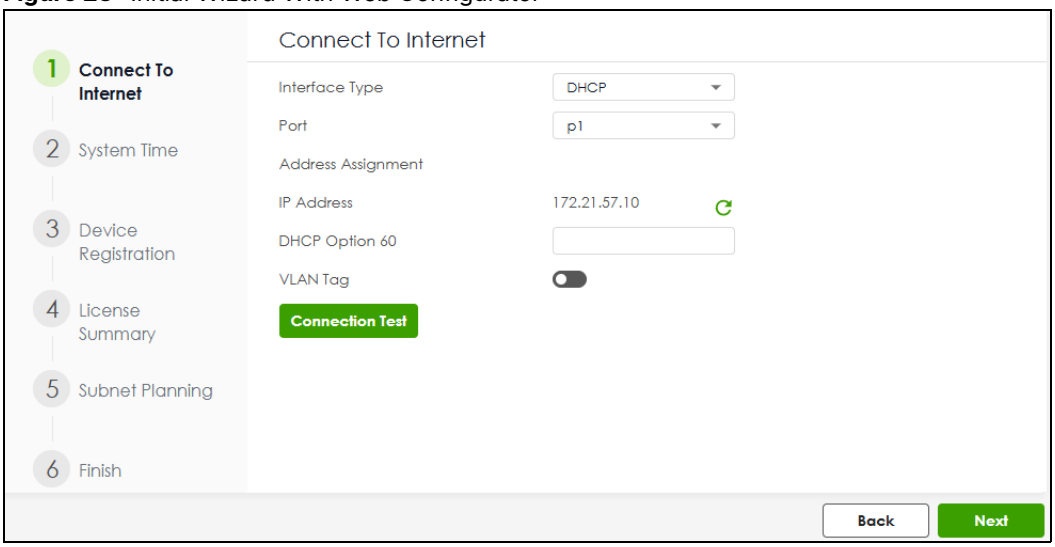
Figure 22 Apply a Configuration File



If the configuration file is valid, the Zyxel Device will then restart after it applies the configuration.

If you do not already have a configuration file that you'd like to apply to the Zyxel Device, select **Web Configurator,** and then click **Next**.

Figure 23 Initial Wizard With Web Configurator



- Complete each screen in the wizard, including registering your Zyxel Device in an Organization and Site at Nebula.

Note: You must register your Zyxel Device at Nebula Control Center (NCC) to use security services and upgrade firmware.

- When you see the **Finish** screen, click **Finish** to close the wizard and go to the Web Configurator **Dashboard**.

2.3 Wizard - Connect to the Internet

Use this screen to set the 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.

Go to **Network** > **Interface** after you log into the web configurator if you want to change the interface settings.

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.

2.3.1 Interface Type - DHCP

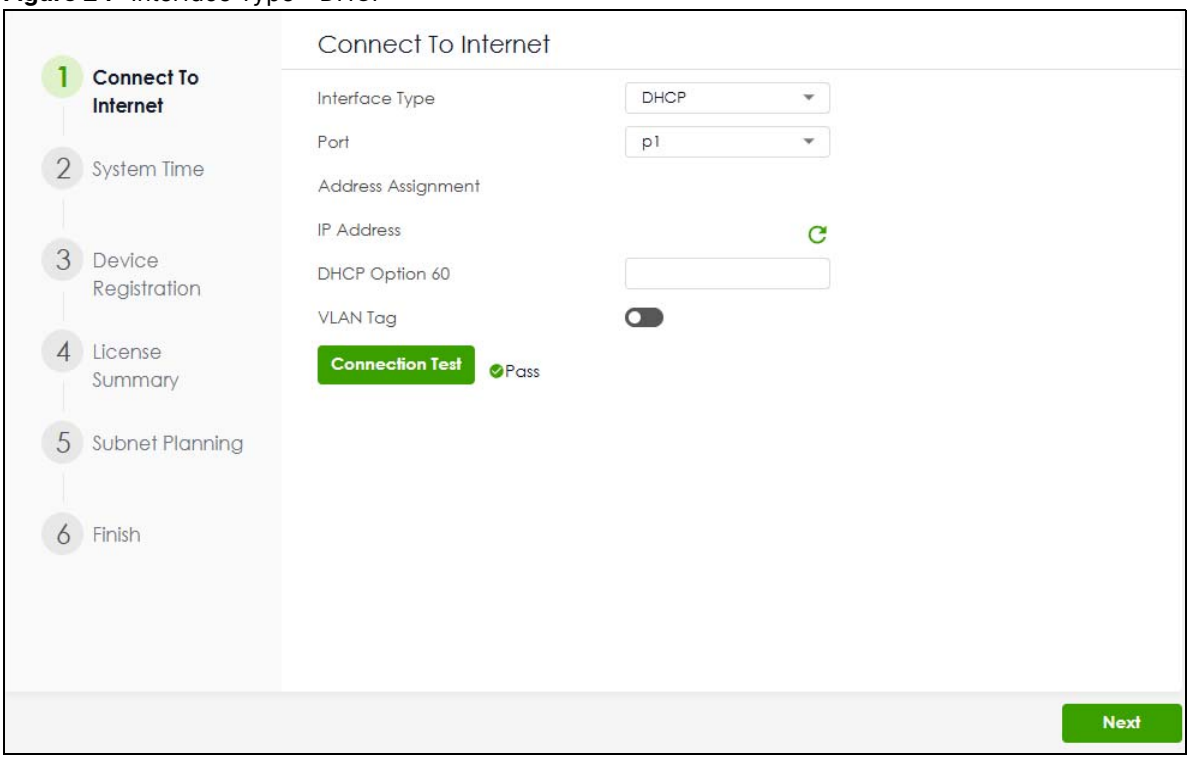
Use this screen to configure your IP address settings.

- **Interface Type:** This displays the type of Internet connection you are configuring. Select DHCP if your ISP did not assign you a fixed IP address.
- **Port:** Select a port to apply the Internet connection settings to.
- **IP Address:** This field is read-only when you set **Interface Type** to **DHCP**.

- **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.

  Type 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.
- **VLAN Tag:** Enable to tag the traffic going out from the Zyxel Device.
- **VLAN ID**: Enter a VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1-4080.
- **Connection Test**: 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 24 Interface Type - DHCP



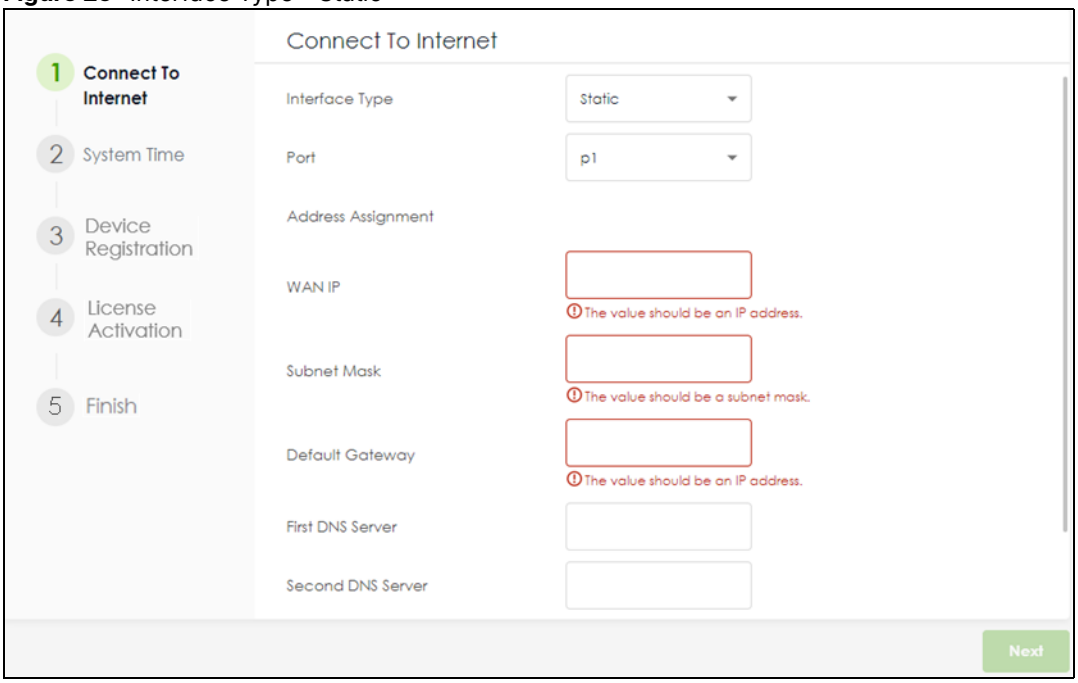
2.3.2 Interface Type - Static

Use this screen to configure your IP address settings.

- **Interface Type:** This displays the type of Internet connection you are configuring. Select **Static** if your ISP assigned you a fixed IP address.
- **Port:** Select a port to apply the Internet connection settings to.
- **WAN IP**: Enter your (static) public IP address.
- **Subnet Mask**: Enter the subnet mask for this WAN connection's IP address.
- **Default Gateway**: 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.
- **VLAN Tag:** Enable to tag the traffic going out from the Zyxel Device.
- **VLAN ID**: Enter a VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1-4080.
- **Connection Test**: 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 25 Interface Type - Static



2.3.2.1 Possible Errors

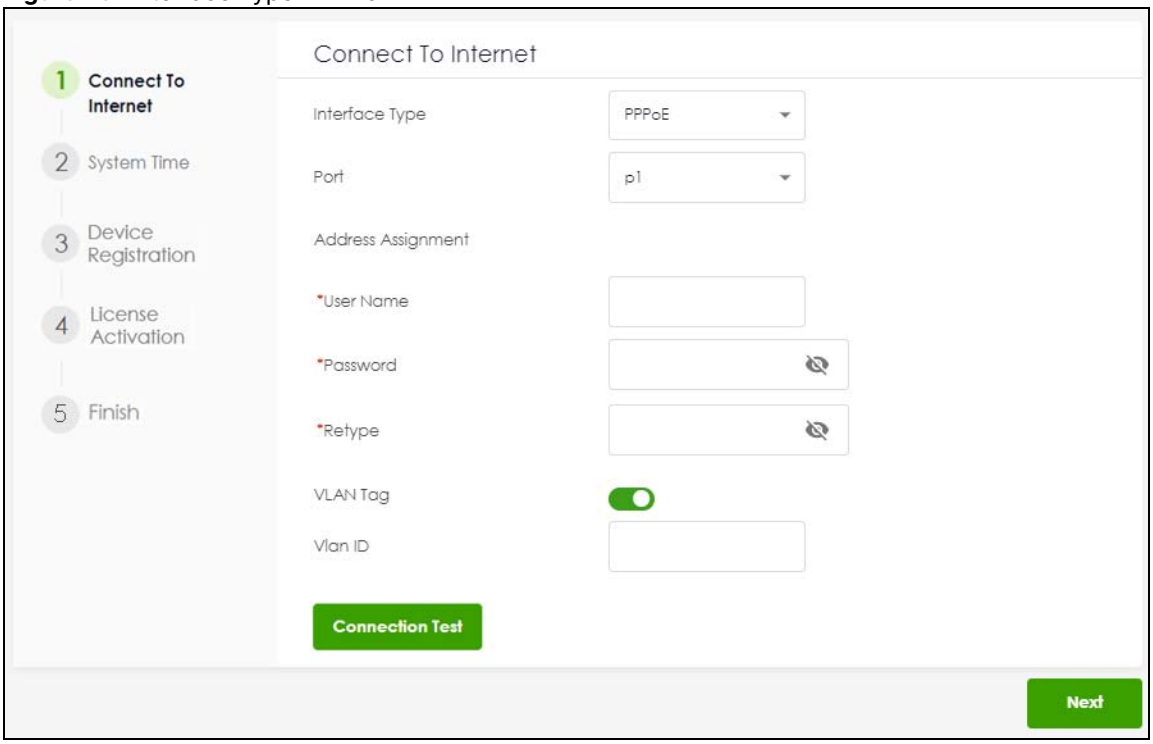
- Check that the cable is connected from the WAN (port 1 or port 2) to the Internet.
- Check that the interface is connected to the device you're using for Internet access such as a broadband router, and that the router is turned on.
- If your Zyxel Device was not able to obtain an IP address, check 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 enter correctly the IP address, subnet mask and gateway IP address exactly as given. If it fails again, check with your Internet service provider or administrator for the correct IP address, subnet mask and gateway address and other WAN settings.

2.3.3 Interface Type - PPPoE

Use this screen to configure your IP address settings.

- **Interface Type:** This displays the type of Internet connection you are configuring. Select **PPPoE** for a dial-up connection according to the information from your ISP.
- **Port:** Select a port to apply the Internet connection settings to.
- **User Name**: Enter the user name given to you by your ISP. You can use up to 64 single-byte characters, including 0-9a-zA-Z-_@$. /+ # ; :%\~^&*() " = {}[]|? ,< ' >'. The user name must begin with 0-9a-zA-Z-_@$. /+. Spaces are not allowed.
- **Password:** Enter the password associated with the user name. You can use up to 63 single-byte characters, including 0-9a-zA-Z-_@$. /+ # ; :%\~^&*() "= {}[]|! ,<'>'. Spaces are not allowed. This field cannot be blank.
- **VLAN Tag:** Enable to tag the traffic going out from the Zyxel Device
- **VLAN ID**: Enter a VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1-4080.
- **Connection Test**: 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 26 Interface Type - PPPoE



2.3.3.1 Possible Errors

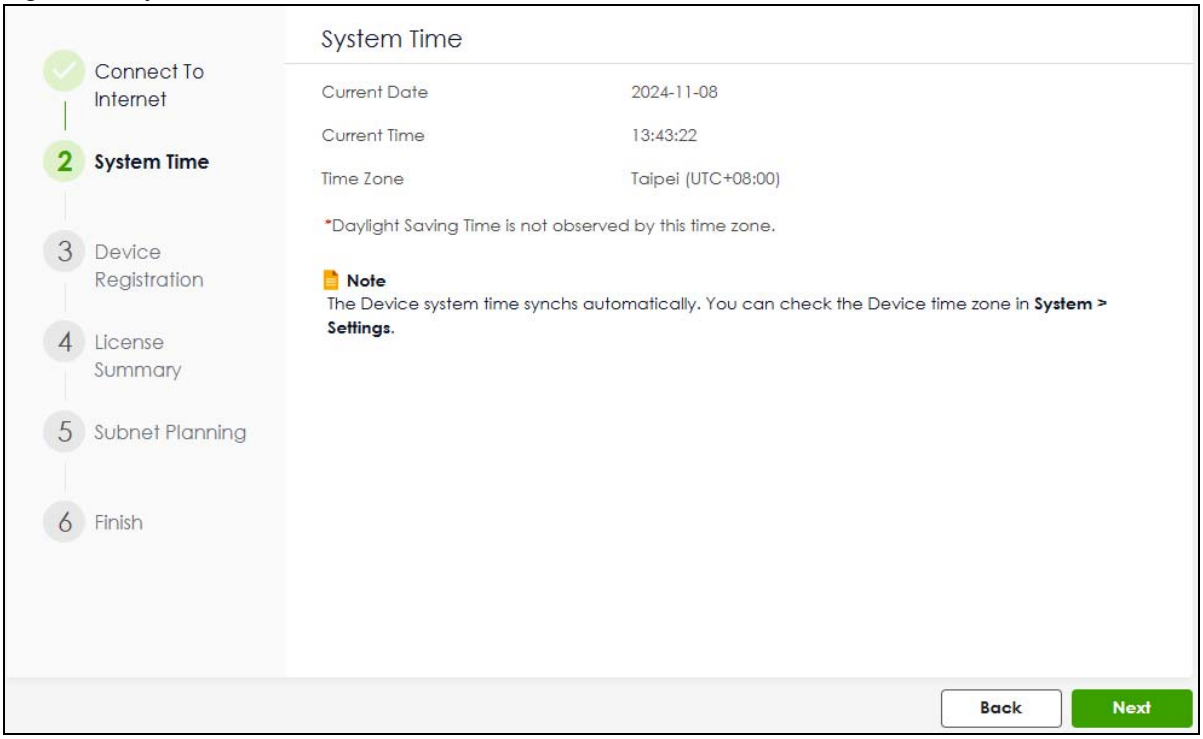
Make sure that your Internet access information uses PPPoE as the WAN connection type. Re-enter your PPPoE user name and password exactly as given. If it fails again, check with your Internet service provider or administrator for correct WAN settings and user credentials.

2.4 Wizard - System 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 the time server settings in **System** > **Settings** after you log into the Zyxel Device.

Figure 27 System Time



2.5 Wizard - Device Registration

Device registration includes:

- Adding your Zyxel Device to a site in an organization at *NCC*
- Activating Zyxel Device service licenses

If you previously activated your service licenses at another Zyxel portal such as myZyxel.com or Circle, you can still use all Zyxel Device services except for SecuReporter and remote support through Nebula. Add your Zyxel Device to a site in an organization at *NCC* to be able to use these features also.

If you did not previously activate your service licenses at another Zyxel portal such as myZyxel.com or Circle, then you must add your Zyxel Device to a site in an organization at *NCC* in order to activate your Zyxel Device service licenses, including SecuReporter, perform firmware upgrades and avail of remote support through Nebula.

After you successfully register your Zyxel Device, security services supported by your model will be activated automatically.

Click the **Register** button in this screen to add your Zyxel Device to a site in an organization at Nebula. There are two ways to add your Zyxel Device to a site at *NCC*.

- Automatically add it by scanning the QR code to use the Nebula Mobile app.

- Manually add it by entering the Zyxel Device's serial number and LAN MAC address at *NCC*. See the label at the back of the Zyxel Device for this information.

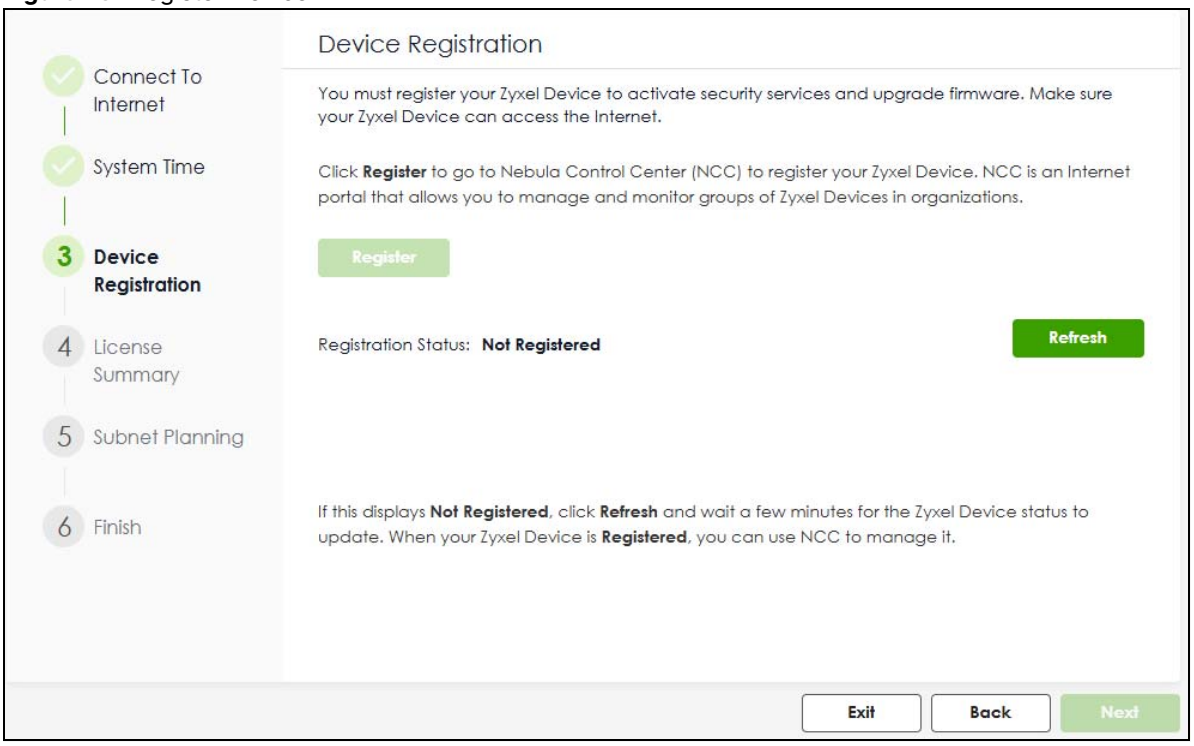
Note: The Zyxel Device must be connected to the Internet in order to connect to *NCC*.

Click **Refresh** or use the **Licensing > Licenses** screen after you log into the web configurator to have the Zyxel Device connect to *NCC* to update its registration status.

The **Registration Status** field may display **Registered** or **Not registered**.

- **Registered**: Your Zyxel Device has been successfully added to a site in *NCC*.
- **Not registered**: Your Zyxel Device has not been successfully added to a site in *NCC*. Make sure the Zyxel Device is connected to the Internet. Wait a few minutes, then click **Refresh** to synchronize again.

Figure 28 Register Device

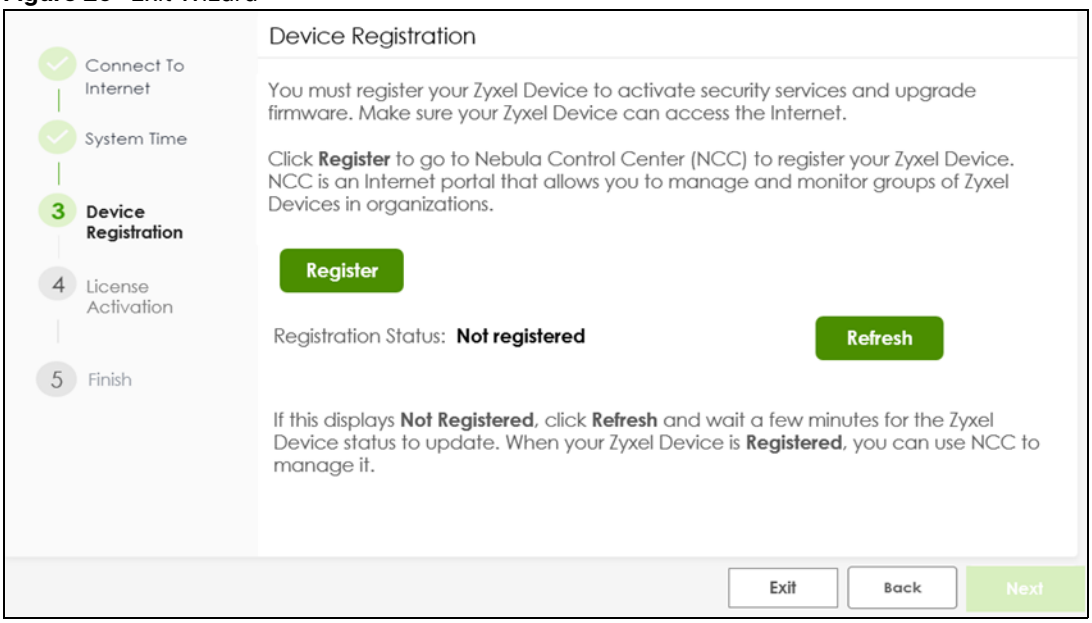


2.5.1 Exit the Wizard

The **Exit** button displays if the Zyxel Device is not connected to the Internet when you are at the **Device Registration** step. You will be redirected to the Zyxel Device login page after you click **Exit**.

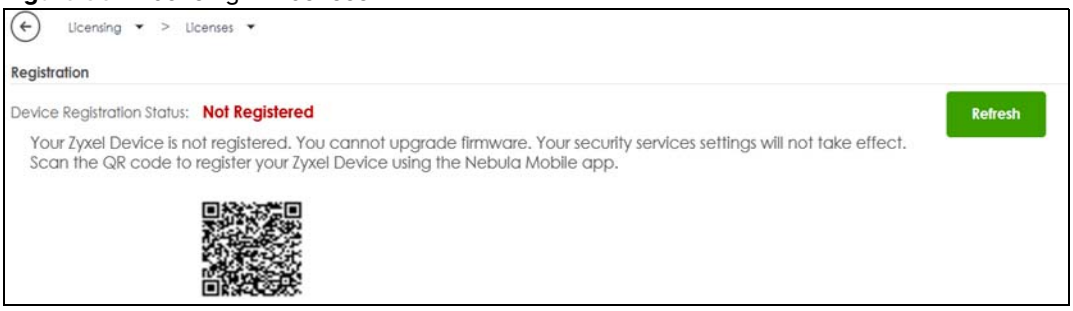
If you did not previously activate your service licenses at another Zyxel portal, then you must add your Zyxel Device to a site in an organization at *NCC* in order to activate your Zyxel Device service licenses, including SecuReporter, perform firmware upgrades and avail of remote support through Nebula.

Figure 29 Exit Wizard



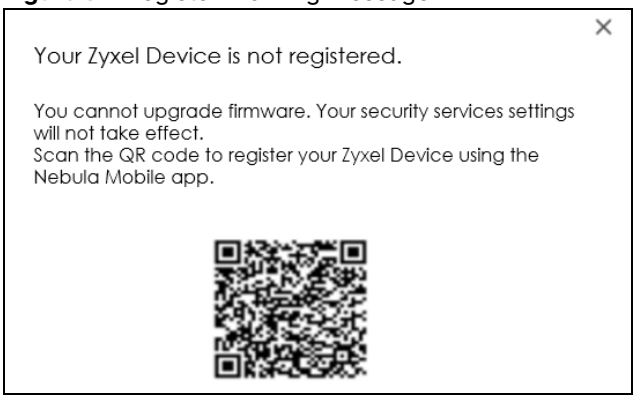
Make sure to go to **Licensing** > **Licenses** and follow the instructions to register your Zyxel Device once your Zyxel Device is connected to the Internet. Please note that you will only see the following screen if you log in using an admin account.

Figure 30 Licensing > Licenses



You will also see a warning message to remind you to register your Zyxel Device every time you log into the web configurator. Please note that you will only see the warning message if you log in using an admin account.

Figure 31 Register Warning Message

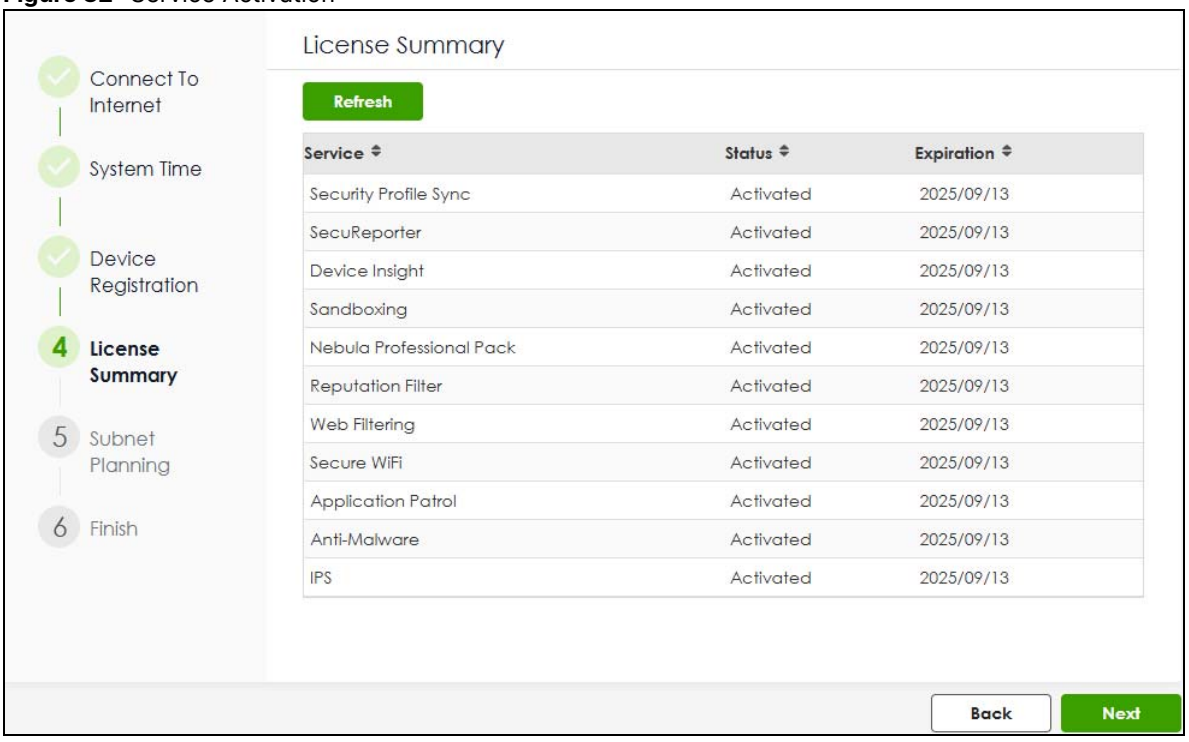


2.6 Wizard - License Summary

After you successfully register your Zyxel Device, security services supported by your model will be activated automatically.

Go to **Licensing** > **Licenses** after you log into the web configurator if you want to check the Zyxel Device services status.

Figure 32 Service Activation



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.

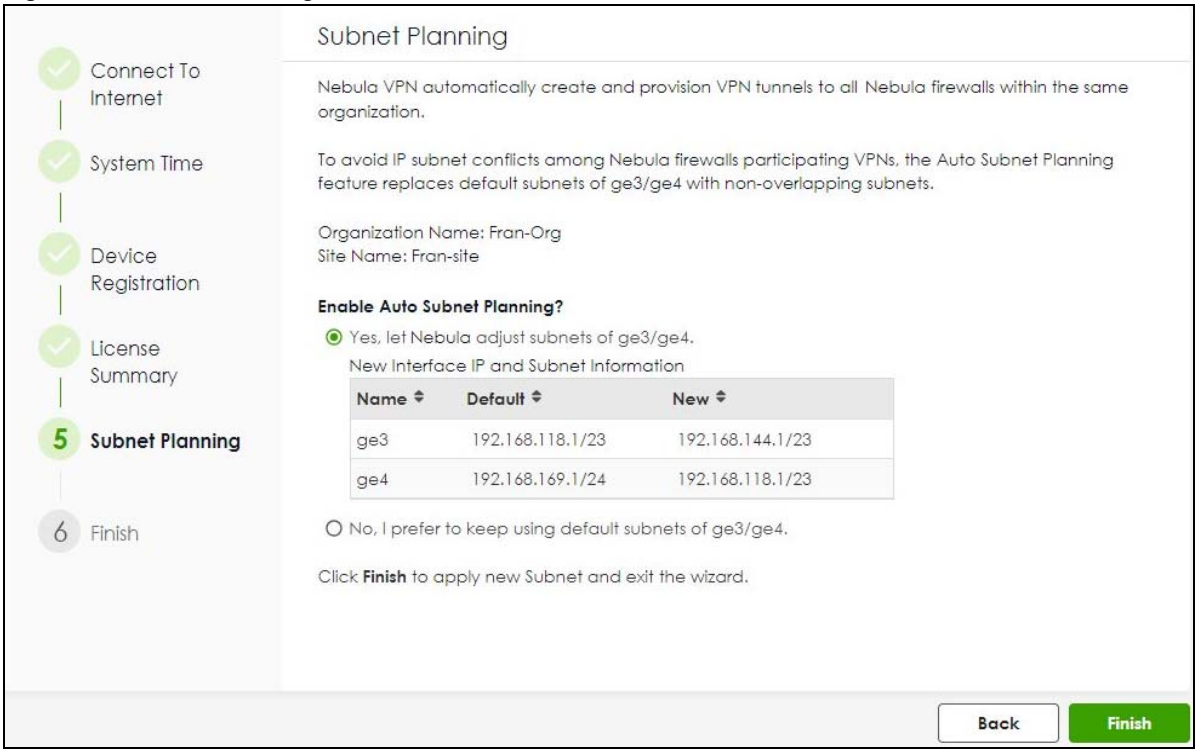
The **Status** column may display **Activated** or **Expired**.

- **Activated**: The service license is enabled.
- **Expired**: The service license has expired. Go to **NCC** > **Organization-wide** > **License & Inventory** to renew your license.

2.7 Wizard - Subnet Planning

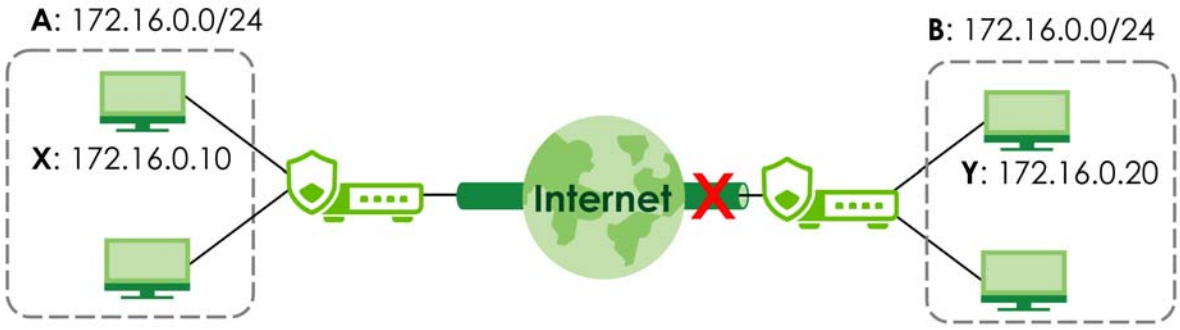
You must register your Zyxel Device to an organization and site in the Nebula Control Center (NCC) to see this screen.

Figure 33 Subnet Planning



If two internal networks (**A** and **B**) in your organization use the same private IP address, they will not be able to communicate with each other through Nebula VPN, as traffic will be routed locally and not through the Zyxel Device. To avoid this, you must let NCC automatically do it (recommended) or manually configure different private IP address ranges for all internal networks in your organization.

Figure 34 IP Address Conflict Causing VPN Failure



Use the **Subnet Planning** screen to select a subnet configuration for the Zyxel Device that is not the same as the subnet configuration in another Zyxel Device in the same organization VPN.

Select **Yes, let Nebula adjust subnets of ge3/ge4** to have the NCC assign a private IP address to your Zyxel Device. Select this if you want your Zyxel Device to join the organization's VPN through the NCC. The assigned IP address will be different from those used by local networks behind other Zyxel Devices in the organization's VPN.

Note: If you apply **Yes, let Nebula adjust subnets of ge3/ge4**, your computer will be temporarily disconnected from the Zyxel Device. Wait 10 seconds for the Zyxel Device to apply the IP address assigned by the NCC.

Note: If your computer is not directly connected to the Zyxel Device, you need to renew the IP address manually or disconnect and reconnect the Ethernet cable to update the IP address.

Select **No, I prefer to keep using default subnets of ge3/ge4** to use the existing IP addresses assigned to the local network behind this Zyxel Device. Select this if you don't want your Zyxel Device to join the organization's VPN through the NCC or you can ensure that this Zyxel Device's IP address is different from the ones used by local networks behind other Zyxel Devices participating in the organization's VPN.

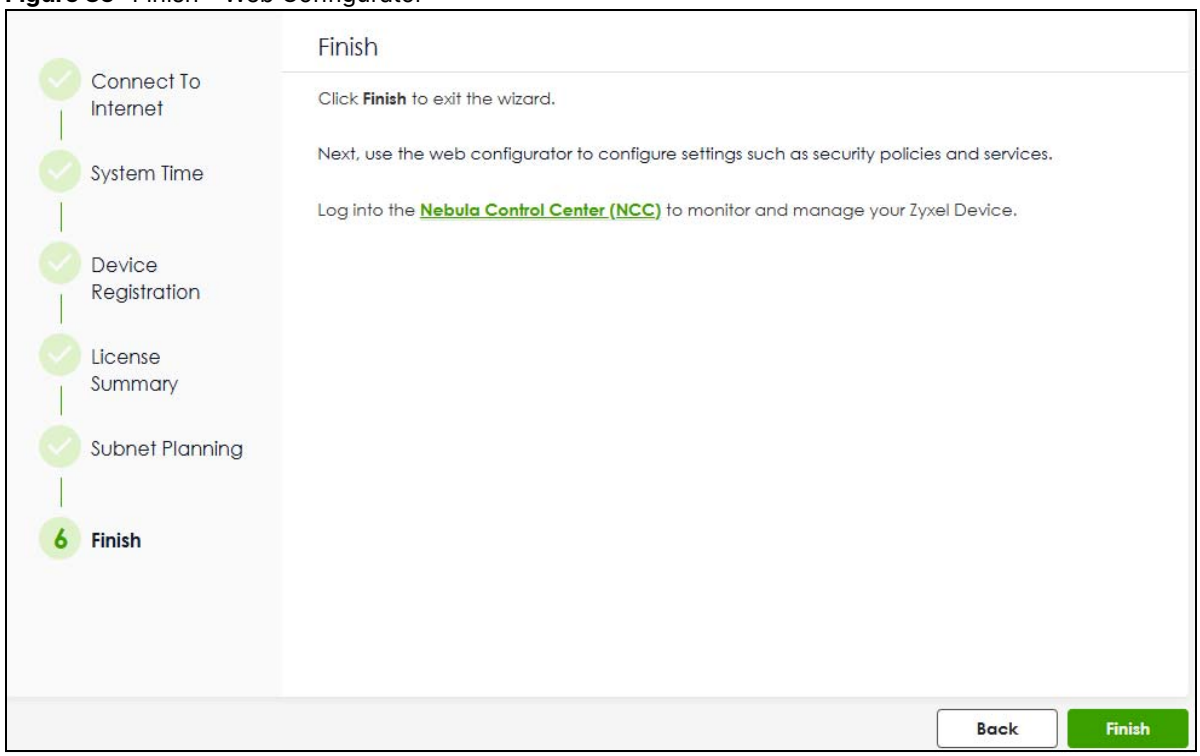
2.8 Finish

Click **Finish** to save all settings to the Zyxel Device and leave the initial wizard.

- To manage security services and policies on this Zyxel Device, log into the Zyxel Device Web Configurator.
- To monitor and manage your Zyxel Devices through the cloud, click **Nebula Control Center (NCC)**.

Note: If you want to run the initial wizard again, you must reset the Zyxel Device. Make sure to back up your current configuration first as you will lose all web configurator settings after the reset.

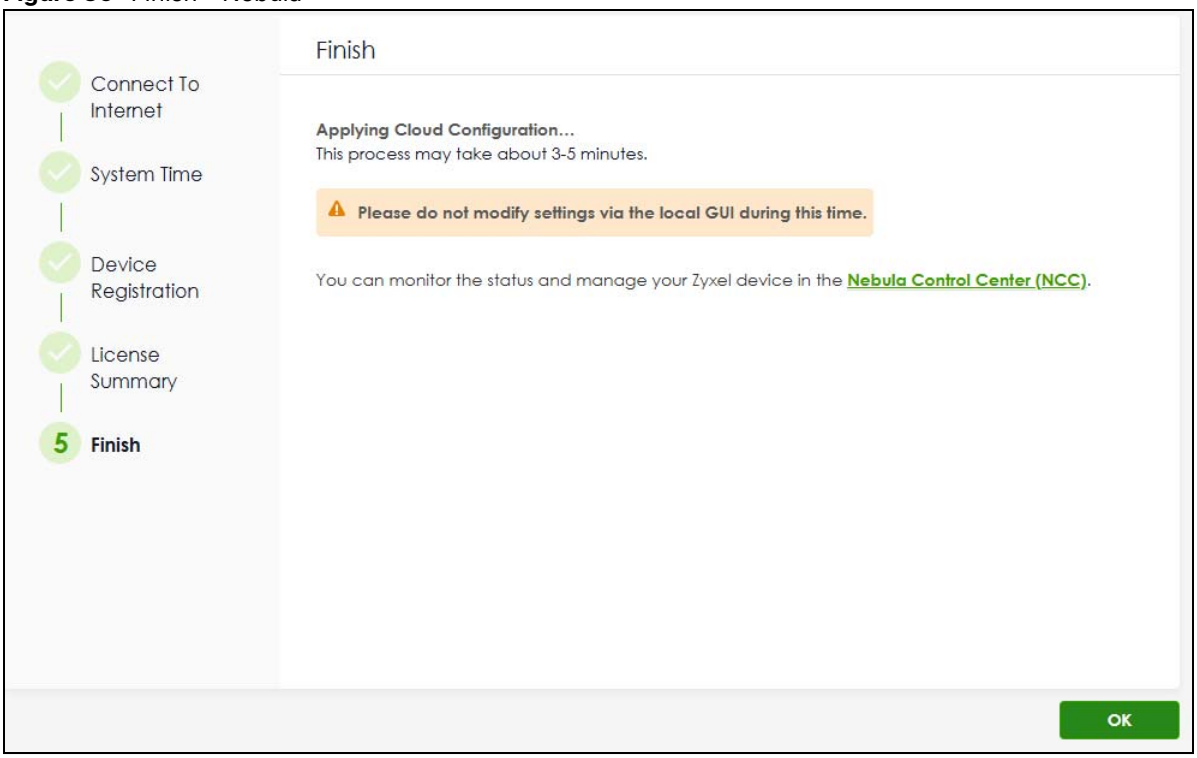
Figure 35 Finish - Web Configurator



- If you chose **Nebula** to initially configure your Zyxel Device, Nebula will send the initial configuration to your Zyxel Device. This may take up to 5 minutes to complete. Click **OK** to close the wizard and wait.

Note: Do not make any changes in the Web Configurator while Nebula is sending the initial configuration.

Figure 36 Finish - Nebula



CHAPTER 3
Hardware, Interfaces and Zones

3.1 Hardware Overview

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

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

Table 9 USG FLEX Series Port Comparison Table

USG FLEX MODELS	USG FLEX 50H	USG FLEX 50HP	USG FLEX 100H	USG FLEX 100HP	USG FLEX 200H	USG FLEX 200HP	USG FLEX 500H	USG FLEX 700H
USB 3.0 Ports	1	1	1	1	1	1	1	1
10 Gbps SFP+ interface	0	0	0	0	0	0	0	2
PoE+ Port	0	1	0	1	0	1	2	2
10/100/1000 Mbps Ethernet Ports	5	5	8	8	6	6	8	8
Multi-Gigabit Ethernet Ports	0	0	0	0	2	2	4	4
Console Port	1 (RJ45)	1 (RJ45)	1 (RJ45)	1 (RJ45)	1 (RJ45)	1 (RJ45)	1 (RJ45)	1 (RJ45)

For information on interface names by model, default port or interface name mapping, and default interface or zone mapping please see Section on page 73.

3.1.1 Multi-Gigabit

Multi-Gigabit Ethernet ports automatically allow connections up to the speed of the connected network device (100M, 1G, 2.5G, 5G, or 10G), and you just need to use a CAT 5e or CAT 6 Ethernet cable. You must use CAT 6A or better Ethernet cables to achieve 10G speeds.

The following table shows which models have which Multi-Gigabit ports.

Table 10 USG FLEX Series Multi-Gigabit Port Comparison

USG FLEX MODELS	USG FLEX 200H	USG FLEX 200HP	USG FLEX 500H	USG FLEX 700H
2.5 Gbps Multi-Gigabit Ethernet Ports	P1, P2	P1, P2	P1, P2, P3, P4	P1, P2
10 Gbps Multi-Gigabit Ethernet Ports				P3, P4

See the following table for the cables required and distance limitation to attain the corresponding speed.

Table 11 Cable Types

CABLE	TRANSMISSION SPEED	MAXIMUM DISTANCE	BANDWIDTH CAPACITY
Category 5	100M	100 m	100 MHz
Category 5e	1G	100 m	100 MHz
Category 6	1G / 10G	100 m:1G 37-50 m:10G	250 MHz
Category 6a	10G	100 m	500 MHz
Category 7	10G	100 m	600 MHz

3.1.2 Default Physical Port – Interface Mapping

You connect cables to the physical ports. You configure interfaces in the web configurator or command line interface (CLI).

The following table shows the default interfaces for each physical port.

Table 12 Default Physical Port – Interface Mapping

PORT / INTERFACE	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14
USG FLEX 50H	ge1	ge2	ge3	ge3	ge3									
USG FLEX 50HP	ge1	ge2	ge3	ge3	ge3									
USG FLEX 100H	ge1	ge2	ge3	ge3	ge3	ge3	ge4	ge4						
USG FLEX 100HP	ge1	ge2	ge3	ge3	ge3	ge3	ge4	ge4						
USG FLEX 200H	ge1	ge2	ge3	ge3	ge3	ge3	ge4	ge4						
USG FLEX 200HP	ge1	ge2	ge3	ge3	ge3	ge3	ge4	ge4						
USG FLEX 500H	ge1	ge2	ge3	ge3	ge3	ge3	ge4	ge4	ge4	ge4	-	-		
USG FLEX 700H	ge1	ge2	ge3	ge3	ge3	ge3	ge4	ge4	ge4	ge4	-	-	-	-

Note: You change the default zone for all interfaces in **Network > Interface** and **Object > Zone**.

The following shows the default zone for each interface.

- ge1 and ge2 are WAN ports
- ge3 and ge4 are LAN ports
- '-' means these ports have no default zone, so you must configure a zone for them in **Network > Interface** and **Object > Zone**

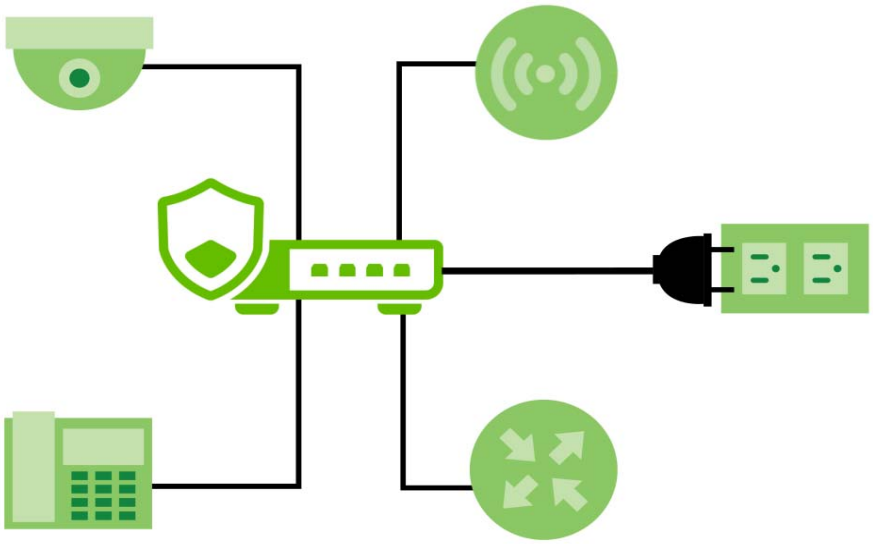
3.1.3 PoE

The Zyxel Device is a Power Sourcing Equipment (PSE) because it provides a source of power through its Ethernet ports. Each device that receives power through an Ethernet port is a Powered Device (PD). A Powered Device (PD) is a device that receives power through PoE, such as an IP camera, a wireless router, an IP telephone or a general outdoor router.

Note: Do not connect the Zyxel Device PoE+ port to a non-Powered Device. If you need to connect a non-Powered Device to the Zyxel Device PoE+ port, make sure to disable PoE in **Network** > **Interface** > **Port** first.

The following example figure shows a Zyxel Device supplying PoE (Power over Ethernet) to PDs that are not within reach of a power outlet.

Figure 37 PoE Application



The Zyxel Device can adjust the power supplied to each PD according to the PoE standard the PD supports. PoE standards are:

- IEEE 802.3af Power over Ethernet (PoE)
- IEEE 802.3at Power over Ethernet (PoE+)

The following table describes the PoE features of the Zyxel Device by PoE standard.

Table 13 Zyxel Device PoE Features

POE FEATURES	USG FLEX 50HP	USG FLEX 100HP	USG FLEX 200HP	USG FLEX 500H	USG FLEX 700H
IEEE 802.3 at PoE+	Port 5	Port 8	Port 2	Port 3-4	Port 3-4
Power Management Mode	Consumption	Consumption	Consumption	Consumption	Consumption
PoE Power Budget	30W	30W	30W	30W	30W

Table 14 PoE Standards

POE FEATURES	POE	POE+
IEEE Standard	IEEE 802.3af	IEEE 802.3at
PoE Type	Type 1	Type 2
Switch Port Power		
IEEE Power Classification	Class 0, 1, 2, 3	Class 4
Maximum Power Per Port	15.4 W	30 W
Port Voltage Range	44 - 57 V	50 - 57 V
Cables		

Table 14 PoE Standards

POE FEATURES	POE	POE+
Twisted Pairs Used	2-pair	2-pair
Supported Cables	Cat3 or Cat5	Cat5 or better

3.1.4 Front Panels

The LED indicators are located on the front panel.

Figure 38 USG FLEX 50H Front Panel

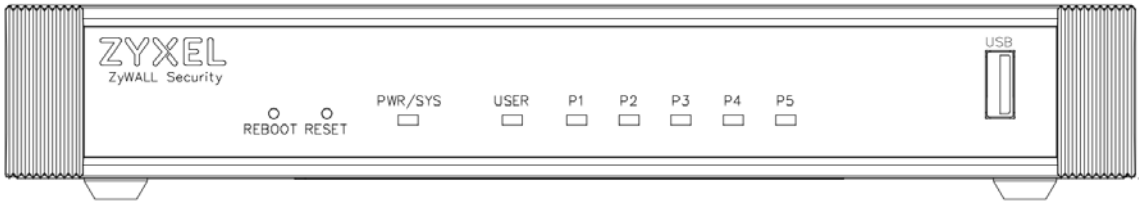


Figure 39 USG FLEX 50HP Front Panel

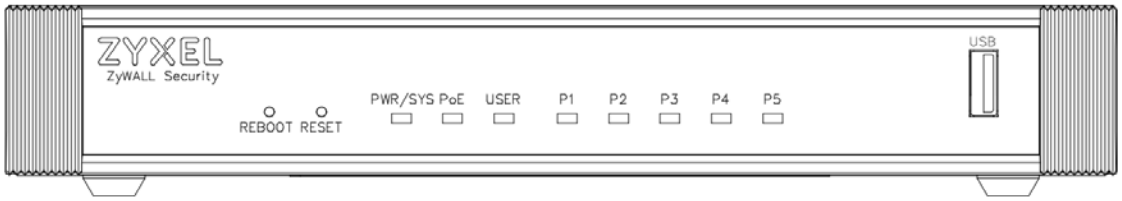


Figure 40 USG FLEX 100H Front Panel

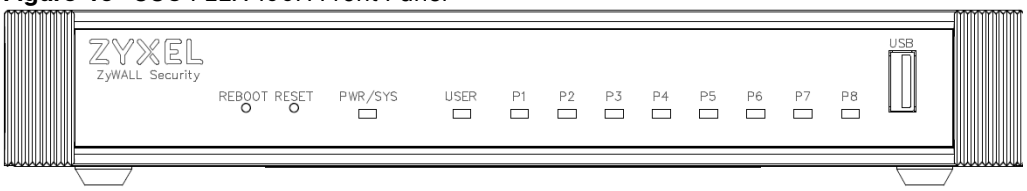


Figure 41 USG FLEX 100HP Front Panel

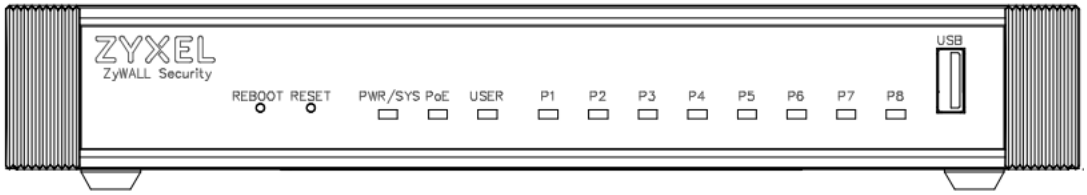


Figure 42 USG FLEX 200H Front Panel



Figure 43 USG FLEX 200HP Front Panel

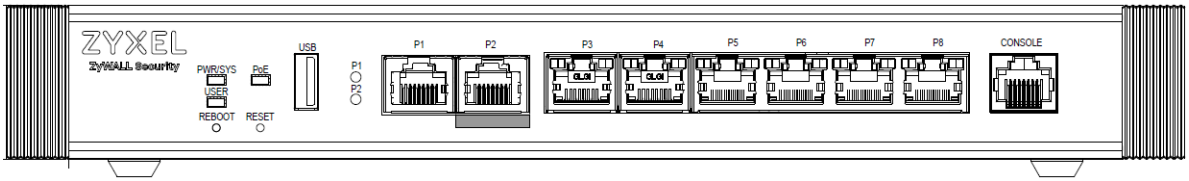


Figure 44 USG FLEX 500H Front Panel

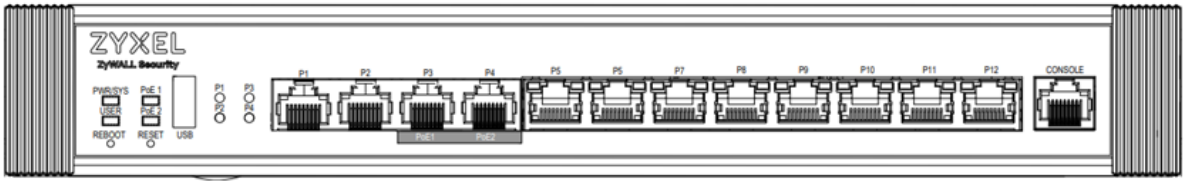
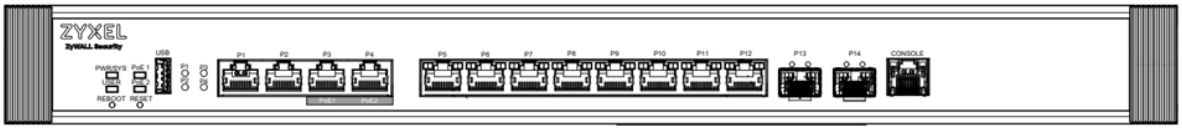


Figure 45 USG FLEX 700H Front Panel



The following table describes the front panel LEDs.

Table 15 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR / 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 or upgrading firmware
	Red	On	The Zyxel Device has an error or has failed.
		Blinking	The Zyxel Device is returning to factory defaults.
USER	Green	On	There are accounts with **User Type** set as **admin** logged into the Zyxel Device.
		Blinking	New firmware is available or your license has expired.
	Amber	On	There are IP addresses locked out of the Zyxel Device.
		Off	USER LED is not enabled in **System** > **Settings**.
PoE (PoE1/PoE2)	Green	On	The PoE connected to this port is in AT mode (PoE AT enabled).
	Amber	On	The PoE connected to this port is in AF mode (PoE AF enabled)
		Off	No PoE is connected to this port (PoE disabled).
P1-P5 (USG FLEX 50H / 50HP); P1-P8 (USG FLEX 100H / 100HP) P3-P8 (USG FLEX200 / 200HP) P5-P12 (USG FLEX 500H / 700H)	Amber	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.
	Green	On	This port has a successful 1 Gbps link.
		Blinking	The Zyxel Device is sending or receiving packets on this port at 1 Gbps.
		Off	There is no connection on this port.
P1, P2 (USG FLEX 200 / 200HP) P1-P4 (USG FLEX 500H)	Sky Blue	On	This port has a successful 2.5 Gbps link.
		Blinking	The Zyxel Device is sending or receiving packets on this port at 2.5 Gbps.
	Green	On	This port has a successful 1 Gbps link.
		Blinking	The Zyxel Device is sending or receiving packets on this port at 1 Gbps.
	Amber	On	This port has a successful 100 Mbps link.
		Blinking	The Zyxel Device is sending or receiving packets on this port at 100 Mbps.
		Off	There is no connection on this port.

Table 15 LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
P3, P4 (USG FLEX 700H)	Blue	On	This port has a successful 10 Gbps link.
		Blinking	The Zyxel Device is sending or receiving packets on this port at 10 Gbps.
	Purple	On	This port has a successful 5 Gbps link.
		Blinking	The Zyxel Device is sending or receiving packets on this port at 5 Gbps.
	Sky Blue	On	This port has a successful 2.5 Gbps link.
		Blinking	The Zyxel Device is sending or receiving packets on this port at 2.5 Gbps.
	Green	On	This port has a successful 1 Gbps link.
		Blinking	The Zyxel Device is sending or receiving packets on this port at 1 Gbps.
	Amber	On	This port has a successful 100 Mbps link.
		Blinking	The Zyxel Device is sending or receiving packets on this port at 100 Mbps.
		Off	There is no connection on this port.
P13, P14 SPF+ (USF FLEX 700H)	Blue	On	This port has a successful 10 Gbps link.
		Blinking	The Zyxel Device is sending or receiving packets on this port at 10 Gbps.
	Green	On	This port has a successful 1 Gbps link.
		Blinking	The Zyxel Device is sending or receiving packets on this port at 1 Gbps.
		Off	There is no connection on this port.

The following table describes the ports on the front panel.

Table 16 Front Panel Ports

LABEL	DESCRIPTION
REBOOT	Press the button for about 5 seconds to reboot the Zyxel Device.
RESET	Press the button in for about 7 seconds (or until the **PWR/SYS** LED starts to blink), then release it to return the Zyxel Device to the default configuration using the system-default.conf file. You may do this if you forgot the login password. You should use the Web Configurator (**Maintenance > Firmware/File Manager > Configuration File**) to create a backup file with a '.conf' extension first. Note: All configuration files including those you saved on the Zyxel Device will be deleted. The **Login** password returns to the password on the back label or 1234, and the LAN IP address returns to 192.168.168.1. Note: License registration bindings, IPSec certificates, remote access VPN certificates, trusted certificates and two-factor authentication (2FA) information are retained. Press the button in for more than 30 seconds, then release it to return the Zyxel Deviceto factory defaults and remove all license registration bindings, certificates, and two-factor authentication (2FA) information. You may do this if the Zyxel Device needs to be replaced or you want to sell it to another person. You should use the Web Configurator (**Maintenance > Firmware/File Manager > Configuration File > Recovery Manager**) to create a recovery file with a '.rbf' extension first if you want to upload it to a replacement Zyxel Device later.
USB	Connect a storage device for system logs and storage.
P1-P8 (USG FLEX 200H / 200HP) P1-P12 (USG FLEX 500H / 700H)	These are Multi-Gigabit 1G/2.5G/10G RJ-45 Ethernet ports.

Table 16 Front Panel Ports (continued)

LABEL	DESCRIPTION
P13-P14 (USG FLEX 700H)	These are 10G SFP+ ports.
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

3.1.5 Rear Panels

The connection ports are located on the rear panel.

Figure 46 USG FLEX 50H Rear Panel

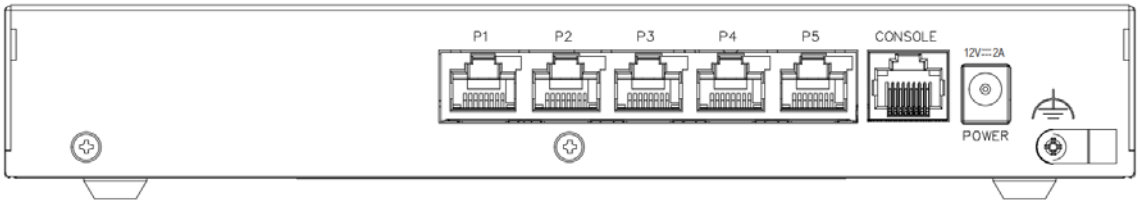


Figure 47 USG FLEX 50HP Rear Panel

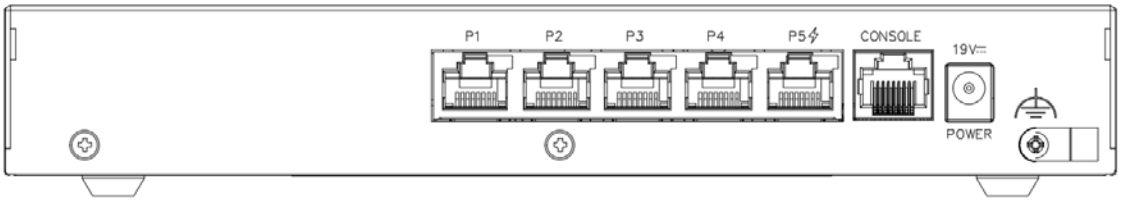


Figure 48 USG FLEX 100H Rear Panel

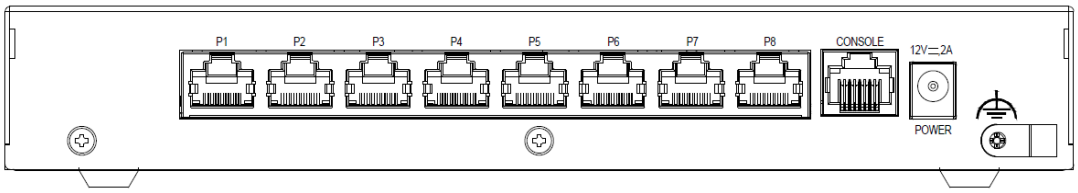


Figure 49 USG FLEX 100HP Rear Panel

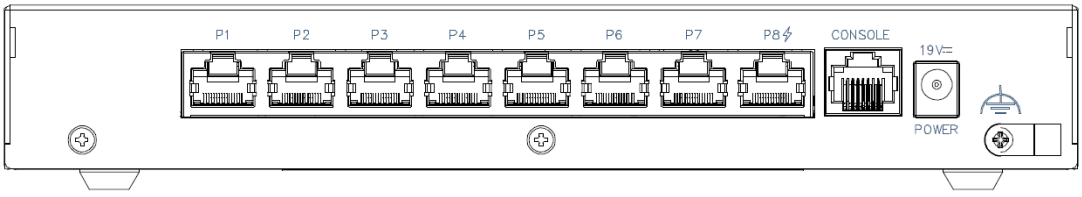


Figure 50 USG FLEX 200H Rear Panel



Figure 51 USG FLEX 200HP Rear Panel



Figure 52 USG FLEX 500H Rear Panel

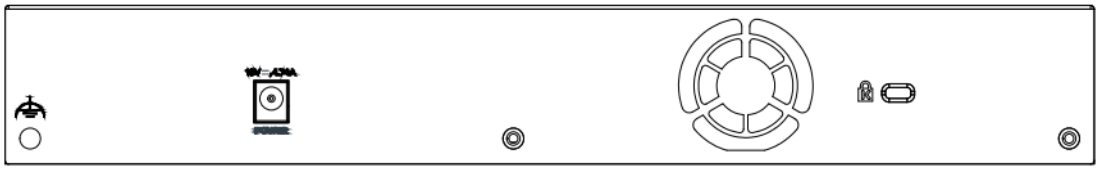
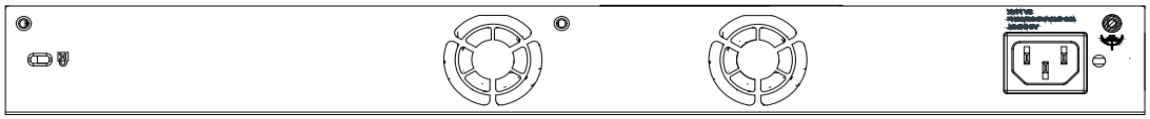


Figure 53 USG FLEX 700H Rear Panel



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

The following table describes the items on the rear panel.

Table 17 Rear Panel Items

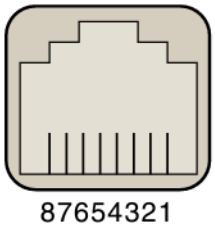
LABEL	DESCRIPTION
Power	Use the included power cord to connect the power socket to a power outlet. Turn the power switch on if your Zyxel Device has a power switch.
Console	You can use the console port to manage the Zyxel Device using CLI commands. You will be prompted to enter your user name and password. 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
P1-P5 (USG FLEX 50H / 50HP) P1-P8 (USG FLEX 100H / 100HP)	These are 1G RJ-45 Ethernet ports.
Fan	The fans are for cooling the Zyxel Device. Make sure they are not obstructed to allow maximum ventilation.
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.

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

3.1.6 Console Port Pin Connectors

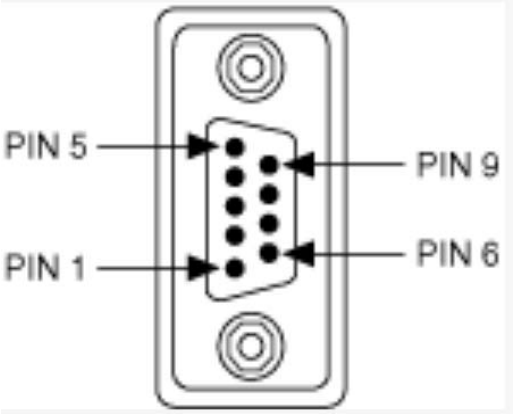
The RJ-45 connector pins are as follows.

Figure 54 RJ-45 Connector Pins



The DB-9 connector pins are as follows.

Figure 55 DB-9 Connector Pins



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

Table 18 Cable Pinouts for RJ-45 to DB-9

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

These are the signal names.

Table 19 Signal Names

SIGNAL	SIGNAL NAME
RXD	Receive Data
TXD	Transmit Data
DTR	Data Terminal Ready
GND	Ground
DSR	Data Set Ready
RTS	Request to Send
CTS	Clear to Send
RI	Ring Indicator
NC	Not Connected

3.2 Installation Scenarios

The Zyxel Device can be:

- Placed on a desktop.
- Wall-mounted on a wall.
- Rack-mounted on a standard EIA rack.

The following table summarizes the installation scenarios of the Zyxel Device by model.

Table 20 USG FLEX Series Installation Comparison Table

USG FLEX MODELS	USG FLEX 50H / 50HP	USG FLEX 100H / 100HP	USG FLEX 200H / 200HP	USG FLEX 500H	USG FLEX 700H
Rubber feet for desktop placement	Yes	Yes	Yes	Yes	Yes
Wall Mounting	Yes	Yes	Yes	No	No
Rack Mounting	No	No	No	Yes	Yes

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.

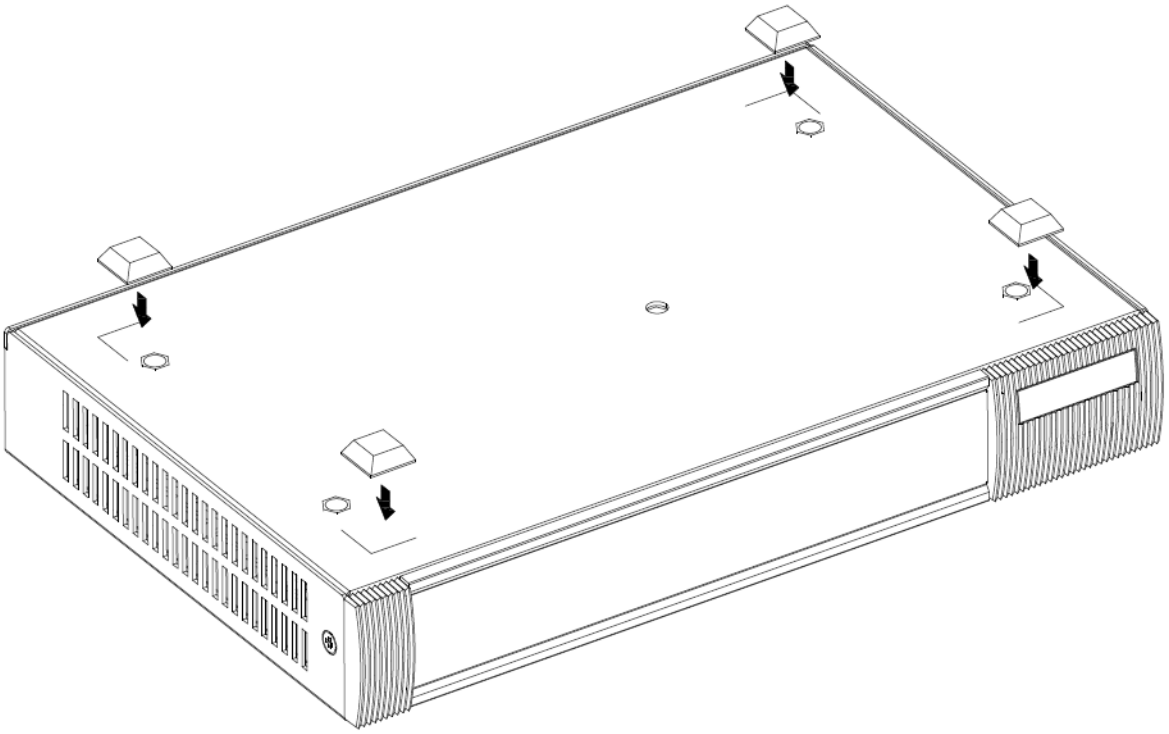
3.2.1 Desktop Installation Procedure

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 56 Attaching Rubber Feet



4 Set the Zyxel Device on a smooth, level surface strong enough to support the weight of the Zyxel Device and the connected cables. Make sure there is a power outlet nearby.

Note: Make sure to use the rubber feet when stacking the Zyxel Devices on a desk.

3.2.2 Rack-mounting

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

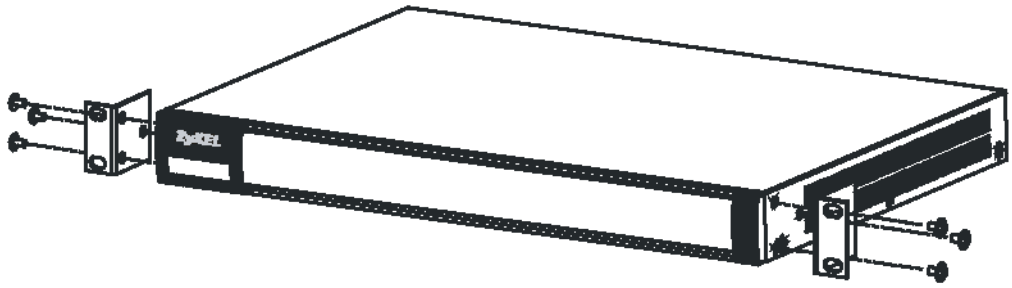
Use a #2 Phillips screwdriver to install the screws.

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

1 Align one bracket with the holes on one side of the Zyxel Device and secure it with the included bracket screws (smaller than the rack-mounting screws).

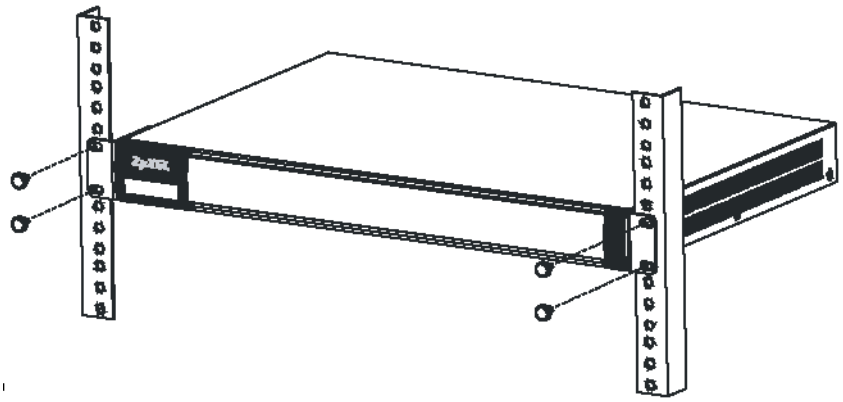
2 Attach the other bracket in a similar fashion.

Figure 57 Attach Brackets



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

Figure 58 Mount on Rack



Note: Make sure there is at least 100 mm of clearance at the sides and 100 mm in the rear to allow air circulation and the attachment of cables and the power cord. When stacking in a rack, make sure there is at least 40 mm of clearance between Zyxel Devices.

3.2.3 Wall-mounting

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

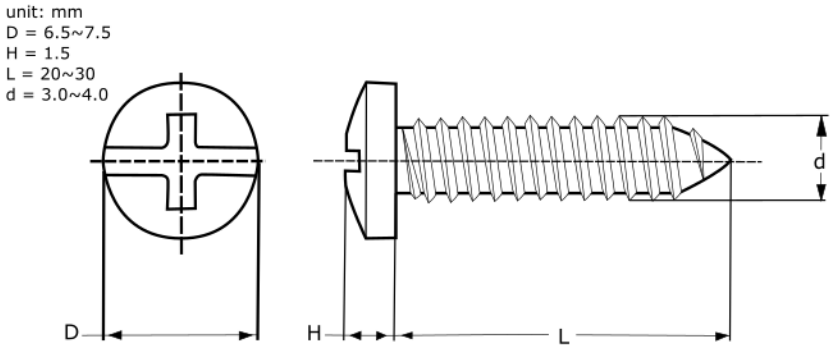
The following table lists the distance “X” between mounting holes for each model:

Table 21 Distance “X” Between FLEX Mounting Holes

MODEL NAME	DISTANCE “X”
USG FLEX 50H	174 mm (6.85”)
USG FLEX 50HP	174 mm (6.85”)
USG FLEX 100H	174 mm (6.85”)
USG FLEX 100HP	174 mm (6.85”)
USG FLEX 200H	206 mm (8.11”)
USG FLEX 200HP	206 mm (8.11”)

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

Figure 59 Wall Mounting Screw Specifications



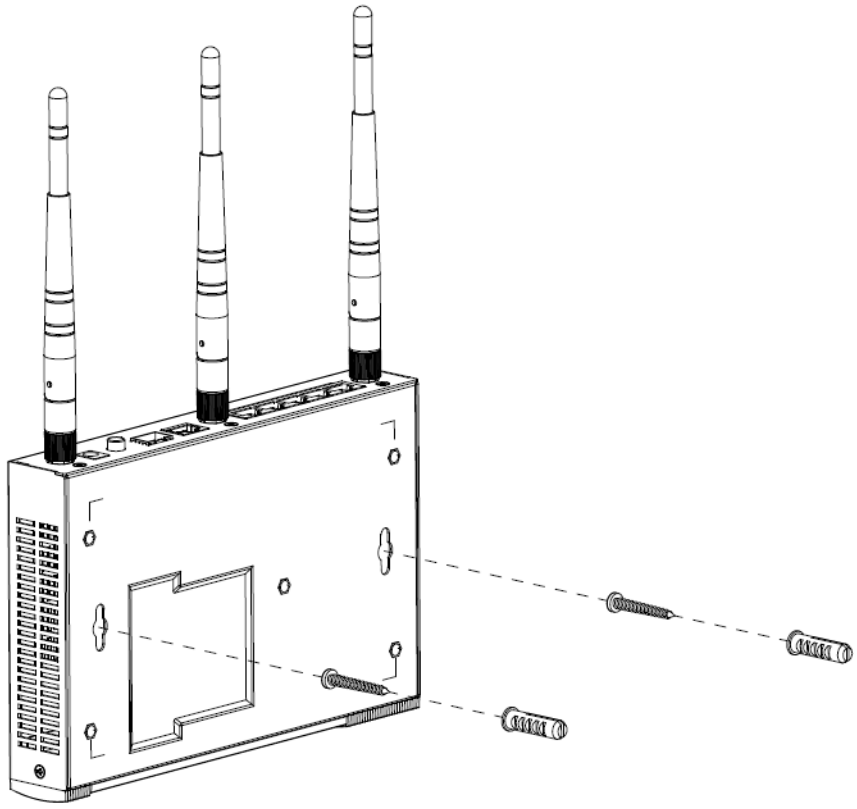
2 Screw two screws with 6 mm – 8 mm (0.24" – 0.31") wide heads into the screw anchors. Do not screw the screws all the way in to the wall; leave a small gap between the head of the screw and the wall.

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

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

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

Figure 60 Wall Mounting



Note: 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.

Make sure there is 100 mm of clearance at the sides and 1 – 1.5 mm distance between the screw head and the wall to allow air circulation and the attachment of cables and the power cord.

3.3 Power Cord Lock

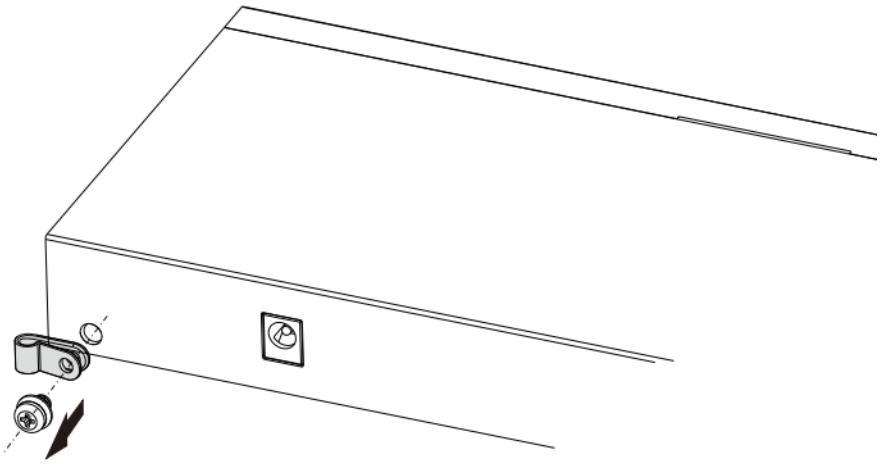
Follow the procedures below to secure the power cord connected to the Zyxel Device.

3.3.1 Procedure A

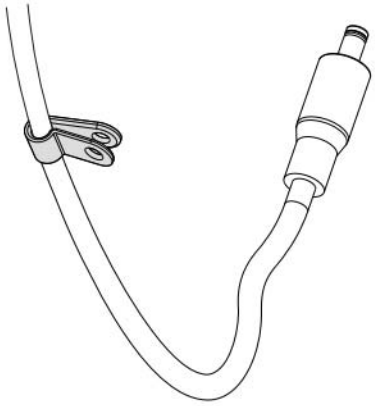
Follow this procedure for the following models:

- USG FLEX 50H
- USG FLEX 100H
- USG FLEX 200H
- USG FLEX 500H
- USG FLEX 50HP
- USG FLEX 100HP
- USG FLEX 200HP

1 Use a screw driver to remove the power cord lock and the screw from the Zyxel Device.

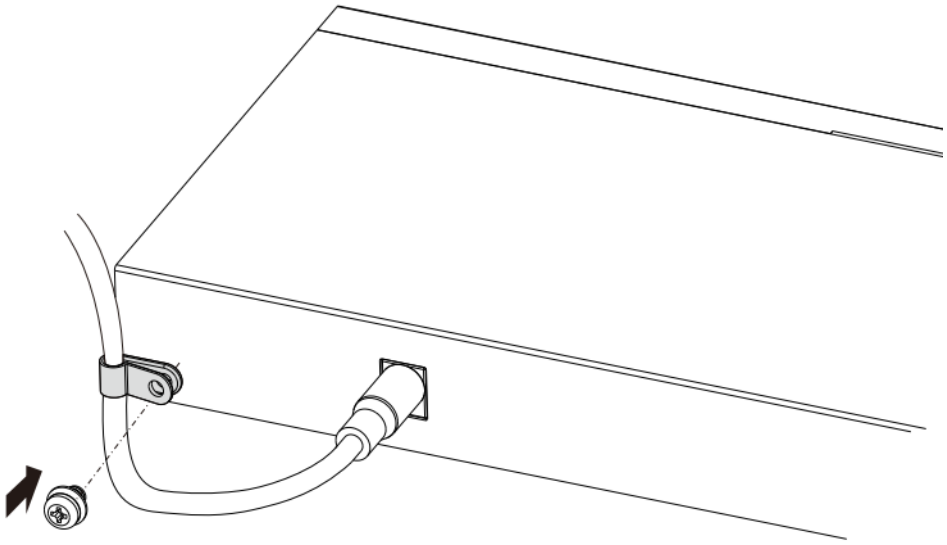


2 Attach the Zyxel Device power cord through the power cord lock.



3 Connect the power cord to the Zyxel Device power socket.

4 Use the screw driver to secure the power cord lock and the screw with the power cord to the hole next to the power socket.

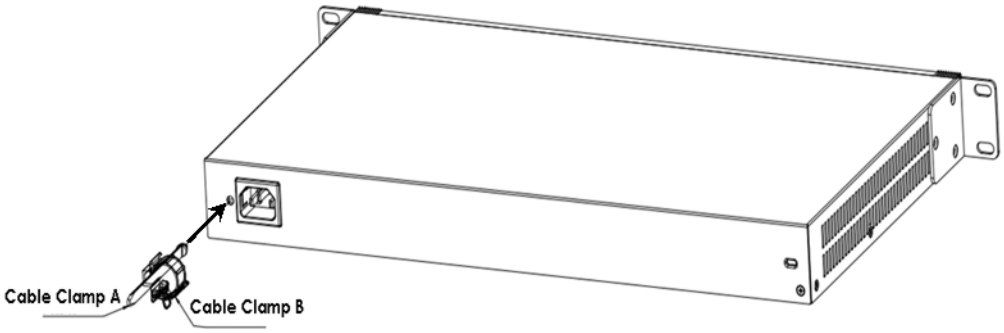


3.3.2 Procedure B

Follow this procedure for:

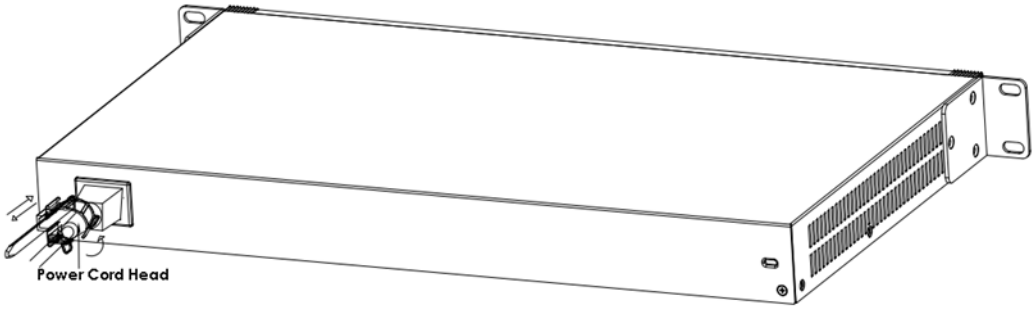
- USG FLEX 700H

1 Insert **Cable Clamp A** into the case hole.



2 Connect the power cord to the Zyxel Device power socket.

3 Open **Cable Clamp B** and attach it to the power cord. Make sure **Cable Clamp B** covers the head of the power cord.



4 Close **Cable Clamp B** to secure the power cord to the power socket.

CHAPTER 4
Dashboard

4.1 Dashboard Overview

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

4.1.1 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.

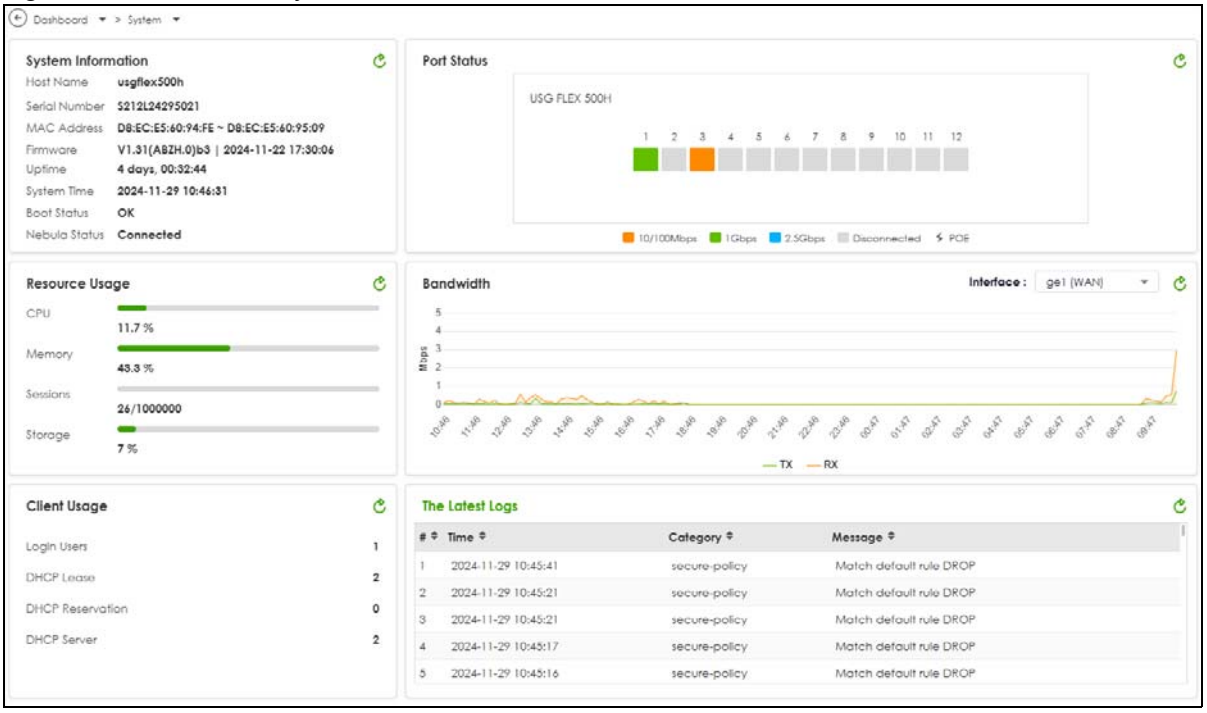
Use the **Dashboard** screens to view the following.

- System Information Screen on page 75
- Port Status Screen on page 77
- Resource Usage Screen on page 78
- Bandwidth on page 80
- Client Usage Screen on page 81
- The Latest Logs Screen on page 81
- The Security Screen on page 82

4.2 The System Screen

The **System** screen displays when you log into the Zyxel Device or click **System** in the navigation panel. The **System** screen displays general device information, system resource usage, and interface status in widgets that you can re-arrange to suit your needs. You can also click the refresh icon ( ) to refresh individual widgets.

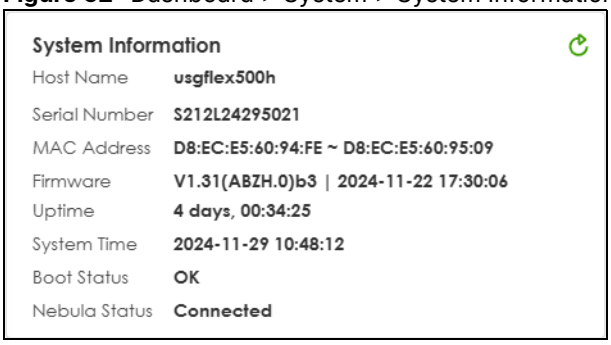
Figure 61 Dashboard > System



4.2.1 System Information Screen

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

Figure 62 Dashboard > System > System Information



The table describes the fields in this screen.

Table 22 Dashboard > System > System Information

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

Table 22 Dashboard > System > System Information (continued)

LABEL	DESCRIPTION
Firmware	This field displays the version number and date of the firmware the Zyxel Device is currently running. Click the link to open the **File Manager** screen where you can upload firmware.
Uptime	This field displays how long the Zyxel Device has been running since it last restarted or was turned on.
System Time	This field displays the current date and time in the Zyxel Device. The format is yyyy-mm-dd hh:mm:ss.
Boot Status	This field displays details about the Zyxel Device's startup state. **OK - Boot success:** The Zyxel Device has started up successfully. **OK - Firmware update at yyyy/mm/dd hh:mm:** This displays the date and time when the Zyxel Device last updated the firmware successfully. **OK - Factory default at yyyy/mm/dd hh:mm:** This displays the date and time when the Zyxel Device was last reset to the factory default settings and rebooted successfully. **OK - User reboot at yyyy/mm/dd hh:mm:** This displays the date and time when the Zyxel Device last rebooted successfully. **OK - Reset default configuration at yyyy/mm/dd hh:mm:** This occurs when the Zyxel Device starts for the first time or you reset the Zyxel Device to the factory default settings. **OK - System recovery at yyyy/mm/dd hh:mm:** This displays the date and time when the Zyxel Device last underwent system recovery and rebooted successfully. **OK - Apply configuration xxxx.conf at at yyyy/mm/dd hh:mm:** This displays the date and time when the Zyxel Device last applied the configuration file and rebooted successfully. **OK - Switch to (1st|2nd) partition at yyyy/mm/dd hh:mm:** This displays the date and time when the Zyxel Device last rebooted using firmware in the backup partition. **OK - Reset admin password at yyyy/mm/dd hh:mm:** This displays the date and time when the Zyxel Device reset the admin password using the "atkz-g" command and rebooted successfully.

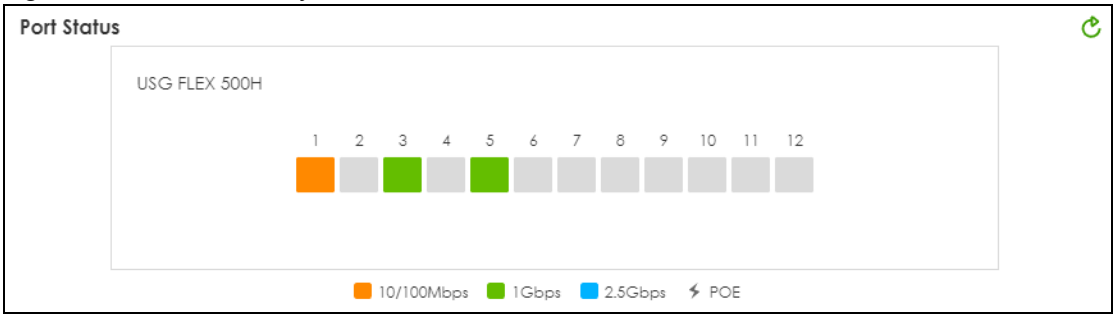
Table 22 Dashboard > System > System Information (continued)

LABEL	DESCRIPTION
Boot Status	**WARN - 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. See Section 32.1.3 on page 656 for more information on configuration file flow at restart. **WARN - Fallback to lastgood configuration after firmware update at yyyy/mm/dd hh:mm:** This displays the date and time when the Zyxel Device was last unable to apply the startup-config.conf configuration file after firmware update and fell back to the lastgood.conf configuration file. See Section 32.1.3 on page 656 for more information on configuration file flow at restart. **ERROR - 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). See Section 32.1.3 on page 656 for more information on configuration file flow at restart. **ERROR - Fallback to system default configuration after firmware update at yyyy/mm/dd hh:mm:** This displays the date and time when the Zyxel Device was unable to apply the lastgood.conf configuration file after the firmware update and fell back to the system default configuration file (system-default.conf). See Section 32.1.3 on page 656 for more information on configuration file flow at restart. **ERROR - Firmware update failed at yyyy-mm-dd hh:mm**: This displays the date and time when the Zyxel Device failed to update firmware due to an active process. During a firmware update, the Zyxel Device temporarily unmounts the partition to ensure a safe upgrade. If there are any active processes on the partition at that time, the Zyxel Device will try to terminate them. If the Zyxel Device cannot terminate these processes, the firmware update will fail.
Nebula Status	The field displays the connection status between the Zyxel Device and the Nebula Control Center (NCC). **Connected** - The Zyxel Device has an Internet connection with the NCC. **Disconnected** - The Zyxel Device does not have an Internet connection with the NCC. **Unknown** - The Zyxel Device was unable to receive a timely response from the Nebula server when checking the Internet connection with the NCC. Go to **Maintenance** > **Diagnostics** > **Network Tool**, select **Nebula Status**, and click **Test** to verify if the Zyxel Device can properly connect to the NCC over the Internet. **No Site Assignment** - The Zyxel Device is registered with the NCC, but is not assigned to a site. **Disabled** - The Internet connection from the Zyxel Device to the NCC was disabled using the Command Line Interface (CLI). Note: To transfer your Zyxel Device management to the NCC, first make sure your Zyxel Device is connected to the Internet.

4.2.2 Port Status Screen

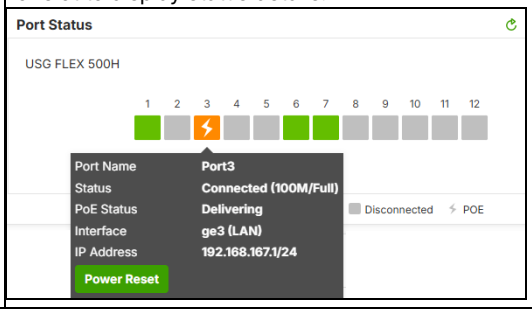
The **Port Status** screen displays Zyxel Device's ports and connections status.

Figure 63 Dashboard > System > Port Status



The following table describes the labels in this screen.

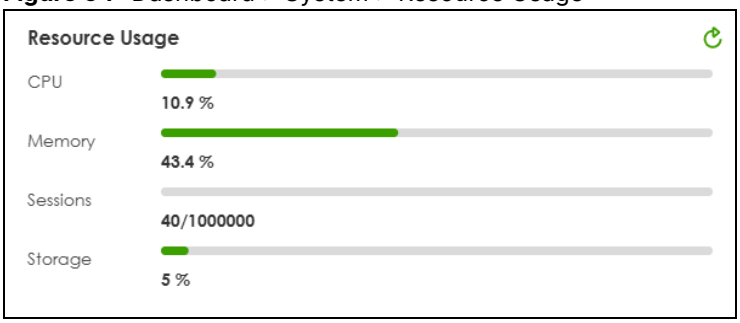
Table 23 Dashboard > System > Port Status

LABEL	DESCRIPTION
Port Status	This field displays details about the status of the Zyxel Device's ports and connections. An unconnected interface or slot appears grayed out. Hover your cursor over a connected interface or slot to display status details. 
The following labels display when you hover your cursor over a connected interface or slot.	
Name	This field displays the name of each interface.
Status	This field displays the current status of each interface or device installed in a slot. The possible values depend on what type of interface it is. • **Disconnected** - 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. • **Connected (Speed/Duplex)** - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (**Full** or **Half**).
PoE Status	This field displays only when the PoE port is connected to a PD (powered device). • **Delivering** - The Zyxel Device is supplying power to the PD. • **Disabled** - The Zyxel Device is not supplying power to the PD. The port is temporarily disabled after you click the **Power Reset**. See My Powered Devices (PDs) are not receiving power. for troubleshooting if the problem persists after the reset.
Interface	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).
Power Reset	Click **Power Reset** to power off the PD connected to the port, by temporarily disabling then re-enabling PoE. This button only appears when the PoE port is connected to a PD.

4.2.3 Resource Usage Screen

Click the bar to see a graphic on that resource.

Figure 64 Dashboard > System > Resource Usage



The table describes the fields in the screen.

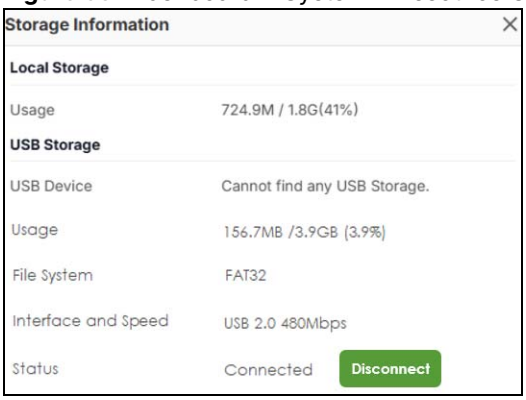
Table 24 Dashboard > System > Resource Usage

LABEL	DESCRIPTION
CPU	This field displays what percentage of the Zyxel Device's processing capability is currently being used. It is an average of all core usage. Click this field to display a chart of the Zyxel Device's recent CPU usage for each core within a specified time period. CPU usage may appear temporarily high when creating graphic-intensive statistics and reports. You may ignore it, and observe the long-term usage.
Memory	This field displays what percentage of the Zyxel Device's RAM is currently being used. Click this field to display a chart of the Zyxel Device's recent system and fastpath memory usage.
Sessions	This field shows how many sessions, established and non-established, that pass through/from/to/within the Zyxel Device. Click this field to display a chart of Zyxel Device's session usage within a specified time period.
Storage	This field displays the percentage of storage currently being used on the Zyxel Device. Click this field to view more information about the Zyxel Device's storage and the connected USB storage device. See Section 4.2.3.1 on page 79 for more details.

4.2.3.1 Storage Information

The **Storage Information** screen displays information of the Zyxel Device's storage and the connected USB storage device.

Figure 65 Dashboard > System > Resource Usage > Storage



The table describes the fields in the screen.

Table 25 Dashboard > System > Resource Usage > Storage

LABEL	DESCRIPTION
Local Storage	
Usage	This field displays the used space (in MB or GB), available space (in MB or GB), and the percentage of used space on the Zyxel Device. Local storage refers to the permanent (flash) memory, where data is retained after rebooting. It stores database files, including actual data, logs, backups, packet capture files, and configuration files. New logs and files are not saved when storage is full. You can try manually deleting logs. See My Zyxel Device's local storage is full. for details.
USB Storage	
USB Device	This field displays the name of the USB storage device. See Table 298 on page 649 for more information on USB storage.
Usage	This field displays the used space (in MB or GB), available space (in MB or GB), and the percentage of used space on the USB storage device.
File System	This field displays what file system the USB storage device is formatted with. The supported formats for the Zyxel Device are FAT16, FAT32, EXT3, and EXT4. See the troubleshooting My USB storage device is not compatible with the Zyxel Device. for how to change the format of your USB storage device.
Interface and Speed	This field displays the USB standard and the connection speed the USB storage device supports.
Status	This field displays the connecting status of the USB storage device. • **Connected** - you can have the Zyxel Device use the USB storage device. • **Connecting** - the Zyxel Device is mounting the USB storage device. • **Disconnected** - the connected USB storage device was manually unmounted by using the **Disconnect** button or for some reason the Zyxel Device cannot mount it. Click the **Disconnect** button to stop the Zyxel Device from using the USB storage device. If you disconnect the USB storage device from the Zyxel Device, you can then use click **Connect** to reconnect the USB storage device.

4.2.4 Bandwidth

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

Figure 66 Dashboard > System > Bandwidth



This table describes the fields in the above screen.

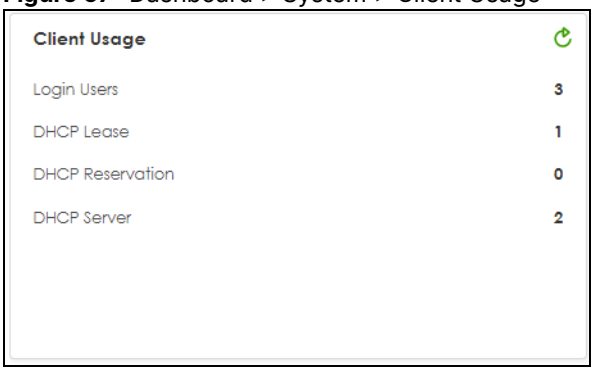
Table 26 Dashboard > Tx/Rx Statistics

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.

4.2.5 Client Usage Screen

This screen displays the number of users logged into the Zyxel Device and a summary of the DHCP settings status. Click the links to go to the **Login Users** or the **DHCP Table** screen.

Figure 67 Dashboard > System > Client Usage



This table describes the fields in the above screen.

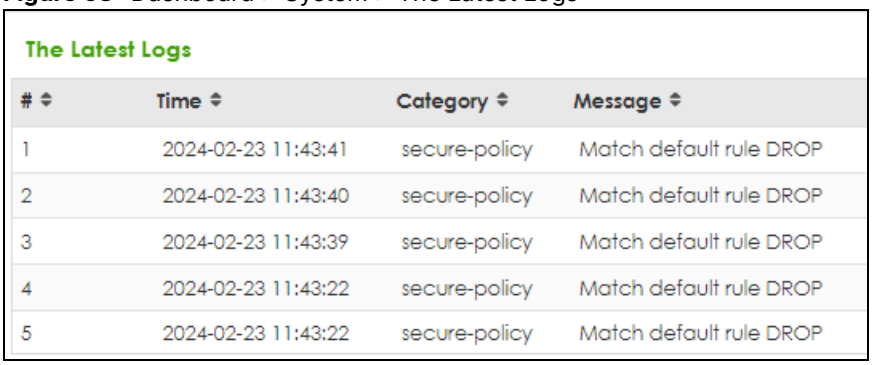
Table 27 Dashboard > System > Client Usage

LABEL	DESCRIPTION
Login Users	This field displays the number of users that are currently logged into the Zyxel Device.
DHCP Lease	This field displays the number of IP addresses that are leased for clients.
Reservation	This field displays the number of IP addresses that are reserved for the MAC addresses.
DHCP Server	This field displays the number of interface that the DHCP server is enabled on the Zyxel Device.

4.2.6 The Latest Logs Screen

In this screen click **The Latest Logs** to go to **Log & Report > Log / Events**.

Figure 68 Dashboard > System > The Latest Logs



The table describes the fields in the screen.

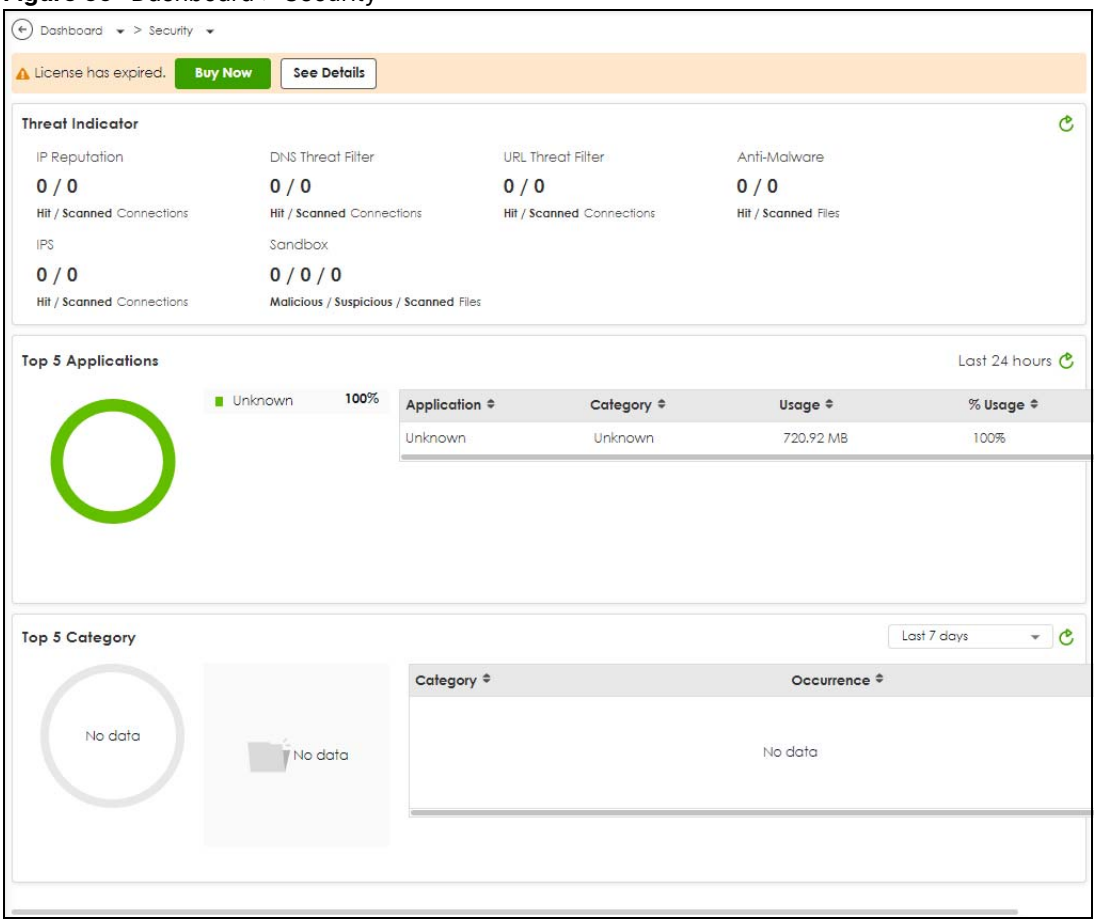
Table 28 Dashboard > System > The Latest Log

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.
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.
Priority	This field displays the severity of the log.

4.3 The Security Screen

Use the **Security** screen to check security status information about the Zyxel Device. If a license has expired, you will see a reminder in this screen. You need to renew the license in order to keep using the feature. Click **Buy Now** to go to Marketplace to purchase a new license. Click **See Details** to go to the Zyxel web page to find more information on licenses for your Zyxel Device.

Figure 69 Dashboard > Security



This screen gives the following information:

- The amount of scanned traffic
- The number of scanned connections for URL threat filtering
- The number of scanned files for anti-malware
- The number of scanned connections for IPS
- The number of scanned files for sandbox.
- Top 5 applications that are used the most
- Top 5 Categories that are detected the most

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

PART II
Technical Reference

CHAPTER 5
Monitor

5.1 Overview

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

5.1.1 What You Can Do in this Chapter

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

- Use the **Traffic Statistics > Application Usage** (Section 5.2 on page 86) screen to view application statistics.
- Use the **Traffic Statistics > Port** (Section 5.3 on page 88) screen to view the packets statistics for each port selected for monitoring.
- Use the **Traffic Statistics > Interface** (Section 5.4 on page 89) screen to view the packets statistics for each interface selected for monitoring.
- Use the **Traffic Statistics > Session Monitor** screen (see Section 5.5 on page 91) to view sessions by user or service.
- Use the **Security Statistics > Content Filter** screen (Section 5.6 on page 93) to start or stop data collection and view content filter statistics.
- Use the **Security Statistics > Reputation Filter** screens (Section 5.7 on page 94) to view statistics of IP reputation, DNS threat filtering and URL threat filtering.
- Use the **Security Statistics > IPS** screen (Section 5.8 on page 98) to start or stop data collection and view IPS statistics.
- Use the **Security Statistics > Anti-Malware** (Section 5.9 on page 100) screen to view anti-malware statistics.
- Use the **Security Statistics > Sandbox** screen (Section 5.10 on page 101) to view sandbox statistics.
- Use the **Security Statistics > SSL Inspection** screen (Section 5.11 on page 102) to see a report on SSL Inspection and a certificate cache list.
- Use the **Network Status > Interface** screen (see Section 5.5 on page 91) to view the interface packets statistics.
- Use the **Network Status > Device Insight** screen (see Section 5.13 on page 106) to view the status of the clients connected to the Zyxel Device.
- Use the **Network Status > Login Users** screen (Section 5.14 on page 109) to look at a list of the users currently logged into the Zyxel Device.
- Use the **Network Status > DHCP Table** screen (see Section 5.16 on page 111) to view a list of interfaces and their DHCP-assigned IP addresses.
- Use the **VPN Status > IPSec VPN > Site to Site VPN** screen (Section 5.17.1 on page 114) to display and manage active IPSec Policies.
- Use the **VPN Status > IPSec VPN > Remote Access VPN** screen (Section 5.17.2 on page 115) to display and manage remote access VPN clients.

- Use the **VPN Status > SSL VPN > Remote Access VPN** screen (Section 5.18 on page 116) to list the users currently logged into the SSL VPN client portal. You can also log out individual users and delete related session information.
- Use the **VPN Status > Tailscale** screen (Section 5.19 on page 117) to display Tailscale VPN connection information.
- Use the **Wireless Status > Access Points** screen (Section 5.20 on page 118) to view traffic usage of managed APs.
- Use the **Wireless Status > WLAN Clients** screen (Section 5.21 on page 121) to view traffic usage of client devices.

5.1.2 What You Need to Know

Collaborative Detection & Response

Collaborative Detection & Response (CDR) allows you to detect wired and WiFi clients that are sending malicious traffic in your network and then block or quarantine traffic coming from them. In this way, malicious traffic is not spread throughout the network. Secure policies can block malicious traffic for specific traffic flows, but CDR can block malicious traffic from the sender. Malicious traffic is identified using a combination of Web Filtering, Anti-Malware and IPS (IDP) signatures.

Note: This feature can only be configured through Nebula. Refer to the NCC User's Guide for details.

5.2 The Application Usage Screen

This screen provides a convenient way to monitor the use of various applications by hosts in the network.

If a license has expired, you will see a reminder in this screen. You need to renew the license in order to keep using the feature. Click **Buy Now** to go to Marketplace to purchase a new license. Click **See Details** to go to the Zyxel web page to find more information on licenses for your Zyxel Device.



Click **Traffic Statistics > Application Usage** to display the following screen. This screen displays usage by application type or the IP addresses of hosts in your network.

Figure 70 Traffic Statistics > Usage by Application

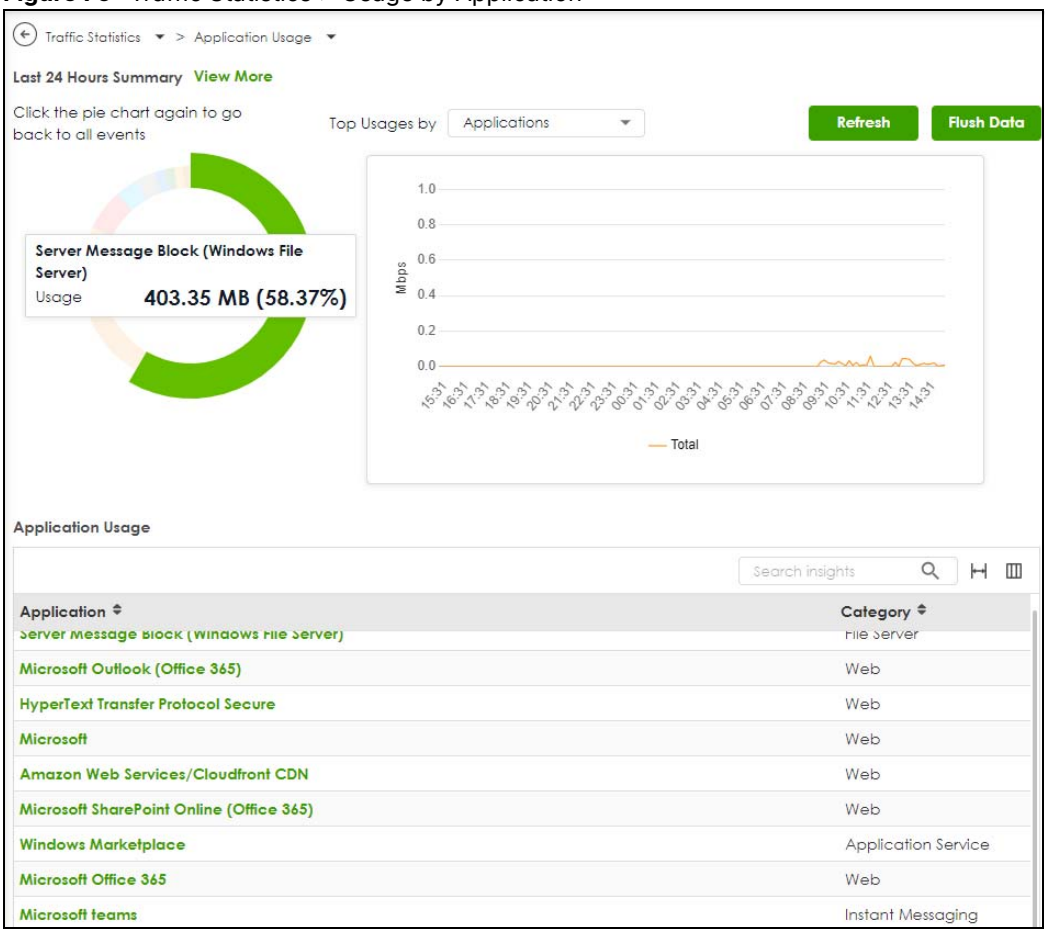
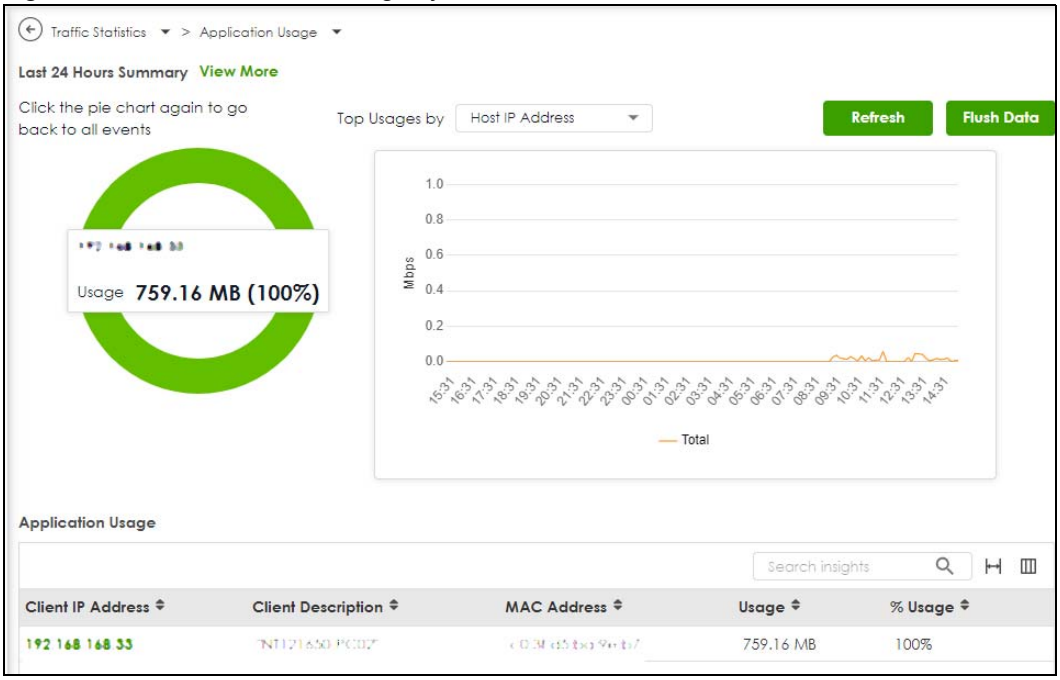


Figure 71 Traffic Statistics > Usage by Host IP



The following table describes the labels in this screen.

Table 29 Traffic Statistics > Application Usage

LABEL	DESCRIPTION
Last 24 Hours Summary	If you want to view more data than the past 24 hours in SecuReporter, click **View More**. You should already have a SecuReporter account.
Pie Chart	Click an item in the pie chart for more detailed information.
Refresh	Click this button to update the report display.
Flush Data	Click this button to discard all of the screen's statistics for inactive sessions. Flushing data only removes traffic logs from ended sessions. Active sessions remain unaffected. Click **Refresh** to update the report display.
Top Usage by	Select to display usage by application or host IP address.
Application	If you selected by application, then this is the name of the application identified.
Category	This is the category the application belongs to.
Usage	This is how much traffic the application has used.
%Usage	This is the percentage of traffic the application has used.
Client IP address	If you selected by host IP address, then this is the IP address of the host identified.
Client Description	This is the name of the host identified.
MAC Address	This is the MAC address of the host device.
Usage	This is how much traffic the host has used.
%Usage	This is the percentage of traffic the host has used.

5.3 The Port Statistics Screen

Use this screen to look at packets statistics for each Gigabit Ethernet port. Ports are physical ports to which you connect cables.

To access this screen, click **Traffic Statistics** > **Port**.

Figure 72 Traffic Statistics > Port

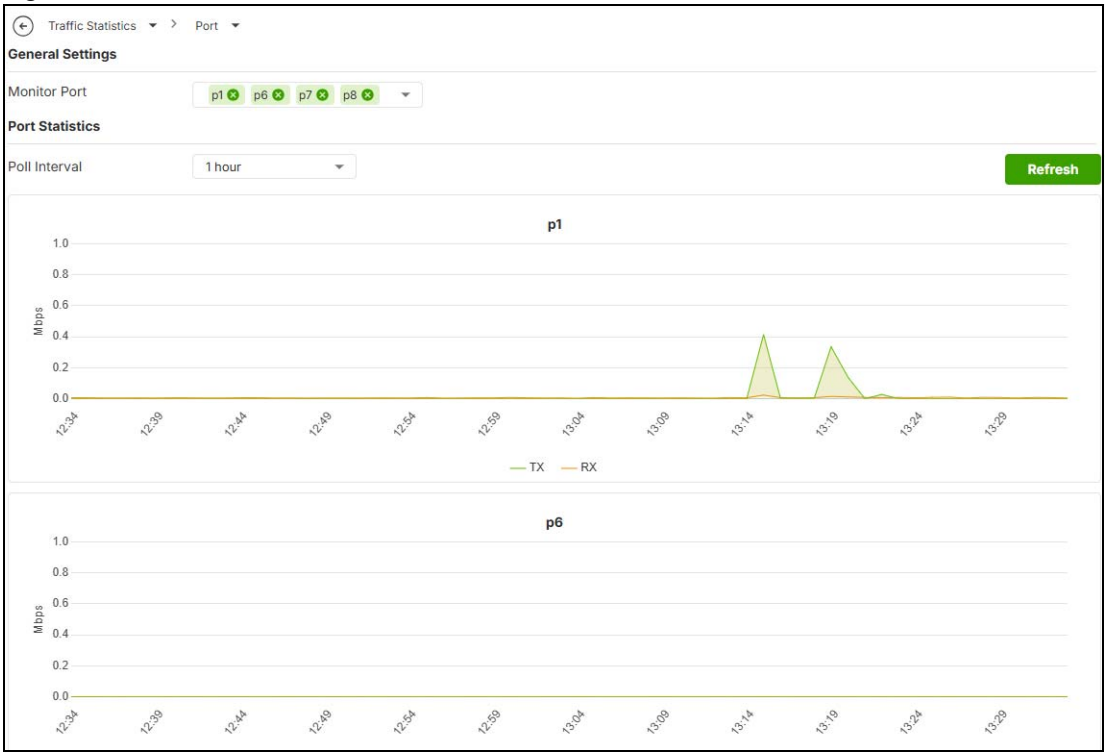


Select one or multiple ports to monitor. The table below lists the maximum number of displayable ports for each model at the time of writing.

Table 30 Maximum Displayable Ports

MODEL	NUMBER OF INTERFACES
USG FLEX 50H USG FLEX 50HP	5
USG FLEX 100H USG FLEX 100HP USG FLEX 200H USG FLEX 200HP USG FLEX 500H USG FLEX 700H	8

Figure 73 Traffic Statistics > Port



The following table describes the labels in this screen.

Table 31 System Statistics > Port

LABEL	DESCRIPTION
Monitor Port	Select one or multiple ports from the drop-down list to view port packet statistics. The maximum number of displayable ports varies by model. See Table 30 on page 88 for the maximum number of ports you can select. A warning message will appear if you attempt to select more than the maximum.
Poll Interval	Enter how often you want this window to be updated automatically, and click **Refresh**.
TX	This line represents traffic transmitted from the Zyxel Device on the selected physical port since it was last connected. Click **TX** to show or hide the TX line in the chart.
RX	This line represents the traffic received by the Zyxel Device on the selected physical port since it was last connected. Click **RX** to show or hide the RX line in the chart.

5.4 The Interface Statistics Screen

Use this screen to look at packets statistics for each interface. Interfaces are used within the system operationally. You use them in configuring various features.

To access this screen, click **Traffic Statistics** > **Interface**.

Figure 74 Traffic Statistics > Interface

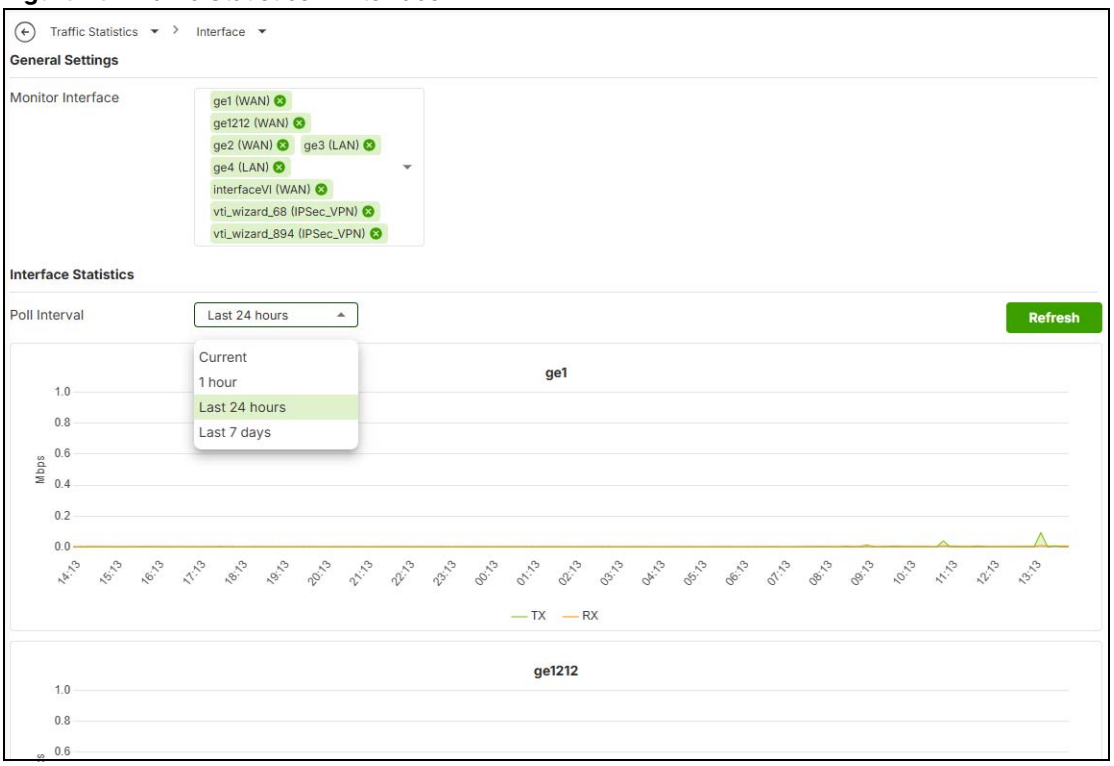


Select one or multiple interfaces to monitor. The table below lists the maximum number of displayable interfaces for each model at the time of writing.

Table 32 Maximum Displayable Interfaces

MODEL	Number of Interfaces
USG FLEX 50H USG FLEX 50HP USG FLEX 100H USG FLEX 100HP USG FLEX 200H USG FLEX 200HP USG FLEX 500H USG FLEX 700H	8

Figure 75 Traffic Statistics > Interface



The following table describes the labels in this screen.

Table 33 Traffic Statistics > Interface

LABEL	DESCRIPTION
Monitor Interface	Select one or multiple interfaces from the drop-down list to view the interface packets statistics. See Table 32 on page 90 for the maximum number of interfaces you can select. A warning message will appear if you attempt to select more than the maximum.
Poll Interval	Enter how often you want this window to be updated automatically, and click **Refresh**.

Table 33 Traffic Statistics > Interface

LABEL	DESCRIPTION
TX	This line displays the transmission speed, in bytes per second, on the interface in the one-second interval before the screen updated.
RX	This line displays the reception speed, in bytes per second, on the interface in the one-second interval before the screen updated.

5.5 The Session Monitor Screen

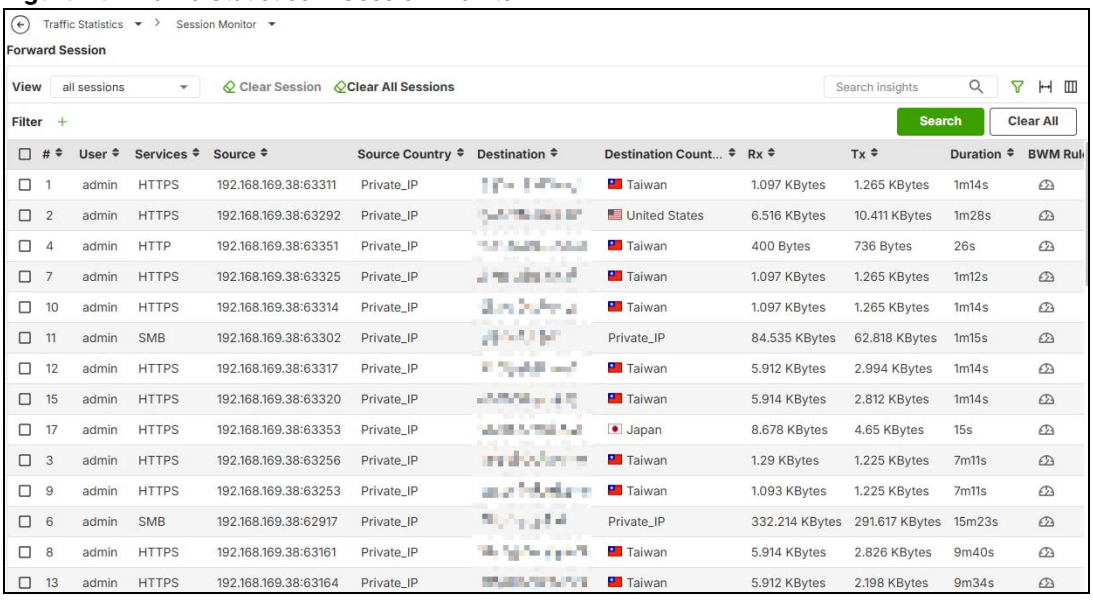
The **Session Monitor** screen displays all established sessions that pass through the Zyxel Device for debugging or statistical analysis. It is not possible to manage sessions in this screen. The following information is displayed.

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

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

Figure 76 Traffic Statistics > Session Monitor



#	User	Services	Source	Source Country	Destination	Destination Count...	Rx	Tx	Duration	BWM Rul
1	admin	HTTPS	192.168.169.38:63311	Private_IP		Taiwan	1.097 KBytes	1.265 KBytes	1m14s	
2	admin	HTTPS	192.168.169.38:63292	Private_IP		United States	6.516 KBytes	10.411 KBytes	1m28s	
4	admin	HTTP	192.168.169.38:63351	Private_IP		Taiwan	400 Bytes	736 Bytes	26s	
7	admin	HTTPS	192.168.169.38:63325	Private_IP		Taiwan	1.097 KBytes	1.265 KBytes	1m12s	
10	admin	HTTPS	192.168.169.38:63314	Private_IP		Taiwan	1.097 KBytes	1.265 KBytes	1m14s	
11	admin	SMB	192.168.169.38:63302	Private_IP		Private_IP	84.535 KBytes	62.818 KBytes	1m15s	
12	admin	HTTPS	192.168.169.38:63317	Private_IP		Taiwan	5.912 KBytes	2.994 KBytes	1m14s	
15	admin	HTTPS	192.168.169.38:63320	Private_IP		Taiwan	5.914 KBytes	2.812 KBytes	1m14s	
17	admin	HTTPS	192.168.169.38:63353	Private_IP		Japan	8.678 KBytes	4.65 KBytes	15s	
3	admin	HTTPS	192.168.169.38:63256	Private_IP		Taiwan	1.29 KBytes	1.225 KBytes	7m11s	
9	admin	HTTPS	192.168.169.38:63253	Private_IP		Taiwan	1.093 KBytes	1.225 KBytes	7m11s	
6	admin	SMB	192.168.169.38:62917	Private_IP		Private_IP	332.214 KBytes	291.617 KBytes	15m23s	
8	admin	HTTPS	192.168.169.38:63161	Private_IP		Taiwan	5.914 KBytes	2.826 KBytes	9m40s	
13	admin	HTTPS	192.168.169.38:63164	Private_IP		Taiwan	5.912 KBytes	2.198 KBytes	9m34s	

The following table describes the labels in this screen.

Table 34 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 user** - 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 • **sessions by source region** - display all active sessions grouped by source IP address • **sessions by destination IP** - display all active sessions grouped by destination IP address • **sessions by destination region** - display all active sessions grouped by destination IP address • **all sessions** - filter the active sessions by the **User**, **Service**, **Source IP**, and **Destination IP**, and display each session individually (sorted by user).
Clear Session	Select a session, then click this button to remove the selected session.
Clear All Sessions	Click this button to remove all sessions.
Refresh	Click this button to update the information on the screen. The screen also refreshes automatically when you open and close the screen.
Search	Type an item in the search box, then click this to display all sessions in the table below according to the item you typed.
Clear All	Click this to remove all items found in the search.
Filter	Click the Filter icon, click + to display **Add Filter,** pick a filter, then click **Search** to display specific sessions according to the filter selected. You may select multiple filters, but just one of each type, configured one at a time. 
	The **User**, **Service**, **Source Address**, **Destination Address, Source Country** and **Destination Country** fields display if you view all sessions.
#	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.
Services	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.
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.
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.
Session Count	Select **sessions by ...** in the **View** field to group the sessions. This field displays the number of sessions. Click this number to view the details of each session.

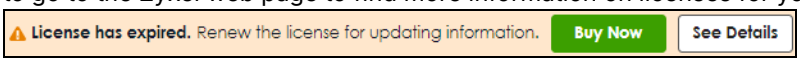
Table 34 Traffic Statistics > Session Monitor (continued)

LABEL	DESCRIPTION
Duration	This field displays the length of the active session in hours, minutes, seconds format.
BWM Rule	Hover over the **BWM Rule** icon for a session to see which BWM rule it is using. This field is displayed only when viewing the table of all sessions. To see it, select **all sessions** in the **View** field, or click the **Session Count** after selecting **sessions by...** in the **View** field.

5.6 The Content Filter Screen

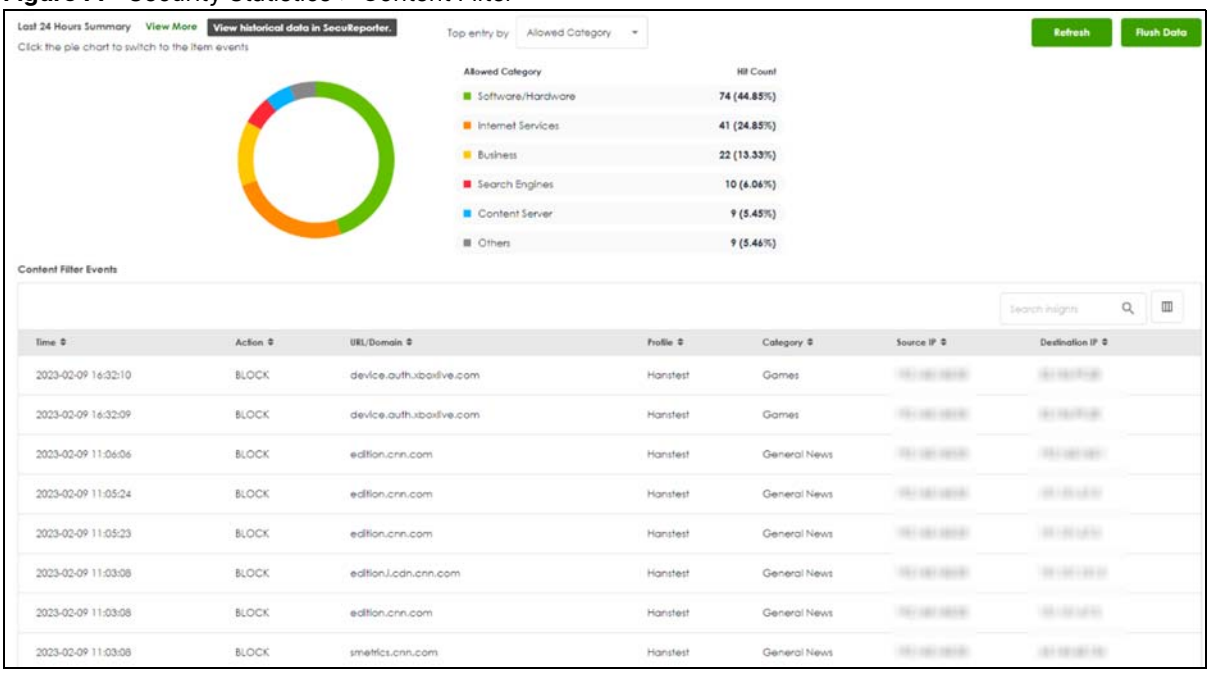
Click **Security Statistics > Content Filter** to display the following screens. The Zyxel Device content filtering includes HTTP(S) traffic scan and DNS domain scan. The HTTP(S) traffic scan allows the Zyxel Device to block access to specific websites, by inspecting the URL or Server Name Indication (SNI) that the user's web browser sends to the web server. The DNS domain scan 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.

If a license has expired, you will see a reminder in this screen. You need to renew the license in order to keep using the feature. Click **Buy Now** to go to Marketplace to purchase a new license. Click **See Details** to go to the Zyxel web page to find more information on licenses for your Zyxel Device.



These screens display some basic statistics on HTTP(S) traffic scan and DNS domain scan.

Figure 77 Security Statistics > Content Filter



The following table describes the labels in this screen.

Table 35 Security Statistics > Content Filter

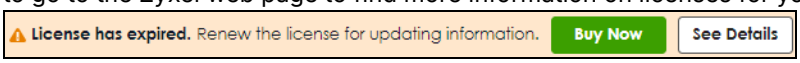
LABEL	DESCRIPTION
Last 24 Hours Summary	If you want to view more data than the past 24 hours in SecuReporter, click **View More**. You should already have a SecuReporter account.
Pie Chart	Click an item in the pie chart for more detailed information.
Top entry by	Use this field to have the following (read-only) table display the top content filter log entries by **Blocked Category, Blocked Source IP, Blocked URL, Allowed Category, Allowed Source IP, or Allowed URL**. This table displays the most common, recent content filter logs. See the log screen for less common content filter logs or use a syslog server to record all content filter logs. Select **Blocked Category** to list the web site categories the Zyxel Device has blocked. Select **Blocked Source IP** to list the source IP addresses of the web sites the Zyxel Device has blocked. Select **Blocked URL** to list the URLs of the web sites the Zyxel Device has blocked. Select **Allowed Category** to list the web site categories the Zyxel Device has allowed. Select **Allowed Source IP** to list the source IP addresses of the web sites the Zyxel Device has allowed. Select **Allowed URL** to list the URLs of the web sites the Zyxel Device has allowed.
Refresh	Click this button to update the report display.
Flush Data	Click this button to discard all of the screen's statistics. Click **Refresh** to update the report display.
Time	This column displays the date and time when the users access the URL or FQDN.
Action	This column displays whether the Zyxel Device blocks or passes the accessed URL or FQDN.
URL/Domain	This column displays the URL or domain name of the web site accessed.
Profile	This column displays the content filter profile the website belongs to.
Category	This column displays the category the accessed web site belongs to.
Source IP	This column displays the source IP address of the web site the Zyxel Device has checked.
Destination IP	This column displays the destination IP address at which the traffic of the web site the Zyxel Device has checked is sent.

5.7 The Reputation Filter Screens

Click **Security Statistics > Reputation Filter** to display the following screens. These screens display reputation filter statistics.

The Zyxel Device reputation filter includes IP reputation, DNS threat filter and URL threat filter.

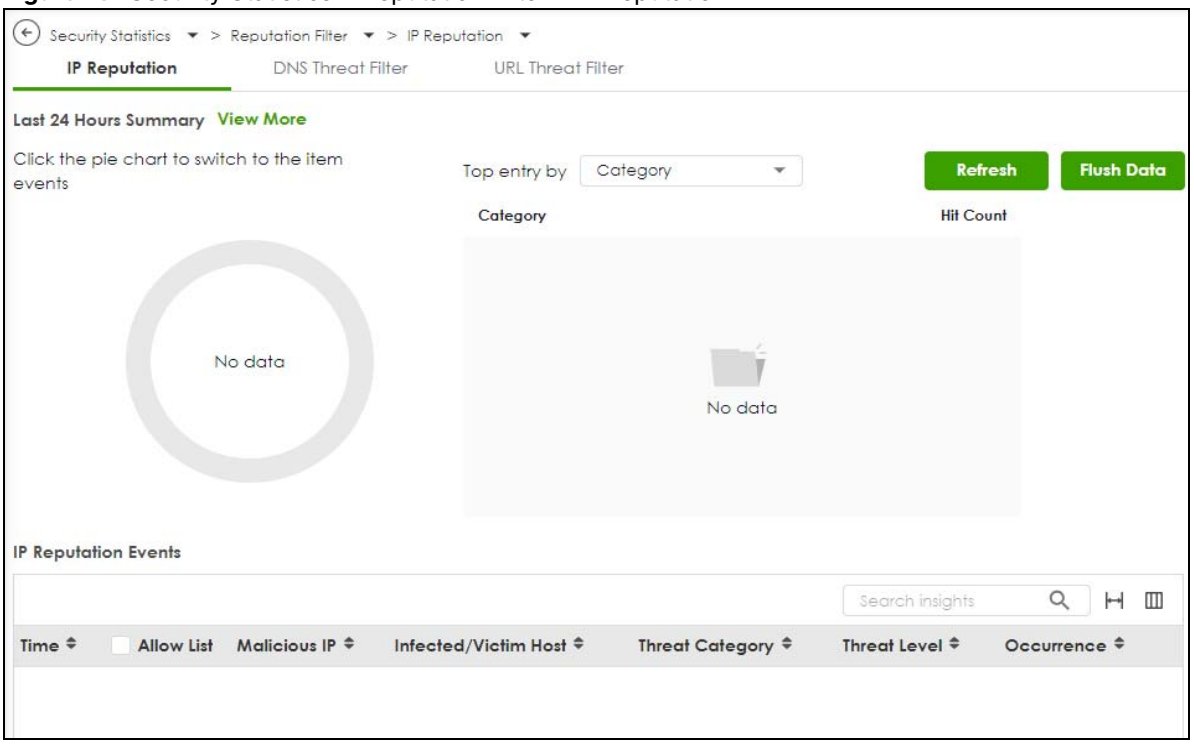
If a license has expired, you will see a reminder in this screen. You need to renew the license in order to keep using the feature. Click **Buy Now** to go to Marketplace to purchase a new license. Click **See Details** to go to the Zyxel web page to find more information on licenses for your Zyxel Device.



5.7.1 IP Reputation

This screen displays IP reputation statistics. IP reputation checks the reputation of an IP address from a database.

Figure 78 Security Statistics > Reputation Filter > IP Reputation



The following table describes the labels in this screen.

Table 36 Security Statistics > Reputation Filter > IP Reputation

LABEL	DESCRIPTION
Last 24 Hours Summary	If you want to view more data than the past 24 hours in SecuReporter, click **View More**. You should already have a SecuReporter account.
Pie Chart	Click an item in the pie chart for more detailed information.
Top Entries By	Use this field to have the following (read-only) table display the top IP reputation log entries by **Category, Infected/Victim Host** or **Malicious IP**. This table displays the most common, recent IP reputation logs. See the log screen for less common IP reputation logs or use a syslog server to record all IP reputation logs. Select **Category** to list the most common categories of packets that the Zyxel Device has detected. Select **Infected/Victim Host** to list the most common IP addresses of the infected hosts. Select **Malicious IP** to list the most common IPv4 addresses with bad reputation that have sent packets to the Zyxel Device.
Refresh	Click this button to update the report display.
Flush Data	Click this button to discard all of the screen's statistics. Click **Refresh** to update the report display.
IP Reputation Events	
Time	This field displays the date and time the entry was created.
+ Allow List	Select an entry and click this to add it to the IP reputation allow list.

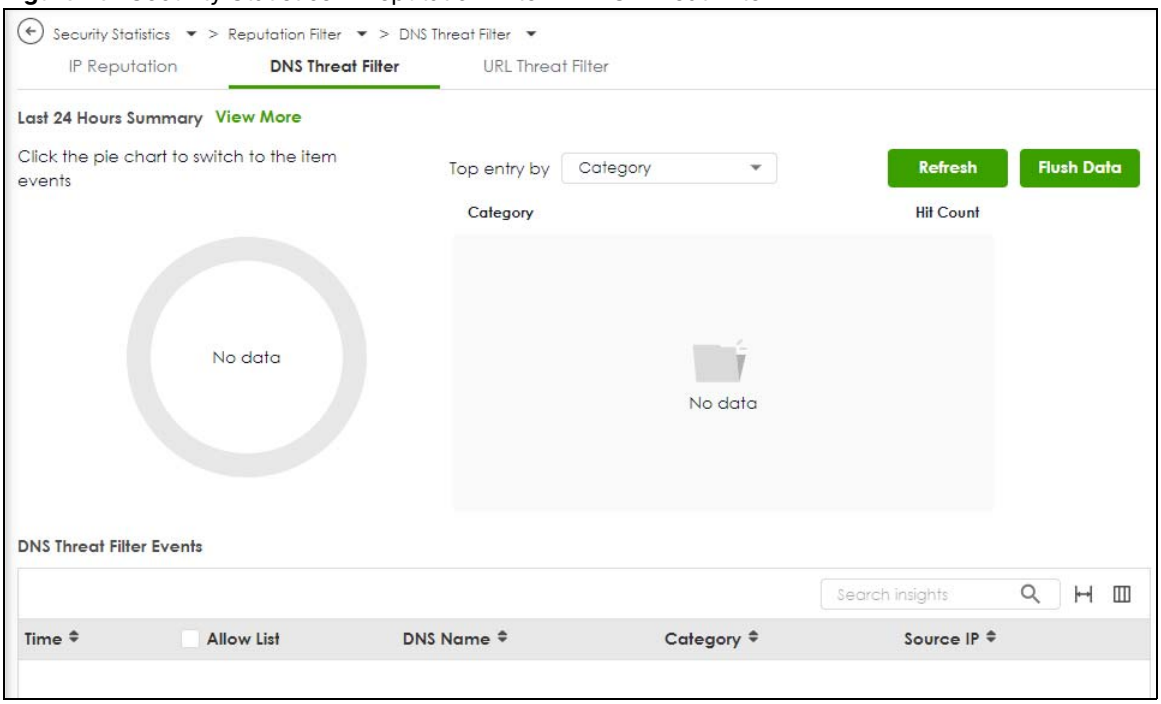
Table 36 Security Statistics > Reputation Filter > IP Reputation

LABEL	DESCRIPTION
Malicious IP	This field displays the IPv4 address with bad reputation.
Infected/Victim Host	This field displays the IP address of the infected host.
Threat Category	This field displays the category of the entry.
Threat Level	This field displays the threat level of the entry.
Occurrence	This field displays how many times the Zyxel Device has detected the event described in the entry.

5.7.2 DNS Threat Filter

This screen displays DNS threat filter statistics. DNS threat filtering inspects DNS queries made by clients on your network and compares the queries against a database of blocked or allowed Fully Qualified Domain Names (FQDNs).

Figure 79 Security Statistics > Reputation Filter > DNS Threat Filter



The following table describes the labels in this screen.

Table 37 Security Statistics > Reputation Filter > DNS Threat Filter

LABEL	DESCRIPTION
Last 24 Hours Summary	If you want to view more data than the past 24 hours in SecuReporter, click **View More**. You should already have a SecuReporter account.
Pie Chart	Click an item in the pie chart for more detailed information.

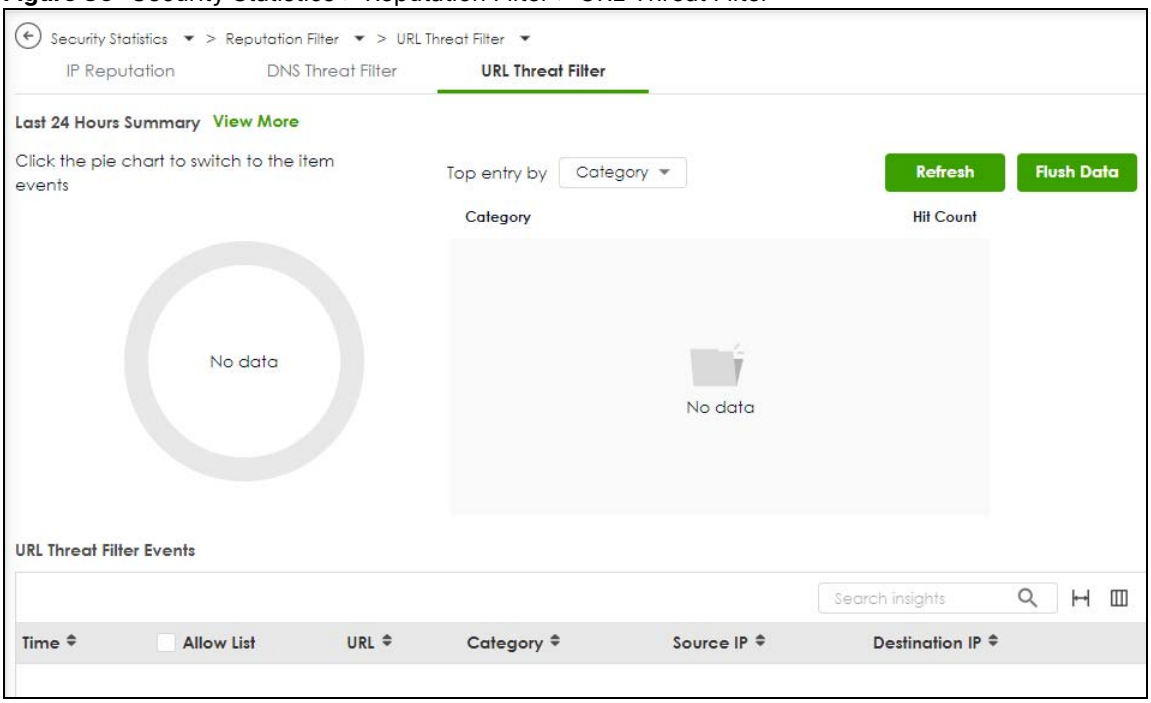
Table 37 Security Statistics > Reputation Filter > DNS Threat Filter

LABEL	DESCRIPTION
Top Entries By	Use this field to have the following (read-only) table display the top DNS threat filter log entries by **Category, Source IP** or **DNS Name**. This table displays the most common, recent DNS threat filter logs. See the log screen for less common DNS threat filter logs or use a syslog server to record all DNS threat filter logs. Select **Category** to list the most common categories of packets that the Zyxel Device has detected. Select **Source IP** to list the most common source IP addresses of traffic. Select **DNS Name** to list the most common FQDNs of the infected websites.
Refresh	Click this button to update the report display.
Flush Data	Click this button to discard all of the screen's statistics. Click **Refresh** to update the report display.
DNS Threat Filter Events	
Time	This field displays the date and time the entry was created.
+ Allow List	Select an entry and click this to add it to the DNS filtering allow list.
DNS Name	This field displays the FQDN of an infected website.
Category	This field displays the category of the entry.
Source IP	This field displays the source IP address of traffic that you want to trace.

5.7.3 URL Threat Filter

This screen displays URL threat filter statistics. URL threat filtering compares access to specific URLs against a database of blocked or allowed sites.

Figure 80 Security Statistics > Reputation Filter > URL Threat Filter



The following table describes the labels in this screen.

Table 38 Security Statistics > Reputation Filter > URL Threat Filter

LABEL	DESCRIPTION
Last 24 Hours Summary	If you want to view more data than the past 24 hours in SecuReporter, click **View More**. You should already have a SecuReporter account.
Pie Chart	Click an item in the pie chart for more detailed information.
Top Entries By	Use this field to have the following (read-only) table display the top URL threat filter log entries by **Category, URL** or **Source IP.** This table displays the most common, recent URL threat filter logs. See the log screen for less common URL threat filter logs or use a syslog server to record all URL threat filter logs. Select **Category** to list the most common categories of packets that the Zyxel Device has detected. Select **URL** to list the most common URLs of the infected websites. Select **Source IP** to list the most common source IP addresses of traffic.
Refresh	Click this button to update the report display.
Flush Data	Click this button to discard all of the screen's statistics. Click **Refresh** to update the report display.
URL Threat Filter Events	
Time	This field displays the date and time the entry was created.
+ Allow List	Select an entry and click this to add it to the URL Threat filtering allow list.
URL	This field displays the URL of an infected website.
Category	This field displays the category of the entry.
Source IP	This field displays the source IP address of traffic that you want to trace.
Destination IP	This field displays the destination IP address of traffic.

5.8 The IPS Screen

Click **Security Statistics > IPS** to display the following screen. This screen displays IPS (Intrusion Prevention System) statistics. An IPS system can detect malicious or suspicious packets and respond instantaneously by rejecting or dropping the packets. The Zyxel Device IPS protects your network against network-based intrusions.

If a license has expired, you will see a reminder in this screen. You need to renew the license in order to keep using the feature. Click **Buy Now** to go to Marketplace to purchase a new license. Click **See Details** to go to the Zyxel web page to find more information on licenses for your Zyxel Device.

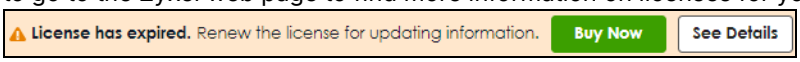
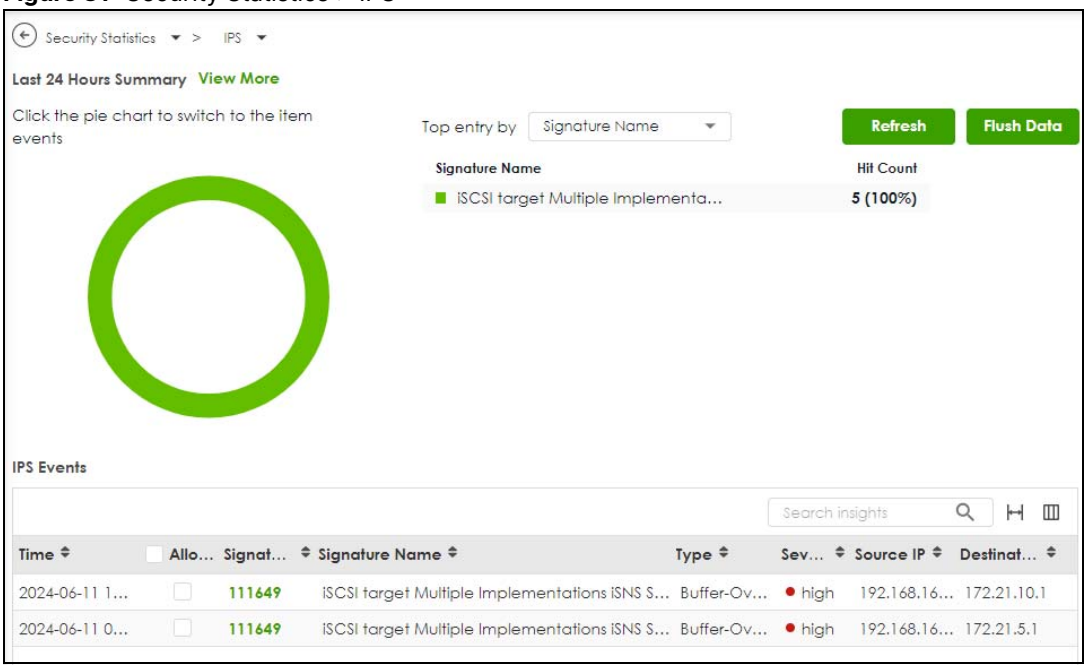


Figure 81 Security Statistics > IPS



The following table describes the labels in this screen.

Table 39 Security Statistics > IPS

LABEL	DESCRIPTION
Last 24 Hours Summary	If you want to view more data than the past 24 hours in SecuReporter, click **View More**. You should already have a SecuReporter account.
Pie Chart	Click an item in the pie chart for more detailed information.
Top Entries By	Use this field to have the following (read-only) table display the top IPS log entries by **Signature Name**, **Source IP** or **Destination IP**. This table displays the most common, recent IPS logs. See the log screen for less common IPS logs or use a syslog server to record all IPS logs. Select **Signature Name** to list the most common signatures that the Zyxel Device has detected. Select **Source IP** to list the source IP addresses from which the Zyxel Device has detected the most intrusion attempts. Select **Destination IP** to list the most common destination IP addresses for intrusion attempts that the Zyxel Device has detected.
Refresh	Click this button to update the report display.
Flush Data	Click this button to discard all of the screen's statistics. Click **Refresh** to update the report display.
Time	This column displays the date and time IPS blocked this IP address.
+ Allow List	Select an entry and click this to add the signature to the IPS allow list.
Signature ID	This column displays when you display the unique value given to each intrusion detected.
Signature Name	This column displays the name to identify the type of intrusion pattern.
Type	This column displays the categories of intrusions.
Severity	This column displays the level of threat that the intrusions may pose.
Source IP	This column displays the source IP address of the intrusion attempts.
Destination IP	This column displays the destination IP address at which intrusion attempts were targeted.

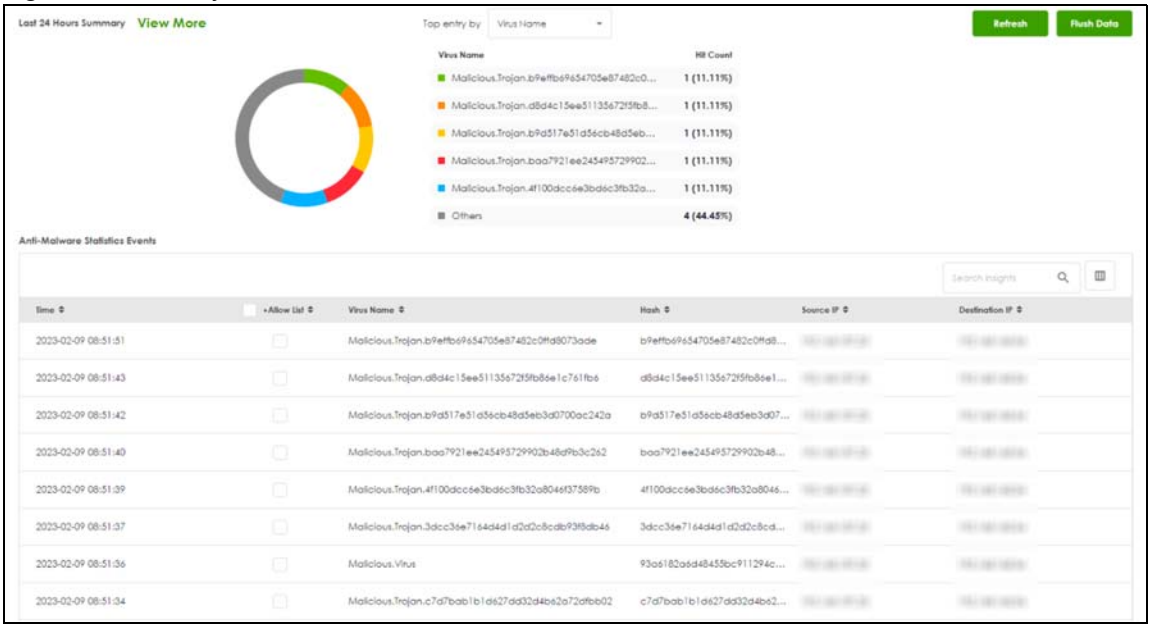
5.9 The Anti-Malware Screen

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

If a license has expired, you will see a reminder in this screen. You need to renew the license in order to keep using the feature. Click **Buy Now** to go to Marketplace to purchase a new license. Click **See Details** to go to the Zyxel web page to find more information on licenses for your Zyxel Device.



Figure 82 Security Statistics > Anti-Malware



The following table describes the labels in this screen.

Table 40 Security Statistics > Anti-Malware

LABEL	DESCRIPTION
Last 24 Hours Summary	If you want to view more data than the past 24 hours in SecuReporter, click **View More**. You should already have a SecuReporter account.
Pie Chart	Click an item in the pie chart for more detailed information.
Top Entries By	Use this field to have the following (read-only) table display the top anti-malware log entries by **Virus Name**, **Source IP**, and **Destination IP**. This table displays the most common, recent anti-malware logs. See the log screen for less common anti-malware logs or use a syslog server to record all anti-malware logs. Select **Virus Name** to list the most common viruses that the Zyxel Device has detected. Select **Source IP** to list the source IP addresses from which the Zyxel Device has detected the most virus-infected files. Select **Destination IP** to list the most common destination IP addresses for virus-infected files that Zyxel Device has detected.
Refresh	Click this button to update the report display.
Flush Data	Click this button to discard all of the screen's statistics. Click **Refresh** to update the report display.

Table 40 Security Statistics > Anti-Malware (continued)

LABEL	DESCRIPTION
Anti-Malware Statistics Events	
Time	This field displays the date and time the entry was created.
Allow List	Select an entry and click this to add it to the anti-malware allow list.
Virus name	This column displays when you display the entries by **Virus Name**. This displays the name of a detected virus.
Hash	This column displays a hash value, SHA-256 (Secure Hash Algorithm) or MD5 (Message Digest 5) of the detected virus file. SHA-256 and MD5 are hash algorithms used to authenticate packet data.
Source IP	This column displays when you display the entries by **Source IP.** It shows the source IP address of virus-infected files that the Zyxel Device has detected.
Destination IP	This column displays when you display the entries by **Destination IP.** It shows the destination IP address of virus-infected files that the Zyxel Device has detected.

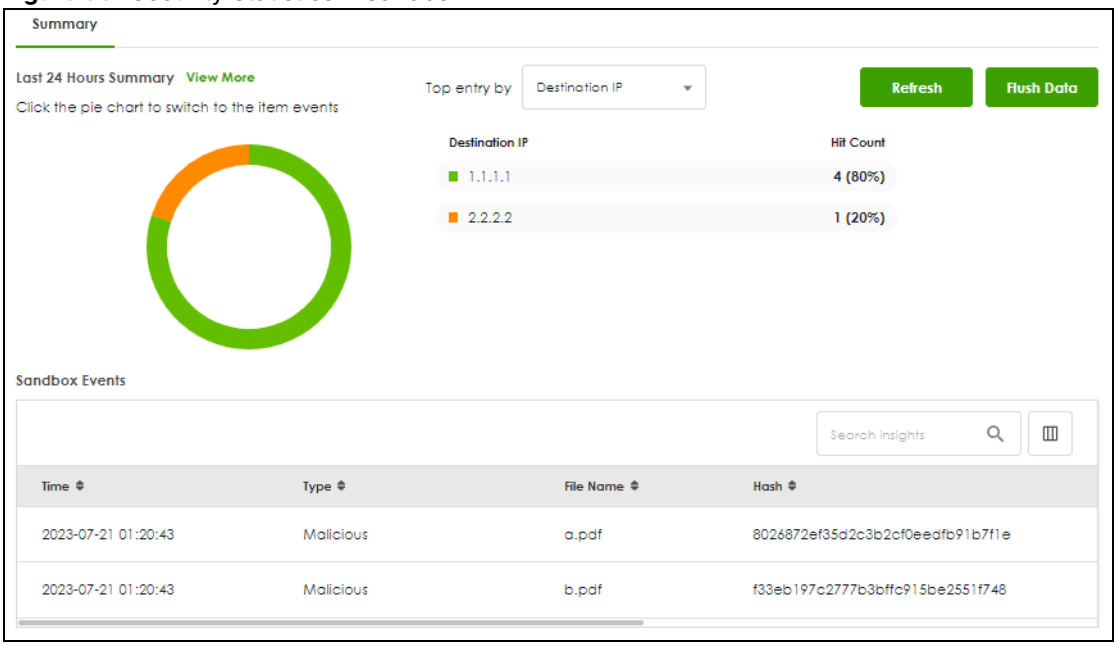
5.10 The Sandbox Screen

Click **Security Statistics > Sandbox** to display the following screen. This screen displays sandbox statistics.

If a license has expired, you will see a reminder in this screen. You need to renew the license in order to keep using the feature. Click **Buy Now** to go to Marketplace to purchase a new license. Click **See Details** to go to the Zyxel web page to find more information on licenses for your Zyxel Device.



Figure 83 Security Statistics > Sandbox



The following table describes the labels in this screen.

Table 41 Security Statistics > Sandbox

LABEL	DESCRIPTION
Last 24 Hours Summary	If you want to view more data than the past 24 hours in SecuReporter, click **View More**. You should already have a SecuReporter account.
Pie Chart	Click an item in the pie chart for more detailed information.
Top Entries By	Use this field to have the following (read-only) table display the top sandbox log entries by **Destination IP**, **Source IP** and **Type**. This table displays the most common, recent sandbox logs. See the log screen for less common sandbox logs or use a syslog server to record all sandbox logs. Select **Source IP** to list the source IP addresses from which the Zyxel Device has detected the most files with unknown or untrusted programs and codes. Select **Destination IP** to list the most common destination IP addresses for files with unknown or untrusted programs and codes that Zyxel Device has detected. Select **Type** to display if the file type of the detected file with unknown or untrusted programs and codes.
Refresh	Click this button to update the report display.
Flush Data	Click this button to discard all of the screen's statistics. Click **Refresh** to update the report display. When the statistics stored reach the limit, new statistics automatically overwrite existing statistics, starting with the oldest statistics first.
Sandbox Events	
Time	This field displays the time the file is scanned by the Zyxel Device.
Type	This field displays the file type of the detected file with unknown or untrusted programs and codes.
File Name	This column displays the file name of the detected virus file.
Hash	This column displays a hash value, MD5 (Message Digest 5, of the detected file with unknown or untrusted programs and codes. MD5 is a hash algorithm used to authenticate packet data.
Source IP	This column displays the source IP address of the file the Zyxel Device has checked.
Destination IP	This column displays the destination IP address at which the traffic of the file the Zyxel Device has checked is sent.

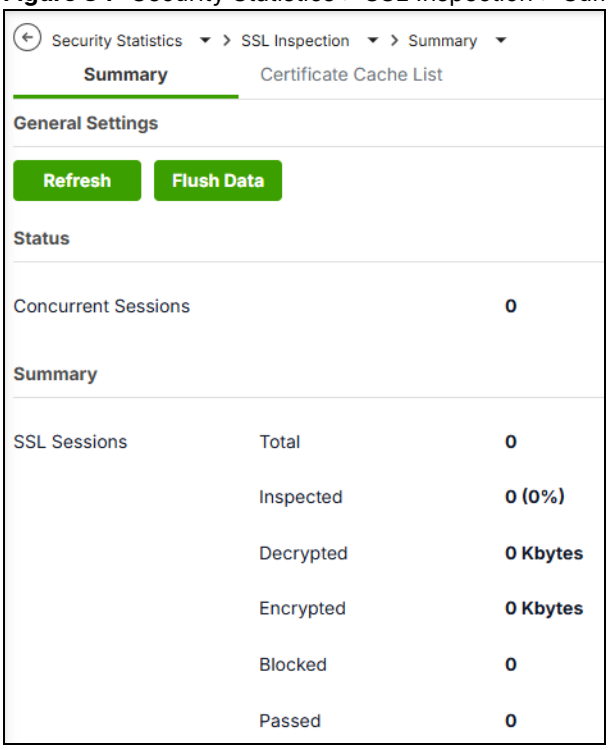
5.11 The SSL Inspection Screens

The Zyxel Device uses SSL Inspection to decrypt SSL traffic, then sends it to Security Service engines for inspection, and then finally encrypts traffic that passes inspection and forwards it.

5.11.1 The Summary Screen

Click **Security Statistics > SSL Inspection > Summary** to display the following screen. This screen shows the number of SSL sessions inspected, blocked and passed.

Figure 84 Security Statistics > SSL Inspection > Summary



The following table describes the labels in this screen.

Table 42 Security Statistics > SSL Inspection > Summary

LABEL	DESCRIPTION
General Settings	
Refresh	Click this button to update the report display.
Flush Data	Click this button to discard all of the screen's statistics. Click **Refresh** to update the report display.
Status	
Concurrent Sessions	This shows the actual number of simultaneous SSL Inspection sessions in progress. This number displays in red when you have reached the maximum number of simultaneous SSL Inspection sessions allowed for your Zyxel Device model. See the Product Features appendix in the User's Guide to see the maximum allowed for each model.
Summary	
Total	This is the total of SSL sessions inspected and number of sessions blocked and number of sessions passed since data was last flushed or the Zyxel Device last rebooted after **Collect Statistics** was enabled.
Inspected	This shows the total number of SSL sessions inspected since data was last flushed or the Zyxel Device last rebooted after **Collect Statistics** was enabled
Decrypted (Kbytes)	This shows the number of kilobytes (KB) of data that was decrypted for Security Service inspection.
Encrypted (Kbytes)	This shows the number of kilobytes (KB) of data that was re-encrypted after Security Service inspection and then forwarded.
Blocked	This shows the number of SSL sessions blocked.
Passed	This shows the number of SSL sessions passed.

5.11.2 The Certificate Cache List Screen

A certificate identifies the source of SSL traffic. Use this screen to decide which sources can be excluded from SSL inspection. Traffic in an **Exclude List** is not intercepted by SSL inspection.

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

Figure 85 Security Statistics > SSL Inspection > Certificate Cache List



The following table describes the labels in this screen.

Table 43 Security Statistics > SSL Inspection > Certificate Cache List

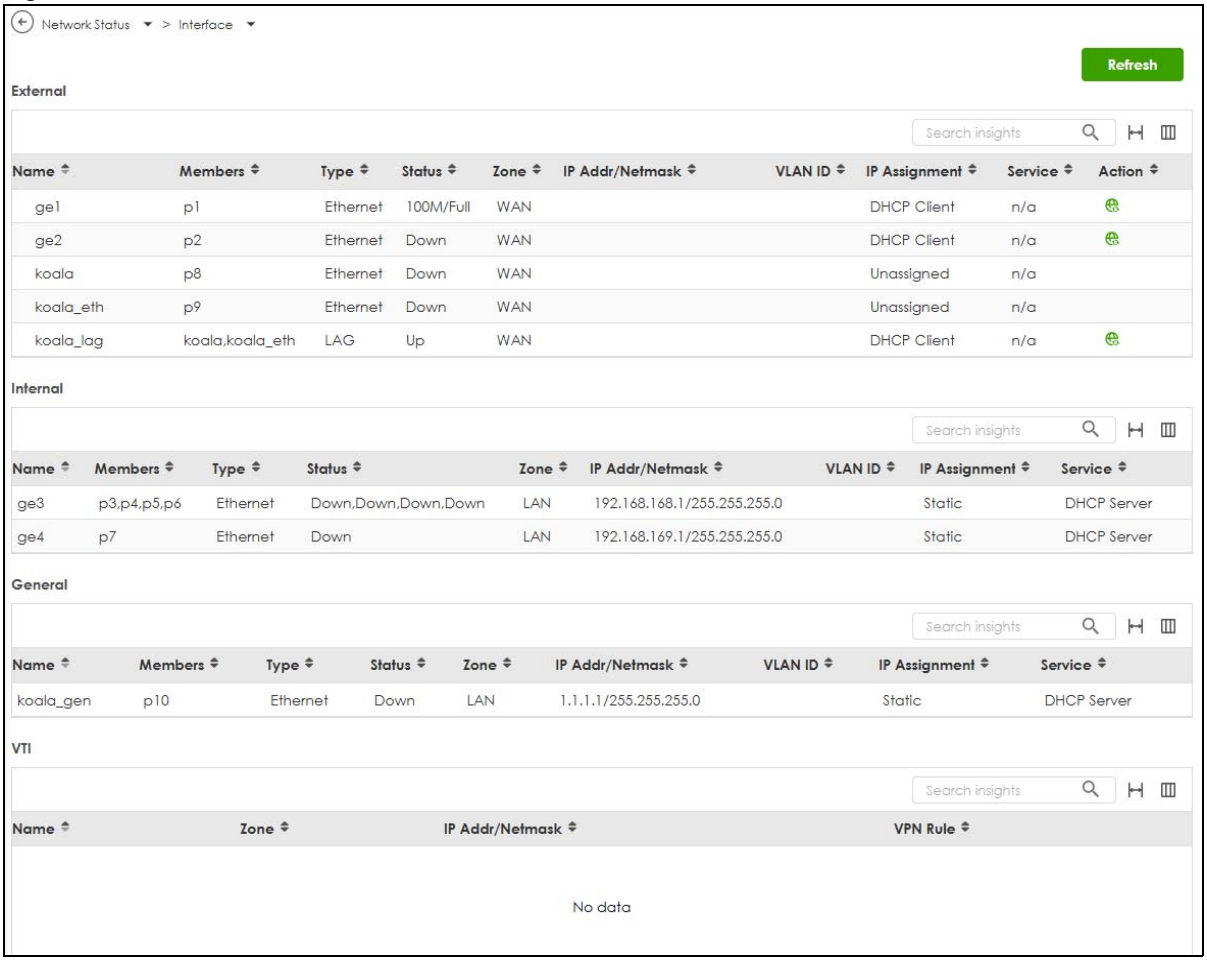
LABEL	DESCRIPTION
Time	This is the latest date (yyyy-mm-dd) and time (hh-mm-ss) that the record in the certificate cache list was met.
Add to Exclude list	Select and item in the list and click this icon to add the common name (CN) to the **Exclude List**.
Common Name	This displays the common name in the certificate of the SSL traffic destination server.
Server Name Indication	Server Name Indication (SNI) is the domain name entered in the browser, FTP client, etc. to begin the SSL session with the server. It allows multiple SSL sessions to the same IP address and port number with different certificates from different SNI. This field displays the SNI for this SSL session.
SSL Version	This field shows the SSL version. TLS1.0/1.1/1.2 are currently supported.
Destination	This displays the IP address and port number of the SSL traffic destination server.
Valid Time	This displays the cache item expiry time in seconds. The cache item is deleted when the remaining time expires.

5.12 The Interface Screen

This screen lists all of the Zyxel Device's interfaces and their information.

Click **Network Status > Interface** to display the following screen.

Figure 86 Network Status > Interface



The following table describes the labels in this screen.

Table 44 Network Status > Interface

LABEL	DESCRIPTION
Refresh	Click this to update the information in this screen.
Name	This field displays the name of each interface.
Members	This field displays the physical port number that is binded to the interface. An interface is binded to a port when the interface is bounded to the physical port. 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. This field displays the bridge interface's members.
Type	This field displays the type of connection the interface is using.

Table 44 Network Status > Interface

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 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.
Zone	This field displays the zone to which the interface is assigned.
IP Addr/Netmask	This field displays the current IP address and subnet mask assigned to the interface. If the IP address and subnet mask are 0.0.0.0, the interface is disabled or did not receive an IP address and subnet mask via DHCP. If this interface is a member of an active virtual router, this field displays the IP address it is currently using. This is either the static IP address of the interface (if it is the master) or the management IP address (if it is a backup).
VLAN ID	This field displays the VLAN ID which is a 12-bit number that uniquely identifies each VLAN.
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.
Service	This field lists which services the interface provides to the network. Examples include **DHCP relay**, **DHCP server** and **DDNS**. 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.
VPN Rule	This field displays the scenario rule the VPN tunnel interface is using.

5.13 The Device Insight Screen

Use **Device Insight** to collect status and basic information of the clients connected to the Zyxel Device internal interfaces or IPSec VPN or Astra clients with or without VPN Zyxel Client software installed. The clients shown 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 built-in access points using WiFi connections.
- Using SecuExtender (IPSec VPN clients).

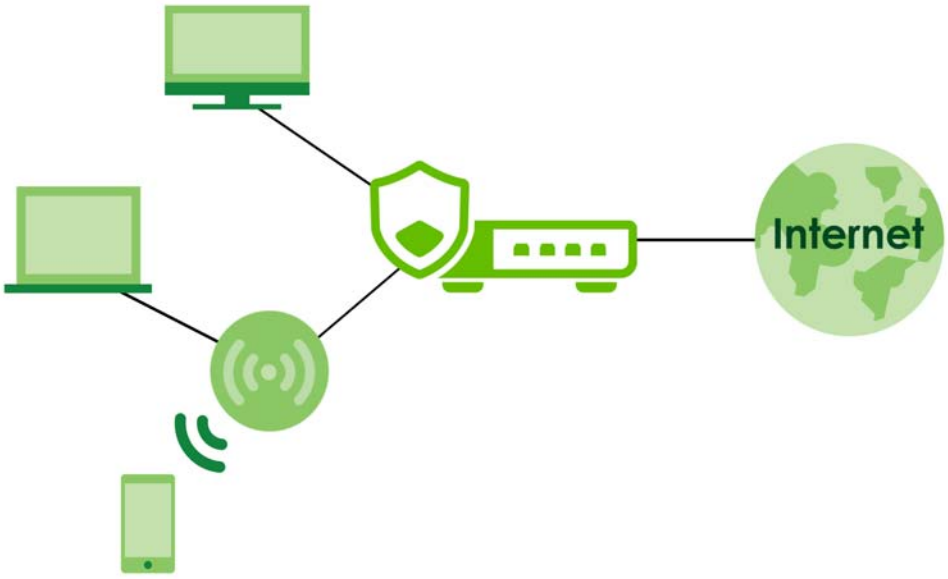
Device Insight collects client information including:

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

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** is a client connected to the Zyxel Device using a wired connection. **B** is a client connected to the Zyxel Device through an AP using a wired connection. **C** is a client connected to the Zyxel Device through an AP using a WiFi connection.

Figure 87 Clients' Device Insight Example

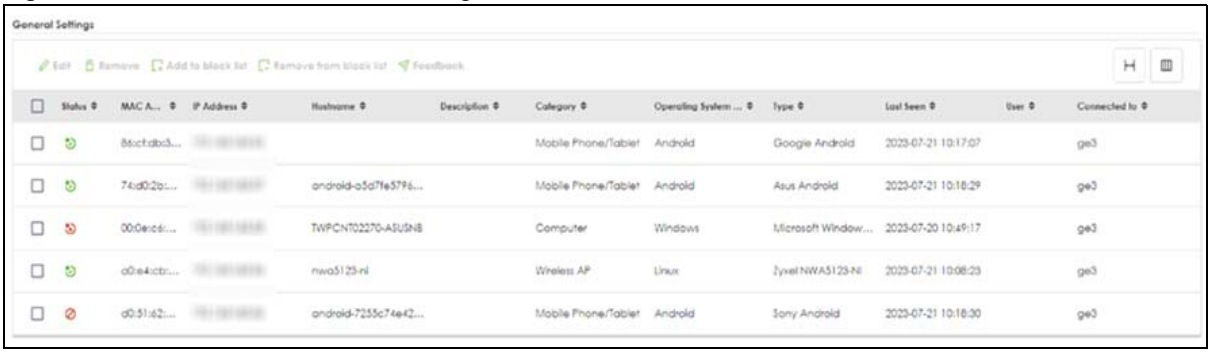


Click **Network Status** > **Device Insight** to show the following screen.

If a license has expired, you will see a reminder in this screen. You need to renew the license in order to keep using the feature. Click **Buy Now** to go to Marketplace to purchase a new license. Click **See Details** to go to the Zyxel web page to find more information on licenses for your Zyxel Device.



Figure 88 Network Status > Device Insight



The following table describes the labels in this screen.

Table 45 Network Status > Device Insight

LABEL	DESCRIPTION
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**.
Status	This field displays the status of the clients. Online ( )- The connection between the client and the Zyxel Device is up. Offline ( )- The connection between the client and the Zyxel Device is down. Block ( )- The client is blocked from the connection to the Zyxel Device.
MAC Address	This field displays the MAC address of the client.
MAC Vendor	This displays the MAC address Organizationally Unique Identifier (OUI). The OUI is the first three octets in a MAC address and uniquely identifies the manufacturer of a network device.
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.
Description	This field displays the descriptive name of the client.
Connected to	This field displays the interface to which a client is connected directly to on the Zyxel Device.
Connected to	This field displays the interface to which a client is connected directly to on the Zyxel Device.
Operating System (OS)	This field displays the operating system of the client.

Table 45 Network Status > Device Insight (continued)

LABEL	DESCRIPTION
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 since the Zyxel Device last reboot.
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 28.1.1 on page 459 for more information the user account types.
Auth method	This field displays the authentication method that is used to authenticate the client.
Astra Group & Role	This field displays the group name and role (**admin** or **member**) of the client on Astra. • **admin**: The Astra web portal is a platform that provides security services to computer or mobile devices. It is managed by an admin. • **member**: A member is a person whose computer or mobile device the admin wishes to protect using Astra. You can add your mobile device or a member's mobile device using this Astra web portal account.
Astra Agent Version	This field displays the version of Astra.
Client Firewall Status	This field displays the firewall status on the client's computer or mobile device, such as a smartphone. The field is blank is if there is no firewall on the client. • **Enabled**: The firewall is enabled on the client. • **Disabled**: The firewall is disabled on the client.
Astra License Status	This field displays the current Astra license status of the client. The following displays for a license you subscribed to from the Astra Portal. • **Activated**: The Astra license is enabled. • **Inactive**: The Astra license is not enabled. • **Overdue**: The payment for the Astra license has failed, and the license will be canceled 15 days after the overdue date. During this period, attempts will be made to process the credit card payment. • **Cancel**: The Astra license will be canceled after the expiration date. • **None**: A standard or trial license has not been enabled. The following displays for a license you purchased offline. You'll need to use the license key to activate the license online. • **Activated**: The Astra license is enabled. • **Grace period**: After a license expires, you have 15 days grace period during which you can extend your current license. • **Expired**: The Astra license has expired. • **None**: A standard or trial license has not been enabled.

5.14 The Login Users Screen

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

Figure 89 Network Status > Login Users



The following table describes the labels in this screen.

Table 46 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.
Role	This field displays the types of user accounts the Zyxel Device uses. See Section 28.1.4 on page 463 for more information on the user accounts.
From	This field displays the IP address of the computer used to log in to the Zyxel Device.
Login Time	This field displays how long a user account has logged into the Zyxel Device.
Type	This field displays the way the user logged into the Zyxel Device. The user can log into the Zyxel Device using HTTP, HTTPS, SSH, FTP and console.
Tunnel IP	This field displays the IP address of the VPN tunnel a user account is using to access the Zyxel Device. This field displays **0.0.0.0** if a user account is not accessing the Zyxel Device through a VPN tunnel.
Reauth/Lease Time	This field displays the amount of reauthentication time remaining and the amount of lease time remaining for each user. See Section 28.1.5 on page 464 for more information on the reauthentication time and lease time.

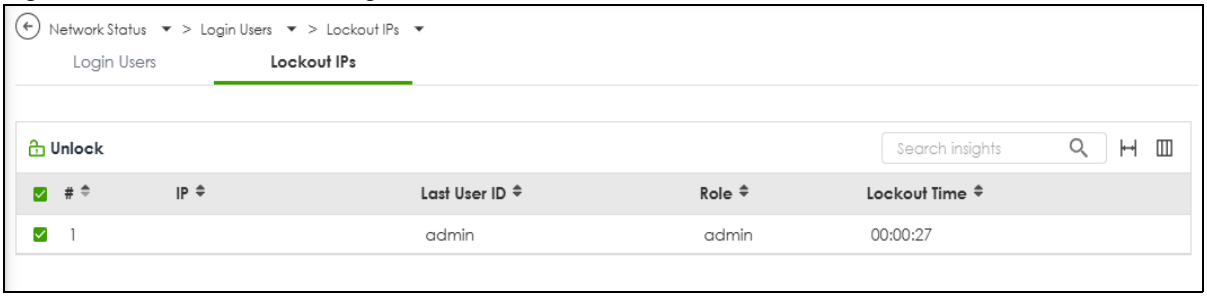
5.15 The Lockout IPs Screen

Use this screen to view and unlock IP addresses blocked from logging in to the Zyxel Device. If a user exceeds the limit on the number of unsuccessful login attempts (for example, wrong password), the Zyxel Device will lock the IP address for a specified amount of time. Go to **User & Authentication** > **User/Group** > **Setting** to configure these user account lockout settings. See Section 28.1.7 on page 473 for more information.

Note: A user account that has exceeded the login attempt limit can still log into the Zyxel Device from another IP address that is not blocked.

To access this screen, click **Network Status > Login Users > Lockout IPs**.

Figure 90 Network Status > Login Users > Lockout IPs



The following table describes the labels in this screen.

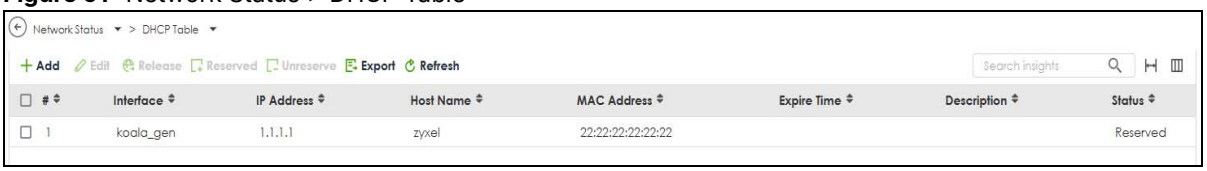
Table 47 Network Status > Login Users > Lockout IPs

LABEL	DESCRIPTION
Unlock	Select an IP address and click **Unlock** to allow the user from that IP address to log into the Zyxel Device.
#	This field is a sequential value and is associated with the lockout IP address entries.
IP	This displays the IP address that exceeded the login attempt limit.
Last User ID	This displays the user name of the user who exceeded the login attempt limit.
Role	This displays the type of user account that attempted to log into the Zyxel Device. • **Admin**: This user can configure the Zyxel Device settings using the web configurator or CLI. • **Viewer**: This user can only view the Zyxel Device settings using the web configurator and perform basic diagnostics for troubleshooting using the command line interface (CLI). • **User**: This user has access to the Zyxel Device's services, such as VPN, and can also browse. This user cannot configure or view the Zyxel Device settings using the web configurator or CLI. • **External User**: This user account is maintained on a remote server, such as RADIUS or LDAP. This user has access to the Zyxel Device's services, such as VPN, and can also browse but cannot configure or view the Zyxel Device settings using the web configurator or CLI.
Lockout Time	This displays how long the IP address has been blocked by the Zyxel Device.

5.16 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 **Network Status > DHCP Table**.

Figure 91 Network Status > DHCP Table



The following table describes the labels in this screen.

Table 48 Network Status > DHCP Table

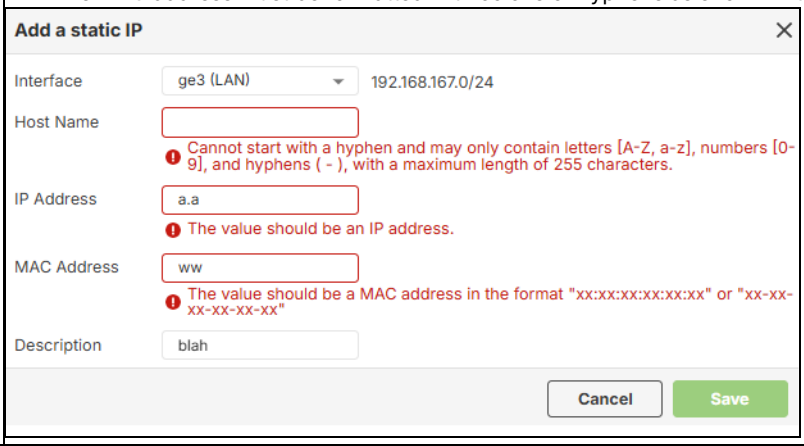
LABEL	DESCRIPTION
Current DHCP List	
Interface	Select a Zyxel Device interface that has DHCP enabled to show to which devices it has assigned DHCP IP addresses.
Add	Click this to add an entry that maps a static IP to a MAC address. • A host name cannot exceed 255 characters. Valid characters are [0-9][a-z][A-Z][-]. You can use duplicate host names, but they cannot start with a space or hyphen. • You must use a valid IPv4 address that is in the DHCP pool. • The MAC address must be formatted with colons or hyphens as shown in the screen. 
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.
Reserved	Select an entry and click on this button to make the entry a static DHCP entry, meaning the DHCP client is always assigned the same IP address from the DHCP server.
Unreserve	Select an entry and click on this button to change the entry from a static DHCP entry to a dynamic DHCP entry, meaning the DHCP client may get a different IP address from the DHCP server when the IP address is renewed.

Table 48 Network Status > DHCP Table (continued)

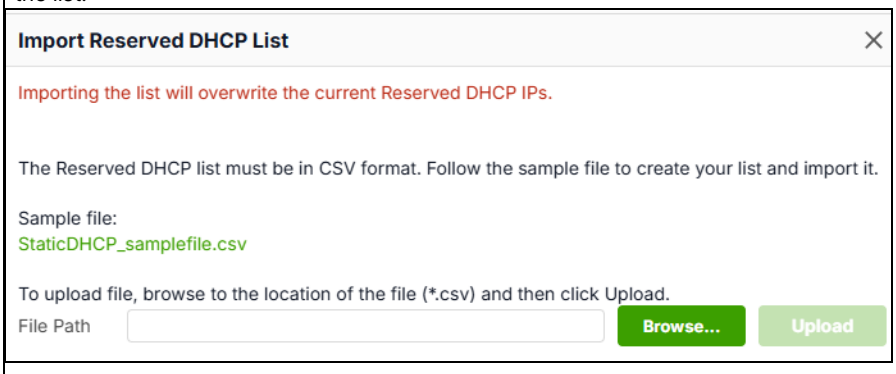
LABEL	DESCRIPTION
Import	A reserved DHCP IP address is an IP address sent from a DHCP server that is aways assigned to the same MAC address. This ensures that the DHCP client always receives the same IP address. This allows you to manage DHCP clients centrally without having to configure static IP addresses on each DHCP client. First create a list of reserved DHCP IP address in a file in CSV (comma separated values) format. Download the sample file (StaticDHCP_samplefile.csv) and follow that format exactly. • The file size must be less than 1MB. • The first row must have the column titles exactly as shown in the sample file: **Interface**, **IP Address**, **Host Name**, **MAC Address**, **Description**, **Status**. • The **Host Name** must be as follows. The first character must be a digit (0–9), or a lowercase letter (a–z), or an uppercase letter (A–Z). Hyphens are not allowed as the first character. After the first character, you may have 0 to 254 more characters. Allowed characters in this part are digits (0–9), lowercase letters (a–z), uppercase letters (A–Z), hyphen (-). The minimum length is 1 character and the maximum length is 255 characters (1 + 254). Valid Examples are a, Z1, abc-123, A0-xyz-9. Invalid Examples are -abc (starts with a hyphen), abc! (contains !), ab@cd (contains @). • The **Host Name** does not need to be unique for each subnet. • **Host Name**s of static DHCP clients cannot be empty. • If the **Host Name** of a reserved DHCP client is empty, the Zyxel Device will replace the hostname with the MAC address of the DHCP client. It will use uppercase letters (for hex A to E), and separate octet pairs with hyphens. • Use the standard format for **IP Address** and **MAC Address**. • The reserved IP addresses must be in the same subnet as the associated interface in the CSV file and the DHCP server. For example, if you have a DHCP server with IP address 192.168.170.200 on the ge3 interface, then please note the following for entries in the CSV file. **1** ge3 192.168.168.33 aa:aa:aa:aa:aa:aa -> this won't be imported as the IP address is not in the DHCP server subnet. **2** ge4 192.168.170.33 aa:aa:aa:aa:aa:ab -> this won't be imported as the interface is wrong **3** ge3 192.168.170.33 aa:aa:aa:aa:aa:ac -> this will be imported • If you use an external DHCP server, by default the DHCP server must have an IP address in the same subnet as the IP address of the Interface on the Zyxel Device. Use the command `usgflex500h running config# vrf main dhcp server subnet` if you want to change the IP address of the DHCP server to be in a different subnet to that of the Zyxel Device interface. For example, you can bind the above DHCP server to the g4 interface with IP subnet 192.168.168.1/24. • **Status** must always be **Reserved**. After you have created the file, click this button to import the file into the Zyxel Device so that the DHCP server can assign these IP addresses to the associated MAC addresses in the list.  If an import fails, please check the points above or check dhcp-import-failed.log in Maintenance > Diagnostics.
Export	Click this button to download all entries in the DHCP table to your computer in csv format with file name containing the current date.
Refresh	Click this button to update the mapping between IP addresses and MAC addresses.

Table 48 Network Status > DHCP Table (continued)

LABEL	DESCRIPTION
Column header	Click a column's heading cell to sort the table entries by the column entry. Click the heading cell again to reverse the sort order.
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. • The Zyxel Device supports the display of host names in languages other than English. • If the DHCP client does not have a hostname, the Zyxel Device uses its MAC address (in uppercase). • **None** shows here for a static DHCP entry. Note: You can have duplicate host names for static (reserved) IP addresses.
MAC Address	This field displays the MAC address to which the IP address is currently assigned or for which the IP address is reserved. The MAC address format can be "xx:xx:xx:xx:xx:xx" or "xx-xx-xx-xx-xx-xx"
VLAN ID	This field displays the VLAN to which the IP address belongs, if any.
Expire Time	This displays the date and time the DHCP-assigned address will be renewed.
Description	This field displays a description of the DHCP client to identify it. The description cannot exceed 64 characters. Valid characters are [0-9][a-z][A-Z][_ -]. Note: You can only edit the description for clients with static (reserved) IP addresses.
Status	This field displays the connection status of the DHCP client. **Reserved** means a static DHCP entry. **-** means a dynamic DHCP entry.

5.17 The IPSec VPN Screen

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.

5.17.1 The Site to Site VPN Screen

Use this screen to display and to manage active IPSec policies.

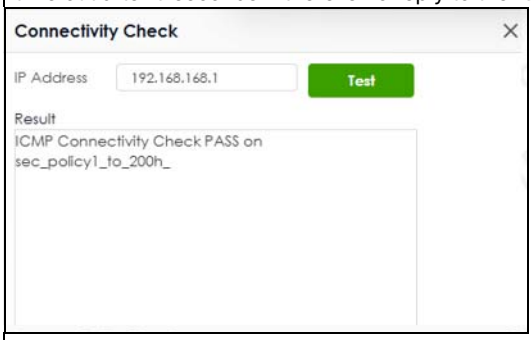
To access this screen, click **VPN Status > IPSec VPN > Site to Site VPN**. The following screen appears.

Figure 92 VPN Status > IPSec VPN > Site to Site VPN



Each field is described in the following table.

Table 49 VPN Status > IPSec VPN > Site to Site VPN

LABEL	DESCRIPTION
Disconnect	Select an IPSec policy and click this button to disconnect it.
Refresh	Select an IPSec policy and click this button to update its status.
Connectivity Check	Select an IPSec policy and click this button to check the connection to a remote client through this VPN tunnel. Enter an IP address in the remote policy subnet range. The Zyxel Device interface must comply with the local policy subnet range. The check will time out after 5 seconds if there is no reply to the ICMP check (Ping). 
#	This field is a sequential value, and it is not associated with a specific SA.
Name	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.
Remote Gateway	This field displays the IP address of the remote gateway.
Remote ID	This field displays the ID of the remote gateway.
My Address	This field displays the IP address of the Zyxel Device.
Policy Route	This field displays the content of the local and remote policies for this IPSec policy. The IP addresses, not the address objects, are displayed.
Uptime	This field displays how many seconds the IPSec policy has been active. This field displays **N/A** if the IPSec policy uses manual keys.
Rekey	This field displays how many seconds remain in the SA life time, before the Zyxel Device automatically disconnects the IPSec policy. This field displays **N/A** if the IPSec policy uses manual keys.
Inbound (Bytes)	This field displays the amount of traffic that has gone through the IPSec policy from the remote IPSec router to the Zyxel Device since the IPSec policy was established.
Outbound (Bytes)	This field displays the amount of traffic that has gone through the IPSec policy from the Zyxel Device to the remote IPSec router since the IPSec policy was established.
Total (Bytes)	This field displays the total traffic that has passed through the IPSec policy (**Inbound + Outbound**) since the IPSec policy was established.
Usage (%)	This field displays the percentage of usage for this IPSec policy among all IPSec policies.
Total Usage for All Tunnels	This displays the total usage of all IPSec policies, including both inbound and outbound usage.

5.17.2 The Remote Access VPN Screen

Use this screen to display or disconnect remote access VPN clients that are connected to the Zyxel Device. The remote access VPN clients must have SecuExtender or use supported computer or mobile operating systems; see Section 13.4 on page 248 for more information.

To access this screen, click **VPN Status > IPSec VPN > Remote Access VPN**. The following screen appears.

Figure 93 VPN Status > IPSec VPN > Remote Access VPN



Each field is described in the following table.

Table 50 VPN Status > IPSec VPN > Remote Access VPN

LABEL	DESCRIPTION
Disconnect	Select a remote access VPN client 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 remote access VPN client.
Username	This field displays the name of the remote access VPN client.
Assigned IP	This field displays the IP address the user used to establish this remote access VPN connection.
Remote IP	This field displays the IP address of the remote IPSec router the remote access VPN client is connected to.
Up Time	This field displays how many seconds the remote access VPN client has been active. This field displays **N/A** if the remote access VPN client uses manual keys.
Reauth/Lease Time	This field displays the amount of reauthentication time remaining and the amount of lease time remaining for each remote access VPN client.
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.

5.18 The SSL VPN Screen

The Zyxel Device keeps track of the SSL VPN clients who are currently logged into the Zyxel Device. Use this screen to:

- 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.

The SSL VPN clients must have SecuExtender or use supported computer or mobile operating systems; see Section 14.2 on page 269 for more information.

Click **VPN Status > SSL VPN > Remote Access VPN** to display the following screen.

Figure 94 VPN Status > SSL VPN > Remote Access VPN



The following table describes the labels in this screen.

Table 51 VPN Status > SSL VPN > Remote Access VPN

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.
Username	This field displays the account user name used to establish this SSL VPN connection.
Assigned IP	This field displays the IP address the user used to establish this SSL VPN connection.
Remote IP	This field displays the remote SSL VPN router the SSL VPN is connected to.
Up Time	This field displays how many seconds the SSL VPN client has been active. This field displays **N/A** if the SSL VPN client uses manual keys.
Reauth/Lease Time	This field displays the amount of reauthentication time remaining and the amount of lease time remaining for each SSL VPN client.
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.

5.18.1 Regular Expressions in Searching IPSec Policies

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.

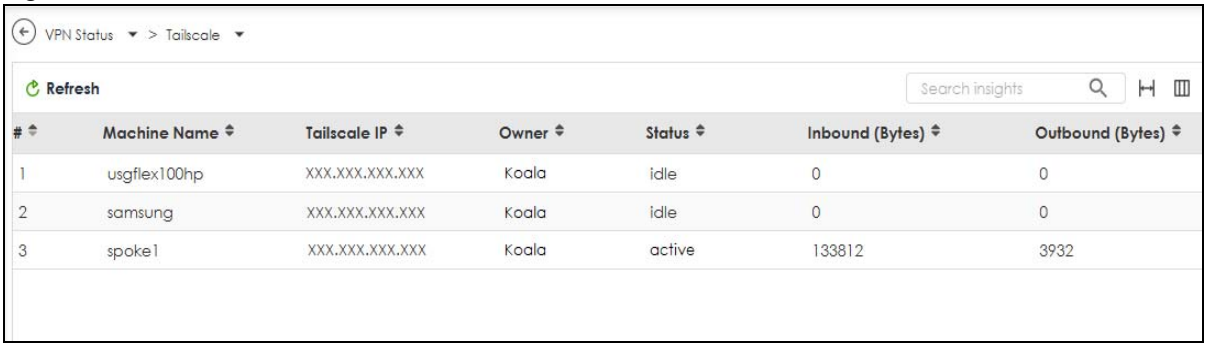
The whole VPN connection or policy name has to match if you do not use a question mark or asterisk.

5.19 The Tailscale Screen

The Zyxel Device supports Tailscale, a mesh VPN (Virtual Private Network) service that connects client devices (such as computers, smartphones, routers, and firewalls) across different networks. Use this screen to view the Tailscale connection status.

Click **VPN Status** > **Tailscale** to display the following screen.

Figure 95 VPN Status > Tailscale



The following table describes the labels in this screen.

Table 52 VPN Status > Tailscale

LABEL	DESCRIPTION
Refresh	Click **Refresh** to update this screen.
#	This field is a sequential value, and it is not associated with a specific VPN connection.
Machine Name	This field displays the domain name of the Tailscale server.
Tailscale IP	This field displays the IP address assigned to the Zyxel Device by the Tailscale server.
Owner	The Tailscale account name that establishes the VPN connection.
Status	This displays the status of the VPN connection. • **active**: The VPN connection is established and data is being transmitted. • **idle**: The VPN connection is established and ready to be used, but no data is being transmitted. • **offline**: The Zyxel Device is currently not connected to the Tailscale network. • **-**: No data has ever been sent to or received from the Zyxel Device.
Inbound (Bytes)	This field displays the number of bytes received by the Zyxel Device on this VPN connection.
Outbound (Bytes)	This field displays the number of bytes transmitted by the Zyxel Device on this VPN connection.

5.20 The Access Points Screen

Use this screen to view the wireless traffic usage and the number of connected stations (wireless clients) for the managed APs.

Each model supports display of data for the following number of historical days.

Table 53 Historical Data Display by Model

MODEL	LAST X DAY(S)
USG FLEX 50H	1
USG FLEX 50HP	1
USG FLEX 100H	1
USG FLEX 100HP	1
USG FLEX 200H	2

Table 53 Historical Data Display by Model

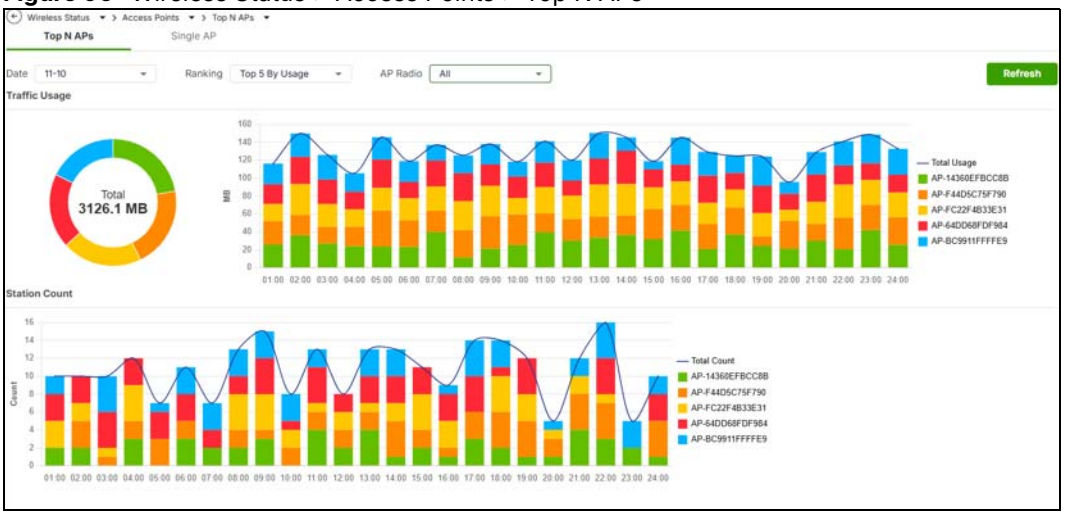
MODEL	LAST X DAY(S)
USG FLEX 200HP	2
USG FLEX 500H	8
USG FLEX 700H	8

5.20.1 The Top N APs Screen

Use this screen to view the wireless traffic usage and associated wireless stations of the top five or top ten managed APs.

Click **Wireless Status > Access Points > Top N APs** to display the following screen.

Figure 96 Wireless Status > Access Points > Top N APs



The following table describes the labels in this screen.

Table 54 Wireless Status > Access Points > Top N APs

LABEL	DESCRIPTION
Date	Select a date to view the preceding 24 hours of data, or select **Last X Days** to view data for the preceding supported days.
Ranking	Select the top five or top ten managed APs by traffic usage or number of connected stations to sort data for display.
AP Radio	If you view data by usage, select the frequency band to display on the graph.
Refresh	The displayed data is updated hourly. Click **Refresh** to get the latest data for the current hour.
Traffic Usage	This graph displays the wireless traffic transmitted to and from the managed APs over time or by date.
Total	This shows the total traffic used by all managed APs on the selected date or over the selected date range.
y-axis	This represents the amount of traffic in **MB** (megabytes), **GB** (gigabytes), **TB** (terabytes), or **PB** (petabytes).
x-axis	This represents the time or date.
Station Count	This graph displays the number of wireless stations connected to the managed APs over time or by date.

Table 54 Wireless Status > Access Points > Top N APs

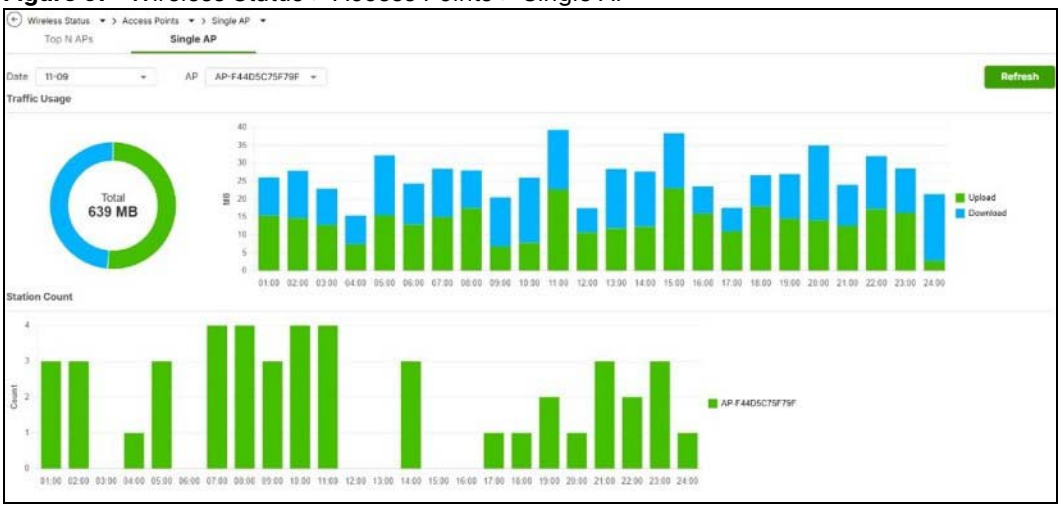
LABEL	DESCRIPTION
y-axis	This represents the number of connected wireless stations.
x-axis	This represents the time or date.

5.20.2 The Single AP Screen

Use this screen to view wireless traffic usage and wireless stations for a managed AP.

Click **Wireless Status > Access Points > Single AP** to display the following screen.

Figure 97 Wireless Status > Access Points > Single AP



The following table describes the labels in this screen.

Table 55 Wireless Status > Access Points > Single AP

LABEL	DESCRIPTION
Date	Select a date to view the preceding 24 hours of data, or select **Last X days** to view data for the preceding supported days.
AP	Select a managed AP to view its wireless data.
Refresh	The displayed data is updated hourly. Click **Refresh** to get the latest data for the current hour.
Traffic Usage	This graph displays the traffic usage of the managed AP over time or by date.
Total	This shows the total traffic used by the managed AP on the selected date or over the selected date range.
y-axis	This represents the amount of traffic in **MB** (megabytes), **GB** (gigabytes), **TB** (terabytes), or **PB** (petabytes).
x-axis	TThis represents the time or date.
Station Count	This graph displays the number of wireless stations connected to the managed AP over time or by date.
y-axis	This represents the number of connected wireless stations.
x-axis	This represents the time or date.

5.21 The WLAN Clients Screen

Use this screen to view the wireless traffic usage of the managed APs' wireless clients.

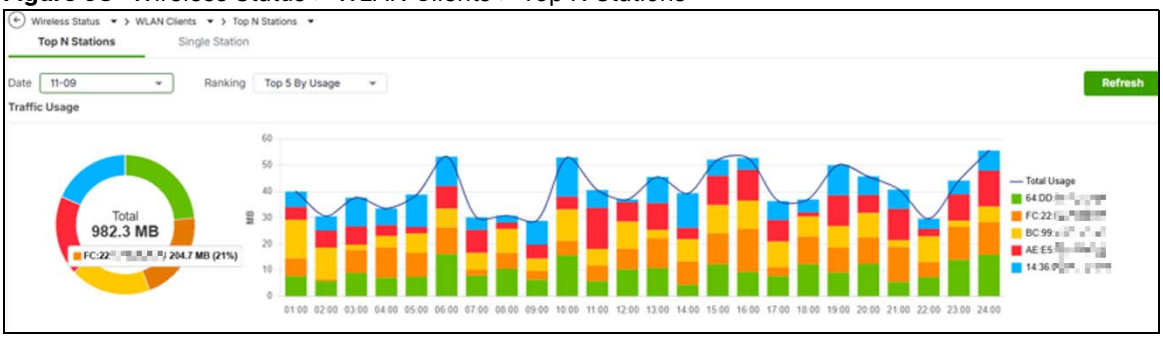
Refer to Historical Data Display by Model for the number of historical days each model supports for display.

5.21.1 The Top N Stations Screen

Use this screen to view the traffic usage of the top five or top ten wireless clients.

Click **Wireless Status > WLAN Clients > Top N Stations** to display the following screen.

Figure 98 Wireless Status > WLAN Clients > Top N Stations



The following table describes the labels in this screen.

Table 56 Wireless Status > WLAN Clients > Top N Stations

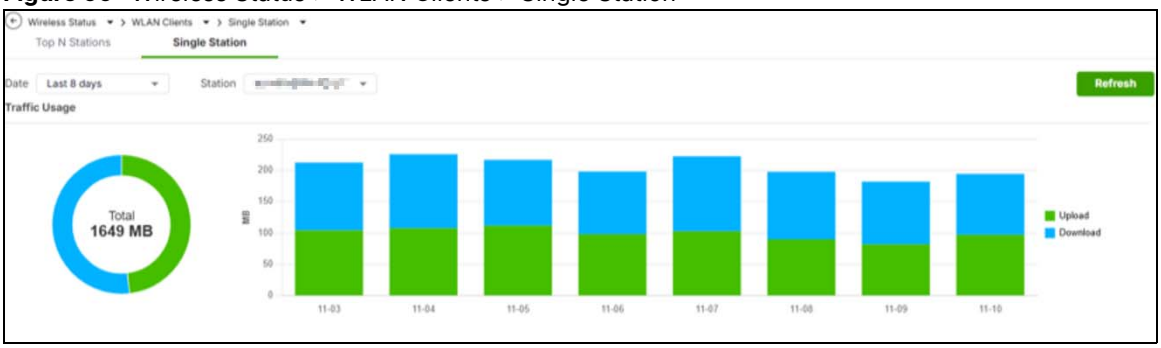
LABEL	DESCRIPTION
Date	Select a date to view the preceding 24 hours of data, or select **Last X days** to view data for the preceding supported days.
Ranking	Select the top five or top ten wireless clients by traffic usage to sort data for display.
Refresh	The displayed data is updated hourly. Click **Refresh** to get the latest data for the current hour.
Traffic Usage	This graph displays the wireless traffic transmitted to and from the wireless clients over time or by date.
Total	This shows the total traffic used by all wireless clients on the selected date or over the selected date range.
y-axis	This represents the amount of traffic in **MB** (megabytes), **GB** (gigabytes), **TB** (terabytes), or **PB** (petabytes).
x-axis	This represents the time or date.

5.21.2 The Single Station Screen

Use this screen to view the traffic usage of a wireless client.

Click **Wireless Status > WLAN Clients > Single Station** to display the following screen.

Figure 99 Wireless Status > WLAN Clients > Single Station



The following table describes the labels in this screen.

Table 57 Wireless Status > WLAN Clients > Single Station

LABEL	DESCRIPTION
Date	Select a date to view the preceding 24 hours of data, or select **Last X days** to view data for the preceding supported days.
Station	Select a wireless client to view its wireless data.
Refresh	The displayed data is updated hourly. Click **Refresh** to get the latest data for the current hour.
Traffic Usage	This graph displays the wireless traffic transmitted to and from the wireless client over time or by date.
Total	This shows the total traffic used by the wireless client on the selected date or over the selected date range.
y-axis	This represents the amount of traffic in **MB** (megabytes), **GB** (gigabytes), **TB** (terabytes), or **PB** (petabytes).
x-axis	This represents the time or date.

CHAPTER 6
Licensing

6.1 Licensing Overview

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

- Use the **Licenses** screen to refresh Zyxel Device registration. Go to nebula.zyxel.com to register your Zyxel Device and activate a service, such as content filtering.
- Use the **Signature Update** screen to download the latest signatures for your licensed services.

Please note that you cannot use the security services and upgrade firmware if your Zyxel Device is not registered at NCC or the services do not have a license. Your Zyxel Device and network will be exposed to threats and attacks. We strongly recommend you to register your Zyxel Device and purchase a license at NCC to better protect your Zyxel Device and network.

6.1.1 What you Need to Know

This section introduces the topics covered in this chapter.

Subscription Services Available

See **Licensing > Signature Update** for the subscription services that your Zyxel Device supports. You can extend a service at **NCC** > **Organization-wide** > **License & Inventory**.

Signature Update

- You need a valid service registration to update the Application Patrol signatures, IPS signatures and IP Reputation signatures.
- Schedule signature updates for a day and time when your network is least busy to minimize disruption to your network.

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

Features Available Without a License

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

Table 58 Features Available Without a License

MONITOR	CONFIGURATION	MAINTENANCE
System Statistics	Network	Maintenance
Network Status	VPN	
VPN Status	Security Policy	
	Object	
	User & Authentication	

Table 58 Features Available Without a License

MONITOR	CONFIGURATION	MAINTENANCE
	System	
	Log & Report (except SecuReporter)	

Check if Your Zyxel Device Has an Inactive License

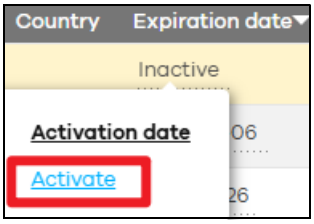
After purchasing a license, assign it to your Zyxel Device. You have to activate the assigned license manually before your Zyxel Device can use it.

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

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.



6.1.2 The Licenses Screen

Use this screen to display the status of your service registrations and upgrade licenses. Go to NCC to register your Zyxel Device or purchase a license.

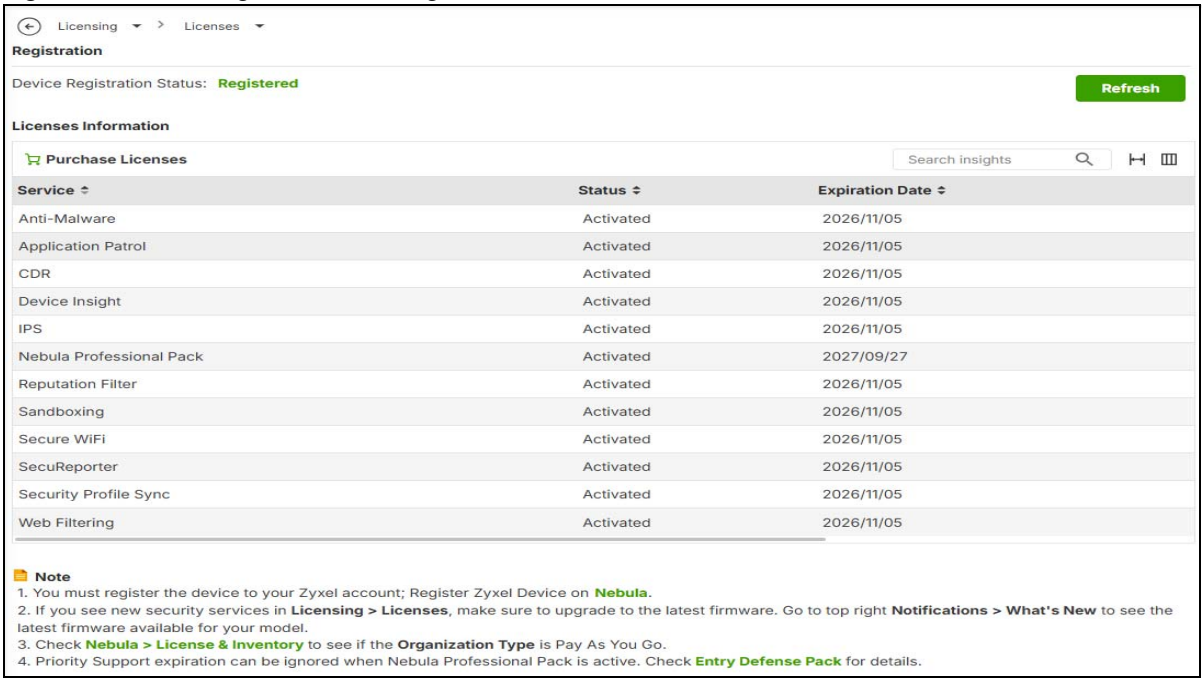
Pay As You Go (PAYG) is a new license payment method for specific organizations known as 'PAYG Orgs'. Instead of paying in full for a license in advance, you reserve your credit card for future monthly payments.

PAYG is charged for a Gold Security Pack license or a Nebula Professional Pack license for each Zyxel Device in the 'PAYG Org'. Each Nebula Device in a PAYG Org will be charged for at least a Nebula Professional Pack license.

See Section 1.3 on page 20 for related information on licensing and grace period.

Click **Licensing** > **Licenses** to display the following screen.

Figure 100 Licensing > Licenses (Registered)



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

The following table describes the labels in this screen.

Table 59 Licensing > Licenses

LABEL	DESCRIPTION
Device Registration Status	This field display the Zyxel Device registration status on NCC. • **Registered**: Your Zyxel Device has successfully registered at NCC. • **Not Registered**: Your Zyxel Device is not registered at NCC. Make sure you're connected to the Internet. Wait a few minutes then click **Refresh** to update the registration status.
Refresh	Click this and wait for a few moments for the license and device registration status to update. The license and device registration status are updated automatically once every day.
Purchase License	Click **Purchase License** to go to Marketplace to renew Zyxel Device licenses.
Licenses Information	
Service	This lists the name of services or service modules that are available on the Zyxel Device.
Anti-Malware	This is a license for cloud database signatures to detect virus patterns in files.
Application Patrol	This is a license to use signatures to manage the use of various applications on the network.
CDR	This is a license to detect wired and wireless clients that have become infected in your network and to block or isolate traffic coming from them. In this way, malicious traffic is not spread throughout the network. Secure policies can block malicious traffic for specific traffic flows, but CDR can block malicious traffic from the sender. Malicious traffic is identified using a combination of Web Filtering, Anti-Malware and IPS (IDP) signatures. You configure Collaborative Detection & Response (CDR) to block or quarantine traffic coming from wired or WiFi clients that are sending malicious traffic in NCC. See Section 1.2 on page 20 for more information on NCC.

Table 59 Licensing > Licenses (continued)

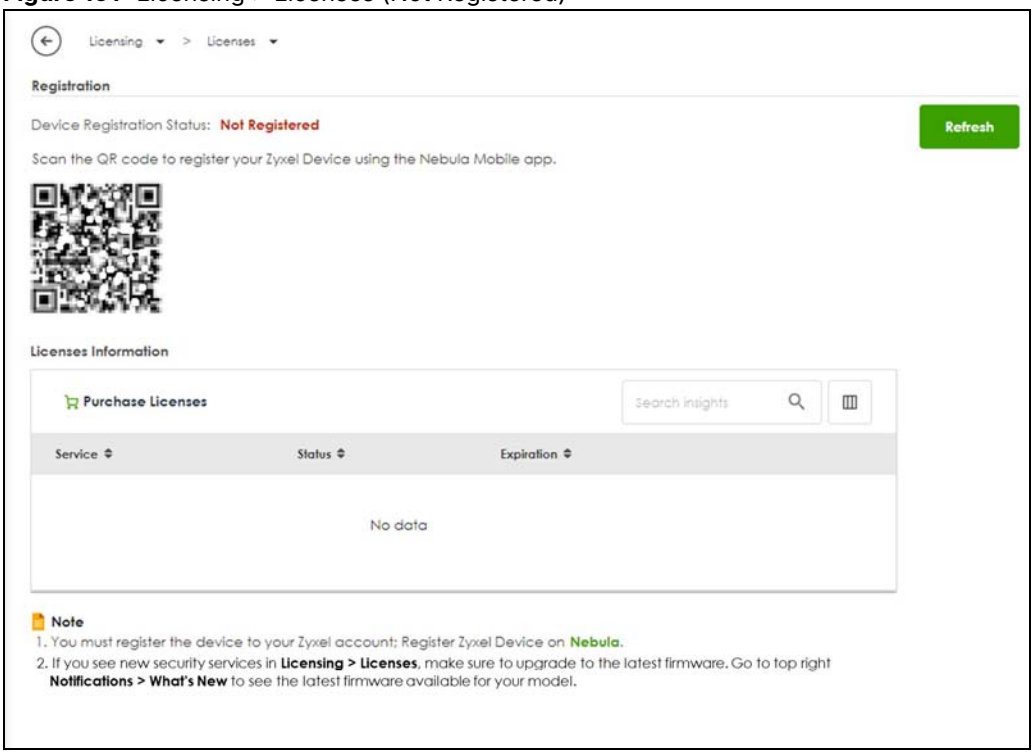
LABEL	DESCRIPTION
Device Insight	This is a license to detect and manage client devices in the Zyxel Device local network and DMZ.
IPS	This is a license to detect Intrusion Prevention System attacks.
Nebula Professional Pack	This is a license that allows you to use NCC to monitor and manage groups of Zyxel Devices in organizations. See the NCC User's Guide for more information on Nebula Plus and Professional pack licenses.
Priority Support	This license only displays if the Gold Security Pack license for this Zyxel Device has expired. It allows you to request support for Zyxel Devices in Nebula organizations that do not have a Nebula Professional Pack license (Base-Tier). If you have a Nebula Professional Pack license, you will have Priority Support (**Activated**), but the **Status** here may display **Expired**. Ignore it.
Reputation Filter	This is a license to recognize packets coming from suspect IPv4 addresses.
Sandboxing	This is a license to provide an isolated environment to scan traffic from the WAN that comes with unknown files or untrusted programs.
Secure WiFi	The Secure WiFi license allows you to manage more than the default number of APs (8 at the time of writing). Remote AP allows an IPSec VPN tunnel from a supported external AP to the Zyxel Device.
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. SecuReporter retains logs for up to 1 year.
Security Profile Sync	Security Profile Sync is a NCC template that allows you to share the same security service settings on Firewalls in different sites in the same organization. Security service settings include Content Filter, Application Patrol, URL Threat Filter, Anti-Malware, and Intrusion Detection / Prevention.
Web Filtering	This is a license to a database that can block websites by category, such as Gambling.
Status	This field displays whether a service license is enabled at NCC (**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.
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 IPS, Application Patrol, Anti-Malware and Web Filtering during the grace period. After the grace period ends, all of these features are disabled.
Note	This displays additional information on a license such as the number of supported APs for the Secure WiFi license.

You will see the following screen if:

- Your Zyxel Device is not registered at NCC.
- You're logging into the Zyxel Device using an admin account.

Scan the QR code or click **Nebula** under **Note** to register your Zyxel Device at NCC. Please note that you need to register your Zyxel Device at NCC to upgrade firmware and use security services.

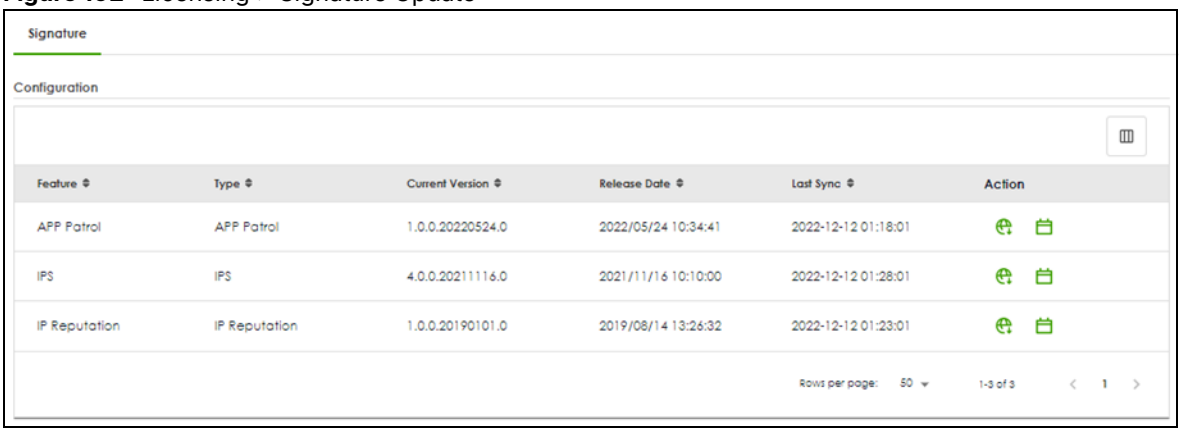
Figure 101 Licensing > Licenses (Not Registered)



6.1.3 The Signature Update Screen

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

Figure 102 Licensing > Signature Update



The following table describes the labels in this screen.

Table 60 Licensing > Signature Update

LABEL	DESCRIPTION
Feature	This field displays the name of the services available on the Zyxel Device.
Type	This field displays the type of service engine used by the Zyxel Device.
Current Version	This field displays the signatures version number currently used by the Zyxel Device. This number gets larger as new signatures are added.

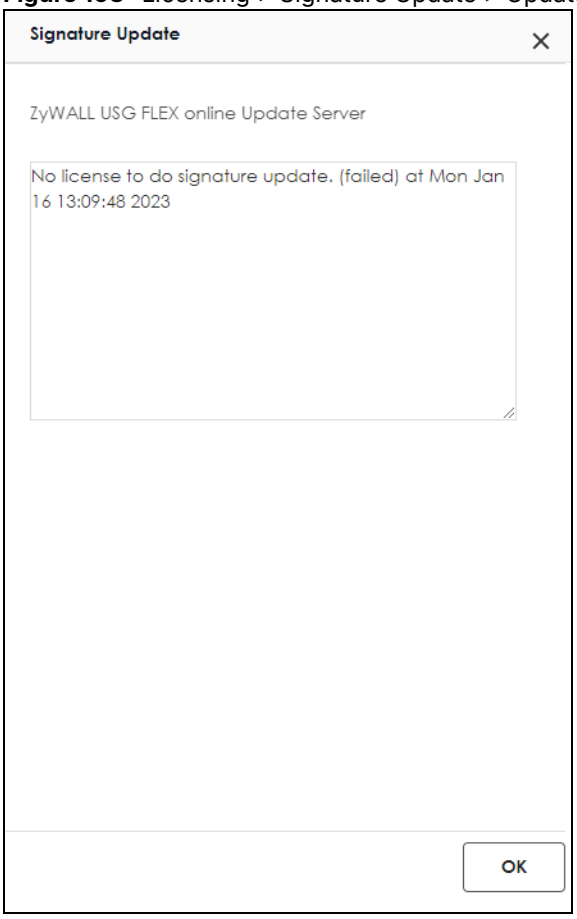
Table 60 Licensing > Signature Update (continued)

LABEL	DESCRIPTION
Release Date	This field displays the date and time the set was released.
Last Sync	This field displays the date and time the Zyxel Device last checked for new signatures.
Action	Click the **Update** icon ( )to have the Zyxel Device immediately check for new signatures. If new signatures are found, they are then downloaded to the Zyxel Device. Click the **Schedule** icon ( ) to have the Zyxel Device automatically check for new signatures regularly at the time and day specified. You should select a time when your network is not busy for minimal interruption.

6.1.4 Signature Update

Click the **Update** icon ( ) of a service to display the following screen. Use this screen to view the service update status.

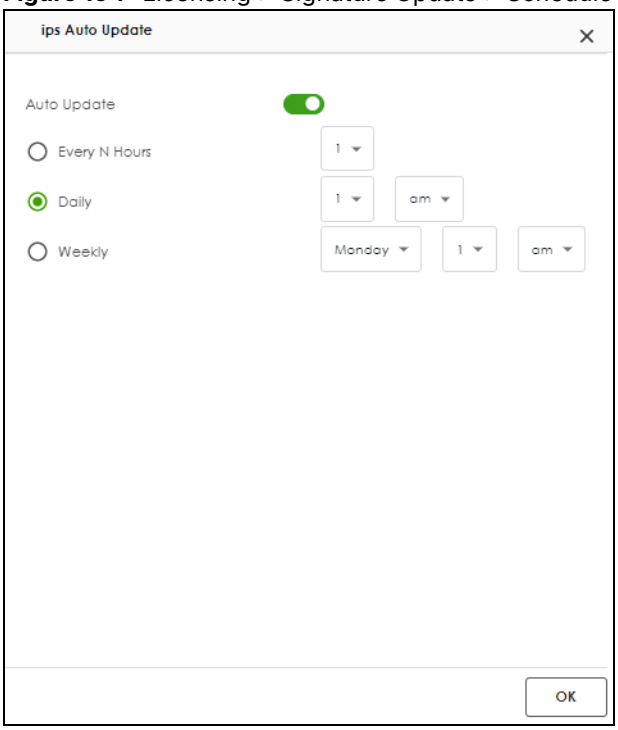
Figure 103 Licensing > Signature Update > Update > Update



6.1.5 Auto Update

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

Figure 104 Licensing > Signature Update > Schedule > Auto Update



The following table describes the labels in this screen.

Table 61 Licensing > Signature Update > Schedule > Auto Update

LABEL	DESCRIPTION
Auto Update	Enable to have the Zyxel Device automatically check for new signatures regularly at the time and day specified. You should select a time when your network is not busy for minimal interruption.
Every N Hours	Select this option to have the Zyxel Device check for new signatures every specified (N) hour.
Daily	Select this option to have the Zyxel Device check for new signatures every day at the specified time. The time format is the 12 hour clock.
Weekly	Select this option to have the Zyxel Device check for new signatures once a week on the day and at the time specified.
OK	Click this button to save your changes to the Zyxel Device.

CHAPTER 7
Interfaces

7.1 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.
- An **Individual Port** is a port for high-performance routing where you need a direct and dedicated path for high-throughput connections such as WAN or uplink connections.

Note: You cannot group Individual ports together or with other ports, nor put more than one individual port in a VLAN interface.

Table 62 Models with Individual Ports

MODEL	INDIVIDUAL PORTS
USG FLEX 500H	P1, P2
USG FLEX 700H	P1, P2, P13, P14

- **Interfaces** are used within the system operationally. You use the fm 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.

7.1.1 What You Can Do in this Chapter

- Use the **Interface** (Section 7.2 on page 139) screen to view a summary of the Zyxel Device interface settings.
- Use the **External/Internal/General/VTI Interface** (Section 7.3 on page 142) screens to configure Ethernet, VLAN, and bridge interfaces.

  Ethernet interfaces are the foundation for defining other interfaces and network policies.

  VLAN interfaces receive and send tagged frames. The Zyxel Device automatically adds or removes the tags as needed.

  Bridge interfaces combine two or more network segments into a single network.

  LAG interfaces combine multiple physical Ethernet interfaces into a single logical interface.
- Use the **Trunk** (Section 7.8 on page 173) screen to configure load balancing.
- Use the **Port** screen (Section 7.9 on page 176) to configure Zyxel Device port settings.

7.1.2 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.

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** screen to set multiple physical ports to be part of the same interface.
- **Ethernet interfaces** are the foundation for defining other interfaces and network policies.
- **VLAN interfaces** receive and send tagged frames. The Zyxel Device automatically adds or removes the tags as needed.
  - By default, Individual ports P13 and P14 do not have an Ethernet interface. If you want to use one of these ports in a VLAN interface, the Zyxel Device will automatically create an Ethernet Interface on top of these physical port.
  - Similarly, if you remove the default Ethernet interface (ge1) from Individual ports P1 or P2, and you want to use one of these ports in a VLAN interface, the Zyxel Device will automatically create an Ethernet Interface on top of these physical ports.

Note: You cannot put more than one individual port in a VLAN 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.
- **Trunk interfaces** manage load balancing between interfaces.
- **PPPoE interfaces** support Point-to-Point Protocols (PPP). ISP accounts are required for PPPoE interfaces.
- **VPN Tunnel Interface (VTI)** encrypts or decrypts IPv4 traffic from or to the interface according to the IP routing table.
- **Link Aggregation Group (LAG) interfaces** combine multiple physical Ethernet interfaces into a single logical interface, thus increasing uplink bandwidth and availability in the event a link goes down.

See the following table for interface types and supported features.

Table 63 Features Per Interface Type

ROLES	EXTERNAL	INTERNAL	GENERAL
Characteristics	Ethernet VLAN Bridge LAG PPPoE	Ethernet VLAN Bridge LAG	Ethernet VLAN Bridge LAG
Configurable Zone	Yes	Yes	Yes
Static IP address	Yes	Yes	Yes
DHCP client	Yes	No	Yes
DHCP server/relay	No	Yes	Yes
Default SNAT	Yes	No	No
Packet size (MTU)	Yes	Yes	Yes
Connectivity Check	Yes	Yes	Yes

Relationships Between Interfaces

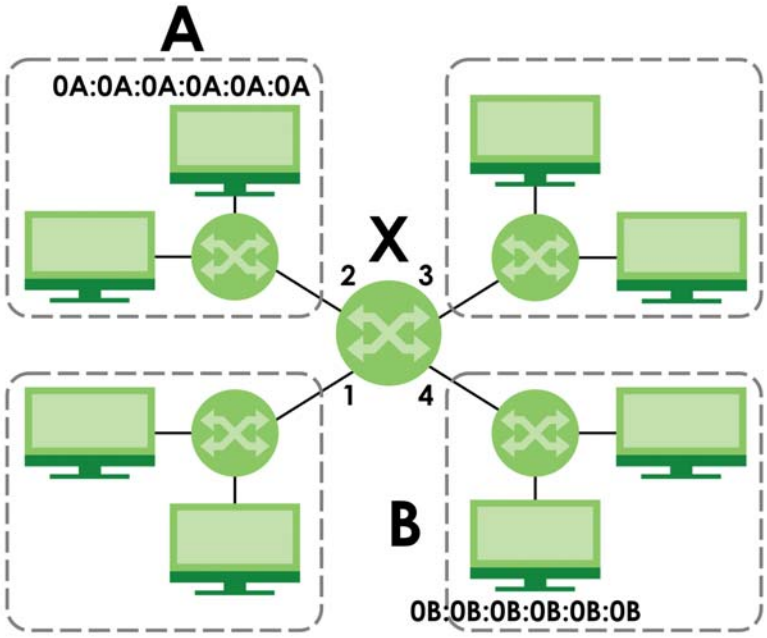
In the Zyxel Device, interfaces are usually created on top of other interfaces. Only Ethernet interfaces are created directly on top of the physical ports or port groups. The relationships between interfaces are explained in the following table.

Table 64 Relationships Between Different Types of Interfaces

INTERFACE	RESTRICTION	REQUIRED PORT / INTERFACE
Ethernet interface	N/A	physical port
LAG	When you configure a LAG interface, you cannot set the LAG interface on an Ethernet interface that is already used by other interfaces.	Ethernet interface
Bridge interface	When you configure a bridge interface, you cannot set the bridge interface on an interface that is already used by other bridge or VLAN interfaces.	Ethernet interface* VLAN interface*
Trunk	When you configure a trunk interface, you cannot set the trunk interface on an interface that is already used by other bridge or LAG interfaces.	External/General Ethernet interface VLAN interface LAG interface PPPoE interface bridge interface
PPPoE interface	N/A	Ethernet interface* VLAN interface* bridge interface

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 65 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 66 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.

The Zyxel Device can bridge traffic between some interfaces while it routes traffic for other interfaces. The bridge interfaces also support 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 67 Example: Routing Table Before 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

Table 68 Example: Routing Table After Bridge Interface br0 Is Created

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.

IP Address Assignment

Most interfaces have an IP address and a subnet mask.

Figure 105 Example: Entry in the Routing Table Derived from Interfaces



This information is used to create an entry in the routing table.

Table 69 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 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 70 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 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.

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 71 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 134.
- Gateway - The interface provides the same gateway you specify for the interface. See IP Address Assignment on page 134.
- 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 Overview

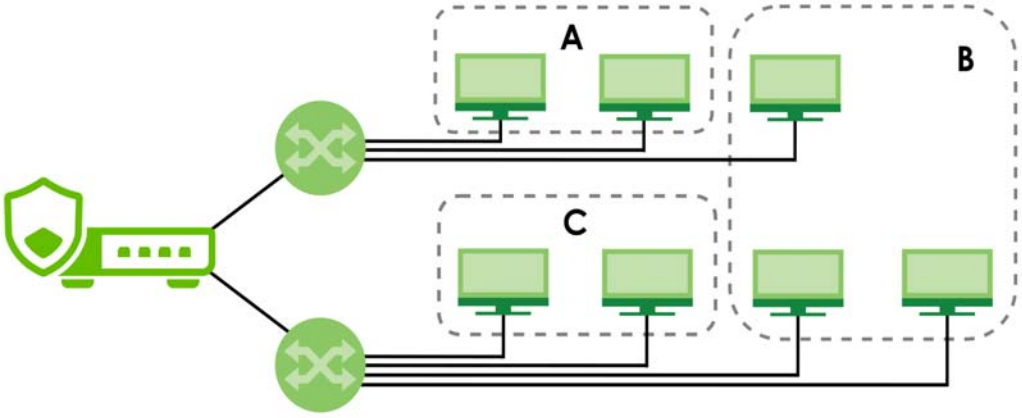
Point-to-Point Protocol over Ethernet (PPPoE, RFC 2516) is usually used to connect two computers over phone lines or broadband connections. PPPoE is often used with cable modems and DSL connections. It provides the following advantages:

- 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.

VLANs

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

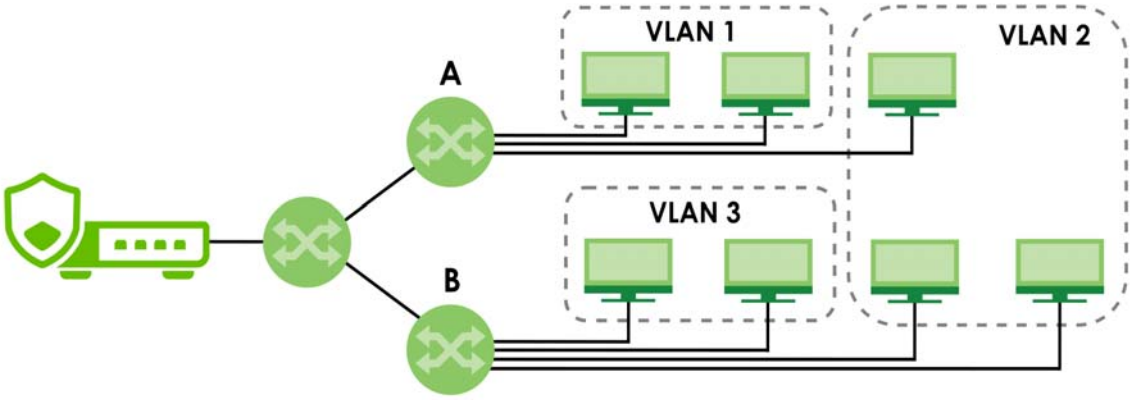
Figure 106 Example: Before VLAN



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 107 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.

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.

VLAN ID

A VLAN ID (Virtual Local Area Network Identifier) is used to identify a specific VLAN within a network. When a device sends a packet tagged with a VLAN ID, other devices recognize which VLAN the packet belongs to.

Note: The valid VLAN ID range is 1 to 4094, but use 1 to 4084, if you are using Device HA.

LAG

Link Aggregation Group (LAG) is a way to combine multiple physical Ethernet interfaces into a single logical interface. This increases uplink bandwidth. It also increases availability as even if a member link goes down, LAG can continue to transmit and receive traffic over the remaining links.

To configure LAG, configure a link number and specify the member ports in the link. All ports must have the same speed and be in full-duplex mode. You must configure the LAG on both sides of the link and you must set the interfaces on either side of the link to be the same speed.

Ethernet interfaces available to join a LAG interface must fulfill the following criteria.

1 The interface cannot be in another LAG. If an interface is in another LAG, it is not available to join the LAG interface until you remove the interface from the other LAG.

2 The interface cannot be in a VLAN or PPPoE. If the interfaces is bound to an interface that is in a VLAN or PPPoE, the interface is not available to join the LAG interface until you remove the interface from the VLAN or PPPoE.

3 The selected interface must be bound to only 1 physical port.
   - If you select an interface that has no ports bound to it, you must bind a port to this interface.
   - If you select an interface that has more than one port bound to it, you must remove all ports but one from this interface.

7.2 Interface Screen

Use this screen to view your Zyxel Device interface settings. To access this screen, click **Network** > **Interface** > **Interface**.

Add an interface to which type of network you will connect. When you select **Internal, External** or **General,** the rest of the screen's options automatically adjust to correspond.

- The **External** interface is for connecting to an external network (like the Internet). The Zyxel Device automatically adds this interface to the default WAN trunk.
- The **Internal** interface 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; for example LAN to WAN traffic.
- The **General** interface is for connecting to either an external network or a local network. Select this option when you want full flexibility to manually define specific routing, NAT, or security rules without the automatic settings applied to **Internal** or **External** interfaces.

7.2.1 Interface Screen Warning Messages

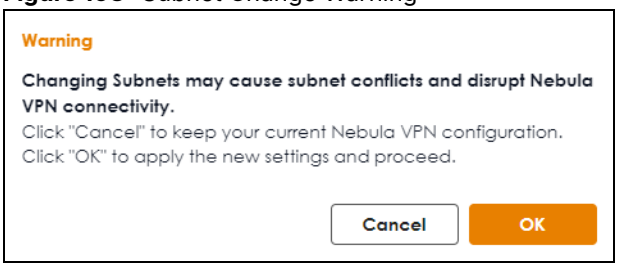
Nebula VPN allows Zyxel Devices from different sites in an organization to communicate through a VPN.

The following reminder appears on the **Network > Interface > Interface** screen if Nebula VPN is enabled. If you change IP addresses locally, there may be a conflict that would impact Nebula VPN.



The following warning appears if Nebula VPN is enabled and you are removing an interface. This may disrupt Nebula VPN. Ensure your Zyxel Device's local IP address and network mask are different from those used by local networks behind other Zyxel Devices participating in Nebula VPN.

Figure 108 Subnet Change Warning



The following warning appears if Nebula VPN is enabled and you are removing an interface. This may disrupt Nebula VPN. Ensure you do not remove a subnet interface that is participating in the organization's VPN in the NCC.

Figure 109 Interface Removal Warning

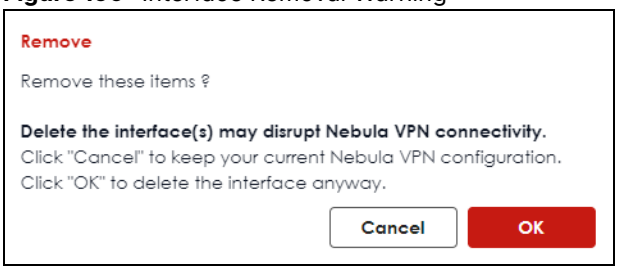
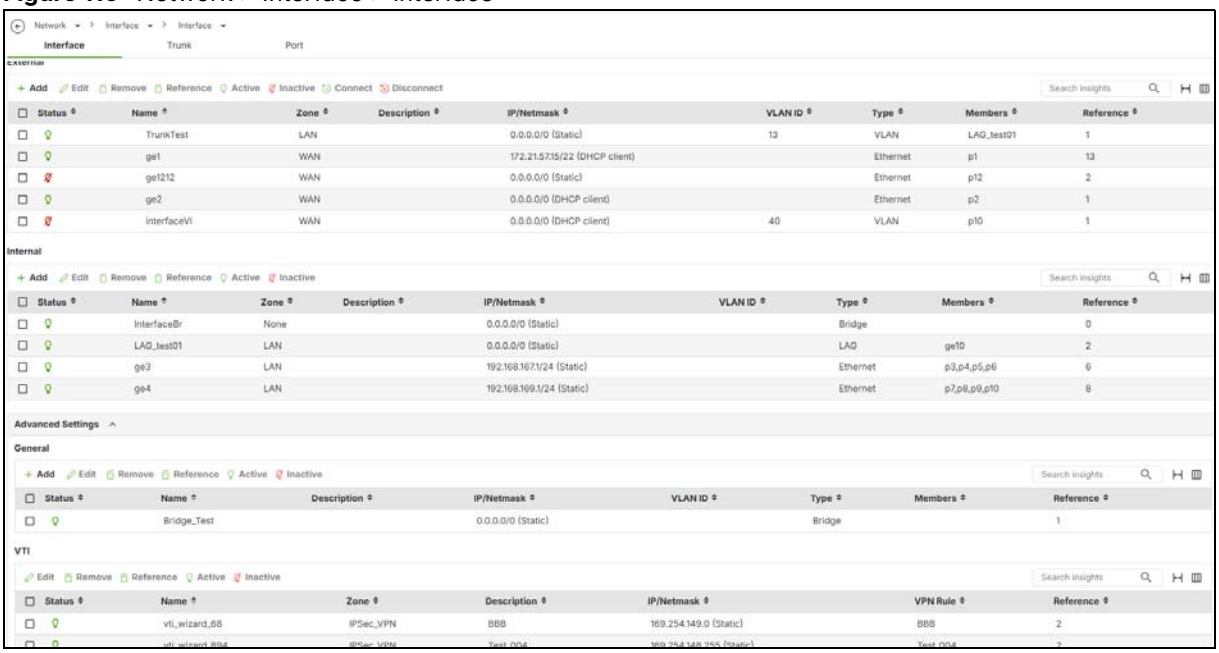


Figure 110 Network > Interface > Interface



Each field is described in the following table.

Table 72 Network > Interface > Interface

LABEL	DESCRIPTION
External	
Add	Click this to add a new entry.
Edit	Select an entry and click **Edit** to open a screen where you can modify the entry's settings.

Table 72 Network > Interface > Interface (continued)

LABEL	DESCRIPTION
Remove	To remove a virtual interface, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Reference	This field displays the objects this entry uses.
Active	To turn on an entry, select it and click **Active**. The **Status** light changes accordingly.
Inactive	To turn off an entry, select it and click **Inactive**. The **Status** light changes accordingly.
Connect	To dial-up to a PPPoE interface, select it and click **Connect**.
Disconnect	To disconnect from a PPPoE interface, select it and click **Disconnect**.
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.
Zone	This displays the zone to which this interface belongs. An interface can only be in one zone.
Description	This field displays the description of the interface.
IP/Netmask	This field displays the current IP address, the subnet mask of the interface and whether the IP address is **Static** or dynamic (**DHCP client**). If this field is 0.0.0.0/0, the interface does not have an IP address yet.
VLAN ID	This field displays the VLAN ID which is a 12-bit number that uniquely identifies each VLAN.
Type	This field displays the interface type: Ethernet or VLAN.
Ports	This field displays the port the interface is using.
Reference	This field displays how many objects this entry uses.
Internal	
Add	Click this to add a new entry.
Edit	Select an entry 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.
Reference	This field displays the objects this entry uses.
Active	To turn on an entry, select it and click **Active**. The **Status** light changes accordingly.
Inactive	To turn off an entry, select it and click **Inactive**. The **Status** light changes accordingly.
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.
Zone	This displays the zone to which this interface belongs. An interface can only be in one zone.
Description	This field displays the description of the interface.
IP/Netmask	This field displays the current IP address and the subnet mask of the interface. If this field is empty, the interface does not have an IP address yet.
MAC Address	This field displays the MAC address of the interface hardwares.
VLAN ID	This field displays the VLAN ID which is a 12-bit number that uniquely identifies each VLAN.
Type	This field displays the interface type.
Members	This field displays the port the interface is using.
Reference	This field displays how many objects this entry uses.
Advanced Settings	
General	
Add	Click this to add a new entry.
Edit	Select an entry and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove a general interface, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.

Table 72 Network > Interface > Interface (continued)

LABEL	DESCRIPTION
Reference	This field displays the objects this entry uses.
Active	To turn on an entry, select it and click **Active**. The **Status** light changes accordingly.
Inactive	To turn off an entry, select it and click **Inactive**. The **Status** light changes accordingly.
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.
Zone	This displays the zone to which this interface belongs. An interface can only be in one zone.
Description	This field displays the description of the interface.
IP/Netmask	This field displays the current IP address and the subnet mask of the interface. If this field is empty, the interface does not have an IP address yet.
VLAN ID	This field displays the VLAN ID which is a 12-bit number that uniquely identifies each VLAN.
Type	This field displays the interface type.
Members	This field displays the Ethernet interfaces and VLAN interfaces in the bridge interface. It is blank for virtual interfaces.
Reference	This field displays how many objects this entry uses.
VTI	
Edit	Select an entry 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.
Reference	This field displays the objects this entry uses.
Active	To turn on an entry, select it and click **Active**. The **Status** light changes accordingly.
Inactive	To turn off an entry, select it and click **Inactive**. The **Status** light changes accordingly.
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.
Zone	This displays the zone to which this interface belongs. An interface can only be in one zone.

7.3 External Interface

Use this screen to configure the external interface settings for connecting to an external network (like the Internet). The Zyxel Device automatically adds an external interface to the default WAN trunk.

7.3.1 External Interface Add/Edit

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.

Figure 111 Network > Interface > Interface > External > Add (General Settings/Ethernet IPv4)

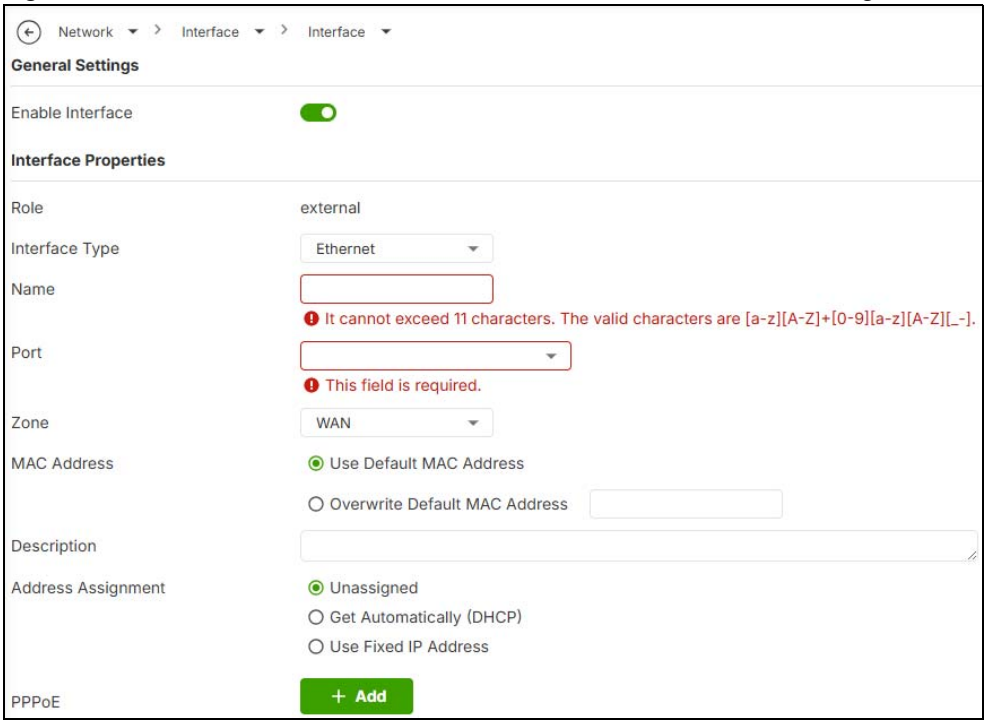


Figure 112 Network > Interface > Interface > External > Add (General Settings/LAG IPv4)

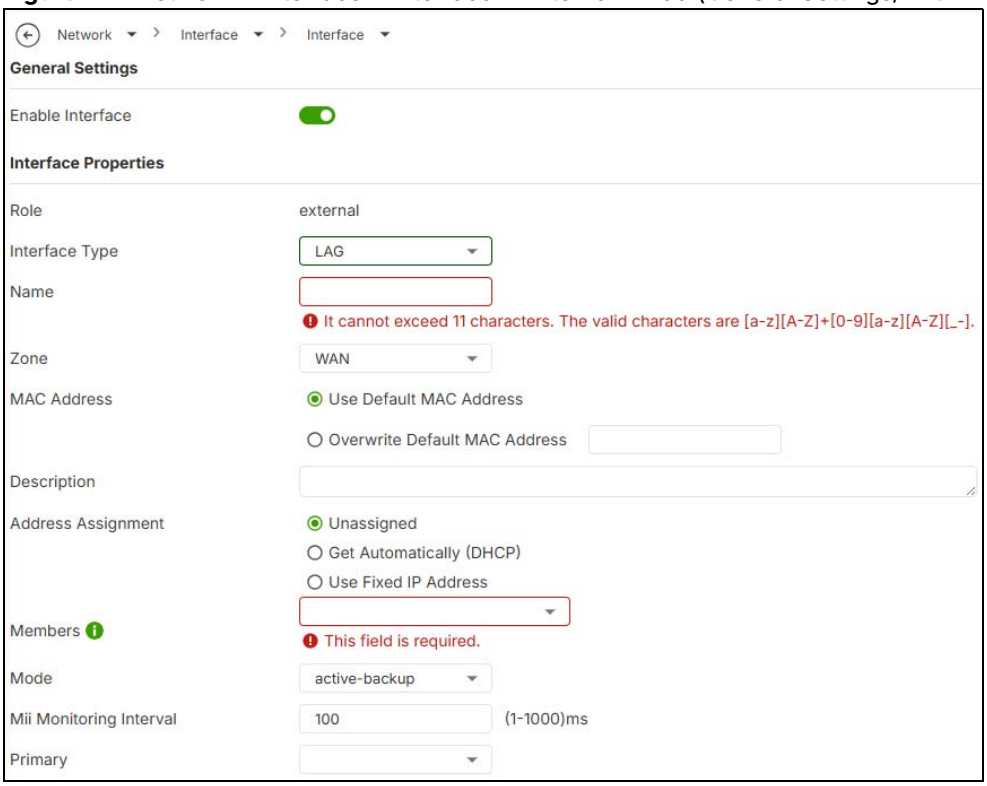


Figure 113 Network > Interface > Interface > External > Add (General Settings/VLAN IPv4)

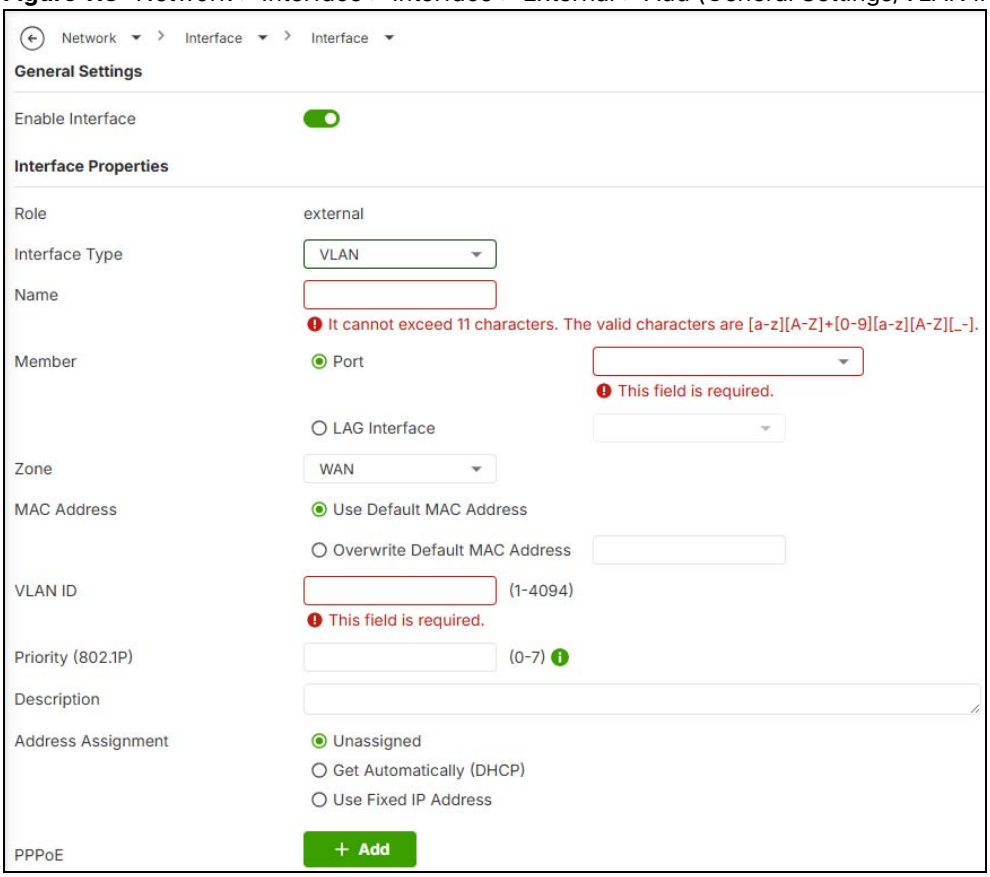


Figure 114 Network > Interface > Interface > External > Add (General Settings/Bridge IPv4)

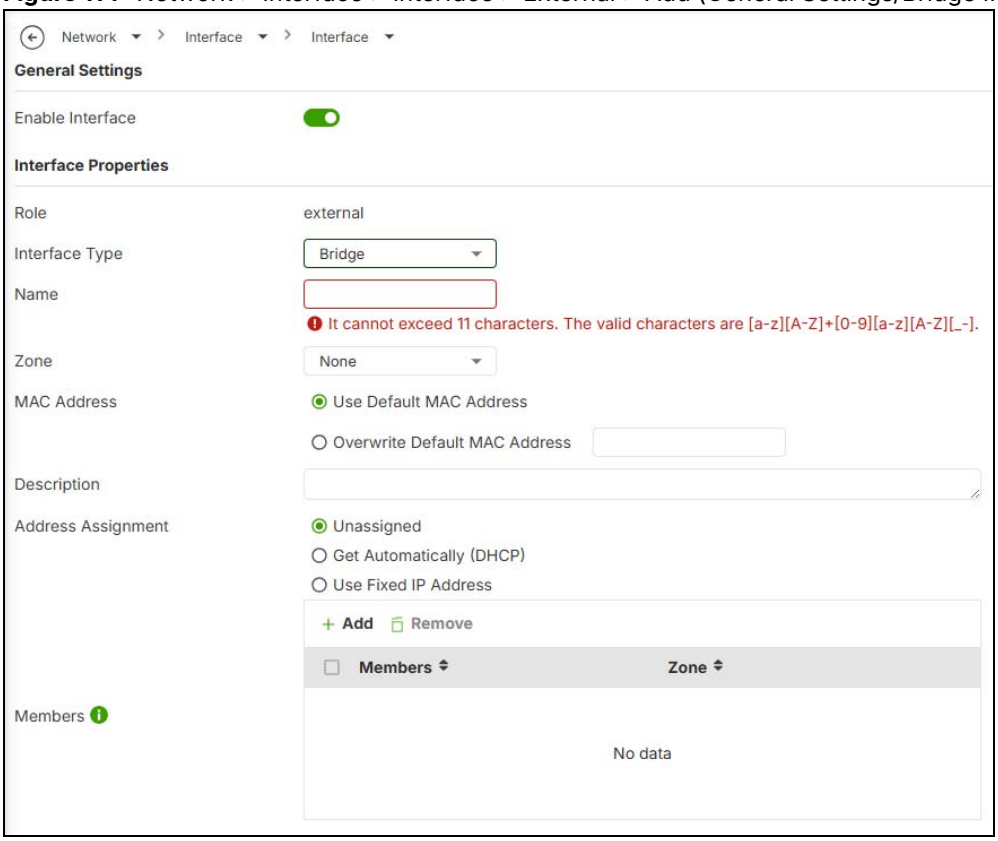


Figure 115 Network > Interface > Interface > External > Add (Ethernet_PPPoE Add)

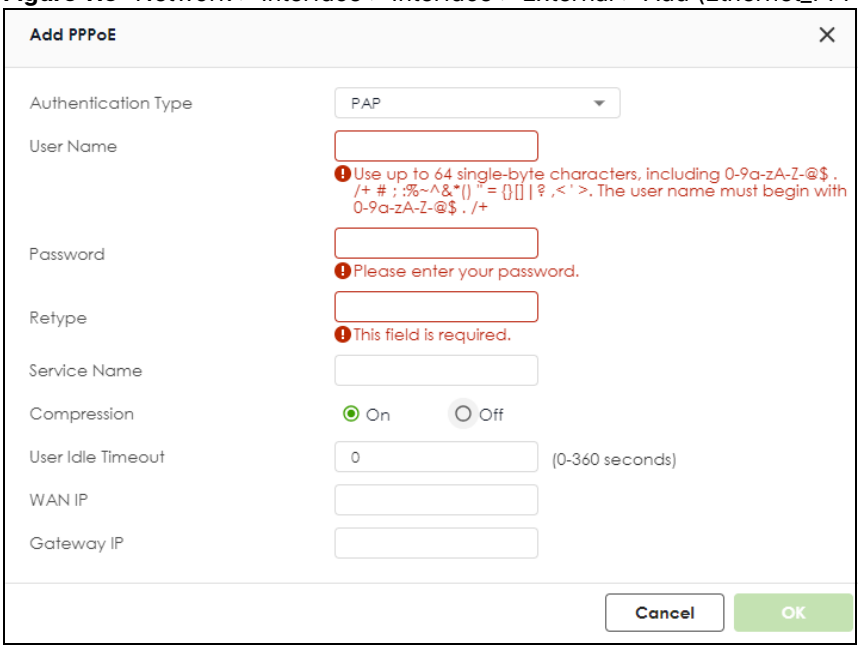
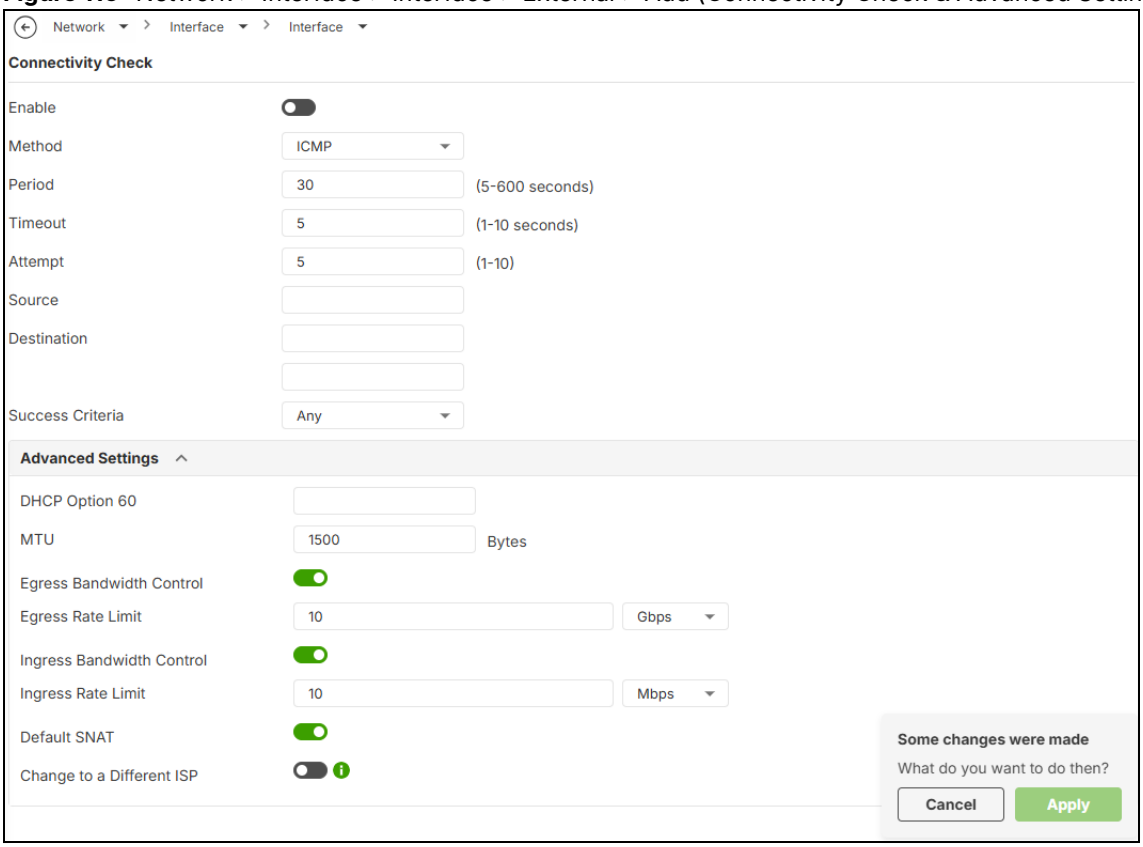


Figure 116 Network > Interface > Interface > External > Add (Connectivity Check & Advanced Settings)



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

Table 73 Network > Interface > Interface > External > Add/Edit

LABEL	DESCRIPTION
General Settings	
Enable Interface	Select this to enable this interface. Clear this to disable this interface.
Interface Properties	
Role	**External** is for connecting to an external network (like the Internet). The Zyxel Device automatically adds this interface to the default WAN trunk.
Interface Type	Select the type of interface you want to configure. • Select **Ethernet** to establish the foundation for defining other interfaces and network policies. • Select **VLAN** to receive and send tagged frames. The Zyxel Device automatically adds or removes the tags as needed. • Select **Bridge** to create a single network 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, such as Policy Control and IP Exception. You can also assign an IP address and subnet mask to the bridge. • Select **LAG** to combine multiple ports into a single logical interface to increase bandwidth and provide redundancy.
Name	Specify a name for the interface. It can use alphanumeric characters, hyphens, and underscores, and it can be up to 11 characters long.
Port	This is the name of the Ethernet interface's physical port.
Member	This field displays when you select the **VLAN** Interface Type. Select the Ethernet interface on which the VLAN interface runs.

Table 73 Network > Interface > Interface > External > Add/Edit

LABEL	DESCRIPTION
Zone	Select the zone to which this interface is to belong. You use zones to apply security settings such as security policy, IPS, remote management, anti-malware, and application patrol. Make sure to select the correct zone as otherwise traffic may be blocked by a security policy.
MAC Address	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. Enter a MAC address in the format "xx:xx:xx:xx:xx:xx" or "xx-xx-xx-xx-xx-xx". 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.
VLAN ID	This field displays when you select the **VLAN** Interface Type. Enter the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 - 4094. (0 and 4095 are reserved.)
Priority (802.1P)	This field displays when you select the **VLAN** Interface Type. Type a number between 0 and 7 to set the priority for the outgoing traffic from this interface. The bigger the number, the higher the priority.
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.
Address Assignment	These IP address fields configure an IPv4 IP address on the specified interface. 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.
Unassigned	Select this if you don't want to specify an IPv4 address for this interface.
Get Automatically (DHCP)	Select this to make the interface a DHCP client and automatically get the IP address, subnet mask, and gateway address from a DHCP server.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually. • **IP/Network Mask:** You must enter the primary IP address to identify the WAN interface's address for sending traffic with other network devices. • **Gateway IP:** Enter the IP address of the neighboring device through which this WAN connection will send traffic.
Secondary IP	This is available when you select **Use Fixed IP Address**. An interface can be bound to three additional public IP addresses. You can assign these IP addresses to different servers on the same interface, enabling the servers to receive traffic using different IP addresses and ports.
Add	Click this to bind up to three additional IP addresses to this interface.
Remove	To remove a secondary IP address, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Note: Ensure the secondary IP is address not being used by any service before removing it; otherwise, or the Zyxel Device might be unable to use the service.
IP/Netmask	Enter the secondary IP address and subnet mask to bind to this interface.
Members	This is available when you select **Bridge** or **LAG** interface type.
Add	Click this to add a new interface. You can add up to eight interfaces to per bridge interface.
Remove	To remove an interface from the bridge interface, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.

Table 73 Network > Interface > Interface > External > Add/Edit

LABEL	DESCRIPTION
Members	Select an Ethernet interface or VLAN interface to add it to 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. • Each bridge interface can only have one VLAN interface.
Zone	Select the zone to which this interface is to belong. You use zones to apply security settings such as security policy, IPS, remote management, anti-malware, and application patrol. Make sure to select the correct zone as otherwise traffic may be blocked by a security policy.
LAG Configuration	
Mode	Select a Mode for this LAG interface. Choices are as follows: • **static:** Traffic is distributed to multiple links. • **active-backup**: Only one member of the LAG interface is active. Another member becomes active only if the current active interface member fails. • **lacp (802.3ad)**: IEEE 802.3ad Dynamic link aggregation. Link Aggregation Control Protocol (LACP) negotiates automatic combining of links and balances the traffic load across the LAG link by sending LACP packets to the directly connected device that also implements LACP. The members must have the same speed and duplex settings.
Mii Monitoring Interval	Set the link check interval in milliseconds that the system polls the Media Independent Interface (MII) to get status. MII monitors the physical network connection, and this interval determines how often the Zyxel Device checks if a connection has failed or been reconnected, especially for LAG interfaces, ensuring that all aggregated links are functioning properly.
Transmit Hash Policy	This field is available when you select **static** or **lacp (802.3ad)** mode. This field sets the algorithm for member selection according to the selected TCP/IP layer. • **src-dst-ip-mac**: Uses source and destination IP addresses and MAC addresses for load balancing. • **src-dst-mac**: Uses only source and destination MAC addresses for load balancing.
Primary	In **active-backup** mode, select a member as the active member to transmit and receive network traffic. If the active member fails, the Zyxel Device will automatically switch to another member as the new active member to ensure continuous network connectivity.
PPPoE	Select this for a dial-up connection according to the information from your ISP. The following fields appear in the **Add PPPoE** screen.
Authentication Type	Select an authentication protocol for outgoing connection requests. • **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 give to you by your ISP. You can use up to 30 single-byte characters, including 0-9a-zA-Z@._-
Password	Enter the password associated with the user name. You can use 4 to 63 single-byte characters, including 0-9a-zA-Z'(){}<>^'+/:!*#@&=$\.~%,|;-"
Retype	Retype the password you entered in the **Password** field to confirm.
Service Name	Enter the service name from your service provider. PPPoE uses a service name to identify and reach the PPPoE server. You can use up to 30 single-byte characters, including 0-9a-zA-Z._-
Compression	Select **On** to turn on stac compression. Select **Off** to turn of stac compression. Stac compression is data compression technique capable of compressing data by a factor of about four.
User Idle Timeout	Enter the idle timeout in seconds that elapses before the router automatically disconnects from the PPPoE server.
WAN IP	Enter the IP address of the WAN interface through which this connection will send traffic.

Table 73 Network > Interface > Interface > External > Add/Edit

LABEL	DESCRIPTION
Gateway IP	Enter the IP address of the router through which this WAN connection will send traffic.
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	Select this to turn on the connection 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.
Period	Enter the number of seconds between connection check attempts (5-600 seconds).
Timeout	Enter the number of seconds to wait for a response before the attempt is a failure (1-10 seconds).
Attempt	Enter the number of consecutive failures before the Zyxel Device stops routing through the gateway.
Source	Enter the IPv4 address that test packets will be sent from. • Leave this field blank to send test packets from this external interface's IP address. • Enter an IPv4 address to send test packets from the specified gateway. If the Zyxel Device uses PPPoE for the WAN and your ISP gave you an IP address, enter that IP address to check the connectivity.
Destination	Enter one or two gateways using either FQDNs or IP addresses to receive test packets. For example, you can check if your ISP's gateway is reachable. You can enter an IPv4 address in one field and a FQDN in the other. For example, type "192.168.1.2" in the top filed and "www.zyxel.com" in the bottom field.
Success Criteria	This field applies when you specify two FQDNs or IP addresses for the connectivity check. • Select **Any** if you want the check to pass if at least one of the gateway with the specified IP address or FQDN responds. • Select **All** if you want the check to pass only if both gateways with the specified IP address or FQDN respond.
Advanced Settings	
DHCP Option 60	This field appears when **Role** is set to **External**. The setting you configure here will only work when **Address Assignment** is set to **Get Automatically**. 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. Type 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.
MTU	This is the Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device divides it into smaller fragments. Allowed values are 1280-1500. Usually, this value is 1500.
Egress Bandwidth Control	Click the switch to the right to limit outgoing traffic on the interface.

Table 73 Network > Interface > Interface > External > Add/Edit

LABEL	DESCRIPTION
Egress Rate Limit	Enter the maximum traffic the Zyxel Device can send through the interface to the network in Kbps (Kilobits per second), Mbps (Megabits per second), or Gbps (Gigabits per second). Allowed values range from 1 Kbps to 10 Gbps. If you also set an **Upload Limit** under **Network > BWM**, the Zyxel Device will apply the lower value as the limit.
Ingress Bandwidth Control	Click the switch to the right to limit incoming traffic on the interface.
Ingress Rate Limit	Enter the maximum traffic the Zyxel Device can receive from the network through the interface in Kbps (Kilobits per second), Mbps (Megabits per second), or Gbps (Gigabits per second). Allowed values range from 1 Kbps to 10 Gbps. If you also set a **Download Limit** under **Network > BWM**, the Zyxel Device will apply the lower value as the limit.
Default SNAT	This field appears when **Role** is set to **External**. 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.
Change to a Different ISP	If the Zyxel Device disconnects from the NCC (Nebula Control Center) after applying a WAN configuration change, it will revert to the last valid local WAN setting. Select this if you want to temporarily disable reverting to the last valid local WAN setting. Note: This field will be automatically disabled after rebooting the Zyxel Device so, you will need to enable this again if the Zyxel Device reboots.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

7.4 Internal Interface

Use this screen to configure the internal interface settings for connecting to a local network. Other corresponding configuration options are DHCP server and DHCP relay. The Zyxel Device automatically applies the default SNAT settings to traffic flowing from an internal interface to an external interface.

7.4.1 Internal Interface Add/Edit

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.

Figure 117 Network > Interface > Interface > Internal > Add/Edit ((General Settings/Ethernet IPv4))

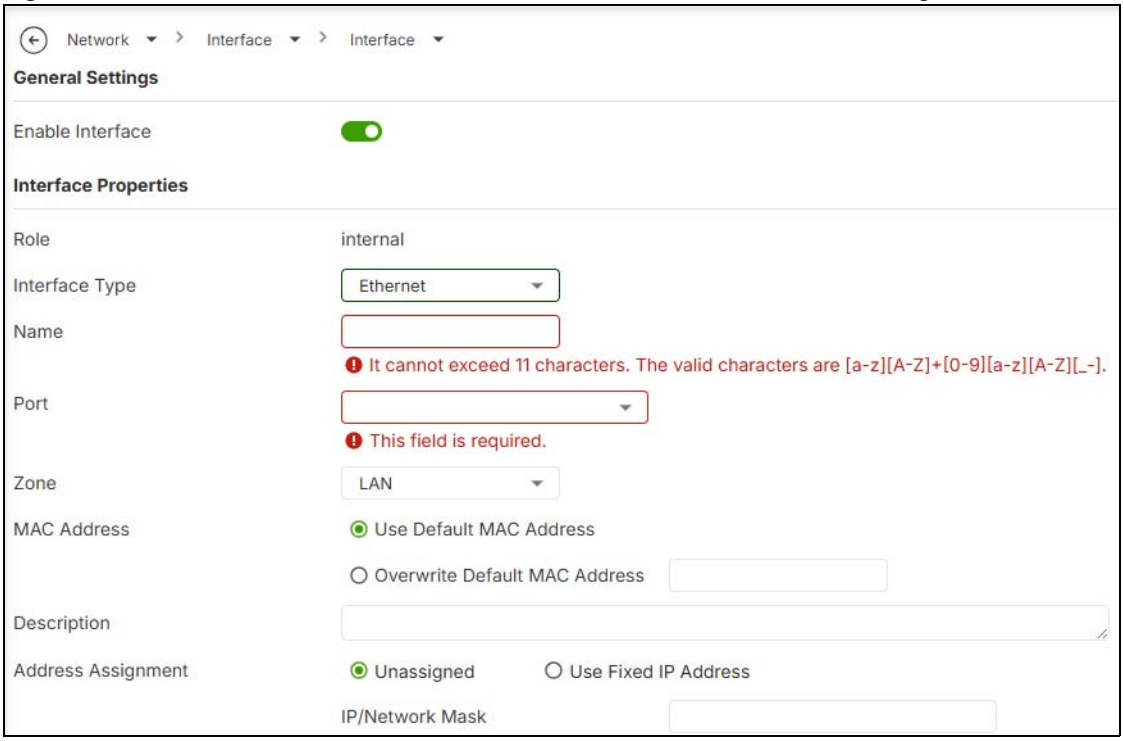


Figure 118 Network > Interface > Interface > Internal > Add/Edit (General Settings/VLAN IPv4))

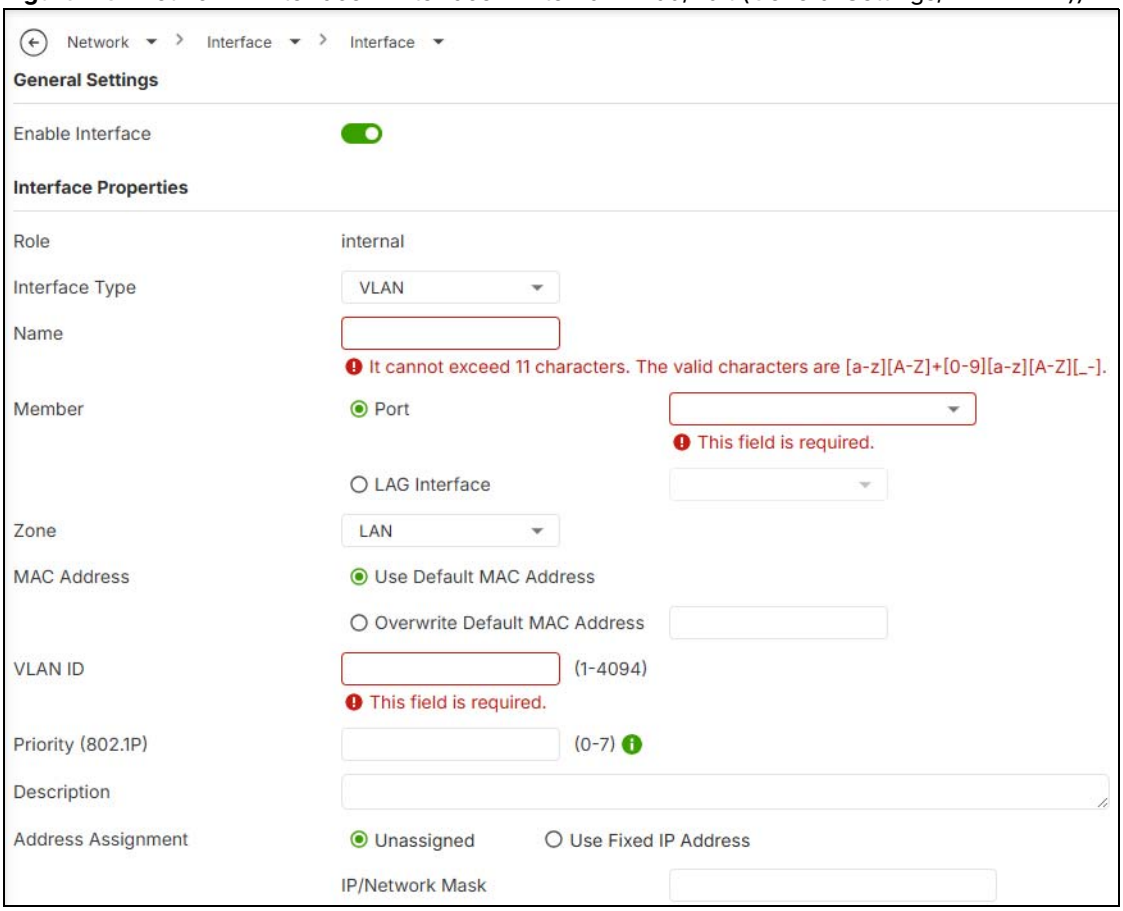


Figure 119 Network > Interface > Interface > Internal > Add/Edit ((General Settings/Bridge IPv4))

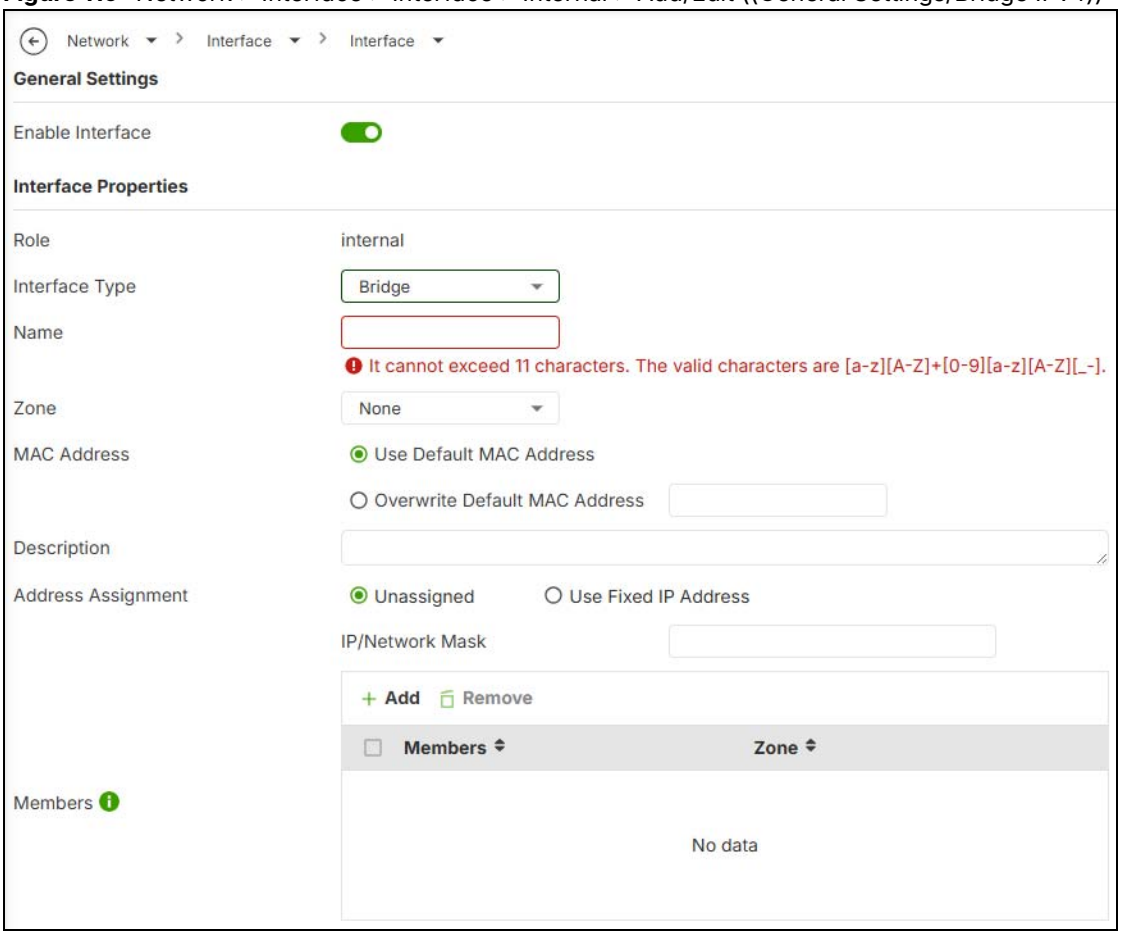


Figure 120 Network > Interface > Interface > Internal > Add/Edit ((General Settings/LAG IPv4))

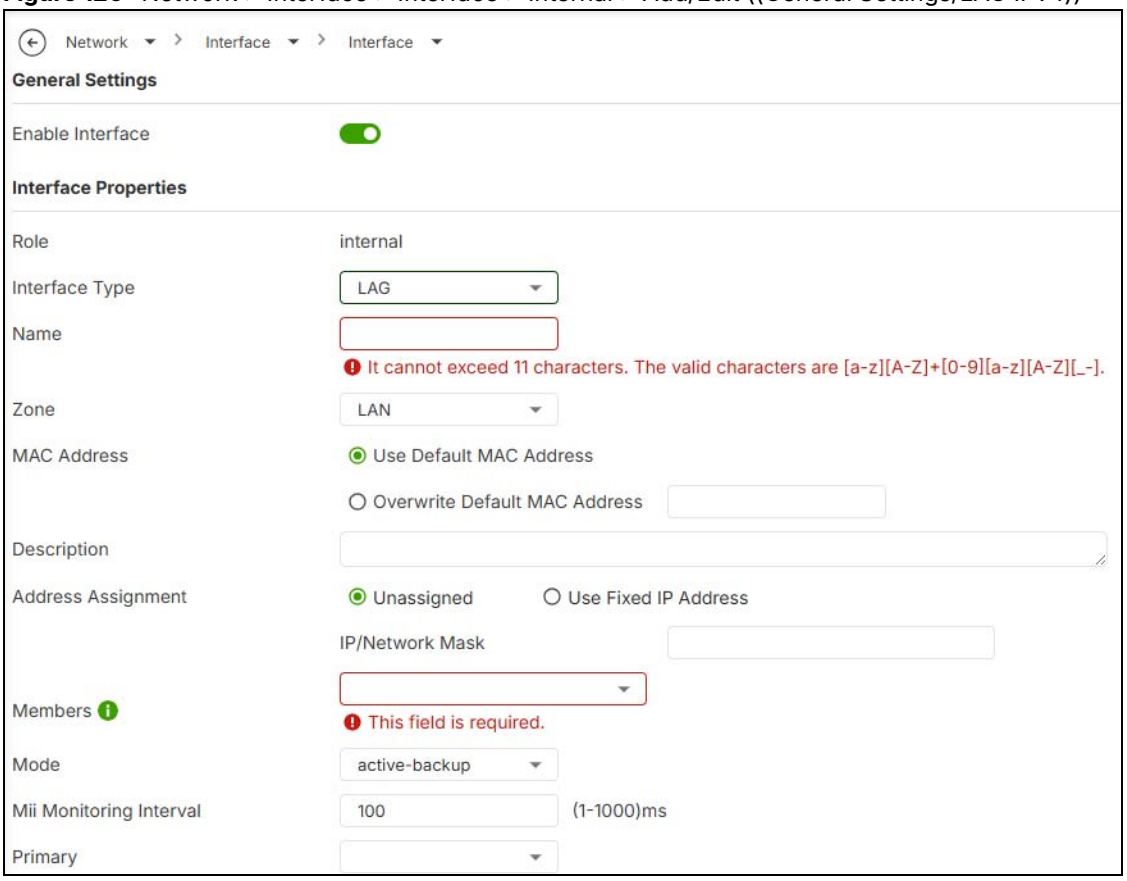
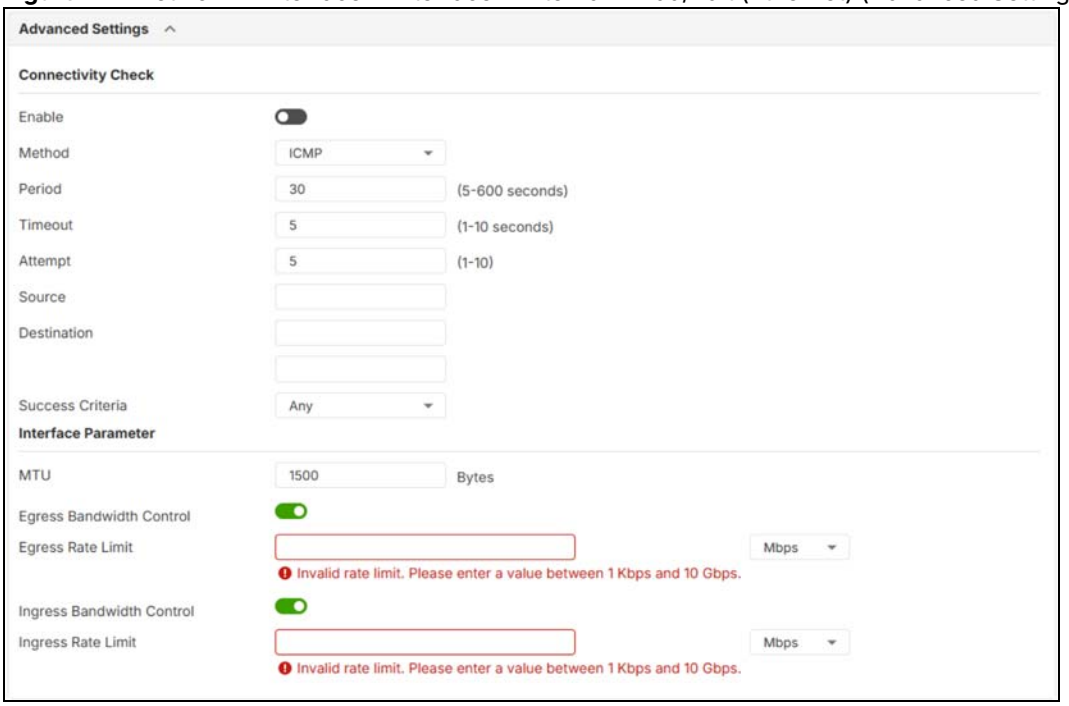


Figure 121 Network > Interface > Interface > Internal > Add/Edit (Ethernet) (Advanced Settings)



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

Table 74 Network > Interface > Interface > Internal > Add/Edit

LABEL	DESCRIPTION
General Settings	
Enable Interface	Select this to enable this interface. Clear this to disable this interface.
Interface Properties	
Role	**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; for example LAN to WAN traffic.
Interface Type	Select the type of interface you want to configure. • Select **Ethernet** to establish the foundation for defining other interfaces and network policies. • Select **VLAN** to receive and send tagged frames. The Zyxel Device automatically adds or removes the tags as needed. • Select **Bridge** to create a single network 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, such as Policy Control and IP Exception. You can also assign an IP address and subnet mask to the bridge. • Select **LAG** to combine multiple ports into a single logical interface to increase bandwidth and provide redundancy.
Name	Specify a name for the interface. It can use alphanumeric characters, hyphens, and underscores, and it can be up to 11 characters long.
Port	This is the name of the Ethernet interface's physical port.
Zone	Select the zone to which this interface is to belong. You use zones to apply security settings such as security policy, IPS, remote management, anti-malware, and application patrol. Make sure to select the correct zone as otherwise traffic may be blocked by a security policy.
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.
IPv4 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.
Unassigned	Select this if you don't want to specify an IP address for this interface.
Use Fixed IP Address	Select this if you want to specify the IP address and subnet mask manually.
Secondary IP	This is available when you select **Use Fixed IP Address**. An interface can be bound to three additional public IP addresses. You can assign these IP addresses to different servers on the same interface, enabling the servers to receive traffic using different IP addresses and ports.
Add	Click this to bind up to three additional IP addresses to this interface.
Remove	To remove a secondary IP address, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Note: Ensure the secondary IP is address not being used by any service before removing it; otherwise, or the Zyxel Device might be unable to use the service.
IP/Netmask	Enter the secondary IP address and subnet mask to bind to this interface.
Members	This is available when you select **Bridge** interface type.
Add	Click this to add a new interface. You can add up to eight interfaces to per bridge interface.
Remove	To remove an interface from the bridge interface, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.

Table 74 Network > Interface > Interface > Internal > Add/Edit (continued)

LABEL	DESCRIPTION
Members	Select an Ethernet interface or VLAN interface to add it to 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 • Each bridge interface can only have one VLAN interface.
Zone	Select the zone to which this interface is to belong. You use zones to apply security settings such as security policy, IPS, remote management, anti-malware, and application patrol. Make sure to select the correct zone as otherwise traffic may be blocked by a security policy.
LAG Configuration	
Mode	Select a Mode for this LAG interface. Choices are as follows: • **static:** Traffic is distributed to multiple links. • **active-backup**: Only one member of the LAG interface is active. Another member becomes active only if the current active interface member fails. • **lacp (802.3ad)**: IEEE 802.3ad Dynamic link aggregation. Link Aggregation Control Protocol (LACP) negotiates automatic combining of links and balances the traffic load across the LAG link by sending LACP packets to the directly connected device that also implements LACP. The members must have the same speed and duplex settings.
Mii Monitoring Interval	Set the link check interval in milliseconds that the system polls the Media Independent Interface (MII) to get status. MII monitors the physical network connection, and this interval determines how often the Zyxel Device checks if a connection has failed or been reconnected, especially for LAG interfaces, ensuring that all aggregated links are functioning properly.
Transmit Hash Policy	This field is available when you select **static** or **lacp (802.3ad)** mode. This field sets the algorithm for member selection according to the selected TCP/IP layer. • **src-dst-ip-mac**: Uses source and destination IP addresses and MAC addresses for load balancing. • **src-dst-mac**: Uses only source and destination MAC addresses for load balancing.
Primary	In **active-backup** mode, select a member as the active member to transmit and receive network traffic. If the active member fails, the Zyxel Device will automatically switch to another member as the new active member to ensure continuous network connectivity.
DHCP Server	This option appears when **Address Assignment** is **Use Fixed IP Address**.
Enable	Select this to enable the DHCP server on the Zyxel Device.
Mode	Select what type of DHCP service the Zyxel Device provides to the network. Choices are: • **DHCP** - 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. • **Relay** - the Zyxel Device routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. You can have at most four DHCP relay servers at the same time.
Start IP	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.
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 **Start IP** 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 **Start IP** 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 74 Network > Interface > Interface > Internal > Add/Edit (continued)

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. • **Custom Defined** - enter a static IP address. • **ZyWALL** - 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	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Default Router	If you set this interface to **DHCP Server**, you can select to use either the interface's IP address or another IP address as the default router. This default router will become the DHCP clients' default gateway. To use another IP address as the default router, select **Custom Defined** and enter the IP address.
Lease Time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again.
Static DHCP Table	Click this link to go to **Network Status > DHCP Table** to see the current DHCP-assigned IP addresses on an interface.
DHCP 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 7.5 on page 158.
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.
PXE Server	PXE (Preboot eXecution Environment) allows a client computer to use the network to boot up and install an operating system via 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. Type the exact file name of the boot loader software file, including filename extension, that is on the PXE server. If the wrong filename is typed, then the client computers cannot boot.
Relay Server 1	
Address	Enter the IP address of a DHCP server for the network.
Upstream Interface	This field is optional. Select up to two interface(s)to use for the Zyxel Device to forward/ receive DHCP packets to/from the DHCP server.
Relay Server 2	
Address	This field is optional. Enter the IP address of another DHCP server for the network.
Upstream Interface	This field is optional. Select up to two interface(s)to use for the Zyxel Device to forward/ receive DHCP packets to/from the DHCP server.
Advanced Settings	
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	Select this to turn on the connection check.

Table 74 Network > Interface > Interface > Internal > Add/Edit (continued)

LABEL	DESCRIPTION
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.
Period	Enter the number of seconds between connection check attempts (5-600 seconds).
Timeout	Enter the number of seconds to wait for a response before the attempt is a failure (1-10 seconds).
Attempt	Enter the number of consecutive failures before the Zyxel Device stops routing through the gateway.
Source	Enter the IPv4 address that test packets will be sent from. • Leave this field blank to send test packets from this internal interface's primary IP address, as configured above in **Address Assignment**. • Enter an IPv4 address to send test packets from the specified gateway. For example, you can enter a secondary IP address of this internal interface to check the connectivity.
Destination	Enter one or two gateways using either FQDNs or IP addresses to receive test packets. For example, you can check if a device (for example, a router) or a server (for example, a DNS server) is reachable. You can enter an IPv4 address in one field and a FQDN in the other. For example, type "192.168.1.2" in the first field and "www.zyxel.com" in the second field.
Success Criteria	This field applies when you specify two FQDNs or IP addresses for the connectivity check. • Select **Any** if you want the check to pass if at least one of the gateway with the specified IP address or FQDN responds. • Select **All** if you want the check to pass only if both gateways with the specified IP address or FQDN respond.
Interface Parameters	
MTU	This is the Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device divides it into smaller fragments. Allowed values are 1280-1500. Usually, this value is 1500.
Egress Bandwidth Control	Click the switch to the right to limit outgoing traffic on the interface.
Egress Rate Limit	Enter the maximum traffic the Zyxel Device can send through the interface to the network in Kbps (Kilobits per second), Mbps (Megabits per second), or Gbps (Gigabits per second). Allowed values range from 1 Kbps to 10 Gbps. If you also set an **Upload Limit** under **Interfaces > BWM**, the Zyxel Device will apply the lower value as the limit.
Ingress Bandwidth Control	Click the switch to the right to limit incoming traffic on the interface.
Ingress Rate Limit	Enter the maximum traffic the Zyxel Device can receive from the network through the interface in Kbps (Kilobits per second), Mbps (Megabits per second), or Gbps (Gigabits per second). Allowed values range from 1 Kbps to 10 Gbps. If you also set a **Download Limit** under **Interfaces > BWM**, the Zyxel Device will apply the lower value as the limit.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

7.5 General Interface

This section introduces general interfaces and then explains the screen for general interfaces.

Use a general interface to connect to either a local network or an external network. If you prefer not to use the automatic settings applied to **Internal** or **External** interfaces, you can create a **General** interface to specify routing policy, SNAT, and security rules.

Figure 122 Network > Interface > Interface > General > Add /Edit (General Settings)

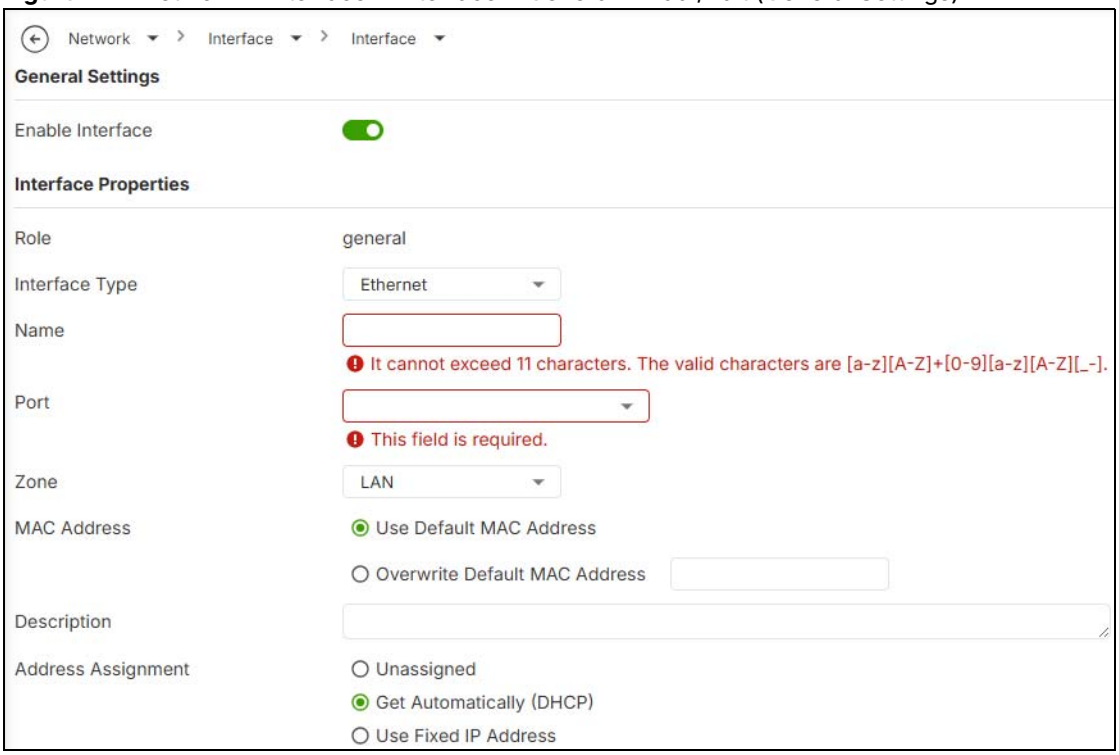
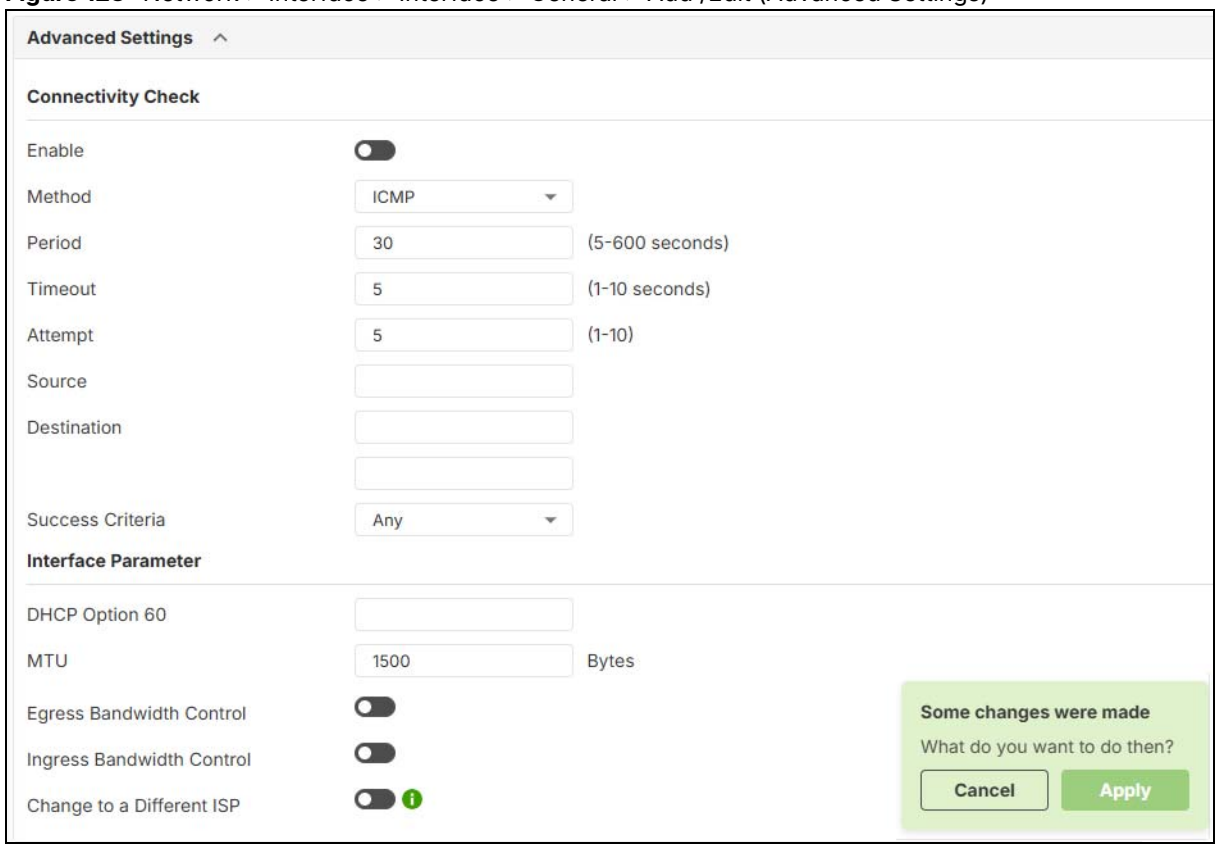


Figure 123 Network > Interface > Interface > General > Add /Edit (Advanced Settings)



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

Table 75 Network > Interface > Interface > General > Add/Edit

LABEL	DESCRIPTION
General Settings	
Enable Interface	Select this to enable this interface. Clear this to disable this interface.
Interface Properties	
Role	**General** is for connecting to either an external network or a local network. 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 Type	Select the type of interface you want to configure. • Select **Ethernet** to establish the foundation for defining other interfaces and network policies. • Select **VLAN** to create an interface over an Ethernet interface that can receive and send tagged frames. The Zyxel Device automatically adds or removes the tags as needed. • Select **Bridge** to create a single network 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, such as Policy Control and IP Exception. You can also assign an IP address and subnet mask to the bridge. • Select **LAG** to combine multiple ports into a single logical interface to increase bandwidth and provide redundancy.
Name	Specify a name for the interface. It can use alphanumeric characters, hyphens, and underscores, and it can be up to 11 characters long.
Port	This is the name of the Ethernet interface's physical port.

Table 75 Network > Interface > Interface > General > Add/Edit

LABEL	DESCRIPTION
Zone	Select the zone to which this interface is to belong. You use zones to apply security settings such as security policy, IPS, remote management, anti-malware, and application patrol. Make sure to select the correct zone as otherwise traffic may be blocked by a security policy. You can create a zone object in the **Object** > **Zone** screen.
MAC Address	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. Enter a MAC address in the format "xx:xx:xx:xx:xx:xx" or "xx-xx-xx-xx-xx-xx". 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.
VLAN ID	This field displays when you select the **VLAN Interface Type**. Enter the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 - 4094. (0 and 4095 are reserved.)
Priority (802.1P)	This field displays when you select the **VLAN Interface Type**. Type a number between 0 and 7 to set the priority for the outgoing traffic from this interface. The bigger the number, the higher the priority.
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.
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.
Unassigned	Select this if you don't want to specify an IP address for this interface.
Get Automatically (DHCP)	Select this to make the interface a DHCP client and automatically get the IP address, subnet mask, and gateway address from a DHCP server. Note: **DHCP Server** is disabled if you select this option. An interface cannot act as both a DHCP client and a DHCP server at the same time.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP/Network Mask	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address 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.for this interface.
Gateway IP	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. Note: If you do not enter a gateway IP address here, you must go to the **Network** > **Routing** screen to create a routing policy so the Zyxel Device knows where to route the packets.
Secondary IP	This is available when you select **Use Fixed IP Address**. An interface can be bound to three additional public IP addresses. You can assign these IP addresses to different servers on the same interface, enabling the servers to receive traffic using different IP addresses and ports.
Add	Click this to bind up to three additional IP addresses to this interface.

Table 75 Network > Interface > Interface > General > Add/Edit

LABEL	DESCRIPTION
Remove	To remove a secondary IP address, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Note: Ensure the secondary IP is address not being used by any service before removing it; otherwise, or the Zyxel Device might be unable to use the service.
IP/Netmask	Enter the secondary IP address and subnet mask to bind to this interface.
Members	This is available when you select **Bridge** interface type.
Add	Click this to add a new interface. You can add up to eight interfaces to per bridge interface.
Remove	To remove an interface from the bridge interface, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Members	Select an Ethernet interface or VLAN interface to add it to 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 • Each bridge interface can only have one VLAN interface.
Zone	Select the zone to which this interface is to belong. You use zones to apply security settings such as security policy, IPS, remote management, anti-malware, and application patrol. Make sure to select the correct zone as otherwise traffic may be blocked by a security policy.
LAG Configuration	
Mode	Select a Mode for this LAG interface. Choices are as follows: • **static:** Traffic is distributed to multiple links. • **active-backup**: Only one member of the LAG interface is active. Another member becomes active only if the current active interface member fails. • **lacp (802.3ad)**: IEEE 802.3ad Dynamic link aggregation. Link Aggregation Control Protocol (LACP) negotiates automatic combining of links and balances the traffic load across the LAG link by sending LACP packets to the directly connected device that also implements LACP. The members must have the same speed and duplex settings.
Mii Monitoring Interval	Set the link check interval in milliseconds that the system polls the Media Independent Interface (MII) to get status. MII monitors the physical network connection, and this interval determines how often the Zyxel Device checks if a connection has failed or been reconnected, especially for LAG interfaces, ensuring that all aggregated links are functioning properly.
Transmit Hash Policy	This field is available when you select **static** or **lacp (802.3ad)** mode. This field sets the algorithm for member selection according to the selected TCP/IP layer. • **src-dst-ip-mac**: Uses source and destination IP addresses and MAC addresses for load balancing. • **src-dst-mac**: Uses only source and destination MAC addresses for load balancing.
Primary	In **active-backup** mode, select a member as the active member to transmit and receive network traffic. If the active member fails, the Zyxel Device will automatically switch to another member as the new active member to ensure continuous network connectivity.
DHCP Server	This option appears when **Address Assignment** is **Use Fixed IP Address**.
Enable	Select this to enable the DHCP server on the Zyxel Device.
Mode	Select what type of DHCP service the Zyxel Device provides to the network. Choices are: • **DHCP** - 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. • **Relay** - the Zyxel Device routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. You can have at most four DHCP relay servers at the same time.

Table 75 Network > Interface > Interface > General > Add/Edit

LABEL	DESCRIPTION
Start IP	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.
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 **Start IP** 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 **Start IP** 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. • **ZyWALL** - 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	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Default Router	If you set this interface to **DHCP Server**, you can select to use either the interface's IP address or another IP address as the default router. This default router will become the DHCP clients' default gateway. To use another IP address as the default router, select **Custom Defined** and enter the IP address.
Lease Time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again.
DHCP 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 7.5 on page 158.
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.
PXE Server	PXE (Preboot eXecution Environment) allows a client computer to use the network to boot up and install an operating system via 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. Type the exact file name of the boot loader software file, including filename extension, that is on the PXE server. If the wrong filename is typed, then the client computers cannot boot.
Relay Server 1	
Address	Enter the IP address of a DHCP server for the network.
Upstream Interface	This field is optional. Select up to two interface(s)to use for the Zyxel Device to forward/ receive DHCP packets to/from the DHCP server.
Relay Server 2	

Table 75 Network > Interface > Interface > General > Add/Edit

LABEL	DESCRIPTION
Address	This field is optional. Enter the IP address of another DHCP server for the network.
Upstream Interface	This field is optional. Select up to two interface(s)to use for the Zyxel Device to forward/ receive DHCP packets to/from the DHCP server.
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	Select this to turn on the connection 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.
Period	Enter the number of seconds between connection check attempts (5-600 seconds).
Timeout	Enter the number of seconds to wait for a response before the attempt is a failure (1-10 seconds).
Attempt	Enter the number of consecutive failures before the Zyxel Device stops routing through the gateway.
Source	Enter the IPv4 address that test packets will be sent from. • Leave this field blank to send test packets from this interface's primary IP address, as configured above in **Address Assignment**. • Enter an IPv4 address to send test packets from the specified gateway. For example, you can enter a secondary IP address of this interface to check the connectivity.
Destination	Enter one or two gateways using either FQDNs or IP addresses to receive test packets. For example, you can check Internet connectivity by entering 8.8.8.8 to see if Google DNS is reachable. You can enter an IPv4 address in one field and a FQDN in the other. For example, type "192.168.1.2" in the top filed and "www.zyxel.com" in the bottom field.
Success Criteria	This field applies when you specify two FQDNs or IP addresses for the connectivity check. • Select **Any** if you want the check to pass if at least one of the gateway with the specified IP address or FQDN responds. • Select **All** if you want the check to pass only if both gateways with the specified IP address or FQDN respond.
Interface Parameter	
MTU	This is the Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device divides it into smaller fragments. Allowed values are 1280-1500. Usually, this value is 1500.
Egress Bandwidth Control	Click the switch to the right to limit outgoing traffic on the interface.
Egress Rate Limit	Enter the maximum traffic the Zyxel Device can send through the interface to the network in Kbps (Kilobits per second), Mbps (Megabits per second), or Gbps (Gigabits per second). Allowed values range from 1 Kbps to 10 Gbps. If you also set an **Upload Limit** under **Interfaces > BWM**, the Zyxel Device will apply the lower value as the limit.
Ingress Bandwidth Control	Click the switch to the right to limit incoming traffic on the interface.

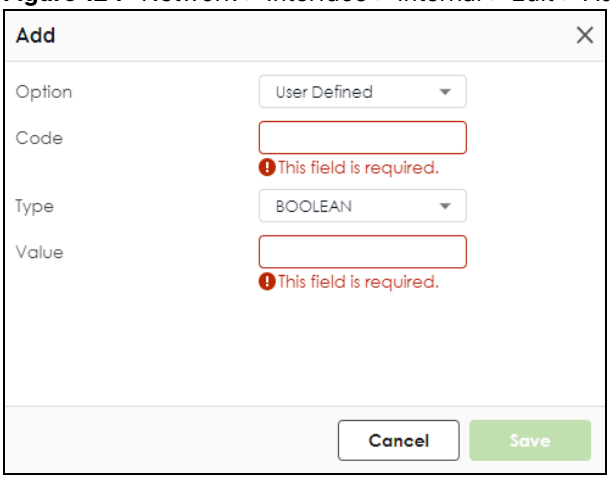
Table 75 Network > Interface > Interface > General > Add/Edit

LABEL	DESCRIPTION
Ingress Rate Limit	Enter the maximum traffic the Zyxel Device can receive from the network through the interface in Kbps (Kilobits per second), Mbps (Megabits per second), or Gbps (Gigabits per second). Allowed values range from 1 Kbps to 10 Gbps. If you also set a **Download Limit** under **Interfaces > BWM**, the Zyxel Device will apply the lower value as the limit.
Change to a Different ISP	If the Zyxel Device disconnects from the Nebula Control Center, it will revert to the previous configuration. If you select this option, the Zyxel Device will not revert to the previous configuration when it loses connection to the NCC due to an ISP change.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

7.5.1 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 **Network > Interface > Internal/General > Edit**, select **DHCP Mode** in the **DHCP Server** section, and then click **Add** or **Edit** in the **DHCP Extended Options** table.

Figure 124 Network > Interface > Internal > Edit > Add/Edit Extended Options



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

Table 76 Network > Interface > Internal > Edit > Add/Edit Extended Options

LABEL	DESCRIPTION
Option	This field displays the name of the selected DHCP option. Select which DHCP option that you want to add in the DHCP packets sent through the interface.
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**.
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.

Table 76 Network > Interface > Internal > Edit > Add/Edit Extended Options (continued)

LABEL	DESCRIPTION
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.
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 77 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.
Domain Name	15	This option specifies the domain name that the client should use when resolving hostnames through the Domain Name System.
Interface MTU	26	This option specifies the MTU (Maximum Transmission Unit) to use on this interface, with an available range of 68 to 65535 bytes for IPv4 packets.
NTP Server	42	This option specifies a list of the NTP servers available to the client by IP address.
Netbios Scope	47	This option specifies the NetBIOS over TCP/IP scope parameter for the client.
DHCP Server Identifier	54	This option specifies the IP address of the DHCP server.
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.

Table 77 DHCP Extended Options (continued)

OPTION NAME	CODE	DESCRIPTION
CAPWAP AC	138	CAPWAP Access Controller addresses option The Control And Provisioning of Wireless Access Points Protocol allows a Wireless Termination Point (WTP) to use DHCP to discover the Access Controllers to which it is to connect. This option carries a list of IPv4 addresses indicating one or more CAPWAP ACs available to the WTP.
TFTP Server	150	The option contains one or more IPv4 addresses that the client may use. The current use of this option is for downloading configuration from a VoIP server via TFTP; however, the option may be used for purposes other than contacting a VoIP configuration server.

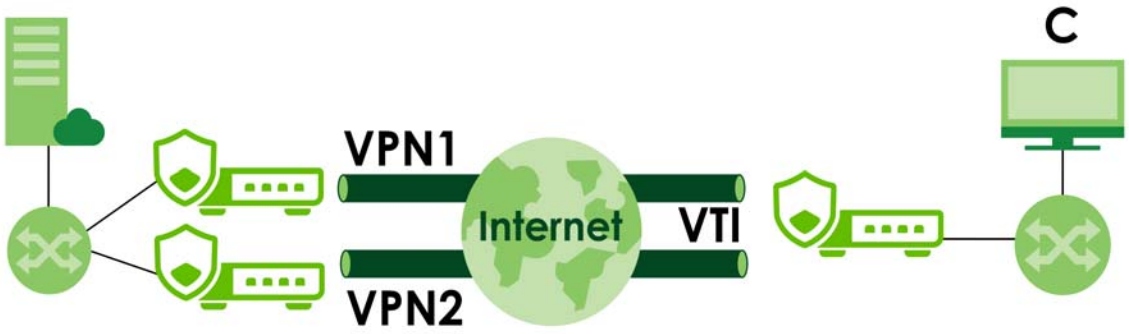
7.6 VTI Interface

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 125 VTI and Trunk for VPN Load Balancing



7.6.1 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.

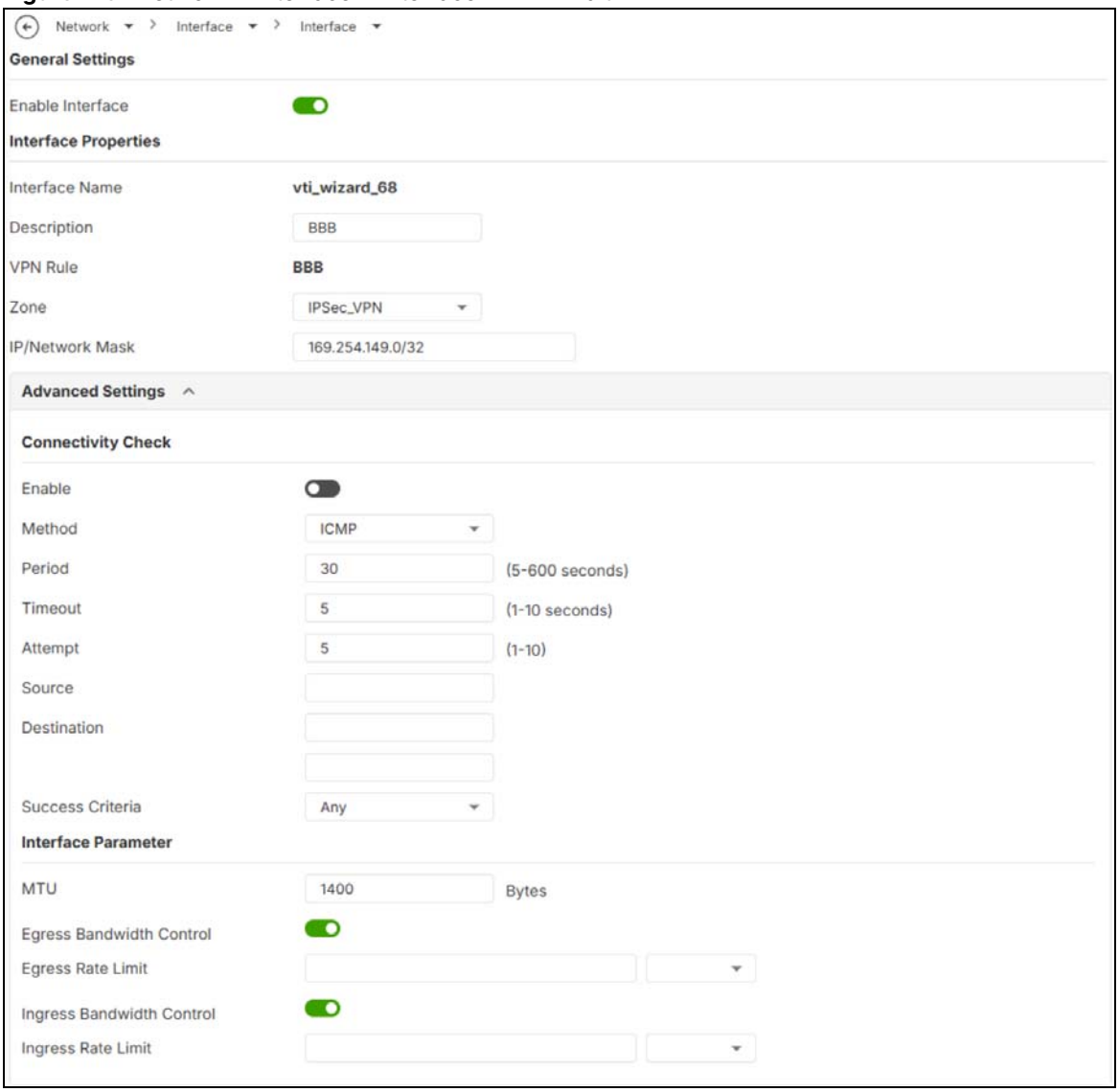
7.6.2 VTI Edit

This screen lets you configure IP address assignment and interface parameters for VTI.

Note: You should have created a route-based VPN tunnel for a VPN Tunnel Interface scenario first.

To access this screen, click the **Network > Interface > Interface > VTI > Edit.** The following screen appears.

Figure 126 Network > Interface > Interface > VTI > Edit



Each field is described in the table below.

Table 78 Network > Interface > Interface > VTI > Edit

LABEL	DESCRIPTION
General Settings	
Enable Interface	Slide the switch to the right to enable VTI.

Table 78 Network > Interface > Interface > VTI > Edit (continued)

LABEL	DESCRIPTION
Interface Properties	
Interface Name	This field displays the name of the VPN tunnel interface. This field is read-only.
VPN Rule	This field displays the scenario rule the VPN tunnel interface is using.
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.
IP Address	Enter the IP address for this interface.
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	Select this to turn on the connection 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.
Period	Enter the number of seconds between connection check attempts.
Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Attempt	Enter the number of consecutive failures before the Zyxel Device stops routing through the gateway.
Source	Enter the IPv4 address that test packets will be sent from. • Leave this field blank to send test packets from this VPN tunnel interface's IP address. • Enter an IPv4 address to send test packets from the specified gateway.
Destination	Enter one or two gateways using either FQDNs or IP addresses to receive test packets. For example, you can check if a remote router at another site connected through the VPN is reachable by this interface. You can enter an IPv4 address in one field and a domain name in the other. For example, type "192.168.1.2" in the top filed and "www.zyxel.com" in the bottom field.
Success Criteria	This field applies when you specify two FQDNs or IP addresses for the connectivity check. • Select **Any** if you want the check to pass if at least one of the gateway with the specified IP address or FQDN responds. • Select **All** if you want the check to pass only if both gateways with the specified IP address or FQDN respond.
MTU	This is the Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device divides it into smaller fragments. Allowed values are 1280-1500.
Egress Bandwidth Control	Click the switch to the right to limit outgoing traffic on the interface.
Egress Rate Limit	Enter the maximum traffic the Zyxel Device can send through the interface to the network in Kbps (Kilobits per second), Mbps (Megabits per second), or Gbps (Gigabits per second). Allowed values range from 1 Kbps to 10 Gbps. If you also set an **Upload Limit** under **Interfaces > BWM**, the Zyxel Device will apply the lower value as the limit.
Ingress Bandwidth Control	Click the switch to the right to limit incoming traffic on the interface.

Table 78 Network > Interface > Interface > VTI > Edit (continued)

LABEL	DESCRIPTION
Ingress Rate Limit	Enter the maximum traffic the Zyxel Device can receive from the network through the interface in Kbps (Kilobits per second), Mbps (Megabits per second), or Gbps (Gigabits per second). Allowed values range from 1 Kbps to 10 Gbps. If you also set a **Download Limit** under **Interfaces > BWM**, the Zyxel Device will apply the lower value as the limit.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

7.7 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 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.

Throughput is the moving average of traffic passing through the Zyxel Device in the last 10 seconds updated every 1 second.

Load Balancing Algorithms

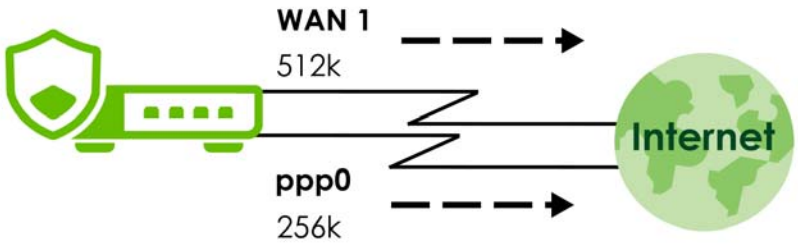
The following sections describe the load balancing algorithms the Zyxel Device can use to decide which interface the traffic (from the LAN) should use for a session. The available bandwidth you configure on the Zyxel Device refers to the actual bandwidth provided by the ISP and the measured bandwidth 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 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 127 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 79 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

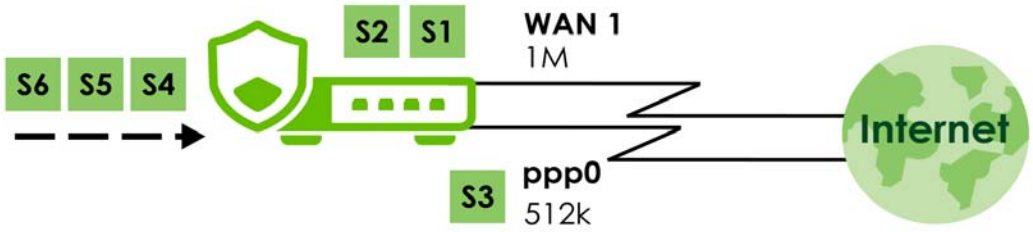
Weighted Round Robin

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 128 Weighted Round Robin Algorithm Example



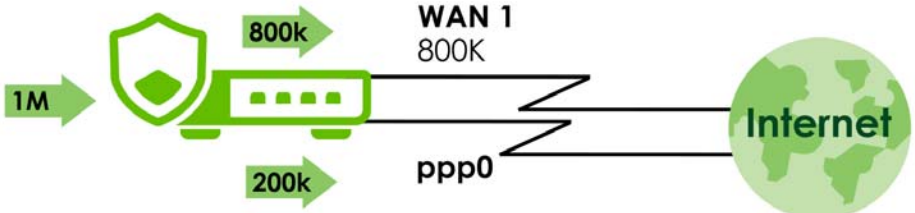
Spillover

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

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

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

Figure 129 Spillover Algorithm Example



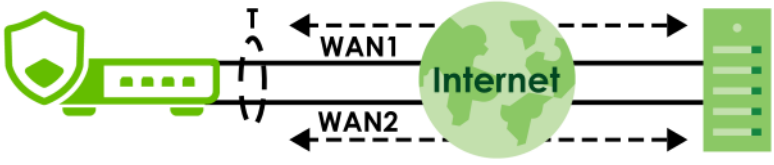
- Use the **Trunk** summary screen (Section 7.8 on page 173) to view the list of configured trunks and which load balancing algorithm each trunk uses.
- Use the **Add Trunk** screen (Section 7.8.1 on page 174) to configure the member interfaces for a trunk and the load balancing algorithm the trunk uses.
- Use the **Add System Default** screen (Section 7.8.2 on page 175) to configure the load balancing algorithm for the system default trunk.

Link Sticking

Link sticking ensures that once a source-destination link uses a WAN interface, all sessions between the source and the destination will continue to use the same WAN interface for five minutes. New sessions started within this period will also use the same WAN interface. This prevents load balancing from redirecting the link to other WAN interfaces. After five minutes, new sessions may use a different WAN interface according to the configured load balancing rules.

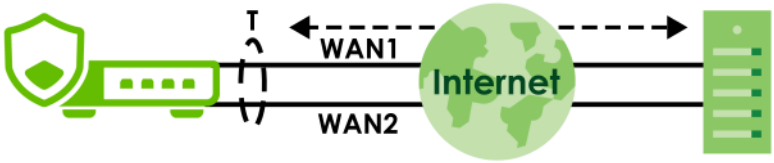
- **Without Link Sticking**: Link traffic may be sent through either **WAN1** or **WAN2** in the trunk (**T**).

Figure 130 Without Link Sticking



- **With Link Sticking**: Link traffic that starts on **WAN1** in the trunk (**T**) continues to use **WAN1**.

Figure 131 With Link Sticking



When multiple WAN interfaces are available, the Zyxel Device distributes traffic for load balancing. However, some servers or applications (such as online banking, VPNs, or authenticated logins) require the traffic to come from the same WAN IP address. Link sticking ensures the source-destination link remains on the same WAN interface to prevent these applications from detecting a different IP address and rejecting access. See the example below:

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 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.

4 If link sticking is enabled, 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.

Note: If traffic matches a configured **Static Route** or **Policy Route** (see Section 8.1 on page 179 for details), the routes have priority over link sticking.

Note: You can configure Link Sticking only through CLI commands. See the Command Reference Guide for more information.

7.7.1 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.

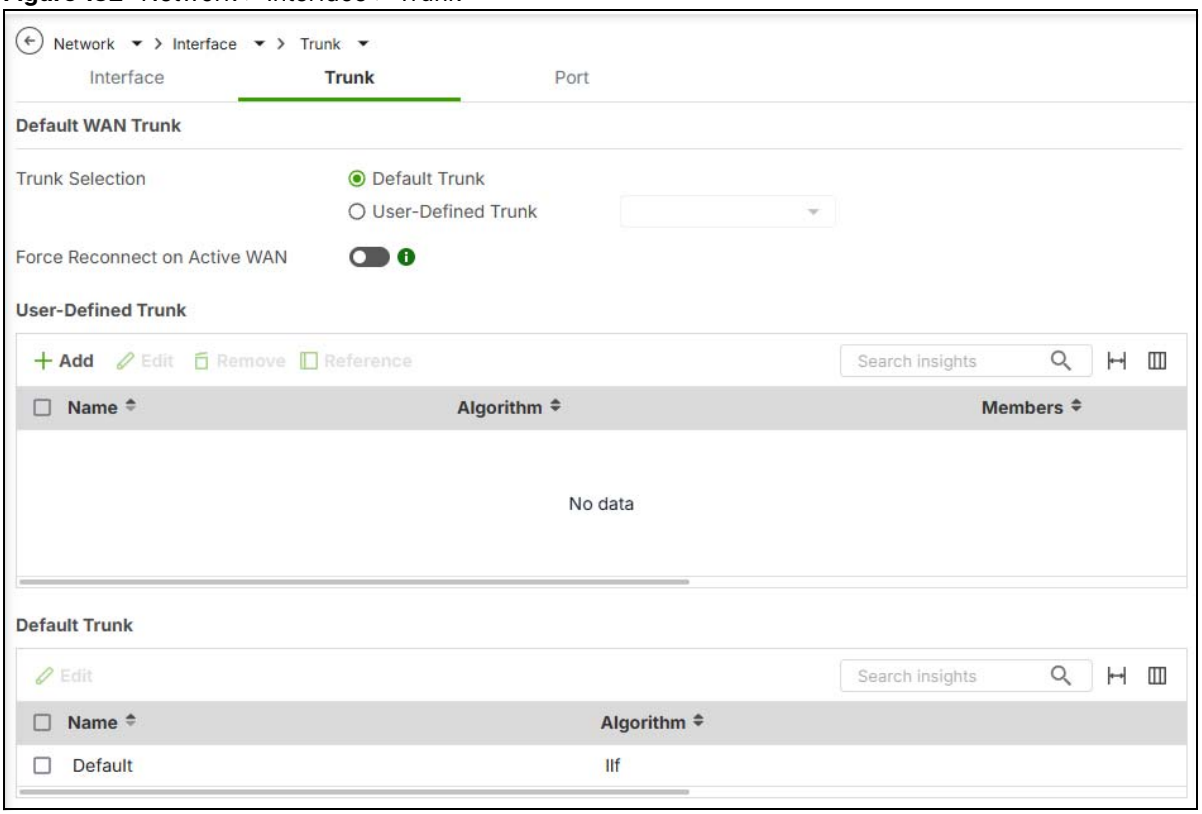
You can also use trunks with policy routing to send specific traffic types through the best WAN interface for that type of traffic.

- 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.

7.8 The Trunk Summary Screen

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

Figure 132 Network > Interface > Trunk



The following table describes the items in this screen.

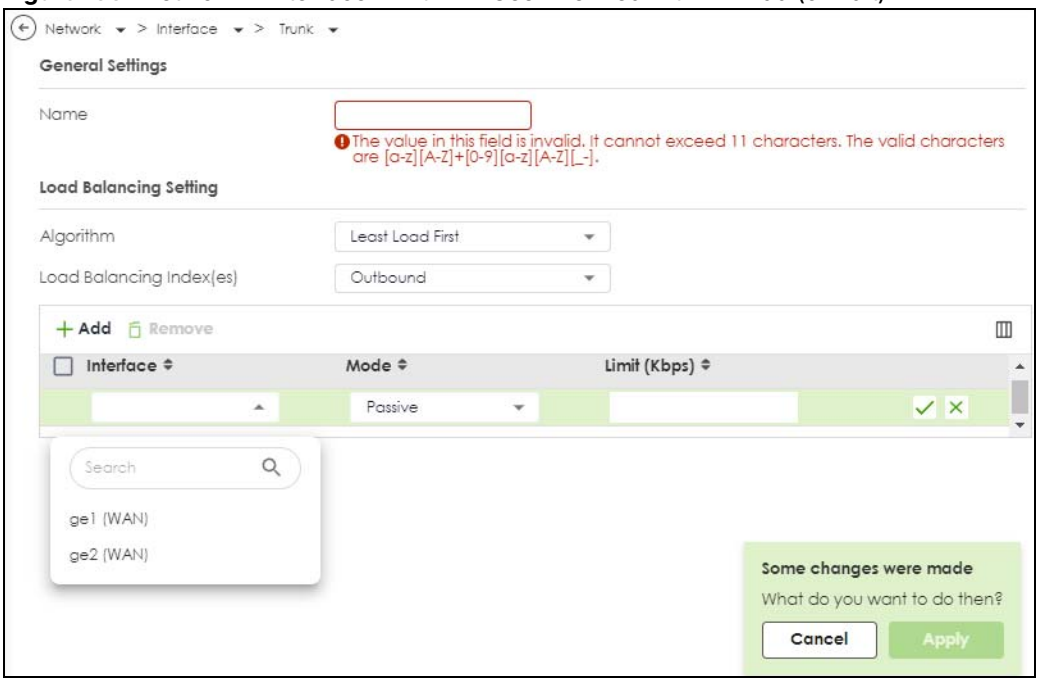
Table 80 Network > Interface > Trunk

LABEL	DESCRIPTION
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.
Force Reconnect on Active WAN	The passive interface is used if the active interface fails. If the active interface comes back up again, enable this if you want the Zyxel Device to end all connections on the passive interface first before the trunk goes back to using the active interface.
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.
Reference	This field displays the objects this entry uses.
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.
Members	This field displays the interfaces that belong to the trunk.
Reference	This field displays which settings use the entry.

7.8.1 Configuring a User-Defined Trunk

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

Figure 133 Network > Interface > Trunk > User-Defined Trunk > Add (or Edit)



Each field is described in the table below.

Table 81 Network > Interface > Trunk > Add/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. The value in this field cannot exceed 11 characters. The valid characters are [a-z][A-Z][_-].
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.
Add	Click this to create a WAN trunk entry.
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.
Name	Select an interface name from the drop-down list box.

Table 81 Network > Interface > Trunk > Add/Edit (continued)

LABEL	DESCRIPTION
Mode	Click this table cell. • 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.
Parameter	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.
Apply	Click this button to save your changes to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

7.8.2 Configuring the System Default Trunk

Go to **Network** > **Interface** > **Trunk** > **Default Trunk**, 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 new session is allocated to each member interface equally and is not allowed to be changed for the default trunk.

Figure 134 Network > Interface > Trunk > Default Trunk > Edit



Each field is described in the table below.

Table 82 Network > Interface > Trunk > Default Trunk > Edit

LABEL	DESCRIPTION
Name	This field displays the name of the selected system default trunk.
Load Balancing Setting	This field displays the load balancing method use for the default trunk. **Weighted Round Robin** (**wrr**) balances 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.
	The table lists the trunk's member interfaces. This table is read-only.

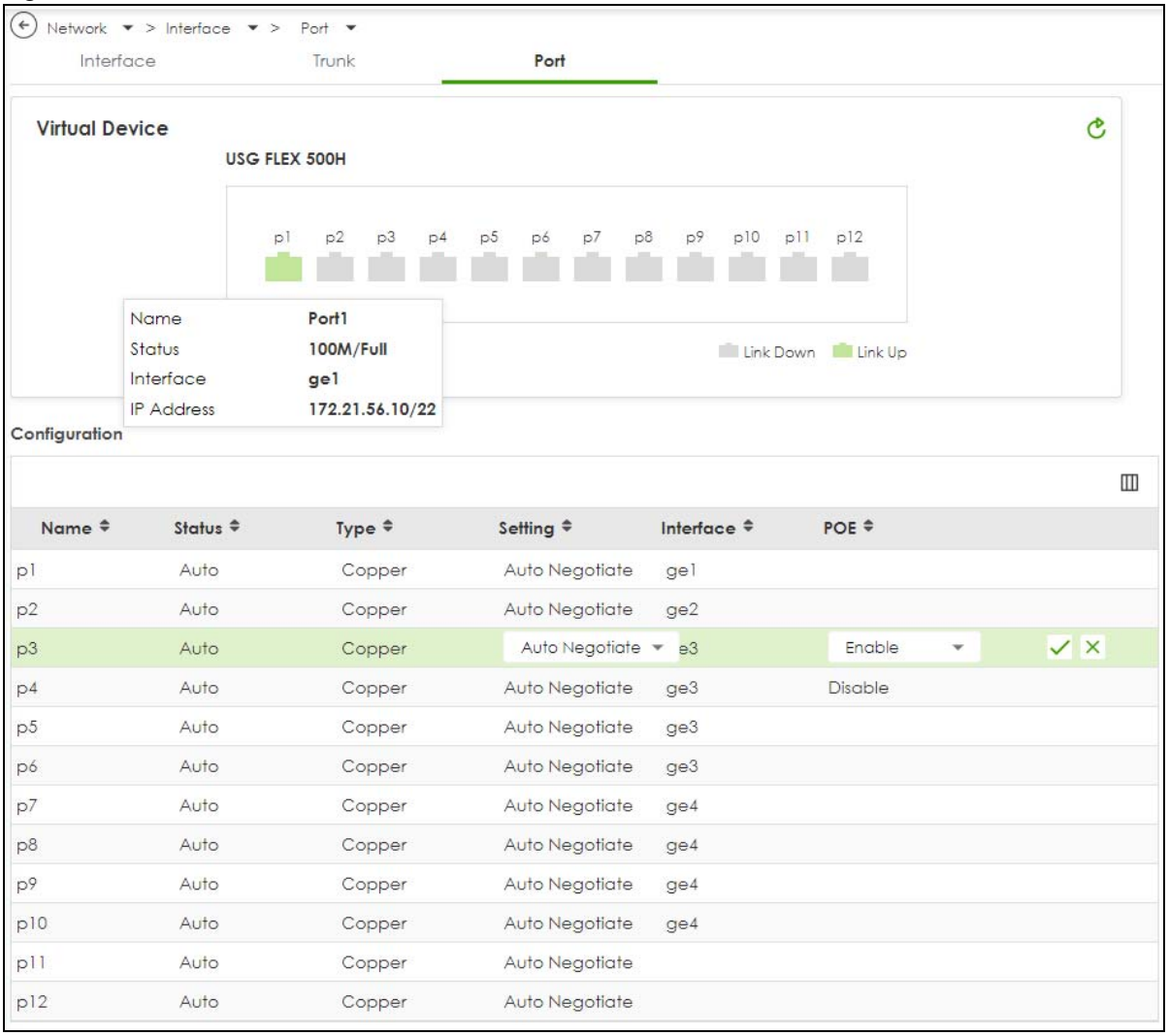
Table 82 Network > Interface > Trunk > Default Trunk > Edit (continued)

LABEL	DESCRIPTION
Interface	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. Note: You cannot configure two **Passive** interfaces for the WAN trunk - at least one interface must be **Active**.
Parameter	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.
Apply	Click **Apply** to save your changes to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

7.9 Port

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

Figure 135 Network > Interface > Port



Each field is described in the following table.

Table 83 Network > Interface > Port

LABEL	DESCRIPTION
Virtual Device	This shows which ports are up or down on the Zyxel Device. Hover over a port to see port details such as name, status , interface and IP address.
Configuration	Select an entry to configure the speed negotiation setting of the Ethernet connection on this port and PoE if the port supports it.
Name	This field displays the name of the port.
Status	This field displays the speed and the duplex mode of the Ethernet connection on the port.
Type	This field displays the cable type that is used on the port.

Table 83 Network > Interface > Port

LABEL	DESCRIPTION
Setting	Select the speed and the duplex mode of the Ethernet connection on this port. Choices are **Auto Negotiate**, **10Mbps, 100Mbps, 1Gbps** and **2.5Gbps.** 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. To avoid errors, it is recommended to set both the Zyxel Device and the peer port to the same speed and duplex mode. For example: • Auto Negotiate—Auto Negotiate • 10Mbps—10Mbps • 100Mbps—100Mbps • 1Gbps—1Gbps • 2.5Gbps—2.5Gbps
Interface	This field displays the interface for the port.
PoE	If the port supports PoE, then this field displays if PoE is enabled on the port.
Edit	Select an entry and click this icon to modify it. 
Remove	Select an entry and click this icon to delete it. 
Save Changes	Click this icon to save the changes in this row. 
Cancel Changes	Click this icon to cancel the changes in this row. 

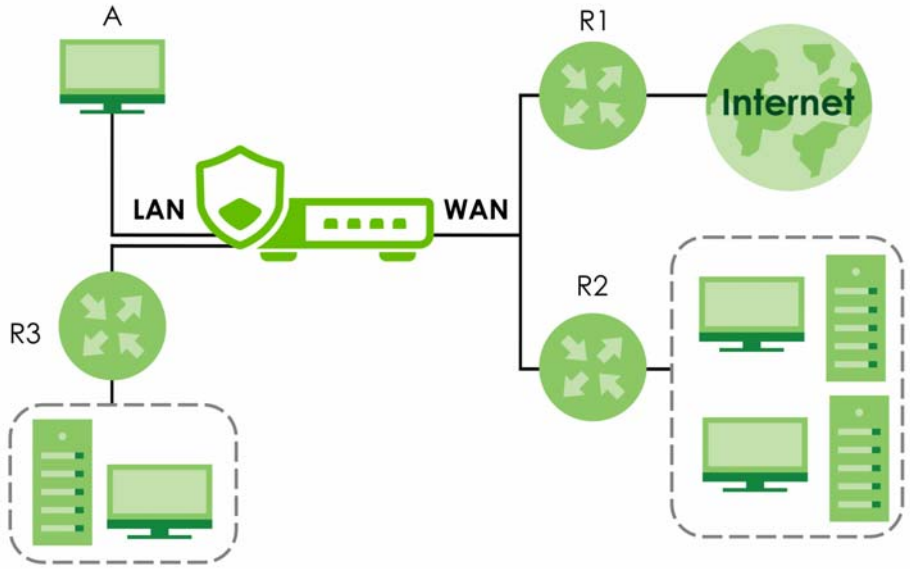
CHAPTER 8
Routing

8.1 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 136 Example of Policy Routing Topology



8.1.1 What You Can Do in this Chapter

- Use the **Policy Route** screens (see Section 8.2 on page 181) to list and configure policy routes.
- Use the **Static Route** screens (see Section 8.3 on page 187) to list and configure static routes.

8.1.2 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.
- 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.

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 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.

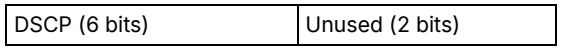
DiffServ

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 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.

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 84 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)

8.2 Policy Route Screen

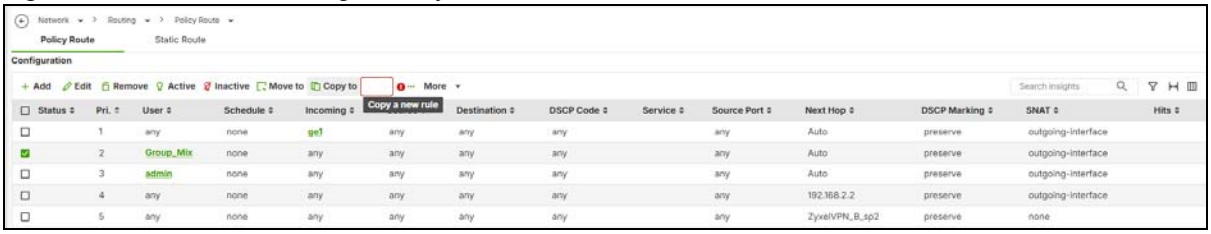
Click **Network > Routing** to open the **Policy Route** screen. Use this screen to see the configured policy routes and turn policy routing based bandwidth management on or off.

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, VTI interface, or trunk.

Figure 137 Network > Routing > Policy Route



The following table describes the labels in this screen.

Table 85 Network > Routing > Policy Route

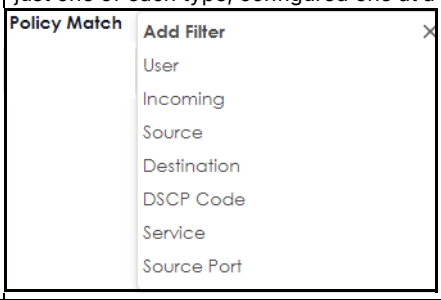
LABEL	DESCRIPTION
Use IPv4 Policy Route to Override Direct Route	Select this to have the Zyxel Device forward packets that match a policy route according to the policy route instead of sending the packets directly to a connected network.
Add	Click this to create a new entry. Select an entry and click **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.
Active	Select one or more policies, then click this to enable the selected policies. The **Status** light changes accordingly.
Inactive	Select one or more policies, then click this to disable the selected policies. The **Status** light changes accordingly.
Move to	Select a policy, click this, enter a new location up to and including the last policy number, then press [ENTER] to move it to the new location. Policies are checked in order beginning from the first.
Copy to	You can create a new policy by copying an existing one to a new position, and then editing it. Select an existing policy and click **Copy** to display a field to type a number for where you want to put that policy, then press [ENTER] to copy the policy to the number that you typed. After copying it, edit it to change it from the one copied. Policies are checked in order beginning from the first.
More	Click this, then click **Refresh** to update the policies listed.
Search	Type an item in the search box, then click this to display all sessions in the table below according to the item you typed.
Clear All	Click this to remove all items found in the search.
Filter	Click the Filter icon, click + to expand **Policy Match,** pick a filter, then click **Find** to display specific sessions according to the filter selected. You may select multiple filters, but just one of each type, configured one at a time. 
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.
Priority	This is the row number of the policy. Policies are checked in order beginning from the first.
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. **any** 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.

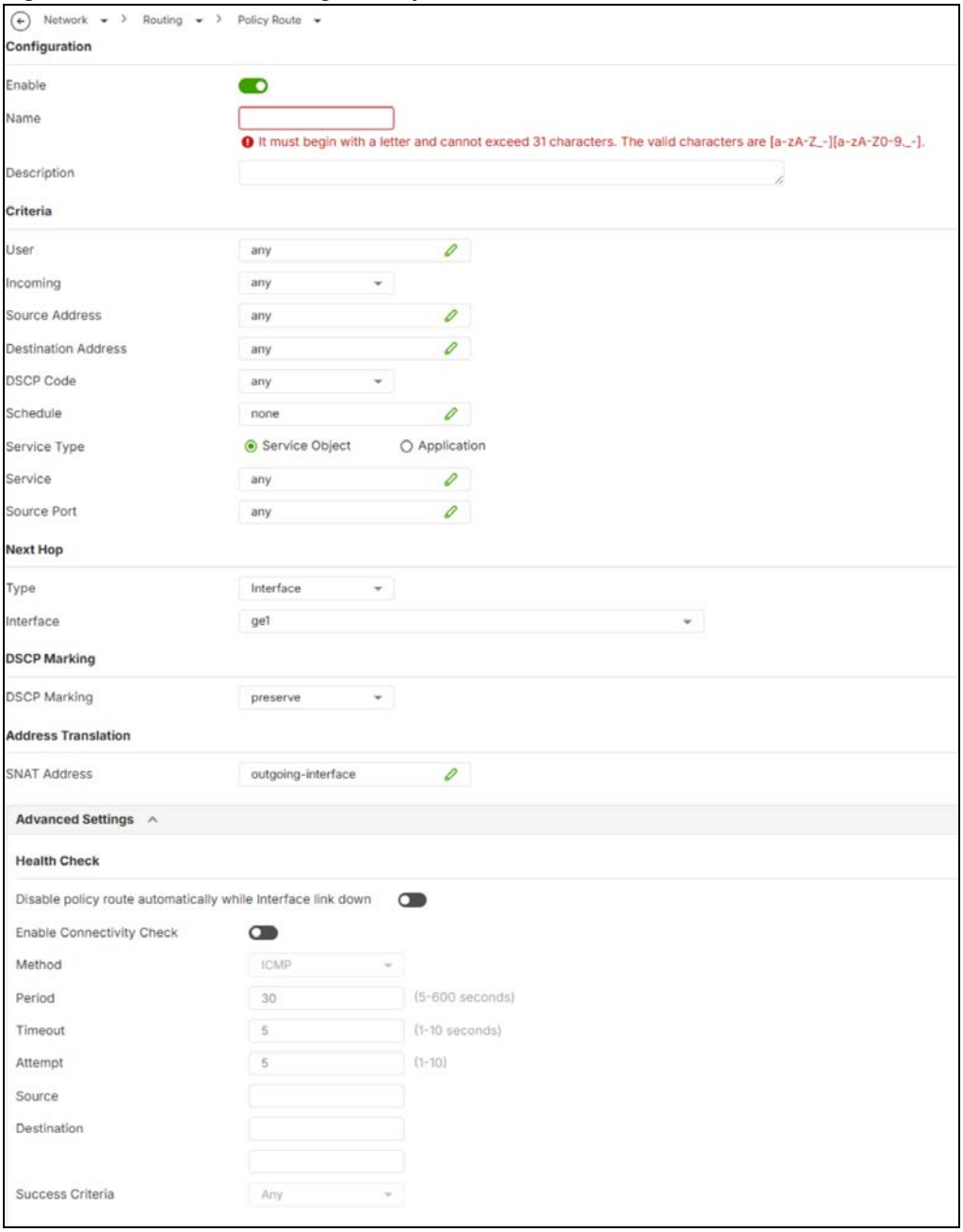
Table 85 Network > Routing > Policy Route (continued)

LABEL	DESCRIPTION
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 destination service object. **any** means all destination services.
Source Port	This is the name of the source service object. **any** means all source services.
Next-Hop	This displays the next immediate router, or a device reachable through an interface or IPSec tunnel, that a packet should be forwarded to on its way to the final destination.
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.
Hits	This is the number of sessions with traffic that matched the policy criteria.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

8.2.1 Policy Route Edit Screen

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

Figure 138 Network > Routing > Policy Route > Add/Edit



The following table describes the labels in this screen.

Table 86 Network > Routing > Policy Route > Add/Edit

LABEL	DESCRIPTION
Enable	Select this to activate the rule.
Name	Enter a name to identify this rule.
Description	Enter a descriptive name consists of 1 to 60 single-byte characters, including a-zA-Z0-9. Special characters and spaces are allowed.
Criteria	
User	Select a user name or user group from which the packets are sent.

Table 86 Network > Routing > Policy Route > Add/Edit (continued)

LABEL	DESCRIPTION
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, 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.
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 Type	Select **Service Object** or **Application** if you want a specific service or application patrol service to which this policy route applies.
Application	This field is available if you selected **Application** as the service type. Select one or more applications to identify the specific traffic to which this policy route applies.
Service	This field is available if you selected **Service Object** as the service type. Select a destination service or service group to identify the type of traffic to which this policy route applies.
Source Port	Select a source service or service group to identify the source port of packets to which the policy route applies.
Next-Hop	Next hop is the next immediate router, or a device reachable through an interface or IPSec tunnel, that a packet should be forwarded to on its way to the final destination.
Type	Select **Auto** to have the Zyxel Device use the routing table to find a next-hop and forward the matched packets automatically. Select **Interface** to route the matched packets through the specified outgoing interface to a gateway (which is connected to the interface). Select **IPSec VPN Tunnel** to route the matched packets through the specified dynamic or static VPN Tunnel. • For a static IPSec tunnel, the peer gateway address is an IP address or an FQDN. Packets that match the policy route's criteria are forwarded through this tunnel. • For a dynamic IPSec tunnel (for example, hub-and-spoke), the peer gateway address is a dynamic IP address. The Zyxel Device will use the dynamic tunnel's remote subnet address as the policy route destination address after the tunnel is built and ignores the destination IP address you configured in this policy route. Select **gateway** to route the matched packets through the selected gateway object to the packets' destination. Select **gateway-ip** to route the matched packets through the gateway IP address you specify in the **Host IP Address** field. You have to set up the gateway as a **HOST** address object first. Select **trunk** to route the matched packets through the interfaces in the trunk group based on the load balancing algorithm.

Table 86 Network > Routing > Policy Route > Add/Edit (continued)

LABEL	DESCRIPTION
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.
IPSec VPN Tunnel	This field displays when you select **IPSec VPN Tunnel** in the **Type** field. Select an IPSec VPN Tunnel to have the Zyxel Device send traffic that matches the policy route through the specified IPSec VPN Tunnel.
Address	This field displays when you select **gateway** in the **Type** field. Select a host address object. **IP6to4-Relay** service enables IPv6 packets to cross IPv4 networks; see Section 8.1.2 on page 179 for more information.
Host IP Address	This field displays when you select **gateway-ip** in the **Type** field. Enter a gateway's IP address. 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).
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.
DSCP Marking	
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.
SNAT Address (Source Network Address Translation Address)	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.
Advanced Settings	
Health Check	Use this to check if the **Next Hop** Interface in the policy route is still available.
Disable policy route automatically while Interface link down	If the configured **Next Hop** Interface goes down but the policy route remains active, traffic will continue to be sent to it and will be lost. Enable this to have the Zyxel Device automatically disable the policy route when the **Next Hop** Interface is down. Traffic will be send through other available routes. This is available for **Interface** in the **Type** field above.
Enable Connectivity Check	Enable this to have the interface regularly check the connection to the Interface you specified to make sure it is still available. This is available for **Interface, gateway** and **gateway-ip** in the **Type** field above.
Method	Select the method that the Interface allows. • Select **ICMP** to have the Zyxel Device regularly ping the Interface you specify to make sure it is still available. • Select **TCP** to have the Zyxel Device regularly perform a TCP handshake with the Interface you specify to make sure it is still available.

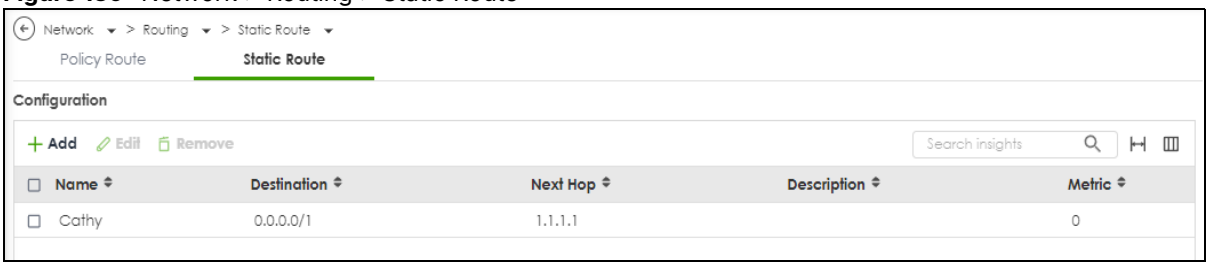
Table 86 Network > Routing > Policy Route > Add/Edit (continued)

LABEL	DESCRIPTION
Period	Enter the number of seconds between connection check attempts (5-600 seconds).
Timeout	Enter the number of seconds to wait for a response before the attempt is a failure (1-10 seconds).
Attempt	Enter the number of consecutive failures before the Zyxel Device stops routing through the Interface.
Source	Enter the IPv4 address that test packets will be sent from. • Leave this field blank to have the Zyxel Device send test packets from this policy route's **Next Hop** Interface. • Enter an IPv4 address to send test packets from the specified Interface.
Destination	Enter one or two interfaces using either FQDNs or IP addresses to receive test packets. You can enter an IPv4 address in one field and a FQDN in the other. For example, type "192.168.1.2" in the first field and "www.zyxel.com" in the second field.
Success Criteria	This field applies when you specify two FQDNs or IP addresses for the connectivity check. • Select **Any** if you want the check to pass if at least one of the Interface with the specified IP address or FQDN responds. • Select **All** if you want the check to pass only if both Interfaces with the specified IP address or FQDN respond.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

8.3 Static Route Screen

Click **Network > Routing > Static Route** to open the **Static Route** screen. This screen displays the configured static routes.

Figure 139 Network > Routing > Static Route



The following table describes the labels in this screen.

Table 87 Network > Routing > Static Route

LABEL	DESCRIPTION
Add	Click this to create a new static route.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Name	This is the name of the static route entry.
Destination	This is the destination IP address.

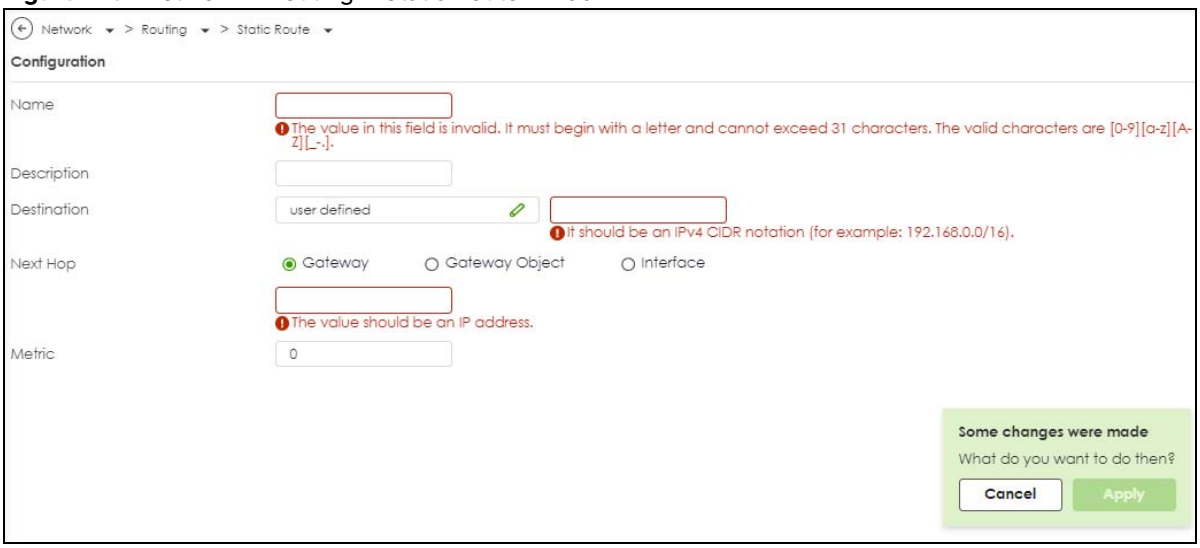
Table 87 Network > Routing > Static Route (continued)

LABEL	DESCRIPTION
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.

8.3.1 Static Route Add/Edit Screen

Click **Network** > **Routing** > **Static Route** > **Add/Edit** to display the next screen. Use this screen to configure the required information for a static route.

Figure 140 Network > Routing > Static Route > Add



The following table describes the labels in this screen.

Table 88 Network > Routing > Static Route > Add

LABEL	DESCRIPTION
Name	Enter a name to identify this rule. You can use up to 30 single-byte characters, including 0-9a-zA-Z. The first character cannot be a number.
Destination	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.
Next Hop	Next hop is the next immediate router, or a device reachable through an interface or IPSec tunnel, that a packet should be forwarded to on its way to the final destination.
Gateway	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.
Gateway Object	Select the radio button to route the matched IPv6 packets through a 6to4 tunnel to the packets' destination.
Interface	Select the radio button and a predefined interface through which the traffic is sent.

Table 88 Network > Routing > Static Route > Add (continued)

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

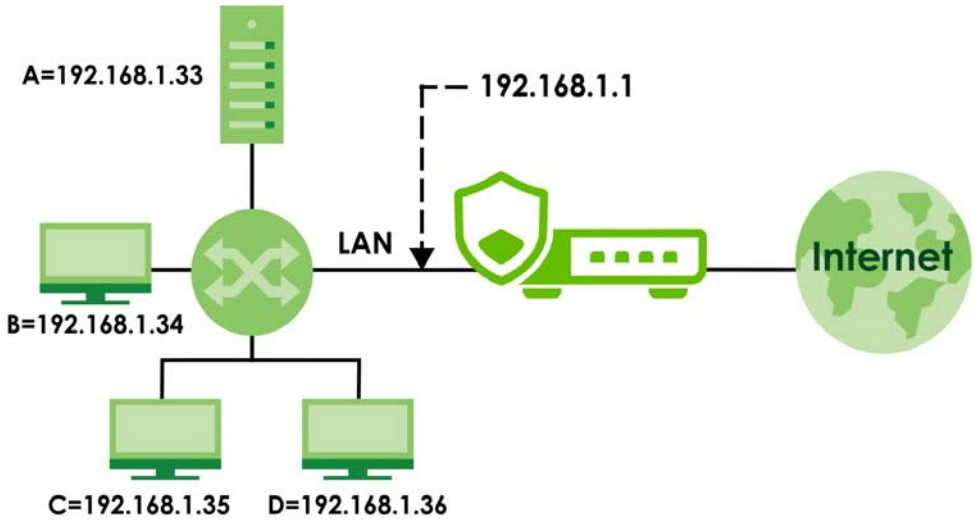
CHAPTER 9
NAT

9.1 NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network. Use Network Address Translation (NAT) to make computers on a private network behind the 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 141 Multiple Servers Behind NAT Example



9.1.1 What You Can Do in this Chapter

Use the **NAT** screens (see Section 9.2 on page 193) 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.

9.1.2 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 18.2 on page 333 (**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 89 Well-known Ports

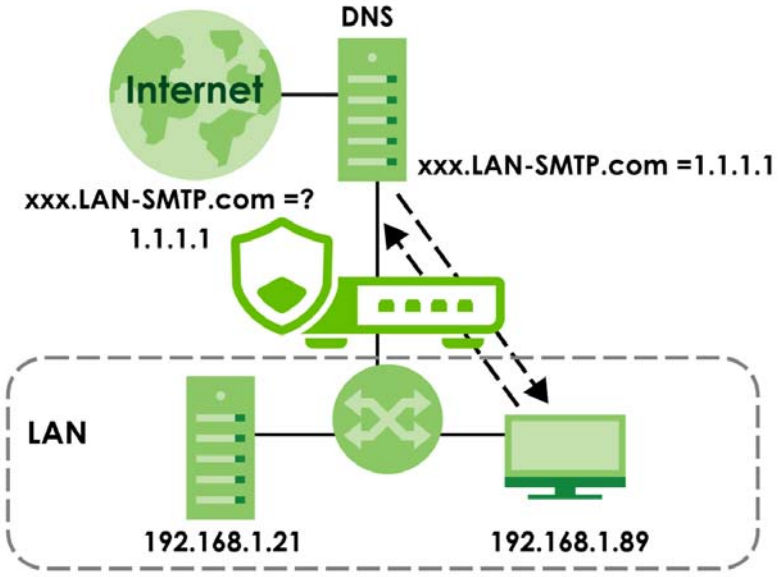
PORT	TCP/UDP	DESCRIPTION
1	TCP	TCP Port Service Multiplexer (TCPMUX)
20	TCP	FTP - Data
21	TCP	FTP - Control
22	TCP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol (SMTP)
42	UDP	Host Name Server (Nameserv)
43	TCP	Whols
53	TCP/UDP	Domain Name System (DNS)
67	UDP	BOOTP/DHCP 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
990	TCP	FTP over TLS/SSL (FTPS)
995	TCP	POP3 over TLS/SSL (POP3S)

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.

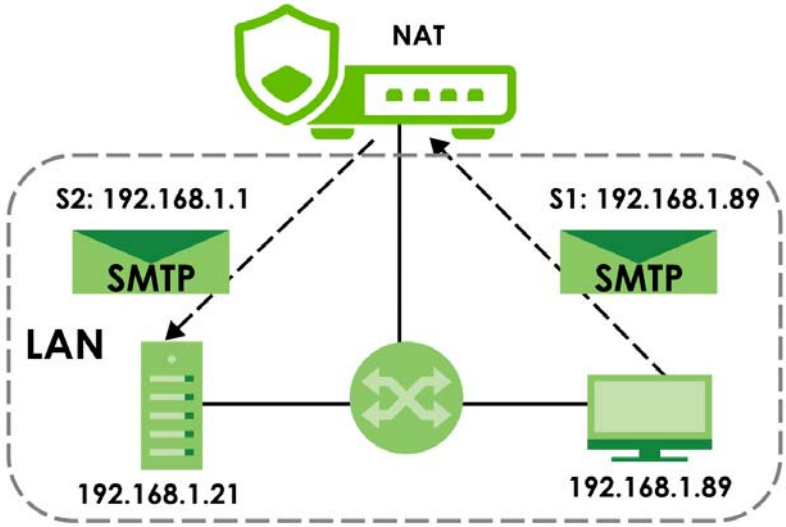
For example, a LAN user's computer at IP address 192.168.1.89 queries a public DNS server to resolve the SMTP server's domain name (xxx.LAN-SMTP.com in this example) and gets the SMTP server's mapped public IP address of 1.1.1.1.

Figure 142 LAN Computer Queries a Public DNS Server



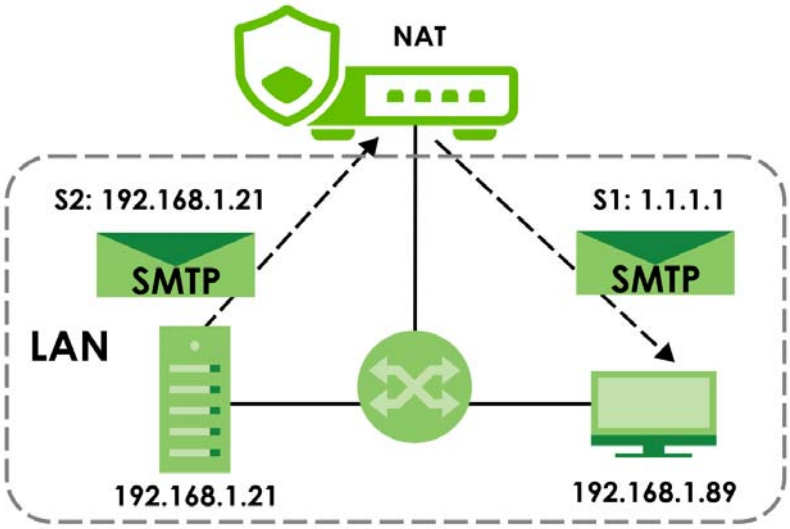
The LAN user's computer then sends traffic to IP address 1.1.1.1. NAT loopback uses the IP address of the Zyxel Device's LAN interface (192.168.1.1) as the source address of the traffic going from the LAN users to the LAN SMTP server.

Figure 143 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 (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 144 LAN to LAN Return Traffic



9.2 The NAT Screen

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

Figure 145 Network > NAT



The following table describes the labels in this screen.

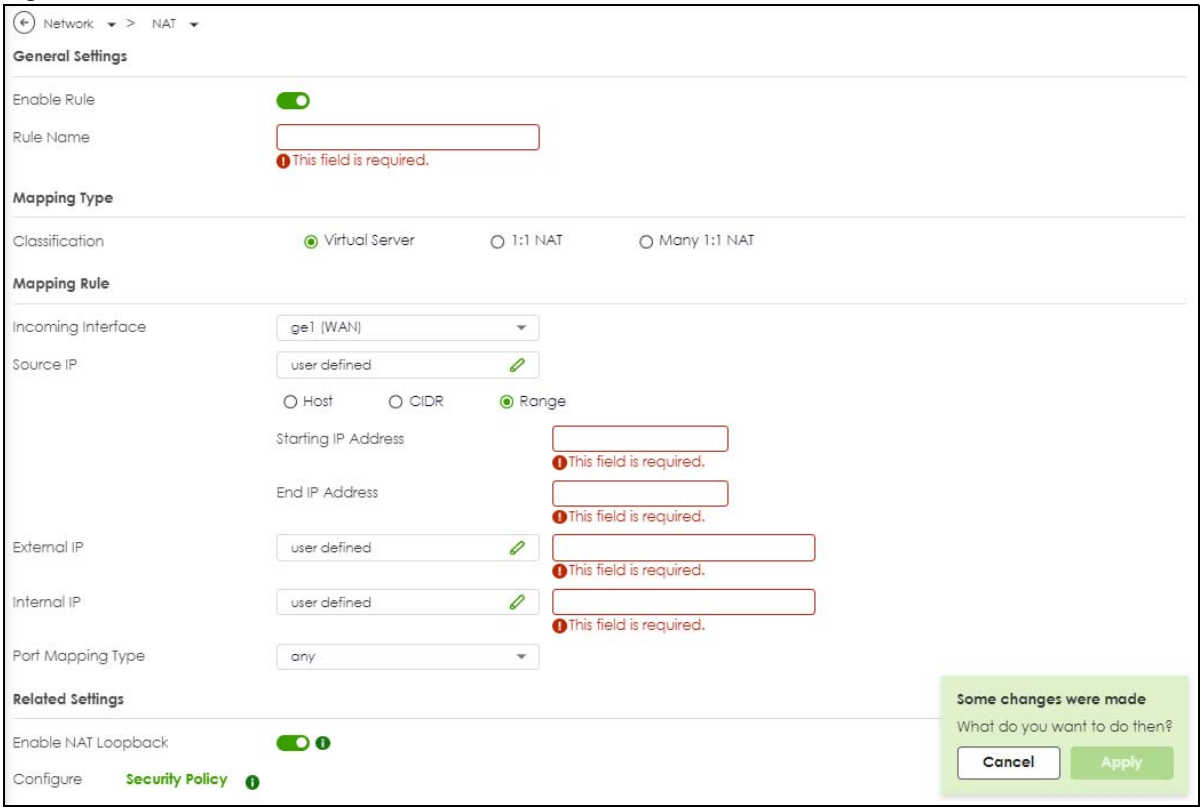
Table 90 Network > NAT

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The 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.
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 **Apply** to save your changes to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

9.2.1 The NAT Add/Edit Screen

The **NAT Add/Edit** screen lets you create new NAT rules and edit existing ones. To open this window, open the **NAT** summary screen. (See Section 9.2 on page 193.) Then, click on an **Add** icon or **Edit** icon to open the following screen.

Figure 146 Network > NAT > Add



The following table describes the labels in this screen.

Table 91 Network > NAT > Add

LABEL	DESCRIPTION
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 or bridge interface.

Table 91 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.
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.
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 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.
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.

Table 91 Network > NAT > Add (continued)

LABEL	DESCRIPTION
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 192 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. NAT loopback cannot be enabled when the **External IP** is set to **any**.
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.
Apply	Click **Apply** to save your changes to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

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.

CHAPTER 10
BWM (Bandwidth Management)

10.1 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.

10.1.1 What You Can Do in this Chapter

Use the **BWM** screens (see Section 10.2 on page 201) to control bandwidth for services passing through the Zyxel Device, and to identify the conditions that define the bandwidth control.

10.1.2 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.

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.

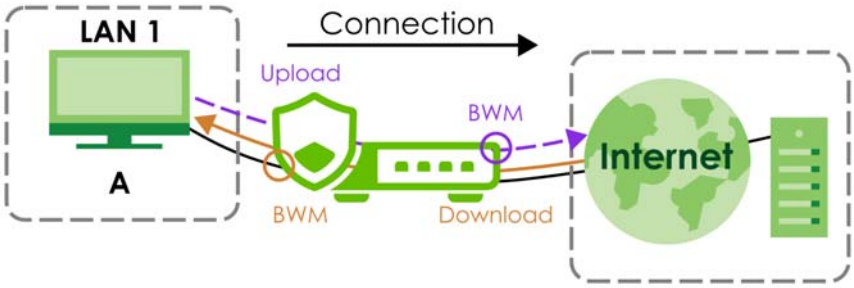
A connection has upload and download packet flows. The Zyxel Device controls the bandwidth of traffic of each flow as it is going out through an interface or IPSec VPN tunnel.

- The upload traffic flows from the connection initiator to the connection responder.
- The download 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.

- Upload 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.
- Download traffic comes back from the WAN device to the LAN1 device. Bandwidth management is applied before sending the traffic out a LAN1 interface.

Figure 147 LAN1 to WAN Connection and Packet Directions

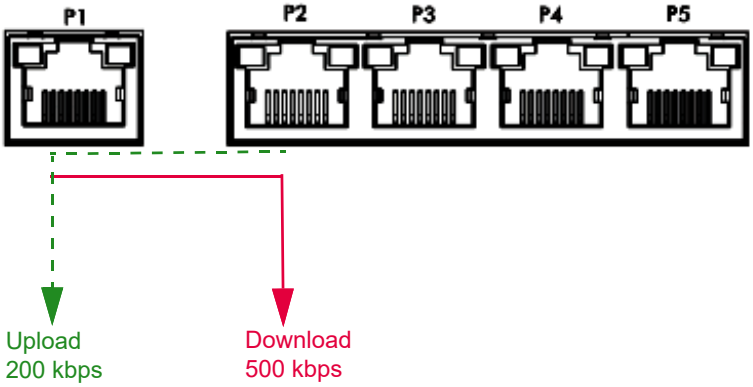


Upload and Download Bandwidth Limits

You can limit an application's upload or download bandwidth. This limit keeps the traffic from using up too much of the upload interface's bandwidth. This way you can make sure there is bandwidth for other applications. When you apply a bandwidth limit to upload or download traffic, each member of the upload zone can send up to the limit. Take a LAN1 to WAN policy for example.

- Upload traffic is limited to 200 kbps. The connection initiator is on the LAN1 so upload 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.
- Download traffic is limited to 500 kbps. The connection initiator is on the LAN1 so download means the traffic traveling from the WAN to the LAN1.

Figure 148 LAN1 to WAN, Upload 200 kbps, Download 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 priority queueing 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).

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 92 Configured Rate Effect

POLICY	CONFIGURED RATE	MAX. BANDWIDTH USAGE	PRIORITY	ACTUAL RATE
A	300 kbps	No	1	300 kbps
B	200 kbps	No	1	200 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 93 Priority and Over Allotment of Bandwidth Effect

POLICY	CONFIGURED RATE	MAX. BANDWIDTH USAGE	PRIORITY	ACTUAL RATE
A	1000 kbps	Yes	1	999 kbps
B	1000 kbps	Yes	2	1 kbps

Limit the Bandwidth for a Specific VLAN

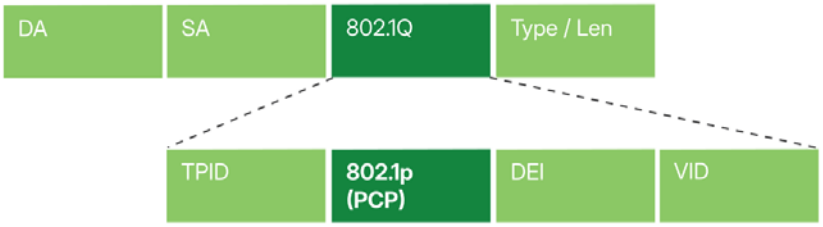
If you want to limit the bandwidth for a specific VLAN, set the VLAN as the incoming interface and VPN as the outgoing interface. Then, set the bandwidth limit for this BWM rule.

The **Configuration > Bandwidth Management Add/Edit** screen allows you to create a new condition or edit an existing one.

802.1p

Use 802.1p to prioritize outgoing traffic from a VLAN interface. The Priority Code Point (**PCP**) 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. Receiving devices will prioritize the traffic according to this tag.

Figure 149 802.1Q Frame.



DA	Destination Address	TPID	Tag Protocol Identifier
SA	Source Address	802.1p (PCP)	802.1p Priority
802.1Q	802.1Q Frame	DEI	Drop Eligible Indicator
Type/ Len	Ethernet Type / Length	VID	VLAN ID

The following table is a guide to the types of traffic for each priority code.

Table 94 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

10.2 The Bandwidth Management Configuration

The Bandwidth management screens control the bandwidth allocation for TCP and UDP traffic. You can use incoming interface, outgoing interface, user, source, destination information, application, 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 allocates bandwidth for the matching packets.

Click **Network > 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 150 Network > Bandwidth Management



The following table describes the labels in this screen. See Section 10.2.1 on page 203 for more information as well.

Table 95 Network > Bandwidth Management

LABEL	DESCRIPTION
Enable	Click to slide the switch to the right to activate bandwidth management on 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	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	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.
Pri (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.
Name	This is the name of the BWM rule.
Description	This field displays additional information about this policy.
User	This is the type of user account to which the policy applies. If **any** displays, the policy applies to all user accounts.
Incoming Interface	This is the source interface of the traffic to which this policy applies.
Outgoing Interface	This is the destination interface of the traffic to which this policy applies.
Source	This is the source address or address group, 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.
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 Download/ Upload/Pri	This field shows the amount of bandwidth the traffic can use. **Download** - This is how much inbound bandwidth, in megabits per second, this policy allows the matching traffic to use. Inbound refers to the traffic the Zyxel Device sends to a connection's initiator. If **0** displays here, it means the download traffic has reached the maximum capacity the Zyxel Device can transmit. **Upload** - This is how much outbound bandwidth, in megabits 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 **0** displays here, it means the upload traffic has reached the maximum capacity the Zyxel Device can transmit. **Pri** - This is the priority for the inbound or outbound 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.

Table 95 Network > Bandwidth Management (continued)

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

10.2.1 The Bandwidth Management Add/Edit Screen

The **Network > BWM > Add/Edit** screen allows you to create a new condition or edit an existing one.

To access this screen, go to the **Network > BWM** screen (see Section 10.2 on page 201), and click either the **Add** icon or an **Edit** icon.

The first BWM policy is the default and can only be edited.

Figure 151 Network > BWM > Edit (For the Default Policy)

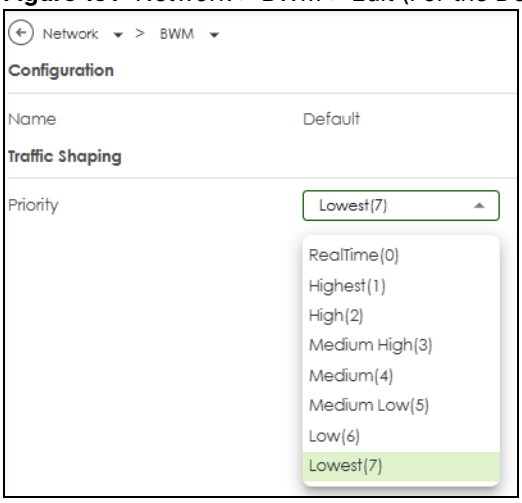
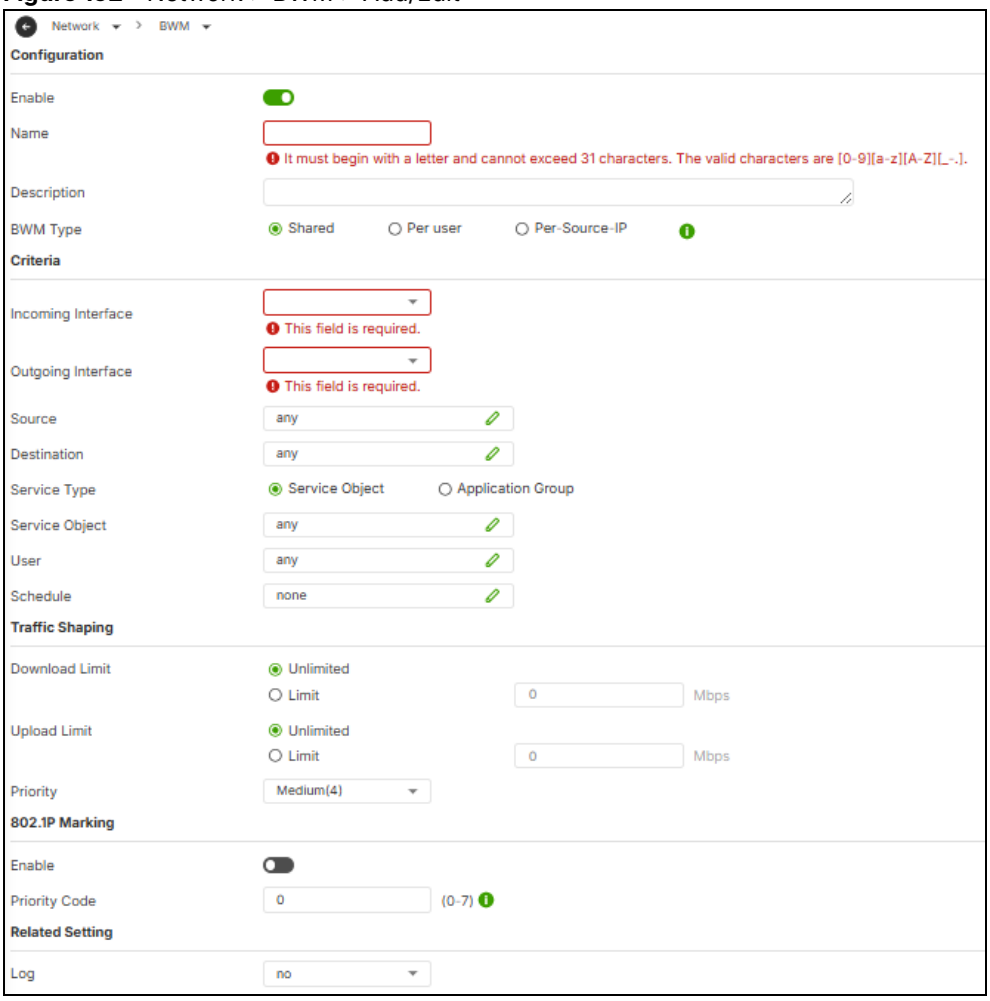


Figure 152 Network > BWM > Add/Edit



The following table describes the labels in this screen.

Table 96 Network > BWM > Add/Edit

LABEL	DESCRIPTION
Configuration	
Enable	Select this check box to turn on this policy.
Name	Enter a name to identify the BWM 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 of this policy. It is not used elsewhere. You can use alphanumeric and ()+/:+?!*#@$_%- characters, and it can be up to 60 characters long.
BWM Type	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. If you select this, the **User** field below cannot be **any**. Select the **Per-Source-IP** type when you want to set the maximum bandwidth for traffic from an individual source IP address object. Only address objects with up to 1,024 IP addresses are available from the **Source** filed below. If you select this, the **Source** field below cannot be **any**.
Criteria	Use this section to configure the conditions of traffic to which this policy applies.

Table 96 Network > BWM > Add/Edit (continued)

LABEL	DESCRIPTION
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.
Service Type	Select **Service Object** or **Application Group** if you want a specific service (defined in a service object) or application patrol service to which the policy applies.
Service Object	This field is available if you selected **Service Object** as the service type. Select a service or service group to identify the type of traffic to which this policy applies. **any** means all services.
Application Group	This field is available if you selected **Application Group** as the service type. Select an application 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
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	If you already created a **One Time** or **Recurring** schedule in **Object > Schedule**, then select a schedule that defines when the policy applies. Alternatively, select **Create Object** to configure a new schedule. Otherwise, select **none** to make the policy always effective.
Traffic Shaping	Configure these fields to set the amount of bandwidth the matching traffic can use.
Download Limit (Mbps)	Type how much inbound bandwidth, in megabits per second, this policy allows the traffic to use. Inbound refers to the traffic the Zyxel Device sends to a connection's initiator. Select **Unlimited** to apply bandwidth management for the matching traffic which is the maximum amount your Zyxel Device can transmit. Select **Limited** to apply bandwidth management for matching traffic, and enter a number from 1 to 10,000 Mbps. Note: Traffic matching a Limited policy may "borrow" all unused bandwidth on the inbound interface. 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 96 Network > BWM > Add/Edit (continued)

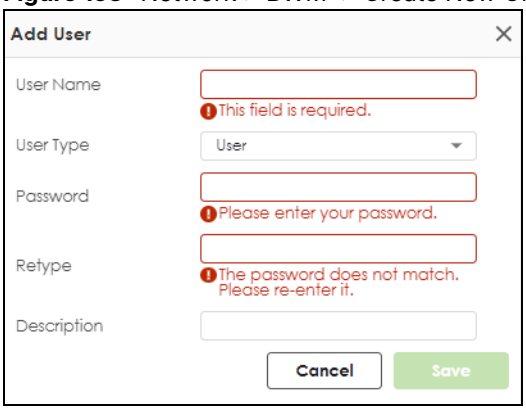
LABEL	DESCRIPTION
Upload Limit (Mbps)	Type how much outbound bandwidth, in megabits per second, this policy allows the traffic to use. Outbound refers to the traffic the Zyxel Device sends out from a connection's initiator. Select **Unlimited** to apply bandwidth management for the matching traffic which is the maximum amount your Zyxel Device can transmit. Select **Limited** to apply bandwidth management for matching traffic, and enter a number from 1 to 10,000 Mbps. Note: Traffic matching a Limited policy may "borrow" all unused bandwidth on the upload interface. If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.
Priority	Choose a number between 0 and 7 to set the priority for traffic that matches this policy. The smaller the number, the higher the priority. 0 is for real-time traffic such as video, and 7 is for lowest priority traffic such as background traffic. 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 priority queueing scheduler to divide bandwidth between traffic flows with the same priority. The number in this field is ignored if the download and upload limits are both set to **Unlimited**.
802.1P Marking	Use 802.1P to prioritize outgoing traffic from a VLAN interface. Receiving devices will prioritize the traffic according to this tag. See 802.1p on page 200 for details.
Enable	Click to slide the switch to the right to enable **802.1P Marking**.
Priority Code	This is a 3-bit field within an 802.1Q VLAN tag that is used to prioritize associated outgoing VLAN traffic. "**0**" is the lowest priority level and "**7**" is the highest. The setting configured here overrides the existing priority settings on the VLAN interface.
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.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

10.2.2 Adding Objects for the BWM Policy

Objects are parameters to which the Policy rules are built upon. You can add/edit **User** and **Address** objects for the BWM policy. Click **Network > BWM > Add** > **Create New Object** > **Add User** to see the following screen.

10.2.2.1 User Objects

Figure 153 Network > BWM > Create New Object > Add User



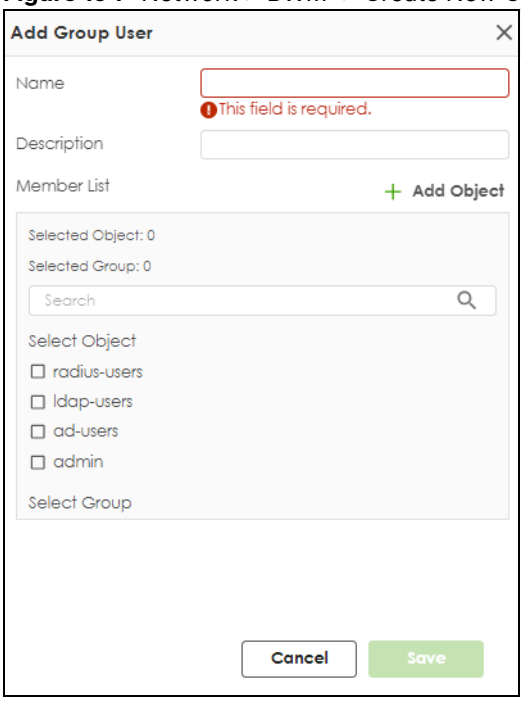
The following table describes the fields in the above screen.

Table 97 Network > 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.
Save	Click **Save** to save the setting.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

10.2.2.2 User Group Objects

Figure 154 Network > BWM > Create New Object > Add User Group



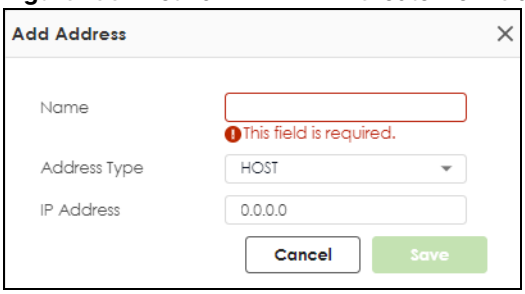
The following table describes the fields in the above screen.

Table 98 Network > BWM > Create New Object > Add User Group

LABEL	DESCRIPTION
Name	Type a user group name of the object.
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.
Member List	Select the users or user groups that will be in this user group.
Save	Click **Save** to save the setting.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

10.2.2.3 Address Objects

Figure 155 Network > BWM > Create New Object > Add Address



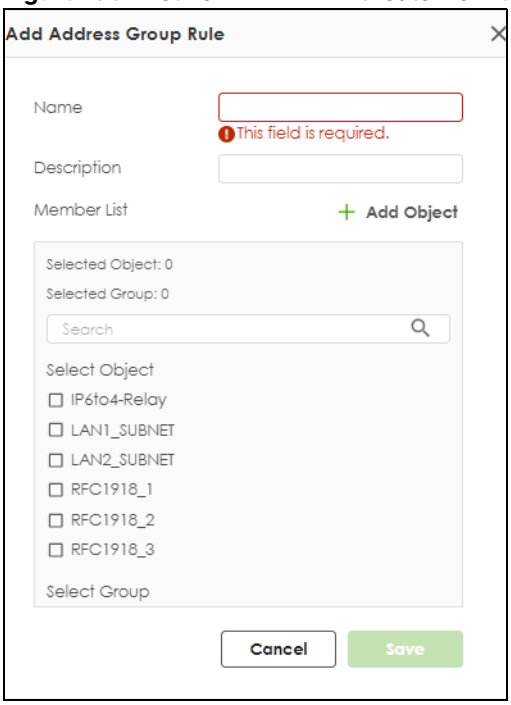
The following table describes the fields in the above screen.

Table 99 Network > 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.
Save	Click **Save** to save the setting.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

10.2.2.4 Address Group Objects

Figure 156 Network > BWM > Create New Object > Add Address Group



The following table describes the fields in the above screen.

Table 100 Network > BWM > Create New Object > Add Address Group

LABEL	DESCRIPTION
Name	Type an address group name of the object.
Description	Enter a description of this object. It is not used elsewhere. You can use alphanumeric and ()+/:+?!*#@$_%- characters, and it can be up to 60 characters long.
Member List	Select the address objects that will be in this user group.
Save	Click **Save** to save the setting.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

10.3 Example: Prioritize a Specific Application

You are a client on the Zyxel Device LAN. 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.

This example uses the parameters given below.

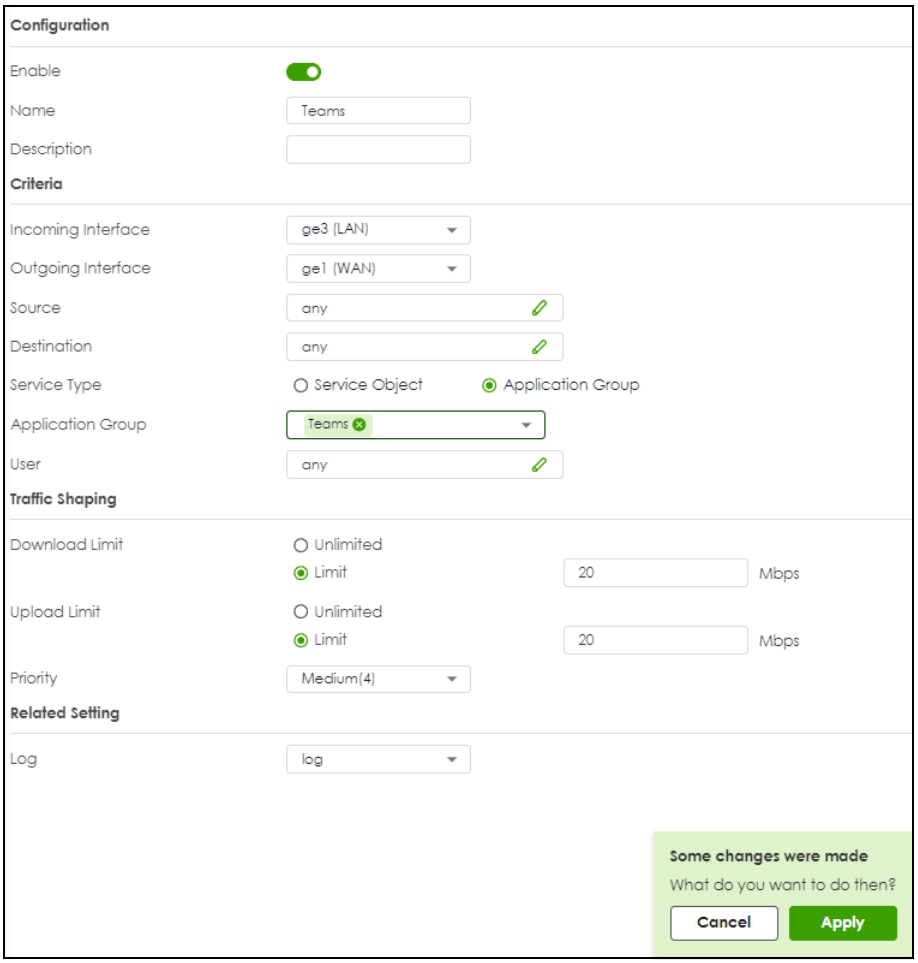
Table 101 BWM Example

DESCRIPTION	SERVICE TYPE	SERVICE OBJECT	GUARANTEED BANDWIDTH
Teams	Application Group	Teams	Download 20 mbps/ Priority: 1 Upload: 20 mbps/ Priority: 1

1 Go to **Network > BWM** . Click **Add** to create a bandwidth management rule using the parameters given in Table 101 on page 210.

2 Select **Teams** under **Application Group**.

3 Click **Apply** to save your changes.



4 The traffic for Teams is now at the highest priority to use the Zyxel Device bandwidth.

CHAPTER 11
ALG

11.1 ALG Overview

Application Layer Gateway (ALG) allows File Transfer Protocol (FTP) to operate properly through the Zyxel Device's NAT.

The ALG feature is only needed for traffic that goes through the Zyxel Device's NAT.

11.1.1 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 unfriendly applications (such as FTP) 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.

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 FTP traffic's data stream. When a device behind the Zyxel Device uses an application for which the Zyxel Device has FTP 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.

FTP ALG

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.

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.

SIP Pinhole

- 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.
- The SIP Pinhole 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 Pinhole allows UDP packets with a specified port destination to pass through.
- The Zyxel Device allows SIP audio connections.
- Configuring the SIP Pinhole to use custom port numbers for SIP traffic also configures the application patrol (see Chapter 19 on page 350) to use the same port numbers for SIP traffic. Likewise, configuring the application patrol to use custom port numbers for SIP traffic also configures SIP Pinhole to use the same port numbers for SIP traffic.

11.1.2 Before You Begin

You must also configure the security policy and enable NAT in the Zyxel Device to allow sessions initiated from the WAN.

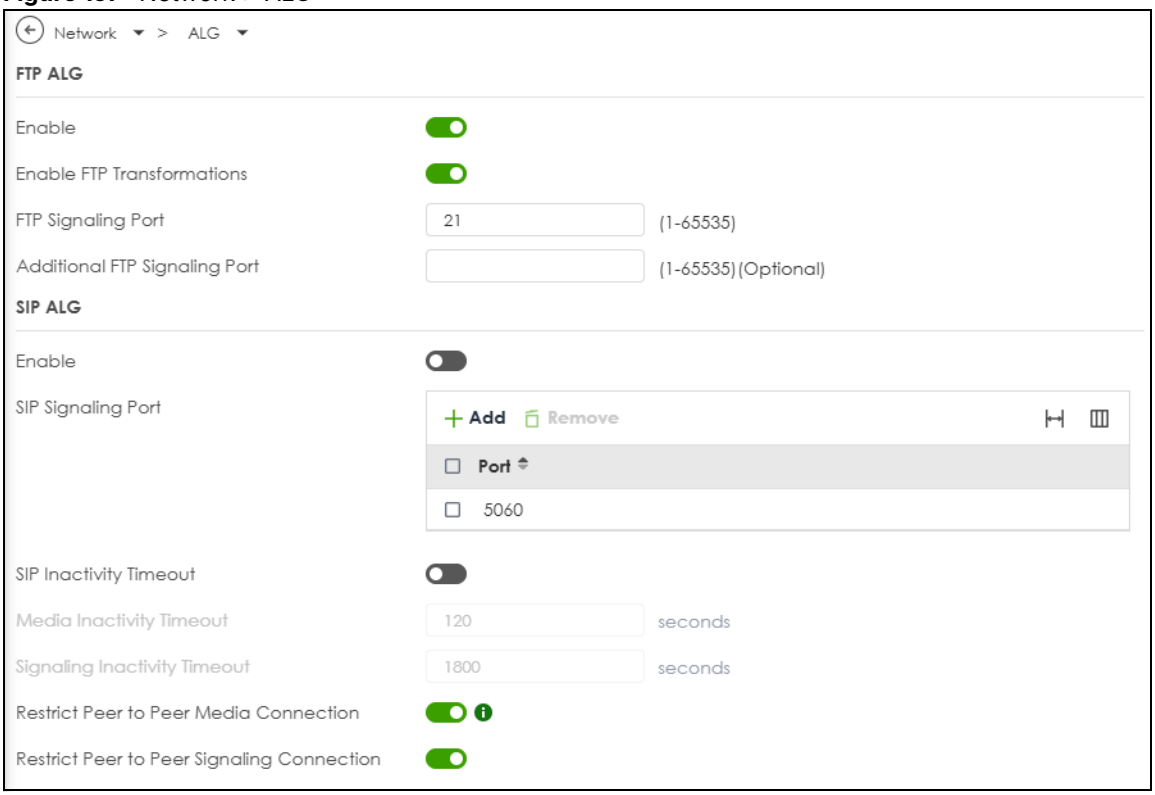
11.2 The ALG Screen

Click **Network** > **ALG** to open the **ALG** screen. Use this screen to:

- Turn ALGs off or on.
- Configure the port numbers to which they apply.

Note: If the Zyxel Device provides an ALG for a service, you must enable the ALG in order to use the application patrol on that service's traffic.

Figure 157 Network > ALG



The following table describes the labels in this screen.

Table 102 Network > ALG

LABEL	DESCRIPTION
FTP ALG	
Enable	Turn on the FTP ALG to detect FTP (File Transfer Program) traffic and help build FTP sessions through the Zyxel Device's NAT. Enabling the FTP ALG also allows you to use the application patrol to detect FTP traffic.
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.
SIP ALG	
Enable	Turn on the SIP ALG to detect SIP traffic and help build SIP sessions through the Zyxel Device's NAT. Enabling the SIP ALG also allows you to use the application patrol to detect SIP traffic and manage the SIP traffic's bandwidth
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.
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.

Table 102 Network > ALG (continued)

LABEL	DESCRIPTION
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 Pinhole 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.
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 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.
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.

CHAPTER 12
Multicast

12.1 Multicast Overview

This chapter shows you how to configure various multicast features.

Traditionally, IP packets are transmitted in one of either two ways – Unicast (one sender to one recipient) or Broadcast (one sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network.

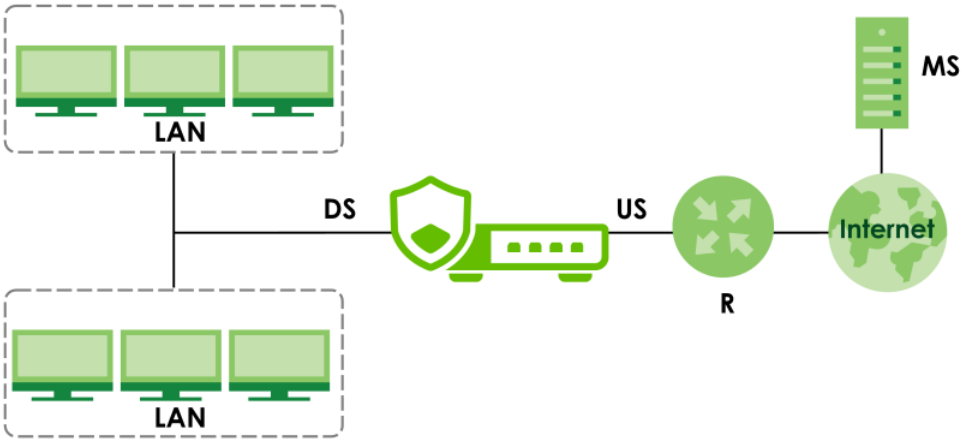
12.1.1 What You Need to Know

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 158 IGMP Proxy



mDNS

Multicast DNS (mDNS) is a protocol that sends discovery packets to resolve hostnames to IP addresses on a local network without using a DNS server. It is commonly used by zero-configuration services that require no manual IP or DNS setup, such as printers, TVs, AirPlay, Chromecast, and IoT devices.

mDNS uses a query and response exchange to allow devices to find each other and then establish a communication session. In the following scenario, the mobile phone (**C1**) connects to the printer (**C2**) on the same LAN.

Step1: Query

C1 sends out multicast discovery packets with host name **C2** to multicast address 224.0.0.251 on port 5353 used for the mDNS queries.

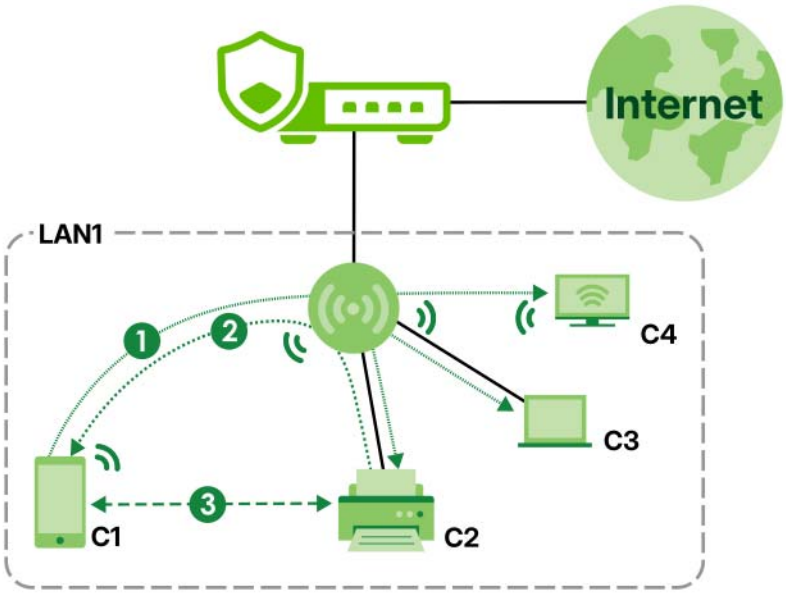
Step 2: Response

C2 receives the multicast query and responds with its IP address.

Step 3: Session Established

C1 receives the response from **C2** and obtains its IP address. **C1** and **C2** have established a communication session.

Figure 159 mDNS



mDNS Proxy

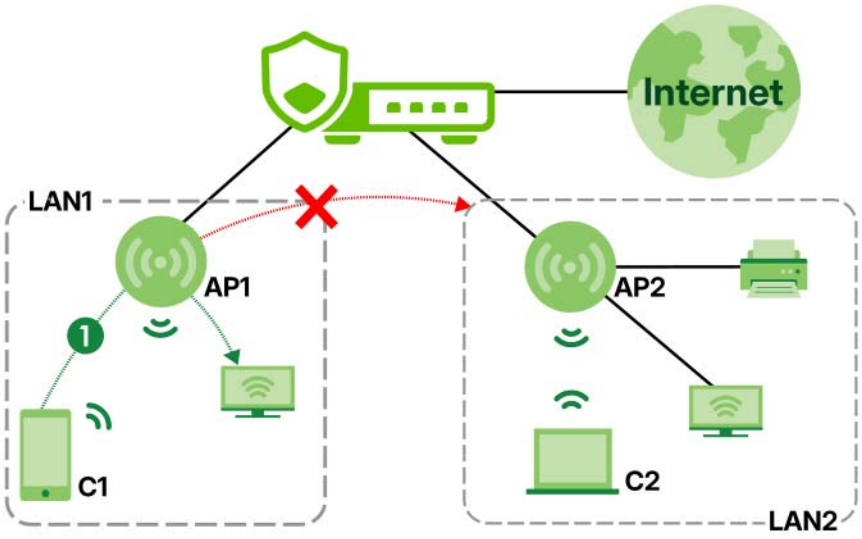
mDNS discovery is only sent to a local network multicast address (224.0.0.251:5353). The Zyxel Device supports mDNS Proxy that allows the Zyxel Device to act as a the mDNS reflector to transmit the multicast discovery packets across subnets.

The examples below show how the mobile phone (**C1**) on **LAN1** connects to the laptop (**C2**) on **LAN2** through the Zyxel Device by using the **mDNS Proxy** feature.

With mDNS Proxy Disabled

When **mDNS Proxy** is disabled, the multicast discovery packets cannot be sent out of **LAN1**. Therefore, **C2** does not receive the query.

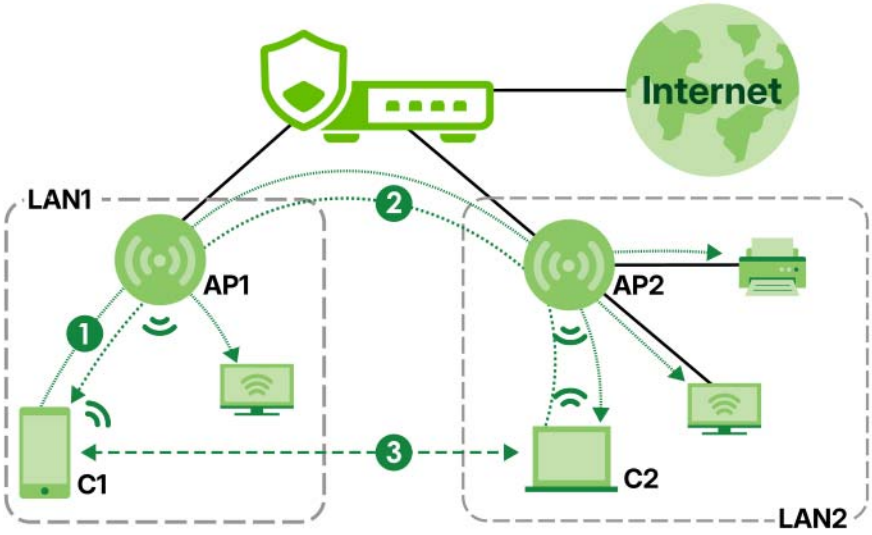
Figure 160 mDNS Proxy Disabled



With mDNS Proxy Enabled

When the **mDNS Proxy** is enabled and the **LAN1** and **LAN2** interfaces are configured as **Allowed Interfaces**, the connection between **C1** and **C2** is successful.

Figure 161 mDNS Proxy Enabled

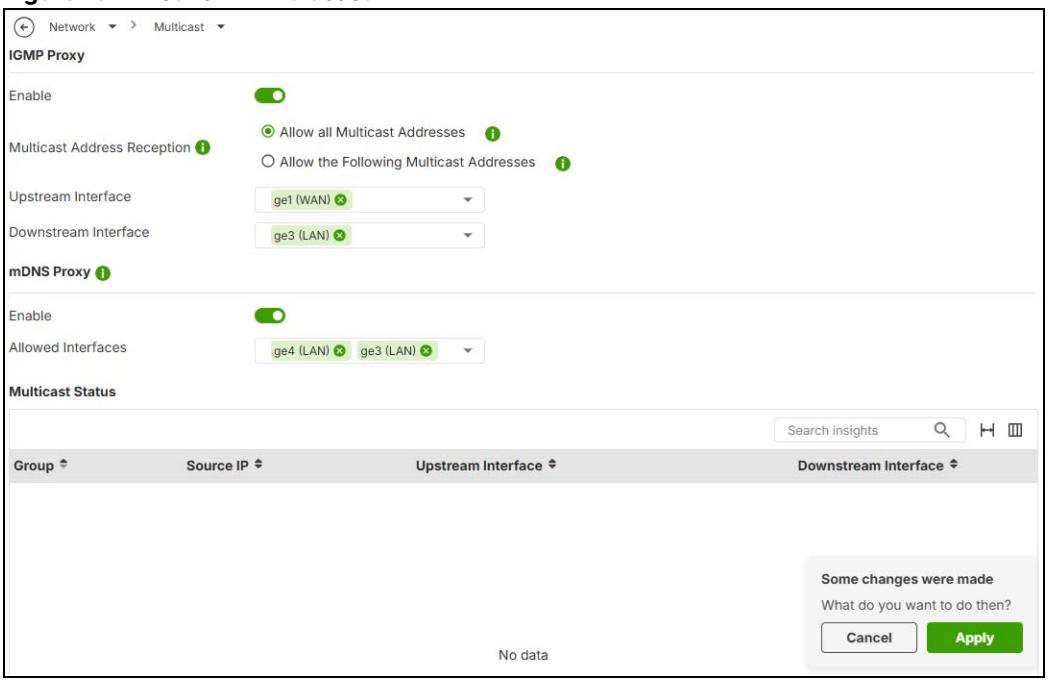


12.2 The Multicast Screen

Click **Network** > **Multicast** to open the **Multicast** screen. Use this screen to:

- Turn IGMP Proxy off or on
- Configure multicast traffic
- View multicast traffic status

Figure 162 Network > Multicast



The following table describes the labels in this screen.

Table 103 Network > Multicast

LABEL	DESCRIPTION
IGMP Proxy	
Enable	Turn on the IGMP Proxy to enable the Zyxel Device to route multicast traffic.
Multicast Address Reception	**Allow all Multicast Addresses**: Select this to have the Zyxel Device send all multicast traffic to all the IGMP hosts. Note: If too much multicast traffic congests your network, you may choose the following option. **Allow the Following Multicast Addresses**: Multicast addresses from the WAN are blocked by default. Select this to have the Zyxel Device forward specific multicast addresses from the WAN to the selected IGMP hosts. Click the edit icon to select existing IP address objects or create new ones.
Upstream Interface	Select the interface that connects to a gateway running IGMP and can receive traffic from the multicast server. Note: You can assign Ethernet, VLAN, Bridge, or LAG interfaces as IGMP Proxy upstream interfaces.
Downstream Interface	Select the interface that connects to the multicast hosts. Note: You can assign Ethernet, VLAN, Bridge, or LAG interfaces as IGMP Proxy downstream interfaces.
mDNS Proxy	

Table 103 Network > Multicast (continued)

LABEL	DESCRIPTION
Enable	Turn on the mDNS Proxy to enable the Zyxel Device to route mDNS multicast traffic across subnets.
Allowed Interfaces	Select the internal interfaces that mDNS multicast packets are allowed to pass. Devices on the selected interfaces can receive and forward mDNS multicast packets. Note: You can select up to four interfaces. Only internal interfaces you configured on **Network > Interface > Interfaces** are allowed.
Multicast Status	This shows information about which multicast groups are currently active and how the multicast traffic pass through the Zyxel Device.
Group	This shows the multicast group IP address the multicast traffic belongs to. The multicast traffic in this group is forwarded to the downstream interfaces.
Source IP	This shows the IP address of the multicast server.
Upstream Interface	This shows the interfaces on which the Zyxel Device receives multicast traffic.
Downstream Interface	This shows the interfaces to which the Zyxel Device forwards multicast traffic.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

CHAPTER 13
IPSec VPN

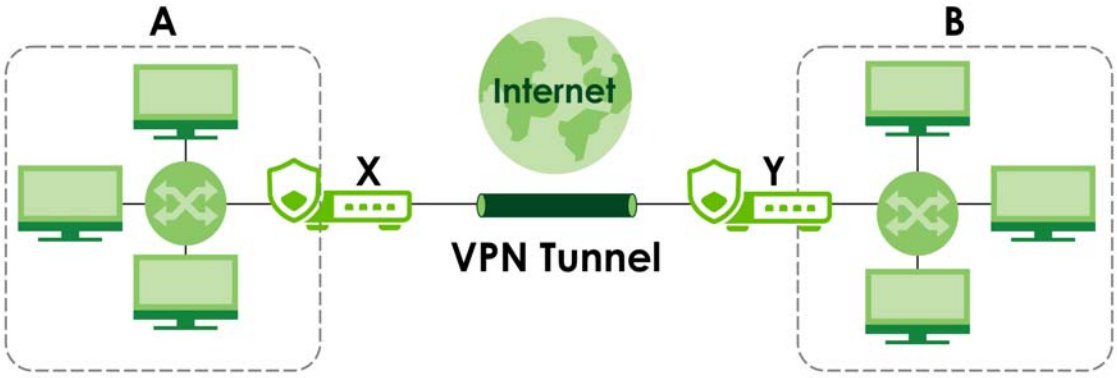
13.1 Virtual Private Networks (VPN) Overview

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 163 IPSec VPN Example



Internet Key Exchange (IKE): IKEv1 and IKEv2

The Zyxel Device supports IKEv1 and IKEv2 for IPv4 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.

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.

13.2 IPSec VPN Background Information

Here is some more detailed IPSec VPN background information.

13.2.1 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 for IKEv1--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 13.1 on page 220 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,

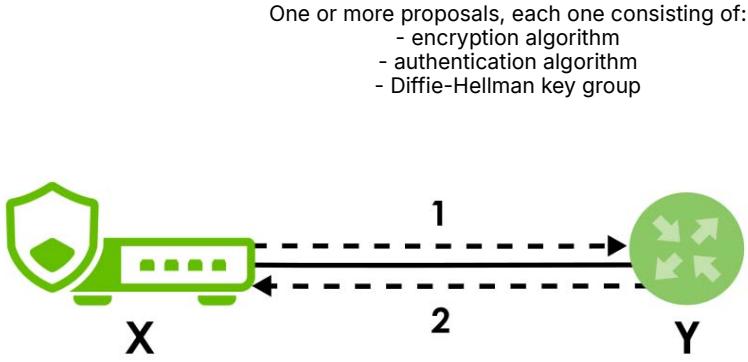
your Zyxel Device might offer another alternative, such as using the IP address of a port or interface, as well.

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 164 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.

Encryption Methods

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.
- **AES-GCM** (Galois/Counter Mode) offers secure (prevents both passive eavesdropping and active tampering), authenticated encryption that is faster than AES as it is optimized for modern CPUs.

Authentication Methods

You can select one of the following authentication algorithms for each proposal. The algorithms are listed in order from weakest to strongest.

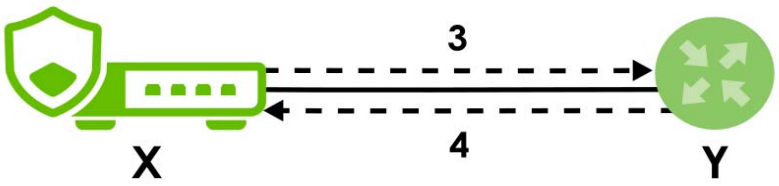
- MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
- SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
- SHA256 (Secure Hash Algorithm) produces a 256-bit digest to authenticate packet data.
- SHA384 (Secure Hash Algorithm) produces a 384-bit digest to authenticate packet data.
- SHA512 (Secure Hash Algorithm) produces a 512-bit digest to authenticate packet data.
- PRF (PseudoRandom Function)-SHA256/384/512 does not encrypt data, but derives keys, authenticates handshake messages and produces strong session keys from initial secrets. It is not used to encrypt or authenticate the VPN data when AES-GCM is the encryption method; it is used to generate the keys that AES-GCM will use.

See Diffie-Hellman (DH) Groups on page 223 for more information about DH key groups.

Diffie-Hellman (DH) Groups

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 165 IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange



Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. ECP (Elliptic Curve Cryptography Prime) and MODP (Modular Exponential) groups are used for the Diffie-Hellman (DH) key exchange protocol in establishing secure VPN tunnels. Higher Diffie-Hellman group numbers of the same algorithm (MODP, ECP NIST, ECP Brainpool) are usually more secure, but also require more processing power to encrypt and decrypt information.

The Zyxel Device supports these Diffie-Hellman groups in increasing order of strength (and required processing power) for each group:

MODP

1 Diffie-Hellman Group 2 (1024-bit)

2 Diffie-Hellman Group 5 (1536-bit)

3 Diffie-Hellman Group 14 (2048-bit)

4 Diffie-Hellman Group 15 (3072-bit)

5 Diffie-Hellman Group 16 (4096-bit)

ECP NIST (National Institute of Standards and Technology)

1 Diffie-Hellman Group 19 (256-bit random)

2 Diffie-Hellman Group 20 (384-bit random)

3 Diffie-Hellman Group 21 (521-bit random)

ECP Brainpool

1 Diffie-Hellman Group 28 (256bp-bit Brainpool elliptic curve group)

2 Diffie-Hellman Group 29 (384bp-bit Brainpool elliptic curve group)

3 Diffie-Hellman Group 30 (512bp-bit Brainpool elliptic curve group)

CFRG (Crypto Forum Research Group)

1 Diffie-Hellman Group 31 (Curve25519 / X25519)

2 Diffie-Hellman Group 32 (Curve448 / X448)

Security strength depends on the DH group as well as the DH group number. The following table lists DH groups by number, not by strength.

Table 104 DH Groups

DH GROUP	CURVE / PRIME	APPROX. SECURITY LEVEL
2	MODP 1024	~80-bit
5	MODP 1536	~96-bit
14	MODP 2048	~112-bit
15	MODP 3072	~128-bit
16	MODP 4096	~152-bit
19	NIST P-256 (secp256r1)	~128-bit
20	NIST P-384 (secp384r1)	~192-bit
21	NIST P-521 (secp521r1)	~256-bit
28	Brainpool ECP group (brainpoolP256r1)	~128-bit
29	Brainpool ECP group (brainpoolP384r1)	~192-bit
30	Brainpool ECP group (brainpoolP512r1)	~256-bit
31	Curve25519 (X25519)	~128-bit
32	Curve448 (X448)	~224-bit

Note: Make sure that both ends of the VPN tunnel use the same DH group number.

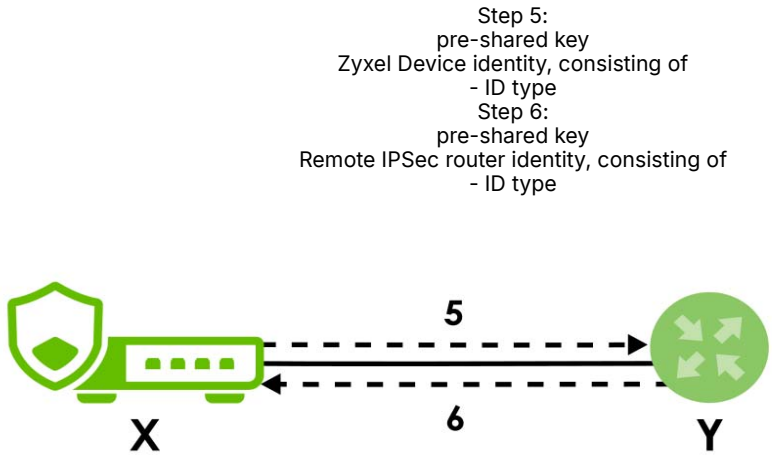
As a guideline, for legacy systems where compatibility is needed, use MODP, such as DH Group 14 or DH Group 15.

Identity Verification

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 166 IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication (continued)



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. The ID type can be 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 refers to the content that applies to the router itself, and remote ID type refers to the content that applies to the other router.

Note: The Zyxel Device's local and remote ID content must match the remote IPSec router's remote and local ID 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 105 VPN Example: Matching ID Type and Content

ZYXEL DEVICE	REMOTE IPSEC ROUTER
Local ID type: tom@youroffice.com	Local ID type: 1.1.1.2
Peer ID type: 1.1.1.2	Peer ID type: tom@youroffice.com

Table 106 VPN Example: Mismatching ID Type and Content

ZYXEL DEVICE	REMOTE IPSEC ROUTER
Local ID type: tom@youroffice.com	Local ID type: 1.1.1.2
Peer ID type: 1.1.1.20	Peer ID type: tom@youroffice.com

It is also possible to configure the Zyxel Device to ignore the identity of the remote IPSec router. In this case, you usually leave the remote ID type field empty. 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.

13.2.2 Additional Topics for IKE SA

This section provides more information about IKE SA.

Negotiation Mode

There are two negotiation modes for IKEv1--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.

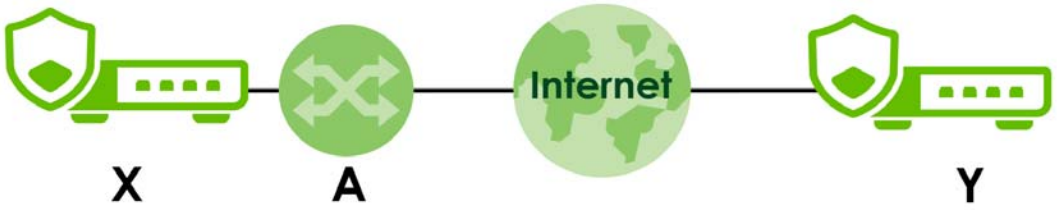
Steps 5 - 6: Finally, the Zyxel Device and the remote IPSec router generate an encryption key (from the shared secret), encrypt their identities, and exchange their encrypted identity information for authentication.

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 167 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 228 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.

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.

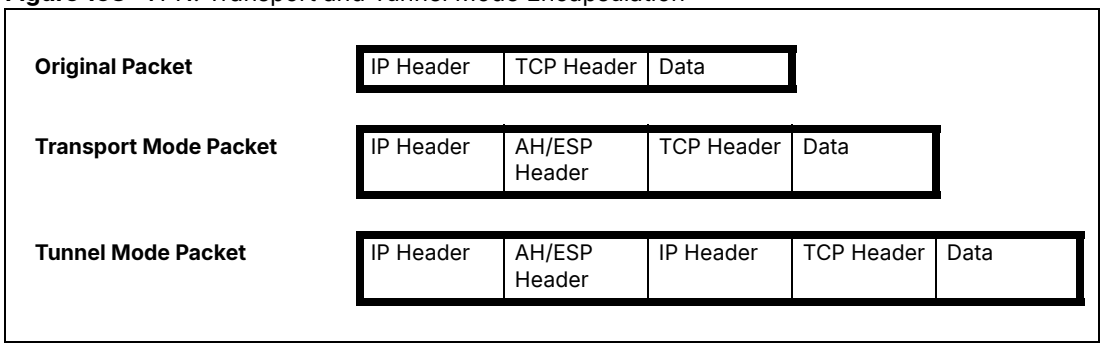
Encapsulation

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 168 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.

13.2.3 Recommended VPN Algorithm Table

IKEv1

Table 107 Recommendations for IKEv1

PHASE	PARAMETER	RECOMMENDED (STRONG)	NOTES
Phase 1 (IKE SA)	DH Group	19 (P-256) or 21 (P-521)	Elliptic Curve DH is faster and strong
	Encryption	AES256	AES256 with SHA256
	Integrity / Authentication	SHA256	
	Lifetime	28800 sec	Standard, can reduce for highly dynamic peers
Phase 2 (Child SA / IPsec ESP)	Encryption	AES256-GCM	AEAD mode handles both encryption & integrity
	Integrity	Not required if using AES-GCM	Optional SHA256/SHA384 if using plain AES
	PFS DH Group	19 or 21	Recommended, especially for sensitive traffic
	Lifetime	3600–28800 sec	Typical, adjust per policy

IKEv2

Table 108 Recommendations for IKEv2

PHASE	PARAMETER	RECOMMENDED (STRONG)	NOTES
Phase 1 (IKE SA)	DH Group	19 (P-256) or 21 (P-521)	Elliptic Curve DH is faster and strong
	Encryption	AES256-GCM (preferred AEAD)	If AES-GCM not available, AES256 with SHA256
	Integrity / Authentication	PRF-SHA256	PRF required for key derivation
	Lifetime	28800 sec	Standard, can reduce for highly dynamic peers
Phase 2 (Child SA / IPsec ESP)	Encryption	AES256-GCM	AEAD mode handles both encryption & integrity
	Integrity	Not required if using AES-GCM	Optional SHA256/SHA384 if using plain AES
	PFS DH Group	19 or 21	Recommended, especially for sensitive traffic
	Lifetime	3600–28800 sec	Typical, adjust per policy

Additional Recommendation Notes

- Choose AES-GCM for encryption and integrity.
- Use strong DH groups (14+ for traditional, 19+ for elliptic curve).
- Avoid legacy algorithms: DES, 3DES, MD5, SHA1.
- PRF-SHA256 (or higher) is mandatory for IKEv2 key derivation.
- Phase 2 Perfect Forward Secrecy should use strong DH groups.

13.2.4 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.

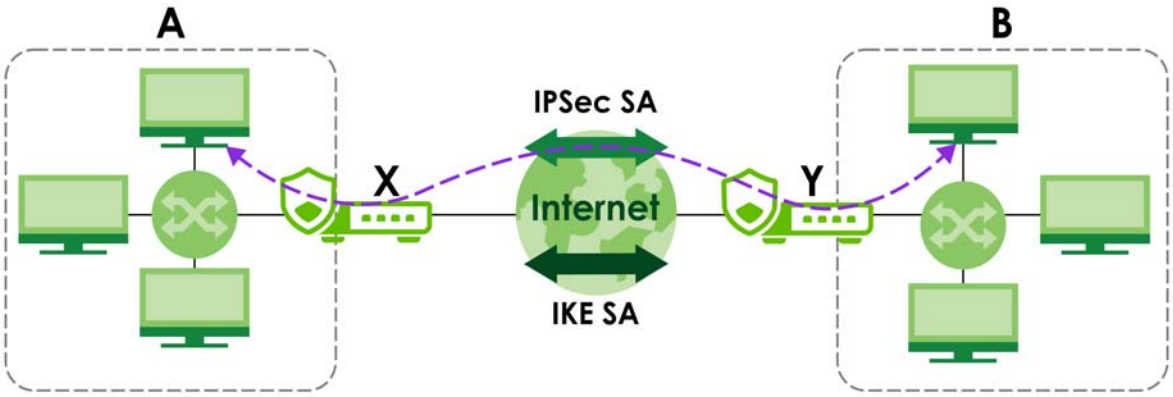
13.2.5 What You Can Do in this Chapter

- Use the **Site to Site VPN** screen (see Section 13.3 on page 232) to view a summary of the VPN rules.
- Use the **Site to Site VPN Add/Edit** screens (see Section 13.3.1 on page 233 and Section 13.3.1 on page 233) to create a VPN rule using the wizard or create a customized VPN rule with advanced settings.
- Use the **Remote Access VPN** screen (see Section 13.4 on page 248) to create a remote access VPN rule.

13.2.6 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 169 VPN: IKE SA and IPSec SA

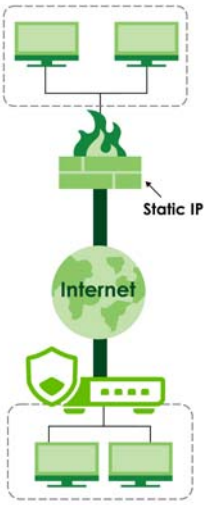
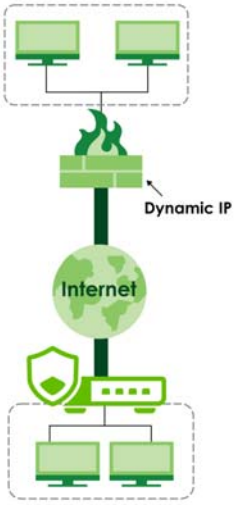


In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, 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.

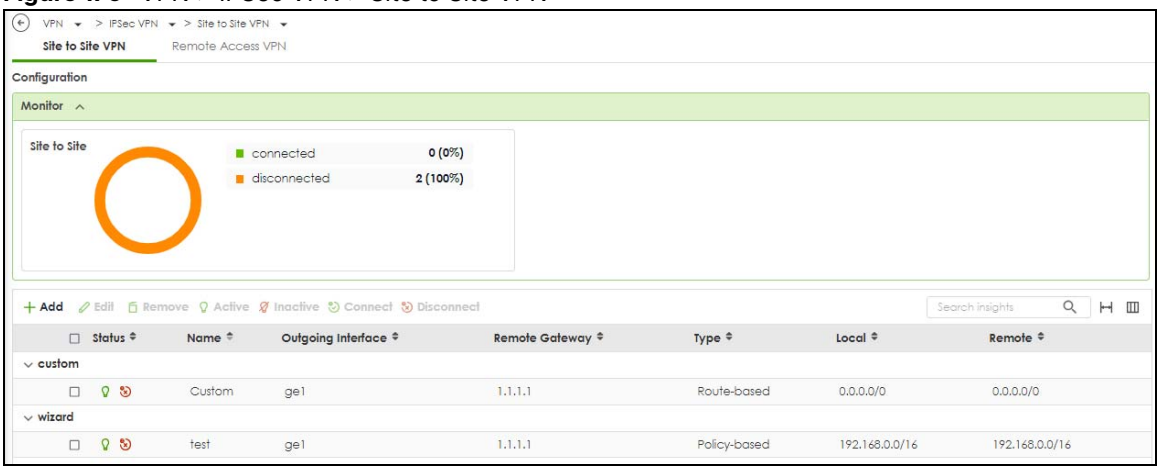
Table 109 IPSec VPN Application Scenarios

SITE-TO-SITE	SITE-TO-SITE WITH DYNAMIC PEER
	
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.

13.3 The Site to Site VPN Screen

Click **VPN > IPSec VPN > Site to Site VPN** to open the **Site to Site VPN** screen. The **Site to Site VPN** screen lists the VPN connection associated VPN gateway(s), and various settings. In addition, it also lets you activate or deactivate and connect or disconnect each VPN connection (each IPSec SA). Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 170 VPN > IPSec VPN > Site to Site VPN



Each field is discussed in the following table.

Table 110 VPN > IPSec VPN > Site to Site VPN

LABEL	DESCRIPTION
Monitor	The graph shows the number of connected and disconnected VPNs.
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.
Active	To turn on an entry, select it and click **Activate**.
Inactive	To turn off an entry, select it and click **Inactivate**.
Connect	To connect an IPSec SA, select it and click **Connect**.
Disconnect	To disconnect an IPSec SA, select it and click **Disconnect**.
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 VPN rule.
Outgoing Interface	This field displays the interface IP address or DNS name the VPN connection uses to transmit packets.
Remote Gateway	This field displays the remote IPSec device IP address or DNS name in use for this VPN connection.
Type	This field displays the type (route based or policy based) the VPN rule is using.
Type	This field displays if the VPN rule is configured through wizard or a customized rule.
Local	This field displays the IP address of the computer on your network. Hover over this field to view the object details.
Remote	This field displays the IP address of the computer behind the remote IPSec device. Hover over this field to view the object details.

13.3.1 The Site to Site VPN Add/Edit Screen- Wizard

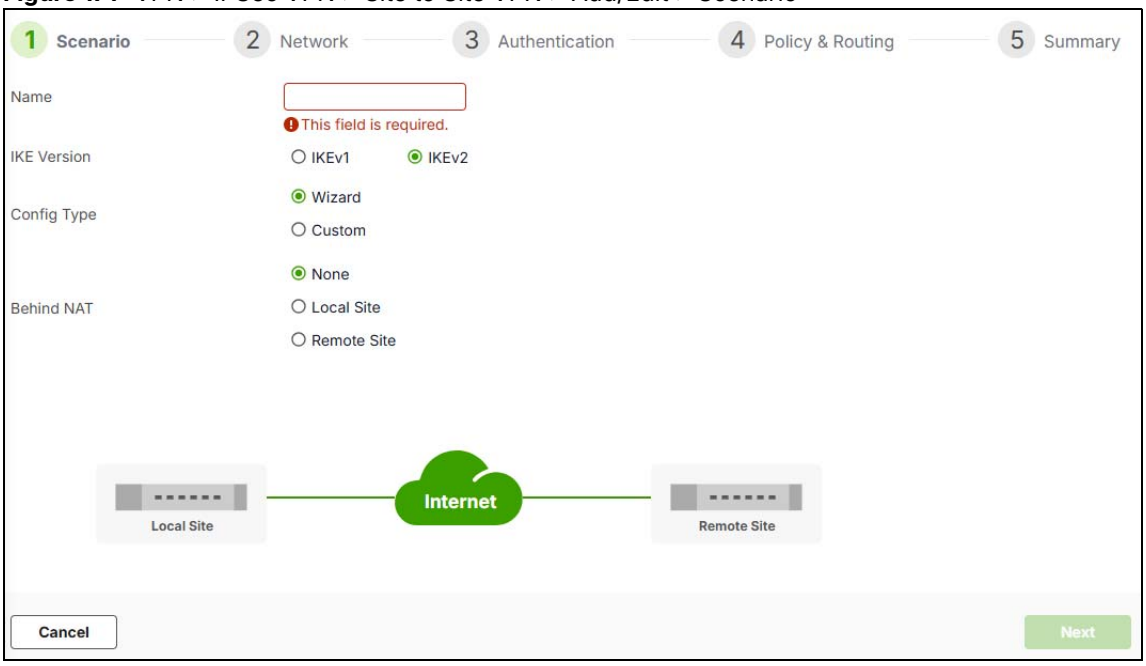
The **Site to Site VPN Add/Edit Gateway** screen allows you to create a new VPN connection policy or edit an existing one. To access this screen, go to the **VPN > IPSec VPN > Site to Site VPN** screen, and click

either the **Add** icon or an **Edit** icon. Select **Site-to-Site** in **VPN > IPSec VPN > Site to Site VPN > Add/Edit > Scenario > Type** to create a VPN rule using the wizard.

13.3.1.1 Scenario

Use this screen to configure the VPN connection name and select the scenario that best describes your intended VPN connection.

Figure 171 VPN > IPSec VPN > Site to Site VPN > Add/Edit > Scenario



Each field is described in the following table.

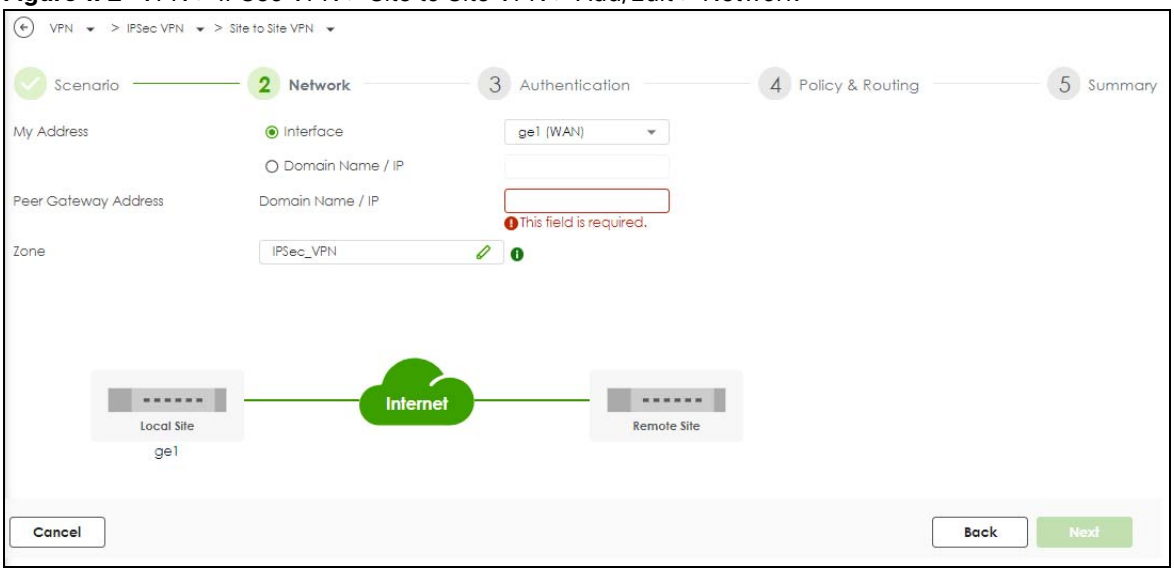
Table 111 VPN > IPSec VPN > Site-to-Site VPN > Add/Edit > Scenario

LABEL	DESCRIPTION
Name	Type the name used to identify this rule. You may use 1-31 single-byte characters, including 0-9a-zA-Z, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
IKE Version	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 13.1 on page 220 for more information on IKEv1 and IKEv2.
Type	Select **Wizard** to configure the VPN rule using the wizard. Select **Custom** to configure the VPN rule with customized settings.
Behind NAT	**None**/ **Local Site**: The remote IPSec device has a static IP address or a domain name. This Zyxel Device can initiate the VPN tunnel. **Remote Site**: The remote IPSec device has a dynamic IP address. Only the remote IPSec device can initiate the VPN tunnel.

13.3.1.2 Network

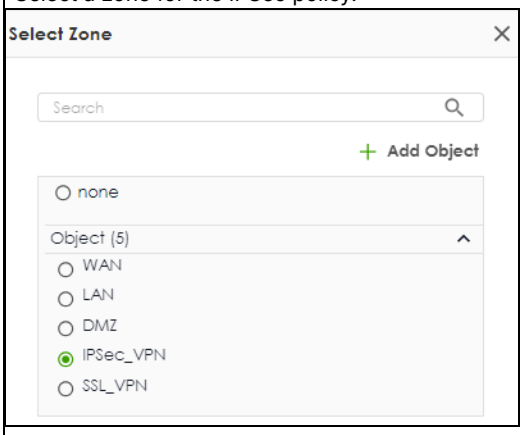
Use this screen to configure the Zyxel Device interface and remote IPSec device settings.

Figure 172 VPN > IPSec VPN > Site to Site VPN > Add/Edit > Network



Each field is described in the following table.

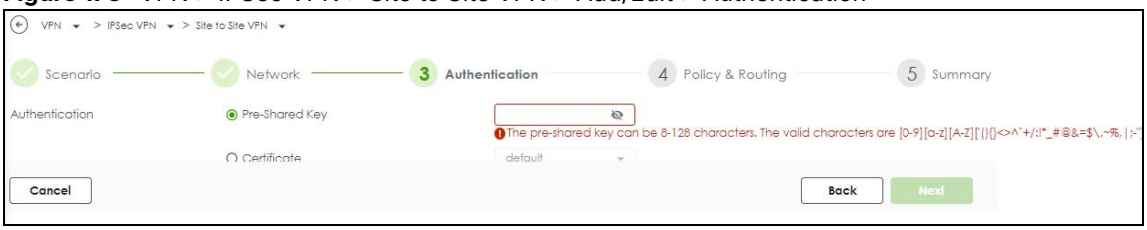
Table 112 VPN > IPSec VPN > Site-to-Site VPN > Add/Edit > Network

LABEL	DESCRIPTION
My Address	Select an interface or enter the IPv4 address or domain name of the interface the VPN connection uses to transmit packets out of the Zyxel Device.
Peer Gateway Address	Enter the WAN IPv4 address or domain name of the remote IPSec device to identify the remote IPSec router by its IP address or domain name.
Zone	Select a zone for the IPSec policy.  Go to **Security Policy > Policy Control** to make sure that a security policy will not block traffic going to the zone you select.

13.3.1.3 Authentication

Use this screen to configure the authentication type and settings.

Figure 173 VPN > IPSec VPN > Site to Site VPN > Add/Edit > Authentication



Each field is described in the following table.

Table 113 VPN > IPSec VPN > Site-to-Site VPN > Add/Edit > Authentication

LABEL	DESCRIPTION
Pre-Shared Key	Select this to have the Zyxel Device and remote IPSec router use a pre-shared key 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: • Plain text: 8 to 128 characters using [0-9][a-z][A-Z], and the special characters ['(){}<>^`+/:!*_#@&?=$\.~%,|;-"]. • Hexadecimal: Begin with 0x, followed by 16 to 256 hexadecimal digits [0-9][a-f][A-F]. The Zyxel Device and remote IPSec router must use the same pre-shared key. Click the eye icon to see the pre-shared key in readable plain text.
Certificate	Alternatively, select **Certificate** to use one of the Zyxel Device certificates for authentication.

13.3.1.4 Policy & Routing

Use this screen to configure the IP addresses of the computer on your network and the computer behind the remote IPSec device.

Figure 174 VPN > IPSec VPN > Site to Site VPN > Add/Edit > Policy & Routing (Route-Based)

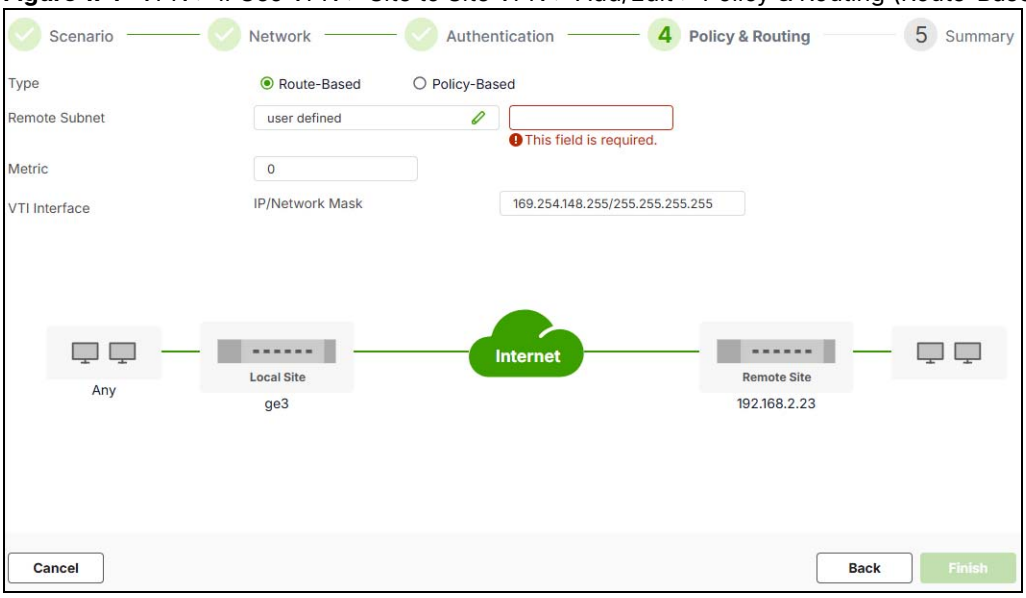
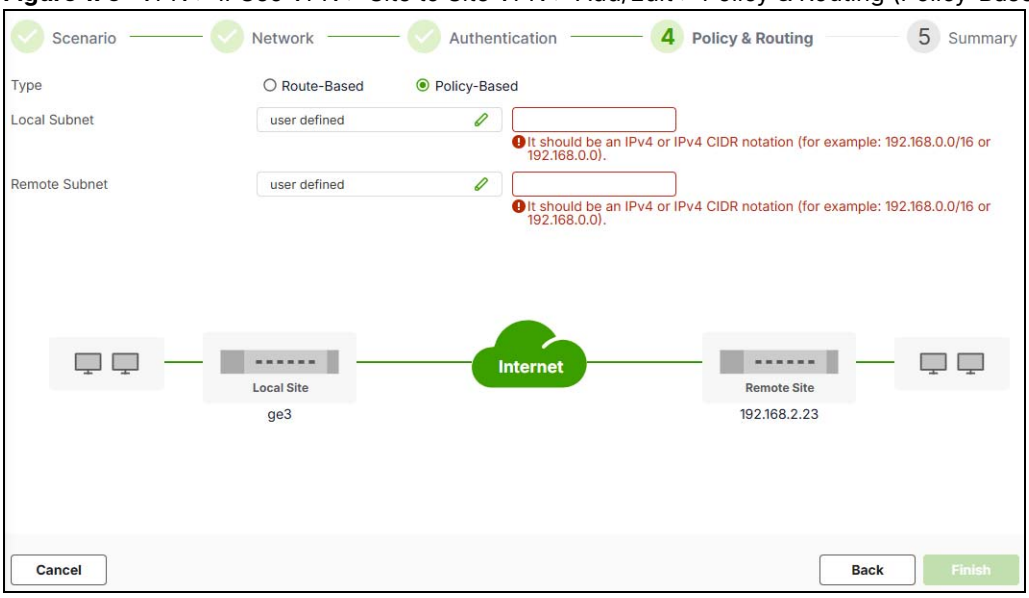


Figure 175 VPN > IPSec VPN > Site to Site VPN > Add/Edit > Policy & Routing (Policy-Based)



Each field is described in the following table.

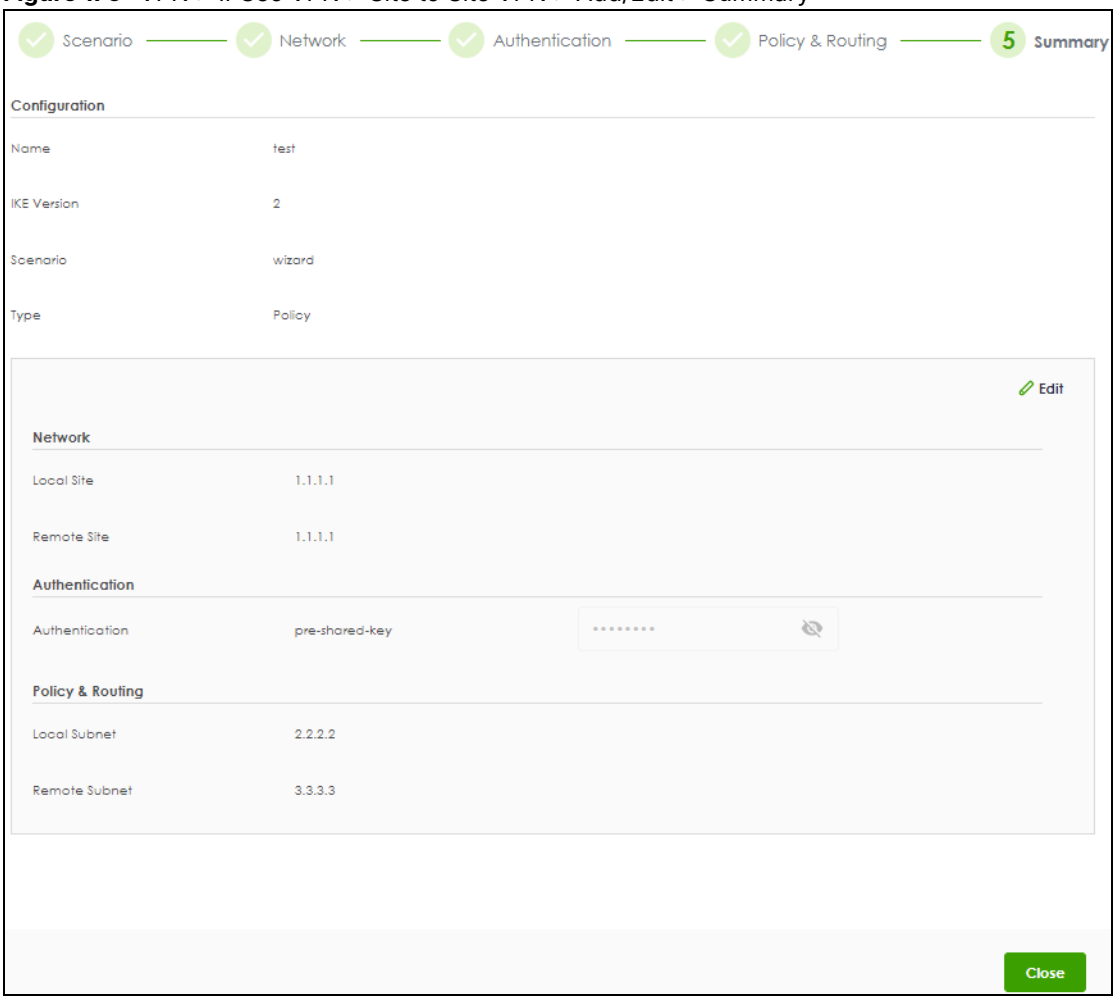
Table 114 VPN > IPSec VPN > Site-to-Site VPN > Add/Edit > Policy & Routing

LABEL	DESCRIPTION
Type	Select **Route-Based** to create a VPN rule that encrypts traffic based on the static route settings. Select **Policy-Based** to create a VPN rule that encrypts traffic based on the IPv4 addresses you set in **Local Subnet** and **Remote Subnet**.
Local Subnet	This field displays when you select **Policy-Based** in the **Type** field. Type the IP address of a computer on your network that can use the tunnel. You can also specify a subnet or an interface subnet. This must match the remote IP address configured on the remote IPSec device.
Remote Subnet	Type the IP address of a computer behind the remote IPSec device. You can also specify a subnet or an interface subnet. This must match the local IP address configured on the remote IPSec device.
Metric	This field displays when you select **Route-Based** in the **Type** field. Type the number for the priority of the route. A lower value indicates higher priority. 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.
VTI Interface	This field displays when you select **Route-Based** in the **Type** field. Type the IP address and subnet mask of the virtual interface to use for the tunnel.

13.3.1.5 Summary

Use this screen to view a summary of the VPN tunnel configurations. You can click **Edit** to change the VPN tunnel configuration settings.

Figure 176 VPN > IPSec VPN > Site to Site VPN > Add/Edit > Summary

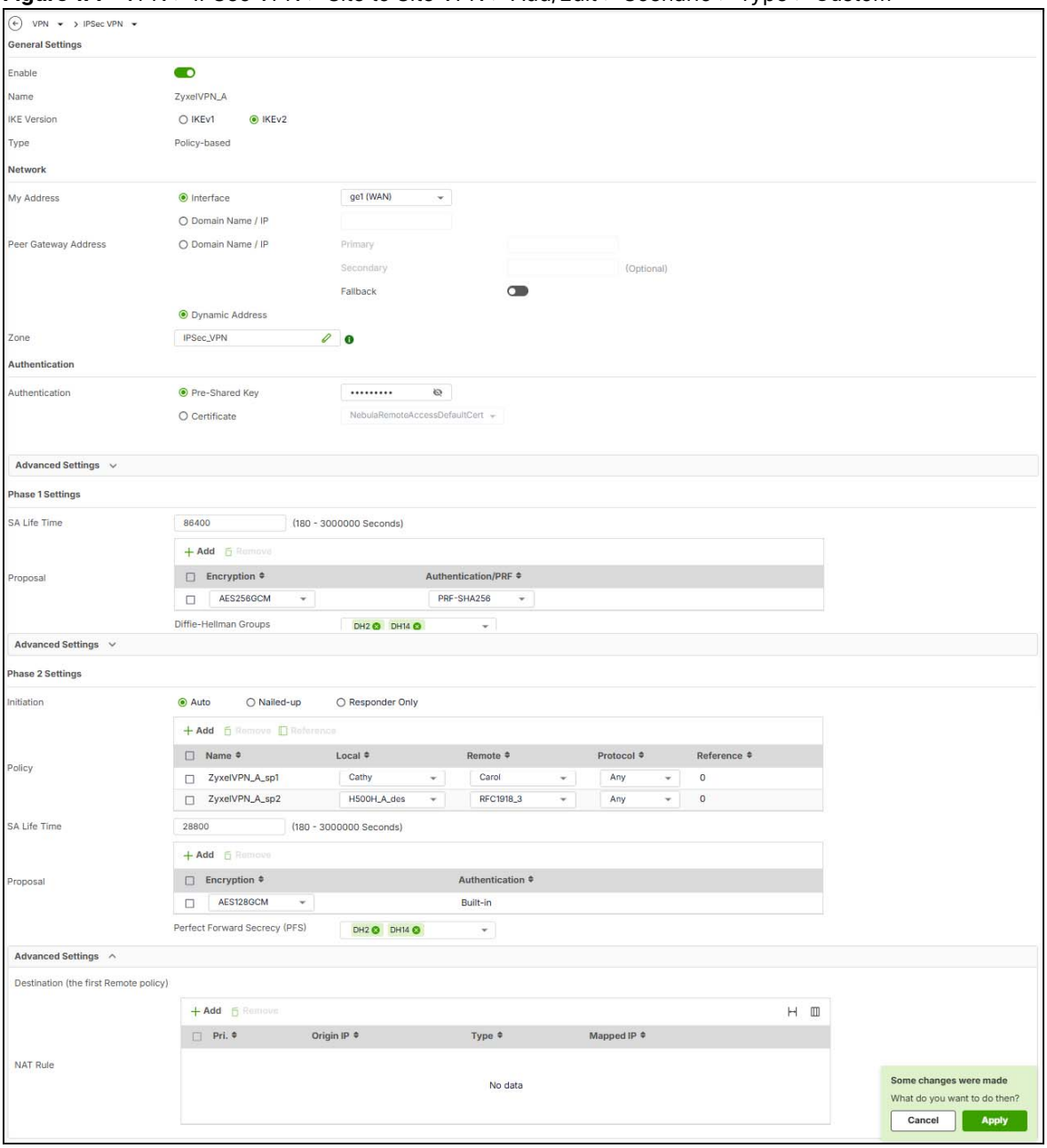


13.3.2 The Site to Site VPN Add/Edit Screen - Custom

The **Site to Site VPN 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 **VPN > IPSec VPN > Site to Site VPN** screen, and click either the **Add** icon or an **Edit** icon. Select **Custom** in **VPN > IPSec VPN > Site to Site VPN> Add/Edit > Scenario > Type** to create a customized VPN rule with advanced settings.

See Section 13.1 on page 220 for more information on phase 1 and phase 2 settings; see Section 13.2 on page 221 for more information on IKE SA proposals.

Figure 177 VPN > IPSec VPN > Site to Site VPN > Add/Edit > Scenario > Type > Custom



Each field is described in the following table.

Table 115 VPN > IPSec VPN > Site-to-Site VPN > Add/Edit > Scenario > Type > Custom

LABEL	DESCRIPTION
General Settings	
Enable	Slide the switch to the right to activate this VPN connection
Name	Type the name used to identify this rule. You may use 1-31 single-byte characters, including 0-9a-zA-Z, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

Table 115 VPN > IPSec VPN > Site-to-Site VPN > Add/Edit > Scenario > Type > Custom (continued)

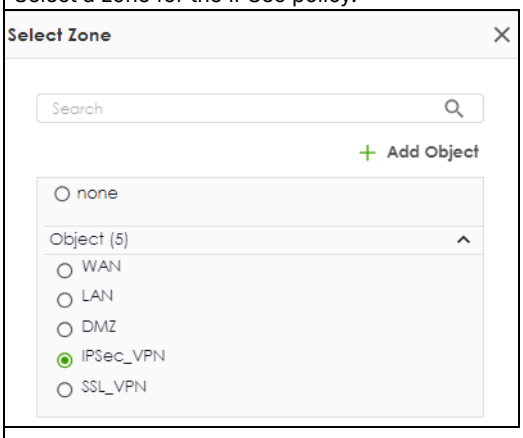
LABEL	DESCRIPTION
IKE Version	Select IKEv1 or IKEv2. IKEv1 applies to IPv4 traffic only. IKEv2 applies to both IPv4 and IPv6 traffic. IKE (Internet Key Exchange) is a protocol used in setting up security associations that allows two parties to send data securely. See Section 13.1 on page 220 for more information on IKEv1 and IKEv2.
Type	Select **Route-Based** to create a VPN rule that encrypts traffic based on the static route settings. Select **Policy-Based** to create a VPN rule that encrypts traffic based on the **Local** and **Remote** IPv4 addresses you set in **Policy** in **Phase 2 Settings**.
Network	
My Address	Select or search for an existing **Interface** on the Zyxel Device that will use this tunnel. Select **Domain Name/IP** to enter the IP address or FQDN of a computer on your network that will use the tunnel. This must match the remote IP address configured on the remote IPSec device.
Peer Gateway Address	Select **Domain Name/IP** to enter the domain name or the IP address of the remote IPSec router. Select **Dynamic Address** if the remote IPSec router has a dynamic IP address (and does not use DDNS).
Primary	Enter the domain name or the IP address of the remote IPSec router.
Secondary	Use this field to configure a backup peer IPSec router. • Enter the domain name or IP address of the backup remote IPSec router. When the primary peer IPSec router becomes unavailable, the Zyxel Device reconnects the tunnel to this secondary peer IPSec router. • Leave this field blank if you do not set up a secondary peer IPSec router for failover.
Fallback	Select this option to have the Zyxel Device automatically reconnect to the primary peer IPSec router when it becomes available again. Once reconnected to the primary IPSec router, the Zyxel Device stops the connection with the secondary peer IPSec router.
Check Interval	Enter the number of seconds (30–300) to define how often the Zyxel Device checks if the primary peer IPSec router is available.
Zone	Select a zone for the IPSec policy.  Go to **Security Policy > Policy Control** to make sure that a security policy will not block traffic going to the zone you select.
Authentication	

Table 115 VPN > IPSec VPN > Site-to-Site VPN > Add/Edit > Scenario > Type > Custom (continued)

LABEL	DESCRIPTION
Pre-Shared Key	Select this to have the Zyxel Device and remote IPSec router use a pre-shared key 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 characters in plain text format using [0-9][a-z][A-Z]['(){}<>^`+/ :!*_#@&?=$\.~%,|;-"] • 16 to 256 characters in 0x hexadecimal format using [0-9][A-F] The Zyxel Device and remote IPSec router must use the same pre-shared key. Click the eye to see the pre-shared key in readable plain text.
Certificate	Alternatively, select **Certificate** to use one of the Zyxel Device certificates for authentication.
Advanced Settings	
Local ID	Enter one of the followings to identify the Zyxel Device during authentication. **IPv4** - 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
Remote ID	Enter one of the followings to identify the remote IPSec router during authentication. **IPv4** - 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 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
Phase 1 Settings	This establishes a secure tunnel between the Zyxel Device and the peer site.
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. The value you set for the SA life time in **Phase 1 Settings** should be greater than or equal to the value you set for the SA life time in **Phase 2 Settings**.
Add	Click this to add an entry.
Edit	Select an entry and click this to edit the entry.
Remove	Select an entry and click this to remove the entry.
Proposal	

Table 115 VPN > IPSec VPN > Site-to-Site VPN > Add/Edit > Scenario > Type > Custom (continued)

LABEL	DESCRIPTION
Encryption	Select or search for an existing encryption algorithm to use in this IPSec SA. Choose an encryption method according to the security strength you need, CPU performance available, and compatibility with peer devices. Choose **AES** if you're using **IKEv1** or you need a legacy mode for compatibility with peer devices. Choose **AES-GCM** (Galois/Counter Mode) if you're using **IKEv2**, as it offers secure (prevents both passive eavesdropping and active tampering), authenticated encryption that is faster than AES as it is optimized for modern CPUs. For key length, 128-bit is strong enough for today, 192-bit is better, and choose 256-bit if the VPN is handling top-secret information or you want to future proof decryption threats such as with quantum computing. Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput. 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 • **AES128-GCM** - a 128-bit key with the Galois/Counter Mode (GCM) encryption algorithm • **AES192-GCM** - a 192-bit key with the Galois/Counter Mode (GCM) encryption algorithm • **AES256-GCM** - a 256-bit key with the Galois/Counter Mode (GCM) 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.
Authentication	Select which hash algorithm to use to authenticate packet data in the IPSec SA. SHA is generally considered stronger than **MD5**, but it is also slower. Choices with DES or AES **Encryption** are: • **MD5** • **SHA1** • **SHA256** • **SHA384** • **SHA512** PRF (PseudoRandom Function)-SHA does not encrypt data, but derives keys, authenticates handshake messages and produces strong session keys from initial secrets. It is not used to encrypt or authenticate the VPN data when AES-GCM is the encryption method; it is used to generate the keys that AES-GCM will use. Choices with AES-GCM **Encryption** are: • **PRF-MD5** • **PRF-SHA1** • **PRF-SHA256** • **PRF-SHA384** • **PRF-SHA512.** The Zyxel Device and the remote IPSec router must both have a proposal that uses the same authentication algorithm.

Table 115 VPN > IPSec VPN > Site-to-Site VPN > Add/Edit > Scenario > Type > Custom (continued)

LABEL	DESCRIPTION
Diffie-Hellman Groups	Select which Diffie-Hellman key group (DH*x*) you want to use to create encryption keys. Choices are **DH2, DH5, DH14, DH15, DH16, DH19, DH20, DH21, DH28, DH29, DH30, DH 31** and **DH32.** The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. The Zyxel Device and the remote IPSec router must use the same DH key group. See Section 13.2 on page 221 for more information on DH key group.
Advanced Settings	
DPD Delay	Configure this field 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 Dead Peer Detection (DPD). Set how many seconds the Zyxel Device will wait before sending a message to the remote IPSec router it there has been no traffic. 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. This field applies for IKEv1 only. DPD is always performed when you use IKEv2.
UDP Encapsulation	Enable to encrypt a UDP connection.
Phase 2 Settings	This secures the actual data transmission between the Zyxel Device and the peer site, based on the secure key settings established in Phase 1.
Initiation	Select how Phase 2 of the IPSec connection is established on the Zyxel Device. **Auto**: Select this to have the Zyxel Device listen for incoming traffic and automatically establish the Phase 2 of the IPSec connection when traffic is detected. **Nailed-Up**: Select this to have the Zyxel Device initiate Phase 2 of the IPSec connection. The Zyxel Device automatically renegotiates the IPSec SA when the SA lifetime expires, ensuring the continuity of the connection. **Responder Only**: Select this to have the Zyxel Device wait for the peer site to initiate the Phase 2 of the IPSec connection.
Policy	
Add	Click this to add an entry.
Remove	Select an entry and click this to remove the entry. This is grayed out if a rule is currently using the selected entry.
Reference	Select an entry and click this to see which rules are currently using it. This is grayed out if no rule is currently using the selected entry.
Name	This field displays the name of the entry. When you add a new entry, a name is automatically generated based on this VPN connection policy name, followed by _sp1. Adding another entry will use _sp2, and so on. For example, if the VPN connection policy is named VPN1, adding a new entry will display the name as VPN1_sp1. You can also manually change the name.

Table 115 VPN > IPSec VPN > Site-to-Site VPN > Add/Edit > Scenario > Type > Custom (continued)

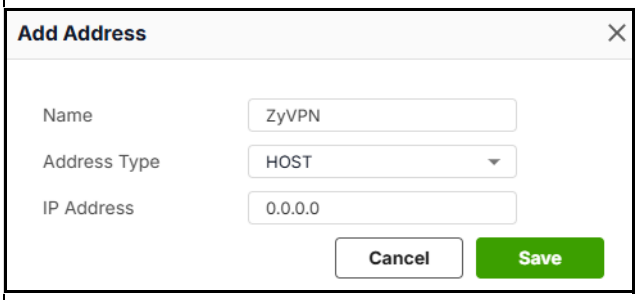
LABEL	DESCRIPTION
Local / Remote	**Local**: Select or search for an existing IP address object that the Zyxel Device uses to send traffic through the VPN tunnel to the peer site. **Remote**: Select or search for an existing IP address object of the peer site to which the Zyxel Device sends traffic through the VPN tunnel. Choose an object you already created or click **User Defined** to specify the IP address directly. To create an object, click **Add Object**.  • **Name**: Enter the name of this object. It must begin with a letter and cannot exceed 31 characters. The valid characters are A-Z, a-z, 0-9, underscores (_), dashes (-), and dots (.). Spaces are not allowed. • **Address Type**: Select the address type of this object from the drop-down list. • **IP Address**: Enter the IP address of the object. • **Network**: Enter an IPv4 address in CIDR notation, for example, 192.168.1.1/24. • **Netmask**: This field displays the subnet mask depends on the **Network** you entered. • **Interface:** Select one of the Zyxel Device's interfaces. • **Cancel**: Click **Cancel** to close the window with changes unsaved. • **Save**: Click **Save** to save the entry.
Protocol	Select the protocol required to use this translation. Choices are: **TCP**, **UDP**, **ICMP**, **GRE** or **Any**.
Reference	This displays the number of rules that currently use this entry.
SA Life Time	Set how often the Zyxel Device renegotiates the IPSec SA. A short SA life time increases security, but renegotiation temporarily disconnects the VPN tunnel. The value you set for the SA life time in **Phase 2 Settings** should be lesser than or equal to the value you set for the SA life time in **Phase 1 Settings**.
Proposal	
Add	Click this to add an entry.
Remove	Select an entry and click this to remove the entry. This will not display if a rule is currently using the entry.

Table 115 VPN > IPSec VPN > Site-to-Site VPN > Add/Edit > Scenario > Type > Custom (continued)

LABEL	DESCRIPTION
Encryption	Select or search for an encryption algorithm to use in the IPSec SA. Choose an encryption method according to the security strength you need, CPU performance available, and compatibility with peer devices. Choose **AES** if you're using **IKEv1** or you need a legacy mode for compatibility with peer devices. Choose **AES-GCM** (Galois/Counter Mode) if you're using **IKEv2**, as it offers secure (prevents both passive eavesdropping and active tampering), authenticated encryption that is faster than AES as it is optimized for modern CPUs. For key length, 128-bit is strong enough for today, 192-bit is better, and choose 256-bit if the VPN is handling top-secret information or you want to future proof decryption threats such as with quantum computing. Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput. 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 • **AES128-GCM** - a 128-bit key with the Galois/Counter Mode (GCM) encryption algorithm • **AES192-GCM** - a 192-bit key with the Galois/Counter Mode (GCM) encryption algorithm • **AES256-GCM** - a 256-bit key with the Galois/Counter Mode (GCM) 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.
Authentication	Select which hash algorithm to use to authenticate packet data in the IPSec SA. SHA is generally considered stronger than **MD5**, but it is also slower. Choices with DES or AES **Encryption** are: • **MD5** • **SHA1** • **SHA256** • **SHA384** • **SHA512** Choices with AES-GCM **Encryption** are: • **Built-in** - this displays in Phase 2 to indicate that the Zyxel Device performs authentication using a **PRF (PseudoRandom Function).** The Zyxel Device and the remote IPSec router must both have a proposal that uses the same authentication algorithm.
Perfect Forward Secrecy (PFS)	Select which Perfect Forward Secrecy (PFS) you want to use to create encryption keys. Choices are **DH2, DH5, DH14, DH15, DH16, DH19, DH20, DH21, DH28, DH29, DH30, DH 31, DH32.** The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. The Zyxel Device and the remote IPSec router must use the same DH key group. See Section 13.2 on page 221 for more information on DH key group.
Advanced Settings	
NAT Rule	This is available if the VPN type is **Policy-based**.
Add	Click this to add an entry.
Remove	Select an entry and click this to remove the entry.

Table 115 VPN > IPSec VPN > Site-to-Site VPN > Add/Edit > Scenario > Type > Custom (continued)

LABEL	DESCRIPTION
Pri.	Select the priority for the entry. The smaller the number, the higher the priority.
Origin IP	Select or search for an existing IP address object that represents the originating source IP address for outgoing traffic, or the destination IP address from the sender that is mapped to the local IP address of the receiver (DNAT). You may also create a new IP address or IP address object.
Type	**SNAT:** Select this when there are no overlapping local and remote VPN IP addresses. **1:1 NAT:** Select this to avoid overlapping local and remote VPN IP addresses. The peer IPSec router must create identical mirror configurations.
Mapped IP	Use this field to map the sender's source IP address or subnet for the VPN rule. • Select or search for an existing IP address object. • Create a new object by clicking **Add Object.** Enter an IP address or subnet in the local IP address range. The local IP address range must not conflict with the peer's local IP address range. In the peer IPSec router, the destination IP from the sender is mapped to the local IP address of the receiver (DNAT). • Enter an IP address by clicking **User Defined.** The IP address should be within the local IP address range. Note: When Type is 1:1 NAT, then Original IP and Mapped IP must have the same range (same total number of IPv4 address).
VTI Setting (You must select **Route-Based** in **Type** to display the VTI setting.)	
Local IP	Enter an IPv4 address for this connection. IPSec VPN Tunnel Interface (VTI) encrypts or decrypts IPv4 traffic from or to the interface according to the IP routing table.
Subnet Mask	Enter the subnet mask of the local networks behind the custom peer gateway.
Route Setting (You must select **Route-Based** in **Type** to display the Route setting.)	
Remote Subnet	
Add	Click this to add an entry.
Remove	Select an entry and click this to remove the entry.
Remote	Specify the destination IP addresses of the remote site that are routed through this VTI interface in a single CIDR format, for example, 192.168.10.0/24.
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.
Description	Enter a description to help identify this policy. You can use alphanumeric and ()+/ :=?!*#@$_%– characters, and it can be up to 512 characters long. The default description is 'IPSec VPN: xxx' where 'xxx' is VPN rule name.
Apply	Click **Apply** to save your settings to the Zyxel Device.
Cancel	Click **Cancel** to return to the profile summary page without saving any changes.

13.3.2.1 Policy-Based VPN NAT Advanced Scenarios

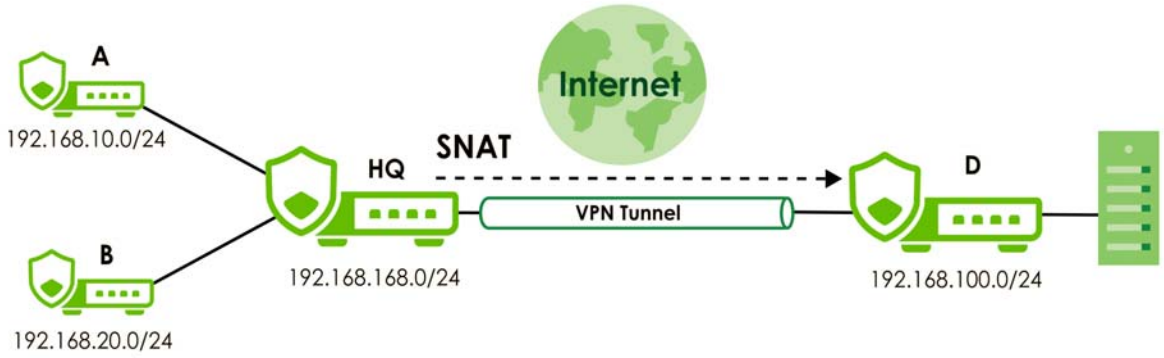
The following are application scenarios for SNAT and 1-1 NAT.

SNAT VPN Scenario

Here is an example of SNAT VPN scenario. Use this when there are no overlapping local and remote VPN IP addresses. Map the source IP address of the sender to an IP address in the Local IP address range (in the **Mapped IP** field) for the VPN rule. The headquarters (**HQ**) and branch sites **A** and **B** need to access the remote data center (**D**). The source IP addresses of sites **A** and **B** are not in the range of the local policy's

IP address (192.168.168.0/24) for Phase 2. NAT rules need to be configured to translate the source IP addresses of sites **A** and **B** to an IP address in the 192.168.168.0/24 range before entering the IPsec tunnel.

Figure 178 Policy Based VPN - SNAT Example Scenario



The administrator need to set up VPN policy on both sites.

Table 116 Phase 2 Local/Remote Policy Settings Example

LOCAL POLICY	REMOTE POLICY
192.168.168.0/24	192.168.100.0/24

Table 117 Phase 2 NAT Rule Settings Example

SITE	TYPE	ORIGIN IP	MAPPED IP
Site A	SNAT	192.168.10.0/24	192.168.168.11/32
Site B	SNAT	192.168.20.0/24	192.168.168.12/32

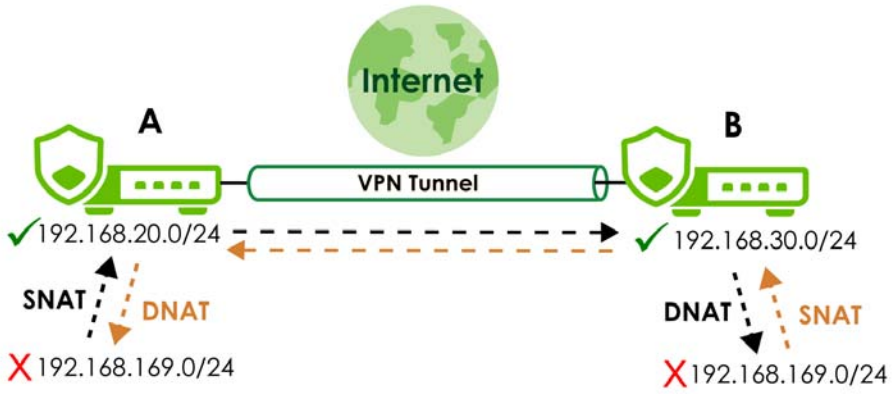
1-1 NAT VPN Scenario

Here is an example of a 1:1 NAT VPN scenario.Use this to avoid overlapping local and remote VPN IP addresses. IPSec router **A** and IPSec router **B** need to access each other, but they have overlapping subnets. To avoid conflicts, both IPSec routers need to create identical 1:1 NAT rules that map their local subnet to a non-overlapping subnet.

In the following example, IPSec router **A** is sending traffic to router **B**. Before data entering the VPN tunnel, the source IP address (set in **Origin IP**) from router **A** is translated to a mapped IP address (set in **Mapped IP**). After data exiting the VPN tunnel, router **B** translates the destination IP address (set in **Mapped IP**) back to the **Origin IP**.

Note: The **Mapped IP** of IPSec router **A** and **B** must not be in conflict.

Figure 179 Policy Based VPN - 1:1 NAT Example Scenario



The administrator need to set up VPN policy on both sites.

Table 118 Phase 2 Local/Remote Policy Settings Example

SITE	LOCAL POLICY	REMOTE POLICY
Site A	192.168.20.0/24	192.168.30.0/24
Site B	192.168.30.0/24	192.168.20.0/24

Table 119 Phase 2 NAT Rule Settings Example

SITE	TYPE	ORIGIN IP	MAPPED IP
Site A	1:1 NAT	192.168.169.0/24	192.168.20.0/24
Site B	1:1 NAT	192.168.169.0/24	192.168.30.0/24

13.4 The Remote Access VPN Screen

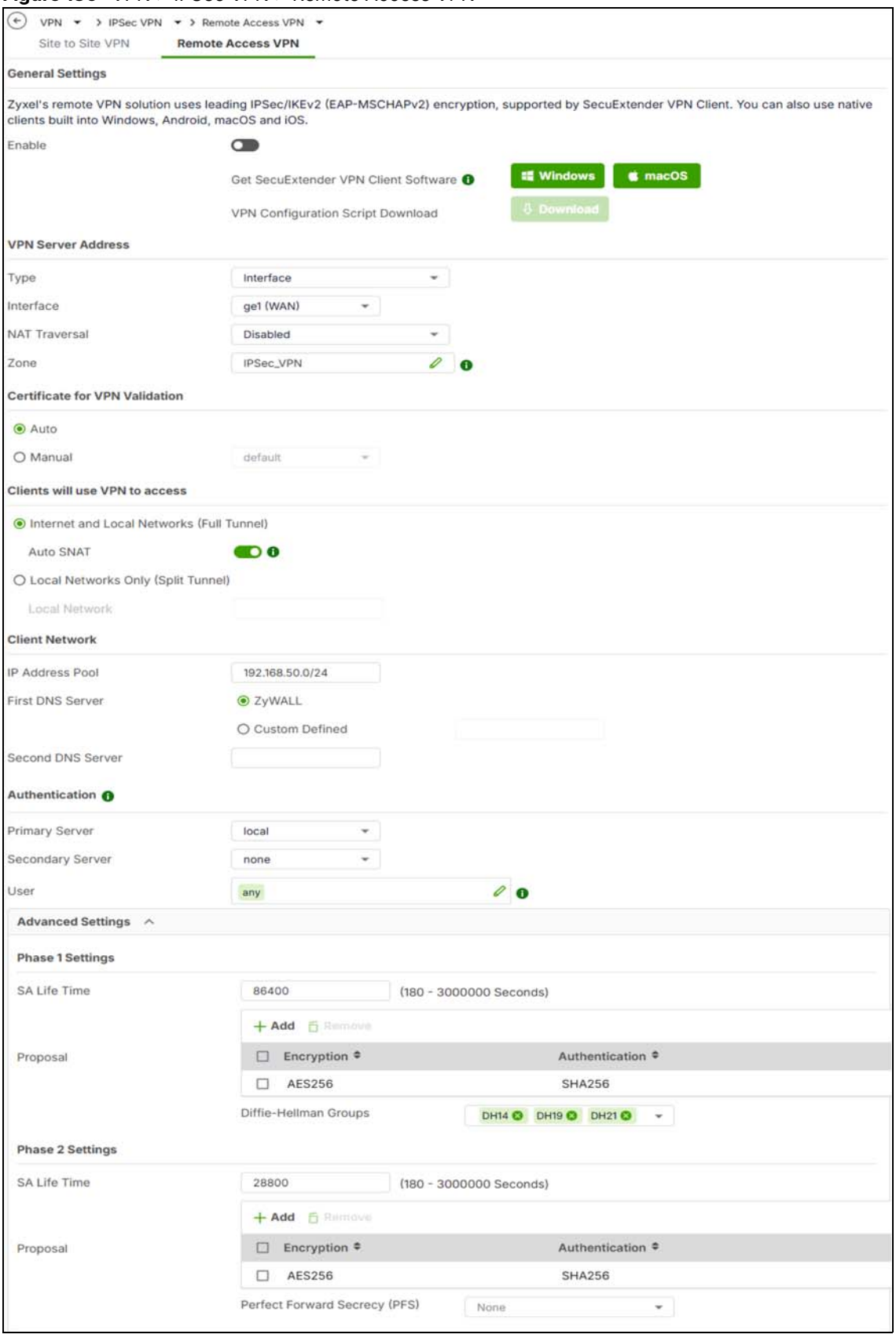
Configure the settings in this screen to create a new or edit an existing remote access VPN rule to securely access the Zyxel Device local networks from anywhere. See Section 13.1 on page 220 for more information on phase 1 and phase 2 settings; see Section 13.2 on page 221 for more information on IKE SA proposals.

SecuExtender is a Zyxel subscription-based VPN client. A remote access VPN client must have SecuExtender VPN client installed on his device and uses a supported computer operating system.

Make sure the settings configured on the IPSec VPN client matches the settings you configured on the Zyxel Device.

Click **VPN** > **IPSec VPN** > **Remote Access VPN** to open the following screen.

Figure 180 VPN > IPSec VPN > Remote Access VPN



The following table describes the labels in this screen.

Table 120 VPN > IPSec VPN > Remote Access VPN

LABEL	DESCRIPTION
Enable	Click the switch to enable the remote access VPN rule.
Get SecuExtender VPN Client Software	Click to download SecuExtender to your computer. The supported operating systems for SecuExtender are: • Windows 10 (64-bit) and later versions. • macOS 10.15 and later versions.
VPN configuration script Download	Click to download a VPN configuration script to send to clients using IPSec VPN clients built into the operating systems. To use the download script, the built-in IPSec VPN clients need to use the following operating systems: • Clients using Windows 7 and later, iOS and macOS built-in IPSec VPN clients can import the VPN configuration script to configure a remote access VPN rule automatically. Click the link to download the script and send it to them. • Clients using Android should download the latest version strongSwan VPN client, then import the script to configure a remote access VPN rule automatically. Click the link to download the script and send it to them. • Clients using built-in IPSec VPN clients earlier than Windows 7 cannot use the script. They must configure a remote access VPN rule manually. Send the Pre-Shared Key and the Zyxel Device interface IP or domain name to them.
VPN Server Address	
Type	Select the method the Zyxel Device uses for incoming traffic from remote clients. If Nebula manages your Zyxel Device and assigns it a domain name, then you will see **Nebula Assigned Domain Name** in this field. • **Interface**: Use the public IP address of the interface. • **IP Address**: Use the static IP address. Select this if the interface uses a static public IP address. • **Domain Name:** Use a domain name. Select this if DDNS is assigning a dynamic IP address to the interface (for example, vpn.zyxel.com). • **Nebula Assigned Domain Name**: Use the domain name Nebula assigns to your network.
Interface	If you chose **Interface** in the **Type** field, select the interface from the drop-down list that the Zyxel Device will use for the remote VPN connection.
IP Address	If you chose **IP Address** in the **Type** field, enter the static IPv4 that the Zyxel Device will use for the remote VPN connection.
Domain Name	If you chose **Domain Name** in the **Type** field, enter the domain name that the Zyxel Device will use for the remote VPN connection. If you chose **Nebula Assigned Domain Name** in the **Type** field, this field displays the assigned domain name.
NAT Traversal	If the Zyxel Device is behind a NAT router, you can select **Custom IP or Domain Name** and enter the public IP address or the domain name that is configured and mapped to the Zyxel Device on the NAT router. Note: To allow a site-to-site VPN connection, the NAT router must have the following ports open: UDP 500, 4500.
Binding Address	If you select **Nebula Assigned Domain Name** in the **Type** field, this field displays the settings from your Nebula.
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, so do not select a zone that a security policy may block.
Certificate for VPN Validation	

Table 120 VPN > IPSec VPN > Remote Access VPN (continued)

LABEL	DESCRIPTION
Auto	Select **Auto** to have the Zyxel Device generate a certificate from the current remote access VPN settings. This is the certificate the Zyxel Device uses to identify itself when setting up the VPN tunnel.
Manual	Select **Manual** to use an existing certificate from the drop-down list box.
Clients will use VPN to Access	
Internet and Local Networks (Full Tunnel)	Select this to encrypt all traffic through the VPN. Enable **Auto SNAT** to allow the Zyxel Device to rewrite the source address of packets being sent to the interface's IP address.
Auto-SNAT	**Auto-SNAT** changes the (private) source IP addresses of VPN clients to the Zyxel Device WAN interface's public IP address for traffic going to the Internet. The Internet cannot route privately-assigned IP addresses, so the Zyxel Device must perform Source NAT (SNAT) to convert them to the public IP address on its WAN interface. For example, if the SSL VPN client has a privately-assigned IP address such as 192.168.1.88, then that IP address is automatically translated to the Zyxel Device's WAN interface IP address, such as 1.1.1.1 when going to the Internet. If you disable **Auto-SNAT**, then SSL VPN clients can reach internal LAN subnets, but not the Internet, unless you create an outbound NAT rule for the SSL VPN pool in **Network > NAT**.
Local Networks Only (Split Tunnel)	Select this to only encrypt traffic going to networks behind the Zyxel Device. Enter an IPv4 address in CIDR notation, for example, type 192.168.1.1/24. Traffic going to the Internet from this IP address is encrypted. Traffic going to the Internet from the remote client does not go through the Zyxel Device is not encrypted.
Client Network	
IP Address Pool	Enter an IPv4 address in CIDR notation, for example, type 192.168.1.1/24. The IP address pool is used to assign IP addresses to the VPN clients. The SSL VPN IP pool should not overlap with IP addresses on the Zyxel Device's local networks and the SSL user's network.
DNS Server	Select which DNS server is used for the client network. Choices are: • **Disabled**: No DNS server is used for the client network. • **ZyWALL**: The Zyxel Device acts as the sole DNS server for the client network. • **ZyWALL, then Custom**: The Zyxel Device acts as the first DNS server, and an external DNS server that you define, acts as the second DNS server that is checked if the first one is unavailable. You must enter a valid IP address for the second DNS server. • **Custom, then ZyWALL**: An external DNS server that you define, acts as the first DNS server, and the Zyxel Device acts as a second DNS server that is checked if the first one is unavailable. You must enter a valid IP address for the first DNS server. • **Custom**: An external DNS server that you define, acts as the sole DNS server for the client network. You must enter a valid IP address for the DNS server.
First DNS Server	Specify the IP address of the DNS 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. **ZyWALL**- the VPN clients use the IP address of the interface you specified in the SSL VPN rule and the Zyxel Device works as a DNS relay. **Custom Defined**- enter a static IPv4 address
Second DNS Server	Enter a secondary DNS server IP address that is checked if the first one is unavailable.

Table 120 VPN > IPSec VPN > Remote Access VPN (continued)

LABEL	DESCRIPTION
Authentication	You must first create a server in **User & Authentication > AAA Server** for it to display in the following fields. • If you have one authentication server, it can be on the Zyxel Device (**local**) or an external AAA server. • If you have two authentication servers, one of them must be on the Zyxel Device (**local**). You cannot use two external AAA servers.
Primary/ Secondary Server	Select **local** or a specified AAA server from the drop-down list box for the Zyxel Device to use for authentication. These are listed in the following order and then sorted alphabetically: Local (1), Nebula Cloud Authentication (2), AD Server (3), LDAP Server (4), OIDC Server (5), RADIUS Server (6).
User	Select or create a user or user group that can use this remote access VPN access policy. • The **User Type** must be: **User**, **External User**, **External Group User, or NID FS User**. • It cannot be an admin or viewer account type. • SecuExtender VPN clients must log in with a **User** account in **Menu > Configuration > Get from Server** screen. See Table 212 on page 459 for more information on user accounts.
Advanced Settings Phase 1 /2 Settings	
SA Life Time	Set how often the Zyxel Device renegotiates the IKE SA in **Phase 1 Settings** and the IPSec SA in **Phase 2 Settings**. A short SA life time increases security, but renegotiation temporarily disconnects the VPN tunnel. The value you set for the SA life time in **Phase 2 Settings** should be lesser than or equal to the value you set for the SA life time in **Phase 1 Settings**.
Add	Click this to add an entry.
Edit	Select an entry and click this to edit the entry.
Remove	Select an entry and click this to remove the entry.
Encryption	Select which key size and encryption algorithm to use in the IPSec SA. Choose an encryption method according to the security strength you need, CPU performance available, and compatibility with peer devices. Remote access VPN uses **IKEv2**, so choose **AES-GCM** (Galois/Counter Mode) as it offers secure (prevents both passive eavesdropping and active tampering), authenticated encryption that is faster than AES as it is optimized for modern CPUs. For key length, 128-bit is strong enough for today, 192-bit is better, and choose 256-bit if the VPN is handling top-secret information or you want to future proof decryption threats such as with quantum computing. Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput. Choices with **AES-GCM** are: • **AES128-GCM** - a 128-bit key with the Galois/Counter Mode (GCM) encryption algorithm • **AES192-GCM** - a 192-bit key with the Galois/Counter Mode (GCM) encryption algorithm • **AES256-GCM** - a 256-bit key with the Galois/Counter Mode (GCM) 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.

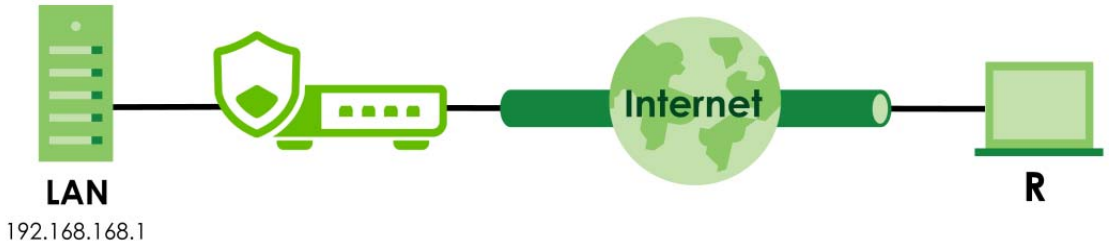
Table 120 VPN > IPSec VPN > Remote Access VPN (continued)

LABEL	DESCRIPTION
Authentication	Select which hash algorithm to use to authenticate packet data in the IPSec SA. PRF (PseudoRandom Function)-SHA does not encrypt data, but derives keys, authenticates handshake messages and produces strong session keys from initial secrets. It is not used to encrypt or authenticate the VPN data when AES-GCM is the encryption method; it is used to generate the keys that AES-GCM will use. Choices with AES-GCM **Encryption** in phase 1 are: • **PRF-MD5** • **PRF-SHA1** • **PRF-SHA256** • **PRF-SHA384** • **PRF-SHA512.** Choices with AES-GCM **Encryption** in phase 2 are: • **Built-in** - this displays in Phase 2 to indicate that the Zyxel Device performs authentication using a PRF (PseudoRandom Function). The Zyxel Device and the remote IPSec router must both have a proposal that uses the same authentication algorithm.
Diffie-Hellman Groups	Select which Diffie-Hellman key group (DH*x*) you want to use to create encryption keys. Choices are **DH2, DH5, DH14, DH15, DH16, DH19, DH20, DH21, DH28, DH29, DH30, DH 31** and **DH32.** The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. The Zyxel Device and the remote IPSec router must use the same DH key group. See Section 13.2 on page 221 for more information on DH key group. Note: Install the latest SecuExtender VPN Client for the latest DH support. The below is a reference at the time of writing. • Zyxel SecuExtender perpetual VPN Windows client versions 3.8.203.61.32 and earlier support DH1 to DH14. Later versions support up to DH28. • Zyxel SecuExtender macOS VPN client 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. Note: Check your operating system documentation for the latest VPN client DH support. The below is a reference at the time of writing. • 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.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

13.5 Remote Access VPN Setup Example

In this example, user **R** is working from home and needs to access the office network behind the Zyxel Device in the office. An administrator first configures the VPN settings on the Zyxel Device, then he provides user **R** with the necessary VPN authentication details, so that user **R** can establish a VPN connection to the office network from their computer at home.

Figure 181 Remote Access VPN Example Topology



See the following table for VPN types and remote software options.

Table 121 SSL / IKEv2 VPN Comparison

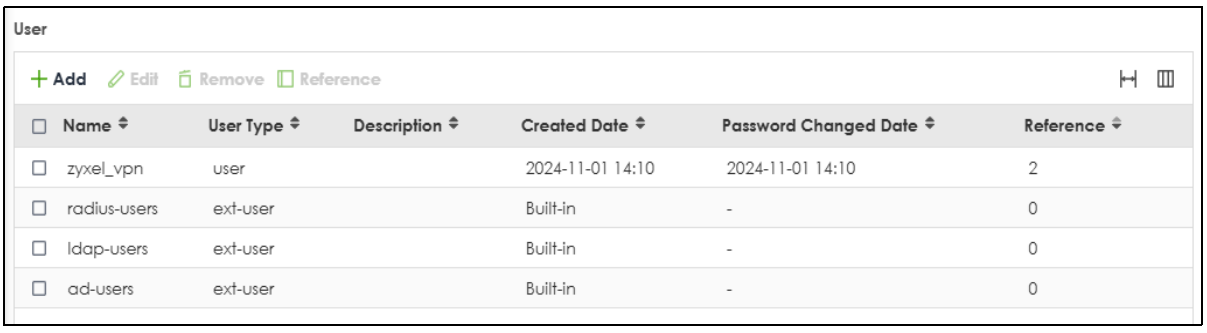
VPN TYPE	FEATURE	HOME USER SOFTWARE	SUPPORTED OPERATING SYSTEMS	AUTHENTICATION REQUIREMENTS
SSL	Provides high security. May have lower connection speed and stability.	OpenVPN Connect	Windows, macOS, Linux, iOS, Android	• VPN account username and password • OVPN configuration file
		SecuExtender	Windows, macOS	• VPN account username and password
IKEv2	Provides high security, connection speed and stability.	The IPSec VPN Client on Your Computer	Windows, macOS, iOS, and Android (strongSwan)	• VPN account username and password • Configuration file
		SecuExtender	Windows, macOS	• VPN account username and password

13.5.1 Zyxel Device Setup

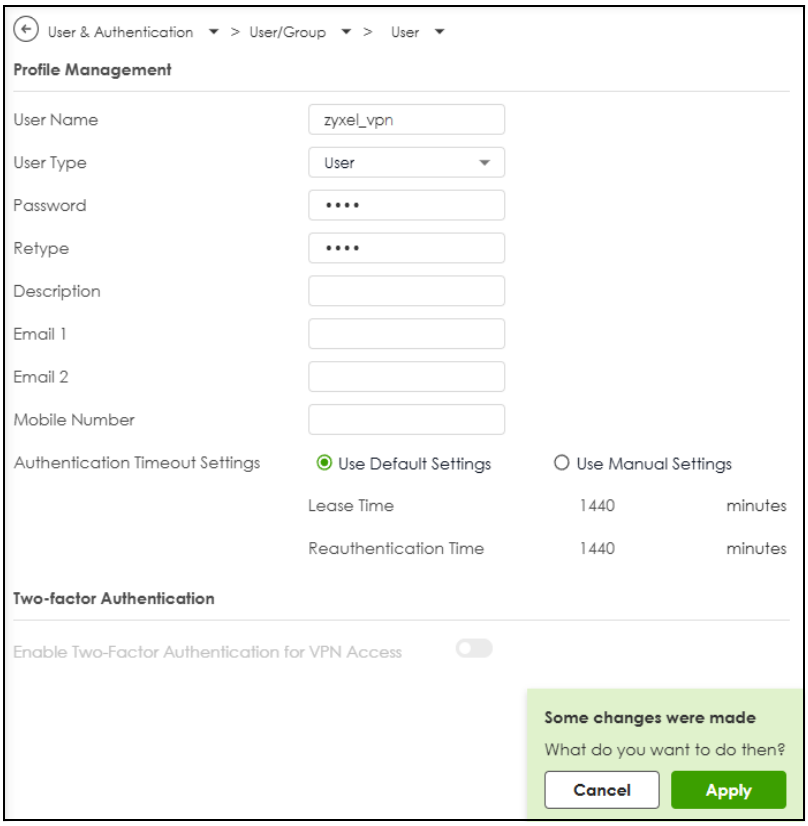
Select SSL or IKEv2 to configure the Zyxel Device in the office. See Table 121 on page 254 for the comparison between two VPN types.

SSL

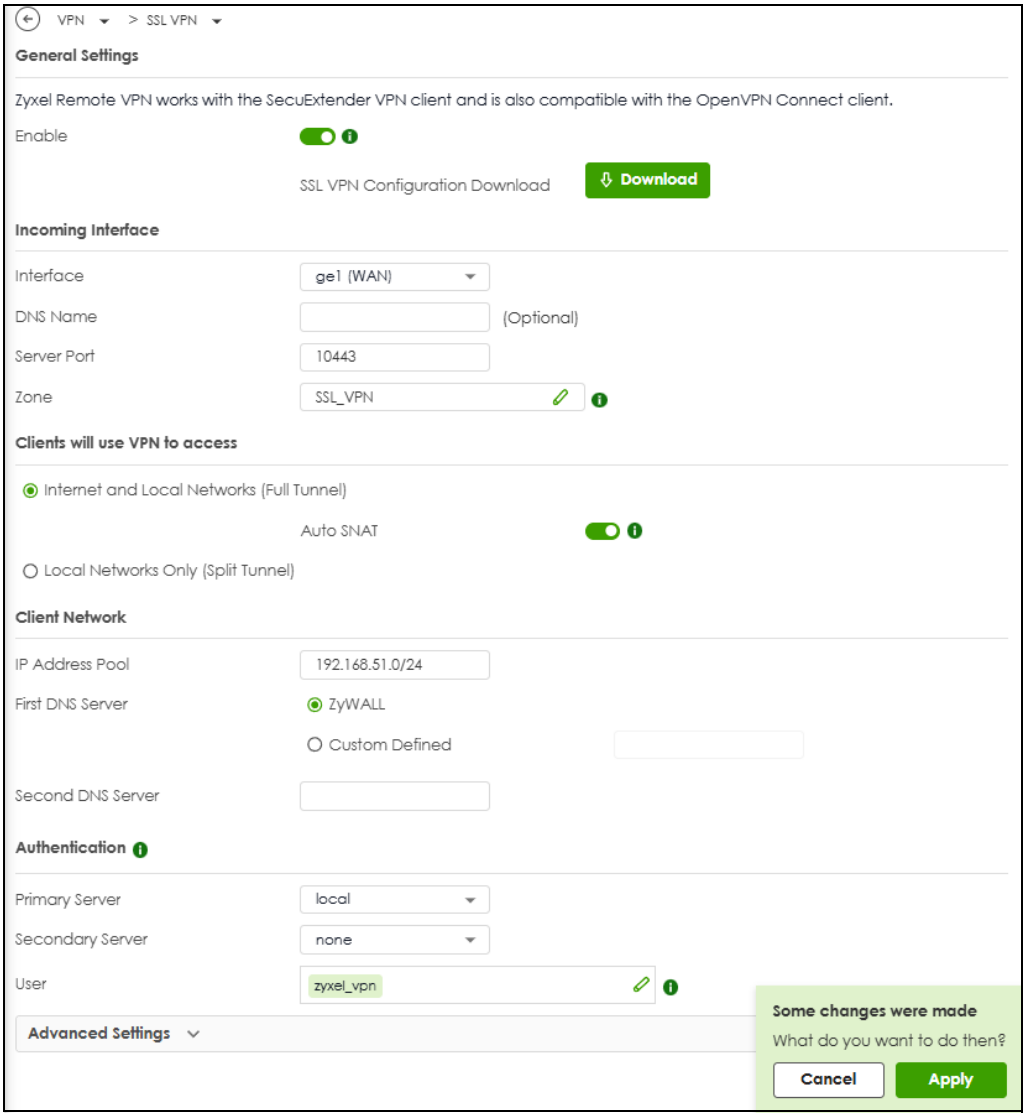
1 Go to **User & Authentication** > **User/Group** > **User**, and click **Add** under **User** to create a VPN user account.



2 Set a VPN user name and password, then click **Apply** to save your changes. Note down the account name and password for the home user who will use this for future remote access authentication.



3 To configure SSL VPN on the Zyxel Device, go to **VPN** > **SSL VPN**.



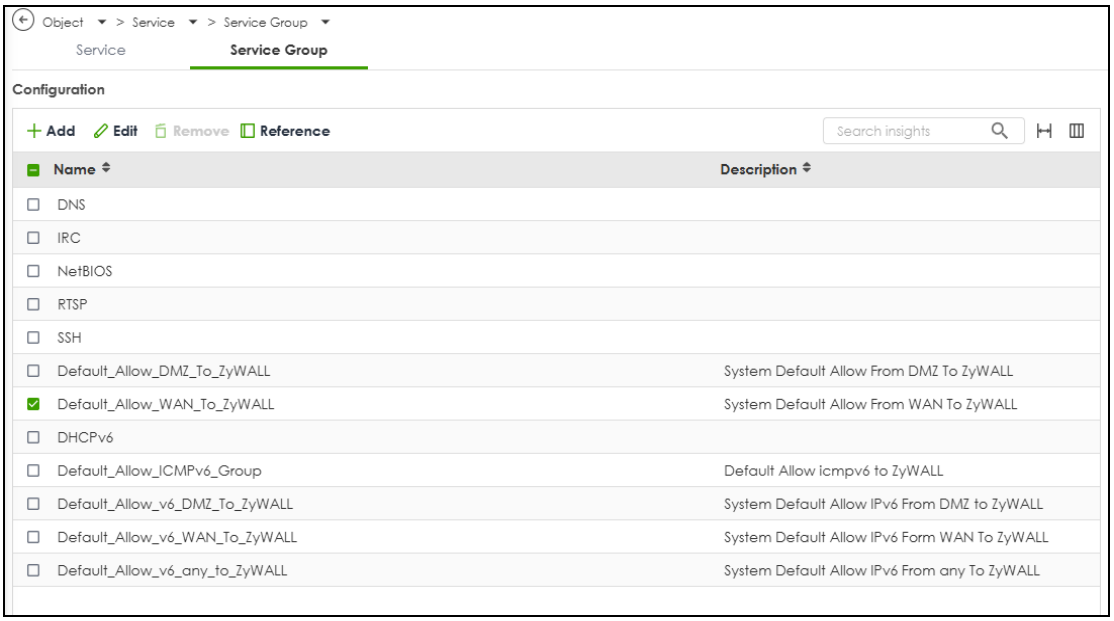
Follow the table below to configure the **VPN** > **SSL VPN** screen.

Table 122 SSL VPN Screen Configuration

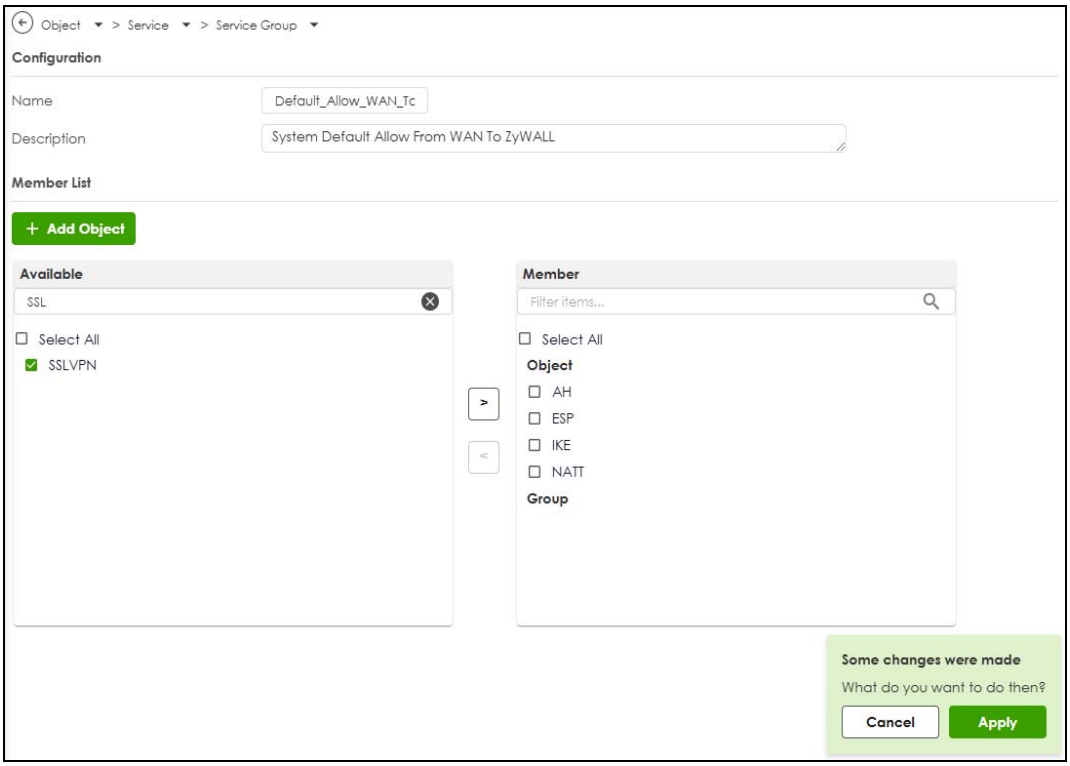
LABEL	DESCRIPTION
Enable	Click this to the right to enable SSL VPN.
Interface	Select an interface for incoming traffic to your Zyxel Device.
Clients will use VPN to access	**Full Tunnel** - Select this to encrypt all traffic through the VPN. **Split Tunnel** - Select this to only encrypt traffic going to networks behind the Zyxel Device. Enter an IPv4 address in CIDR notation, for example, type IP address 192.168.51.0/24. Traffic going to the Internet from this IP address is encrypted, and not encrypt traffic going to the Internet through the Zyxel Device.
User	Select the user account you created in step 2 to allow SSL VPN access

4 Click **Apply** to save the changes.

5 To allow the Zyxel Device to access VPN traffic from WAN, go to **Object** > **Service** > **Service Group**. Select **Default_Allow_WAN_To_ZyWALL** and click **Edit**.

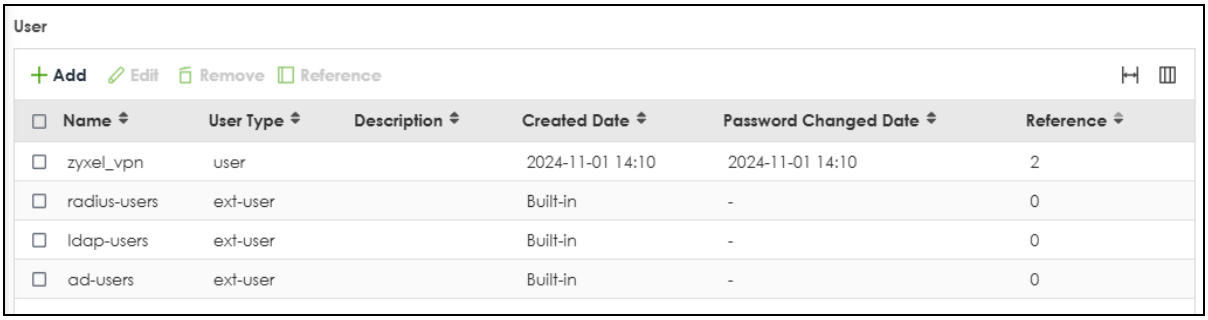


6 Search for **SSL VPN** under **Available** and click **>** to add it to the allow list of traffic from the WAN to the Zyxel Device. Then, click **Apply** to save the changes.

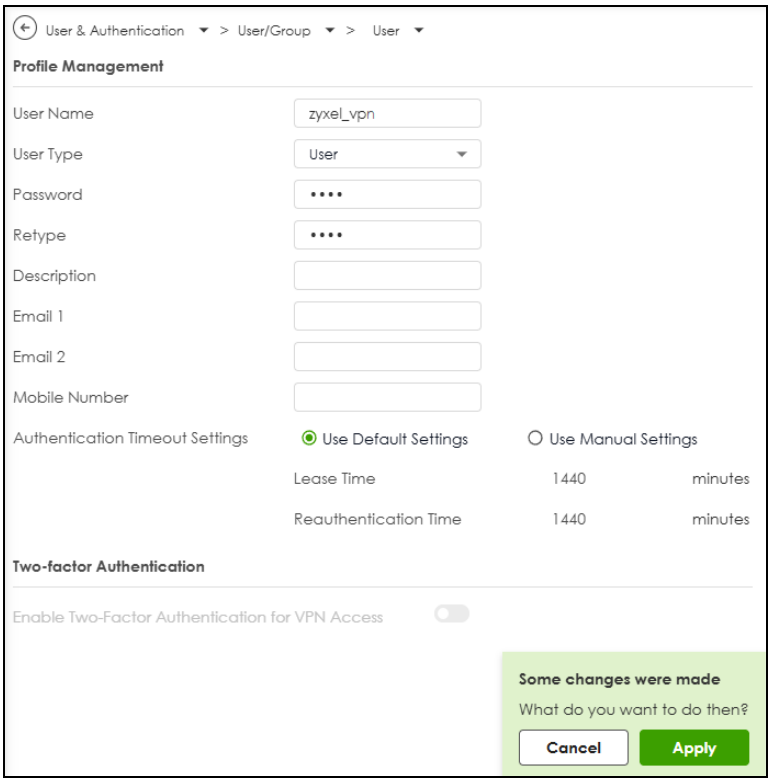


IKEv2

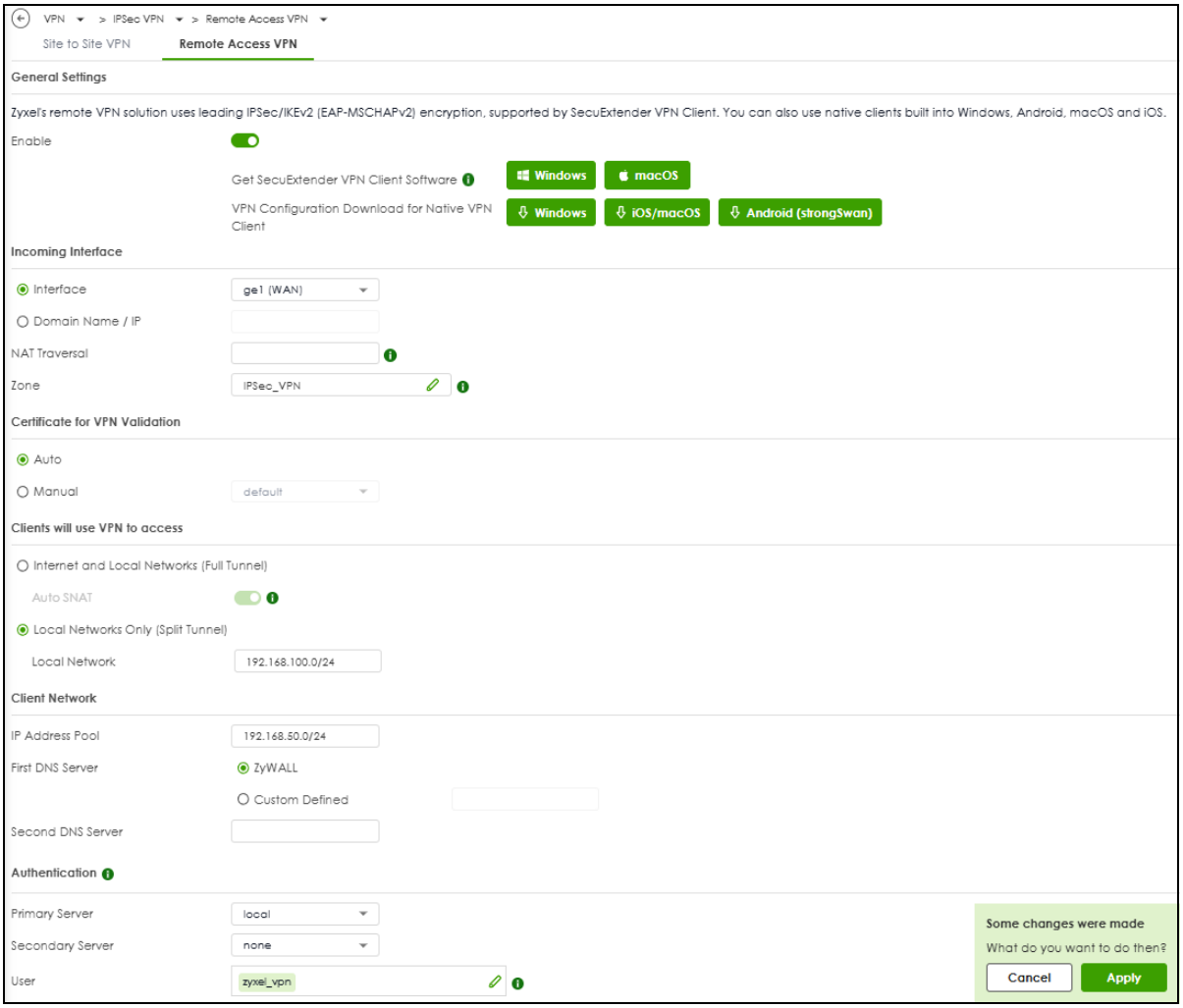
1 Go to **User & Authentication** > **User/Group** > **User**, and click **Add** under **User** to create a VPN user account.



2 Set a VPN user name and password, then click **Apply** to save your changes. Note down the account name and password for future remote access authentication.



3 To configure IKEv2 VPN on the Zyxel Device, go to **VPN** > **IPSec VPN** > **Remote Access VPN** and enable IKEv2 VPN.



Follow the table below to configure the **VPN** > **IPSec VPN** > **Remote Access VPN** screen.

Table 123 IKEv2 VPN Screen Configuration

LABEL	DESCRIPTION
Enable	Click this to the right to enable SSL VPN.
Interface	Select an interface for incoming traffic to your Zyxel Device.
Clients will use VPN to access	**Internet and Local Networks (Full Tunnel)** - Select this to encrypt all traffic through the VPN. **Local Networks Only (Split Tunnel)** - Select this to only encrypt traffic going to networks behind the Zyxel Device. Enter an IPv4 address in CIDR notation, for example, type IP address 192.168.51.0/24. Traffic going to the Internet from this IP address is encrypted, and not encrypt traffic going to the Internet through the Zyxel Device.
User	Select the user account you created in step 2 to allow IKEv2 VPN access

4 Click **Apply** to save your changes.

5 Send authentication details to the home user.

13.5.2 Home User Setup

The administrator has now finished setting up the VPN configuration on the Zyxel Device. Now, the home user needs to set up a VPN client software on their computer or mobile device to connect to the office network. See Table 121 on page 254 for VPN software options for home user and more details.

SecuExtender

SecuExtender is a Zyxel subscription-based VPN client.

Home users using SecuExtender need the following:

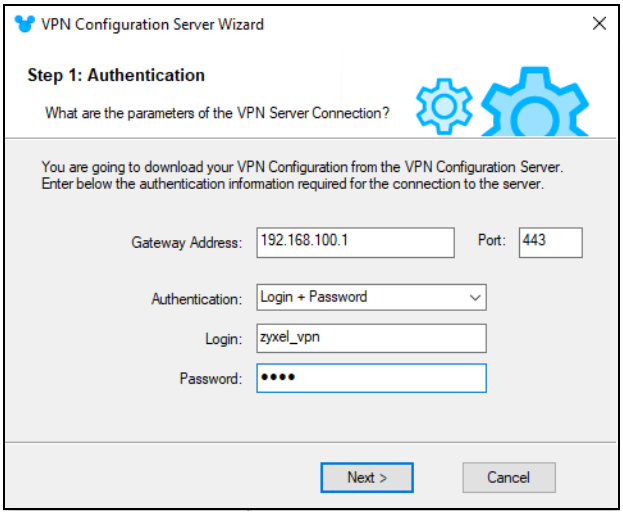
- The SecuExtender VPN client software: They should get this from the Zyxel Device administrator, who downloads it from the **VPN** > **IPSec VPN** > **Remote Access VPN** > **Get SecuExtender VPN Client Software** screen. Alternatively, you can download it directly from the Zyxel website.
- VPN account username and password: They should get this from the Zyxel Device administrator, who sets it in the **User & Authentication** > **User/Group** > **User** screen.

Follow these steps to establish a VPN connection to the office's network through SecuExtender:

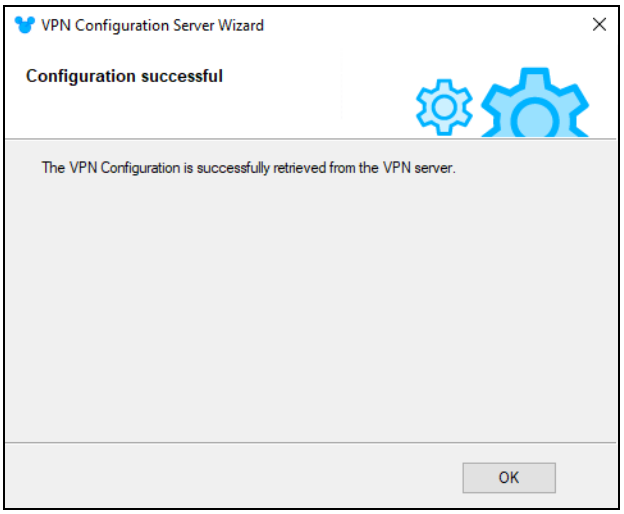
1 Unzip, install, and open the SecuExtender VPN Client on your computer. Click **Configuration** > **Get from Server**, then enter the parameters as described below and click **Next**.

Note: You must log in with an account of type **User**, not **Local Administrator**.

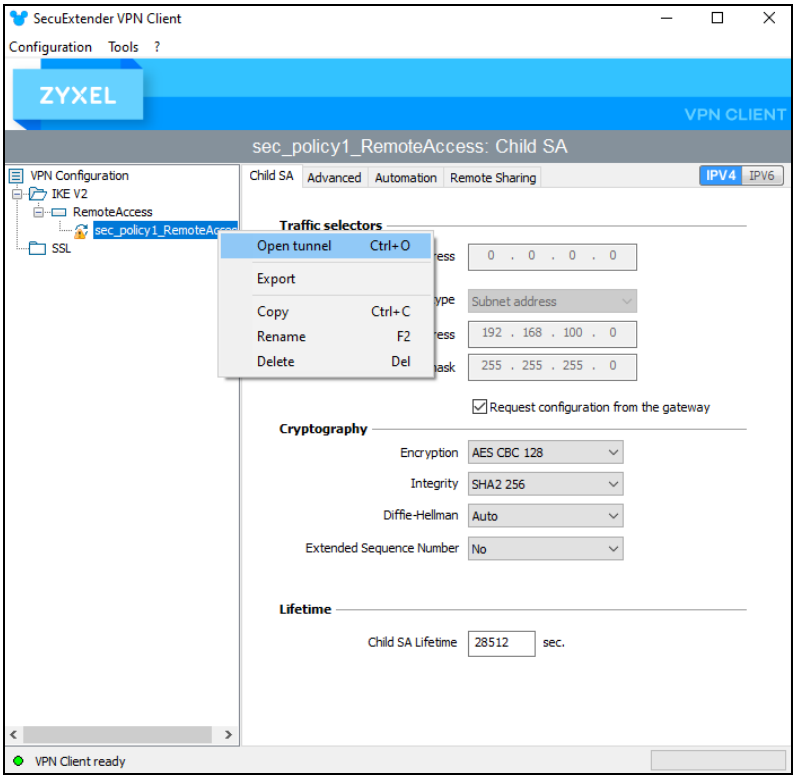
LABEL	DESCRIPTION
Gateway Address	Enter the WAN IP address of the Zyxel Device.
Authentication	Set as **Login + Password**.
Login/Password	Enter the username and password the Zyxel Device administrator gave.



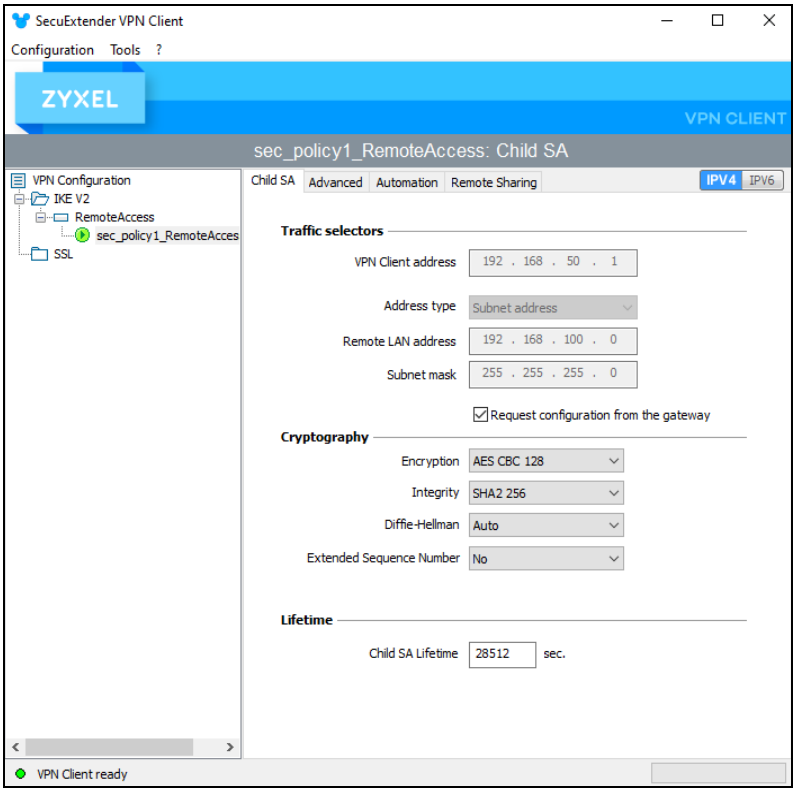
2 The following screen appears, click **OK**.



3 Right click on the VPN policy you just created, then click **Open tunnel** to establish a remote VPN connection.



4 Re-enter the user name and password, then click **OK**. The icon next to the VPN policy turns green. You can now access the office network through the Zyxel Device.



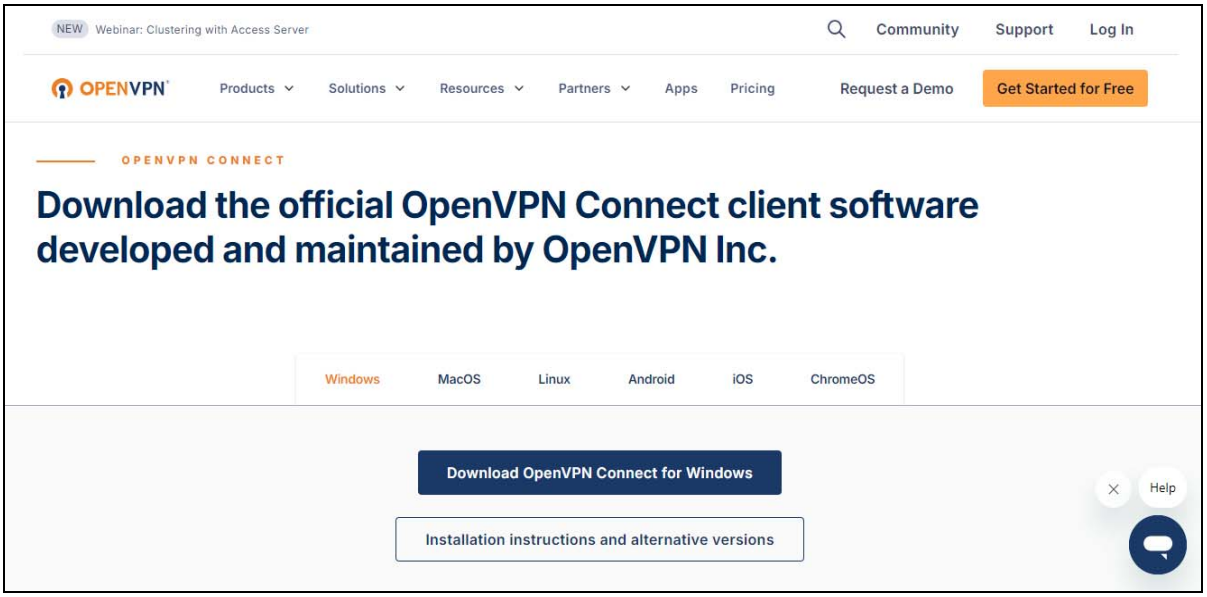
OpenVPN Connect

Follow these steps to establish a VPN connection to the office's network through OpenVPN Connect:

1 Home users using OpenVPN Connect need the following:

- The OpenVPN Connect client software.
- The VPN account username and password: They should get this from the Zyxel Device administrator, who sets it in the **User & Authentication** > **User/Group** > **User** screen.
- The OVPN configuration file: They should get this from the Zyxel Device administrator, who downloads it from the **VPN** > **SSL VPN** screen.

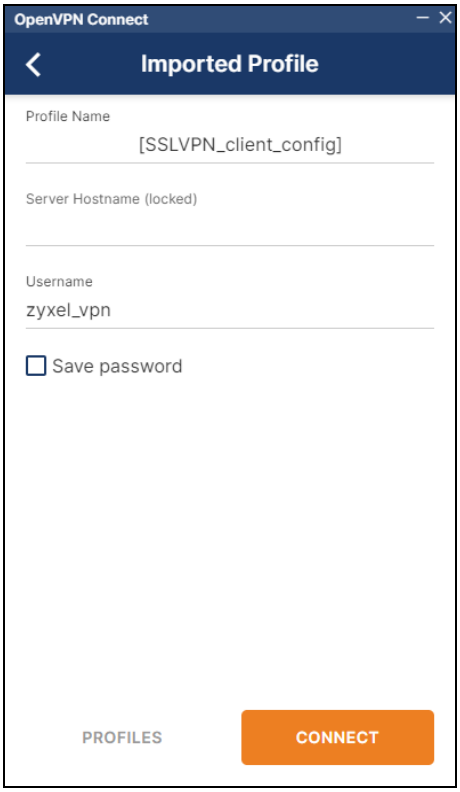
2 Go to the *OpenVPN Connect* website and download the OpenVPN Connect client for your computer's operation system.



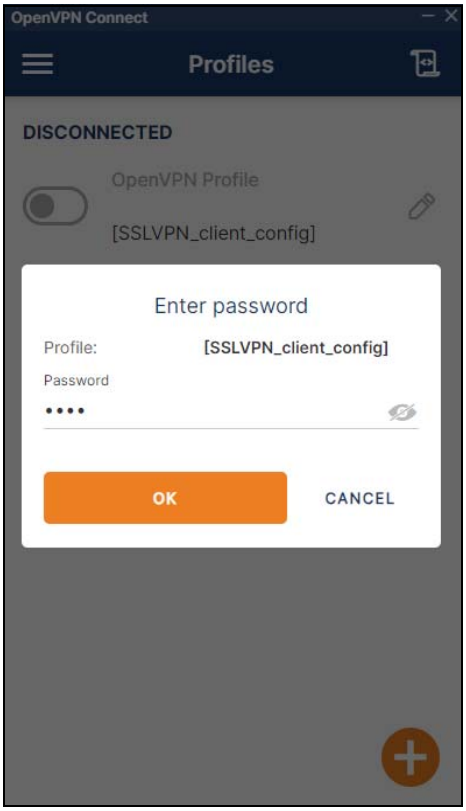
3 Run the OpenVPN Connect client on your computer. Click **Browse** and import the .OVPN file provided by Zyxel Device administrator.



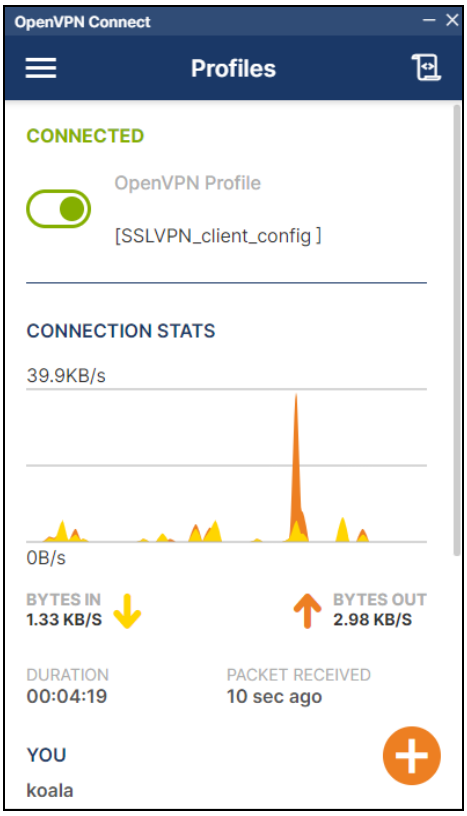
4 In the **Username** field, enter the VPN user name the Zyxel Device administrator set. Click **Connect** to connect your computer to the office network.



5 Enter the VPN user password provided by the Zyxel Device administrator.



6 Your home computer can now access the office network through the Zyxel Device.



The IPSec VPN Client on Your Computer

Use the built-in VPN client in Windows, macOS, iOS, or Android (strongSwan).

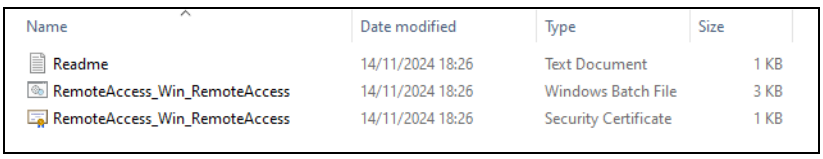
Home users using the IPSec VPN client on their computers need the following:

- Configuration file: They should get this from the Zyxel Device administartor, who downloaded it from the **VPN** > **IPSec VPN** > **Remote Access VPN** screen.

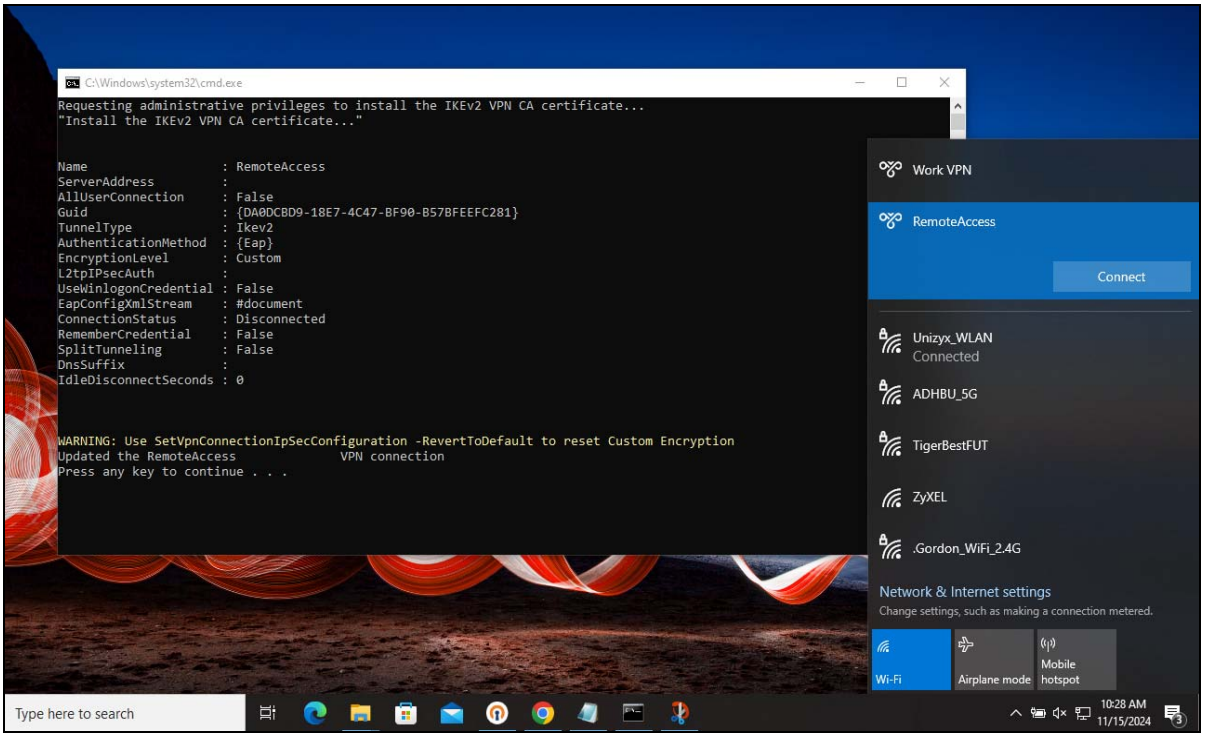
Follow these steps to establish a VPN connection to the office's network through the IPSec VPN client on a computer with a Windows operating system:

1 Obtain the configuration file, VPN account name and password from the Zyxel Device administrator.

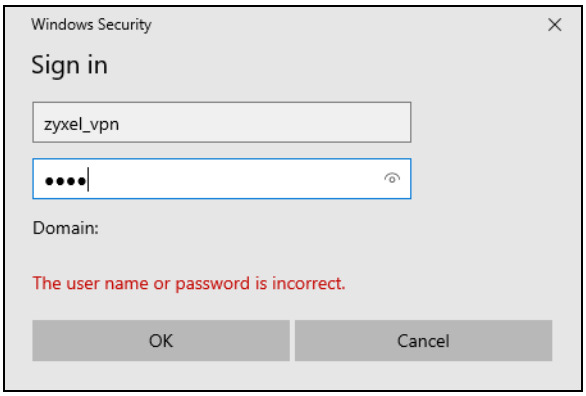
2 Unzip and open the configuration file, then double-click on the .bat file to set up the certificate for the VPN connection.



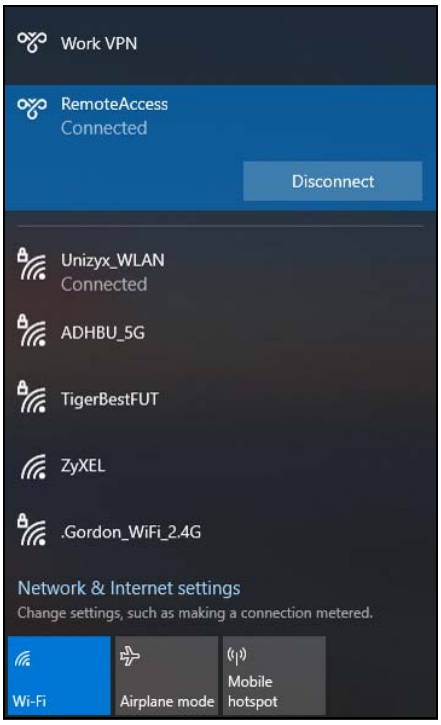
3 A command-line interface will appear, showing the status of the VPN connection. To connect to the office network, click the **Internet access** icon, then click **Connect** next to the **RemoteAccess** network.



4 Enter the username and password provided by the administrator in the pop-up window, then click **OK**.

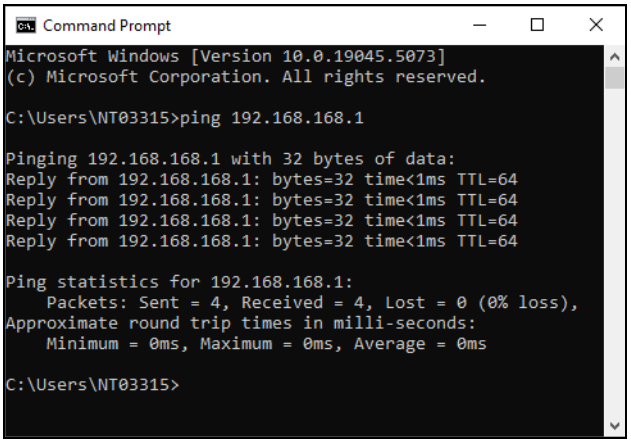


5 The following screen indicates you are now connected to the office network.



13.5.3 Test the VPN Connection

To test if the home user's computer can successfully connect to the office's network, they should open the Command Prompt and ping the IP address of a device in the LAN. If the connection is successful, the following result will appear.



CHAPTER 14
SSL VPN

14.1 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.

14.1.1 What You Can Do in this Chapter

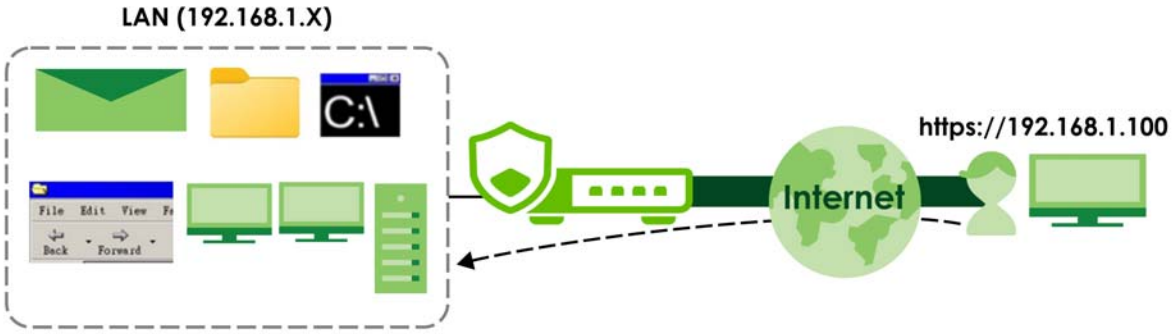
Use the **VPN > SSL VPN** screen (see Section 14.2 on page 269) to configure a SSL access policy.

14.1.2 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.

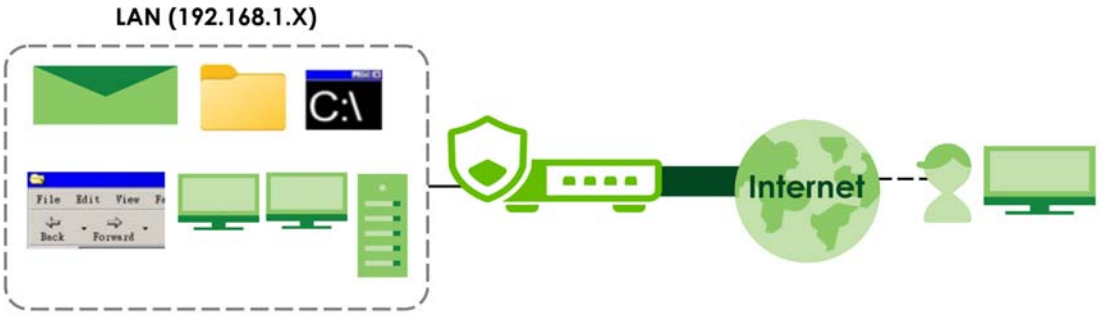
Figure 182 Network Access Mode: Full Tunnel Mode



Split Tunnel Mode

In split tunnel mode, only the traffic going to the networks behind the Zyxel Device is encrypted. Traffic going to the Internet from the remote client does not go through the Zyxel Device and is not encrypted.

Figure 183 Network Access Mode: Split Tunnel Mode



SSL VPN Policy

An SSL VPN 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 124 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.

Please note that you cannot delete an object that is referenced by other settings.

14.2 The SSL VPN Screen

Configure the settings in this screen to create a new or edit an existing SSL access policy.

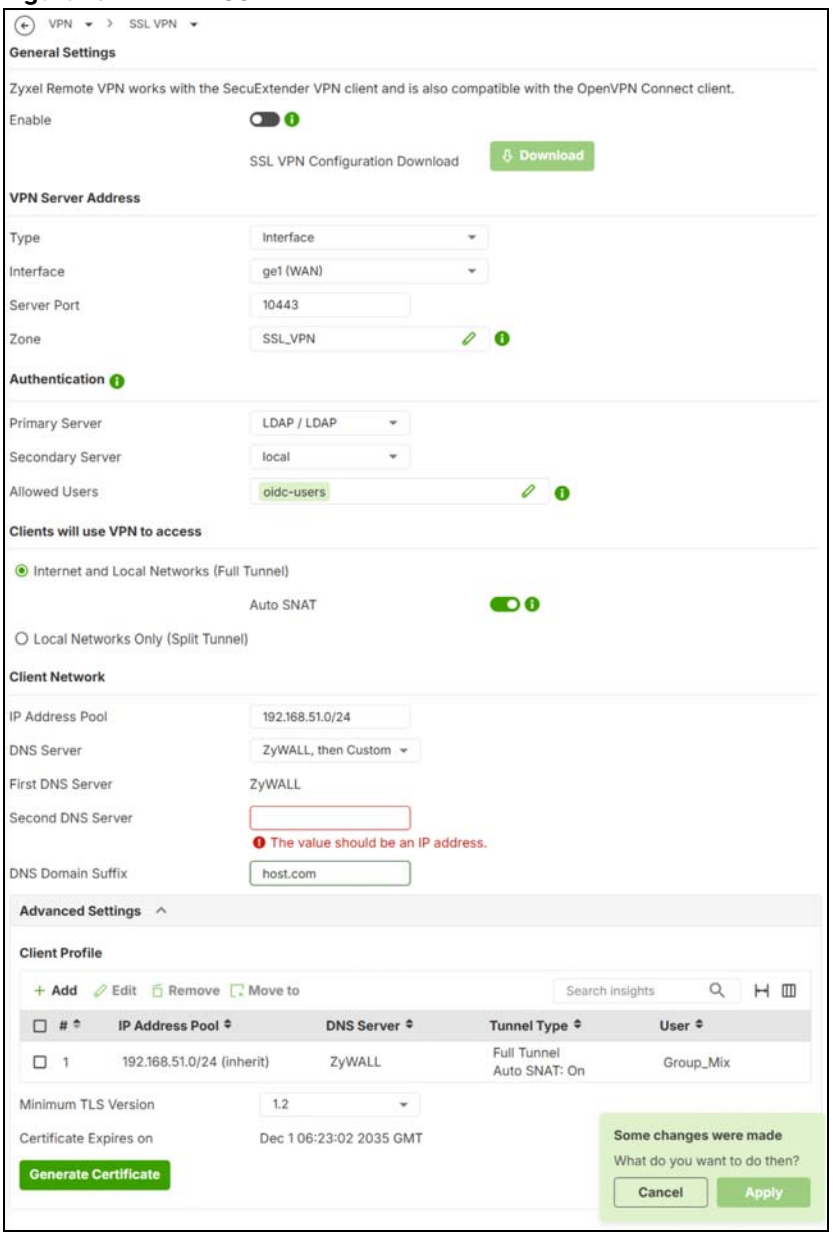
SecuExtender is a Zyxel subscription-based VPN client. A remote access VPN client must have SecuExtender VPN client installed on his device and uses a supported computer operating system. The supported computer operating systems are:

- Window 10 (64-bit) and later versions.
- macOS 10.15 and later versions.

Make sure the settings configured on the SSL VPN client matches the settings you configured on the Zyxel Device.

Click **VPN** > **SSL VPN** to open the following screen.

Figure 184 VPN > SSL VPN



The following table describes the labels in this screen.

Table 125 VPN > SSL VPN

LABEL	DESCRIPTION
Enable	Click the switch to enable the SSL access policy.
Download	Click to download a VPN configuration script to send to clients using SecuExtender VPN client or OpenVPN Connect VPN client. The supported operating systems for SecuExtender are: • Windows 10 (64-bit) and later versions. • macOS 10.15 and later versions.
VPN Server Address	
Type	Select the method the Zyxel Device uses for incoming traffic from remote clients. If Nebula manages your Zyxel Device and assigns it a domain name, then you will see Nebula Assigned Domain Name in this field. • **Interface**: Use the public IP address of the interface. • **Domain Name:** Use a domain name. Select this if DDNS is assigning a dynamic IP address to the interface (for example, vpn.zyxel.com). • **Nebula Assigned Domain Name**: Use the domain name Nebula assigns to your network.
Interface	Select an interface from the drop-down list box for incoming traffic to your Zyxel Device.
DNS Name	Enter the domain name (for example, vpn.zyxel.com) if you're using DDNS to assign the interface a dynamic IP address.
Domain Name	If you chose **Nebula Assigned Domain Name** in the **Type** field, this field displays the assigned domain name.
Binding Address	If you select **Nebula Assigned Domain Name** in the **Type** field, this field displays the settings from your Nebula.
Server Port	Specify the server port of the Zyxel Device for full tunnel mode SSL VPN access. Leave this field to default settings unless it conflicts with another interface.
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, so do not select a zone that a security policy may block.
Authentication	You must first create a server in **User & Authentication > AAA Server** for it to display in the following fields. • If you have one authentication server, it can be on the Zyxel Device (**local**) or an external AAA server. • If you have two authentication servers, one of them must be on the Zyxel Device (**local**). You cannot use two external AAA servers.
Primary/ Secondary Server	Select **local** or a specified AAA server from the drop-down list box for the Zyxel Device to use for authentication. These are listed in the following order and then sorted alphabetically: Local (1), Nebula Cloud Authentication (2), AD Server (3), LDAP Server (4), OIDC Server (5), RADIUS Server (6).

Table 125 VPN > SSL VPN (continued)

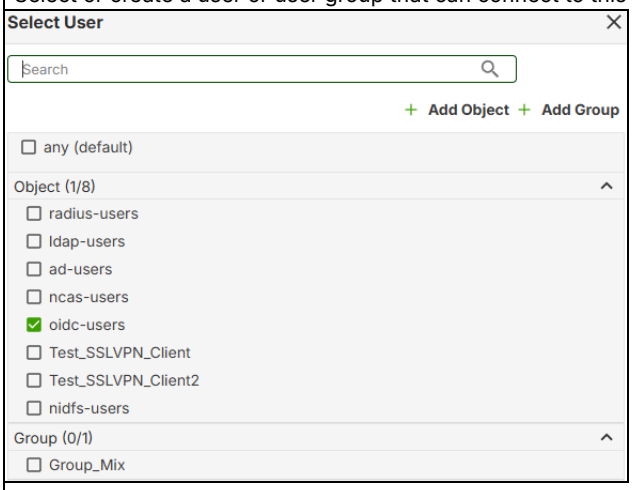
LABEL	DESCRIPTION
Allowed Users	Select or create a user or user group that can connect to this SSL access policy.  • This is a required field. • The **User Type** must be: **User**, **External User**, or **External Group User**. • It cannot be an admin or viewer account type. • SecuExtender VPN clients must log in with a **User** account in **Menu > Configuration > Get from Server** screen. See Section 28.1.1 on page 459 for more information on user accounts. • ncas-users are users authenticated by Nebula - see Section 28.1.2 on page 461. • oidc-users are users authenticated by OpenID Connect (OIDC) - see Section 28.3.5 on page 487. • nidfs-users are users authenticated by NID FS (Nebula IDentity Federation Service) - see Section 28.1.3 on page 462. When the number of connections to the Zyxel Device reaches the number of IP addresses specified in the **IP Address Pool**, then additional VPN clients cannot access the Zyxel Device.
Clients will use VPN to access	
Internet and Local Networks (Full Tunnel)	Select this to encrypt all traffic through the VPN. Enable **Auto SNAT** to allow the Zyxel Device to rewrite the source address of packets being sent to the interface's IP address.
Auto-SNAT	**Auto-SNAT** changes the (private) source IP addresses of VPN clients to the Zyxel Device WAN interface's public IP address for traffic going to the Internet. The Internet cannot route privately-assigned IP addresses, so the Zyxel Device must perform Source NAT (SNAT) to convert them to the public IP address on its WAN interface. For example, if the SSL VPN client has a privately-assigned IP address such as 192.168.1.88, then that IP address is automatically translated to the Zyxel Device's WAN interface IP address, such as 1.1.1.1 when going to the Internet. If you disable **Auto-SNAT**, then SSL VPN clients can reach internal LAN subnets, but not the Internet, unless you create an outbound NAT rule for the SSL VPN pool in **Network > NAT**.
Local Networks Only (Split Tunnel)	Select this to only encrypt traffic going to networks behind the Zyxel Device. Enter an IPv4 address in CIDR notation. Traffic going to the Internet from this IP address is encrypted. Traffic going to the Internet from the remote client does not go through the Zyxel Device is not encrypted. • Define a range of IP address using a subnet mask. For example, enter 192.168.1.0/24. • Define a specific IP address. For example, enter 192.168.1.1/32.
Client Network	

Table 125 VPN > SSL VPN (continued)

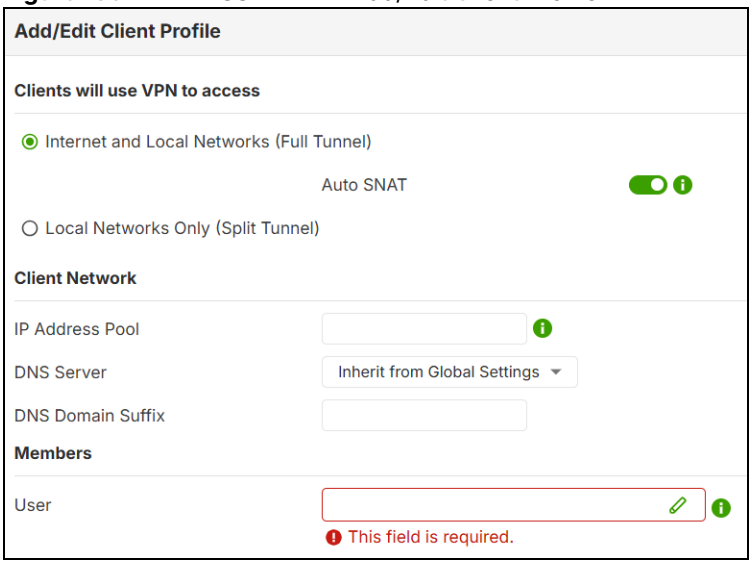
LABEL	DESCRIPTION
IP Address Pool	Enter an IPv4 address in CIDR notation. The IP address pool is used to assign IP addresses to the VPN clients. The SSL VPN IP pool should not overlap with IP addresses on the Zyxel Device's local networks and the SSL user's network. • Define a range of IP address using a subnet mask. For example, enter 192.168.1.0/24. • Define a specific IP address. For example, enter 192.168.1.1/32.
DNS Server	Specify up to two DNS servers for VPN clients to use. This allows them to access devices on the local network using domain names instead of IP addresses. • **Disable:** No DNS server is defined. • **ZyWALL:** The VPN clients use the IP address of the WAN interface you specified in the SSL VPN rule and the Zyxel Device works as a DNS relay. • **Custom:** Enter the static IP address of the DNS server.
First DNS Server	Specify the IP address of the DNS server for the VPN clients to use.
Second DNS Server	Specify a secondary DNS server IP address that is checked if the first one is unavailable.
DNS Domain Suffix	Set the DNS suffix that is appended to hostnames typed by VPN clients to form a complete domain name. For example, if a user types only a hostname (fileserver), the DNS suffix (example.com.) is automatically appended, resulting in fileserver.example.com.
Advanced Settings	
Client Profile	You can create one or more profiles to apply the configured settings to specific user(s).
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.
Move to	To change a policy's position in the numbered list, select the policy and click **Move to**. Enter the position number and press [ENTER] to move the policy to that position.
#	This is the entry's index number in the list. If a user belongs to two or more profiles, the profile with the lower index number is applied first.
IP Address Pool	This displays the IP address pool used to assign IP addresses to VPN clients in this profile.
DNS Server	This displays the DNS server used by VPN clients in this profile.
Tunnel Type	This displays whether VPN clients in this profile use a full tunnel or split tunnel to access the network.
User	This displays the VPN clients in this profile.
Minimum TLS Version	Select the minimum TLS version required for this SSL access policy. TLS connections using a version lower than the selected one will be blocked. The Zyxel Device requires a TLS 1.2 minimum to block insecure protocols (like TLS 1.0/1.1) that have known vulnerabilities. TLS 1.3 provides stronger cipher suites and more secure key exchange methods than earlier versions.
Generate Certificate	Click this to have the Zyxel Device generate a self-signed certificate for the Zyxel Device to identify itself when setting up the SSL VPN tunnel. Note the expiry date in **Certificate Expires on**. Click **Generate Certificate** to generate a new certificate when the certificate expires and notify all SSL VPN and OpenVPN clients to import the SSL VPN file again as all SSL VPN and OpenVPN clients have to update their SSL VPN settings to match the Zyxel Device SSL VPN settings.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

14.2.1 Add/Edit Client Profile

You can create one or more profiles to apply the configured settings to specific user(s). The settings here have higher priority than the global settings on the **VPN > SSL VPN** screen. In the **VPN** > **SSL VPN** screen, click the **Add** or **Edit** icon under **Client Profile.**

Note: See the **Product Feature** appendix for the maximum number of profiles your Zyxel Device can create and the maximum number of users allowed per profile.

Figure 185 VPN > SSL VPN > Add/Edit Client Profile



The following table describes the labels in this screen.

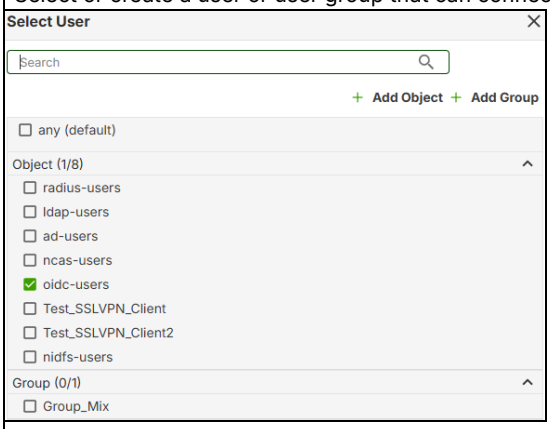
Table 126 VPN > SSL VPN > Add/Edit Client Profile

LABEL	DESCRIPTION
Clients will use VPN to access	
Internet and Local Networks (Full Tunnel)	Select this to encrypt all traffic through the VPN. Enable **Auto SNAT** to allow the Zyxel Device to rewrite the source address of packets being sent to the interface's IP address.
Auto-SNAT	**Auto-SNAT** changes the (private) source IP addresses of VPN clients to the Zyxel Device WAN interface's public IP address for traffic going to the Internet. The Internet cannot route privately-assigned IP addresses, so the Zyxel Device must perform Source NAT (SNAT) to convert them to the public IP address on its WAN interface. For example, if the SSL VPN client has a privately-assigned IP address such as 192.168.1.88, then that IP address is automatically translated to the Zyxel Device's WAN interface IP address, such as 1.1.1.1 when going to the Internet. If you disable **Auto-SNAT**, then SSL VPN clients can reach internal LAN subnets, but not the Internet, unless you create an outbound NAT rule for the SSL VPN pool in **Network > NAT**.

Table 126 VPN > SSL VPN > Add/Edit Client Profile (continued)

LABEL	DESCRIPTION
Local Networks Only (Split Tunnel)	Select this to only encrypt traffic going to networks behind the Zyxel Device. Enter an IPv4 address in CIDR notation. Traffic going to the Internet from this IP address is encrypted. Traffic going to the Internet from the remote client does not go through the Zyxel Device is not encrypted. • Define a range of IP address using a subnet mask. For example, enter 192.168.1.0/24. • Define a specific IP address. For example, enter 192.168.1.1/32. Note: Make sure to add the local network after selecting this.
Client Network	
IP Address Pool	Enter an IPv4 address in CIDR notation. The IP address pool is used to assign IP addresses to the VPN clients. The SSL VPN IP pool should not overlap with IP addresses on the Zyxel Device's local networks and the SSL user's network. • Define a range of IP address using a subnet mask. For example, enter 192.168.1.0/24. • Define a specific IP address. For example, enter 192.168.1.1/32. Note: The IP address pool you configure here for users in this profile must be within the **IP Address Pool** configured in the **VPN > SSL VPN** screen.
DNS Server	Specify up to two DNS servers for VPN clients to use. This allows them to access devices on the local network using domain names instead of IP addresses. • **Inherit from Global Settings:** Use the DNS server(s) configured in the **VPN > SSL VPN** screen. • **ZyWALL:** The VPN clients use the IP address of the interface you specified in the SSL VPN rule and the Zyxel Device works as a DNS relay. • **Custom:** Enter the static IP address of the DNS server.
First DNS Server	Specify the IP address of the DNS server for the VPN clients to use.
Second DNS Server	Specify a secondary DNS server IP address that is checked if the first one is unavailable.
DNS Domain Suffix	A DNS suffix is the domain name of where the DNS server is located. Set the DNS suffix that is appended to hostnames typed by VPN clients to complete the domain name. For example, if a user types only a hostname (fileserver), the DNS suffix (company.com.) is automatically appended, resulting in fileserver.company.com. You can use a subdomain of your real domain, such as corp.company.com, resulting in fileserver.corp.company.com.
Members	

Table 126 VPN > SSL VPN > Add/Edit Client Profile (continued)

LABEL	DESCRIPTION
User	Select or create a user or user group that can connect to this SSL access policy.  • This is a required field. • The **User Type** must be: **User**, **External User**, or **External Group User**. • It cannot be an admin or viewer account type. • SecuExtender VPN clients must log in with a **User** account in **Menu > Configuration > Get from Server** screen. See Section 28.1.1 on page 459 for more information on user accounts. ncas-users are users authenticated by Nebula. oidc-users are users authenticated by OpenID Connect (OIDC). See Section 28.3.5 on page 487 for more information on OIDC. Note: When the number of connections to the Zyxel Device reaches the number of IP addresses specified in the **IP Address Pool**, then additional VPN clients cannot access the Zyxel Device.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

CHAPTER 15 Tailscale

15.1 Overview

The Zyxel Device supports Tailscale, a site-to-site mesh VPN (Virtual Private Network) service that connects client devices (computer, smartphone, router, firewall) across different networks.

15.1.1 What You Can Do in this Chapter

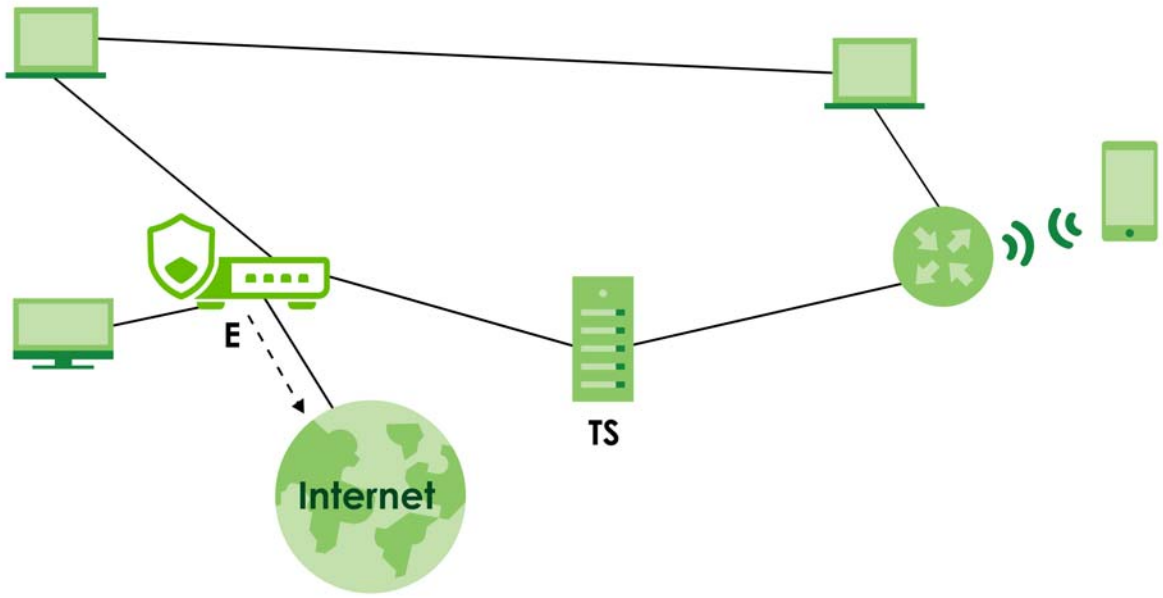
Use the **VPN > Tailscale** screen (see Section 15.2 on page 278) to configure Tailscale settings.

15.1.2 What You Need to Know

By default, Tailscale only routes traffic between client devices running Tailscale and does not protect public Internet traffic. However, there may be times when you want to route traffic from the Tailscale VPN to the public Internet, such as when you need access to an online service only available in another country.

In the following figure, the Tailscale server (**TS**) creates a mesh network, allowing each client device to connect directly with others, resulting in lower latency. The Zyxel Device act as the exit node (**E**) to route the VPN traffic to the public Internet.

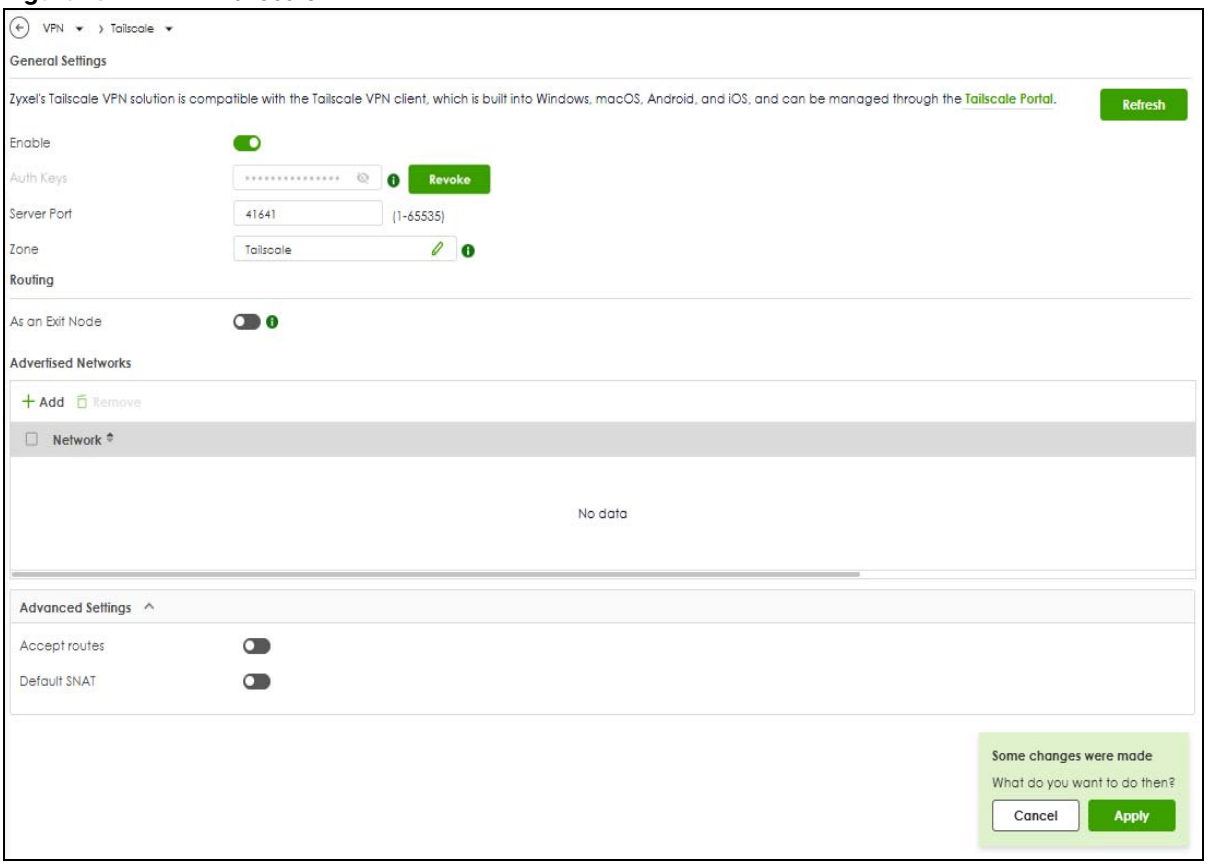
Figure 186 Tailscale Example Topology



15.2 The Tailscale Screen

Use this screen to configure Tailscale settings. Click **VPN** > **Tailscale** to open this screen.

Figure 187 VPN > Tailscale



The following table describes the labels in this screen.

Table 127 VPN > Tailscale

LABEL	DESCRIPTION
General Settings	
Enable	Enable this to run Tailscale on the Zyxel Device so that VPN clients with Tailscale software can establish a VPN connection.
Auth Keys	Input the authentication key from the Tailscale admin console here. You cannot reuse an authentication key. You should disable key expiry in the Tailscale admin console. After you click **Apply** the **Revoke** button appears.
Revoke	Click **Revoke** to disconnect and log out from Tailscale. To reconnect to Tailscale, you will need to log into Tailscale again and create a new authentication key to enter in **Auth Keys**.
Server Port	Enter the port number for the Tailscale service. The default port number is 41641.
Zone	Select a Tailscale zone object for incoming or outgoing Tailscale VPN traffic.
Routing	
As an Exit Node	By default, Tailscale only routes VPN traffic between running client devices, but does not route VPN traffic to the Internet. Enable this if you want Tailscale to route the client devices' Internet traffic through the Zyxel Device. See Section 15.1.2 on page 277 for more information about exit node.

Table 127 VPN > Tailscale (continued)

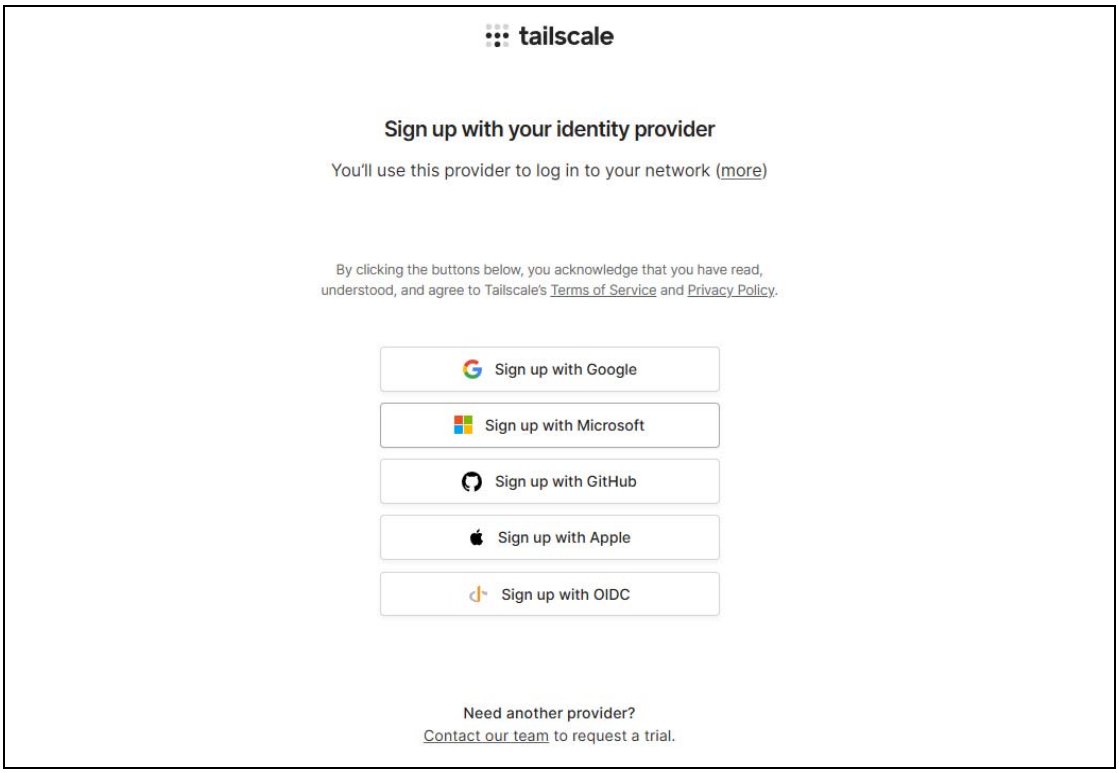
LABEL	DESCRIPTION
Advertised Networks	You must first enable Tailscale, enter the **Auth Key**, and click **Apply** in this screen to select a **SUBNET**-type object. Select an address object of host or subnet type if you want to share them with other Tailscale VPN nodes. The selected subnets are open for access by the Tailscale network. Other client devices in the Tailscale network that accept advertised routes can access these resources through the Zyxel Device. This must also be configured on the Tailscale admin console.
Add	Click **Add** to add a **SUBNET**-type object for other Tailscale client devices to access.
Remove	Select an entry and click **Remove** to remove a subnet from the table.
Network	This displays the subnet(s) on the Zyxel Device that other Tailscale client devices can access.
Advanced Settings	
Accept routes	Enable this to accept advertised routes from other Tailscale VPN nodes. If you disable this, the Zyxel Device can only access peer VPN nodes, but not the advertised routes of those nodes.
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 trunk interfaces. The Zyxel Device automatically adds local source IP addresses for traffic it routes from internal interfaces to external interfaces.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

15.2.1 Set Up a Tailscale Network

Follow these steps to set up a Tailscale network and have your Zyxel Device connect to it.

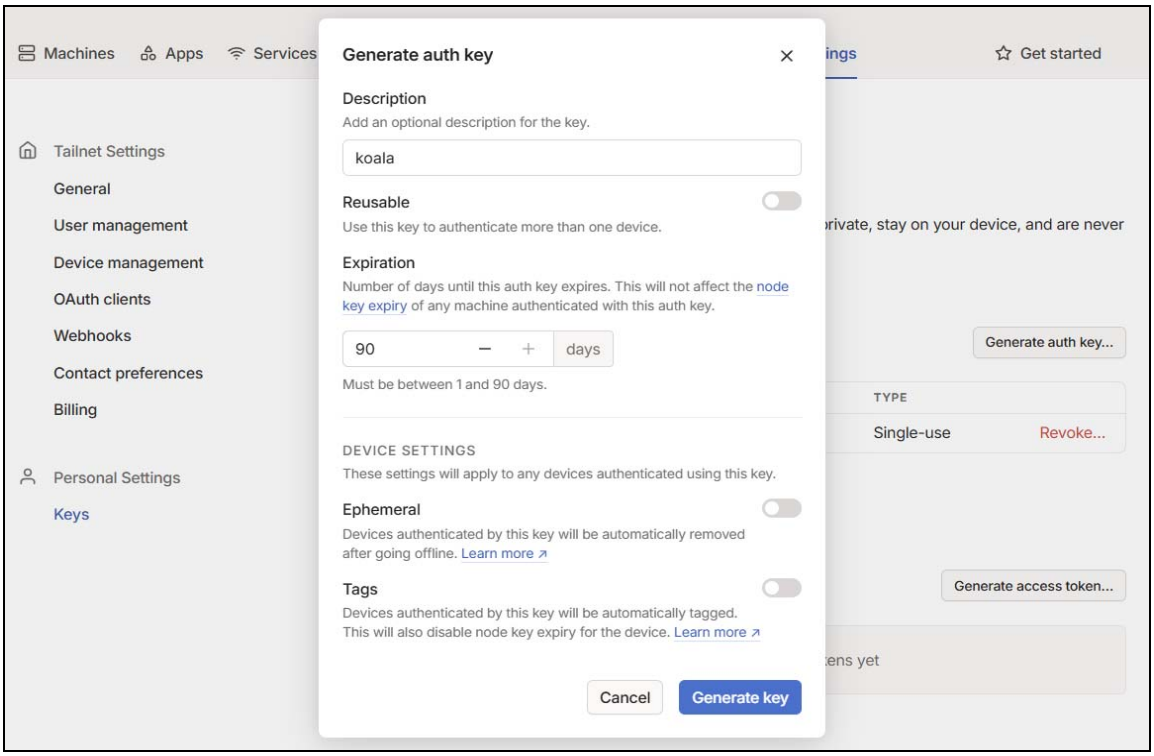
Sign Up for Tailscale

1 Go to the *Tailscale* website and click **Get started**. Alternatively, you can download and install the Tailscale software on your network device, such as a computer or smartphone, then sign up and log in.

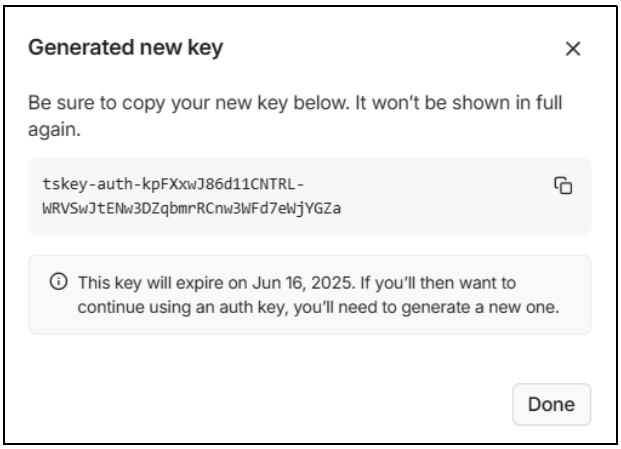


Connect the Zyxel Device to Tailscale

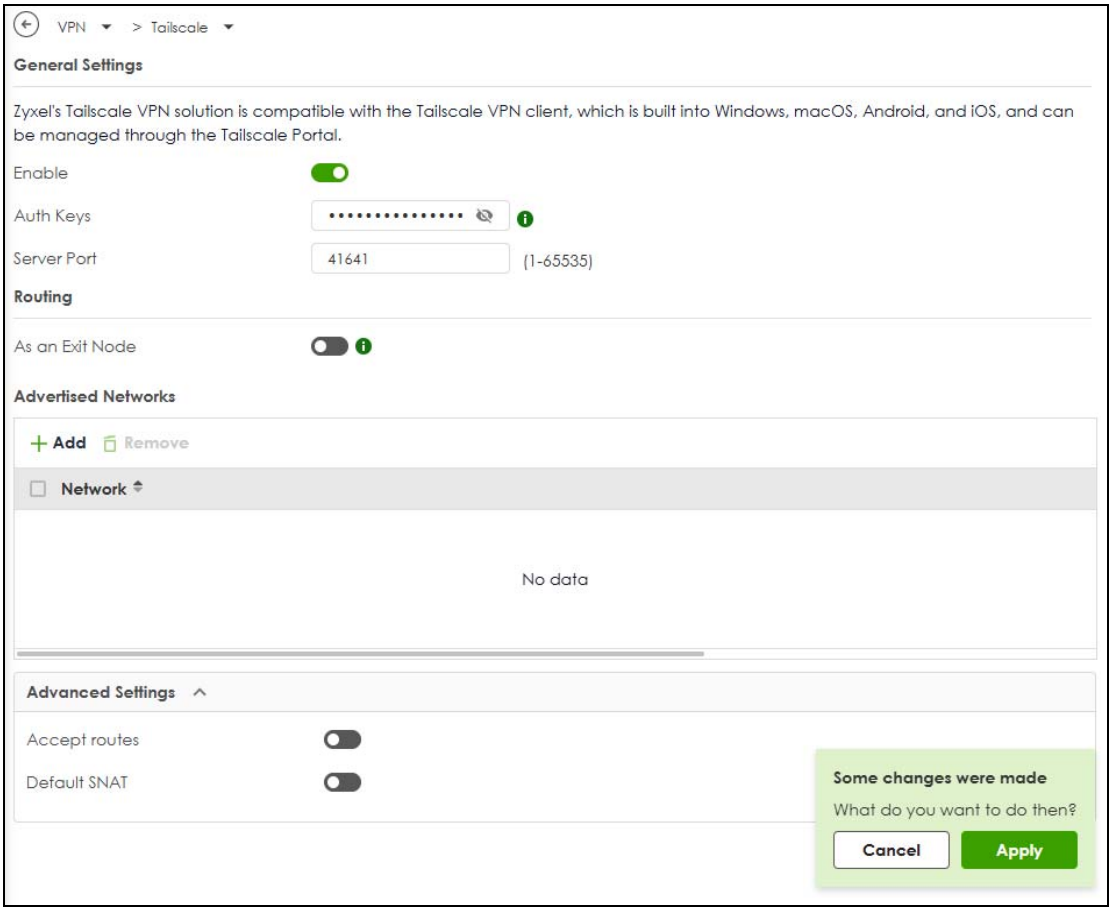
1 First, you need to create an authentication key for your Zyxel Device to join the Tailscale network. Go to **Settings** > **Keys** in the Tailscale admin console, and click **Generate auth key**. The following screen appears. Enter a description to identify the key, then click **Generate key** to create the key.



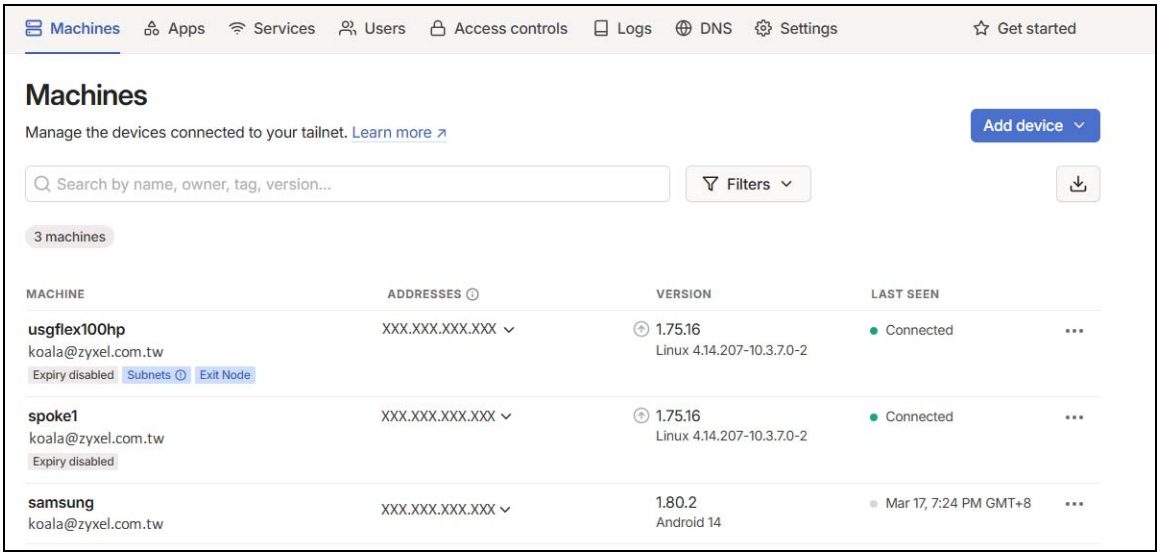
2 The following screen appears. Copy the key to the clipboard and click **Done**. This key will be used to authenticate the Zyxel Device to the Tailscale network. Keep it in a safe place.



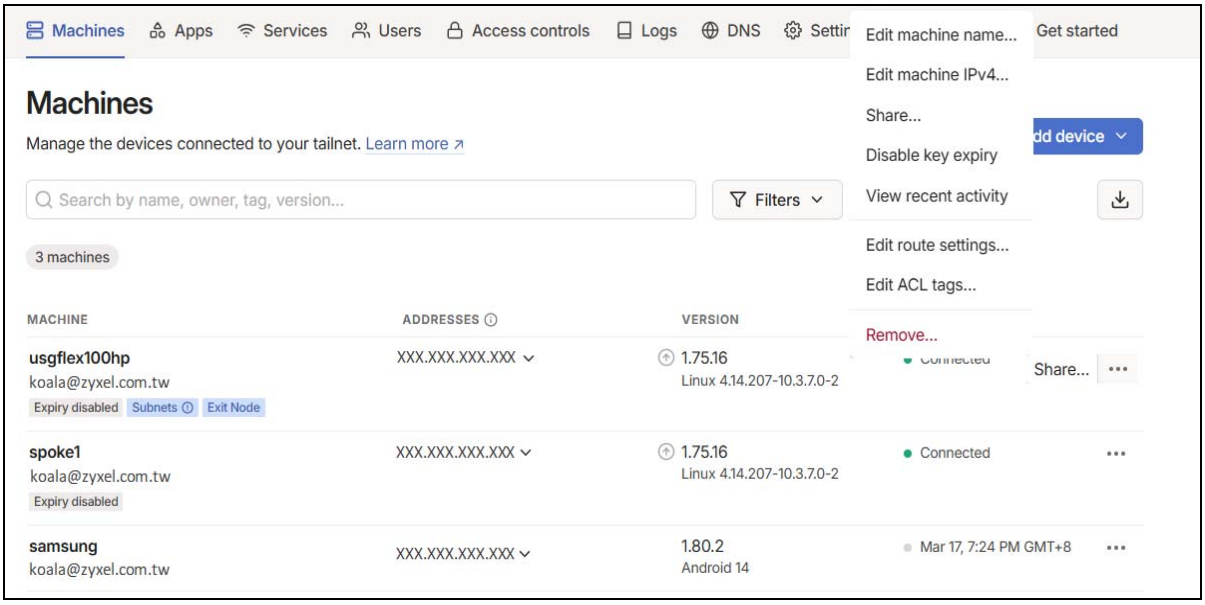
3 Go to **VPN** > **Tailscale** in the Zyxel Device's Web Configurator, enable Tailscale, paste the copied key into the **Auth Keys** field, then click **Apply** to authenticate and connect the Zyxel Device to the Tailscale network.



4 To check if the Zyxel Device has successfully connected to the Tailscale network, go to the **Machines** screen in the Tailscale admin console. Your Zyxel Device should appear in the list.

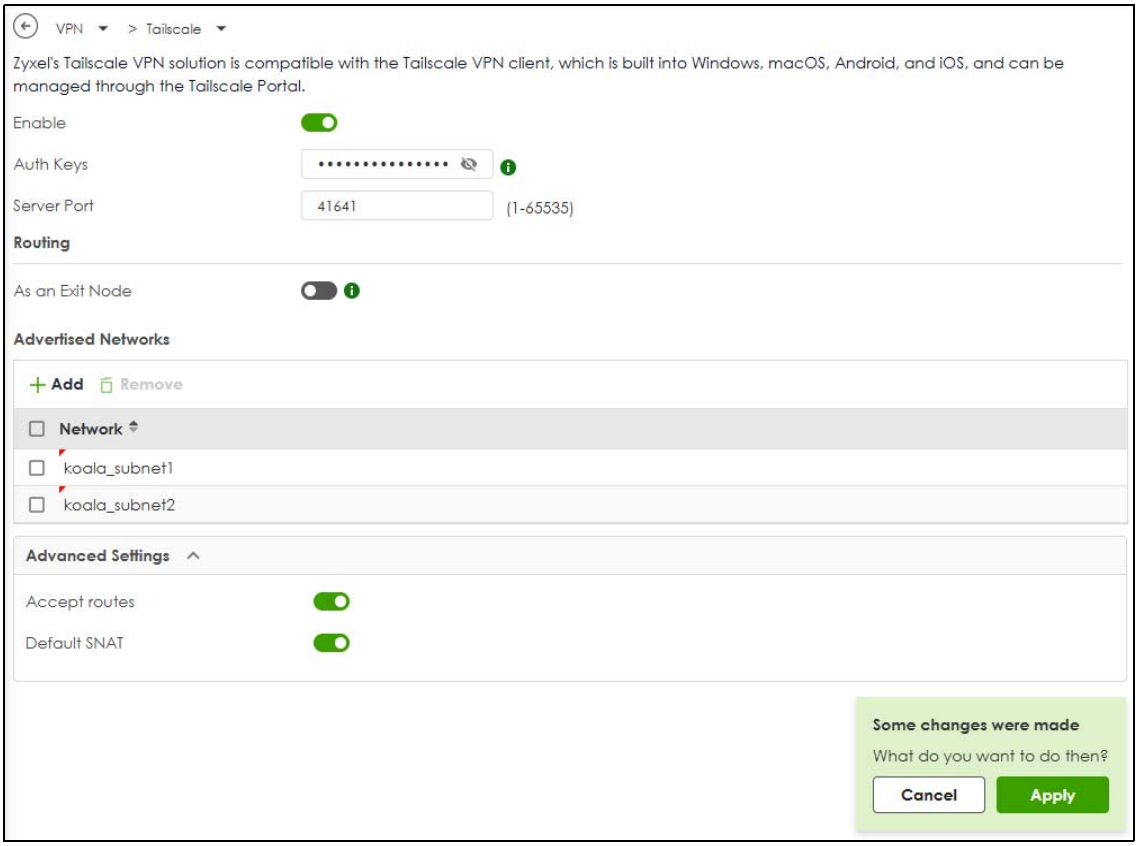


5 To ensure the key never expires, go to the **Machines** screen, click the **More** icon next to your Zyxel Device, then click **Disable key expiry**.

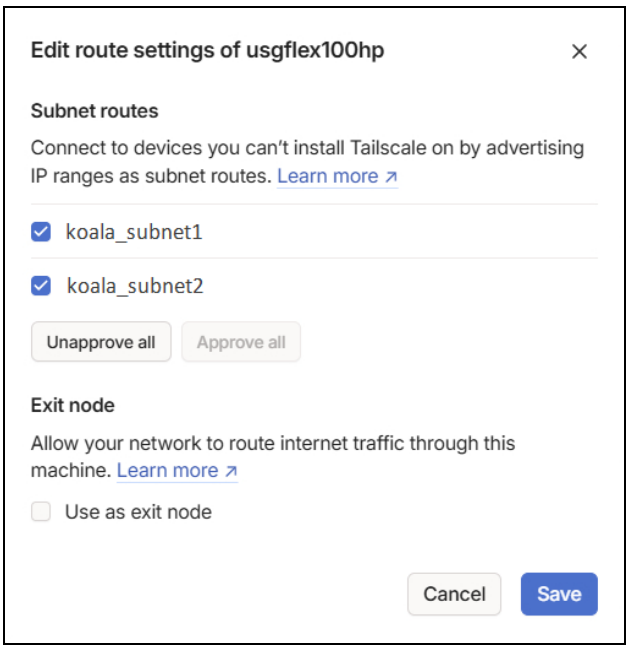


Add Subnets for Tailscale Access

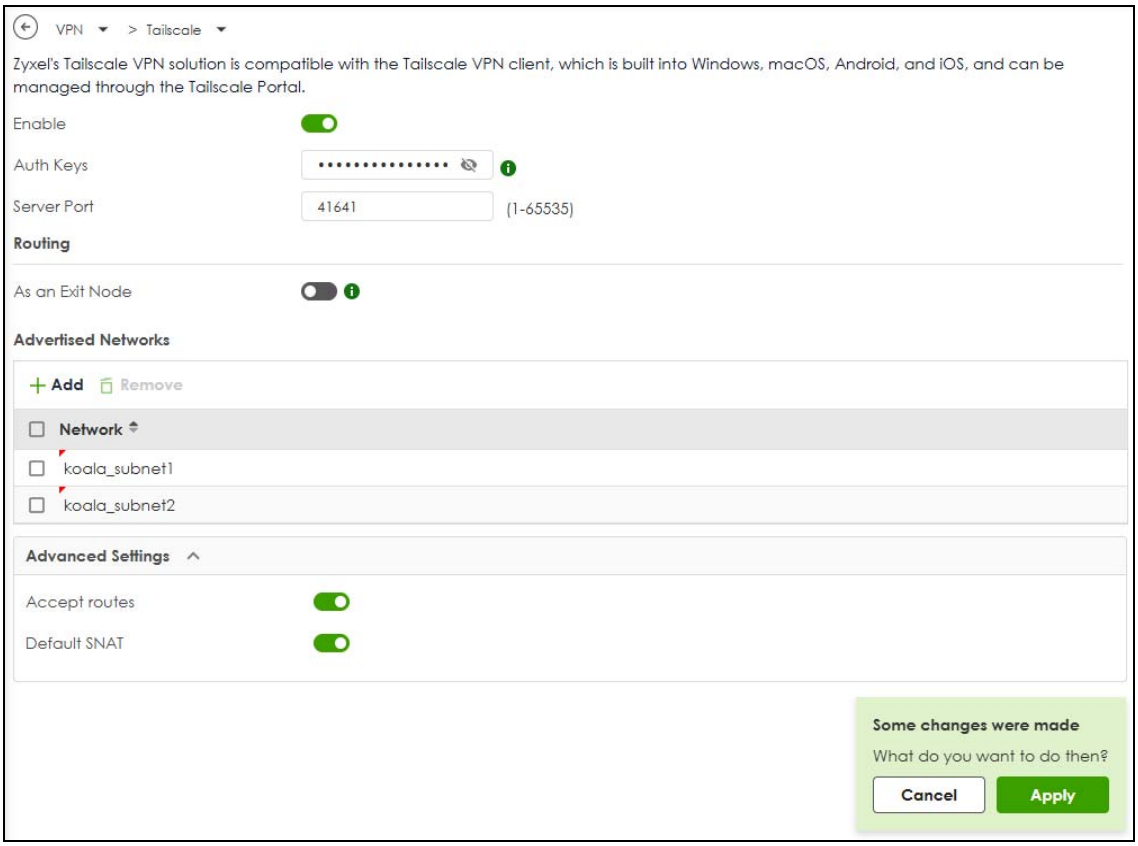
1 Go to **VPN** > **Tailscale** in the Web Configurator, click **Add Advertised Networks**, and select a **SUBNET**-type object to add the subnet on the Zyxel Device for the Tailscale network to access. Click the ✓ icon, then click **Apply** to save the settings.



2 To approve the Zyxel Device's subnets to join Tailscale, go to the **Machines** screen in the Tailscale admin console, click your Zyxel Device from the list. The following screen appears, select the subnet(s) for Tailscale to access, and click **Save**.



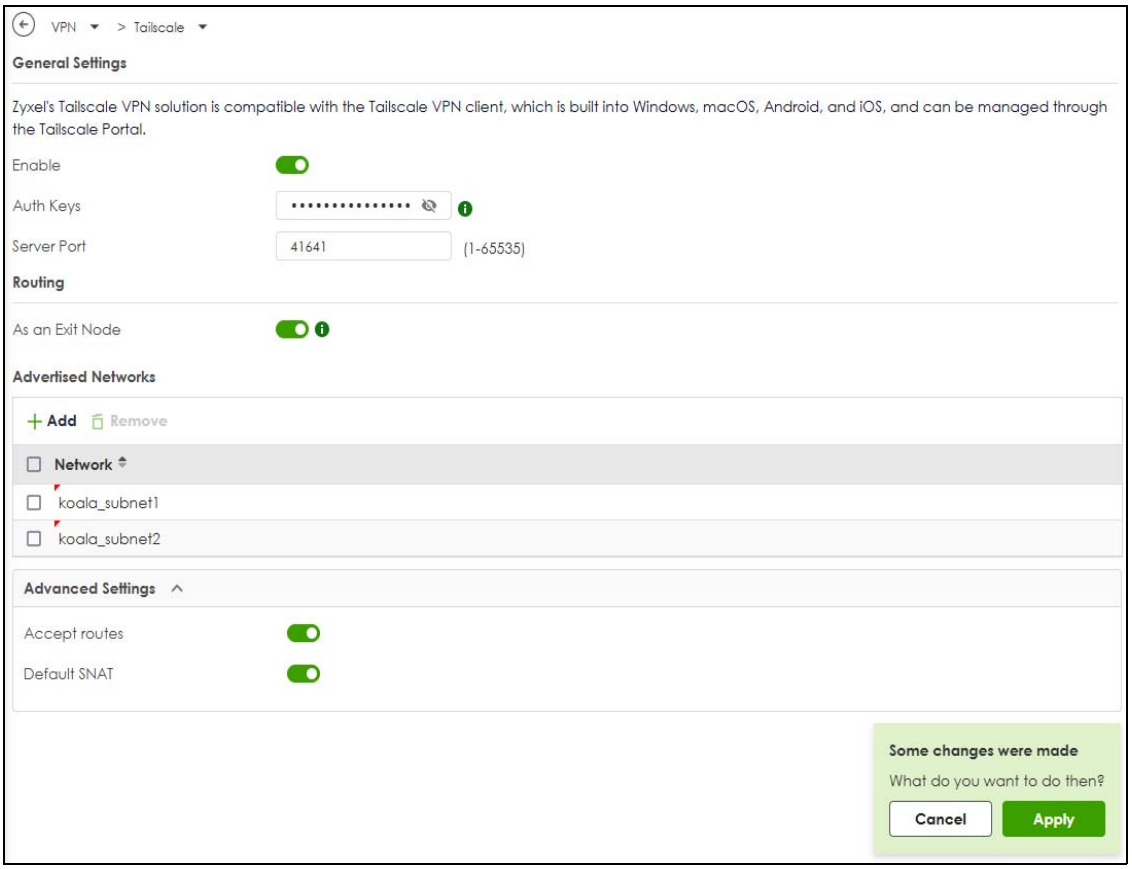
3 To have the Zyxel Device access the subnet behind other sites, go to **VPN** > **Tailscale** in the Web Configurator and enable **Accept routes** and **Default SNAT**, and click **Apply** to save the changes.



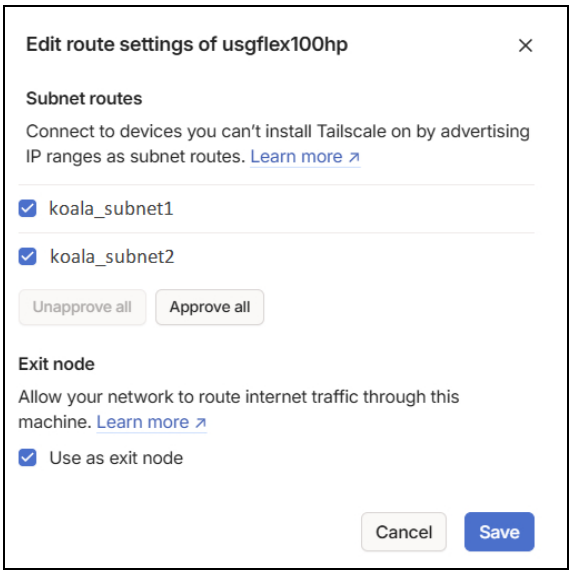
Set the Zyxel Device as an Exit Node

Set the Zyxel Device as an exit node to allow other client devices to route traffic to the Internet through the Zyxel Device. See Section 15.2 on page 278 for more information about exit node.

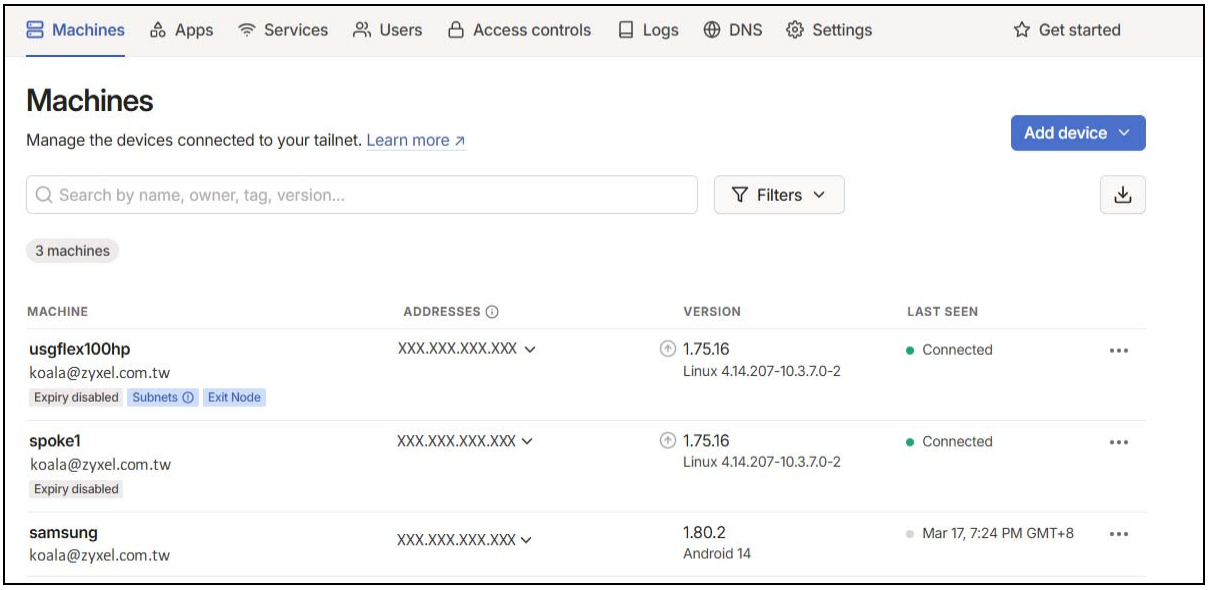
1 Go to **VPN** > **Tailscale** in the Web Configurator and enable **As an Exit Node** on the Zyxel Device.



2 Go to the **Machines** screen in the Tailscale admin console, click your Zyxel Device from the list. The following screen appears, select **Use as exit node**, and click **Save**.



3 In the machine list, your Zyxel Device will be displayed as an exit node.



CHAPTER 16
Security Policy

16.1 Overview

A security policy is a template of security settings that can be applied to specific traffic at specific times. The policy can be applied:

- to a specific direction of travel of packets (from / to)
- to a specific source and destination address objects
- to a specific type of traffic (services)
- to a specific user or group of users
- at a specific schedule

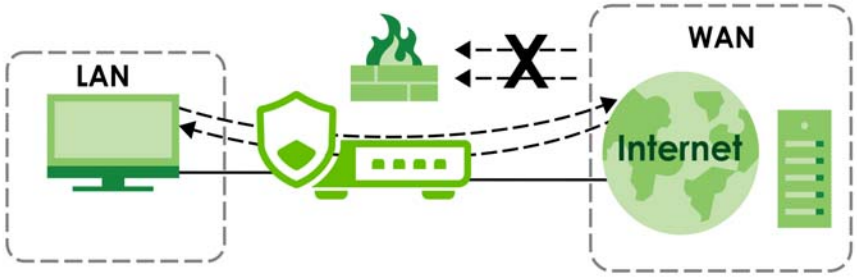
The policy can be configured:

- to allow or deny traffic that matches the criteria above
- send a log or alert for traffic that matches the criteria above
- to apply the actions configured in the profiles (application patrol, content filter, IDP, anti-malware, email security) to traffic that matches the criteria above

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 an SSH session from within the LAN zone and the Zyxel Device allows the response. However, the Zyxel Device blocks incoming SSH traffic initiated from the WAN zone and destined for the LAN zone.

Figure 188 Default Directional Security Policy Example



16.2 What You Can Do in this Chapter

- Use the **Policy Control** screens (Section 16.3 on page 289) to enable or disable policies, asymmetrical routes, and manage and configure policies.

- Use the **DoS Prevention** screens (Section 16.4 on page 296) to detect traffic with protocol anomalies and take appropriate action.
- Use the **IP Spoofing Prevention** screen (Section 16.5 on page 303) to bind IP addresses to MAC addresses.
- Use the **Session Control** screen (Section 16.6 on page 305) to limit the number of concurrent NAT/ Security Policy sessions a client can use.

16.2.1 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. The Zyxel Device has default Security Policy behavior for traffic going through the Zyxel Device in various directions.

Table 128 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-aware 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.

High CPU Usage Caused by Excessive Logging

Logging too many security policies may cause high CPU usage and obscure useful information. For example, logging "any–any" security policies can quickly overload system resources. To reduce CPU usage due to logs, do the following:

- In **Security Policy > Policy Control**, just log dropped or rejected policies that you need to monitor.
- In the **Security Services** menus, only log dropped or rejected packets for critical services.
- In **Log & Report > Log Setting**, only enable important **Log Categories**, enable **Log Consolidation** and set the **Consolidation Interval** to the maximum (600 seconds).

16.3 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.

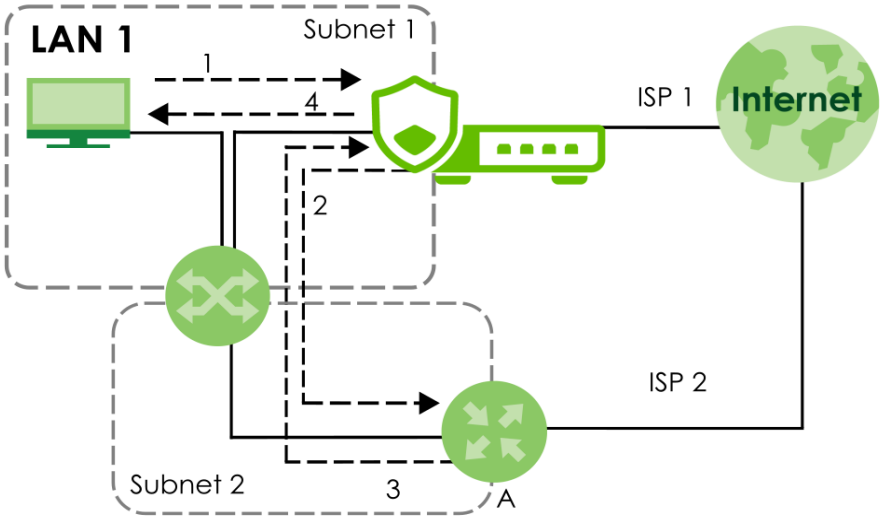
1 A computer on the LAN1 initiates a connection by sending a SYN packet to a receiving server on the WAN.

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 189 Using Virtual Interfaces to Avoid Asymmetrical Routes



16.3.1 Configuring the Security Policy Control Screen

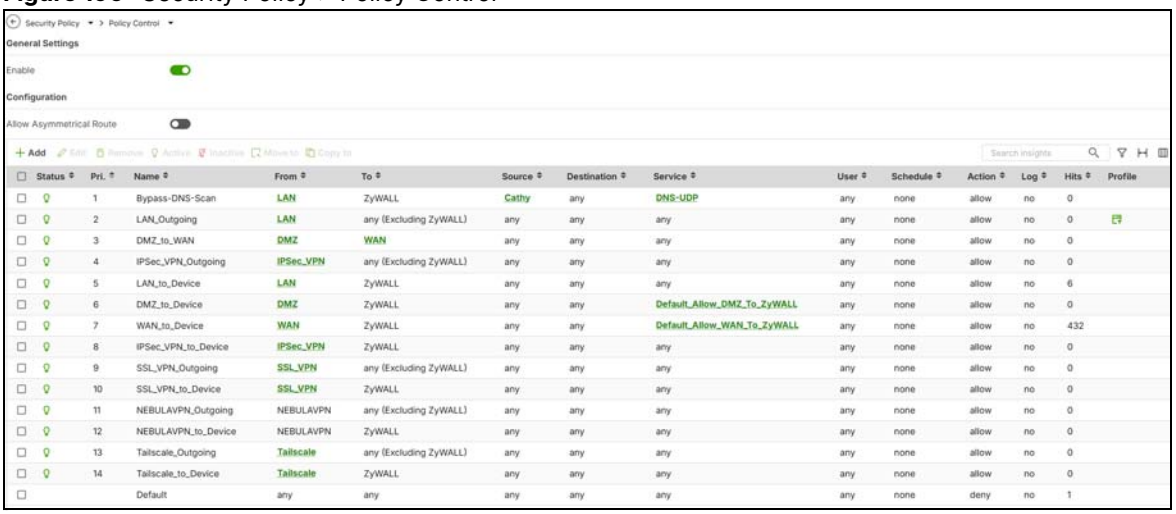
Click **Security Policy > Policy Control** to open the **Policy Control** screen. Use this screen to enable or disable the security policies and asymmetrical routes, set a maximum number of sessions per host, and display the configured Security Policies. Specify from which zone packets come and to which zone packets travel to display only the policies specific to the selected direction. Note the following.

- Besides configuring the security policies, 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 **Policy Control** summary screen.

Figure 190 Security Policy > Policy Control

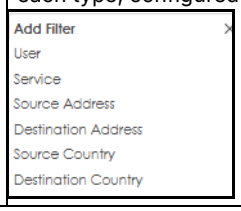


The following table describes the labels in this screen.

Table 129 Security Policy > Policy Control

LABEL	DESCRIPTION
General Settings	Enable or disable the policy control feature on the Zyxel Device.
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 check box 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 if you want to remove it before doing so.
Active	To turn on an entry, select it and click **Activate**.
Inactive	To turn off an entry, select it and click **Inactivate**.
Move to	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.
Copy to	You can create a new policy by copying an existing one to a new position, and then editing it. Select an existing policy and click **Copy** to display a field to type a number for where you want to put that policy, then press [ENTER] to copy the policy to the number that you typed. After copying it, edit it to change it from the one copied.

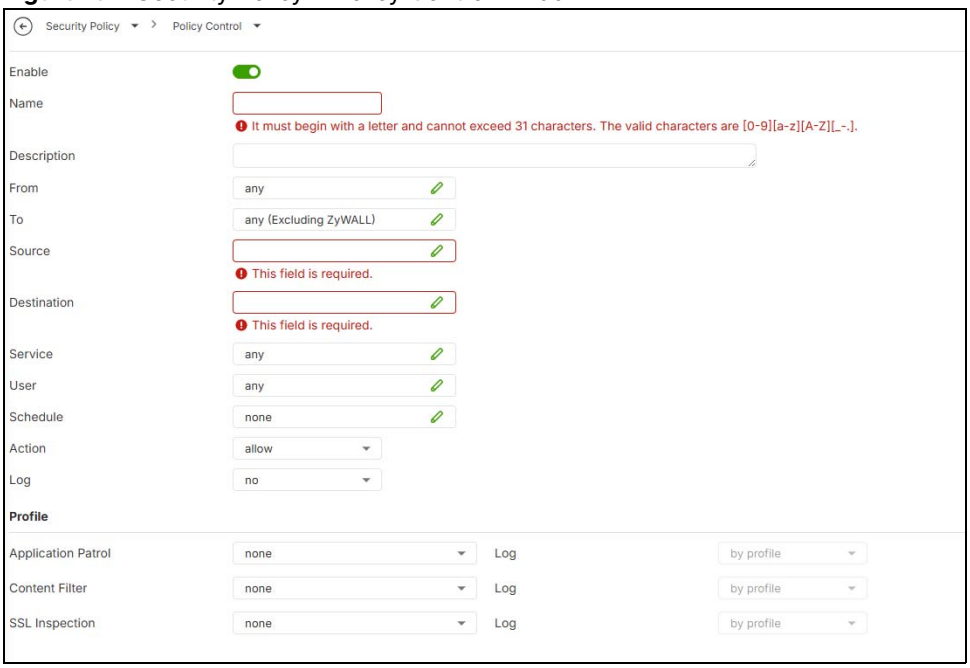
Table 129 Security Policy > Policy Control (continued)

LABEL	DESCRIPTION
Search	Type an item in the search box, then click this to display all sessions in the table below according to the item you typed.
Clear All	Click this to remove all items found in the search.
Filter	Click the Filter icon, click + to expand **Policy Match,** pick a filter, then click **Find** to display specific sessions according to the filter selected. You may select multiple filters, but just one of each type, configured one at a time. 
The following read-only fields summarize the policies you have created that apply to traffic traveling in the selected packet direction.	
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
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.
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.
Source	This displays the IPv4 source address object, including geographic address and FQDN (group) objects, to which this Security Policy applies.
Destination	This displays the IPv4 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 (application patrol, content filter and SSL inspection) apply to the policy control rule. Click the icon to edit the profile directly.

16.3.2 The Policy Control Add/Edit Screen

In the **Policy Control** screen, click the **Edit** or **Add** icon to display the **Policy Control Edit or Add** screen.

Figure 191 Security Policy > Policy Control > Add



The following table describes the labels in this screen.

Table 130 Security Policy > Policy Control > Add

LABEL	DESCRIPTION
Enable	Select this check box to activate the policy control.
Name	Type a name with 1 to 30 single-byte characters to identify the policy, including a-zA-Z0-9. Special characters and spaces are not allowed.
Description	Enter a descriptive name of 1 to 30 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. **ZyWALL** means packets destined for the Zyxel Device itself.
Source	Select an IPv4 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 addresses. Note: If you select an FQDN address with a wildcard in this field, the rule might not be applied because an FQDN with a wildcard cannot cache IP addresses using DNS queries on the Zyxel Device.
Destination	Select an IPv4 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 addresses.
Service	Select a service or service group from the drop-down list box.

Table 130 Security Policy > Policy Control > Add (continued)

LABEL	DESCRIPTION
User	Select a user or user group to which to apply the policy. The Security Policy is activated only when the specified user logs into your network. Otherwise, select **any** and there is no need for user logging. You can click **+Add Object** or **+Add Group** to create a user object or group and apply this policy to it. See Section 28.1 on page 459 for the user types and the necessary configuration for each type. Note: If you specified a source IP address, 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	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 **Security Services** 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.
Application Patrol	Select an Application Patrol profile from the list box; **none** displays if no profiles have been created in the **Security Service > App Patrol** screen.
Content Filter	Select a Content Filter profile from the list box; **none** displays if no profiles have been created in the **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 **Security Service > SSL Inspection** screen.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

16.3.3 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 131 Address Object Configuration Example

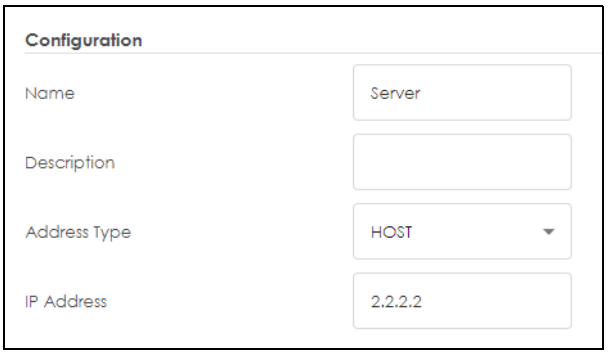
NAME	ADDRESS TYPE	IP ADDRESS
Server	Host	2.2.2.2

Table 132 Security Policy Configuration Example

NAME	FROM	TO	SOURCE	DESTINATION	SERVICE	ACTION	LOG
LAN_to_Device	LAN	ZyWALL	Server	Any	Ping	Allow	No

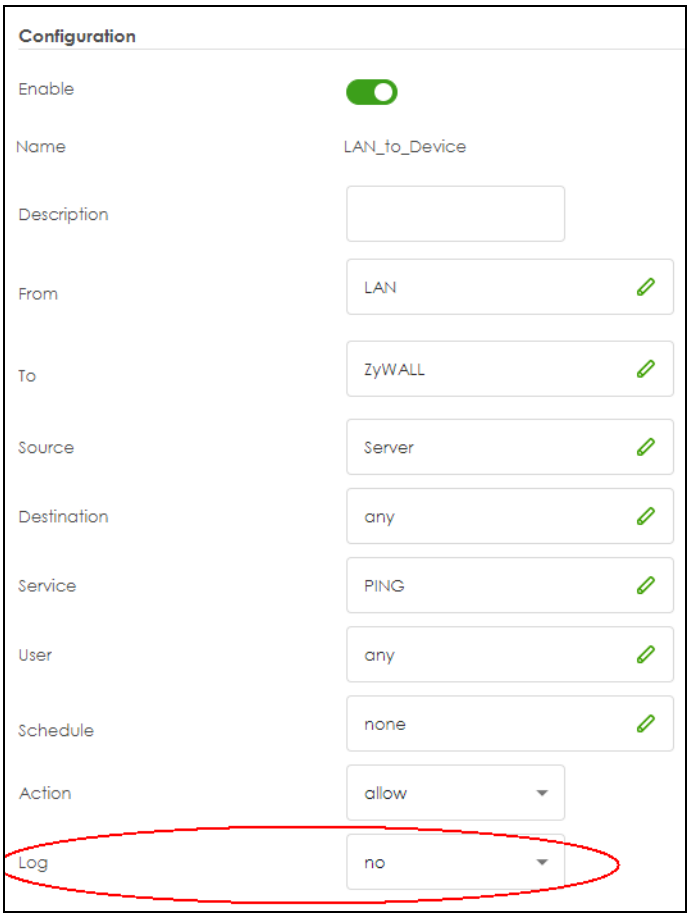
1 Go to **Object** > **Address** > **Address** and click **Add**.

2 Configure the settings using the parameters given in Table 131 on page 294. Click **Apply** to save your changes.



3 Go to **Security Policy** > **Policy Control** and click **Add**.

4 Configure the settings using the parameters given in Table 132 on page 295. Set **Log** to **no** so when the server pings the Zyxel Device, the Zyxel Device will not create logs. Click **Apply** to save your changes.



16.4 DoS Prevention Overview

DoS attacks can flood your Internet connection with invalid packets and connection request, using so much bandwidth and so many resources that Internet access becomes unavailable. The goal of DoS attacks is not to steal information, but to disable a device or network on the Internet.

DoS prevention protects against anomalies based on violations of protocol standards (RFCs – Requests for Comments) and abnormal flows such as port scans. This section introduces DoS prevention profiles and applying a DoS prevention profile to a traffic direction.

Traffic Anomalies

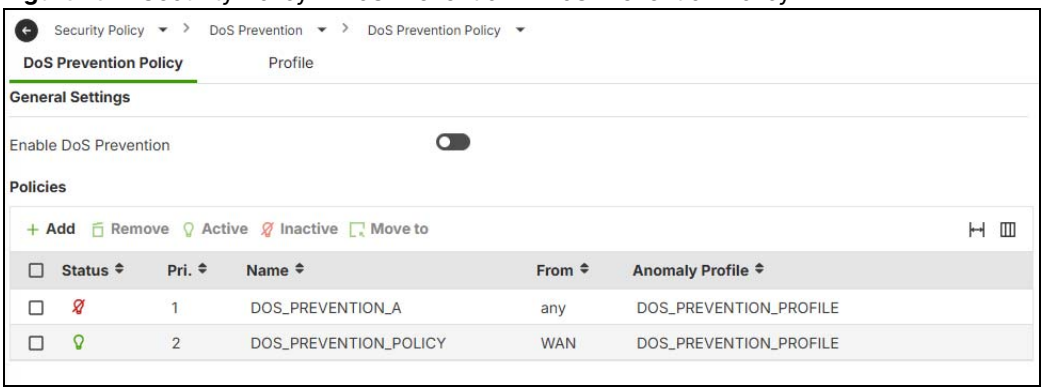
Traffic anomaly policies look for abnormal behavior or events such as port scanning, sweeping or network flooding. They operate at OSI layer-3 and layer-4. Traffic anomaly policies may be updated when you upload new firmware.

Note: First, create a DoS prevention profile in the In the **Security Policy > DoS Prevention > Profile** screen. Then, apply the profile to traffic originating from a specific zone in the **Security Policy > DoS Prevention > DoS Prevention Policy** screen.

16.4.1 The DoS Prevention Policy Screen

Click **Security Policy > DoS Prevention > DoS Prevention Policy** to display the next screen.

Figure 192 Security Policy > DoS Prevention > DoS Prevention Policy



The following table describes the labels in this screen.

Table 133 Security Policy > DoS Prevention > DoS Prevention Policy

LABEL	DESCRIPTION
General Settings	
Enable DoS Prevention	Select this to enable DoS 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.
Active	To turn on an entry, select it and click **Activate**.
Inactive	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.
Priority	This is the rank in the list of anomaly profile policies. The list is applied in order of priority.
Name	This is the name of the anomaly profile policy.

Table 133 Security Policy > DoS Prevention > DoS Prevention Policy

LABEL	DESCRIPTION
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 via 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.

16.4.2 The DoS Prevention Profile Screen

Create new DoS prevention profiles in the **Security Policy > DoS Prevention > Profile** screens.

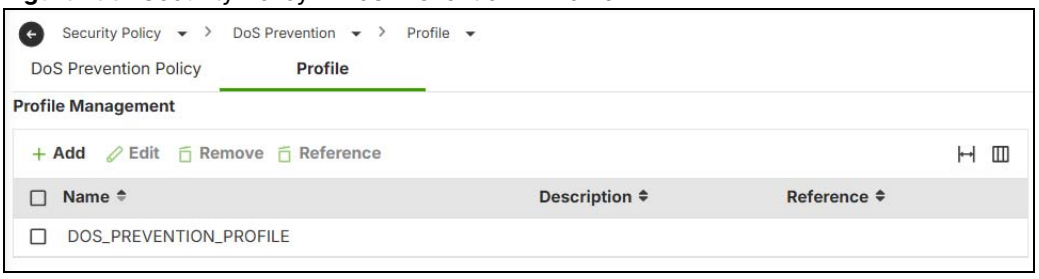
When creating DoS prevention profiles. you may find that certain policies are triggering too many false positives or false negatives. A false positive is when valid traffic is flagged as an attack. A false negative is when invalid traffic is wrongly allowed to pass through the Zyxel Device. As each network is different, false positives and false negatives are common on initial DoS prevention 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.

DoS prevention profiles consist of traffic anomaly profiles. To create a new profile, click **Add**. Type a new profile name, enable or disable individual policies and then edit the default log options and actions.

Click **Security Policy > DoS Prevention > Profile** to view the following screen.

Figure 193 Security Policy > DoS Prevention > Profile



The following table describes the labels in this screen.

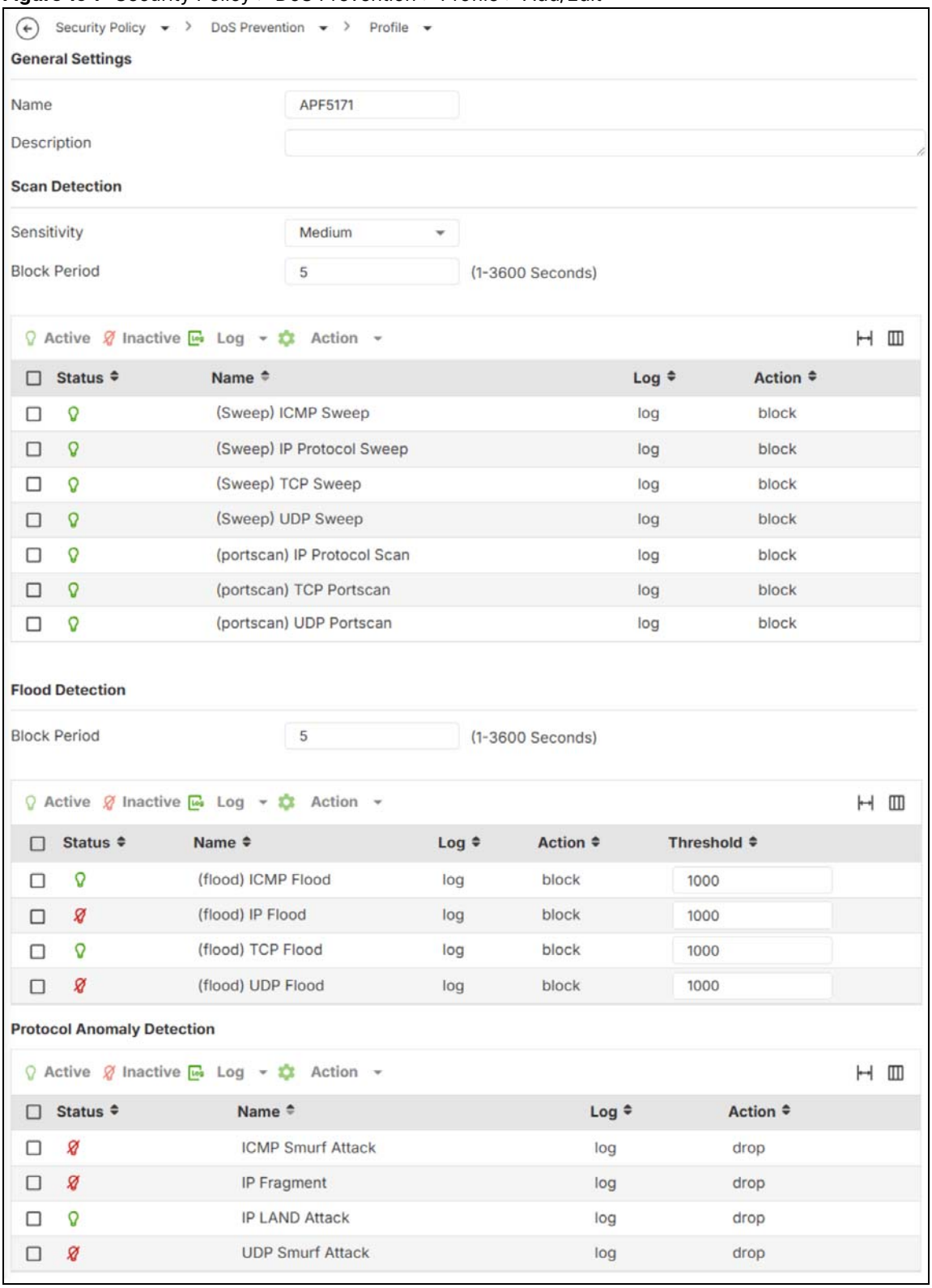
Table 134 Security Policy > DoS Prevention > Profile

LABEL	DESCRIPTION
Profile Management	Create ADP profiles here and then apply them in the **Security Policy > DoS Prevention > DoS Prevention Policy** screen.
Add	Click **Add** to create a new profile.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Reference	Select an entry and click **Reference** to check which settings use the entry.
Name	This is the name of the profile you created.
Description	This is the description of the profile you created.
Reference	This displays the number of rules that currently use this entry.

16.4.3 The Dos Prevention Profile Add/Edit Screen

DoS prevention looks for abnormal behavior such as scan or flooding attempts. In the **Security Policy > DoS Prevention > Profile** screen, click the **Edit** or **Add** icon to create or edit an existing profile.

Figure 194 Security Policy > DoS Prevention > Profile > Add/Edit



The following table describes the labels in this screen.

Table 135 Security Policy > DoS Prevention > Profile > Add/Edit

LABEL	DESCRIPTION
General Settings	
Name	A name is automatically generated that you can edit. The name must be the same in the DoS Prevention screens for the same DoS prevention 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 DoS prevention profile.
Scan 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.
Sensitivity	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	If the Zyxel Device detects possible scan attack packets, such as port scanning, specify the time in seconds that the Zyxel Device blocks the source IP address from which the packets are coming.
Active	To turn on an entry, select it and click **Active**.
Inactive	To turn off an entry, select it and click **Inactive**.
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.
Status	The active (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.
Flood Detection	Flood detection tries to find attacks that saturate a network with a large number of packets, use up all available bandwidth, and so aim to make communications on the network impossible.

Table 135 Security Policy > DoS Prevention > Profile > Add/Edit (continued)

LABEL	DESCRIPTION
Block Period	If the Zyxel Device detects a large number of packets, that are possibly attempting to flood your network, specify the time in seconds that the Zyxel Device blocks the source IP address from which the packets are coming.
Active	To turn on an entry, select it and click **Active**.
Inactive	To turn off an entry, select it and click **Inactive**.
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.
Status	The active (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.
Threshold	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.
Protocol Anomaly Detection	The supported detections include: • ICMP Smurf Attack An ICMP Smurf attack is a distributed denial-of-service (DDoS) attack that floods a target (victim) with pings (ICMP echo request packets) where the source IP address is spoofed as the victim's IP address. The destination IP address of each packet is the broadcast address of the network, so all hosts on the network reply to the victim at once, overwhelming the victim. • UDP Smurf Attack A UDP Smurf attack is a distributed denial-of-service (DDoS) attack that floods a target (victim) with small UDP requests where the source IP address spoofed as the victim's IP address. Servers reply with responses to the victim, overwhelming the victim. The Zyxel Device detects the attack when it receives a UDP packet in which the destination IP address matches the broadcast address of the network and the destination port is 7 or 19. • IP Fragment The Zyxel Device detects IP fragments when it receives packets with malformed, overlapping, or oversized fragments. • IP LAND Attack A LAND attack sends a spoofed packet where the source IP address is the same as destination IP address, so the victim replies to itself, causing DoS and making the victim unavailable.
Active	To turn on an entry, select it and click **Active**.
Inactive	To turn off an entry, select it and click **Inactive**.

Table 135 Security Policy > DoS Prevention > Profile > Add/Edit (continued)

LABEL	DESCRIPTION
Log	To edit a policy's log option, select the policy and click this. 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 traffic matches a policy, select the policy and click this. **None**: The Zyxel Device takes no action when traffic matches the policy. **Drop**: The Zyxel Device silently drops packets that match the policy. Neither the sender nor the receiver is notified.
Status	The active (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This is the name of the 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 a policy and click the **Log** icon above.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

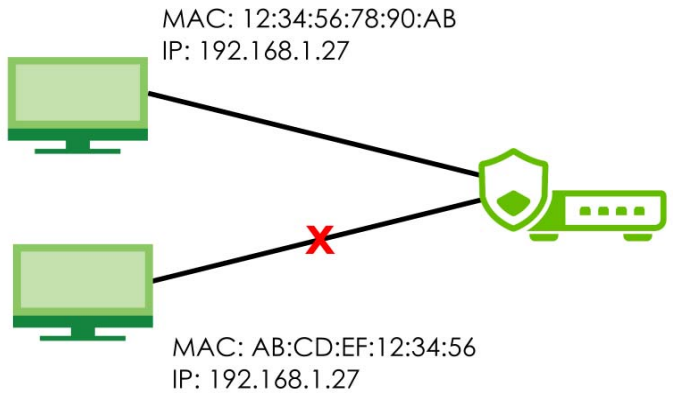
16.5 IP Spoofing Prevention Overview

Trusted IP/MAC Pair

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 195 Trusted IP/MAC Pair Example



16.5.1 The IP Spoofing Prevention Screen

Click **Security Policy** > **IP Spoofing Prevention** to display the **IP Spoofing Prevention** screen. Use this screen to configure an interface's IP to MAC address binding settings.

Figure 196 Security Policy > IP Spoofing Prevention



The following table describes the labels in this screen.

Table 136 Security Policy > IP Spoofing Prevention

LABEL	DESCRIPTION
Source IP Spoofing Prevention	
Enable	Click to slide the switch to the right to enable IP spoofing prevention.
Log	Select whether to have the Zyxel Device generate a log (**log**), log and alert (**log alert**) or neither (**no**) if a device connected to this interface attempts to use an IP address that is bound to another device's MAC address.
Enable Interface	Select the interface to enforce links between specific IP addresses and specific MAC addresses on this interface. 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.
Trusted IP/MAC Pair	
Include DHCP Leasing Entries	Enable this to allow traffic from devices that is listed in the current DHCP table. To manage the list of DHCP-assigned IP addresses, click **Include DHCP Leasing Entries** to go to the **Network** > **DHCP Table** screen.
Add	Click this to create a new entry.
Remove	Select an entry and click this to delete it.
Interface	This field displays the name of the interface within the Zyxel Device.
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.
Trusted IP	

Table 136 Security Policy > IP Spoofing Prevention (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.
Object Name	This is the name of the IP address object to allow traffic.
Description	This is the description of the profile you created.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

16.5.2 The Trusted IP Add / Edit Screen

In the **Security Policy > IP Spoofing Prevention** screen, click the **Edit** or **Add** icon to create or edit an existing profile.

Figure 197 Security Policy > IP Spoofing Prevention > Trusted IP Add/Edit



The following table describes the labels in this screen.

Table 137 Security Policy > IP Spoofing Prevention > Trusted IP Add/Edit

LABEL	DESCRIPTION
Trusted IP	
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.
Object Name	Select an IP address object to allow traffic from all devices with that IP address.
Description	This helps identify the entry.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

16.6 The Session Control Screen

Click **Security Policy > Session Control** to display the **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 198 Security Policy > Session Control



The following table describes the labels in this screen.

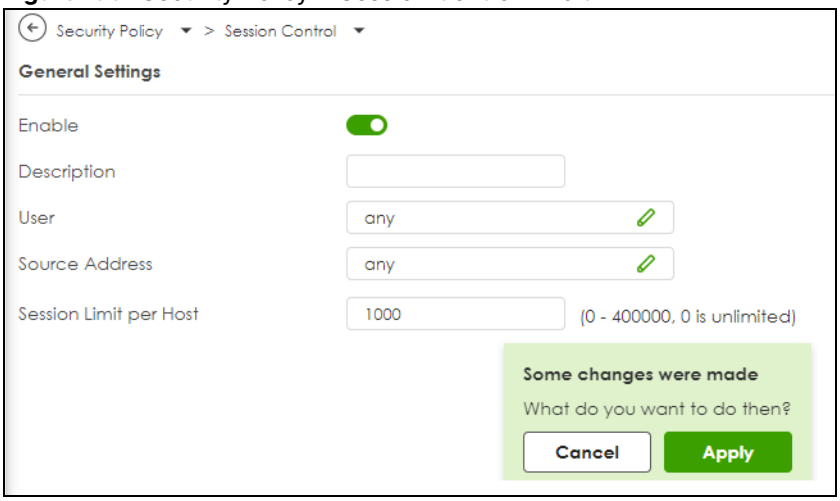
Table 138 Security Policy > Session Control

LABEL	DESCRIPTION
General Settings	
Session Control	Click to slide the switch to the right to enable session control.
Default Session per Host	Use this field to set a common limit to the number of concurrent NAT/Security Policy sessions each client computer can have. '0' means unlimited. 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.
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	To change a rule's position in the numbered list, select the rule and click **Move to** 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 priority number.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Priority	This is the priority of a session limit rule. Rules are applied according to priority number.
User	This is the user name or user group name to which this session limit rule applies.
Source IP	This is the IP address of the host 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.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

16.6.1 The Session Control Add/Edit Screen

Click **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 199 Security Policy > Session Control > Edit



The following table describes the labels in this screen.

Table 139 Security Policy > Session Control > Add/Edit

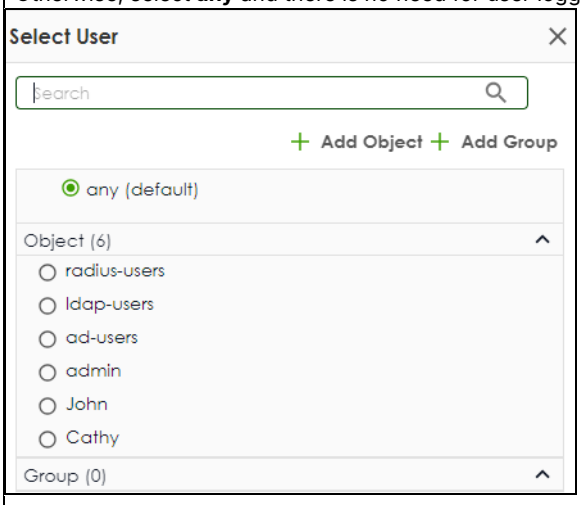
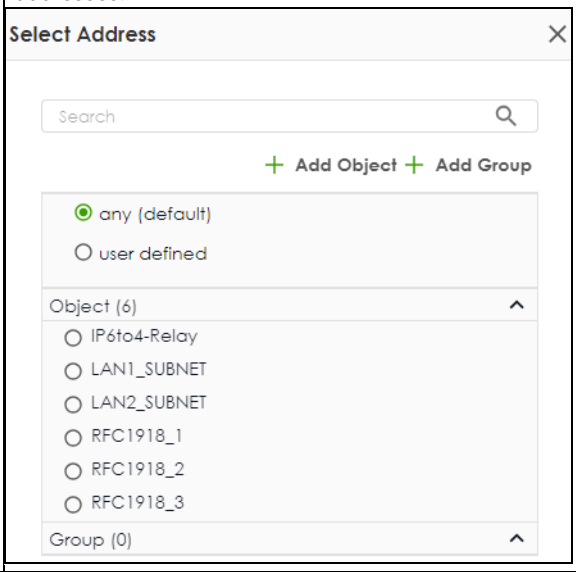
LABEL	DESCRIPTION
Enable	Click to slide the switch to the right to turn on this session limit rule.
Description	Enter information to help you identify this rule. Use up to 60 printable ASCII characters. Spaces are allowed.
User	Select a user name or user group to which to apply the rule. The rule is 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.

Table 139 Security Policy > Session Control > Add/Edit (continued)

LABEL	DESCRIPTION
Address	Select the IPv4/IPv6 source address (range) or address group, including geographic address (group) object, to which this rule applies. Select **any** to apply the rule to all IPv4 source addresses. 
Session Limit per Host	Use this field to set a limit to the number of concurrent NAT/Security Policy sessions this rule's users or addresses can have. For this rule's users and addresses, this setting overrides the **Default Session per Host** setting in the general **Security Policy Session Control** screen.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

16.7 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 200 Blocking All LAN to WAN IRC Traffic Example



Your Security Policy would have the following settings.

Table 140 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.

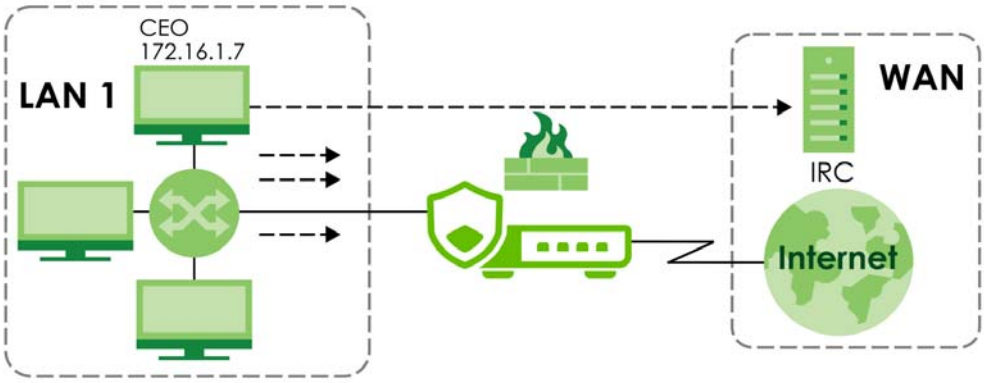
Now suppose you need to let the CEO use IRC. You configure a LAN1 to WAN security policy that allows IRC traffic from the IP address of the CEO's computer. You can also configure a LAN to WAN policy that allows IRC traffic from any computer through which the CEO logs into the Zyxel Device with his/her 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 201 Limited LAN to WAN IRC Traffic Example



Your security policy would have the following configuration.

Table 141 Limited LAN1 to WAN IRC Traffic Example 1

#	USER	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	Any	172.16.1.7	Any	Any	IRC	Allow

Table 141 Limited LAN1 to WAN IRC Traffic Example 1 (continued)

#	USER	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
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 142 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 17
Captive Portal

17.1 Overview

Use this screen to configure captive portal settings for each interface. A captive portal is a designated login web page for client authentication before network access.

The policy can be applied:

- to a specific interface or zone
- with the walled garden feature
- to a specific client or group of clients

The policy can be configured:

- to exempt specific source and destination address objects
- to exempt specific type of traffic
- to use with HTTP or HTTPS server

17.2 What You Can Do in This Chapter

Use the **Authentication Policy** screens (Section 17.3 on page 312) to configure the policy of the captive portal.

17.2.1 What You Need to Know

Walled Garden

With a walled garden, you can define one or more web site addresses that all clients can access without logging in. These can be used for advertisements for example.

HSTS

HSTS (HTTP Strict Transport Security) is a web security policy that instructs browsers to always use HTTPS to prevent unencrypted connections. This protects users from man-in-the-middle attacks and protocol downgrade attacks.

Redirect TCP Port 443 Traffic to Login Page

The table below shows scenarios for enabling or disabling the ‘Redirect TCP Port 443 Traffic to Login Page’ option in a captive portal policy.

Table 143 Redirect TCP Port 443 Traffic to Login Page

SCENARIO	DISABLED (DEFAULT)	ENABLED
Access HTTP website	Browser redirected to Captive Portal landing page	Browser redirected to Captive Portal landing page
Access HTTPS website without HSTS	Browser cannot load page and shows ‘Site cannot be reached’	Browser shows certificate warning and requires user to proceed
Access HTTPS website with HSTS	Browser cannot load page and shows ‘Site cannot be reached’	Browser shows certificate warning and does not allow user to proceed
Access with Captive Network Assistance (CNA)	Pop-up browser redirected to Captive Portal landing page	Pop-up browser redirected to Captive Portal landing page

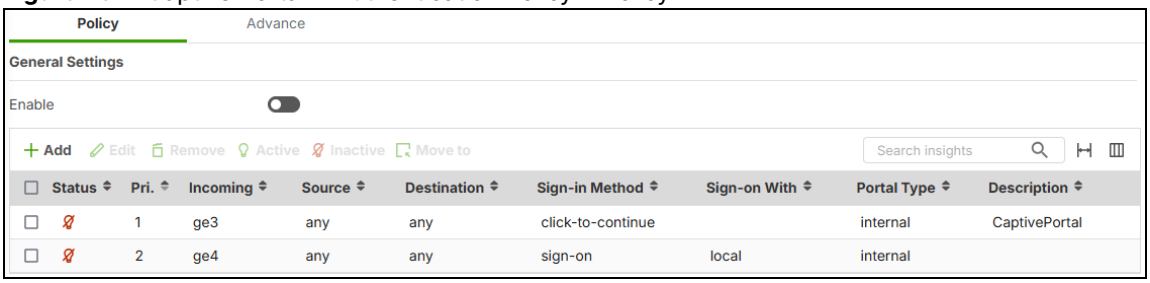
17.3 Authentication Policy Overview

Use this screen to configure the authentication policy that the captive portal applies to control client’s access.

17.3.1 The Policy Screen

Click **Captive Portal** > **Authentication Policy** > **Policy** to display the **Policy** screen. Use this screen to configure the authentication policy for the captive portal.

Figure 202 Captive Portal > Authentication Policy > Policy



The following table describes the labels in this screen.

Table 144 Captive Portal > Authentication Policy > Policy

LABEL	DESCRIPTION
General Settings	
Enable	Click to slide the switch to the right to activate captive portal on 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 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 if you want to remove it before doing so.

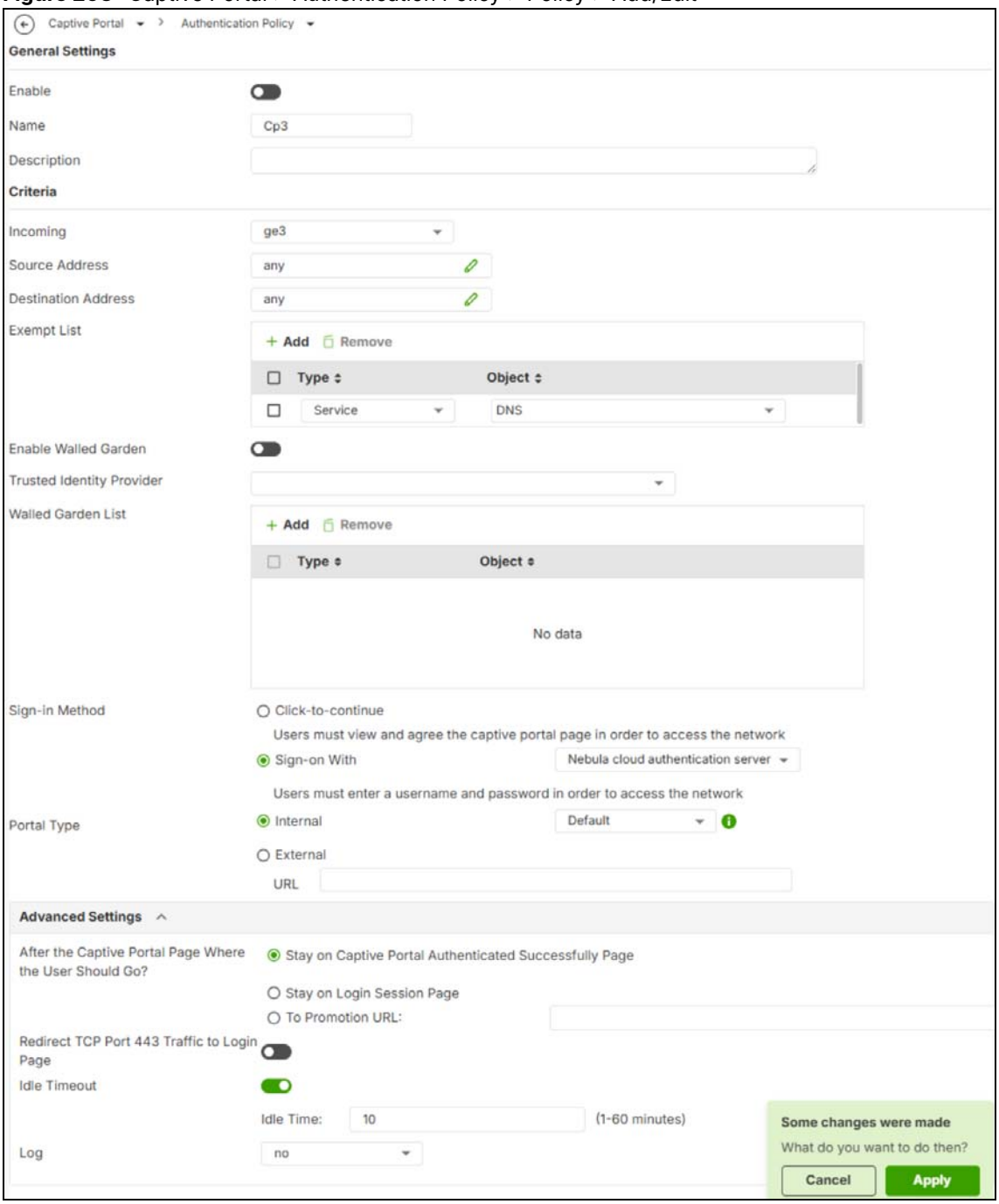
Table 144 Captive Portal > Authentication Policy > Policy (continued)

LABEL	DESCRIPTION
Active	To turn on an entry, select it and click **Active**.
Inactive	To turn off an entry, select it and click **Inactive**.
Move to	To change a policy's priority in the list, select the policy and click **Move to**. Enter the desired priority number for the selected policy and press [ENTER].
Search	Enter an item in the search box, then click this to display all sessions in the table below according to the item you entered.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Pri.	This field displays the policy's priority. The policies are applied in this numerical order. You can use **Move to** to change the order (priority).
Name	This field displays the name of the policy.
Incoming	This field displays the interface or zone that enforces the policy.
Source	This field displays the object or group whose outgoing traffic the policy will apply to.
Destination	This field displays the object or group whose incoming traffic the policy will apply to.
Sign-in Method	This field displays the authentication server that enforces the policy.
Sign-on With	This field displays the sign in method of the policy.
Portal Type	This field displays the portal type of the policy.
Description	This field displays the description of the policy.

17.3.2 The Policy Add/Edit Screen

In the **Captive Portal** > **Authentication Policy** > **Policy** screen, click the **Add** or **Edit** icon to create or edit an existing profile.

Figure 203 Captive Portal > Authentication Policy > Policy > Add/Edit



The following table describes the labels in this screen.

Table 145 Captive Portal > Authentication Policy > Policy > Add/Edit

LABEL	DESCRIPTION
General Settings	
Enable	Slide the switch to the right to enable the policy.
Name	Enter a name for the policy.
Description	Enter a description for the policy.

Table 145 Captive Portal > Authentication Policy > Policy > Add/Edit (continued)

LABEL	DESCRIPTION
Criteria	
Incoming	Select an interface or zone from the drop-down list to enforce the policy on the incoming traffic from the selected interface or zone interface member. Select **any** to enforce the policy on any incoming traffic from internal interfaces. Note: The captive portal will not function on external and general interfaces. If the selected zone includes both an external interface and the internal interface 'ge3', the captive portal will function only on 'ge3'.
Source Address	Select an object or group from the drop-down list to enforce the policy on traffic from the selected object or group members. Select **any** to apply the policy to all traffic from IPv4 addresses.
Destination Address	Select an object or group from the drop-down list to enforce the policy on traffic to the selected object or group members. Select **any** to apply the policy to all traffic going to IPv4 addresses.
Exempt List	Create a list to exempt specific traffic from the policy. You can exempt traffic by source IP address or service. Select an entry from the list to exempt specific traffic with that IP address or service from captive portal authentication.
Add	Click this to create a new entry.
Remove	Select an entry and click this to delete it.

Table 145 Captive Portal > Authentication Policy > Policy > Add/Edit (continued)

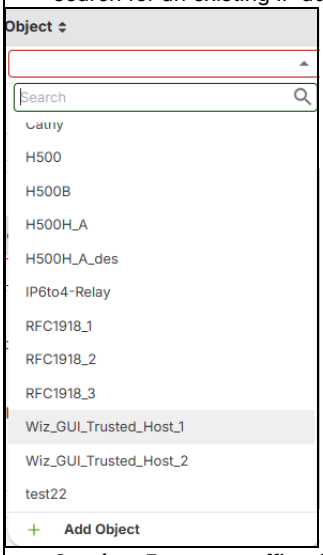
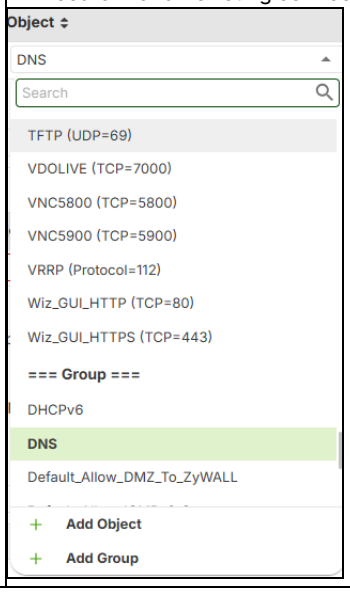
LABEL	DESCRIPTION
Type	Select the type of traffic: • **Source IP:** Exempts traffic with a specific source destination ports or IP protocol. You may search for an existing IP address object or create a new one.  • **Service**: Exempts traffic with a specific service port, such as 21 for FTP traffic. You may search for an existing service (group) object or create a new one. 

Table 145 Captive Portal > Authentication Policy > Policy > Add/Edit (continued)

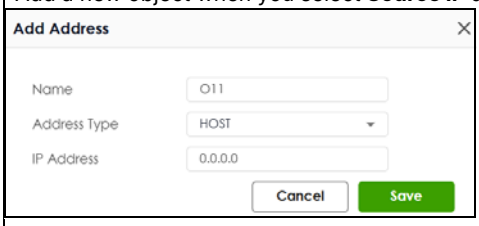
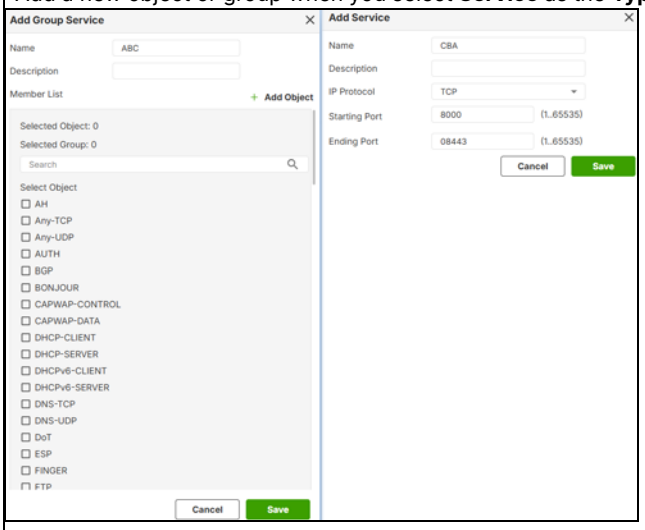
LABEL	DESCRIPTION
Object	Select an object of IP address or service you created. To create an object, click **Add Object**. Add a new object when you select **Source IP** as the **Type**:  • **Name**: Enter the name of this object. It must begin with a letter and cannot exceed 31 characters. The valid characters are A-Z, a-z, 0-9, underscores (_), dashes (-), and dots (.). Spaces are not allowed. • **Address Type**: Select the address type of this object from the drop-down list. • **IP Address**: Enter the source IP address of the object. • **Network**: Enter an IPv4 address in CIDR notation, for example, 192.168.1.1/24. • **Netmask**: This field displays the subnet mask depends on the **Network** you entered. • **Cancel**: Click **Cancel** to close the window with changes unsaved. • **Save**: Click **Save** to save the entry. Add a new object or group when you select **Service** as the **Type**:  • **Name**: Enter the name of this object. It must begin with a letter and cannot exceed 30 characters. The valid characters are A-Z, a-z, 0-9, underscores (_), dashes (-), and dots (.). Spaces are not allowed. • **Description**: Enter a description for the object. • **IP Protocol**: Select the IP portal of the object from the drop-down list. **TCP and UDP**: If you select **TCP** or **UDP** as the **IP Protocol**, enter the **Starting Port** and **Ending Port** from 1 to 65535. **ICMP**: If you select **ICMP** or **ICMPv6** as the **IP Protocol**, select the **ICMP Type** from the drop-down list. **User Defined**: If you select **User Defined** as the **IP Protocol**, enter the **IP Protocol No.** from 1 to 255. • **Cancel**: Click **Cancel** to close the window with changes unsaved. • **Save**: Click **Save** to save the entry.
Remove	Select an entry and click this icon to delete it. 
Enable Walled Garden	Slide the switch to the right to enable walled garden of the policy**.** Enable this and define one or more web site addresses that all clients can access without logging in.

Table 145 Captive Portal > Authentication Policy > Policy > Add/Edit (continued)

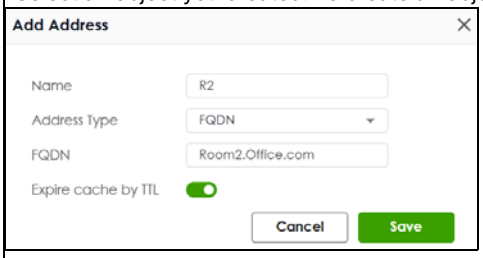
LABEL	DESCRIPTION
Trusted Identity Provider	If an OIDC server is used for user authentication, select the OIDC provider to enable the predefined walled garden list associated with that provider. See Section 17.3.3 on page 320 for details on keeping this allow list up to date. See Section 28.3.5 on page 487 for more information on OIDC.
Walled Garden List	Select the object you created. The selected objects will be applied to the policy. This list allows you to specify walled garden web site links, which use a FQDN (Fully Qualified Domain Name, consist of a host name and a domain name), domain name, and IPv4 address for web sites that clients are allowed to access without logging in.
Add	Click this to create a new entry.
Remove	Select an entry and click this to delete it.
Type	Select the type of traffic allowed in the walled garden: • **FQDN Object:** Allows traffic to the specified fully qualified domain name (for example, host.example.com) without logging in. • **Domain Name**: Allows traffic to any host within the specified domain (for example, 'example.com' or '*.example.com', which does not include 'example.com') without logging in. • **IPv4 Address**: Allows traffic to the specified IP address (for example, 192.168.1.10) without logging in.
Object	Select an object you created. To create an object, click **Add Object**.  • **Name**: Enter the name of this object. It must begin with a letter and cannot exceed 30 characters. The valid characters are A-Z, a-z, 0-9, underscores (_), dashes (-), and dots (.). Spaces are not allowed. • **Address Type**: Select the address type of the object you want to create from the drop-down list. • **FQDN**: Enter the FQDN of the of a web site. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain. Underscores are not allowed. Use "*" as a prefix in the FQDN for a wildcard domain name (for example, *.example.com). • **Expire cache by TTL**: Slide the switch to refresh the data in the cache when it expires based on the Time-to-Live (TTL). The cached data remains valid for the specified TTL duration before it is refreshed or discarded. • **Cancel**: Click **Cancel** to close the window with changes unsaved. • **Save**: Click **Save** to save the entry.
Remove	Select an entry and click this icon to delete it. 
Sign-in Method	Use this to configure how clients authenticate or acknowledge terms before accessing the network.
Click-to-continue	Select this to block network access until clients agree to the user agreement policy.

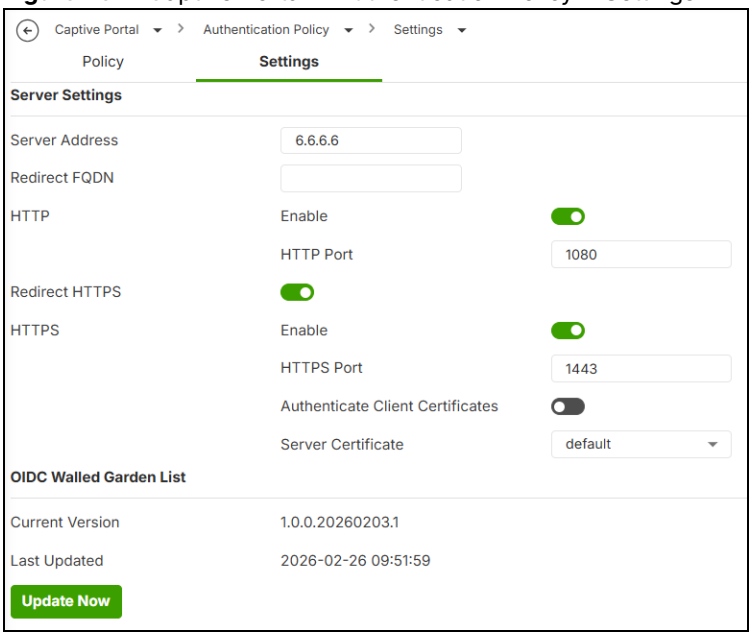
Table 145 Captive Portal > Authentication Policy > Policy > Add/Edit (continued)

LABEL	DESCRIPTION
Sign-on With	Select this and choose an authentication policy you configured in **User & Authentication > User Authentication > AAA Server** to block network access until a client authenticates. • **local:** Use the default authentication policy on the Zyxel Device. • **Nebula cloud authentication**: Use the NCAS (Nebula Cloud Authentication Server). Refer to Section 28.1.2 on page 461 for details. • **Nebula identity federation service**: Use the NID FS (Nebula Identity Federation Service) you configured in Nebula. Refer to Section 28.1.3 on page 462 for details. • AD / LDAP / RADIUS / OIDC server. Note: If you use an OIDC server for authentication, enable the **Walled Garden** and add the corresponding OIDC provider to the **Trusted Identity Provider** field to allow client access to the login portal. Note: If there is no response from an external authentication server for over 15 seconds, then the connection to the authentication server is considered disconnected. If disconnected, there is only limited access for captive portal users. Limited means that only already authorized captive portal users can continue to access the network, but new authentication requests cannot be granted until the connection to the authentication server is restored.
Portal Type	Use this to configure a portal that clients are directed to for network access.
Internal	Select this to use the **Default** web page on the Zyxel Device or a custom web page you configured on Nebula. • **Default**: Use the default web page on the Zyxel Device, or the default Nebula web page if the Zyxel Device is managed through Nebula. • (Custom Theme Name): Use the custom web page configured on Nebula if the Zyxel Device is managed through Nebula. Note: The portal will display the default web page if the selected custom theme is unavailable.
External	Select this and enter the URL of an external portal. The format must be "http(s)://domain", with a maximum of 255 characters. These are the allowed characters: [a-zA-Z0-9.-/?@=.&_-]. You can configure the look and feel of the web portal page. Specify the login page's URL, for example, http://IIS server IP Address/login.asp. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Advanced Settings	
After the Captive Portal Page Where the User Should Go?	• Select **Stay on Captive Portal Authenticated Successfully Page** to keep users on the success page after a successful login. • Select **Stay on Login Session Page** to keep users on the login page after a successful login. • Select **To promotion URL** and specify an URL to redirect users to after a successful login.
Redirect TCP Port 443 Traffic to Login Page	Slide the switch to the right to require that users use HTTPS for access to the captive portal. Users may see a certificate warning when they log into the captive portal. Refer to Redirect TCP Port 443 Traffic to Login Page for example scenarios.
Idle Timeout	Slide the switch to the right and enter the number of minutes a user can remain logged in but without activity before being automatically logged out.
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.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

17.3.3 The Settings Screen

You can use another server for clients to access the captive portal. Click **Captive Portal** > **Authentication Policy** > **Settings** to display the **Settings** screen.

Figure 204 Captive Portal > Authentication Policy > Settings



The following table describes the labels in this screen.

Table 146 Captive Portal > Authentication Policy > Settings

LABEL	DESCRIPTION
Server Settings	
Server Address	Enter the IP address of the service address.
Redirect FQDN	Enter the FQDN for the server containing the captive portal.
HTTP	Configure the HTTP connection of the captive portal.
Enable	Slide the switch to the right to allow clients access to the captive portal web page using HTTP.
HTTP Port	Enter the HTTPS port. This HTTPS server listens on port 1080 by default. If you choose a port already in use, you will see a port conflict message telling you to choose another port.
Redirect HTTPS	Slide the switch to the right to allow only secure access by redirecting all HTTP connection requests to the HTTPS server.
HTTPS	Configure the HTTPS connection of the captive portal.
Enable	Slide the switch to the right to require clients access to the captive portal web page using secure HTTPS connections.
HTTPS Port	Enter the HTTPS port. This HTTPS server listens on port 1443 by default. If you choose a port already in use, you will see a port conflict message telling you to choose another port.
Authenticate Client Certificates	Slide the switch to the right to require the captive portal client to authenticate to the HTTPS server by sending a certificate. To do that the captive portal client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the Zyxel Device. Note: Make sure the common name of certificate matches the **Redirect FQDN** setting.

Table 146 Captive Portal > Authentication Policy > Settings (continued)

LABEL	DESCRIPTION
Server Certificate	Select a certificate the Zyxel Device will use to authenticate HTTPs connections or actual certificates that users will use to log into the Captive portal. Use a certificate you created or imported in **System > Certificates > My Certificates** or a trusted certificate from **System > Certificates > Trusted Certificates**. You can use a private certificate or a public certificate from either screen. A private certificate is free but it requires certificate installation on clients or users will get browser warnings if the certificate not trusted. You may use a private certificate for a Captive portal that has users with devices where trusted certificates can be installed on them or they can trust the Zyxel Device's private certificate. Users should authenticate to the Zyxel Device from a Wired LAN, corporate WiFi, or an established VPN tunnel to the Zyxel Device. A public certificate is issued by a public Certificate Authority, such as DigiCert, Sectigo, Let's Encrypt, and so on. It is automatically trusted by browsers, operating systems, mobile devices, so there's no client configuration, nor browser warnings. However, it's not free, requires a public DNS name and needs Internet access. It's recommended for Captive portals for guests, external HTTPS proxy authentication from the Internet, and authentication using OIDC (some IdPs reject private/self-signed certificates). • Use a public certificate if you want to use proxy server authentication with OIDC or with Captive portal for guests. • Use a private certificate for Captive portal with users behind the Zyxel Device. Select **Auto** to use the default certificate for the Zyxel Device provided by Nebula. The server address and redirect FQDN used for captive portal authentication are automatically displayed.
OIDC Walled Garden List	The fields below show the predefined walled garden list currently used by the Zyxel Device for the corresponding OIDC provider. It includes the domains associated with the OIDC providers. When an OIDC provider is selected in the **Trusted Identity Provider** field under **Captive Portal > Authentication Policy > Add/Edit.** The Zyxel Device allows clients to access these listed domains to reach the OIDC server for authentication.
Current Version	This field displays the version number of the list.
Last Updated	This field displays the date and time the list was updated.
Update Now	The list is automatically updated periodically and after the Zyxel Device reboots. To update immediately, click this to update the list. Check the displayed message for the update result.

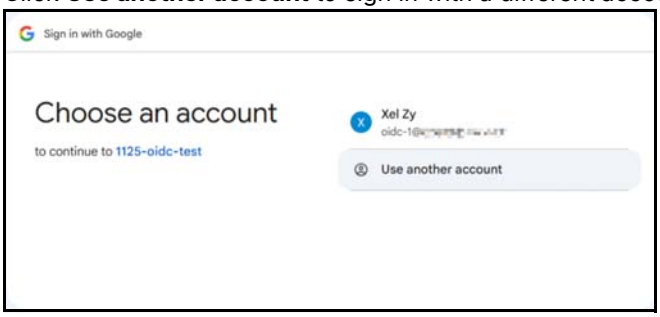
17.4 Captive Portal Client Sign-In Steps

This section describes the client sign-in steps for the captive portal when using an OIDC server for authentication.

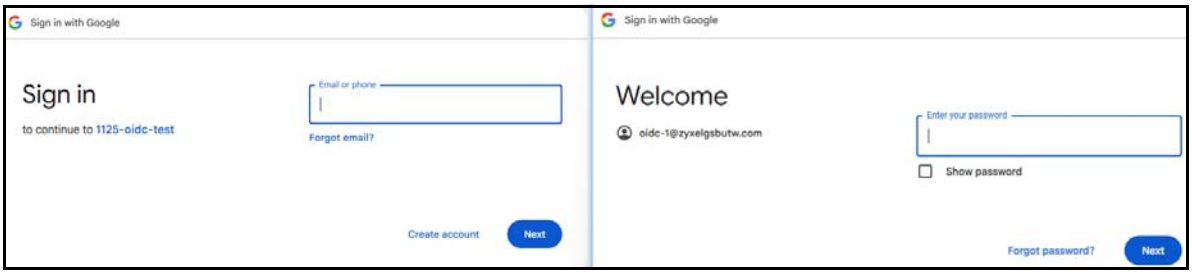
1 After connecting to the WiFi network (SSID) of an manged AP, the captive portal welcome page displays. If you have signed in before and want to sign in with another account, select the **Sign in as a different user** checkbox. Click **Sign in**.



Click **Use another account** to sign in with a different account.

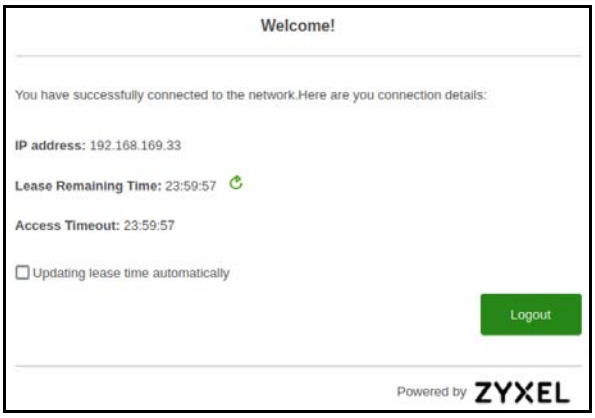


2 Enter your email or phone number and the corresponding password.



3 The success page displays. You will be logged out when the **Lease Remaining Time** expires. Select **Update lease time automatically** to prevent session timeout before the **Access Timeout**.

Note: Regardless of whether the **Update lease time automatically** checkbox is selected, you will be logged out after the **Access Timeout**.


Welcome!
You have successfully connected to the network.Here are you connection details:
IP address: 192.168.169.33
Lease Remaining Time: 23:59:57
Access Timeout: 23:59:57
Updating lease time automatically
Logout
Powered by ZYXEL

CHAPTER 18
Object

18.1 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 18.1.2 on page 324) 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 18.1.3 on page 327) and the **Address Group Add/Edit** screen, to maintain address groups in the Zyxel Device.
- Use the **Geo IP** screen (Section 18.1.4 on page 330) to update the database of country-to-IP address mappings and to manually configure country-to-IP address mappings.

Note: Renaming objects may take a long time, it is recommended to use the Command Line Interface (CLI) for renaming. See the CLI Reference Guide for details.

18.1.1 What You Need To Know

Address objects and address groups are used in policy routes, security policies, application patrol, 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.

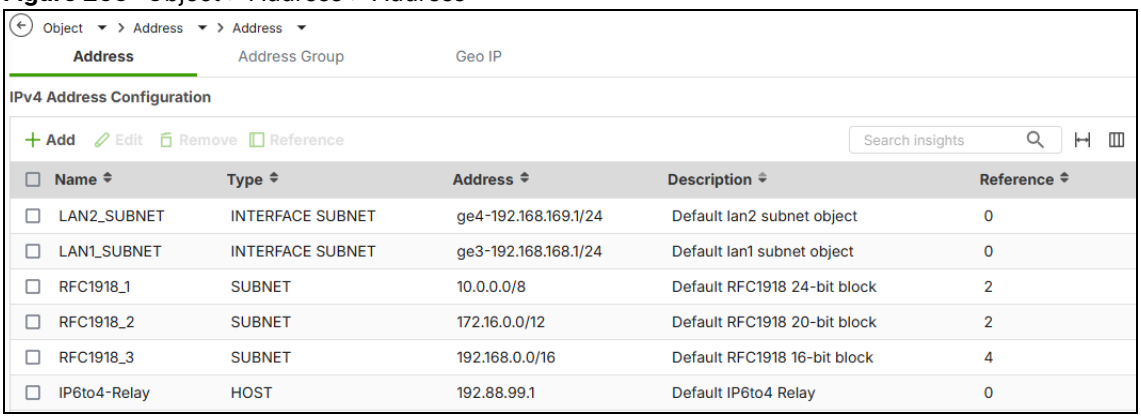
Address groups are composed of address objects and address groups. The sequence of members in the address group is not important.

18.1.2 Address Summary Screen

The address screens are used to create, maintain, and remove addresses.

The **Address** screen provides a summary of all addresses in the Zyxel Device. To access this screen, click **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 205 Object > Address > Address



The following table describes the labels in this screen. See Section 18.1.2.1 on page 325 for more information as well.

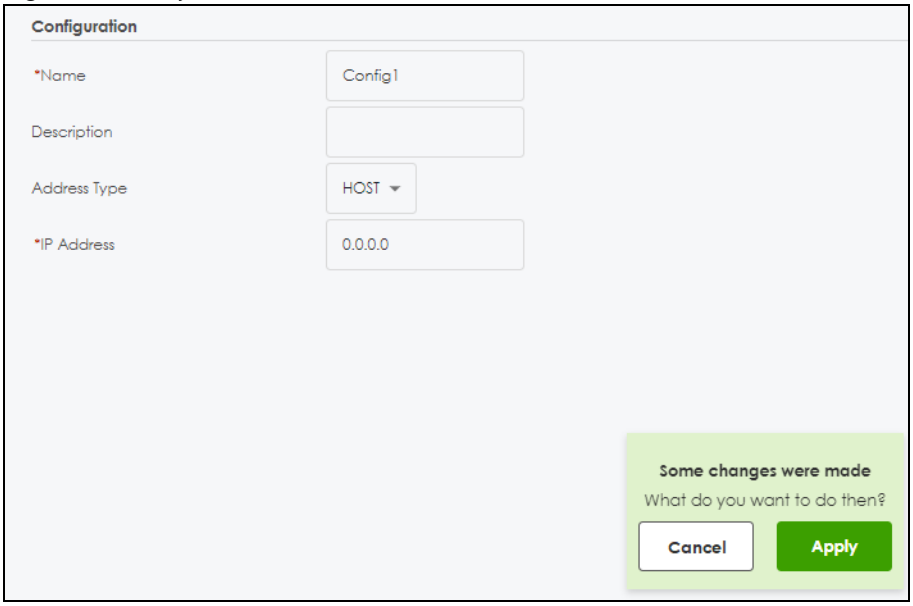
Table 147 Object > Address > Address

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.
Reference	Select an entry and click **Reference** to check which settings use the entry.
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.
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.
Reference	This displays the number of times an object reference is used in a profile.

18.1.2.1 IPv4 Address Add/Edit Screen

The **Object > Address > Address > Add/Edit** screen allows you to create a new address or edit an existing one. To access this screen, go to the **Address** screen (see Section 18.1.2 on page 324), and click either the **Add** icon or an **Edit** icon in the **IPv4 Address Configuration** section.

Figure 206 Object > Address > Address > Add/Edit



The following table describes the labels in this screen.

Table 148 Object > Address > Address > Add/Edit

LABEL	DESCRIPTION
Name	Type the name used to refer to the address. You may use 2-30 single-byte characters, including [0-9] [a-z] [A-Z], underscores[_], or dashes [-], but the first character cannot be a number. This value is case-sensitive.
Description	Enter the description associated with the zone, if any. You can use 1 to 30 single-byte characters, including [0-9] [a-z] [A-Z]. Special characters are not allowed
Address Type	Select the type of address you want to create. • **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 the Fully Qualified Domain Name (FQDN) to represent a website. 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. 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 148 Object > Address > Address > Add/Edit

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. Scroll through the drop-down list or type a letter or part of the name to search for a country or continent. A **GEOGRAPHY** object uses the data from the country-to-IP/continent-to-IP address database. Go to the **Object** > **Address** > **Geo IP** screen to configure the custom country-to-IP/continent-to-IP address mappings for a **GEOGRAPHY** object.
FQDN	This field is only available if the **Address Type** is **FQDN**, in which case this field cannot be blank. Enter the FQDN of the website that this address object represents. You can enter a wildcard in the first position. For example, '*.zyxel.com'. Click **Test** to check if the FQDN you entered is valid and to view the result of the DNS query. The **Test** button is disabled if you enter a FQDN with a wildcard.
Expire cache by TTL	Enable this to automatically clear the cache when the duration for storing a DNS record in the DNS cache has expired. Disable this if you want to keep the DNS record in the DNS cache after it has expired.
IPv4 Cache List You must first configure IPv4 FQDN objects in this screen.	
IP Address	This field displays the mapping of the FQDN to an IP address. This is the IP address of a host.
TTL	Time to Live (TTL) shows the number of seconds remaining before the DNS record expires. If the **Expire cache by TTL** option is disabled, the DNS record will not be cleared from the **IPv4 Cache List** when the TTL expires. The **IPv4 Cache List** will be updated if the following conditions are met. • The FQDN does not include a wildcard, and • Two minutes after all the TTL (Time To Live)values have expired.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

18.1.3 Address Group Summary Screen

The **Address Group** screen provides a summary of all address groups. To access this screen, click **Object** > **Address > Address Group**. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 207 Object > Address > Address Group



The following table describes the labels in this screen. See Section 18.1.3.1 on page 328 for more information as well.

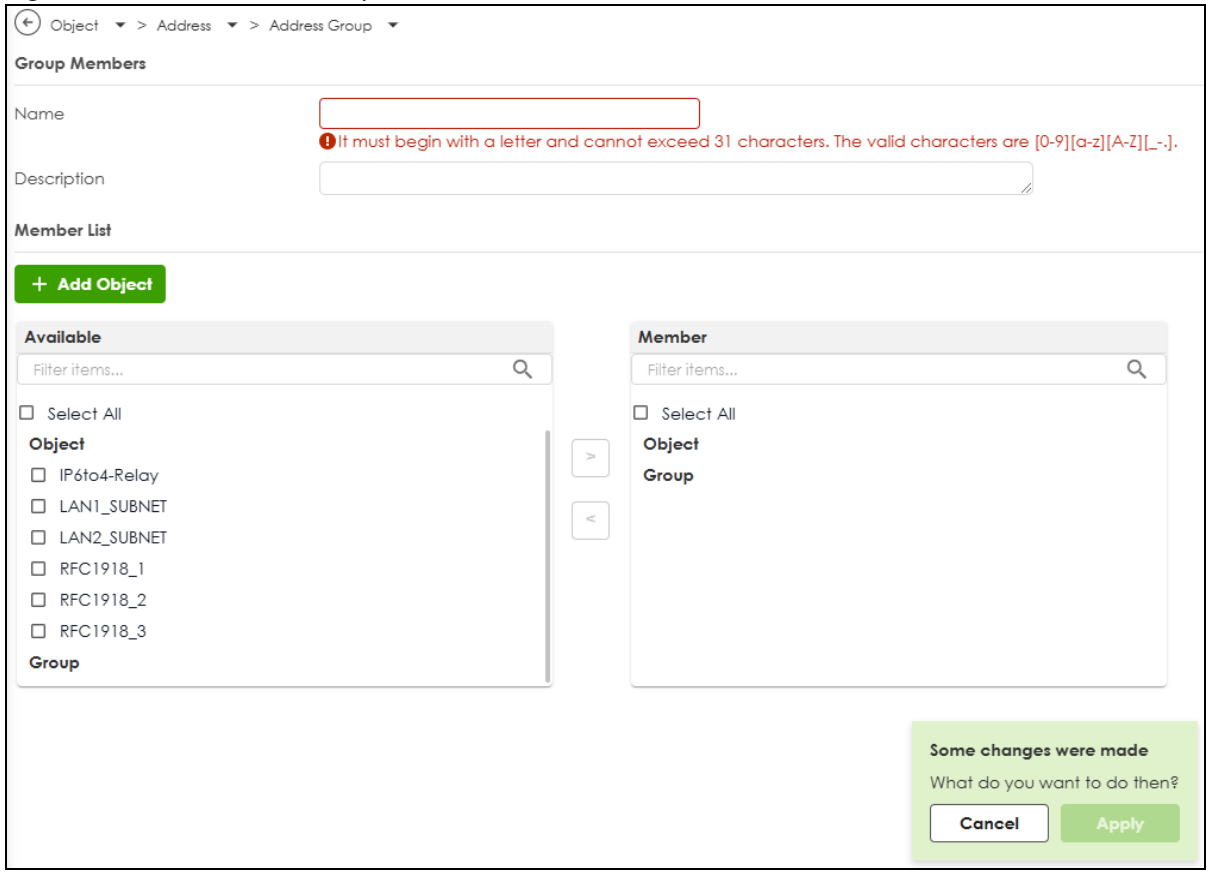
Table 149 Object > Address > Address Group

LABEL	DESCRIPTION
IPv4 Address Group Configuration	
Add	Click this to create a new entry.
Edit	Select an entry 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.
Reference	Select an entry and click it to check which settings use the entry.
Name	This field displays the name of each address group.
Description	This field displays the description of each address group, if any.
Reference	This field displays the number of times an object reference is used in a profile.
Member Count	This field displays the number of member in the group.
Reference	This displays the number of times an object reference is used in a profile.

18.1.3.1 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 18.1.3 on page 327), and click either the **Add** icon or an **Edit** icon in the **IPv4 Address Group Configuration** section.

Figure 208 IPv4 Address Group > Add



The following table describes the labels in this screen.

Table 150 IPv4 Address Group > Add

LABEL	DESCRIPTION
Name	Enter a name for the address group. You may use 2-30 single-byte characters, including 0-9a-zA-Z, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	You can use 1 to 30 single-byte characters, including 0-9a-zA-Z!"#$%'()*+,-/:;=?@_ &.<>[\]{|}^`are not allowed.
Add Object	Click this button to create an address object. See Section 18.1.2.1 on page 325 for more information on configuring an address object.
Search	Type an item in the search box, then click this to display all address objects in the table below according to the item you typed.
Select All	Select this to select all address objects and address groups in the table.
Member List	The list on the left 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 fro this list that you want to be members and move them to the list on the right. Move any members you do not want included to the list on the left. Note: Only objects of the same address type can be added to a address group.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

18.1.4 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 209 Object > Address > Geo IP

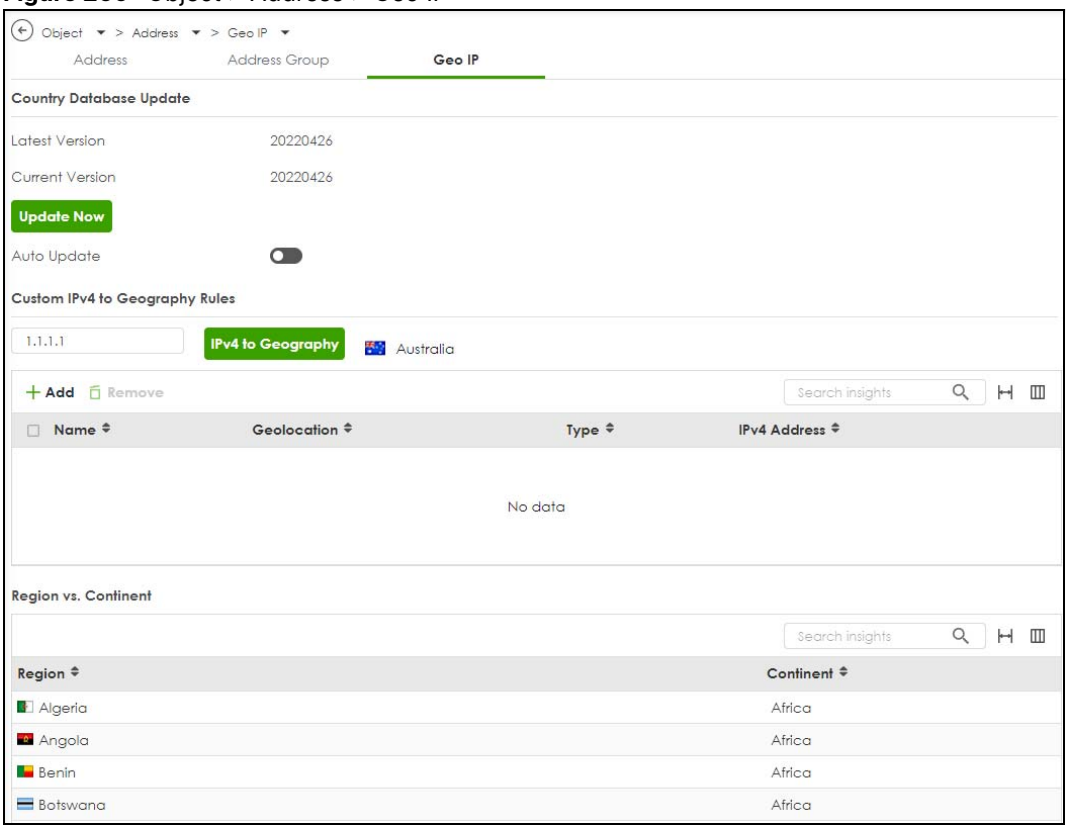


Figure 210 Object > Address > Geo IP > Region vs. Continent



Region vs. Continent

Region	Continent
Afghanistan	Asia
Aland Islands	Europe
Albania	Europe
Algeria	Africa
American Samoa	Oceania
Andorra	Europe
Angola	Africa
Anguilla	North America
Antarctica	Antarctica
Antigua and Barbuda	North America
Argentina	South America
Armenia	Asia
Aruba	North America
Australia	Oceania
Austria	Europe
Azerbaijan	Asia
Bahamas	North America
Bahrain	Asia
Bangladesh	Asia
Barbados	North America
Belarus	Europe
Belgium	Europe
Belize	North America
Benin	Africa
Bermuda	North America
Bhutan	Asia
Bolivia	South America
Bonaire, Sint Eustatius, and Saba	North America
Bosnia and Herzegovina	Europe
Botswana	Africa
Bouvet Island	Antarctica
Brazil	South America
British Indian Ocean Territory	Asia
Brunei	Asia
Bulgaria	Europe
Burkina Faso	Africa
Burundi	Africa
Cambodia	Asia
Cameroon	Africa
Canada	North America
Cabo Verde	Africa
Cayman Islands	North America
Central African Republic	Africa
Chad	Africa
Chile	South America
China	Asia
Christmas Island	Asia
Cocos (Keeling) Islands	Asia
Colombia	South America

The following table describes the labels in this screen.

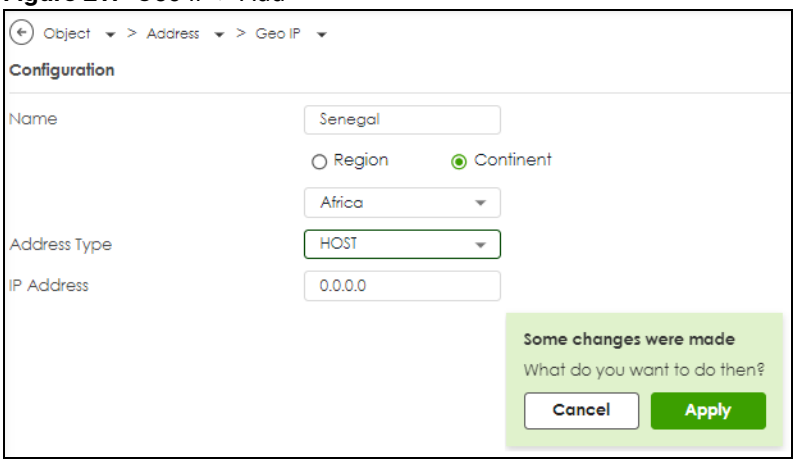
Table 151 Object > Address/Geo IP > Geo IP

LABEL	DESCRIPTION
Country Database Update	
Latest Version	This is the latest country-to-IP address database version.
Current Version	This is the country-to-IP address database version currently on the Zyxel Device.
Update Now	Click this to check for the latest country-to-IP address database version. 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, select the checkbox, choose a day and time each week and then click **Apply**.
Custom IPv4 to Geography Rules	Enter an IP address, then click the **IPv4 to Geography** button to query which country this IP address belongs to.
Add	Click this to create a new entry.
Edit	Select an entry 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.
Name	This filed displays the name of the 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 Address	This field displays the IPv4/IPv6 addresses represented by the type of address object.
Region vs. Continent	
Region vs. Continent	Enter a country or continent name in the **Search** field to query which continent this country belongs to or which countries belong to the continent.

18.1.4.1 Add Custom IPv4 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 18.1.4 on page 330), and click the **Add** icon in the **Custom IPv4 to Geography Rules** section.

Figure 211 Geo IP > Add



The following table describes the labels in this screen.

Table 152 Geo IP > Add

LABEL	DESCRIPTION
Name	Enter a name for the address group. You may use 2-30 single-byte characters, including 0-9 a-z A-Z, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
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**, **CIDR**.
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.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

18.2 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 18.2.2 on page 335) to view and configure the Zyxel Device's list of services and their definitions.
- Use the **Service Group** screens (Section 18.2.2 on page 335) to view and configure the Zyxel Device's list of service groups.

18.2.1 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.

Reference

Use **Reference** in a screen to view which configuration settings reference to the object.

For example, go to **Object** > **Service**. select an entry, then click **Reference** to open the **References** screen. The **References** screen displays which settings are using the selected entry.

Figure 212 Reference



This table describes the fields in this screen.

Table 153 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.

Table 153 References

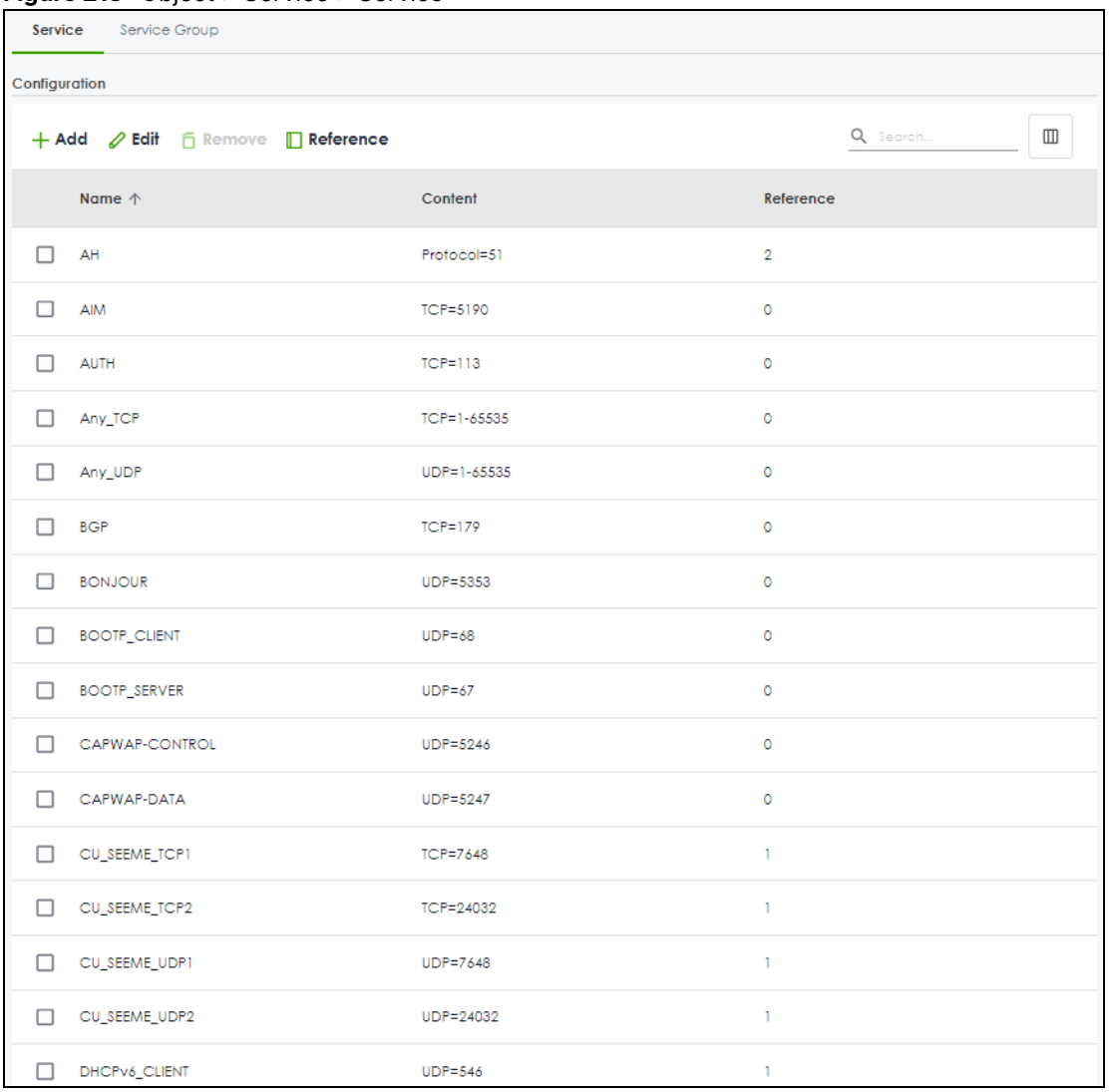
LABEL	DESCRIPTION
Service	This is the type of setting that references the selected object. Click a service's name to display the service's configuration screen in the main window.
Priority	If it is applicable, this field displays the referencing configuration item's position in its list; otherwise - displays.
Name	This field identifies the configuration item that references the object.
Description	If the referencing configuration has a description configured, it displays here.
Refresh	Click this to update the information in this screen.
Cancel	Click this to close the screen.

18.2.2 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 **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 213 Object > Service > Service



The following table describes the labels in this screen.

Table 154 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.
Reference	Select an entry and click **Reference** to check which settings use the entry.
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.

18.2.2.1 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 18.2.2 on page 335), and click either the **Add** icon or an **Edit** icon.

Figure 214 Object > Service > Service > Add/Edit



The following table describes the labels in this screen.

Table 155 Object > Service > Service > Add/Edit

LABEL	DESCRIPTION
Name	Type the name used to refer to the service. You may use 1-30 single-byte characters, including [0-9] [a-z] [A-Z] [!"#$%'()*+,-/:;=?@_], but the first character cannot be a number. [&.<>[\]{|}^'] are not allowed. This value is case-sensitive.
Description	Type the description used to refer to the service. You may use 1-30 single-byte characters, including [0-9] [a-z] [A-Z] [!"#$%'()*+,-/:;=?@_], but the first character cannot be a number. [&.<>[\]{|}^'] are not allowed.
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.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

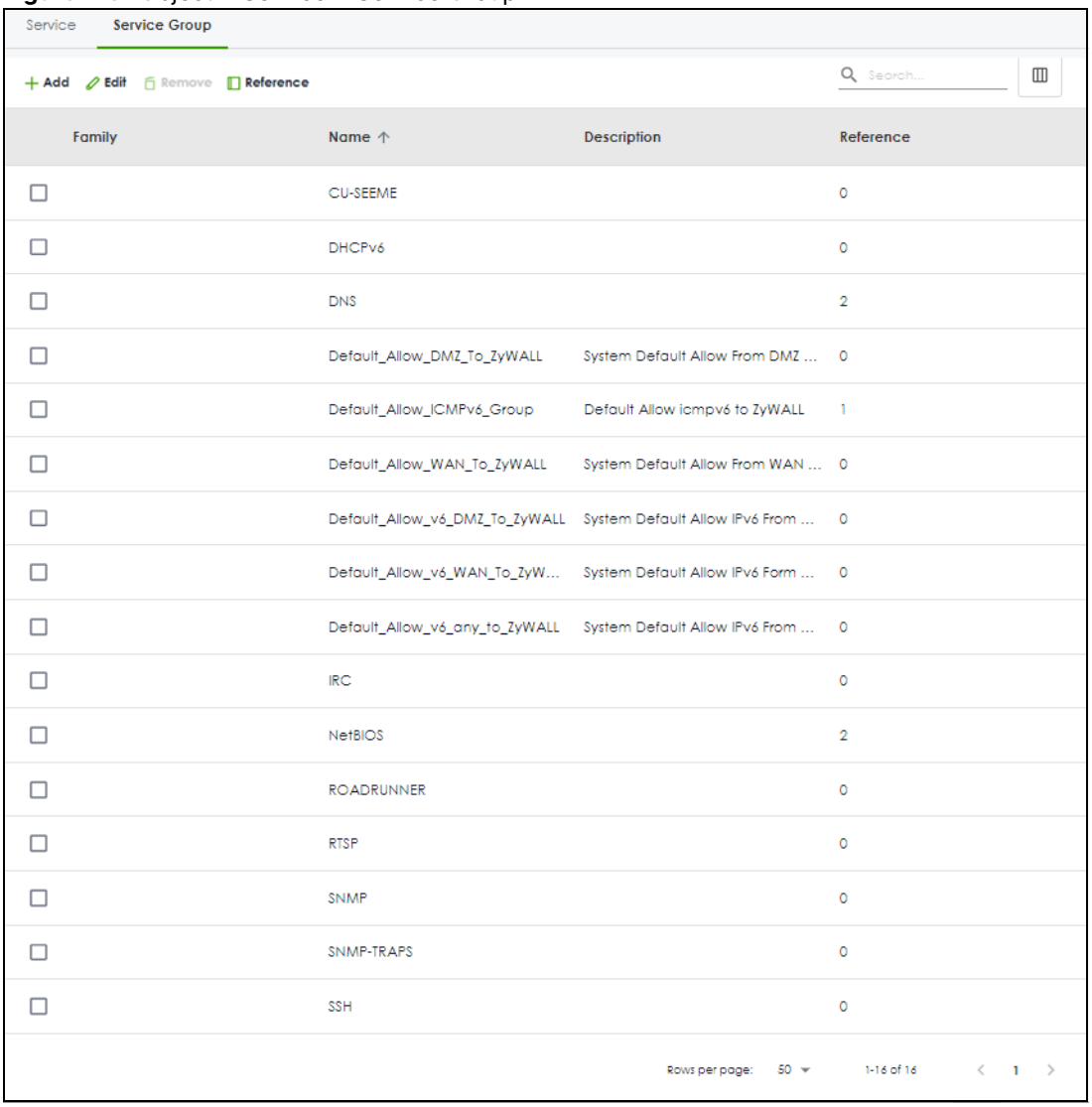
18.2.3 The Service Group Summary Screen

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,** and/or **SSH**, 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, click **Object** > **Service** > **Service Group**.

Figure 215 Object > Service > Service Group



The following table describes the labels in this screen. See Section 18.2.3.1 on page 339 for more information as well.

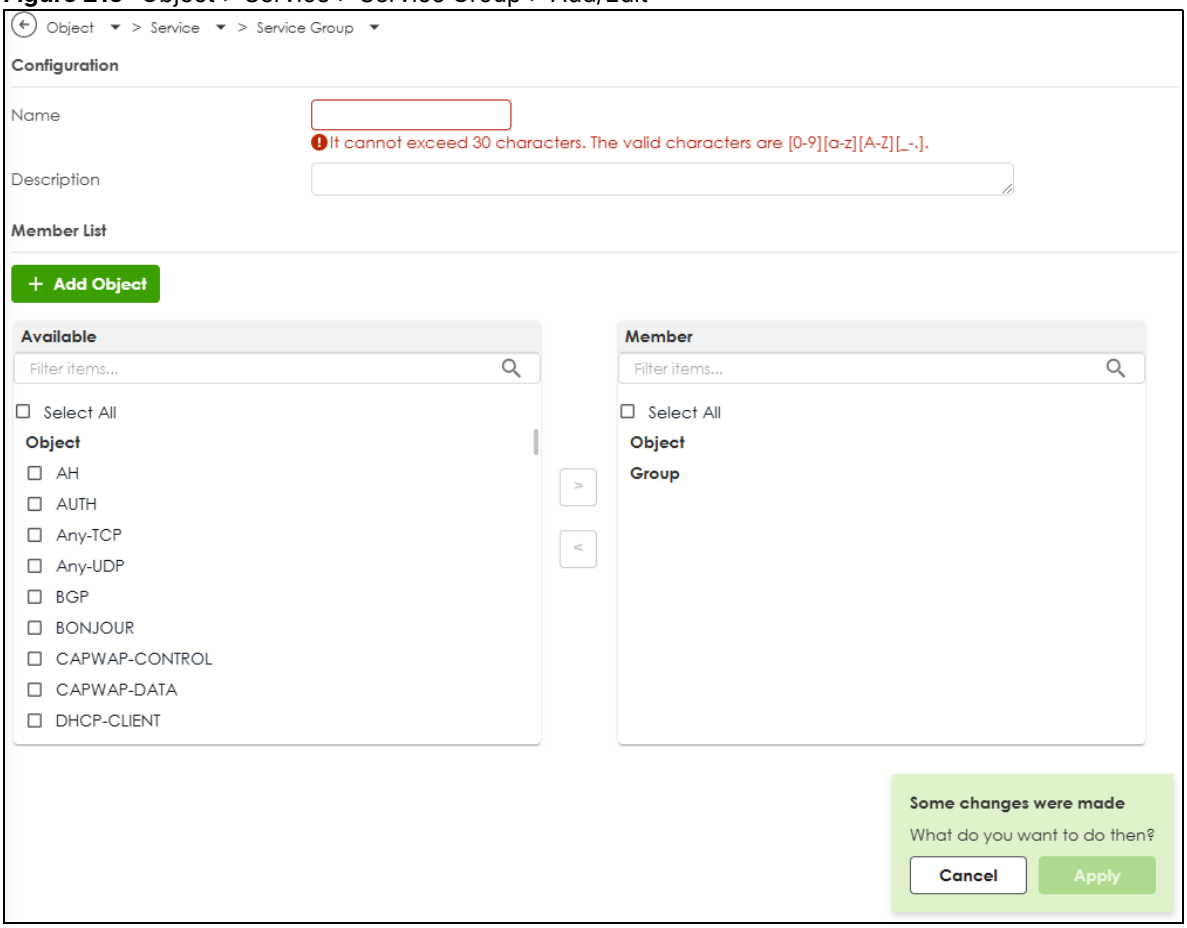
Table 156 Object > Service > Service Group

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.
Reference	Select an entry and click **Reference** to check which settings use the entry.
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.

18.2.3.1 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 18.2.3 on page 338), and click either the **Add** icon or an **Edit** icon.

Figure 216 Object > Service > Service Group > Add/Edit



The following table describes the labels in this screen.

Table 157 Object > Service > Service Group > Edit

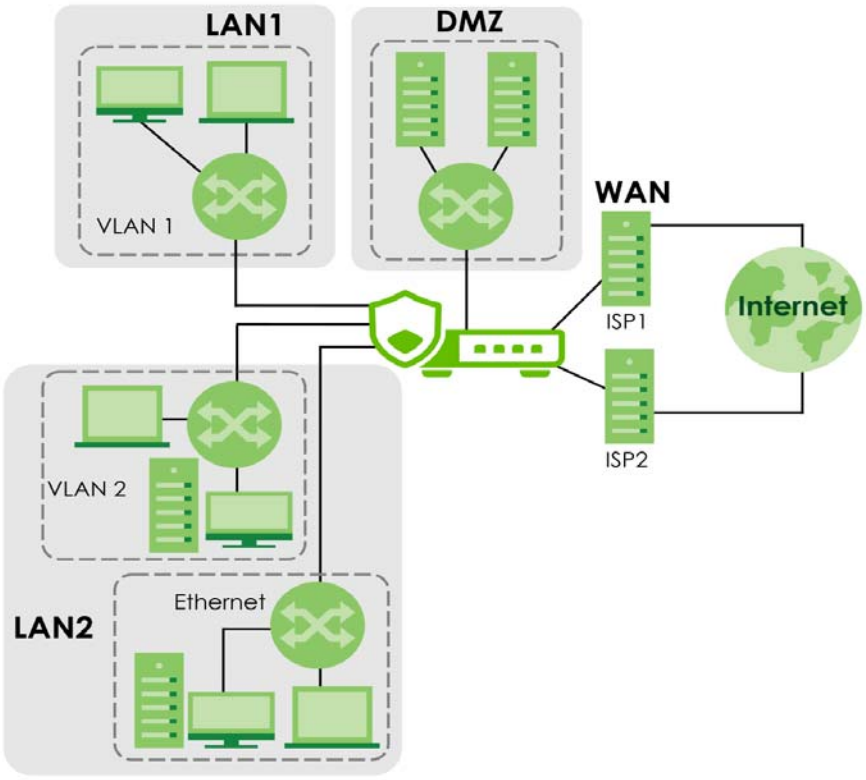
LABEL	DESCRIPTION
Name	Type the name used to refer to the service group. You may use 1-30 single-byte characters, including [0-9] [a-z] [A-Z] [!"#$%'()*+,-/:;=?@_], but the first character cannot be a number. [&.<>[\]{|}^`] are not allowed. This value is case-sensitive.
Description	Type the description used to refer to the service group. You may use 1-30 single-byte characters, including [0-9] [a-z] [A-Z] [!"#$%'()*+,-/:;=?@_], but the first character cannot be a number. [&.<>[\]{|}^`] are not allowed.
Add Object	Click this button to create an address object. See Section 18.1.2.1 on page 325 for more information on configuring an address object.
Search	Type an item in the search box, then click this to display all address objects in the table below according to the item you typed.
Select All	Select this to select all address objects and address groups in the table.
Member List	This 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 list on the left that you want to be members and move them to the list on the right. Move any members you do not want included to the list on the left.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

18.3 Zone 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 Security Policy 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 217 Example: Zones



Use the **Zone** screens (see Section 18.4.2 on page 344) to manage the Zyxel Device's zones.

18.3.1 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 217 on page 341, 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 217 on page 341, traffic between VLAN 1 and the Internet is inter-zone traffic. This is the normal case when zone-based security and policy settings apply.

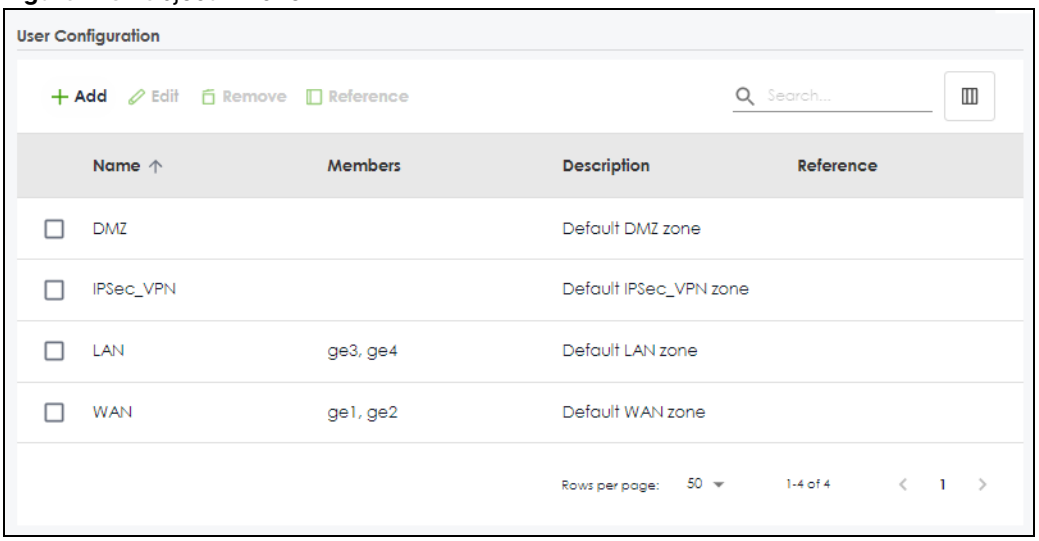
Extra-zone Traffic

- Extra-zone traffic is traffic to or from any interface or VPN tunnel that is not assigned to a zone. For example, in Figure 217 on page 341, 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.

18.3.2 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 **Object > Zone**.

Figure 218 Object > Zone



The following table describes the labels in this screen.

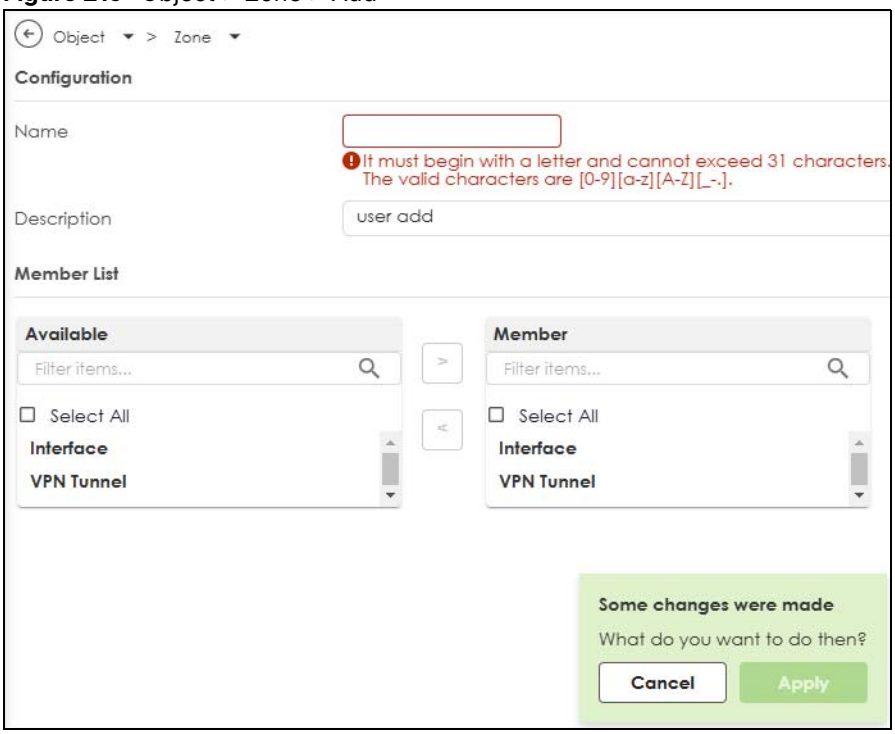
Table 158 Object > Zone

LABEL	DESCRIPTION
User Configuration	The Zyxel Device comes with pre-configured system default zones that you cannot delete. You can create your own zones by clicking **Add**.
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.
Reference	Select an entry and click **Reference** to check which settings use the entry.
Name	This field displays the name of the zone.
Members	This field displays the names of the interfaces that belong to each zone.
Description	This field displays the description of the zone.
Reference	This field displays the number of times an Object Reference is used in a policy.

18.3.2.1 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 18.4.2 on page 344), and click the **Add** icon or an **Edit** icon.

Figure 219 Object > Zone > Add



The following table describes the labels in this screen.

Table 159 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 2-30 single-byte characters, including [0-9] [a-z] [A-Z] [_.-], but the first character cannot be a number. This value is case-sensitive.
Description	Enter the description associated with the zone, if any. You can use 1 to 30 single-byte characters, including [0-9] [a-z] [A-Z] [!'#$%'()*+,-/:;=?@_&.<>[\]{|}^'] are not allowed.
Search	Type an item in the search box, then click this to display all address objects in the table below according to the item you typed.
Select All	Select this to select all address objects and address groups in the table.
Member List	The list on the left displays 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. The list on the right displays 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.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

18.4 Schedule Overview

Use schedules to set up one-time and recurring schedules for policy routes, security policies, application patrol, 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 18.4.2 on page 344) to see a list of all schedules in the Zyxel Device.
- Use the **One-Time Schedule Add/Edit** screen (Section 18.4.2.1 on page 345) to create or edit a one-time schedule.
- Use the **Recurring Schedule Add/Edit** screen (Section 18.4.2.2 on page 347) to create or edit a recurring schedule.
- Use the **Schedule Group** screen (Section 18.4.3 on page 348) to merge individual schedule objects as one object.

18.4.1 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.

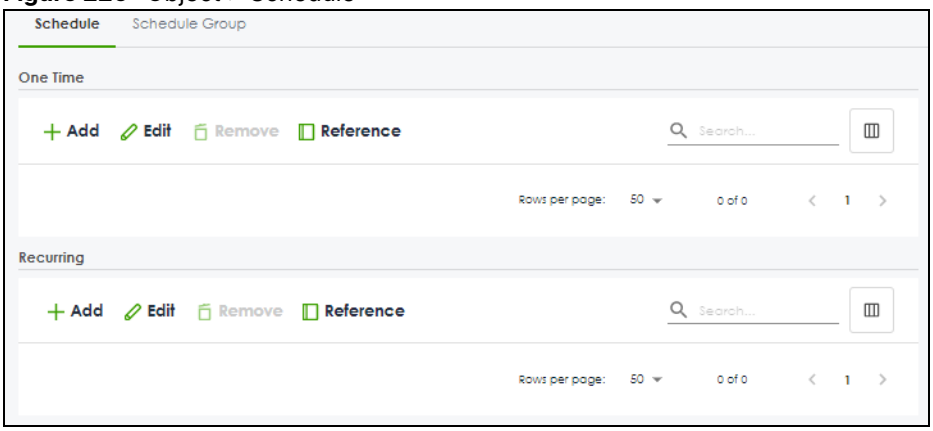
Recurring Schedules

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.

18.4.2 The Schedule Screen

The **Schedule** screen provides a summary of all schedules in the Zyxel Device. To access this screen, click **Object** > **Schedule**.

Figure 220 Object > Schedule



The following table describes the labels in this screen. See Section 18.4.2.1 on page 345 and Section 18.4.2.2 on page 347 for more information as well.

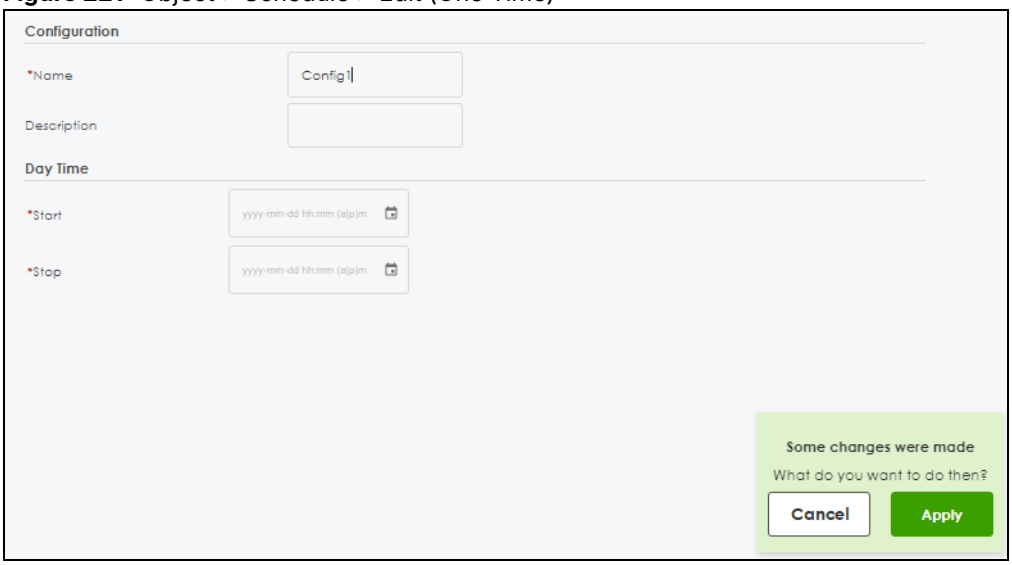
Table 160 Object > Schedule

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.
Reference	Select an entry and click **Reference** to check which settings use the entry.
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.
Reference	Select an entry and click **Reference** to check which settings use the entry.
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.

18.4.2.1 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 18.4.2 on page 344), and click either the **Add** icon or an **Edit** icon in the **One Time** section.

Figure 221 Object > Schedule > Edit (One Time)



The following table describes the labels in this screen.

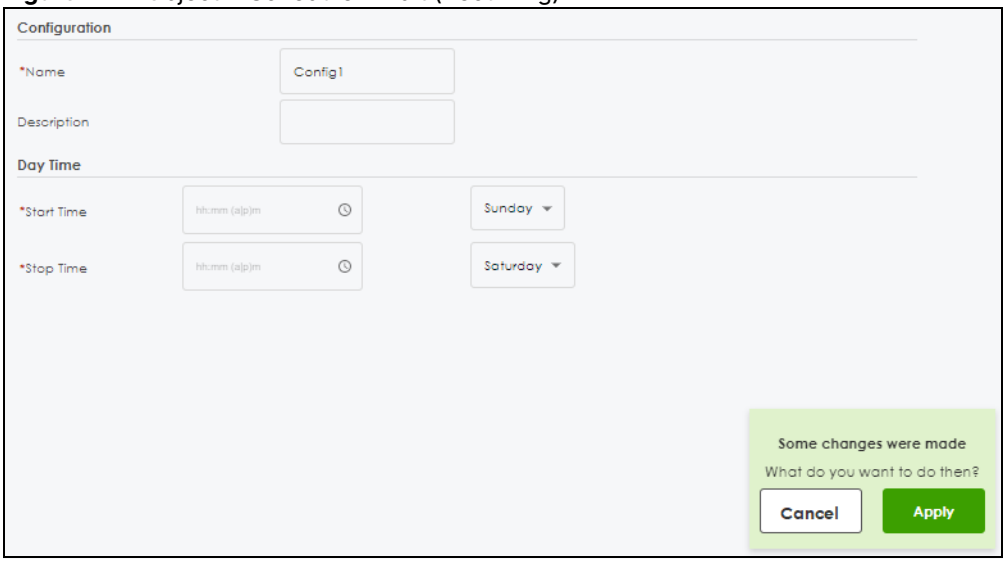
Table 161 Object > Schedule > Edit (One Time)

LABEL	DESCRIPTION
Configuration	
Name	Type the name used to refer to the one-time schedule. You may use 2-30 single-byte characters, including [0-9] [a-z] [A-Z], underscores [_], or dashes [-], but the first character cannot be a number. This value is case-sensitive.
Description	Type a description used to identify the one-time schedule. You may use 1-30 single-byte characters, including [0-9] [a-z] [A-Z] [’()+,/:=?;!*#@$_%-”]
Day Time	
Start	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.) Specify the hour and minute when the schedule begins. • **Hour** - 1-12 AM/PM • **Minute** - 0 - 59
Stop	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.) Specify the hour and minute when the schedule ends. • **Hour** - 1-12 AM/PM • **Minute** - 0 - 59
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

18.4.2.2 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 18.4.2 on page 344), and click either the **Add** icon or an **Edit** icon in the **Recurring** section.

Figure 222 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.

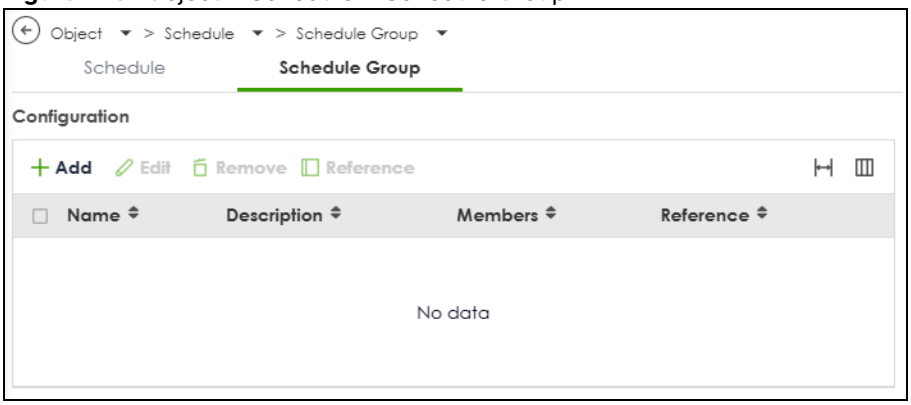
Table 162 Object > Schedule > Edit (Recurring)

LABEL	DESCRIPTION
Configuration	
Name	Type the name used to refer to the recurring schedule. You may use 2-30 single-byte characters, including 0-9a-zA-Z, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Type a description used to identify the one-time schedule. You may use 1-30 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-"
Date Time	
StartTime	Specify the hour and minute when the schedule begins each day. Then, select each day of the week the recurring schedule is effective. • **Hour** - 1-12 AM/PM • **Minute** - 0 - 59
StopTime	Specify the hour and minute when the schedule ends each day. Then, select each day of the week the recurring schedule is effective. • **Hour** - 1-12 AM/PM • **Minute** - 0 - 59
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

18.4.3 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 **Object** > **Schedule > Schedule Group**.

Figure 223 Object > Schedule > Schedule Group



The following table describes the fields in the above screen.

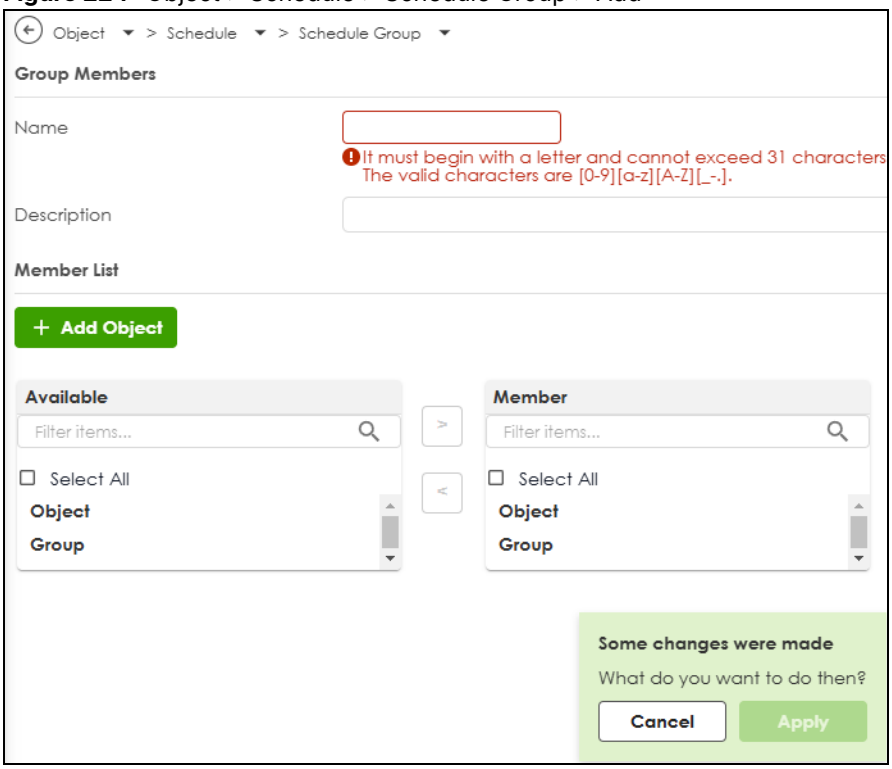
Table 163 Object > Schedule > Schedule Group

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.
Reference	Select an entry and click **Reference** to check which settings use the entry.
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.

18.4.3.1 The Schedule Group Add/Edit Screen

The **Schedule Group Add/Edit** screen allows you to define a schedule group or edit an existing one. To access this screen, go to the **Schedule** screen (see), and click either the **Add** icon or an **Edit** icon in the **Schedule Group** section.

Figure 224 Object > Schedule > Schedule Group > Add



The following table describes the fields in the above screen.

Table 164 Object > Schedule > Schedule Group > Add

LABEL	DESCRIPTION
Group Members	
Name	Type the name used to refer to the recurring schedule. You may use 2-30 single-byte characters, including [0-9] [a-z] [A-Z], 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 30 single-byte characters, special characters and spaces are allowed.
Member List	
Add Object	Click this button to create an address object. See Section 18.1.2.1 on page 325 for more information on configuring an address object.
Search	Type an item in the search box, then click this to display all address objects in the table below according to the item you typed.
Select All	Select this to select all address objects and address groups in the table.
Member List	This 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 list on the left that you want to be members and move them to the list on the right. Move any members you do not want included to the list on the left.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

CHAPTER 19
Application Patrol

19.1 Overview

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

If a license has expired, you will see a reminder in this screen. You need to renew the license in order to keep using the feature. Click **Buy Now** to go to Marketplace to purchase a new license. Click **See Details** to go to the Zyxel web page to find more information on licenses for your Zyxel Device.



19.1.1 What You Can Do in this Chapter

- Use the **App Patrol** summary screen (see Section 19.2 on page 351) to manage the application patrol profiles. You can also view license registration and signature information.
- Use the **App Patrol Add/Edit** screens (see Section 19.2.1 on page 353) to set actions for application categories and for specific applications within the category.

19.1.2 What You Need to Know

If you want to use a service, make sure both the Security Policy and application patrol allow the service's packets to go through the Zyxel Device.

Note: The Zyxel Device checks secure policies before it checks application patrol rules for traffic going through the Zyxel Device.

Application patrol examines every TCP and UDP connection passing through the Zyxel Device and identifies what application is using the connection. Then, you can specify whether or not the Zyxel Device continues to route the connection. Traffic not recognized by the application patrol signatures is ignored.

Application Profiles & Policies

An application patrol profile is a group of categories of application patrol signatures. For each profile, you can specify the default action the Zyxel Device takes once a packet matches a signature (forward, drop, or reject a service's connections and/or create a log alert).

Use policies to link profiles to traffic flows based on criteria such as source zone, destination zone, source address, destination address, schedule, user.

Classification of Applications

There are two ways the Zyxel Device can identify the application. The first is called auto. The Zyxel Device looks at the IP payload (OSI level-7 inspection) and attempts to match it with known patterns for specific applications. Usually, this occurs at the beginning of a connection, when the payload is more consistent across connections, and the Zyxel Device examines several packets to make sure the match is correct. Before confirmation, packets are forwarded by App Patrol with no action taken. The number of packets inspected before confirmation varies by signature.

Note: The Zyxel Device allows the first eight packets to go through the security policy, regardless of the application patrol policy for the application. The Zyxel Device examines these first eight packets to identify the application.

The second approach is called service ports. The Zyxel Device uses only OSI level-4 information, such as ports, to identify what application is using the connection. This approach is available in case the Zyxel Device identifies a lot of "false positives" for a particular application.

Custom Ports for SIP and the SIP Pinhole

Configuring application patrol to use custom port numbers for SIP traffic also configures the SIP Pinhole to use the same port numbers for SIP traffic. Likewise, configuring the SIP Pinhole to use custom port numbers for SIP traffic also configures application patrol to use the same port numbers for SIP traffic.

19.2 Application Patrol Profile

Use the application patrol screens to customize action and log settings for a group of application patrol signatures. You then link a profile to a policy. Use this screen to create an application patrol profile, and view signature information. It also lists the details about the signature set the Zyxel Device is using.

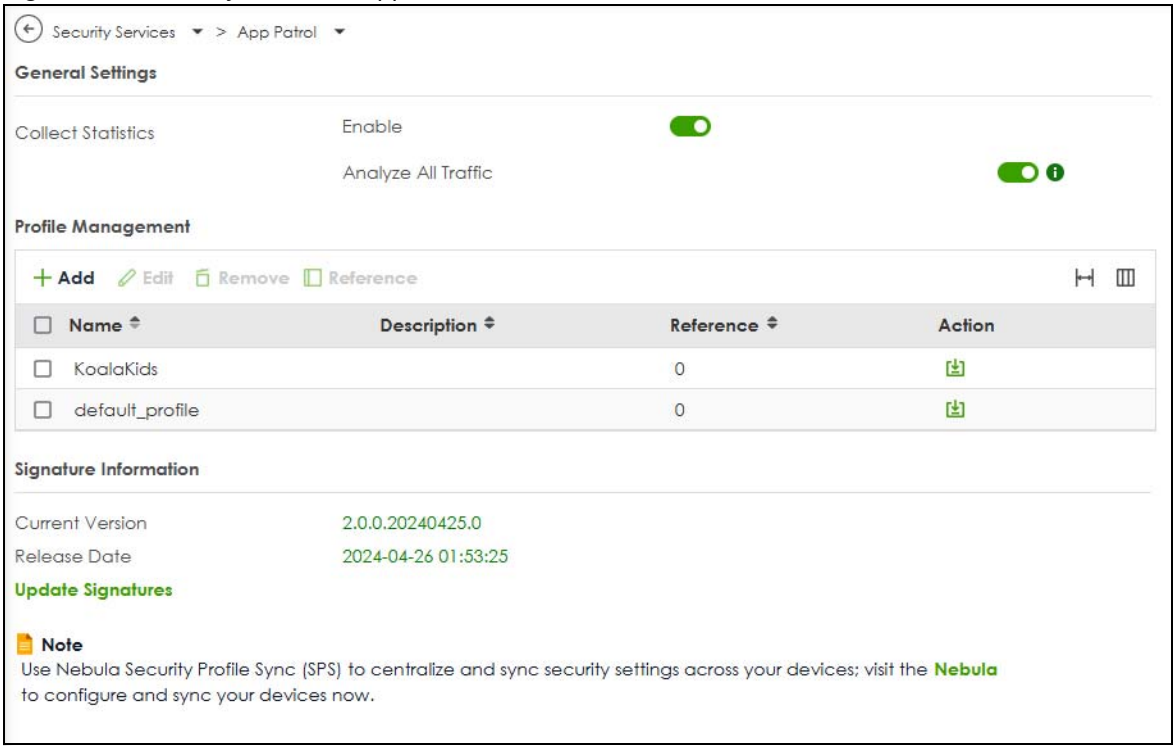
Note: You must register for the AppPatrol signature service (at least the trial) before you can use it.

A profile is an application object(s) or application group(s) that has customized action and log settings.

Click **Security Service > App Patrol** to open the following screen.

Click the **Application Patrol** icon for more information on the Zyxel Device's security features.

Figure 225 Security Service > App Patrol



The following table describes the labels in this screen.

Table 165 Security Service > App Patrol

LABEL	DESCRIPTION
Collect Statistics	
Enable	Enable to have the Zyxel Device identify and display application traffic statistics in **Traffic Statistics > Application Usage**. All statistics are erased if you restart the Zyxel Device or click **Flush Data** in **Security Statistics** > **App Patrol**.
Analyze All Traffic	Enable this to have the Zyxel Device identify applications in all traffic. Traffic is identified, but no action is taken. Use security policies to take action on matched traffic. Disable this to have the Zyxel Device identify applications only from traffic that matches security policies that have app patrol profiles applied. For example, if you create an app patrol profile and apply it to the **LAN_Outgoing** security policy, the Zyxel Device will only collect application statistics from traffic that matches the **LAN_Outgoing** security policy.
Profile Management	
Add	Click this to create a new profile. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Select an entry and click **Edit** to open a screen where you can modify the entry's settings.
Remove	Select one or more entries and click **Remove** to delete the selected entry.
Reference	Select an entry and click **Reference** to check which settings use the entry.
Copy	You can create a new entry by copying an existing one to a new position, and then editing it. Select an existing policy and click **Copy** to display a field to type a number for where you want to put that entry, then press [ENTER] to copy the entry to the number that you typed. After copying it, edit it to change it from the one copied.
Name	This displays the name of the profile created.
Description	This displays the description of the App Patrol Profile.

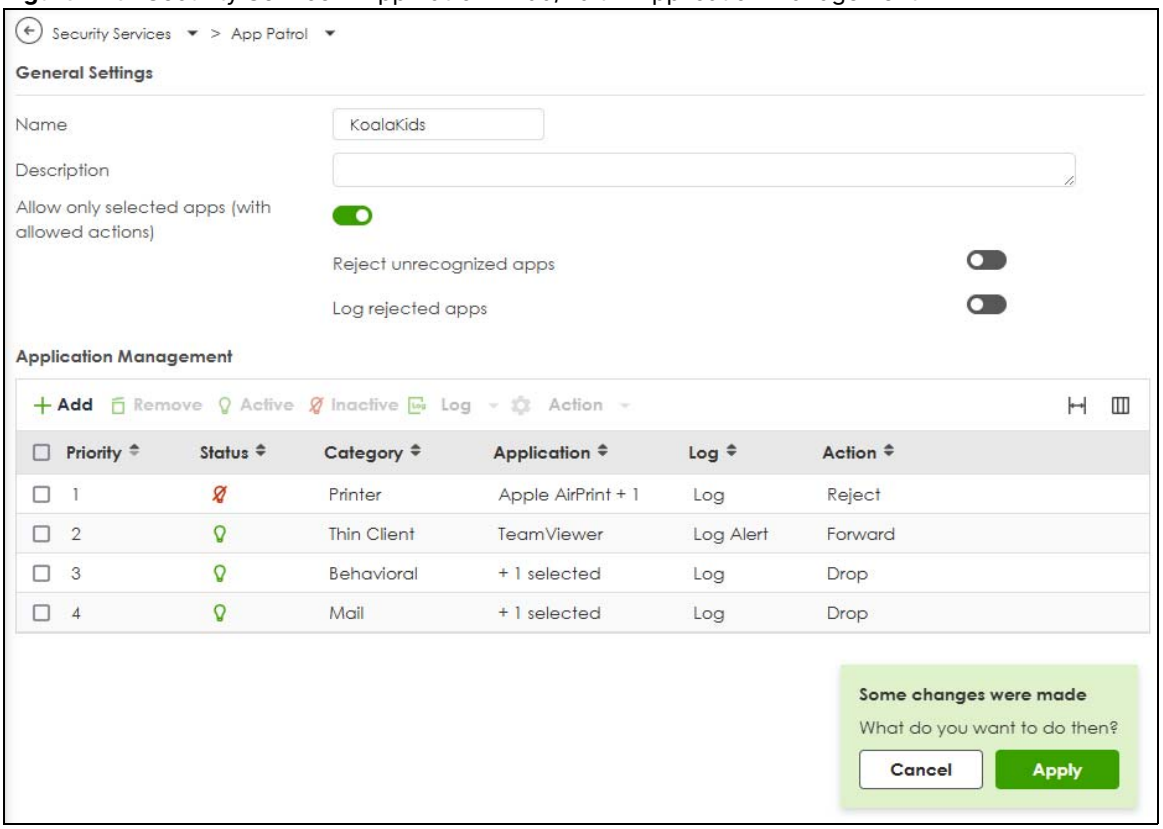
Table 165 Security Service > App Patrol

LABEL	DESCRIPTION
Reference	This displays the number of times an object reference is used in a profile.
Action	Click this icon to go to a screen to apply the entry to a policy control rule. Go to the **Security Policy** > **Policy Control** screen to check the result.
Signature Information	The following fields display information on the current signature set that the Zyxel Device is using.
Current Version	This field displays the App Patrol signature set version number.
Released Date	This field displays the date and time the set was released.
Update Signatures	Click this link to go to the screen you can use to download signatures from the update server.

19.2.1 Application Patrol Profile > Add/Edit - Application Management

Use this screen to configure profile settings. Click **Security Service > App Patrol > Add/Edit** to open the following screen.

Figure 226 Security Service > App Patrol > Add/Edit > Application Management



The following table describes the labels in this screen.

Table 166 Security Service > App Patrol > Add/Edit > Application Management

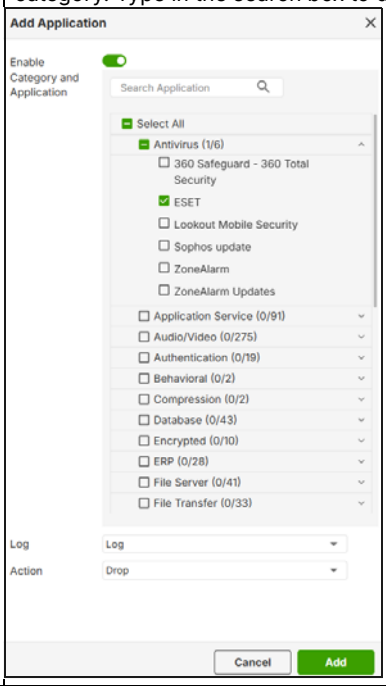
LABEL	DESCRIPTION
General Settings	
Name	Type the name of the profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. These are valid, unique profile names: • MyProfile • mYProfile • Mymy12_3-4 These are invalid profile names: • 1mYProfile • My Profile • MyProfile? • Whatalongprofilename123456789012
Description	Type a description for the 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.
Allow only selected apps (with allowed actions)	Enable this to have the Zyxel Device drop packets from applications that are not included in this profile and send a TCP RST or ICMP host unreachable message to both the sender and receiver.
Rejected unrecognized apps	Enable this to have the Zyxel Device drop packets from applications that are not recognized and send a TCP RST or ICMP host unreachable message to both the sender and receiver.
Log rejected apps	Enable this to have the Zyxel Device generate a log when it rejects applications that are not included in this profile or are unrecognized.
Application Management	
Add	Click **Add** to create a new profile. You may select individual applications within each category. Type in the search box to display all associated entries. 
Remove	To remove one or more entries, select them and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.

Table 166 Security Service > App Patrol > Add/Edit > Application Management

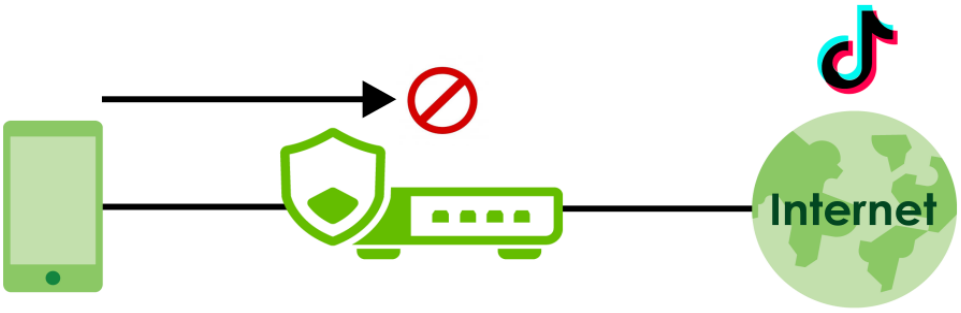
LABEL	DESCRIPTION
Active	To turn one or more entries, select them and click **Active**. The **Status** light changes accordingly.
Inactive	To turn off one or more entries, select them and click **Inactive**. The **Status** light changes accordingly.
Log	Select whether to have the Zyxel Device generate a log (**log**), log and alert (**log alert**) or neither (**no**) by default when traffic matches a signature in the selected profiles. You may still edit individual profiles within the profile row.
Action	Select the default action for all signatures in the selected profiles. You may still edit individual profiles within the profile row. • **forward** - the Zyxel Device routes packets that matches these signatures. • **drop** - the Zyxel Device silently drops packets that matches these signatures without sending a TCP RST or ICMP host unreachable message to both the sender and receiver. • **reject** - the Zyxel Device drops packets that matches these signatures and sends a TCP RST or ICMP host unreachable message to both the sender and receiver.
Priority	This field is a sequential value showing the number of the profile. The ordering of your profiles is important as profiles are applied in sequence.
Status	Set whether this entry is **Active** or **Inactive**.
Category	This field displays the category type of the application. You may edit this for each entry.
Application	This field displays the application name or numbers of applications included in the policy. You may edit this for each entry.
Log	Select whether to have the Zyxel Device generate a log (**log**), log and alert (**log alert**) or neither (**no**) by default when traffic matches a signature in this category.
Action	Select the default action for all signatures in this category. **forward** - the Zyxel Device routes packets that matches these signatures. **drop** - the Zyxel Device silently drops packets that matches these signatures without notification. **reject** - the Zyxel Device drops packets that matches these signatures and sends notification.
Apply	Click **Apply** to save your settings to the Zyxel Device.
Cancel	Click **Cancel** to return to the profile summary page without saving any changes.

19.3 Example: Block an Application

In this example, you want to block clients on the Zyxel Device LAN from accessing a specific application (for example, TikTok). You also want to receive a log and an alert when traffic going out from the LAN tries to access TikTok.

Create an **App Patrol** profile that includes TikTok,. Then apply it to the **LAN_Outgoing** security policy. Clients on the Zyxel Device LAN will be blocked from accessing TikTok.

Figure 227 App Patrol Tutorial Example



This example uses the parameters listed below.

Table 167 App Patrol Profile Configuration Example

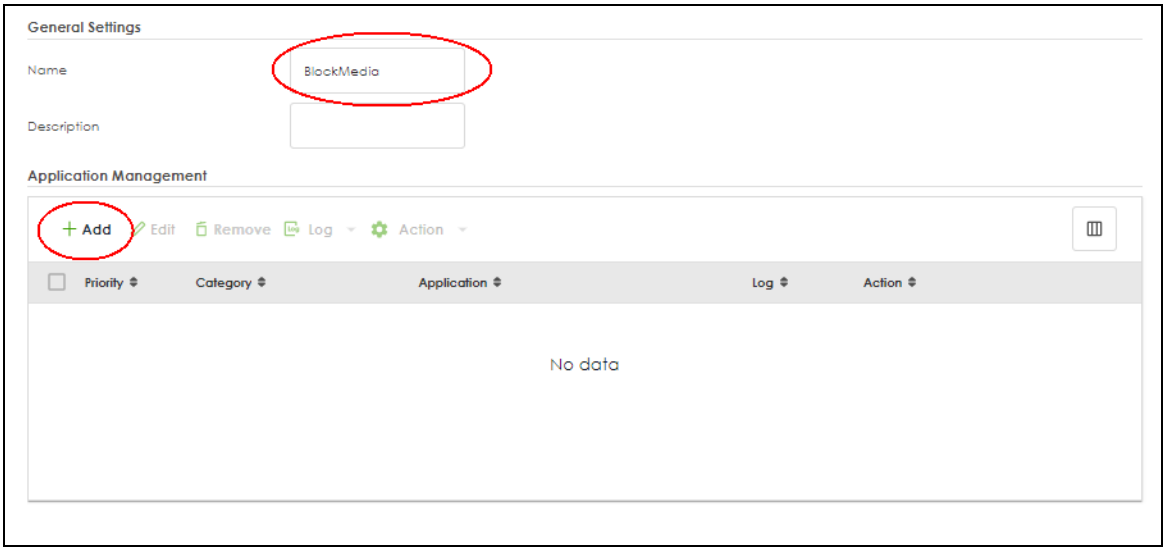
PROFILE NAME	APPLICATION	ACTION	LOG
BlockMedia	TikTok	Reject	Log Alert

Table 168 Security Policy Configuration Example

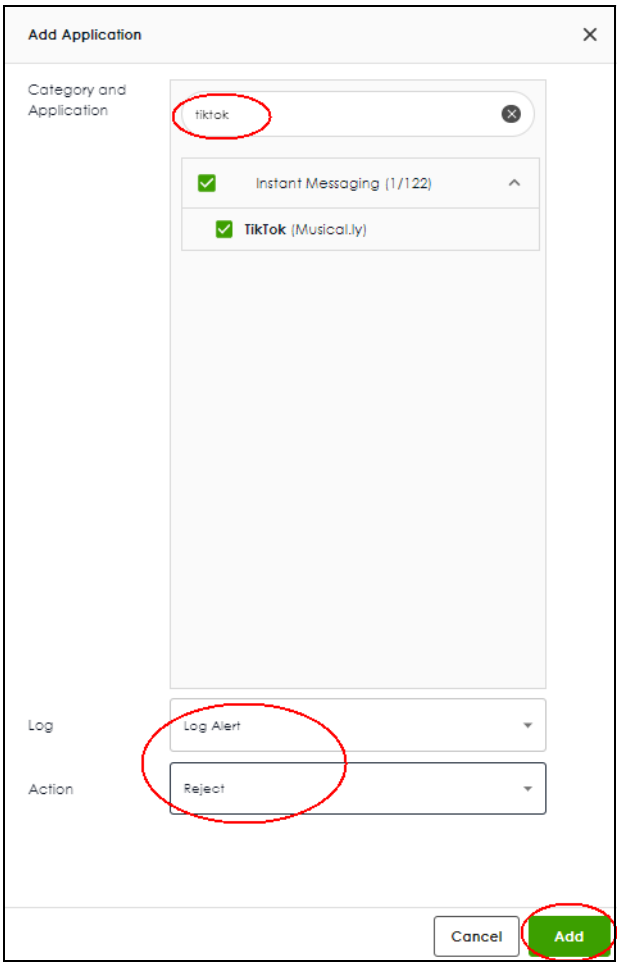
TO	FROM	LOG	APP PATROL PROFILE
WAN	LAN	By Profile	BlockMedia

1 Go to **Security Service** > **App Patrol** and click **Add**.

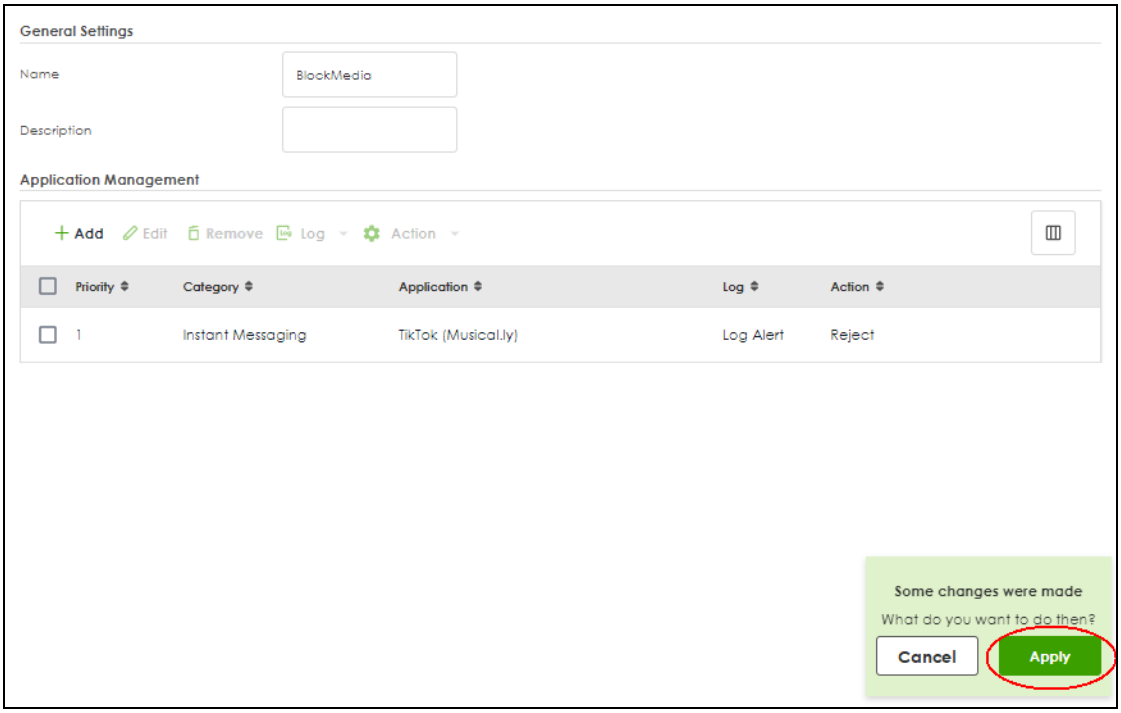
2 In the following screen, enter the profile name using the parameter given in Table 167 on page 356. Click **Add** under **Application Management** to open the **Add Application** screen.



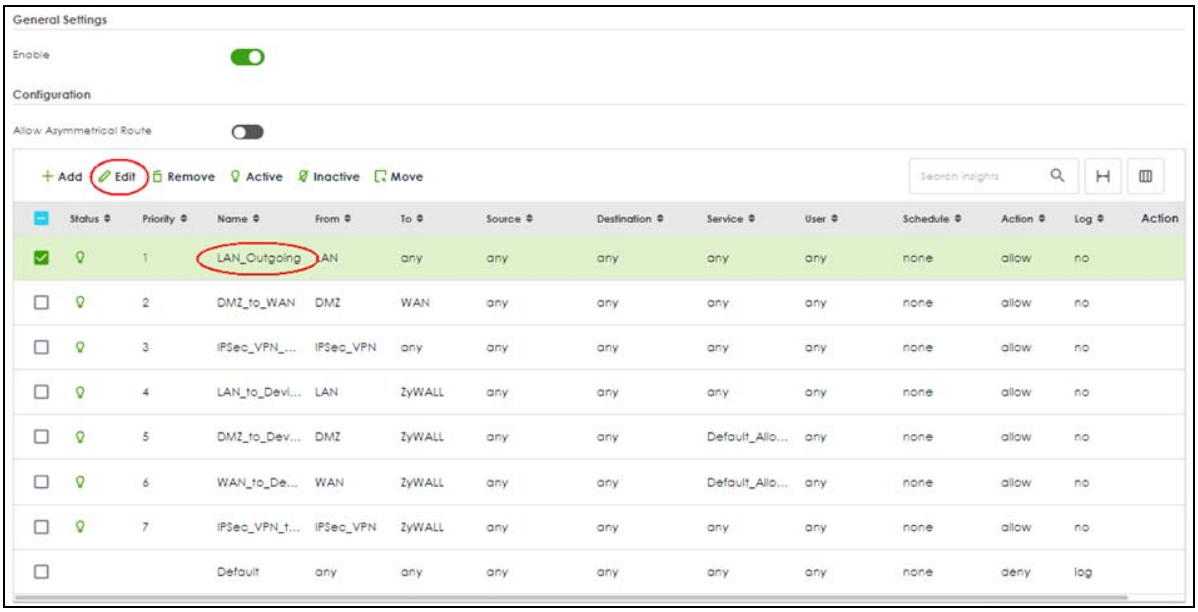
3 Search for TikTok in **Category and Application** and select the checkbox. Set **Log** to **Log Alert** and **Action** to **Reject**. Click **Add** to save your changes.



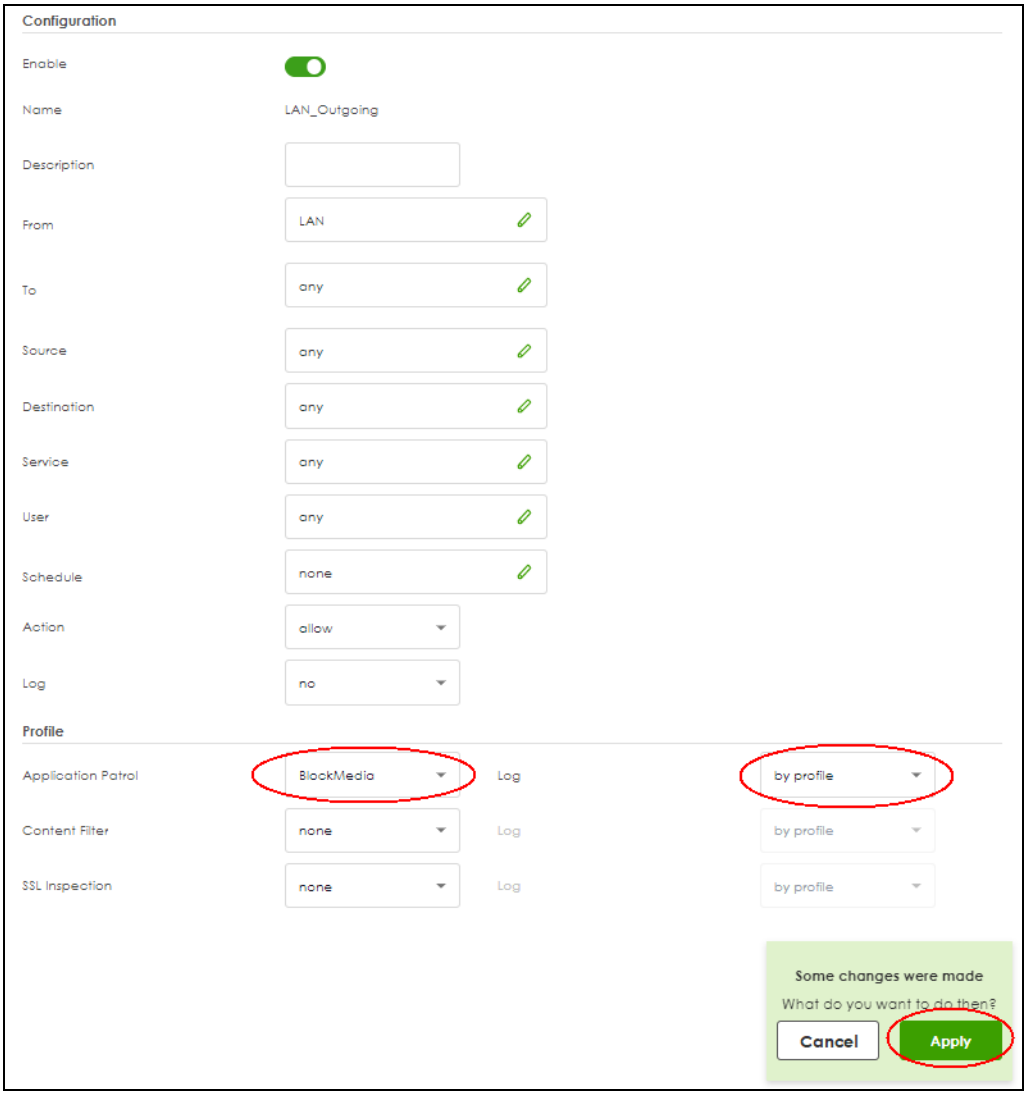
4 Click **Apply** to save the app patrol profile.



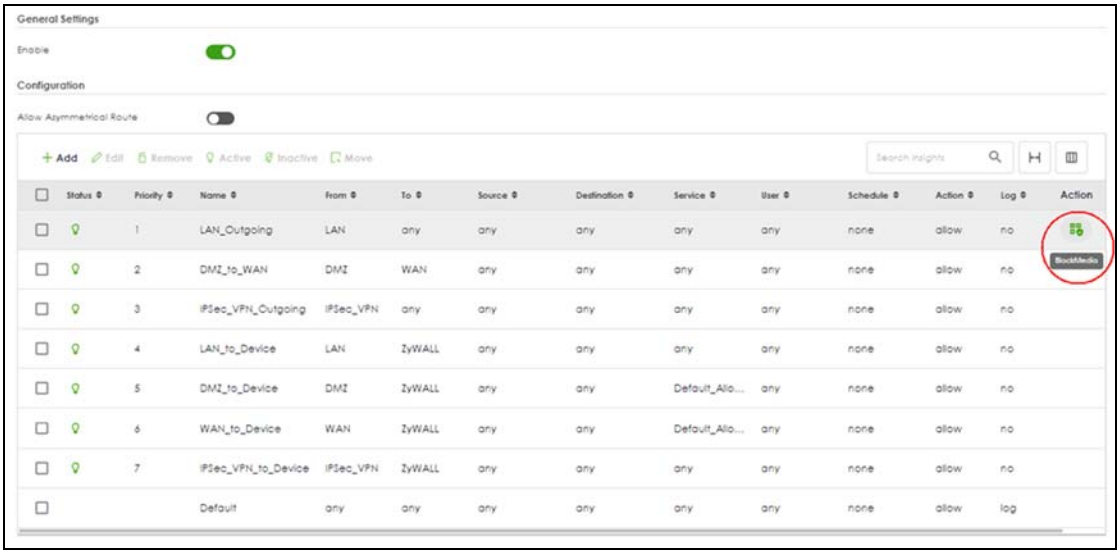
5 Go to **Security Policy** > **Policy Control**. Select **LAN_Outgoing** then click **Edit**.



6 Set **Application Patrol** to **BlockMedia** and **Log** to **by profile**. Click **Apply** to save your changes.



7 You can check the result in the **Policy Control** screen. Mouse-over the icon under the **Action** column to check that the **BlockMedia** profile has been applied to the **LAN_Outgoing** security policy. You can also check the logs in **Log & Report** > **Log / Events**. The Zyxel Device will create logs if the clients on the Zyxel Device LAN try to access TikTok.

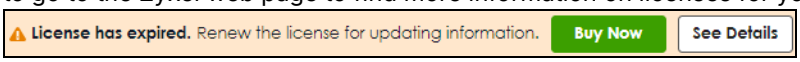

General Settings
Enable
Configuration
Allow Asymmetrical Route
+ Add
Edit
Remove
Active
Inactive
Move
Search insights
Status
Priority
Name
From
To
Source
Destination
Service
User
Schedule
Action
Log
Action
1 LAN_Outgoing LAN any any any any any none allow no
2 DMZ_to_WAN DMZ WAN any any any any none allow no
3 IPSec_VPN_Outgoing IPSec_VPN any any any any any none allow no
4 LAN_to_Device LAN ZyWALL any any any any none allow no
5 DMZ_to_Device DMZ ZyWALL any any Default_Allo... any none allow no
6 WAN_to_Device WAN ZyWALL any any Default_Allo... any none allow no
7 IPSec_VPN_to_Device IPSec_VPN ZyWALL any any any any none allow no
Default any any any any any any none allow log

CHAPTER 20
Content Filtering

20.1 Overview

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

If a license has expired, you will see a reminder in this screen. You need to renew the license in order to keep using the feature. Click **Buy Now** to go to Marketplace to purchase a new license. Click **See Details** to go to the Zyxel web page to find more information on licenses for your Zyxel Device.



20.1.1 What You Can Do in this Chapter

- Use the **Content Filtering** screens (Section 20.2 on page 364) to set up web content filtering profiles.
- Use **Content Filtering Allow List** (Section 20.2.3 on page 382) to create a common list of good (allowed) web site addresses.
- Use **Content Filtering Block List** (Section 20.2.4 on page 383) to create a common list of bad (blocked) web site addresses.
- Use **Content Filtering Blocked URL keywords** (Section 20.2.5 on page 384) to create a common list of bad (blocked) URL keywords.

20.1.2 What You Need to Know

HTTP(S) Traffic Scan

The HTTP(S) Traffic Scan allows the Zyxel Device to 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.

HTTP(S) Traffic Scanning Process

1. The Zyxel Device Content Filter detects an HTTP(S) connection, and inspects the website sent.
2. If the website contains prohibited material, the HTTP(S) request is redirected to a block page.

Note: If the user's web browser is using encryption, then you must enable SSL Inspection for HTTP(S) Traffic Scan to work.

Content Filtering Policies

A content filter policy allows you to do the following.

- Use schedule objects to define when to apply a content filter profile.

- Use address and/or user/group objects to define to whose web access to apply the content filter profile.
- Apply a content filter profile that you have custom-tailored.

Content Filtering Profiles

A content filtering profile conveniently stores your custom settings for the following features.

- Category-based Blocking

  The Zyxel Device can block access to particular categories of web site content, such as pornography or racial intolerance.
- 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.

HTTP(S) Traffic Scanning 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.

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 Domain Scan

The DNS Domain Scan 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 HTTP(S) Traffic Scan, the DNS Domain Scan works if the user is using TLS 1.3 with ESNI.

DNS Domain Scan 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 Domain Scan inspects the website in the DNS query packet.

If the website contains prohibited material, the DNS reply is redirected to a block page.Finding Out More

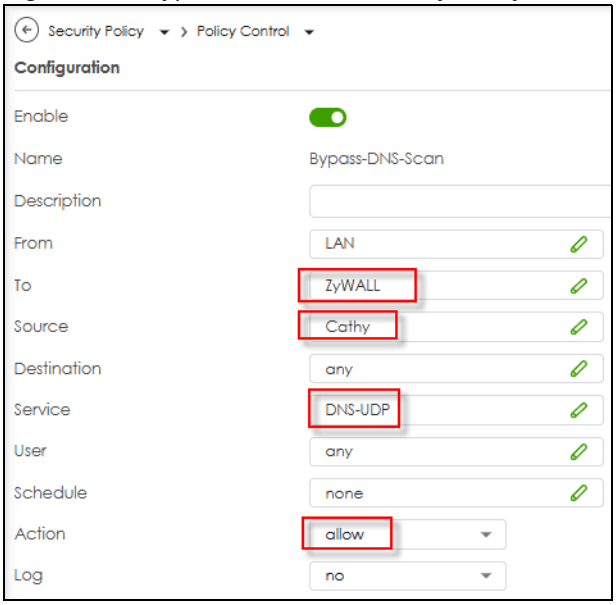
4 See Section 20.3 on page 386 for content filtering background/technical information

The Zyxel Device inspect DNS queries made by users on traffic flows where the security policy has a Content Filter profile applied. When you apply a Content Filter profile to a security policy, the Zyxel Device automatically adds a hidden 'To ZyWALL' rule for DNS-UDP service (port 53), so that DNS queries in outgoing traffic in the security policy can also be scanned for prohibited websites.

Bypassing DNS Scans in Security Policies with a Content Filter Profile

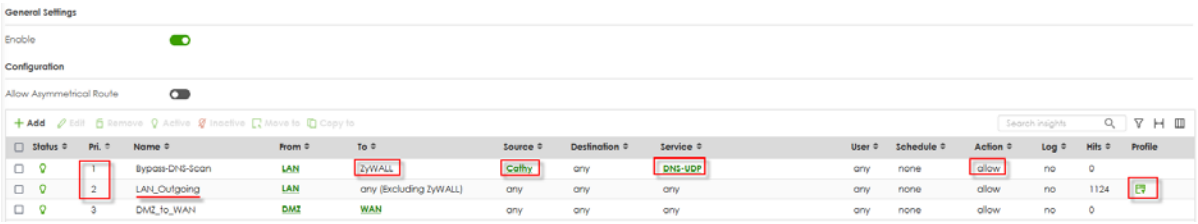
If you do not want DNS scans to be done from specific IP addresses on a specific security policy traffic flow, then you must create another 'To ZyWALL" security policy before the said security policy to allow DNS-UDP service. For example, the LAN_Outgoing security policy has an applied Content Filter. To bypass DNS scans from the address object 'Cathy', create a 'To ZyWALL' policy with DNS-UDP allowed

Figure 228 Bypass DNS Scan Security Policy



Make sure this policy is before the LAN_Outgoing security policy.

Figure 229 Bypass DNS Scan Security Policy



External Category-Based Content Filtering Server

When you register for and enable the external content 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.

External Content Filtering Server Lookup Procedure

The content filtering lookup process is described below.

Figure 230 Content Filtering 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. If the Zyxel Device has no record of the web site, it queries the external content filtering database.
4. The external content filtering 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.

20.2 Content Filtering General Screen

Use this screen to enable HTTP(S), DNS domain scanning, test website categories and view / create content filter policies.

20.2.1 HSTS and QUIC

HSTS (HTTP Strict Transport Security) forces browsers to use HTTPS only when connecting to a website. With HSTS, the browser will automatically convert future HTTP requests to HTTPS, refuse insecure connections, prevent SSL stripping attacks.

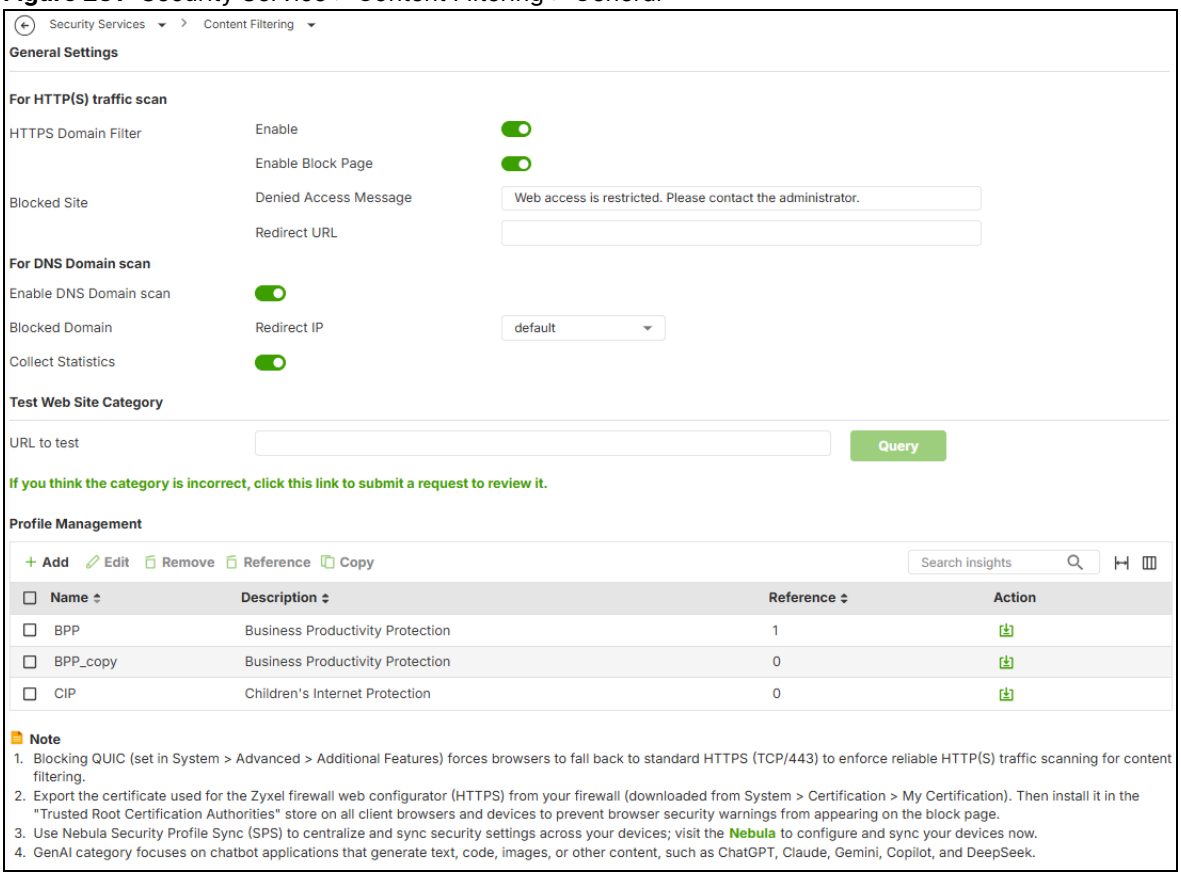
Note: Export a certificate from **System > Certificate > My Certificates** and send it to users to import into their browsers so as they can avoid seeing certificate error warnings. Users should see their browser help to see how to import certificates.

QUIC (Quick UDP Internet Connections) is a transport protocol that encrypts most of the transport layer. If QUIC is not blocked, the Zyxel Device may not be able to inspect this encrypted traffic and apply this content filtering category.

Note: Enable **Block QUIC Protocol** in **System > Advanced** to stop browsers using QUIC so that the Zyxel Device can use SSL inspection to inspect encrypted traffic for AI requests and replies.

Click **Security Services > Content Filtering** > **General** to open the **Content Filtering** screen.

Figure 231 Security Service > Content Filtering > General



The following table describes the labels in this screen.

Table 169 Security Service > Content Filtering > General

LABEL	DESCRIPTION
For HTTP(S) traffic scan	
HTTPS Domain Filter	The following two fields apply to the domain filter.
Enable	Select this check box 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 Block Page	Use this field to have the Zyxel Device display a warning page instead of a blank page when an HTPPS connection is redirected.
Blocked Site	The following two fields apply to the blocked site.
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;/?:@&=+$\.-_!~*'()%,"]. For example, "Web access is restricted. Please contact the administrator". This field cannot be blank.
Redirect URL	Enter the URL of the web page to which you want to send users when their web access is blocked by content filter. The web page you specify here opens in a new frame below the denied access message. Use "http://" or "https://" followed by up to 255 characters [0-9a-zA-Z;/?:@&=+$.-_!~*'()%]. For example, http://192.168.1.17/blocked access.
For DNS Domain scan	
Enable DNS Domain scan	Select this to have the Zyxel Device inspect DNS queries made by users on traffic flows where the security policy has a **Content Filter** profile applied. See DNS Domain Scan on page 363 for more details on how this feature works.
Blocked Domain	This is 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.
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. 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.
Collect Statistics	Enable to have the Zyxel Device collect content filtering statistics. All of the statistics are erased if you restart the Zyxel Device or click **Flush Data** in **Security Statistics** > **Content Filter**.

Table 169 Security Service > Content Filtering > General (continued)

LABEL	DESCRIPTION
Test Web Site Category	
URL to test	Enter a web site URL in the text box. When content filtering is active, you should see the web page's category. The query fails if content filtering is not active. Content Filterilg can query a category by full URL string (for example, http://www.google.com/picture/index.html), 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	Profiles cannot be added to 'To ZyWALL' security policies. 'ZyWALL' may also be referred to as 'Device'
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.
Reference	Select an entry and click **Reference** to check which settings use the entry.
Copy	You can create a new rule by copying an existing one to a new position, and then editing it. Select an existing policy and click **Copy** to display a field to type a number for where you want to put that rule, then press [ENTER] to copy the rule to the number that you typed. After copying it, edit it to change it from the one copied.
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 shows the number of references this profile uses.
Action	Click this icon to apply the entry to a policy control rule. Go to the **Security Policy** > **Policy Control** screen to check the result.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

20.2.2 Content Filtering Add Profile

Click **Security Service > Content Filtering > Add or Edit** to open the following screen.

Figure 232 Security Service > Content Filter > Add Profile (General Settings)

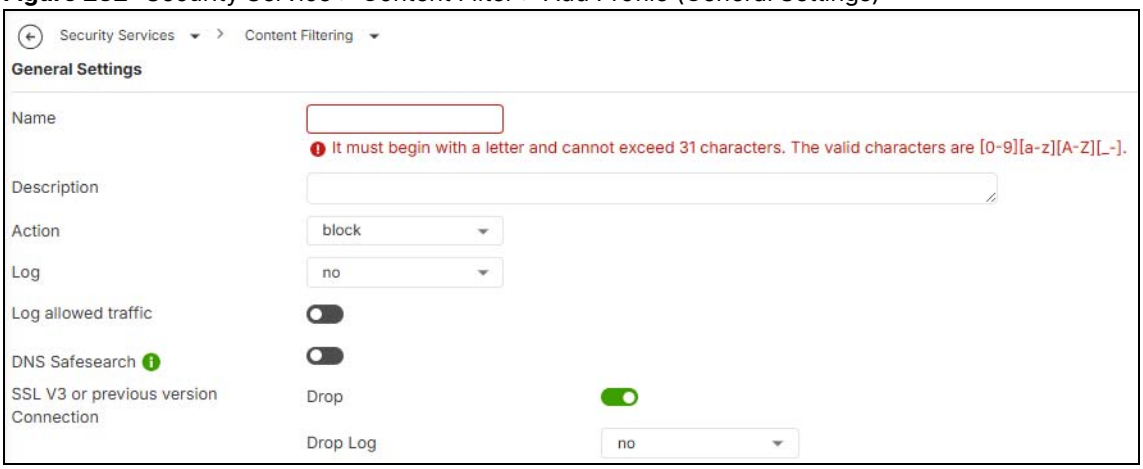


Figure 233 Security Service > Content Filter > Add Profile (Managed Categories)

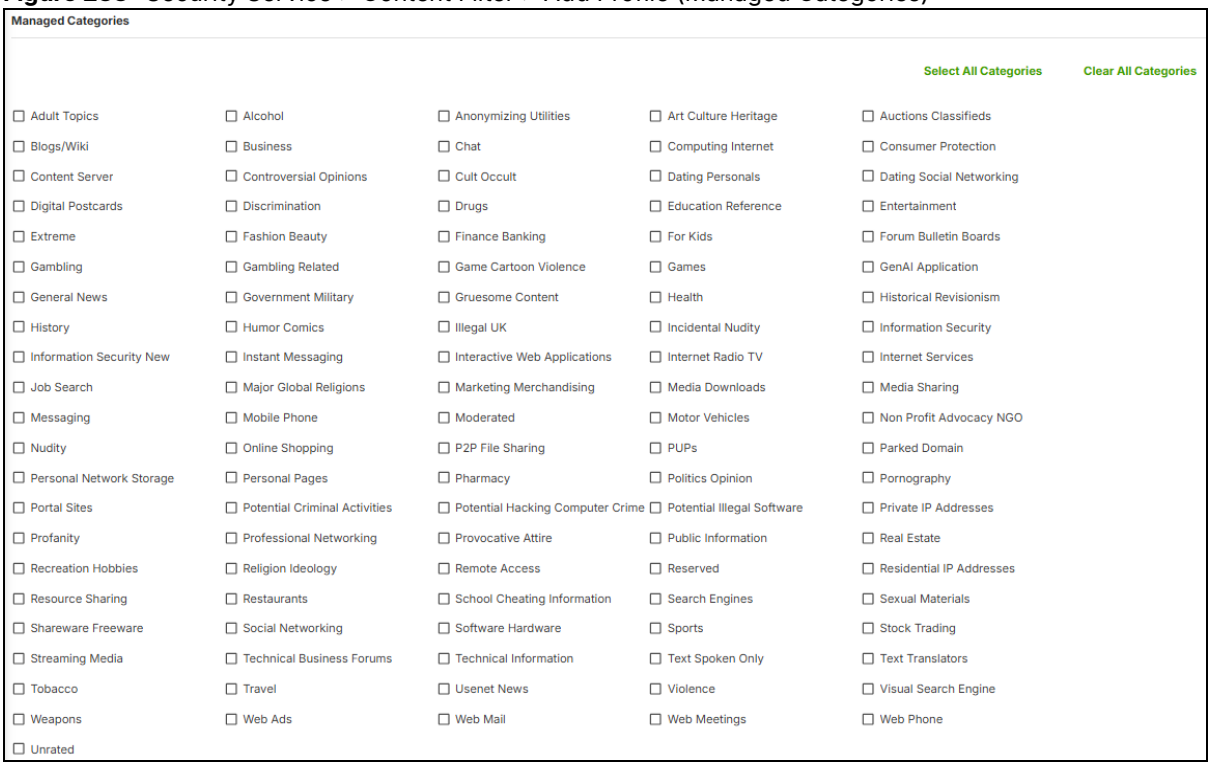


Figure 234 Security Service > Content Filter > Add Profile (Allow Block Lists)

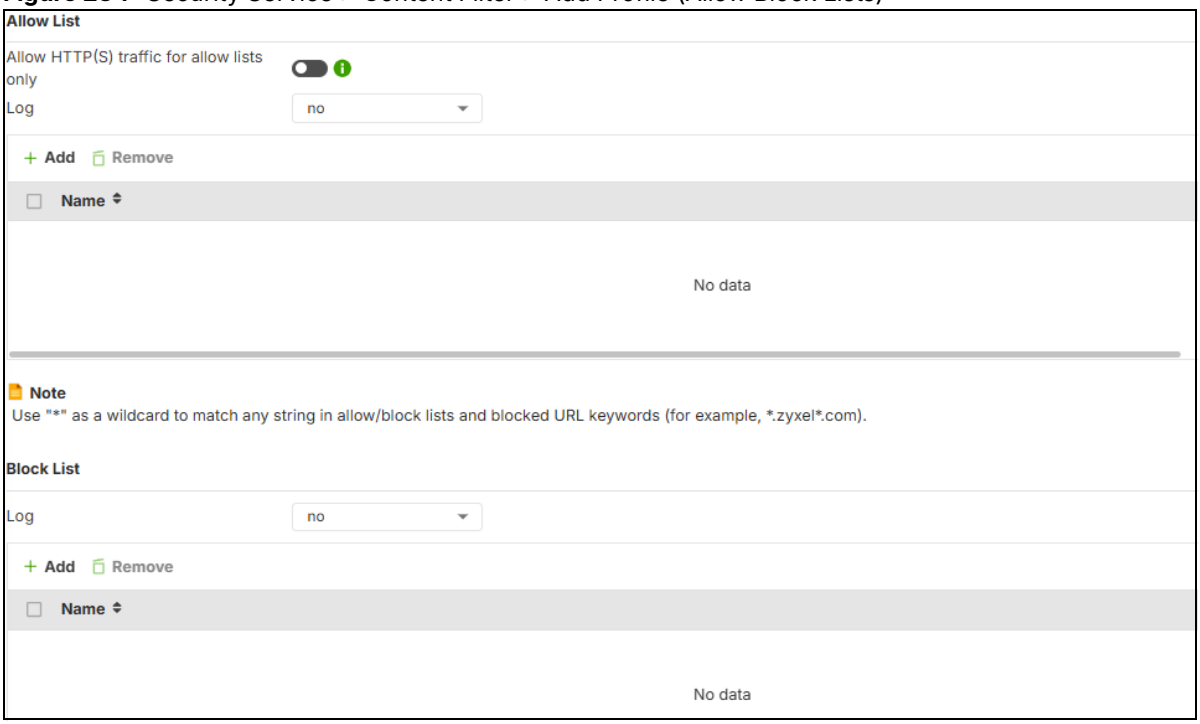
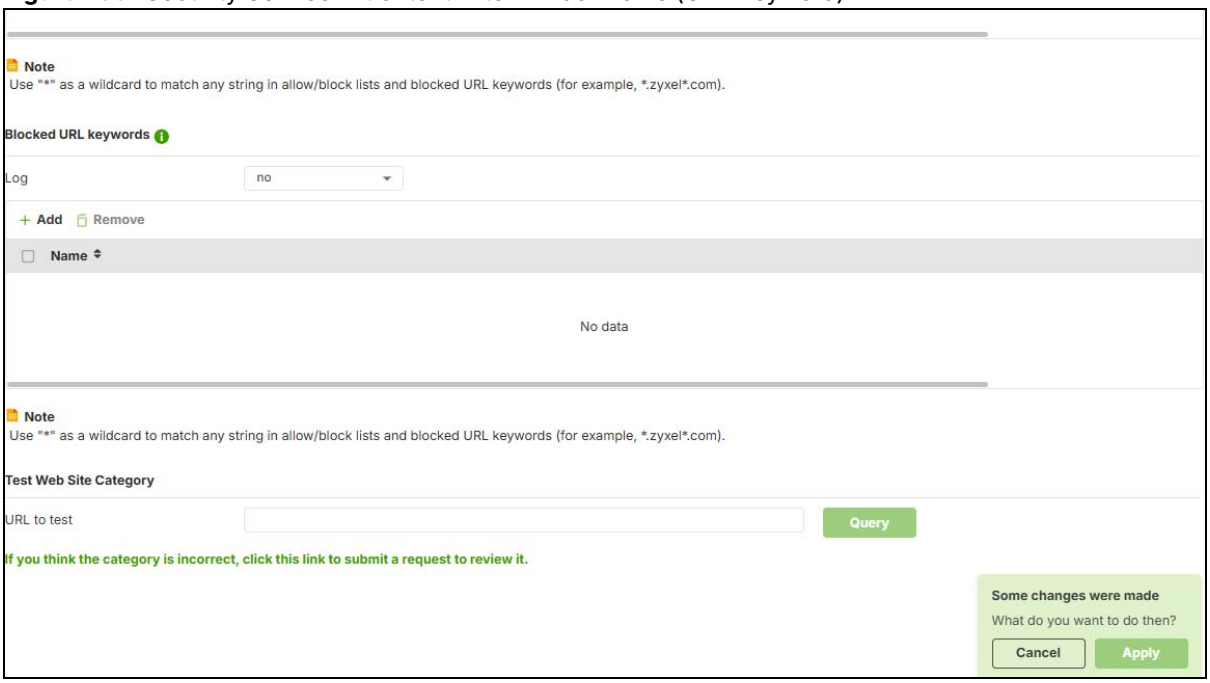


Figure 235 Security Service > Content Filter > Add Profile (URL Keyword)



The following table describes the labels in this part of the screen.

Table 170 Security Service > Content Filtering > Add Profile (General & Managed Categories)

LABEL	DESCRIPTION
Name	Enter a descriptive name for this content filtering profile name. You may use 1-31 alphanumeric characters, special characters -_@$./ are allowed, 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 **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.
Log	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**. Then select **log** to have the Zyxel Device generate logs at the info level or select **log alert** to have the Zyxel Device generate logs at the alert level. Select **no** if you don't want the Zyxel Device to generate logs.
Log allowed traffic	Enable to generate logs when users access web pages that match the categories you allow.
DNS Safesearch	DNS safe search enforces safe search mode in the Yahoo, Google, MSN Live Bing, and Yandex search engines to prevent inappropriate or adult-oriented search results in these search engines. DNS Safe Search works by intercepting DNS queries from client devices and redirecting them to safe search mode of these search engines. No setup is required on client browsers nor can safe search be disabled by the client browser. Make sure to enable **DNS Domain Scan** in **Security Services > Content Filtering**.
Restrict YouTube Access	When you enable DNS safe search, you have two choices for YouTube search. • **Strict**: This setting filters out many videos, including those with potentially harmful or adult content. This may be suitable for younger viewers. • **Moderate**: This setting allows access to a wider range of videos, but it still filters out potentially objectionable content. This may be a better option for older children or those who need access to more mature educational or informational content.
SSL V3 or previous version Connection	Secure Socket Layer version 3 (SSLv3) is a deprecated security protocol that is used to secure application protocols such as HTTP, FTP, SIP, SMTP, NNTP, and XMPP.
Drop	Select this to have the Zyxel Device block HTTPS web pages using SSLS V3 or a previous version.
Drop Log	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 drug-related web pages. When the Zyxel Device blocks HTTPS web pages using SSL V3 or a previous version, • Select **no** to not generate logs. • Select **log** to have the Zyxel Device generate logs at the info level. • Select **log alert** to have the Zyxel Device generate logs at the alert level.

Table 170 Security Service > Content Filtering > Add Profile (General & Managed Categories) (continued)

LABEL	DESCRIPTION
Managed Categories	These are categories of web pages based on their content. Select categories in this section to control access to specific types of Internet content. You must have the Category Service content filtering license to filter these categories. See the next table for category details.
Select All Categories	Select this check box to restrict access to all site categories listed below.
Clear All Categories	Select this check box to clear the selected categories below.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to exit this screen without saving your changes.

The following table describes the managed categories.

Table 171 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.

Table 171 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
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.
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 via 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.

Table 171 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
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.
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.

Table 171 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
Gen AI Application	Select this to have the Zyxel Device block Generative AI (GenAI) web pages and cloud services such as, ChatGPT, Claude, Gemini, Copilot, X, DeepSeek and so on, that generate text, code, images, audio, or other content. Note: You must apply the profile with **GenAI Application** enabled to a security policy in **Security Policy > Policy Control** to block GenAI for the traffic flow in that policy. The block page suggests you access these pages and services through *anyinsight.ai*. With an account, *anyinsight.ai* can filter, mask, and enforce company policies between users and these GenAI web pages and cloud services. See *anyinsight.ai* and **System > External Integrations > Heartbot** for more information.
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.
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.

Table 171 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
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.
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.

Table 171 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
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.
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.

Table 171 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
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.
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.
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.
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.

Table 171 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
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.
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.

Table 171 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
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 via 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.
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.

Table 171 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
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.
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.

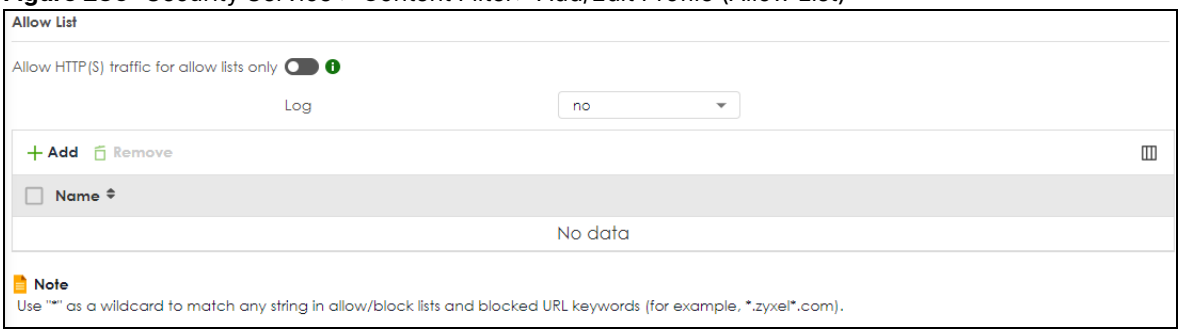
Table 171 Managed Category Descriptions (continued)

CATEGORY	DESCRIPTION
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.
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 via 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 via TCP/ IP networks.
Unrated	Web pages that cannot be categorized into the categories listed above.

20.2.3 Content Filtering Profile (Allow List)

Click **Security Service > Content Filtering > Add/Edit** to open the profile screen and scroll to the **Allow List** part. You can create a common list of good (allowed) web site addresses. Use this part of screen to add or remove specific sites from the filter list.

Figure 236 Security Service > Content Filter> Add/Edit Profile (Allow List)



The following table describes the labels in this part of the screen.

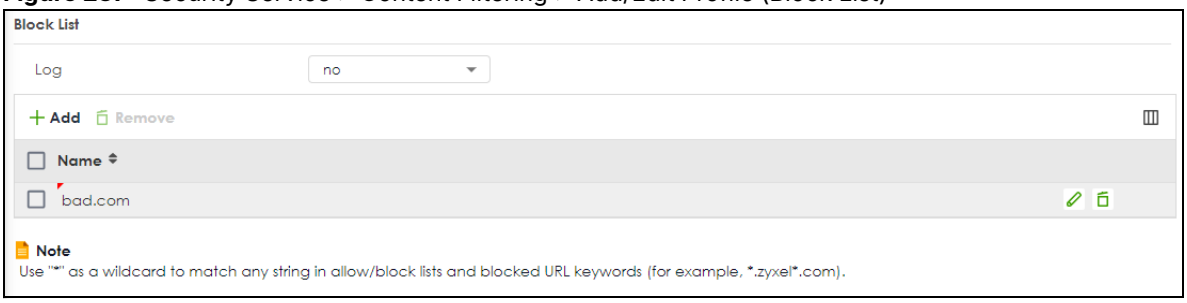
Table 172 Security Service > Content Filter > Add/Edit Profile (Allow List)

LABEL	DESCRIPTION
Allow HTTP(S) traffic for allow lists only	Select this to have the Zyxel Device only allow access to the web sites listed in the allow list.
Log	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. Select **log** to have the Zyxel Device generate logs at the info level or select **no** if you don't want the Zyxel Device to generate logs.
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.
Name	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.
Edit	Select an entry and click this icon to modify it. 
Remove	Select an entry and click this icon to delete it. 
Save Changes	Click this icon to save the changes in this row. 
Cancel Changes	Click this icon to cancel the changes in this row. 

20.2.4 Content Filtering Profile (Block List)

Click **Security Service > Content Filtering > Add/Edit** to open the profile screen and scroll to the **Block List** part. You can create a common list of bad (blocked) web site addresses. Use this part of the screen to add or remove specific sites from the filtering list.

Figure 237 Security Service > Content Filtering > Add/Edit Profile (Block List)



The following table describes the labels in this screen.

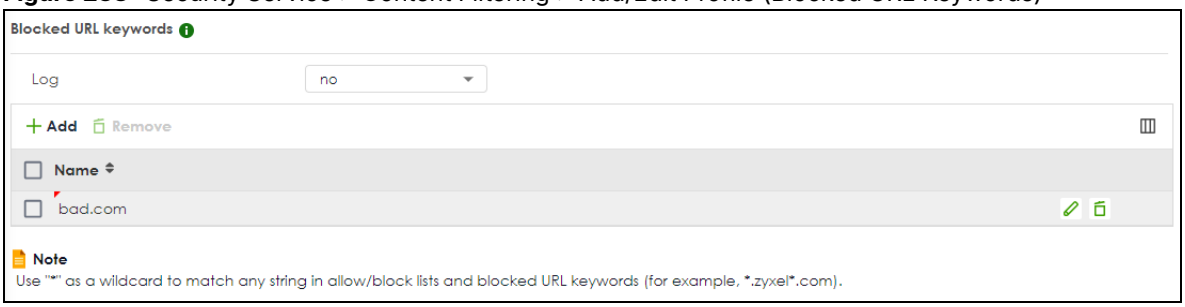
Table 173 Security Service > Content Filtering > Add/Edit Profile (Block List)

LABEL	DESCRIPTION
Log	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. Select **log** to have the Zyxel Device generate logs at the info level or select **log alert** to have the Zyxel Device generate logs at the alert level. Select **no** if you don't want the Zyxel Device to generate logs.
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.
Name	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.
Edit	Select an entry and click this icon to modify it.
Remove	Select an entry and click this icon to delete it.
Save Changes	Click this icon to save the changes in this row.
Cancel Changes	Click this icon to cancel the changes in this row.

20.2.5 Content Filtering Profile (Blocked URL Keywords)

Click **Security Service > Content Filtering > Add/Edit** to open the profile screen and scroll to the **Blocked URL keywords** part. You can create a common list of bad (blocked) URL keywords to block web sites with URLs that contain certain keywords in the domain name or IP address. Use this part of the screen to add or remove specific URL keywords from the filter list.

Figure 238 Security Service > Content Filtering > Add/Edit Profile (Blocked URL Keywords)



The following table describes the labels in this part of the screen.

Table 174 Security Service > Content Filtering > Add/Edit Profile (Blocked URL Keywords)

LABEL	DESCRIPTION
Log	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. Select **log** to have the Zyxel Device generate logs at the info level or select **log alert** to have the Zyxel Device generate logs at the alert level. Select **no** if you don't want the Zyxel Device to generate logs.
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.
Name	This list displays the forbidden 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-sensitive 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). Please note that the Zyxel Device checks the URL's domain name (or IP address) and file path separately when performing keyword blocking; see Section 20.1.2 on page 361 for more information. When the Zyxel Device inspects URL queries made by users on your network, the Zyxel Device will check both the URL domain name and file path for keywords that are blocked. Note: When the Zyxel Device inspects DNS queries made by users on your network, the Zyxel Device will only check URL domain name for keywords that are blocked, but not the file path.

Table 174 Security Service > Content Filtering > Add/Edit Profile (Blocked URL Keywords)

LABEL	DESCRIPTION
Edit	Select an entry and click this icon to modify it.
Remove	Select an entry and click this icon to delete it.
Save Changes	Click this icon to save the changes in this row.
Cancel Changes	Click this icon to cancel the changes in this row.

20.2.6 Content Filtering Profile (Test Web Site Category)

Click **Security Service > Content Filter > Add/Edit** to open the profile screen and scroll to the **Test Web Site Category** part.Use this part of the screen to check which category a web page belongs to.

Figure 239 Security Service > Content Filtering > Add/Edit Profile (Test Web Site Category)



The following table describes the labels in this part of the screen.

Table 175 Security Service > Content Filtering > Add/Edit Profile (Test Web Site Category)

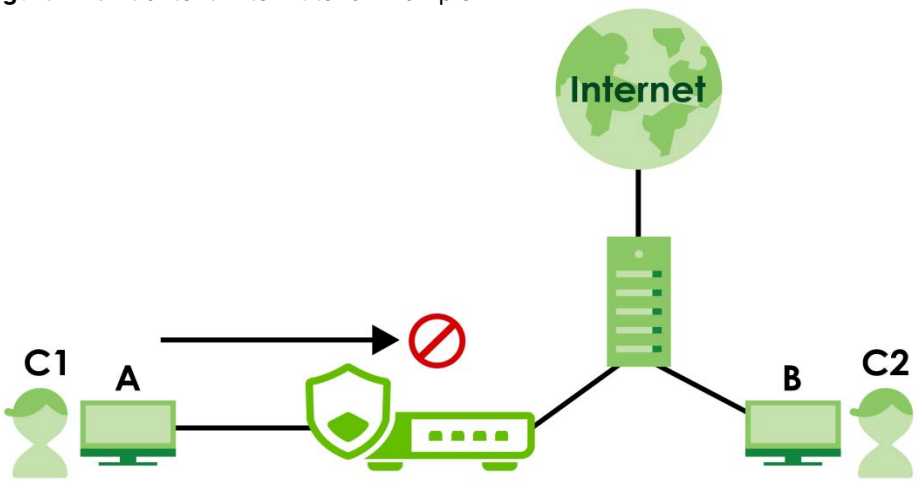
LABEL	DESCRIPTION
Test Web Site Category	
URL to test	Enter a web site URL in the text box. When content filtering is active, you should see the web page's category. The query fails if content filtering is not active. Content Filterilg can query a category by full URL string (for example, http://www.google.com/picture/index.html), 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).
Apply	Click **Apply** to save your screen changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

20.3 Content Filtering Example: Block LAN Users

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 240 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 **Content Filtering** block list 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 176 Content Filtering Profile Configuration Example

PROFILE NAME	ACTION	LOG	MANAGED CATEGORIES
NoRemoteAccess	Block	Log Alert	Remote Access

Table 177 Block List Configuration Example

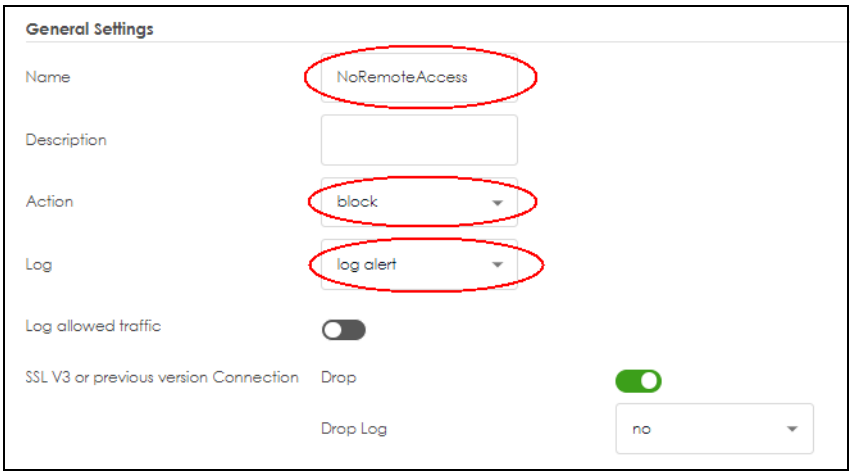
LOG	BLOCK LIST KEYWORD
Log Alert	*.*teamviewer*.*

Table 178 Security Policy Configuration Example

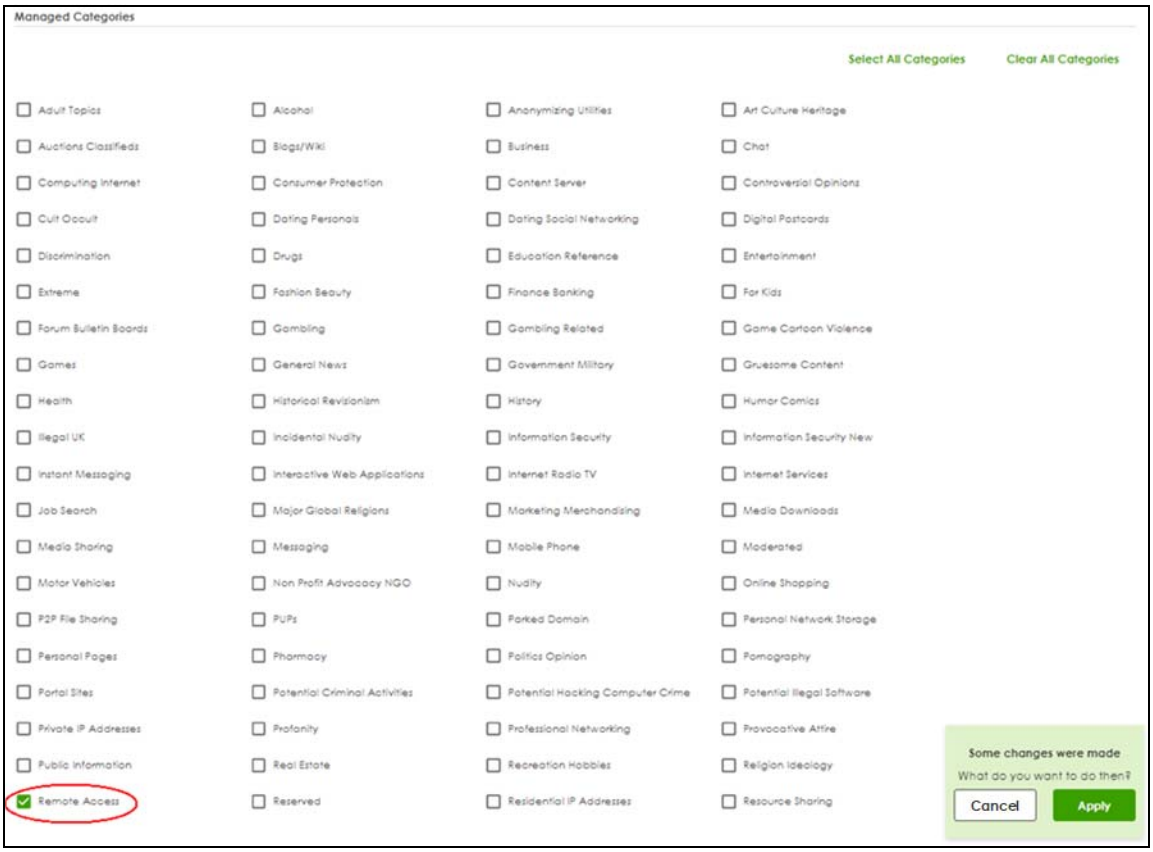
TO	FROM	LOG	CONTENT FILTERING PROFILE
WAN	LAN	By Profile	NoRemoteAccess

1 Go to **Security Service** > **Content Filtering** and click **Add**.

2 Configure the profile settings using the parameters given in Table 176 on page 386.



3 Select the **Remote Access** checkbox under **Managed Categories**.



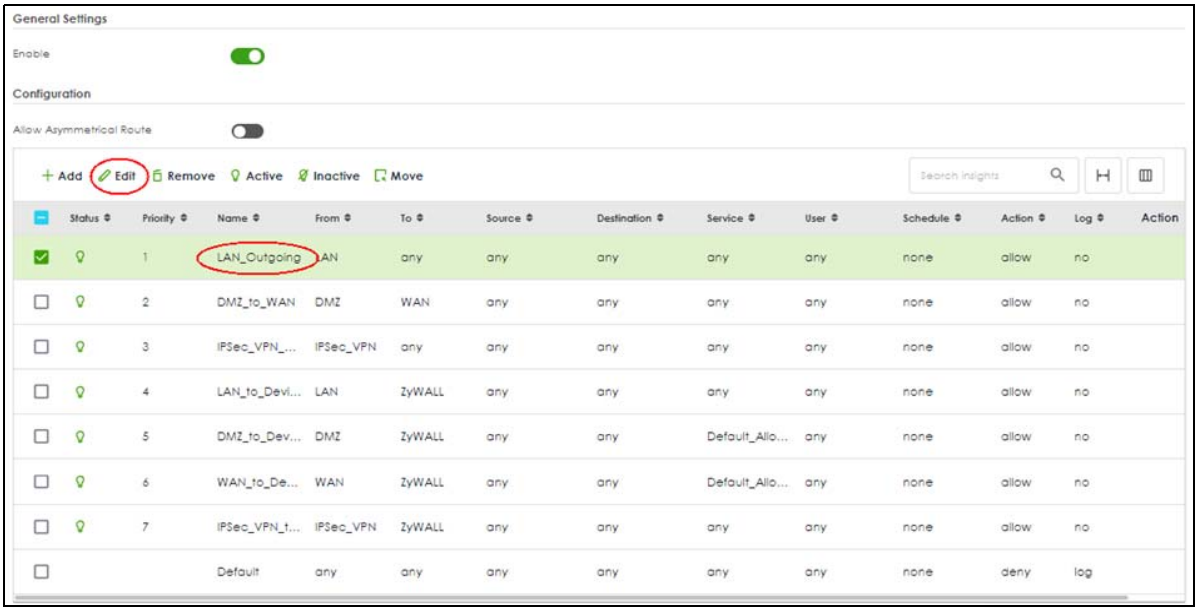
4 Set the block list log action to **log alert**.

5 Click **Add** to add a block list rule using the parameters given in Table 177 on page 386.

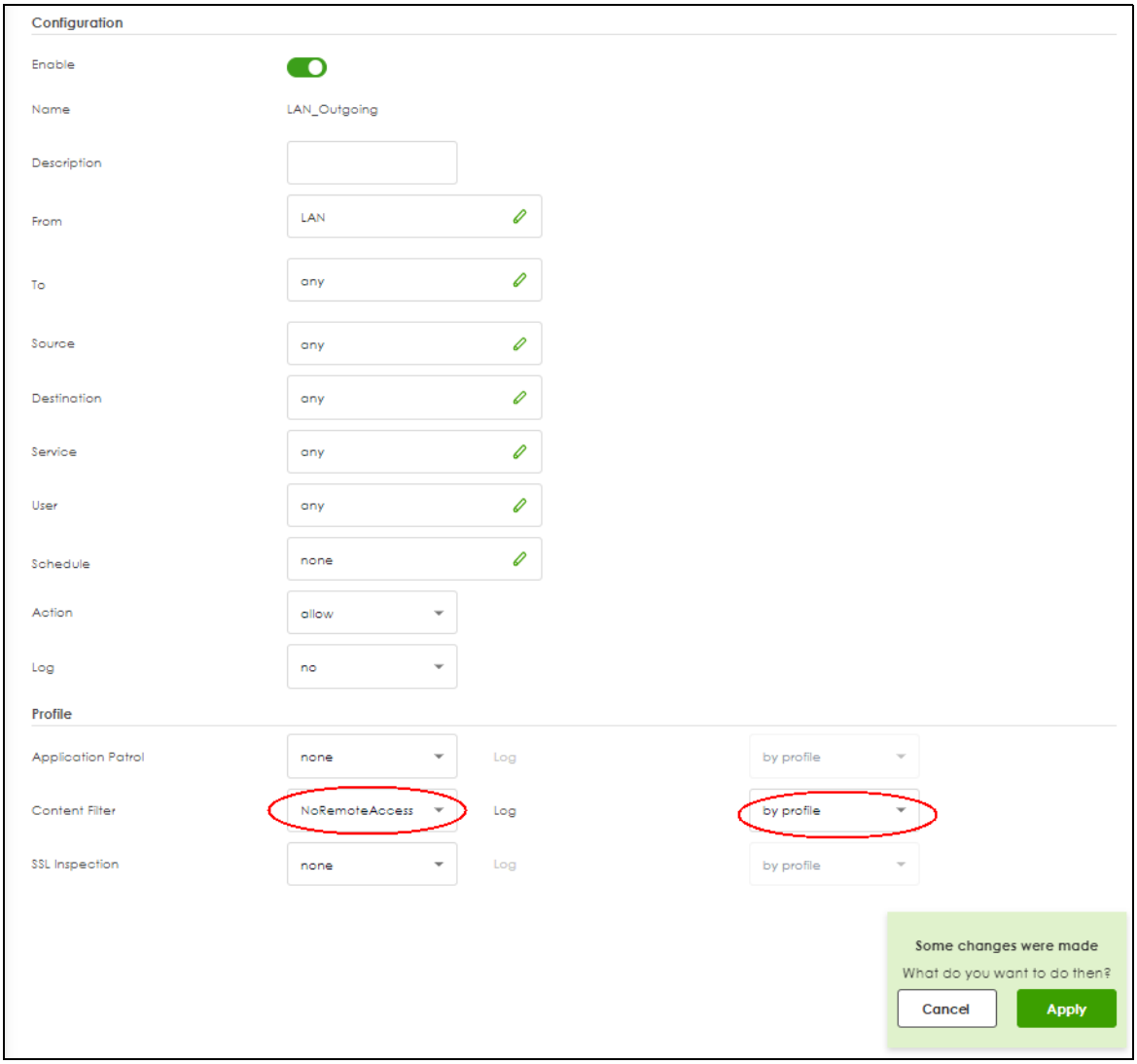


6 Click **Apply** to save your changes.

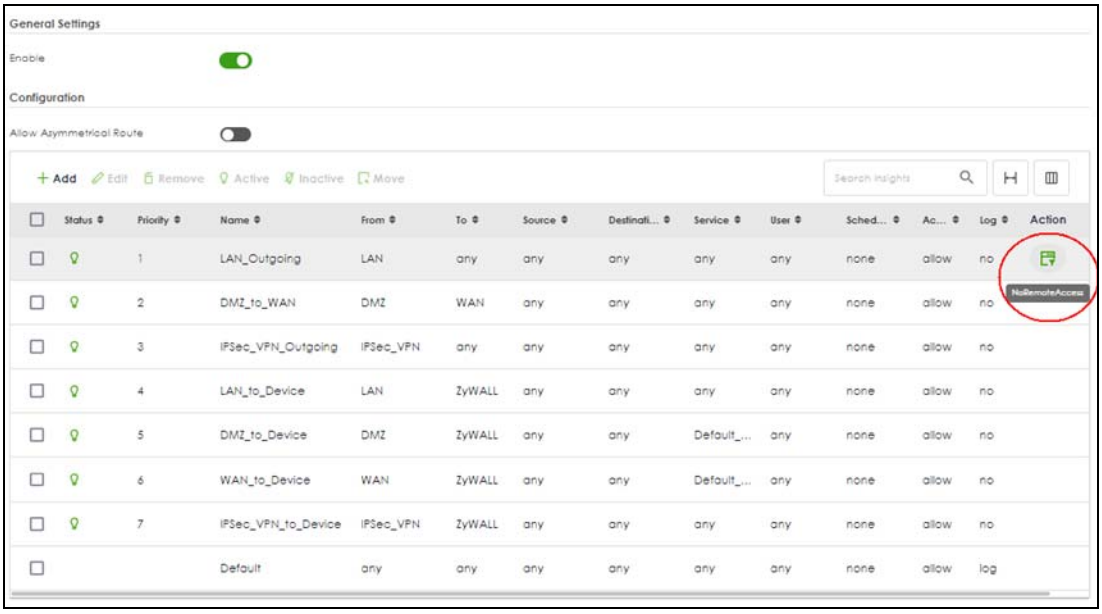
7 Go to **Security Policy** > **Policy Control**. Select **LAN_Outgoing** then click **Edit**.



8 Set **Content Filter** to **NoRemoteAccess** and **Log** to **by profile**. Click **Apply** to save your changes.



9 You can check the result in the **Policy Control** screen. Mouse-over the icon under the **Action** column to check that the **NoRemoteAccess** profile has been applied to the **LAN_Outgoing** security policy. You can also check the logs in **Log & Report** > **Log / Events**. The Zyxel Device will create logs if the clients on the Zyxel Device LAN try to access TeamViewer.

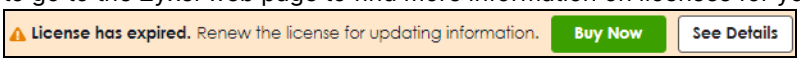

General Settings
Enable
Configuration
Allow Asymmetrical Route
+ Add
Edit
Remove
Active
Inactive
Move
Search insights
Status
Priority
Name
From
To
Source
Destinati...
Service
User
Sched...
Ac...
Log
Action
1 LAN_Outgoing LAN any any any any any none allow no
2 DMZ_to_WAN DMZ WAN any any any any none allow no
3 IPSec_VPN_Outgoing IPSec_VPN any any any any any none allow no
4 LAN_to_Device LAN ZyWALL any any any any none allow no
5 DMZ_to_Device DMZ ZyWALL any any Default_... any none allow no
6 WAN_to_Device WAN ZyWALL any any Default_... any none allow no
7 IPSec_VPN_to_Device IPSec_VPN ZyWALL any any any any none allow no
Default any any any any any any none allow log
NoRemoteAccess

CHAPTER 21
Reputation Filter

21.1 Overview

Use the **Reputation Filter** screens to configure settings for IP Reputation, DNS Threat Filter and URL Threat filtering.

If a license has expired, you will see a reminder in this screen. You need to renew the license in order to keep using the feature. Click **Buy Now** to go to Marketplace to purchase a new license. Click **See Details** to go to the Zyxel web page to find more information on licenses for your Zyxel Device.



The following table shows the number of entries allowed in each screen.

Table 179 Number of Entries Allowed Comparison Table

SCREEN	NUMBER OF ENTRIES ALLOWED
IP Reputation > Allow List	256
IP Reputation > Block List	256
IP Reputation > SecuReporter Allow List	1000
DNS Threat Filter > Allow List	1024
DNS Threat Filter > Block List	1024
DNS Threat Filter > SecuReporter Allow List	1000
URL Threat Filter > Allow List	256
URL Threat Filter > Block List	256
URL Threat Filter > SecuReporter Allow List	1000

21.1.1 What You Need to Know

IP Reputation

IP reputation checks the reputation of an IP address from a database. An IP address with bad reputation associates with suspicious activities, such as spam, virus, and/or phishing. The Zyxel Device will respond when there are packets coming from an IPv4 address with bad reputation. Supported formats are:

- Single IP 4.4.4.4
- CIDR 192.168.1.0/32
- IP range (1.2.3.4-1.2.3.100)

DNS Threat Filter

DNS threat filtering inspects DNS queries made by clients on your network and compares the queries against a database of blocked or allowed Fully Qualified Domain Names (FQDNs). The Zyxel Device DNS Threat Filter will either drop the DNS query or reply to the user with a fake DNS response. URL Threat Filter

URL threat filtering compares access to specific URLs against a database of blocked or allowed sites. Sites on the database are sorted into categories such as:

• Anonymizers	• Browser Exploits	• Malicious Downloads
• Malicious Sites	• Phishing	• Spam URLs
• Spyware Adware Keyloggers		

URL Threat Filter

Supported formats are:

- hostname (www.google.com)
- URL http - check full url (http://xxx.yyy.zzz/qqq/wwww)
- URL https - only check hostname) (https://xxx.yyy.zzz/qqq/wwww)

Allow List

An allow list is a list of entries that will bypass the related feature filtering, and are permitted to pass through the Zyxel Device. You can also create allow lists in SecuReporter and view them in the Zyxel Device.

Block List

A block list is a list of entries that will bypass the related feature filtering, but are not permitted to pass through the Zyxel Device.

21.1.2 What You Can Do in this Chapter

- Use the **IP Reputation** screen (Section 21.2 on page 392) to enable IP reputation and specify what action the Zyxel Device takes when any IP address with bad reputation is detected.
- Use the **DNS Threat Filter** screen (Section 21.3 on page 399) to allow the Zyxel Device to inspect DNS queries made by clients on your network and specify what action the Zyxel Device takes when a DNS query packet contains an FQDN with a bad reputation.
- Use the **URL Threat Filter** screen (Section 21.4 on page 405) to enable URL Threat filtering and specify what action the Zyxel Device takes when any suspicious activity is detected.

21.2 IP Reputation Screen

Use this screen to enable IP reputation and specify the action the Zyxel Device takes when it detects a suspicious activity or a connection attempt to or from an IPv4 address with bad reputation.

The priority for IP Reputation checking is as follows:

1 Allow List

2 SecuReporter Allow List

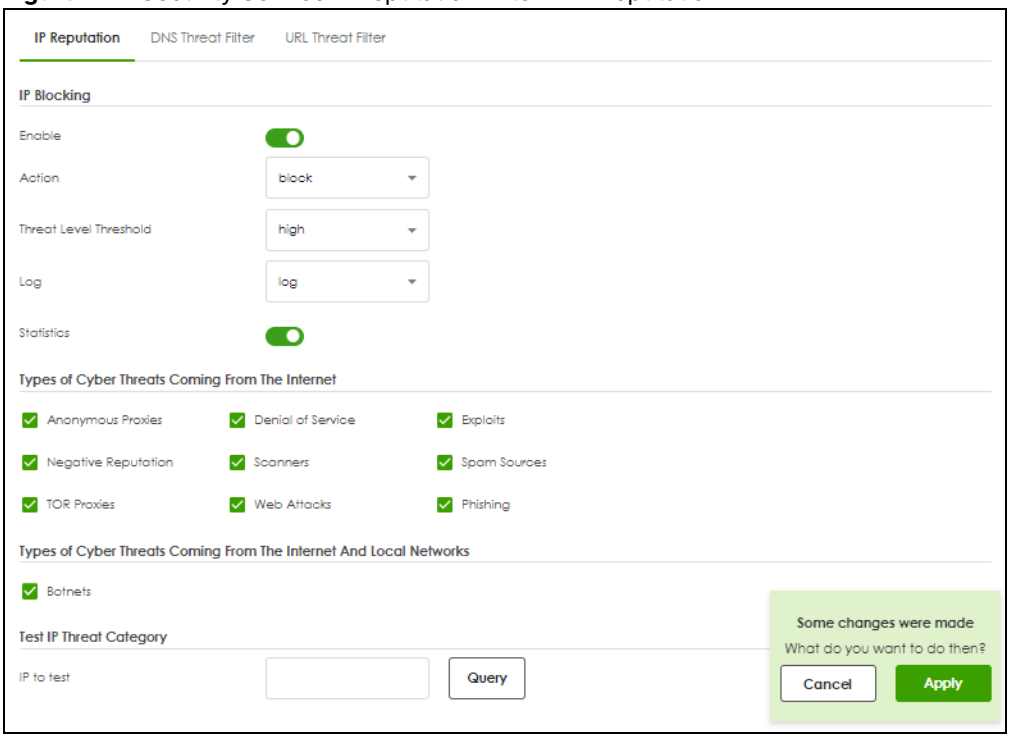
3 Block List

4 External Block List

5 Local Zyxel Device Signatures

Click **Security Service > Reputation Filter > IP Reputation** to display the configuration screen as shown next.

Figure 241 Security Service > Reputation Filter > IP Reputation



The following table describes the labels in this screen.

Table 180 Security Service > Reputation Filter > IP Reputation

LABEL	DESCRIPTION
IP Blocking	
Enable	Select this option to turn on IP blocking on the Zyxel Device. Otherwise, clear it.
Action	Set what action the Zyxel Device takes when packets come from or go to an IPv4 address with bad reputation. **pass**: Select this action to have the Zyxel Device allow the packet to go through. **block**: Select this action to have the Zyxel Device deny the packets and send a TCP RST to both the sender and receiver when a packet comes from an IPv4 address with bad reputation.

Table 180 Security Service > Reputation Filter > IP Reputation (continued)

LABEL	DESCRIPTION
Threat Level Threshold	Select the threshold threat level to which the Zyxel Device will take action (**high**, **medium and above**, **Low and above**). The threat level is determined by the IP reputation engine. It grades IPv4 addresses. • **high**: An IPv4 address that scores 0 to 20 points. • **medium and above**: An IPv4 address that scores 0-60 points. • **Low and above**: An IPv4 address that scores 0-80 points.
Log	These are the log options: **no**: Do not create a log when the packet comes from or goes to an IPv4 address with bad reputation. **log**: Create a log on the Zyxel Device when the packet comes from or goes to an IPv4 address with bad reputation. **log alert**: An alert is an emailed log for more serious events that may need more immediate attention. Select this option to have the Zyxel Device send an alert when the packet comes from or goes to an IPv4 address with bad reputation.
Statistics	Enable to have the Zyxel Device collect IP reputation statistics. All of the statistics are erased if you restart the Zyxel Device or click **Flush Data** in **Security Statistics** > **Reputation Filter** > **IP Reputation**.
Types of Cyber Threats Coming From The Internet	Select the categories of packets that come from or go to the Internet and are known to pose a security threat to users or their computers.
Anonymous Proxies	These are sites and proxies that act as an intermediary for surfing to other websites in an anonymous fashion, whether to circumvent Web filtering or for other reasons.
Denial of Service	These are sites that issue Denial of Service (DoS) attacks, such as DoS, DDoS, SYN flood, and anomalous traffic detection. DoS attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The goal of DoS attacks is not to steal information, but to disable a device or network on the Internet. A Distributed Denial of Service (DDoS) attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system. SYN flood is an attack that attackers flood SYN packets to a server in TCP handshakes, and not respond with ACK packets on purpose. This keeps the server waiting for attackers' responses to establish TCP connections, and make the server unavailable. Anomalous traffic detection could be malicious activities, such as malware outbreaks or hacking attempts.
Exploits	These are sites that distribute exploits or exploit kits to infect website visitors' devices. Exploits include shellcode, root kits, worms, or viruses that download additional malware to infect devices. An exploit kit consists of different exploits.
Negative Reputation	These are sites that have bad reputation and associate with suspicious activities, such as spam, virus, and/or phishing.
Scanners	These are sites that run unauthorized system vulnerabilities scan to look for vulnerabilities in website visitors' devices.
Spam Sources	These are sites that have been promoted through spam techniques.

Table 180 Security Service > Reputation Filter > IP Reputation (continued)

LABEL	DESCRIPTION
TOR Proxies	These are sites that act as the exit nodes in a Tor (The Onion Router) network. Tor is a service that keep users anonymous in the Internet and make users' Internet activities untraceable. Tor hides user's real IP addresses by encrypting data and transmitting the encrypted data in a chain of selected nodes acting as intermediaries. Each node can only decrypt the data sent from the node before it. The first node that receives the encrypted data is called the entry node. The last node is the last intermediary that the encrypted data will go through before it arrives at the destination.
Web Attacks	These are sites that launch web attacks, such as SQL injection, cross site scripting, iframe injection, and brute force attack. SQL injection (SQLI) is an attack that attackers insert malicious SQL (Structured Query Language) code into a web application database query. Attackers can then access, add, modify, or delete data in users' databases. Cross site scripting (XSS) is an attack that attackers injects malicious scripts to websites or web applications in the form of HTML or JavaScript code. The scripts execute when users visit the infected web page or perform the infected web applications. XSS will cause failures to encrypt traffic, cookie stealing, identity impersonation, and phishing. Iframe injection is an attack that attackers injects malicious iframe (inline frame) tags to websites. The malicious iframe tag downloads malware to the devices of the infected websites' visitors, and steal users' sensitive information. An iframe tag is an HTML tag that is used to embed contents from another source in a website, but attackers misuse this feature. Brute force attack is an attack that attackers attempt to gain access to websites or device via a succession of different passwords.
Phishing	These are sites that are used for deceptive or fraudulent purposes (e.g. phishing), such as stealing financial or other user account information. These sites are most often designed to appear as legitimate sites in order to mislead users into entering their credentials.
Types of Cyber Threats Coming From The Internet And Local Networks	These are packets that come from or go to the Internet and local networks and are known to pose a security threat to users or their computers.
Botnets	A botnet is a network consisting of computers that are infected with malware and remotely controlled. The infected computers will contact and wait for instructions from a command and control (C&C) server. An attacker can control the botnet by setting up a C&C server and then sending commands to the infected computers. Alternatively, a peer-to-peer network approach is used. The infected computer scans and communicates with the peer devices in the same botnet to share commands or malware sent by the C&C server. These are botnet sites including command-and-control (C&C) servers.
Test IP Threat Category	
IP to test	Enter an IPv4 address of a website, and click the **Query** button to check if the website associates with suspicious activities that could pose a security threat to users or their computers.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

21.2.1 IP Reputation Allow List

Use this to create allow list entries. The Zyxel Device will allow packets coming from the Internet and going out from the local network that match the listed IPv4 addresses.

Click **Security Service > Reputation Filter > IP Reputation (Allow List)** to display the configuration screen as shown next.

Figure 242 Security Service > Reputation Filter > IP Reputation (Allow List)



The following table describes the labels in this part of the screen.

Table 181 Security Services > Reputation Filter > IP Reputation (Allow List)

LABEL	DESCRIPTION
Enable	Select this to bypass checking by this feature (if enabled) and automatically allow: • incoming packets that come from the listed IPv4 addresses. • outgoing packets that go to the listed IPv4 addresses.
Log	Select **log** if you want the Zyxel Device to create a log recording when there are incoming or outgoing packets that come from or go to the listed IPv4 addresses. Select **no** if you don't want the Zyxel Device to create a log.
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.
Active	To turn on an entry, select it and click **Active**.
Inactive	To turn off an entry, select it and click **Inactive**.
Status	The status (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
IPv4 Address	Enter an IPv4 address that will bypass IP Reputation filtering.
Description	Enter a description for this profile.
Edit	Select an entry and click this icon to modify it.
Remove	Select an entry and click this icon to delete it.
Save Changes	Click this icon to save the changes in this row.
Cancel Changes	Click this icon to cancel the changes in this row.

21.2.2 IP Reputation Block List

Use this to create block list entries. The Zyxel Device will block packets coming from the Internet and going out from the local network that match the listed IPv4 addresses.

Click **Security Service > Reputation Filter > IP Reputation (Block List)** to display the configuration screen as shown next.

Figure 243 Security Service > Reputation Filter > IP Reputation (Block List)



The following table describes the labels in this part of the screen.

Table 182 Security Services > Reputation Filter > IP Reputation (Block List)

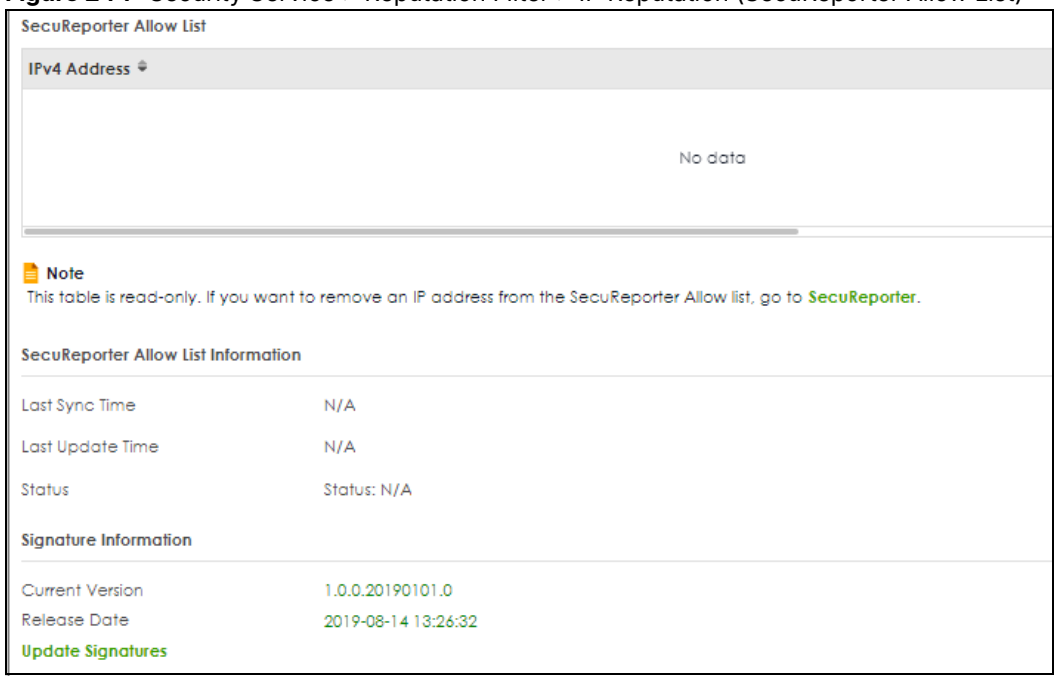
LABEL	DESCRIPTION
Enable	Select this to bypass checking by this feature (if enabled) and automatically block: • incoming packets coming from the listed IPv4 addresses. • outgoing packets going to the listed IPv4 addresses.
Log	Select **log** if you want the Zyxel Device to create a log recording when there are incoming or outgoing packets that come from or go to the listed IPv4 addresses. Select **no** if you don't want the Zyxel Device to create a log.
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.
Active	To turn on an entry, select it and click **Active**.
Inactive	To turn off an entry, select it and click **Inactive**.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
IPv4 Address	Enter an IPv4 address that will be blocked without processing IP Reputation filtering.
Description	Enter a description for this profile.
Edit	Select an entry and click this icon to modify it.
Remove	Select an entry and click this icon to delete it.
Save Changes	Click this icon to save the changes in this row.
Cancel Changes	Click this icon to cancel the changes in this row.

21.2.3 IP Reputation SecuReporter Allow List

Use this to view SecuReporter allow list entries. To remove an items from this list, you must go to SecuReporter. The Zyxel Device will allow packets coming from the Internet and going out from the local network that match the listed IPv4 addresses.

Click **Security Service > Reputation Filter > IP Reputation (SecuReporter Allow List)** to display the configuration screen as shown next.

Figure 244 Security Service > Reputation Filter > IP Reputation (SecuReporter Allow List)



The following table describes the labels in this screen.

Table 183 Security Services > Reputation Filter > IP Reputation (SecuReporter Allow List)

LABEL	DESCRIPTION
IPv4 Address	This read-only table displays the SecuReporter allow list entries.
SecuReporter Allow List Information	The Zyxel Device synchronizes with SecuReporter periodically (every 10 minutes at the time of writing).
Last Sync Time	This field displays the date and time the Zyxel Device last checked for new SecuReporter allow list entries.
Last Update Time	This field displays the date and time the Zyxel Device last updated SecuReporter allow list entries.
Status	This field displays the status of SecuReporter allow list entries: **Success**, **Parse message error**, **HTTP error**, **Connection timeout** and **Error**. If an error is received, make sure the Zyxel Device has Internet access and can connect to the SecuReporter portal.
Signature Information	The following fields display information on the current signature set that the Zyxel Device is using.
Current Version	This field displays the IP Reputation signature set version number. This number gets larger as the set is enhanced.
Release Date	This field displays the date and time the set was released.
Update Signatures	Click this link to go to the screen you can use to download signatures from the update server.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

21.3 DNS Threat Filter Screen

A Domain Name System (DNS) server records mappings of FQDN (Fully Qualified Domain Names) to IP addresses. A 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.

DNS threat filtering inspects DNS queries made by clients on your network and compares the queries against a database of blocked or allowed Fully Qualified Domain Names (FQDNs).

If a user attempts to connect to a suspect site, where the DNS query packet contains an FQDN with a bad reputation, then a DSN query is sent from the user’s computer and detected by the DNS Threat Filter.

The Zyxel Device DNS Threat Filter will either drop the DNS query or reply to the user with a fake DNS response using the default *dnsft.cloud.zyxel.com* IP address (where the user will see a “Web Page Blocked!” page) or a custom IP address.

The following types of DNS queries are allowed by the Zyxel Device:

- Type “A” for IPv4 addresses

The Zyxel Device replies with a DNS server error for the following types of DNS queries:

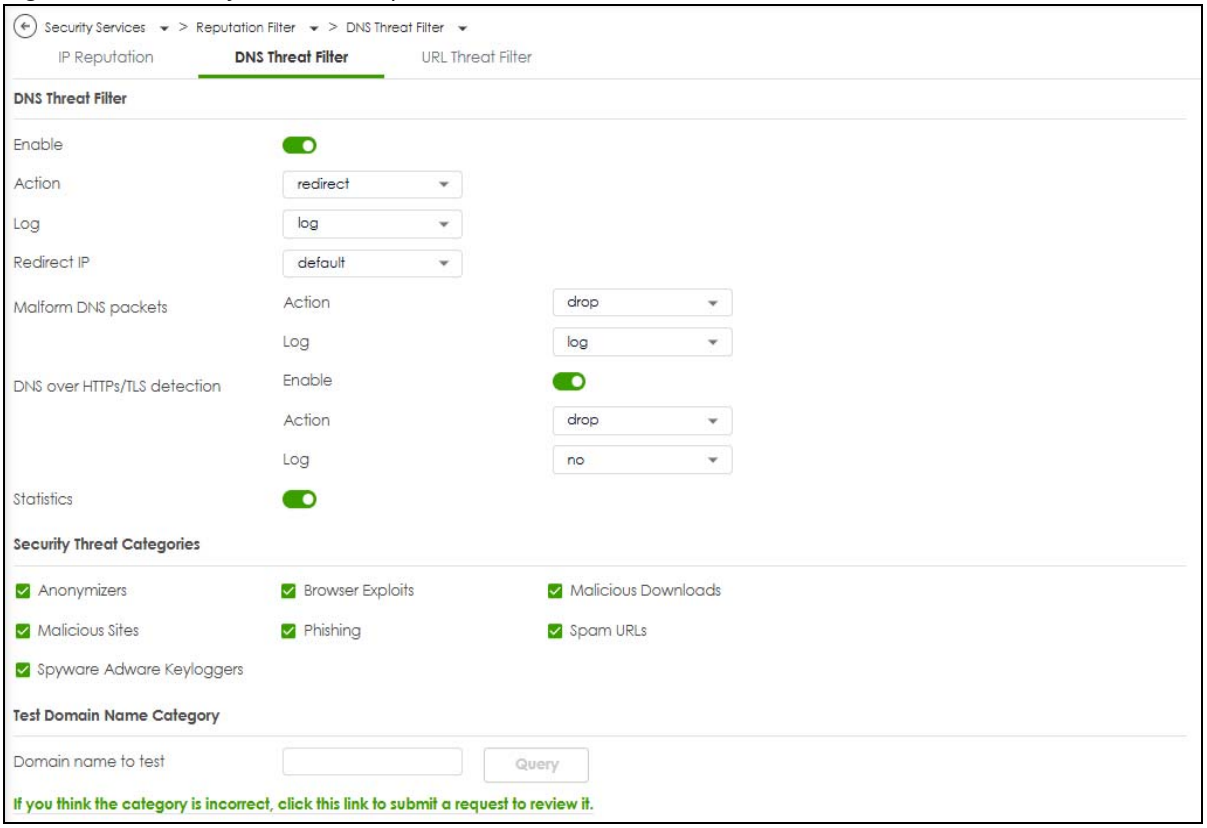
- Type “NS” (Name Server) to get information about the authoritative name server
- Type “MX” (Mail eXchange) to request information about the mail exchange server for a specific DNS domain name.
- Type “CNAME” (Canonical Names) that specifies a domain name that has to be queried in order to resolve the original DNS query
- Type “PTR” (Pointer) that specifies a reverse query (requesting the FQDN corresponding to the IP address you provided)
- Type “SOA” (Start Of zone Authority) used when transferring zones

The priority for DNS Threat Filter checking is as follows:

1. Allow List
2. SecuReporter Allow List
3. Block List
4. External Block List
5. Cloud Query Cache
6. Cloud Query

Click **Security Service > Reputation Filter > DNS Threat Filter** to display the configuration screen as shown next.

Figure 245 Security Service > Reputation Filter > DNS Threat Filter



The following table describes the labels in this screen.

Table 184 Security Service > Reputation Filter > DNS Threat Filter

LABEL	DESCRIPTION
DNS Threat Filter	
Enable	Select this option to turn on DNS threat filtering on the Zyxel Device. Otherwise, clear it. **Action** and **Log** settings apply to DNS query packets triggered by the security threat categories.
Action	Set what action the Zyxel Device takes when there is a DNS query packet containing an FQDN with a bad reputation. **redirect**: Select this action to have the Zyxel Device reply with a DNS reply packet containing a default or custom-defined IP address. **pass**: Select this action to have the Zyxel Device allow the DNS query packet and not reply with a DNS reply packet containing a default or custom-defined IP address.
Log	These are the log options: **no**: Do not create a log when there is a DNS query packet containing an FQDN with a bad reputation. **log**: Create a log on the Zyxel Device when there is a DNS query packet containing an FQDN with a bad reputation. **log alert**: An alert is an emailed log for more serious events that may need more immediate attention. Select this to have the Zyxel Device send an alert when there is a DNS query packet containing an FQDN with a bad reputation.

Table 184 Security Service > Reputation Filter > DNS Threat Filter (continued)

LABEL	DESCRIPTION
Redirect IP	Select this action to have the Zyxel Device reply with a DNS reply packet containing a default or custom-defined IP address when a DNS query packet contains an FQDN with a bad reputation. The default IP is the *dnsft.cloud.zyxel.com* IP address. If you select **custom-defined IP**, then enter a valid IPv4 address in the text box.
Malform DNS packets	Set what action the Zyxel Device takes when there is an abnormal DNS query packet. A DNS packet is defined as malformed when: • The number of entries in the question count field in the DNS header is 0 • An error occurs when parsing the domain name in the question field • The length of the domain name exceeds 255 characters. **pass**: Select this action to have the Zyxel Device allow the DNS query packet through the Zyxel Device. **drop**: Select this action to have the Zyxel Device discard the abnormal DNS query packet Select **log** to create a log on the Zyxel Device when there is an abnormal DNS query packet.
DNS over HTTPs/TLS detection	Set what action the Zyxel Device takes when there is an encrypted DNS query packet. An encrypted DNS query packet might endanger your network because the Zyxel Device cannot inspect it to check if a user on your network tries to access a suspect site. **pass**: Select this action to have the Zyxel Device allow the encrypted DNS query packet through the Zyxel Device. **drop**: Select this action to have the Zyxel Device discard the encrypted DNS query packet. Select **log** to create a log on the Zyxel Device when there is an encrypted DNS query packet.
Statistics	Enable to have the Zyxel Device collect DNS threat filter statistics. All of the statistics are erased if you restart the Zyxel Device or click **Flush Data** in **Security Statistics** > **Reputation Filter** > **DNS Threat Filter**.
Security Threat Categories	Select the categories of FQDNs that may pose a security threat to network devices behind the Zyxel Device.
Anonymizers	Sites and proxies that act as an intermediary for surfing to other Web sites in an anonymous fashion, whether to circumvent Web filtering or for other reasons.
Browser Exploits	Sites that contain browser exploits. A browser exploit is any content that forces a web browser to perform operations that you do not explicitly intend.
Malicious Downloads	Sites that have been identified as containing malicious downloads or malware harmful to a user's computer.
Malicious Sites	Sites that install unwanted software on a user's computer with the intent to enable third-party monitoring or make system changes without the user's consent.
Phishing	Sites that are used for deceptive or fraudulent purposes, such as stealing financial or other user account information. These sites are most often designed to appear as legitimate sites in order to mislead users into entering their credentials.
Spam URLs	Sites that have been promoted through spam techniques.
Spyware Adware Keyloggers	Sites that contain spyware, adware or keyloggers. • Spyware is a program installed on your computer, usually without your explicit knowledge, that captures and transmits personal information or Internet browsing habits and details to companies. Companies use this information to analyze browsing habits, to gather marketing data, and to sell your information to others. • Key logger programs try to capture and steal your passwords and watch and record everything you do on your computer. • Adware programs typically display blinking advertisements or pop-up windows when you perform a certain action. Adware programs are often installed in exchange for another service, such as the right to use a program without paying for it.
Test Domain Name Category	
Domain name to test	Enter an FQDN and click the **Query** button to check if the domain name is associated with suspicious activities that could pose a security threat to users or their computers.

Table 184 Security Service > Reputation Filter > DNS Threat Filter (continued)

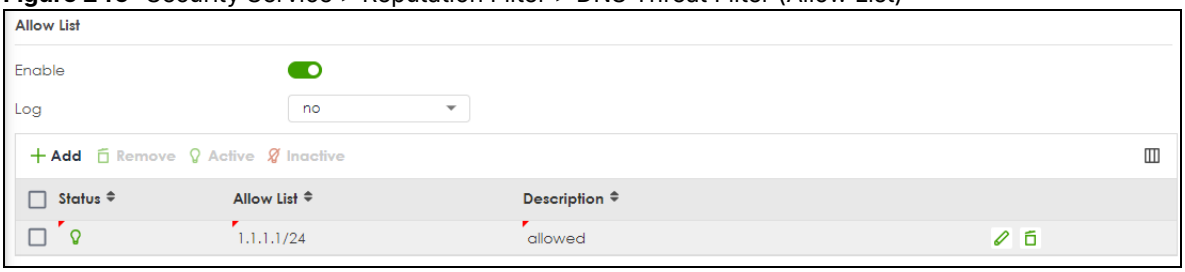
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to return the screen to its last-saved settings.

21.3.1 DNS Threat Filter Allow List

Use this to create allow list entries. The Zyxel Device will not reply with a DNS reply packet containing a default or custom-defined IP address when a DNS query packet contains an FQDN in the allow list.

Click **Security Service > Reputation Filter > DNS Threat Filter (Allow List)** to display the configuration screen as shown next.

Figure 246 Security Service > Reputation Filter > DNS Threat Filter (Allow List)



The following table describes the labels in this screen.

Table 185 Security Service > Reputation Filter > DNS Threat Filter (Allow List)

LABEL	DESCRIPTION
Enable	Select this check box and the Zyxel Device will not reply with a DNS reply packet containing a default or custom-defined IP address when a DNS query packet contains an FQDN in the white list.
Add	Click this to create a new entry. To add an FQDN, type a Fully-Qualified Domain Name (FQDN) of a web site. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the third-level domain, “com” is the second-level domain, and “tw” is the top level domain. Underscores are not allowed. Use "*." as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Active	To turn on an entry, select it and click **Active**.
Inactive	To turn off an entry, select it and click **Inactive**.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Allow List	Enter an IP address (with CIDR or a range) or a domain name (wildcard permitted) that will be allowed without DNS Threat filtering.
Description	Enter a description for this profile.
Edit	Select an entry and click this icon to modify it.
Remove	Select an entry and click this icon to delete it.

Table 185 Security Service > Reputation Filter > DNS Threat Filter (Allow List) (continued)

LABEL	DESCRIPTION
Save Changes	Click this icon to save the changes in this row.
Cancel Changes	Click this icon to cancel the changes in this row.

21.3.2 DNS Threat Filter Block List

Use this to create block list entries. The Zyxel Device will reply with a DNS reply packet containing a default or custom-defined IP address when a DNS query packet contains an FQDN in the block list. For matched items in the block list, the action is always **Redirect IP** and log is always **log alert.**

Click **Security Service > Reputation Filter > DNS Threat Filter (Block List)** to display the configuration screen as shown next.

Figure 247 Security Service > Reputation Filter > DNS Threat Filter (Block List)



The following table describes the labels in this screen.

Table 186 Security Service > Reputation Filter > DNS Threat Filter (Block List)

LABEL	DESCRIPTION
Block List	
Enable	Select this check box and the Zyxel Device will reply with a DNS reply packet containing a default or custom-defined IP address when a DNS query packet contains an FQDN in the black list.
Add	Click this to create a new entry. To add an FQDN, type a Fully-Qualified Domain Name (FQDN) of a web site. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the third-level domain, “com” is the second-level domain, and “tw” is the top level domain. Underscores are not allowed. Use "*." as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Active	To turn on an entry, select it and click **Active**.
Inactive	To turn off an entry, select it and click **Inactive**.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Block List	Enter an IP address (with CIDR or a range) or a domain name (wildcard permitted) that will be blocked without DNS Threat filtering.
Description	Enter a description for this profile.

Table 186 Security Service > Reputation Filter > DNS Threat Filter (Block List) (continued)

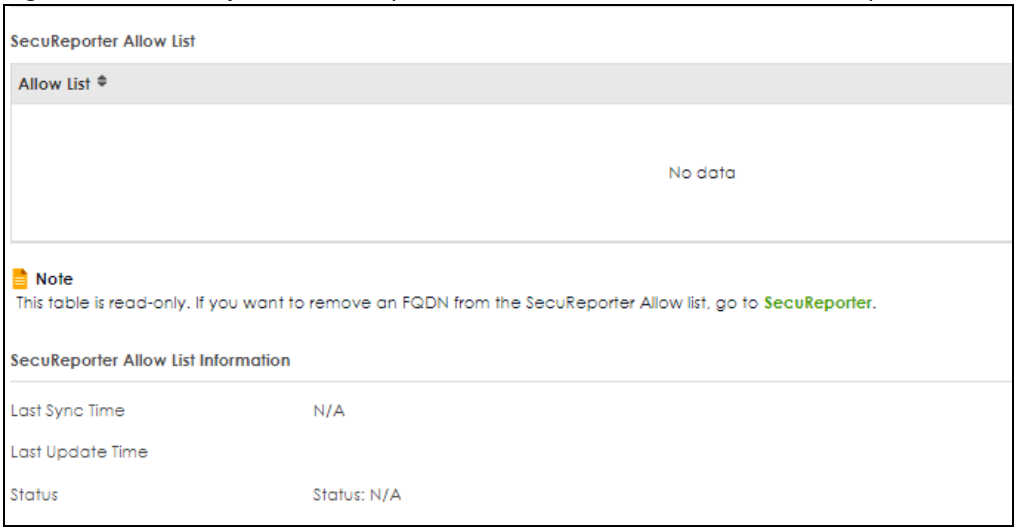
LABEL	DESCRIPTION
Edit	Select an entry and click this icon to modify it.
Remove	Select an entry and click this icon to delete it.
Save Changes	Click this icon to save the changes in this row.
Cancel Changes	Click this icon to cancel the changes in this row.

21.3.3 DNS Threat Filter SecuReporter Allow List

Use this to view SecuReporter allow list entries. To remove an items from this list, you must go to SecuReporter. The Zyxel Device will not reply with a DNS reply packet containing a default or custom-defined IP address when a DNS query packet contains an FQDN in the allow list.

Click **Security Service > Reputation Filter > DNS Threat Filter_SecuReporter Allow List** to display the configuration screen as shown next.

Figure 248 Security Service > Reputation Filter > DNS Threat Filter_SecuReporter Allow List



The following table describes the labels in this screen.

Table 187 Security Services > Reputation Filter > DNS Threat Filter_SecuReporter Allow List

LABEL	DESCRIPTION
Allow List	This read-only table displays the SecuReporter allow list entries.
SecuReporter Allow List Information	
Last Sync Time	This field displays the date and time the Zyxel Device last checked for new SecuReporter allow list entries.
Last Update Time	This field displays the date and time the Zyxel Device last updated SecuReporter allow list entries.

Table 187 Security Services > Reputation Filter > DNS Threat Filter_SecuReporter Allow List (continued)

LABEL	DESCRIPTION
Status	This field displays the status of SecuReporter allow list entries: **Success**, **Parse message error**, **HTTP error**, **Connection timeout** and **Error**. If an error is received, make sure the Zyxel Device has Internet access and can connect to the SecuReporter portal.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

21.4 URL Threat Filter Screen

The Zyxel Device will access the Cloud Query database, that has millions of web sites categorized based on content. You can have the Zyxel Device allow, block, warn and/or log access to web sites or hosts based on these categories.

The priority for URL Threat checking is as follows:

1 Allow List

2 SecuReporter Allow List

3 Block List

4 External Block List

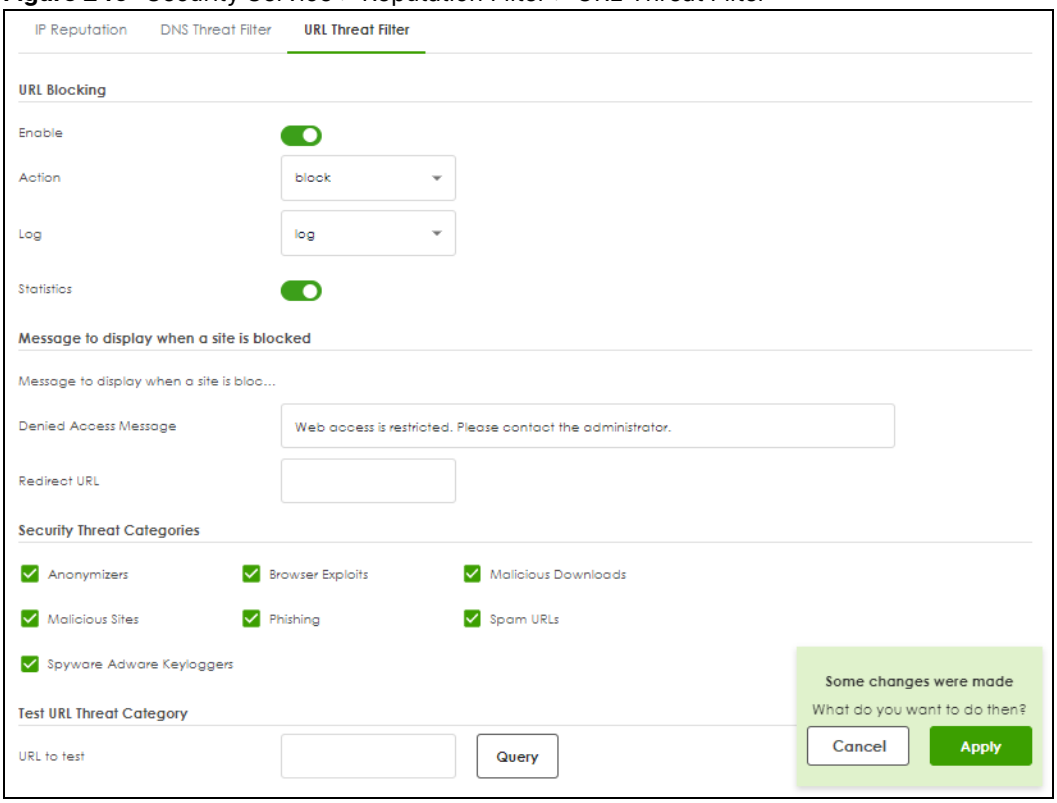
5 Cloud Query Cache

6 Cloud Query

Use this screen to enable URL Threat filtering and specify the action the Zyxel Device takes when it detects a suspicious activity or a connection attempt to or from a site in a selected category.

Click **Security Service > Reputation Filter > URL Threat Filter** to display the configuration screen as shown next.

Figure 249 Security Service > Reputation Filter > URL Threat Filter



The following table describes the labels in this screen.

Table 188 Security Service > Reputation Filter > URL Threat Filter

LABEL	DESCRIPTION
URL Blocking	
Enable	Select this option to turn on URL blocking on the Zyxel Device.
Action	Set what action the Zyxel Device takes when it detects a connection attempt to or from the web pages of the specified categories. **block**: Select this action to have the Zyxel Device block access to the web pages that match the categories that you select above. **pass**: Select this action to have the Zyxel Device allow access to the web pages that match the categories that you select above.
Log	These are the log options: • **no**: Do not create a log when it detects a connection attempt to or from the web pages of the specified categories. • **log**: Create a log on the Zyxel Device when it detects a connection attempt to or from the web pages of the specified categories. • **log alert:** An alert is an emailed log for more serious events that may need more immediate attention. Select this option to have the Zyxel Device send an alert when a connection matches web pages of the specified categories.
Statistics	Enable to have the Zyxel Device collect URL threat filter statistics. All of the statistics are erased if you restart the Zyxel Device or click **Flush Data** in **Security Statistics** > **Reputation Filter** > **URL Threat Filter**.
Message to display when a site is blocked	
Denied Access Message	Enter a message to be displayed when the URL Threat filter blocks access to a web page. Use up to 127 characters [0-9a-zA-Z;/?:@&=+$\.-_!~*'()%,"]. For example, "Web access is restricted. Please contact the administrator". This field cannot be blank.

Table 188 Security Service > Reputation Filter > URL Threat Filter (continued)

LABEL	DESCRIPTION
Redirect URL	Enter the URL of the web page to which you want to send users when their web access is blocked by the URL Threat 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.
Security Threat Categories	Select the categories of web pages that may pose a security threat to network devices behind the Zyxel Device.
Anonymizers	Sites and proxies that act as an intermediary for surfing to other Web sites in an anonymous fashion, whether to circumvent Web filtering or for other reasons.
Browser Exploits	Sites that contain browser exploits. A browser exploit is any content that forces a web browser to perform operations that you do not explicitly intend.
Malicious Downloads	Sites that have been identified as containing malicious downloads or malware harmful to a user's computer.
Malicious Sites	Sites that install unwanted software on a user's computer with the intent to enable third-party monitoring or make system changes without the user's consent.
Phishing	Sites that are used for deceptive or fraudulent purposes, such as stealing financial or other user account information. These sites are most often designed to appear as legitimate sites in order to mislead users into entering their credentials.
Spam URLs	Sites that have been promoted through spam techniques.
Spyware Adware Keyloggers	Sites that contain spyware, adware or keyloggers. • Spyware is a program installed on your computer, usually without your explicit knowledge, that captures and transmits personal information or Internet browsing habits and details to companies. Companies use this information to analyze browsing habits, to gather marketing data, and to sell your information to others. • Key logger programs try to capture and steal your passwords and watch and record everything you do on your computer. • Adware programs typically display blinking advertisements or pop-up windows when you perform a certain action. Adware programs are often installed in exchange for another service, such as the right to use a program without paying for it.
Test URL Threat Category	
URL to test	Enter a URL using http://domain or https://domain and click the **Query** button to check if the domain belongs to a URL threat category.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

21.4.1 URL Threat Filter Allow List

Use this to create allow list entries. The Zyxel Device will allow incoming packets from the listed IPv4 addresses and URLs.

Click **Security Service > Reputation Filter > URL Threat Filter (Allow List)** to display the configuration screen as shown next.

Figure 250 Security Service > Reputation Filter > URL Threat Filter (Allow List)



The following table describes the labels in this screen.

Table 189 Security Service > Reputation Filter > URL Threat Filter (Allow List)

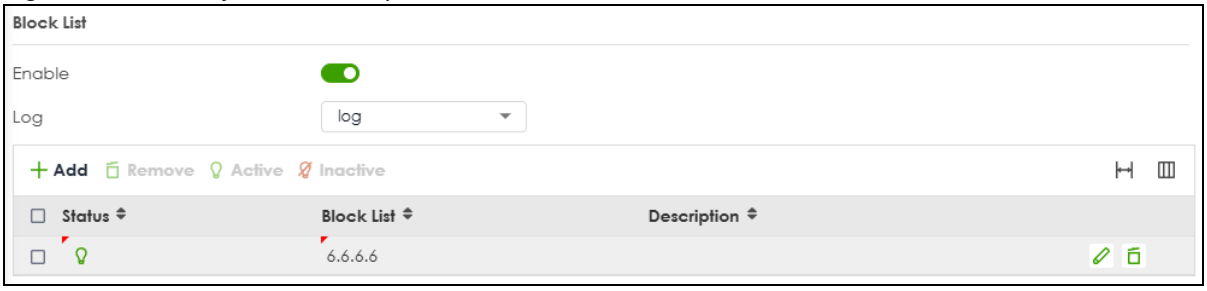
LABEL	DESCRIPTION
Enable	Select this to bypass checking by this feature (if enabled) and automatically allow packets from the listed IPv4 addresses and URLs.
Log	These are the log options: • **no**: Do not create a log when the Zyxel Device detects a connection attempt to or from the web pages of the specified categories listed in the allow list. • **log**: Create a log on the Zyxel Device when it detects a connection attempt to or from the web pages of the specified categories listed in the allow list.
Add	Click this to create a new entry.
Remove	Select an entry and click this to delete it.
Active	To turn on an entry, select it and click **Active**.
Inactive	To turn off an entry, select it and click **Inactive**.
Status	The status (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Allow List	Enter an IP address (with CIDR or a range) or a domain name (wildcard permitted) that will be allowed without URL Threat filtering.
Description	Enter a description for this profile.
Edit	Select an entry and click this icon to modify it.
Remove	Select an entry and click this icon to delete it.
Save Changes	Click this icon to save the changes in this row.
Cancel Changes	Click this icon to cancel the changes in this row.

21.4.2 URL Threat Filter Block List

Use this to create block list entries. The Zyxel Device will block incoming packets from the listed URLs.

Click **Security Service > Reputation Filter > URL Threat Filter (Block List)** to display the configuration screen as shown next.

Figure 251 Security Service > Reputation Filter > URL Threat Filter (Block List)



The following table describes the labels in this screen.

Table 190 Security Service > Reputation Filter > URL Threat Filter (Block List)

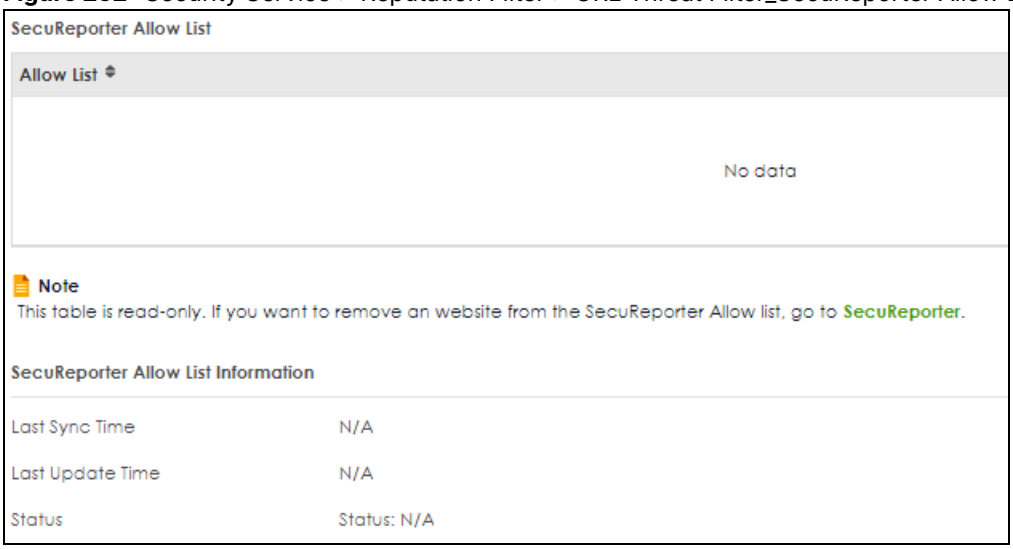
LABEL	DESCRIPTION
Enable	Select this to bypass checking by this feature (if enabled) and automatically block packets from the listed IPv4 addresses and URLs.
Log	These are the log options: • **no**: Do not create a log when it detects a connection attempt to or from the web pages of the specified categories listed in the block list. • **log**: Create a log on the Zyxel Device when it detects a connection attempt to or from the web pages of the specified categories listed in the block list. • **log alert:** An alert is an emailed log for more serious events that may need more immediate attention. Select this option to have the Zyxel Device send an alert when a connection matches web pages of the specified categories listed in the block list.
Add	Click this to create a new entry.
Active	To turn on an entry, select it and click **Active**. The **Status** light changes accordingly.
Inactive	To turn off an entry, select it and click **Inactive**. The **Status** light changes accordingly.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Remove	Select an entry and click this to delete it.
Block List	Enter an IP address (with CIDR or a range) or a domain name (wildcard permitted) that will be blocked without URL Threat filtering.
Description	Enter a description for this profile.
Edit	Select an entry and click this icon to modify it.
Remove	Select an entry and click this icon to delete it.
Save Changes	Click this icon to save the changes in this row.
Cancel Changes	Click this icon to cancel the changes in this row.

21.4.3 URL Threat Filter SecuReporter Allow List

Use this to view SecuReporter allow list entries. To remove an items from this list, you must go to SecuReporter. The Zyxel Device will allow packets coming from the Internet and going out from the local network that match the listed URLs.

Click **Security Service > Reputation Filter > URL Threat Filter.** Go to the **SecuReporter Allow List** section as shown next.

Figure 252 Security Service > Reputation Filter > URL Threat Filter_SecuReporter Allow List



The following table describes the labels in this screen.

Table 191 Security Services > Reputation Filter > URL Threat Filter_SecuReporter Allow List

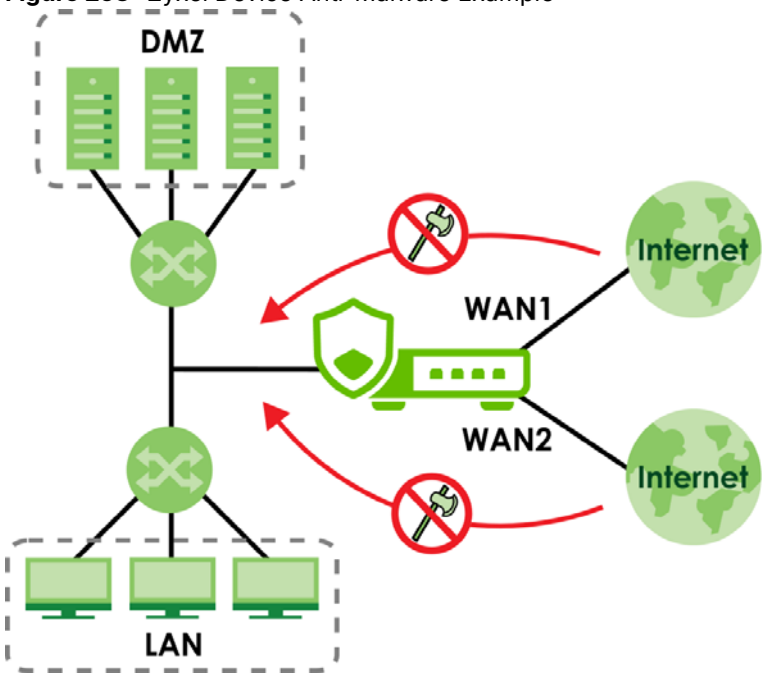
LABEL	DESCRIPTION
Allow List	This read-only table displays the SecuReporter allow list entries.
SecuReporter Allow List Information	
Last Sync Time	This field displays the date and time the Zyxel Device last checked for new SecuReporter allow list entries.
Last Update Time	This field displays the date and time the Zyxel Device last updated SecuReporter allow list entries.
Status	This field displays the status of SecuReporter allow list entries: **Success**, **Parse message error**, **HTTP error**, **Connection timeout** and **Error**. If an error is received, make sure the Zyxel Device has Internet access and can connect to the SecuReporter portal.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

CHAPTER 22
Anti-Malware

22.1 Overview

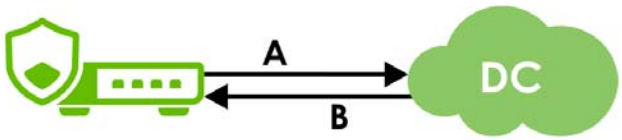
Malware is short for malicious software, such as computer viruses, worms and spyware. The Zyxel Device anti-malware feature protects your connected network from malware by scanning traffic coming in from the WAN and going out from the WAN. The traffic scanned by the Zyxel Device may include FTP traffic and email with attachments.

Figure 253 Zyxel Device Anti-Malware Example



The Zyxel Device queries the **Defend Center** database by sending the file's has value (**A**) and receiving the scan results (**B**) through the Defend Center (**DC**).

Figure 254 Cloud Query



Viruses, Worms, and Spyware

A computer virus is a type of malicious software designed to corrupt and/or alter the operation of other legitimate programs. A worm is a self-replicating virus. Spyware infiltrates your device to secretly gather information, such as your network activity, passwords, bank details, and so on.

The following describes a simple life cycle of malware.

1. A computer gets a copy of malware from a source such as the Internet, email, file sharing or any removable storage media. The malware is harmless until the execution of an infected program.
2. The malware spreads to other files and programs on the computer.
3. The infected files are unintentionally sent to another computer thus starting the spread of the malware.
4. Once the malware is spread through the network, the number of infected networked computers can grow exponentially.

Types of Malware

The following table describes some of the common malware.

Table 192 Common Malware Types

TYPE	DESCRIPTION
File Infector	This is a small program that embeds itself in a legitimate program. A file infector is able to copy and attach itself to other programs that are executed on an infected computer.
Boot Sector Virus	This type of virus infects the area of a hard drive that a computer reads and executes during startup. The virus causes computer crashes and to some extend renders the infected computer inoperable.
Macro Virus	Macro viruses or Macros are small programs that are created to perform repetitive actions. Macros run automatically when a file to which they are attached is opened. Macros spread more rapidly than other types of viruses as data files are often shared on a network.
Email Virus	Email viruses are malicious programs that spread through email.
Polymorphic Virus	A polymorphic virus (also known as a mutation virus) tries to evade detection by changing a portion of its code structure after each execution or self replication. This makes it harder for an anti-malware scanner to detect or intercept it. A polymorphic virus can also belong to any of the virus types discussed above.

Hash Value

A hash function is an algorithm that maps data of arbitrary size to data of fixed size. The value returned by a hash function is a hash value. Hash values can be used to identify if the contents of a file have changed. At the time of writing, the MD5 (Message Digest 5) and SHA-256 (Secure Hash Algorithm) hash algorithms are supported.

Anti-Malware Scan Process

Before going through the Anti-Malware scan, the Zyxel Device first identifies the packets sent by the following four major protocols with corresponding standard ports:

- FTP (File Transfer Protocol)

- HTTP (Hyper Text Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- POP3 (Post Office Protocol version 3)

The Zyxel Device records the orders of packets in TCP connection-oriented sessions to check for matching malware signatures. The order of non-setup packets such as SYN, ACK and FIN is ignored.

Anti-Malware Scanning Procedure:

1 The Zyxel Device uses **Cloud Query** to forward the file's hash value to Defend Center.

2 If the hash value is incorrect, then the last packet of the file is removed. The file is still forwarded to the receiver, but they will not be able to open it. You can configure to receive an alert or log when this happens.

Note: The receiver is not notified if a file is modified by the Zyxel Device. If the file cannot be used, the receiver should contact the Zyxel Device administrator to confirm if the Zyxel Device modified the file by checking the logs.

File Scanning Cloud Query Supported File Types

At the time of writing, the following file types are supported:

Table 193 File Scanning Cloud Query Supported File Types

• 7z Archive (7z)	• AVI Video (avi)	• BMP Image (bmp)	• BZ2 Archive (bz2)
• Executables (exe)	• Macromedia Flash Data (swf)	• GIF Image (gif)	• GZ Archive (gz)
• JPG Image (jpg)	• MOV Video (mov)	• MP3 Audio (mp3)	• MPG Video (mpg)
• MS Office Document (doc...)	• PDF Document (pdf)	• PNG Image (png)	• RAR Archive (rar)
• RM Video (rm)	• RTF Document (rtf)	• TIFF Image (tif)	• WAV Audio (wav)
• ZIP Archive (zip)			

Notes About the Zyxel Device Anti-Malware

The following lists important notes about the Zyxel Device's anti-malware feature:

1 Zyxel's anti-malware feature can detect polymorphic malware (see Section 22.1 on page 411).

2 When malware is detected in a file, the file is blocked and a log is created or an alert message is sent to the administrator depending on your log settings.

3 Changes to the Zyxel Device's anti-malware settings only affect new sessions, not sessions that already existed before you applied the changed settings.

4 Enabling **Cloud Query** may affect file transfer speeds.

5 The Zyxel Device does not scan the following file/traffic types:

- Simultaneous downloads of a file using multiple connections. For example, when you use FlashGet to download sections of a file simultaneously.
- Encrypted traffic. This could be password-protected files or VPN traffic where the Zyxel Device is not the endpoint (pass-through VPN traffic).
- Traffic through custom (non-standard) ports. The Zyxel Device scans whatever port number is specified for FTP in the ALG screen.

Finding Out More

- See Section 22.5 on page 420 for anti-malware background information.

22.1.1 What You Can Do in this Chapter

- Use the **Anti-Malware** screen (Section 22.2 on page 414) to turn anti-malware on or off. In addition, you can set up anti-malware blocked and allowed lists to bypass anti-malware checking.
- Use the **Allow List** screen (Section 22.3 on page 416) to specify the file or encryption pattern to allow in order to avoid false positives.
- Use the **Block List** screen (Section 22.4 on page 418) to specify the file or encryption pattern that you want to block.

22.2 Anti-Malware Screen

Click **Security Service** > **Anti-Malware** to display the configuration screen as shown next.

If a license has expired, you will see a reminder in this screen. You need to renew the license in order to keep using the feature. Click **Buy Now** to go to Marketplace to purchase a new license. Click **See Details** to go to the Zyxel web page to find more information on licenses for your Zyxel Device.



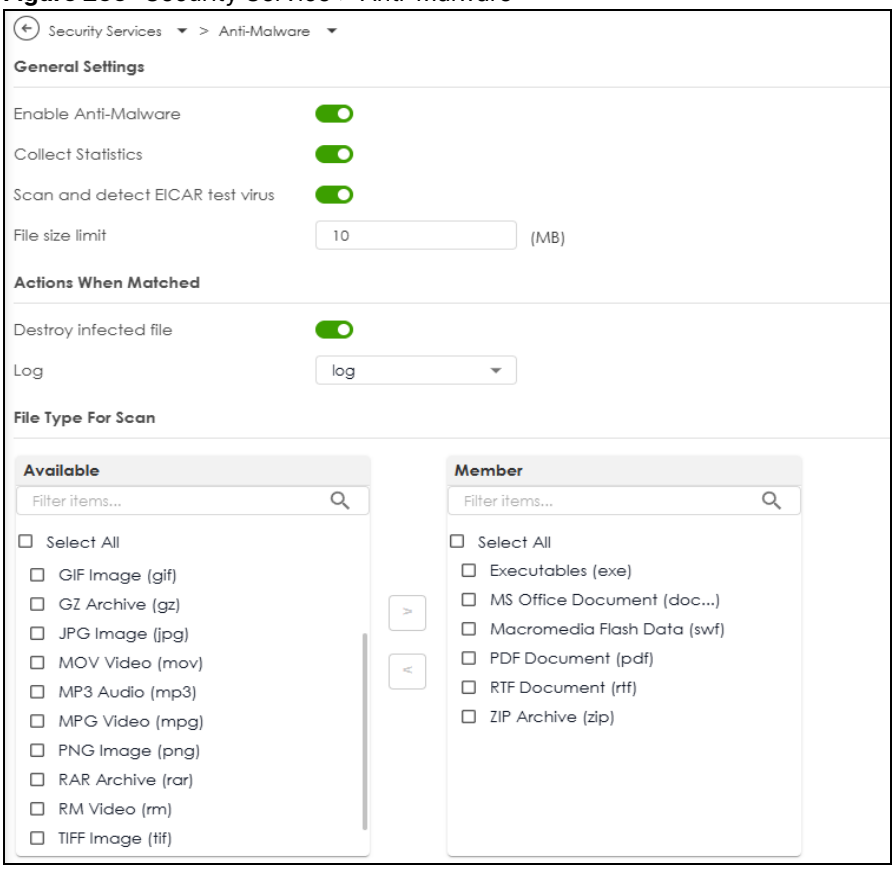
Click the **Anti-Malware** icon for more information on the Zyxel Device's security features.

Note: See Section 1.3 on page 20 for more information on the subscription services for the two types of security packs.

Note: If **Destroy infected file** is disabled and **log** is set to **no**, the Zyxel Device will still perform the scan but will not do anything else. It is recommended to enable at least one of the two functions.

If Destroy infected file is disabled, any malicious file found can still be executed by the end user after it is forwarded. The administrator would have to inform the user if there is an infected file.

Figure 255 Security Service > Anti-Malware



The following table describes the labels in this screen.

Table 194 Security Service > Anti-Malware

LABEL	DESCRIPTION
General Setting	
Enable	Click to activate the anti-malware feature to protect your connected network from infection and the installation of malicious software.
Collect Statistics	Click to have the Zyxel Device collect anti-malware statistics. All of the statistics are erased if you restart the Zyxel Device or click **Flush Data** in **Security Statistics** > **Anti-Malware.**
Scan and detect EICAR test virus	Click to have the Zyxel Device check for an EICAR test file and treat it in the same way as a real malware file. The EICAR test file is a standardized test file for signature based anti-malware scanners. When the scanner detects the EICAR file, it responds in the same way as if it found real malware. The EICAR file can also be compressed to test whether the anti-malware software can detect it in a compressed file. The test string consists of the following human-readable ASCII characters. X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
File size limit	Set the limit of the file size the Zyxel Device anti-malware will scan. A file that exceeds the file size you set here will pass without been scanned by the Zyxel Device anti-malware.
Destroy infected file	When you select this check box, if a malware signature is matched, the Zyxel Device overwrites the infected portion of the file with zeros before being forwarded to the user. The uninfected portion of the file will pass through unmodified.

Table 194 Security Service > Anti-Malware (continued)

LABEL	DESCRIPTION
Log	These are the log options: • **no**: Do not create a log when a packet matches a signature. • **log**: Create a log on the Zyxel Device when a packet matches a signature. • **log alert**: An alert is an emailed log for more serious events that may need more immediate attention. Select this option to have the Zyxel Device send an alert when a packet matches a signature(s).
File Type for Scan	File types that can be checked by the Zyxel Device are listed here. Note that the files on this list are currently bypassed. To use this feature on a specific file type, click this file type and then click the right arrow button. See available file types in Table 193 on page 413.
Search	Type an item in the search box, then click this to display all file types in the table below according to the item you typed.
Select All	Select this to select all file types in the table.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

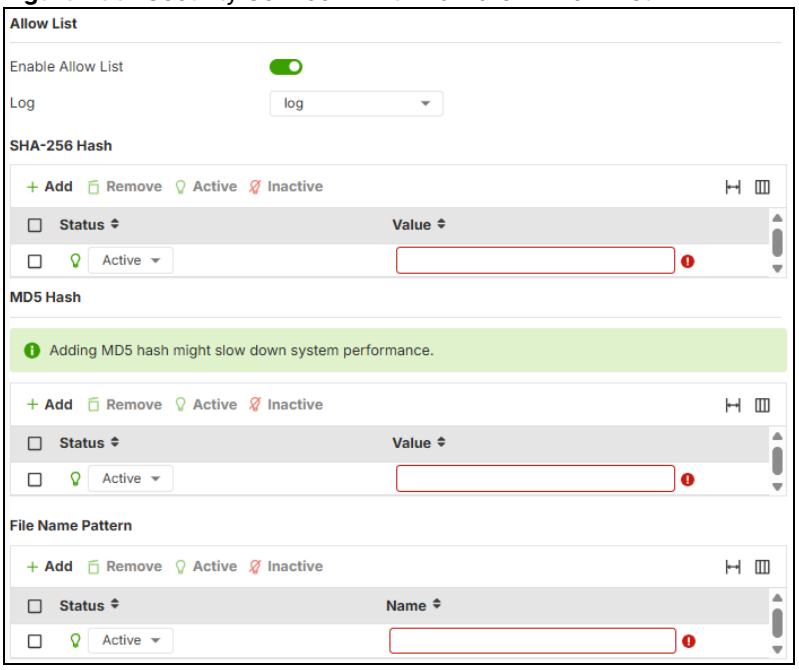
22.3 The Allow List Screen

An allow list allows you to specify a SHA-256 hash, MD5 hash or file pattern to ignore in order to avoid false positives. False positives occur when a non-infected file matches a malware signature.

Enter a file or encryption pattern that would cause the Zyxel Device to allow this file.

Click **Security Service** > **Anti-Malware** > **Allow List** to display the following screen. Use **Add** to put a new entry in the list or **Edit** to change an existing one or **Remove** to delete an existing entry.

Figure 256 Security Service > Anti-Malware > Allow List



The following table describes the fields in this screen.

Table 195 Security Service > Anti-Malware > Allow List

LABEL	DESCRIPTION
Enable Allow List	Select this to bypass checking by this feature (if enabled) and automatically allow incoming files with names or hash value (**MD5 Hash**) that match the white list patterns.
Log	These are the log options: • **no**: Do not create a log when a packet matches a signature. • **log**: Create a log on the Zyxel Device when a packet matches a signature.
SHA-256 / MD5 Hash	Configure the settings to automatically allow incoming files with SHA-256 Hash or MD5 Hash value that match the patterns you set. A SHA-256 hash can consist of 64 alpha-numerical characters. An MD5 hash can consist of 32 alpha-numerical characters. Note: By default, the Zyxel Device calculates only the SHA-256 hash. Adding an MD5 hash will require additional processing, which will increase CPU usage and slow down system performance.
Add	Click this to create a new entry.
Remove	Select an entry and click this to delete it.
Active	To turn on an entry, select it and click **Active**.
Inactive	To turn off an entry, select it and click **Inactive**.
Column ( )	Click the column icon to select the fields you want to show in the table. Uncheck the checkbox if you want to hide a field in the table.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Value	This field displays the hash pattern of the entry. Enter the hash pattern for this entry. Specify a pattern to identify the names of files that the Zyxel Device should not scan for viruses.
Edit	Select an entry and click this icon to modify it. 
Remove	Select an entry and click this icon to delete it. 
File Name Pattern	Configure the settings to automatically allow incoming files with names that match the patterns you set.
Add	Click this to create a new entry.
Remove	Select an entry and click this to delete it.
Active	To turn on an entry, select it and click **Active**.
Inactive	To turn off an entry, select it and click **Inactive**.
Column ( )	Click the column icon to select the fields you want to show in the table. Uncheck the checkbox if you want to hide a field in the table.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.

Table 195 Security Service > Anti-Malware > Allow List

LABEL	DESCRIPTION
Name	This field displays the file pattern of the entry. Enter the file pattern for this entry. Specify a pattern to identify the names of files that the Zyxel Device should not scan for viruses. • Use up to 80 characters. Alphanumeric characters, underscores (_), dashes (-), question marks (?) and asterisks (*) are allowed. • A question mark (?) lets a single character in the file name vary. For example, use “a?.zip” (without the quotation marks) to specify aa.zip, ab.zip and so on. • Wildcards (*) let multiple files match the pattern. For example, use “*a.zip” (without the quotation marks) to specify any file that ends with “a.zip”. A file named “testa.zip would match. There could be any number (of any type) of characters in front of the “a.zip” at the end and the file name would still match. A file named “test.zipa” for example would not match. • A * in the middle of a pattern has the Zyxel Device check the beginning and end of the file name and ignore the middle. For example, with “abc*.zip”, any file starting with “abc” and ending in “.zip” matches, no matter how many characters are in between. • The whole file name has to match if you do not use a question mark or asterisk. • If you do not use a wildcard, the Zyxel Device checks up to the first 80 characters of a file name.
Edit	Select an entry and click this icon to modify it. 
Remove	Select an entry and click this icon to delete it. 

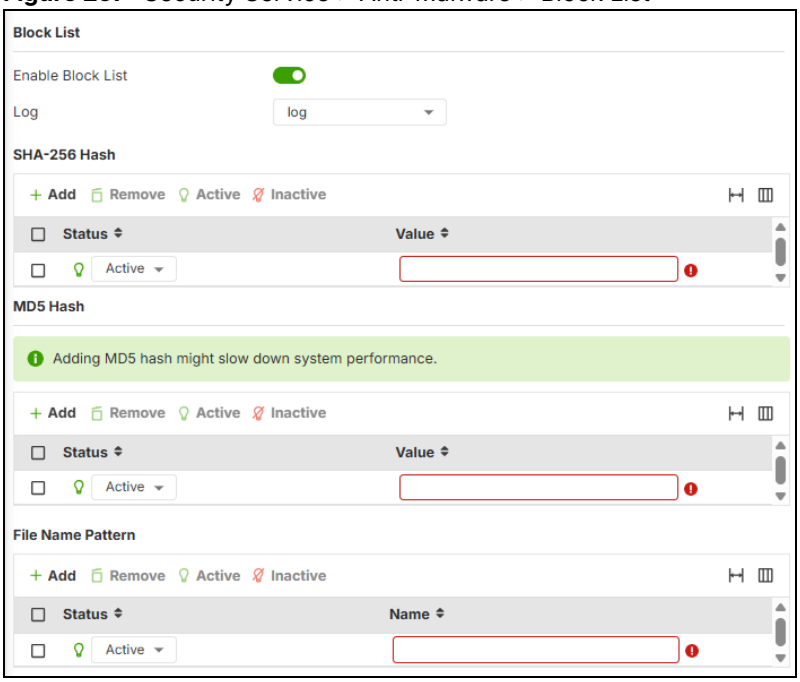
22.4 The Block List Screen

A block list allows you to specify a specific SHA-256 hash, MD5 hash or file pattern that you want to block.

Enter a file or encryption pattern that would cause the Zyxel Device to log and then destroy this file.

Click **Security Service** > **Anti-Malware** > **Block List** to display the following screen. Use **Add** to put a new entry in the list or **Edit** to change an existing one or **Remove** to delete an existing entry.

Figure 257 Security Service > Anti-Malware > Block List



The following table describes the fields in this screen.

Table 196 Security Services > Anti-Malware > Block/Allow List > Block List

LABEL	DESCRIPTION
Enable Block List	Select this to bypass checking by this feature (if enabled) and automatically block incoming files with names or hash value (**MD5 Hash**) that match the block list patterns.
Log	These are the log options: • **no**: Do not create a log when a packet matches a signature. • **log**: Create a log on the Zyxel Device when a packet matches a signature.
SHA-256 Hash / MD5 Hash	Configure the settings to automatically block incoming files with SHA-256 or MD5 Hash value that match the patterns you set. A SHA-256 hash can consist of 64 alpha-numerical characters. An MD5 hash can consist of 32 alpha-numerical characters. Note: By default, the Zyxel Device calculates only the SHA-256 hash. Adding an MD5 hash will require additional processing, which will increase CPU usage and slow down system performance.
Add	Click this to create a new entry.
Remove	Select an entry and click this to delete it.
Active	To turn on an entry, select it and click **Active**.
Inactive	To turn off an entry, select it and click **Inactive**.
Column ( )	Click the column icon to select the fields you want to show in the table. Clear the check box if you want to hide a field in the table.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Value	This field displays the hash pattern of the entry. Enter the hash pattern for this entry. Specify a pattern to identify the names of files that the Zyxel Device should not scan for viruses.

Table 196 Security Services > Anti-Malware > Block/Allow List > Block List (continued)

LABEL	DESCRIPTION
Edit	Select an entry and click this icon to modify it. 
Remove	Select an entry and click this icon to delete it. 
File Name Pattern	Configure the settings to automatically block incoming files with names that match the patterns you set.
Add	Click this to create a new entry.
Remove	Select an entry and click this to delete it.
Active	To turn on an entry, select it and click **Active**.
Inactive	To turn off an entry, select it and click **Inactive**.
Column ( )	Click the column icon to select the fields you want to show in the table. Uncheck the checkbox if you want to hide a field in the table.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Value	This field displays the file pattern of the entry. Enter the file pattern for this entry. Specify a pattern to identify the names of files that the Zyxel Device should not scan for viruses. • Use up to 80 characters. Alphanumeric characters, underscores (_), dashes (-), question marks (?) and asterisks (*) are allowed. • A question mark (?) lets a single character in the file name vary. For example, use “a?.zip” (without the quotation marks) to specify aa.zip, ab.zip and so on. • Wildcards (*) let multiple files match the pattern. For example, use “*a.zip” (without the quotation marks) to specify any file that ends with “a.zip”. A file named “testa.zip would match. There could be any number (of any type) of characters in front of the “a.zip” at the end and the file name would still match. A file named “test.zipa” for example would not match. • A * in the middle of a pattern has the Zyxel Device check the beginning and end of the file name and ignore the middle. For example, with “abc*.zip”, any file starting with “abc” and ending in “.zip” matches, no matter how many characters are in between. • The whole file name has to match if you do not use a question mark or asterisk. • If you do not use a wildcard, the Zyxel Device checks up to the first 80 characters of a file name.
Edit	Select an entry and click this icon to modify it. 
Remove	Select an entry and click this icon to delete it. 

22.5 Anti-Malware Technical Reference

Types of Anti-Malware Scanner

The section describes two types of anti-malware scanner: host-based and network-based.

A host-based anti-malware (HAM) scanner is often software installed on computers and/or servers on the network. It inspects files for malware patterns as they are moved in and out of the drive. However, host-based anti-malware scanners cannot eliminate all malware for a number of reasons:

- HAM scanners are slow in stopping malware threats through real-time traffic (such as from the Internet).
- HAM scanners may reduce computing performance as they also share resources (such as CPU time) on the computer for file inspection.
- You have to update the malware signatures and/or perform malware scans on all computers on the network regularly.

Note: The Zyxel Device does not support host-based anti-malware (HAM).

A network-based anti-malware (NAM) scanner is often deployed as a dedicated security device (such as your Zyxel Device) on the network edge. NAM scanners inspect real-time data traffic (such as email messages or web) that tends to bypass HAM scanners. The following lists some of the benefits of NAM scanners.

- NAM scanners stop malware threats at the network edge before they enter or exit a network.
- NAM scanners reduce computing loading on computers as the read-time data traffic inspection is done on a dedicated security device.

CHAPTER 23
Sandbox

23.1 Overview

Zyxel sandbox is a security mechanism which provides a safe environment to separate running programs from your network and host devices. Files with unknown or untrusted programs and codes are uploaded to the cloud. These files are executed within an isolated virtual machine (VM) to monitor and analyze the zero-day malware and advanced persistent threats (APTs). The zero-day malware refers to malware that is unknown to any software vendor or developer. It is dangerous because there is no available defenses against it at the time of discovery.

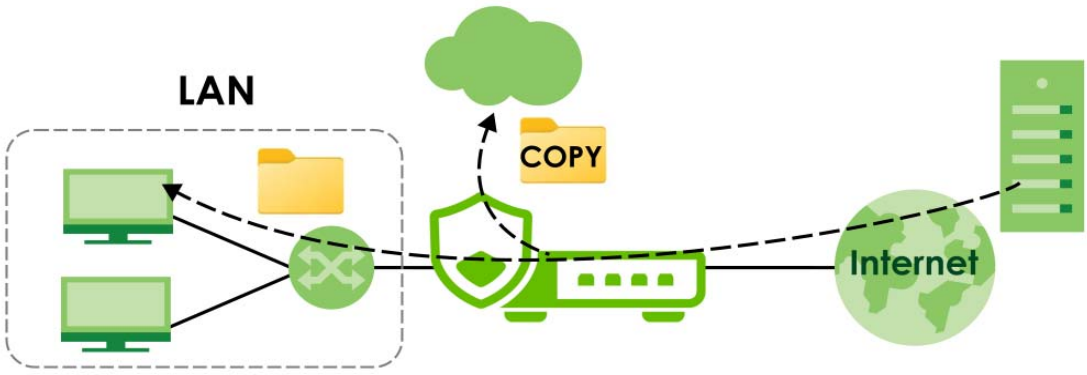
The zero-day malware and APTs may evade the Zyxel Device's detection, such as anti-malware. Results of cloud sandbox are sent from the server to the Zyxel Device.

After checking the received files against its local cache, the Zyxel Device sandbox uploads a copy of the files for inspection if the files are not recorded in the local cache. The scan result from the cloud is added to the Zyxel Device cache and used for future inspection. When a file with malicious or suspicious code is detected, the Zyxel Device takes specific actions on the threats.

By default, the Zyxel Device sandbox forwards all files that have not been checked before to the clients behind the Zyxel Device.

Note: The scan results will be removed from the Zyxel Device cache after the Zyxel Device restarts. When the scan results stored reach the limit, new scan results automatically overwrite existing scan results, starting with the oldest scan result first.

Figure 258 Zyxel Sandbox Inspection



23.1.1 What You Need to Know

The Zyxel Device forwards files that are not recorded in the local cache to the client behind the Zyxel Device before sandbox has completed checking. The scan result will display in **Log & Report** > **Log/ Events**. We suggest you to inform your client not to open the file until sandbox has completed checking. If the client already opened it, then please urge the client to run an up-to-date anti-malware scanner.

If the receiver of a suspect file cannot open a file, sandbox may have already modified the file by deleting the infected portion. Please check the logs and let the receiver know if this is so.

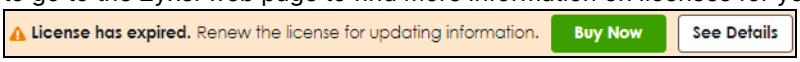
Sandbox can only check the types of files listed under **File Submission Options** in the **Sandbox** screen. If you disabled **Scan and detect EICAR test virus** in the **Anti-Malware** screen, then EICAR test files will be sent to sandbox.

To use the sandbox, you need to register your Zyxel Device and activate the service license at NCC, and then turn on the sandbox function on the Zyxel Device. See Chapter 6 on page 123 for more information about registration and service licenses.

23.2 Sandbox Screen

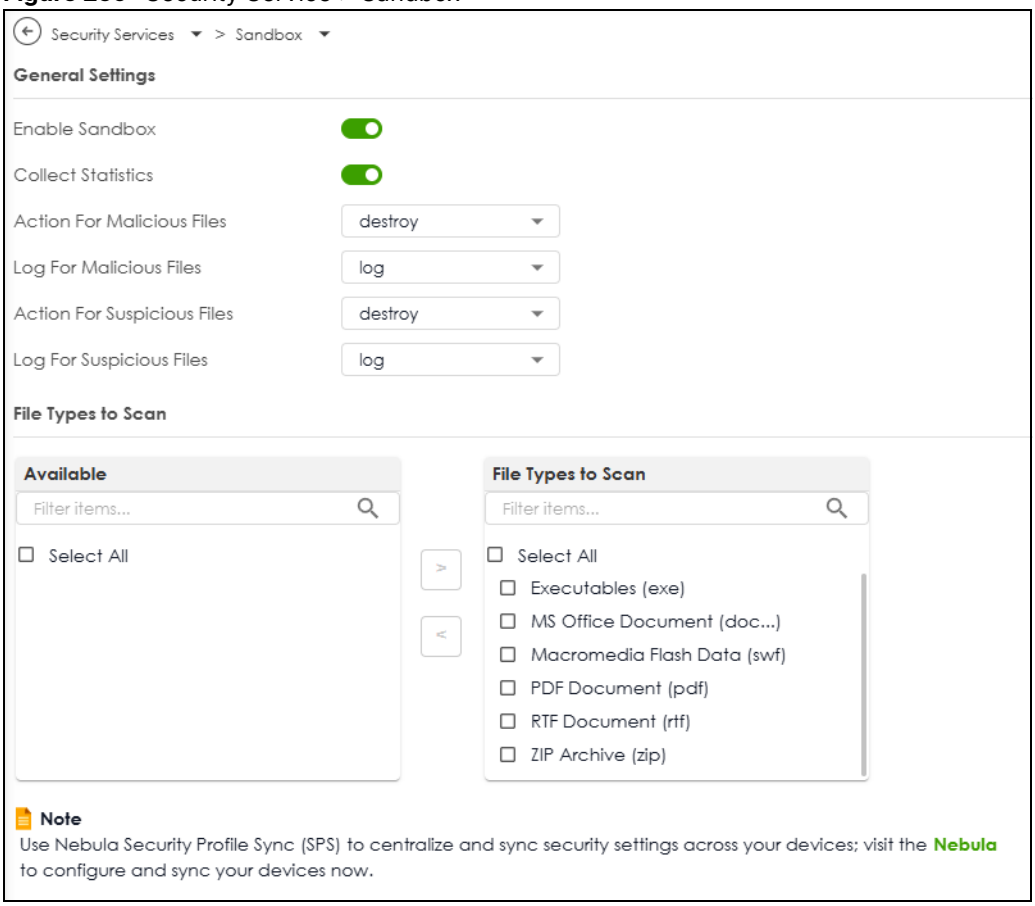
Click **Security Service** > **Sandbox** to display the configuration screen as shown next.

If a license has expired, you will see a reminder in this screen. You need to renew the license in order to keep using the feature. Click **Buy Now** to go to Marketplace to purchase a new license. Click **See Details** to go to the Zyxel web page to find more information on licenses for your Zyxel Device.



Use this screen to enable sandbox and specify the actions the Zyxel Device takes when malicious or suspicious files are detected.

Figure 259 Security Service > Sandbox



The following table describes the labels in this screen.

Table 197 Security Service > Sandbox

LABEL	DESCRIPTION
General	
Enable Sandbox	Select this option to turn on sandbox if you have a license and have activated it on the Zyxel Device. Otherwise, deselect it.
Collect Statistics	Enable to have the Zyxel Device collect sandbox statistics, such as the time, type and name of the files scanned. The statistics collected will display in **Security Statistics** > **Sandbox**. All of the statistics are erased if you restart the Zyxel Device or click **Flush Data** in **Security Statistics** > **Sandbox**.
Action For Malicious File	Specify whether the Zyxel Device deletes (**destroy**) or forwards (**allow**) malicious files. Malicious files are files given a high score for malware characteristics by the cloud. You can check the medium score for malware characteristics given by the cloud in the logs.
Log For Malicious File	These are the log options for malicious files: • **no**: Do not create a log when a malicious file is detected. • **log**: Create a log on the Zyxel Device when a malicious file is detected. • **log alert**: An alert is an emailed log. Select this option to have the Zyxel Device send an alert when a malicious file is detected.
Action For Suspicious File	Specify whether the Zyxel Device deletes (**destroy**) or forwards (**allow**) suspicious files. Suspicious files are files given a medium score for malware characteristics by the cloud. You can check the medium score for malware characteristics given by the cloud in the logs.

Table 197 Security Service > Sandbox (continued)

LABEL	DESCRIPTION
Log For Suspicious File	These are the log options for suspicious files: **no**: Do not create a log when a suspicious file is detected. **log**: Create a log on the Zyxel Device when a suspicious file is detected. **log alert**: An alert is an emailed log for more serious events that may need more immediate attention. Select this option to have the Zyxel Device send an alert when a suspicious file is detected.
File Types to Scan	Specify the type of files to be sent for sandbox inspection. • **Executables (exe)**: An executable file is a file that contains a program or application which your computer can run • **MS Office Document (doc...)**: This category includes Microsoft Word files, Microsoft Excel files and Microsoft PowerPoint files. MS Office Document are files that are created using software developed by Microsoft. • **Macromedia Flash Data (swf)**: A flash file (.swf) is a file that contains animations, multimedia elements or games. A flash file is often embedded into a web page. • **PDF Document (pdf)**: A Portable Document Format (PDF) file is a file that maintains the presentation and formatting of documents across different platform and devices. • **RTF Document (rtf)**: A Rich Text Format (RTF) file is a file that allows you to create text with different formats, such as bold or italics. • **ZIP Archive (zip)**: A zip file is a file used to compress multiple files together into a single file. A zip file can reduce the overall size of a collection of files.
Search	Type an item in the search box, then click this to display all file types in the table below according to the item you typed.
Select All	Select this to select all file types in the table.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

CHAPTER 24
IPS

24.1 Overview

This chapter introduces packet inspection IPS (Intrusion Prevention System), custom signatures, and updating signatures. An IPS system can detect malicious or suspicious packets and respond instantaneously by rejecting or dropping the packets. The Zyxel Device IPS protects your network against network-based intrusions.

24.1.1 What You Can Do in this Chapter

- Use the **Security Service > IPS** screen (Section 24.2 on page 428) to view registration and signature information.
- Use the **Security Service > IPS > Allow List** screen (Section 24.3 on page 435) to list signatures that will be exempted from IPS inspection.

24.1.2 What You Need To Know

Packet Inspection Signatures

A signature is a pattern of malicious or suspicious packet activity. You can specify an action to be taken if the system matches a stream of data to a malicious signature. You can change the action in the profile screens. Packet inspection examine OSI (Open System Interconnection) layer-4 to layer-7 packet contents for malicious data. Generally, packet inspection signatures are created for known attacks while anomaly detection looks for abnormal behavior.

Rate Based Signatures

While IPS signatures have the Zyxel Device respond instantaneously, **Rate Based Signatures** are IPS signatures that allow the Zyxel Device to just respond after a number of occurrences (**Count**) within a certain time period (**Period**) you set.

Figure 260 IPS Signatures Example

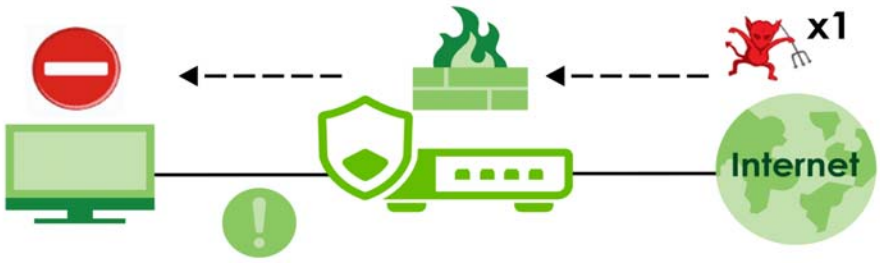
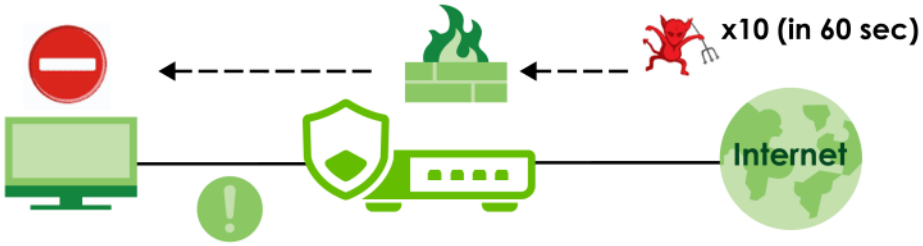


Figure 261 Rate Based Signatures Example



Bypass IPS Scanning of Packets from Trusted Applications

Many UDP packets are now encrypted, and IPS will scan them, so increasing CPU usage. In order to reduce CPU usage, the Zyxel Device will bypass IPS scanning of UDP packets from trusted applications.

Use the following Command Line Interface (CLI) command to see what applications are currently trusted by default.

```
MyUSGFLEX500H> show ips trusted-app
show-trusted-app
    data
        type "Default Trusted APP List"
        app "Microsoft teams"
        app "Microsoft SharePoint"
        app "Microsoft SharePoint Administration Application"
        app "Microsoft SharePoint Blog Management Application"
        app "Microsoft SharePoint Calendar Management Application"
        app "Microsoft SharePoint Document Management Application"
        app "Microsoft SharePoint Online (Office 365)"
        app Instagram
        app "YouTube TV"
        app Youtube.com
        app "youtube Audio/Video"
        app "youtube Upload"
        app "youtube HD"
        app "youtube Kids"
        app "youtube Music"
        app quic
        app Microsoft
        app "Microsoft OneDrive"
        ..
    ..
MyUSGFLEX500H>
```

You may also use the CLI to disable scanning of trusted applications and see if scanning of trusted applications is enabled.

```
MyUSGFLEX500H> edit running
MyUSGFLEX500H running config# vrf main ips bypass trusted-app enabled false
MyUSGFLEX500H running config# commit
Configuration committed.
MyUSGFLEX500H running config# show config vrf main ips bypass
bypass
    trusted-app
        enabled false
        ..
    ..
MyUSGFLEX500H running config#
```

Applying Your IPS Configuration

Changes to the Zyxel Device's IPS settings affect new sessions, but not the sessions that already existed before you applied the new settings. Before You Begin

Register for a trial IPS license in the **Licenses** screen. This gives you access to free signature updates. This is important as new signatures are created as new attacks evolve. When the trial license expires, purchase and enter a license key using the same screens to renew the license.

24.2 The IPS Screen

An IPS profile is a set of packet inspection signatures.

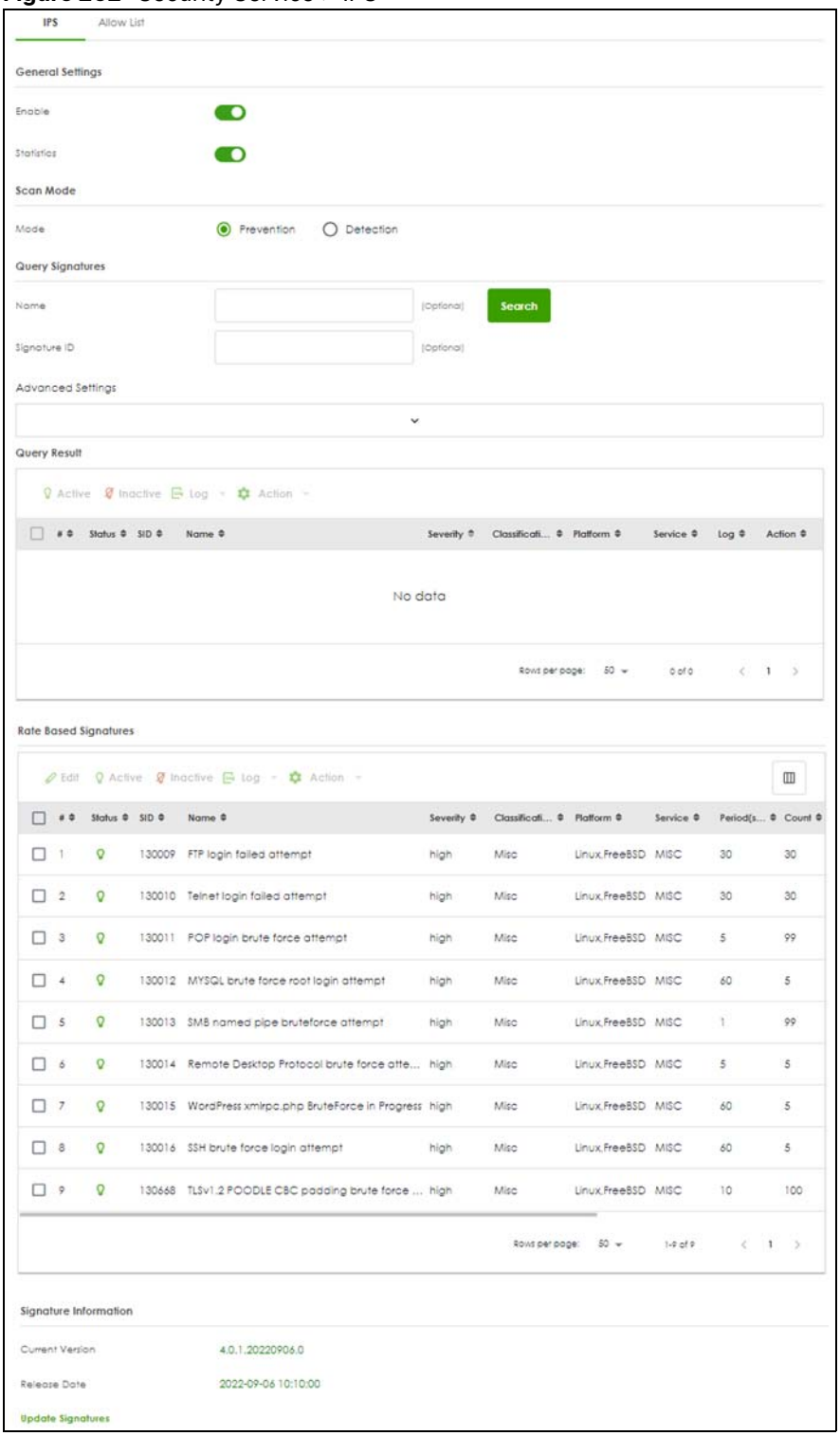
Click **Security Service > IPS** to open this screen. Use this screen to view signature information.

If a license has expired, you will see a reminder in this screen. You need to renew the license in order to keep using the feature. Click **Buy Now** to go to Marketplace to purchase a new license. Click **See Details** to go to the Zyxel web page to find more information on licenses for your Zyxel Device.



Note: You must register for the IPS signature service (at least the trial) before you can use it. See the **Licensing** screens.

Figure 262 Security Service > IPS



The following table describes the fields in this screen.

Table 198 Security Service > IPS

LABEL	DESCRIPTION
General Settings	
Enable	Click the switch to the right to activate the IPS feature which detects and prevents malicious or suspicious packets and responds instantaneously.
Statistics	Click the switch to the right to have the Zyxel Device collect IPS statistics. All of the statistics are erased if you restart the Zyxel Device or click **Flush Data** in **Security Statistics** > **IPS**.
Scan Mode	
Prevention	Select this to have the Zyxel Device perform a user-specified action when a stream of data matches a malicious signature.
Detection	Select this to have the Zyxel Device only create a log message when a stream of data matches a malicious signature.
Query Signatures	
Name	Type the name or part of the name of the signature(s) you want to find.
Signature ID	Type the ID or part of the ID of the signature(s) you want to find.
Advanced Settings	Configure these settings for more advanced queries.
Severity	Search for signatures by severity level(s). Hold down the [Ctrl] key if you want to make multiple selections. These are the severities as defined in the Zyxel Device. The number in brackets is the number you use if using commands. **Severe** (16): These denote attacks that try to run arbitrary code or gain system privileges. **High** (8): These denote known serious vulnerabilities or attacks that are probably not false alarms. **Medium** (4): These denote medium threats, access control attacks or attacks that could be false alarms. **Low** (2): These denote mild threats or attacks that could be false alarms. **Very-Low** (1): These denote possible attacks caused by traffic such as Ping, trace route, ICMP queries etc.
Classification	Search for signatures by attack type(s) (see Table 199 on page 432).
Platform	Search for signatures created to prevent intrusions targeting specific operating system(s).
Service	Search for signatures by IPS service group(s). See Table 200 on page 434 for group details.
Action	Search for signatures by the response the Zyxel Device takes when a packet matches a signature.
Activation	Search for activated and/or inactivated signatures here.
Log	Search for signatures by log option here.
Query Result	The results are displayed in a table showing the **Status**, **SID, Name, Severity, Classification, Platform, Service, Log**, and **Action** criteria as selected in the search. Click the **SID** column header to sort search results by signature ID.
Rate Based Signature	IPS signatures identify traffic packets with suspicious malicious patterns. The Zyxel Device can then respond instantaneously according to the action you define. If you do not want the Zyxel Device to respond instantaneously for each suspicious packet detected, use rate based signatures to only respond after a number of occurrences (**Count**) within a certain time period (**Period**). See Section 24.1.2 on page 426 for more information on rate based signatures.
Edit	Select an entry and click **Edit** to modify the entry's settings.

Table 198 Security Service > IPS (continued)

LABEL	DESCRIPTION
Active	To turn on an entry, select it and click **Activate**.
Inactive	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 a packet matches a signature.
Action	To edit what action the Zyxel Device takes when a packet matches a signature, select the entry and use the **Action** icon. **none**: Select this action to have the Zyxel Device take no action when a packet matches a signature. **drop**: Select this action to have the Zyxel Device silently drop a packet that matches a signature. Neither sender nor receiver are notified. **reject**: Select this action to have the Zyxel Device send a reset to both the sender and receiver when a packet matches the signature. 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.
SID	SID is the signature ID that uniquely identifies a signature. Click the SID header to sort signatures in ascending or descending order.
Name	This is the name of your rate-based signature. The name is the type of attack the Zyxel Device can identify.
Severity	This field displays signatures by severity level(s). Hold down the [Ctrl] key if you want to make multiple selections. These are the severities as defined in the Zyxel Device. The number in brackets is the number you use if using commands. **Severe** (5): These denote attacks that try to run arbitrary code or gain system privileges. **High** (4): These denote known serious vulnerabilities or attacks that are probably not false alarms. **Medium** (3): These denote medium threats, access control attacks or attacks that could be false alarms. **Low** (2): These denote mild threats or attacks that could be false alarms. **Very-Low** (1): These denote possible attacks caused by traffic such as Ping, trace route, ICMP queries etc.
Classification	This field displays signatures by attack types (see Table 199 on page 432).
Platform	This field displays signatures created to prevent intrusions targeting specific operating system(s). Hold down the [Ctrl] key if you want to make multiple selections.
Service	This field displays signatures by IPS service group(s). See Table 200 on page 434 for group details.Hold down the [Ctrl] key if you want to make multiple selections.
Log	This fields displays the log action the Zyxel Device takes when a packet matches a signature. **log**- The Zyxel Device generates a log. **log an alert**- The Zyxel Device generates a log and alerts the users. **no**- The Zyxel Device will neither generate a log nor alert the users.

Table 198 Security Service > IPS (continued)

LABEL	DESCRIPTION
Action	This field displays the response the Zyxel Device takes when a packet matches a signature. Hold down the [Ctrl] key if you want to make multiple selections. **none**: Select this action to have the Zyxel Device take no action when a packet matches a signature. **drop**: Select this action to have the Zyxel Device silently drop a packet that matches a signature. Neither sender nor receiver are notified. **reject**: Select this action to have the Zyxel Device send a reset to both the sender and receiver when a packet matches the signature. 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.
Period (sec)	Type the length of time in seconds the event should occur a **Count** number of times to trigger an IPS **Action**. For example, **Count** is set to 5, and **Period** is set to 60. If the Zyxel Device detects more than 5 occurrences of malicious traffic in less than 60 seconds, then an IPS **Action** is triggered.
Count	Type the number of security events that need to occur within the defined **Period** in order to trigger an IPS **Action**. The allowed range is 1 to 300.
Block Period	This field displays the time period the attacker's IP will be blocked. Click on the number in this column to set the value from 0 to 86400 seconds. 0 means that the IP will not be blocked.
Signature Information	The following fields display information on the current signature set that the Zyxel Device is using.
Current Version	This field displays the IPS signature set version number. This number gets larger as the set is enhanced.
Update Signatures	Click this link to go to the screen you can use to download signatures from the update server.

Classifications

This table describes attack **Classifications** as categorized in the Zyxel Device.

Table 199 Attack Classifications

POLICY TYPE	DESCRIPTION
Any	Any attack includes all other kinds of attacks that are not specified in the policy such as password, spoof, hijack, phishing, and close-in.
Misc	Miscellaneous attacks takes advantage of vulnerable computer networks and web servers by forcing cache servers or web browsers into disclosing user-specific information that might be sensitive and confidential. The most common type of Misc. attacks are HTTP Response Smuggling, HTTP Response Splitting and JSON Hijacking.
Web-Attacks	Web attacks refer to attacks on web servers such as IIS (Internet Information Services).
Buffer Overflow	A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. The excess information can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Intruders could run codes in the overflow buffer region to obtain control of the system, install a backdoor or use the victim to launch attacks on other devices.

Table 199 Attack Classifications (continued)

POLICY TYPE	DESCRIPTION
Backdoor/Trojan Horse	A backdoor (also called a trapdoor) is hidden software or a hardware mechanism that can be triggered to gain access to a program, online service or an entire computer system. A Trojan horse is a harmful program that is hidden inside apparently harmless programs or data. Although a virus, a worm and a Trojan are different types of attacks, they can be blended into one attack. For example, W32/Blaster and W32/Sasser are blended attacks that feature a combination of a worm and a Trojan.
Access Control	Access control refers to procedures and controls that limit or detect access. Access control attacks try to bypass validation checks in order to access network resources such as servers, directories, and files.
P2P	Peer-to-peer (P2P) is where computing devices link directly to each other and can directly initiate communication with each other; they do not need an intermediary. A device can be both the client and the server. In the Zyxel Device, P2P refers to peer-to-peer applications such as e-Mule, e-Donkey, BitTorrent, iMesh, etc.
IM	IM (Instant Messenger) refers to chat applications. Chat is real-time, text-based communication between two or more users via networks-connected computers. After you enter a chat (or chat room), any room member can type a message that will appear on the monitors of all the other participants.
Virus/Worm	A computer virus is a small program designed to corrupt and/or alter the operation of other legitimate programs. A worm is a program that is designed to copy itself from one computer to another on a network. A worm's uncontrolled replication consumes system resources, thus slowing or stopping other tasks.
BotNet	A Botnet is a number of Internet computers that have been set up to forward transmissions including spam or viruses to other computers on the Internet though their owners are unaware of it. It is also a collection of Internet-connected programs communicating with other similar programs in order to perform tasks and participate in distributed Denial-Of-Service attacks.
DoS-DDoS	The goal of Denial of Service (DoS) attacks is not to steal information, but to disable a device or network on the Internet. A Distributed Denial of Service (DDoS) attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.
Scan	A scan describes the action of searching a network for an exposed service. An attack may then occur once a vulnerability has been found. Scans occur on several network levels. A network scan occurs at layer-3. For example, an attacker looks for network devices such as a router or server running in an IP network. A scan on a protocol is commonly referred to as a layer-4 scan. For example, once an attacker has found a live end system, he looks for open ports. A scan on a service is commonly referred to a layer-7 scan. For example, once an attacker has found an open port, say port 80 on a server, he determines that it is a HTTP service run by some web server application. He then uses a web vulnerability scanner (for example, Nikto) to look for documented vulnerabilities.
File Transfer	File transfer is a protocol to transfer files over the Internet. An attack may then occur if you're transferring files over an unsecured connection. Personal data stored in the files uploaded can also be easily accessed by attackers if these files are not encrypted.
Mail	A Mail or email bombing attack involves sending several thousand identical messages to an electronic mailbox in order to overflow it, making it unusable.
Stream Media	A Stream Media attack occurs when a malicious network node downloads an overwhelming amount of media stream data that could potentially exhaust the entire system. This method allows users to send small requests messages that result in the streaming of large media objects, providing an opportunity for malicious users to exhaust resources in the system with little effort expended on their part.

Table 199 Attack Classifications (continued)

POLICY TYPE	DESCRIPTION
Tunnel	A Tunneling attack involves sending IPv6 traffic over IPv4, slipping viruses, worms and spyware through the network using secret tunnels. This method infiltrates standard security measures through IPv6 tunnels, passing through IPv4 undetected. An external signal then triggers the malware to spring to life and wreak havoc from inside the network.
ACL	This attack is a violation of an ACL (Access Control List) rule. These are packet filter rules that check source, destination IP addresses / ports, and routing information in the packet.

IPS Service Groups

An IPS service group is a set of related packet inspection signatures.

Table 200 IPS Service Groups

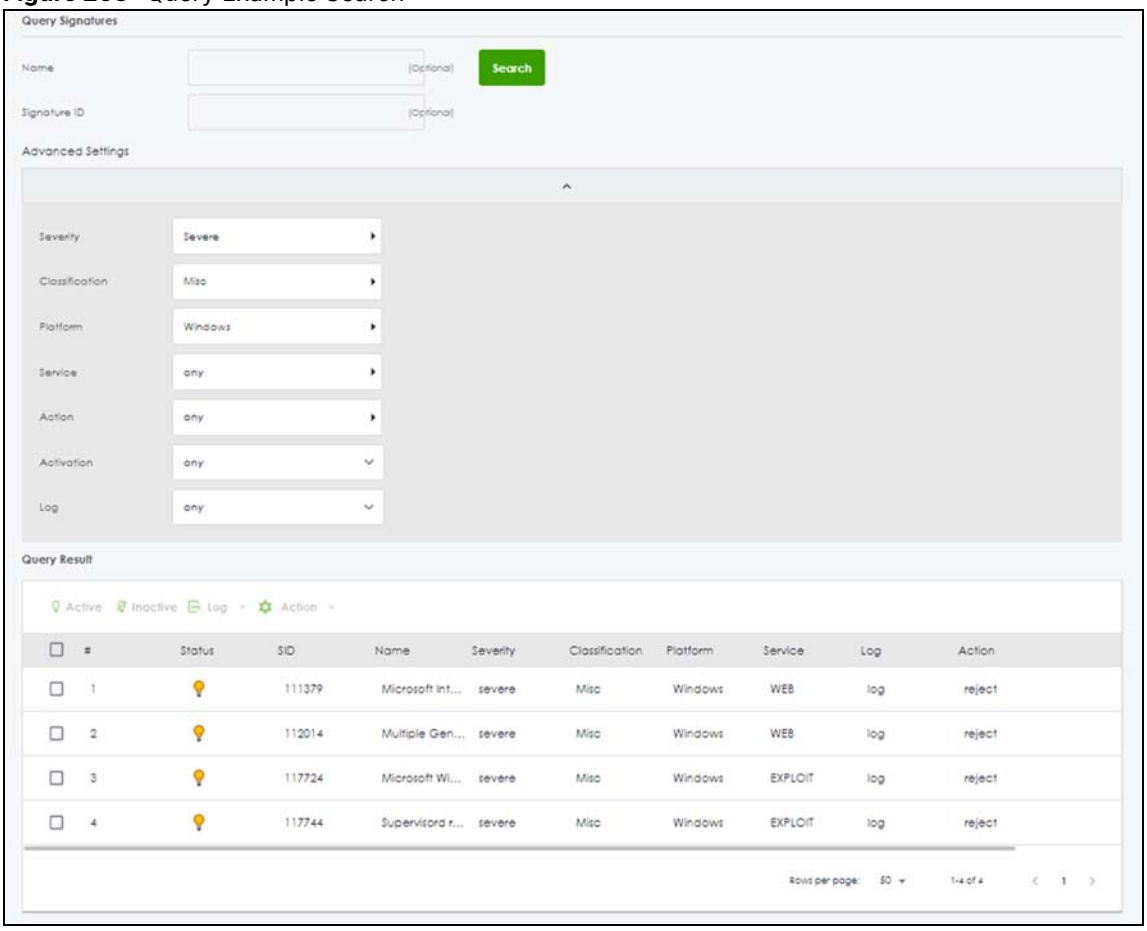
WEB_PHP	WEB_MISC	WEB_IIS	WEB_FRONTPAGE
WEB_CGI	WEB_ATTACKS	TFTP	TELNET
SQL	SNMP	SMTP	RSERVICES
RPC	POP3	POP2	P2P
ORACLE	NNTP	NETBIOS	MYSQL
MISC_EXPLOIT	MISC_DDOS	MISC_BACKDOOR	MISC
IMAP	IM	ICMP	FTP
FINGER	DNS	n/a	

24.2.1 Query Example

This example shows a search with these criteria:

- Severity: Severe
- Classification Type: Misc
- Platform: Windows
- Service: Any
- Actions: Any

Figure 263 Query Example Search

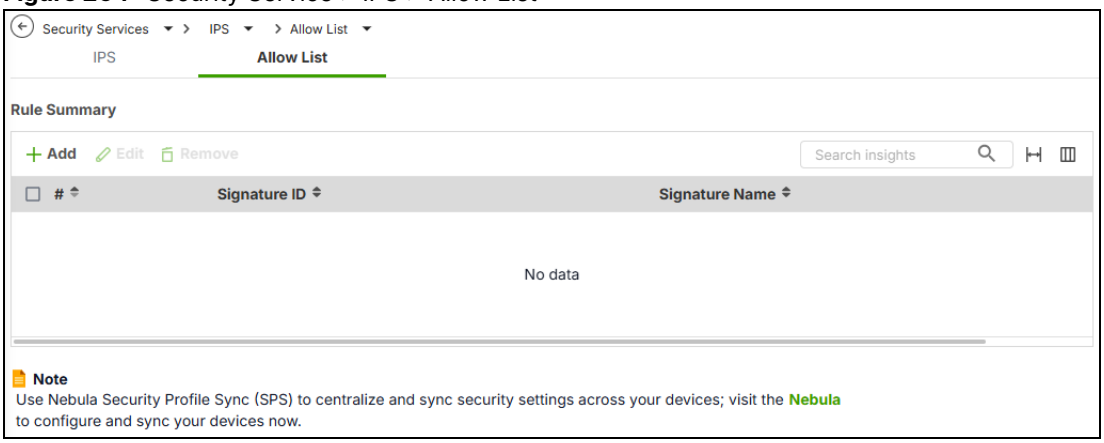


24.3 The Allow List Screen

Use this screen to exempt packets with these signatures from IPS inspection. The Zyxel Device will exclude incoming packets with the listed signature(s) from being intercepted and inspected.

Click **Security Services > IPS > Allow List** to display the following screen. Use **Add** to put a new item in the list or **Edit** to change an existing one or **Remove** to delete an existing entry.

Figure 264 Security Service > IPS > Allow List



The following table describes the fields in this screen.

Table 201 Security Service > IPS > Allow List

LABEL	DESCRIPTION
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.
#	This is the entry's index number in the list.
Signature ID	This field displays the signature ID of this entry.
Signature Name	This field displays the signature name of this entry.

24.4 IPS Technical Reference

This section contains some background information on IPS.

Host Intrusions

The goal of host-based intrusions is to infiltrate files on an individual computer or server in with the goal of accessing confidential information or destroying information on a computer.

You must install a host IPS directly on the system being protected. It works closely with the operating system, monitoring and intercepting system calls to the kernel or APIs in order to prevent attacks as well as log them.

Disadvantages of host IPSs are that you have to install them on each device (that you want to protect) in your network and due to the necessarily tight integration with the host operating system, future operating system upgrades could cause problems.

Network Intrusions

Network-based intrusions have the goal of bringing down a network or networks by attacking computer(s), switch(es), router(s) or modem(s). If a LAN switch is compromised for example, then the

whole LAN is compromised. Host-based intrusions may be used to cause network-based intrusions when the goal of the host virus is to propagate attacks on the network, or attack computer/server operating system vulnerabilities with the goal of bringing down the computer/server. Typical “network-based intrusions” are SQL slammer, Blaster, Nimda MyDoom etc.

Note: The Zyxel Device IPS protects your network against network-based intrusions.

CHAPTER 25
IP Exception

25.1 Overview

IP Exception allows incoming IP packets to bypass specific security services based on the packet's source or destination address. Bypassing a security service means the security service does not intercept nor inspect the packet.

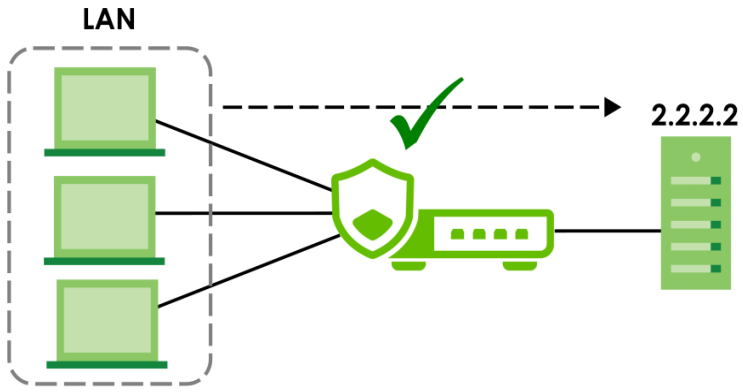
For example, 192.168.100.100 is a trusted LAN computer. Add the IP address of the LAN computer to **Source** in **IP Exception** so the Zyxel Device will not perform security checking on traffic coming from this computer.

Figure 265 IP Exception Bypass Source Example



You can also add a trusted destination to bypass security checking. For example, 2.2.2.2 is a trusted web site. Add the IP address of the trusted web site to **Destination** in **IP Exception** so the Zyxel Device will not perform security checking when you access the web site to save resources.

Figure 266 IP Exception Bypass Destination Example



IP Exception supports bypassing the following security services:

- Anti-Malware
- URL Threat Filter
- IPS (Intrusion Prevention System)

- IP Reputation.
- DNS Threat Filter

25.2 The IP Exception Screen

Use this screen to view the IP exception list for the specified services. The Zyxel Device will not inspect incoming packets that match the listed source and destination IP address(es) with the specified services.

Click **Security Service > IP Exception** to display the following screen. Use **Add** to put a new entry in the list or **Edit** to change an existing one or **Remove** to delete an existing entry.

Figure 267 Security Service > IP Exception



The following table describes the fields in this screen.

Table 202 Security Service > IP Exception

LABEL	DESCRIPTION
Configuration	
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.
Active	To turn off an entry, select it and click **Active**. The **Status** light changes accordingly.
Inactive	To turn off an entry, select it and click **Inactive**. The **Status** light changes accordingly.
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 this entry.
IPv4 Source	This field displays the source IP address (or address object) of incoming traffic. It displays **any** if there is no restriction on the source IP address.
IPv4 Destination	This field displays the destination IP address (or address object) of incoming traffic. It displays **any** if there is no restriction on the destination IP address.
Service to Bypass	This field displays which services will not inspect matched packets.
Log	This field displays if the Zyxel Device will generate a log when the incoming traffic is in the exception list.

Table 202 Security Service > IP Exception (continued)

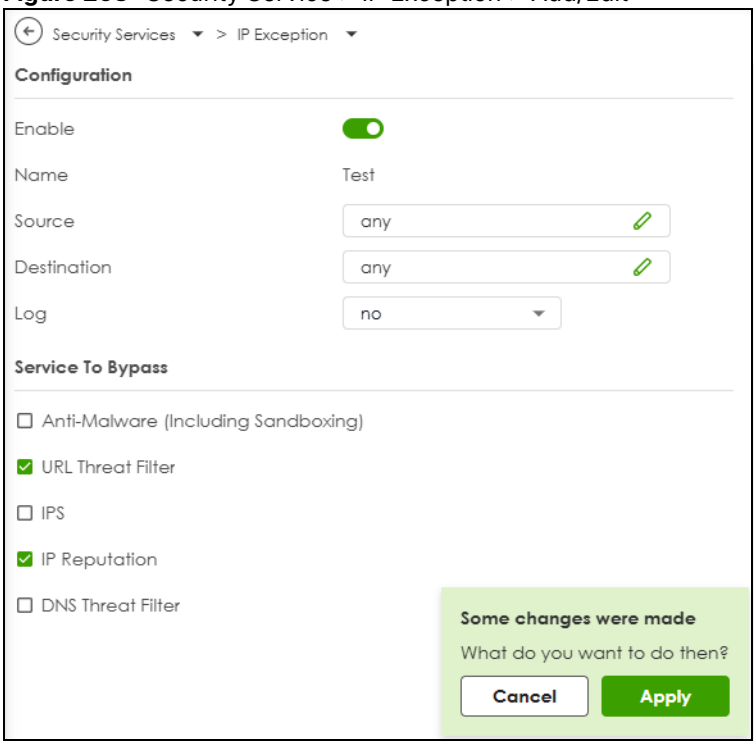
LABEL	DESCRIPTION
Cancel	Click **Cancel** to return the screen to its last-saved settings.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

25.2.1 The IP Exception Add/Edit Screen

Use this screen to add or edit entries of IPv4 address in the IP exception list.

Click **Security Service > IP Exception > Add/Edit** to display the following screen.

Figure 268 Security Service > IP Exception > Add/Edit



The following table describes the fields in this screen.

Table 203 Security Service > IP Exception > Add/Edit

LABEL	DESCRIPTION
Enable	Click this to the right to enable the rule on the Zyxel Device.
Name	Enter a descriptive name of this entry. You may use 2-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Source	Select **any** or an address object of the source IP address for this entry. Select **any** so there's no restriction on the source IP address.
Destination	Select **any** or an address object of the destination IP address for this entry. Select **any** so there's no restriction on the destination IP address.
Log	The Zyxel Device does not inspect packets with the selected service if you select **Yes**. The Zyxel Device will also generate a log when the incoming traffic is in th exception list. Otherwise, select **No**.
Service to Bypass	Selected services do not inspect packets that match source/destination criteria above. Non-selected services do inspect packets that match source/destination criteria above.

Table 203 Security Service > IP Exception > Add/Edit (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

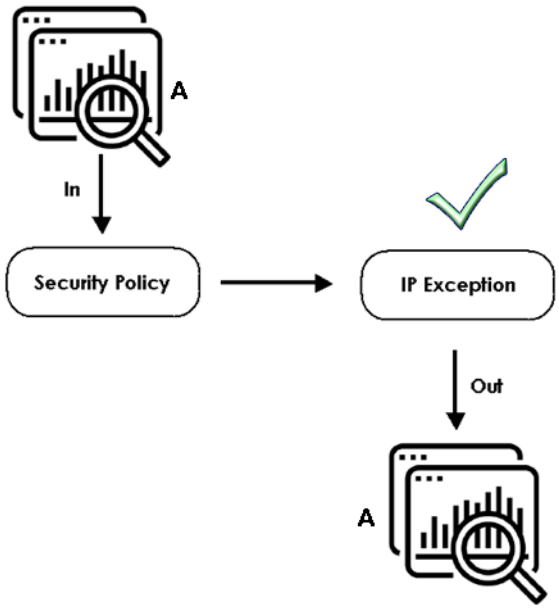
25.3 Example: Bypass a Website

You often access a website 1.1.1.1 that you are sure is safe. Every time you access the website, the packets sent by the website will be inspected by the Zyxel Device security services, such as anti-malware, content filter, reputation filter and app patrol.

This not only causes your web browser to take more time to load the website, but also takes up more Zyxel Device resources than necessary.

For example, you create an **IP Exception** profile for the website 1.1.1.1. IP exception allows incoming IP packets from the website 1.1.1.1 (**A**) to bypass specific security services. Bypassing a security service means the security service does not intercept nor inspect the packet.

Figure 269 Bypass Security Services Flow



This example uses the parameters given below.

Table 204 Address Object Configuration Example

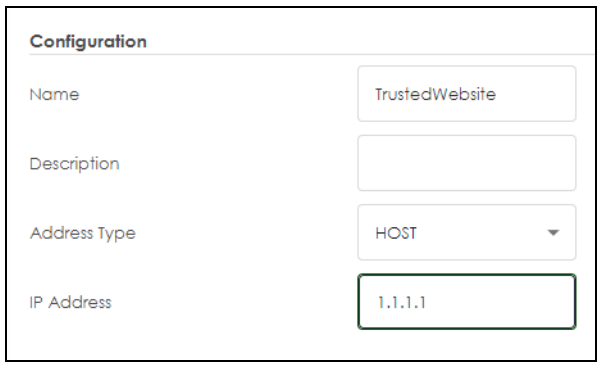
NAME	ADDRESS TYPE	IP ADDRESS
TrustedWebsite	Host	1.1.1.1

Table 205 IP Exception Configuration Example

NAME	SOURCE	DESTINATION	LOG	SERVICES TO BYPASS
ForTrustedWebsite	TrustedWebsite	Any	No	Anti-Malware URL Threat filter IPS IP Reputation DNS Threat Filter

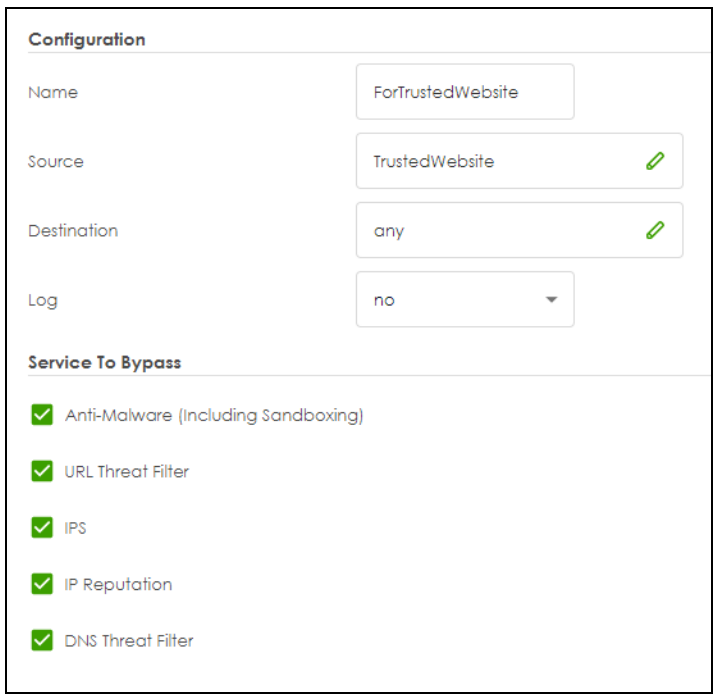
1 Go to **Object** > **Address** > **Address** and click **Add**.

2 Configure the settings using the parameters given in Table 204 on page 441. Click **Apply** to save your changes.



3 Go to **Security Service** > **IP Exception** and click **Add**.

4 Configure the settings using the parameters given in Table 205 on page 442. Click **Apply** to save your changes.



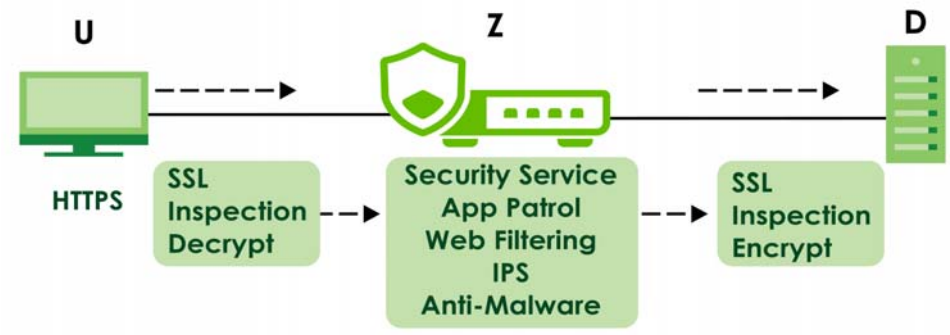
CHAPTER 26
SSL Inspection

26.1 Overview

Secure Socket Layer (SSL) traffic, such as https://www.google.com/HTTPS, FTPs, POP3s, SMTPs, and so on, is encrypted, and cannot be inspected using Security Service profiles such as App Patrol, Web Filtering, Intrusion Prevention System (IPS), or Anti-Malware. The Zyxel Device uses SSL Inspection to decrypt SSL traffic, sends it to the Security Service engines for inspection, then encrypts traffic that passes inspection and forwards it to the destination server, such as Google.

An example process is shown in the following figure. User **U** sends a HTTPS request (SSL) to destination server **D**, via the Zyxel Device, **Z**. The traffic matches an SSL Inspection profile in a security policy, so the Zyxel Device decrypts the traffic using SSL Inspection. The decrypted traffic is then inspected by the Security Service profiles in the same security profile that matched the SSL Inspection profile. If all is OK, then the Zyxel Device re-encrypts the traffic using SSL Inspection and forwards it to the destination server **D**. SSL traffic could be in the opposite direction for other examples.

Figure 270 SSL Inspection Overview



26.1.1 What You Can Do in this Chapter

- Use the **Security Service > SSL Inspection > Profile** screen (Section 26.2 on page 444) to view SSL Inspection profiles. Click the **Add** or **Edit** icon in this screen to configure the CA certificate, action and log in an SSL Inspection profile.
- Use the **Security Service > SSL Inspection > Exclude List** screens (Section 26.3 on page 448) to create a whitelist of destination servers to which traffic is passed through uninspected.
- Use the **Security Service > SSL Inspection > Certificate Update** screens (Section 26.4 on page 450) to update the latest certificates of servers using SSL connections to the Zyxel Device network

26.1.2 What You Need To Know

SSL Inspection supports the following TLS protocols and encryption algorithms

- TLS 1.0 AES-CBC

- TLS 1.2 AES-CBC/AES-GCM
- TLS 1.3

SSL Inspection does not support the following:

- Compression Support
- Client Authentication

26.1.3 What You Can Do in this Chapter

- See **Object > Certificate > My Certificates** for information on creating certificates on the Zyxel Device.
- See **Security Statistics > SSL Inspection** to get usage data and easily add a destination server to the whitelist of exclusion servers.
- See **Security Policy > Policy Control > Policy** to bind an SSL Inspection profile to a traffic flow(s).

26.1.4 Before You Begin

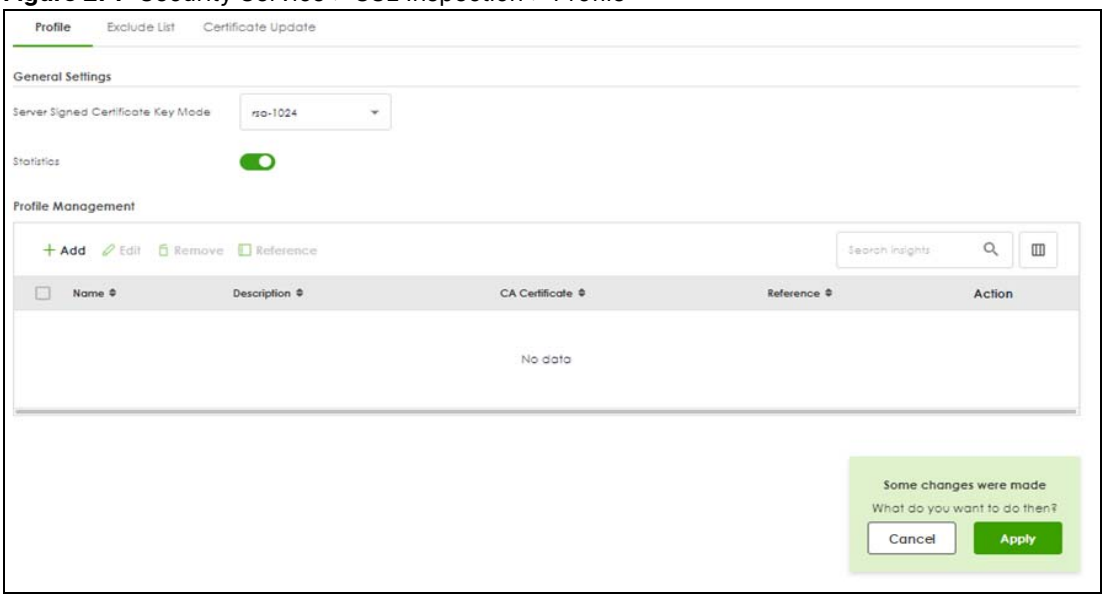
- If you don't want to use the default Zyxel Device certificate, then create a new certificate in **Object > Certificate > My Certificates**.
- Decide what destination servers to which traffic is sent directly without inspection. This may be a matter of privacy and legality regarding inspecting an individual's encrypted session, such as financial websites. This may vary by locale.

26.2 The SSL Inspection Profile Screen

An SSL Inspection profile is a template with pre-configured certificate, action and log.

Click **Security Service > SSL Inspection > Profile** to open this screen.

Figure 271 Security Service > SSL Inspection > Profile



The following table describes the fields in this screen.

Table 206 Security Service > SSL Inspection > Profile

LABEL	DESCRIPTION
General Settings	
Server Signed Certificate Key Mode	With SSL inspection, the Zyxel Device acts as a 'man-in-the-middle' between a client and a remote server, when the client and server are communicating using an SSL-encrypted session. Every time the client and server send data to each other, the Zyxel Device decrypts the sender's encrypted data, scans the plain data for threats, re-encrypts the data, and then sends the encrypted data to the receiver. • For outgoing sessions from the client to the remote server, the Zyxel Device creates a virtual server to decrypt data and a virtual client to re-encrypt data. • For incoming sessions from the remote server to the client, the Zyxel Device creates a virtual client to decrypt data, and a virtual server to re-encrypt data. To perform SSL Inspection for clients using SSL (HTTPS, SSH, SMTP) through the Zyxel Device, the Zyxel Device must check that the server's certificate with corresponding public key are valid and were issued by a Certificate Authority (CA) listed in the Zyxel Device's list of trusted CAs. According to the selected key mode **RSA 1024**, **RSA 2048**, **ECDSA-RSA-1024** or **ECDSA-RSA-2048**, the Zyxel Device will construct the corresponding self-signed certificate for the virtual server. RSA is a public-key cryptosystem used for data encryption or signing messages. For data encryption, the encryption key is public and the decryption key is private. For signing messages, the signing key is private and the verification key is public. Elliptic Curve Cryptography (ECC) is a public-key cryptosystem based on elliptic curve theory, and more efficient than RSA. ECC allows smaller keys compared to RSA to provide equivalent security. For example, a 224-bit elliptic curve public key should provide comparable security to a 2048-bit RSA public key. • **ECDSA-RSA-1024** indicates Zyxel Device support for clients that support both ECDSA-256 and RSA-1024 with ECDSA-256 having higher priority, that is ECDSA-256 is used by the virtual server, if a client supports both ECDSA-256 and RSA-1024. • **ECDSA-RSA-2048** indicates Zyxel Device support for clients that support both ECDSA-256 and RSA-2048 with ECDSA-256 having higher priority, that is ECDSA-256 is used by the virtual server, if a client supports both ECDSA-256 and RSA-2048. Select a mode that the client's browser, FTP client, or mail client supports. The Zyxel Device will use different keys (cryptosystems) for each client according to the client's support list. For example, if there are three clients behind a Zyxel Device with the following key mode support: • Client 1 - **RSA-1024** • Client 2 - **RSA-2048** and **RSA-1024** • Client 3 - ECDSA-256 and **RSA-2048**. If you set the key mode to **ECDSA-RSA-1024**, then the following will be used by each client: • Client 1 - **RSA-1024** • Client 2 - **RSA-1024** • Client 3 - **ECDSA-256**. If you set the key mode to **ECDSA-RSA-2048**, then the following will be used by each client: • Client 1 - sessions will not be processed (**pass**) by SSL inspection • Client 2 - **RSA-2048** • Client 3 - **ECDSA-256**.
Statistics	Enable this to have the Zyxel Device collect SSL inspection statistics.
Profile Management	
Add	Click **Add** to create a new profile.

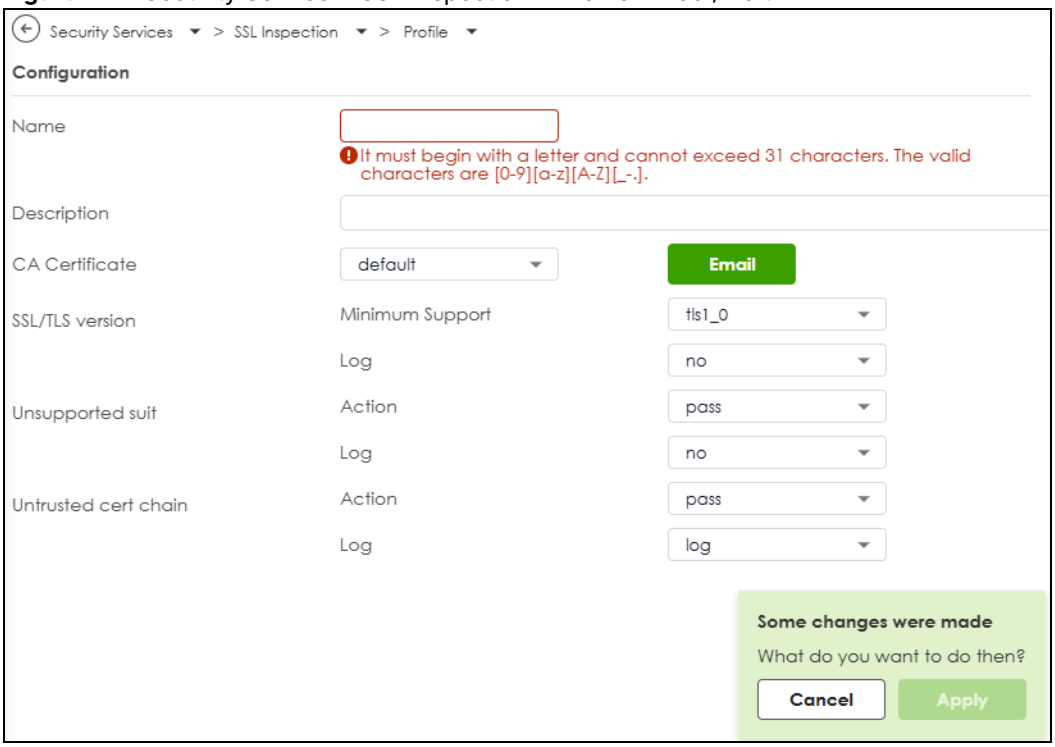
Table 206 Security Service > SSL Inspection > Profile (continued)

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.
References	Select an entry and click **References** to open a screen that shows which settings use the entry.
Action	Click this icon to apply the entry to a policy control rule. Go to the **Security Policy** > **Policy Control** screen to check the result.
#	This is the entry's index number in the list.
Name	This displays the name of the profile.
Description	This displays the description of the profile.
CA Certificate	This displays the CA certificate being used in this profile.
Reference	This displays the number of times an object reference is used in a profile.

26.2.1 Add/Edit SSL Inspection Profiles

Click **Security Service > SSL Inspection > Profile > Add** to create a new profile or select an existing profile and click **Edit** to change its settings.

Figure 272 Security Service > SSL Inspection > Profile > Add / Edit



The following table describes the fields in this screen.

Table 207 Security Service > SSL Inspection > Profile > Add/Edit

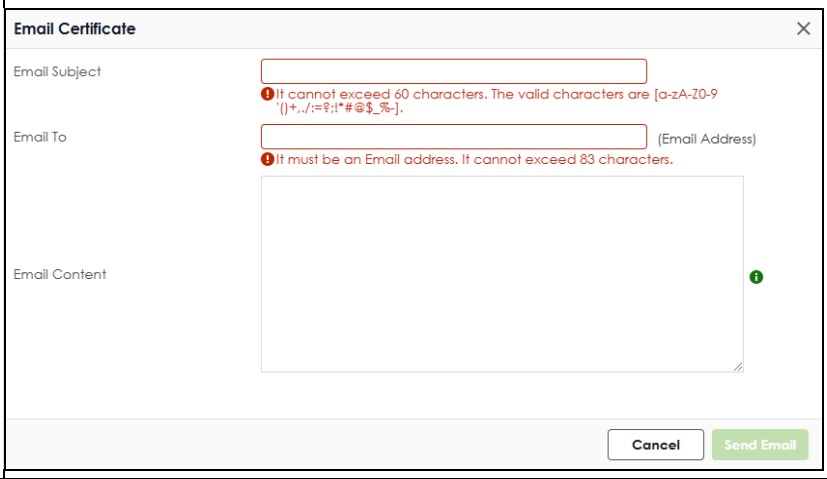
LABEL	DESCRIPTION
Name	This is the name of the profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. These are valid, unique profile names: • MyProfile • mYProfile • Mymy12_3-4 These are invalid profile names: • 1mYProfile • My Profile • MyProfile? • Whatalongprofilename123456789012
Description	Enter additional information about this SSL Inspection entry. You can enter up to 60 characters (0-9a-zA-Z'()+:=?;!*#@$_%-"). The first character must be a letter.
CA Certificate	This contains the default certificate and the certificates created in **Object > Certificate > My Certificates**. Choose the certificate for this profile.
Email	Use this button to have the Zyxel Device send the selected certificate to a valid email address. Click a certificate's row to select it and click **Email** to have the Zyxel Device mail that certificate. The following screen displays. 
Email Subject	Enter a email subject text with 1-60 characters. It may consist of letters, numbers, and the following special characters: '()+,./:=?;!*#@$%-
Email to	Enter up to 83 characters for the email address of the receiver
Email 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.
Cancel	Click this to send the email to the email address you configured.
Send Email	Click this to close the screen.
SSL/TLS version	
Minimum Support	SSL / TLS connections using versions lower than this setting are blocked.

Table 207 Security Service > SSL Inspection > Profile > Add/Edit (continued)

LABEL	DESCRIPTION
Log	These are the log options for unsupported traffic that matches traffic bound to this policy: • **no**: Select this option to have the Zyxel Device create no log for unsupported traffic that matches traffic bound to this policy. • **log**: Select this option to have the Zyxel Device create a log for unsupported traffic that matches traffic bound to this policy • **log alert**: An alert is an emailed log for more serious events that may need more immediate attention. They also appear in red in the **Log & Report > Log/Events** screen. Select this option to have the Zyxel Device send an alert for unsupported traffic that matches traffic bound to this policy.
Unsupported suit	
Action	SSL Inspection supports the AES cipher suites: Select to **pass** or **block** unsupported traffic (such as other cipher suites, compressed traffic, client authentication requests, and so on) that matches traffic bound to this policy here.
Log	These are the log options for unsupported traffic that matches traffic bound to this policy: • **no**: Select this option to have the Zyxel Device create no log for unsupported traffic that matches traffic bound to this policy. • **log**: Select this option to have the Zyxel Device create a log for unsupported traffic that matches traffic bound to this policy • **log alert**: An alert is an emailed log for more serious events that may need more immediate attention. They also appear in red in the **Log & Report > Log/Events** screen. Select this option to have the Zyxel Device send an alert for unsupported traffic that matches traffic bound to this policy.
Untrusted cert chain	
Action	A certificate chain is a certification process that involves the following certificates between the SSL/TLS server and a client. A certificate chain will fail if one of the following certificates is not correct. • A certificate owned by a user • The certificate signed by a certification authority • A root certificate Select to **pass**, **inspect**, or **block** an untrusted certification chain.
Log	These are the log options for unsupported traffic that matches traffic bound to this policy: • **no**: Select this option to have the Zyxel Device create no log for unsupported traffic that matches traffic bound to this policy. • **log**: Select this option to have the Zyxel Device create a log for unsupported traffic that matches traffic bound to this policy • **log alert**: An alert is an emailed log for more serious events that may need more immediate attention. They also appear in red in the **Log & Report > Log/Events** screen. Select this option to have the Zyxel Device send an alert for unsupported traffic that matches traffic bound to this policy.
Apply	Click **Apply** to save your settings to the Zyxel Device, and return to the profile summary page.
Reset	Click **Reset** to return to the profile summary page without saving any changes.

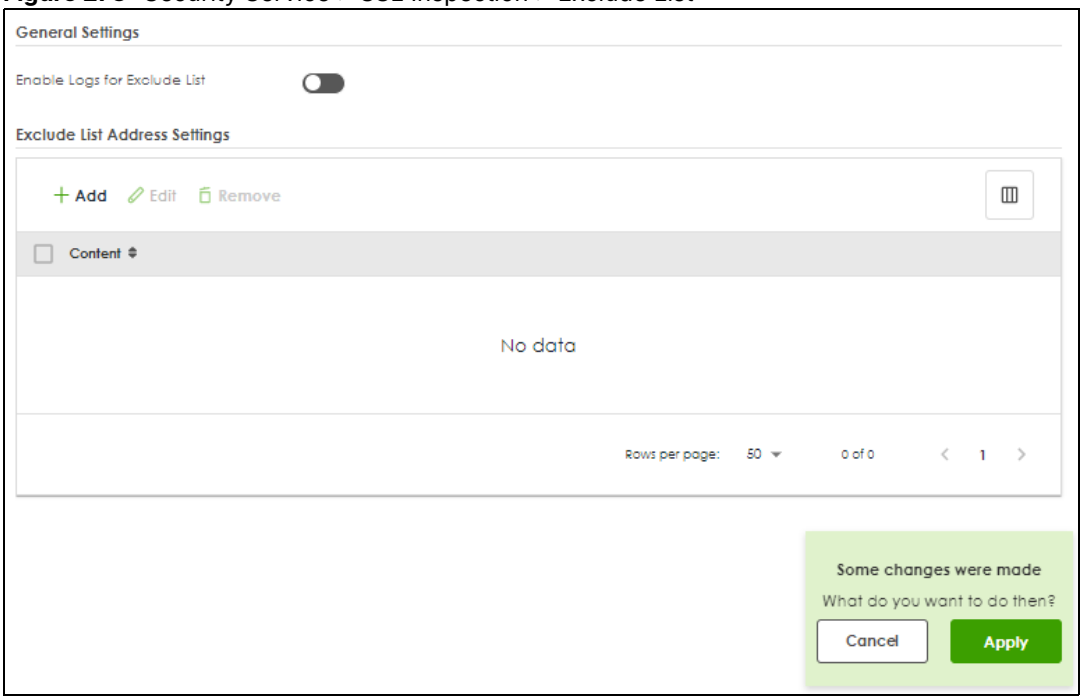
26.3 Exclude List Screen

There may be privacy and legality issues regarding inspecting a user's encrypted session. The legal issues may vary by locale, so it's important to check with your legal department to make sure that it’s OK to intercept SSL traffic from your Zyxel Device users.

To ensure individual privacy and meet legal requirements, you can configure an exclusion list to exclude matching sessions to destination servers. This traffic is not intercepted and is passed through uninspected.

Click **Security Services > SSL Inspection > Exclude List** to display the following screen. Use **Add** to put a new item in the list or **Edit** to change an existing one or **Remove** to delete an existing entry.

Figure 273 Security Service > SSL Inspection > Exclude List



The following table describes the fields in this screen.

Table 208 Security Service > SSL Inspection > Exclude List

LABEL	DESCRIPTION
General Settings	
Enable Logs for Exclude List	Click this to create a log for traffic that bypasses SSL Inspection.
Exclude List Address Settings	Use this part of the screen to create, edit, or delete items in the SSL Inspection exclusion list.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select a row and click this to delete it.
Content	SSL traffic to a server to be excluded from SSL Inspection is identified by its certificate. Identify the certificate in one of the following ways: • The Common Name (CN) of the certificate. The common name of the certificate can be created in the **System > Certificate > My Certificates** screen. • Type an IPv4 address. For example, type 192.168.1.35 • Type an IPv4 in CIDR notation. For example, type 192.168.1.1/24 • Type an IPv4 address range. For example, type 192.168.1.1-192.168.1.35 • Type an email address. For example, type abc@zyxel.com.tw • Type a DNS name or a common name (wildcard char: '*', escape char: '\'). 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.

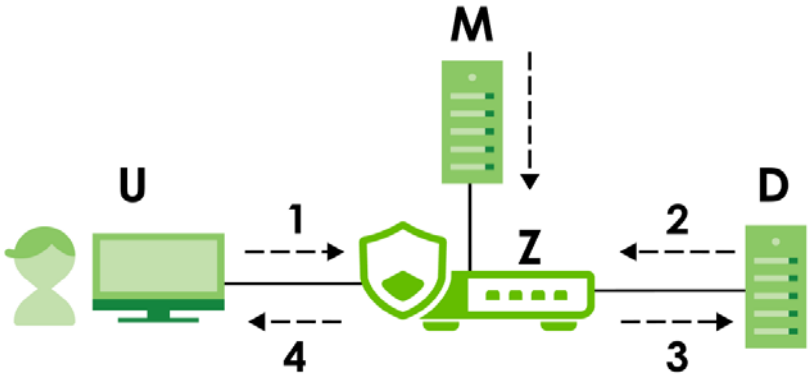
Table 208 Security Service > SSL Inspection > Exclude List (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your settings to the Zyxel Device.
Cancel	Click **Cancel** to return to the profile summary page without saving any changes.

26.4 Certificate Update Screen

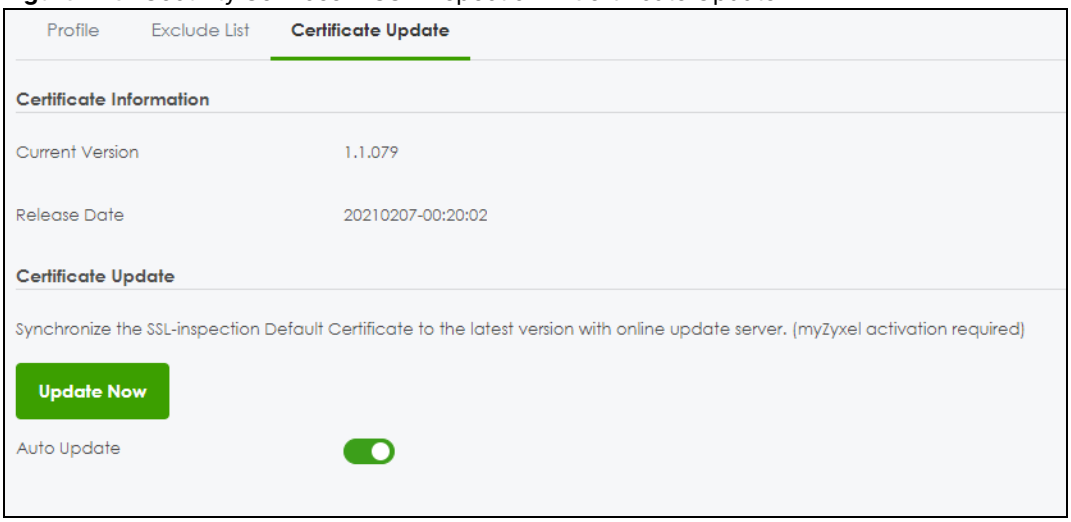
Use this screen to update the latest certificates of servers using SSL connections to the Zyxel Device network. User **U** sends an SSL request to destination server **D** (**1**), via the Zyxel Device, **Z**. D replies (**2**); **Z** intercepts the response from **D** and checks if the certificate has been previously signed. **Z** then replies to **D** (**3**) and also to **U** (**4**). D's latest certificate is stored at myZyxel (**M**) along with other server certificates and can be downloaded to the Zyxel Device.

Figure 274 SSL Inspection Certificate Update Overview



Click **Security Services > SSL Inspection > Certificate Update** to display the following screen.

Figure 275 Security Services > SSL Inspection > Certificate Update



The following table describes the fields in this screen.

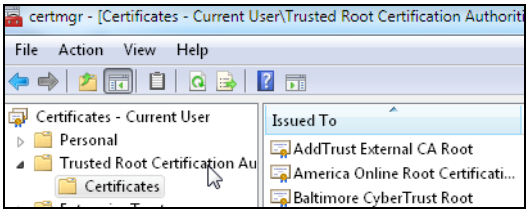
Table 209 Security Services > SSL Inspection > Certificate Update

LABEL	DESCRIPTION
Certificate Information	
Current Version	This displays the current certificate set version.
Released Date	This field displays the date and time the current certificate set was released.
Certificate Update	You should have Internet access and have activated SSL Inspection on the Zyxel Device at NCC.
Update Now	Click this button to download the latest certificate set (Windows, MAC OS X, and Android) from the Zyxel cloud server and update it on the Zyxel Device.
Auto Update	Select this to automatically have the Zyxel Device update the certificate set when a new one becomes available on the Zyxel cloud server.
Apply	Click **Apply** to save your settings to the Zyxel Device.
Cancel	Click **Cancel** to return to the profile summary page without saving any changes.

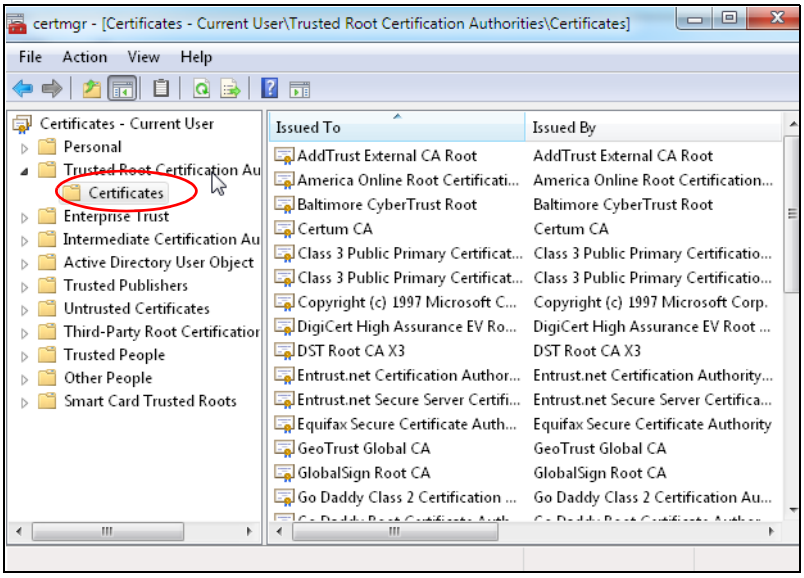
26.5 Install a CA Certificate in a Browser

Certificates used in SSL Inspection profiles should be installed in user web browsers. Do the following steps to install a certificate in a computer with a Windows operating system (PC). First, save the certificate to your computer.

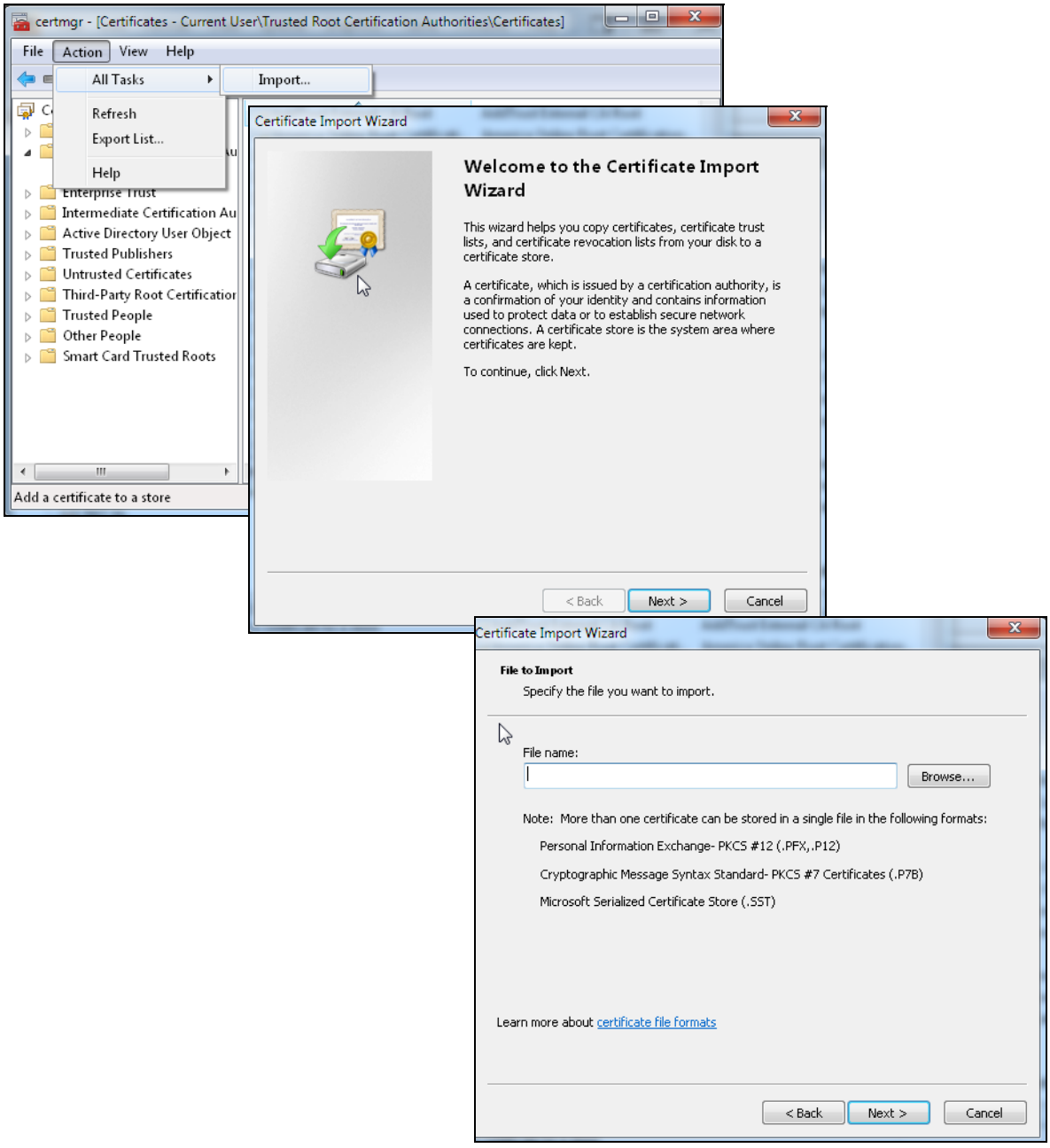
1 Run the certificate manager using certmgr.msc.



2 Go to **Trusted Root Certification Authorities > Certificates**.



3 From the main menu, select **Action > All Tasks > Import** and run the **Certificate Import Wizard** to install the certificate on the PC.



26.5.0.1 Firefox Browser

If you're using a Firefox browser, in addition to the above you need to do the following to import a certificate into the browser.

Click **Tools > Options > Advanced > Encryption > View Certificates**, click **Import** and enter the filename of the certificate you want to import. See the browser's help for further information.

CHAPTER 27
External Block Lists

27.1 Overview

Use these screens to use block IP, FQDN or URL list entries stored in a file on a web server that supports HTTP or HTTPS and is reachable from the Zyxel Device. The Zyxel Device will bypass checking by this feature (if enabled) and block incoming and outgoing packets from the block list entries in this file. In this way, different Zyxel Devices can use the same block list.

The external block list file must be in text format (*.txt) with each entry separated by a new line.

27.1.1 IP Reputation External Block List Screen

External block list entries can consist of single IPv4 / IPv6 IP addresses, IP address ranges, CIDR (Classless Inter-Domain Routing entries such as 192.168.1.1/24, 2001:7300:3500::1/64. These are some examples for your reference only:

- Single IP 4.4.4.4
- CIDR 192.168.1.0/32
- IP range (1.2.3.4-1.2.3.100)

If the external block list file contains any invalid entries, the Zyxel Device will not use the file.

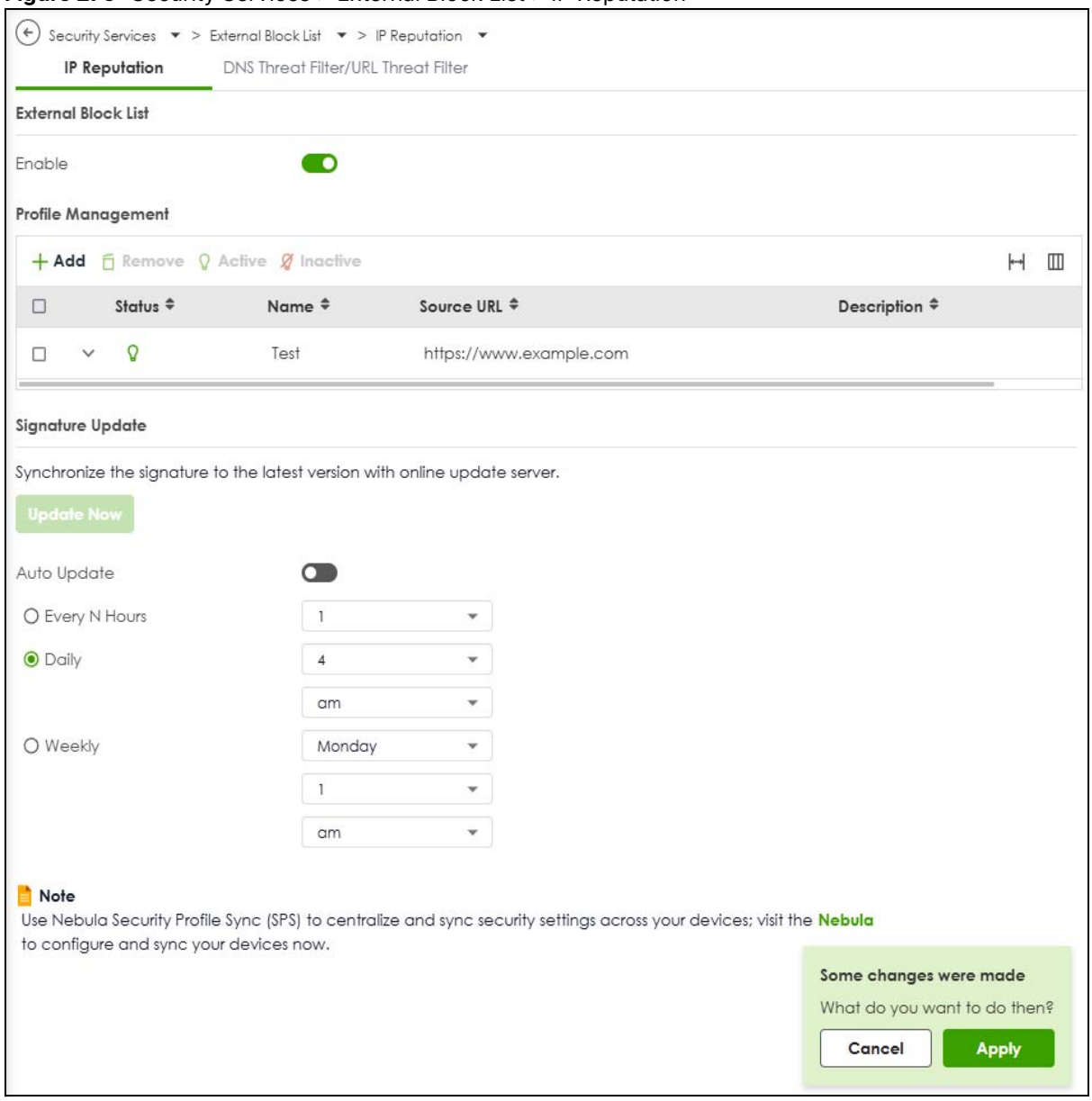
The external block list file can contain up to 50,000 entries. A warning message displays when the maximum is reached.

Go to **Security Services > External Block List > IP Reputation** to display the following screen.

If a license has expired, you will see a reminder in this screen. You need to renew the license in order to keep using the feature. Click **Buy Now** to go to Marketplace to purchase a new license. Click **See Details** to go to the Zyxel web page to find more information on licenses for your Zyxel Device.



Figure 276 Security Services > External Block List > IP Reputation



The following table describes the labels in this screen.

Table 210 Security Services > External Block List > IP Reputation

LABEL	DESCRIPTION
Enable	Select this to have the Zyxel Device block packets that come from the listed addresses in the block list file on the server.
Profile Management	
Add	Click this to create a new IP reputation external block list profile entry.
Remove	Select an entry and click this to delete it.
Active	To turn off an entry, select it and click **Active**. The **Status** light changes accordingly.
Inactive	To turn off an entry, select it and click **Inactive**. The **Status** light changes accordingly.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.

Table 210 Security Services > External Block List > IP Reputation (continued)

LABEL	DESCRIPTION
Name	Enter an identifying name for the block list file. You can use alphanumeric and ()+/ :=?!*#@$_%- characters, and it can be up to 60 characters long.
Source URL	Enter the exact file name, path and IP address of the server containing the block list file. For example, http://172.16.107.20/blocklist-files/myip-ebl.txt The server must be reachable from the Zyxel Device.
Description	Enter a description of the block list file. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
Edit	Select an entry and click this icon to modify it.
Remove	Select an entry and click this icon to delete it.
Save Changes	Click this icon to save the changes in this row.
Cancel Changes	Click this icon to cancel the changes in this row.
Signature Update	New IP reputation signatures can be downloaded to the Zyxel Device periodically if you have subscribed for the IP reputation signatures service. You need to create a Zyxel account, register your Zyxel Device and then subscribe for IP reputation service in order to be able to download new signatures (see the **Registration** screens). Schedule signature updates for a day and time when your network is least busy to minimize disruption to your network.
Update Now	Click this to have the Zyxel Device immediately check for new signatures. If new signatures are found, they are then downloaded to the Zyxel Device.
Auto Update	Click this to have the Zyxel Device automatically check for new signatures regularly at the time and day specified. You should select a time when your network is not busy for minimal interruption.
Every N Hours	Select this to have the Zyxel Device check for new signatures every specified number of hours (N).
Daily	Select this to have the Zyxel Device check for new signatures every day at the specified time (**am**/**pm**). The time format is the 12 hour clock.
Weekly	Select this option to have the Zyxel Device check for new signatures once a week on the day and at the time (**am**/**pm**) specified.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

27.1.2 DNS / URL Threat Filter External Block List Screen

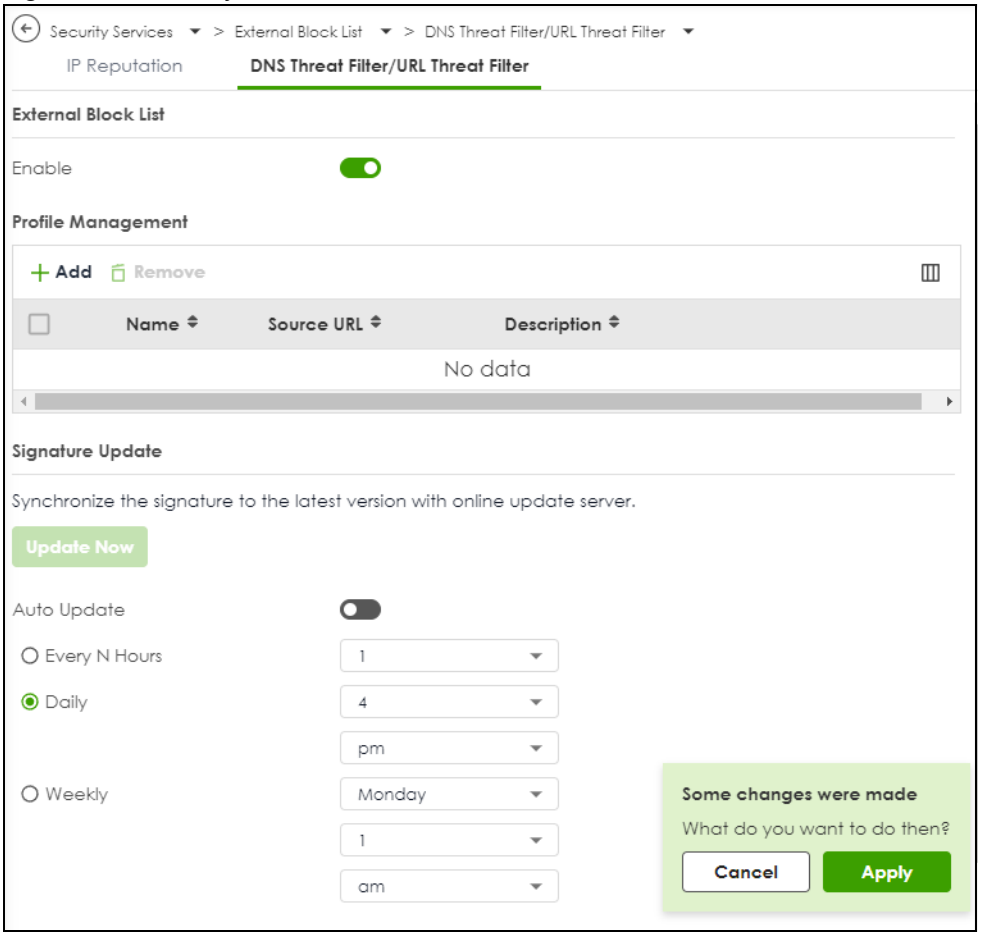
Use this screen to use block list entries stored in a file on a web server that supports HTTP or HTTPS. The Zyxel Device will block incoming and outgoing packets from the block list entries in this file. Supported formats are:

- hostname (www.google.com)
- URL http - check full url (http://xxx.yyy.zzz/qqq/wwww)
- URL https - only check hostname (https://xxx.)

Please note the following:

- The external block list file must be in text format (*.txt) with each entry separated by a new line.
- External block list entries can consist of a complete URL or a hostname and may contain wildcards. There are some examples for your reference only:
  - https://www.zyxel.com/products_services/smb.shtml?t=s (complete URL)
  - www.zyxel.com (hostname)
  - *.zyxel.* (hostname with wildcards)
- If the external block list file contains any invalid entries, the Zyxel Device will not use the file.
- The external block list file can contain up to 50,000 entries. A warning message displays when the maximum is reached.

Figure 277 Security Services > External Block List > DNS / URL Threat Filter



The following table describes the labels in this screen.

Table 211 Security Services > External Block List > DNS / URL Threat Filter

LABEL	DESCRIPTION
Enable	Select this check box to have the Zyxel Device automatically block packets that come from the listed addresses in the block list file on the server.
Profile Management	
Add	Click this to create a new DNS/URL threat filter external block list entry.
Remove	Select an entry and click this to delete it.

Table 211 Security Services > External Block List > DNS / URL Threat Filter (continued)

LABEL	DESCRIPTION
Name	Enter an identifying name for the block list file. You can use alphanumeric and ()+/ :=?!*#@$_%- characters, and it can be up to 60 characters long.
Source	Enter the exact file name, path and IP address of the server containing the block list file. For example, http://172.16.107.20/blocklist-files/myip-ebl.txt The server must be reachable from the Zyxel Device.
Description	Enter a description of the block list file. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
Edit	Select an entry and click this icon to modify it. 
Remove	Select an entry and click this icon to delete it. 
Save Changes	Click this icon to save the changes in this row. 
Cancel Changes	Click this icon to cancel the changes in this row. 
Signature Update	New IP reputation signatures can be downloaded to the Zyxel Device periodically if you have subscribed for the IP reputation signatures service. You need to create a Zyxel account, register your Zyxel Device and then subscribe for IP reputation service in order to be able to download new signatures (see the **Registration** screens). Schedule signature updates for a day and time when your network is least busy to minimize disruption to your network.
Update Now	Click this to have the Zyxel Device immediately check for new signatures. If new signatures are found, they are then downloaded to the Zyxel Device.
Auto Update	Click this to have the Zyxel Device automatically check for new signatures regularly at the time and day specified. You should select a time when your network is not busy for minimal interruption.
Every N Hours	Select this to have the Zyxel Device check for new signatures every specified number of hours (N).
Daily	Select this to have the Zyxel Device check for new signatures every day at the specified time (**am**/**pm**).
Weekly	Select this option to have the Zyxel Device check for new signatures once a week on the day and at the time (**am**/**pm**) specified.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

CHAPTER 28
User & Authentication

28.1 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 28.1.4 on page 463) provides a summary of all user accounts.
- The **Group** screen (see Section 28.1.6 on page 471) 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 28.1.7 on page 473) 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.

28.1.1 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 and application patrol, 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 212 Types of User Accounts

TYPE	ABILITIES	LOGIN METHOD(S)
Local Administrator		
admin	Change the Zyxel Device settings (web, CLI)	WWW, SSH, FTP, Console
viewer	Look at the Zyxel Device settings (web configurator, CLI) Perform basic diagnostics (CLI)	WWW, SSH, Console
User		
user	Access network services	WWW
External User (ext-user)	A user that is authenticated using an AD, LDAP or RADIUS authentication server.	WWW
External Group User (ext-user)	A user group whose members are authenticated using an AD, LDAP or RADIUS authentication server.	WWW

Table 212 Types of User Accounts (continued)

TYPE	ABILITIES	LOGIN METHOD(S)
Captive Portal Click to Continue User (ctc-user)	A user who accesses the network through the captive portal using the Click to Continue sign-in method, which allows access without authentication.	Captive Portal - Click to Continue
NID FS User (nidfs-user)	A user who is authenticated through NID FS.	NID FS

External 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 212 on page 459) 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.

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.

Reserved Accounts

The following accounts are autocratically created or reserved user names.

- admin

- ad-users
- ldap-users
- radius-users
- root
- debug
- shutdown
- support
- ctc-users (Captive Portal)
- ncas-users (Nebula Cloud Authentication)
- nidfs-users (Nebula IDentity Federation Service) users

RADIUS, AD, LDAP Login Authentication Timeout

Login With RADIUS:

- If the server replies with a specific attribute (for example, session-timeout or a vendor-specific attribute), the Zyxel Device will apply the server's value.
- If the server does not provide a specific attribute, the Zyxel Device will instead use the values from the radius-users settings.

  (Standard) session-timeout

  0 = unlimited

  1 ~ 31536000 seconds

  (Standard) idle-timeout

  0 = unlimited

  1 ~ 65535 seconds

Login With AD/LDAP:

The Zyxel Device will take the values from ad-users and ldap-users settings.

28.1.2 NCAS

NCAS (Nebula Cloud Authentication Server) is a Nebula cloud service to authenticate Nebula-managed devices and services only. All user accounts are managed centrally through Nebula. NCAS allows you to store and manage user credentials in the Nebula cloud without having to deploy your own authentication server.

If there is no response from NCAS for over 15 seconds, then NCAS is considered disconnected. Applications which were already authenticated may continue, but new requests must wait until the connection to NCAS is restored.

NCAS authentication methods are:

- Email / Password
- Two-Factor Authentication
- Passkey

The number of users that can be managed through NCAS depends on the NCC license you have. At the time of writing, these are the limits:

- Nebula Base Pack (default, free): Up to 50 users.
- Nebula Plus Pack: Up to 100 users.
- Nebula Professional Pack: No limit on users.

28.1.2.1 NCAS in Nebula

Configure NCAS in the following Nebula menus:

- **Configure > Nebula cloud authentication server**
- **Organization-wide manage > Nebula cloud authentication server**

28.1.2.2 NCAS in the Web Configurator

Configure NCAS in the following Web Configurator menus:

- For Captive portal, use the **Sign-in With** field in **Captive Portal > Authentication Policy > Add**
- For SSL VPN, go to the **Primary Server** field in **VPN > SSL VPN** (Authentication)

Note: NID FS is set up automatically in NCC for NCAS.

28.1.3 NID FS

Federation allows one organization or system to trust another organization or system to authenticate users. An Identity Federation Service (IFS) is a system that lets one identity be used across multiple services. There is no need to set up an IdP (Identity Provider) individually for each service with separate user names and passwords for each application.

NID FS (Nebula IDentity Federation Service) is IFS implemented by Nebula.

You should already have an account with an IdP such as Google Workspace or Microsoft Entra ID. When a user logs into an application such as Captive Portal or SSL VPN, the IdP authenticates the user using OIDC. The Zyxel Device receives a trusted identity token from the IdP to authorize application access. The application then grants access without asking for a separate account.

Note: You need a Nebula Pro license to use NID FS.

If the Nebula Pro license expires and reverts to a Nebula Base license, then all NID FS settings are kept, but you can't enter the **Organization-wide manage > Nebula identity federation service** page in Nebula until you buy a Nebula Pro license.

28.1.3.1 NID FS in Nebula

Configure NID FS in Nebula as follows:

- Create an NID FS in **Organization-wide manage > Nebula identity federation service**
- Bind IdPs to the NID FS in **User privileges -> IDP Binding**

You then create services, such as Captive Portal and Remote Access VPN.

- For Captive Portal, go to **Site-wide > Configure > Firewall > Captive portal > Authentication policy > Add**.
- For SSL VPN, go to **Site-wide > Configure > Firewall > Remote access VPN.**

28.1.3.2 NID FS in the Web Configurator

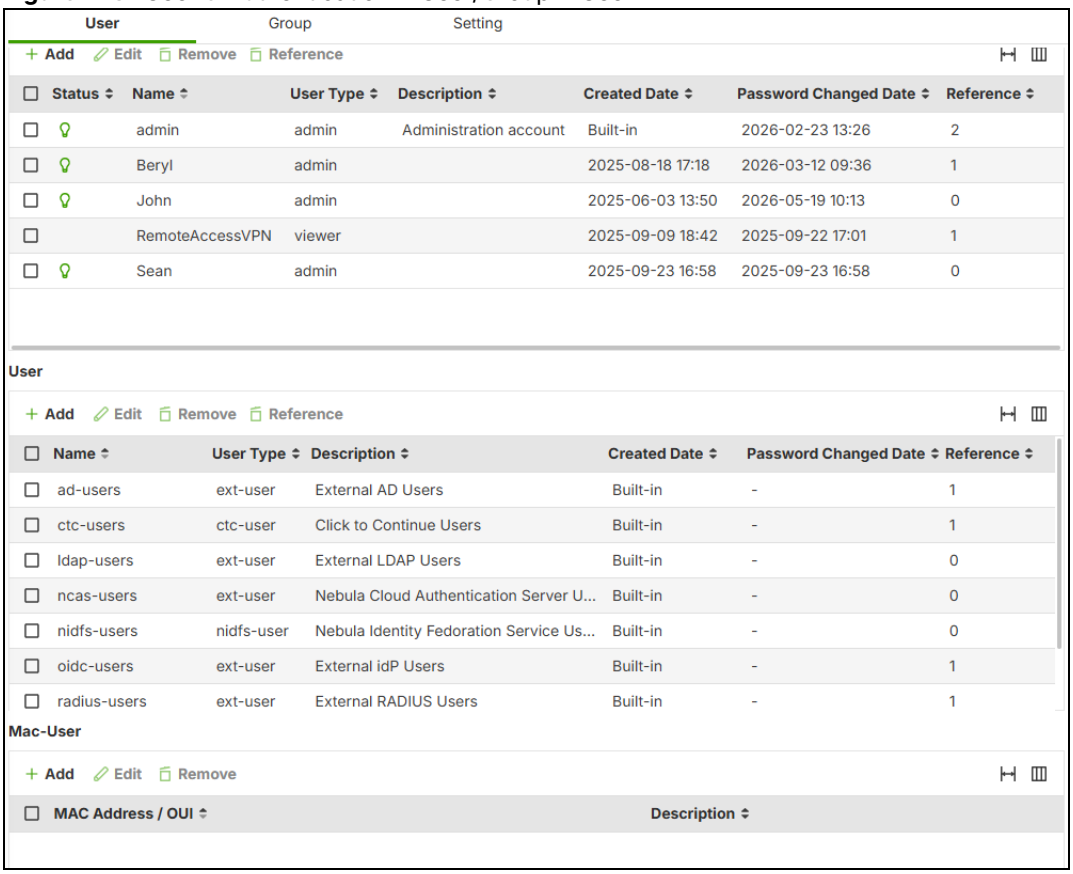
Configure NID FS in the Web Configurator as follows:

- For Captive portal, use the **Sign-in With** field in **Captive Portal > Authentication Policy > Add**.
- For SSL VPN, go to the **Primary Server** field in **VPN > SSL VPN** (**Authentication**).
- For the NID FS server certificate to redirect endpoint settings, go to **User & Authentication > User Authentication > Advanced**.
- To create an external group user mapping for specific users authenticated by NID FS, go to **U.ser & Authentication > User/Group > User > Edit**.

28.1.4 User/Group User Summary Screen

The **User** screen provides a summary of all user accounts. To access this screen, click **User & Authentication > User/Group > User**.

Figure 278 User & Authentication > User/Group > User



The following table describes the labels in this screen.

Table 213 User & Authentication > 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.

Table 213 User & Authentication > User/Group > User (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.
Reference	Select an entry and click **Reference** to view which service is currently using it.
Local Administrator	Use this table to view and configure the Zyxel Device admin accounts.
Status	This shows whether the local administrator is enabled or disabled.
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. **Viewer** accounts are users that can just look at the configuration of the Zyxel Device.
Description	This field displays the description for each user.
Created Date	This field displays the date the account was created.
Password Changed Date	This field displays the last time the user changed the account password.
Reference	This displays the number of times an object reference is used in a profile.
User	Use this table to configure the Zyxel Device: • User accounts. • Ext-user accounts.
Name	This field displays the user name of each user.
User Type	This field displays the types of user accounts the Zyxel Device uses: • **user** - this user has access to the captive portal or remote access VPN services through the Zyxel Device. • **ext-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See External User Accounts on page 460 for more information about this type. • **ctc-user** - this user has access to the Zyxel Device through the captive portal using the 'click to continue' sign-in method, which allows access without authentication. • **nidfs-user** - this user has access to the Zyxel Device after authenticating through NID FS.
Description	This field displays the description for each user.
Created Date	This field displays the date the account is created.
Password Changed Date	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.
Mac User	In **Wireless > WLAN Settings > SSID Settings > Advanced Mode > Edit**, if you configure **MAC-based Authentication** with **Internal Authentication Server** and set the **Authentication Server** to **local**, then you need to enter a Mac User here for successful authentication. See Section 29.9.2 on page 538 for more information.
MAC Address /OUI	This displays a valid MAC address or OUI (Organizationally Unique Identifier) of the device that this user will use for authentication. This is used in conjunction with login credentials.
Description	This displays some text to identify this user.

28.1.5 User Add/Edit Screen

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

28.1.5.1 Rules for User Names

Enter a user name from 1 to 30 characters.

The user name can only contain the following characters: [0-9][a-z][A-Z][(){}<>^`+/:!*#@&=$\.~%;-].

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

- User names are case-sensitive. If you enter a user 'bob' but use 'BOB' when connecting via CIFS or FTP, it will use the account settings used for 'BOB' not ‘bob’.
- User names have to be different than user group names.
- The Zyxel Device will automatically rename existing user accounts named “support” to “supportx”, where x is a unique number, during Nebula configuration provisioning. The account name “support” is reserved for Nebula use and is only managed through Nebula. The Nebula support account is only visible through Nebula. In the Zyxel Device you will not see the Nebula-managed support account, but you can see the renamed local version (for example, support1).

28.1.5.2 Rules for Passwords

Enter a password from 4-63 characters.

The name can only contain the following characters: [0-9][a-z][A-Z][(){}<>^`+/:!*#@&=$\.~%;-].

It cannot contain these characters: ?|'",[] and spaces.

The first character must be alphabetical [a-z][A-Z], an underscore [_], or a dash [-].

To access the he **User Add/Edit General** screen, go to the **User** screen, and click either the **Add** icon or an **Edit** icon.

Figure 279 User & Authentication > User/Group > User > Add/Edit (Local Administrator)

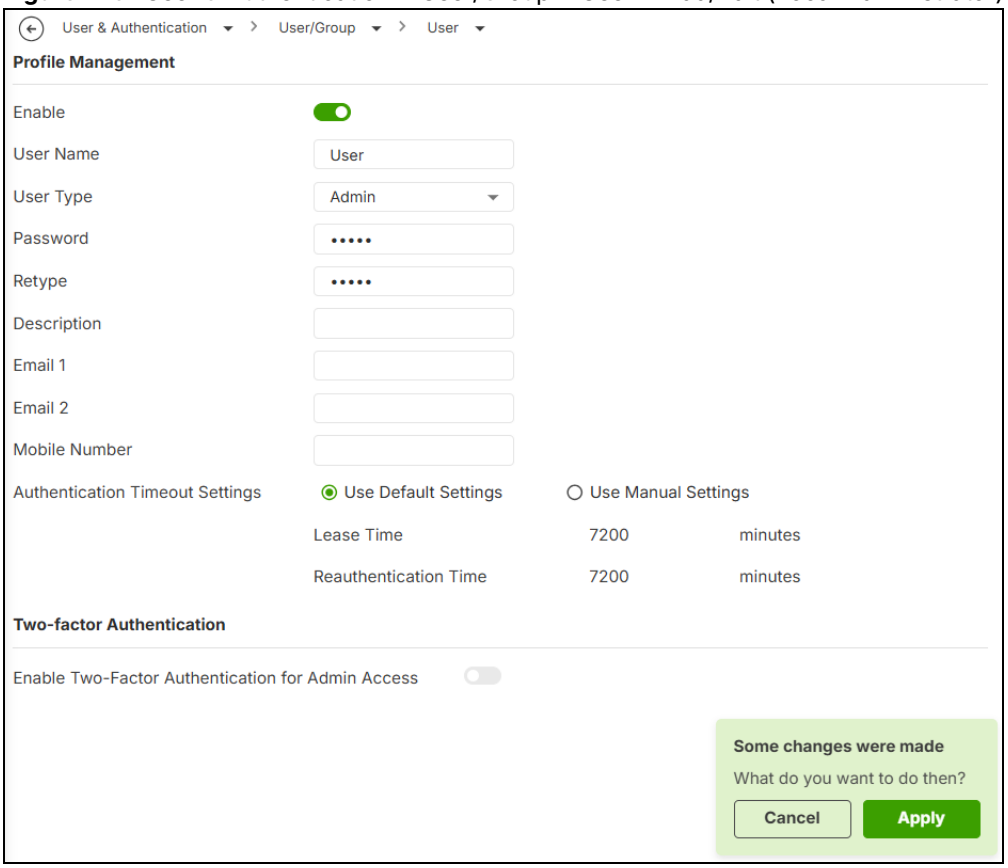


Figure 280 User & Authentication > User/Group > User > Add/Edit (Local Administrator with 2FA)

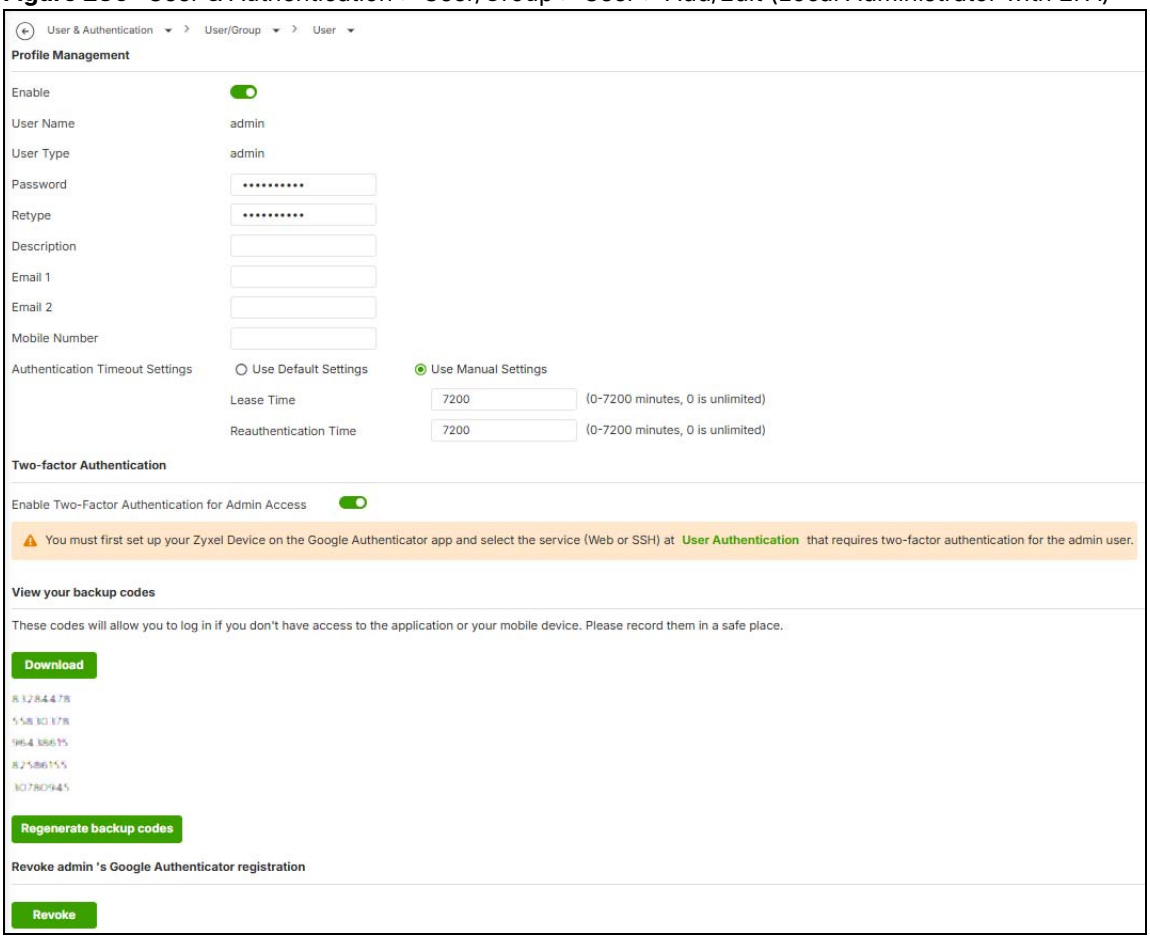


Figure 281 User & Authentication > User/Group > User > Add/Edit (User)

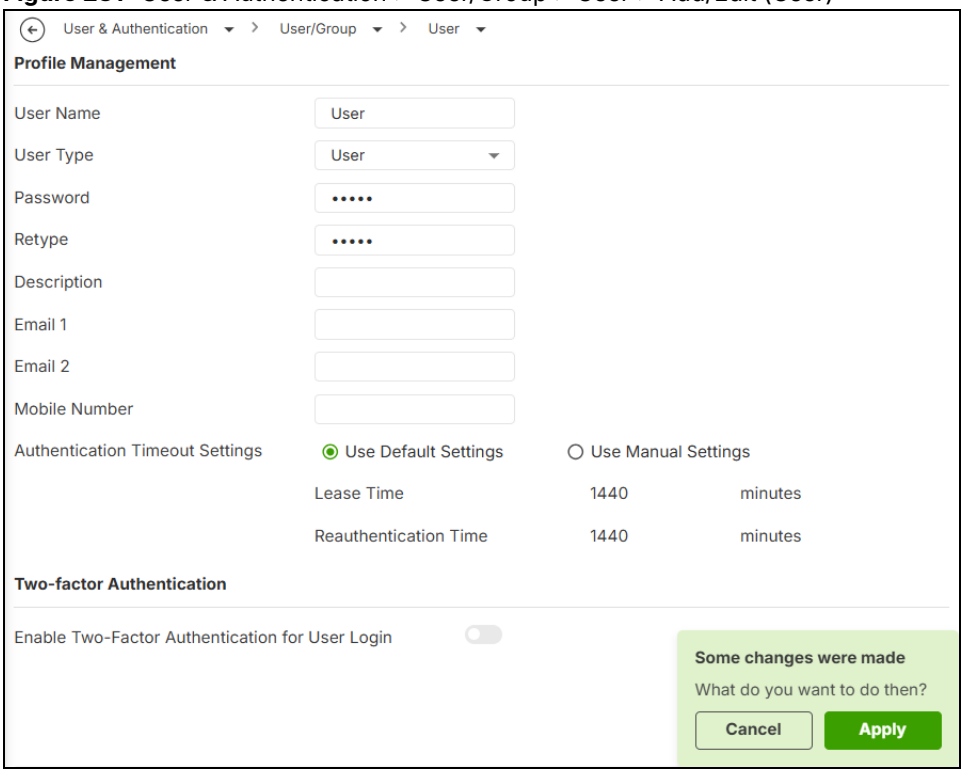


Figure 282 User & Authentication > User/Group > User > Add/Edit (Mac-User)

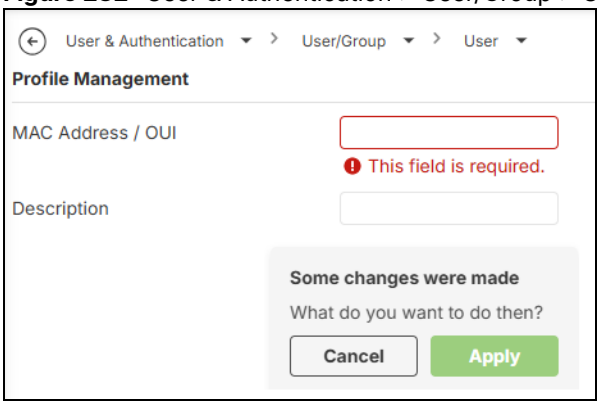


Figure 283 User & Authentication > User/Group > User > Add/Edit (External Group User - RADIUS or OIDC)

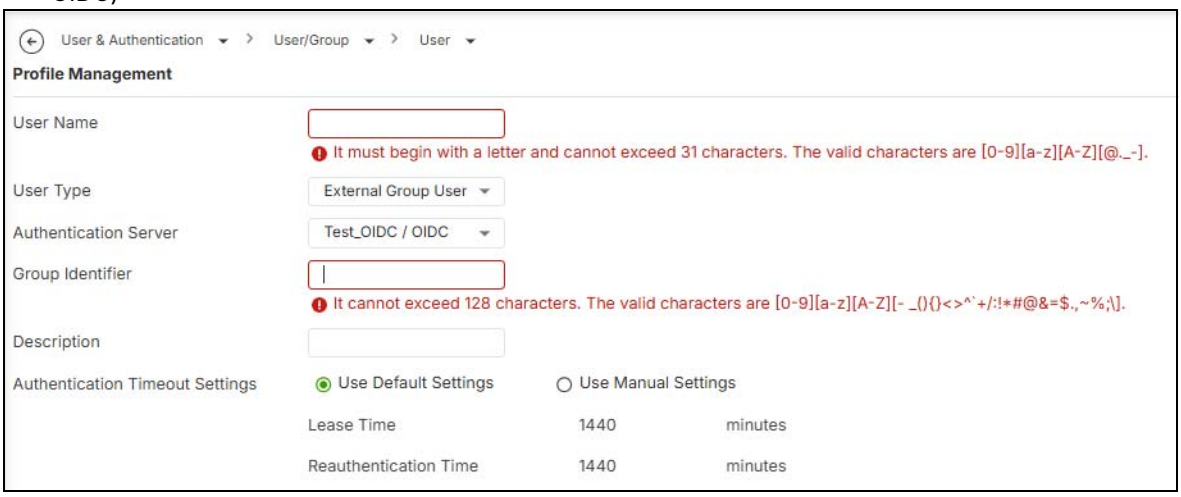


Figure 284 User & Authentication > User/Group > User > Add/Edit (External Group User - AD or LDAP)

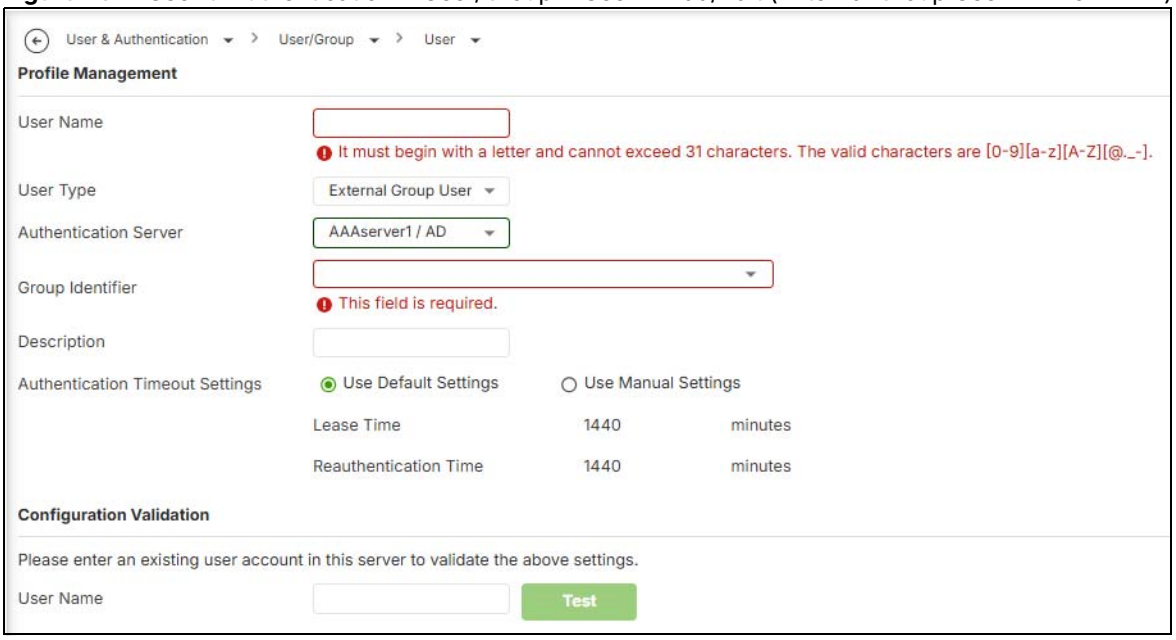
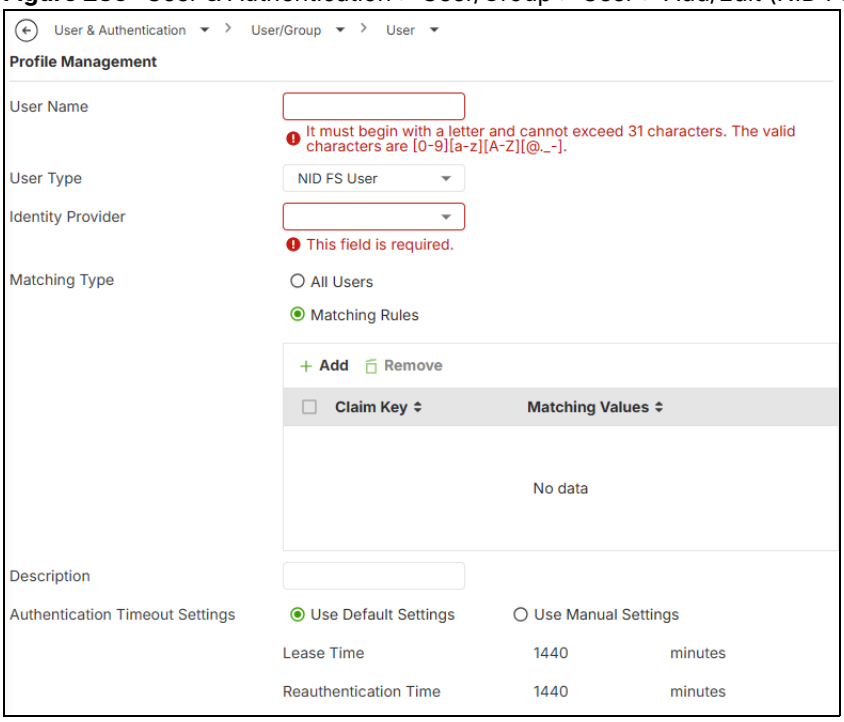


Figure 285 User & Authentication > User/Group > User > Add/Edit (NID FS User)



The following table describes the labels in this screen.

Table 214 User & Authentication > User/Group > User > Add/Edit

LABEL	DESCRIPTION
Enable	Click the switch to the right to enable the local administrator. Click the switch to the left to disable the local administrator. A disabled administrator cannot log in to the Zyxel Device. This feature is available only to local administrators with an **admin** user type. You can also disable the built-in the local administrator named **admin**. At least one administrator must remain enabled on the Zyxel Device. Note: Be careful not to disable your own account, or you will be unable to log into the Zyxel Device.
User Name	Type the user name for this user account. You may use 1-30 alphanumeric characters, periods (.), at (@), 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 28.1.5.1 on page 464.
User Type	Select the type of user account the Zyxel Device uses for the **Local Administrator** account from the drop-down list box. • **Admin**- this user can configure the Zyxel Device settings using the web configurator or CLI. • **Viewer**- this user can only view the Zyxel Device settings using the web configurator and perform basic diagnostics for troubleshooting using the command line interface (CLI). Select the type of user account the Zyxel Device uses for the **User** account from the drop-down list box: • **User** - this user has access to the captive portal or remote access VPN services through the Zyxel Device. • **External Group User** - this user account is maintained on a remote server, such as RADIUS or LDAP. See External User Accounts on page 460 for more information about this type. • **NID FS User** - this user has access to the Zyxel Device after authenticating through NID FS.

Table 214 User & Authentication > User/Group > User > Add/Edit (continued)

LABEL	DESCRIPTION
Identity Provider	This field is available if you select **NID FS User** as the **User Type**. This should be configured in NID FS in Nebula that manages users' credentials and pushed to the Zyxel Device. Select the Identity Provider specified in NID FS in Nebula. This is required. It must match the IdP name claim extracted from the incoming OIDC ID token in order to proceed with the login user to be assigned the user role.
Matching Type	Select **All users** to include all users in the selected Identity Provider in this profile. It applies the user role to the login user unconditionally, as long as IdP provider verification passes. No further claim validation is required Select **Matching rules** to include users whose claim keys match the specified values in the selected Identity Provider in this profile. Click **+Add** to create a rule. A **Claim Key** is the configuration path used to locate the target value within the OIDC ID token. It can have up to 3 hierarchical levels of nested JSON data using dots ('.') as segment delimiters. This is mandatory. Note: At the time of writing, you can only create one rule. A **Matching Value** is the expected value or values to match against the content extracted by the **Claim Key**. This is mandatory. You can set up to 5 values for one claim key. The runtime claim value can match any of the 5 values for the login user to be assigned the user role.
Password	This field is not available if you select the **External User** type. Enter a password consisting of 4 to 63 characters for this user account, including [0-9] [a-z] [A-Z] [(){}<>^`+/:!*#@&=$.~%;-]. If the **Password Policy** is enabled in the **User & Authentication** > **User/Group** > **Setting** screen, the password criteria might be different. See Section 28.1.7.1 on page 476 for more information.
Retype	This field is not available if you select the **External User** type.
Email 1, Email 2	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 [+*#()-].
Authentication Server	This field is available when you choose **External Group User**. Select the AD, LDAP, RADIUS or OIDC server that authenticates this external group.
Group Identifier	An authentication server uses attributes to store information about users, including their group memberships. For example, the attribute memberOf may contain values such as Sales, RD, and Management, which represent the groups a user belongs to. On the Zyxel Device, you can create ext-group-user user objects that correspond to these server groups. Each object uses a **Group Identifier**, which is the value that identifies the group on the authentication server (for example, Sales, RD, or Management). These are example values of attributes (**Group Identifier**). • CN=Sales,OU=Groups,DC=company,DC=com • CN=RD,OU=Groups,DC=company,DC=com • CN=Management,OU=Groups,DC=company,DC=com Enter the **Group Identifier** (the group value used on the authentication server) that corresponds to this user group.
Description	Enter the description of each user, if any. You can use 1 to 512 single-byte characters. Leading spaces and line breaks are not allowed.
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 214 User & Authentication > User/Group > User > Add/Edit (continued)

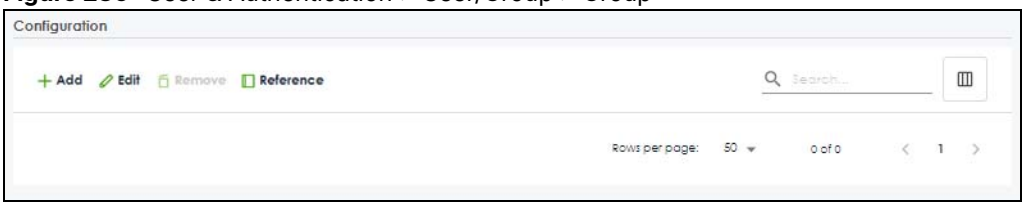
LABEL	DESCRIPTION
Lease Time	If you select **Use Default Settings** in the **Authentication Timeout Settings** field, the default lease time is shown. If you select **Use Manual Settings**, you need to enter the number of minutes this user has to renew the current session before the user is logged out. 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 28.1.7 on page 473), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.
Reauthentication Time	If you select **Use Default Settings** in the **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.
Configuration Validation	This is only available for AD and LDAP servers that authenticate **External Group User**s.
User Name	Enter a user group account that exists on this server, then click the **Test** button to validate the configuration settings for the account.
Enable Two-Factor Authentication for Admin Access	Two-Factor Authentication requires double-layer security to access the Zyxel Device or a secured network behind the Zyxel Device using VPN. This field is available when you are editing a **Local Administrator** or **User** account. A **Local Administrator** may use two-factor authentication for Zyxel Device management using the Web Configurator or SSH. **A User** account may use two-factor authentication for remote VPN access using SSL VPN or IPSec VPN. After setting up Google Authenticator, backup codes are created. Backup codes are single-use codes that allow you to sign in when you cannot use your authenticator device. You may download backup codes and keep in a secure place. Because backup codes are single-use, you may regenerate a fresh set when you've already used existing ones, or if you suspect someone unauthorized might have seen or copied them. Existing backup codes are revoked when you regenerate codes. You may also revoke codes without regenerating new ones for a specific user, who for example, may no longer have permission to access a service.
Mac User	In **Wireless > WLAN Settings > SSID Settings > Advanced Mode > Edit**, if you configure **MAC-based Authentication** with **Internal Authentication Server** and set the **Authentication Server** to **local**, then you need to enter a Mac User here for successful authentication. See Section 29.9.2 on page 538 for more information.
MAC Address / OUI	Enter a valid MAC address or OUI (Organizationally Unique Identifier) of the device that this user will use for authentication. This is used in conjunction with login credentials.
Description	This field is optional. You may enter some text to identify this user.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

28.1.6 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 **User & Authentication > User/Group > Group**.

Figure 286 User & Authentication > User/Group > Group



The following table describes the labels in this screen. See Section 28.1.6.1 on page 472 for more information as well.

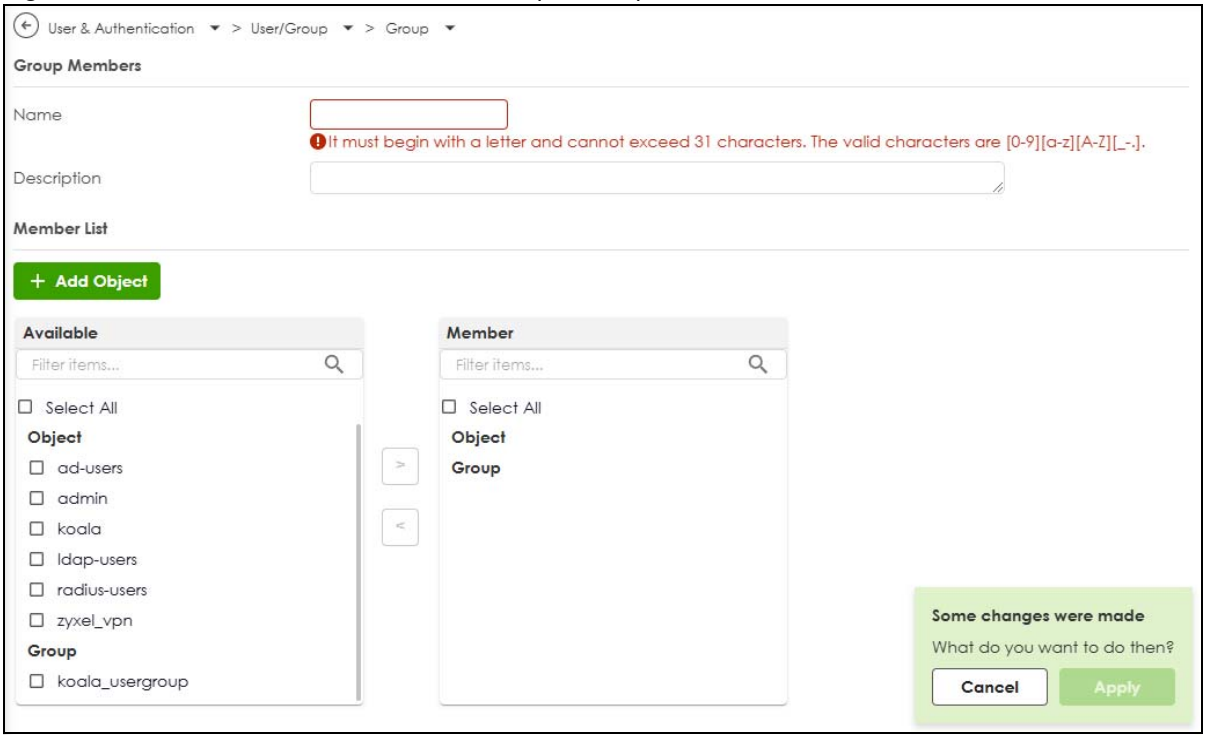
Table 215 User & Authentication > User/Group > Group

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.
Group Name	This field displays the name of each user group.
Description	This field displays the description for each user group.
Members	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.

28.1.6.1 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, and click either the **Add** icon or an **Edit** icon.

Figure 287 User & Authentication > User/Group > Group > Add



The following table describes the labels in this screen.

Table 216 User & Authentication > User/Group > Group > Add

LABEL	DESCRIPTION
Name	Type the name for this user group. You may use 2-30 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.
Add Object	Click this button to create a new user account.
Search	Type an item in the search box, then click this to display all user accounts in the table below according to the item you typed.
Select All	Select this to select all user accounts and user groups in the table.
Member List	This 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 items from the list on the left that you want to be members and move them to the list on the right. Move any members you do not want included to the list on the left.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

28.1.7 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 **User & Authentication > User/Group > Setting**.

Figure 288 User & Authentication > User/Group > Setting



The following table describes the labels in this screen.

Table 217 User & Authentication > User/Group > Setting

LABEL	DESCRIPTION
User Default 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.

Table 217 User & Authentication > User/Group > Setting (continued)

LABEL	DESCRIPTION
Edit row	Hover over an entry and click this icon to modify it. 
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 • **viewer** - this user can look at the configuration of the Zyxel Device • **user** - this user has access to the captive portal or remote access VPN services through the Zyxel Device. • **ext_user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See External User Accounts on page 460 for more information about this type. • **ext_group_user** - this is a group of **ext-user**s. See External User Accounts on page 460 for more information about this type. • **ctc_user** - this user has access to the Zyxel Device through the captive portal using the 'click to continue' sign-in method, which allows access without authentication. • **nidfs_user** - this user has access to the Zyxel Device after authenticating through NID FS.
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 **Edit row** button on their screen. If you allow access users to renew time automatically (see Section 28.1.7 on page 473), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires. To edit the 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.
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. To edit the reauthentication time, enter 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.
Miscellaneous Settings	
Auto renew lease time	Enable to let access users renew lease time automatically.
Admin User Type Login Security	
Force change password	Enable to force local admin type users to change their password after the specified period of time when they log into the Zyxel Device. If the **Password Policy** is enabled, you will then be required to change your password to comply with the new rules.
Period	Enter how often users must change their password when they log into the Zyxel Device. You can choose from once a day to once a year.
Password Policy	
Enabled	Enable this to set minimum length and character rules for the web configurator login password. The new password rules will take effect the next time you change your password.
Name	This field displays the user name of the account.
Setting	Click this to set minimum length and character rules for the web configurator login password. See Section 28.1.7.1 on page 476 for more information.

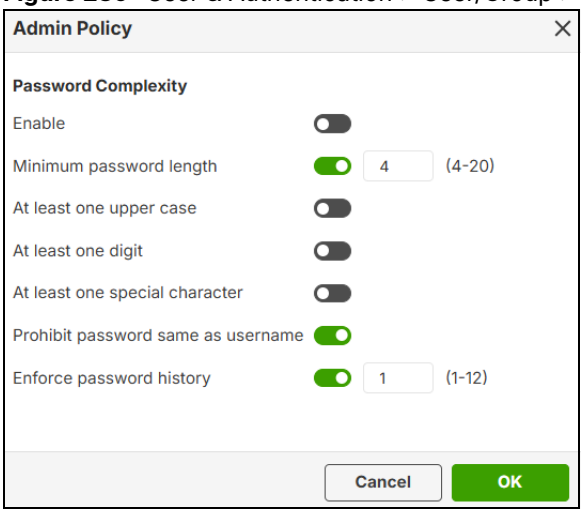
Table 217 User & Authentication > User/Group > Setting (continued)

LABEL	DESCRIPTION
User Logon Settings	
Limit simultaneous admin logons enable	Enable 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 admin account	Type the maximum number of simultaneous logins by each admin user.
Limit the simultaneous access logons enable	Select this check box if you want to set a limit on the number of simultaneous logins by non-admin users. If you do not select this, access users can login as many times as they want as long as they use different IP addresses.
Maximum number per access account	Type the maximum number of simultaneous logins by each access user.
Reach maximum number per account	Set the action the Zyxel Device will take when the limit you set for the numbers of simultaneous logins by admin users or non-admin users has exceeded. Select **Block** to have the Zyxel Device block any accounts that try to log in. Select **Remove previous user and login** to have the Zyxel Device remove the most recently login account
User Lockout Settings	
Enable logon retry limit enable	Enable 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.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

28.1.7.1 Password Policy Setting Screen

The **Password Policy Setting** screen allows you to set minimum length and character rules for the web configurator login password. To access this screen, go to the **User & Authentication** > **User/Group** > **Setting** screen, and click the **Setting** icon under **Password Policy**.

Figure 289 User & Authentication > User/Group > Setting > Password Policy Setting



The following table describes the labels in this screen.

Table 218 User & Authentication > User/Group > Setting > Password Policy Setting

LABEL	DESCRIPTION
Enable	Enable this to set the following rules on the web configurator login password.
Minimum password length	Enable this and enter a number from 4-20 to specify the minimum number of characters for the web configurator login password.
At least one upper case	Enable this to require the web configurator login password to include at least one uppercase letter (A-Z).
At least one digit	Enable this to require the web configurator login password to include at least one number (0-9).
At least one special character	Enable this to require the web configurator login password to include at least one special character, including [(){}<>^`+/:!*#@&=$.~%;-].
Prohibit password same as username	Enable this to prevent the web configurator login password from being the same as the username.
Enforce password history	Enable this to prevent reusing previously configured web configurator passwords. Enter a number from 1–12 to specify how many previous passwords cannot be reused.
OK	Click **OK** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

28.2 User Authentication Overview

This section describes how to set up AAA server and two-factor authentication.

- Use the **AAA Server** screen (see Section 28.3 on page 480) to configure the default authentication server (Local/LDAP/AD/RADIUS) to use for user authentication.
- Use the **Two-factor Authentication** screen (see Section 28.4 on page 493) to have double-layer security for local users to access a secured network behind the Zyxel Device.
- Use the **Advanced** screen to set up a HTTPS port and certificate in a proxy authentication server.

28.2.1 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.

- OIDC Server

  OpenID Connect (OIDC) is used to provide single sign-on from a primary authenticator to an application. For the Zyxel Device, the OIDC server passes primary authentication from an Identity Provider (IdP) such as at Microsoft or Google to the Captive Portal and SSL VPN applications. Users must have a Microsoft Entra ID account (set up by the company administrator) or a Google workspace account. Refer to the Zyxel Account Authentication appendix.

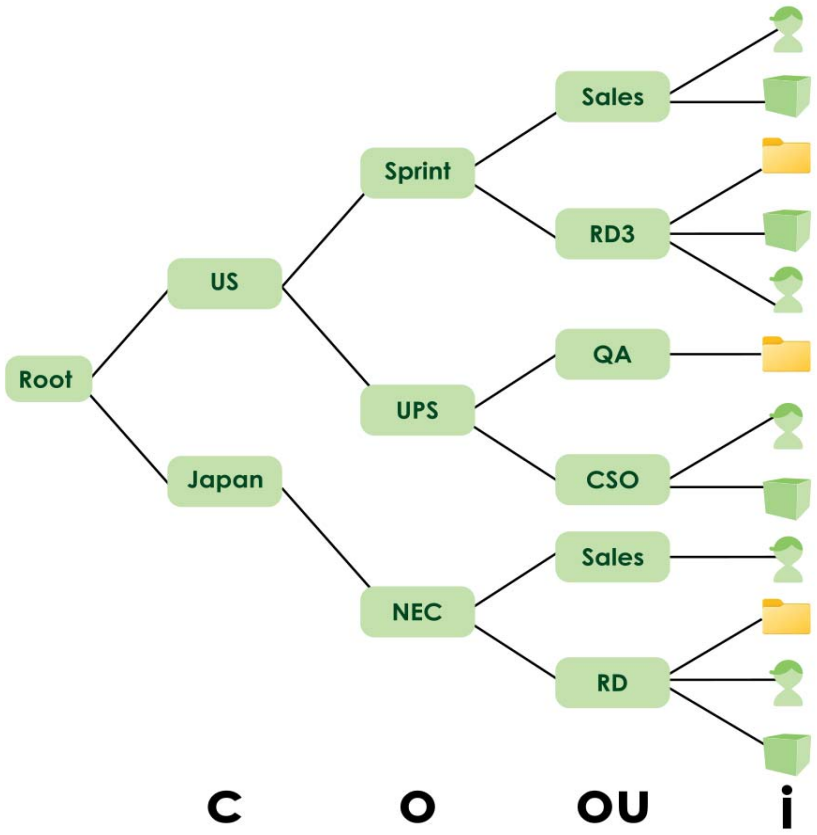
- RADIUS

  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 290 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.

28.3 AAA Server Overview

You can use an AAA (Authentication, Authorization, Accounting) server to control access to your network. A Zyxel Device AAA server can be a Windows Active Directory (AD), a Lightweight Directory Access Protocol (LDAP) server or a RADIUS server, Use the **AAA Server** screens to create and manage objects that contain settings for using AAA servers. You can use AAA server objects in configuring IPSec VPN and SSL VPN rules.

Use RADIUS, AD and LDAP servers to authenticate users instead of (or in addition to) an internal Zyxel Device user database that is limited to the memory capacity of the Zyxel Device. In essence, AAA servers allow you to authenticate a large number of users from a central location.

Figure 291 AAA Server Network Example

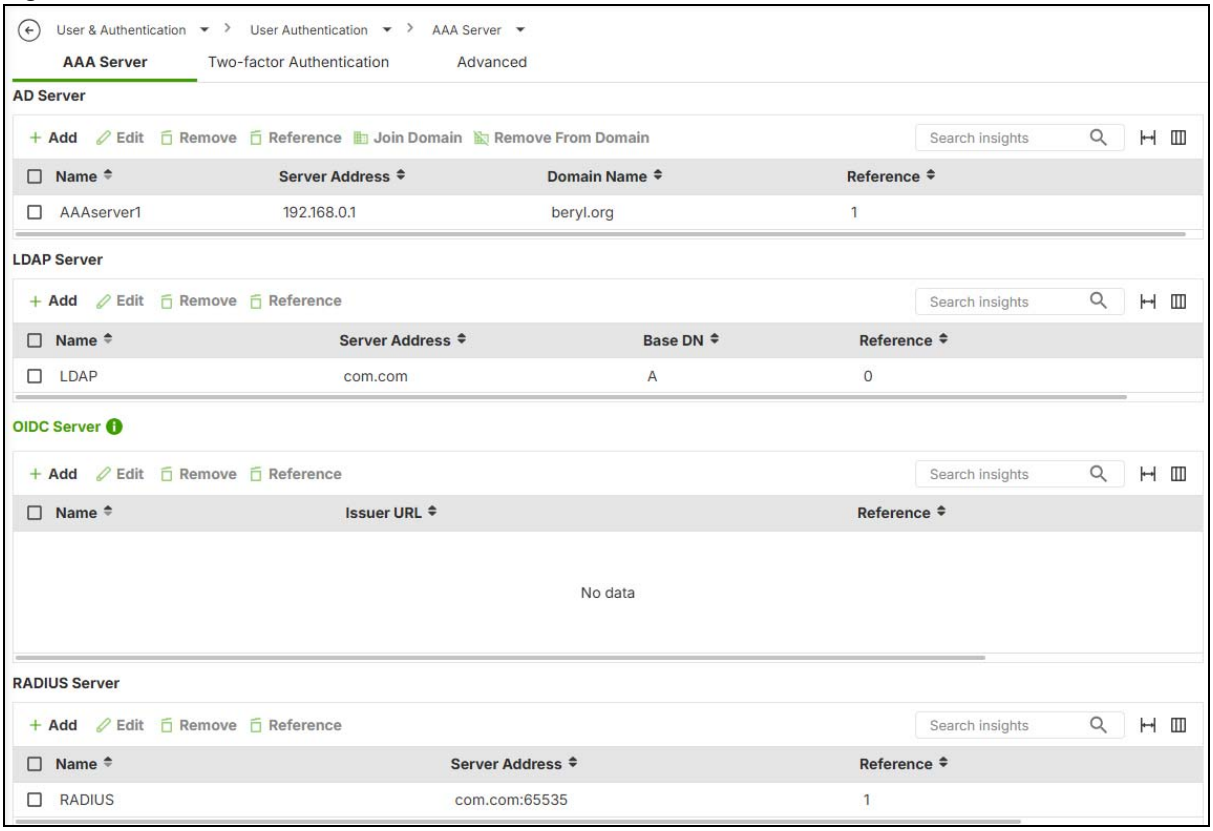


28.3.1 AAA Server Configuration

Use the **AAA Server** screen to manage AD servers, LDAP servers and RADIUS servers the Zyxel Device can use in authenticating users.

Click **User & Authentication > User Authentication > AAA Server** to display the following screen.

Figure 292 User & Authentication > User Authentication > AAA Server



The following table describes the labels in this screen.

Table 219 User & Authentication > User Authentication > AAA Server

LABEL	DESCRIPTION
Server	This is the AD, LDAP, OIDC or RADIUS server section summary.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The 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.
Join Domain	Select an AD server entry and click **Join Domain** to open a screen where you can add the AD server to the same domain as the Zyxel Device for central authentication management. See Section 28.3.3 on page 484 for more information. Note: The Zyxel Device can only be joined to one AD domain at a time. Adding a new AD domain will replace existing domain associations. Note: Ensure that the **Domain Zone Forwarder** configuration in the **System > DNS & DDNS > DNS** screen is correct before joining a domain.
Remove From Domain	Select an AD server entry and click **Remove From Domain** to remove the entry from the same domain as the Zyxel Device. The AD server is not isolated if it is not in the same domain as the Zyxel Device. You may do this for non-central authentication management such as when managing the Zyxel Device through NCC.

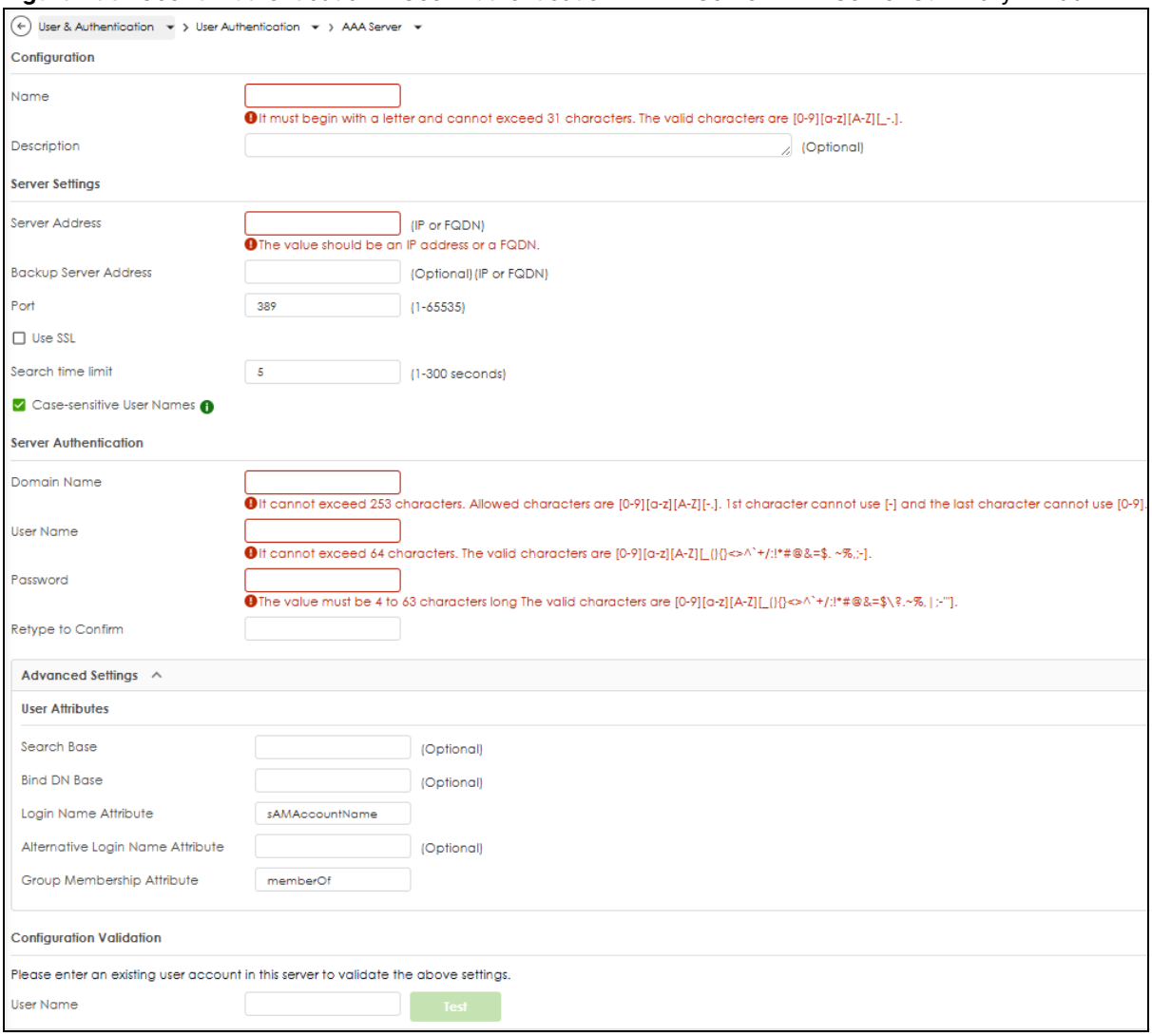
Table 219 User & Authentication > User Authentication > AAA Server (continued)

LABEL	DESCRIPTION
Name	This field displays the name of the AD, LDAP, OIDC or RADIUS server.
Server Address	This is the address of the AD, LDAP or RADIUS server.
Domain Name	This is the domain name of the AD server.
Issuer URL	This is the URL that uniquely identifies the OIDC server.
Reference	This is the number of times the entry is used in other settings.

28.3.2 Add an AD Server

Click **User & Authentication > User Authentication > AAA Server > AD Server Summary > Add** to display the following screen. Use this screen to create a new AD server entry or edit an existing one.

Figure 293 User & Authentication > User Authentication > AAA Server > AD Server Summary > Add



The following table describes the labels in this screen.

Table 220 User & Authentication > User Authentication > AAA Server > AD Server Summary > Add

LABEL	DESCRIPTION
Configuration	
Name	Enter a descriptive name for identification purposes. Use up to 31 single-byte characters, including [0-9][a-z][A-Z] [_-]. 'local' and 'cloud-auth' are reserved names.
Description	Enter the description of each server, if any. The value cannot exceed 61 characters. Valid characters are [0-9][a-z][A-Z]['()+,/:=?;!*#@$_%-"].
Server Settings	
Server Address	Enter the IPv4 address of the AD server.
Backup Server Address	If the AD 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 server(s) in this group.
Use SSL	Select **Use SSL** to establish a secure connection to the AD server(s) from the Zyxel Device.
Search time limit	Specify the timeout period (between 1 and 300 seconds) before the Zyxel Device disconnects from the AD server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the AD server(s) or the AD server(s) is down.
Case-sensitive User Names	Select this if the AD server checks the case of usernames.
Server Authentication	
Domain Name	Enter the Domain Controller (DC) to which AD server belongs. The Zyxel Device uses this to access the AD server. For example, zyxel.com.
User Name	Enter the user name that the Zyxel Device uses to access the AD server. For example, user01.
Password	Enter the password that the Zyxel Device uses to access the AD server.
Retype to Confirm	Retype your new password for confirmation.
Advanced Settings	You just need to configure **Search Base** and **Bind DN Base** if you want to change or add AD search settings other than the default **Domain Name** and **User Name** above. See Section 28.2.1 on page 478 for more information on Base DN, Bind DN and AD directory structure. In the following fields, cn = Common Name, ou = Organization Unit and dc = Domain Controller
User Attributes	
Search Base	An Active Directory server has a hierarchical structure for user account entries. The search base is where the search starts for user account entries. This can help to make the authentication procedure faster. To limit the search to begin in a container beneath the root of the domain, you must specify the fully-qualified name of the container in comma-delimited form. Start with the name of the base container and progress to the root of the domain. The search string is not case-sensitive; you can use either uppercase or lowercase letters. The entry cannot exceed 128 characters. Valid characters are [0-9][a-z][A-Z][_(){}<>^`+/:!*#@&=$.~%,;]. If you enter nothing in this field, and the **Domain Name** above is zyxel.com, then the default Search Base is: dc=zyxel,dc=com. This is an example **Search Base** entry: ou=adminGroup,dc=zyxel,dc=com. This entry allows search only in the adminGroup organization unit, in the zyxel.com domain.

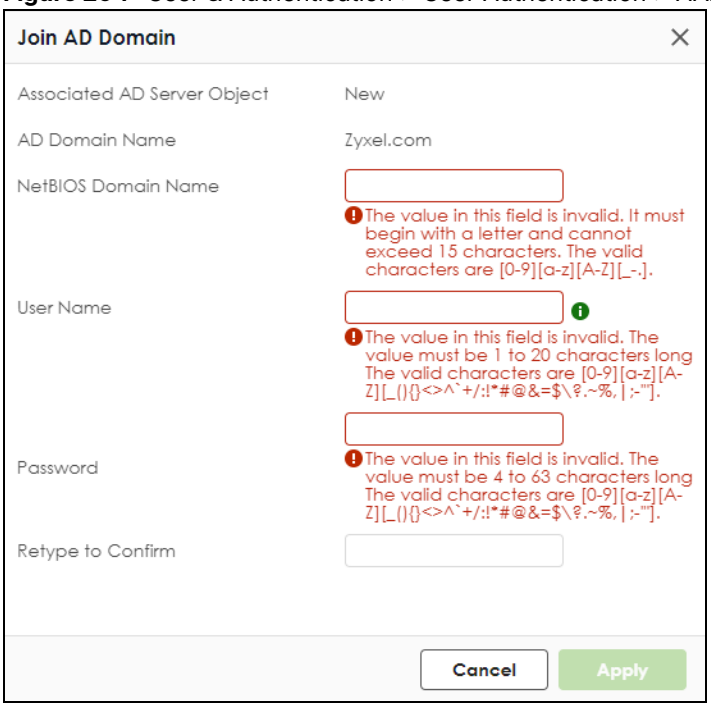
Table 220 User & Authentication > User Authentication > AAA Server > AD Server Summary > Add

LABEL	DESCRIPTION
Bind DN Base	A bind DN is used to authenticate with the AAA server in conjunction with a bind password. As long as it has permission, it can search in any sub-tree under the Search Base (Base DN). Bind DN = **User Name** + **Bind DN Base** If you enter nothing in this field, and the **Domain Name** above is zyxel.com, then the default **Bind DN Base** is: cn=Users,dc=zyxel,dc=com This is an example **Bind DN Base** entry: ou=adminGroup,dc=zyxel,dc=com. So, user01, for example, must be located in the adminGroup organization unit, in the zyxel.com domain.
Login Name Attribute	This is the user name claim for login. It must be in the claims. When a user authenticates through an AAA server containing user attributes called claims. The **Login Name Attribute** tells the Zyxel Device which claim should be used as the user's username to identify the user. Typical values include: userPrincipalName (UPN), sAMAccountName (SAM Account Name, used by legacy Windows systems), name, and email. The name must match the external user name pattern and be between 1 and 128 characters long. Valid characters include the following characters within the square brackets: [0-9a-zA-Z_(){}<>^`+/:!*#@&=$.~%,;-]. Spaces are not allowed. Note: It is not recommended to use "name" as the Login Name Attribute because full names often include spaces, which will cause authentication to fail.
Alternative Login Name Attribute	If there is a second type of user name claim that the users can use to log in, enter it here. For example, userPrincipalName (UPN), sAMAccountName (SAM Account Name), name, email.
Group Membership Attribute	An authentication server uses attributes to store information about users. Some of these attributes contain group membership information. For example, the attribute 'memberOf' may contain values such as Sales, RD, and Management, which represent the groups a user belongs to. Enter the name of the attribute that the Zyxel Device is to check to determine to which group a user belongs.
Configuration Validation	
User Name	Enter a user account that exists on this server, then click the **Test** button to validate the configuration settings for the account.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

28.3.3 Join an AD Domain

Click **User & Authentication > User Authentication > AAA Server > Join AD Domain** to display the following screen. Use the **Join AD Domain** screen to add the AD server to the same domain as the Zyxel Device for central authentication management.

Figure 294 User & Authentication > User Authentication > AAA Server > AD Server > Join AD Domain



The following table describes the labels in this screen.

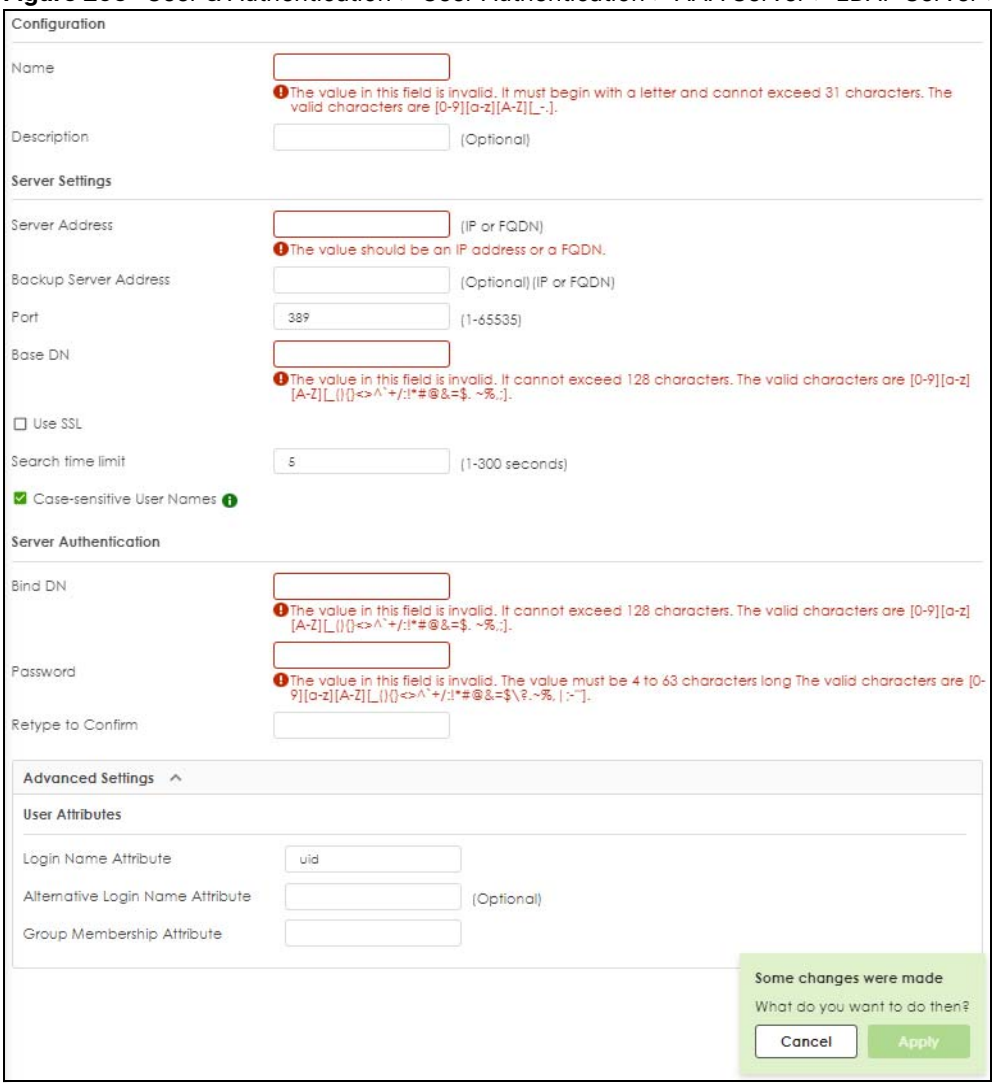
Table 221 User & Authentication > User Authentication > AAA Server > AD server > Join AD Domain

LABEL	DESCRIPTION
Associated AD Server Object	This field shows the name of the AD server object.
AD Domain Name	This field shows the AD server domain name you want the Zyxel Device to join.
NetBIOS Domain Name	Type the NetBIOS name. This field is required by the AD server to join its AD domain. 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. The name must begin with a letter and cannot exceed 15 characters. Valid characters are [0-9][a-z][A-Z][_-.].
User Name	Enter the user name for the Zyxel Device to access the AD server. The value must be 1 to 20 characters long. Valid characters are [0-9][a-z][A-Z][_(){}<>[]^`+/:!*#@&=$\?.~%,|;-'"].
Password	Enter the password associated with the user name. The value must be 4 to 63 characters long. Valid characters are [0-9][a-z][A-Z][_(){}<>^`+/:!*#@&=$\?.~%,|;-'"].
Retype to Confirm	Retype the password you entered in the Password field to confirm.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

28.3.4 Add an LDAP Server

Click **User & Authentication > User Authentication > AAA Server > LDAP Server > Add** to display the following screen. Use this screen to create a new LDAP server entry or edit an existing one.

Figure 295 User & Authentication > User Authentication > AAA Server > LDAP Server > Add



The following table describes the labels in this screen.

Table 222 User & Authentication > User Authentication > AAA Server > LDAP Server Summary > Add

LABEL	DESCRIPTION
Configuration	
Name	Enter a descriptive name for identification purposes. Use up to 31 single-byte characters, including 0-9a-zA-Z_-. 'local' and 'cloud-auth' are reserved names.
Description	Enter the description of each server, if any. Use up to 61 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-".
Server Settings	
Server Address	Enter the IPv4 address of the LDAP server.
Backup Server Address	If the LDAP server has a backup server, enter its address here.
Port	Specify the port number on the 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 LDAP server(s) in this group.

Table 222 User & Authentication > User Authentication > AAA Server > LDAP Server Summary > Add

LABEL	DESCRIPTION
Base DN	A base DN is the point from where a server will search for users. The entry cannot exceed 128 characters. Valid characters are [0-9][a-z][A-Z][_(){}<>^`+/:!*#@&=$. ~%,;].
Use SSL	Select **Use SSL** to establish a secure connection to the LDAP server(s).
Search time limit	Specify the timeout period (between 1 and 300 seconds) before the Zyxel Device disconnects from the LDAP server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the LDAP server(s) or the LDAP server(s) is down.
Case-sensitive User Names	Select this if you want configure your username as case-sensitive.
Server Authentication	
Bind DN	A bind DN is an object that you bind to inside LDAP to give you permission to make changes. The entry cannot exceed 128 characters. Valid characters are [0-9][a-z][A-Z][_(){}<>^`+/:!*#@&=$. ~%,;].
Password	Enter the password that the Zyxel Device uses to access the LDAP server.
Retype to Confirm	Retype your new password for confirmation.
Advanced Settings	
User Attributes	
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	A 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”.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

28.3.5 Add an OIDC Server

The OIDC server passes primary authentication from an Identity Provider (IdP) such as Microsoft or Google to the Captive portal and SSL VPN applications. Users must have a Microsoft Entra ID account (set up by the company administrator) or a Google workspace account. Refer to the Zyxel Account Authentication appendix.

28.3.5.1 User Authentication and Authorization Flow with OIDC

1. A user visits the Captive portal or SSL VPN login page.
2. The Zyxel Device redirects user to the IdP (with client_id, redirect_uri, scope, and so on.)
3. The user signs in at the IdP.
4. The IdP sends an authorization code to the user’s browser using the **Redirect URI**.

5 The Zyxel Device sends the authorization code, client ID, client secret, Redirect URI, and grant_type=authorization_code to a Token Endpoint, a back end API URL on the Identity Provider (IdP).

6 The Zyxel Device receives an ID Token and Access Token from the IdP. The ID Token is used to identify the login user. The Access Token is used to authorize access to the service, such as Captive portal or SSL VPN.

7 The Zyxel Device retrieves the JWKS (JSON Web Key Set), the public keys from the IdP, in order to verify token signatures.

8 The Zyxel Device checks the token signature and claims.

9 If they are valid, the user is logged into the Captive portal or SSL VPN application from step 1.

28.3.5.2 Process Overview for Microsoft Entra ID

This is what you, as the administrator, have to do at the Entra Microsoft portal to set up OIDC for your users. This section is for your reference. These are the menu names and paths used at the time of writing. See the help at the below portal for more up-to-date or more detailed information.

1 Go to *https://entra.microsoft.com/* to create an OIDC Application with a Microsoft Entra ID.

2 In **App registration**, click **New registration**. Configure an **App Name** and **Supported account types**, then click **Register**.

3 In the new registration **Overview**, copy the **Application (client) ID**.

4 Under **Endpoints**, select and copy the beginning of **OpenID Connect metadata document** up to v2.0 as the **Issuer-url**. For example, copy 'https://login.microsoftonline.com/{tenant}/v2.0', where {tenant} is a variable. This will be used in the Zyxel Device web configurator in the **Issuer URL** field.

5 Next, click **Add a certificate or secret**. Under **Client secrets**, click **New client secret**. Type a name in the Description, then click **Add**. Copy the entry under **Value** for the newly created client secret. This will be used as the **Client-Secret** in the Zyxel Device web configurator.

6 Next, in **Overview**, click **Add a Redirect URI**.

7 In **Authentication**, click **Add a platform**, then select a platform such as **Web**.

8 In the Zyxel Device web configurator, set the **Redirect Address** to be where the **OIDC server** can connect to the Zyxel Device. For example:

- For **Captive Portal**, this can be an interface IP, external interface IP, Captive portal redirect FQDN, external FQDN or a DNS record for the Zyxel Device.
- For **SSL VPN**, this can be an external interface IP, external FQDN or an IP address that can connect to the Zyxel Device.

9 Copy the above **Redirect Address** and paste it into **Redirect URI** under **Authentication**.

10 Select **ID tokens used for implicit and hybrid flows**, then click **Configure**.

11 In the Zyxel Device web configurator, go to **User & Authentication > User Authentication > AAA Server > OIDC Server > Add**, and use the **Issuer URL**, **Client ID** and **Client Secret** you copied from Microsoft Entra ID (above).

28.3.5.3 Process Overview For Google Workspace

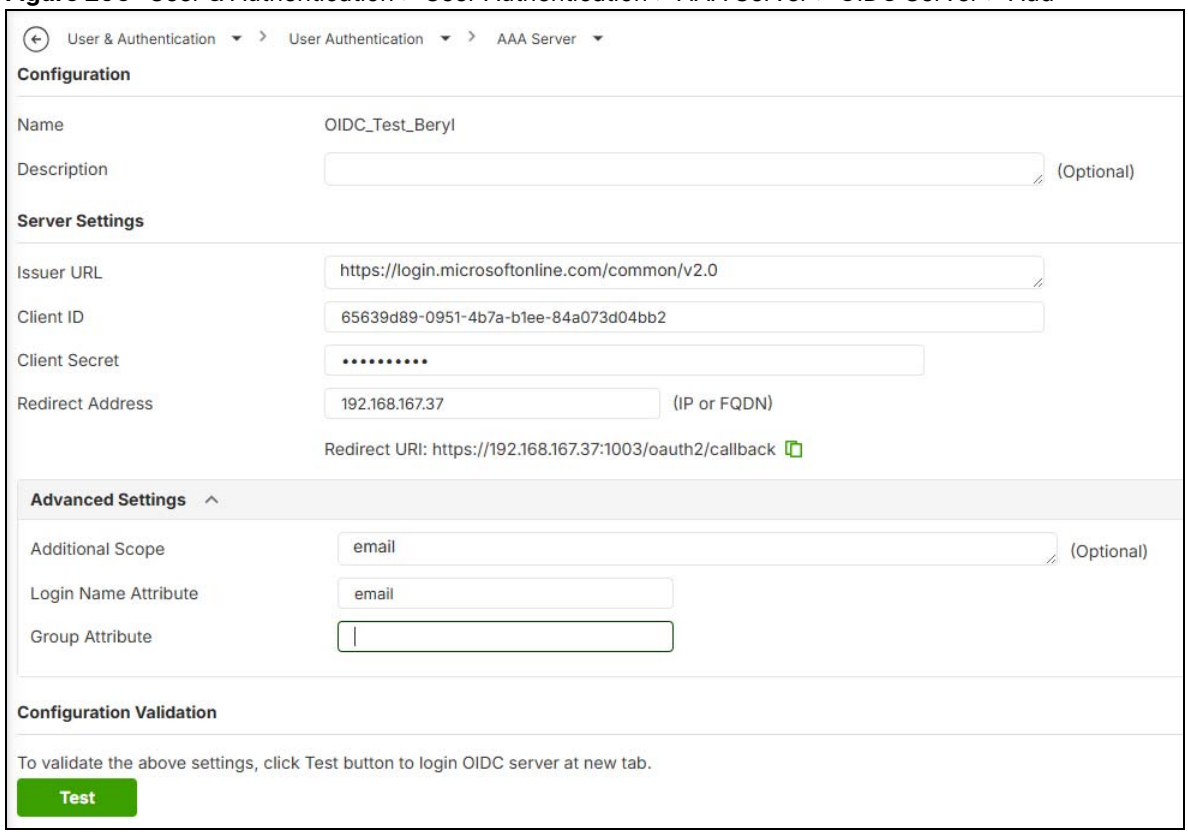
This is what you, as the administrator, have to do at Google Workspace to set up OIDC for your users. This section is for your reference. These are the menu names and paths used at the time of writing. See the help at the below portal for more up-to-date or more detailed information.

1. Go to *https://console.cloud.google.com/*.
2. Click **Open project picker**, then **New project**.
3. Enter a **Project name**, **Organization** and **Location**, then click **Create**.
4. Go to your new project, then go to **APIs & Services > OAuth consent.**
5. Enter an **App name**, **User support email**, and then click **Next**.
6. In **Audience** set the user type to **Internal** (recommended), then click **Next**.
7. In **Contact Information,** set your **Email address**, then click **Next**.
8. In **Finish**, read, then select **I agree to the Google API Services: User Data Policy**, click **Continue**, and then click **Create**.
9. Next, in **Overview**, click **Create OAuth client**.
10. Set an **Application type** such as **Web application**, and then enter the **Name** of the OAuth client. This is used as the **Client ID** in the Zyxel Device web configurator to identify an app to the Google OAuth servers.
11. In the Zyxel Device web configurator, set the **Redirect Address** to be where the **OIDC server** can connect to the Zyxel Device. FQDN is required for Google. For example:
    - For **Captive Portal**, this can be the Captive portal redirect FQDN, external FQDN or a DNS record for the Zyxel Device.
    - For **SSL VPN**, this can be an external FQDN or a DNS record for the Zyxel Device.
12. Copy the **Redirect Address** above and enter it as a URL under **Authorized redirect URIs.**
13. Next click the Edit Client icon and copy the **Client ID** and **Client secret**.
14. In the Zyxel Device web configurator, go to **User & Authentication > User Authentication > AAA Server > OIDC Server > Add**, and use the **Client ID** and **Client Secret** you copied from Google Workspace (above). Set the **Issuer URL** as *https://accounts.google.com*.

28.3.5.4 Zyxel Device Configuration

Click **User & Authentication > User Authentication > AAA Server > OIDC Server > Add** to display the following screen. Use this screen to create a new OIDC server entry or edit an existing one.

Figure 296 User & Authentication > User Authentication > AAA Server > OIDC Server > Add



The following table describes the labels in this screen.

Table 223 User & Authentication > User Authentication > AAA Server > OIDC Server > Add

LABEL	DESCRIPTION
Configuration	
Name	Enter a descriptive name for identification purposes. Use up to 31 single-byte characters, including the following characters within the square brackets: [0-9a-zA-Z_-]. 'local' and 'cloud-auth' are reserved names.
Description	Enter the description of the server, if any. Use up to 512 single-byte printable characters, including the following characters within the square brackets: [0-9a-zA-Z'()+,/:=?;!*#@$_%-"].
Server Settings	
Issuer URL	Enter a URL that uniquely identifies the OIDC server. This is the address from which the Zyxel Device retrieves the configuration and public keys for the Captive portal or SSL VPN user login. It must begin with “https://” and have a maximum of 256 single-byte characters. Examples are: • https://accounts.google.com • https://login.microsoftonline.com/{tenant}/v2.0 • https://mycompany.auth0.com/ • https://idp.company.com/.
Client ID	Enter a public identifier ‘user name’ for your Captive portal or SSL VPN application. This is for the OIDC server to identify which application is making requests. It must be between 10 and 128 characters long. Valid characters include the following characters within the square brackets: [0-9a-zA-Z._-]. This is an example: ssl-vpn-client

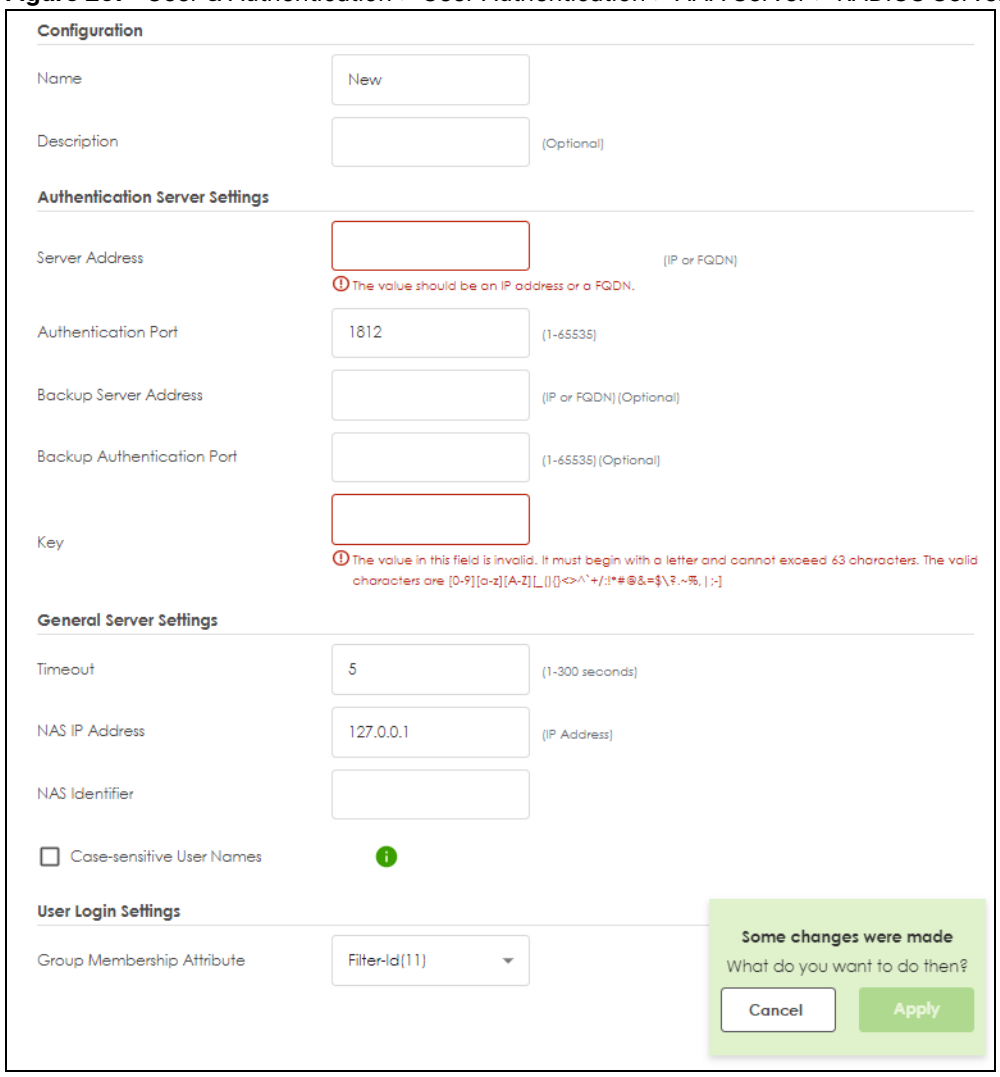
Table 223 User & Authentication > User Authentication > AAA Server > OIDC Server > Add (continued)

LABEL	DESCRIPTION
Client Secret	Enter a 'password' for your application. This is saved on the OIDC server. Your application uses this client secret to prove its identity when requesting tokens from the OIDC server. This is an example: s3cr3tValueFromIdP. The Zyxel Device uses this to exchange the authorization code for tokens. It must be stored and encrypted in the Zyxel Device and kept secret. It must be between 1 and 128 characters long. Valid characters include the following characters within the square brackets: [0-9a-zA-Z`~!@#$%^&*()_-+={}|;:<>,./"'\]
Redirect Address	Enter an IP address or FQDN to where the OIDC server sends an authorization code (or token) after the user successfully signs in at an Identity Provider (IdP) such as Microsoft or Google. You must copy this exact URL into the Identity Provider's **Allowed Redirect URIs** during app registration.
Advanced Settings	
Additional Scope	Additional scope tells the IdP what data and permissions the client is requesting. The scope openid is required by default, and email is recommended. Separate scopes with spaces. Other examples are: • email: get user's email • phone: get user's telephone number • address: get user's mailing address • profile: get user's profile • groups: map groups to local user roles • offline_access: allow long-lived sessions using refresh tokens
Login Name Attribute	This is the user name claim for login. It must be in the claims. When a user authenticates through OIDC, the IdP sends an ID Token, which is a JSON Web Token (JWT) containing user attributes called claims. The **Login Name Attribute** tells the Zyxel Device which claim should be used as the user's username to identify the user. Typical values include: • Microsoft Entra ID: preferred_username (recommended), name, upn (User Principal Name), email, oid (Object ID) • Google: name (recommended), email The name must match the external user name pattern and be between 1 and 128 characters long. Valid characters include the following characters within the square brackets: [0-9a-zA-Z`~!@#$%^&*()_-+={}|;:<>,./"'\]. Spaces are allowed but are replaced by underlines.
Group Attribute	This is the claim name in the OIDC token that contains external group information used for authorization to services such as Captive Portal or SSL VPN. The Identity Provider (IdP) returns this claim as a list of strings, such as group names or Object IDs. The exact format depends on your IdP configuration. The Zyxel Device reads this claim and matches its values against the **Group Identifier**s configured for an **External Group User** in **User & Authentication > User/Group > User**. A user is considered a member if any value in the claim exactly matches the configured Group Identifier. The value must exactly match the value returned by your IdP.
Configuration Validation	First, click **Apply** to save the changes, then click **Test** to log into the OIDC server with the above settings. If the login fails, check the above settings.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

28.3.6 Add a RADIUS Server

Click **User & Authentication > User Authentication > AAA Server > RADIUS Server > Add** to display the following screen. Use this screen to create a new RADIUS server entry or edit an existing one.

Figure 297 User & Authentication > User Authentication > AAA Server > RADIUS Server > Add



The following table describes the labels in this screen.

Table 224 User & Authentication > User Authentication > AAA Server > RADIUS Server > Add

LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes. Use up to 30 single-byte characters, including 0-9a-zA-Z_-. 'local' and 'cloud-auth' are reserved names.
Description	Enter the description of each server, if any. Use up to 61 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-".
Server Address	Enter the IPv4 address or FQDN 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.
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.

Table 224 User & Authentication > User Authentication > AAA Server > RADIUS Server > Add (continued)

LABEL	DESCRIPTION
Key	Enter a password (up to 63 single-byte characters, including 0-9a-zA-Z_(){}<>^`+/ :!*#@&=$\?.~%,|;-) 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.
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 the RADIUS server requires case-sensitive usernames. Make sure usernames are configured correctly on the Zyxel Device.
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.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

28.4 Two-Factor Authentication Overview

Use two-factor authentication to have double-layer security for local users in the Zyxel Device database to access the Zyxel Device or a secured network behind the Zyxel Device via a VPN tunnel.

The first layer is the Zyxel Device's login user name / password and the second layer is using the Google Authenticator app.

Note: The user must download and set up the Google Authenticator app first.

This section introduces how two-factor authentication works.

Admin Access Via the Web Configurator or SSH

1. A local admin user connects to the Zyxel Device through the Web Configurator or SSH.
2. The Zyxel Device requests the admin user's user-name and password from the local Zyxel Device database in order to authenticate this admin user.
3. If all credentials are correct, then the Zyxel Device requests the Google Authenticator code.
4. The admin user must 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 or the code was not received, then the admin user should contact the network administrator.

28.4.0.1 Two-factor Authentication Pre-configuration

Before configuration, you must:

- Set up the user's user-name and password in the local Zyxel Device database.
- Enable Two-factor Authentication in **User & Authentication > User/Group > User > Edit > Two-factor Authentication** for a specific user
- Enable Two-factor Authentication in **User & Authentication > User Authentication > Two-factor Authentication** for the Zyxel Device
- Enable **HTTP**, **HTTPS** and/or **SSH** in **System > Settings > Administration Settings**.
- Add **HTTP**, **HTTPS** and/or **SSH** 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.

Two-Factor authentication will fail under the following conditions:

- The user's credentials are not in the in the local Zyxel Device database.
- You omit any of the pre-configuration items. Make sure to perform all pre-configuration items.
- Authorization times out. Extend the **Valid Time** in **User & Authentication > User Authentication > 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.

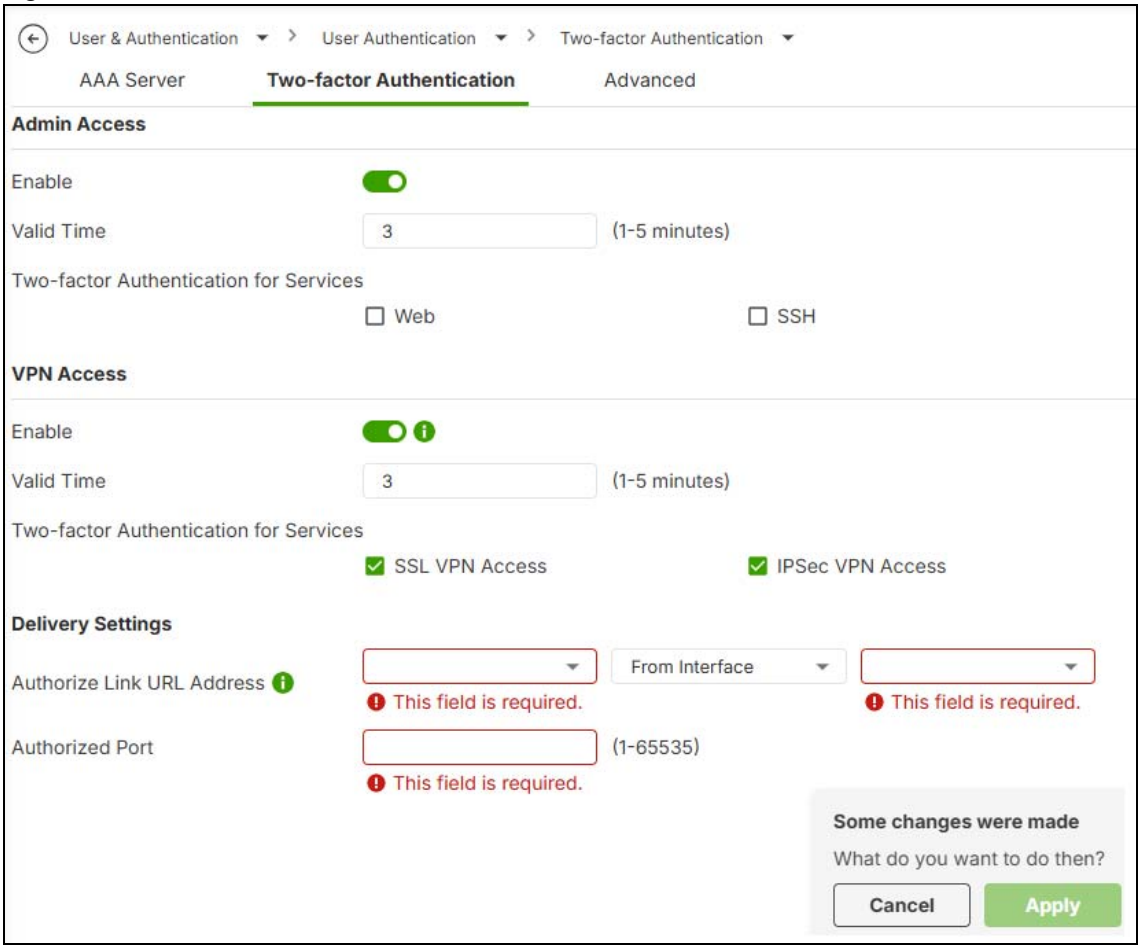
- Users authenticated by external servers, such as AD (Windows Active Directory), LDAP (Lightweight Directory Access Protocol), or RADIUS are not supported.
- A user must setup Google Authenticator on their mobile device before they can successfully authenticate with the Zyxel Device.
- Verification code length: 6 digits.
- Maximum verification code failed attempts: 3
- Backup code length: 8 digits

28.4.1 User Authentication Two-Factor Authentication

Use this screen to configure double-layer security for local users to access the Zyxel Device or a secured network behind the Zyxel Device via a VPN tunnel.

Go to **User & Authentication > User Authentication > Two-factor Authentication** and configure the following screen as shown.

Figure 298 User & Authentication > User Authentication > Two-factor Authentication



The following table describes the labels in this screen.

Table 225 User & Authentication > User Authentication > Two-factor Authentication

LABEL	DESCRIPTION
Enable	Enable this to require double-layer security to access the Zyxel Device via the Web Configurator or SSH.
Valid Time	Enter the maximum time (in minutes) within which the user must enter the key received in Google Authenticator.
Two-factor Authentication for Services	Select which services require Two-Factor Authentication for the admin user. You must select at least one. • Web • SSH
VPN Access	
Enable	Enable this to require double-layer security to access a secured network behind the Zyxel Device via a VPN tunnel.
Valid time	Enter the maximum time (in minutes) within which the user must enter the key received in Google Authenticatorl in order to get authorization for access to a secured network behind the Zyxel Device via a VPN tunnel.

Table 225 User & Authentication > User Authentication > Two-factor Authentication (continued)

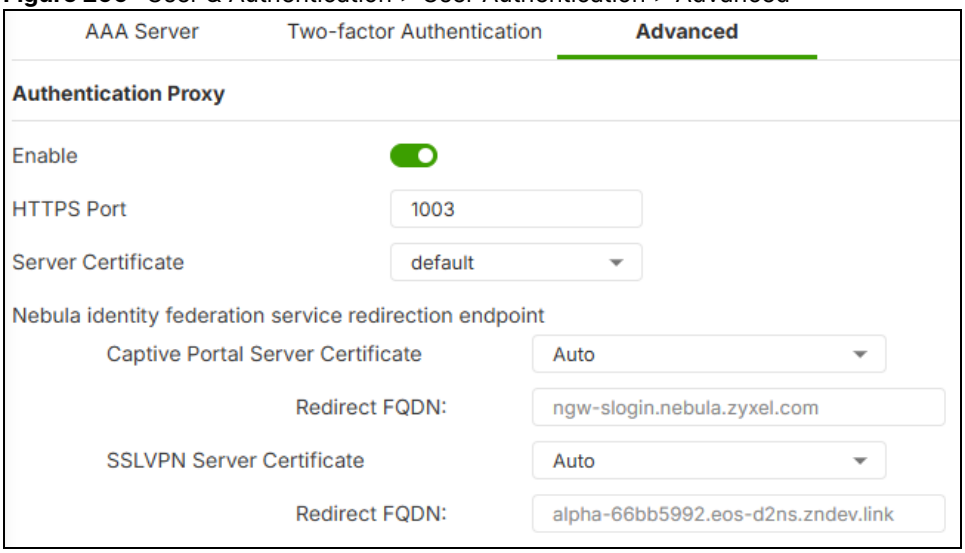
LABEL	DESCRIPTION
Two-factor Authentication for Services	Select which types of VPN tunnels require Two-Factor Authentication for the admin user. You must select at least one. You should have configured the VPN tunnel first. • SSL VPN Access • IPSec VPN Access
Delivery Settings	Use this section to configure how to send the VPN link.
Authorize Link URL Address	Configure the link that the user will receive. The user must be able to access the link. • **http**/**https**: you must enable **HTTP** or **HTTPS** in **System > Settings** • **From Interface**/**User-Defined:** select the Zyxel Device WAN interface (**ge3**/**4**) or select **User-Defined** and then enter an IP address or domain name.
Authorized Port	Configure a port between 1 and 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. You must configure a security policy to allow access to this port from the WAN.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

28.5 Advanced

Use this screen to configure an intermediary server for identification of remote users with an account on an AAA server. The backend AAA server does not need to authenticate users.

Go to **User & Authentication > User Authentication > Advanced** and configure the following screen as shown.

Figure 299 User & Authentication > User Authentication > Advanced



The following table describes the labels in this screen.

Table 226 User & Authentication > User Authentication > Advanced

LABEL	DESCRIPTION
Enable	Click the switch to the right to enable a proxy server for remote user authentication.
HTTPS Port	The Zyxel Device uses this port to communicate user authentication requests (only) with the proxy server.
Server Certificate	Select a certificate that the proxy server will use for authentication of remote users. You can use a certificate you created or imported in **System > Certificates > My Certificates** or a trusted certificate from **System > Certificates > Trusted Certificates**. You can use a private certificate or a public certificate from either screen. A private certificate is free but it requires certificate installation on clients or users will get browser warnings if the certificate not trusted. You may use a private certificate for SSL VPN or a Captive portal that has users with devices where trusted certificates can be installed on them, or they can trust the Zyxel Device's private certificate. Users should authenticate to the Zyxel Device from a wired LAN, corporate WiFi, or an established VPN tunnel to the Zyxel Device. A public certificate is issued by a public Certificate Authority, such as DigiCert, Sectigo, Let's Encrypt, and so on. It is automatically trusted by browsers, operating systems, mobile devices, so there's no client configuration, nor browser warnings. However, it's not free, requires a public DNS name and needs Internet access. It's recommended for Captive portals for guests, external HTTPS proxy authentication from the Internet, and authentication using OIDC (some IdPs reject private/self-signed certificates). • Use a public certificate if you want to use proxy server authentication with OIDC or with Captive portal for guests. • Use a private certificate for Captive portal with users behind the Zyxel Device or for SSL VPN proxy server authentication.
Nebula identity federation service redirection endpoint	You can use the Nebula Identity Federation Service (NID FS) to redirect clients to the configured Identity Provider (IdP) for authentication. You can configure NID FS in Nebula. See Section 28.1.3 on page 462 for details. To connect your Zyxel Device to the NID FS, configure the Fully Qualified Domain Name (FQDN) and its associated certificate.
Captive Portal Server Certificate	Select the certificate used to authenticate client access through captive portal login. You can select **Auto** to use the certificate automatically associated with your NID FS.
Redirect FQDN	Enter the FQDN that users will access to access the Zyxel Device after successful authentication. When **Auto** is selected for the **Captive Portal Server Certificate**, the associated FQDN is displayed.
SSLVPN Server Certificate	Select the certificate used to authenticate client access from the SSL VPN. You can select **Auto** to use the certificate automatically associated with your NID FS.
Redirect FQDN	Enter the FQDN that users will access to access the Zyxel Device after successful authentication. When **Auto** is selected for the **SSLVPN Server Certificate**, the associated FQDN is displayed. If the Zyxel Device has not yet received the FQDN from Nebula, **not ready** is displayed. Check the connection with Nebula.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

CHAPTER 29
Wireless

29.1 Overview

Use the **Wireless** screens to configure how the Zyxel Device manages supported Access Points (APs). Supported APs should be in managed mode.

29.1.1 What You Can Do in this Chapter

- Use the **AP Control Service** screen (Section 29.2 on page 509) to set the password for the admin accounts of APs connected to the Zyxel Device.
- Use the **AP List** screen (Section 29.3 on page 510) to manage all of the APs connected to the Zyxel Device.
- Use the **Policy** screen (Section 29.4 on page 521) to configure the AP controller's IP address on the managed APs and determine the action the managed APs take if the current AP controller fails.
- Use the **AP Firmware** screen (Section 29.5 on page 522) to check for and download new AP firmware when it becomes available on the firmware server.
- Use the **Client List** screen (Section 29.6 on page 524) to view a list of WiFi clients connected to APs.
- Use the **WiFi Aid** screen (Section 29.7 on page 531) to view the failed WiFi connection.
- Use the **Connection Log** screen (Section 29.8 on page 534) to view detailed information about the WiFi connection failure.
- Use the **SSID Settings** screen (Section 29.9 on page 535) to configure up to 8 different SSID profiles for each AP group.
- Use the **Radio Settings** screen (Section 29.10 on page 543) to configure global radio settings for all managed APs.
- Use the **AP Settings** screen (Section 29.11 on page 551) to configure general AP settings and enable or disable a port on the managed AP and configure the port's VLAN settings.
- Use the **AP Group Settings** screen (Section 29.12 on page 555) to configure AP group settings and remove an AP group.
- Use the **Wireless Health** screen (Section 29.13 on page 556) to monitor the health of WiFi networks for your APs and connected WiFi clients.
- Use the **SSID Info** screen (Section 29.14 on page 557) to monitor the WiFi network (SSID) usage.
- Use the **Rogue AP Detection** screen (Section 29.15 on page 558) to detect a suspected rogue.

29.1.2 What You Need to Know

Supported APs

At the time of writing, the following APs can be managed by the Zyxel Device.

Table 227 Supported APs with Supported Frequency Bands and Channel Widths

MODEL	SUPPORTED FREQUENCY BANDS AND CHANNEL WIDTHS
WAC500H	2.4G: 20 / 40 MHz 5G: 20 / 40 / 80 MHz
WAX300H	2.4G: 20 / 40 MHz 5G: 20 / 40 / 80 / 160 MHz
WAX510D	2.4G: 20 / 40 MHz 5G: 20 / 40 / 80 MHz
WAX610D	2.4G: 20 / 40 MHz 5G: 20 / 40 / 80 / 160 MHz
WAX630S	2.4G: 20 / 40 MHz 5G: 20 / 40 / 80 / 160 MHz
WAX650S	2.4G: 20 / 40 MHz 5G: 20 / 40 / 80 / 160 MHz
WAX655E	2.4G: 20 / 40 MHz 5G: 20 / 40 / 80 / 160 MHz
WAX620D-6E	2.4G: 20 / 40 MHz 5G: 20 / 40 / 80 / 160 MHz 6G: 20 / 40 / 80 / 160 MHz
WAX640S-6E	2.4G: 20 / 40 MHz 5G: 20 / 40 / 80 / 160 MHz 6G: 20 / 40 / 80 / 160 MHz
WBE510D	2.4G: 20 / 40 MHz 5G: 20 / 40 / 80 / 160 / 240 MHz 6G: 80 / 160 / 320MHz
WBE530	2.4G: 20 / 40 MHz 5G: 20 / 40 / 80 / 160 / 240 MHz 6G: 80 / 160 / 320MHz
WBE630S	2.4G: 20 / 40 MHz 5G: 20 / 40 / 80 / 160 / 240 MHz 6G: 80 / 160 / 320MHz
WBE660S	2.4G: 20 / 40 MHz 5G: 20 / 40 / 80 / 160 / 240 MHz 6G: 80 / 160 / 320MHz
IAP500BE	2.4G: 20 / 40 MHz 5G: 20 / 40 / 80 / 160 / 240 MHz
WBE665S	2.4G: 20 / 40 MHz 5G: 20 / 40 / 80 / 160 / 240 MHz 6G: 80 / 160 / 320MHz

WiFi 6 (IEEE 802.11ax)

WiFi 6 (802.11ax) is a WiFi standard that supports both 2.4GHz and 5GHz frequency bands and brings the following major improvements:

High Data Transmission Speed

WiFi 6 provides faster transmission data rate than its previous WiFi standards with the following features:

- 1024-QAM (Quadrature Amplitude Modulation)- enhances the data capacity of each transmission unit.
- 160 MHz Channel Bandwidth- extends the supported channel bandwidth to 160 MHz, providing higher data throughput.

Enhanced Air Time Utilization

WiFi 6 increases transmission performance in high-density environments that have multiple client devices with the following features:

- OFDMA (Orthogonal Frequency-Division Multiple Access)- divides channels into sub-channels that enables multiple transmissions in a single channel.
- BSS Coloring- tags traffic by BSS (Basic Server Set) and identifies traffic from overlapping BSSs. The AP can ignore traffic of unrelated BSSs and transmit data when a channel is occupied.
- MU-MIMO (Multiple User-Multiple Input Multiple Output)- enables multiple users to connect to the AP and download/upload traffic simultaneously.

Extended Signal Range

Beamforming forms the radiating signals into one direction. This enhances the signal strength and extends the signal transmission range.

Extended Battery Life

Target Wake Time (TWT) allows the AP to negotiate with client devices so client devices only wakes up and communicates with the AP in specific periods. This conserve client devices battery life.

WiFi 6E (IEEE 802.11ax - Extended Standard)

WiFi 6E is an extended standard of WiFi 6 (IEEE 802.11ax). WiFi 6E inherits all the WiFi 6 features and brings with an additional 6 GHz band. The 6 GHz band allows you to avoid possible congested traffic in the lower 2.4 GHz and 5 GHz bands. WiFi clients must support WiFi 6E to connect to an AP using the 6 GHz band.

You must use WPA3 for security with WiFi 6E.

Note: Check your client device’s product specification to see if your client device supports the 6 GHz band (WiFi 6E). If not, you should still use the 2.4/5 GHz bands for connection.

WiFi 6E MBSSID Beacon Management

The AP supports MBSSID, which allows you to create multiple virtual WiFi networks (SSIDs) on the AP. With the WiFi 6E (802.11ax-extended) standard, the AP divides SSIDs into groups, and includes information of all SSIDs in a group in one SSID beacon. Therefore, the Zyxel Device doesn’t need to send beacons for individual SSIDs, which improves air time efficiency.

Note: If you disable a virtual WiFi network (SSID) whose beacon contains the group SSID information, WiFi clients of that group will be disconnected until the AP reselects another SSID to send the beacon.

Out-of-Band Discovery

Out-of-band discovery allows the AP to include information of the 6 GHz band in management frames sent over the 2.4 GHz /5 GHz bands. WiFi 6E clients only need to scan the lower bands (2.4 GHz/5 GHz) to connect to the AP in the 6 GHz band, reducing the discovery time.

PSC Channel (In-Band Discovery)

PSCs (Preferred Scanning Channels) are dedicated channels for WiFi 6E clients to send probe requests on to discover a compatible AP, instead of scanning the entire 6 GHz band. In this way, WiFi 6E clients are able to efficiently discover and connect to the AP within the 6 GHz band.

Note: The available PSCs differ by country for the unlicensed use in the 6 GHz band.

Resource Unit

A resource unit is a portion of a channel bandwidth. For example, a 20 MHz channel can be divided into several resource units. Each resource unit can be allocated to a specified WiFi client, allowing simultaneous data transmission.

WiFi 7 (IEEE802.11be)

WiFi 7 (802.11be) is backward-s compatible with WiFi 6 and WiFi 6E. WiFi 7 is a WiFi standard that supports 2.4 GHz, 5 GHz and 6 GHz frequency bands with the following improvements over WiFi 6 and WiFi 6E.

Table 228 WiFi 6, WiFi 6E and WiFi 7 Comparison

FEATURES		WIFI 6	WIFI 6E	WIFI 7
Theoretical Maximum Speed (Up-to)		9.6 Gbps		46 Gbps
Supported Frequency Bands		2.4 GHz/5 GHz	2.4 GHz/5 GHz/6 GHz	2.4 GHz/5 GHz/6 GHz
Supported Channel Bandwidth		20/40/80/160 MHz	20/40/80/160 MHz	20/40/80/160/320 MHz
Total Spectrum (Up-to)	2.4 GHz	80 MHz		80 MHz
	5 GHz	500 MHz		500 MHz
	6 GHz	Not supported.	1200 MHz	1200 MHz
Other Features (OFDMA/BSS Coloring/TWT/Two-Way MU-MIMO/ Beamforming/1024-QAM)		The same (WiFi 6E inherits all the features from WiFi 6).		WiFi 7 inherits all the features from WiFi 6 and WiFi 6E, with the addition of multi-link operation and preamble puncturing.

Faster Data Transmission

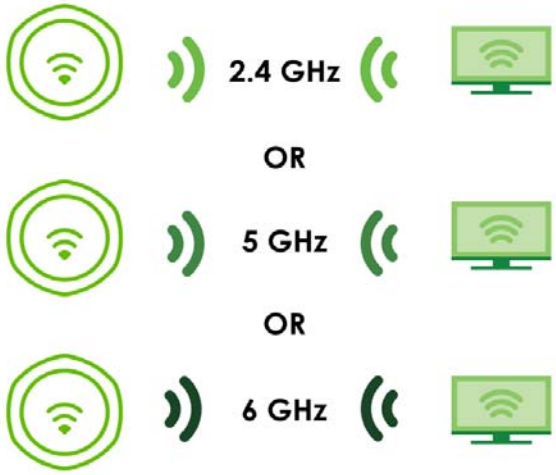
WiFi 7 allows faster data transmission using:

- 4096 QAM (Quadrature Amplitude Modulation)- enhances the amount of data transmitted over the available bandwidth.
- 320 MHz Channel Bandwidth- enlarges the supported channel bandwidth to 320 MHz, allowing higher data throughput.
- Multiple Resource Units (RUs)- allows an AP to allocate multiple RUs to a WiFi client.

Multi-Link Operation (MLO)

An AP can support multiple frequency bands (2.4 GHz, 5 GHz and 6 GHz), but a WiFi client can only connect to the AP using one of these frequency bands. The other frequency bands are unused. The client's data transmission speed depends on the frequency band they are connected to.

Figure 300 Without Multi-Link Operation



WiFi 7 MLO allows a WiFi client to connect to the AP using multiple frequency bands simultaneously. This increases speed and improves reliability of the WiFi connection. MLO makes WiFi 7 ideal for streaming 4K/8K videos, using augmented reality (AR), virtual reality (VR) applications and playing online games.

To use MLO, both the AP and the WiFi client have to support MLO.

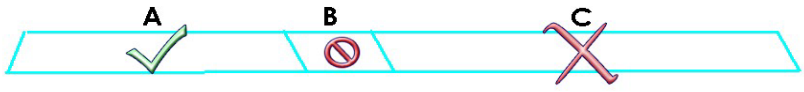
Figure 301 Multi-Link Operation Example



Preamble Puncturing

In WiFi 6 and earlier, any interference would cause the entire WiFi channel to become unavailable. In the figure below, if part of the WiFi channel (**B**) experiences interference, the rest of the WiFi channel (**C**) becomes unavailable.

Figure 302 Without Preamble Puncturing



WiFi 7 preamble puncturing allows you to block the specific portion of the channel that is experiencing interference while continuing to use the rest of the WiFi channel. In the figure below, if part of the WiFi channel (**B**) experiences interference, the rest of the WiFi channel (**C**) is still available.

Figure 303 Preamble Puncturing Example



AP Group

AP group (Access Point group) allows you to organize multiple APs into a single group. You can use an AP group to manage multiple APs at once, instead of configuring each AP individually. WiFi clients in a same AP group can move between without losing connection or needing to re-authenticate. To create an AP group:

1 Go to **Wireless > WLAN Settings**. Clink **Add** from the **AP Group** drop-down list to add an AP group.

2 Go to **Wireless > Access Points > AP List**. Select the APs you want to add to the AP group.

3 Click **More > Move to Group**.

4 Select the AP group you want the selected APs join. Click **Apply**.

SSID Broadcast Control Using AP and SSID Tags

When managing a large number of APs, you can use tags to control SSID broadcast from specific APs. When the tags of an SSID and an AP in the same group match, the SSID will be broadcast.

An SSID is a WiFi network name. An AP may have several unique SSIDs. An AP broadcasts SSIDs for WiFi clients to join.

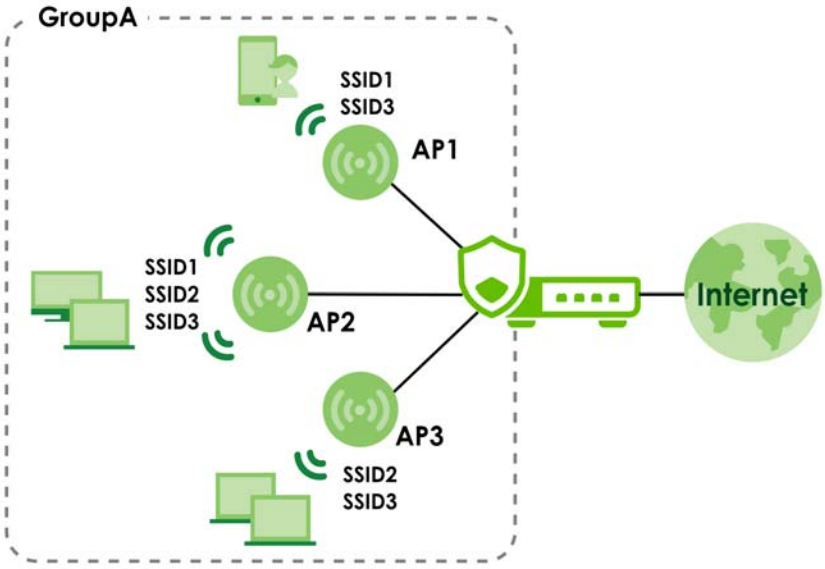
- You can assign multiple tags to APs that are in the same AP group (**Wireless > Access Points > AP List > Managed AP > Edit AP**)
- You can then assign an AP tag or multiple AP tags to an SSID. (**Wireless > WLAN Settings > SSID Settings > Advanced**)
- When an SSID has an AP tag, only APs (in the same AP group) with that tag will broadcast that SSID for WiFi clients to join. APs that do not have that tag will not broadcast that SSID.
- If you do not assign an AP tag to an SSID, then only the AP with that SSID will broadcast the SSID.

The advantage of tags is that you can have multiple APs broadcast the same SSID to easily allow roaming within the same AP group coverage area.

Application Scenario

- AP1 has tags 1F, 2F, 3F with SSID1, SSID2, SSID3
- AP2 has tags 3F, 4F with SSID1, SSID2, SSID3
- AP3 has tags 4F, 5F with SSID1, SSID2, SSID3
- You assign AP tag 3F to SSID1. Therefore AP1 and AP2 will broadcast SSID1. AP3 will not broadcast SSID1.
- You assign AP tag 4F to SSID2. Therefore AP2 and AP3 will broadcast SSID2. AP1 will not broadcast SSID2.
- You do not assign an AP tag to SSID3. Therefore AP1, AP2 and AP3 will each broadcast SSID3.

AP Name	AP1	AP2	AP3
AP Tag	1F, 2F, 3F	3F, 4F	4F, 5F
SSID1 (3F)	V	V	X
SSID2 (4F)	X	V	V
SSID3 (no tag)	V	V	V



Airtime Fairness

Airtime is the time it takes for a client to receive packets from the AP it is associated with. The amount of time each client needs may vary depending on various reasons, such as the distance between the client and the AP, the client's operating system, or the IEEE standard the client is using.

Airtime fairness is a feature that makes sure all connected clients of an AP get the same amount of time to receive packets. Without airtime fairness, a client that needs more airtime will take up more time and bandwidth of an AP to receive packets. This will slow down your WiFi network overall.

For example, you have computer **A** and computer **B** at your house. They're both connected to the same AP. Here are the conditions in the scenario examples below:

- The example time period is 60 milliseconds.
- Computer **A** needs 5 milliseconds to receive a packet from the AP.
- Computer **B** needs 10 milliseconds to receive a packet from the AP.

Airtime Fairness Disabled

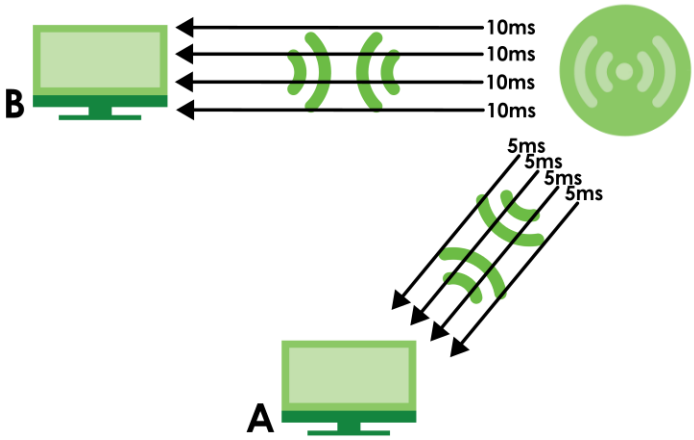
Computer **A** and computer **B** will take turn to receive packets from the AP. With airtime fairness disabled, the AP will not equally allocate the 60 milliseconds between **A** and **B**.

Table 229 Packets Received without Airtime Fairness

PACKETS RECEIVED	A	B
1 packet		10ms
1 packet	5ms	
1 packet		10ms
1 packet	5ms	
1 packet		10ms
1 packet	5ms	
1 packet		10ms
1 packet	5ms	
Total Packets Received: 8	Total Time Period: 60ms	

A has 20 milliseconds to receive packets. **B** has 40 milliseconds to receive packets. In total, they can receive 8 packets in 60 milliseconds.

Figure 304 Airtime Fairness Example-Disabled



Airtime Fairness Enabled

With airtime fairness enabled, the AP will equally allocate the 60 milliseconds between computer **A** and computer **B**. After **B** uses 10 milliseconds to receive a packet, the AP will also allocate10 milliseconds to **A** to receive packets.

Table 230 Packets Received without Airtime Fairness

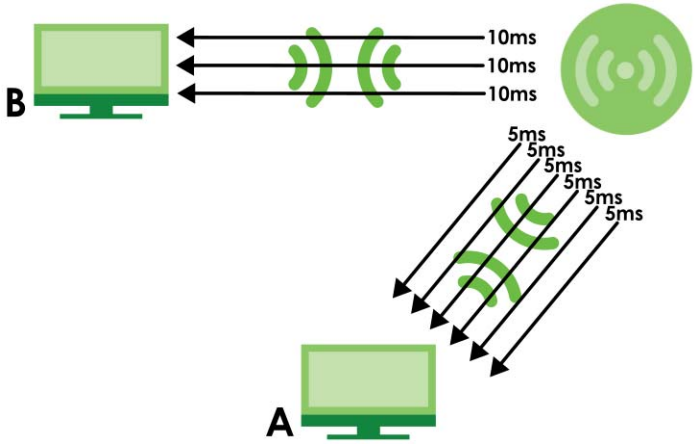
PACKETS RECEIVED	A	B
1 packet		10ms
1 packet	5ms	
1 packet	5ms	
1 packet		10ms
1 packet	5ms	
1 packet	5ms	

Table 230 Packets Received without Airtime Fairness

PACKETS RECEIVED	A	B
1 packet		10ms
1 packet	5ms	
1 packet	5ms	
Total Packets Received: 9	Total Time Period: 60ms	

A and **B** both have 30 milliseconds to receive packets. In total, they can receive 9 packets in 60 milliseconds.

Figure 305 Airtime Fairness Example-Enabled

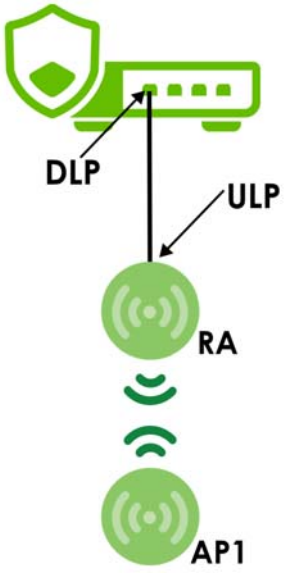


Uplink and Downlink

For the Zyxel Device, connections to the (root) AP are downlink. For the (root) AP, connections to the Zyxel Device are uplink, and connections to other APs further away from the Zyxel Device are downlink.

The following picture shows these uplink and downlink concepts:

Figure 306 Uplink and Downlink Concepts



- The Zyxel Device establishes a network with Root AP (**RA**) and **AP1**. The Zyxel Device sends traffic to **RA** through its downlink port (**DLP**). **RA** receives that traffic through its uplink port (**ULP**). **RA** then extends the network to **AP1**.
- In this scenario, Zyxel Device is the uplink device of **RA**. **RA** is a downlink device of Zyxel Device and a uplink device of **AP1**. **AP1** is a downlink device of **RA**.

Dynamic Channel Selection (DCS)

Dynamic Channel Selection (DCS) is a feature that allows an AP to automatically select the radio channel which it broadcasts. For more information, see Dynamic Channel Selection on page 562.

Dynamic Frequency Selection (DFS)

Dynamic Frequency Selection (DFS) is a WiFi channel 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.

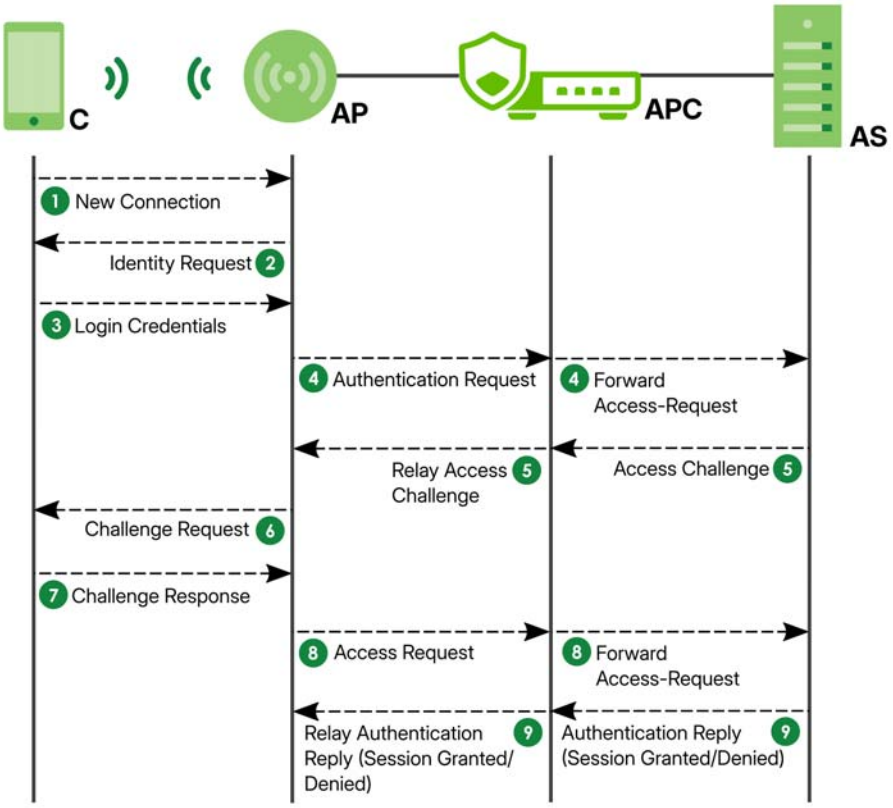
IEEE 802.1X Authentication Using EAP

The following figure illustrates how an AP client gains Internet access through IEEE 802.1X authentication using EAP.

- EAP (Extended Authentication Protocol): the protocol used within 802.1X to carry authentication messages.

When an AP client (**C**) attempts to connect to the AP (**AP**), the AP prompts the client for login information. Once the client provides the credentials, the AP sends the authentication request to the Zyxel Device (**APC**, AP Controller). The Zyxel Device then forwards the request to the authentication server (**AS**). The authentication server sends an access challenge to the AP client through the Zyxel Device and the AP. The AP client responds to the challenge, and the authentication server validates whether the AP client is authorized to access the Internet.

Figure 307 IEEE 802.1x Authentication Process

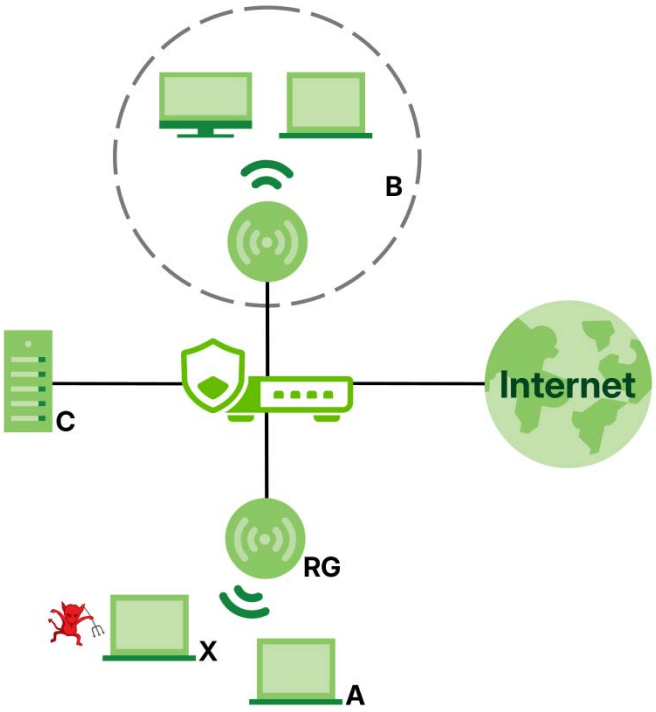


Rogue APs

A rogue AP is a wireless access point operating in a network's coverage area that is not under the control of the network administrator, and which can potentially open up holes in a network's security.

In the following example, a corporate network's security is compromised by a rogue AP (**RG**) set up by an employee at his workstation in order to allow him to connect his notebook computer wirelessly (**A**). The company's legitimate WiFi network (**B**) is well-secured, but the rogue AP uses inferior security that is easily broken by an attacker (**X**) running readily available encryption-cracking software. The attacker now has access to the company network, including sensitive data stored on the file server (**C**).

Figure 308 Rogue AP Example



Enable **Rogue AP Detection** to scan your network for rogue APs. For all APs in a group, go to **Wireless > WLAN Settings > AP Settings**. For a single AP, go to **Wireless > Access Points > Add/Edit**.

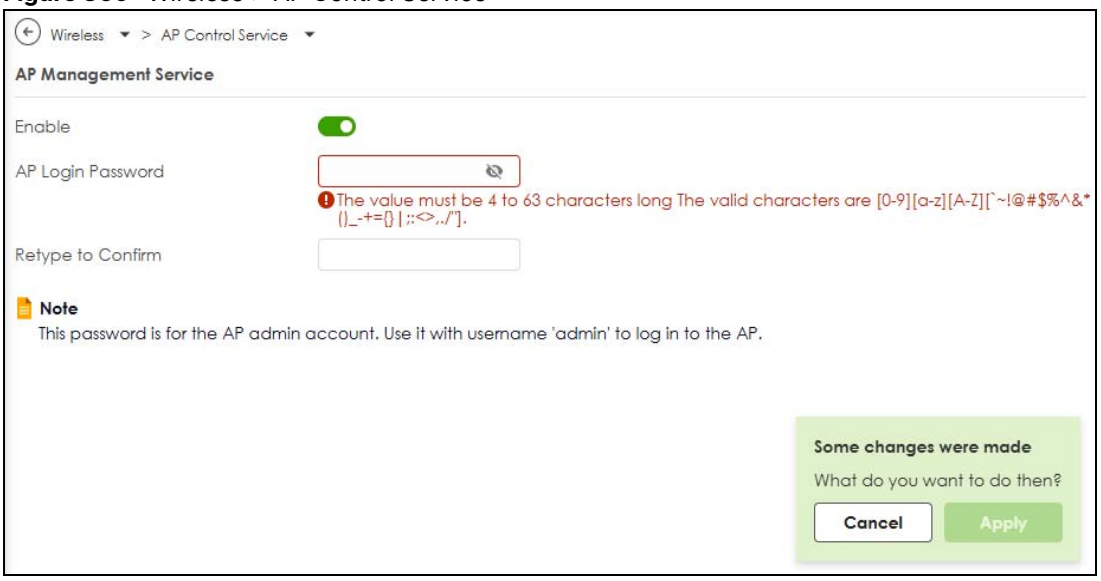
Note: If the **Rogue AP Detection** is enabled, the Zyxel Device will perform detection every 30 minutes and display the detected devices on **Wireless > Rogue AP Detection**.

29.2 The AP Control Service Screen

The **Wireless** > **AP Control Service** screen allows you to change the password for all accounts with the username "admin" on APs listed in the managed AP list. View the managed AP list in **Wireless** > **Access Points** > **AP List**.

Note: Only the account passwords with the username “admin” will be changed, not all admin-type account passwords will be.

Figure 309 Wireless > AP Control Service



The following table describes the labels in this screen.

Table 231 Wireless > AP Control Service

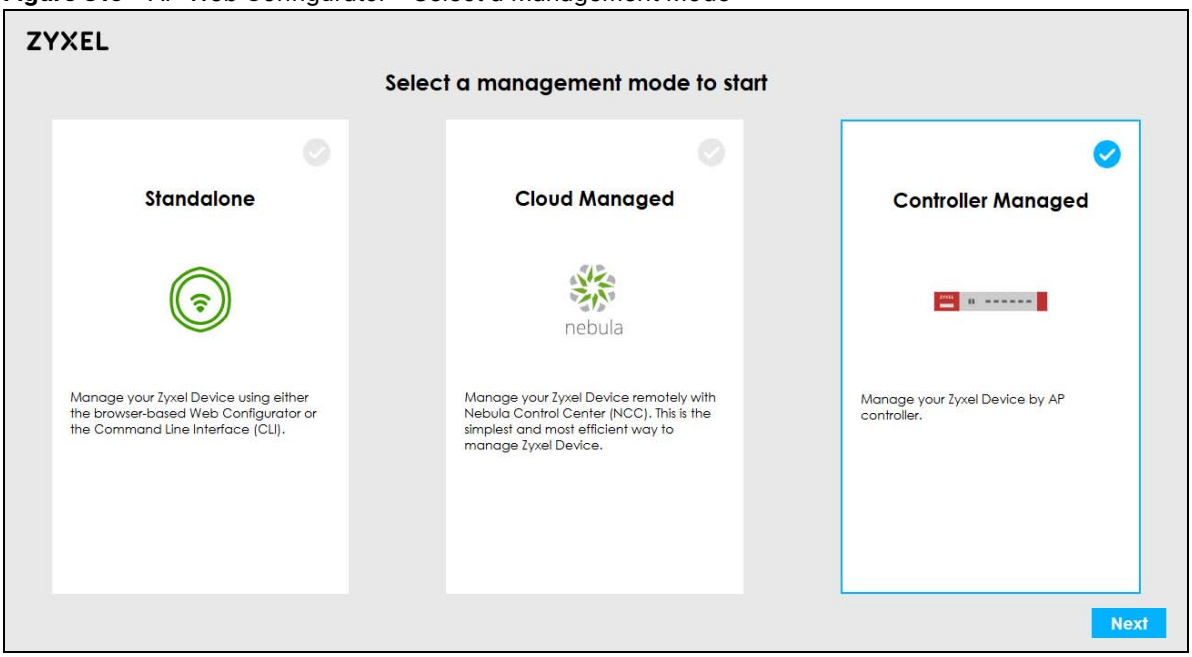
LABEL	DESCRIPTION
AP Management Service	
Enable	Click the switch to the right to change the password for accounts with the username “admin” on the managed APs.
AP Login Password	Set the password for accounts with the username “admin” on the managed APs. You can use 4 to 63 alphanumeric characters. The following special characters are allowed: ~!@#$%^&*()_-+={}|;:<>,./"
Retype to Confirm	Enter the password again for confirmation.
Server Certificate	Select the certificate that will be used when wireless clients on managed APs perform 802.1X authentication against the Zyxel Device’s internal authentication server. By default, the Zyxel Device uses the “default” certificate for AP management. To use a different certificate, click the drop-down list and select a certificate that you have configured in the **System > My Certificates** screen.
Cancel	Click **Cancel** to return the screen to its last-saved settings.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

29.3 The AP List Screen

To ensure the AP you want to manage appears on the AP list:

- Make sure the AP connected to the Zyxel Device is in the same subnet as the Zyxel Device.
- Make sure the AP is in **Controller Managed** mode. If not, reset the AP. On your first login, the following screen appears, select **Controller Managed** mode.

Figure 310 AP Web Configurator – Select a Management Mode

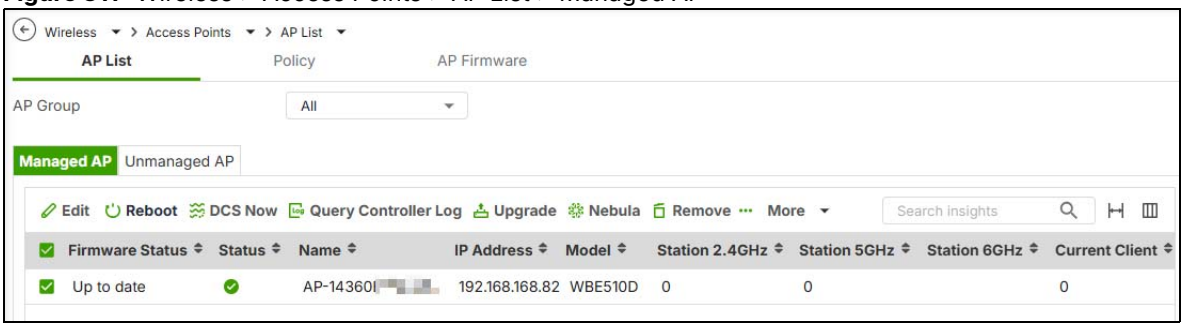


29.3.1 The AP List > Managed AP Screen

Use this screen to view the managed APs. Click **Wireless** > **Access Points** > **AP List** > **Managed AP** to open this screen.

Note: You must enable **AP Control Service** in the **Wireless** > **AP Control Service** screen to view this screen.

Figure 311 Wireless > Access Points > AP List > Managed AP



The following table describes the labels in this screen.

Table 232 Wireless > Access Points > AP List > Managed AP

LABEL	DESCRIPTION
AP Group	Select the group of APs you want to display. You can create or remove an AP group in **Wireless** > **WLAN Settings** > **SSID Settings** > **AP Group Settings**.
Managed AP	The APs managed by the Zyxel Device appear here.
Refresh	Click this button to update the information on the screen. The screen also refreshes automatically when you open the screen.

Table 232 Wireless > Access Points > AP List > Managed AP (continued)

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Reboot	Select one or multiple APs and click this button to force the AP(s) to restart.
DCS Now	Select one or multiple APs and click this button to use DCS to allow the AP to automatically find a less-used channel in an environment where there are many APs and there may be interference. See Dynamic Channel Selection (DCS) on page 507. Note: You should have enabled DCS in the applied AP radio profile before the APs can use DCS. DCS is not supported on the radio which is working in repeater AP mode.
Query Controller Log	Select one or multiple APs and click this button to go to the **Log & Report** > **Log/ Events** > **AP** screen to view the selected AP's current log messages.
Upgrade	Select one or more APs and click this button to update the APs' firmware version.
Nebula	Select an AP and click this to open a screen where you can set whether the AP's IP address and VLAN settings will be changed when it goes into Nebula cloud management mode. Note: The AP will be set to Nebula cloud management mode and removed from the managed AP list right after you click **OK**.
Remove	Select one or multiple APs and click this button to remove the AP(s) from the manged AP list.
Move to Group	Select an AP and click this button to change the AP group it belongs to.
Suppression On	Select an AP and click this button to enable the AP's LED suppression mode. All the LEDs of the AP will turn off after the AP is ready. This button is not available if the selected AP doesn't support suppression mode.
Suppression Off	Select an AP and click this button to disable the AP's LED suppression mode. The AP LEDs stay lit after the AP is ready. This button is not available if the selected AP doesn't support suppression mode.
Locator On	Select an AP and click this button to run the locator feature. The AP's Locator LED will start to blink for 10 minutes by default. It will show the actual location of the AP between several devices on the network.
Smart Mesh Reconnect	Select an AP and click this button to make the AP look for and connect to another uplink AP with a stronger signal. Smart Mesh is a WiFi mesh solution for APs. With Smart Mesh, you can have two or more APs automatically create a mesh network within your home or office, ensuring there are no areas with a weak WiFi signal.
Tag	Select an AP group from the **AP Group** drop-down list first. Select one or more APs and click this button to manage their tags. You can add or remove one or more tags at once to the selected AP(s) using the **Append** and **Remove** drop-down lists. You can assign up to 32 tags to one AP. You can also create new tags. A tag name can contain 1–32 single-byte characters, including [A–Z], [a–z], [0–9], [@#-_]. Note: An AP's tags are removed when you move it to another AP group.
Firmware Status	This shows whether the firmware installed on the AP is up-to-date. Click **Update Available** to update the AP's firmware.

Table 232 Wireless > Access Points > AP List > Managed AP (continued)

LABEL	DESCRIPTION
Status	This shows the status of AP. Hover your mouse over the icon to view the status. • **RUN**: The AP is online and operating normally. • **Config Failure**: The AP failed to apply the configuration from the Zyxel Device. • **Limited AP**: The AP has features that are not supported by the Zyxel Device. • **VLAN Conflict**: The AP is not reachable by the Zyxel Device due to the VLAN configuration. • **Offline Update**: The AP is rebooting in preparation for the firmware update. • **Updating**: The AP has rebooted and is currently updating the firmware. • **Offline**: The Zyxel Device has not received keep-alive packets from the AP for the past 2 minutes. Double-click the AP to view its **Status** in the **Edit AP** screen for details.
Name	This shows the descriptive name of the AP.
IP Address	This shows the IP address of the AP.
Model	This shows the model number of the AP.
Station 2.4GHz	This shows the number of 2.4G wireless clients connected to the AP.
Station 5GHz	This shows the number of 5G wireless clients connected to the AP.
Station 6GHz	This shows the number of 6G wireless clients connected to the AP.
Current Client	This shows how many clients are currently connecting to the AP.
MAC Address	This shows the MAC address of the AP.
2.4GHz	This shows the number of WiFi clients in the 2.4 GHz band.
5GHz	This shows the number of WiFi clients in the 5 GHz band.
6GHz	This shows the number of WiFi clients in the 6 GHz band.
Channel Utilization 2.4GHz	This shows the percentage of the 2.4 GHz channel ID usage.
Channel Utilization 5GHz	This shows the percentage of the 5 GHz channel ID usage.
Channel Utilization 6GHz	This shows the percentage of the 6 GHz channel ID usage.
Transmit Power 2.4GHz	This shows the current transmitting power of the connected AP's 2.4 GHz band.
Transmit Power 5GHz	This shows the current transmitting power of the connected AP's 5 GHz band.
Transmit Power 6GHz	This shows the current transmitting power of the connected AP's 6 GHz band.
% Usage	This shows the percentage of the AP's data usage.
Serial Number	This shows the serial number of the AP.
Recent On-line Time	This shows the most recent time the AP came on-line. **N/A** shows if the AP has not come on-line since the Zyxel Device last started up.
Hop	This shows how many APs away the AP is from the Root AP. (the AP connected to the Zyxel Device). For example, a value of 1 indicates the AP is the first AP after the root AP, while 2 indicates there is one AP between the AP and the root AP. This field is blank when the AP is the root AP.
Uplink AP	This shows the name of the uplink AP connected to the AP. See Uplink and Downlink on page 506 for the definition of uplink.
Uplink Signal	This shows the signal strength the AP receives from the uplink AP.
Uplink Tx/Rx Rate	This shows the maximum transmission/reception rate of the uplink AP to which the AP is connected.
Wireless Bridge	This shows whether wireless bridge is enabled on the AP. Wireless bridge enables two devices to automatically bridge two network segments through a WiFi connection. When enabled, the system will automatically create VLAN and bridge interfaces based on the **Allowed VLANs** you configure below. The Zyxel Device can continue data transmission through its Ethernet port(s) even after the smart-mesh link is established.

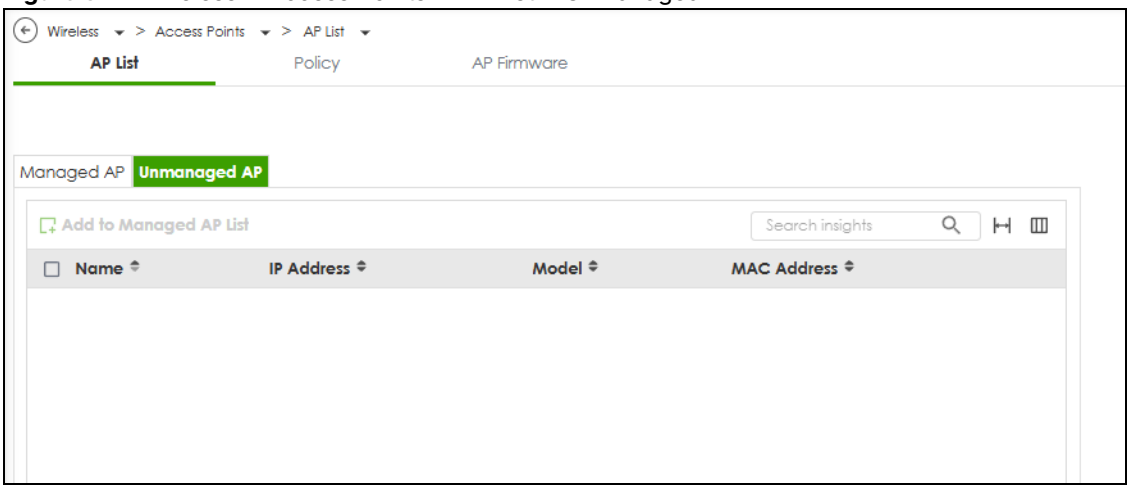
Table 232 Wireless > Access Points > AP List > Managed AP (continued)

LABEL	DESCRIPTION
Uplink	This shows the frequency band the AP uses to connect to the uplink AP.
Mgnt. VLAN ID (AC/AP)	This shows the Access Controller (the Zyxel Device) and runtime management VLAN ID setting for the AP. **VLAN Conflict** shows if the AP's management VLAN ID does not match the **Mgnt. VLAN ID(AC)**. This shows **n/a** if the Zyxel Device cannot get VLAN information from the AP.
Last Off-line Time	This shows the date and time that the AP was last logged out.
Ethernet Uplink	This shows whether the AP is connected to the gateway through a wired Ethernet APconnection or WiFi connection.
Power Mode	This shows the AP's power status. The AP receives power using a power adapter and/or through a PoE switch/injector. • **Full** – the AP receives power using IEEE 802.3at PoE plus. The PoE device that supports IEEE 802.3at PoE Plus can supply power of up to 30W per Ethernet port. When the AP's power mode is **Limited**, the AP throughput decreases and has just one transmitting radio APchain. • **Limited** – the AP receives power using IEEE 802.3af PoE even when it is also connected to a power source using a power adapter. The PoE device that supports IEEE 802.3af PoE can supply power of up to 15.4W per Ethernet port. It always shows **Full** if the AP does not support power detection.
Current Version	This shows the AP's current firmware version.
Group	This shows the name of the AP group to which the AP belongs.
LED	This shows the AP LED status. • **N/A** shows if the AP does not support LED suppression mode and/or have a locator LED to show the actual location of the AP. • A gray LED icon signifies that the AP LED suppression mode is enabled. All the LEDs of the AP will turn off after the AP is ready. • A green LED icon signifies that the AP LED suppression mode is disabled and the AP LED stay lit after the AP is ready. • A sun icon signifies that the AP's locator LED is blinking. • A circle signifies that the AP's locator LED is extinguished.
Tag	This shows the tag(s) assigned to the AP.
Bluetooth	This shows the AP's Bluetooth Low Energy (BLE) capability. Bluetooth Low Energy, which is also known as Bluetooth Smart, transmits less data over a shorter distance and consumes less power than classic Bluetooth. APs communicate with other BLE enabled devices using advertisements. • **N/A** shows if the AP does not support BLE. • **Unavailable** shows if the AP supports Bluetooth, but there is no BLE USB dongle connected to the USB port of the AP. Some APs, such as the WAC5302D-S, need to have a supported BLE USB dongle attached to act as a beacon to broadcast packets. • **Available** shows if the AP supports Bluetooth, detects a BLE device and advertising is inactive. • **Advertising** shows if the AP supports Bluetooth, detects a BLE device and advertising is activated, which means the BLE device can broadcasts packets to every device around it.
Location	This shows the AP's location you configured.
System Name	This shows the system name to identify the AP on a network.
Load Balancing Group	AP load balancing lets the Zyxel Device distribute WiFi clients and traffic across APs connected to the Zyxel Device to prevent overloading of APs with higher loads and lower signal quality. This shows the load balancing group name to which this AP belongs. An AP can belong to up to two load balancing groups. APs in the same load balancing group within an AP group share the client load.

29.3.2 The AP List > Unmanaged AP Screen

Use this screen to view the unmanaged APs detected by the Zyxel Device. Click **Wireless** > **Access Points** > **AP List** > **Unmanaged AP** to open this screen.

Figure 312 Wireless > Access Points > AP List > Unmanaged AP



The following table describes the labels in this screen.

Table 233 Wireless > Access Points > AP List > Unmanaged AP

LABEL	DESCRIPTION
Unmanaged AP	The APs connected to and detected by the Zyxel Device appear here. To have the Zyxel Device manage an AP, select it and click **Add to Managed AP List**.
Refresh	Click this button to update the information on the screen. The screen also refreshes automatically when you open the screen.
Add to Managed AP List	Select an AP and click this to add the selected AP to the managed AP list.
Name	This shows the descriptive name of the AP.
IP Address	This shows the global (WAN) IP address of the AP.
Model	This shows the model number of the AP.
MAC Address	This shows the MAC address of the AP.

29.3.3 Edit AP List

This screen allows you to configure AP's settings. Click **Wireless** > **Access Points** > **AP List** > **Edit AP List** to open the following screen.

29.3.3.1 Storm Control

Storm control prevents broadcast/multicast storms on AP interfaces. A broadcast/multicast storm occurs when broadcast/multicast packets flood devices in the same subnet, creating excessive traffic and degrading network performance.

When storm control is enabled on the Zyxel Device, the AP monitors packets received on the its interface and determines whether the packets are broadcast or multicast. The AP monitors the number of broadcast packets received within a one-second time interval. When the interface maximum packets per second threshold is met, incoming data traffic on the AP interface is dropped until the maximum packets per second falls below the threshold.

Figure 313 Wireless > Access Points > AP List > Edit AP List

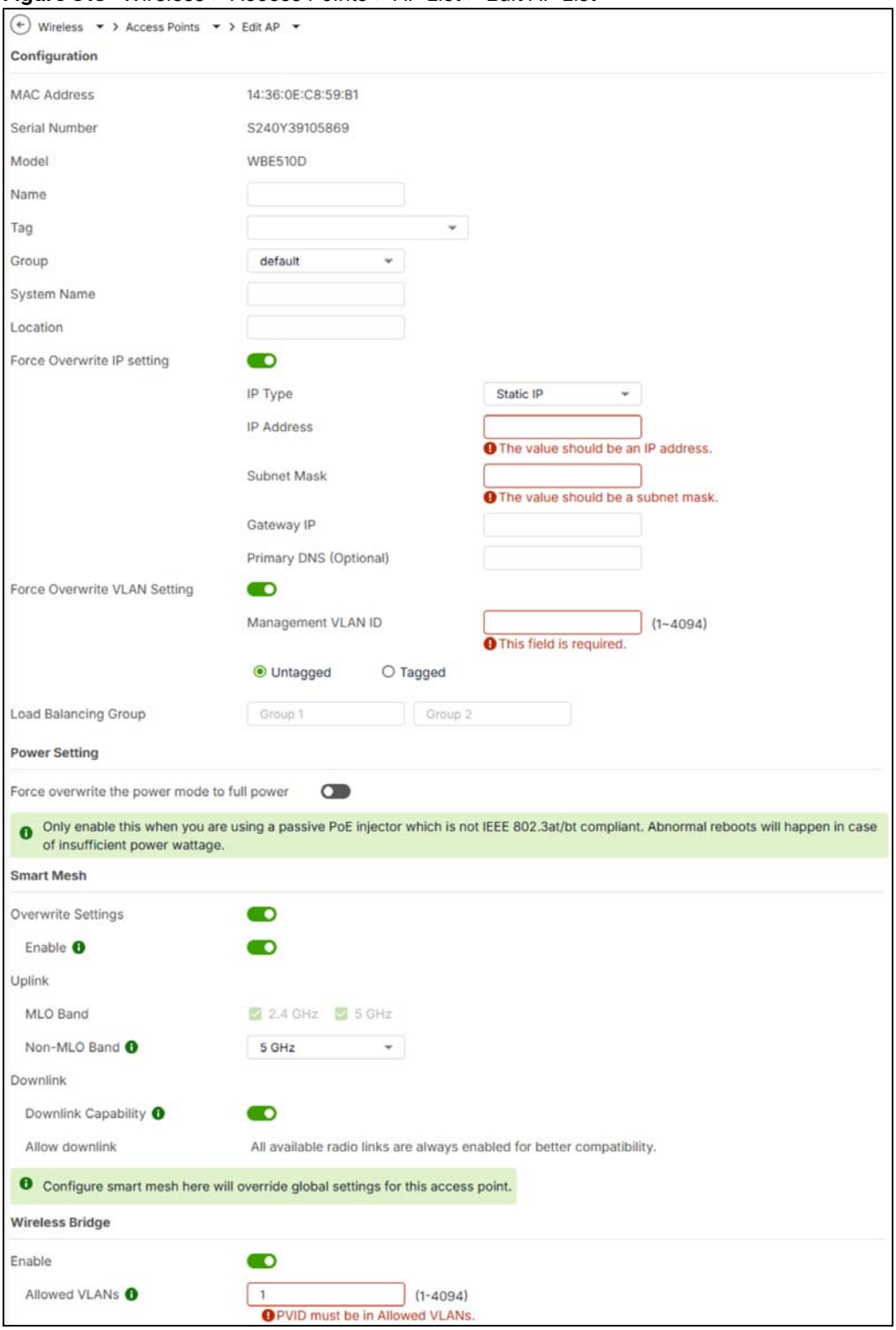
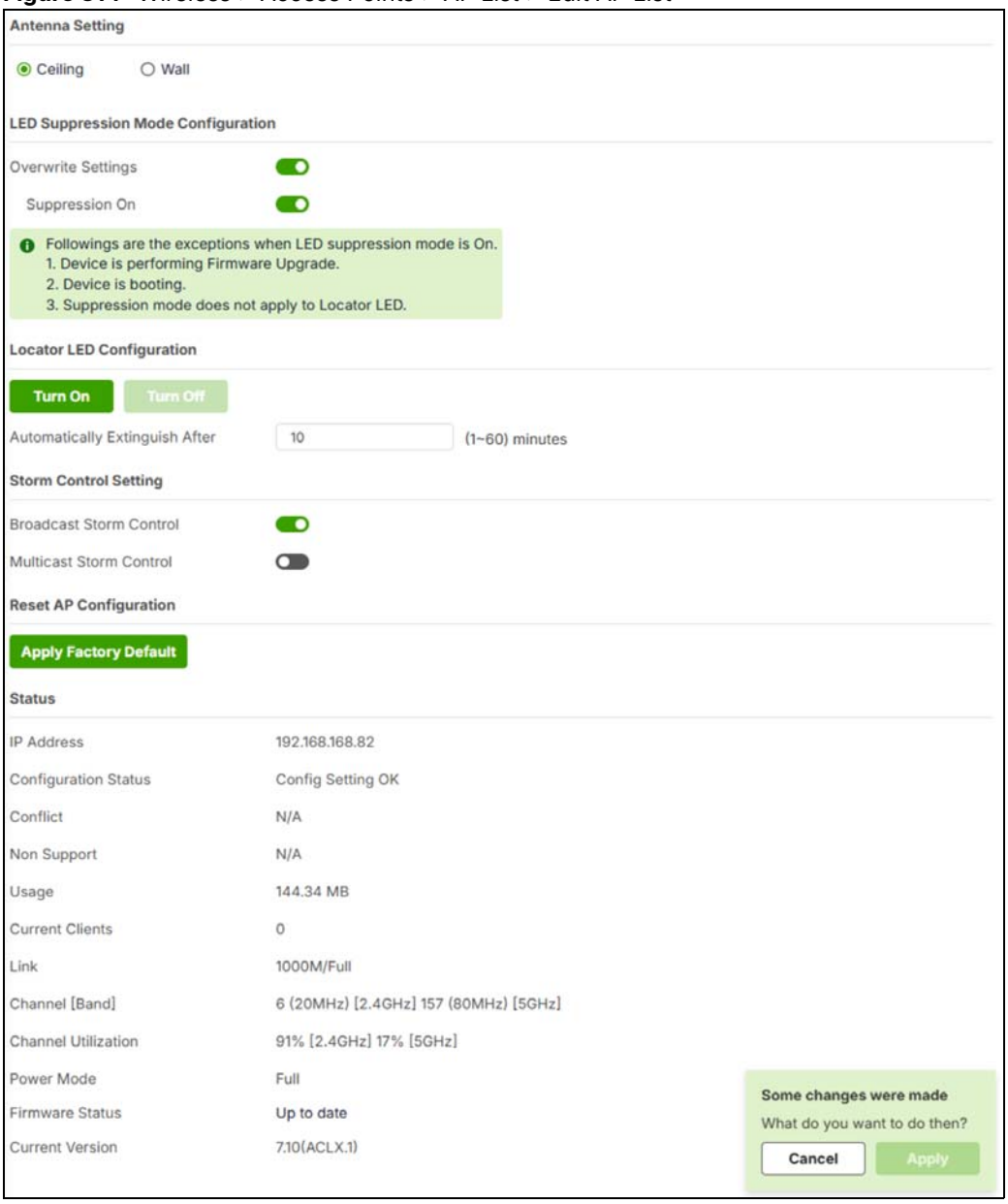


Figure 314 Wireless > Access Points > AP List > Edit AP List



The following table describes the labels in this screen.

Table 234 Wireless > Access Points > AP List > Edit AP List

LABEL	DESCRIPTION
Configuration	
MAC Address	This shows the MAC address of the AP.
Serial Number	This shows the serial number of the AP.
Model	This field displays the AP's hardware model information. It displays **N/A** (not applicable) only when the AP disconnects from the Zyxel Device and the information is unavailable as a result.
Name	Enter a descriptive name for the AP.

Table 234 Wireless > Access Points > AP List > Edit AP List (continued)

LABEL	DESCRIPTION
Tag	Select the tags you want to assign to the AP. You can also create new tags. You can assign up to 32 tags to one AP. A tag name can contain 1–32 single-byte characters, including [A–Z], [a–z], [0–9], [@#-_].
Group	Select an AP group to which you want the AP to belong.
System Name	Enter a name to identify the AP on a network. This is usually the AP's fully qualified domain name.
Location	Specify the name of the place where the AP is located.
Force Overwrite IP setting	Select this to change the AP's IP address setting to match the configuration in this screen.
IP Type	• Select **DHCP** to have the AP act as a DHCP client and automatically get the IP address, subnet mask, and gateway address from a DHCP server. • Select **Static IP** if you want to specify the IP address, subnet mask, gateway and DNS server address manually.
IP Address	Enter the IP address for the AP.
Subnet Mask	Enter the subnet mask of the AP in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all devices in the network.
Gateway IP	Enter the IP address of the gateway. The AP 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 AP.
Primary DNS (Optional)	Enter the IP address of the DNS server.
Force Overwrite VLAN Setting	Select this to have the Zyxel Device change the AP's management VLAN to match the configuration in this screen.
Management VLAN ID	Enter a VLAN ID for the AP.
Untagged	Select this so the outbound traffic transmitted through the Zyxel Device Ethernet port will not be tagged with the Management VLAN ID.
Tagged	Select this to make the Zyxel Device adds the Management VLAN ID to outbound traffic transmitted through its Ethernet port.
Load Balancing Group	A load balancing group name can contain 1–32 single-byte characters, including [A–Z], [a–z], [0–9], [@#-_].
Rogue AP Detection	
Overwrite Settings	Enable this to override the **Rogue AP Detection** settings for the entire AP group in **Wireless** > **WLAN Settings** > **AP Settings**, so you can control the managed AP individually.
Enable	Enable this to allow the Zyxel Device to monitor the managed AP for rogue AP detection. You can configure detection rules for suspected rogue APs on the **Wireless > Rogue AP Detection** screen. See Section 29.15 on page 558 for details.
Power Setting	
Force overwrite the power mode to full power	Enable this if your AP is using a PoE injector that does not support PoE negotiation. Otherwise, the AP cannot draw full power from the power sourcing equipment. Enable this power mode to improve the AP's performance in this situation. Note: Ensure that the power sourcing equipment can supply enough power to the AP to avoid abnormal system reboots. Note: Only enable this if you are using a passive PoE injector that is not IEEE 802.3at/bt compliant but can still provide full power.
Smart Mesh	
Overwrite Settings	Enable this to override the Smart Mesh settings for the entire AP group in **Wireless** > **WLAN Settings** > **AP Settings**, so you can control the AP individually.

Table 234 Wireless > Access Points > AP List > Edit AP List (continued)

LABEL	DESCRIPTION
Enable	Click to enable or disable the Smart Mesh feature on the AP. Smart Mesh is a WiFi mesh solution for APs. With Smart Mesh, you can have two or more APs automatically create a mesh network within your home or office, ensuring there are no areas with a weak WiFi signal.
Uplink See Uplink and Downlink on page 506 for the definition of uplink.	
MLO Band	Select at least two frequency bands for MLO to work. With MLO (Multi-Link Operation), a WiFi7 client can connect to the AP using multiple frequency bands simultaneously. This increases speed and improves reliability of the WiFi connection. MLO makes WiFi7 ideal for streaming 4K / 8K videos, using augmented reality (AR), virtual reality (VR) applications and playing online games.
Non-MLO Band	This shows the frequency band which this network uses if the AP does not support MLO. • Select **Auto (High Band Preferred)** to allow the AP to select a higher radio band mesh controller. • Select **2.4 GHz** to use the 2.4 GHz band for regular Internet surfing and downloading. • Select **5 GHz** or **6 GHz** to use the 5 or 6 GHz band for time sensitive traffic like high-definition video, music, and gaming. Note: 6 GHz displays only for APs that support it.
Downlink See Uplink and Downlink on page 506 for the definition of downlink.	
Downlink Capability	Enable this to allow the AP provides downlink capability to other APs (repeaters).
Wireless Bridge	This feature enables two devices to automatically bridge two network segments through a WiFi connection. Enable **Wireless Bridge** when the Zyxel Device is connected to a root AP, so as to allow traffic through the Ethernet port on the Zyxel Device to a wired network. When enabled, the system will automatically create VLAN and bridge interfaces based on the **Allowed VLANs** you configure below. The Zyxel Device can continue data transmission through its Ethernet port(s) even after the smart-mesh link is established. Note: Be careful to avoid bridge loops. A bridge loop occurs when there are two layer-2 paths between the same endpoints, causing broadcast packets to be sent back and forth indefinitely.
Allowed VLANs	Enter the IDs of the VLANs that the Zyxel Device will forward over the wireless bridge. You can enter multiple IDs separated by a comma (1,3,5) or a range separated by a hyphen (7-11) or a combination of both (1,3,5,7-11).
Antenna Setting	This section is available only when the AP has an antenna switch. The screen varies depending on whether the AP has a physical antenna switch or allows you to change antenna orientation settings on a per-radio basis or on a per-AP basis.
Ceiling / Wall	This allows you to adjust coverage depending on the antenna orientation of the AP's radios for better coverage. Select **Wall** if you mount the AP to a wall. Select **Ceiling** if the AP is mounted on a ceiling. You can switch from **Wall** to **Ceiling** if there are still wireless dead zones, and vice versa.
LED Suppression Mode Configuration	LED suppression turns off all the LEDs on the AP. To check if this managed AP supports LED suppression, see the AP User's Guide or Online Help.
Overwrite Settings	Enable this to allow the AP **LED Suppression Mode Configuration** setting (on or off) to override the AP group setting.

Table 234 Wireless > Access Points > AP List > Edit AP List (continued)

LABEL	DESCRIPTION
Suppression On	Click to slide the switch to the right to enable the AP's LED suppression mode. All the LEDs of the AP will turn off after the AP is ready. Click to slide the switch to the left to disable the AP's LED suppression mode. All the LEDs of the AP will turn on (default) after the AP is ready.
Locator LED Configuration	Click **Turn On** button to activate the locator. The Locator function will show the actual location of the Zyxel Device between several devices in the network. Otherwise, click **Turn Off** to disable the locator feature.
Automatically Extinguish After	Enter a time interval between 1 and 60 minutes to stop the locator LED from blinking. Default is 10 minutes.
Storm Control Setting	
Broadcast Storm Control	Enabling this will drop ingress broadcast traffic in the physical Ethernet port if it exceeds the maximum traffic rate. The maximum traffic rate can be changed using the CLI (see CLI Reference Guide). Ethernet storm control prevents WiFi clients from receiving excessive broadcast traffic sent from wired clients in the same subnet. Wireless storm control prevents wired clients from receiving excessive broadcast traffic sent from WiFi clients in the same subnet. See Section 29.3.3.1 on page 515 for more information on storm control.
Multicast Storm Control	Enabling this will drop ingress multicast traffic in the physical Ethernet port if it exceeds the maximum traffic rate. The maximum traffic rate can be changed using the CLI (see CLI Reference Guide). Ethernet storm control prevents WiFi clients from receiving excessive multicast traffic sent from wired clients in the same subnet. Wireless storm control prevents wired clients from receiving excessive multicast traffic sent from WiFi clients in the same subnet. See Section 29.3.3.1 on page 515 for more information on storm control.
Reset AP Configuration	Click **Apply Factory Default** to reset all of the AP settings to the factory defaults.
Status	
IP Address	This shows the IP address of the AP.
Configuration Status	This shows whether or not any of the AP's configuration is in conflict with the Zyxel Device's settings for the AP.
Conflict	This shows the settings configured in this screen that the AP does not support and cause the radio to go down. If the AP supports all settings, it shows **N/A**.
Non Support	This shows the settings configured on the AP that are not supported by the AP. If the AP supports all settings, it shows **N/A**.
Usage	This shows the amount of data consumed by the AP's clients.
Current Clients	This shows how many clients are currently connecting to the AP.
Link	This shows the speed and duplex mode of the Ethernet connection on the AP's ports.
Channel [Band]	This shows the radio's channel ID.
Channel Utilization	This shows how much IEEE 802.11 traffic the radio can receive on the channel. It displays what percentage of the radio's channel is currently being used.

Table 234 Wireless > Access Points > AP List > Edit AP List (continued)

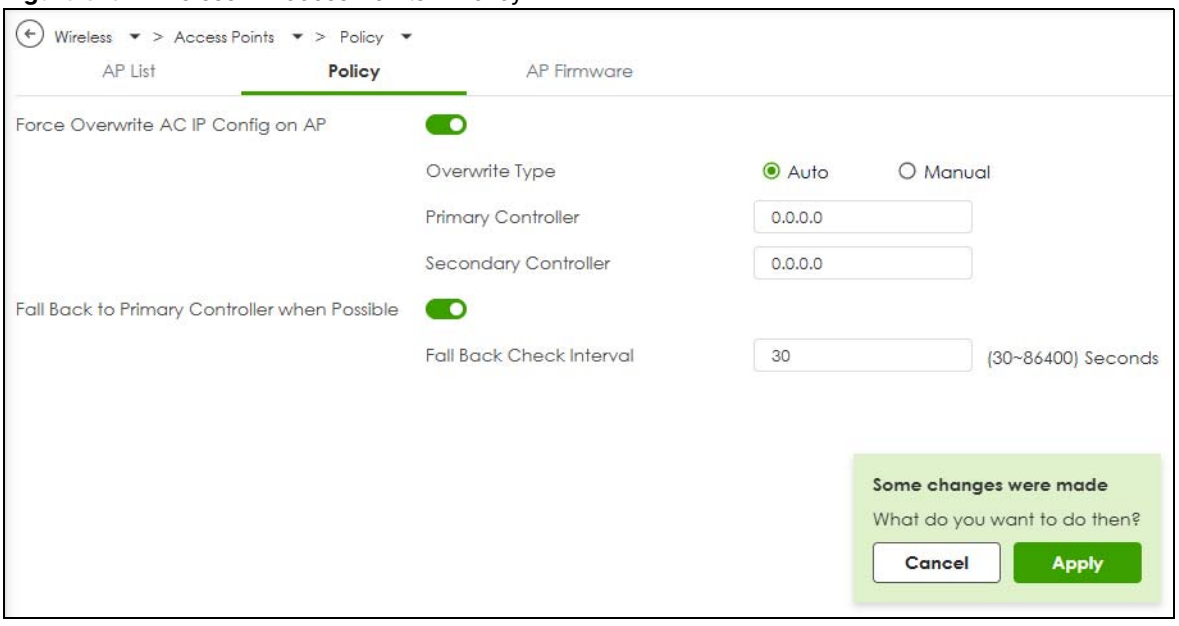
LABEL	DESCRIPTION
Power Mode	This field displays the AP's power status. • **Full** - the AP receives power using a power adapter and/or through a PoE switch/injector using IEEE 802.3at PoE plus. The PoE device that supports IEEE 802.3at PoE Plus can supply power of up to 30W per Ethernet port. When the AP is in **Limited** power mode, the AP throughput decreases and has just one transmitting radio chain. • **Limited** - the AP receives power through a PoE switch/injector using IEEE 802.3af PoE even when it is also connected to a power source using a power adaptor. The PoE device that supports IEEE 802.3af PoE can supply power of up to 15.4W per Ethernet port. It always shows **Full** if the AP does not support power detection.
Firmware Status	This shows whether the firmware installed on the AP is up-to-date.
Current Version	This shows the AP's current firmware version.
Cancel	Click **Cancel** to return the screen to its last-saved settings.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

29.4 The Policy Screen

Use this screen to configure the AP controllers' IP addresses on the managed APs and determine if managed APs should use the **Primary Controller** when possible.

Click **Wireless** > **Access Points** > **Policy** to open this screen.

Figure 315 Wireless > Access Points > Policy



The following table describes the labels in this screen.

Table 235 Wireless > Access Points > Policy

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

29.5 The AP Firmware Screen

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

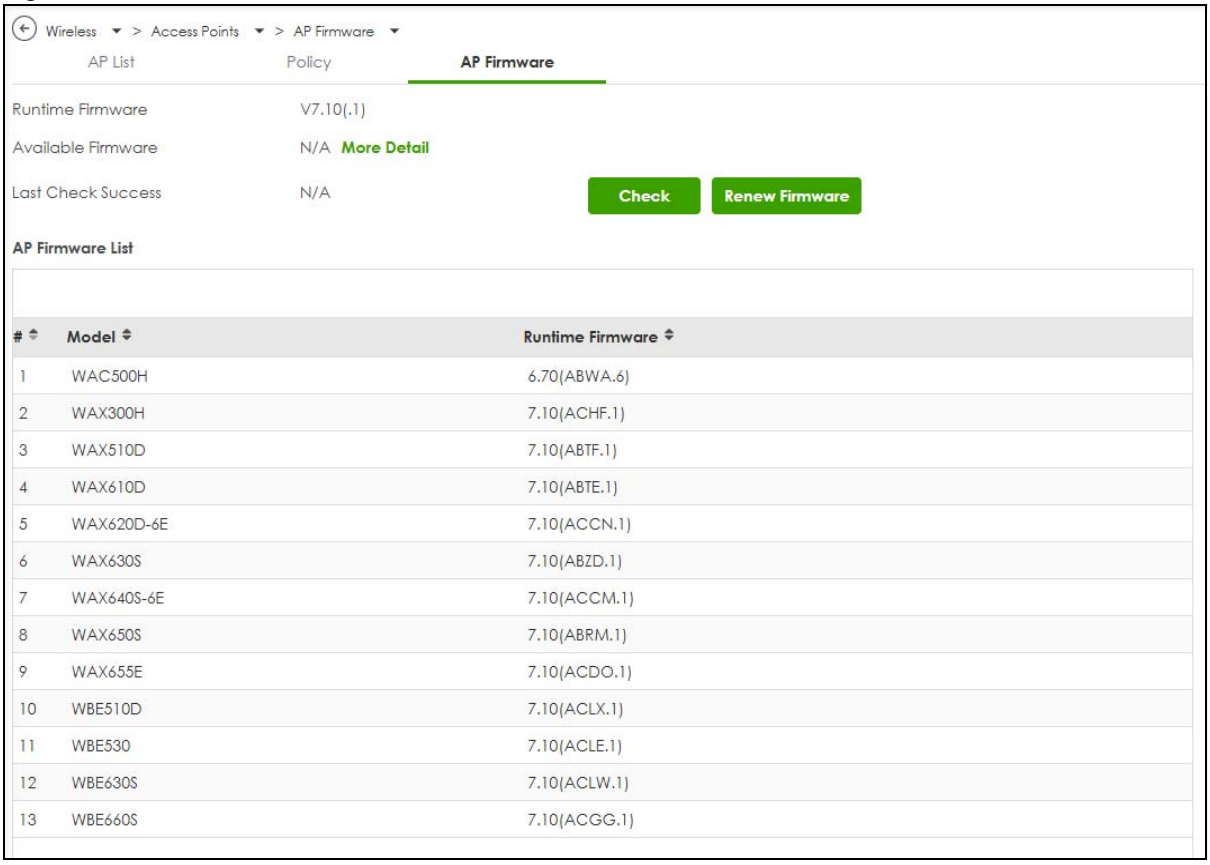
When an AP connects to the Zyxel Device wireless controller, the Zyxel Device will check if the AP has the same firmware version as the AP firmware on the Zyxel Device. If yes, then the Zyxel Device can manage it. If no, then the AP must upgrade (or downgrade) its firmware to be the same version as the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

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

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

Click **Wireless** > **Access Points** > **AP Firmware** to open this screen.

Figure 316 Wireless > Access Points > AP Firmware



The following table describes the labels in this screen.

Table 236 Wireless > Access Points > AP Firmware

LABEL	DESCRIPTION
Runtime Firmware	This shows the current AP firmware version on the Zyxel Device. The Zyxel Device must have the latest AP firmware to manage all supported APs.
Available Firmware	This shows if there is a later AP firmware version available on the firmware server. It shows **N/A** if the Zyxel Device is not connected to the firmware server. Check that the Zyxel Device has Internet access if **N/A** shows and then click the **Check** button below. If a newer Zyxel Device AP firmware is available, its version number and a **More Details** icon shows here.
Last Check Success	This shows the date and time the last check for new firmware was made and whether the check is in progress (**Checking**), was successful (**Success**), or has failed (**Fail**).
Check	Click this button to have the Zyxel Device display the latest AP firmware version available on the firmware server.
AP Firmware List	
#	This is an index number of a managed AP.
Model	This shows the name of all manageable AP models.
Runtime Firmware	This shows the firmware version that the managed AP must have in order to be managed by the Zyxel Device. Firmware for APs that the Zyxel Device already has shows in bold; firmware that the Zyxel Device doesn't have or is still downloading is grayed out. Firmware that is in the download queue will show **To be downloaded**.

29.6 The Client List Screen

This screen shows a list of WiFi clients connected to APs in the specified AP group.

29.6.1 The WLAN Clients > Client List > All Clients Screen

Click **Wireless** > **WLAN Clients** > **Client List** > **All Clients** to open this screen.

Note: Blocked WiFi clients cannot associate with all APs in the AP group and the Zyxel Device.

Figure 317 Wireless > WLAN Clients > Client List > All Clients



The following table describes the labels in this screen.

Table 237 Wireless > WLAN Clients > Client List > All Clients

LABEL	DESCRIPTION
AP Group	Select the type of APs you want to display. Select **All** to show all kinds of APs that are currently or used to be connected to the Zyxel Device. Select **default** to show APs that do not belong to a specific AP group. These APs will automatically belong to the **default** group.
All Clients	
Refresh	Click this button to update the information on the screen. The screen also refreshes automatically when you open the screen.
Policy	First select one or multiple WiFi clients identify by their MAC address to edit. Click this to configure the policy for the selected client. See Section 29.6.2 on page 525 for more information.
Add Policy Clients	Click this to add a WiFi client and configure its policy. See Section 29.6.3 on page 526 for more information.
MAC Address	This shows the MAC address of the WLAN client.
Host Name	This shows the host name of the WLAN client.
Connected to	This shows if the client is connected directly to the Zyxel Device or to an AP that is connected to the Zyxel Device.
AP Group	This shows the name of the AP to which the client is connected.
SSID	This shows the name of the Access Point and Zyxel Device's WiFi network to which the client is connected.
Security	This shows the encryption method used to connect to the Access Point and the Zyxel Device.
Channel	This shows the channel number currently used by the WiFi interface.
Band	This shows the frequency band which is currently being used by the WLAN client.
Signal Strength	This shows the signal strength of the WLAN client.

Table 237 Wireless > WLAN Clients > Client List > All Clients (continued)

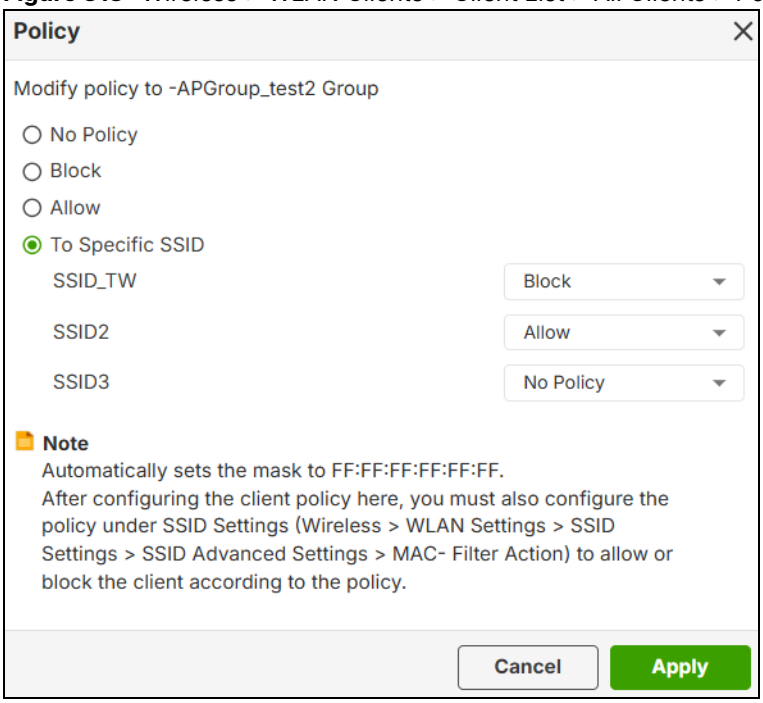
LABEL	DESCRIPTION
IPv4 Address	This shows the IP address of the WLAN client.
TX Rate	This shows the transmit data rate of the WLAN client.
RX Rate	This shows the receive data rate of the WLAN client.
Upload	This shows the number of bytes transmitted from the WLAN client.
Download	This shows the number of bytes received by the WLAN client.
Usage	This shows the amount of data consumed by the AP's clients.
Association time	This shows the time duration the WLAN client was online and offline.
Capability	This shows the supported standard currently being used by the station or the standards supported by the station.
802.11 Features	This shows whether the station supports IEEE802.11r, IEEE 802.11k, IEEE 802.11v or none of the above (**N/A**).
VLAN	This shows the ID number of the VLAN to which the client belongs.

29.6.2 The WLAN Clients > All Clients > Client List > Policy Screen

Use this screen to configure a policy to block or allow a connected WiFi client.

Click **Wireless** > **WLAN Clients > Client List** > **All Clients** > **Policy**, then select an AP group, a WiFi client and click **Policy** to open this screen.

Figure 318 Wireless > WLAN Clients > Client List > All Clients > Policy



The following table describes the labels in this screen.

Table 238 Wireless > WLAN Clients > Client List > All Clients > Policy

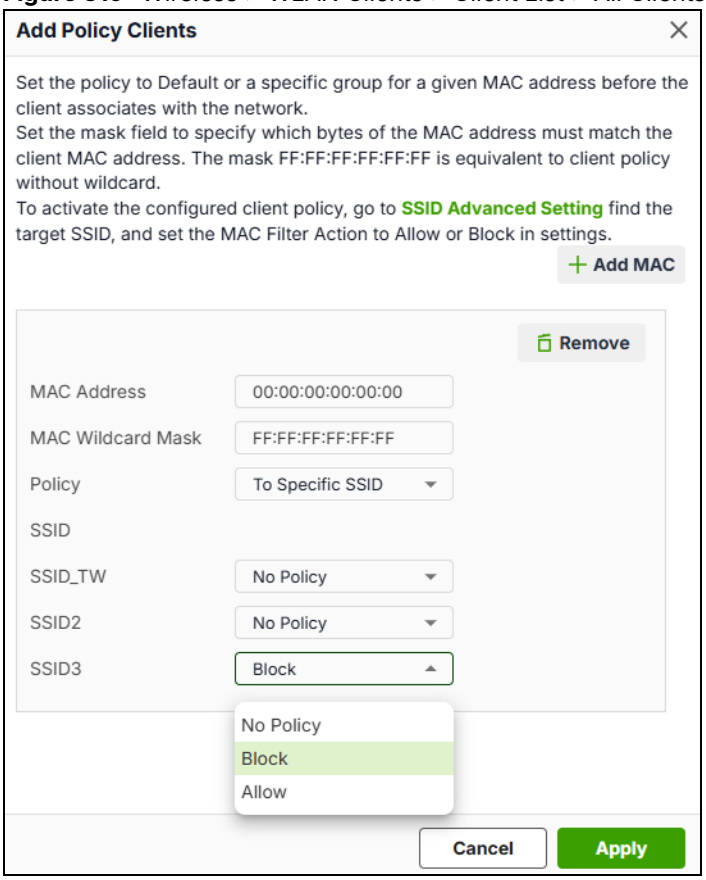
LABEL	DESCRIPTION
No Policy	The Zyxel Device ignores checking the selected WiFi clients' policies for the WiFi networks (SSIDs) in this AP group.
Block	The selected WiFi clients cannot connect to the Zyxel Device and the APs in the AP group.
Allow	The selected WiFi clients can connect to the Zyxel Device and the APs in the AP group.
To Specific SSID	To apply the selected clients' policies to a WiFi network (SSID), you must first enable the WiFi network (SSID) in the **Wireless** > **WLAN Settings** > **SSID Settings** screen.
No Policy	The Zyxel Device ignores checking the selected WiFi clients' policies for the WiFi network (SSID).
Block	The selected clients cannot connect to the WiFi network (SSID).
Allow	The selected clients can connect to the WiFi network (SSID).
Cancel	Click **Cancel** to return the screen to its last-saved settings.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

29.6.3 The WLAN Clients > Client List > All Clients > Add Policy Clients Screen

Use this screen to configure a policy to block or allow a specific MAC address.

Click **Wireless** > **WLAN Clients** > **Client List** > **All Clients**, then select an AP group and click **Add Policy Clients** to open this screen.

Figure 319 Wireless > WLAN Clients > Client List > All Clients > Add Policy Clients



The following table describes the labels in this screen.

Table 239 Wireless > WLAN Clients > Client List > All Clients > Add Policy Clients

LABEL	DESCRIPTION
Add MAC	Click this to add a specific MAC address of a client and configure a policy.
Remove	Click this to remove the policy.
MAC Address	Enter the client's MAC address to apply this security policy.
MAC Wildcard Mask	Use a MAC wildcard mask with a MAC address to create a range of allowed MAC addresses for policy clients. Unlike IP subnet masks, a MAC wildcard mask specifies which parts of a MAC address must match for a rule to apply. An F or f in the mask requires an exact match for the corresponding digit. A 0 allows any value for the corresponding digit. For example, a mask of FF:FF:FF:00:00:00 applied to a MAC address of 96:FA:95:1D:67:4A creates a MAC address range of 96:FA:95:00:00:00 to 96:FA:95:FF:FF:FF. This field cannot be left blank. You must enter 17 characters using F, f, and 0, with every two characters separated by a colon. The default value is all Fs, which represents a specific MAC address.
Policy	Select a security policy that you want to apply to the client with the specified MAC address.
Block	The WiFi client cannot connect to the Zyxel Device and the APs in the AP group.
Allow	The WiFi client can connect to the Zyxel Device and the APs in the AP group.
To Specific SSID	To apply the client's policy to a WiFi network (SSID), you must first enable the WiFi network (SSID) in the **Wireless** > **WLAN Settings** > **SSID Settings** screen.

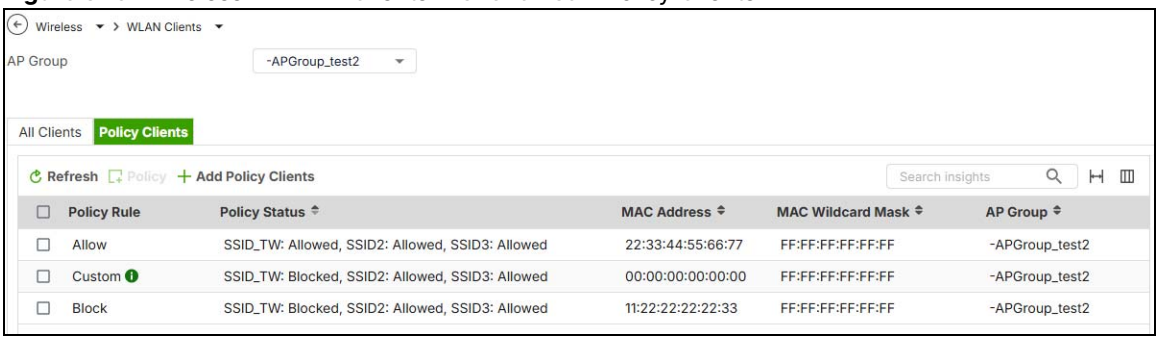
Table 239 Wireless > WLAN Clients > Client List > All Clients > Add Policy Clients

LABEL	DESCRIPTION
No Policy	The Zyxel Device ignores checking the client's policy for the WiFi network (SSID).
Block	The client cannot connect to the WiFi network (SSID).
Allow	The client can connect to the WiFi network (SSID).
Cancel	Click **Cancel** to return the screen to its last-saved settings.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

29.6.4 The WLAN Clients > Client List > Policy Clients Screen

Click **Wireless** > **WLAN Clients** > **Client List** > **Policy Clients** to open this screen.

Figure 320 Wireless > WLAN Clients > **Client List** > Policy Clients



The following table describes the labels in this screen.

Table 240 Wireless > WLAN Clients > Client List > Policy Clients

LABEL	DESCRIPTION
AP Group	Select the type of APs you want to display. Select **All** to show all kinds of APs that are currently or used to be connected to the Zyxel Device. Select **default** to show APs that do not belong to a specific AP group. These APs will automatically belong to the **default** group.
Policy Clients	
Refresh	Click this button to update the information on the screen. The screen also refreshes automatically when you open the screen.
Policy	Click this to configure the policy for the selected clients. See Section 29.6.5 on page 529 for more information.
Add Policy Clients	Click this to add a client and configure its policy. See Section 29.6.6 on page 530 for more information.
Policy Rule	This shows the security policy applied to the client. This field displays **Custom** when the policy is set to allow or block access to specific WiFi networks (SSIDs). Hover over the note icon to view the details.
Policy Status	This shows whether the client is allowed or blocked from connecting to each enabled WiFi Networks (SSIDs). The status are determined by the client's **Policy Rule** and the **MAC-Filter Action** in each SSID profile. Refer to Section 29.9.1 on page 537 for SSID advanced settings.
MAC Address	This shows the MAC address of the WLAN client. for more information.

Table 240 Wireless > WLAN Clients > Client List > Policy Clients (continued)

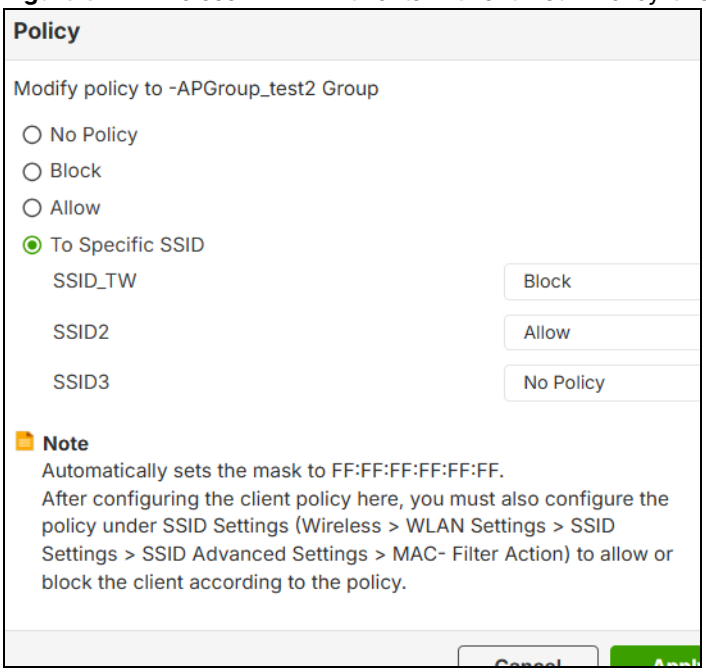
LABEL	DESCRIPTION
MAC Wildcard Mask	Use a MAC wildcard mask with a MAC address to create a range of allowed MAC addresses for policy clients. Unlike IP subnet masks, a MAC wildcard mask specifies which parts of a MAC address must match for a rule to apply. An F or f in the mask requires an exact match for the corresponding digit. A 0 allows any value for the corresponding digit. For example, a mask of FF:FF:FF:00:00:00 applied to a MAC address of 96:FA:95:1D:67:4A creates a MAC address range of 96:FA:95:00:00:00 to 96:FA:95:FF:FF:FF. This field cannot be left blank. You must enter 17 characters using F, f, and 0, with every two characters separated by a colon. The default value is all Fs, which represents a specific MAC address.
AP Group	This shows the name of the AP to which the client is connected.

29.6.5 The WLAN Clients > Client List > Policy Clients > Add Policy Screen

Use this screen to configure a policy to block or allow a connected WiFi client.

Click **Wireless** > **WLAN Clients** > **Client List** > **Policy Clients**, then select an AP group, a WiFi client and click **Add Policy** to open this screen.

Figure 321 Wireless > WLAN Clients > Client List > Policy Clients > Add Policy



The following table describes the labels in this screen.

Table 241 Wireless > WLAN Clients > Client List > Policy Clients > Add Policy

LABEL	DESCRIPTION
No Policy	The Zyxel Device ignores checking the selected WiFi clients' policies for the WiFi networks (SSIDs) in this AP group.
Block	The selected WiFi clients cannot connect to the Zyxel Device and the APs in the AP group.

Table 241 Wireless > WLAN Clients > Client List > Policy Clients > Add Policy (continued)

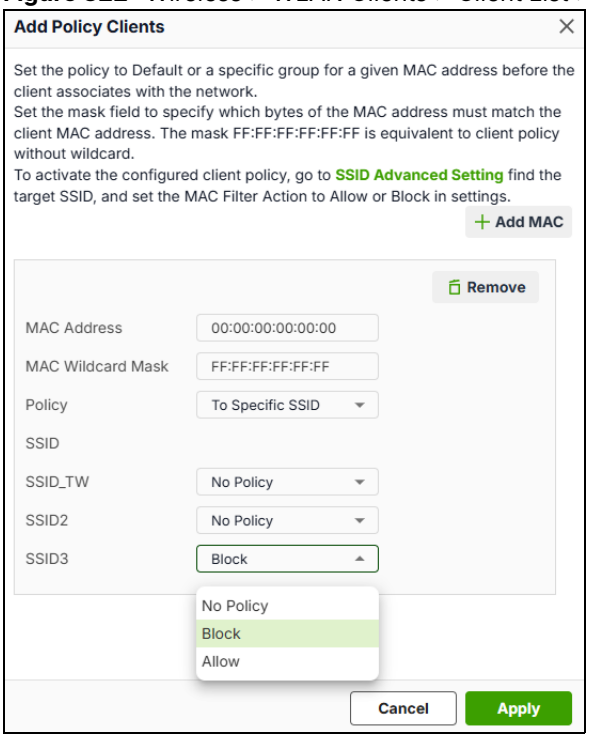
LABEL	DESCRIPTION
Allow	The selected WiFi clients can connect to the Zyxel Device and the APs in the AP group.
To Specific SSID	To apply the selected clients' policies to a WiFi network (SSID), you must first enable the WiFi network (SSID) in the **Wireless** > **WLAN Settings** > **SSID Settings** screen.
No Policy	The Zyxel Device ignores checking the selected WiFi clients' policies for the WiFi network (SSID).
Block	The selected clients cannot connect to the WiFi network (SSID).
Allow	The selected clients can connect to the WiFi network (SSID).
Cancel	Click **Cancel** to return the screen to its last-saved settings.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

29.6.6 The WLAN Clients > Client List > Policy Clients > Add Policy Clients Screen

Use this screen to configure a policy to block or allow a specific MAC address.

Click **Wireless** > **WLAN Clients** > **Client List** > **Policy Clients**, then select an AP group and click **Add Policy Clients** to open this screen.

Figure 322 Wireless > WLAN Clients > Client List > Policy Clients > Add Policy Clients



The following table describes the labels in this screen.

Table 242 Wireless > WLAN Clients > Client List > Policy Clients > Add Policy Clients

LABEL	DESCRIPTION
Add MAC	Click this to add a specific MAC address of a client and configure a policy.
Remove	Click this to remove the policy.

Table 242 Wireless > WLAN Clients > Client List > Policy Clients > Add Policy Clients (continued)

LABEL	DESCRIPTION
MAC Address	Enter the client's MAC address to apply this security policy.
MAC Wildcard Mask	Use a MAC wildcard mask with a MAC address to create a range of allowed MAC addresses for policy clients. Unlike IP subnet masks, a MAC wildcard mask specifies which parts of a MAC address must match for a rule to apply. An F or f in the mask requires an exact match for the corresponding digit. A 0 allows any value for the corresponding digit. For example, a mask of FF:FF:FF:00:00:00 applied to a MAC address of 96:FA:95:1D:67:4A creates a MAC address range of 96:FA:95:00:00:00 to 96:FA:95:FF:FF:FF. This field cannot be left blank. You must enter 17 characters using F, f, and 0, with every two characters separated by a colon. The default value is all Fs, which represents a specific MAC address.
Policy	Select a security policy that you want to apply to the client with the specified MAC address.
Block	The WiFi client cannot connect to the Zyxel Device and the APs in the AP group.
Allow	The WiFi client can connect to the Zyxel Device and the APs in the AP group.
To Specific SSID	To apply the client's policy to a WiFi network (SSID), you must first enable the WiFi network (SSID) in the **Wireless** > **WLAN Settings** > **SSID Settings** screen.
No Policy	The Zyxel Device ignores checking the client's policy for the WiFi network (SSID).
Block	The client cannot connect to the WiFi network (SSID).
Allow	The client can connect to the WiFi network (SSID).
Cancel	Click **Cancel** to return the screen to its last-saved settings.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

29.7 The WiFi Aid Screen

Use this screen to identify connection issues between WiFi clients and managed AP(s) across three connection stages: Wireless, DHCP, and DNS. You can check which connection stage failed to determine the cause of a failed WiFi connection.

Note: At the time of writing, this feature is not supported on all AP models.

At the time of writing, each model supports connection history for the following number of historical days.

Table 243 WiFi Connection Historical Data by Model

MODEL	LAST X DAY(S)
USG FLEX 50H USG FLEX 50HP USG FLEX 100H USG FLEX 100HP USG FLEX 200H USG FLEX 200HP	1
USG FLEX 500H USG FLEX 700H	7

WiFi Connection Stages

See the three connection stages below and their potential failure causes.

1 **Wireless - Client associates with the WiFi network (SSID)**

Potential failure causes:

- Client entered the wrong password
- 802.1X Authentication failed
- Client is connected to another AP by functions such as load balancing (see Section 29.11 on page 551)
- Client is blocked by functions such as legacy client restrictions (see Section 29.10 on page 543), or MAC filtering (see Section 29.6 on page 524)

Troubleshooting:

- Make sure the client is within transmission range of the manged AP
- Make sure the client is connecting to the correct WiFi network and has entered the correct password
- Make sure the Wi-Fi adapter on the client is functioning properly by trying to connect to another WiFi network

2 **DHCP - Client gets the IP address from the network**

Potential failure causes:

- DHCP server does not respond (failure/timeout)

Troubleshooting:

- Check that the DHCP server is online is reachable from the Zyxel Device and the correct info is entered on the Zyxel Device
- Increase the number of IP addresses that the DHCP server can allocate
- Shorten the DHCP lease time to free up IP addresses faster for high-turnover networks, such as cafes with guest WiFi

3 **DNS - DNS server translates domain names into IP addresses**

Potential Failure Causes:

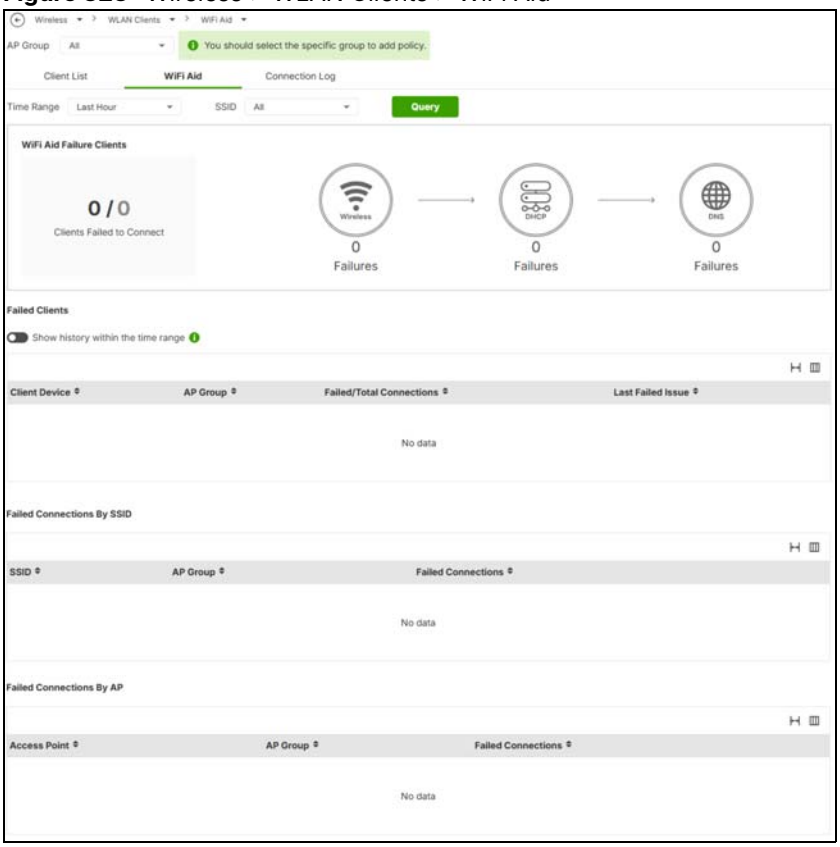
- DNS server does not respond (failure/timeout)

Troubleshooting:

- Check that the DNS server is reachable from the Zyxel Device and the correct info is entered on the Zyxel Device

Click **Wireless** > **WLAN Clients** > **WiFi Aid** to open this screen.

Figure 323 Wireless > WLAN Clients > WiFi Aid



The following table describes the labels in this screen.

Table 244 Wireless > WLAN Clients > WiFi Aid

LABEL	DESCRIPTION
Time Range	Select a time range to display the WiFi connection issues within the configured period. Click **Update** to apply the setting.
SSID	Select **All** or a specific WiFi network (SSID) to display WiFi connection issues.
Query	After selecting a time range and SSID, click this button to display WiFi connection issues based on your selection.
WiFi Aid Failure Clients	The left side shows the number of WiFi clients with failed WiFi connection attempts and the total number of WiFi connection attempts. Note: Each client is counted as one failed connection attempt, no matter how many connection attempts were made. The right side shows the number of WiFi clients with failed WiFi connection attempts broken down by stage: Wireless, DHCP, or DNS. Note: A failure at a specific stage indicates that the connection failed at that stage.
Failed Clients	This displays detailed information about connection failures by WiFi clients.
Show history within the time range	Click the switch to the right to display past failed connection attempts, including those of clients that have successfully connected. Click the switch to the left to display past failed connection attempts only for clients that have not yet successfully connected.

Table 244 Wireless > WLAN Clients > WiFi Aid

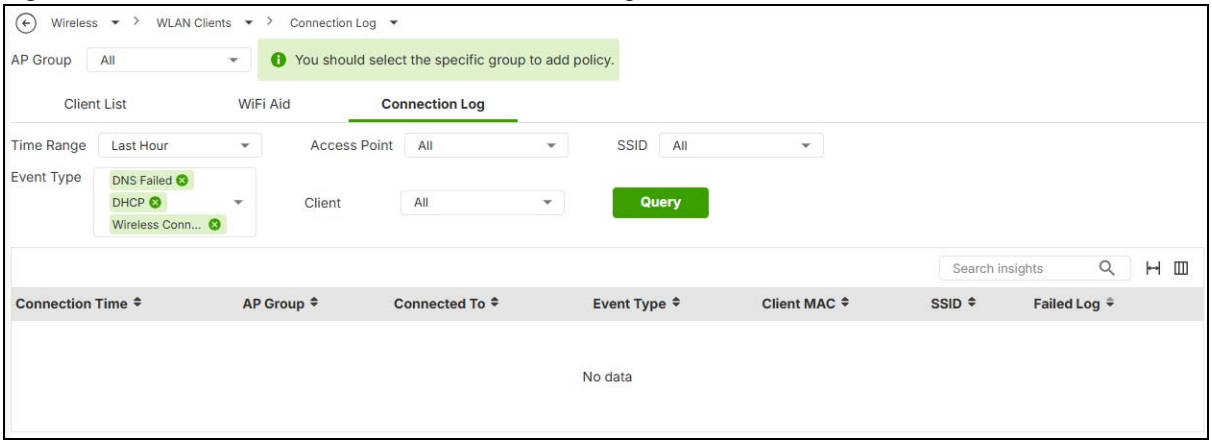
LABEL	DESCRIPTION
Client Device	This displays the WiFi client's MAC address.
AP Group	This displays the AP group of the managed AP that the WiFi client attempted to connect.
Failed/Total Connection	This displays the number of failed WiFi connections and the total WiFi connection attempts of the WiFi client. Click the number to view detailed logs on the **Connection Log** screen.
Last Failed Issue	This displays the stage (Wireless, DHCP, or DNS) at which the last WiFi connection attempt failed.
Failed Connection by SSID	This displays the failed WiFi connections that occurred on each WiFi network (SSID).
SSID	This displays the name of WiFi network (SSID).
AP Group	This displays the AP group of the WiFi network (SSID) that the WiFi client attempted to connect.
Failed Connection	This displays the number of failed connection attempts. Click the number to view detailed logs on the **Connection Log** screen.
Failed Connection by AP	This displays the failed WiFi connections that occurred on each managed AP.
Access Point	This displays the name of managed AP.
AP Group	This displays the AP group of the manged AP that the WiFi client attempted to connect.
Failed Connection	This displays the number of failed connection attempts. Click the number to view detailed logs on the **Connection Log** screen.

29.8 The Connection Log Screen

Use this screen to view failed WiFi connection logs for troubleshooting. Refer to Table 243 on page 531 for the number of days of historical data supported by each model. Click **Wireless** > **WLAN Clients** > **Connection Log** to open this screen.

Note: At the time of writing, this feature is only supported on WBE530 and WBE665S with firmware version 7.35 or later, and on other models with firmware version 7.40 or later.

Figure 324 Wireless > WLAN Clients > Connection Log



The following table describes the labels in this screen.

Table 245 Wireless > WLAN Clients > Connection Log

LABEL	DESCRIPTION
Time Range	Select a time range to display the WiFi connection issues within the configured period. Click **Update** to apply the setting.
Access Point	Select all managed APs or a specific managed AP that the WiFi client attempted to connect to for display.
SSID	Select all WiFi network (SSID) or a specific WiFi network (SSID) that the WiFi client attempted to connect to for display.
Even Type	Select the stage (Wireless, DHCP, or DNS) at which the WiFi connection attempt failed for display.
Client	Select all WiFi clients or a specific WiFi client for display. WiFi connection attempts within the supported historical days are selectable.
Query	Click this button to display the data base on the filter you configure above.
Connection Time	This displays the time when the WiFi connection attempt failed.
AP Group	This displays the AP group of the WiFi network (SSID) that the WiFi client attempted to connect.
Connect to	This displays the name of managed AP that the WiFi client attempted to connect.
Event Type	This displays the stage (Wireless, DHCP, or DNS) at which the WiFi connection attempt failed.
Client MAC	This displays the WiFi client's MAC address.
SSID	This displays the name of the WiFi network (SSID) that the WiFi client attempted to connect.
Failed Log	This displays detailed information about the failed connection.

29.9 The SSID Settings Screen

This screen allows you to configure up to 8 different SSID profiles for each AP group. An SSID, or Service Set IDentifier, is basically the name of the WiFi network to which a WiFi client can connect. The SSID appears as readable text to any device capable of scanning for WiFi frequencies (such as the WiFi adapter in a laptop), and is displayed as the WiFi network name when a person makes a connection to it.

MLO Security Settings

To view the introduction of MLO (Multi-Link Operation), please refer to **Multi-Link Operation (MLO)** **on page 502**.

With Zyxel APs, MLO is automatically enabled for WiFi networks using the 802.11be radio. However, you cannot use **Open**, **WEP**, **WPA1**, **WPA2**, **WPA2-Mixed** security settings for any WiFi network using this radio nor hide a WiFi network (SSID). In Nebula, you also cannot use **DPPSK** (Dynamic Personal Pre-Shared Key).

Note: If you configure any of these features for a WiFi network (SSID) using the 802.11be radio, then that WiFi network (SSID) will be disabled. You will see a log for this in the event logs. To re-enable the WiFi network (SSID), you must change the security setting to one of **Open**, **WPA1**, **WPA2**, **WPA2-Mixed**, unhide the SSID, and disable **DPPSK** (in Nebula).

To minimize impact on your existing WiFi network configurations, that may be using the above settings, Zyxel APs will cause the 2.4Ghz band to use the 802.11ax radio.

Note: **Open**, **WEP**, **WPA1**, **WPA2**, **WPA2-Mixed** and **DPPSK** will only work in the 2.4GHz band. If your WiFi clients in this band do not use these settings, then set the radio mode to 802.11be for full WiFi 7 MLO functionality.

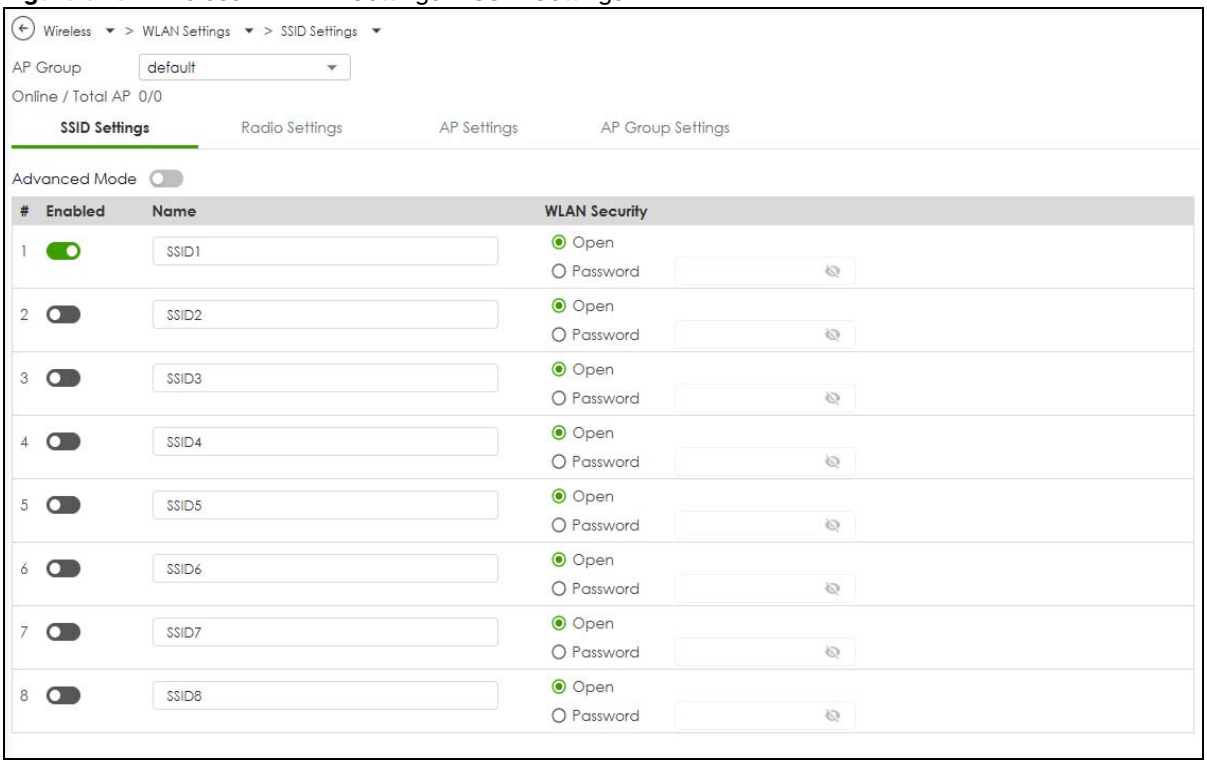
You should use **WPA3**, **WPA3 Transition**, or **Enhanced Open** security for WiFi networks using the 802.11be radio.

Please refer to Zyxel AP User's Guide or Web Help more details.

Click **Wireless** > **WLAN Settings** > **SSID Settings** to open this screen.

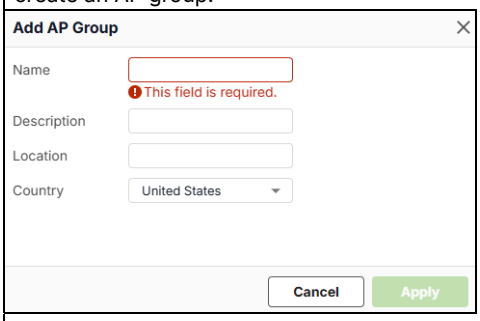
Note: You must select the AP group to which the AP you want to configure belongs before configuring this screen. For example, if you want to configure AP 'WBE660S' and 'WBE660S' belongs to AP group 'RD-APs', make sure to select 'RD-APs' in **AP Group** first before configuring 'WBE660S'.

Figure 325 Wireless > WLAN Settings > SSID Settings



The following table describes the labels in this screen.

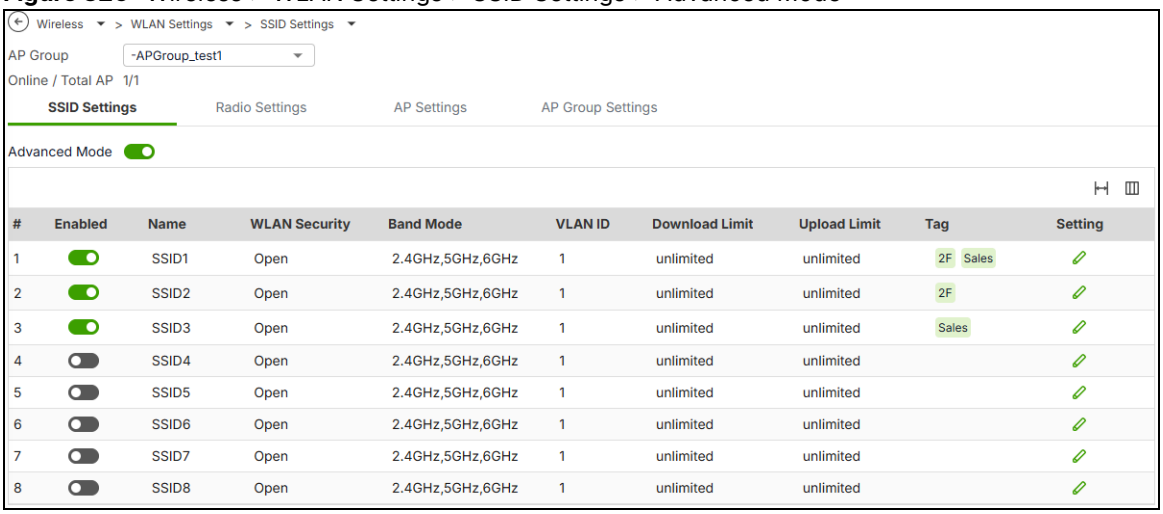
Table 246 Wireless > WLAN Settings > SSID Settings

LABEL	DESCRIPTION
AP Group	Select the AP group to which the AP you want to configure belongs. Or click **Add** to create an AP group.  • **Name:** Specify the name of the AP group. You can use up to 32 characters, starting with a letter, a hyphen [-], or an underscore [_]. The valid characters are [0-9][a-z][A-Z][_-]. Spaces are not allowed. • **Description:** Enter a description for the group. You can use up to 61 characters. The valid characters are [A– Z], [a–z], [0–9], ['"()+,/:=?;!*#@$_%-]. Spaces are allowed. • **Location:** Specify the name of the place where the AP group is located. You can use up to 30 characters. The valid characters are [A– Z], [a–z], [0–9], ['()+,/ :=?;!*#@$_%-]. Spaces are allowed. • **Country**: Select the country where the AP group is located from drop-down list.
Advanced Mode	Select **Off** to disable Advanced mode. This allows you to create SSID profiles by only specifying an SSID name and optional password.
#	This is the SSID's index number in this list.
Enabled	Click to turn on or off this profile.
Name	This shows the SSID name for this profile. Click the text box and enter a new SSID if you want to change it. Enable **UTF-8 SSID** in **Advanced Mode** if you want to use special characters.
WLAN Security	Select the encryption and authentication method used in this profile. • Select **Open** to allow any client to associate this network without any data encryption or authentication. This is not recommended. • Select **Password** and enter a pre-shared key from 8 to 63 case-sensitive keyboard characters to enable WPA1/2/3-PSK data encryption.

29.9.1 The SSID Advanced Settings Screen

Use this screen to view the 2.4G/5G/6G band mode, VLAN ID, and download/upload limits. Click **Wireless** > **WLAN Settings** > **SSID Settings**, and enable **Advanced Mode** to open this screen.

Figure 326 Wireless > WLAN Settings > SSID Settings > Advanced Mode



The following table describes the labels in this screen.

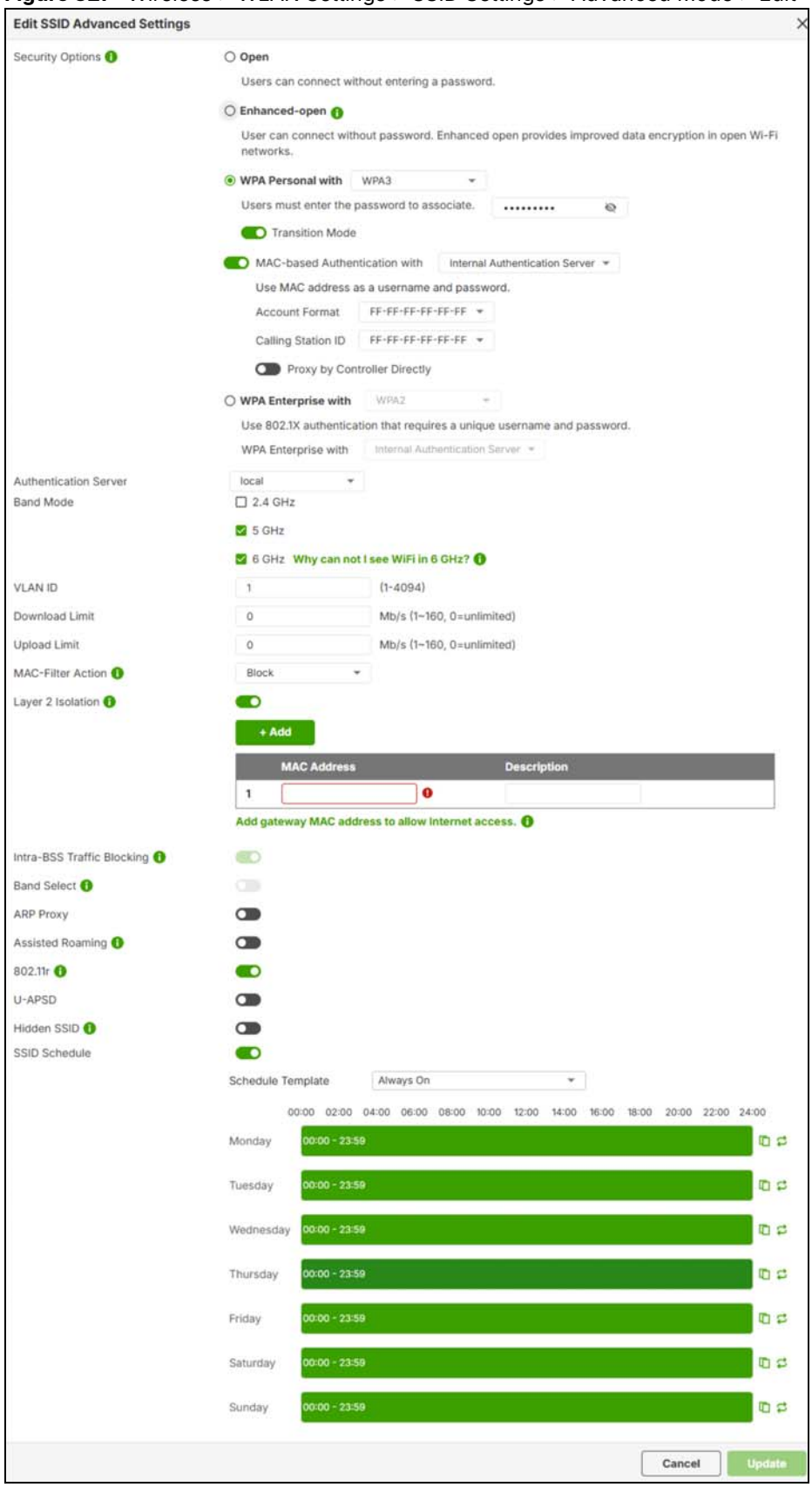
Table 247 Wireless > WLAN Settings > SSID Settings > Advanced Mode

LABEL	DESCRIPTION
#	This is the SSID's index number in this list.
Enabled	Click to turn on or off this profile.
Name	The shows the SSID name for this profile. This is the name visible on the network to wireless clients.
WLAN Security	This shows the encryption method used in this profile.
Band Mode	This shows the wireless band which this WiFi 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. 6 GHz is the frequency used by IEEE 802.11ax/ac/a/n wireless clients.
VLAN ID	This shows the VLAN ID for the AP to use to tag traffic originating from this SSID.
Download Limit	This shows the maximum downstream bandwidth allowed for each client.
Upload Limit	This shows the maximum upstream bandwidth allowed for each client.
Tag	This shows the AP tags associated with this WiFi network (SSID).
Setting	Click the icon to edit the SSID settings.

29.9.2 Edit SSID Advanced Settings

Use this screen to configure detailed settings for the WiFi network (SSID). Click **Wireless** > **WLAN Settings** > **SSID Settings**, enable **Advanced Mode**, and click **Edit** to open this screen.

Figure 327 Wireless > WLAN Settings > SSID Settings > Advanced Mode > Edit



The following table describes the labels in this screen.

Table 248 Wireless > WLAN Settings > SSID Settings > Advanced Mode > Edit

LABEL	DESCRIPTION
Enabled	Click this to enable the SSID to be discoverable by WiFi clients.
UTF-8 SSID	Enable this to allow SSIDs to be UTF-8 encoded, allowing for more descriptive and user-friendly SSID names that could include special characters, accents, emojis and characters from different languages such as Chinese. However, be aware that some older hardware or software might not properly handle certain Unicode characters.
Name	This shows the SSID name as it appears to WiFi clients. Click the text box and enter a new SSID if you want to change it. If you enabled **UTF-8 SSID,** you may enter special characters.
Tag	Select one or more AP tags to associate with the WiFi network (SSID). Click the drop-down list to display the tags you have created for the AP group that this profile belongs to (in The AP List Screen).
Security Options	
Open	Select this to allow any client to associate this network without any data encryption or authentication.
Enhanced-open	Select this to allow any client to associate this network without any password but with improved data encryption. Note: Upon selecting **Enhanced-open** or **WPA Personal With WPA3, transition mode** generates two VAP so devices that do not support **Enhanced-Open/WPA Personal With WPA3** can connect using **Open/WPA Personal With WPA2** network. This is always on at the time of writing.
WPA Personal with WPA1/WPA2/WPA3	Select this and enter a pre-shared key from 8 to 63 case-sensitive keyboard characters to enable WPA1/2/3-PSK data encryption. Upon selecting **WPA Personal With WPA3**, APs that do not support it will revert to WPA2.
MAC-based Authentication with	Select this to authenticate WiFi clients by their MAC addresses together with a user name and password. • Select **External Authentication Server** to use an external RADIUS server for 802.1X authentication. • Select **Internal Authentication Server** to use the Zyxel Device for 802.1X authentication. Note: If you configure **MAC-based Authentication** with **Internal Authentication Server** and set the **Authentication Server** to **local**, then you need to create a Mac User in **User & Authentication > User/ Group > User** for successful authentication. See Section 28.1.4 on page 463 for more information.
WPA-Enterprise with WPA2/WPA3	Select this to enable 802.1X secure authentication. • Select **External Authentication Server** to use an external RADIUS server for 802.1X authentication. • Select **Internal Authentication Server** to use the Zyxel Device for 802.1X authentication.
Proxy by Controller Directly	When you select **Internal Authentication Server** for use in **Security Options**, the Zyxel Device relays EAP packets between the AP's clients and the RADIUS server by default. See IEEE 802.1X Authentication Using EAP for details. Enable this to allow EAP packets pass between the AP's clients and the RADIUS server directly. The Zyxel Device will only forward the packets without inspecting or modifying them. Enable this when clients use certain EAP methods (for example, EAP-SIM).
Authentication Server	If you enable **MAC-based Authentication** or select **WPA Enterprise** in **Security Options**, select an server from the drop-down list.

Table 248 Wireless > WLAN Settings > SSID Settings > Advanced Mode > Edit (continued)

LABEL	DESCRIPTION
Band Mode	Select the WiFi band which this profile should use. **2.4 GHz** is the frequency used by IEEE 802.11b/g/n/ax WiFi clients. **5 GHz** is the frequency used by IEEE 802.11a/n/ac/ax WiFi clients. **6 GHz** is the frequency used by IEEE 802.11ax WiFi clients.
VLAN ID	Enter a VLAN ID for the AP to use to tag traffic originating from this SSID.
Download Limit	Set the maximum downstream bandwidth for each client (1 to 160 megabits per second). Enter 0 to not set a limit (default).
Upload Limit	Set the maximum upstream bandwidth for each client (1 to 160 megabits per second). Enter 0 to not set a limit (default).
MAC-Filter Action	Use this field to allow or block clients from connecting to this SSID. Refer to Section 29.6 on page 524 to configure the access policy for specific clients. • **Allow**: Only clients with the policy rule '**Allow**' can connect to this SSID. All others are blocked. • **Block**: Only clients with the policy rule '**Block**' cannot connect to this SSID. All others are allowed. • **Disable**: Any client can connect to this SSID.
Layer 2 Isolation	This field is not configurable if you select NAT mode. Select to turn on or off layer-2 isolation. If a device's MAC addresses is NOT listed, it is blocked from communicating with other devices in an SSID on which layer-2 isolation is enabled. Click **Add** to enter the MAC address of each device that you want to allow to be accessed by other devices in the SSID on which layer-2 isolation is enabled.
Intra-BSS Traffic Blocking	Enable to prevent crossover traffic from within the same SSID. Disable to allow intra-BSS traffic.
Band Select	Select to enable band steering. When enabled, the AP steers WiFi clients to the 5 GHz band. Note: This feature is not available when you enable MLO. Note: Band mode must be set to Concurrent operation (2.4 GHz and 5 GHz).
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.
Assisted Roaming	Select this option to enable IEEE 802.11k/v assisted roaming on the Zyxel Device. When the connected clients request 802.11k neighbor lists, the Zyxel Device will response with a list of neighbor APs that can be candidates for roaming.
802.11r	Select to turn on or off IEEE 802.11r fast roaming on the AP. 802.11r fast roaming reduces the delay when the clients switch from one AP to another, by allowing security keys to be stored on all APs in a network. Information from the original association is passed to the new AP when the client roams. The client does not need to perform the whole 802.1x authentication process. Note: This feature is not available when you enable MLO.
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 WiFi clients connected to the Zyxel Device using this SSID profile.
Hidden SSID	Select this option to hide the SSID from clients' WiFi network lists. Clients will need to manually enter the SSID name to connect.

Table 248 Wireless > WLAN Settings > SSID Settings > Advanced Mode > Edit (continued)

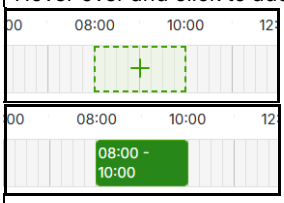
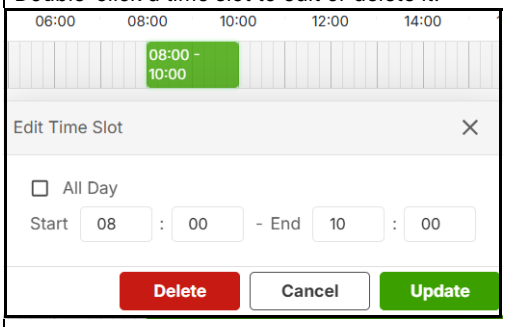
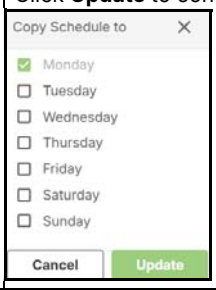
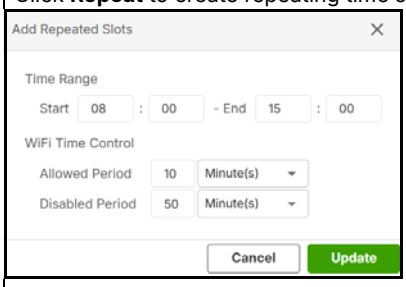
LABEL	DESCRIPTION
SSID Schedule	Select this option to enable and configure a schedule. Use the multi-range slider to set a schedule. Green time slots indicate when the WiFi network (SSID) is enabled. You can create up to 12 time slots per day. See Section 29.16 on page 560 for an application example. The schedule is executed according to the managed AP's system time.
Schedule template	Select a pre-defined schedule template to configure the day and time at which the SSID is enabled or disabled: • Available 8–5 daily • Available 8–5 daily except weekends • Weekdays only • Always on • Always off
Monday to Sunday 00:00 to 24:00	Use the multi-range slider to customize the schedule. Hover over and click to add a time slot.  Click and drag a time slot to move it.  Click and drag an edge to adjust the range.  Double-click a time slot to edit or delete it.  • Select **All Day** checkbox to keep the SSID enabled all day. • Set the start and end time of a slot. • Click **Delete** to remove the time slot. • Click **Update** to save changes. • Click **Cancel** to discard changes.

Table 248 Wireless > WLAN Settings > SSID Settings > Advanced Mode > Edit (continued)

LABEL	DESCRIPTION
Copy	Click **Copy** on a day and select the target day(s) for copying the time slot settings. Click **Update** to confirm. 
Repeat	Click **Repeat** to create repeating time slots.  • Set a **Start** and **End** time interval for the cycles. • Define **Allowed** and **Disallowed** periods within each cycle. A cycle begins with an allowed period at the start of the **Start Time Range** and repeats according to the configured allowed and disabled periods. For example, a time range of 8:00 to 11:00 with a 10-minute allowed period followed by a 50-minute disabled period results in the following enabled periods: • 8:00 - 8:10 • 9:00 - 9:10 • 10:00 - 10:10 Click **Update** to confirm.
Cancel	Click **Cancel** to return the screen to its last-saved settings.
Update	Click **Update** to save your changes back to the Zyxel Device.

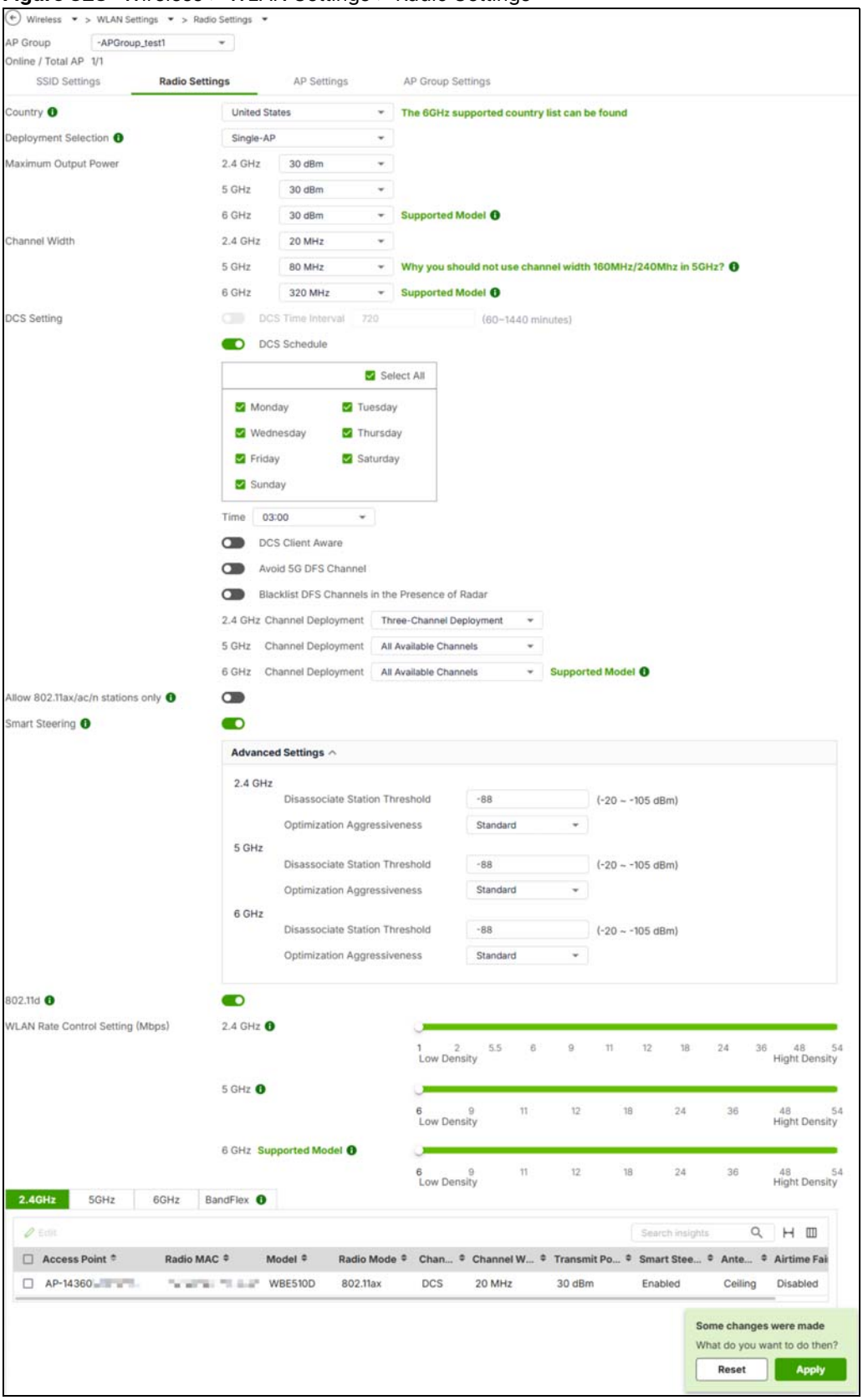
29.10 The Radio Settings Screen

Use this screen to configure global radio settings for all managed APs. See Section 29.1.2 on page 499 for more information on radio settings.

Click **Wireless** > **WLAN Settings** > **Radio Settings** to open this screen.

Note: You must select the AP group to which the AP you want to configure belongs before configuring this screen. For example, if you want to configure AP 'WBE660S' and 'WBE660S' belongs to AP group 'RD-APs', make sure to select 'RD-APs' in **AP Group** first before configuring 'WBE660S'.

Figure 328 Wireless > WLAN Settings > Radio Settings



The following table describes the labels in this screen.

Table 249 Wireless > WLAN Settings > Radio Settings

LABEL	DESCRIPTION
AP Group	Select the AP group to which the AP you want to configure belongs. Or click **Add** to create an AP group.
Country	Select the country where the AP is located or installed. The available channels vary depending on the country you select. Be sure to select the correct or same country for both radios on an AP and all connected APs in order to prevent roaming failure and interference with other systems.
Deployment Selection	• Select **High-density (More than 10 APs)** for the lowest output power to reduce interference to the minimum in areas where you have 10 or more Access Points. • Select **Moderate-density (6-9 APs)** for moderate output power to reduce interference in areas where you have 5 to 9 Access Points. • Select **Low-density (2-5 APs)** for higher concentration of output power for less than 5 Access Points. • Select **Single AP** to maximize WiFi coverage in areas where you have just 1 Access Point.
Maximum Output Power	Selecting any of the options in the **Deployment selection** field will automatically set the maximum output power for 2.4/5/6 GHz. You can change the setting (1-30 dBm according to the number of APs you have in your environment. The higher the AP output power, the greater the WiFi coverage, but the more interference there will be with nearby APs).
Channel Width	Select the wireless channel bandwidth you want the access point to use. • A standard 20 MHz channel offers transfer speeds of up to 144 Mbps (2.4 GHz) or 217 Mbps (5 GHz) whereas a 40 MHz channel uses two standard channels and offers speeds of up to 300 Mbps (2.4 GHz) or 450 Mbps (5 GHz). An IEEE 802.11ac-specific 80 MHz channel offers speeds of up to 1.3 Gbps. An IEEE 802.11be-specific 160 MHz channel offers speeds of up to 2.9 Gbps (6 GHz with 2 spatial streams) whereas a 320 MHz channel offers speeds of up to 5.8 Gbps (6 GHz with 2 spatial streams). • 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. It is often better to use the 20 MHz setting in a location where the environment hinders the WiFi signal. Note: It is suggested that you select 20 MHz when there is more than one 2.4 GHz AP in the network.
DCS Setting See Dynamic Channel Selection (DCS) on page 507 for more information.	
DCS Time Interval	Enable to set the DCS time interval (in minutes) to regulate how often an AP surveys 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 channel with lower interference.
DCS Schedule	Enable to have the AP automatically find a less-used channel within its broadcast radius at a specific time on selected days of the week. You then need to select each day of the week and specify the time of the day (in 24-hour format) to have the AP use DCS to automatically scan and find a less-used channel.
DCS Client Aware	Enable to have the AP wait until all connected clients have disconnected or currently have no traffic before switching channels.
Avoid 5G DFS Channel	If your APs are operating in an area known to have RADAR devices, enable this to have the selected APs choose non-DFS channels to provide a stable WiFi service. See Dynamic Frequency Selection (DFS) on page 507 for more information.
Blacklist DFS Channels in the Presence of Radar	Enable to have the selected APs avoid DFS channels if RADAR is detected until the APs are rebooted. However, the AP can still use other non-specified DFS channels.

Table 249 Wireless > WLAN Settings > Radio Settings (continued)

LABEL	DESCRIPTION
2.4 GHz Channel Deployment	These settings apply to the 2.4G radio. • Select **Three-Channel Deployment** to limit channel switching to channels 1, 6, and 11, the three channels that are sufficiently separated 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. If the only allowable channels in your country are 1 – 11 then the AP uses channels 1, 4, 7, 11; otherwise, the AP uses channels 1, 5, 9, 13. Four channel deployment expands your pool of possible channels while keeping the channel interference to a minimum. • Select **All available channels** to allow channel-hopping across all channels to have the AP automatically select the best channel. • Select **Manual** to specify certain individual channels that the AP can switch between.
5 GHz Channel Deployment	These settings apply to the 5G radio. • Select **All available channels** to have the AP automatically select the best channel. • Select **Manual** to specify certain individual channels that the AP can switch between. Note: The method is automatically set to **All available channels** when no channel is selected or any one of the previously selected channels is not supported.
6 GHz Channel Deployment	These settings apply to the 6G radio. • Select **All available channels** to have the AP automatically select the best channel. • Select **Manual** to select the individual channels the AP switches between. Note: The method is automatically set to **All available channels** when no channel is selected or any one of the previously selected channels is not supported.
Allow Legacy Stations	Enable to have the AP allow only IEEE 802.11n/ac/ax clients to connect, and reject IEEE 802.11a/b/g clients.
Smart Steering	Click the switch to the right to enable smart client steering on the AP. Client steering helps monitor WiFi clients and drop the connections of clients that are idle or have a low signal in order to optimize the bandwidth available for other clients. Dropped WiFi clients have may connect to an AP with a stronger signal. Additionally, dual band WiFi clients can also steer from one band to change from a busy band with many WiFi clients to a less busy band with fewer clients. Click the switch to the left to disable this feature on the AP.
Advanced Settings	Click this to display a greater number of configuration fields.
2.4G/5G/6G Settings	
Disassociate Station Threshold	Set a minimum disconnect signal strength. When a WiFi client's signal strength is lower than the specified threshold, the AP disconnects the WiFi client. –20 dBm is the strongest signal you can require for automatic disconnection and –105 dBm is the weakest.

Table 249 Wireless > WLAN Settings > Radio Settings (continued)

LABEL	DESCRIPTION
Optimization Aggressiveness	**High, Standard** and **Low** stand for different traffic rate threshold levels. The level you select here decides when the AP takes action to improve the access point's WiFi network performance. The AP will postpone the actions implemented on access points until the threshold you set here is exceeded. Select a suitable traffic rate threshold level for your network. • **Low**: Select this if you want the AP to postpone the action while the access point network traffic is low. Select this if the AP is usually connected to only a few devices and there are no heavy users. • **Standard/High**: Select this if you want the AP to postpone the action only when the access point network traffic is medium to heavy. Select this if multiple users are connected at the same time and are streaming videos, using cloud services, or transferring large files.
802.11d	Click this to enable 802.11d on the access point. 802.11d allows clients to automatically configure themselves to their local regulatory domain, ensuring compliance with country-specific rules regarding allowed frequencies, power levels, and signal bandwidth. Enabling 802.11d causes the AP to broadcast the country where it is located, which is determined by the **Country** setting. Note: Disable **802.11d** on older client devices with connection issues.
WLAN Rate Control Setting (Mbps)	Sets the minimum data rate in Mbps that 2.4 GHz, 5 GHz, and 6 GHz WiFi clients can connect to the AP. Increasing the minimum data rate can reduce network overhead and improve WiFi network performance in high density environments. However, WiFi clients that do not support the minimum data rate will not be able to connect to the AP.
2.4GHz	Click this to display the connected APs using the 2.4 GHz frequency band.
5GHz	Click this to display the connected APs using the 5 GHz frequency band.
6GHz	Click this to display the connected APs using the 6 GHz frequency band.
BandFlex	Click this to display the connected APs that supports BandFlex (5 GHz or 6 GHz frequency bands).
Edit	Select one or more APs and click **Edit** to open a screen where you can modify the AP settings.
Access Point	This displays the descriptive name or MAC address of the AP.
Radio MAC	An AP has multiple radios, each radio typically has its own MAC address. This displays the unique MAC address of the radio inside the AP.
Model	This displays the model name of the AP.
Radio Mode	This displays the type of WiFi radio the AP is currently using, for example 802.11b/g/n / 802.11be.
Channel	This displays the channel ID currently being used by the AP's radio.
Channel Width	This displays the wireless channel bandwidth the AP's radio is set to use.
Transmit Power	This displays the current transmitting power of the AP's radio. If the AP is offline, this shows the maximum output power you configured for the AP.
Smart Steering	This displays whether smart client steering is enabled or disabled on the connected APs.
Antenna	This displays the antenna orientation settings for the AP that comes with internal antennas and also has an antenna switch.
Airtime Fairness	This displays whether airtime fairness is enabled or disabled on the AP. With enabled Airtime Fairness, the AP allocates airtime equally between all connected clients. See Airtime Fairness on page 504 for the details.

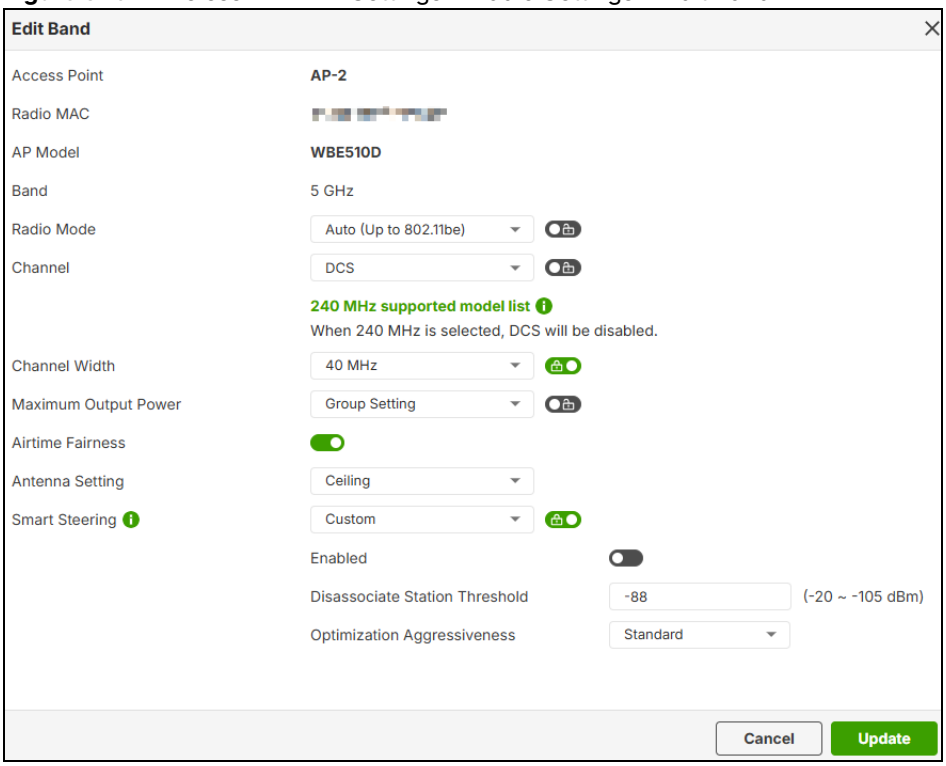
29.10.1 The Wireless > WLAN Settings > Radio Settings > Edit Band Screen

For some radio settings, you can configure them either on an AP group or on individual APs. By default, an AP uses the settings of the AP group it belongs to. Use this screen to configure the radio settings on each individual AP. The settings on each individual AP takes the priority over the group setting.

Note: An unlocked icon next to each field indicates the setting is the same as the group setting, while a locked icon indicates it is different. You can click the icon to unlock it to apply the group setting.

Go to **Wireless > WLAN Settings > Radio Settings**, then click the edit icon of the AP you want to configure.

Figure 329 Wireless > WLAN Settings > Radio Settings > Edit Band



The following table describes the labels in this screen.

Table 250 Wireless > WLAN Settings > Radio Settings > Edit Band

LABEL	DESCRIPTION
Access Points	This displays the descriptive name or MAC address of the AP. This displays **Multiple Values** when you select more then one AP to edit.
Radio MAC	An AP has multiple radios, each radio typically has its own MAC address. This displays the unique MAC address of the wireless radio interface inside the AP. This displays **Multiple Values** when you select more then one AP to edit.
AP Model	This displays the model name of the AP. This displays **Multiple Values** when you select more then one AP to edit.
Band	This displays the frequency band the AP is currently using. When configuring one or more APs with BandFlex, select a frequency band to use together with the 2.4 GHz band.

Table 250 Wireless > WLAN Settings > Radio Settings > Edit Band (continued)

LABEL	DESCRIPTION
Radio Mode	Select how to let WiFi clients connect to the AP(s). • **Multiple Values:** Indicates that the APs you selected to edit are currently using different radio modes. **If 802.11 Band is set to 2.4GHz:** • **Auto (Up to 802.11ax):** allows either IEEE802.11b, IEEE802.11g, IEEE802.11n, and IEEE802.11ax compliant WiFi devices to associate with the AP(s). The AP(s) adjusts the transmission rate automatically according to the WiFi standard supported by the wireless devices. • **802.11b/g**: allows either IEEE 802.11b or IEEE 802.11g compliant WiFi devices to associate with the AP(s). • **802.11b/g/n**: allows IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WiFi devices to associate with the AP(s). • **802.11ax**: allows IEEE802.11b, IEEE802.11g, IEEE802.11n, and IEEE802.11ax compliant WiFi devices to associate with the AP(s). If the WiFi device isn't compatible with 802.11ax, the AP(s) will communicate with the WiFi device using 802.11n, and so on. • **802.11be**: allows IEEE802.11b, IEEE802.11g, IEEE802.11n, IEEE802.11ax and IEEE802.11be compliant WiFi devices to associate with the AP(s). If the WiFi device isn't compatible with 802.11be, the AP(s) will communicate with the WiFi device using 802.11ax, and so on. **If 802.11 Band is set to 5GHz:** • **Auto (Up to 802.11be):** allows either IEEE802.11a, IEEE802.11n, IEEE802.11ac, IEEE802.11ax, and IEEE802.11be compliant WiFi devices to associate with the AP(s). The AP(s) adjusts the transmission rate automatically according to the WiFi standard supported by the wireless devices. • **802.11a**: allows only IEEE 802.11a compliant WiFi devices to associate with the AP. • **802.11a/n**: allows both IEEE802.11n and IEEE802.11a compliant WiFi devices to associate with the AP. • **802.11ac**: allows IEEE802.11n, IEEE802.11a, and IEEE802.11ac compliant WiFi devices to associate with the AP(s). If the WiFi device isn't compatible with 802.11ac, the AP(s) will communicate with the WiFi device using 802.11n, and so on. • **802.11ax**: allows IEEE802.11n, IEEE802.11a, IEEE802.11ac, and IEEE802.11ax compliant WiFi devices to associate with the AP(s). If the WiFi device isn't compatible with 802.11ax, the AP(s) will communicate with the WiFi device using 802.11ac, and so on. • **802.11be**: allows IEEE802.11a, IEEE802.11n, IEEE802.11ac, IEEE802.11ax and IEEE802.11be compliant WiFi devices to associate with the AP(s). If the WiFi device isn't compatible with 802.11be, the AP(s) will communicate with the WiFi device using 802.11ax, and so on. **If 802.11 Band is set to 6GHz:** • **Auto:** allows either IEEE802.11ax and IEEE802.11be compliant WiFi devices to associate with the AP(s). The AP(s) adjusts the transmission rate automatically according to the WiFi standard supported by the wireless devices. • **802.11ax**: allows IEEE802.11ax compliant WiFi devices to associate with the AP(s). • **802.11be**: allows IEEE802.11be compliant WiFi devices to associate with the AP(s). If the WiFi device isn't compatible with 802.11be, the AP(s) will communicate with the WiFi device using 802.11ax. Note: 802.11be and Auto (up to 802.11be) is available for WiFi 7 devices only.
Channel	Select the radio channel which the signal will use for broadcasting by the AP. Select **DCS** (Dynamic Channel Selection) to have the AP choose a radio channel that has least interference. See Dynamic Channel Selection (DCS) and Dynamic Frequency Selection (DFS) for more information. On the 5 GHz band, DCS is not available for 160 MHz and 240 MHz channels.

Table 250 Wireless > WLAN Settings > Radio Settings > Edit Band (continued)

LABEL	DESCRIPTION
Channel Width	Select the wireless channel bandwidth you want the AP(s) to use. A standard 20 MHz channel offers transfer speeds of up to 144 Mbps (2.4 GHz) or 217 Mbps (5 GHz) whereas a 40 MHz channel uses two standard channels and offers speeds of up to 300 Mbps (2.4 GHz) or 450 Mbps (5 GHz). An IEEE 802.11ac-specific 80 MHz channel offers speeds of up to 1.3 Gbps. An IEEE 802.11be-specific 160 MHz channel offers speeds of up to 2.9 Gbps (6 GHz with 2 spatial streams) whereas a 320 MHz channel offers speeds of up to 5.8 Gbps (6 GHz with 2 spatial streams). 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. It is often better to use the 20 MHz setting in a location where the environment hinders the WiFi signal. Select 20MHz if you want to lessen radio interference with other wireless devices. • Select **Group Setting** to use the channel bandwidth configured for the AP group the AP(s) belongs to. • Select **40 MHz** to allow the AP(s) to choose the channel bandwidth (20 or 40 MHz) that has least interference. • Select **80 MHz** to allow the AP(s) to choose the channel bandwidth (20, 40 or 80) that has least interference. • Select **160 MHz** to allow the AP(s) to choose the channel bandwidth (20, 40, 80 or 160MHz) that has least interference. • Select **240 MHz** to allow the AP(s) to choose the channel bandwidth (20, 40, 80, 160 or 240MHz) that has least interference. • Select **320 MHz** to allow the AP(s) to choose the channel bandwidth (20, 40, 80, 160, 240 or 320 MHz) that has least interference. Note: If the environment has poor signal-to-noise (SNR), the AP(s) will switch to a lower bandwidth.
Maximum Output Power	• Select **Group Setting** to use the maximum output power configured for the AP group that the AP(s) belongs to. • If there is a high density of APs in an area, decrease the output power of the AP(s) to reduce interference with other APs. You can change the setting from 1 to 30 dBm. Note: Reducing the output power also reduces the AP(s)' effective broadcast radius.
Zero-Wait DFS	When an AP operates on the 5 GHz band, DFS may cause service interruptions because the AP must pause, scan for radar signals, and switch to a new channel. See Dynamic Frequency Selection (DFS) for details. Click the switch to the right to enable Zero-Wait DFS, allowing the AP to continue forwarding traffic without interruption during the channel switch. Note: This feature is not supported on all AP models.
Airtime Fairness	Click the switch to the right to enable Airtime Fairness to have the AP(s) allocate airtime equally between all connected clients. Airtime fairness makes sure clients that can receive packets faster will not be slowed down by clients that receive packets slower. Use this if clients that need less airtime in your WiFi networks need priority to receive packets, such as clients that use real time traffic to stream videos or play games. This field is not available if the AP does not support airtime fairness. Note that if you enable this feature, clients that originally need more time to receive packets will become slower than before. Clear the check box if you want better performance on slower clients in your network, such as a gaming computer that's far away from the AP. Note: When you disable or enable airtime fairness on an AP, all connected clients of the AP will be disconnected.

Table 250 Wireless > WLAN Settings > Radio Settings > Edit Band (continued)

LABEL	DESCRIPTION
Antenna Setting	This allows you to adjust coverage depending on the antenna orientation of the AP's radios for better coverage. This field is not available if the AP does not allow you to adjust antenna orientation. Select **Wall** if you mount the AP to a wall. Select **Ceiling** if the AP is mounted on a ceiling. You can switch from **Wall** to **Ceiling** if there are still wireless dead zones, and vice versa.
Smart Steering	• Select **Group Setting** to use the radio setting you configured for the AP group this AP belongs to. • Select **Custom** to configure a different radio setting from the group setting.
Enabled	Click the switch to the right to enable smart client steering on the AP. Client steering helps monitor WiFi clients and drop the connections of clients that are idle or have a low signal in order to optimize the bandwidth available for other clients. Dropped WiFi clients have may connect to an AP with a stronger signal. Additionally, dual band WiFi clients can also steer from one band to change from a busy band with many WiFi clients to a less busy band with fewer clients. Click the switch to the left to disable this feature on the AP.
Disassociate Station Threshold	Set a minimum disconnect signal strength. When a WiFi client's signal strength is lower than the specified threshold, the AP disconnects the WiFi client. –20 dBm is the strongest signal you can require for automatic disconnection and –105 dBm is the weakest.
Optimization Aggressiveness	**High**, **Standard** and **Low** stand for different traffic rate threshold levels. The level you select here decides when the AP takes action to improve the access point's WiFi network performance. The AP will postpone the actions implemented on access points until the threshold you set here is exceeded. Select a suitable traffic rate threshold level for your network. • **Low**: Select this if you want the AP to postpone the action while the access point network traffic is low. Select this if the AP is usually connected to only a few devices and there are no heavy users. • **Standard**/**High**: Select this if you want the AP to postpone the action only when the access point network traffic is medium to heavy. Select this if multiple users are connected at the same time and are streaming videos, using cloud services, or transferring large files.
Cancel	Click **Cancel** to return the screen to its last-saved settings.
Update	Click **Update** to save your changes back to the Zyxel Device.

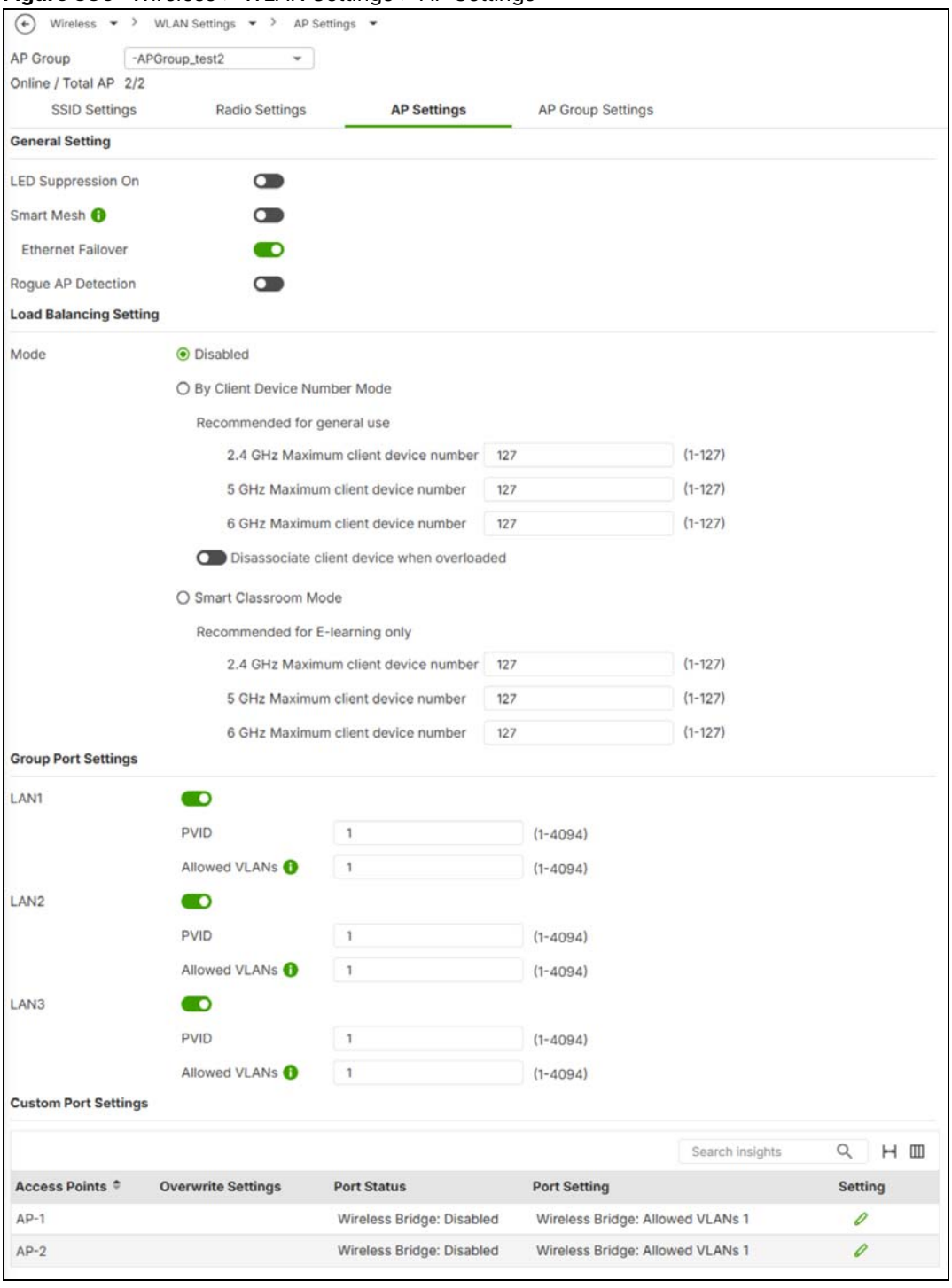
29.11 The AP Settings Screen

Use this screen to configure general AP settings and enable or disable a port on the managed AP and configure the port's VLAN settings. The port settings apply to all managed APs in the selected group and have one or more than one Ethernet LAN port (except the uplink port).

Click **Wireless** > **WLAN Settings** > **AP Settings** to open this screen.

Note: You must select the AP group to which the AP you want to configure belongs before configuring this screen. For example, if you want to configure AP 'WBE660S' and 'WBE660S' belongs to AP group 'RD-APs', make sure to select 'RD-APs' in **AP Group** first before configuring 'WBE660S'.

Figure 330 Wireless > WLAN Settings > AP Settings



The following table describes the labels in this screen.

Table 251 Wireless > WLAN Settings > AP Settings

LABEL	DESCRIPTION
AP Group	Select the AP group to which the AP you want to configure belongs. Or click **Add** to create an AP group.
General Setting	

Table 251 Wireless > WLAN Settings > AP Settings

LABEL	DESCRIPTION
Smart Mesh	Click to enable or disable the Smart Mesh feature on all managed APs in the selected group. Smart Mesh is a WiFi mesh solution for APs. With Smart Mesh, you can have two or more APs automatically create a mesh network within your home or office, ensuring there are no areas with a weak WiFi signal.
Ethernet Failover	When enabled, a wired AP connected to the Zyxel Device changes its role from mesh controller to mesh extender if the AP is unable to reach the Zyxel Device. When disabled, a wired AP connected to the Zyxel Device automatically changes its role from mesh controller to mesh extender only if the AP's uplink Ethernet cable is unplugged.
Rogue AP Detection	Select this to enable rogue AP detection on all managed APs in this AP group. You can configure and view detection results on the **Wireless > Rogue AP Detection** screen. See Section 29.15 on page 558.
Load Balancing Setting AP load balancing lets the Zyxel Device distribute WiFi clients and traffic across APs connected to the Zyxel Device to prevent overloading of APs with higher loads and lower signal quality.	
Mode	With load balancing enabled, when an AP reaches the set limit, new clients are steered to another AP in the group. Select a mode for this AP group to distribute client devices evenly across multiple access points.
Disabled	Select this to disable load balancing on all the APs in this AP group.
By Client Device Number Mode	Select this to balance network traffic based on the number of client devices connected to an AP.
2.4G / 5G / 6G Maximum client device number	Enter the maximum number of client devices (1 to 127) that can simultaneously use a radio band.
Disassociate client device when overloaded	Turn this on to disconnect clients to the APs when they become overloaded. Turn this off to disable this option. The APs will then either delay the connection until they have enough bandwidth or transfer the connection to other APs within its broadcast range. The disassociation priority is determined automatically by the Zyxel Device and is as follows: • Idle Time – Client devices that have been idle the longest will be disconnected first. If none of the connected devices are idle, then the priority shifts to Signal Strength. • Signal Strength – Client devices with the weakest signal strength will be disconnected first.
Smart Classroom Mode	Select this to balance network traffic based on the number of client devices connected in an e-learning environment. APs ignore association requests and authentication request packets from any new client device when the maximum number of client devices is reached.
2.4G / 5G / 6G Maximum client device number	Enter the maximum number of client devices (1 to 127) at which an AP begins load balancing its connections.
Group Port Settings	
LAN x	This is the name of the physical Ethernet port on the AP. This section lets you configure global port VLAN settings for all managed APs.
PVID	Enter the port's PVID. A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines.

Table 251 Wireless > WLAN Settings > AP Settings

LABEL	DESCRIPTION
Allowed VLANs	Enter the VLAN ID numbers to which the port belongs. Only the network traffic from the allowed VLANs will be sent or received through this port. You can enter individual VLAN ID numbers separated by a comma or a range of VLANs by using a dash, such as 1, 3, 5–8.
Reset	Click **Reset** to return the screen to its last-saved settings.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Custom Port Settings	This displays the individual settings of the APs in the selected AP group.
Access Points	This displays the descriptive name or MAC address of the AP.
Overwrite Settings	• This displays **Enable** if the individual settings on the AP differ from the **Group Port Settings**. • This displays **Disable** if the individual settings on the AP are the same as the **Group Port Settings**. This field is blank if the AP does not have LAN ports.
Port Status	• If the AP has LAN ports, this displays whether the port settings on each AP's LAN ports are enabled or not. • If the AP does not have LAN ports, this displays whether the AP's wireless bridge is enabled or not.
Port Setting	This displays the details of the AP's PVID and allowed VLANs settings.
Setting	Click the icon to edit the AP's port settings.

29.11.1 The Wireless > WLAN Settings > AP Settings > Edit AP Screen

By default, an AP uses the port settings of the AP group it belongs to. Use this screen to configure the port settings on each individual AP. The settings on each individual AP takes the priority over the group setting.

Go to **Wireless > WLAN Settings > AP Settings**, then click the edit icon of the AP you want to configure from the **Custom Port Settings**.

Figure 331 Wireless > WLAN Settings > AP Settings > Edit AP (LANx)

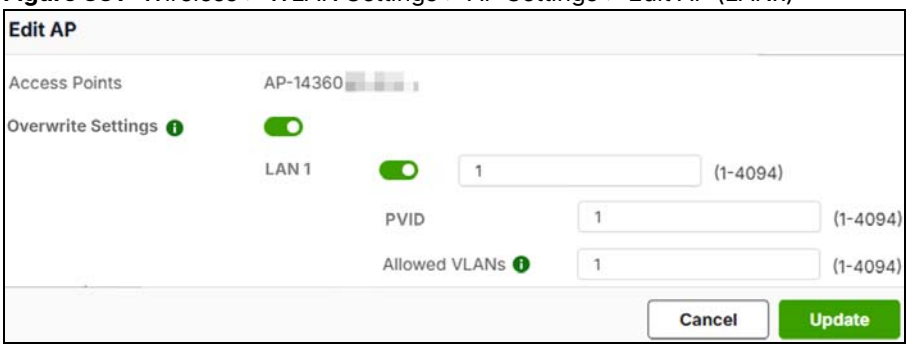
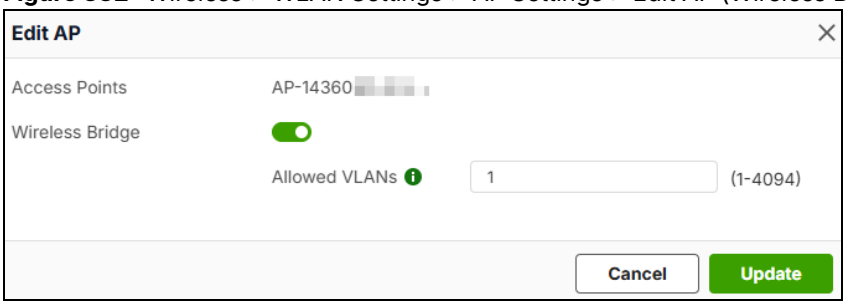


Figure 332 Wireless > WLAN Settings > AP Settings > Edit AP (Wireless Bridge)



The following table describes the labels in this screen.

Table 252 Wireless > WLAN Settings > AP Settings > Edit AP

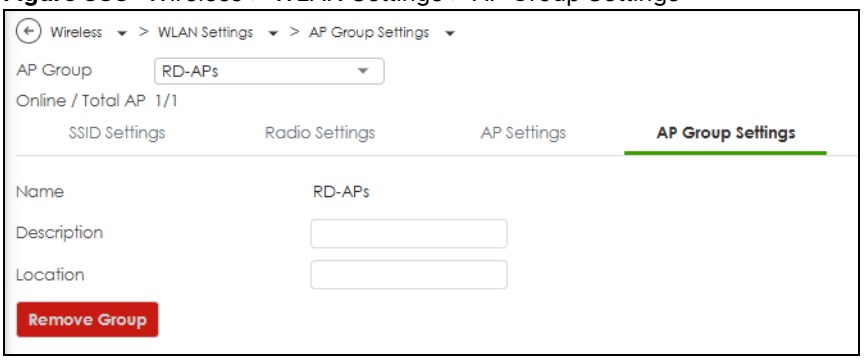
LABEL	DESCRIPTION
Access Points	This displays the descriptive name or MAC address of the AP.
Overwrite Settings	Click the switch to the right to make the AP use its individual settings instead of the **Group Port Settings**.
LAN x	This is the name of the physical Ethernet port on the AP. Click the switch to the right to enable the configured port setting for the port.
PVID	Enter the port's PVID. A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines.
Allowed VLANs	Enter the VLAN ID numbers to which the port belongs. Only the network traffic from the allowed VLANs will be sent or received through this port. You can enter individual VLAN ID numbers separated by a comma or a range of VLANs by using a dash, such as 1, 3, 5–8.
Wireless Bridge	Wireless bridge enables two devices to automatically bridge two network segments through a WiFi connection. When enabled, the system automatically creates VLAN and bridge interfaces according to the **Allowed VLANs** you configure. Note: Be careful to avoid bridge loops. A bridge loop occurs when there are two layer-2 paths between the same endpoints, causing broadcast packets to be sent back and forth indefinitely. For example, the AP and another AP both connects to the Zyxel Device, and these two APs also connect to each other using a WiFi connection. This will create bridge loops.
Allowed VLANs	Enter the VLAN ID numbers that the Zyxel Device will forward over the wireless bridge. The traffic with entered VLAN IDs can pass through the wireless bridge. You can enter individual VLAN ID numbers separated by a comma or a range of VLANs by using a dash, such as 1, 3, 5–8.
Cancel	Click **Cancel** to return the screen to its last-saved settings.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

29.12 The AP Group Settings Screen

Use this screen to configure AP group settings and remove an AP group. Click **Wireless** > **WLAN Settings** > **AP Settings** to open this screen.

Note: You must select the AP group to which the AP you want to configure belongs before configuring this screen. For example, if you want to configure AP 'WBE660S' and 'WBE660S' belongs to AP group 'RD-APs', make sure to select 'RD-APs' in **AP Group** first before configuring 'WBE660S'.

Figure 333 Wireless > WLAN Settings > AP Group Settings



The following table describes the labels in this screen.

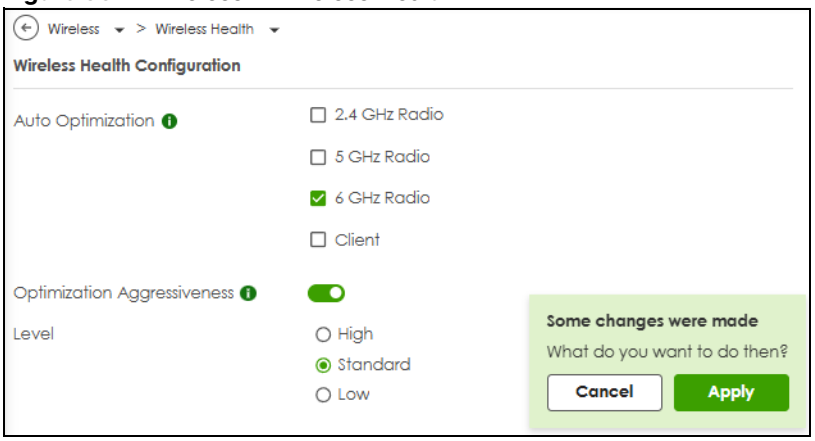
Table 253 Wireless > WLAN Settings > AP Group Settings

LABEL	DESCRIPTION
AP Group	Select the AP group to which the AP you want to configure belongs. Or click **Add** to create an AP group.
Name	This displays the AP group to which the AP you want to configure belongs.
Description	Enter a description for this group. You can use up to 31 characters, spaces and underscores allowed.
Location	Specify the name of the place where the AP group is located.
Remove Group	Select an entry and click this button to remove it from the AP group list. Note: You cannot remove a group with which an AP is associated.
Reset	Click **Reset** to return the screen to its last-saved settings.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

29.13 The Wireless Health Screen

Use this screen to monitor the health of WiFi networks for your APs and connected WiFi clients.

Figure 334 Wireless > Wireless Health



The following table describes the labels in this screen.

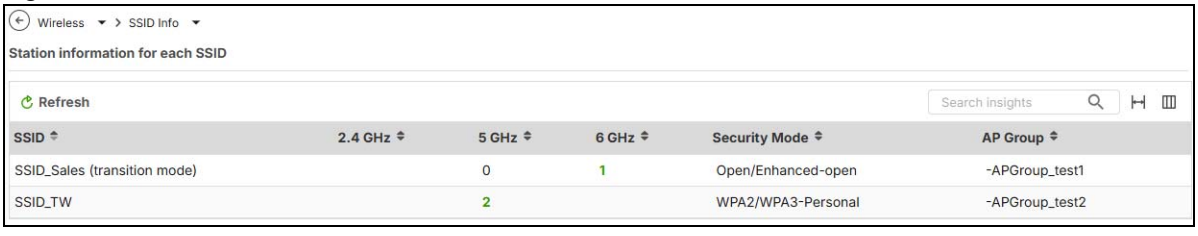
Table 254 Wireless > Wireless Health

LABEL	DESCRIPTION
Auto Optimization	
2.4 GHz Radio	Select this to have the AP scan and choose a radio channel that has least interference.
5 GHz Radio	Select this to have the AP change the channel bandwidth from 80 MHz to 20 MHz to reduce the radio interference with other APs. If the AP wireless performance has not improved, the Zyxel Device will have the AP scan and choose a radio channel that has least interference.
6 GHz Radio	Select this to have the AP change the channel bandwidth to reduce the radio interference with other APs. • For WiFi 7 APs, the channel bandwidth changes from 320 MHz to 80 MHz. • For WiFi 6E APs, the channel bandwidth changes from 160 MHz to 80 MHz. If the AP wireless performance has not improved, the Zyxel Device will have the AP scan and choose a radio channel that has least interference.
Client	Select this to have the AP try to steer the wireless clients in poor health to an AP or SSID with a strong signal every 30 minutes.
Optimization Aggressiveness	**High, Standard** and **Low** stand for different traffic rate threshold levels. The level you select here decides when the Zyxel Device takes actions to improve the APs WiFi network performance. The Zyxel Device will postpone the actions implemented on APs until your network is less busy if the threshold is exceeded. Select a suitable traffic rate threshold level for your network. • **High**: Select this if you want the Zyxel Device to postpone the action set when the AP network traffic is heavy. • **Standard**: Select this if you want the Zyxel Device to postpone the action set when the AP network traffic is medium. • **Low**: Select this if you want the Zyxel Device to postpone the action set when the AP network traffic is low.
Cancel	Click **Cancel** to return the screen to its last-saved settings.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

29.14 The SSID Info Screen

Use this screen to monitor the WiFi networks (SSIDs) currently in use and the clients connected to them.

Figure 335 Wireless > SSID Info



The following table describes the labels in this screen.

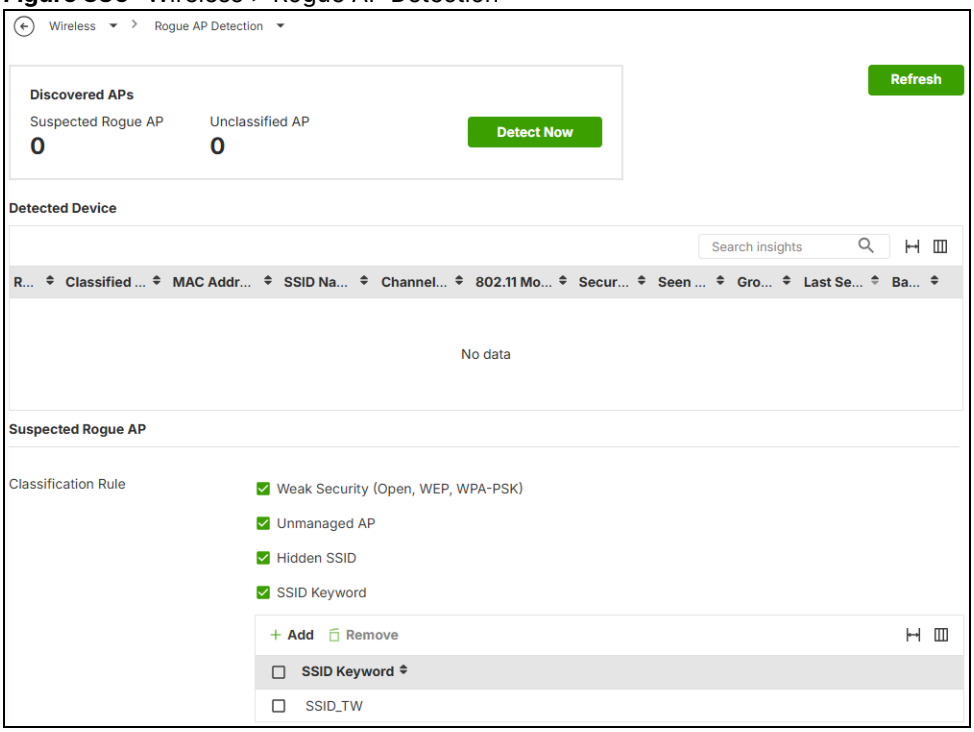
Table 255 Wireless > SSID Info

LABEL	DESCRIPTION
Refresh	Click this button to update the information on the screen. The screen also refreshes automatically when you open the screen.
SSID	This displays the WiFi network (SSID) that is currently used by the connected WiFi clients.
2.4 GHz / 5 GHz / 6 GHz	This displays the number of WiFi clients currently using the WiFi network on the corresponding band. • An empty field indicates that the band on the WiFi network (SSID) is not open. • A **0** indicates that the band on the WiFi network (SSID) is open, but no WiFi clients are connected. • A number with a hyperlink indicates the number of WiFi clients currently connected to the WiFi network (SSID) on the band. Click the number to go to the **Wireless > WLAN Clients > All Clients** screen, with the corresponding AP group automatically pre-selected.
Security Mode	This displays the encryption method used by the WiFi network (SSID).
AP Group	This displays the AP group that the WiFi network (SSID) belongs to.

29.15 The Rogue AP Detection Screen

Use this screen to enable **Rogue AP Detection**, configure detection rules, and view detected APs. See Rogue APs for details about rogue APs. Click **Wireless > Rogue AP Detection** to access this screen.

Figure 336 Wireless > Rogue AP Detection



The following table describes the labels in this screen.

Table 256 Wireless > Rogue AP Detection

LABEL	DESCRIPTION
Discovered APs	
Suspected Rogue AP	This shows how many APs are detected as possible rogue APs based on the classification rule(s).
Unclassified AP	This shows how many devices are detected, but have not been classified as a rogue AP by the Zyxel Device.
Detect Now	Click this button to scan for managed APs in the network.
Refresh	Click this to refresh the items displayed on this page.
Detected Device	
Role	This field displays the detected device's role.
Classified By	This field displays the classification rule matched by the detected device.
MAC Address	This field displays the detected device's MAC address.
SSID Name	This field displays the detected device's SSID.
Channel ID	This field displays the detected device's channel ID.
802.11 Mode	This field displays the 802.11 mode (a/b/g/n/ac/ax) transmitted by the detected device.
Security	This field displays the encryption method used by the detected device.
Seen By	This shows which AP detects the device. If an AP in monitor mode detected this AP, this column will show "**N/A**". This field displays the name of the AP and the signal strength from the detected device. If the is detected by more than one AP, only the top 5 APs with the highest signal strength will be shown.
Group	This field displays which group the detected device belongs.
Last Seen	This field displays the last time the device was detected by the Zyxel Device.
Band	This field displays the frequency band to which the detected device is connected.
Suspected Rogue AP	
Classification Rule	Select one or more characteristics an AP should have for the Zyxel Device to determine it as a suspected rogue AP.
Weak Security (Open, WEP, WPA-PSK)	Select this to determine a device as a suspected rogue AP if it is using an SSID with weak security (Open, WEP, WPA-PSK).
Unmanaged AP	Select this to determine a device as a suspected rogue AP if it is not managed by the Zyxel Device.
Hidden SSID	Select this to determine a device as suspected rogue AP if it broadcast hidden SSIDs for wireless clients.
SSID Keyword	Select this option to mark a device as a suspected rogue AP if it broadcasts an SSID containing the configured keyword.
Add	Click this to add a keyword based on the SSID name as a detection rule. Note: You can add up to ten keywords.
Remove	Click this to remove the selected keyword(s).
SSID Keyword	Enter a keyword from the SSID name for detection. Use up to 32 characters [0-9a-zA-Z`~!@#$%^&*()-_=+,<.>/?;:'"[{]} |].
Edit	Select an SSID Keyword and click this button to modify it.
Delete	Select an SSID Keyword and click this button to remove it.

Table 256 Wireless > Rogue AP Detection (continued)

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

29.16 Wireless Application Example

This section contains application examples about the features described in this chapter.

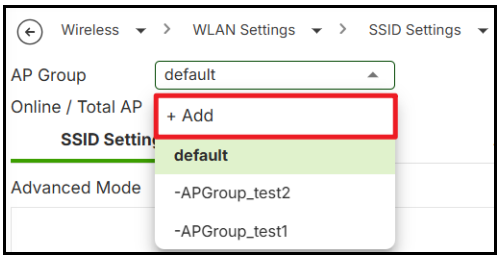
Set Up a WiFi Network (SSID) and Schedule the Enabled Time

In this example, you want to schedule a WiFi network (SSID) for school students. School hours are Monday to Friday, from 08:10 to 14:00.

Enable the WiFi network (SSID) during the following periods:

- 10 minutes before school starts: 8:00–8:10
- Morning class break times (10 minutes each): 9:00–9:10, 10:00–10:10, 11:00–11:10
- Lunch break (1 hour and 10 minutes): 12:00–13:10
- 1 hour after school ends: 14:00–15:00

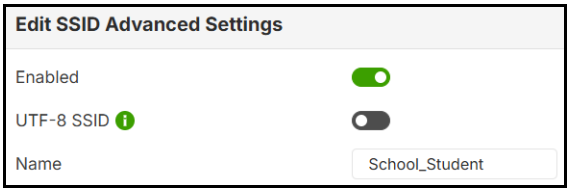
1 Go to **Wireless > WLAN Settings**. Click the **AP Group** drop-down list and select **+Add** to create an AP group for your school. Click **Apply**.



2 Go to **Wireless > Access Points**. Select the managed AP set up for the school and click **Edit**. Select the AP group you created from the **Group** drop-down list. Click **Apply**.

3 Go to **Wireless > WLAN Settings > SSID Settings**. Select the AP group for your school from the **AP Group** drop-down list. Slide **Advanced Mode** to the right to display advanced SSID settings. Click **Edit** for an SSID profile.

4 Configure a name for the WiFi network (SSID), for example, **School_Student**.

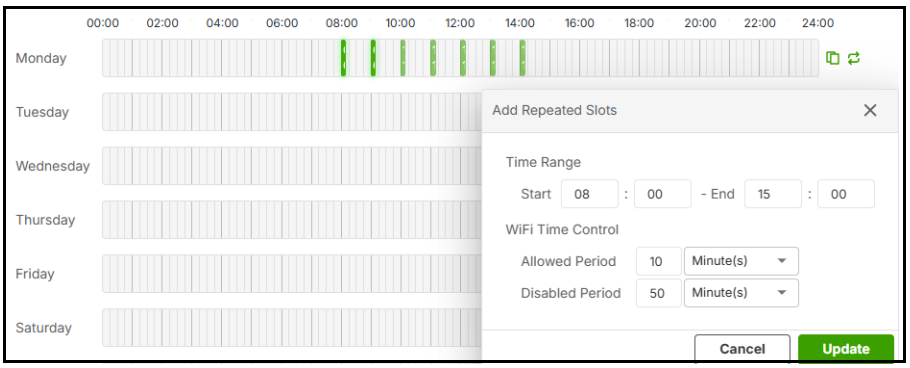


5 Slide the **SSID Schedule** switch to the right to enable it.

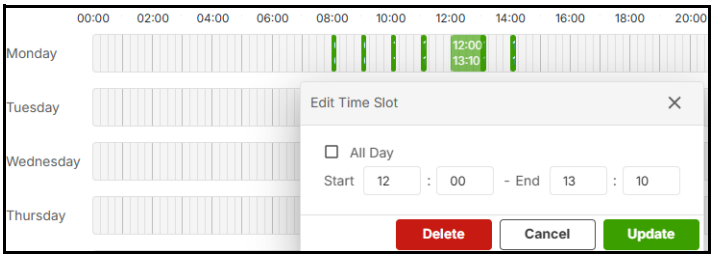
6 Clink **Repeat** for **Monday**.

Set the **Start** time to **08:00** and the **End** time to **15:00** to cover the school hour period, including the 10 minutes before classes start and 1 hour after school hour.

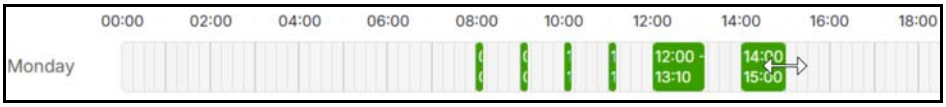
Set the **Allowed Period** to **10 Minute(s)** and the **Disallowed Period** to **50 Minute(s)**. Click **Update**.



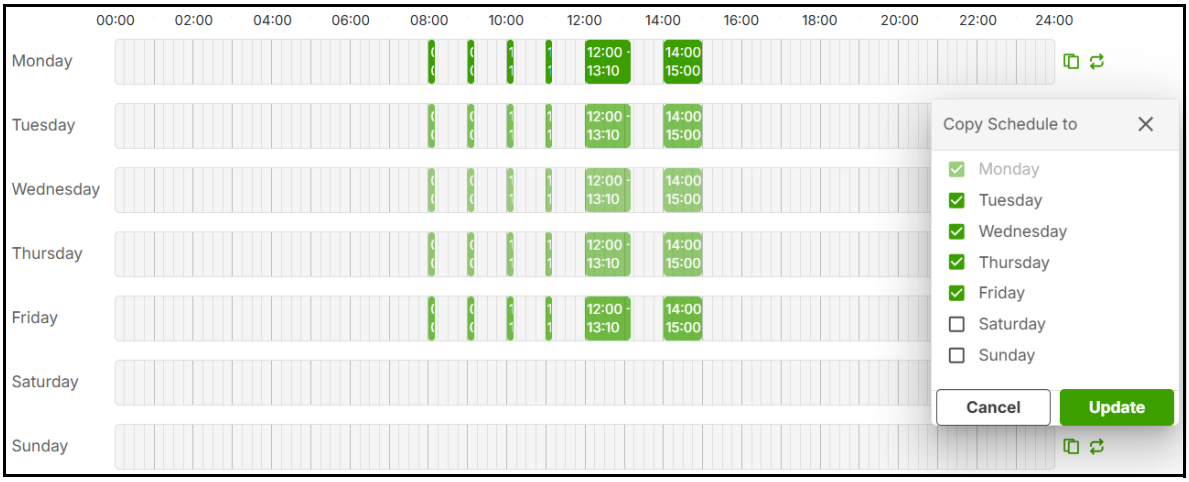
7 Double-click the time slot starting at 12:00 and adjust the **End** time to **13:10** to cover the lunch break. Click **Update**.



8 Click and drag the right edge of the time slot starting at 14:00 to adjust the **End** time to **15:00** for the after-school period.



9 Click **Copy** for **Monday** and select **Tuesday** through **Friday** to copy **Monday**'s settings to those days. Click **Update**.



29.17 Wireless Technical Reference

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

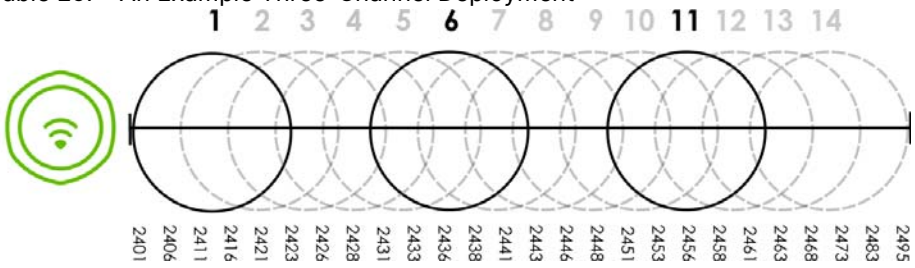
Dynamic Channel Selection

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.

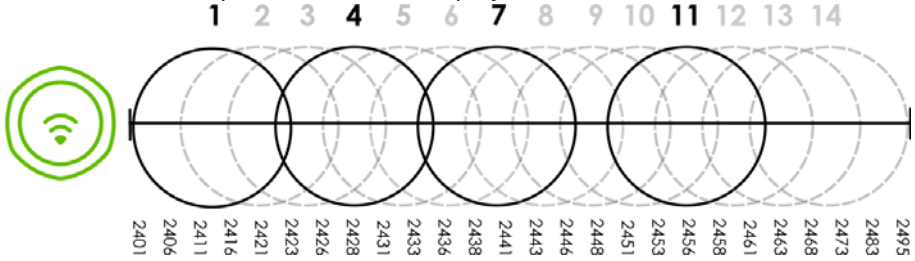
Three channels are situated in such a way as to create almost no interference with one another if used exclusively: 1, 6 and 11. When an AP broadcasts on any of these 3 channels, it should not interfere with neighboring APs as long as they are also limited to same trio.

Table 257 An Example Three-Channel Deployment



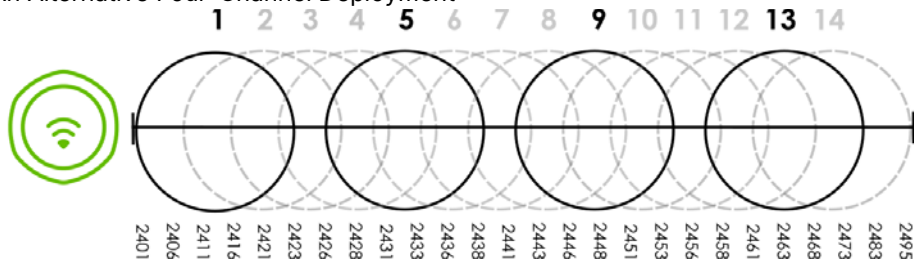
However, some regions require the use of other channels and often use a safety scheme with the following four channels: 1, 4, 7 and 11. While they are situated sufficiently close to both each other and the three so-called “safe” channels (1,6 and 11) that interference becomes inevitable, the severity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

Table 258 An Example Four-Channel Deployment



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.

An Alternative Four-Channel Deployment



CHAPTER 30
System

30.1 Overview

Use the system screens to configure general Zyxel Device settings.

30.1.1 What You Can Do in this Chapter

- Use the **System > Settings** screen (see Section 30.2 on page 564) to configure the Zyxel Device basic system settings.
- Use the **System > Device HA** screens (see Section 30.3 on page 570) to configure a backup for the Zyxel Device.
- Use the **System > DNS & DDNS** screen (see Section 30.4 on page 581) to configure the Zyxel Device DNS and DDNS settings.
- Use the **System > SNMP** screen (see Section 30.5 on page 596) to configure the Zyxel Device SNMP settings.
- Use the **System > Notification** screen (see Section 30.6 on page 601) to configure a mail server to receive reports and notification emails.
- For an overview of certificates, see Section 30.7 on page 609.
- Use the **System > My Certificates** screen (see Section 30.8 on page 612) to generate self-signed certificates or certification requests.
- Use the **System > Trusted Certificates** screens (see Section 30.9 on page 621) 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.
- Use the **System > Let's Encrypt Certificate** screen (see Section 30.10 on page 625) to specify certificates generated by **Let's Encrypt**.
- Use the **System > Advanced** screen (see Section 30.11 on page 629) to view UDP and ICMP timeout settings on your Zyxel Device and to enable or disable ARP spoofing prevention, device insight, and LLDP functions.
- Use the **System > External Integrations** screen (see Section 30.12 on page 633) to integrate the Zyxel Device with other cloud-based security platforms such as the Avast Business Hub.

See each section for related background information and term definitions.

30.2 Settings

Use the **Settings** screen to configure the hostname, system time, the Zyxel Device connection settings and language settings.

30.2.1 System Settings

Use this section to configure the Zyxel Device host name. A host name is the unique name by which a device is known on a network.

30.2.2 System Time

Use this section to configure the Zyxel Device time settings. 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, go to **System > Settings > System Time**. 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.

To manually set the Zyxel Device date and time.

1 Go to **System > Settings > System Time**.

2 Select **Manual** in the **Time** field. Then enter or select the Zyxel Device's time and date.

3 In the **Timezone** field, select your timezone from the list.

4 Click **Apply**.

To get the Zyxel Device date and time from a time server

1 Go to **System > Settings > System Time**.

2 Select **Auto Sync** in the **Time** and **Timezone** field.

3 Click **Apply**.

30.2.3 Administration Settings

Use this section to configure secure and insecure connection of the Zyxel Device coming in from the WAN. HTTPS and SSH access are secure. HTTP access is 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, slide the switch to the left in the corresponding service screen to disable the service.

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.

HTTPS

You can set the Zyxel Device to use HTTP or HTTPS (HTTPS adds security) for Web Configurator sessions.

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.

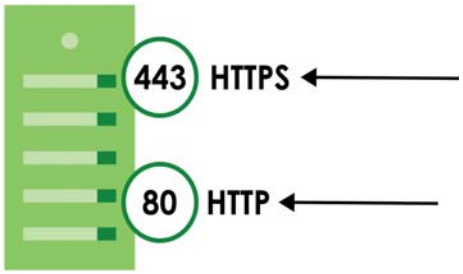
HTTPS on the Zyxel Device is used so that you can securely access the Zyxel Device using the Web Configurator. The SSL protocol specifies that the HTTPS server (the Zyxel Device) must always authenticate itself to the HTTPS client (the computer which requests the HTTPS connection with the Zyxel Device), whereas the HTTPS client only should authenticate itself when the HTTPS server requires it to do so (enable **Authenticate Client Certificates** in the **Administration Settings** 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 337 HTTP/HTTPS Implementation



Note: If you disable **HTTP** in the **Administration Settings** screen, then the Zyxel Device blocks all HTTP connection attempts.

SSH

You can use SSH (Secure SHell) to securely access the Zyxel Device's command line interface.

SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. In the following figure,

computer **A** on the Internet uses SSH to securely connect to the WAN port of the 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 338 SSH Communication Over the WAN Example



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).

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.

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.

Device Insight

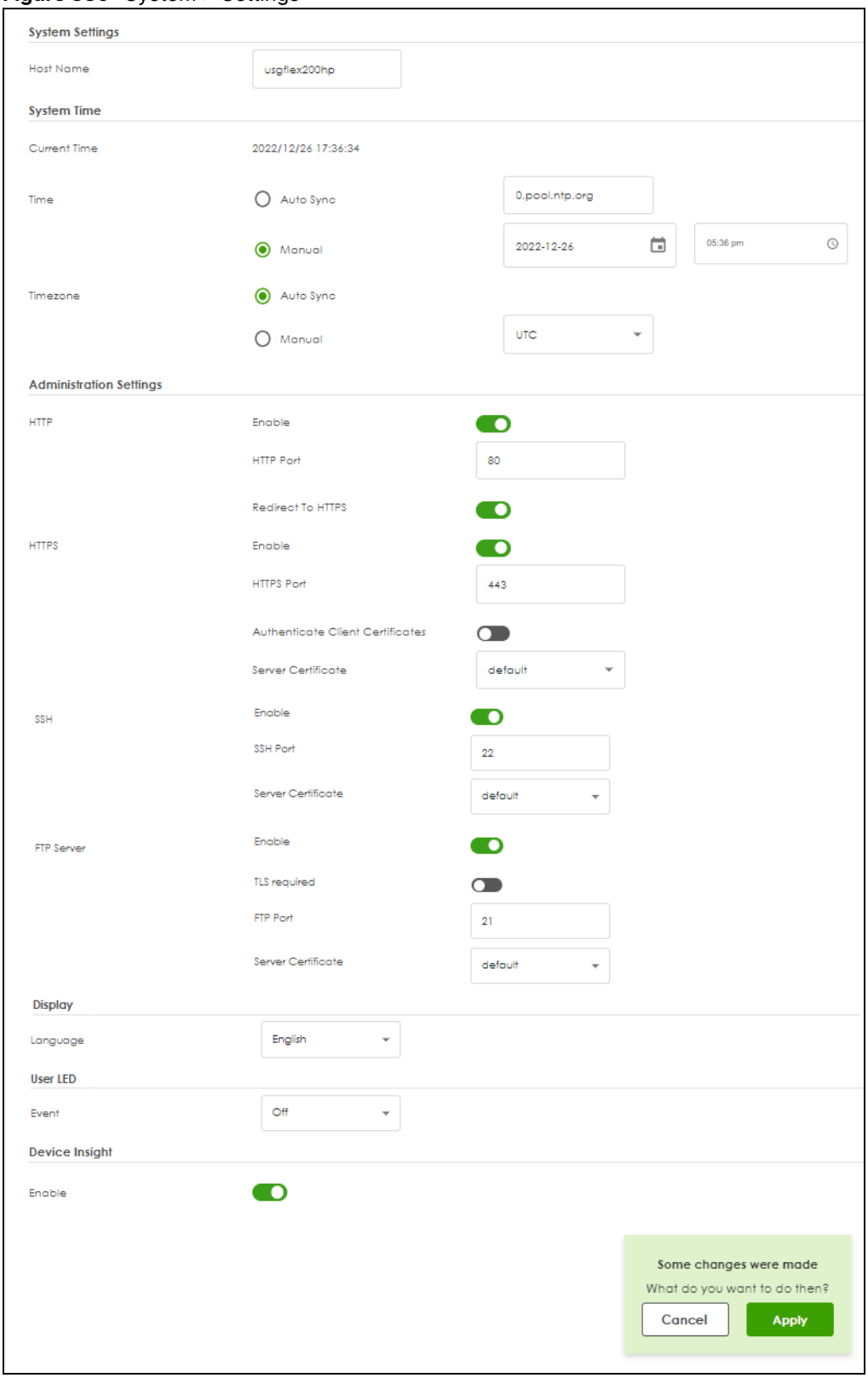
Use **Device Insight** to collect status and basic information of the clients connected to the Zyxel Device internal interfaces or IPSec VPN; see Section 5.13 on page 106 for more information.

30.2.4 Settings

Use this section to select a display language for the Zyxel Device's Web Configurator screens.

Click **System > Settings** to open the following screen.

Figure 339 System > Settings



The following table describes the labels in this screen.

Table 259 System > System Settings

LABEL	DESCRIPTION
System Settings	
Host Name	Enter a descriptive name to identify your Zyxel Device device. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes (-) underscores (_) and periods (.) are accepted.
System Time	
Current Time	This field displays the present date and time of your Zyxel Device.
Time	Select **Auto Sync** to have the Zyxel Device get the time and date from the time server. 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** after selecting **Auto Sync** in this screen. • 24-hour intervals after starting up. Select **Manual** to enter or select the time and date manually. When you enter the time and date settings manually, the Zyxel Device uses the new settings once you click **Apply**.
Timezone	Select **Auto Sync** for the Zyxel Device to automatically get its timezone. Select **Manual** to choose the timezone of your location. This will set the time difference between your timezone and Greenwich Mean Time (GMT).
Administration Settings	
HTTP Enable	Enable to allow access to the Zyxel Device using HTTP connections.
HTTP Port	The HTTP server listens on port 80 by default. If you change the HTTP port to a different number on the Zyxel Device, for example 8080, then you must notify people who need to access the Zyxel Device Web Configurator to use "http://Zyxel Device IP Address:8080" as the URL. If you choose a port already in use, you will see a port conflict message telling you to choose another port. System > Settings > HTTP port conflict with another service System > Settings > HTTPS. Choose a different port for configuration changes.
Redirect to HTTPS	Enable this to redirect all HTTP connection requests to the HTTPS server to allow only secure Web Configurator access.
HTTPS Enable	Enable to allow access to the Zyxel Device Web Configurator using secure HTTPS connections.
HTTPS Port	The HTTPS server listens on port 443 by default. If you change the HTTPS 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. If you choose a port already in use, you will see a port conflict message telling you to choose another port. System > Settings > HTTPS port conflict with another service System > Settings > HTTP. Choose a different port for configuration changes.
Authenticate Client Certificates	Enable this 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.
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.
SSH Enable	Enable to allow access to the Zyxel Device using SSH connections.
SSH Port	The SSH port is 22 by default. 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. If you choose a port already in use, you will see a port conflict message telling you to choose another port. System > Settings > SSH port conflict with another service System > Settings > FTP. Choose a different port for configuration changes.

Table 259 System > System Settings (continued)

LABEL	DESCRIPTION
Server Certificate	Select a 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.
FTP Enable	Enable to allow access to the Zyxel Device using FTP connections.
TLS required	Enable to use FTP over TLS (Transport Layer Security) to encrypt communication. This implements TLS as a security mechanism to secure FTP clients and servers.
FTP Port	The FTP port is 21 by default. 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. If you choose a port already in use, you will see a port conflict message telling you to choose another port. System > Settings > FTP port conflict with another service System > Settings > SSH. Choose a different port for configuration changes.
Server Certificate	Select a 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.
Display	
Language	Select a display language for the Zyxel Device's web configurator screens. The web configurator screens will display in the new language after you click **Apply**.
User LED	The **USER** LED is located at the front panel of the Zyxel Device. Use this LED to check one of the following: • Admin account login status. • User IP address locked out status. • License status. • New firmware available for update.
Event	Select how you want the **USER** LED to behave. • Select **Admin login (green on)** if you want the **USER** LED to be steady green when there are admin accounts logged into the Zyxel Device. • Select **User Lockout (amber on)** if you want the **USER** LED to be steady amber when a user IP address is locked out of the Zyxel Device. A user IP address will be locked out when the user has logged into the Zyxel Device unsuccessfully (for example, wrong password) for more than three times. • Select **License Expired (amber on)** if you want the **USER** LED to be steady amber when a Zyxel Device service license has expired. • Select **New Firmware Available (green blinking)** if you want the **USER** LED to blink green when there is new firmware available for upload. • Select **Off** to turn off the **USER** LED.
Device Insight	Enable Device Insight to collect status and basic information of the clients connected to the Zyxel Device internal interfaces or IPSec VPN.
Apply	Click **Apply** to save your changes to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

30.3 Device HA (High Availability)

Device HA lets a passive (secondary) Zyxel Device automatically take over if the active (primary) Zyxel Device fails. The secondary Zyxel Device will use the same management mode as the primary Zyxel Device (Nebula or Web Configurator). Both Zyxel Devices must be the same model with the same firmware version. Device HA pairing occurs when Device HA is set up successfully on both Zyxel Devices.

The primary Zyxel Device is the license controller. Existing licenses on the secondary Zyxel Device are appended to the licenses on the primary Zyxel Device after pairing occurs. When updating licenses, update them on the primary Zyxel Device.

The following features can be transferred to the secondary Zyxel Device when it becomes active using Device HA:

- Start-up and Running Configuration
- Signatures
- Device Insight
- External Block List
- DHCP Leasing Entries
- Two-factor Authentication
- Certificates
- Licenses Including NCC if applicable
- Zyxel Device Time

For HTTP and Captive Portal, session states (login / logout events, idle timeout) are also synchronized between active and passive Zyxel Devices.

Device HA uses SSH port 49058 for file synchronization between the active and passive Zyxel Devices. You cannot change this port number.

30.3.1 What You Can Do in These Screens

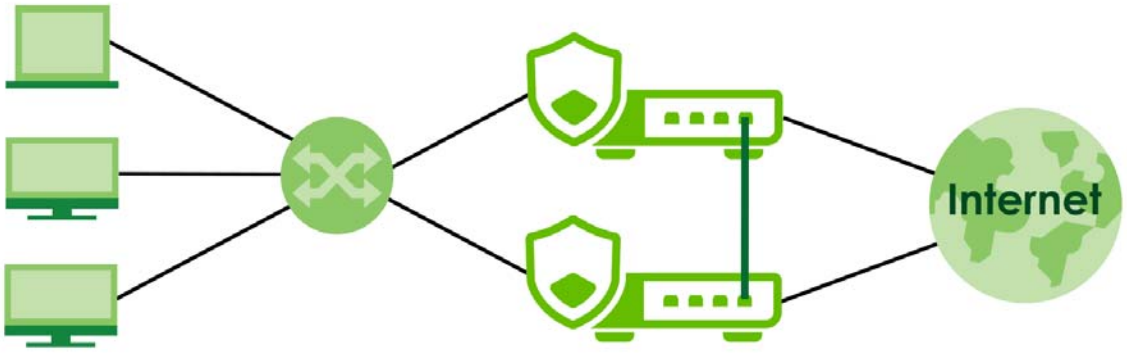
- Use the **HA Status** screen (Section 30.3.7 on page 574) to see the license status for Device HA, and see the status of the active and passive devices.
- Use the **HA Configuration** screen (Section 30.3.8 on page 576) to configure Device HA global settings, monitored interfaces and synchronization settings.
- Use the **HA Log** screen (Section 30.3.9 on page 578) to see logs of the active and passive devices.

30.3.2 Heartbeat

Device HA uses a dedicated heartbeat link between an active and a passive device for status syncing and to trigger failover and backup to the passive device if the active device becomes unresponsive. On the passive device, all ports are disabled except for the port with the heartbeat link.

In the following example, Zyxel Device **A** is the active device that is connected to passive device Zyxel Device **B** through a dedicated link that is used for heartbeat control, configuration synchronization and troubleshooting. All links on Zyxel Device **B** are down except for the dedicated heartbeat link.

Figure 340 Device HA Overview



Note: Make sure that the heartbeat port is not already in an interface that is already configured for other features such as LAG, VLAN, Bridge.

Note: The dedicated heartbeat link port must be the highest-numbered copper Ethernet port on each Zyxel Device for Device HA to work. At the time of writing, these are the models that support HA with associated heartbeat link ports.

Table 260 Device HA Heartbeat Ports

MODEL	HEARTBEAT PORT
USG FLEX 200H / 200HP	8
USG FLEX 500H / 700H	12

Failover from the active Zyxel Device to the passive Zyxel Device occurs when:

- A monitored interface is down on the active Zyxel Device.
- The connectivity check on the heartbeat link exceeds the failure tolerance.
- The active Zyxel Device reboots.

After failover, the initially active Zyxel Device becomes the passive Zyxel Device.

30.3.3 GARP and Virtual IP / MAC Address

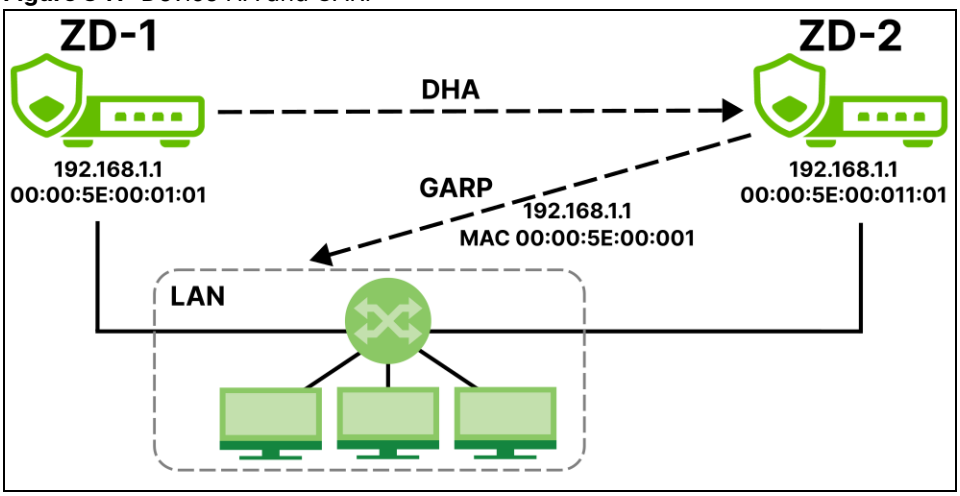
A Virtual MAC (VMAC) address is a shared, logical MAC address that is tied to a Virtual IP (VIP) address and not a physical network interface. In Device HA, both Zyxel Devices use the same VMAC and VIP.

An ARP (Address Resolution Protocol) is a request that must be sent to find the MAC address of another device. A Gratuitous ARP (GARP) is an unsolicited ARP message used to announce or refresh a device's IP-to-MAC mapping on a local network.

In Device HA, only the active Zyxel Device uses the VMAC to respond to requests for the virtual IP. If the active Zyxel Device fails, then the passive Zyxel Device takes over. The newly active Zyxel Device uses GARP to announce its IP address on the local network and begins using the same VMAC. All connected hosts update their ARP tables, and connected switches update their MAC address tables, to map the VIP to the newly active Zyxel Device port. This ensures traffic is redirected instantly to the newly active Zyxel Device, without waiting for ARP entries to time out.

In the following figure, ZD-1 is the original active Zyxel Device, and ZD-2 the original passive Zyxel Device. If ZD-1 fails, then ZD-2 takes over as the active Zyxel Device, and sends GARP to all devices on the local network, so that they can update their ARP tables.

Figure 341 Device HA and GARP



30.3.4 Preparing to Deploy Device HA

1. Make sure the passive Zyxel Device is offline, then enable Device HA in **System > Device HA > HA Configuration** in the active Zyxel Device.
2. The management IP addresses for both the active and passive Zyxel Devices must be in the same subnet.
3. Make sure the SSH service in **System > SSH** is enabled on both Zyxel Devices. SFTP (Secure File Transfer Protocol) is used to transfer files from the active to the passive Zyxel Device.
4. Connect the passive Zyxel Device to the active Zyxel Device using the heartbeat ports. These are the highest-numbered copper Ethernet ports on the Zyxel Devices - see Table 260 on page 572.
5. If both Zyxel Devices are turned on at the same time with Device HA enabled, then they may send the heartbeat at the same time. In this case, the Zyxel Device with the **Primary (License Controller)** role becomes the active Zyxel Device.

30.3.5 Using NCC To Manage Device HA

You must register both Zyxel Devices on NCC, that is they must both belong to an organization. The passive Zyxel Device will be registered automatically in NCC if it is not already registered in NCC.

Both Zyxel Devices must be in the same organization and be registered to the same account.

The passive Zyxel Device is removed from the NCC site after Device HA pairing is complete, as a site in NCC can only have one Zyxel Device firewall (at the time of writing).

NCC automatically sends an email to notify users when Zyxel Devices are paired with licenses transferred.

30.3.6 Deployment Overview

Register both Zyxel Devices on NCC if you are using NCC.

1 Set up Device HA on the active Zyxel Device in **System > Device HA > HA Configuration**. Check the HA status in **System > Device HA > HA Status**, and view the log of the active Zyxel Device in **System > Device HA > HA Log**.

2 Configure Device HA on the passive Zyxel Device in **System > Device HA > HA Configuration**.

3 Connect the heartbeat Ethernet cable between the active and passive Zyxel Devices.

4 Verify the HA status of the active and passive Zyxel Devices in **System > Device HA > HA Status**.

5 Check the logs on the active Zyxel Device in **System > Device HA > HA Log**.

When you log into a Zyxel Device after Device HA pairing, you will see a banner to show if you are logged into the active or passive Zyxel Device.

30.3.7 HA Status

After you have configured Device HA in **System > Device HA > HA Configuration** go to this screen to view Device HA synchronization and failover status.

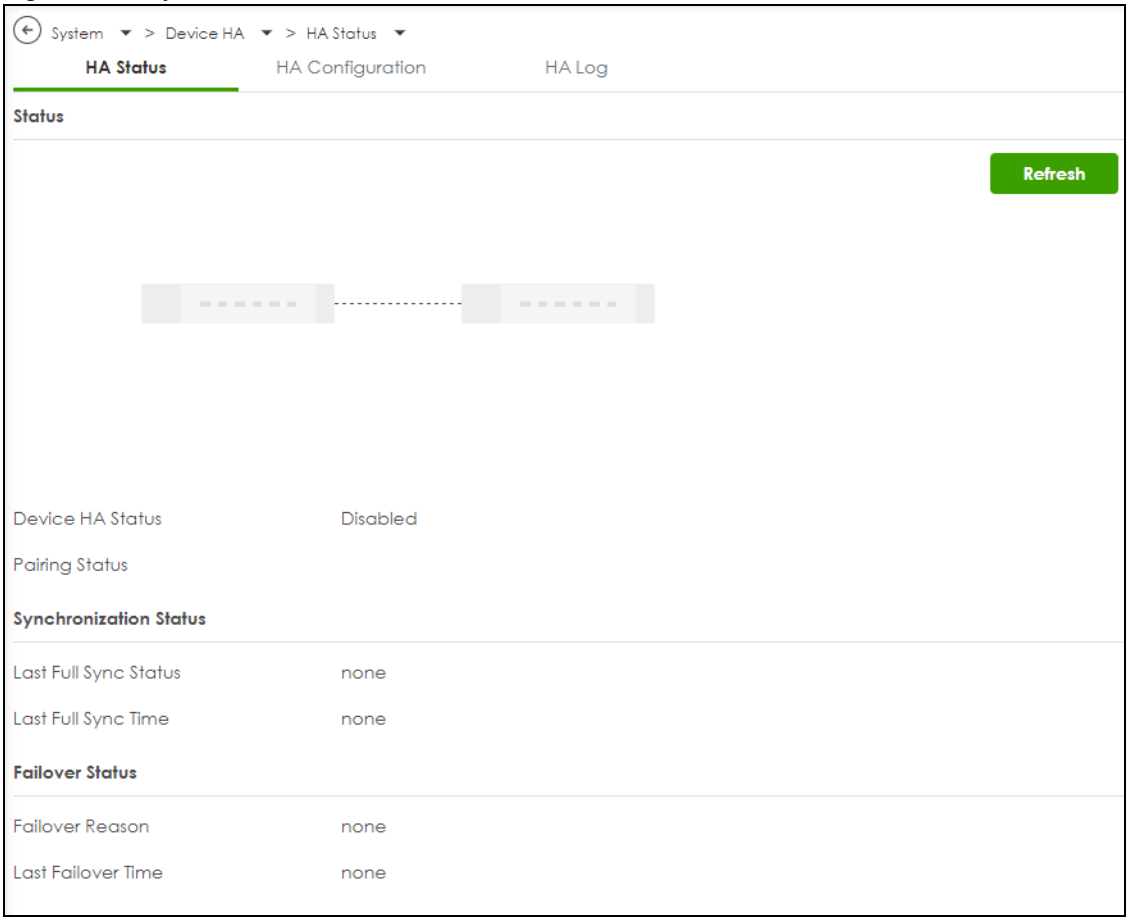
You may also see Device HA status from the PWR/SYS LED.

Table 261 Device HA Status: PWR / SYS LED

DEVICE HA STATUS	ACTIVE ZYXEL DEVICE	PASSIVE ZYXEL DEVICE
Pairing in Progress	Green / Red Alternating	Green Steady On
Pairing Failed	Red Blinking	Green Steady On
Full Synch In Progress	Green Steady On	Amber Blinking
Full Synch Complete	Green Steady On	Amber Steady On
Running	Green Steady On	Amber Steady On

Go to **System > Device HA > HA Status** to view the following screen.

Figure 342 System > Device HA > HA Status



The following table describes the labels in this screen.

Table 262 System > Device HA > HA Status

LABEL	DESCRIPTION
Status	Zyxel Devices are displayed according to role with the active Zyxel Device on the left and the passive Zyxel Device on the right. The active Zyxel Device is the initial active Zyxel Device, and the passive Zyxel Device is the initial passive Zyxel Device. The active becomes passive if failover occurs. The heartbeat link shows one of the following icons: • Running, indicating that the link is connected and the peer Zyxel Device is replying • Disconnect, indicating that the link is not connected • No response, indicating that the link is connected, but the peer Zyxel Device is not replying
Device HA Status	This displays if Device HA is **Enabled** or **Disabled**.
Pairing Status	Device HA pairing occurs when Device HA is set up successfully on both Zyxel Devices. This field displays one of the following: • **Pairing**, indicating that Device HA is in progress • **Paired**, indicating that Device HA has completed successfully • Error, showing the reason that Device HA failed.

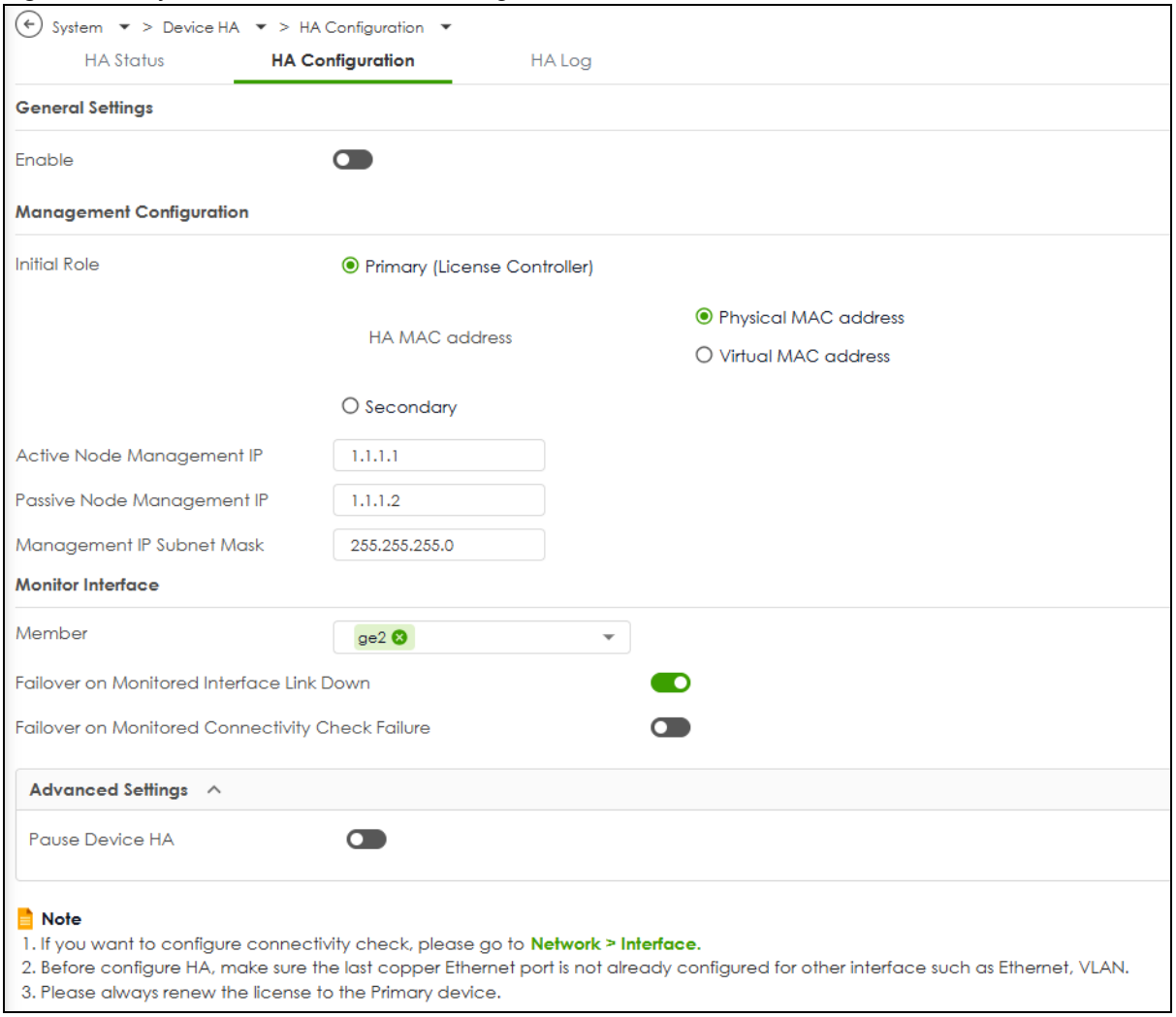
Table 262 System > Device HA > HA Status (continued)

LABEL	DESCRIPTION
Synchronization Status	This section displays information on feature transfer status and time after full synchronization occurs.
Last Full Sync Status	This displays **In Progress, Success**, **Fail** or **none** (if Device HA is not enabled or just after the Zyxel Device reboots).
Last Failover Time	This displays the date and time feature transfer occurred or **none** (if Device HA is not enabled or just after the Zyxel Device reboots).
Failover Status	This section displays the reason for failover and the time it occurred.
Failover Reason	This displays the reason for failover, such as **Heartbeats missed, Monitor interface link down, Monitor interface connectivity check fail, Firmware upgrade, Heartbeats conflict, Active device reboot**. **Heartbeats conflict** may occur if both Zyxel Devices send heartbeats at the same time, for example, if both Zyxel Devices start up at the same time.
Last Failover Time	This displays the date and time the failover occurred.

30.3.8 HA Configuration

Configure Device HA on the Zyxel Device in **System > Device HA > HA Configuration**.

Figure 343 System > Device HA > HA Configuration



The following table describes the labels in this screen.

Table 263 System > Device HA > HA Configuration

LABEL	DESCRIPTION
General Settings	
Enable Device HA	You must enable Device HA on both the active and passive Zyxel Devices. Before enabling Device HA, go to **Network > Interface** to configure the heartbeat link connectivity check between the initial active and initial passive Zyxel Devices. Make sure the passive Zyxel Device is offline when you enable Device HA on the active Zyxel Device. You cannot use Recovery Manager when you enable Device HA.
Management Configuration	Management IPs allows you to manage whichever is the active Zyxel Device when Device HA is paired. You must configure management IP addresses for both the active and passive Zyxel Devices and they must have the same subnet mask.

Table 263 System > Device HA > HA Configuration (continued)

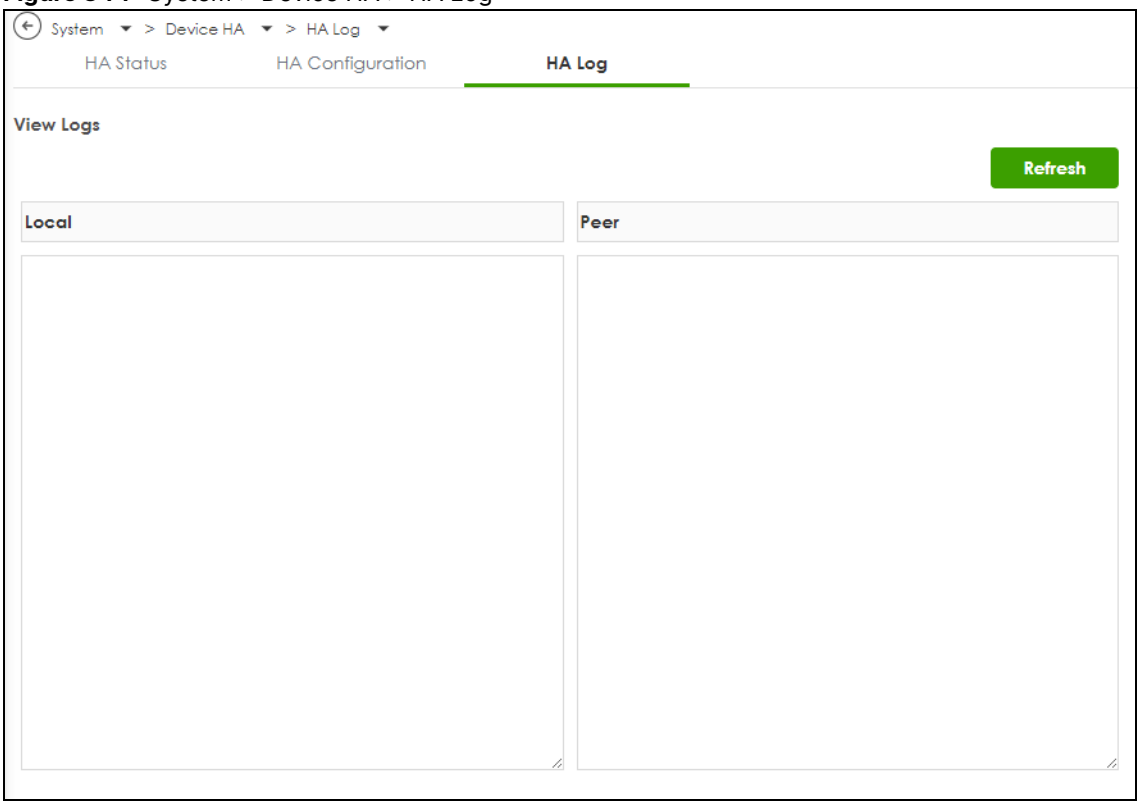
LABEL	DESCRIPTION
Initial Role	Select if this Zyxel Device is the initial active (**Primary (License Controller)**) or initial passive (**Secondary**) Zyxel Device. When you apply Device HA on the **Secondary** Zyxel Device, the LAN/WAN links will go down and you will be logged out of the web configurator. The following fields will also be grayed out. You must configure the following fields when you select **Primary (License Controller).**
HA MAC Address	Enter either the **Physical MAC address** of the initially active Zyxel Device or the **Virtual MAC address**. See **Dashboard > System** for the **Physical MAC address** of this Zyxel Device**.** The Zyxel Device automatically generates the **Virtual MAC address**. It has priority over the **Physical MAC address**. With a **Virtual MAC address**, the passive Zyxel Device can take over from the active Zyxel Device without reconfiguring Device HA. At the time of writing, the **Virtual MAC address** begins with "X6", (X6:XX:XX:XX:XX:XX). You can see the **Virtual MAC address** generated in **Network > Interface > Edit** of the active Zyxel Device.
Active Node Management IP	Type the IPv4 address of the highest-numbered copper Ethernet port on the active Zyxel Device (the heartbeat dedicated link port).
Passive Node Management IP	Type the IPv4 address of the highest-numbered copper Ethernet port on the passive Zyxel Device (the heartbeat dedicated link port).
Management IP Subnet Mask	**Primary** and **Secondary** Zyxel Devices must use the same subnet mask. Enter a subnet mask such as 255.255.255.0, of the management IP addresses.
Monitor Interface	
Member	Member interface types can be Ethernet, VLAN, or Bridge. Select an interface to be monitored by Device HA to determine if a passive Zyxel Device should become active.
Failover on Monitored Interface Link Down	Enable this to have the passive Zyxel Device become the active Zyxel Device when a selected monitored interface fails.
Failover on Monitored Connectivity Check Failure	Enable this to have the passive Zyxel Device become the active Zyxel Device when the connectivity check fails on a selected monitored interface.
Advanced Settings	
Pause Device HA	Enable this if you want to temporarily stop Device HA without unpairing the active and passive Zyxel Devices. You may do this to troubleshoot the active Zyxel Device for example. Note: Before you click **Apply** in this screen, first make sure to turn off or disconnect ALL cables from the passive Zyxel Device! After successfully troubleshooting, remember to disable **Pause Device HA**, then turn on and reconnect ALL cables on the passive Zyxel Device. Note: You cannot upload firmware while **Pause Device HA** is enabled.
Cancel	Click **Cancel** to return the screen to its last-saved settings.
Apply	Click **Apply** to save your Device HA configurations back to the Zyxel Device but keep the Zyxel Device using Device HA (general).

30.3.9 HA Log

Use this screen to see Device HA logs on the local and peer Zyxel Devices. The local Zyxel Device is the Zyxel Device that you are currently logged into.

Go to **System > Device HA > HA Log** to display the following screen.

Figure 344 System > Device HA > HA Log



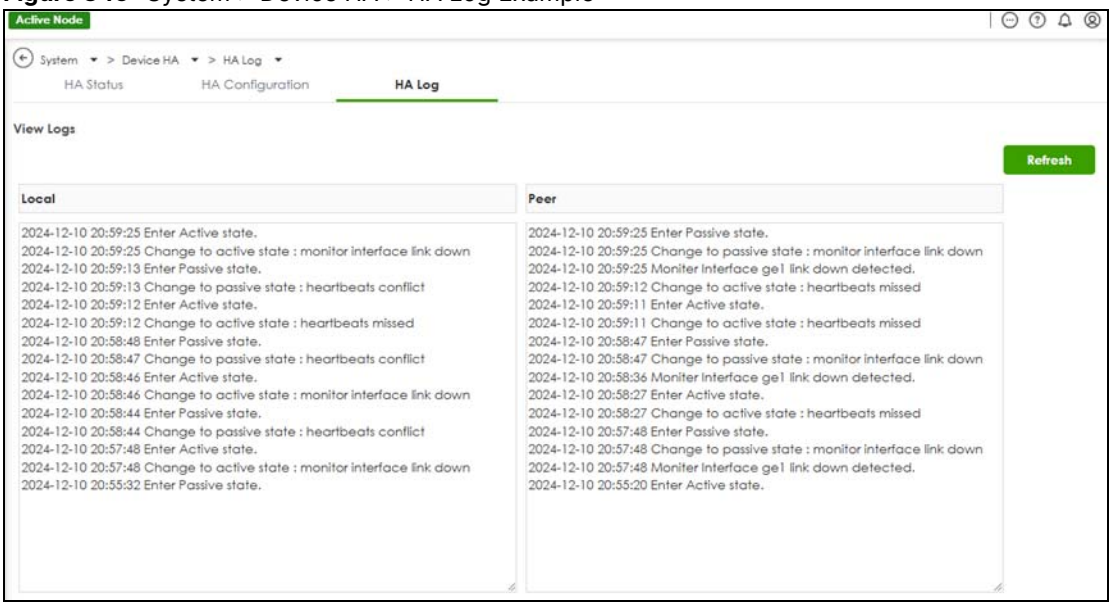
The following table describes the labels in this screen.

Table 264 System > Device HA > HA Log

LABEL	DESCRIPTION
View Logs	
Local	This displays Device HA logs on the Zyxel Device that you are currently logged into.
Peer	This displays Device HA logs on the Zyxel Device that has a heartbeat link to the Zyxel Device that you are currently logged into, that is, the Device HA peer.
Refresh	Click **Refresh** to update information in this screen.

The following is an example HA log screen when logging into the active Zyxel Device.

Figure 345 System > Device HA > HA Log Example



30.3.10 Firmware Upgrade on Paired Zyxel Devices

You cannot upload firmware while Device HA is enabled, but paused. You must first disable **Pause Device HA** in **System > Device HA > HA Configuration** before uploading firmware.

1 Upgrade the firmware to the active Zyxel Device.

2 Device HA will then perform the following steps to upgrade the firmware to the passive Zyxel Device.

2a Device HA upgrades the firmware to the passive Zyxel Device.

2b After the passive Zyxel Device reboots, the firmware upgrade process then continues on the original active Zyxel Device.

2c While the original active Zyxel Device reboots, the passive Zyxel Device becomes the active Zyxel Device and handles all traffic during the firmware upgrade.

After the firmware upgrade is complete on both Zyxel Devices, the original passive Zyxel Device becomes the active Zyxel Device.

If Device HA is disabled, you can use the CLI command `cmd firmware boot-option 1` to upload firmware to the Zyxel Device (on which you issued the command) without triggering a reboot.

However, when Device HA is enabled, the Zyxel Device will automatically reboot if you use this CLI command, and it will also ignore the boot-option if you changed the default.

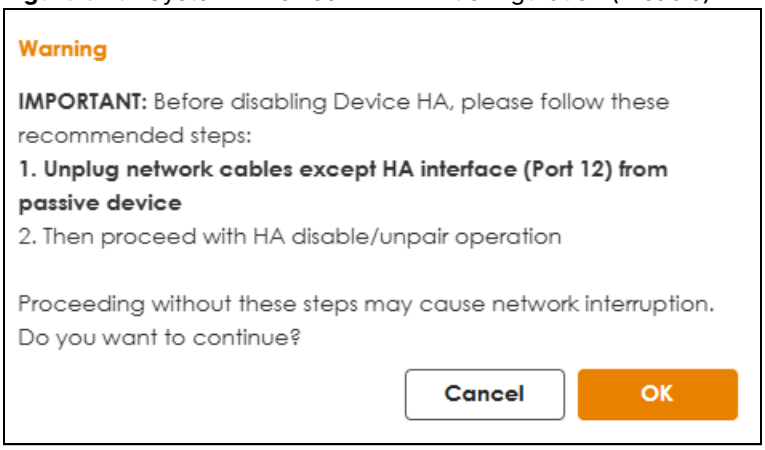
30.3.11 Disabling Device HA

Turning off an active or passive Zyxel Device alone does not disable Device HA. To disable Device HA, you must use **System > Device HA > HA Configuration** in the web configurator or CLI commands.

Note: Before disabling Device HA, you should turn off the passive Zyxel Device or disconnect all network cables from it.

When you disable Device HA, you will see the following warning screen.

Figure 346 System > Device HA > HA Configuration (Disable)



30.4 DNS & DDNS

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.

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 265 DDNS Service Providers

PROVIDER	SERVICE TYPES SUPPORTED	WEBSITE
Cloudflare	Dynamic DNS, Static DNS, and Custom DNS	www.cloudflare.com
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
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.

30.4.1 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.

30.4.2 The DNS Screen

Click **System > DNS & DDNS > 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.

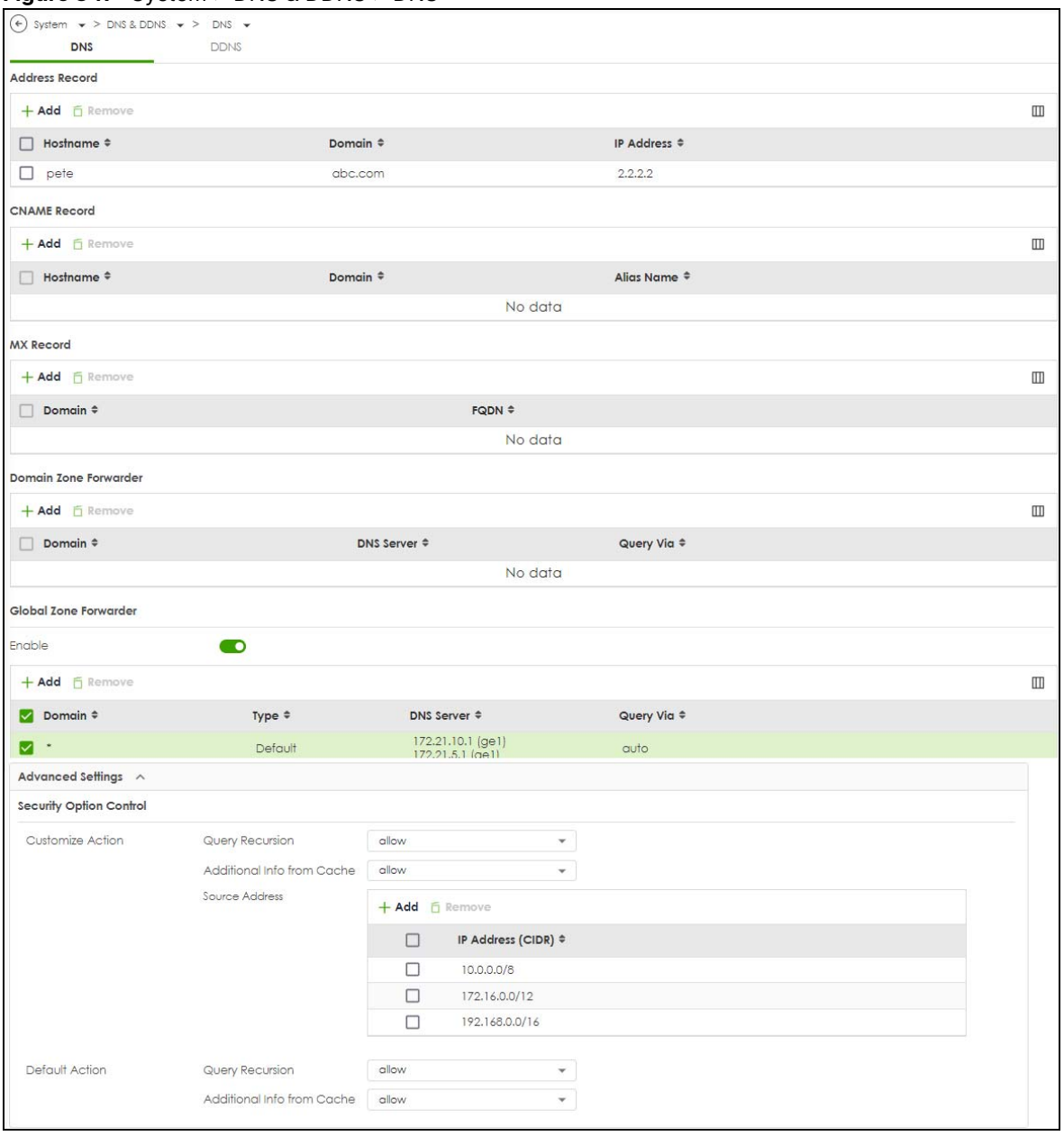
The Zyxel Device can ask a DNS server to use recursion to resolve its DNS client requests. If recursion on the Zyxel Device or a DNS server is disabled, they cannot forward DNS requests for resolution.

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 **System > DNS & DDNS > DNS** screen 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 347 System > DNS & DDNS > DNS



The following table describes the labels in this screen.

Table 266 System > DNS & DDNS > 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.
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.
Edit icon	Double-click an entry or select it to display an **Edit** icon that allows you to modify the entry’s settings.

Table 266 System > DNS & DDNS > DNS (continued)

LABEL	DESCRIPTION
Hostname	This is the name of the host.
Domain	This is the 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 30.4.5 on page 586) 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.
Hostname	This is the name of the host.
Domain	This is the host's fully qualified domain name.
Alias Name	This displays the alias name.
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.
Hostname	This is the name of the host.
Domain	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.
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.
Priority	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	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.

Table 266 System > DNS & DDNS > DNS (continued)

LABEL	DESCRIPTION
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.
Security Option Control	Click the arrow in the **Advanced Settings** field to display this part of the screen. There are two control policies: **Default Action** and **Customize Action**.
Query Recursion	This displays if the Zyxel Device is allowed or denied to forward DNS client requests to DNS servers for resolution.
Additional Info from Cache	This displays if the Zyxel Device is allowed or denied to cache Resource Records (RR) obtained from previous DNS queries.
Source 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**.

30.4.3 Address/PTR Record

An address record contains the mapping of a Fully-Qualified Domain Name (FQDN) to an IP address.

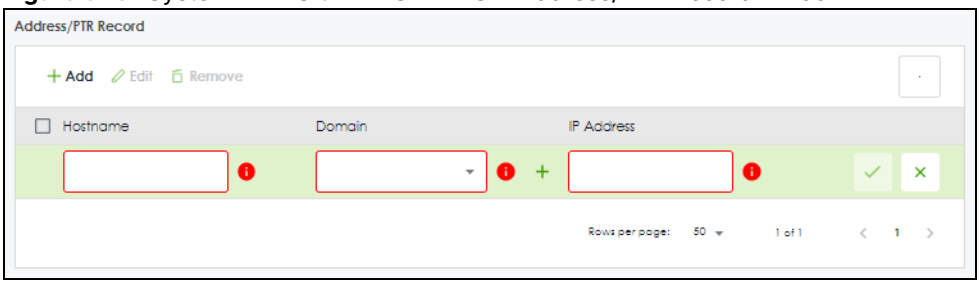
The Zyxel Device allows you to configure address records about the Zyxel Device itself or another device. This way you can keep a record of DNS names and addresses that people on your network may use frequently. If the Zyxel Device receives a DNS query for an FQDN for which the Zyxel Device has an address record, the Zyxel Device can send the IP address in a DNS response without having to query a DNS name server.

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.

30.4.4 Adding an Address/PTR Record

Click the **Add** icon in the **Address/PTR Record** table to add an IPv4 address/PTR record.

Figure 348 System > DNS & DDNS > DNS > Address/PTR Record > Add



The following table describes the labels in this screen.

Table 267 System > DNS & DDNS > DNS > Address/PTR Record > Add

LABEL	DESCRIPTION
Hostname	Enter the hostname of a server.
Domain	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).

Table 267 System > DNS & DDNS > DNS > Address/PTR Record > Add

LABEL	DESCRIPTION
IP Address	Enter the IP address of the host in dotted decimal notation.
Save changes	Click the Save changes icon to save your customized settings and exit this screen.
Cancel changes	Click the Cancel changes icon to exit this screen without saving.

30.4.5 CNAME Record

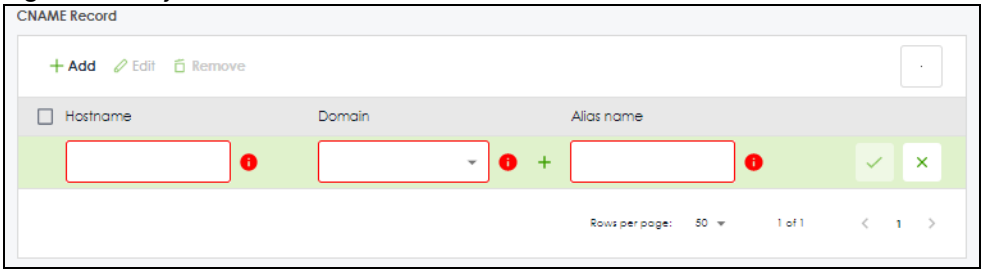
A Canonical Name Record or CNAME record is a type of resource record in the Domain Name System (DNS) that specifies that the domain name is an alias of another, canonical domain name. This allows users to set up a record for a domain name which translates to an IP address, in other words, the domain 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.

30.4.6 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 349 System > DNS & DDNS > DNS > CNAME Record > Add



The following table describes the labels in this screen.

Table 268 System > DNS & DDNS > DNS > CNAME Record > Add

LABEL	DESCRIPTION
Hostname	Enter the hostname of a server.
Domain	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).
Alias name	Enter an Alias Name. Use "*." as a prefix in the Alias name for a wildcard domain name (for example, *.example.com).

Table 268 System > DNS & DDNS > DNS > CNAME Record > Add

LABEL	DESCRIPTION
Save changes	Click the Save changes icon to save your customized settings and exit this screen.
Cancel changes	Click the Cancel changes icon to exit this screen without saving.

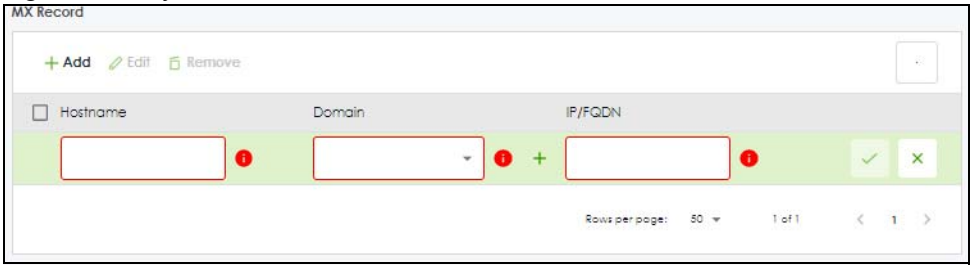
30.4.7 MX Record

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.

30.4.8 Adding a MX Record

Click the **Add** icon in the **MX Record** table to add a MX record.

Figure 350 System > DNS & DDNS > DNS > MX Record > Add



The following table describes the labels in this screen.

Table 269 System > DNS & DDNS > MX Record > Add

LABEL	DESCRIPTION
Hostname	Enter the hostname of a server.
Domain	Enter the domain name where the mail is destined for.
IP/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.
Save changes	Click the Save changes icon to save your customized settings and exit this screen.
Cancel changes	Click the Cancel changes icon to exit this screen without saving.

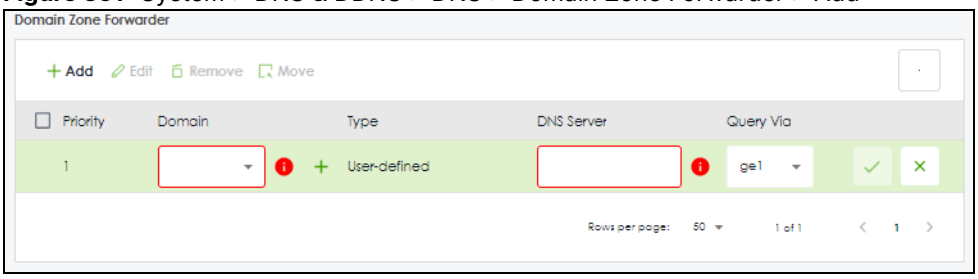
30.4.9 Domain Zone Forwarder

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.

30.4.10 Adding a Domain Zone Forwarder

Click the **Add** icon in the **Domain Zone Forwarder** table to add a domain zone forwarder record.

Figure 351 System > DNS & DDNS > DNS > Domain Zone Forwarder > Add



The following table describes the labels in this screen.

Table 270 System > DNS & DDNS > DNS > Domain Zone Forwarder > Add

LABEL	DESCRIPTION
Domain	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).
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	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. 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.
Query Via	Use the **Query Via** field to select the interface through which the Zyxel Device sends DNS queries to a DNS server.
Save changes	Click the Save changes icon to save your customized settings and exit this screen.
Cancel changes	Click the Cancel changes icon to exit this screen without saving.

30.4.11 Security Option Control

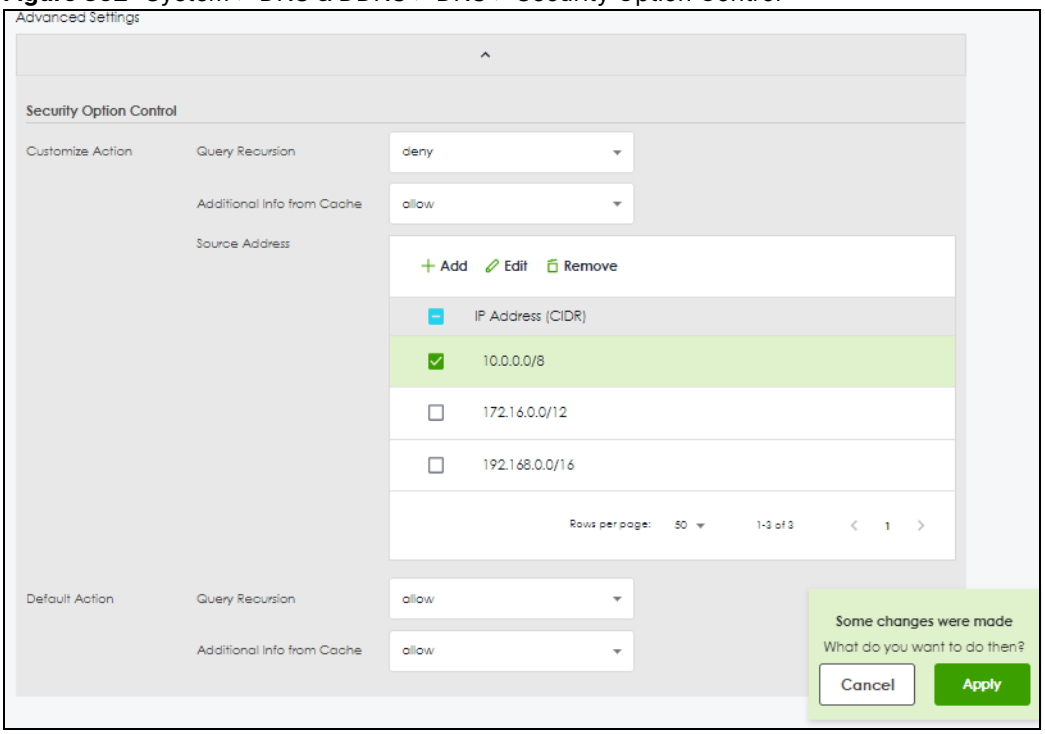
Configure the **Security Option Control** section in the **System > DNS & DDNS > DNS** screen if you suspect the Zyxel Device is being used by hackers in a DNS amplification attack.

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.

30.4.12 Editing a Security Option Control

Use this screen to change **allow** or **deny** actions for **Query Recursion** and **Additional Info from Cache**.

Figure 352 System > DNS & DDNS > DNS > Security Option Control



The following table describes the labels in this screen.

Table 271 System > DNS & DDNS > DNS > Security Option Control

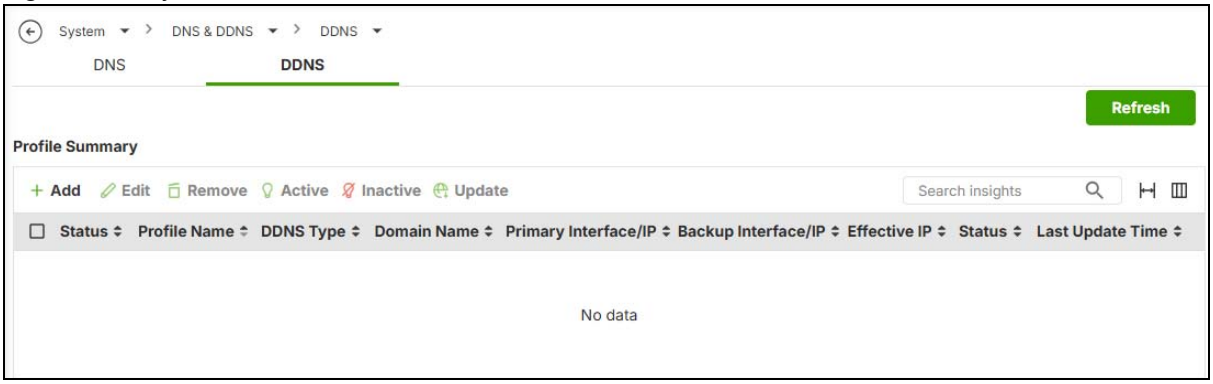
LABEL	DESCRIPTION
Query Recursion	Choose if the Zyxel Device is allowed or denied to forward DNS client requests to DNS servers for resolution. This can apply to specific open DNS servers using the address objects in a customized rule.
Additional Info from Cache	Choose if the Zyxel Device is allowed or denied to cache Resource Records (RR) obtained from previous DNS queries.
Source Address	This field displays address objects created in **Object > Address**. Select one or more address object(s) to have it (them) to 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.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

30.4.13 The DDNS Screen

The Zyxel Device provides DDNS (Dynamic DNS) services that can map a fixed domain name to a dynamic IP address. The DDNS service provider stores the DNS record for the domain name, and updates the associated IP address if it changes.

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 **System > DNS & DDNS > DDNS** to open the following screen.

Figure 353 System > DNS & DDNS > DDNS



The following table describes the labels in this screen.

Table 272 System > DNS & DDNS > 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**.
Update	To refresh information for an entry, select it and click **Update**.
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 the domain name for which the DDNS service provider stores a DNS record.
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.
Effective IP	This is the IP address currently associated with the domain name.

Table 272 System > DNS & DDNS > DDNS (continued)

LABEL	DESCRIPTION
Status	This displays the current state of the Zyxel Device to DDNS service provider connection. Example states are as follows: • **Success**: The IP address for the domain name was successfully resolved with the DDNS service provider. • **Updating**: The Zyxel Device is currently sending an update request. • **Failed**: The update request to the DDNS provider failed. • **Disabled**: The DDNS profile is not active.
Last Update Time	This displays the date and time the Effective IP address was last updated for this domain name.
Apply	Click this button to save your changes to the Zyxel Device.
Cancel	Click this button to return the screen to its last-saved settings.

30.4.14 The DDNS 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.

The fields available vary depending on the DDNS provider you choose. The following tables show the required fields for each type.

A check mark denotes that this attribute is required. For example, in the below table, **Cloudflare** requires a domain name, zone ID and an API token, but not HTTPS, a username nor password.

Table 273 Required General Settings and DDNS Account Settings for Each DDNS Provider Type

DDNS TYPE	HTTPS	USERNAME	PASSWORD	DOMAIN NAME	ZONE ID	API TOKEN
Cloudflare				✓	✓	✓
Dyndns Static	✓	✓	✓	✓		
Dyndns Custom	✓	✓	✓	✓		
Dynu Basic	✓		✓	✓		
Dynu Premium			✓	✓		
No-IP	✓	✓	✓	✓		
Selfhost	✓	✓	✓	✓		
User-custom	✓	✓	✓	✓		

These are the required **Interface** and **IP Address Settings**. In the below table, **Cloudflare** must have an **Interface** settings.

Table 274 Required Interface and IP Address Settings for Each DDNS Provider Type

DDNS TYPE	INTERFACE	INTERFACE	INTERFACE	IP	IP	IP	IP
DDNS Type	Interface object	any	none	auto	interface	custom	public
Cloudflare	✓	✓			✓	✓	✓
Dyndns Static	✓	✓	✓	✓	✓	✓	✓
Dyndns Custom	✓	✓	✓	✓	✓	✓	✓
Dynu Basic	✓	✓	✓		✓	✓	✓
Dynu Premium	✓	✓	✓		✓	✓	✓
No-IP	✓	✓	✓		✓	✓	✓
Selfhost	✓	✓	✓	✓	✓	✓	✓
User-custom	✓	✓	✓	✓			✓

Only **Dyndns Static** and **Dyndns Custom** support **Advanced Settings**.

Table 275 Required Advanced Settings for Each DDNS Provider Type

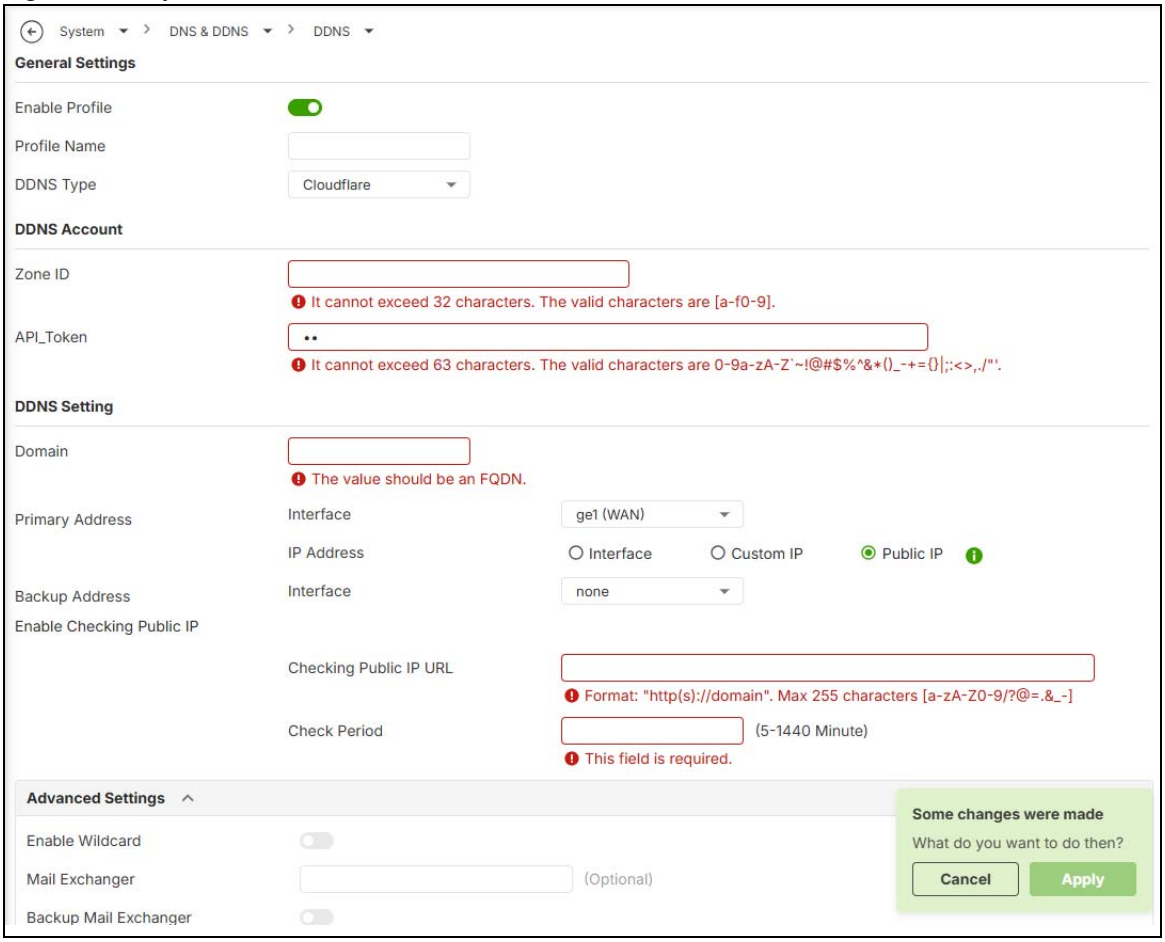
DDNS TYPE	WILDCARD	MX	BACKUP MX
Cloudflare			
Dyndns Static	✓	✓	✓
Dyndns Custom	✓	✓	✓
Dynu Basic			
Dynu Premium			
No-IP			
Selfhost			
User-custom			

Using DDNS with a connection exposes services to the Internet. These are some best practices:

- Use strong passwords
- Enable HTTPS
- Use VPN when possible
- Keep software updated
- Avoid exposing unnecessary ports

Click **System > DNS & DDNS > DDNS** and then an **Add** or **Edit** icon to open this screen.

Figure 354 System > DNS & DDNS > DDNS > Add/Edit



The following table describes the labels in this screen.

Table 276 System > DNS & DDNS > DDNS > Add/Edit

LABEL	DESCRIPTION
Enable Profile	Slide the switch to the right 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 [0-9][a-z][A-Z, underscores [_], or dashes [-], but the first character must be a letter. This value is case-sensitive. This field is read-only when you are editing an entry.

Table 276 System > DNS & DDNS > DDNS > Add/Edit (continued)

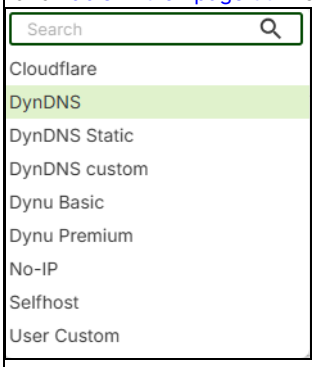
LABEL	DESCRIPTION
DDNS Type	Select the DDNS service provider you are using. Required fields in this screen vary depending on the provider you choose. See Table 273 on page 591, Table 274 on page 592 and Table 275 on page 592 for details.  Select **User custom** to create your own DDNS service and configure the DDNS Server **URL Hostname**, **URL Path**, and **Additional DDNS Options** fields below.
HTTPS	Enable 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.
DDNS Account	
Username	Type the user name used when you registered your domain name with the DDNS service provider. You can use up to 31 alphanumeric characters and (:_.-@), but the first character must be a letter.. 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.
Password	Type the password associated with the username for your DDNS provider account. You can use 1-63 characters. Valid characters are [0-9][a-z][A-Z][_(){}<>^`+/:!*#@&=$'\.~%,|;-"]. Spaces are not allowed. Your password will be encrypted when you configure this field.
Retype to Confirm	Type the password again exactly as you typed it above.
Zone ID	This field is available for Cloudflare DDNS. For Cloudflare DDNS, the **Zone ID** is the unique identifier for your domain name inside Cloudflare. The Zyxel Device uses the **Zone ID** to tell Cloudflare which domain name DNS records to update. The **Zone ID** is a long unique string assigned by Cloudflare, such as 8f4e1234567890abcdef1234567890ab. To find the **Zone ID** in Cloudflare (at the time of writing), log into the Cloudflare **Dashboard**, and select your domain name. In **Overview**, you will see the **Zone ID**. Copy it, then enter it here.
API_Token	This field is available for Cloudflare DDNS. The Zyxel Device uses the API token to log into Cloudflare to automatically update a DNS record in Cloudflare when the associated IP address for the domain name changes. After you sign up to Cloudflare DDNS, you generate an API token in the Cloudflare **Dashboard**. In Cloudflare, click your profile icon, then go to **Profile > API Tokens** and click **Create Token**. (See the Cloudflare documentation for the latest paths.) The Cloudflare API token does not expire by default unless you set an expiration date when creating it. If you lose the token, you must create a new token, and then update the Zyxel Device with the new token. If the token becomes invalid, DNS updates stop, so your existing DNS record remains unchanged, and remote access will stop if your ISP-assigned IP address changes.
DDNS Settings	
Domain	This is the domain name that maps to the dynamic IP address. Type the domain name you registered with the DDNS provider. You can use up to 255 characters.

Table 276 System > DNS & DDNS > DDNS > Add/Edit (continued)

LABEL	DESCRIPTION
Primary 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 DNS records. The Zyxel Device uses the **Backup Address** if the interface specified by these settings is not available.
Interface	Select the network interface the Zyxel Device should monitor for updating the IP address mapped to the domain name. For example, it could be WAN1 or WAN2. The IP Address for Cloudflare can be **Interface**, **Custom IP** or **Public IP** – it cannot be **None**. See Table 274 on page 592 for details. For other DDNS service providers, **Any** lets 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 correct IP address if there is an HTTP proxy server between the Zyxel Device and the DDNS server. **Custom IP** - 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. Type the IP address in the **user defined** field or you can select an address object to use for the domain name. **Public IP** - Select this if your Zyxel Device is behind a NAT router, and the NAT router has a public WAN IP address. The DDNS provider will use the public WAN IP address of the NAT router for domain name mapping of the Zyxel Device.
Backup Address	Use these fields to set an alternate interface to map the domain name to when the interface specified by the **Primary 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 IP** - 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. Type the IP address in the **user defined** field or you can select an address object to use for the domain name. **Public IP** - Select this if your Zyxel Device is behind a NAT router, and the NAT router has a public WAN IP address. The DDNS provider will use the public WAN IP address of the NAT router for domain name mapping of the Zyxel Device.
Enable Checking Public IP	
Checking Public IP URL	Type the URL the Zyxel Device uses to check its public WAN IP address for DDNS updates. Use “http://” or “https://” followed by up to 255 characters (a-zA-Z0-9/?@=.&_-). This field is only available when the IP Address is **Public IP**.
Check Period	Type the number of minutes between URL check attempts. Enter a number between 5 and 1440. This field is only available when the IP Address is **Public IP**.

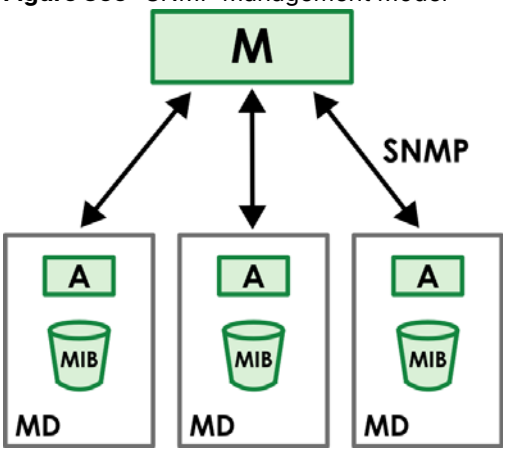
Table 276 System > DNS & DDNS > DDNS > Add/Edit (continued)

LABEL	DESCRIPTION
URL Hostname	This field is only available when the **DDNS Type** is **User Custom**. Type the FQDN of the server that will host the DDSN service.
URL Path	This field is only available when the **DDNS Type** is **User Custom**. Type the URL that can be used to access the server that will host the DDSN service.
Additional DDNS Options	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/
Advanced Settings	Click the arrow in the **Advanced Settings** field to show the following options.
Enable Wildcard	Enable the wildcard feature to alias subdomains to be aliased to the same IP address as your (dynamic) domain name. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.
Mail Exchanger	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	Select this check box 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.
Apply	Click this button to save your changes to the Zyxel Device.
Cancel	Click this button to return the screen to its last-saved settings.

30.5 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 two (SNMPv2c) and version 3 (SNMPv3). The next figure illustrates an SNMP management operation.

Figure 355 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the 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. 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.

30.5.1 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.

30.5.2 Supported MIBs

The Zyxel Device supports MIB II that is defined in RFC-1213 and RFC-1215. The Zyxel Device also supports private MIBs (zywall.mib and zyxel-zywall-ZLD-Common.mib) 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.

30.5.3 SNMP Traps

The Zyxel Device will send traps to the SNMP manager when any one of the following events occurs.

Table 277 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.

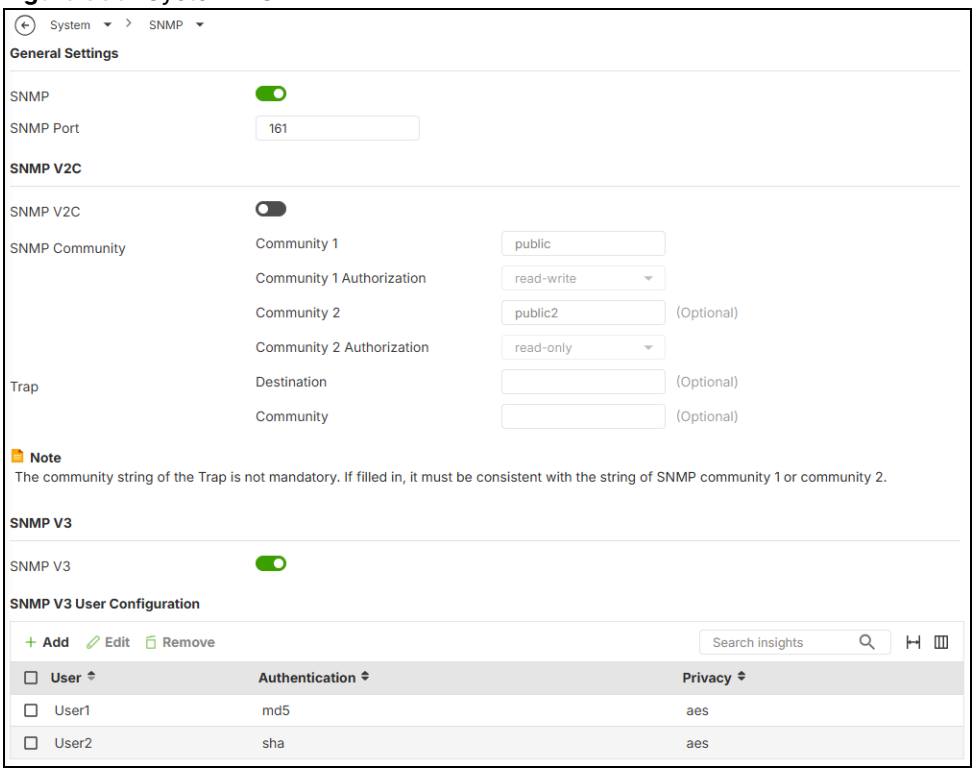
Table 277 SNMP Traps (continued)

OBJECT LABEL	OBJECT ID	DESCRIPTION
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.

30.5.4 Configuring SNMP

To change your Zyxel Device's SNMP settings, click **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 356 System > SNMP



The following table describes the labels in this screen.

Table 278 System > SNMP

LABEL	DESCRIPTION
SNMP	Enable this to allow to access the Zyxel Device using this service.
SNMP Port	The SSH port is 161 by default. 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.
SNMP V2C	SNMPv2c provides enhanced performance, improved error handling, and support for bulk data retrieval, using community-based security for network management Click the switch to the right to enable the SNMP V2C for the Zyxel Device. The SNMP version on the Zyxel Device must match the version on the SNMP manager.
SNMP Community	
Community 1/2	Enter the community, which is the password for the incoming Get or Set requests from the management station. You can use up to 64 single-byte characters, including 0-9a-zA-Z_.-. The first character cannot be a period (.).
Community 1/2 Authorization	Select the access rights to the community. • **read-write**: A read-write community string enables users to both retrieve and modify device data, allowing for comprehensive network management and configuration. • **read-only**: A read-only community string allows the retrieval of device data for monitoring but prevents any configuration changes.
Trap	
Destination	Type the IP address of the station to send your SNMP traps to.
Community	A Trap community in SNMP is a string used to define the group or community to which an SNMP agent sends trap messages (alerts). It acts as a password-like identifier, ensuring that trap notifications are sent to authorized network management systems (NMS) that belong to the specified community. The community string of the Trap is not mandatory. If filled in, it must be consistent with the string of SNMP community 1 or community 2.
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.
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.

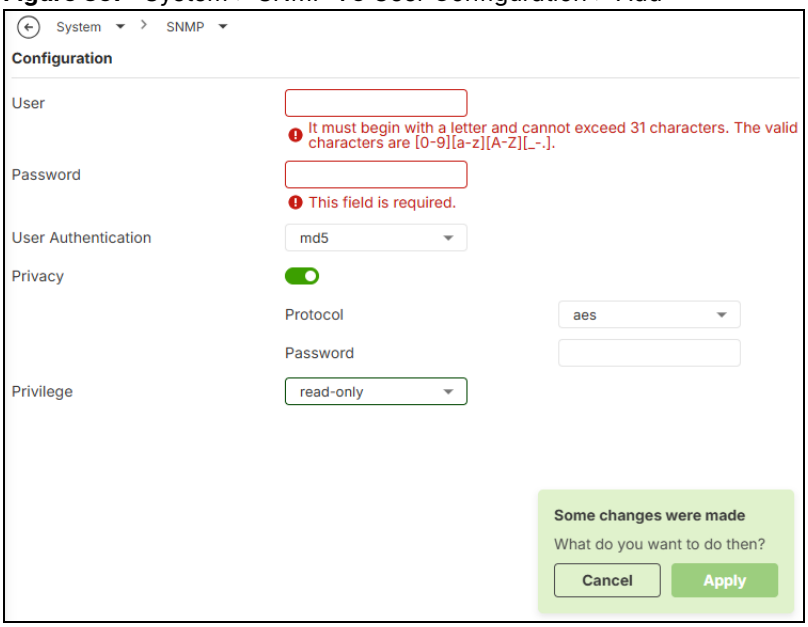
Table 278 System > SNMP (continued)

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

30.5.5 Add SNMP V3 User

Click **Add** under **SNMP V3 User Configuration** in **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 357 System > SNMP V3 User Configuration > Add



The following table describes the labels in this screen.

Table 279 System > SNMPV3 User Configuration > 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. It must begin with a letter and cannot exceed 31 characters. The valid characters are [0-9][a-z][A-Z][_-.].
Password	Enters a password consists of eight characters. Your login password must consist of at least 8 printable characters for SNMPv3.
User 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.

Table 279 System > SNMPV3 User Configuration > Add (continued)

LABEL	DESCRIPTION
Privacy	Click the switch to the right to enable the specified encryption method. 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.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

30.6 Notification

Use these screens to configure the mail server settings and alert settings.

30.6.1 The Mail Server Screen

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 **Log & Report > Email Daily Report** to configure what reports to send and to whom.

Click **System > Notification > Mail Server** to display the following screen.

Figure 358 System > Notification > Mail Server (Without Authentication)

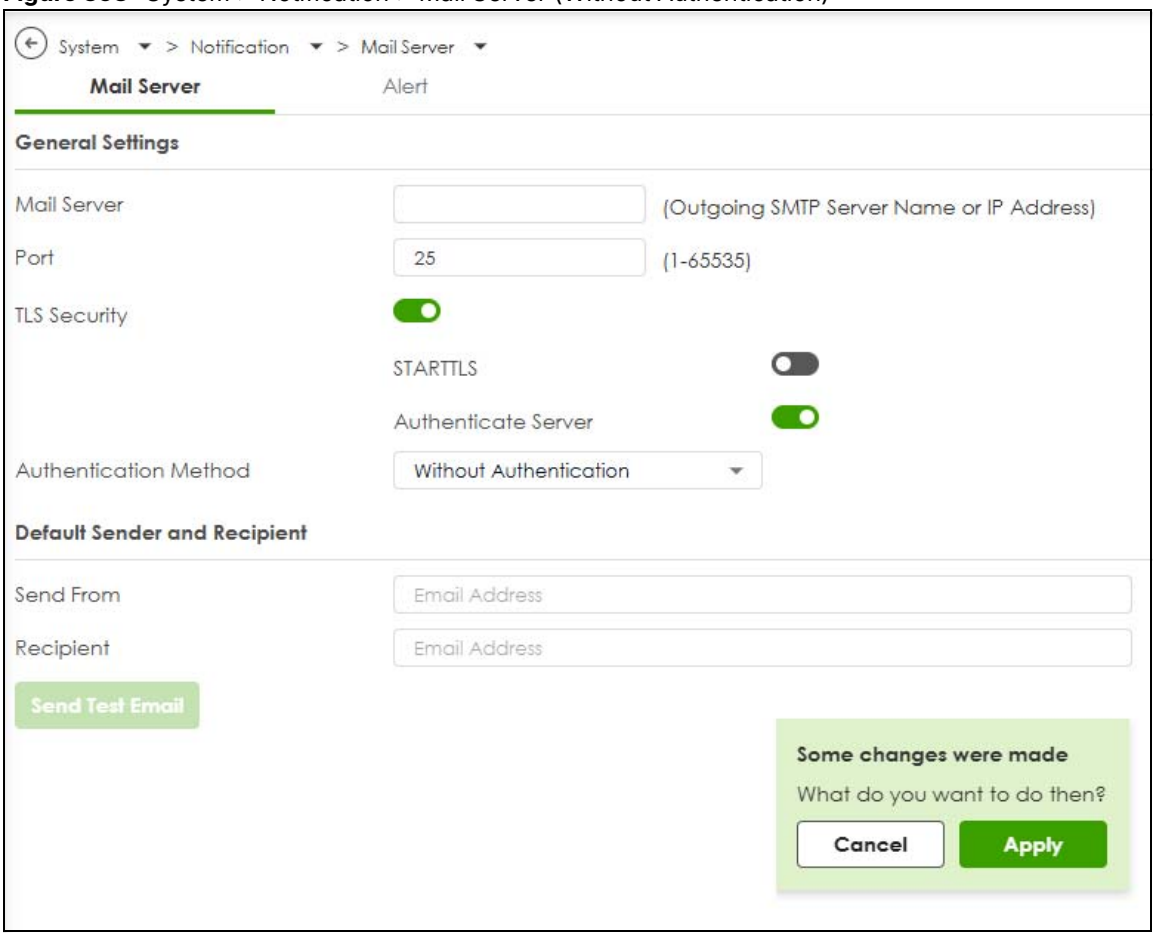


Figure 359 System > Notification > Mail Server (Basic Authentication)

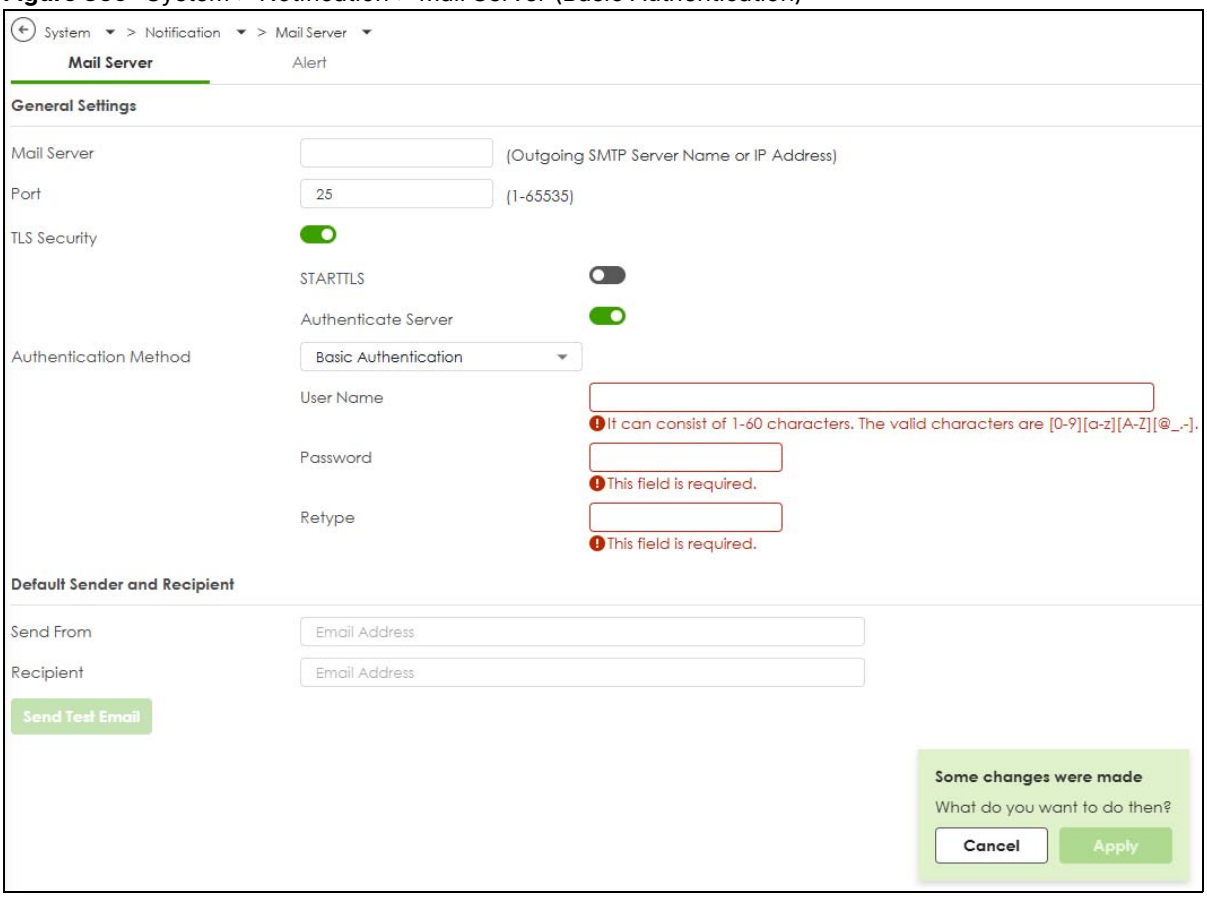
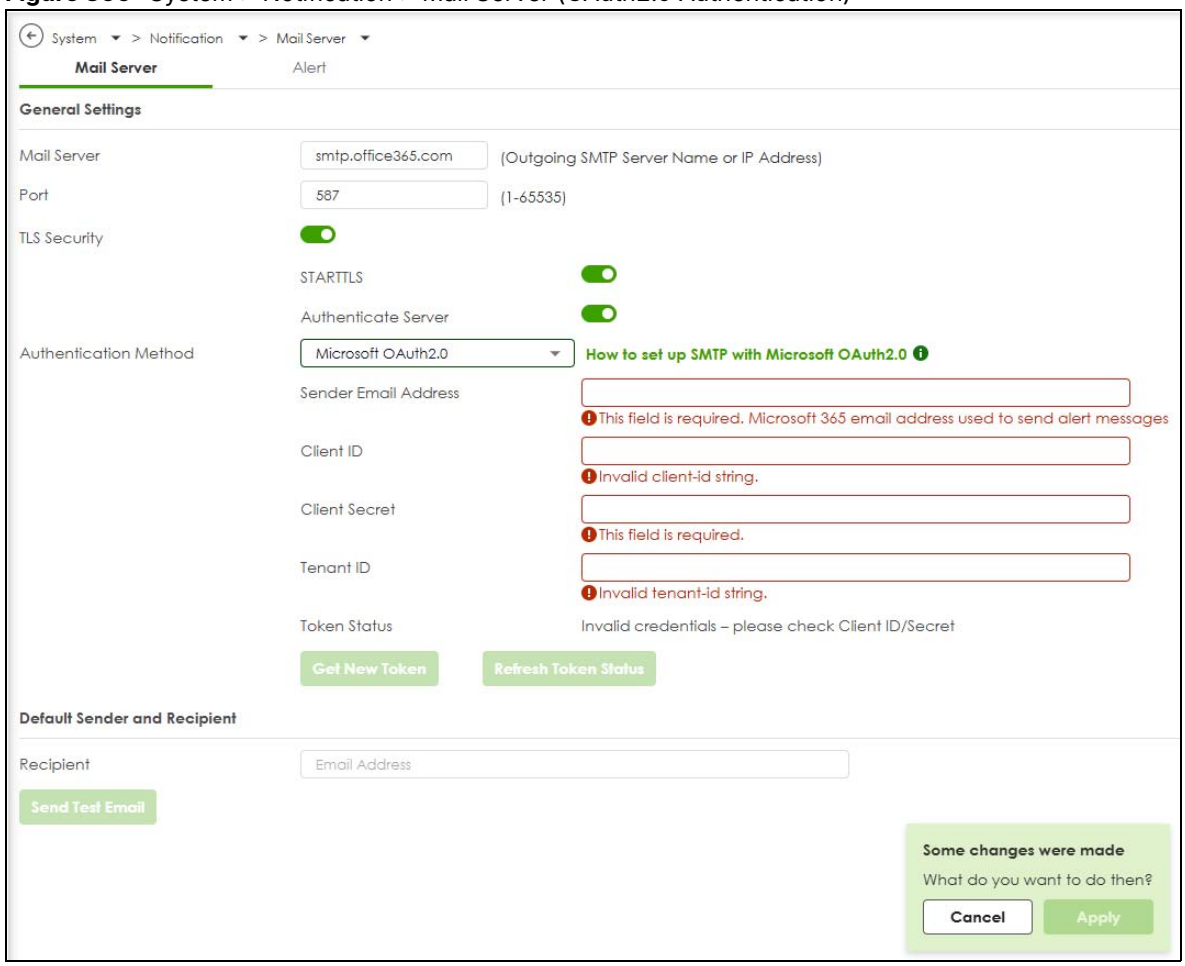


Figure 360 System > Notification > Mail Server (OAuth2.0 Authentication)



The following table describes the labels in this screen.

Table 280 System > Notification > Mail Server

LABEL	DESCRIPTION
Mail Server	Type the name or IP address of the outgoing SMTP server.
Port	Enter the same port number here as is on the mail server for mail traffic.
TLS Security	Enable this if the mail server uses Transport Layer Security (TLS) for encrypted communications between the mail server and the Zyxel Device.
STARTTLS	Enable this if the mail server uses SSL or TLS for encrypted communications between the mail server and the Zyxel Device.
Authenticate Server	Enable this if the Zyxel Device authenticates the mail server in the TLS handshake.
Authentication Method	Select how to authenticate with the SMTP mail server. • **Without Authentication**: select this if the SMTP mail server used for the sender email does not require login credentials. • **Basic**: select this if the SMTP mail server used for the sender email requires username and password login credentials. • **Microsoft OAuth2.0**: select this if the SMTP mail server used for the sender email uses a Microsoft 365 email address. The Microsoft 365 application is built into Microsoft Azure, a cloud computing platform, that uses Microsoft products locally and in the cloud.
User Name	This is required when you select **Basic** authentication. Type the user name to provide to the SMTP server when the log is emailed. Use up to 30 characters, including 0-9a-zA-Z@._-

Table 280 System > Notification > Mail Server (continued)

LABEL	DESCRIPTION
Password	This is required when you select **Basic** authentication. Type a password to provide to the SMTP server when the log is emailed. Use 4 to 63 characters, including 0-9a-zA-Z'~!@#$%^&*()_+={}|\;:"<>'./
Retype	Type the password again to make sure that you have entered it correctly.
Sender Email Address	This is required when you select **Microsoft OAuth2.0** authentication.
Client ID	This is required when you select **Microsoft OAuth2.0** authentication. **Client ID**, **Client Secret** and **Tenant ID** are credentials for your registered Azure application. When you register your application in Azure, it will generate a unique **Client ID** to uniquely identify your application. To see your **Client ID** (at the time of writing), go to the Azure portal, and locate your application in the **App registrations** overview page.
Client Secret	This is required when you select **Microsoft OAuth2.0** authentication. When you register your application in Azure, you need to create a **Client Secret** to authenticate with Azure when obtaining access tokens. The **Client Secret** value is displayed only once during creation, so make sure to store it securely.
Tenant ID	This is required when you select **Microsoft OAuth2.0** authentication. This identifies your specific Azure Active Directory (Azure AD) instance (directory ID). To see it (at the time of writing), go to the Azure Active Directory, and select **Properties**.
Token Status	This is required when you select **Microsoft OAuth2.0** authentication. **Token Status** refers to the validity and state of access tokens used for authentication and authorization in Azure. These tokens have specific lifespans and properties that determine how long they can be used and for what. You may need to **Refresh Token Status** or reenter **Client ID** and **Client Secret** to **Get New Token.** • If your token has expired, click **Refresh Token** or **Get New Token**. • If refreshing a token fails, click **Get New Token.** • If there is no token available, click **Get New Token**. • If you see a "Invalid credentials" message, check your **Client ID** and **Client Secret.**
Default Sender and Recipient	
Send From	This field is not available when you select **Microsoft OAuth2.0** authentication. Type the default email address to which the outgoing email is delivered. The value should be an email address. It can be up to 83 characters. The valid characters are [a-z][A-Z][/=?^_.{|}~w-!#$%*+]. The entry will be automatically filled into other sender fields in the Web Configurator and cannot be edited: • The **Email From** field in the **Log & Report** > **Email Daily Report**. • The **Send From** field in **System** > **Notification** > **Alert** > **Event Notification/Log Alert.**
Recipient	Enter the email address of the recipient to whom the outgoing email is sent. This is the address that will receive the email. It can be up to 83 characters. The valid characters are [a-z][A-Z][/=?^_.{|}~w-!#$%*+]. The entry will be automatically filled into other recipient fields in the Web Configurator and can be edited: • The **Recipients** field in **Log & Report** > **Email Daily Report.** • The **Recipients** field in **System** > **Notification** > **Alert** > **Event Notification/Log Alert**. • The **Recipients** field in **Maintenance** > **Firmware/File Manager** > **Configuration File.**
Send Test Email	Click this button to send an email to the default mail to recipient to test if the email can be successfully received.

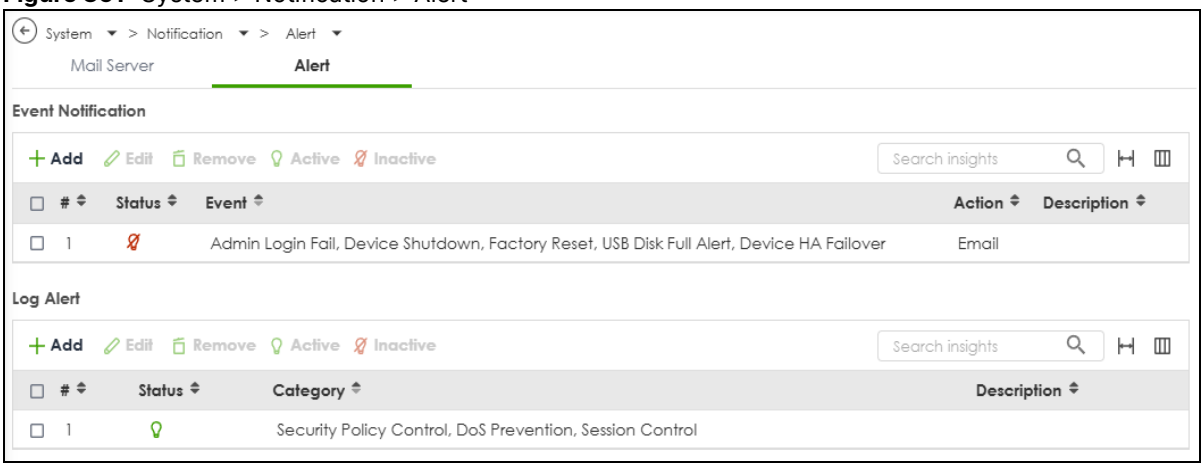
Table 280 System > Notification > Mail Server (continued)

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

30.6.2 The Alert Screen

Click **System** > **Notification** > **Alert** to display the following screen.

Figure 361 System > Notification > Alert



The following table describes the labels in this screen.

Table 281 System > Notification > Alert

LABEL	DESCRIPTION
Event Notification	
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 if you want to remove it before doing so.
Active	To turn on an entry, select it and click **Activate**.
Inactive	To turn off an entry, select it and click **Inactivate**.
#	This field is a sequential value and is not associated with any entry.
Status	This field displays the current status of each profile.
Event	This field displays the type(s) of event to create a log or send an email notification.
Action	This field displays the action to take when specified type(s) of events occur: • **Email**: Create a log and send an email notification. • **Log**: Create a log.
Description	This field displays the profile's description.
Log Alert	
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.

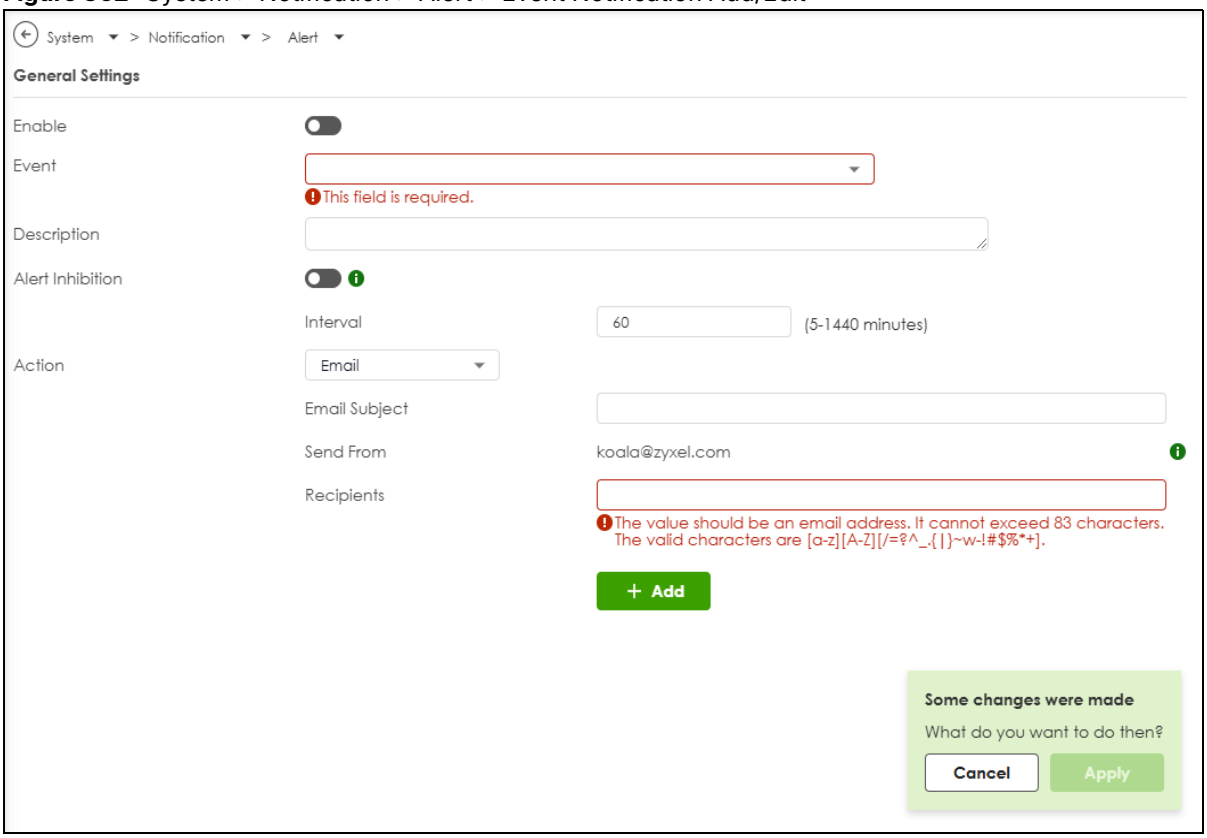
Table 281 System > Notification > Alert (continued)

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms if you want to remove it before doing so.
Active	To turn on an entry, select it and click **Activate**.
Inactive	To turn off an entry, select it and click **Inactivate**.
#	This field is a sequential value and is not associated with any entry.
Status	This field displays the current status of each profile.
Category	This field displays the type(s) of log to send an email notification.
Description	This field displays the profile's description.

30.6.2.1 The Event Notification Add/Edit Screen

Click **System** > **Notification** > **Alert** > **Event Notification Add/Edit** to display the following screen.

Figure 362 System > Notification > Alert > Event Notification Add/Edit



The following table describes the labels in this screen.

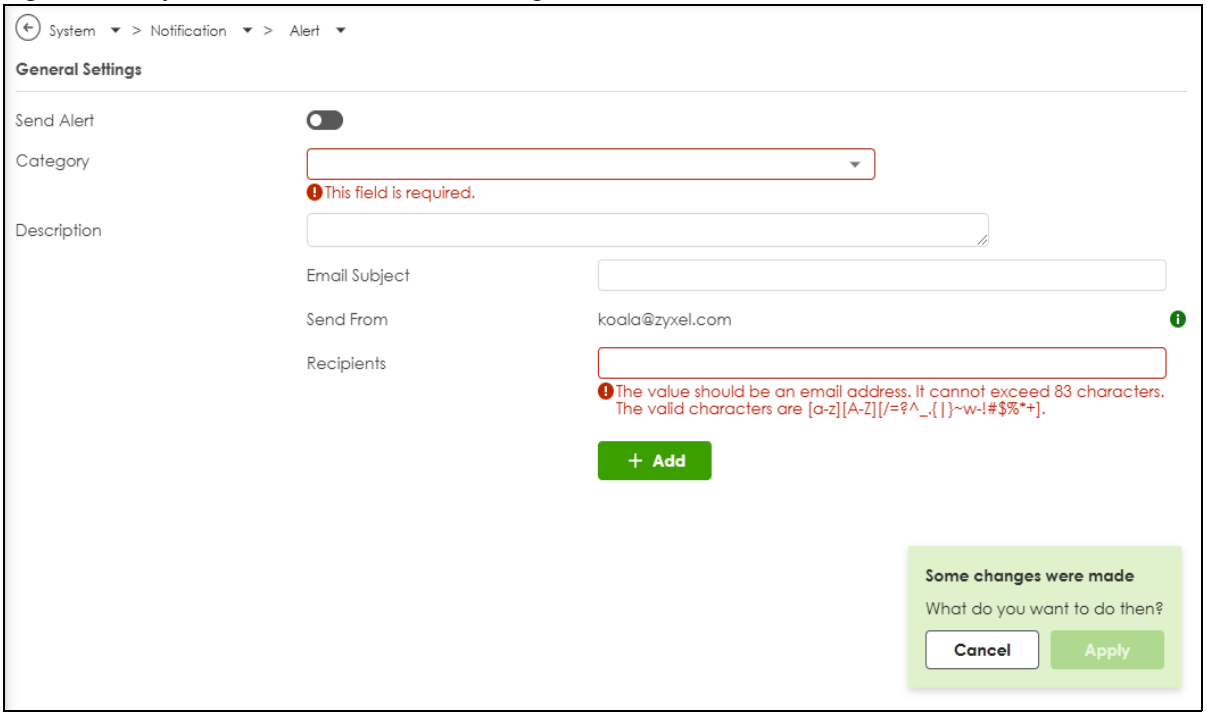
Table 282 System > Notification > Alert > Event Notification Add/Edit

LABEL	DESCRIPTION
Enable	Enable this to create a log or send an email notification when the specified type(s) of event occur.
Event	Select the type(s) of event to create a log or send an email notification when that event(s) occurs. • Select All • Admin Login • Admin Login Fail • CPU usage over Threshold • Device HA Failover • Device Reboot • Device Shutdown • Factory Reset • Memory Usage over Threshold • New firmware Available • Physical Port Down • Physical Port Up • Storage Usage over Threshold • Temperature too high (CPU, Switch, Board) • USB Disk Full Alert • USB Disk Full Warning • User Lockout • User Login • User Login Fail
Description	Enter a description of this policy to identify it. You can use up to 512 single-byte characters, special characters and spaces are allowed.
Alert Inhibition	Enable this to temporarily stop receiving notifications for **CPU Usage over Threshold**, **Memory Usage over Threshold**, **Temperature too high (CPU, Switch, Board)**, **USB Disk Full Alert**, **USB Disk Full Warning**, and **Storage Usage over Threshold**. Other event types will not be affected.
Interval	Specify how long to stop receiving the above notifications. The range is from 5 to 1440 minutes. The default is 60 minutes.
Action	Select the action to take when specified type(s) of event occur: • **Email:** Create a log and send an email notification when the selected type(s) of event occur. • **Log:** Create a log when the selected type(s) of event occur.
Email Subject	Enter the subject line for the outgoing email with 1-128 characters. It may consist of letters, numbers, and the following special characters: '()+,./:=?;!*#@$_%-. If you leave this field blank, the email subject will be the event name(s).
Send From	Enter the email address from which the outgoing email is delivered. This address is used in replies.
Recipients	Enter up to 83 characters for the email address of the receiver. It may consist of letters, numbers, and the following special characters: /=?^_.{|}~w-!#$%*+. You can enter up to five recipients.
Cancel	Click **Cancel** to return the screen to its last-saved settings.
Apply	Click **Apply** to save your settings to the Zyxel Device.

30.6.2.2 The Log Alert Add/Edit Screen

Click **System** > **Notification** > **Alert** > **Log Alert Add/Edit** to display the following screen.

Figure 363 System > Notification > Alert > Log Alert Add/Edit



The following table describes the labels in this screen.

Table 283 System > Notification > Alert > Log Alert Add/Edit

LABEL	DESCRIPTION
Send Alert	Enable this to send an email notification when the specified type(s) of log occur.
Category	Select the type(s) of log to send an email notification.
Description	Enter a description of this policy to identify it. You can use up to 512 single-byte characters, special characters and spaces are allowed.
Email Subject	Enter the subject line for the outgoing email with 1-128 characters. It may consist of letters, numbers, and the following special characters: '()+,./:=?;!*#@$_%-
Send From	Enter the email address from which the outgoing email is delivered. This address is used in replies.
Recipients	Enter up to 83 characters for the email address of the receiver. It may consist of letters, numbers, and the following special characters: /=?^_.{|}~w-!#$%*+. You can enter up to five recipients.
Cancel	Click **Cancel** to return the screen to its last-saved settings.
Apply	Click **Apply** to save your settings to the Zyxel Device.

30.7 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.

30.7.1 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.

30.7.2 Verifying a Certificate

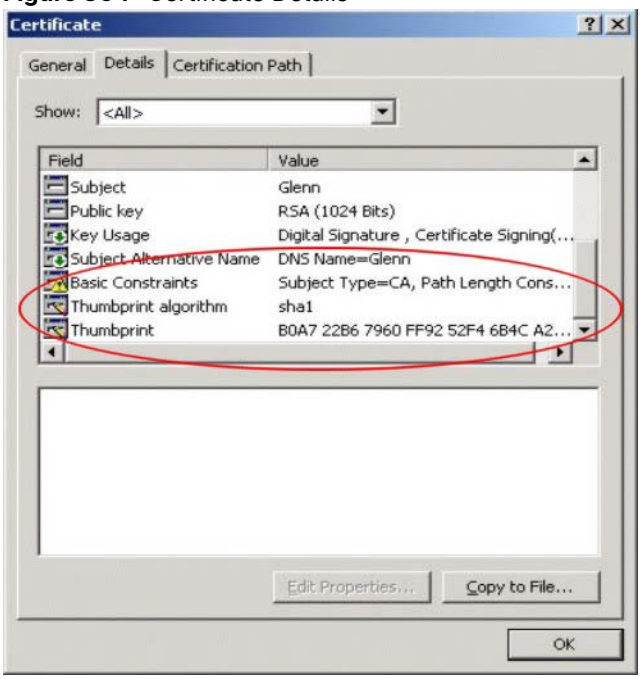
Before you import a trusted certificate into the Zyxel Device, you should verify that you have the correct certificate. You can do this using the certificate's fingerprint. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithm. The following procedure describes how 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.

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 364 Certificate Details

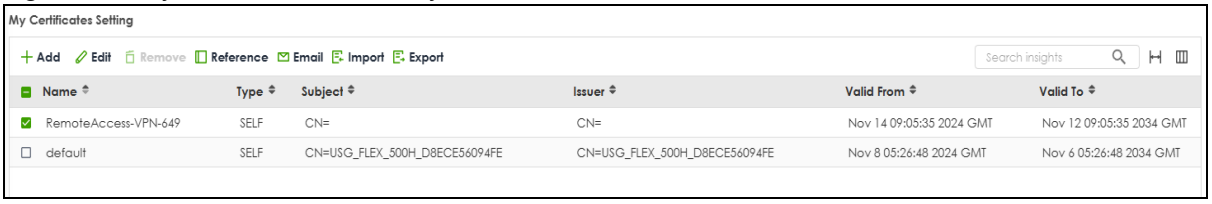


4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may very based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

30.8 My Certificates

Click **System > Certificate > My Certificates** to open the **My Certificates** screen. This is the Zyxel Device's summary list of certificates and certification requests.

Figure 365 System > Certificate > My Certificates



The following table describes the labels in this screen.

Table 284 System > Certificate > My Certificates

LABEL	DESCRIPTION
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.

Table 284 System > Certificate > My Certificates (continued)

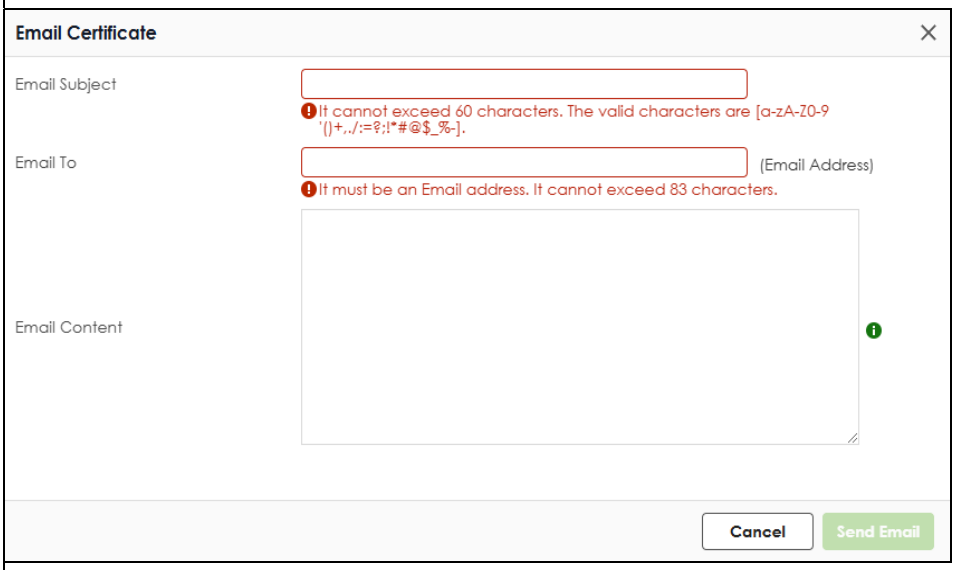
LABEL	DESCRIPTION
Reference	Select an entry and click **Reference** to check which settings use the entry.
Email	Click this to email the selected certificate to the configured email address(es) for SSL or site to site VPN connection establishment. This enables you to establish an connection on your laptops, tablets, or smartphones. Click this and the following screen will appear. Here are the field descriptions: • **Email Subject**: Type the subject line for outgoing email from the Zyxel Device. Enter a email subject text of 1-60 characters. It may consist of letters, numbers, and the following special characters: '()+,./:=?;!*#@$%- • **Email To:** Type the email address to which the outgoing email is delivered using up to 83 characters. • **Email Content:** Create the email content in English, and use up to 250 keyboard characters. The special characters listed in the brackets [0-9a-zA-Z!"#$%&'()*+,-./:;<=>@\[]^_'{}|] are allowed. • **Cancel:** Click this to return to the previous screen without saving your changes. • **Send Email:** Click this to send the selected certificate. 
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.
Export	Click this and the following screen will appear. Type the selected certificate's password and save the selected certificate to your computer. 
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.

Table 284 System > Certificate > My Certificates (continued)

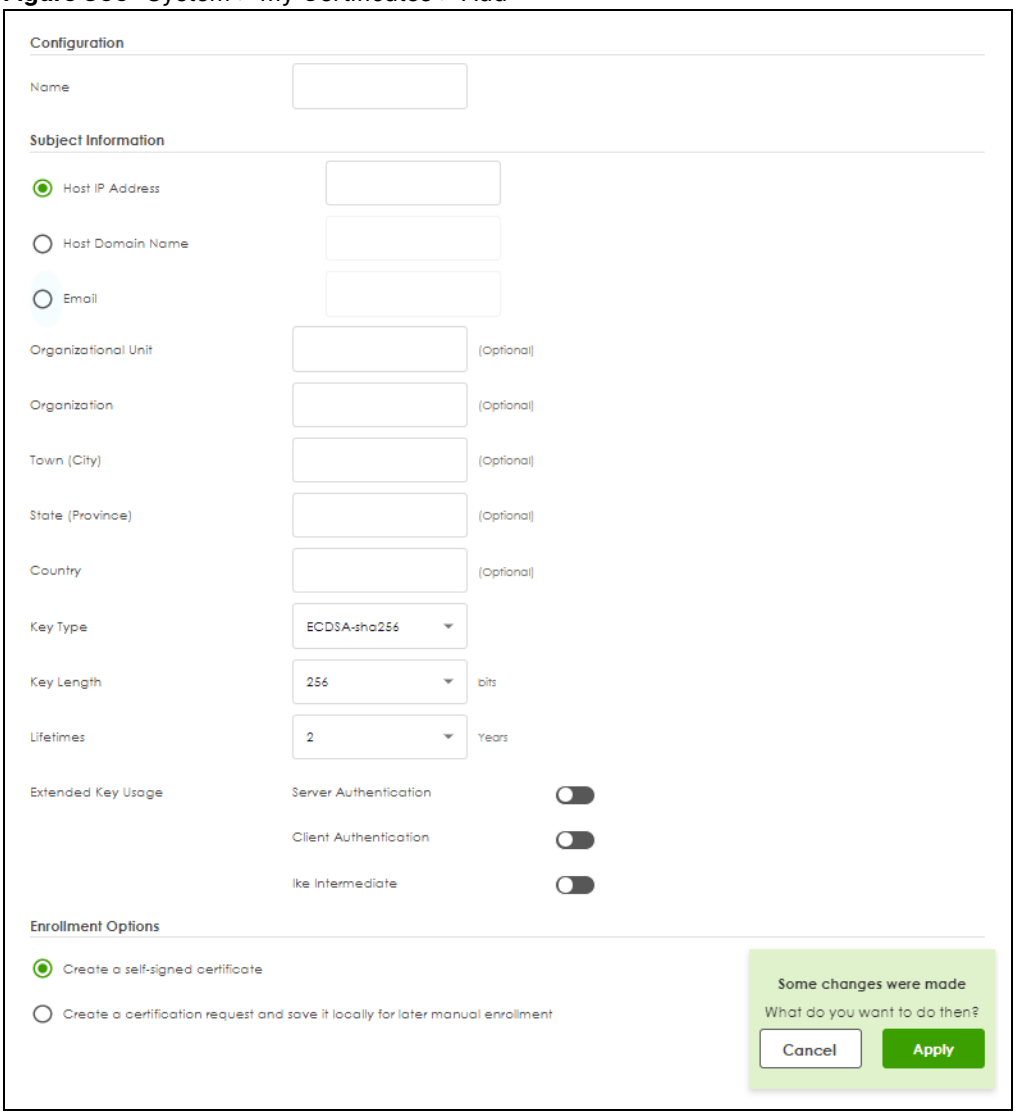
LABEL	DESCRIPTION
Type	This field displays what kind of certificate this is. **REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate Import** screen to import the 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.
Reference	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.

30.8.1 The My Certificates Add Screen

Click **System > My Certificates** and then the **Add** icon to open the following 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.

If you configured the **My Certificate > Add** screen to have the Zyxel Device enroll a certificate and the certificate enrollment is not successful, you will not see the certificate you configured in the **My Certificates** screen after you click **Apply.** 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.

Figure 366 System > My Certificates > Add



The following table describes the labels in this screen.

Table 285 System > 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 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 30 characters. You can use alphanumeric characters 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.
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 (256 to 384). 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 1 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.

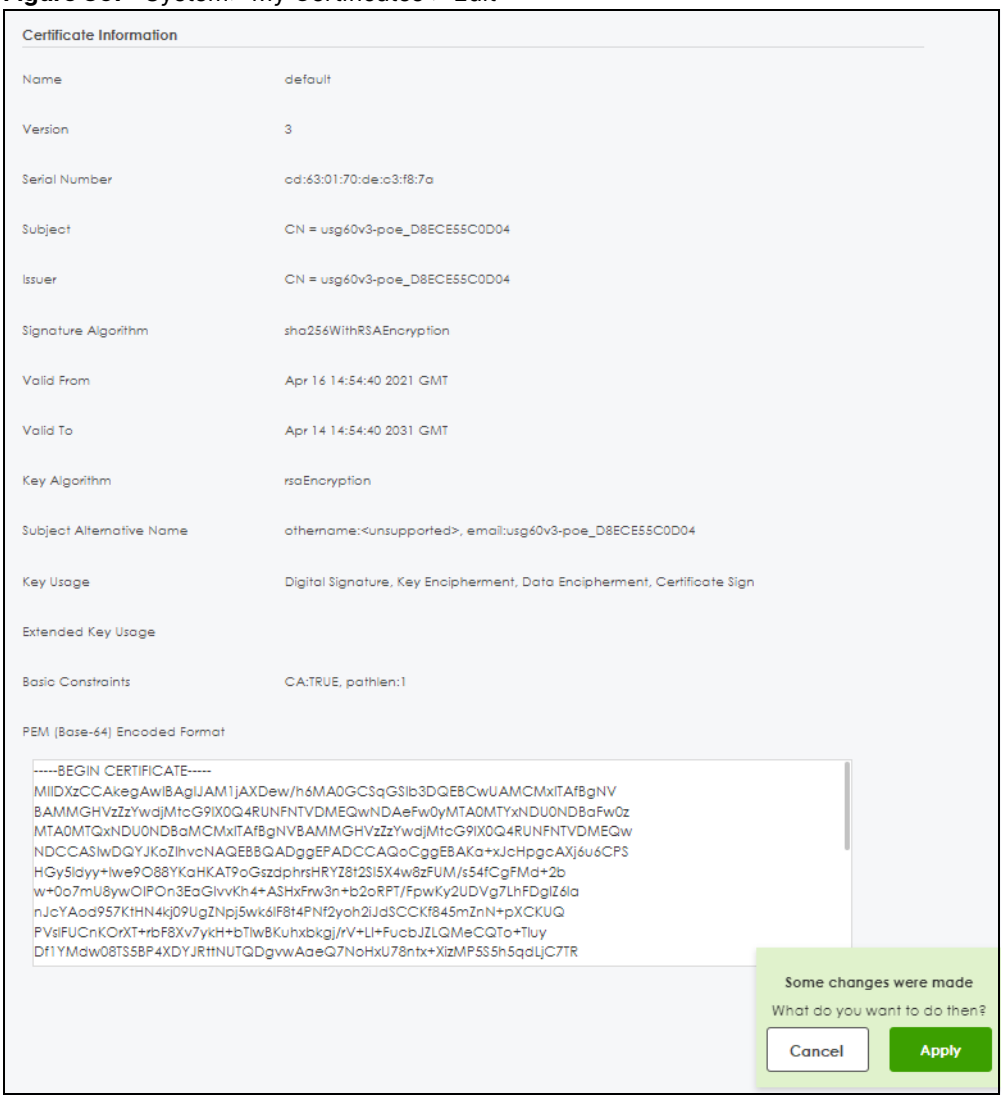
Table 285 System > My Certificates > Add (continued)

LABEL	DESCRIPTION
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 30.8.2 on page 617) and then send it to the certification authority.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

30.8.2 The My Certificates Edit Screen

Click **System > 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 367 System> My Certificates > Edit



The following table describes the labels in this screen.

Table 286 System > My Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
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).

Table 286 System > My Certificates > Edit (continued)

LABEL	DESCRIPTION
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.
PEM 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 (via external storage device for example).
MD5 Fingerprint	It is a unique 128-bit checksum value generated by the MD5 hashing algorithm, used to verify data integrity and identify cryptographic keys, though it is no longer considered secure.
SHA1 Fingerprint	It is a 160-bit hash value produced by the SHA-1 hashing algorithm, commonly used to verify data integrity and identify cryptographic keys, although it is now considered weak due to vulnerabilities.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

30.8.3 The My Certificates Import Screen

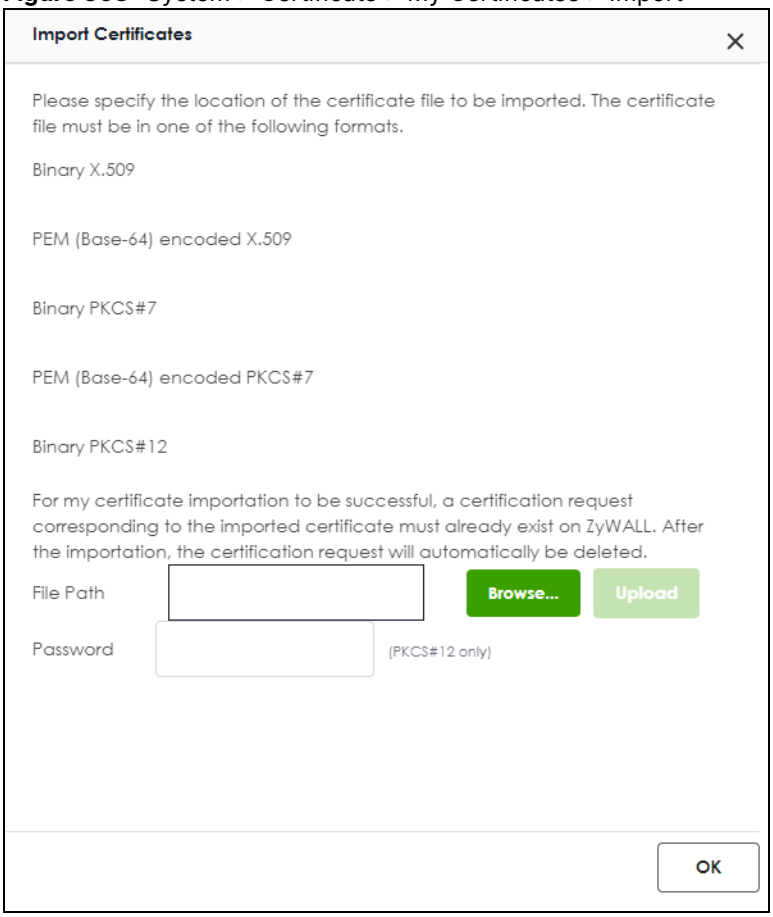
Click **System > Certificate > My Certificates > Import** to open the **Import Certificates** screen. Follow the instructions in this screen to save an existing certificate to the Zyxel Device.

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 368 System > Certificate > My Certificates > Import



The following table describes the labels in this screen.

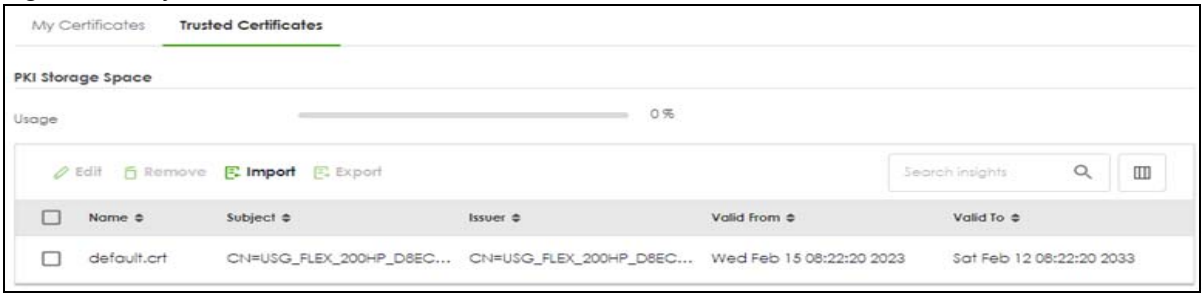
Table 287 System > Certificate > My Certificates > Import

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.

30.9 Trusted Certificates

Click **System > 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 369 System > Certificate > Trusted Certificates



The following table describes the labels in this screen.

Table 288 System > Certificate > Trusted Certificates

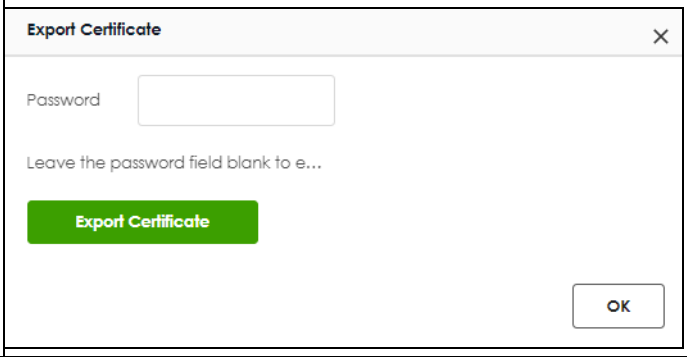
LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click **Edit** to open a screen with an in-depth list of information about the certificate.
Remove	The Zyxel Device keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file 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.
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.
Export	Click this and the following screen will appear. Type the selected certificate's password and save the selected certificate to your computer. 
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.

Table 288 System > Certificate > Trusted Certificates (continued)

LABEL	DESCRIPTION
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.

30.9.1 The Trusted Certificates Edit Screen

Click **System > Certificate > Trusted Certificates** > **Edit** icon to open the **Trusted Certificates Edit** screen. Use this screen to view in-depth information about the certificate.

Figure 370 System > Certificate > Trusted Certificates > Edit



The following table describes the labels in this screen.

Table 289 System > Certificate > Trusted Certificates > Edit

LABEL	DESCRIPTION
Certification Path	Click the **Refresh** button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certificate, it may be the only certification authority in the list (along with the end entity's own certificate). The 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.
Name	This field displays the identifying name of this certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the **Subject Name** field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the 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.
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	It is a unique 128-bit checksum value generated by the MD5 hashing algorithm, used to verify data integrity and identify cryptographic keys, though it is no longer considered secure.

Table 289 System > Certificate > Trusted Certificates > Edit (continued)

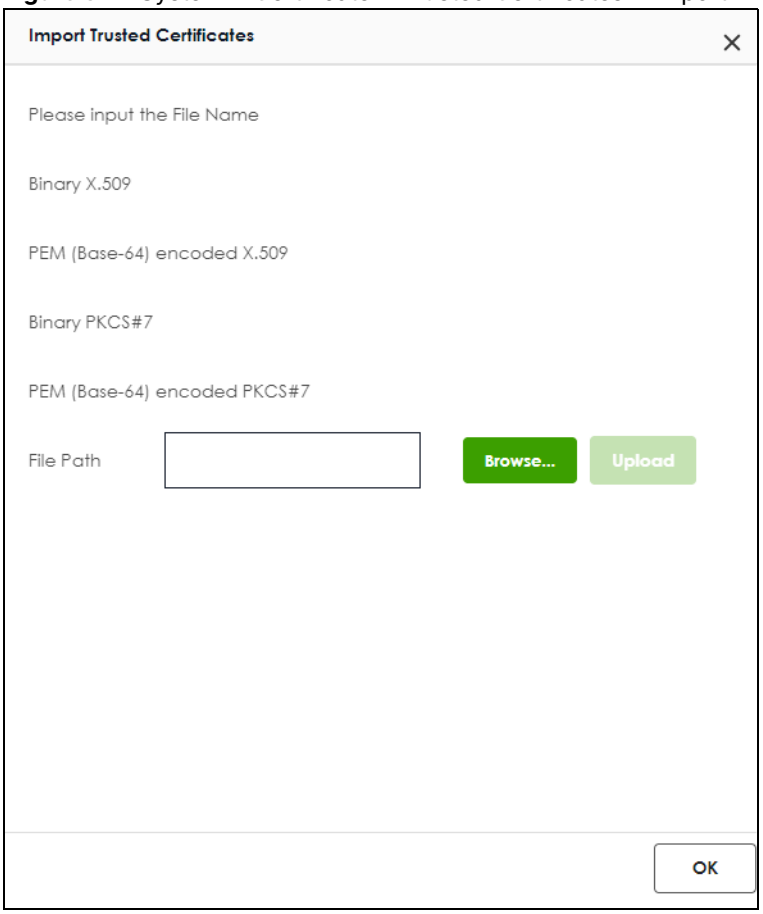
LABEL	DESCRIPTION
SHA1 Fingerprint	It is a 160-bit hash value produced by the SHA-1 hashing algorithm, commonly used to verify data integrity and identify cryptographic keys, although it is now considered weak due to vulnerabilities.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form. You can copy and paste the certificate into an 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 (via external storage device for example).

30.9.2 The Trusted Certificates Import Screen

Click **System > Certificate > Trusted Certificates > Import** to open the **Import Trusted Certificates** 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 371 System > Certificate > Trusted Certificates > Import



The following table describes the labels in this screen.

Table 290 System > 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.

30.10 Let’s Encrypt Certificate

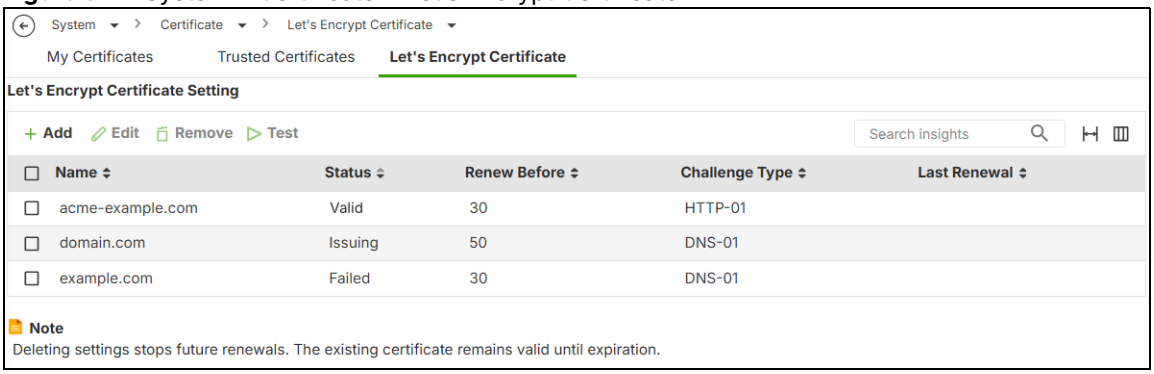
Let's Encrypt provides free SSL/TLS certificates for HTTPS. The Zyxel Device acts as an ACME client to communicates with Let's Encrypt using the Automatic Certificate Management Environment (ACME) protocol to automatically request and renew certificates.

Let's Encrypt verifies that you control a domain using either the HTTP-01 or DNS-01 challenge method before issuing a certificate.

- HTTP-01: Proves domain ownership by checking the web server over HTTP. Select this method if the WAN interface of your Zyxel Device has a public IP address and is reachable through HTTP (port 80). The domain name must resolve to the public IP address through DNS records. If the public IP address is dynamic, DDNS should be configured to keep the DNS records updated. Refer to Section 30.4 on page 581 for details.
- DNS-01: Proves domain ownership by checking a TXT record in DNS. Select this method if your domain's DNS records are managed by Cloudflare. A Cloudflare API token will be used to automatically add and remove TXT records for DNS validation.

Click **System > Certificate > Let's Encrypt Certificate** to open the **Let's Encrypt Certificate** screen. This screen displays a summary list of certificates configured on the Zyxel Device through Let’s Encrypt using the ACME protocol.

Figure 372 System > Certificate > Let’s Encrypt Certificate



The following table describes the labels in this screen.

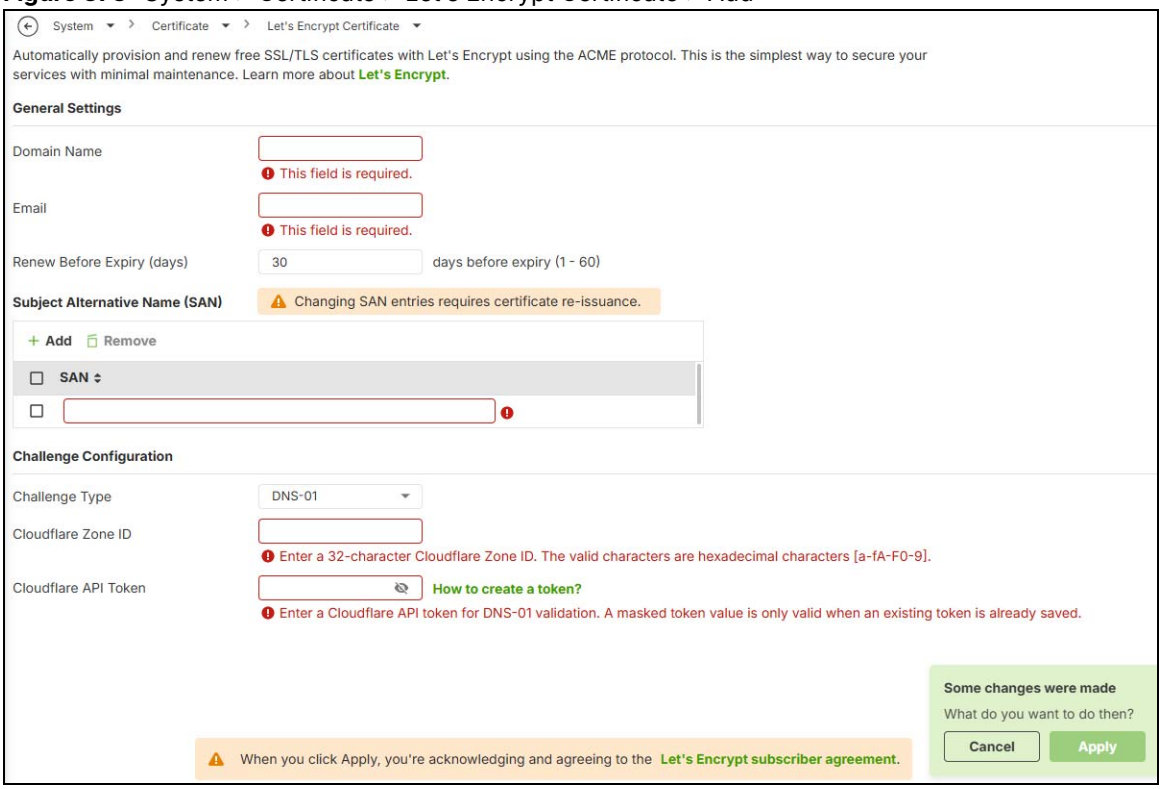
Table 291 System > Certificate > Let's Encrypt Certificate

LABEL	DESCRIPTION
Let's Encrypt Certificate Setting	
+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**.
Test	Select an entry and click **Test** to start a validation test for the entry.
Name	This field displays the domain name (FQDN) used to identify this certificate. It is recommended that you give each certificate a unique name.
Status	This field displays the current status of the entry. • Issuing: The certificate request is being processed. • Valid: The certificate has been successfully validated. • Failed: The certificate validation or issuance failed. • Scheduled: The certificate has not been validated. Go to **Maintenance > Diagnostics > System Log**, and download the **lets-encrypt.log** file to view the logs for troubleshooting.
Renew Before	This field displays the number of days before certificate expiration when the system will automatically renew the certificate.
Challenge Type	This field displays the challenge type used for this certificate.
Last Renewal	This field displays the last time the certificate was renewed.

30.10.1 The Let's Encrypt Certificate Add Screen

Click **System > Certificate > Let's Encrypt Certificate** > **Add** icon to open the **Let's Encrypt Certificate Add** screen. Use this screen to specify a certificate issued by Let's Encrypt.

Figure 373 System > Certificate > Let's Encrypt Certificate > Add



The following table describes the labels in this screen.

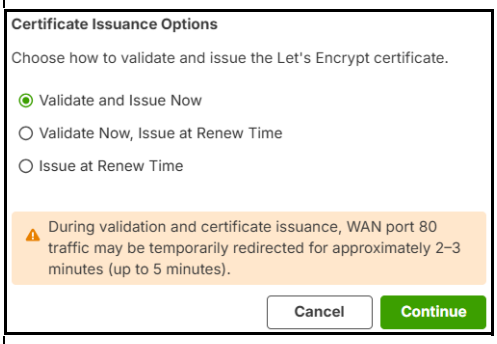
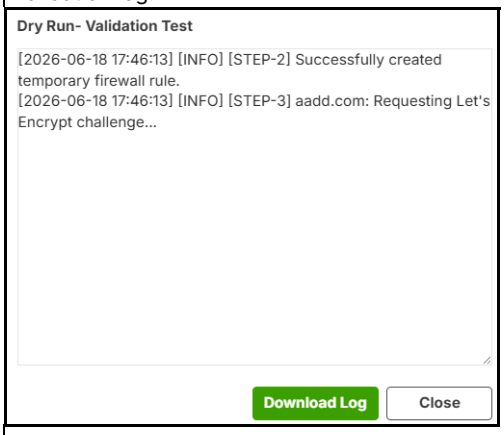
Table 292 System > Certificate > Let's Encrypt Certificate > Add/Edit

LABEL	DESCRIPTION
General Settings	
Domain Name	Enter the Fully Qualified Domain Name (FQDN) that you want to secure with this certificate. • The domain name can be up to 253 characters long. • Use only alphanumeric characters and periods: [A-Za-z0-9.]. • Wildcard domains (for example, *.company.com) are not supported.
Email	Enter the email address to receive notifications about certificate renewal and expiration. • Use up to 83 characters. • Allowed characters: [a-zA-Z0-9/=?^_.{|}~-!#$%*+]
Renew Before Expiry (days)	Specify how many days before certificate expiration the system should renew the certificate. From 1 to 60 days. The default is 30 days.
Subject Alternative Names (SAN)	
+Add	Enter additional domain names (FQDNs) to use with this certificate, excluding the primary domain specified above. You can specify up to 5 additional domains. Wildcard domains (for example, *.company.com) are not supported. Note: If the challenge type is HTTP-01, ensure that each SAN domain resolves to the Zyxel Device's public IP address through DNS or DDNS records. Note: If you change the SAN entries, the certificate will need to be validated and issued again.
Remove	Remove the specified domain from this certificate.

Table 292 System > Certificate > Let's Encrypt Certificate > Add/Edit (continued)

LABEL	DESCRIPTION
Challenge Configuration	
Challenge Type	Select the method used to verify that you own the specified domain. See Section 30.9 on page 621 for the difference.
Renew Time	Enter the scheduled time to start the HTTP-01 challenge during the specified certificate renewal date (Renew Before Expiry (days)). HTTP port will be temporarily used for validation. Schedule the validation during off-peak hours to avoid impacting HTTP traffic forwarded to the LAN server through NAT on HTTP port (port 80).
Cloudflare Zone ID	Enter your 32-character Cloudflare Zone ID to allow automatic DNS updates for domain verification.
Cloudflare API Token	Enter your Cloudflare API token to allow automatic DNS updates for domain verification. Click *How to create a token?* to view the instruction.
Dry Run Validation	Go to **Maintenance > Diagnostics > System Log**, and download the **lets-encrypt.log** file to view the logs for troubleshooting.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

Table 292 System > Certificate > Let's Encrypt Certificate > Add/Edit (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to acknowledge and agree to the Let's Encrypt Subscriber Agreement and save your configuration. See *https://letsencrypt.org/repository/*.
Certificate Issuance Options	If you select HTTP-01 as the challenge type, the following screen appears, allowing you to choose when to validate and issue the certificate. • Validate: Runs a domain ownership verification to check whether the configuration is correct. • Issue: Generates and signs the certificate after successful validation.  You can choose one of the following options: • Validate and Issue Now • Validate Now, Issue at Renew Time • Issue at Renew Time If you select **Validate and Issue Now** or **Validate Now, Issue at Renew Time**, validation starts after you click **Continue**. The **Dry Run Validation Test window** appears and displays the validation log.  You can click **Download Log** to download the log file to your computer for troubleshooting. The log is also saved in the **lets-encrypt.log** file under **Maintenance > Diagnostics > System Log**.

30.11 Advanced

Use this screen to view UDP and ICMP timeout settings on your Zyxel Device and to enable or disable advanced functions as shown in the screen.

30.11.1 SecuManager v3

SecuManager v3 is a hardware-based management system that uses the NETCONF protocol (port 4335) to send commands to the Zyxel Devices for management and monitoring.

SecuManager v3 features include:

- Batch import of managed devices at one time using one CSV file
- See an overview of all managed devices and system information in one place
- Monitor and manage devices
- Install firmware to multiple devices of the same model at one time
- Backup and restore device configuration

To allow SecuManager v3 management of your Zyxel Device:

- You must have a SecuManager v3 server URL.
- The Zyxel Device must be able to communicate with the SecuManager v3 server.

When you enable SecuManager v3, you allow SecuManager v3 to send and run commands (CLI scripts) on the Zyxel Device.

30.11.1.1 SecuManager v3 Scripts

Here are some example scripts. The following script displays interface details of the Zyxel Device.

```
netconf connect
show interface
exit
```

The following script sets specific interface information. Note the extra exit to leave configuration mode.

```
netconf connect
edit running
vrf main interface ethernet ge1 description aaa
commit
exit
exit
```

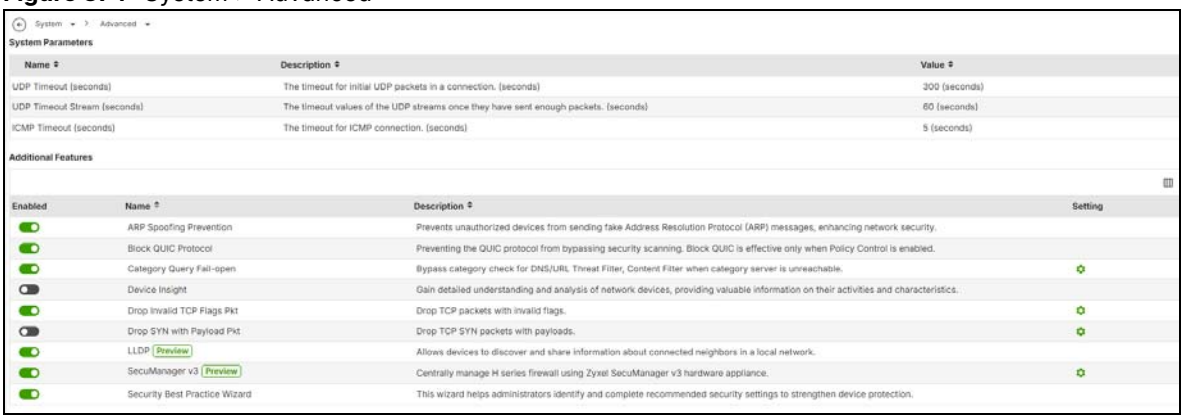
30.11.1.2 SecuManager v3 Error Log

The SecuManager v3 error log can be up to 1 MB in size with up to 1,000 entries. New entries overwrite the oldest entries. The log can be seen in secumanager-script.log in **Maintenance > Diagnostics > System Log**.

30.11.2 Advanced System Screen

Click **System > Advanced** to open the **Advanced** screen.

Figure 374 System > Advanced



The following table describes the labels in this screen.

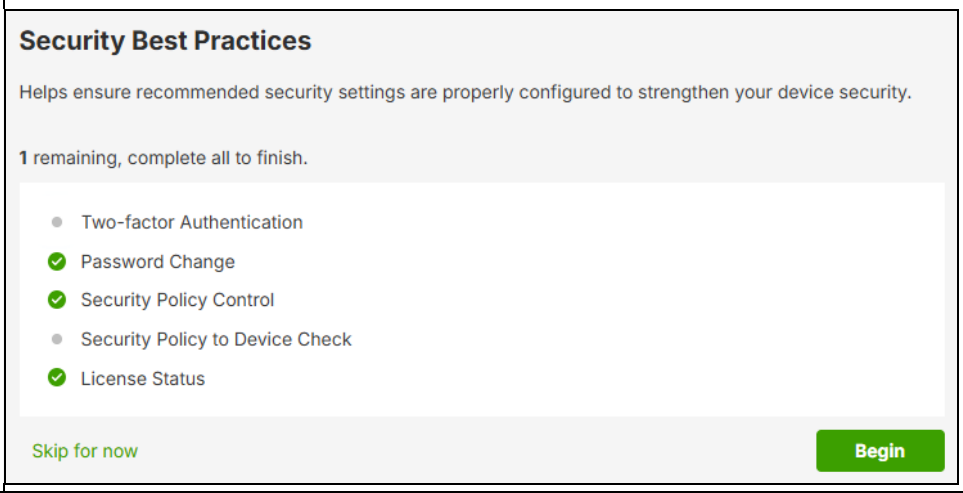
Table 293 System > Advanced

LABEL	DESCRIPTION
System Parameters	
Name	This field displays the name of the system parameter. **UDP Timeout**: After the UDP client sends a request to the server, if there is no response from the server within this set time, the Zyxel Device ends the UDP connection. **UDP Timeout Stream**: The UDP client sends a request to the server and receives a response, but the connection is interrupted. If there is no further response from the server within this set time, the Zyxel Device ends the UDP connection **ICMP Timeout:** This shows how long the Zyxel Device waits before considering the ICMP connection attempt a failure.
Description	This field displays the description of the system information.
Value	This field displays the value of the system information. Click the **Edit** icon to modify the value.
Additional Features	
Enabled	Click this switch to enable or disable the feature. When the switch turns green, the function is enabled.
Name	This field displays the name of the following features.
ARP Spoofing Prevention	Enable this feature to prevent and create a log on the Zyxel Device when there is a fake ARP message that failed the ARP verification.
Block QUIC Protocol	QUIC (Quick UDP Internet Connections) is a transport protocol that encrypts most of the transport layer, and not just the payload. If QUIC is not blocked, the Zyxel Device may not be able to inspect AI requests and replies in order to apply content filtering correctly (**Security Services > Content Filtering**) in a security policy (**Security Policy > Policy Control**). Enable **Block QUIC Protocol** to stop browsers using QUIC so that the Zyxel Device can use SSL inspection to inspect encrypted traffic for AI requests and replies.
Category Query Fail-open	A category server classifies IP addresses and URLs to different categories, such as anonymizers, browser exploits, and malicious downloads. Enable this feature to allow traffic to bypass if the Zyxel Device cannot access the category server. Click on the **Edit** icon next to this field to configure more settings. Use **Log** to generate a log (**log**)or not (**no**) when the query to the category server failed.
Device Insight	Enable this feature to collect status and basic information of the clients connected to the Zyxel Device.

Table 293 System > Advanced (continued)

LABEL	DESCRIPTION
Drop Invalid TCP Flags Pkt	Enable this feature to allow the Zyxel Device to inspect TCP packets and drop any with invalid flags, such as FIN + SYN, FIN + RST, and SYN + RST flag combinations. Click on the **Edit** icon next to this field to configure more settings. Use **Log** to generate a log (**log**), log and alert (**log alert**) or not (**no**) when the Zyxel Device detects an invalid TCP flag.
Drop SYN with Payload Pkt	When setting up a TCP connection, a SYN packet is used during the initial handshake to establish connection between two network devices, and typically does not carry any data payload. A SYN packet with a payload may indicate a potential attack, such as a SYN flood. Enable this feature to allow your Zyxel Device to drop SYN packets with a payload. Click on the **Edit** icon next to this field to configure more settings. **Log:** Generate a log (**log**), log and alert (**log alert**) or not (**no**) when there is a SYN packet with payload detected by the Zyxel Device. **Destination Port:** Specify a destination port number to drop SYN packets with a payload sent to that port. If set to 0, SYN packets with a payload sent to any port will be dropped. **Payload Size (greater than or equal to):** Specify the size (in bytes) to drop SYN packets with a payload of this size or larger.
LLDP	Link Layer Discovery Protocol (LLDP, IEEE 802.1AB) is a Layer 2 protocol that allows network devices to advertise their identity and capabilities on a LAN. Enable this feature to allow your Zyxel Device to share its identity and capabilities on the local network.
SecuManager v3	Click **Enabled** to the right to enable SecuManager v3. Click on the **Edit** icon next to the right of this field to configure more settings.  Note: If you enable SecuManager v3, NCC is automatically disabled and cannot manage the Zyxel Device. SecuManager v3 Settings: **Enable**: Click this to the right to enable SecuManager v3. **Server Address**: Enter the IPv4 IP address of the SecuManager v3 server. This should be an IPv4 address or a FQDN (Fully Qualified Domain Name), such as server01.corp.zyxel.com. **Server Port**: Port 4335 (NETCONF) is the default TCP port to communicate with SecuManager v3. Note: Make sure port 4335 is not blocked by a security policy on the Zyxel Device. **Server Certificate**: Select a certificate the Zyxel Device uses to authenticate itself with the SecuManager v3.

Table 293 System > Advanced (continued)

LABEL	DESCRIPTION
Security Best Practice Wizard	Click **Enabled** to the left to disable the security check wizard from displaying after you log in. A selected item means it is NOT checked. **Security Policy Control** checks if **Security Policy > Policy Control** is enabled or not. It is enabled by default. **Security Policy to Device Check** queries if you have set specific IP addresses (trusted hosts) from which an admin can exclusively access the Zyxel Device. The default is from **any**. If you choose to set a trusted host, a new WAN-to-Device security policy is created at the top of the policy rules in **Security Policy > Policy Control**, for the specified host. 
Description	This field displays what the feature does.

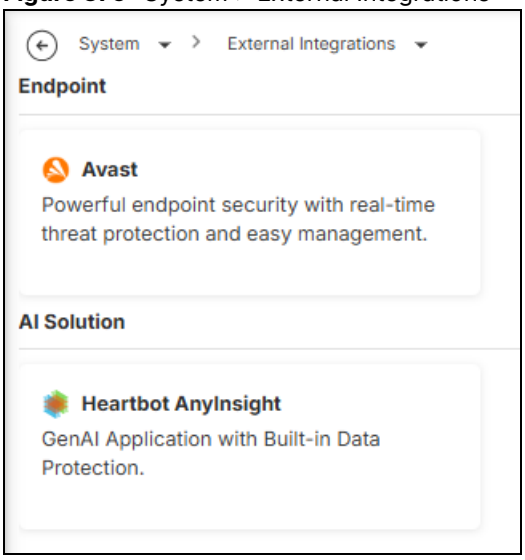
30.12 External Integrations

Use this screen to integrate the Zyxel Device with other cloud-based security platforms. At the time of writing, the Zyxel Device supports:

- Avast Business Hub
- Heartbot AnyInsight.

Click **System** > **External Integrations** to display the following screen.

Figure 375 System > External Integrations



30.12.1 Avast

Avast is a cloud-based security platform where you can manage the endpoint devices to display:

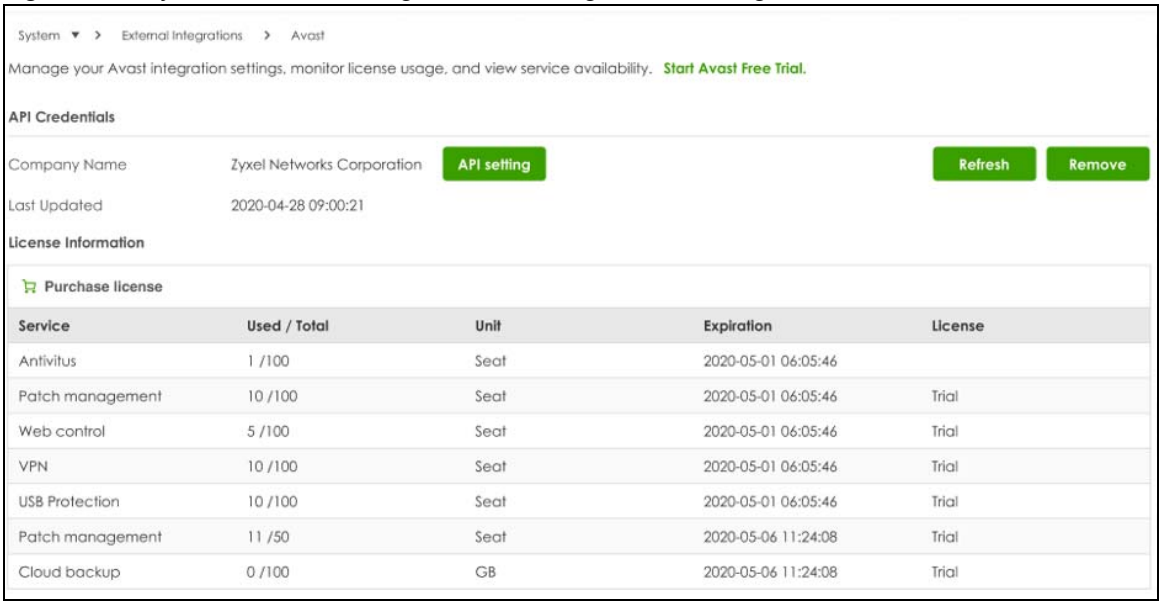
- License information
- Device Insight details
- Security policy synchronization

The Avast Business Hub can also protect your endpoints, applications, and networks from:

- Ransomware (malware that encrypts your files preventing you from accessing them
- Phishing (fraudulent emails and messages seeking private information)
- Antivirus
- Web attacks.

Click **Avast**. The following screen then displays.

Figure 376 System > External Integrations > Manage Avast Settings



The following table describes the labels in this screen.

Table 294 System > External Integrations > Manage Avast Settings

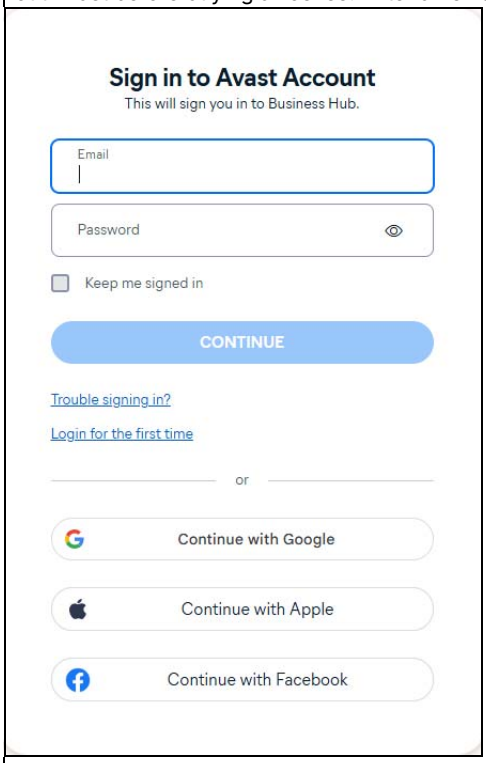
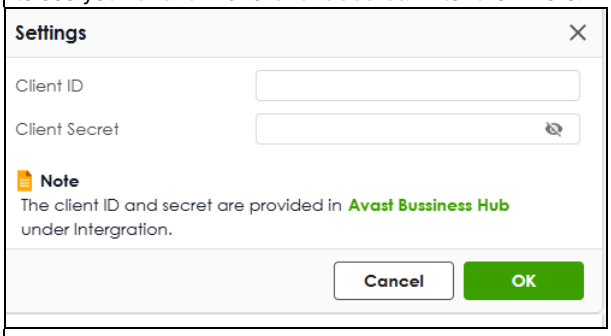
LABEL	DESCRIPTION
Start Avast Free Trial	Click this link to go to the Avast Business Hub. Click **Free Trial** to create an Avast account to try out Avast before buying a license. Enter an email address and password for your Avast account. 
API Credentials	
Company Name	This displays the company name you used to register with Avast.

Table 294 System > External Integrations > Manage Avast Settings (continued)

LABEL	DESCRIPTION
API Setting	Avast API settings are the configurations within the Avast Business Hub for integrating the Zyxel Device with Avast. This allows for managing devices and other functions through the API. You need a **Client ID** and **Client Secret** for authentication and authorization of the Zyxel Device with Avast. After you create your Avast account, go to the Avast Business Hub portal, then find **Integration** to see your **Client ID** and **Client Secret**. Enter them here. 
Last Updated	This displays the date and time the license information through the Avast API was last updated in yyyy-mm-dd hh-mm-ss format. Click **Refresh** to renew the settings or click **Remove** if you want to enter a new **Client ID** and **Client Secret**.
Licenses Information	
Purchase Licenses	After your trial expires and you are happy with the services, click this link to log into your Avast account and purchase standard licenses.
Service	This displays the services covered under the Avast license.
Used Total	This displays how much you have used for the total allowed for each service.
Unit	This displays the measurement unit for the service, such as the number of seats or the amount in Gigabytes (GB).
License	This displays the type of license you have for this service.
Expiration	This displays the date and time the license for the service will expire in yyyy-mm-dd hh-mm-ss format.

30.12.2 AnyInsight

Traditional DLP ((Data Loss Prevention) relies on predefined rules, pattern matching, keyword detection. An AI DLP solution uses machine learning and artificial intelligence to analyze context, intent, behavior patterns, document meaning, and user risk profile. Traditional DLP may flag too much, and block legitimate business. AI DLP learns normal behavior, reduces unnecessary alerts, and improves accuracy over time.

AnyInsight.ai checks what gets sent to or is produced by AI models. AnyInsight's platform includes an AI firewall and policy engine that act as a layer of filtering and rule enforcement around AI interactions. Vetting actions include the following:

- Input filtering: AnyInsight can examine prompts before they reach the AI portal to reject or block queries containing unwanted text (such as harmful or prohibited topics).
- Output filtering: AnyInsight can scan the portal's responses and apply policies to remove, quarantine, or mask content that violates organizational guidelines, such as toxic language and revealing sensitive data.
  - Masking: Sensitive data or context can be automatically masked (hidden) in both user prompts and AI outputs.

- Output quarantine: Responses that don't meet safety or policy criteria can be held for review instead of being immediately delivered to a user.

Sign up for an account with *anyinsight.ai* so that you can manage access to AI web pages and cloud services through *anyinsight.ai*.

Click **System** > **External Integrations** > **Heartbot** to display the following screen.

Figure 377 System > External Integrations > Heartbot

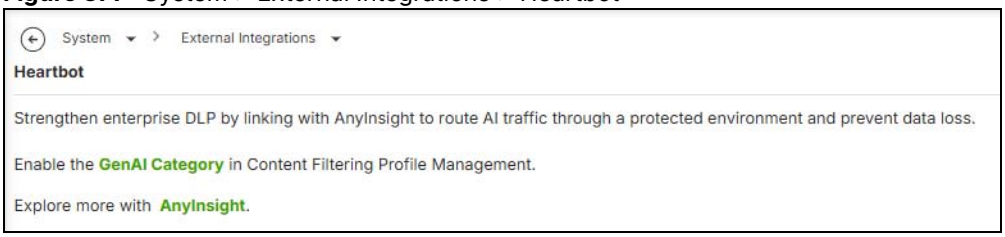
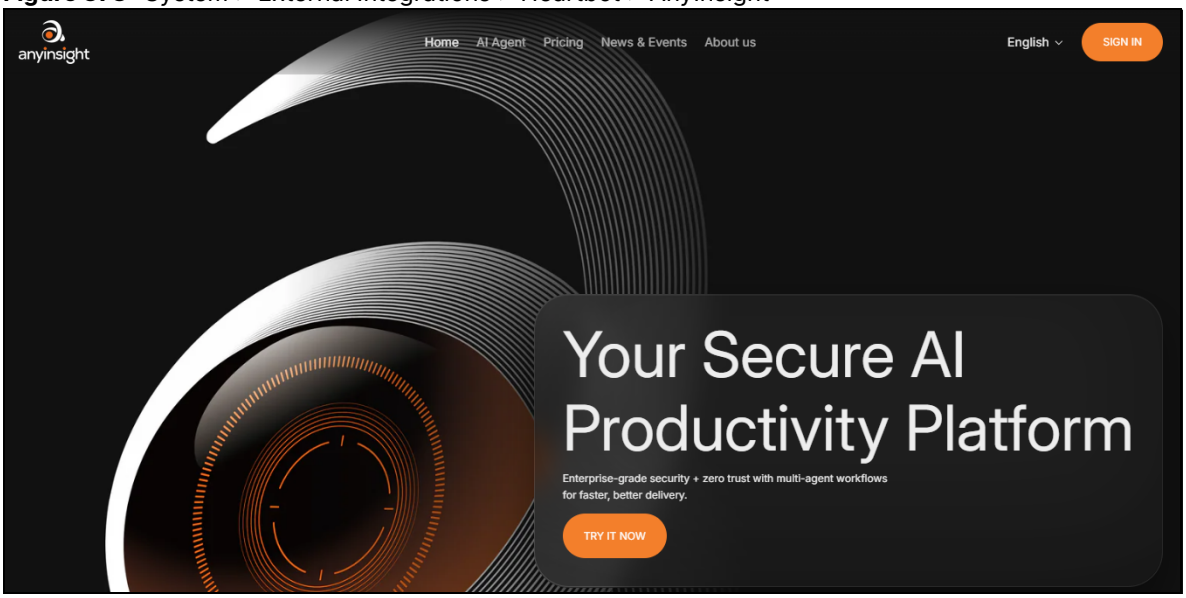


Figure 378 System > External Integrations > Heartbot > AnyInsight



CHAPTER 31
Log and Report

31.1 Overview

Use these screens to configure daily reporting and log settings.

31.1.1 What You Can Do In this Chapter

- Use the **Log/Events** screens (Section 31.2 on page 638) to view the Zyxel Device log messages.
- Use the **Log Settings** screen (Section 31.3 on page 647) to specify settings for recording log messages and alerts and storing them on a connected USB storage device.
- Use the **SecuReporter** screen (Section 31.4 on page 650) 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 the **Email Daily Report** screen (Section 31.5 on page 652) to start or stop traffic collection and view reports on traffic passing through the Zyxel Device.

31.2 Log/Events Screens

To access these screens, click **Log & Report > Log/Events**. 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.

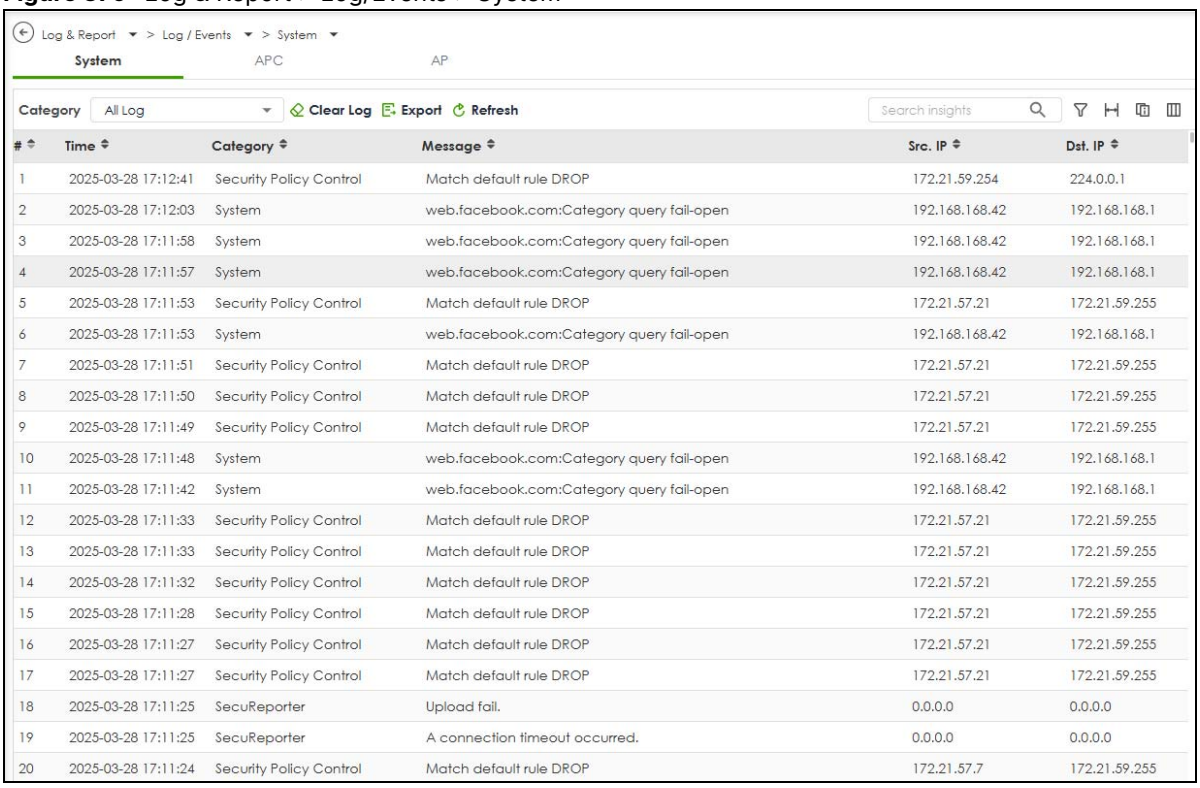
- The maximum possible number of log messages in the Zyxel Device varies by model.

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 **Log/Events** screen and return to it later.

31.2.1 System Logs

The following screen shows **System** logs.

Figure 379 Log & Report > Log/Events > System



#	Time	Category	Message	Src. IP	Dst. IP
1	2025-03-28 17:12:41	Security Policy Control	Match default rule DROP	172.21.59.254	224.0.0.1
2	2025-03-28 17:12:03	System	web.facebook.com:Category query fail-open	192.168.168.42	192.168.168.1
3	2025-03-28 17:11:58	System	web.facebook.com:Category query fail-open	192.168.168.42	192.168.168.1
4	2025-03-28 17:11:57	System	web.facebook.com:Category query fail-open	192.168.168.42	192.168.168.1
5	2025-03-28 17:11:53	Security Policy Control	Match default rule DROP	172.21.57.21	172.21.59.255
6	2025-03-28 17:11:53	System	web.facebook.com:Category query fail-open	192.168.168.42	192.168.168.1
7	2025-03-28 17:11:51	Security Policy Control	Match default rule DROP	172.21.57.21	172.21.59.255
8	2025-03-28 17:11:50	Security Policy Control	Match default rule DROP	172.21.57.21	172.21.59.255
9	2025-03-28 17:11:49	Security Policy Control	Match default rule DROP	172.21.57.21	172.21.59.255
10	2025-03-28 17:11:48	System	web.facebook.com:Category query fail-open	192.168.168.42	192.168.168.1
11	2025-03-28 17:11:42	System	web.facebook.com:Category query fail-open	192.168.168.42	192.168.168.1
12	2025-03-28 17:11:33	Security Policy Control	Match default rule DROP	172.21.57.21	172.21.59.255
13	2025-03-28 17:11:33	Security Policy Control	Match default rule DROP	172.21.57.21	172.21.59.255
14	2025-03-28 17:11:32	Security Policy Control	Match default rule DROP	172.21.57.21	172.21.59.255
15	2025-03-28 17:11:28	Security Policy Control	Match default rule DROP	172.21.57.21	172.21.59.255
16	2025-03-28 17:11:27	Security Policy Control	Match default rule DROP	172.21.57.21	172.21.59.255
17	2025-03-28 17:11:27	Security Policy Control	Match default rule DROP	172.21.57.21	172.21.59.255
18	2025-03-28 17:11:25	SecuReporter	Upload fail.	0.0.0.0	0.0.0.0
19	2025-03-28 17:11:25	SecuReporter	A connection timeout occurred.	0.0.0.0	0.0.0.0
20	2025-03-28 17:11:24	Security Policy Control	Match default rule DROP	172.21.57.7	172.21.59.255

The following table describes the labels in this screen.

Table 295 Log & Report > Log/Events > System

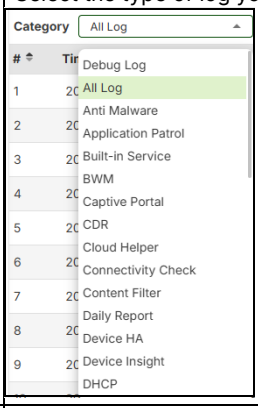
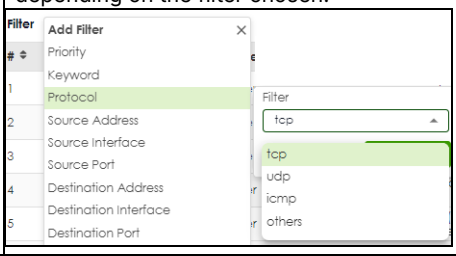
LABEL	DESCRIPTION
Category	Select the type of log you want to display from this list box. 
Clear Log	Click this button to clear the whole log, regardless of what is currently displayed on the screen.
Export	Click this button to download logs of the chosen category to your computer in Excel (format (.xlsx).

Table 295 Log & Report > Log/Events > System (continued)

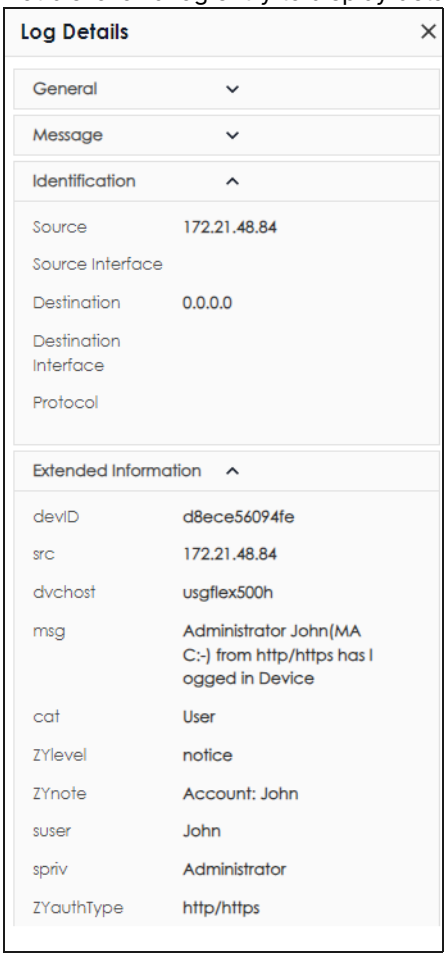
LABEL	DESCRIPTION
SecuReporter	The following category of logs show a SecuReporter icon SecuReporter. Click this icon to view more historical logs in SecuReporter. You should already have a SecuReporter account. • Anti-Malware • Application Patrol • Content Filter • DNS Threat Filter • IP Reputation • IPS • Sandbox • URL Threat Filter
Refresh	Click this button to update the information on the screen.
Search	Type a keyword to look for in the **Message**, **Source**, **Destination** and **Note** fields. If a match is found in any field, the log message is displayed. You can use up to 63 alphanumeric characters and the underscore, as well as punctuation marks ()' ,:;?! +-*/= #$% @ ; the period, double quotes, and brackets are not allowed. 
Filter	Click this icon then click + to display the add filter, pick a filter, then click **Search** to display specific sessions according to the filter selected. You may select multiple filters, but just one of each type, configured one at a time.
Priority	This displays when you click the filter icon. Select the priority of log messages to display. The log displays the log messages with this priority or higher. Choices from highest priority to lowest priority are: **emergency**, **alert**, **critical**, **error**, **warning**, **notice**, and **info**.
Keyword	This displays when you click the filter icon. Type a keyword to display logs with this keyword.
Protocol	This displays when you click the filter icon. Select a service protocol to display logs with this protocol.
Source Address	This displays when you click the filter icon. Type the source IP address of the incoming packets to display logs with this source IP address. Do not include the port in this filter.
Source Interface	This displays when you click the filter icon. Type the source interface of the incoming packets to display logs with this source interface.
Source Port	This displays when you click the filter icon. Type the source port number to display logs with this source IP port.
Destination Address	This displays when you click the filter icon. Type the IP address of the destination of the incoming packets to display logs with this destination IP address. Do not include the port in this filter.
Destination Interface	This displays when you click the filter icon. Type the interface of the destination of the incoming packets to display logs with this destination interface.
Destination Port	This displays when you click the filter icon. Type the destination port number to display logs with this destination IP port.

Table 295 Log & Report > Log/Events > System (continued)

LABEL	DESCRIPTION
Filter	Click this icon to display specific types of logs. Select a type or type a keyword depending on the filter chosen. 
#	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.
Pri	This displays when you click the filter icon. Select the priority of log messages to display. The log displays the log messages with this priority or higher. Choices are: **emerg**, **alert**, **crit**, **error**, **warn**, **notice**, and **info**, from highest priority to lowest priority.
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.
Src. IP	This field displays the source IP address in the event that generated the log message.
Src. Port	This field displays the source port number in the event that generated the log message.
Dst. IP	This field displays the destination IP address of the event that generated the log message.
Dst. Port	This field displays the destination port number of the event that generated the log message.
Note	This field displays any additional information about the log message.
Action	This field displays whether packets were dropped, blocked or if no action was taken as a result of the log. It should correspond to the action configured in **Security Policy > Policy Control**.

31.2.2 Log Details

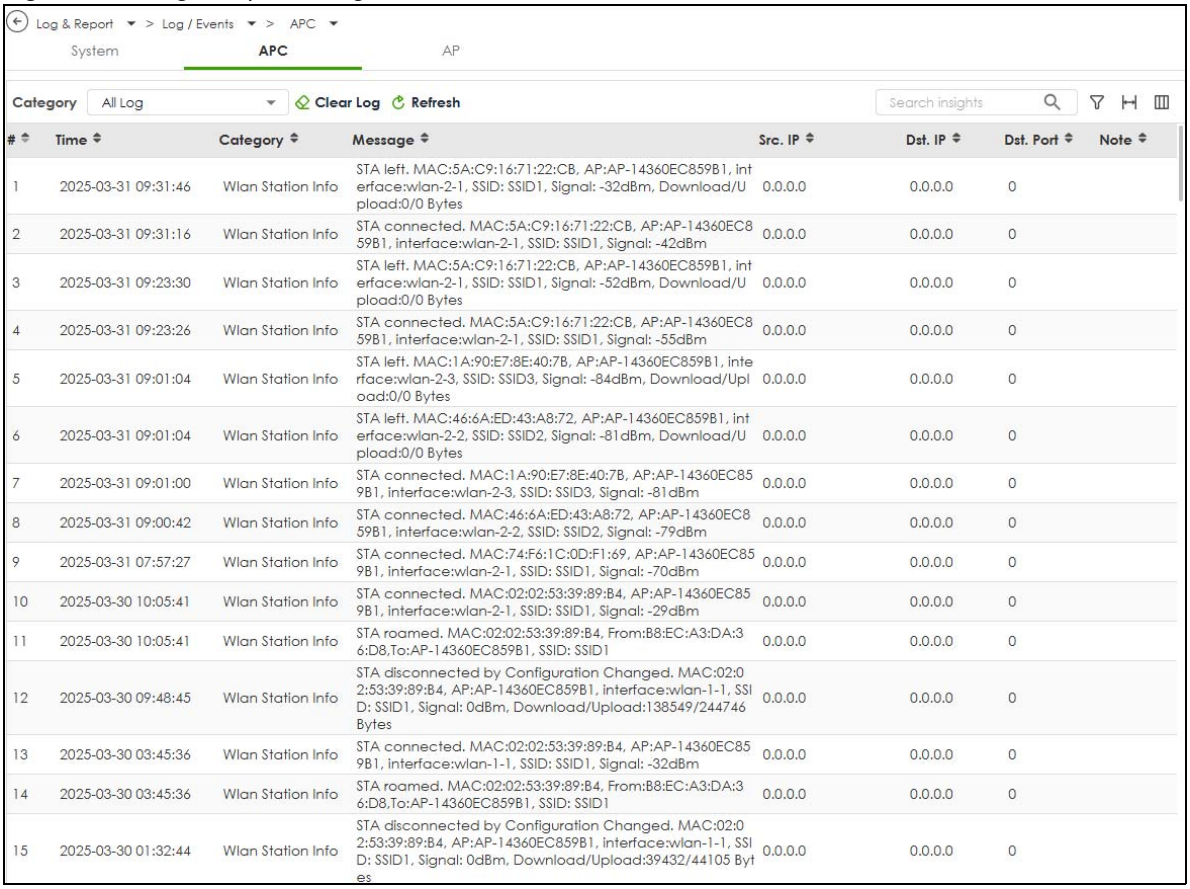
Double-click a log entry to display details on the log. The below is an example.



31.2.3 APC Logs

The following screen shows APC logs. To access this screen, click **Log & Report > Log/Events > APC**.

Figure 380 Log & Report > Log/Events > APC



#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
1	2025-03-31 09:31:46	Wlan Station Info	STA left. MAC:5A:C9:16:71:22:CB, AP:AP-14360EC859B1, interface:wlan-2-1, SSID: SSID1, Signal: -32dBm, Download/Upload:0/0 Bytes	0.0.0.0	0.0.0.0	0	
2	2025-03-31 09:31:16	Wlan Station Info	STA connected. MAC:5A:C9:16:71:22:CB, AP:AP-14360EC859B1, interface:wlan-2-1, SSID: SSID1, Signal: -42dBm	0.0.0.0	0.0.0.0	0	
3	2025-03-31 09:23:30	Wlan Station Info	STA left. MAC:5A:C9:16:71:22:CB, AP:AP-14360EC859B1, interface:wlan-2-1, SSID: SSID1, Signal: -52dBm, Download/Upload:0/0 Bytes	0.0.0.0	0.0.0.0	0	
4	2025-03-31 09:23:26	Wlan Station Info	STA connected. MAC:5A:C9:16:71:22:CB, AP:AP-14360EC859B1, interface:wlan-2-1, SSID: SSID1, Signal: -55dBm	0.0.0.0	0.0.0.0	0	
5	2025-03-31 09:01:04	Wlan Station Info	STA left. MAC:1A:90:E7:8E:40:7B, AP:AP-14360EC859B1, interface:wlan-2-3, SSID: SSID3, Signal: -84dBm, Download/Upload:0/0 Bytes	0.0.0.0	0.0.0.0	0	
6	2025-03-31 09:01:04	Wlan Station Info	STA left. MAC:46:6A:ED:43:A8:72, AP:AP-14360EC859B1, interface:wlan-2-2, SSID: SSID2, Signal: -81dBm, Download/Upload:0/0 Bytes	0.0.0.0	0.0.0.0	0	
7	2025-03-31 09:01:00	Wlan Station Info	STA connected. MAC:1A:90:E7:8E:40:7B, AP:AP-14360EC859B1, interface:wlan-2-3, SSID: SSID3, Signal: -81dBm	0.0.0.0	0.0.0.0	0	
8	2025-03-31 09:00:42	Wlan Station Info	STA connected. MAC:46:6A:ED:43:A8:72, AP:AP-14360EC859B1, interface:wlan-2-2, SSID: SSID2, Signal: -79dBm	0.0.0.0	0.0.0.0	0	
9	2025-03-31 07:57:27	Wlan Station Info	STA connected. MAC:74:F6:1C:0D:F1:69, AP:AP-14360EC859B1, interface:wlan-2-1, SSID: SSID1, Signal: -70dBm	0.0.0.0	0.0.0.0	0	
10	2025-03-30 10:05:41	Wlan Station Info	STA connected. MAC:02:02:53:39:89:B4, AP:AP-14360EC859B1, interface:wlan-2-1, SSID: SSID1, Signal: -29dBm	0.0.0.0	0.0.0.0	0	
11	2025-03-30 10:05:41	Wlan Station Info	STA roamed. MAC:02:02:53:39:89:B4, From:B8:EC:A3:DA:36:D8,To:AP-14360EC859B1, SSID: SSID1	0.0.0.0	0.0.0.0	0	
12	2025-03-30 09:48:45	Wlan Station Info	STA disconnected by Configuration Changed. MAC:02:02:53:39:89:B4, AP:AP-14360EC859B1, interface:wlan-1-1, SSID: SSID1, Signal: 0dBm, Download/Upload:138549/244746 Bytes	0.0.0.0	0.0.0.0	0	
13	2025-03-30 03:45:36	Wlan Station Info	STA connected. MAC:02:02:53:39:89:B4, AP:AP-14360EC859B1, interface:wlan-1-1, SSID: SSID1, Signal: -32dBm	0.0.0.0	0.0.0.0	0	
14	2025-03-30 03:45:36	Wlan Station Info	STA roamed. MAC:02:02:53:39:89:B4, From:B8:EC:A3:DA:36:D8,To:AP-14360EC859B1, SSID: SSID1	0.0.0.0	0.0.0.0	0	
15	2025-03-30 01:32:44	Wlan Station Info	STA disconnected by Configuration Changed. MAC:02:02:53:39:89:B4, AP:AP-14360EC859B1, interface:wlan-1-1, SSID: SSID1, Signal: 0dBm, Download/Upload:39432/44105 Bytes	0.0.0.0	0.0.0.0	0	

The following table describes the labels in this screen.

Table 296 Log & Report > Log/Events > APC

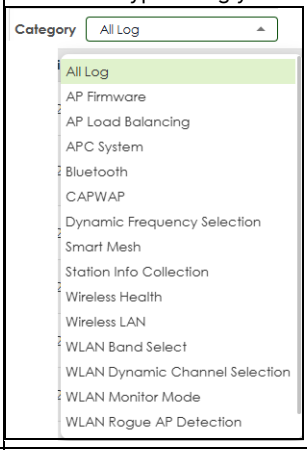
LABEL	DESCRIPTION
Category	Select the type of log you want to display from this list box. 
Clear Log	Click this button to clear the whole log, regardless of what is currently displayed on the screen.
Refresh	Click this button to update the information on the screen.

Table 296 Log & Report > Log/Events > APC (continued)

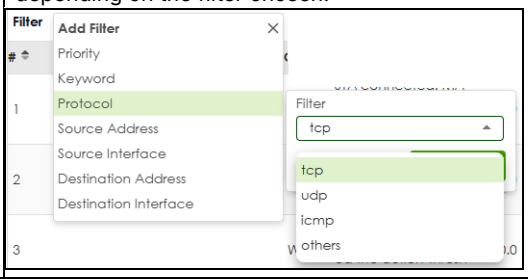
LABEL	DESCRIPTION
Search	Type a keyword to look for in the **Message**, **Source**, **Destination** and **Note** fields. If a match is found in any field, the log message is displayed. You can use up to 63 alphanumeric characters and the underscore, as well as punctuation marks ()' ,:;?! +-*/= #$% @ ; the period, double quotes, and brackets are not allowed. 
Filter	Click this icon then click + to display the add filter, pick a filter, then click **Search** to display specific sessions according to the filter selected. You may select multiple filters, but just one of each type, configured one at a time.
Priority	This displays when you click the filter icon. Select the priority of log messages to display. The log displays the log messages with this priority or higher. Choices from highest priority to lowest priority are: **emergency**, **alert**, **critical**, **error**, **warning**, **notice**, and **info**.
Keyword	This displays when you click the filter icon. Type a keyword to display logs with this keyword.
Protocol	This displays when you click the filter icon. Select a service protocol to display logs with this protocol.
Source Address	This displays when you click the filter icon. Type the source IP address of the incoming packets to display logs with this source IP address. Do not include the port in this filter.
Source Interface	This displays when you click the filter icon. Type the source interface of the incoming packets to display logs with this source interface.
Destination Address	This displays when you click the filter icon. Type the IP address of the destination of the incoming packets to display logs with this destination IP address. Do not include the port in this filter.
Destination Interface	This displays when you click the filter icon. Type the interface of the destination of the incoming packets to display logs with this destination interface.
Filter	Click this icon to display specific types of logs. Select a type or type a keyword depending on the filter chosen. 
#	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.
Pri	This displays when you click the filter icon. Select the priority of log messages to display. The log displays the log messages with this priority or higher. Choices are: **emerg**, **alert**, **crit**, **error**, **warn**, **notice**, and **info**, from highest priority to lowest priority.

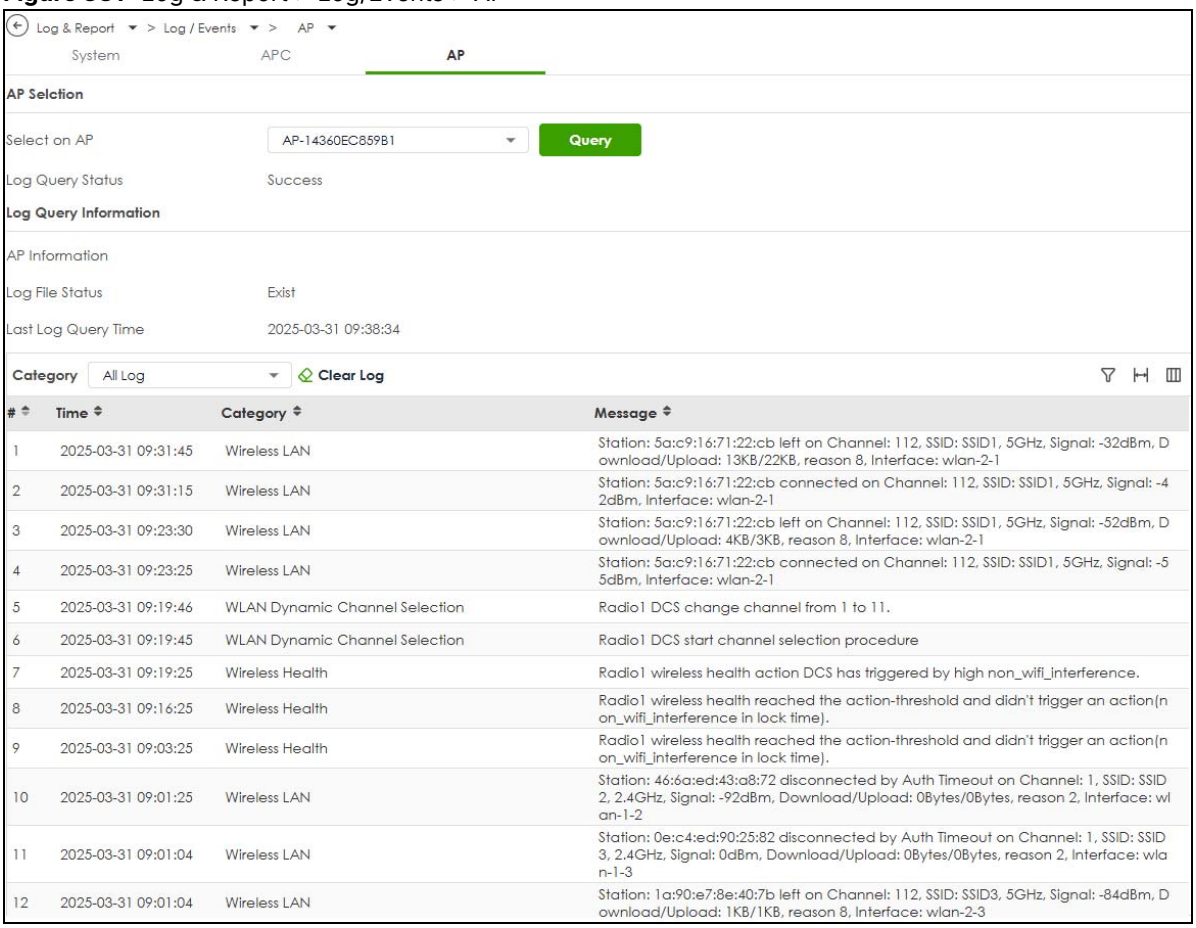
Table 296 Log & Report > Log/Events > APC (continued)

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.
Src. IP	This field displays the source IP address in the event that generated the log message.
Src. Port	This field displays the source port number in the event that generated the log message.
Dst. IP	This field displays the destination IP address of the event that generated the log message.
Dst. Port	This field displays the destination port number of the event that generated the log message.
Note	This field displays any additional information about the log message.
Action	This field displays whether packets were dropped, blocked or if no action was taken as a result of the log. It should correspond to the action configured in **Security Policy > Policy Control**.

31.2.4 AP Logs

The following screen shows AP logs. To access this screen, click **Log & Report > Log/Events > AP**.

Figure 381 Log & Report > Log/Events > AP



The following table describes the labels in this screen.

Table 297 Log & Report > Log/Events > AP

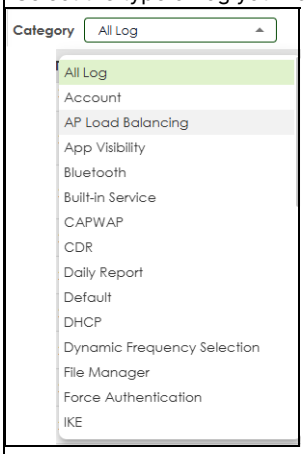
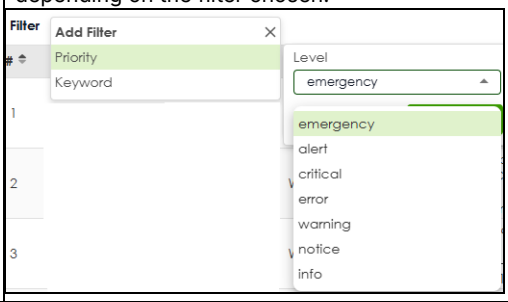
LABEL	DESCRIPTION
AP Selection	
Select on AP	Select an AP from this list box to view its AP logs. Click **Query**.
Log Query Status	This field displays the current status of the Zyxel Device retrieving the AP logs. **Init**: The Zyxel Device has not yet queried the AP logs. **Querying**: The Zyxel Device is retrieving the AP logs. **Success**: The Zyxel Device has successfully retrieved the AP logs. **Query Fail**: The Zyxel Device fails to retrieved the AP logs. This occurs when the connection between the Zyxel Device and the AP is unstable. To check the connection status between the Zyxel Device and the AP, go to **Log & Report > Log/Events >APC**.
Log Query Information	
AP Information	This field displays the MAC address of the AP that the Zyxel Device last successfully queried.
Log File Status	This field displays the current status of the AP logs. **Empty**: The Zyxel Device has no AP logs available. **Exist**: The Zyxel Device contains AP logs retrieved from the currently connected AP. **Last**: The Zyxel Device saves the AP logs from the previous query.
Last Log Query Time	This field displays the most recent time the Zyxel Device retrieved the AP logs.
Category	Select the type of log you want to display from this list box. 
Clear Log	Click this button to clear the queried logs from the selected AP on the Zyxel Device and flush the zylog on the selected AP remotely.
Filter	Click this icon then click + to display the add filter, pick a filter, then click **Search** to display specific sessions according to the filter selected. You may select multiple filters, but just one of each type, configured one at a time.
Priority	This displays when you click the filter icon. Select the priority of log messages to display. The log displays the log messages with this priority or higher. Choices from highest priority to lowest priority are: **emergency**, **alert**, **critical**, **error**, **warning**, **notice**, and **info**.
Keyword	This displays when you click the filter icon. Type a keyword to display logs with this keyword.

Table 297 Log & Report > Log/Events > AP (continued)

LABEL	DESCRIPTION
Filter	Click this icon to display specific types of logs. Select a type or type a keyword depending on the filter chosen. 
#	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.
Pri	This displays when you click the filter icon. Select the priority of log messages to display. The log displays the log messages with this priority or higher. Choices are: **emerg**, **alert**, **crit**, **error**, **warn**, **notice**, and **info**, from highest priority to lowest priority.
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.
Src. IP	This field displays the source IP address in the event that generated the log message.
Dst. IP	This field displays the destination IP address of the event that generated the log message.
Note	This field displays any additional information about the log message.

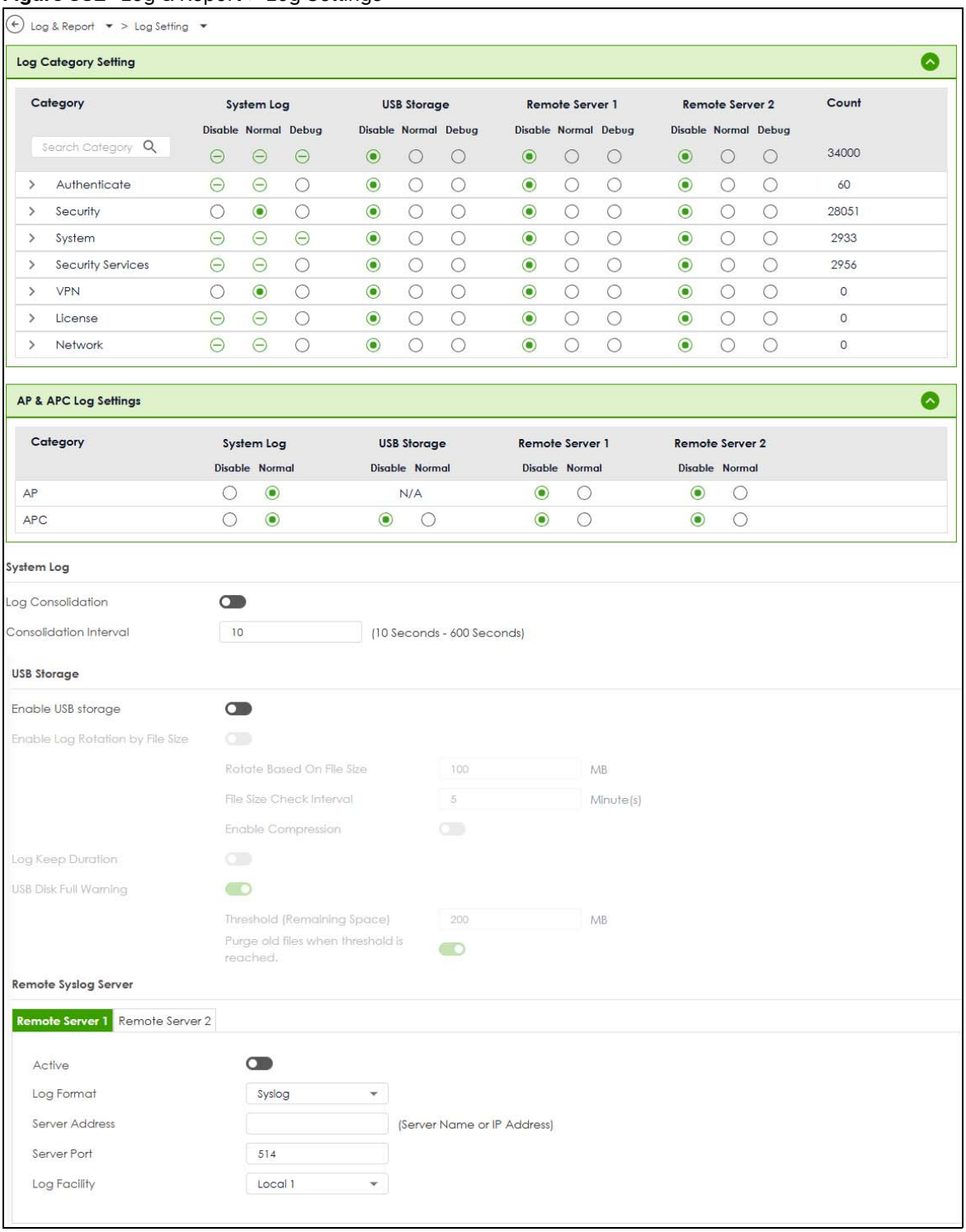
31.3 Log Settings Screen

The **Log Settings** screen control log messages. A log message stores the information for viewing or regular emailing later.

The Zyxel Device provides a system log and supports email profiles and remote syslog servers. 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 two logs are stored on specified syslog servers.

To access this screen, click **Log & Report > Log Settings**.

Figure 382 Log & Report > Log Settings



The following table describes the labels in this screen.

Table 298 Log & Report > Log Settings

LABEL	DESCRIPTION
Log Category Setting	Select which events you want to log for the Zyxel Device by **Category**. There are three choices: **Disable** - do not log any information from this category **Normal** - create log messages and alerts from this category **Debug** - 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.
AP & APC Log Settings	Select which events you want to log for the AP and APC by **Category**. There are two choices: **Disable** - do not log any information from this category **Normal** - create log messages and alerts from this category.
System Log	
Log Consolidation	Enable this to activate log consolidation. Log consolidation aggregates multiple log messages that arrive within the specified **Consolidation Interval**. In **Log Category Setting**, the **Count** field is the number of original log messages when multiple log messages were aggregated.
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 in the **Count** field in **Log Category Setting**.
USB Storage	
Enable USB Storage	Enable this if you want to use a connected USB device. The USB log file is saved as YYYY-MM-DD.log where YYYY-MM-DD is the current system date. Note: The Zyxel Device supports USB file systems FAT16, FAT32, EXT3, and EXT4. Note: The USB device must use MBR mode (Master Boot Record). It cannot have multiple partitions (GUID Partition Table). You can remove a USB stick and replace it with a new one for new logs while the Zyxel Device is on.
Enable Log Rotation by File Size	Use this to maximize the size of a file containing logs on the USB stick. Any number of files, each up to the maximum size, can be saved to the USB stick daily. 'Rotated' log files, for example, 2025-01-03.log.1, 2025-01-03.log.2. etc., are also saved to the USB stick.
Rotate Based On File Size	Set the maximum size of a file containing logs on the USB stick. For example, if you set this to 100MB, and the 2025-01-03.log file exceeds 100MB, then the contents of 2025-01-03.log is moved to 2025-01-03.log.1, so that logs can be added to 2025-01-03.log again. If the 2025-01-03.log.1 already exists, then 2025-01-03.log.1 is renamed to 2025-01-03.log.2, and its content is then moved from 2025-01-03.log to 2025-01-03.log.1.
File Size Check Interval	Set how often to check log file sizes on the USB stick. The range is from 1 to 360 minutes. The default is 5 minutes.
Enable Compression	Enable this to gzip log files to reduce size. You will be able to save more log files to the USB stick, but you will have to have to unzip them first to perform analysis of the logs. 'Rotated' compressed log files, for example, 2025-01-03.log.1.gz, 2025-01-03.log.2.gz etc., are also saved on the USB stick.
Log Keep Duration	Set a number of days (1 to 365) that the Zyxel Device keeps a log file on the USB stick. When a log file exceeds the number of days set here, the file is deleted from the USB stick. When the USB stick is full, new logs are not sent to the USB stick until files are removed from there.
USB Disk Full Warning	Enable this to create a log when the available space on the USB stick connected to the Zyxel Device is below the specified threshold.
Threshold (Remaining Space)	Set the minimum size needed to save logs on the connected USB stick (100 to 9999) in MB. When the available space on the USB stick is below this value, a log will be created. The default value is 200 MB.

Table 298 Log & Report > Log Settings (continued)

LABEL	DESCRIPTION
Purge old file when reached threshold	If the available space on the USB stick is below the specified threshold, the oldest log files will be removed until the available space is above the threshold. Then, the new logs can be saved to the USB stick.
Remote Syslog Server	
Remote Server 1/2	
Active	Enable this to send log information according to the information in this section.
Log Format	This field displays the format of the log information. It is read-only. **Syslog** - 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.
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.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

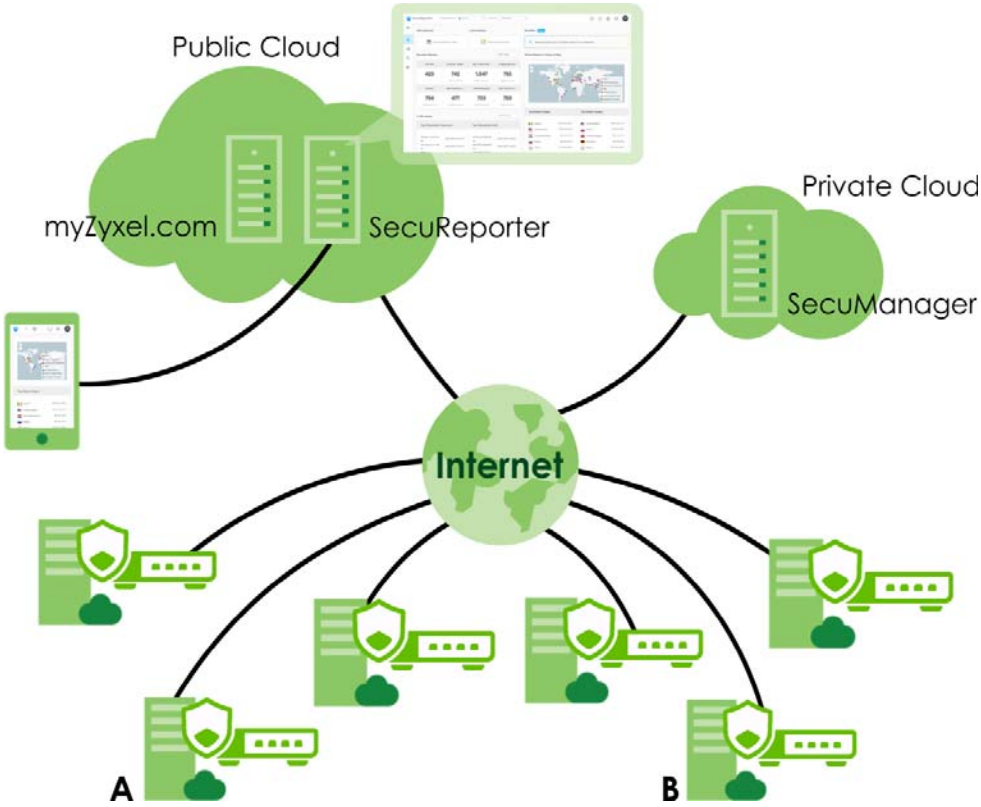
31.4 SecuReporter

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 NCC.

If a license has expired, you will see a reminder in this screen. You need to renew the license in order to keep using the feature. Click **Buy Now** to go to Marketplace to purchase a new license. Click **See Details** to go to the Zyxel web page to find more information on licenses for your Zyxel Device.



Figure 383 SecuReporter Application Scenario



How to activate and enable SecuReporter

1 If SecuReporter **Service Status** does not display **Activated**, you have to log in to NCC and activate the SecuReporter license for this Zyxel Device. The Zyxel Device must be able to communicate with the NCC server.

2 After the SecuReporter license is activated, go back to the **Log & Report** > **SecuReporter** screen, and select the categories of logs that you want this Zyxel Device to send to the SecuReporter portal.

3 Slide the switch to the right under **General Settings** to enabled 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

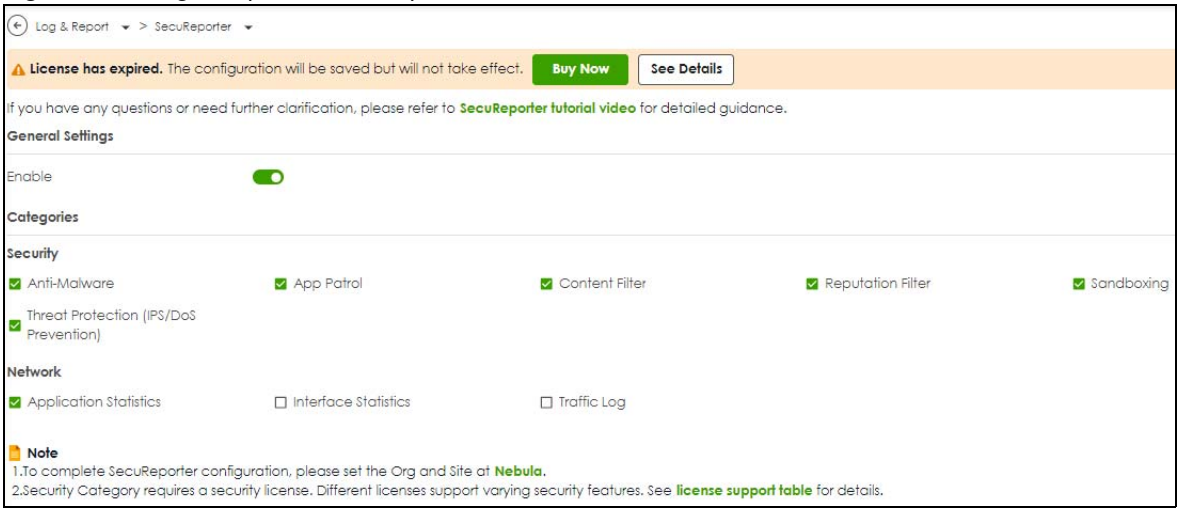
1 Log in to the SecuReporter portal.

2 Go to **More** > **Organization & Devices**, click **Add Organization** to create an organization.

3 Add this Zyxel Device to the organization you created using the hyper link under **Unclaimed**.

Click **Log & Report** > **SecuReporter** to open the following screen.

Figure 384 Log & Report > SecuReporter



The following table describes the labels in this screen.

Table 299 Log & Report > SecuReporter

LABEL	DESCRIPTION
Enable	This must be enabled to have SecuReporter collect and analyze logs from this Zyxel Device. Click **SecuReporter tutorial video** to go to YouTube to see related configuration videos. It's selected by default if you have activated a SecuReporter license.
Categories	Select the categories of logs that you want this Zyxel Device to send to SecuReporter for analysis and trend spotting. You need an active license for the **Security** categories.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

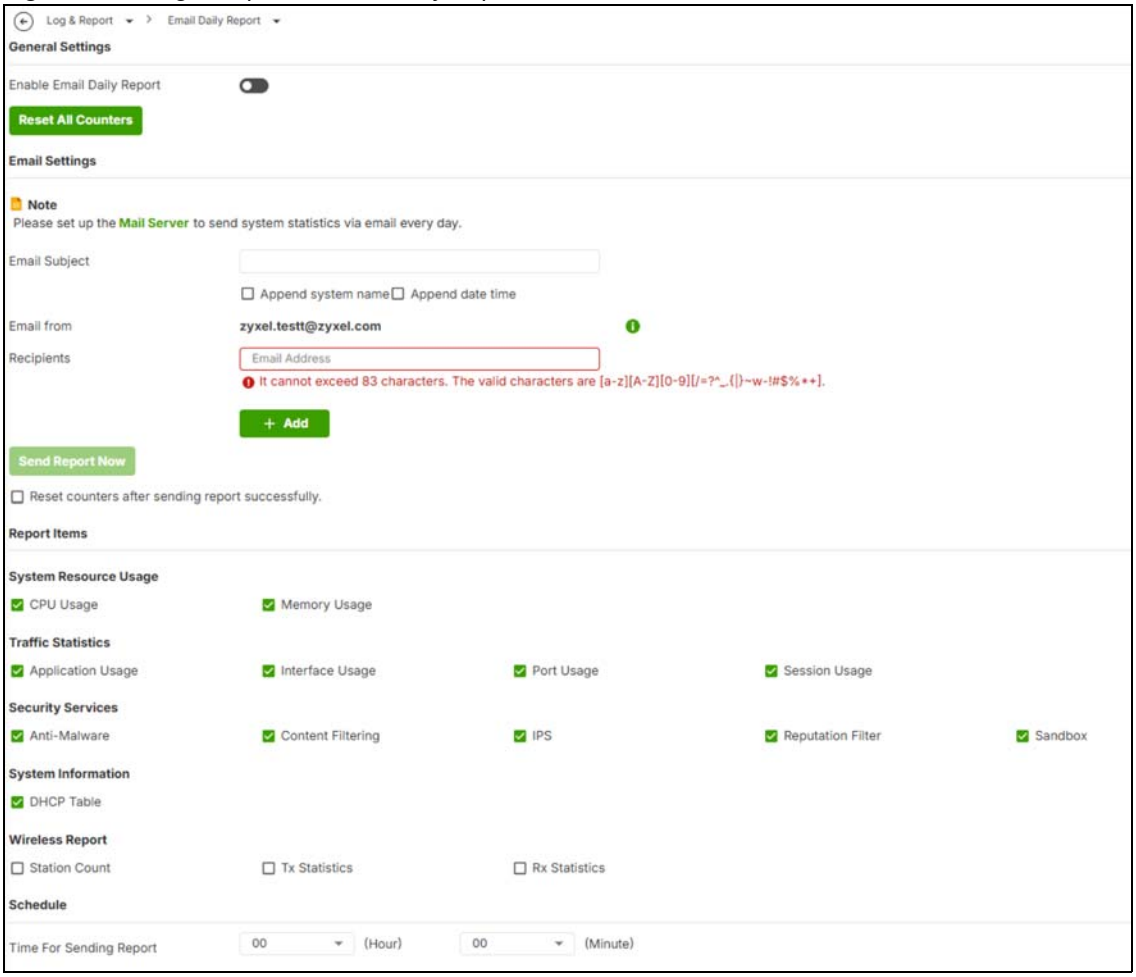
31.5 Email Daily Report

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 **Log & Report > Email Daily Report** to display the following screen. Configure this screen to have the Zyxel Device email you system statistics at the specified time.

Figure 385 Log & Report > Email Daily Report



The following table describes the labels in this screen.

Table 300 Log & Report > Email Daily Report

LABEL	DESCRIPTION
Enable Email Daily Report	Select this to send reports by email every day.
Reset All Counters	Click this to discard all report data and start all of the counters over at zero.
E-mail Subject	Enter the subject line for outgoing email from the Zyxel Device. Enter a string using up to 60 of these characters [a-zA-Z0-9'()+,./:=?;!#@$_%-]. • Select **Append system name** to add the Zyxel Device's system name to the subject. • Select **Append date time** to add the Zyxel Device's system date and time to the subject.
E-mail From	Enter the email address from which the outgoing email is sent.
Recipients	Enter the email address (or addresses) to which outgoing emails will be delivered. Click **+Add** to add more email addresses as recipients.
Send Report Now	Click this button to have the Zyxel Device send the daily email report immediately. Check your spam mail folder if you cannot receive the report.
Reset counters after sending report successfully	Select **Reset counters after sending report successfully** if you only want to see statistics for a 24 hour period.

Table 300 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**, **Traffic Statistics**, **Security Services, System Information,** and **Wireless Report**. Note: The **Port Usage** report includes data for all ports. The **Interface Usage** report includes only the interface data selected in the **Monitor Interface** field on the **Traffic Statistics > Interface** screen.
Schedule	Select the time of the day the report is emailed.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

31.5.1 Example Reports

The following screens are an example of a email daily report.

Figure 386 Email Daily Report: System Resource Usage

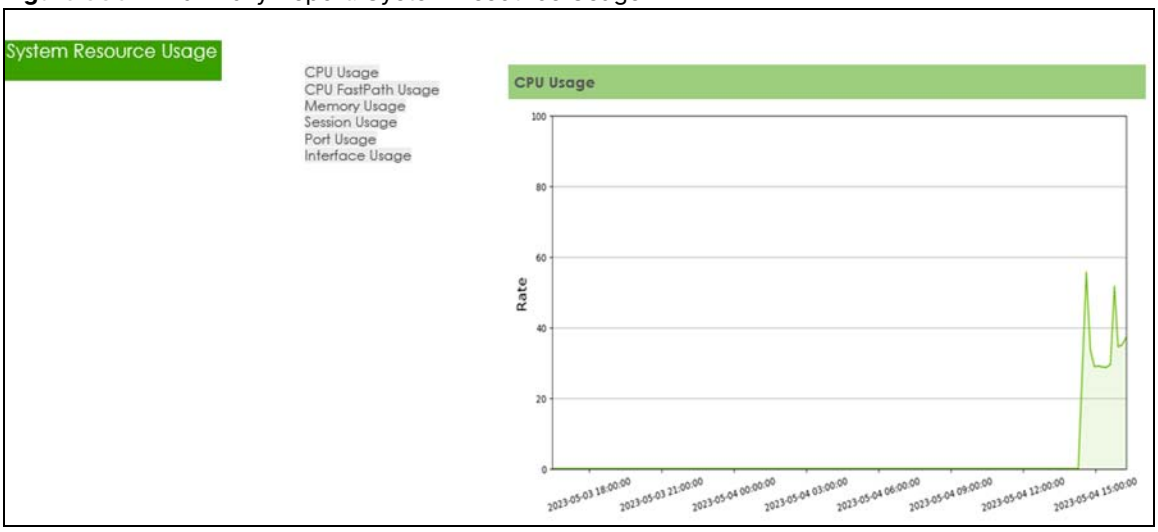


Figure 387 Email Daily Report- Licensing

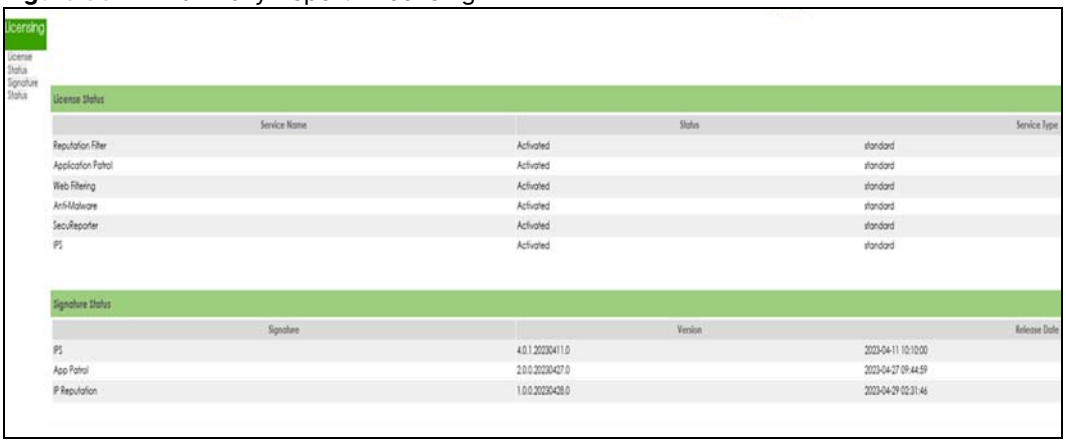


Figure 388 Email Daily Report: Threat Report

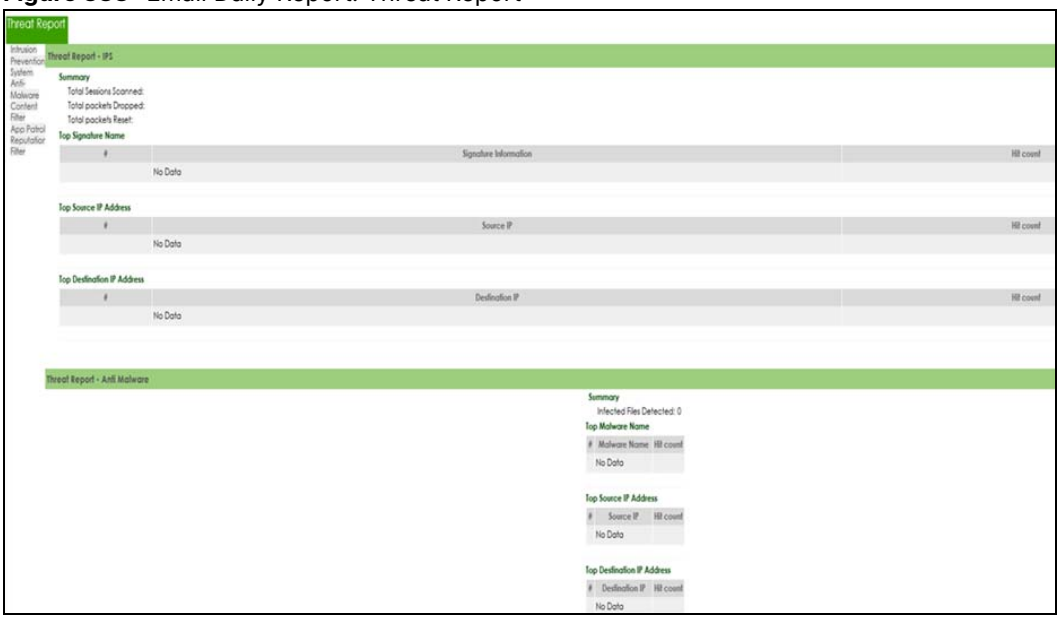


Figure 389 Email Daily Report: DHCP Table

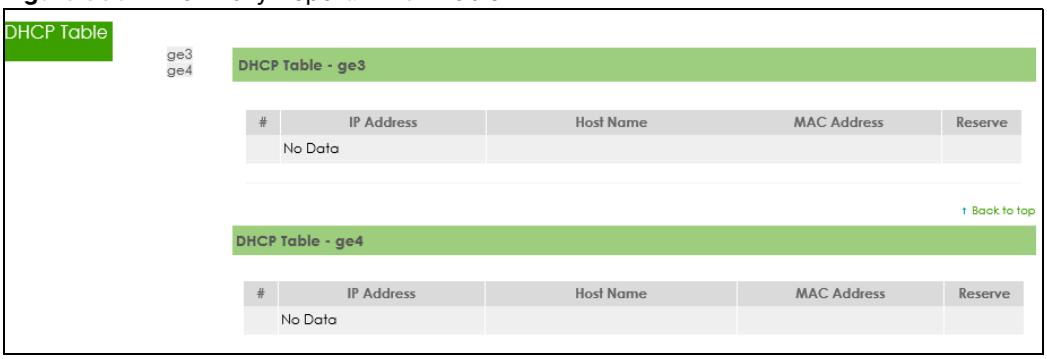
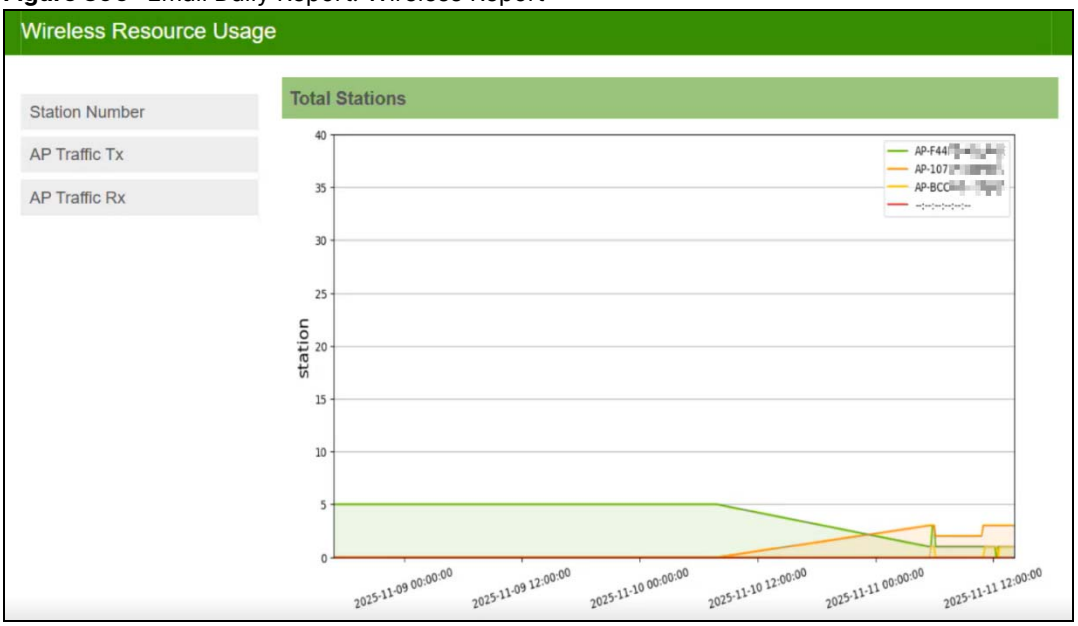


Figure 390 Email Daily Report: Wireless Report



CHAPTER 32
Firmware/File Manager

32.1 Overview

Configuration files define the Zyxel Device's settings. You can store multiple configuration files on the Zyxel Device. You can edit configuration files in a text editor and upload them to the Zyxel Device. Configuration files use a .conf extension.

32.1.1 What You Can Do in this Chapter

- Use the **Configuration File** screen (see Section 32.2 on page 657) 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 32.3 on page 666) to check your current firmware version and upload firmware to the Zyxel Device.
- Use the **CLI Script** screen (see Section 32.4 on page 669) to have the Zyxel Device execute the commands specified in a text file.

32.1.2 What you Need to Know

Configuration Files

When you apply a configuration file, the Zyxel Device uses the factory default settings for any features that the configuration file does not include. Other settings do not change.

The Zyxel Device applies configuration files in the following way:

- Reset to default configuration.
- Go into CLI **Configuration** mode.
- Run the commands in the configuration file.

Note: Device HA remains disabled even if you apply a configuration file in which Device HA is enabled. This prevents the Zyxel Device from becoming a passive (secondary) device.

Note: You cannot apply a configuration file when Device HA is enabled.

32.1.3 Configuration File Flow at Restart

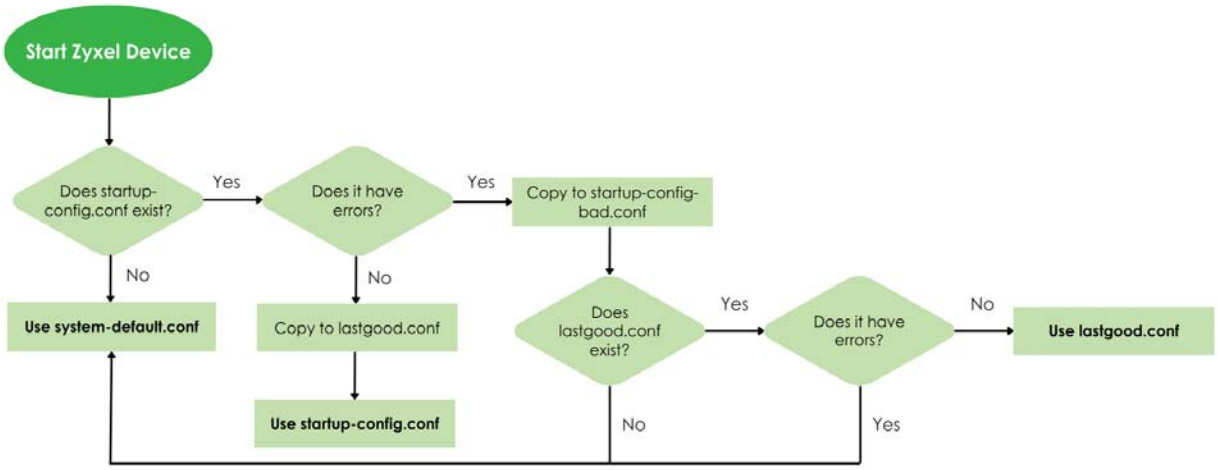
You can manually restart the Zyxel Device through a management interface or by physically turning the power off and back on.

The Zyxel Device restarts automatically when you upload new firmware.

The Zyxel Device always checks for errors in any configuration file when rebooting. The Zyxel Device generates a log for any errors.

- If there is not a **startup-config.conf** when you restart the Zyxel Device, the Zyxel Device uses the **system-default.conf** configuration file with the Zyxel Device's default settings. The Zyxel Device will apply the **system-default.conf** when it boots without a **startup-config.conf**, even if you have a **lastgood.conf**.
- 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 also copies it to the **lastgood.conf** configuration file as a back up file.
- If there is an error in **startup-config.conf**, the Zyxel Device generates a log and copies **startup-config.conf** to **startup-config-bad.conf** and then 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.

Figure 391 Zyxel Device Start-up Flow



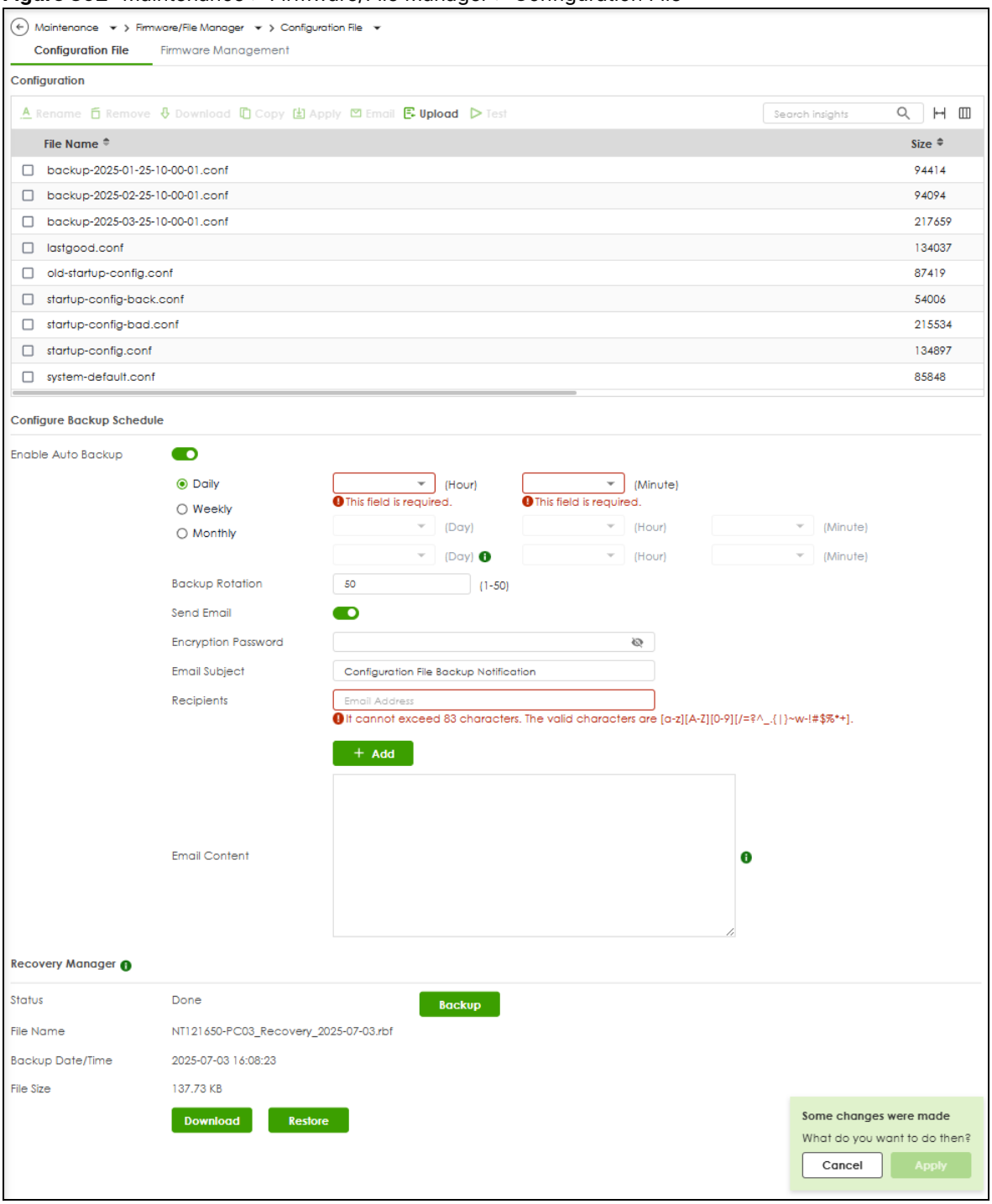
32.2 The Configuration File Screen

Click **Maintenance > Firmware/File Manager> Configuration File** to open the **Configuration File** 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.

Figure 392 Maintenance > Firmware/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 301 Maintenance > Firmware/File Manager > Configuration File

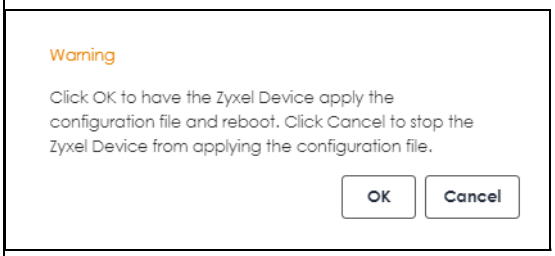
LABEL	DESCRIPTION
Configuration	
Rename	Use this button to change the label of a configuration file on the Zyxel Device. You can only rename manually saved configuration files. You cannot rename the **lastgood.conf**, **system-default.conf** and **startup-config.conf** files. You cannot rename a configuration 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. Specify the new name for the configuration file. Use up to 63 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the renamed label or click (✕) to close the screen without saving the renamed label.
Remove	Click a configuration file's row to select it and click **Remove** to delete it from the Zyxel Device. You can only delete manually saved configuration files. You cannot delete the **system-default.conf**, **startup-config.conf** and **lastgood.conf** files. A pop-up window asks you to confirm that you want to delete the configuration file. Click **OK** to delete the configuration file or click **Close** to close the screen without deleting the configuration file.
Download	Click a configuration file's row to select it and click **Download** to save the configuration into your computer.
Copy	Use this button to save a duplicate of a configuration file on the Zyxel Device. Click a configuration file's row to select it and click **Copy** to open the **Copy File** screen. Specify a name for the duplicate configuration file. Use up to 63 characters, including [a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-]. Click **OK** to save the duplicate or click (✕) 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 following screen displays. Click **OK** to have the Zyxel Device start applying the configuration file or click **Cancel** to close the screen.  An error message appears if the Zyxel Device fails to apply the selected configuration file. To view detailed error information, click the link to go to the **Diagnostics > System Log** screen and download the **apply-config-error.log** file. Contact customer support if the issue cannot be resolved. Note: This button is not available when **Device HA** is enabled. To apply a configuration file, first disable **Device HA** in **System** > **Device HA** > **HA Configuration**.

Table 301 Maintenance > Firmware/File Manager > Configuration File (continued)

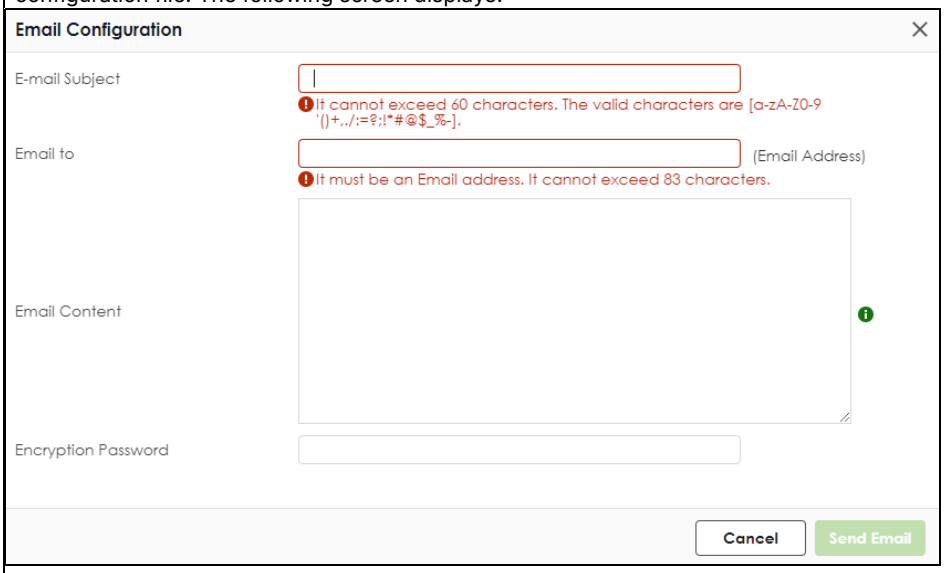
LABEL	DESCRIPTION
Email	Use this button to have the Zyxel Device send the selected configuration file to a valid email address. Click a configuration file's row to select it and click **Email** to have the Zyxel Device mail that configuration file. The following screen displays. 
E-mail Subject	Enter a email subject text with 1-60 characters. It may consist of letters, numbers, and the following special characters: '()+,./:=?;!*#@$%-
Email To	Enter up to 83 characters for the email address of the receiver.
Email Content	Enter the backup email body text using 1 to 251 single-byte characters, including [0-9a-zA-Z!"#$%&'()*+,-./:;<=>@[\]^_'{|}] and spaces are allowed. ? is not allowed.
Encryption Password	Configuration files are zipped when they are emailed. For security, enter an unzip password to require the recipient to use this password to unzip the configuration file. The password cannot exceed 128 characters. Valid characters are [0-9a-zA-Z~!@#$%^&*()_-+={}|;:<>,./]. If you do not set a password here, then none is needed to unzip the configuration file.
Send Email	Click this to send the email to the email address you configured.
Cancel	Click this to close the screen.
Upload	Click this 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**, **startup-config.conf** or **lastgood.conf**.
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.
Cancel	Click this to close the screen.

Table 301 Maintenance > Firmware/File Manager > Configuration File (continued)

LABEL	DESCRIPTION
Test	Before applying a configuration file to the Zyxel Device, you can select the file and click **Test** to check if the configuration file has errors. **Configuration Test: Pass** - The configuration file is correct. **Configuration Test: Fail** - An error was found in the configuration file. Applying a configuration file with errors may cause malfunctions in your Zyxel Device. To view detailed error information, click the link to go to the **Diagnostics > System Log** screen and download the **apply-config-error.log** file. Contact customer support if errors cannot be solved. Note: Make sure **startup-config.conf** does not have an error before you restart the Zyxel Device or upload new firmware.
File Name	This column displays the label that identifies a configuration file. You cannot change the following configuration files 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.
Configure Backup Schedule	Backups created by a schedule are given an automatic name by the Zyxel Device. The name of a scheduled backup file follows this format: 'backup-yyyy-mm-dd-hh-mm-ss'.conf. To restore a configuration file, click **Upload** to upload the file, then select the file and click **Apply** to apply the file to the Zyxel Device.
Enable Auto Backup	Select the check box to back up the running (current) configuration file automatically at a scheduled time. Note: After the first backup, subsequent back ups only occur if the configuration file is different from the previous backed up configuration file.
Daily	Set the Zyxel Device to back up its current configuration file once a day at the specified hour and minute.
Weekly	Set the Zyxel Device to back up its current configuration file once a week on the specified day, at the specified hour and minute.
Monthly	Set the Zyxel Device to back up its current 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.
Backup Rotation	Use this field to have a newer backup replace the oldest backup when the number you enter here is reached. Enter a number from 1 to 50. For example, if you use 50, then the 51st backup configuration file will replace the first configuration file. You will always have a maximum of 50 backup configuration files.

Table 301 Maintenance > Firmware/File Manager > Configuration File (continued)

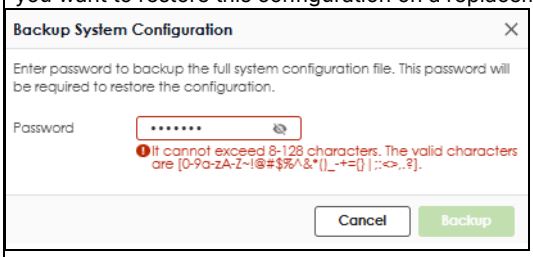
LABEL	DESCRIPTION
Send Email	Enable this to send the backed up configuration file to the email address(es) you configured.
Encryption Password	For security, enter a password for the recipient to unzip the compressed backup configuration file. Use 1 to 128 characters. [" \] are invalid.
E-mail Subject	Enter a email subject text with 1-60 characters. It may consist of letters, numbers, and the following special characters: '()+,./:=?;!*#@$%-
Email To	Enter up to 83 characters for the email address of the receiver. You and send the configuration file to a maximum of five recipients.
Email Content	Enter the backup email body text using 1 to 251 single-byte characters, including 0-9a-zA-Z!"#$%&'()*+,-./:;<=>@[\]^_'{|} and spaces are allowed. ? is not allowed.
Recovery Manager	Use this to create a complete recovery file of the Zyxel Device that can be used if the Zyxel Device needs to be replaced or you want to sell it to someone else. You should save a backup or recovery file to your computer each time you make a configuration change. The recovery file can then be restored on a replacement Zyxel Device. You must set a password for the recovery file. The password must be 8 to 128 characters long, and can contain [0-9a-zA-Z~!@#$%^&*()_-+={}|;:<>,.?]. Write this password down in a safe place as it will be required if you want to restore this configuration on a replacement Zyxel Device later.  The Zyxel Device automatically names the recovery file to 'Hostname_Recovery_YYYY-MM-DD.rbf', where YYYY-MM-DD is the date created. This is an example file name: 'MyUSGFLEX500H_Recovery_2025-07-28.rbf'. You set the **Host Name** for this Zyxel Device in **System > Settings**. You can only upload recovery files with an '.rbf' extension. The recovery file includes the following: **Configuration files** Contains all configuration files from the **Maintenance** > **Firmware/File Manager** > **Configuration File** screen. **Certificates** • My Certificates (Site-to-Site VPN, Remote access VPN) • SSL VPN Certificates • Trusted Certificates: Certificates that you have set the Zyxel Device to accept as trusted. **Google Authenticator File** Contains two-factor authentication (2FA) information. Google Authenticator adds an extra layer of security for local users accessing the Zyxel Device or a secured network behind the Zyxel Device through a VPN tunnel.

Table 301 Maintenance > Firmware/File Manager > Configuration File (continued)

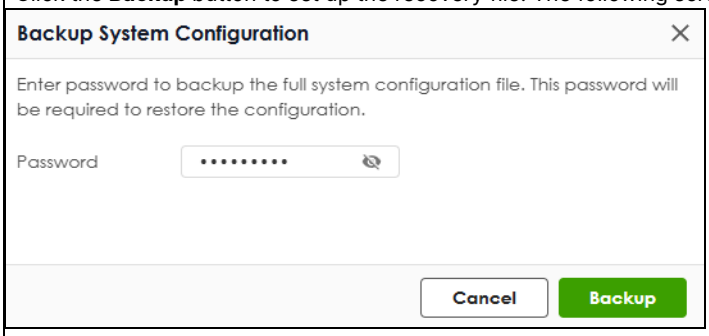
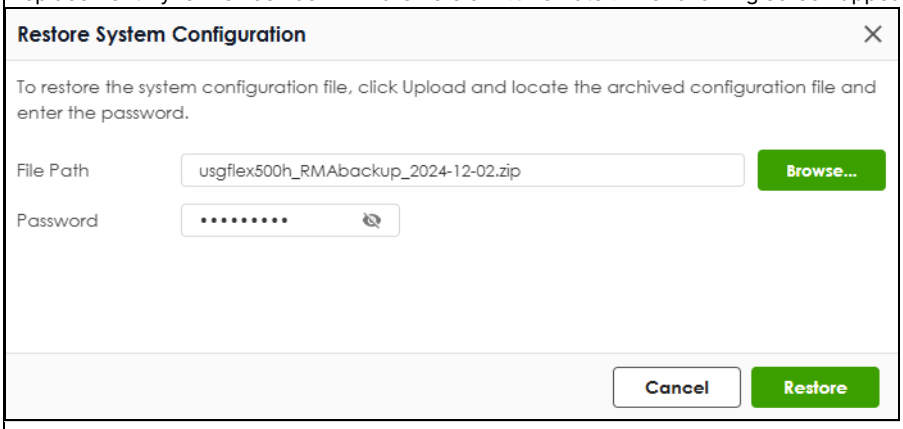
LABEL	DESCRIPTION
Status	This displays the status of the file backup. You must first back up the file to the Zyxel Device and then download it to your computer. This recovery file does not display in the **Configuration** list. • **Done** - The recovery file has been successfully saved to the Zyxel Device. • **None** - No backup of the recovery file has been made. • **Failed** - The backup of the recovery file failed. Ensure the Internet is working. Click the **Backup** button to set up the recovery file. The following screen appears. 
Password	Enter a password for the recovery file. You will need this password to restore the recovery file on the replacement Zyxel Device. It can contain 8 to 128 single-byte characters, including 0-9, a-z, A-Z, and the following characters: ~!@#$%^&*()_-+={}|;:<>,.? Spaces are not allowed. This field cannot be blank.
Cancel	Click **Cancel** to exit this screen without saving.
Backup	Click **Backup** to save the recovery file to the Zyxel Device.
File Name	This displays the name of the recovery file that will be downloaded to your computer. You can rename the file when you are saving it to your computer.
Backup Date/Time	This field displays the date and time when the recovery file was saved to the Zyxel Device. The format is yyyy-mm-dd hh:mm:ss.
File Size	This field displays the file size of the recovery file that will be downloaded to your computer.
Download	Click **Download** to save the backup file to your computer in ZIP format.
Restore	Click **Restore** to upload a recovery file to the replacement Zyxel Device. Check that the replacement Zyxel Device has firmware version 1.31 or later. The following screen appears.  Note: The replacement Zyxel Device must be the same model with the exact same firmware version as the one on which the backup was done. You must use the password that you configured when you downloaded the recovery file.
File Path	Click **Browse** to select a recovery file on your computer that you want to upload.
Password	Enter the password for the recovery file created during the backup.

Table 301 Maintenance > Firmware/File Manager > Configuration File (continued)

LABEL	DESCRIPTION
Cancel	Click **Cancel** to exit this screen without saving.
Restore	Click **Restore** to upload the recovery file to the replacement Zyxel Device. The Zyxel Device automatically reboots when you apply the new recovery file.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

32.2.1 Example: Back Up and Restore Zyxel Device Configuration

It is recommended that you back up your configuration file before making further configuration changes. This ensures you can restore to previous device settings if new changes cause problems.

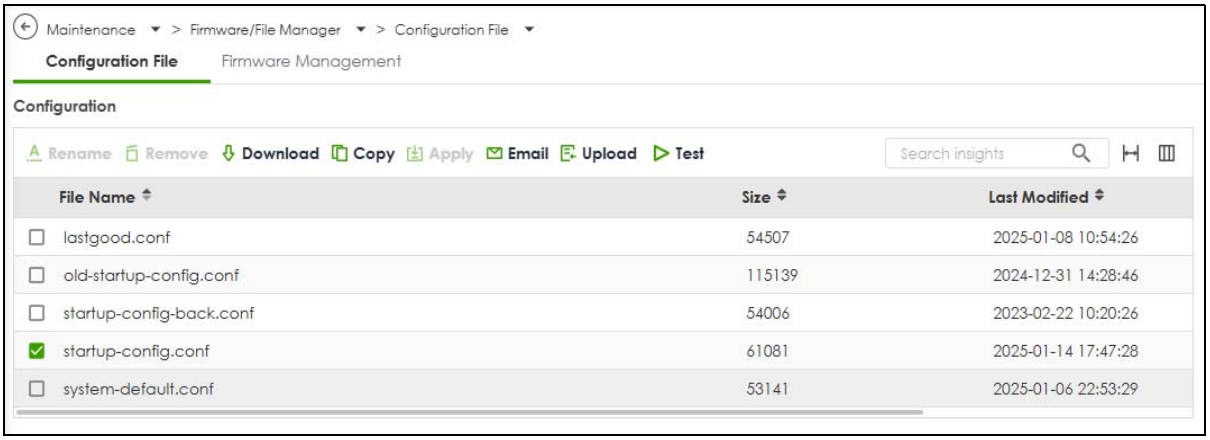
Here are the default configuration files on the Zyxel Device:

- The **system-default.conf** file is the configuration file that resets all of the Zyxel Device settings to the factory defaults.
- The **startup-config.conf** file is the configuration file that the Zyxel Device is currently using.
- The **lastgood.conf** is the most recently used (valid) configuration file that was saved when the device last restarted.

Back Up the Current Configuration

Follow these steps to save the current configuration file from the Zyxel Device to your computer:

1 Go to **Maintenance** > **Firmware/File Manager**, select **startup-config.conf,** and click **Download** to save the configuration file to your computer.

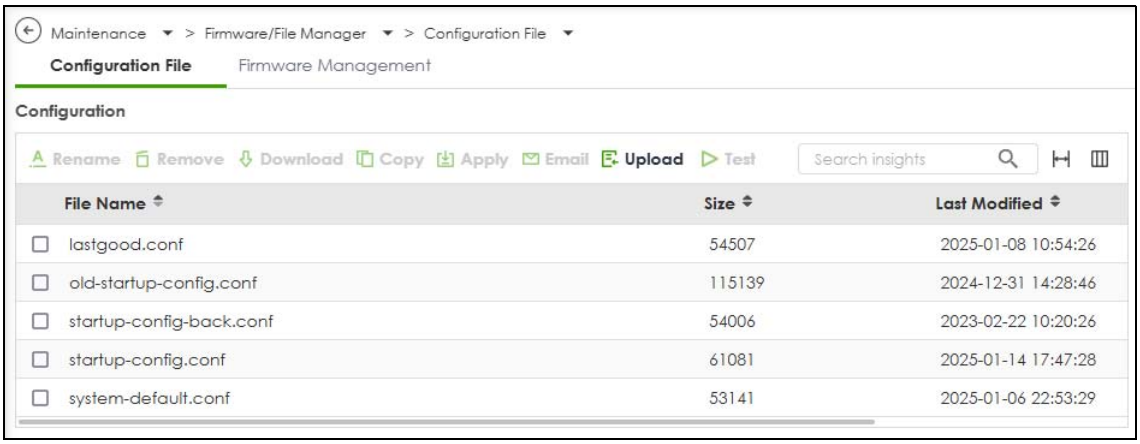


2 Rename the downloaded configuration file with the current date.

Upload a Configuration File to the Zyxel Device

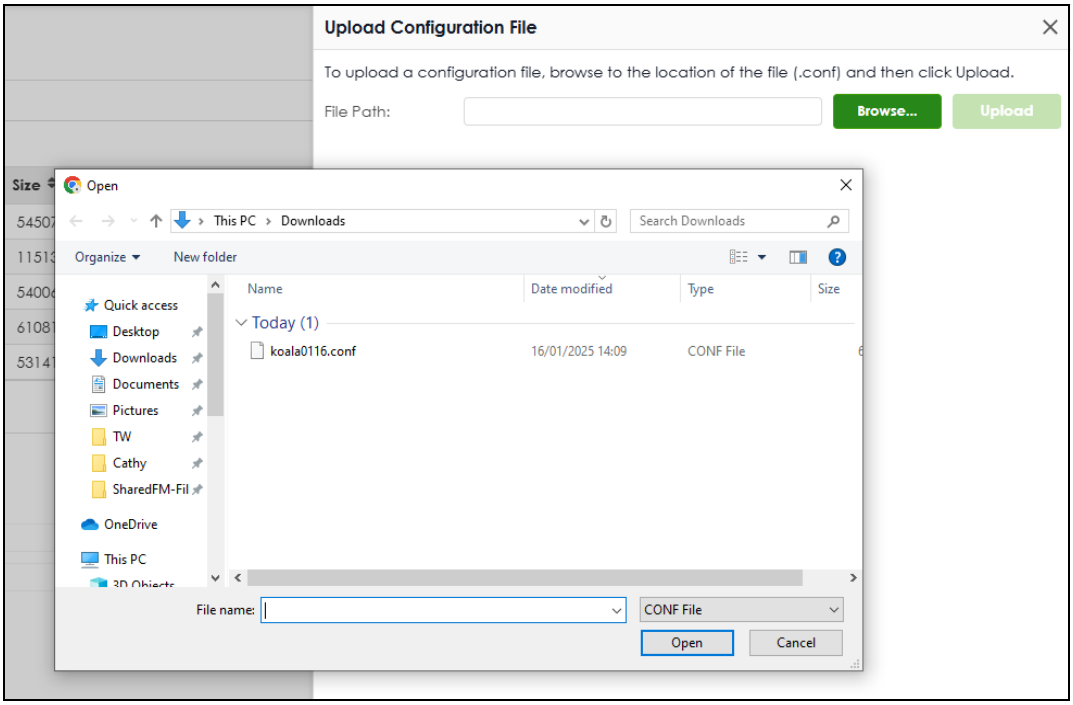
Follow these steps to upload a previously saved configuration file from your computer to the Zyxel Device:

1 Go to **Maintenance** > **Firmware/File Manager** and click **Upload**.

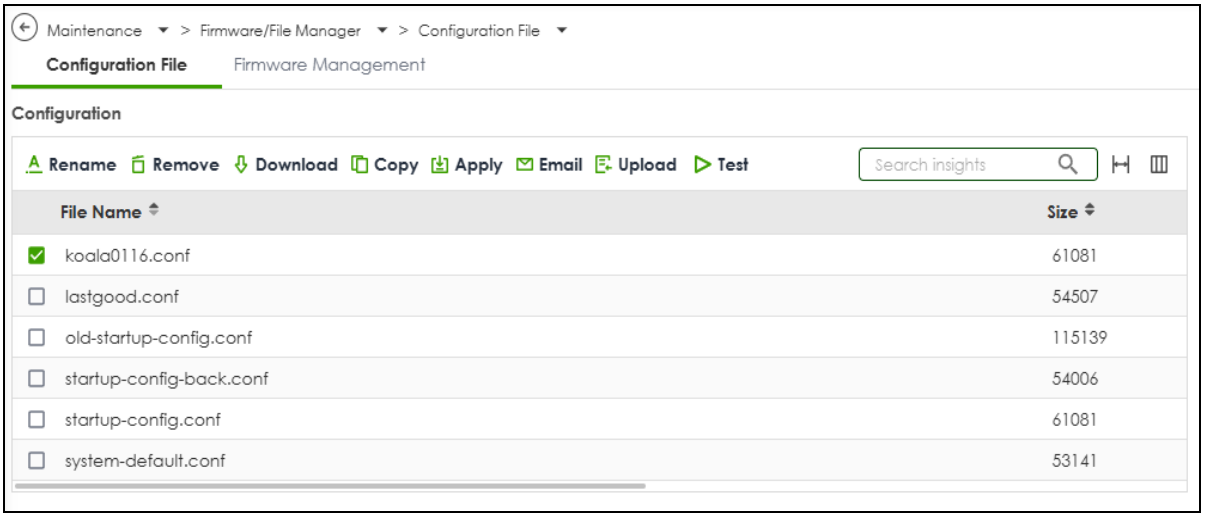


2 Click **Browse...** to locate the .conf file on your computer to restore, then click **Upload**.

Note: The configuration file must have a ".conf" filename extension. You cannot upload a file named **system-default.conf**, **startup-config.conf**, or **lastgood.conf**.



3 Select the configuration file and click **Apply** to have the Zyxel Device use the configuration file.



32.3 Firmware Management

Use the **Firmware Management** screen to check your current firmware version and upload firmware to the Zyxel Device.

Note: The Web Configurator or NCC 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 USG FLEX 200HP is “100ABEX0b3s1.bin”.

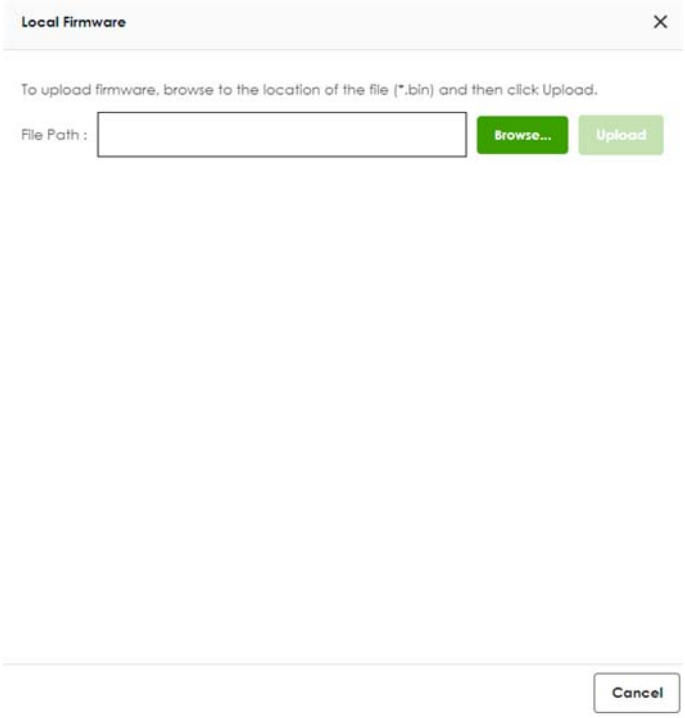
Note: The Zyxel Device restarts automatically when you upload new firmware.

32.3.1 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 NCC, create an account and register your Zyxel Device first. Then you will be able to get notifications on new firmware available when you log into the Zyxel Device web configurator.

Table 302 Cloud Helper Firmware Icons

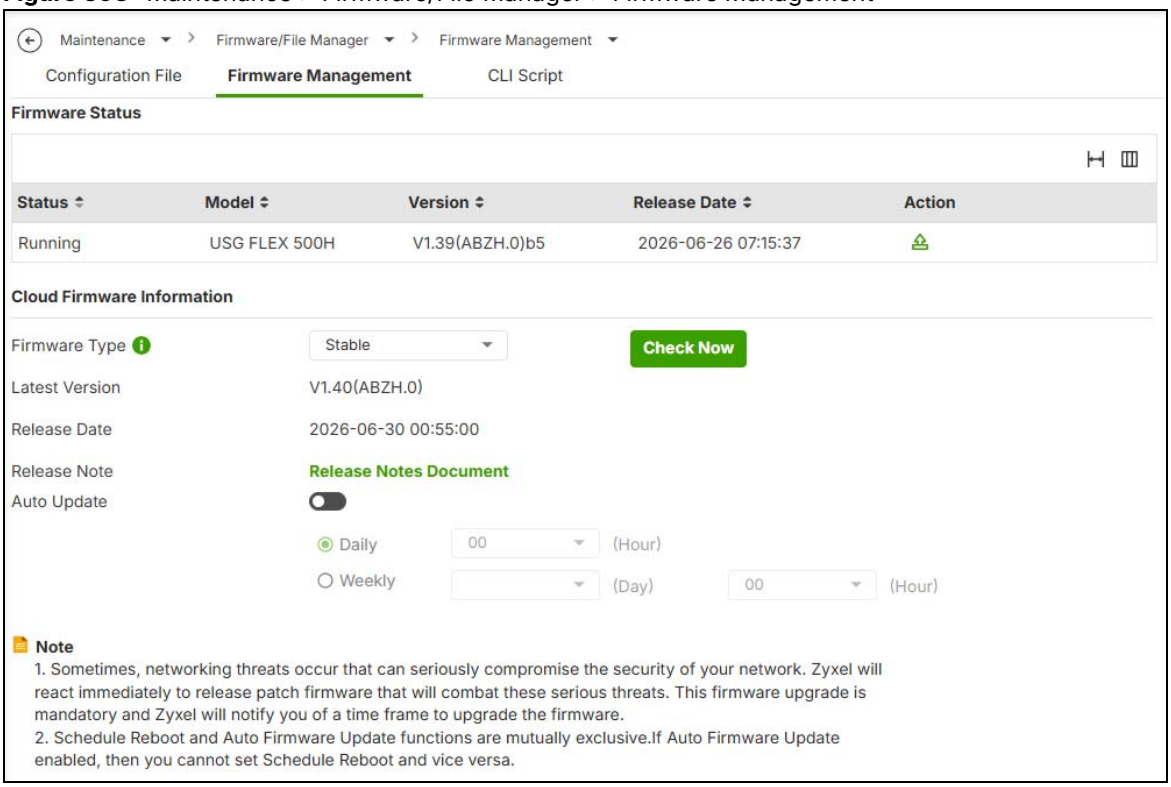
Cloud Firmware 	Cloud firmware is being downloaded from the Cloud Helper Server.
Local Firmware 	Use this if you have already downloaded the latest firmware from the Zyxel website to your computer and unzipped it. Click the icon and then browse to the location of the unzipped files.  The Zyxel Device will reboot automatically when it finishes uploading.

32.3.2 The Firmware Management Screen

Click **Maintenance > Firmware/File Manager > Firmware Management** to open the **Firmware Management** screen.

Note: The Zyxel Device automatically reboots when you upload new firmware.

Figure 393 Maintenance > Firmware/File Manager > Firmware Management



The following table describes the labels in this screen.

Table 303 Maintenance > Firmware/File Manager > Firmware Management

LABEL	DESCRIPTION
Status	This displays the running firmware status.
Model	This is the model name of the device which the firmware is running on.
Version	The firmware on each Zyxel Device is identified by the firmware trunk version, followed by a unique code which identifies the model, and then the release number after the period. For example, V1.31 (ABXE.0) is a firmware for the 1.31 version trunk, the ABXE code identifies the USG FLEX 200HP model, and .0 is the first firmware release for the model.
Released Date	This is the date that the version of the firmware was created.
Action	Click ( ) to upload a firmware from your computer to the Zyxel Device. Click **Upload** to upload the firmware as the running firmware after the Zyxel Device reboots. Your current configuration settings will be saved and applied after reboot. Click ( ) to download a later firmware from the Cloud Helper Server. This icon shows if there is a later firmware on the Cloud Helper Server than the running firmware on your Zyxel Device.
Cloud Firmware Information	You must register your Zyxel Device at NCC first to use cloud firmware.
Firmware Type	Use this to check if there is a later firmware of the selected type on the Cloud Helper Server. • The **Latest** firmware is the most recent officially released firmware that has undergone extensive internal testing. It has the most advanced firmware features and fixes - see the Release notes. • A **Stable** firmware is a previously released firmware that has undergone extensive internal testing, and has also been used by customers with no major issues reported. Use this if you do not need the most advanced firmware features at this time.
Latest Version	This displays the latest firmware version of the selected type (**Latest** or **Stable)** at the Cloud Helper Server. If the running firmware version is earlier than the version displayed here, then a cloud icon will display under **Action** in the above screen to take you to the Cloud Helper Server.

Table 303 Maintenance > Firmware/File Manager > Firmware Management (continued)

LABEL	DESCRIPTION
Check Now	Click **Check Now** to see if there is a later firmware of the selected type (**Latest** or **Stable)** on the Cloud Helper Server.
Release Date	This displays the date the latest firmware of the selected type (**Latest** or **Stable)** was made available.
Release Note	The release note contains details of firmware of the selected type (**Latest** or **Stable)** such as new or changed features and bug fixes.
Auto Update	If you have not enabled **Schedule Reboot** in **Maintenance > Reboot/Shutdown**, you may use **Auto Update** in this screen to have the Zyxel Device automatically check for and download new firmware at a particular time each day, or at a particular time once a week. The Zyxel Device will automatically reboot after new firmware is downloaded. You should select a time when your network is not busy for minimal interruption. If you have enabled **Schedule Reboot** in **Maintenance > Reboot/Shutdown**, then you cannot use **Auto Update** in this screen.
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.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return the screen to its last-saved settings.

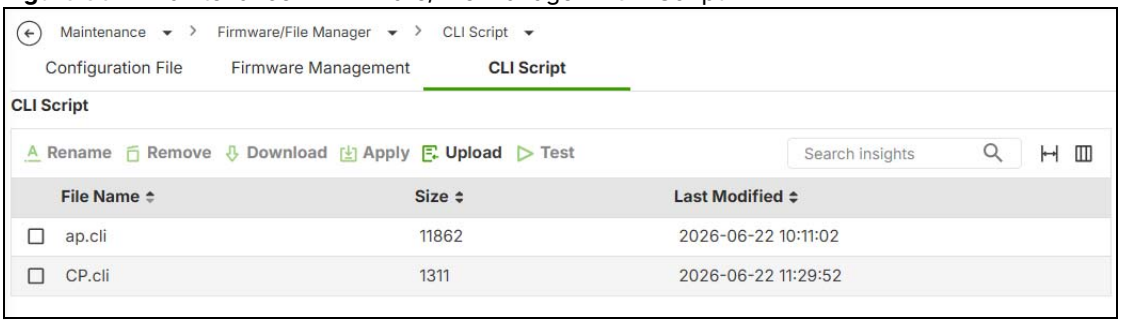
32.4 The CLI Script Screen

Use CLI script files to have the Zyxel Device execute commands that you specify. You can use a script file to apply multiple configuration commands at once.

Use a text editor to create CLI script files. The file must have a .cli extension. Refer to Section 32.4.1 on page 670 for script file command rules and examples.

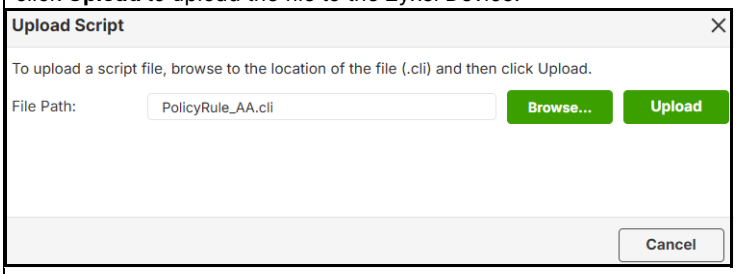
Click **Maintenance > Firmware/File Manager > CLI Script** to open the **CLI Script** screen.

Figure 394 Maintenance > Firmware/File Manager > CLI Script



The following table describes the labels in this screen.

Table 304 Maintenance > Firmware/File Manager > CLI Script

LABEL	DESCRIPTION
CLI Script	
Rename	Use this button to rename the selected uploaded script file. The file must have a .cli extension. Use up to 63 characters [0-9a-zA-Z~_=-]. Click a script file's row to select it and click **Rename**. Enter the new name in the **Target file** field. Click **OK** to save the renamed label or click **Cancel** to close the screen without saving the renamed label.
Remove	Use this button to delete the selected uploaded script file. A pop-up window asks you to confirm that you want to delete the script file. Click **OK** to delete the script file or click **Cancel** to close the screen without deleting the script file.
Download	Select an uploaded script file and click this button to download it to your computer.
Apply	Click this button to have the Zyxel Device execute the commands in the selected script file. An error message appears if the Zyxel Device fails to apply the selected script file. To view the error information, click the link to go to the **Diagnostics > System Log** screen and download the **apply-script-error.log** file.
Upload	Click this button to upload a specified script file. Click **Browse** to select the script file, and then click **Upload** to upload the file to the Zyxel Device.  • The file must have a .cli extension. • You can upload up to five files. • The file size cannot exceed 5 MB. • You cannot upload an empty file.
Test	Before applying a script file to the Zyxel Device, select the file and click this button to check for errors. **Test: Pass** - No error was found. **Test: Failed** - An error was found in the script file. You can click the link to go to the **Diagnostics > System Log** screen and download the **apply-script-error.log** file to view the error information.
File Name	This column displays the name of the script files.
Size	This column displays the size (in Bytes) of the script files.
Last Modified	This column displays the date and time that the script files were last changed or saved.

32.4.1 CLI Script File Command Rules and Examples

You can refer to the CLI RG for descriptions of Zyxel Device commands and how to use them.

Only configuration commands are supported. RPC (Remote Procedure Call) commands are not supported. You can use the **Test** button to check whether the commands in the script file are supported after uploading the file.

- Configuration commands modify or store the Zyxel Device configuration. For example: configure VLAN, set hostname.
- RPC commands send requests to the Zyxel Device and receive responses or perform actions without changing the configuration. For example: ping 8.8.8.8, reboot device.

Follow the rules below to specify commands in the script file.

Table 305 Command Rules

RULE	EXAMPLE
Start with / and a space	`/ vrf main interface ...`
Use # for comments	`# this is a comment`
Add `del` and a space before a command to delete configurations	`del / vrf main interface ethernet ge4` → Delete ge4 and all its settings `del / vrf main interface ethernet ge4 ports p7` → Delete only port p7 on ge4
Enclose values containing spaces in quotation marks.	`/ vrf main system hostname "my device"`

The following script file example shows how to add multiple interfaces along with their detailed configurations.

```
#VLAN100 for the sales team
/ vrf main interface vlan vlan100 vlan-id 10
/ vrf main interface vlan vlan100 type internal
/ vrf main interface vlan vlan100 enabled true
/ vrf main interface vlan vlan100 link-port p10
/ vrf main interface vlan vlan100 ipv4 address 192.168.10.1/24
/ vrf main interface vlan vlan100 mtu 1400

#VLAN200 for the IT team
/ vrf main interface vlan vlan200 vlan-id 20
/ vrf main interface vlan vlan200 type internal
/ vrf main interface vlan vlan200 enabled true
/ vrf main interface vlan vlan200 link-port p11
/ vrf main interface vlan vlan200 ipv4 address 192.168.20.1/24
/ vrf main interface vlan vlan200 mtu 1400

#VLAN300 for the guests
/ vrf main interface vlan vlan300 vlan-id 30
/ vrf main interface vlan vlan300 type internal
/ vrf main interface vlan vlan300 enabled true
/ vrf main interface vlan vlan300 link-port p12
/ vrf main interface vlan vlan300 ipv4 address 192.168.30.1/24
/ vrf main interface vlan vlan300 mtu 1400
```

CHAPTER 33 Diagnostics

33.1 Overview

Use the diagnostics screens for troubleshooting.

33.1.1 What You Can Do in this Chapter

- Use the **Diagnostics** screens (see Section 33.2 on page 672) 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 33.3 on page 674) to capture packets going through the Zyxel Device.
- Use the **CPU / Memory Status** screens (see Section 33.4 on page 678) to view the CPU and memory performance of various applications on the Zyxel Device.
- Use the **System Log** screen (see Section 33.5 on page 680) to view the files of diagnostic information the Zyxel Device has collected and stored on a connected USB storage device.
- Use the **Network Tool** screen (see Section 33.6 on page 681) to ping an IP address or trace the route packets take to a host.

33.2 The Diagnostics Screens

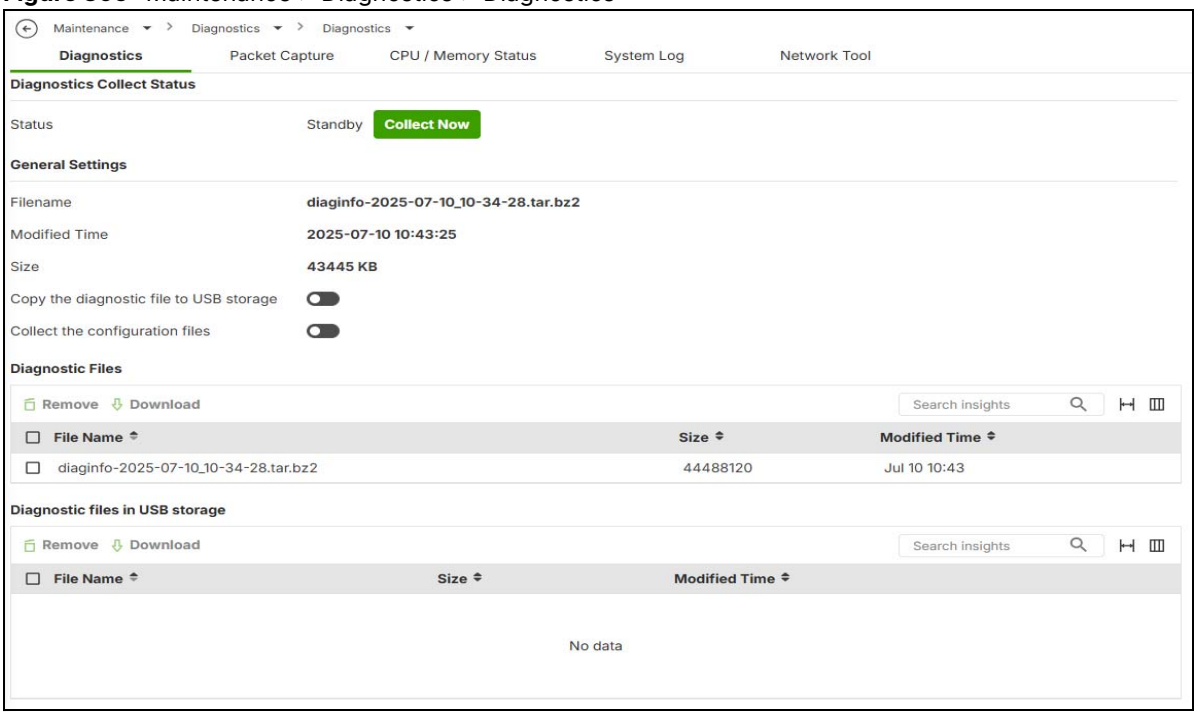
The **Diagnostics** screens provide an easy way for you to generate a file containing the Zyxel Device's configuration and diagnostic information. You may need to send this file to customer support for troubleshooting.

33.2.1 The Diagnostics Screen

Click **Maintenance > Diagnostics > Diagnostics** to open the following screen. When you click **Collect Now**, a series of commands are run to display information about the Zyxel Device.

This screen also 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 395 Maintenance > Diagnostics > Diagnostics



The following table describes the labels in this screen.

Table 306 Maintenance > Diagnostics > Diagnostics

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 device:** The Zyxel Device is generating a diagnostic file containing its own configuration and diagnostic information.
Collect Now	Click this to have the Zyxel Device run the uploaded script and create a new diagnostic file. Please wait until the collection finishes.
General Setting	
Filename	This is the name of the most recently created diagnostic file.
Modified Time	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	Select this to have the Zyxel Device create an extra copy of the diagnostic file to a connected USB storage device.
Collect the configuration files	Select this to include the configuration file currently used by the Zyxel Device in the generated diagnostic file.
Diagnostic files	This lists the most recently generated diagnostic file stored on the Zyxel Device. If there is insufficient flash storage space for the diagnostic file and **Copy the diagnostic file to USB storage** is enabled, the file is stored on the connected USB device. You can check the log under the **System** category in **Log & Report > Log / Events > System**.
Diagnostic files in USB storage	This lists the files of generated diagnostic information stored in a connected USB storage device.
Remove	Select files and click **Remove** to delete them from the Zyxel Device or the USB storage device.

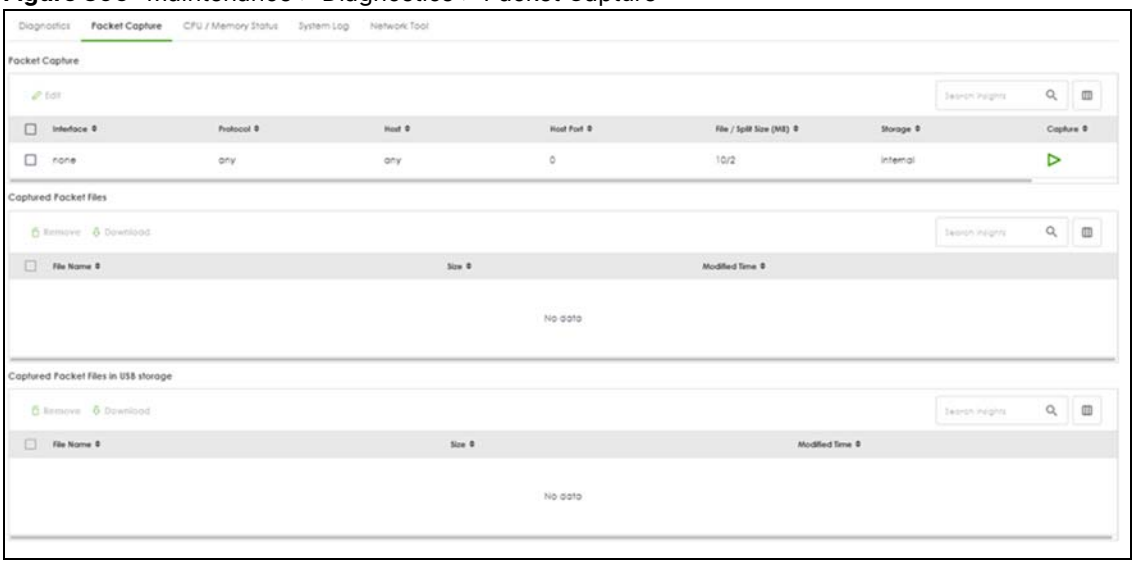
Table 306 Maintenance > Diagnostics > Diagnostics (continued)

LABEL	DESCRIPTION
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. A Zyxel Device diagnostic file name starts with “diaginfo”.
Size	This column displays the size (in bytes) of a file.
Modified Time	This column displays the date and time that the individual files were saved.

33.3 The Packet Capture Screen

Click **Maintenance > Diagnostics > Packet Capture** 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 396 Maintenance > Diagnostics > Packet Capture



The following table describes the labels in this screen.

Table 307 Maintenance > Diagnostics > Packet Capture

LABEL	DESCRIPTION
Edit	Click this to configure packet capture settings.
Interface	This field displays the interface for which to capture packets.
Protocol	This field displays the protocol of traffic for which to capture packets.
Host	this field displays the host IP address object for which to capture packets.
Host Port	This field displays the port number of traffic to capture.
File/Split Size (MB)	This field displays the maximum size limit in megabytes for individual packet capture files.
Storage	This field displays where the packet capture entry is saved.

Table 307 Maintenance > Diagnostics > Packet Capture

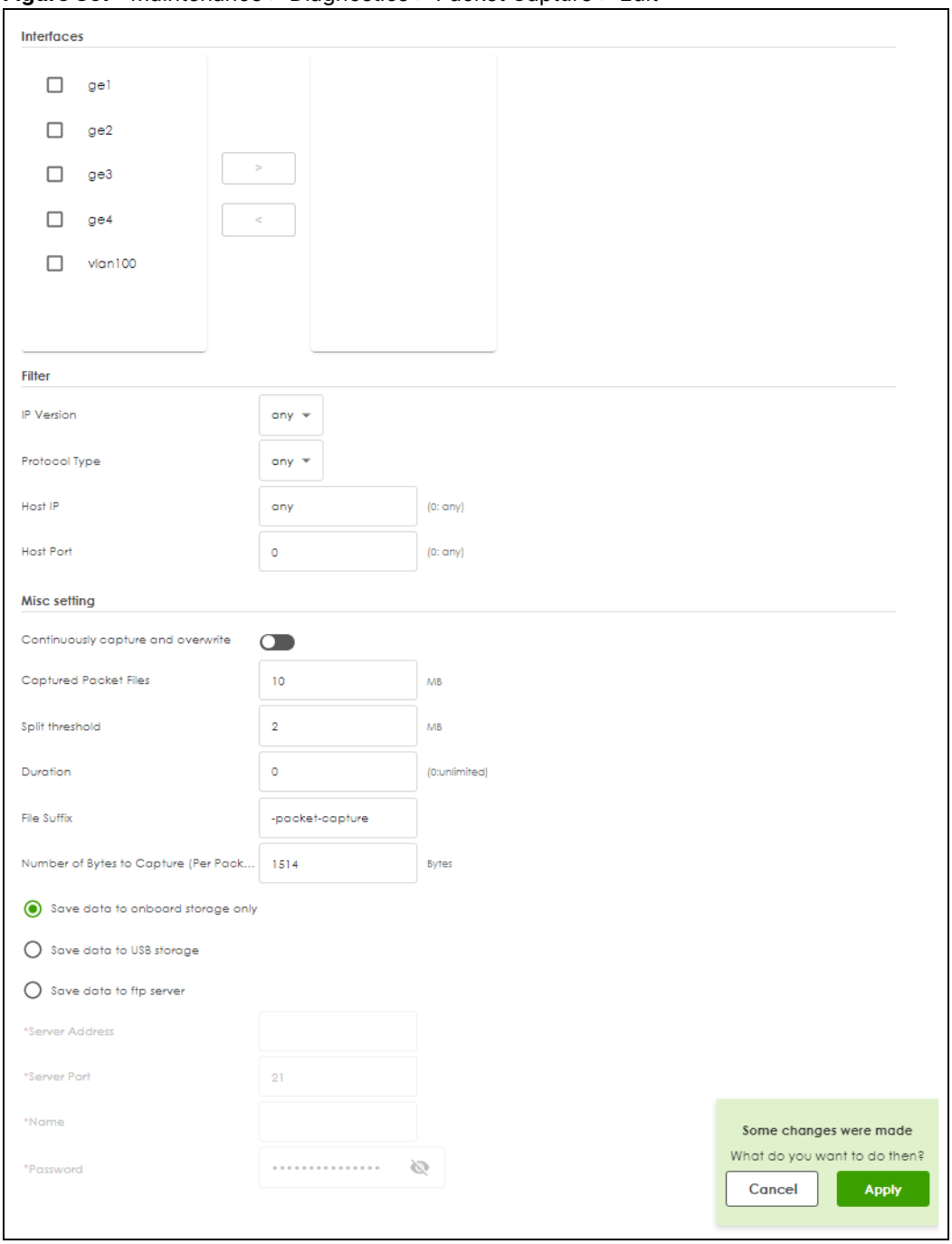
LABEL	DESCRIPTION
Capture	Click this button to have the Zyxel Device capture packets according to the settings configured in this screen. You can configure the Zyxel Device while a packet capture is in progress although you cannot modify the packet capture settings. The Zyxel Device's throughput or performance 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. If there is insufficient flash storage space for the capture file, packet capture will stop. You can check the log under the **System** category in **Log & Report > Log / Events > System**.
Status	This field is blank when no packet capture is in progress. It shows **Capturing** when packet capture is active.
Remove	Select files and click **Remove** to delete them from the Zyxel Device or the connected USB storage device.
Download	Click a file to select it and click **Download** to save it to your computer.
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.
Modified Time	This column displays the date and time that the individual files were saved.

33.3.1 The Packet Capture Edit 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 > Edit** 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 397 Maintenance > Diagnostics > Packet Capture > Edit



The following table describes the labels in this screen.

Table 308 Maintenance > Diagnostics > Packet Capture > Edit

LABEL	DESCRIPTION
Interfaces	Select interfaces for which to capture packets and click the right arrow button to move them to the right.
IP Version	Select the version of IP for which to capture packets. Select **any** to capture packets for all IP versions.

Table 308 Maintenance > Diagnostics > Packet Capture > Edit (continued)

LABEL	DESCRIPTION
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.
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. The USB file format should be FAT32. 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 **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.

Table 308 Maintenance > Diagnostics > Packet Capture > Edit (continued)

LABEL	DESCRIPTION
Save data to ftp server	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.

33.4 The CPU / Memory Status Screen

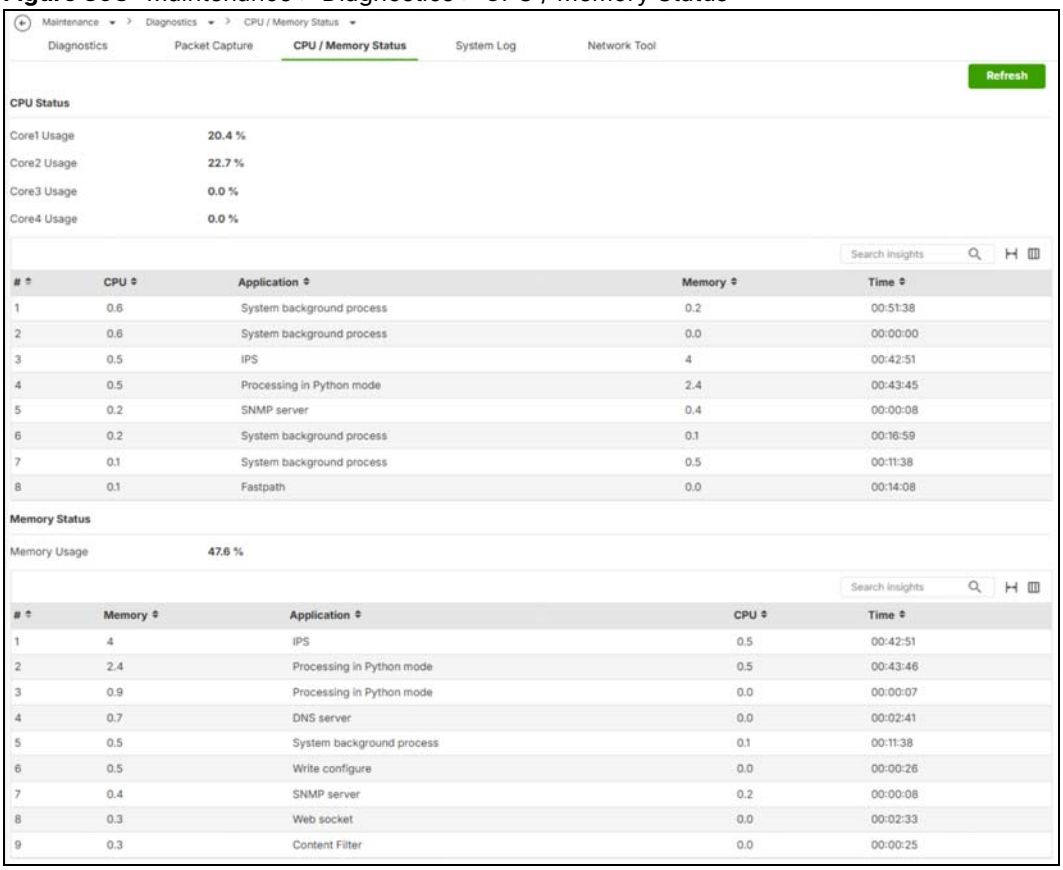
Click **Maintenance > Diagnostics > CPU / Memory Status** to open the **CPU/Memory Status** screen. Use this screen to view the CPU and memory performance of various applications on the Zyxel Device.

A system log will be generated as a reminder when the Zyxel Device's memory utilization reaches the threshold. You can view it in **Log & Report > Log / Event > System**. You can also set up an email notification in **System > Notification > Alert** when the Zyxel Device's memory reaches the threshold. The following table shows the default thresholds for each model at the time of writing.

Table 309 Default Memory Usage Threshold

MODEL	THRESHOLD
USG FLEX 50H USG FLEX 50HP USG FLEX 100H USG FLEX 100HP	90%
USG FLEX 200H USG FLEX 200HP USG FLEX 500H USG FLEX 700H	80%

Figure 398 Maintenance > Diagnostics > CPU / Memory Status



The following table describes the labels in this screen.

Table 310 Maintenance > Diagnostics > CPU / Memory Status

LABEL	DESCRIPTION
Refresh	Click this to update the information in this screen.
CPU Status This table displays the applications that use the most Zyxel Device CPU processing.	
CPU 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. CPU usage may appear temporarily high when creating graphic-intensive statistics and reports. You may ignore it, and observe the long-term usage.
#	This field is a sequential value, and it is not associated with any entry.
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.

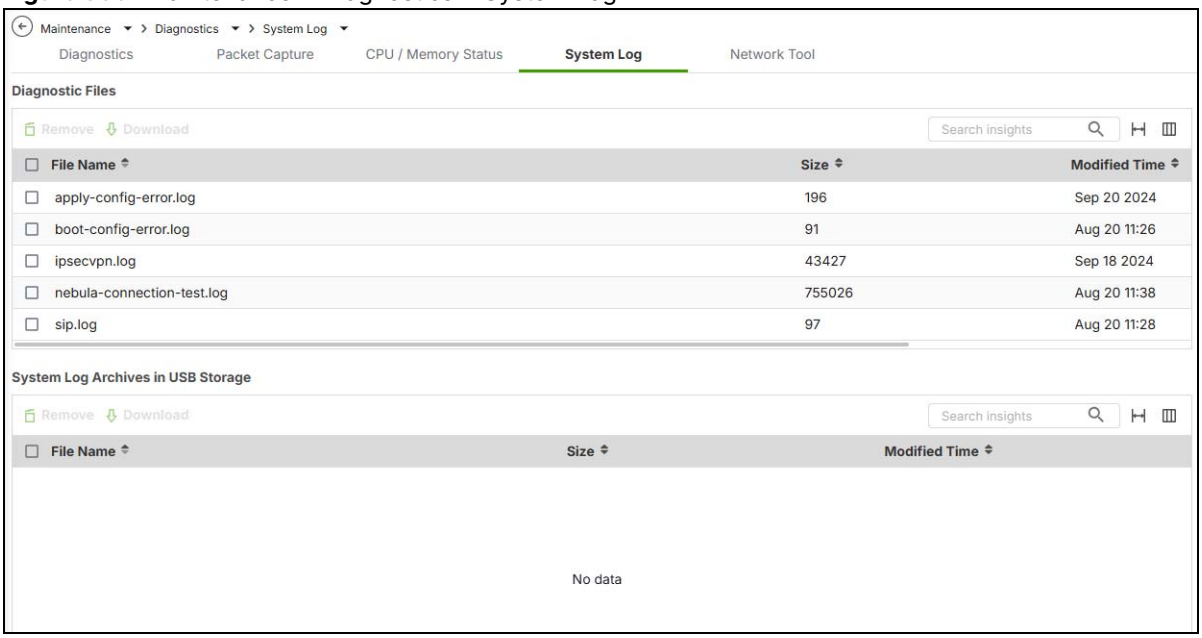
Table 310 Maintenance > Diagnostics > CPU / Memory Status

LABEL	DESCRIPTION
#	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.

33.5 The System Log Screen

Click **Maintenance > Diagnostics > System Log** to open the **System Log** screen. This screen lists the files of diagnostic information the Zyxel Device has collected and stored on a connected USB storage device. You may need to send these files to customer support for troubleshooting.

Figure 399 Maintenance > Diagnostics > System Log



The following table describes the labels in this screen.

Table 311 Maintenance > Diagnostics > System Log

LABEL	DESCRIPTION
Diagnostic Files	
Remove	Select files and click **Remove** to delete them from the Zyxel Device. A pop-up window asks you to confirm that you want to delete.
Download	Select a file and click **Download** to save it to your computer.

Table 311 Maintenance > Diagnostics > System Log

LABEL	DESCRIPTION
File Name	This column displays the label that identifies the file. • The **apply-config-error.log** file logs the configuration file the Zyxel Device is applying. • The **boot-config-error.log** file logs errors that occur during the Zyxel Device's booting process. • The **ipsecvpn.log** file logs events related to IPsec VPN connections. • If the Zyxel Device is disconnected from the NCC, the **nebula-connection-test.log** file will log the Zyxel Device's Internet connection status and the NCC connection status. • The **sip.log** file logs the voice that passes through the Zyxel Device.
Size	This column displays the size (in bytes) of a file.
Modified Time	This column displays the date and time that the individual files were saved.
System Log Archives in USB Storage	
Remove	Select files and click **Remove** to delete them from the USB storage device. A pop-up window asks you to confirm that you want to delete.
Download	Select a file and click **Download** to save it to your computer.
File Name	This column displays the label that identifies the file.
Size	This column displays the size (in bytes) of a file.
Modified Time	This column displays the date and time that the individual files were saved.

33.6 The Network Tool Screen

Use this screen to perform various network tests.

Click **Maintenance > Diagnostics > Network Tool** to display this screen.

Figure 400 Maintenance > Diagnostics > Network Tool (PING IPv4)

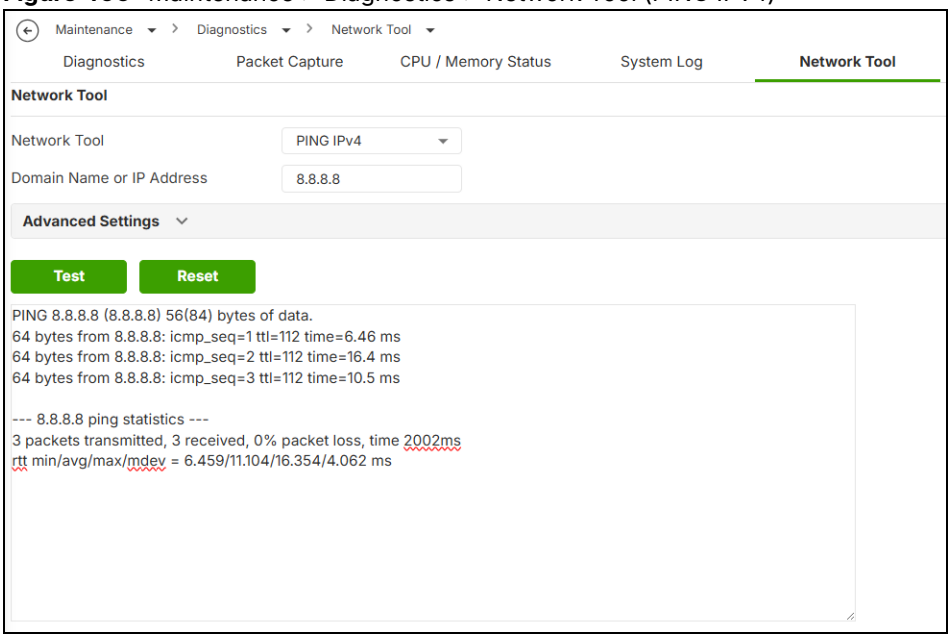


Figure 401 Maintenance > Diagnostics > Network Tool (IPSec Trace Log)

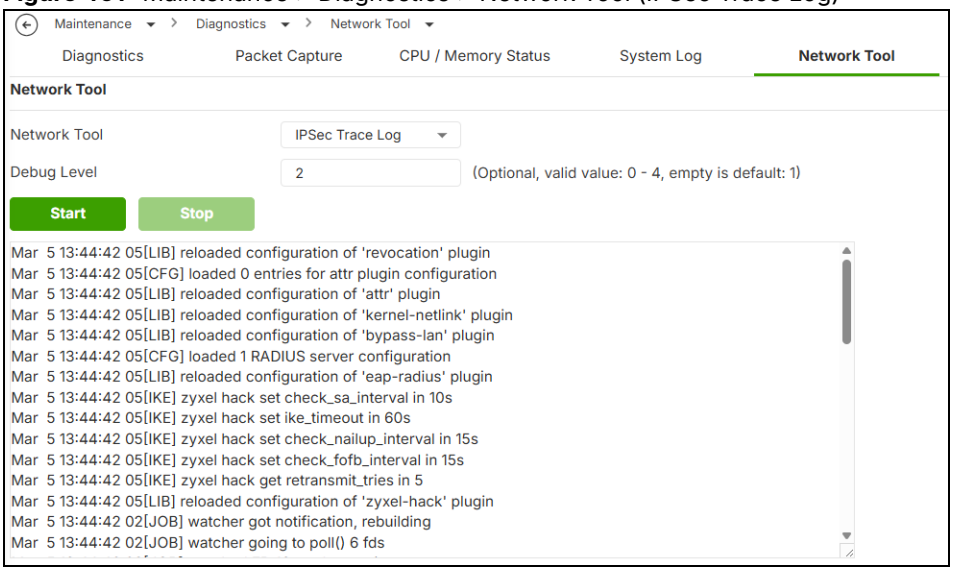
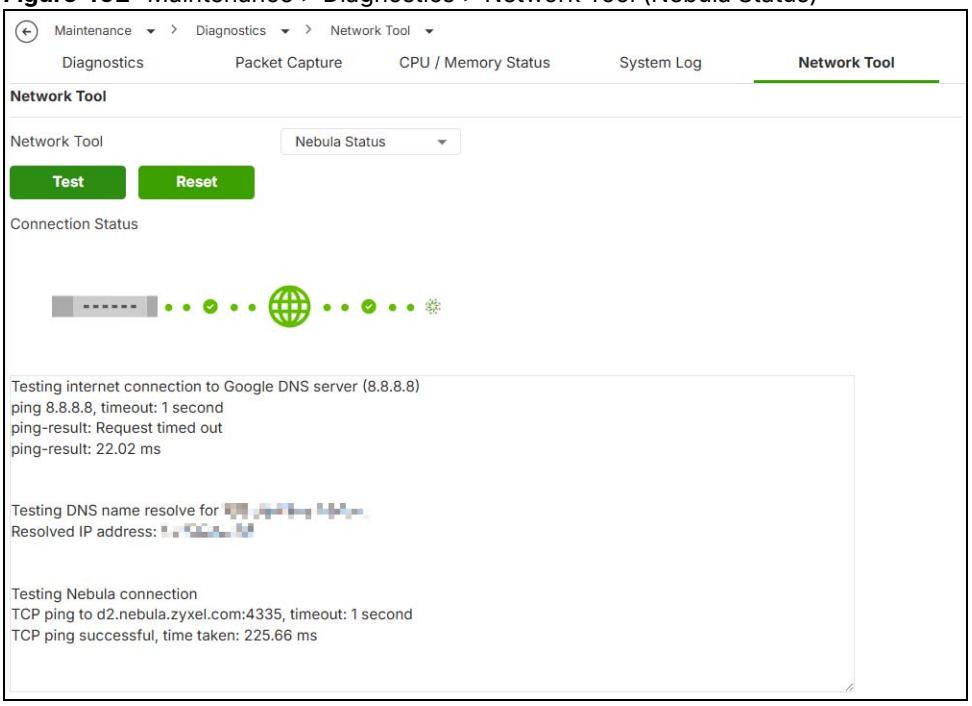


Figure 402 Maintenance > Diagnostics > Network Tool (Nebula Status)



The following table describes the labels in this screen.

Table 312 Maintenance > Diagnostics > Network Tool

LABEL	DESCRIPTION
Network Tool	Select a network tool from the list. • Select **NSLOOKUP IPv4** to perform name server lookup for querying the Domain Name System (DNS) to get the domain name or IP address mapping. • Select **PING IPv4** to ping the IP address that you entered. • Select **TRACEROUTE IPv4** to run the traceroute function. This determines the path a packet takes to the specified computer. • Select **IPSec Trace Log** to run the strongSwan debug log function. • Select **Nebula Status** to test the connection from the Zyxel Device to the Nebula Control Center (NCC). This screen displays if the test passes.  This screen displays if the test fails. 
Domain Name or IP Address	Type the IP address that you want to use to for the NSLOOKUP, PING and TRACEROUTE network tools.
Debug Level	This field displays when you choose the I**PSec Trace Log** network tool. Select a log level from 0 to 4, then click **Start**. Wait, or click **Stop** to see the log result. The higher the log level, the more detailed the log. The debug log levels are as follows: • 0: Very basic auditing logs, such as SA up / down) • 1: Generic control flow with errors (default) • 2: Contains more detailed control flow logs • 3: Includes RAW data dumps in hex • 4: Includes sensitive material such as keys.
Test	This field displays when you choose the **Nebula Status** network tool. Click **Test**, then wait for the result. Click **Reset** to remove the results and test again.
Advanced Settings	
Query Server	This field appears when you choose **NSLOOKUP IP v4**. Enter the IP address of a server to which the Zyxel Device sends queries for NSLOOKUP.
Interface	This field appears when you choose **PING IPv4** or **TRACEROUTE IPv4**. Select an interface from which to ping the specified IP address when running **PING IPv4** or route to the specified IP address when running **TRACEROUTE IPv4**.
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. 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.
Test	Click this button to start the test.
Reset	Click this button to return the screen to its last-saved settings.

CHAPTER 34
AP Diagnostics

34.1 Overview

Use the AP diagnostics screens for troubleshooting.

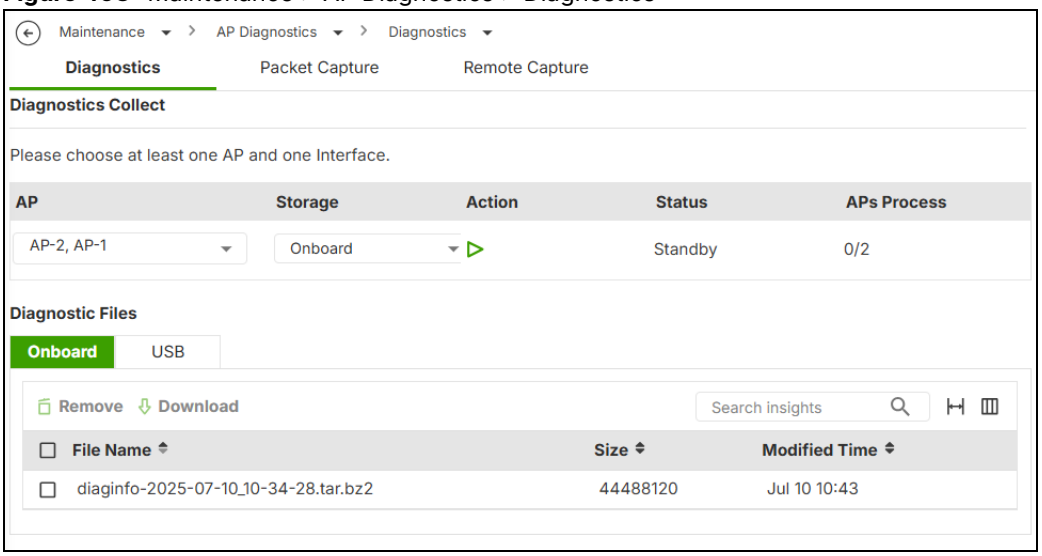
34.1.1 What You Can Do in this Chapter

- Use the **Diagnostics** screen (see Section 34.2 on page 684) to generate a file containing the managed APs' diagnostic information.
- Use the **Packet Capture** screen (see Section 34.3 on page 685) to generate a file containing specific network traffic passing through the managed APs for troubleshooting wireless connection issues.
- Use the **Remote Capture** screen (see Section 34.4 on page 688) to enable remote packet captures on wired or wireless interfaces through an external packet analyzer.

34.2 Diagnostics Screen

Use this screen to generate a file containing the managed AP's diagnostic information.

Figure 403 Maintenance > AP Diagnostics > Diagnostics



The following table describes the labels in this screen.

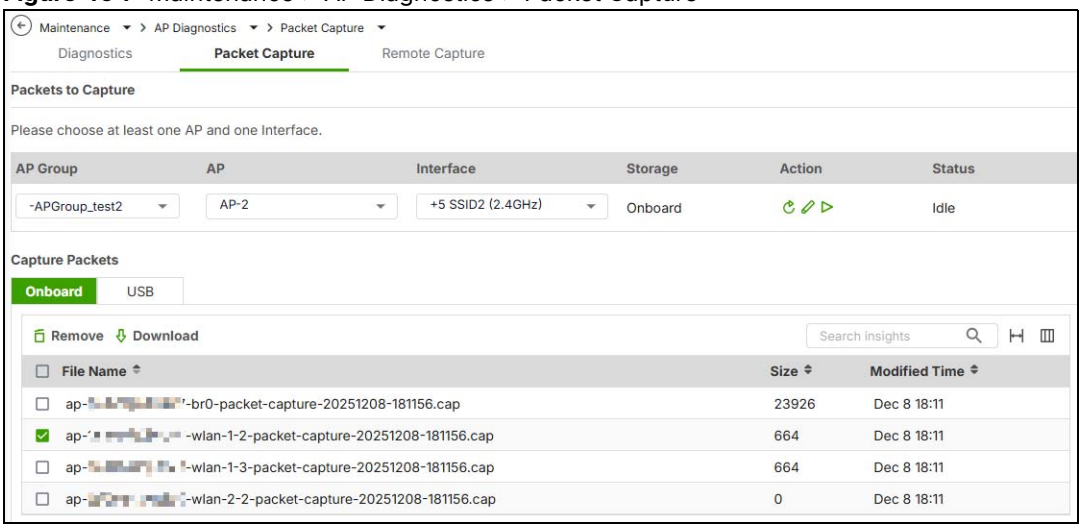
Table 313 Maintenance > AP Diagnostics > Diagnostics

LABEL	DESCRIPTION
Diagnostics Collect	
AP	Select the managed AP(s) whose diagnostic information you want to collect. You can select up to five APs. Diagnostic data from each AP is stored in an individual AP diagnostic file.
Storage	Select **Onboard** to store diagnostic information on the Zyxel Device. Select **USB** to store diagnostic information on a USB storage device connected to the Zyxel Device if the Zyxel Device allows this.
Action	**Start collect info**: Click this to start collecting diagnostic information. **Stop collect info**: Click this to stop collecting diagnostic information. A file will not be created.
Status	This shows **Standby** when no collection is in progress and **Collecting** during data collection.
APs Process	This shows the number of APs selected for collection and the number of APs that have completed the collection. For example, 2/3 means that three APs are being collected and two of them have finished. If the status shows Standby while one or more APs have not finished data collection, check the details in **Log & Report > Log / Events > System** under the **System** category. After resolving the issue, click **Start Collect Info** in the **Action** field to restart the collection.
Diagnostic Files	
Onboard / USB	Select the tab to view the diagnostic files saved on the Zyxel Device or a connected USB storage device.
Remove	Select files and click **Remove** to delete them from the Zyxel Device or the USB storage device.
Download	Select a diagnostic file and click **Download** to save it to your computer.
File Name	This is the name of the created diagnostic file. An AP diagnostic file name starts with “apdiaginfo”, followed by the AP’s MAC address.
Size	This is the size (in bytes) of the created diagnostic file.
Modified Time	This is the date and time that the diagnostic file was created. The format is mm dd hh:mm.

34.3 Packet Capture Screen

Use this screen to capture specific traffic of the managed APs’ WiFi network for troubleshooting. You can then download the capture files for analysis.

Figure 404 Maintenance > AP Diagnostics > Packet Capture



The following table describes the labels in this screen.

Table 314 Maintenance > AP Diagnostics > Packet Capture

LABEL	DESCRIPTION
Packets to Capture	
AP Group	Select the AP group the managed APs whose packets you want to capture belongs to.
AP	Select the managed APs whose packets you want to capture.
Interface	Select the interfaces for which to capture packets passing through the managed APs. If multiple interfaces are selected and the field is too short, extra interfaces are shown as +<number>. • **SSID Name (xGHz)**: WiFi packets on a specific WiFi network (SSID) or a specific frequency band. x indicates the frequency band. • **WIRELESS (xGHz)**: WiFi packets transmitted and received by client devices on a specific frequency band. x indicates the frequency band. • **WDS-x-9**: WiFi packets transmit through the downlink AP using a specific radio profile. x indicates the radio profile number 1, 2, or 3. • **WDS-x-10**: WiFi packets transmit through the uplink AP using a specific radio profile. x indicates the radio profile number 1, 2, or 3. • **UPLINK**: Packets transmitted and received through the uplink port. • **LANx**: Packets passing through a specific LAN port of the managed AP. x indicates the LAN port number. • **Br0**: Packets transmitted and received through the AP's virtual bridge, connecting uplink and downlink interfaces. Learn more about Uplink and Downlink.
Storage	This displays **Onboard** if the capture file is saved on the Zyxel Device, and **USB** if the capture file is saved to a connected USB storage device. Click the **Edit** icon in the **Action** field to change this setting.

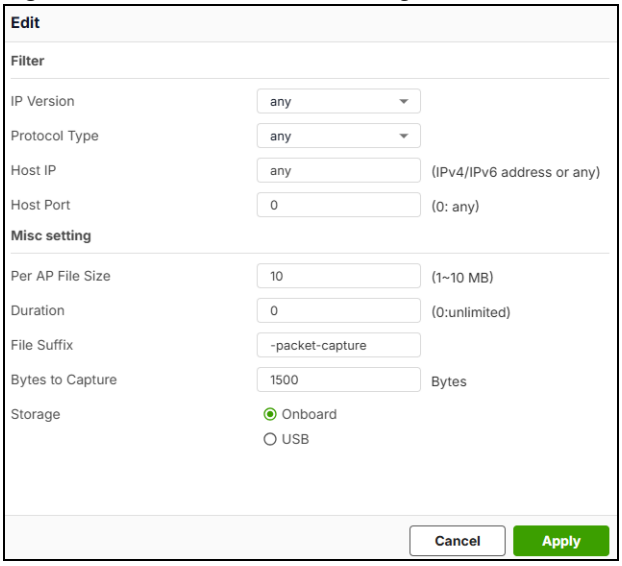
Table 314 Maintenance > AP Diagnostics > Packet Capture (continued)

LABEL	DESCRIPTION
Action	**Refresh**: Click this to update the packet captures on the interfaces you selected above. **Edit**: Click this to configure additional details, such as setting a filter to capture specific packets. **Start packet capturing**: Click this to start capturing packets from the selected interfaces you selected above. If packet capture fails because of insufficient storage, you can download the existing files to your computer and remove them from the Zyxel Device or USB storage. **Stop packet capturing**: Click this to stop capturing packets. The captured packets will be saved to a capture file. You can find the files below on the screen.
Status	The status displays **Idle** when no packet capture is in progress, **Preparing** while the AP retrieves capture requirements, and **Capturing** when packet capture is active.
Capture Packets	
Onboard / USB	Select the tab to view the capture packet files saved on the Zyxel Device or a connected USB storage device.
Remove	Select files and click **Remove** to delete them from the Zyxel Device or the USB storage device.
Download	Select a file and click **Download** to save it to your computer.
File Name	This is the name of the created packet capture file.
Size	This is the size (in bytes) of the created packet capture file.
Modified Time	This is the date and time that the packet capture file was created. The format is mm dd hh:mm.

34.3.1 Packet Capture Edit Screen

Use this screen to configure additional details for packets capture network traffic.

Figure 405 Maintenance > AP Diagnostics > Packet Capture > Edit



The following table describes the labels in this screen.

Table 315 Maintenance > Diagnostics > Packet Capture > Edit

LABEL	DESCRIPTION
Filter	
IP Version	Select the packets with a specific IP version that you want to capture. Select **any** to capture packets for all IP versions.
Protocol Type	Select the packets with a specific protocol type that you want to capture. Give an example of a protocol. Select **any** to capture packets for all types of traffic.
Host IP	Enter the packets from a specific IP host that you want to capture. Enter **any** to capture packets for all hosts.
Host Port	This field is configurable when you set the **Protocol Type** to **any**, **tcp**, or **udp**. Enter the port number for the **Protocol Type** to selected above. For example, FTP traffic is port 21 for Protocol Type TCP.
Misc setting	
Per AP File Size	Specify a maximum size limit in megabytes (MB) for the total combined size of all the capture files from each AP. The valid range is 1 to 10 MB. The Zyxel Device stops capturing when the size limit is reached.
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 **Per AP 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”.
Bytes To Capture	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.
Storage	Select **Onboard** to have the Zyxel Device stores packet capture files on the Zyxel Device. Select **USB** to have the Zyxel Device stores packet capture files on a USB storage device connected to the Zyxel Device if the Zyxel Device allows this.
Apply	Click this button to save your changes.
Cancel	Click this button to return the screen to its last-saved settings.

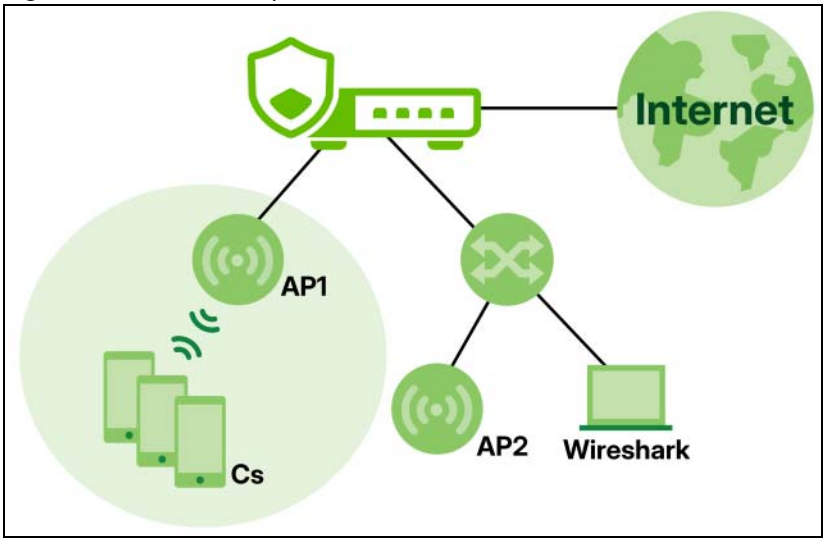
34.4 Remote Capture Screen

Use this screen to capture wireless traffic going through a managed AP and output the captured packets to a packet analyzer (also known as network or protocol analyzer) such as Wireshark.

You can connect your laptop running a network analyzer to a switch, along with **AP2** configured as a monitor AP, to capture wireless traffic between **AP1** and its client devices (**Cs**).

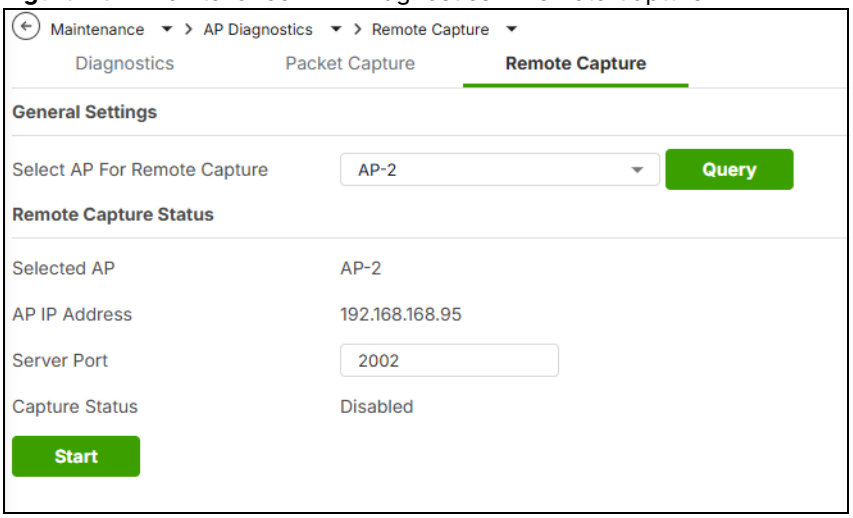
Note: **AP1** and **AP2** have to use the same channel.

Figure 406 Remote Capture



Note: Not all AP models support remote capture. Check your AP's user guide to see if your model supports remote capture.

Figure 407 Maintenance > AP Diagnostics > Remote Capture



The following table describes the labels in this screen.

Table 316 Maintenance > AP Diagnostics > Remote Capture

LABEL	DESCRIPTION
General Settings	
Select AP For Remote Capture	Select the managed AP that is connected to the device used for capturing wireless packets. This AP will act as the monitor AP.
Query	After selecting a managed AP, click this button to see its IP address and remote capture status. Note: Click this button before each remote capture to obtain the latest status of the selected AP.
Remote Capture Status	
Selected AP	This is the name of the managed AP you select.

Table 316 Maintenance > AP Diagnostics > Remote Capture (continued)

LABEL	DESCRIPTION
AP IP Address	This is the IP address of the managed AP you select.
Server Port	Enter the number of the server port you want the packet analyzer to connect to in order to capture traffic going through the managed AP. The default port number is 2002.
Capture Status	This displays **Enabled** when remote capture is in progress and **Disabled** when no remote capture is in progress.
Start / Stop	Click the **Start** button to allow the packet analyzer to start capturing traffic going through the managed AP. Click the **Stop** button to stop the packet analyzer from capturing traffic going through the managed AP.

CHAPTER 35
Packet Flow Explore

35.1 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.

35.1.1 What You Can Do in this Chapter

- Use the **Routing Status** screen (see Section 35.2 on page 691) to view the overall routing flow and each routing function's settings.
- Use the **SNAT Status** screen (see Section on page 683) to view the overall source IP address conversion (SNAT) flow and each SNAT function's settings.
- Use the **Route Traces** screen (see Section 35.4 on page 702) to configure traceroute to identify where packets are dropped for troubleshooting.

35.2 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**.

Different features may have overlapping criteria that trigger different actions for the same traffic. Packet Flow Explore defines the order that features check criteria. This resolves conflicts when criteria overlap in different features. Features that may encounter overlapping criteria are:

- Routing
- NAT

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.

Note: If you use the `vrf main routing policy-route override-direct-route` command, the Zyxel Device will prioritize **Policy Route** over **Direct Route** for packets routing.

Dynamic/SiteToSite VPN

This is where packets are forwarded according to the criteria you configure in **VPN** > **IPSec VPN** > **Site to Site VPN**.

Figure 408 Maintenance > Packet Flow Explore > Routing Status (Dynamic/SiteToSite VPN)



The following table describes the labels in this screen.

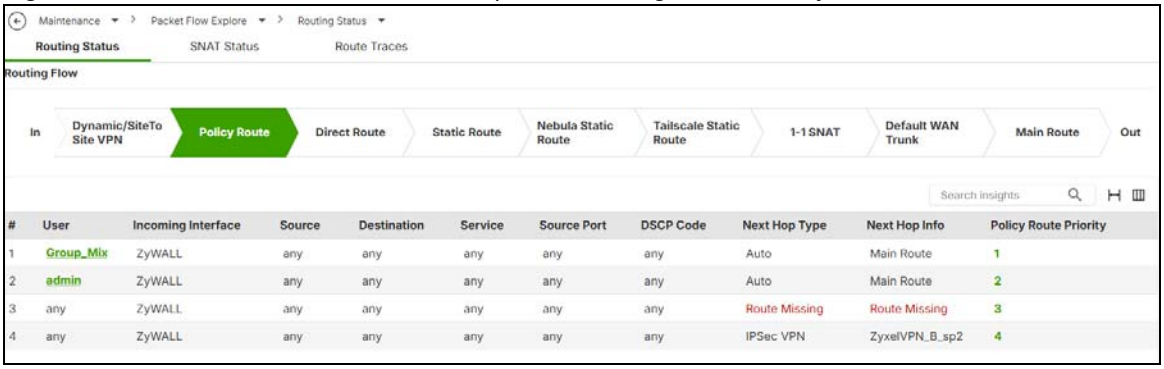
Table 317 Maintenance > Packet Flow Explore > Routing Status (Dynamic/SiteToSite VPN)

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.
#	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.

Policy Route

This is where packets are forwarded according to the criteria you configure in **Network** > **Routing** > **Policy Route**.

Figure 409 Maintenance > Packet Flow Explore > Routing Status (Policy Route)



The following table describes the labels in this screen.

Table 318 Maintenance > Packet Flow Explore > Routing Status (Policy Route)

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.

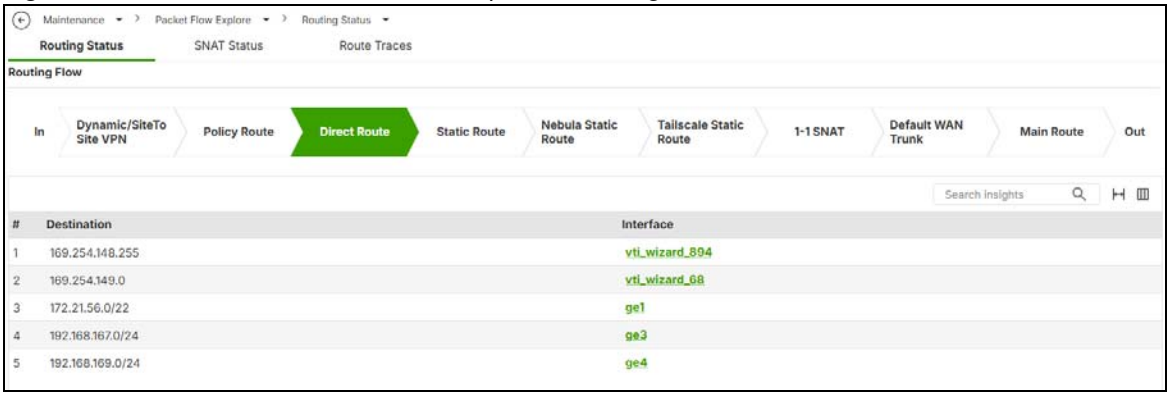
Table 318 Maintenance > Packet Flow Explore > Routing Status (Policy Route) (continued)

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with any entry.
User	This is the name of the user (group) object from which the packets are sent. **any** means all users. Hover your mouse over internal users of type **Admin**, **User**, or **Group** to display additional information such as the IP address that user used to log in, if the user has already logged out, or the group name of a **Group** type For external users such as ncas-users, ctc-users, only the name is displayed without additional IP address or logout status information.
Incoming Interface	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.
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 trunk name if the **Next Hop Type** is **Trunk**. • This is the IPSec VPN Tunnel name if the **Next Hop Type** is **IPSec VPN**.
Policy Route Priority	Enter the priority of the rule on the Zyxel Device. The Zyxel Device uses this priority to determine which rule to apply. The lower the number, the higher the priority.

Direct Route

This is where packets are sent to directly connected subnets.

Figure 410 Maintenance > Packet Flow Explore > Routing Status (Direct Route)



The following table describes the labels in this screen.

Table 319 Maintenance > Packet Flow Explore > Routing Status (Direct Route)

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.
#	This field is a sequential value, and it is not associated with any entry.

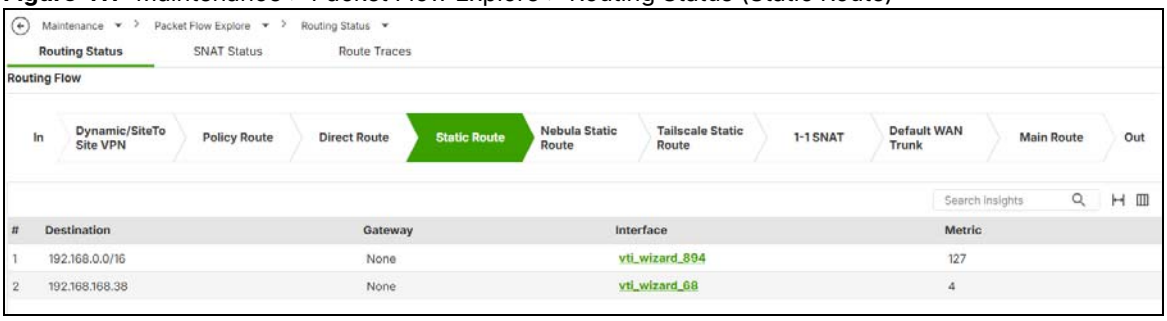
Table 319 Maintenance > Packet Flow Explore > Routing Status (Direct Route) (continued)

LABEL	DESCRIPTION
Destination	This is the destination IP address of a route.
Interface	This is the name of an interface associated with the route.

Static Route

This is where packets are forwarded according to the criteria you configured in **Network** > **Routing** > **Static Route**.

Figure 411 Maintenance > Packet Flow Explore > Routing Status (Static Route)



The following table describes the labels in this screen.

Table 320 Maintenance > Packet Flow Explore > Routing Status (Static Route)

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.
#	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. The lower the number, the higher the priority.

Nebula Static Route

This is the static route created when you are using Nebula VPN.

Figure 412 Maintenance > Packet Flow Explore > Routing Status (Nebula Static Route)



The following table describes the labels in this screen.

Table 321 Maintenance > Packet Flow Explore > Routing Status (Nebula Static Route)

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.
#	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.
Destination Site	This is the Nebula site name of the next-hop gateway or the interface through which the traffic is routed.
Metric	This is the route's priority among the displayed routes. The lower the number, the higher the priority.

Tailscale Static Route

This is the static route created when you are using Tailscale VPN.

Figure 413 Maintenance > Packet Flow Explore > Routing Status (Tailscale Static Route)



The following table describes the labels in this screen.

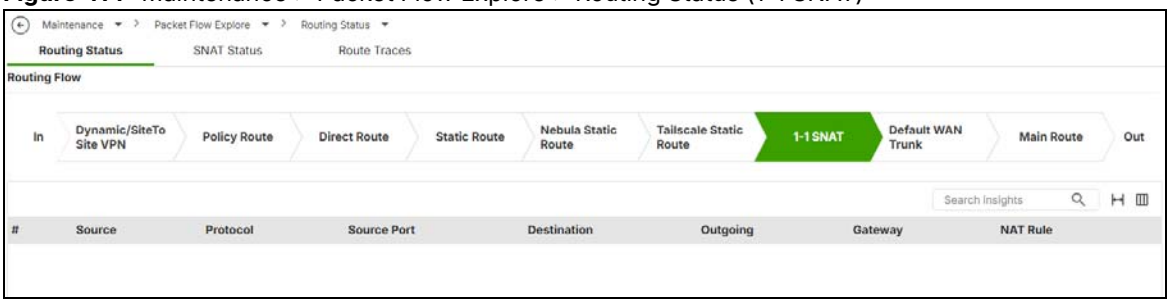
Table 322 Maintenance > Packet Flow Explore > Routing Status (Tailscale Static Route)

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.
#	This field is a sequential value, and it is not associated with any entry.
Destination	This is the destination IP address of a route.
Interface	This is the interface through which the Tailscale traffic is routed.

1-1 SNAT

This maps an internal private IP address to a single external public IP address for outbound traffic.

Figure 414 Maintenance > Packet Flow Explore > Routing Status (1-1 SNAT)



The following table describes the labels in this screen.

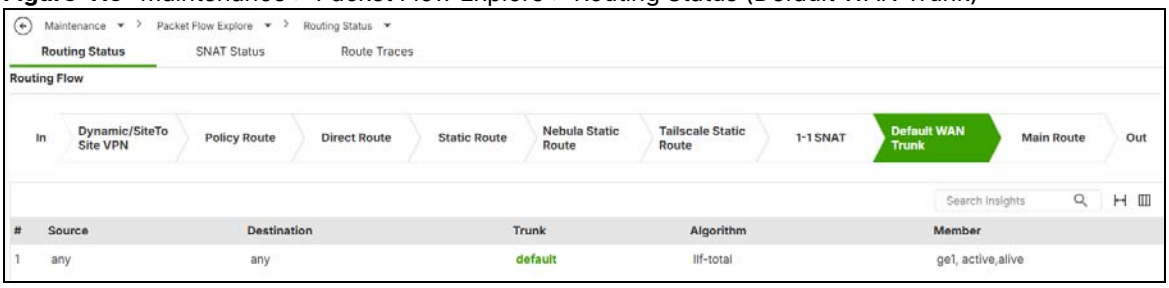
Table 323 Maintenance > Packet Flow Explore > Routing Status (1-1 SNAT)

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.
#	This field is a sequential value, and it is not associated with any entry.
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.
Gateway	This is the IP address of the gateway in the same network of the outgoing interface.
NAT Rule	This is the name of an activated 1:1 or Many 1:1 NAT rule in the NAT table.

Default WAN Trunk

This is where packets are forwarded to the active interface in a WAN trunk and then onto the destination IP address.

Figure 415 Maintenance > Packet Flow Explore > Routing Status (Default WAN Trunk)



The following table describes the labels in this screen.

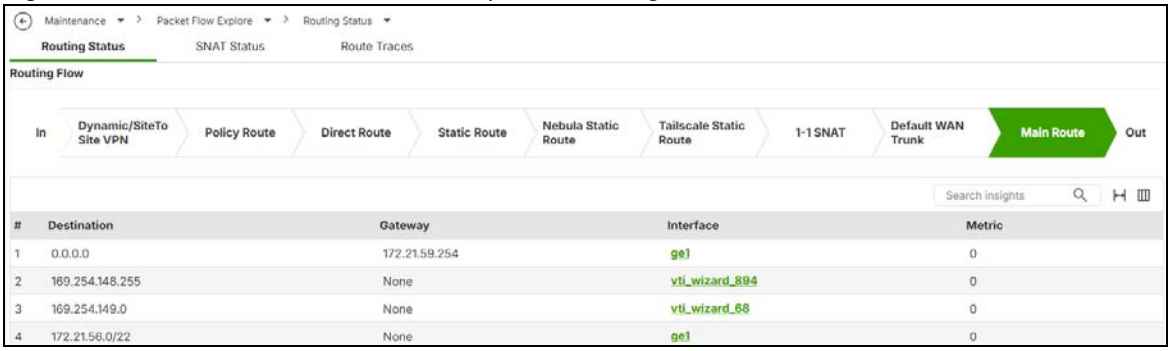
Table 324 Maintenance > Packet Flow Explore > Routing Status (Default WAN Trunk)

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.
#	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.
Algorithm	This displays the load balancing method of the WAN 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).
Member	This displays the trunk member's interface(s).

Main Route

This is the default routing table of the Zyxel Device system kernel where packets are forwarded onto the destination IP address.

Figure 416 Maintenance > Packet Flow Explore > Routing Status (Main Route)



The following table describes the labels in this screen.

Table 325 Maintenance > Packet Flow Explore > Routing Status (Main Route)

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.
#	This field is a sequential value, and it is not associated with any entry.

Table 325 Maintenance > Packet Flow Explore > Routing Status (Main Route) (continued)

LABEL	DESCRIPTION
Destination	This is the destination IP address(es) to which the packets are transmitted. **any** means any IP address.
Gateway	This is the IP address of the gateway in the same network of the outgoing interface.
Interface	This is the name of an interface associated with the route.
Metric	This is the route's priority among the displayed routes. The lower the number, the higher the priority.

35.3 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**.

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.

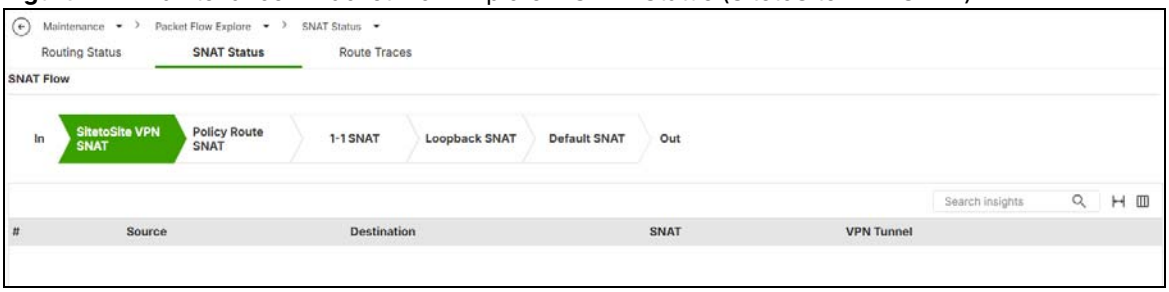
The order of the SNAT flow may vary depending on whether you:

- Enable/disable **Default SNAT** in the **Network > Interface > Edit External** interface screen.

SitetoSite VPN SNAT

SNAT for policy-based **SitetoSite IPsec VPN** maps all internal private IP addresses of a site to a single IP address for outbound traffic.

Figure 417 Maintenance > Packet Flow Explore > SNAT Status (SitetoSite VPN SNAT)



The following table describes the labels in this screen.

Table 326 Maintenance > Packet Flow Explore > SNAT Status (SitetoSite VPN SNAT)

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.
#	This field is a sequential value, and it is not associated with any entry.
Source	This is the external source IP address(es).

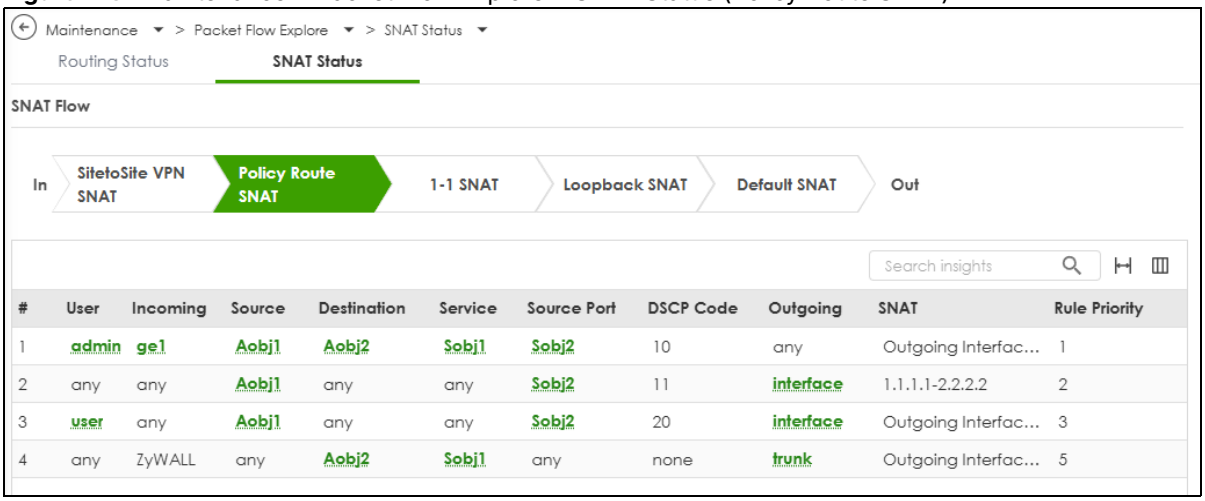
Table 326 Maintenance > Packet Flow Explore > SNAT Status (SitetoSite VPN SNAT) (continued)

LABEL	DESCRIPTION
Destination	This is the external destination IP address(es).
SNAT	This is the source IP address(es) that the SNAT rule uses finally.
VPN Tunnel	This is the name of the VPN tunnel.

Policy Route SNAT

This is where packets are forwarded according to the criteria you configured in **Network** > **Routing** > **Policy Route**, with the private source IP address of the sender replaced with a public IP address for outbound traffic.

Figure 418 Maintenance > Packet Flow Explore > SNAT Status (Policy Route SNAT)



The following table describes the labels in this screen.

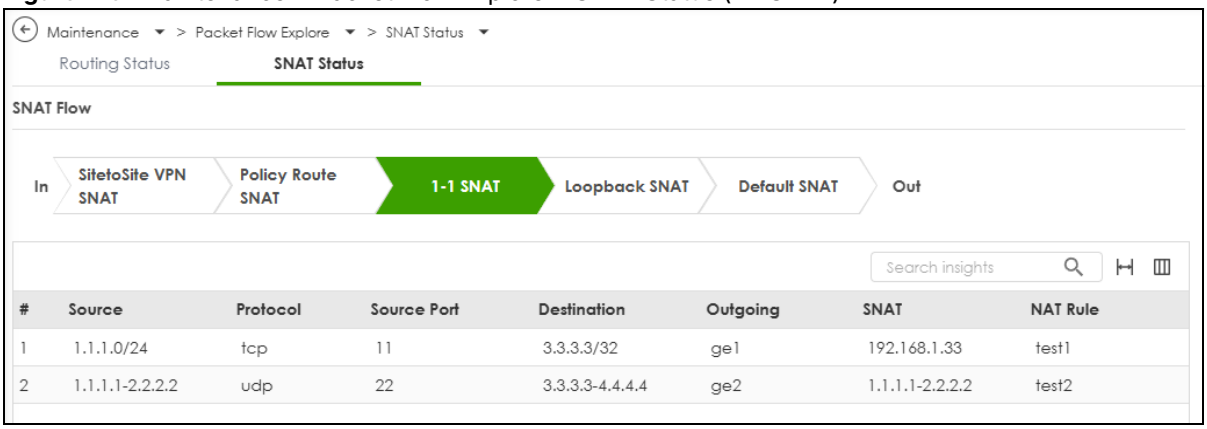
Table 327 Maintenance > Packet Flow Explore > SNAT Status (Policy Route SNAT)

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.
#	This field is a sequential value, and it is not associated with any entry.
User	This is the name of the user (group) object from which the packets are sent. **any** means all users.
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.
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.
Rule Priority	Enter the priority of the rule on the Zyxel Device. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority.

1-1 SNAT

1-1 SNAT maps an internal private IP address to a single external public IP address for outbound traffic.

Figure 419 Maintenance > Packet Flow Explore > SNAT Status (1-1 SNAT)



The following table describes the labels in this screen.

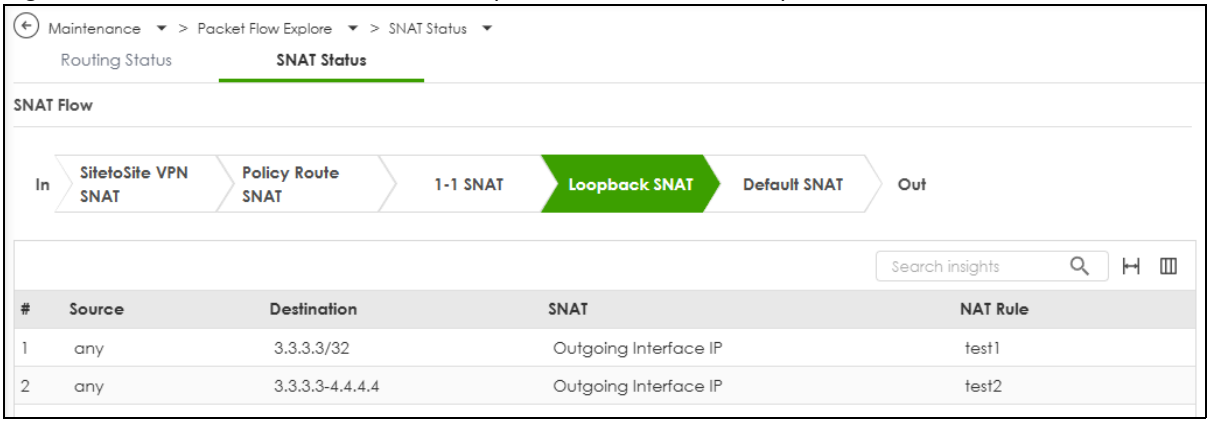
Table 328 Maintenance > Packet Flow Explore > SNAT Status (1-1 SNAT)

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.
#	This field is a sequential value, and it is not associated with any entry.
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.
NAT Rule	This is the name of an activated NAT rule which uses SNAT.

Loopback SNAT

Loopback SNAT maps an internal private IP address to the public IP address of an internal server.

Figure 420 Maintenance > Packet Flow Explore > SNAT Status (Loopback SNAT)



The following table describes the labels in this screen.

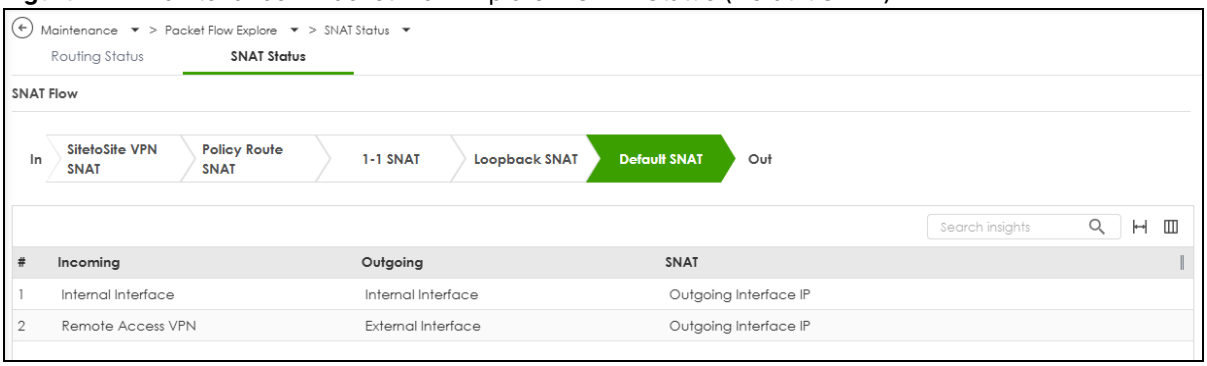
Table 329 Maintenance > Packet Flow Explore > SNAT Status (Loopback SNAT)

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.
#	This field is a sequential value, and it is not associated with any entry.
Source	This is the original source IP address(es). **any** means any IP address.
Destination	This is the original destination IP address(es). **any** means any IP address.
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.
NAT Rule	This is the name of an activated NAT rule which uses SNAT and enables NAT loopback.

Default SNAT

Default SNAT maps internal private IP addresses to a single external public IP address for outbound traffic.

Figure 421 Maintenance > Packet Flow Explore > SNAT Status (Default SNAT)



The following table describes the labels in this screen.

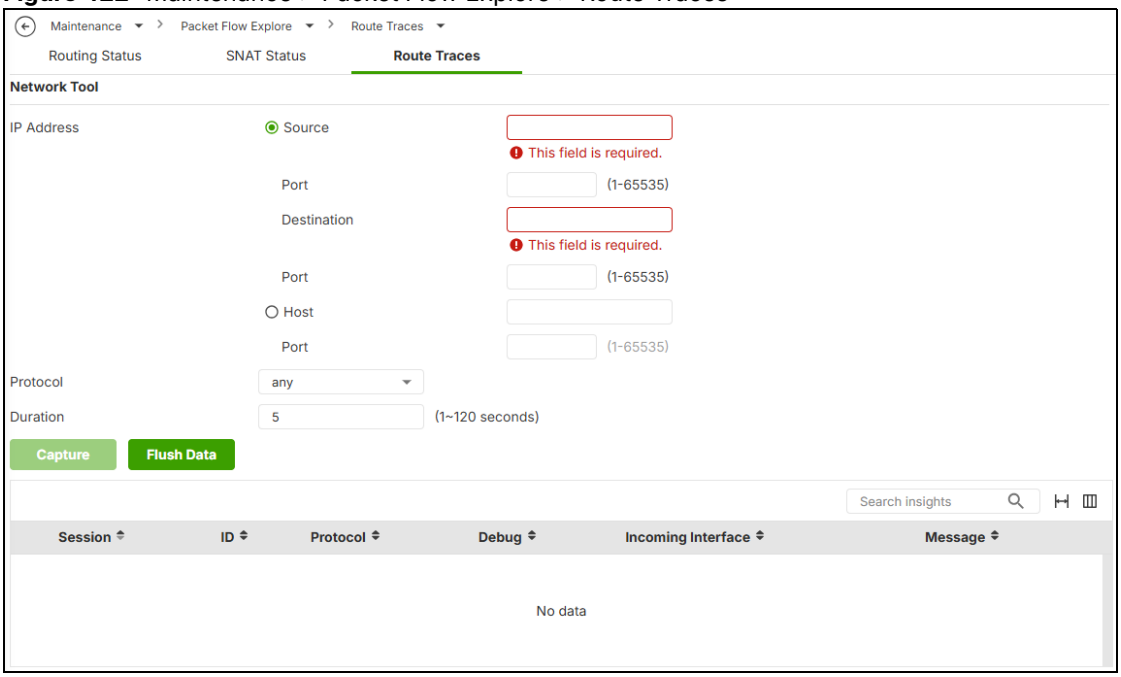
Table 330 Maintenance > Packet Flow Explore > SNAT Status (Default SNAT)

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.
#	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.

35.4 Route Traces

Click **Maintenance > Packet Flow Explore > Route Traces** to display this screen. Use this screen to configure a traceroute to identify where packets are dropped for troubleshooting.

Figure 422 Maintenance > Packet Flow Explore > Route Traces



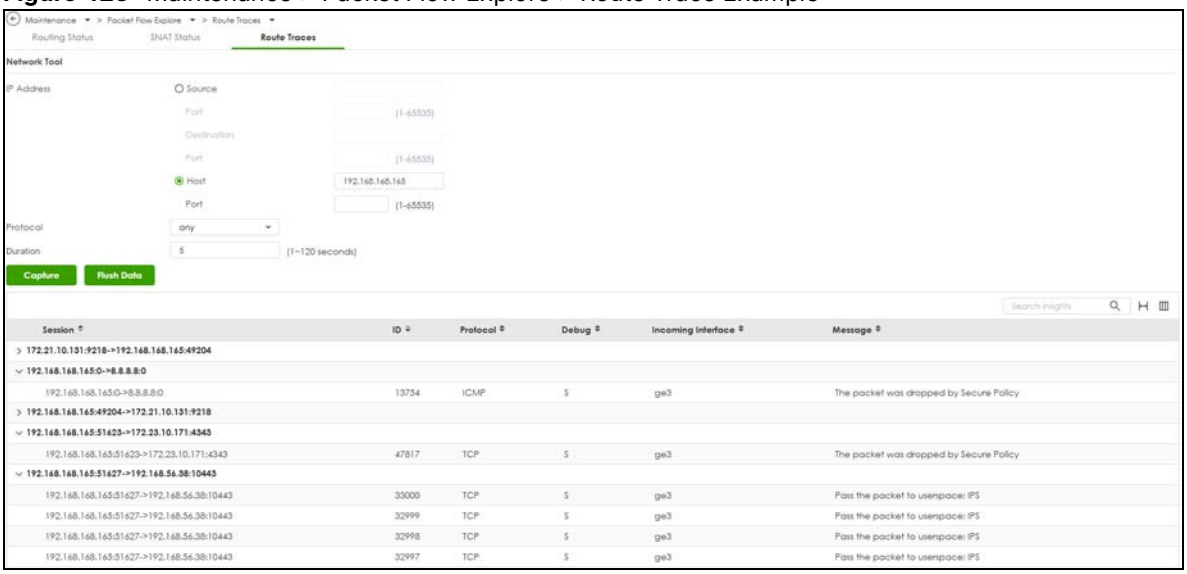
The following table describes the labels in this screen.

Table 331 Maintenance > Packet Flow Explore > Route 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.
Duration	Enter a time duration between 1 and 120 seconds to renew the route trace. The default duration 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 passing through the Zyxel Device that match 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.
Debug	This field displays debug information for the session. Customer support may ask to see these debug messages when investigating a problem. There are three types of debug messages: • The packet outgoing interface: [interface name] • The packet was dropped by [feature name] • Pass the packet to userspace: [feature name]
Incoming Interface	This is the source interface of packets to which this active session applies.
Message	This field displays traceroute information.

The following screen is an example of Route Trace information.

Figure 423 Maintenance > Packet Flow Explore > Route Trace Example



CHAPTER 36
Reboot/Shutdown

36.1 Overview

Use this screen to restart or turn off the Zyxel Device.

36.2 The Reboot/Shutdown Screen

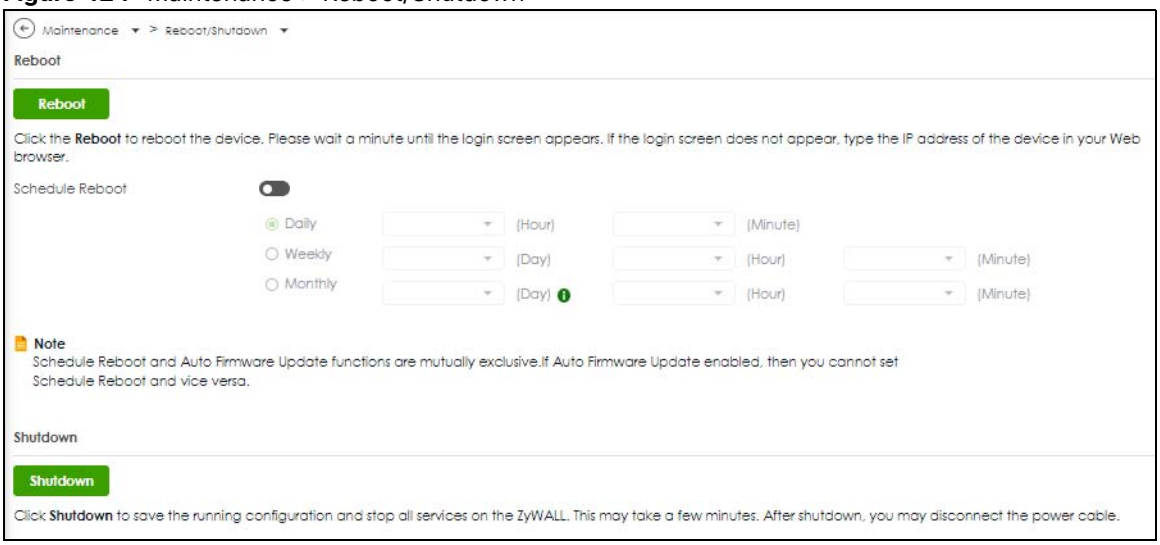
To access this screen, click **Maintenance** > **Reboot/Shutdown**.

When you click **Reboot** or **Shutdown**, your current configurations made using the web configurator are saved.

Note: Your current configurations made using the command line interface (CLI) are not saved if you didn't use the `copy running startup` command to save the current configurations as the startup configurations.

Note: If **startup-config.conf** has an error, the Zyxel Device may restart with an older configuration file or the factory default configuration file with all your configurations lost. Use **Test** in **Maintenance > Firmware/File Manager > Configuration** to check that **startup-config.conf** does not have an error. See Section 32.1.3 on page 656 for details on which configuration files are used at start-up.

Figure 424 Maintenance > Reboot/Shutdown



Click **Reboot** to restart the Zyxel Device immediately without turning the power off.

Alternatively, if you have not enabled **Auto Update** in **Maintenance > Firmware/File manager > Firmware Management**, you may use **Schedule Reboot** in this screen to automatically restart the Zyxel Device at a particular time each day, once a week, or once a month.

- Select **Daily** to have the Zyxel Device automatically restart every day at the specified time. The time format is the 24 hour clock, so '0' means midnight for example.
- Select **Weekly** to have the Zyxel Device automatically restart once a week on the day and at the time specified.
- Select **Monthly** to have the Zyxel Device automatically restart once a month on the day and at the time specified.

Click **Shutdown** to prepare the Zyxel Device to turn off. Wait for the **PWR/SYS** LED to turn off before you remove the Zyxel Device power cable.

Part III
Appendices and Troubleshooting

CHAPTER 37
Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. You can also refer to the logs; see Section 31.2 on page 638 for more information.

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.

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 (192.168.168.1 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 7 seconds (or until the **PWR/SYS** LED starts to blink), then release it. It returns the Zyxel Device to the default configuration with password is 1234, LAN IP address 192.168.168.1. All configuration files, including those you saved on the Zyxel Device, will be deleted.

- 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 HyperTerminal) set to VT100 terminal emulation, no parity, 8 data bits, 1 stop bit, no flow control and 115200 bps port speed.

I cannot access the Internet.

- Check the 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 would like to configure a WAN interface to take over if the active WAN interface(s) go down.

To configure a backup WAN interface that takes over when the active WAN interface(s) fail, follow these steps:

Create a backup WAN interface

1 Go to **Network > Interface > Interface**.

2 Click **+Add** under **External** to create an external interface. See Section 7.3.1 on page 142 for details about each field.

Create a trunk

1 Go to **Network > Interface > Trunk**.

2 Click **+Add** under **User-Defined Trunk** to create a trunk.

3 Add the WAN interface(s) and set **Mode** to **Active**.

4 Add the backup WAN interface and set **Mode** to **Passive**. Click **Apply**.

Activate the trunk

1 Go to **Network > Interface > Trunk**.

2 Select the trunk you created from the **User-Defined Trunk** drop-down list in **Trunk Selection**.

Note: Make sure the backup interface you configured is active. You can check its status in **Network > Interface > Trunk**.

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 Authentication Timeout. To change this:

1 Go to **User & Authentication > 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**.

I cannot update the IPS/application patrol/IP reputation signatures.

- Make sure your Zyxel Device has the IPS/application patrol/IP reputation 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.

I downloaded updated IPS/application patrol/IP reputation signatures. Why has the Zyxel Device not re-booted yet?

The Zyxel Device does not have to reboot when you upload new signatures.

My Zyxel Device is not performing the action I set in **Security Service** > **IPS** when a stream of data matches a malicious signature.

Make sure you set the Zyxel Device to **Prevention** mode for the Zyxel Device to take action. The Zyxel Device only creates log messages in **Detection** mode and does not take action.

The content filtering category service is not working.

Make sure your Zyxel Device is connected to the Internet. Use the feedback link in the screen to give feedback on a link that should or should not be in a certain content filtering category.

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.

I blocked myself from the Zyxel Device due to a misconfigured security policy.

In this example, you disabled the **LAN_to_Device** security policy and lost access to the Zyxel Device. Refer to Using CLI to access the CLI. Test if you can access the CLI if you disabled this policy. If yes, run the following command to re-enable the security policy.

```
MyUSGFLEX500H> edit running
MyUSGFLEX500H running config# vrf main secure-policy rule LAN_to_Device enabled
true
MyUSGFLEX500H running config# commit
Configuration committed.
MyUSGFLEX500H running config# copy running startup
Overwrite startup configuration? [y/N] y
```

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.

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 can create a PPPoE or PPTP interface.

I cannot configure a particular VLAN interface on top of an Ethernet interface even though I have it configured on top of another Ethernet interface.

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

The Zyxel Device's performance slowed down after I configured many new application patrol entries.

The Zyxel Device checks the ports and conditions configured in application patrol entries in the order they appear in the list. While this sequence does not affect the functionality, you might improve the performance of the Zyxel Device by putting more commonly used ports at the top of the list.

The Zyxel Device's anti-malware scanner cleaned an infected file but now the receiver cannot use the file.

If the MD5 hash value is incorrect, then Anti-Malware removes the last packet of the file. The file is still forwarded to the receiver, but they will not be able to open it. The receiver is not notified if a file is modified by the Zyxel Device. If the file cannot be used, the receiver should contact the Zyxel Device administrator to confirm if the Zyxel Device modified the file by checking the logs.

The Zyxel Device sent an alert that a malware-infected file has been found, but the file was still forwarded to the user and could still be executed.

Make sure you enable **Destroy Infected File** in the **Security Services > Anti-Malware** screen to modify infected files before forwarding the files to the user, preventing them from being executed.

I added a file pattern in the anti-malware allow list, but the Zyxel Device still checks and modifies files that match this pattern.

Make sure you enable the anti-malware allow list. If it is already enabled, make sure that the allow list entry corresponding to this file pattern is activated.

The Zyxel Device's performance seems slower after configuring IPS.

Depending on your network topology and traffic load, binding every packet direction to an IPS profile may affect the Zyxel Device's performance. You may want to focus IPS scanning on certain traffic directions such as incoming traffic.

IPS is dropping traffic that matches a rule that says no action should be taken.

The Zyxel Device checks all signatures and continues searching even after a match is found. If two or more rules have conflicting actions for the same packet, then the Zyxel Device applies the more restrictive action (**reject-both**, **reject-receiver** or **reject-sender**, **drop**, **none** in this order). If a packet matches a rule for **reject-receiver** and it also matches a rule for **reject-sender**, then the Zyxel Device will reject-both.

The Zyxel Device's performance seems slower after configuring DoS Prevention.

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.

Some of the files I download don’t go through Sandbox even though it is enabled.

The Sandbox feature only applies to certain file types. Check the list in **File Submission Options** to see if the file types you use are included. If they are, make sure you select their corresponding check box.

Sandbox detected a malicious file, but the file still went through the Zyxel Device and is still usable.

Make sure you set your Sandbox settings to destroy malicious files in the **Security Services** > **Sandbox**: **Action For Malicious File** drop-down list box.

The Zyxel Device destroyed/dropped a file/email without notifying me.

Make sure you enable logs for your security features, such as in the following screens:

- **Security Services** > **IPS**
- **Security Services** > **Anti-Malware**
- **Security Services** > **Sandbox**
- **Security Services** > **Reputation Filter**

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, SNAT is used for 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 Device HA to work.

Make sure to check the following:

- Both Zyxel Devices must be the same model with the same firmware version.
- Connect the Zyxel Devices using the correct heartbeat port. This is the highest-numbered copper Ethernet ports on the Zyxel Devices - see Table 260 on page 572.
- The heartbeat port must not be in an interface that is already configured for other features.
- Enable Device HA on both Zyxel Devices.
- The management IP addresses for both the active and passive Zyxel Devices must be in the same subnet.

- SSH service in **System > SSH** must be enabled on both Zyxel Devices.

If you are using NCC to manage the Zyxel Device, check the following:

- Both Zyxel Devices must be registered to the same account.
- The primary Zyxel Device must be registered to a site.
- Both Zyxel Devices must be in the same organization.

You may see the following error message if Device HA fails.

- **Device firmware or model mismatch detected**. Check that both Zyxel Devices are the same model with the same firmware version. Update both Zyxel Devices to the latest firmware available.

You may see one of the following error messages if Device HA fails in On Cloud mode (when using NCC to manage the Zyxel Device).

Note: See the *Nebula Online Help* for instructions on how to register and manage Zyxel Devices in NCC.

After fixing the error, wait a few moments, then do the Device HA pairing process again.

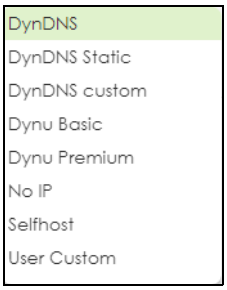
- **Device registration failed**. Device registration fails if both Zyxel Devices are not in an organization. Go to NCC and add both Zyxel Devices to an organization.
- **Devices belong to different organizations**. Both Zyxel Devices must be in the same organization. Go to NCC and add both Zyxel Devices to the same organization.
- **Device ownership mismatch**. Check that both Zyxel Devices are registered to the same account.
- **Device is not assigned to a site**. The primary Zyxel Device must be registered to a site. Go to NCC, and add the primary Zyxel Device to a site.
- **Internal server error**. A NCC server issue occurred during the pairing process. Check that the Zyxel Device has a stable network connection to NCC. If the error persists, contact technical support with the error details.

I cannot edit a configuration file while using Device HA.

If you apply a configuration file with Device HA enabled and you come across a problem such as being unable to edit the configuration file or interface ports go down, then use the CLI command `device-ha enable false` to disable Device HA, then apply the configuration file again. If the problem is now fixed, you can enable Device HA again using the Web Configurator or the CLI command `device-ha enable true`.

I cannot get Dynamic DNS to work.

- You must have set up an account for Dynamic DNS service. These are supported at the time of writing.



- Make sure you recorded your DDNS account's user name, password, and domain name and have entered them properly in the Zyxel Device.
- You must have a public WAN IP address to use Dynamic DNS.
- 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 get the application patrol to manage FTP traffic.

Make sure you have the FTP ALG enabled in **Network > ALG**.

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 and the chapter about interfaces for more information.

How can I see who is currently logged in and the login history?

See the login history from the logs. Go to **Log & Report > Log / Events > System**. Select **User** from the **Category** drop-down list.

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 IPSec VPN.

- 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 (via 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.
- 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.

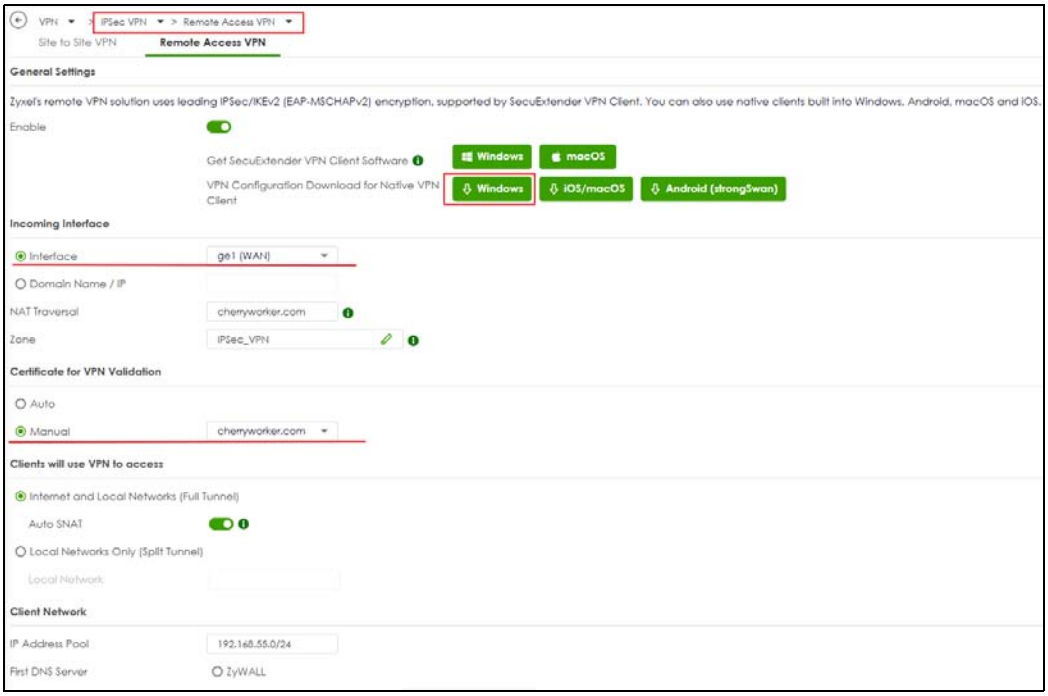
Windows 11 will not verify the certificate used in the Remote Access IPsec VPN script.

If the Remote Access IPsec VPN policy uses an interface, the **ServerAddress** in the downloaded Windows script will be the interface IP address. However, if the issuer of the certificate is a domain name instead of an interface IP address, then Windows 11 will not verify the certificate.

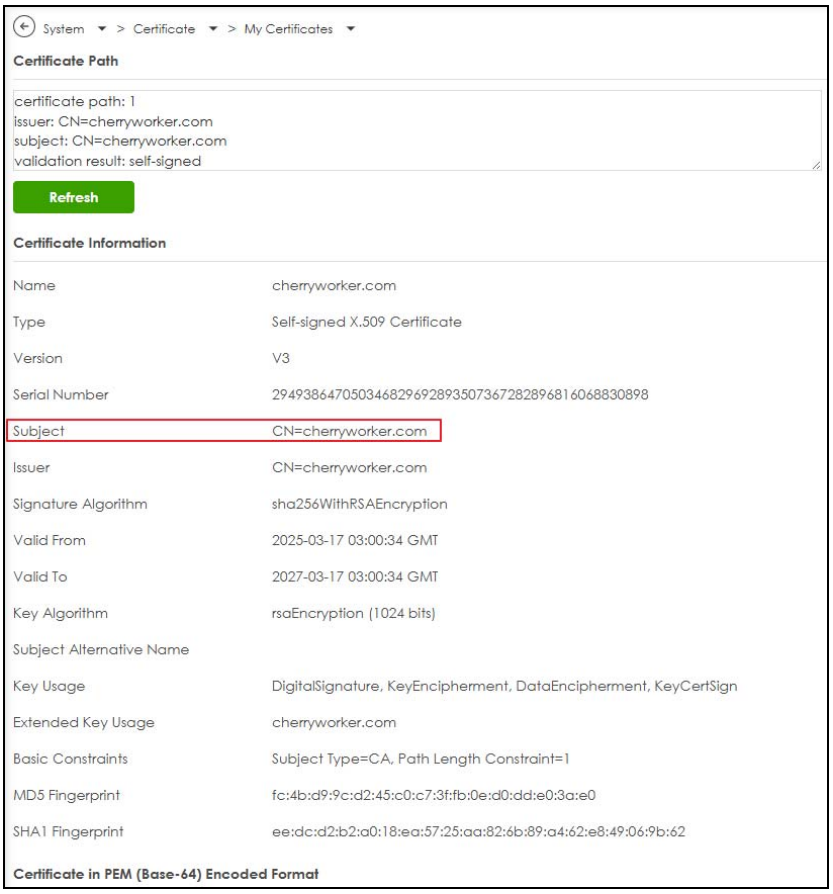
If you select **Interface** as the **Incoming Interface**, and the certificate is using a domain name or FQDN, then you must fill-in the same domain name or FQDN in **NAT Traversal**.

If you're using DDNS, make sure the DDNS IP address maps to the Incoming Interface IP address.

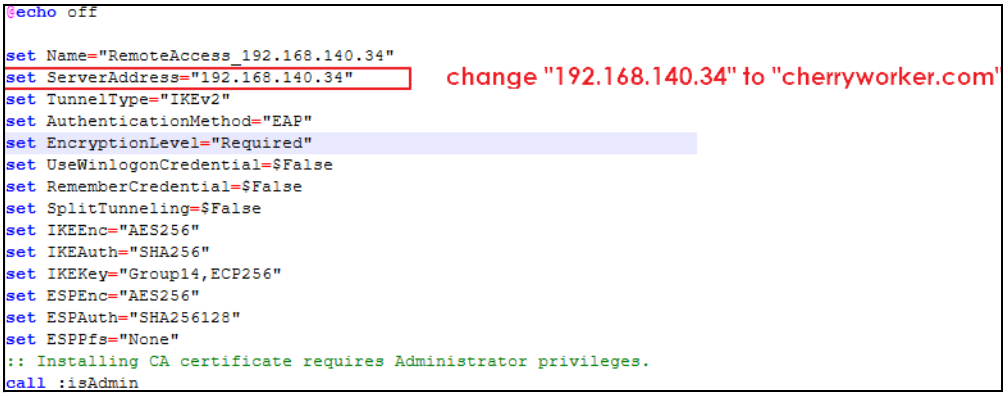
In the following Remote Access IPsec VPN policy example, you can see that the **Incoming Interface** is ge1, but the certificate for VPN validation uses a domain name (cherryworker.com).



In the certificate, the issuer of the certificate is shown in the **Subject** field (using the domain name, cherryworker.com for example).



To fix this you must edit the downloaded script using a text editor as follows. Change the **ServerAddress** IP address (192.168.140.34) to the domain name used in the **Subject** field of the certificate as shown in the above example certificate. Save the certificate, then use it in your IPSec VPN client on your Windows 11 computer.



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 application patrol to allow and manage access to a specific service but access is blocked.

If you want to use a service, make sure the security policy allows Security Service application patrol to go through the Zyxel Device.

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.

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.

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.

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.

My Zyxel Device CPU usage is too high. I see an alert log that says "abnormal TCP flag attack detected".

Your FTP server is in active mode. It is sending too much traffic to the Zyxel Device. Set your FTP server to passive mode.

My Zyxel Device's local storage is full.

Local storage contains database files, including data, logs, backups, packet capture files, and configuration files. When the local storage is full, new logs and files will not be saved. You can try manually deleting old logs from the GUI.

- **Remove** in **Maintenance > Configuration File > Configuration** to remove old configuration files
- **Remove** in **Maintenance > Diagnostics > Diagnostics** to remove old diagnostic files
- **Remove** in **Maintenance > Diagnostics > Packet Capture** to remove old packet capture files
- **Remove** in **Maintenance > Diagnostics > System Log** to remove old system logs

I cannot apply a configuration file.

The configuration file you upload to the Zyxel Device must meet the following requirements:

- The configuration file size cannot be 0.
- The configuration file must be a text file, a JSON file or a XML file.
- The model name in the configuration file must be the same as the Zyxel Device model you're uploading to.
- Use **Test** to check the configuration file for errors before applying it to the Zyxel Device.

My Zyxel Device cannot assign correct IP addresses to DHCP clients in my LAN and DMZ.

Make sure your Zyxel Device is the only device with DHCP server enabled in your network.

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 **Network Status** > **Device Insight** > **Feedback**.

I cannot remove a client in **Network Status** > **Device Insight**.

Clients that are blocked cannot be removed. Please make sure to unblock the client you want to remove first.

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. Can store files up to 2 GB.

   FAT32 supports Windows, macOS, and Linux. Can store files up to 4 GB.

   EXT3 supports Linux. Can store files up to 2 TB.

   EXT4 supports Linux. Can store files up to 16 TB.
4. Click **Start** to begin the formatting process.

I cannot use SNMP to control or monitor the managed APs through the Zyxel Device.

Go to Wireless > Access Points > AP List. If the managed AP's status is **Limited AP** and its **Edit AP** screen's **Status** shows **SNMP 2 Community** in the **Non Support** field, the managed AP does not support the SNMP configuration on the Zyxel Device. Managed APs with firmware version 7.20 or lower can only support one read-only and one read-write SNMP community. Make sure the firmware versions of both your Zyxel Device and managed AP are up to date.

Wireless clients are not being load balanced among my Zyxel Device.

- Make sure that the managed APs you want to share the client load are in the same load balancing group. See Section 29.3.3 on page 515 for details.
- Make sure that the wireless clients are in range of the other managed APs; if they are only in range of a single manged AP, then load balancing may not be as effective.

My Powered Devices (PDs) are not receiving power.

If the **Port Status** in **Dashboard > System** displays **Disabled** in the **PoE Status** field when you hover the mouse over the port, follow the steps below for troubleshooting.

1. Check the Table 13 on page 60 for the PoE Power Budget of the Zyxel Device. When the total power requested by the PoE-enabled devices exceeds the budget, the last PoE-enabled device connected to the Zyxel Device will not be powered up. At the time of writing, you can only use CLI commands to view the power usage on each port. Refer to the CLI RG for details.
2. Make sure the PDs are functional.
   - Check whether the PDs are malfunctioning. See your PDs user's guide for more information.
   - Make sure the connected PDs support PoE.
   - If the connected PDs do not fully comply with the Zyxel Device's supported PoE standard (See Table 13 on page 60 for the Zyxel Device's supported PoE standards), replace the PDs with PoE standard-compliant devices for better compatibility.
3. Make sure the Ethernet cables connected to the PDs are functional.
   - Use the correct type of Ethernet cable for the corresponding PoE standard you are using. See Table 14 on page 60 for the Zyxel Device's supported PoE standards and supported Ethernet cables.
   - Check whether the Ethernet cables are malfunctioning. Use functional Ethernet cables to reconnect the PDs to the Zyxel Device.

There is no data or data is missing in SecuReporter.

If no data is displayed for your Zyxel Device in SecuReporter, check the following:

- Make sure the Zyxel Device is registered with and connected to Nebula. See How to activate and enable SecuReporter for details.
- Make sure the SecuReporter license is valid and has not expired.
- Use the CLI command `vrf main secureporter traffic-log enabled true` to have the Zyxel Device send traffic logs to SecuReporter. Refer to the CLI RG for details.

If partial data for your Zyxel Device is missing in SecuReporter, check the following:

- Make sure the license required for the feature with missing data is valid and has not expired.
- Make sure the categories related to the missing data are enabled in **Log & Report > SecuReporter**.
- If the missing data is related to client information, make sure **Device Insight** is enabled in **System > Advanced** so that the Zyxel Device can collect status and basic information about clients connected to its internal interfaces or IPSec VPNs.

37.1 Reserved System Ports

The Zyxel Device reserves the following system ports.

Note: You cannot change a service port to a reserved system port.

Table 332 Reserved System Ports

TCP PORTS	UDP PORTS
53	53
179	67
830	68
953	500
2601	546
2602	547
2603	1812
2604	1813
2605	3799
2616	4500
5432	5246
7681	5247
7682	18121
8089	

37.2 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 will need to reset the Zyxel Device to its factory-default settings.

Note: All configuration files, including those you saved on the Zyxel Device, will be deleted.

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. It is recommended you regularly save configuration changes to your computer.

Note: This procedure removes the current configuration.

Using the RESET Button

1 Make sure the **PWR/SYS** LED is on and not blinking.

2 Press the **RESET** button and hold it until the **PWR/SYS** LED begins to blink. (This usually takes about 7 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.

Using CLI

If the **RESET** button is not working, use a terminal emulation program to reset your Zyxel Device:

1 Connect the console port of Zyxel Device to your computer using a console cable.

2 Open a Terminal Emulation program, such as Tera Term. Click **Setup** > **Serial port**, set the **Speed** to **115200**, and click **New setting** to save the changes.

3 Press the **REBOOT** button and hold it until the **PWR/SYS** LED begins to blink. (This usually takes about 5 seconds.)

4 When the following text appears in the terminal emulation program, press any key within 3 seconds to enter debug mode.

```
BootModule Version: V1.1.5 Oct 11 2024 02:52:20
DRAM: Size = 8192 Mbytes

Press any key to enter debug mode within 3 seconds.
```

5 You will see `Enter Debug mode` in the terminal emulation program, indicating the Zyxel Device is now in debug mode. Type `atkz -b` and press **Enter** to reset the Zyxel Device to the factory defaults.

6 Type `atgo` and press **Enter** to restart the Zyxel Device. All configurations on the Zyxel Device are now reset to the factory defaults.

```
USG FLEX 500H> atkz -b
-b
OK

USG FLEX 500H> atgo
Booting…
RAM test …… done!
```

37.3 Restarting the Zyxel Device

You may want to restart the Zyxel Device when experiencing network connectivity issues. If you want to use the standby firmware as the running firmware, then select the standby firmware and restart.

Note: When you restart the Zyxel Device, current configurations saved will not be removed.

Note: If **startup-config.conf** has an error, the Zyxel Device may restart with an older configuration file or the factory default configuration file with all your configurations lost. Use **Test** in **Maintenance** > **Firmware/File Manager** > **Configuration** to make sure that **startup-config.conf** does not have an error. See Configuration File Flow at Restart for details on which configuration files are used at start-up.

Use one of the following procedures to restart the Zyxel Device.

Using the REBOOT Button

Use a pin to press and hold the **REBOOT** button on the Zyxel Device until the **PWR/SYS** LED starts blinking.

Using the Web Configurator

Go to the **Maintenance** > **Reboot/Shutdown** screen and click the **Reboot** button to restart the Zyxel Device.

Using CLI

Use a terminal emulation program, such as Tera Term, to restart your Zyxel Device.

1. Connect the console port of Zyxel Device to your computer using a console cable.
2. Open a terminal emulation program. Click **Setup** > **Serial port**, set the **Speed** to **115200**, and click **New setting** to save the changes.
3. Log in first. Type the command `copy running startup` to save the current configurations as the startup configurations.
4. Type `cmd reboot force` and press **Enter** to restart the Zyxel Device.

37.4 Getting More Troubleshooting Help

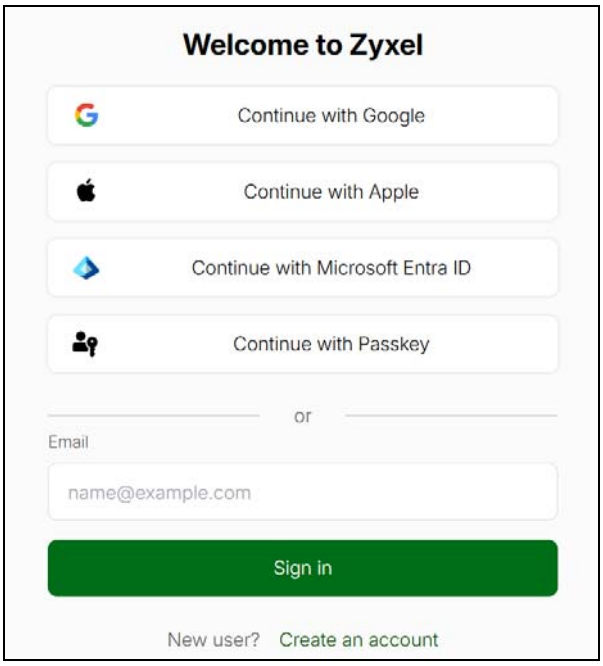
Go to *support.zyxel.com* to find other information on the Zyxel Device.

APPENDIX A
Zyxel Account Authentication

Overview

There are several ways to log into Zyxel Web Portals, such as Nebula, Circle, SecuReporter, and so on. At the time of writing, the available login methods are listed below.

- Google or Apple Account Login (Google or Apple)
- Microsoft Entra ID
- Passkey (fingerprint, Face ID or PIN)



Google or Apple Account Login

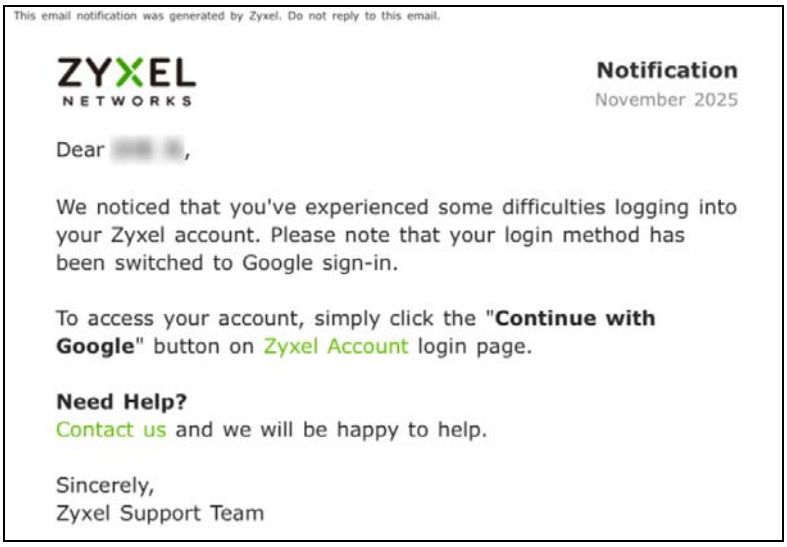
Zyxel Web Portals support logging in with Google or Apple accounts. This section shows you how to:

- Continue with Google
- Continue with Apple

However, there are a few limitations. If you want to switch from email and password login to Google or Apple account login, the system will prompt you to confirm the change. You must accept this prompt to use your Google or Apple account for future logins.

For example, if you already have a Zyxel Account and want to use **Continue with Google** so you can log in with your Google credentials, you can follow the steps below to switch the login method to Google.

Note: Once you have successfully logged in with a Google or Apple account, you can only use this method for future logins. If you try to log in with email and password after a successful login with your Google or Apple account, the login will fail, and you will receive an email notifying you that your login method has been switched to Google or Apple sign-in. Contact customer support if you want to undo this change.



This email notification was generated by Zyxel. Do not reply to this email.

ZYXEL NETWORKS

Notification
November 2025

Dear [redacted],

We noticed that you've experienced some difficulties logging into your Zyxel account. Please note that your login method has been switched to Google sign-in.

To access your account, simply click the "**Continue with Google**" button on Zyxel Account login page.

Need Help?
Contact us and we will be happy to help.

Sincerely,
Zyxel Support Team



This email notification was generated by Zyxel. Do not reply to this email.

ZYXEL NETWORKS

Notification
November 2025

Dear [redacted],

We noticed that you've experienced some difficulties logging into your Zyxel account. Please note that your login method has been switched to Apple sign-in.

To access your account, simply click the "**Continue with Apple**" button on Zyxel Account login page.

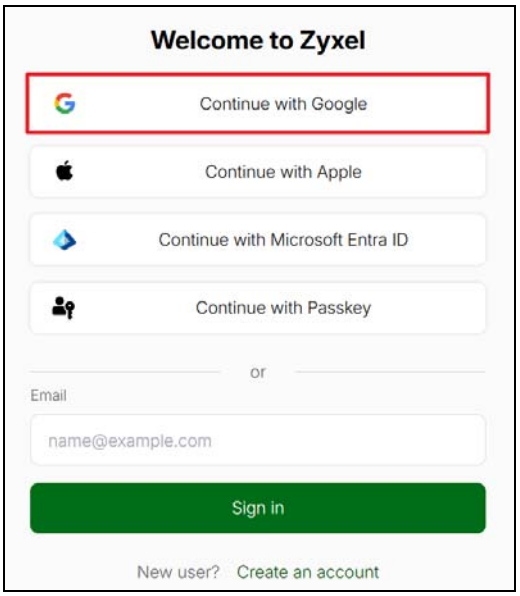
Need Help?
Contact us and we will be happy to help.

Sincerely,
Zyxel Support Team

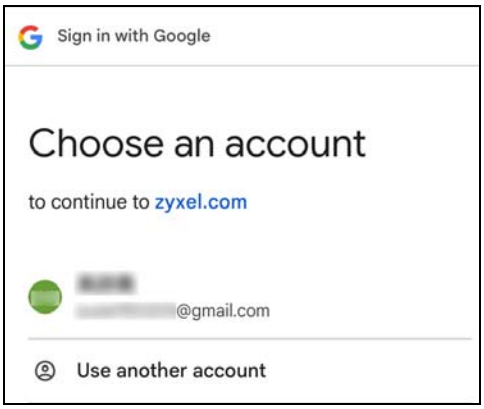
Note: Configure two-factor authentication, password changes, and password recovery through your Google or Apple account. You cannot use organization-wide two-factor authentication when you log in using a Google or Apple account.

Continue with Google

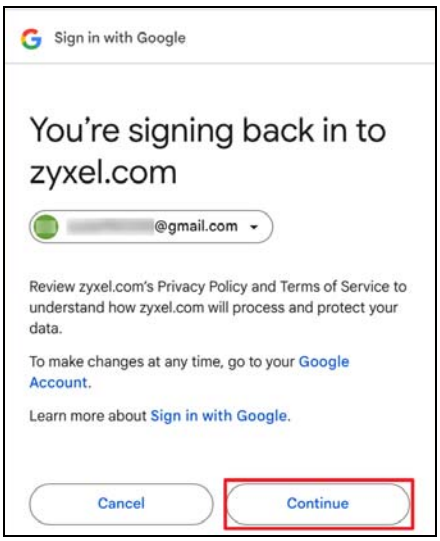
1 On the Zyxel Account login page, click **Continue with Google**.



2 Log in to your Google account. If you are already logged in, follow the system prompt and select an account you want to log in with.

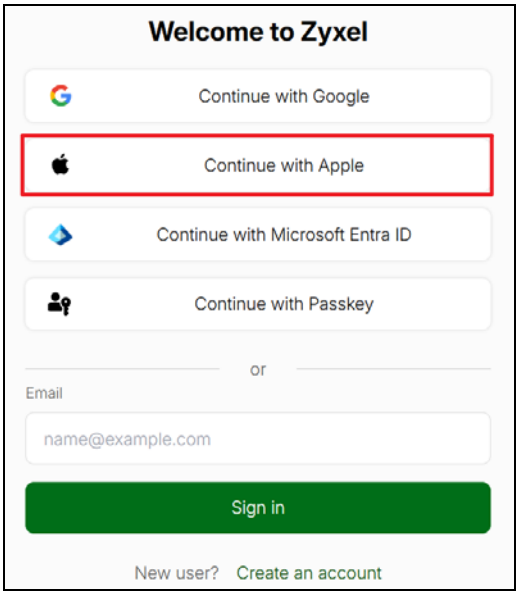


3 Click **Continue** so your future login method will be **Continue with Google** only.

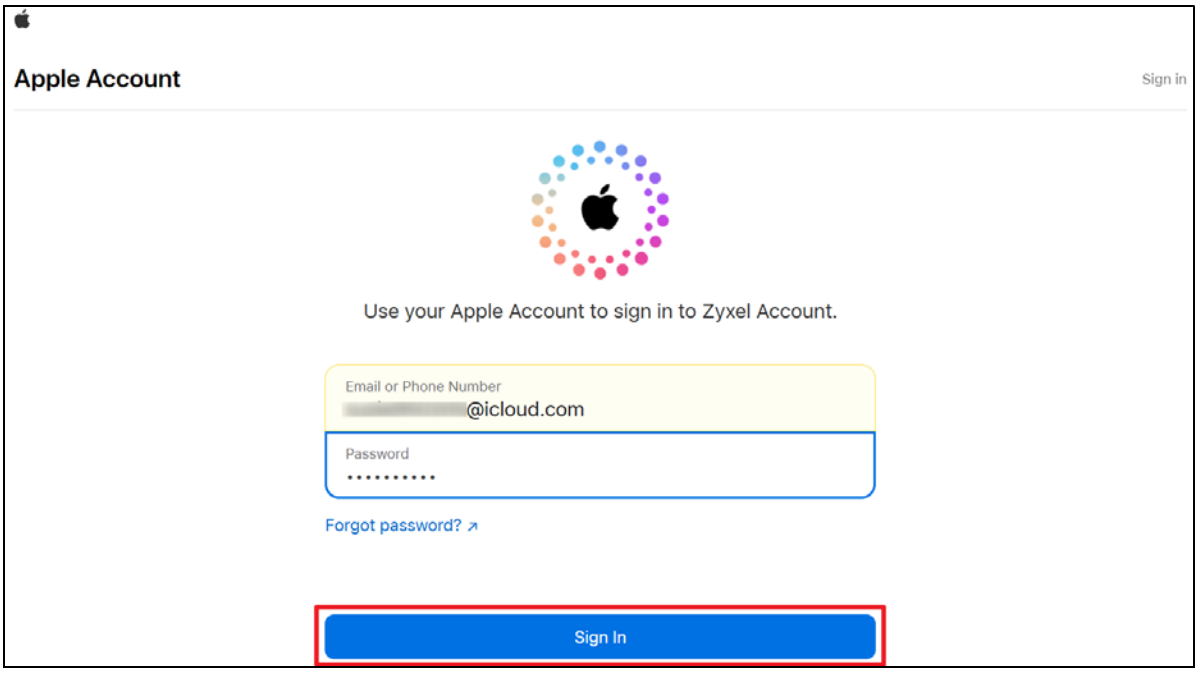


Continue with Apple

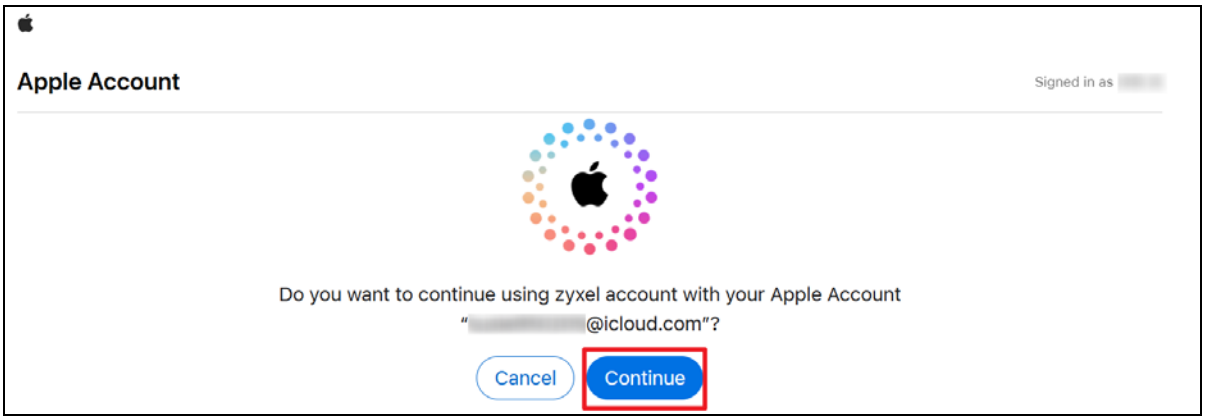
1 On the Zyxel Account login page, click **Continue with Apple**.



2 Log into your Apple account.



3 Click **Continue** so your future login method will be **Continue with Apple** only.



Microsoft Entra ID

Microsoft Entra ID is Microsoft's cloud-based identity and access management service that allows organizations to manage user accounts, and enables Single Sign-On (SSO) across all platforms. Entra ID reduces password management overhead and improves security by ensuring that only authenticated users can access the Zyxel Account.

The following tutorial is for administrators, most likely the IT team in your organization, to configure the initial settings before general users can log in using this method.

In this section, we show you how to:

- Enable Microsoft Entra ID
- Create Enterprise Application
- Configure Single Sign-on
- Configure **Attributes & Claims**
- Download and Upload the Metadata File
- Verify the Entra ID Configuration
- Assign Users and Groups
- Deploy Entra ID Settings

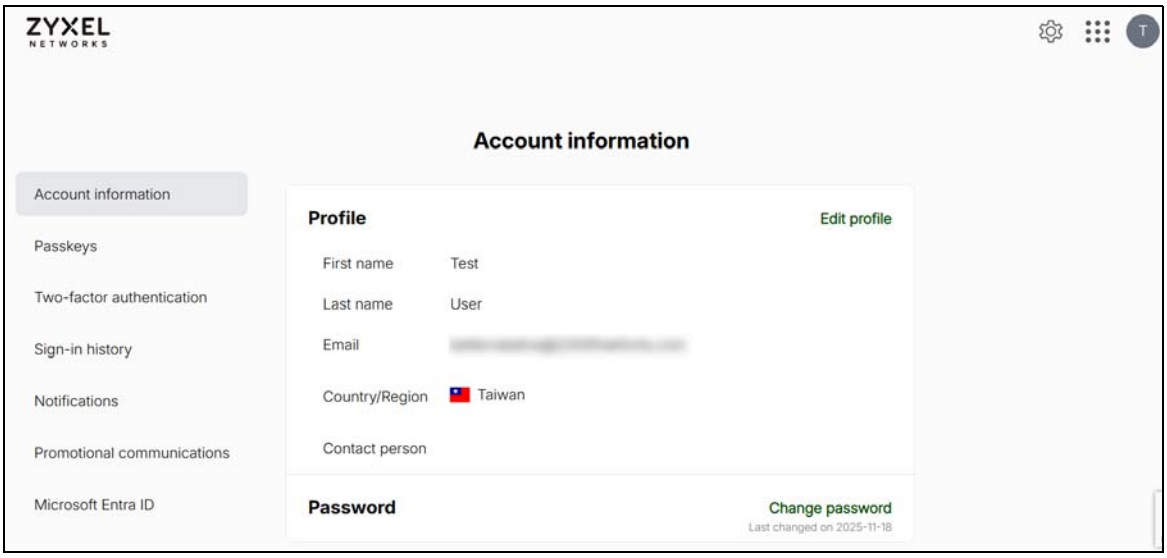
Before You Begin

You must have the following to set up Entra ID sign-in.

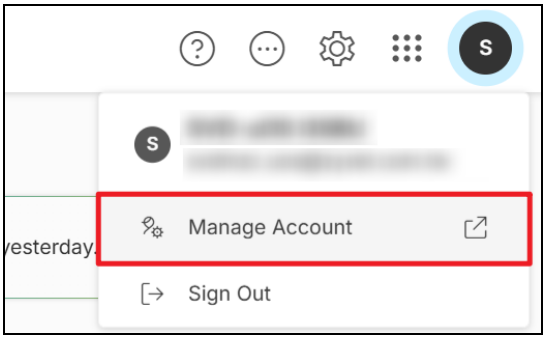
- Microsoft Entra ID administrator account with global administrator privileges.
- Zyxel Account using email and password sign-in method.

Enable Microsoft Entra ID

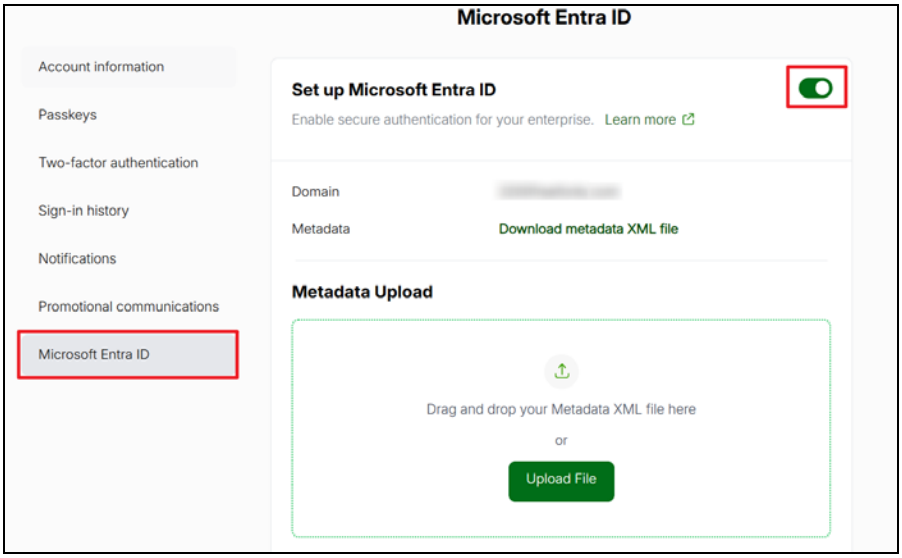
1 Go to your *Zyxel Account*.



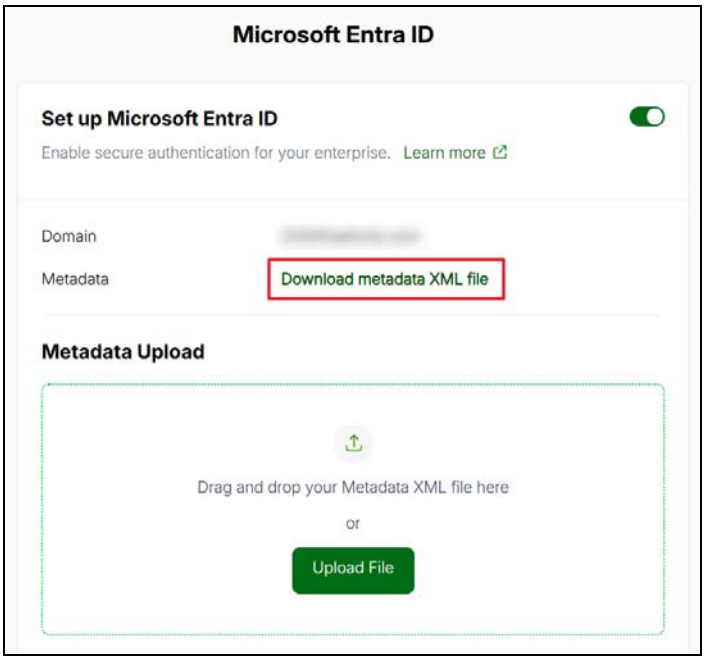
Alternatively, navigate to **Manage Account** under the profile picture when you are in another Zyxel platform.



2 Go to the Microsoft Entra ID tab, and click the **Set up Microsoft Entra ID** switch to the right.

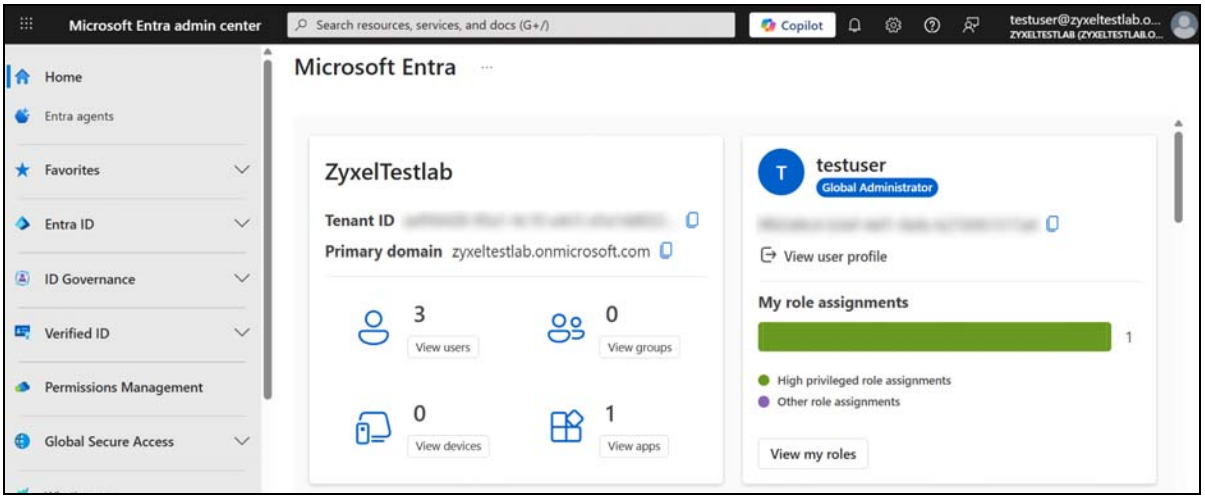


3 Click **Download metadata XML file**. You will need this later.



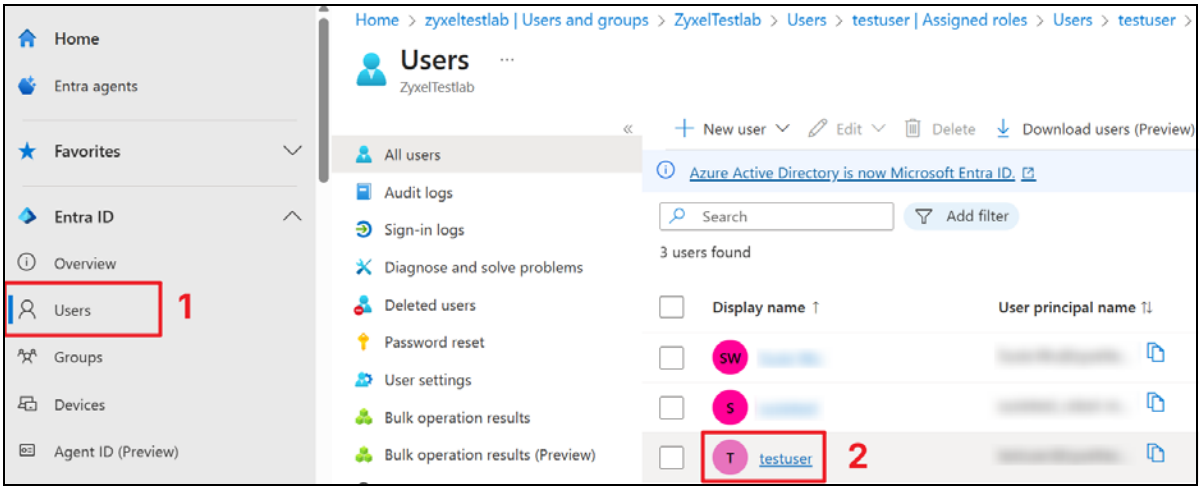
Create Enterprise Application

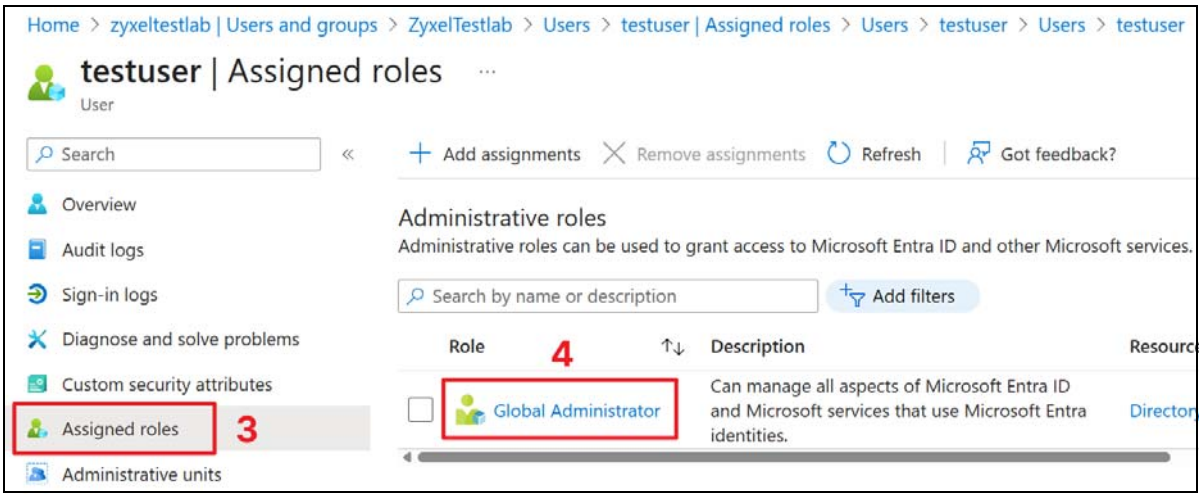
1 Go to the *Microsoft Entra admin center*. Sign in with a Microsoft Entra tenant account that has global administrator privileges.



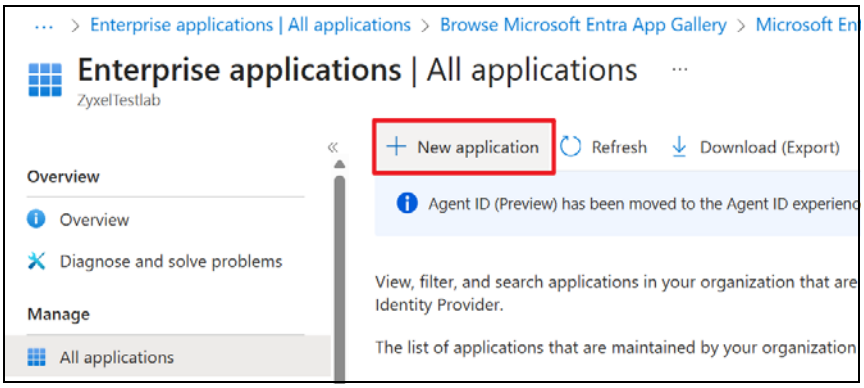
Note: A personal Microsoft account (such as Outlook.com) will not work. If your company uses Microsoft 365, a valid account would be something like username@yourcompany.com.

Note: To know if your account has global administrator privileges, go to **Users > your user name > Assigned roles > Role** to view your role.

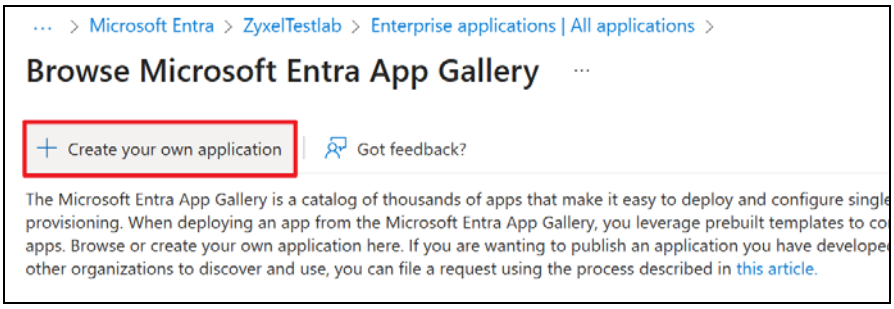




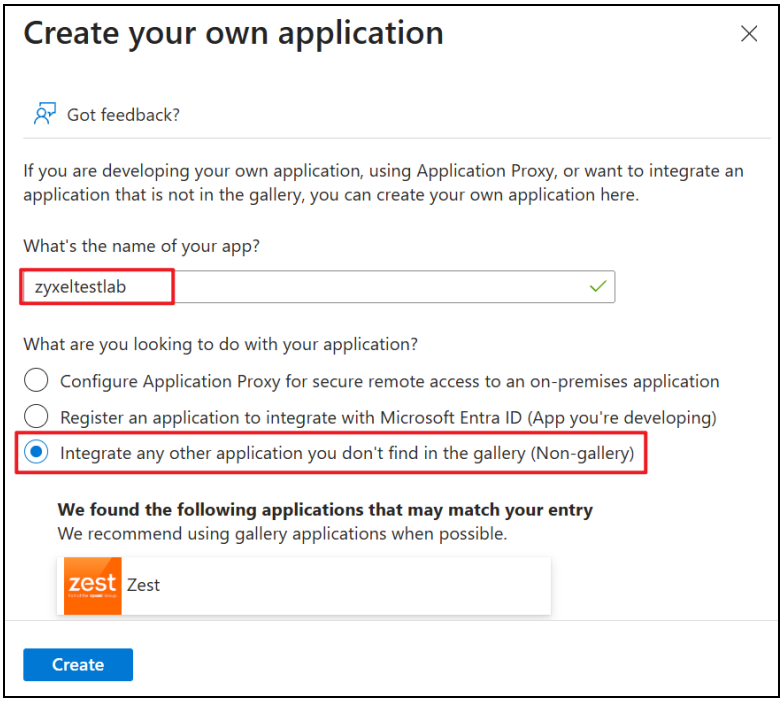
2 Go to **Enterprise apps > All applications**, and click **New application**.



3 Click **Create your own application**.



4 Enter a name for your application. Select **Integrate any other application you don't find in the gallery**. Then, click **Create**.

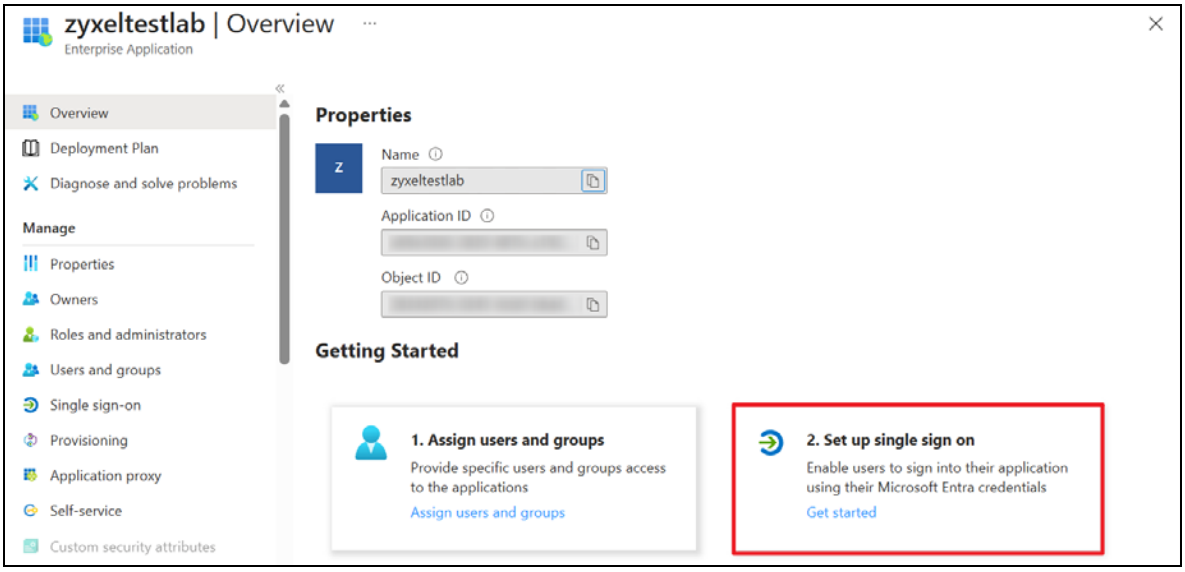


Note: The application name must not exceed 93 characters and cannot contain the following characters: '<', '>', ':', '&', '%'.

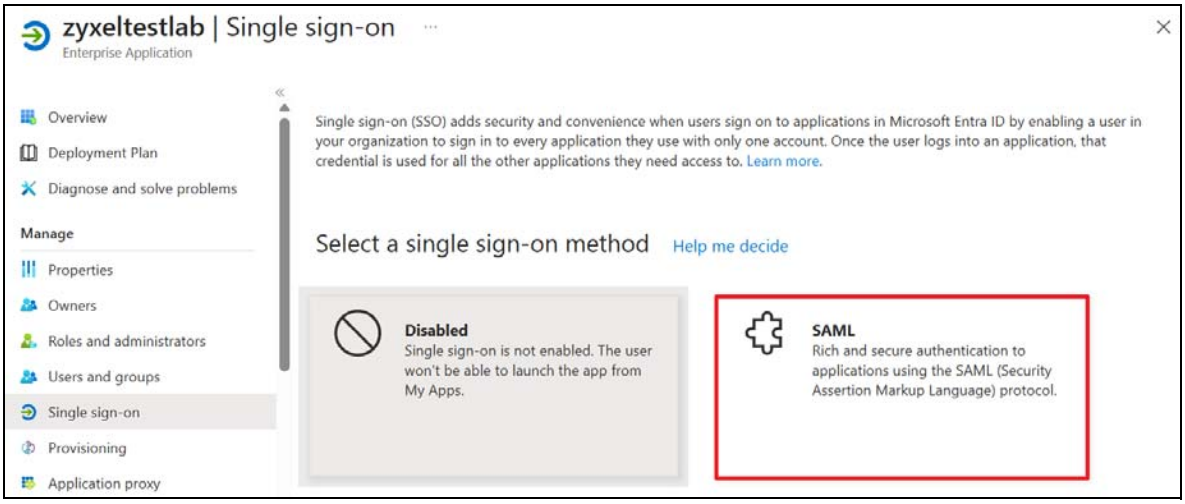
Configure Single Sign-on

Next, you need to configure single sign-on, which allows you to use the same login criteria on different platforms.

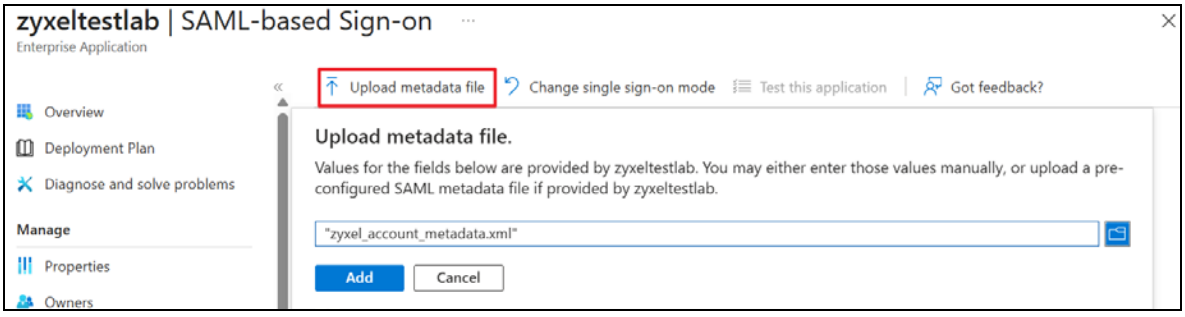
1 Select **Set up single sign on**.



2 Select **SAML** as the sign-on method.



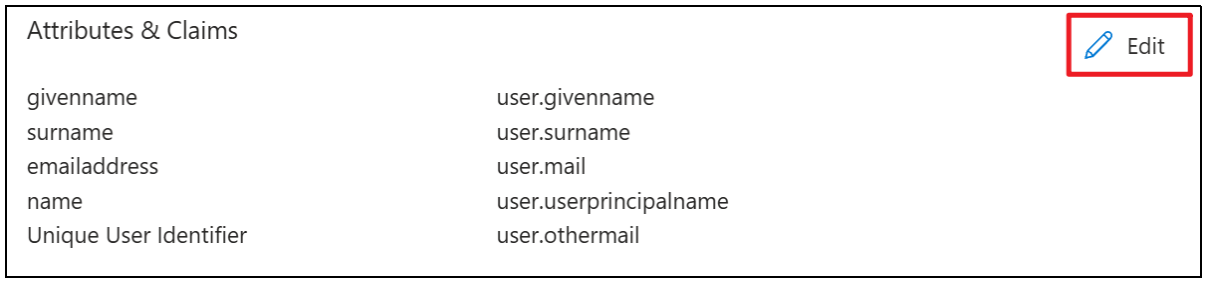
3 Upload the metadata XML file you downloaded in step 3 of the **Enable Microsoft Entra ID** section.



Configure Attributes & Claims

Define **Attributes & Claims** at the application level. These claims tell the portal what user information to expect during login. All users assigned to this application automatically inherit these claims. You only need to configure this once.

1 Click **Edit** to configure this section.

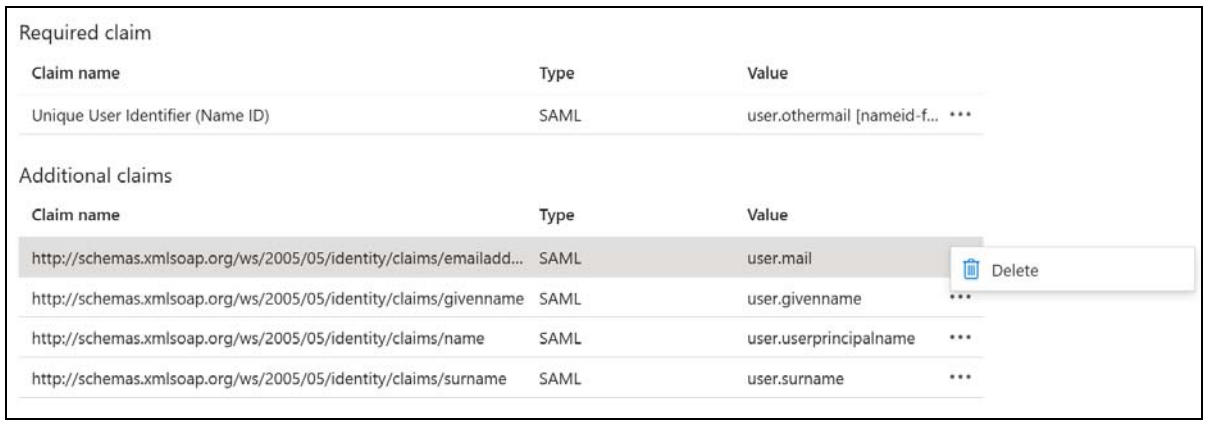


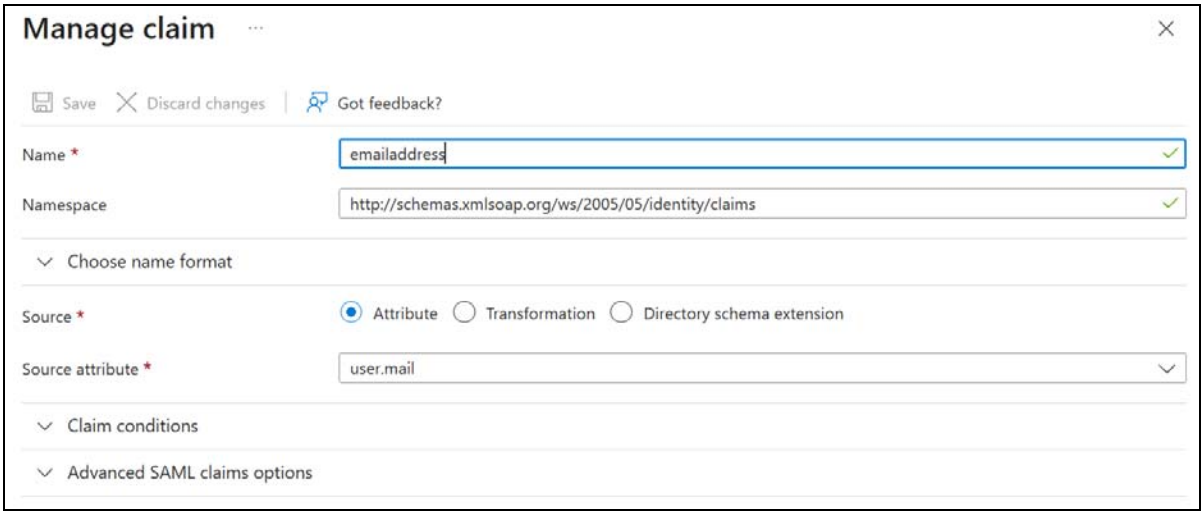
The default value and descriptions of each claim are shown in the table below.

CLAIM	DEFAULT VALUE	OPTIONAL / REQUIRED	DESCRIPTION
givenname	user.givenname	Optional	User's first name.
surname	user.surname	Optional	User's last name.
emailaddress	user.mail	Optional	User's primary email.
name	user.userprincipalname	Optional	User's login ID or display name shown in the portal.
Unique User Identifier	user.othermail	Required	Unique internal ID used by the portal to identify the user.

Note: Most Zyxel portals accept the system's default Attributes & Claims. When integrating Entra ID login with other portals, check if they require any specific attribute mappings.

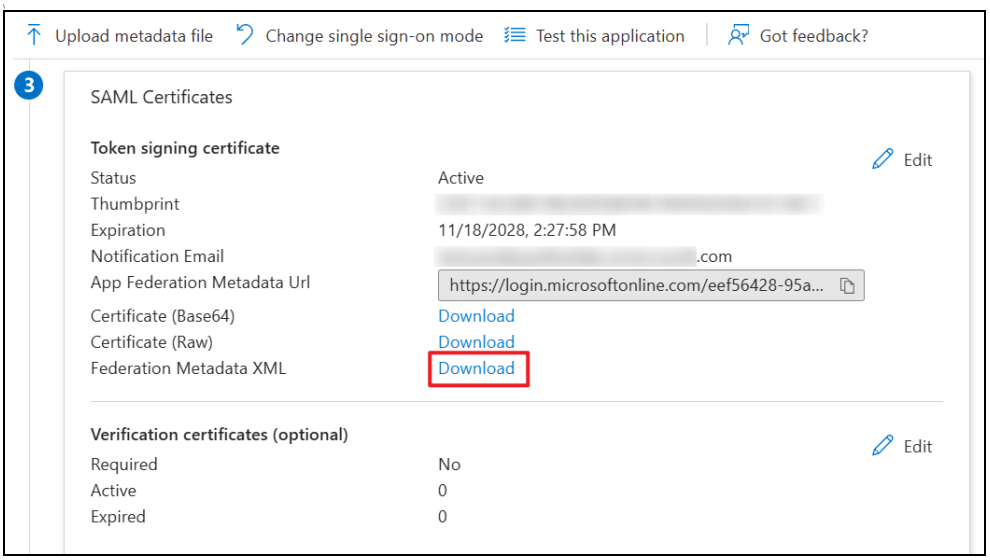
2 Click the claim that you want to edit to enter the **Manage claim** screen, or delete any claims you do not need.



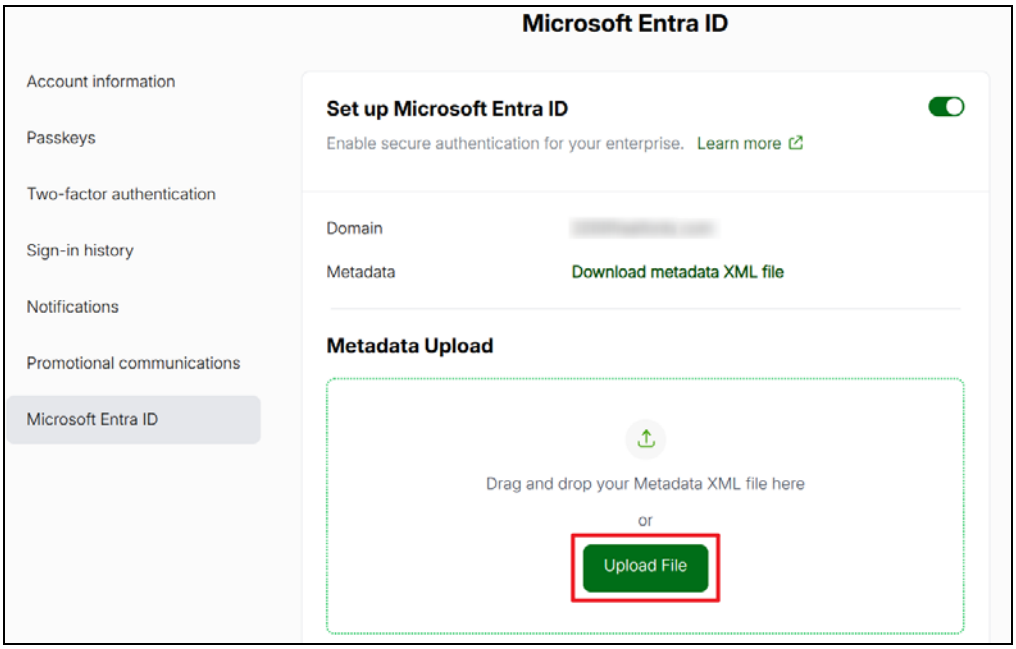


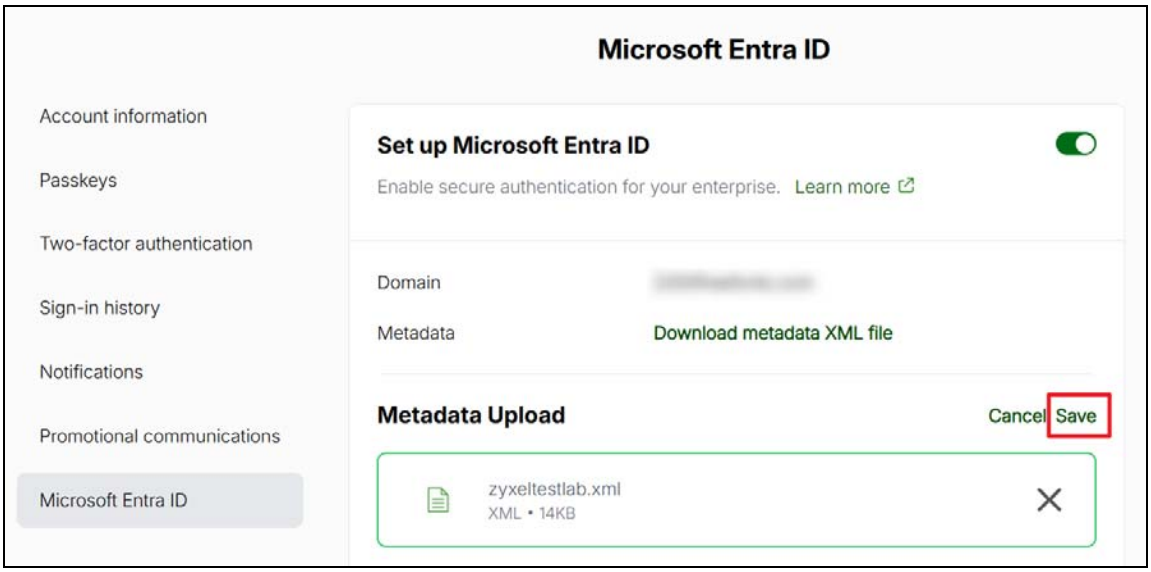
Download and Upload the Metadata File

1 On the **Single sign-on** page, go to the **SAML Certificates** section, and download the **Federation Metadata XML** file.



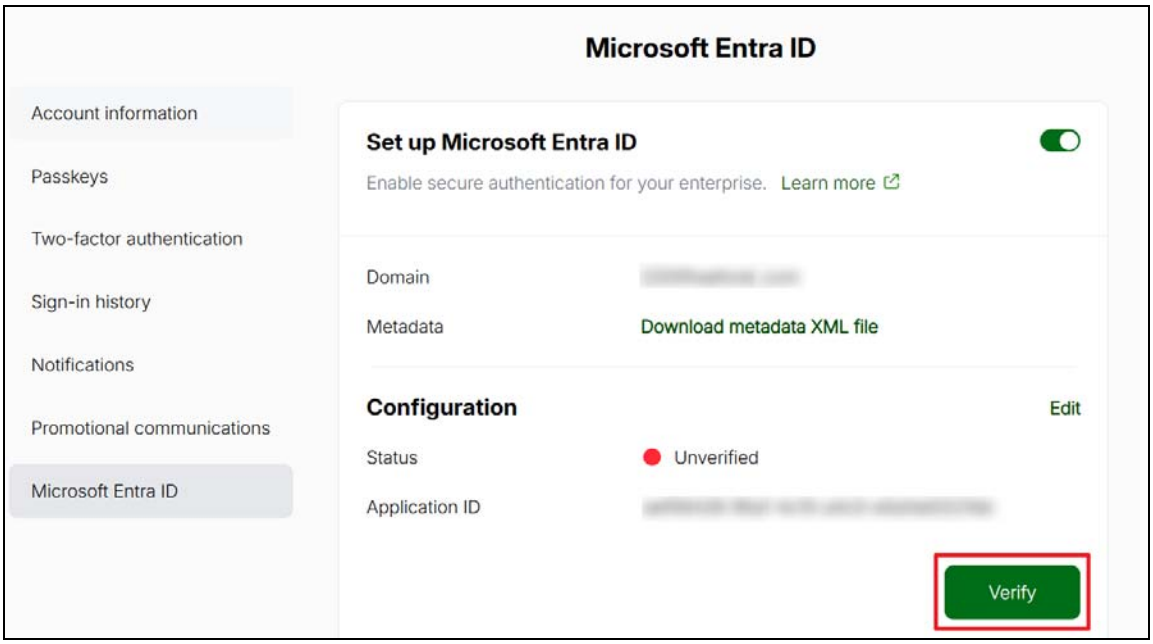
2 Open your Zyxel Account page. Click **Upload File**, and select the file you downloaded in the previous step. Then, click **Save**.



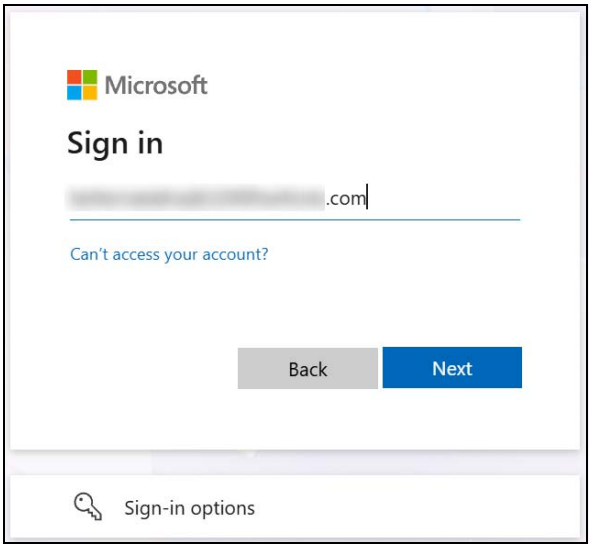


Verify the Entra ID Configuration

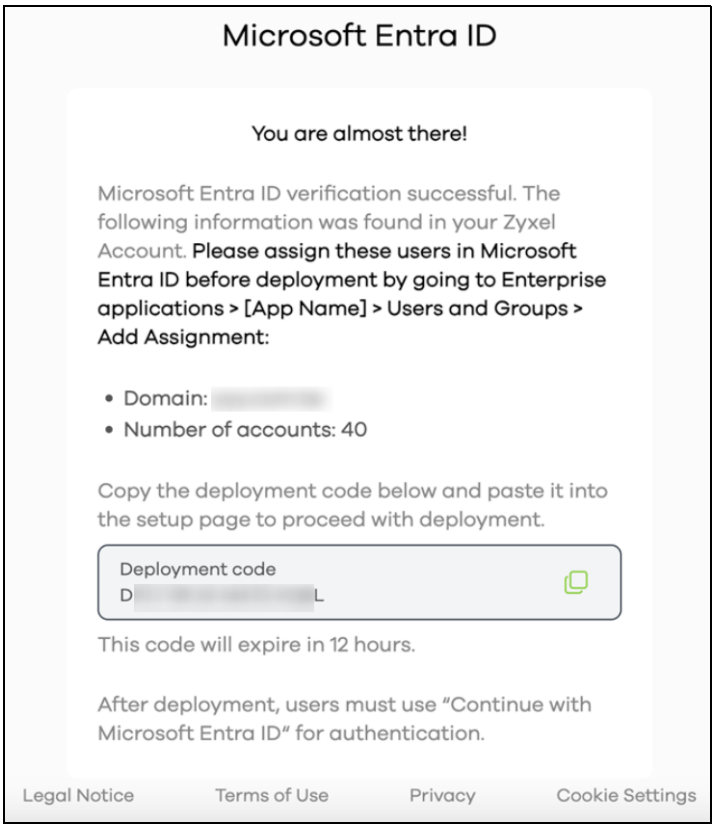
1 Click **Verify** to open a new verification page.



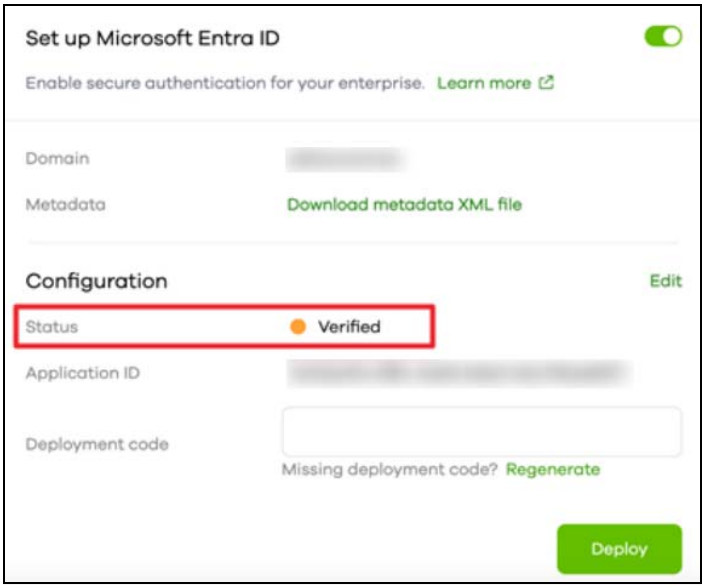
2 Sign in using the same email as your Zyxel Account.



3 Upon successful login, you will see a verification success page with a Deployment code.

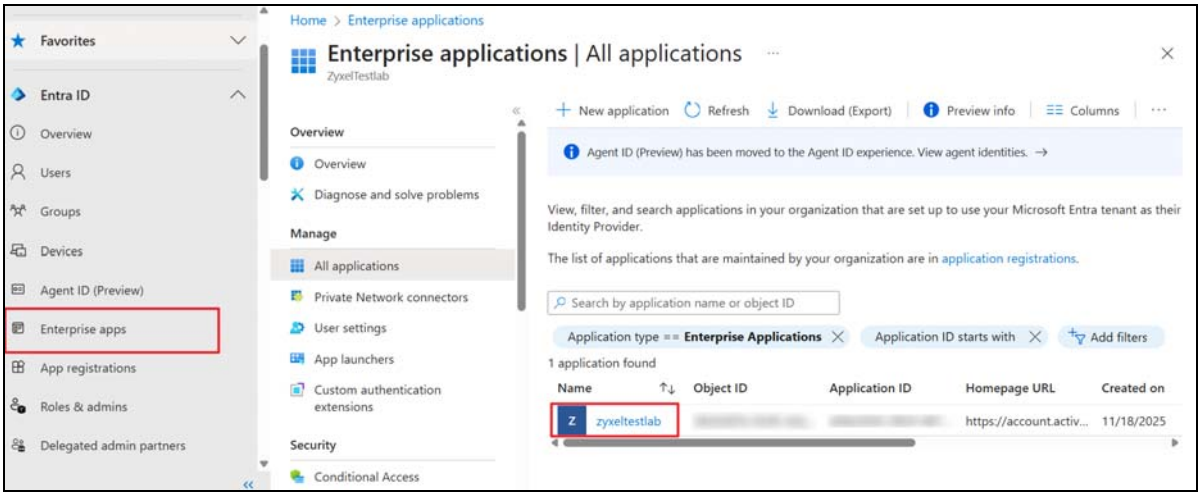


4 The status will change to **Verified** on the Entra ID Settings page.

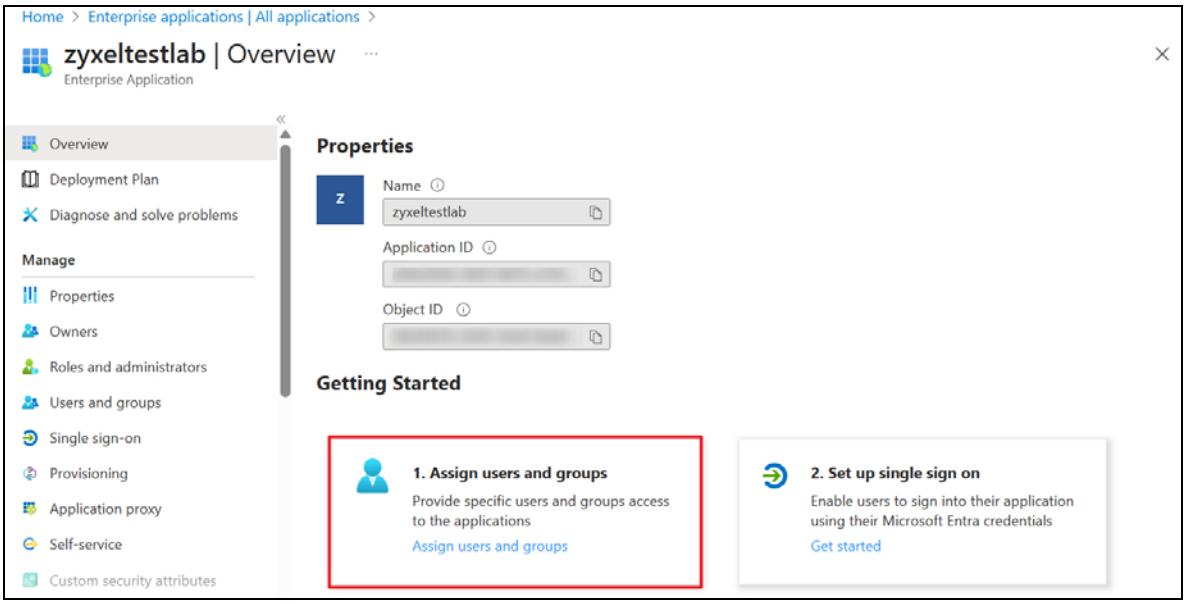


Assign Users and Groups

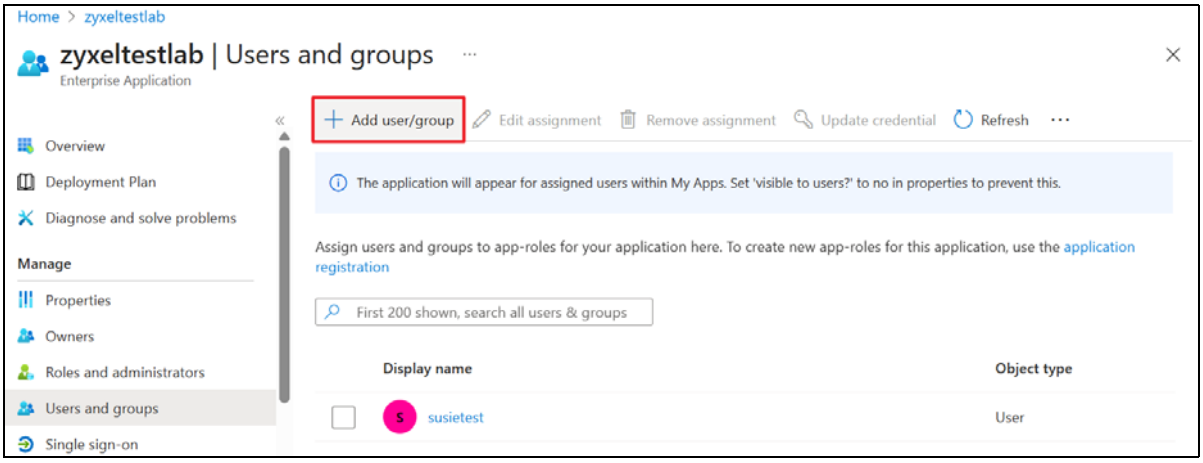
1 Return to the Microsoft Entra admin center. Go to **Enterprise apps**, and click on the application that you created earlier.



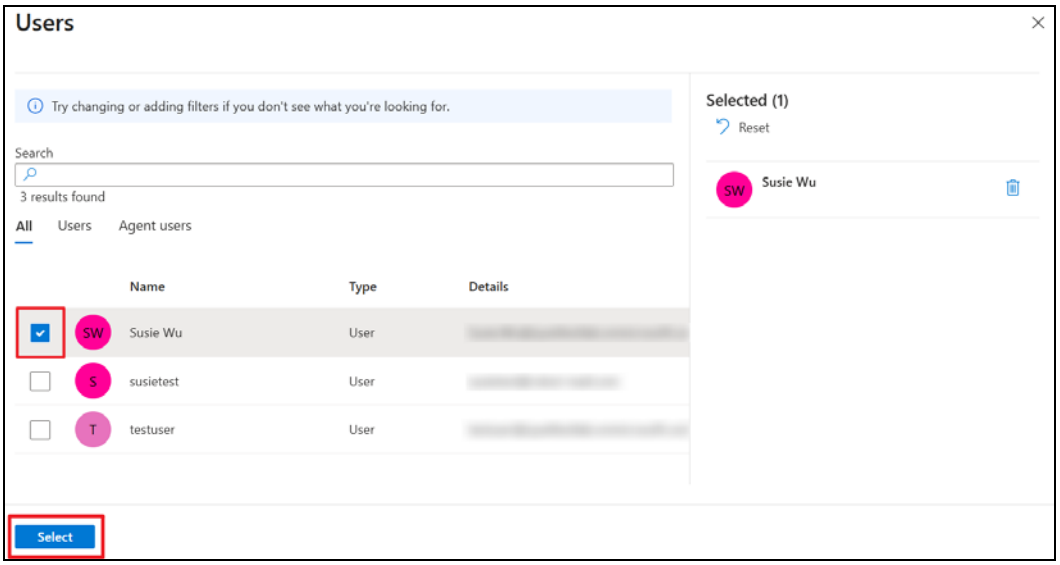
2 Click **Assign users and groups**.



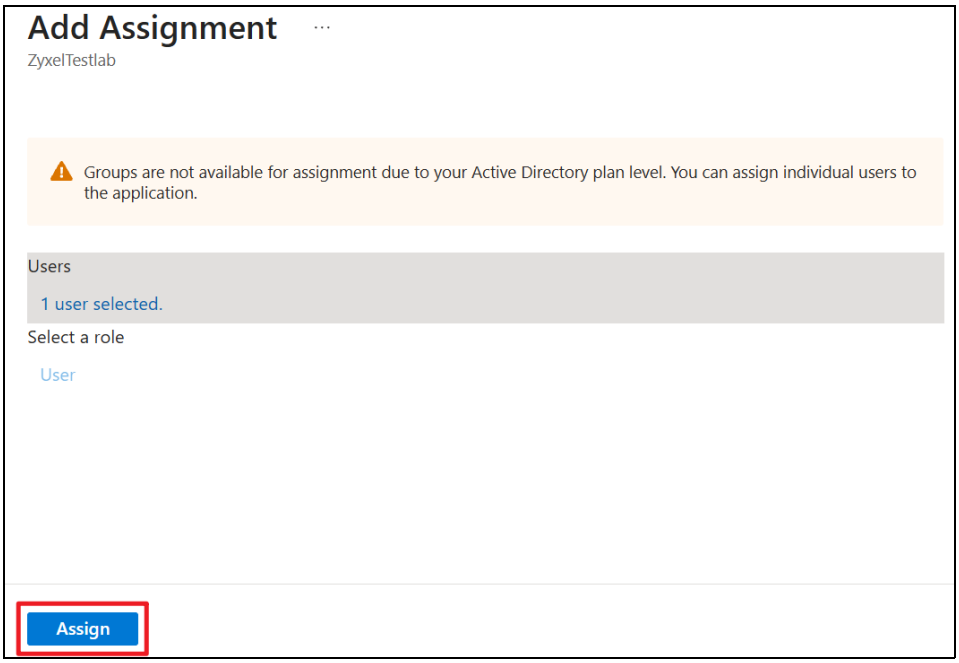
3 Click **Add user/group**.



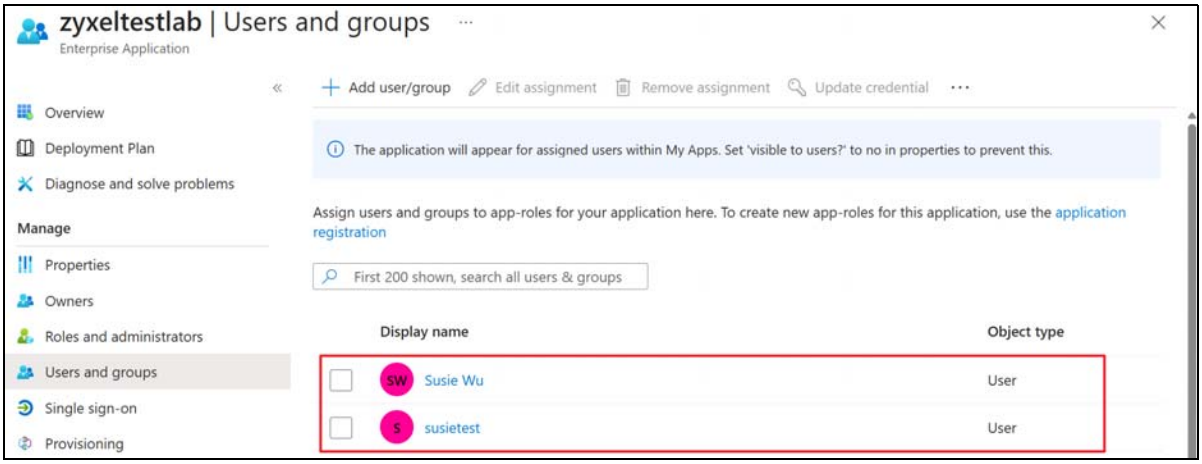
4 Select which users can use Microsoft Entra ID to access the company platform. Click **Select**.



5 Click **Assign** to assign a role to the users.

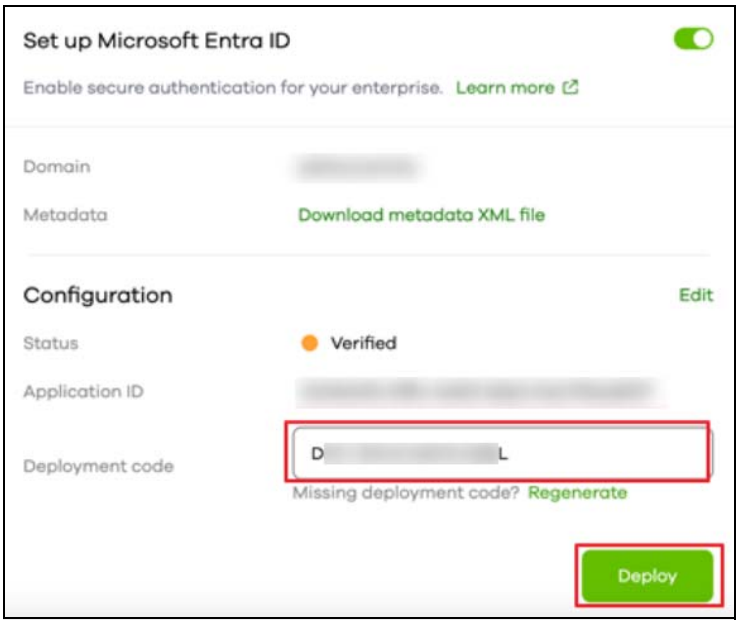


6 The users that are added to this application will display on the **Users and groups** screen.

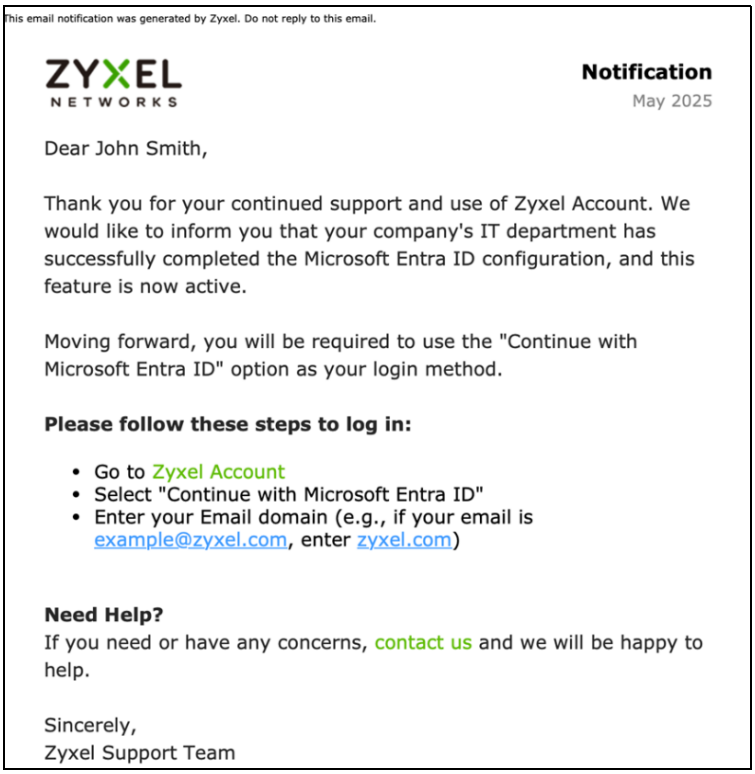


Deploy Entra ID Settings

1 Copy the Deployment code from step 3 of the **Verify the Entra ID Configuration** section, and paste it in the **Deployment code** field on your Zyxel Account page. Then, click **Deploy**.



2 Selected users will receive a notification email.



This email notification was generated by Zyxel. Do not reply to this email.

ZYXEL NETWORKS

Notification
May 2025

Dear John Smith,

Thank you for your continued support and use of Zyxel Account. We would like to inform you that your company's IT department has successfully completed the Microsoft Entra ID configuration, and this feature is now active.

Moving forward, you will be required to use the "Continue with Microsoft Entra ID" option as your login method.

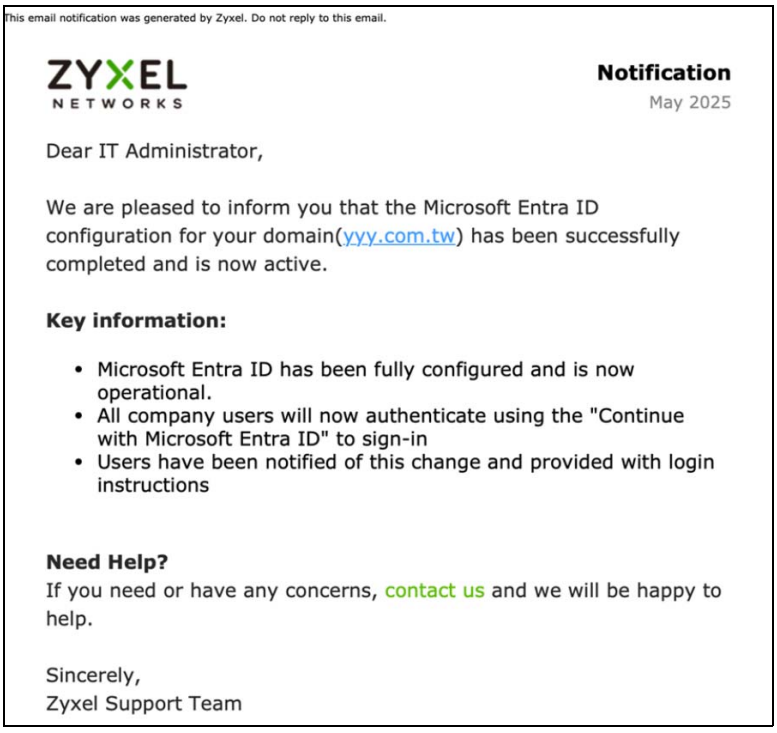
Please follow these steps to log in:

- Go to Zyxel Account
- Select "Continue with Microsoft Entra ID"
- Enter your Email domain (e.g., if your email is example@zyxel.com, enter zyxel.com)

Need Help?
If you need or have any concerns, contact us and we will be happy to help.

Sincerely,
Zyxel Support Team

3 You as the administrator will also receive a confirmation email.



This email notification was generated by Zyxel. Do not reply to this email.

ZYXEL NETWORKS

Notification
May 2025

Dear IT Administrator,

We are pleased to inform you that the Microsoft Entra ID configuration for your domain(yyy.com.tw) has been successfully completed and is now active.

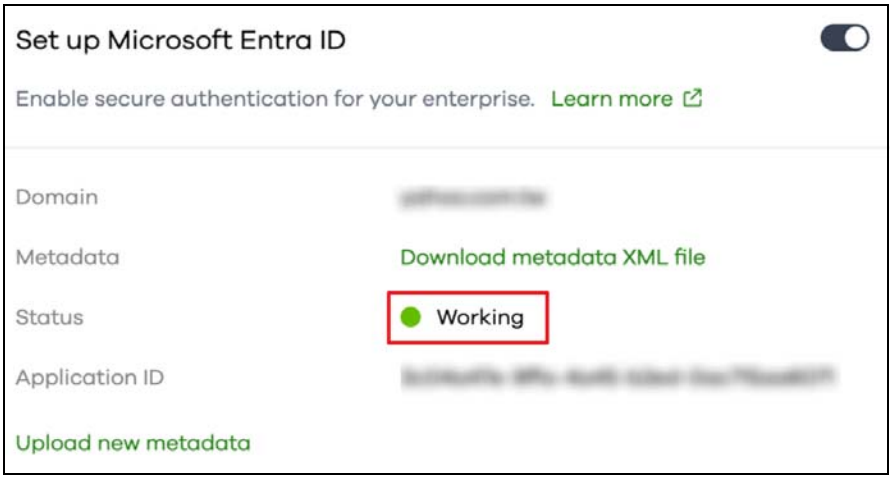
Key information:

- Microsoft Entra ID has been fully configured and is now operational.
- All company users will now authenticate using the "Continue with Microsoft Entra ID" to sign-in
- Users have been notified of this change and provided with login instructions

Need Help?
If you need or have any concerns, contact us and we will be happy to help.

Sincerely,
Zyxel Support Team

4 On the Entra ID Settings page, the status will now display **Working**.



Passkey

In this section, we show you how to:

- Add a Passkey Using Windows Computers
- Add a Passkey Using Android Devices
- Add a Passkey Using Apple Devices
- Log in with a Passkey

A passkey is a login method that lets you log into a Zyxel Web Portal using the same way you unlock your computer or mobile device – fingerprint, Face ID, or PIN. You can use passkeys to log into Zyxel Web Portals, such as Nebula, Circle, SecuReporter, and so on.

When you create a passkey, your computer or mobile device generates two keys:

- Public key – stored on the Zyxel server.
- Private key – stored locally on your computer or mobile device.

Your device's PIN or biometrics (for example, fingerprint, Face ID) is used only to unlock the private key, and is only stored locally on your computer or mobile device.

Note: The passkey limit for every account is shown below.

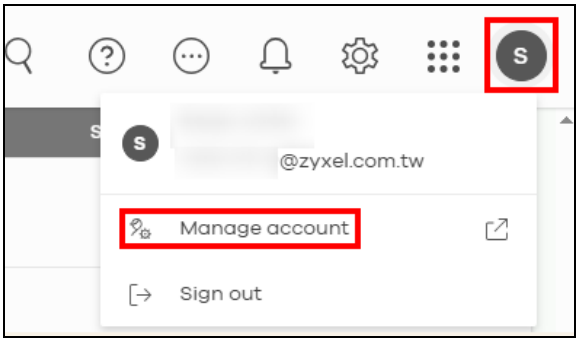
Maximum number of passkeys	5

Note: The following are the minimum computer or mobile device operating system and web browser version requirements to run passkey at the time of writing:

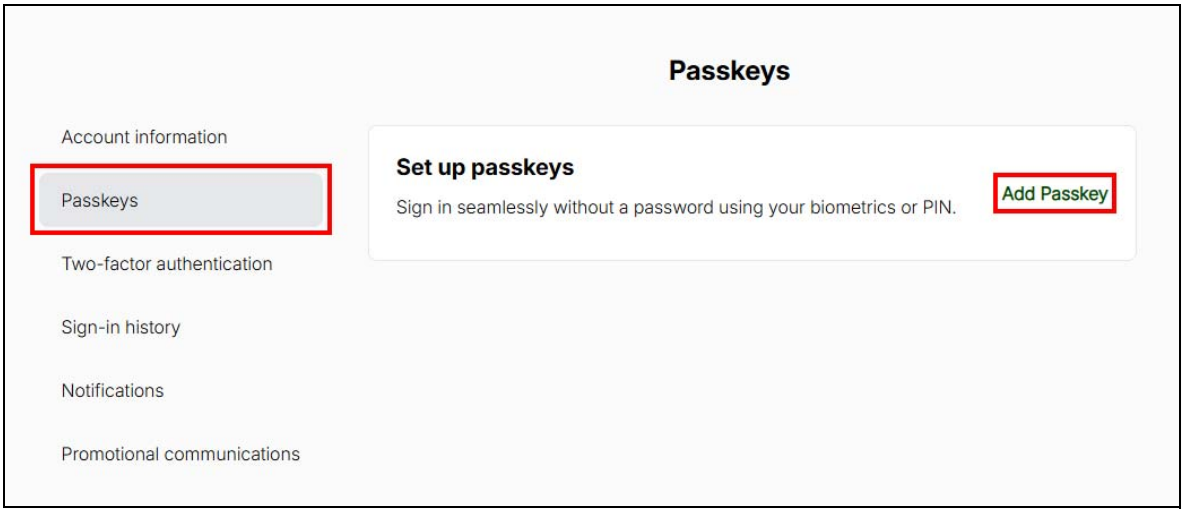
COMPUTER OS VERSION	MOBILE DEVICE OS VERSION	WEB BROWSER VERSION
Windows 10 or later	iOS 16 or later	Chrome 109 or later
macOS 13 Ventura or later	iPadOS 16 or later	Safari 16.1 or later
ChromeOS 109 or later	Android 9 or later	Edge 109 or later

Add a Passkey Using Windows Computers

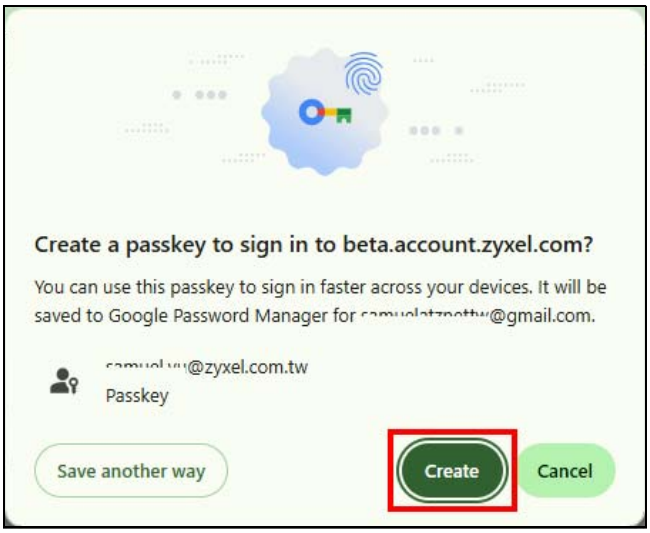
1 Log into a Web Portal, click the Account icon at the top right corner, select **Manage account**.



2 Go to the **Passkeys** tab and click **Add Passkey**.



3 Click **Create**.



4 Your computer will prompt you to authenticate using biometrics (fingerprint or facial recognition) or your PIN.

Note: Your computer must have one of the following Windows Hello sign-in options enabled: PIN, fingerprint, or facial recognition. To set up these sign-in options on your Windows computer, go to **Settings** > **Accounts** > **Sign-in options**.

Note: For biometrics, your computer must have a fingerprint reader or camera for facial recognition. If not, select the PIN option instead.

Note: If you lose your PIN, do the following:

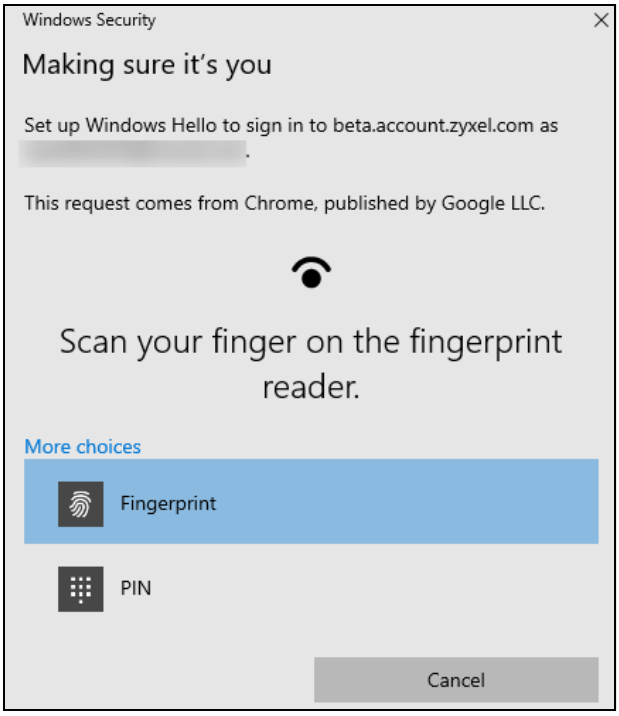
- In Windows:

  Go to **Settings** > **Accounts** > **Sign-in options** > **PIN (Windows Hello)** > **I forgot my PIN**. You will be prompted to re-authenticate using your Microsoft Account password or recovery options.
- In macOS:

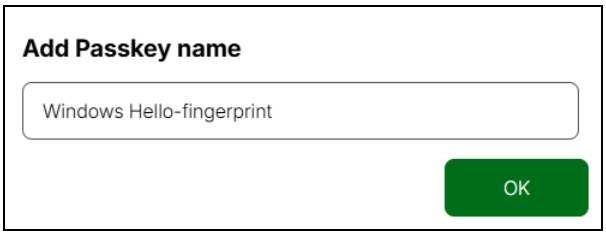
  Use your Apple ID to reset the passcode, or restore from another Apple device where you are still signed in.
- For Cloud Password Managers:

  If you forget it, you can usually log in again using your master password or account recovery flow.

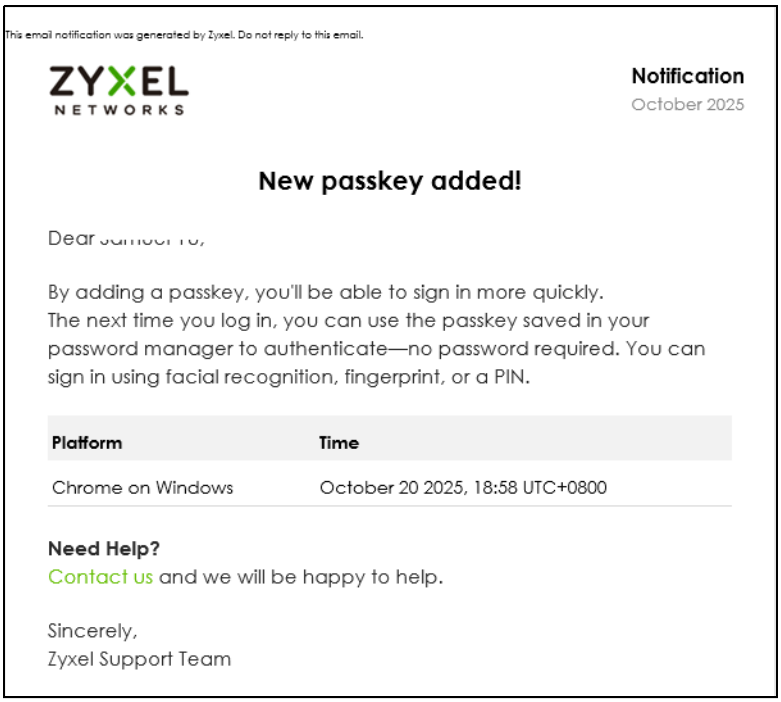
5 Authenticate using the PIN or biometrics that you already set on your device.



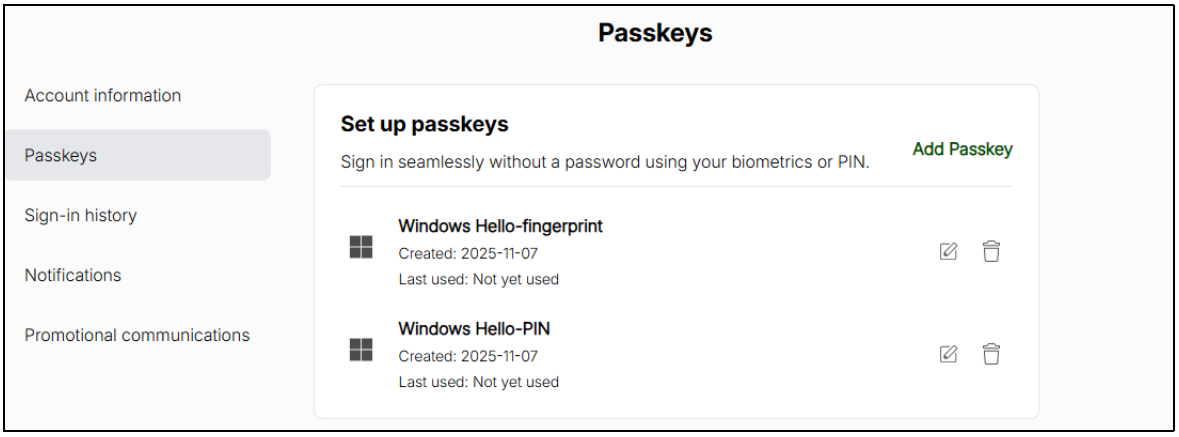
6 The passkey is now saved on this Windows computer. Name your passkey after completing the PIN authentication or biometrics authentication, and then click **OK**.



7 A **New passkey added!** email will be sent to the same email address used for your Zyxel Account.

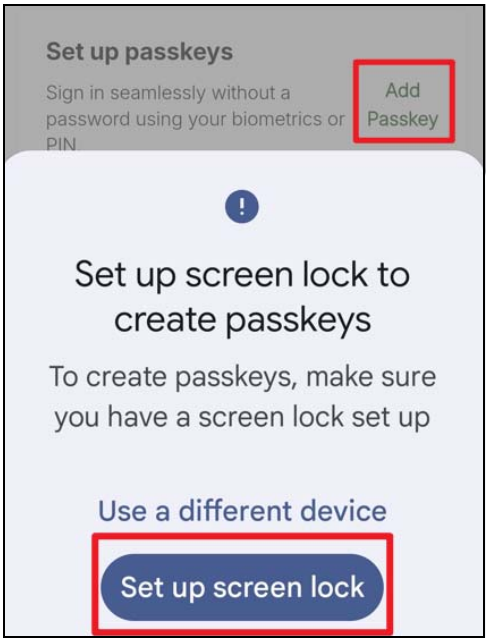


8 You can view all your saved passkeys on the **Manage account** > **Passkeys** page. Select the passkey that matches the Windows computer you are using to sign in.

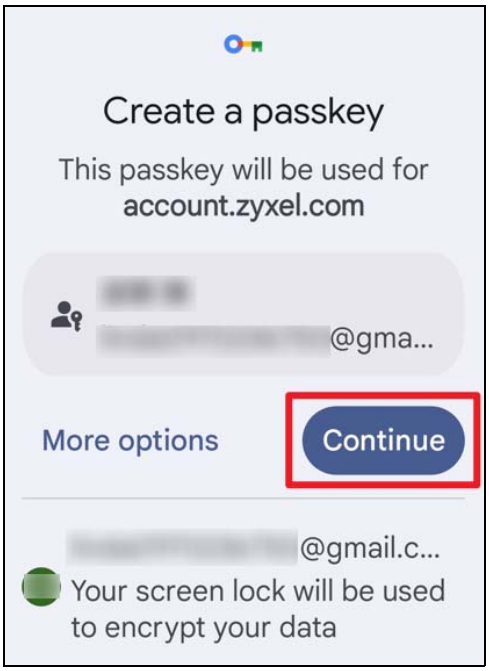


Add a Passkey Using Android Devices

1 Log into your Zyxel Account, click **Add Passkey**. Click **Set up screen lock**, the system will lead you to **Settings > Lock screen and AOD > Screen lock and biometrics**.



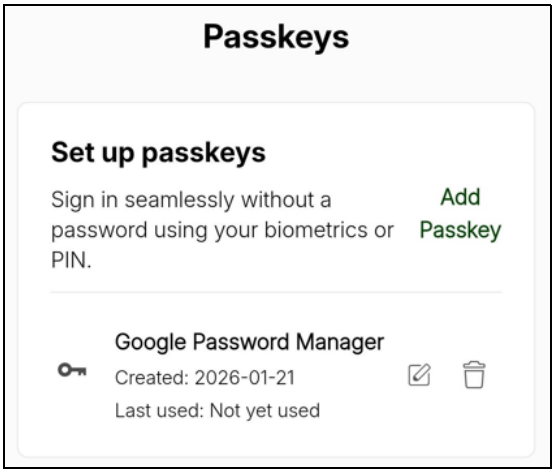
2 If you already have screen lock set up, click **Continue** to create a passkey.



3 Authenticate using your fingerprint, face recognition, or screen lock PIN.

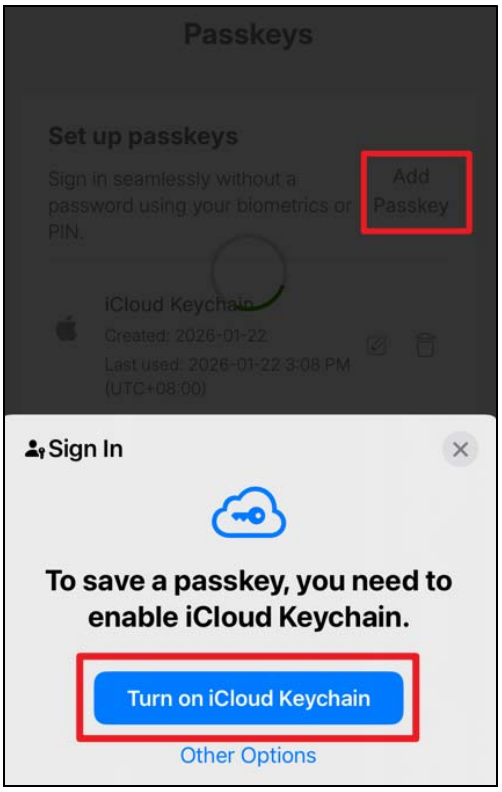


4 The passkey is now added and saved to your Google account.

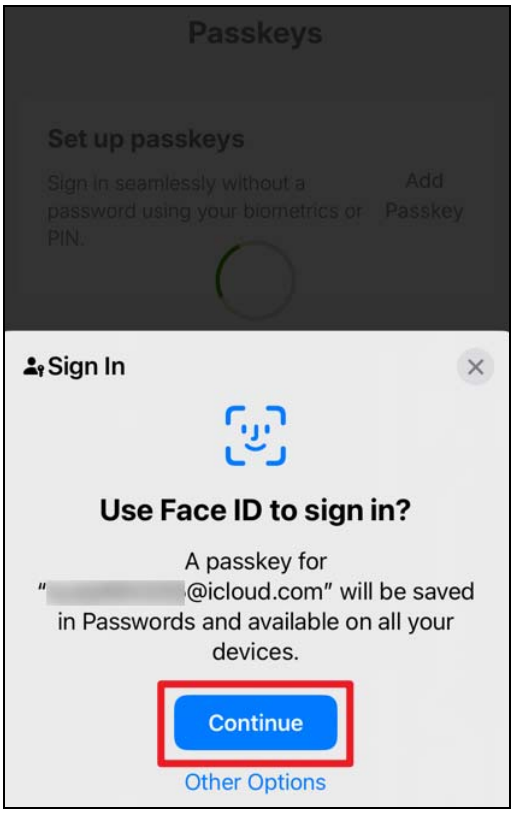


Add a Passkey Using Apple Devices

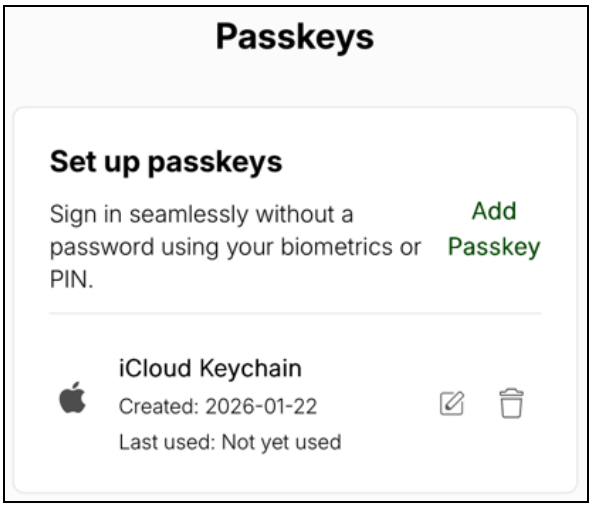
1 Log into your Zyxel Account, click **Add Passkey**. Click **Turn on iCloud Keychain** to enable iCloud Keychain.



2 If your Apple device's iCloud Keychain is already on, click **Continue** to sign in with Face ID.



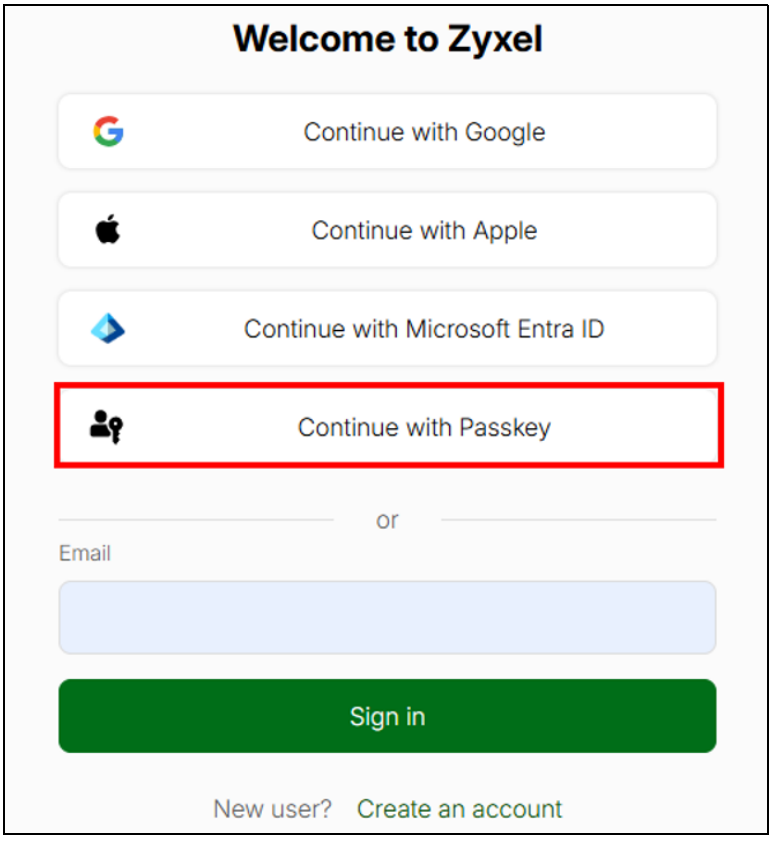
3 The passkey is now added and saved to iCloud Keychain.



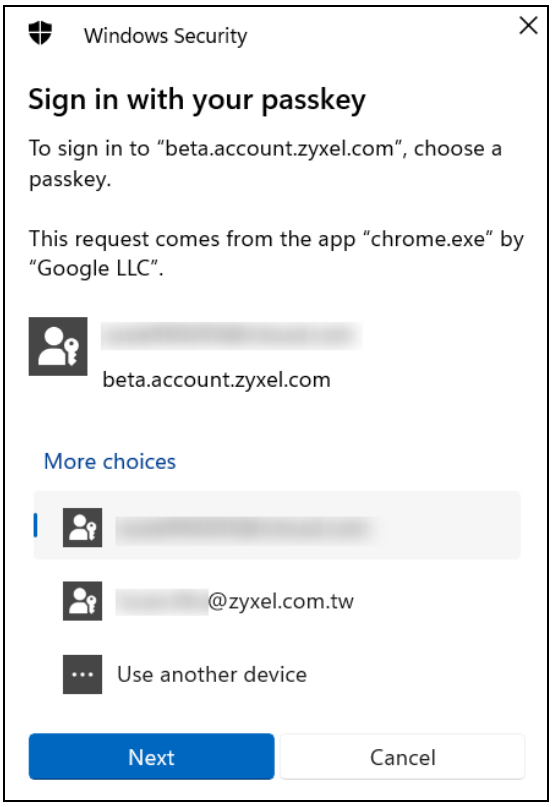
Log in with a Passkey

The passkey is stored locally on your computer or mobile device. If you have enabled cloud synchronization on your computer or mobile device, you can log in from other devices, but those devices must use the same operating system, such as Windows, Google (Android) or Apple. If not, you must log in using the same computer or mobile device where the passkey was registered.

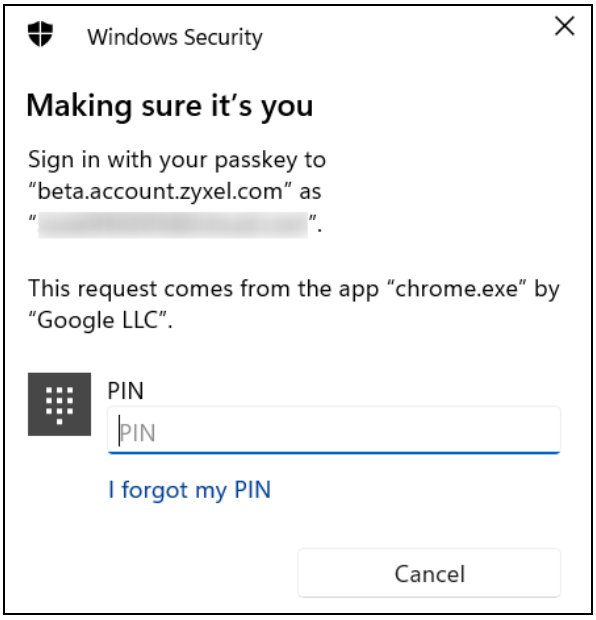
1 On the login screen, click **Continue with Passkey**.



2 Select the account email you want to sign in with, and click **Next**.



3 Complete the biometric authentication by using your device's fingerprint reader to scan your fingerprint, or camera to map your face, or by entering a PIN to log into the Zyxel Web Portal.



APPENDIX B
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.

For Zyxel Communication offices, see *https://service-provider.zyxel.com/global/en/contact-us* for the latest information.

For Zyxel Network offices, see *https://www.zyxel.com/index.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 (Taiwan) Co., Ltd.
- *https://www.zyxel.com*

Asia

China

- Zyxel Communications Corporation–China Office
- *https://www.zyxel.com/cn/sc*

India

- Zyxel Communications Corporation–India Office
- *https://www.zyxel.com/in/en-in*

Kazakhstan

- Zyxel Kazakhstan
- *https://www.zyxel.com/ru/ru*

Korea

- Zyxel Korea Co., Ltd.
- *http://www.zyxel.kr/*

Malaysia

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Philippines

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Singapore

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Taiwan

- Zyxel Communications (Taiwan) Co., Ltd.
- *https://www.zyxel.com/tw/zh*

Thailand

- Zyxel Thailand Co., Ltd.
- *https://www.zyxel.com/th/th*

Vietnam

- Zyxel Communications Corporation–Vietnam Office
- *https://www.zyxel.com/vn/vi*

Europe

Belarus

- Zyxel Communications Corp.
- *https://www.zyxel.com/ru/ru*

Belgium (Netherlands)

- Zyxel Benelux
- *https://www.zyxel.com/nl/nl*
- *https://www.zyxel.com/fr/fr*

Bulgaria

- Zyxel Bulgaria

- *https://www.zyxel.com/bg/bg*

Czech Republic

- Zyxel Communications Czech s.r.o.
- *https://www.zyxel.com/cz/cs*

Denmark

- Zyxel Communications A/S
- *https://www.zyxel.com/dk/da*

Finland

- Zyxel Communications
- *https://www.zyxel.com/fi/fi*

France

- Zyxel France
- *https://www.zyxel.com/fr/fr*

Germany

- Zyxel Deutschland GmbH.
- *https://www.zyxel.com/de/de*

Hungary

- Zyxel Hungary & SEE
- *https://www.zyxel.com/hu/hu*

Italy

- Zyxel Communications Italy S.r.l.
- *https://www.zyxel.com/it/it*

Norway

- Zyxel Communications A/S
- *https://www.zyxel.com/no/no*

Poland

- Zyxel Communications Poland
- *https://www.zyxel.com/pl/pl*

Romania

- Zyxel Romania
- *https://www.zyxel.com/ro/ro*

Russian Federation

- Zyxel Communications Corp.
- *https://www.zyxel.com/ru/ru*

Slovakia

- Zyxel Slovakia
- *https://www.zyxel.com/sk/sk*

Spain

- Zyxel Iberia
- *https://www.zyxel.com/es/es*

Sweden

- Zyxel Communications A/S
- *https://www.zyxel.com/se/sv*

Switzerland

- Studerus AG
- *https://www.zyxel.com/ch/de-ch*
- *https://www.zyxel.com/fr/fr*

Turkey

- Zyxel Turkey A.S.
- *https://www.zyxel.com/tr/tr*

UK

- Zyxel Communications UK Ltd.
- *https://www.zyxel.com/uk/en-gb*

Ukraine

- Zyxel Ukraine
- *https://www.zyxel.com/ua/uk-ua*

South America

Argentina

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

Brazil

- Zyxel Communications Brasil Ltda.

- *https://www.zyxel.com/br/pt*

Colombia

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

Ecuador

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

South America

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

Middle East

Israel

- Zyxel Communications Corp.
- *https://il.zyxel.com*

North America

USA

- Zyxel Communications, Inc. – North America Headquarters

https://www.zyxel.com/us/en-us

APPENDIX C
Product Features

Please refer to the product datasheet for the latest product features.

VERSION	1.39	1.39	1.39	1.39
MODEL NAME	**USG FLEX 50H**	**USG FLEX 50HP**	**USG FLEX 100H**	**USG FLEX 100HP**
# Of MAC	5	5	8	8
Interface				
VLAN	8	8	16	16
Virtual (Alias)	4 per interface	4 per interface	4 per interface	4 per interface
PPP Interface Number	4	4	8	8
Bridge	2	2	4	4
LAG	2	2	4	4
Routing				
Static Route Rules	64	64	64	64
Policy Route Rules	100	100	100	100
Reserved Sessions for Managed Devices	500	500	500	500
Trunk				
Max. Trunk Number (System Default)	1	1	1	1
Max. Trunk Number (User Define)	4	4	4	4
Max. Member Number Per Trunk	12	12	12	12
Sessions				
Max. TCP Concurrent Sessions (Forwarding, NAT/Firewall)	100,000	100,000	300,000	300,000
Max. UTM TCP Concurrent Sessions (CF, URL Threat Filter)	60,000	60,000	200,000	200,000
Session Rate	6,000	6,000	8,000	8,000
NAT				
Max. Virtual Server Number	64	64	64	64
Firewall (Secure Policy)				
Max Firewall ACL Rule Number = Secure Policy Number	500	500	500	500
Max Session Limit per Host Rules	100	100	100	100
DoS Prevention				
Max. DoS Prevention Profile Number	32	32	32	32
Max. DoS Prevention Rule Number	20	20	20	20
Source IP Spoofing Prevention				
Max. Interface	15	15	28	28
Max. Trusted IP/MAC Pairs	50	50	50	50
Max. Trusted IP	64	64	64	64
User Profile				
Max. Local User	64	64	64	64
Max. Admin User	5	5	5	5
Max. User Group	16	16	16	16
Max. User In One User Group	64	64	64	64
Max. Concurrent Device Login	64	64	64	64
On-Cloud Max. Concurrent Device Login	64	64	64	64
Max. Device Insight Entry	192	192	192	192
HTTPd				
Max. HTTPd Number	2	2	2	2
Objects				
Address Object	300	300	300	300
Address Group	25	25	50	50
Max. Address Object In One Group	64	64	128	128
Max. Multicast Address Reception	20	20	20	20

VERSION	1.39	1.39	1.39	1.39
MODEL NAME	USG FLEX 50H	USG FLEX 50HP	USG FLEX 100H	USG FLEX 100HP
Service Object	200	200	200	200
Service Group	50	50	50	50
Max. Service Object In One Group	64	64	64	64
Schedule Object	32	32	32	32
Schedule Group	16	16	16	16
Max. Schedule Object In One Group	24	24	24	24
Application Object	500	500	500	500
Max. LDAP Server Object #	4	4	4	4
Max. RADIUS Server Object #	4	4	4	4
Max. AD Server Object #	4	4	4	4
Max. OIDC Server Object #	4	4	4	4
VPN				
Max. VTI / VPN Tunnels Number	20	20	50	50
Max. Remote Access VPN Tunnel Number	10	10	25	25
SSL VPN				
Max. SSL VPN Connections	15	15	25	25
Max. SSL VPN Network List	8	8	8	8
SSL VPN Max. Policy	32	32	32	32
Max. Profiles	16	16	16	16
Max. Profiles User List	32	32	32	32
Certificate				
Certificate Buffer Size	1024K	1024K	1024K	1024K
Built-In Service				
A Record	32	32	64	64
CNAME Record	8	8	8	8
NS Record (DNS Domain Zone Forward)	8	8	8	8
MX Record	4	4	8	8
Max. DHCP Network Pool (vlan+brg+ethernet)	15	15	28	28
Max. DHCP Host Pool (Static DHCP)	64	64	128	128
Max. DHCP User Defined (Custom) Extended Options (per Pool Server-Global)	5	5	5	5
Maximum DHCP options (pre-defined + User defined) (per pool)	15	15	15	15
Max. DDNS Profiles	10	10	10	10
DHCP Relay	2 per interface	2 per interface	2 per interface	2 per interface
Max. DHCP Relay Server	4	4	4	4
Max. DHCP Relay Interface per DHCP Relay Server	24	24	24	24
USB Storage				
Device Number	1	1	1	1
Centralized Log				
Log Entries	512	512	1,024	1,024
Debug Log Entries	1024	1024	1,024	1,024
Admin E-Mail Address	2	2	2	2
Syslog Server	4	4	4	4
BWM				
Max. BWM Rule	128	128	128	128
SIP Pinhole				
Maximum SIP concurrent call	50	50	50	50
Maximum SIP Signaling Port	8	8	8	8
Application Patrol				
Max. App Patrol Profile Number	32	32	32	32
Max. Nebula App Patrol Profile Number (Org-wide)	20	20	20	20
SSL Inspection				
Max. SSL Inspection Profile	8	8	8	8
Max. Exclude List	256	256	256	256
Content Filtering				
Max. Content Filtering Profile Number	16	16	16	16

VERSION	1.39	1.39	1.39	1.39
MODEL NAME	USG FLEX 50H	USG FLEX 50HP	USG FLEX 100H	USG FLEX 100HP
Max. Nebula Content Filtering Profile Number (Org-wide)	16	16	16	16
Forbidden Domain Entry Number	256 per profile	256 per profile	256 per profile	256 per profile
Trusted Domain Entry Number	256 per profile	256 per profile	256 per profile	256 per profile
Keyword Blocking Number	128 per profile	128 per profile	128 per profile	128 per profile
Nebula Content Filtering Allow/Block Website Number (Org-wide)	100	100	100	100
URL Threat Filter				
Max. Statistic Number	1024	1024	1024	1024
Max. Allow List Rule	256	256	256	256
Max. Block List Rule	256	256	256	256
Max. Nebula Allow / Block List Rule (Org-wide)	100	100	100	100
IP Reputation				
Max. Statistic Number	1024	1024	1024	1024
Max. Allow List Rule	256	256	256	256
Max. Block List Rule	256	256	256	256
Max. Nebula Allow / Block List Rule (Org-wide)	100	100	100	100
DNS Threat Filter				
Max. Statistic Number	1024	1024	1024	1024
Max. Allow List Rule	256	256	256	256
Max. Block List Rule	256	256	256	256
Max. Nebula Allow / Block List Rule (Org-wide)	100	100	100	100
External Block List				
Max. External Block List DB Number	4	4	4	4
IP Exception				
Max. IP Exception Number	64	64	64	64
Anti-Malware				
Max. Statistic Number	512	512	1024	1024
Max. Allow List Rule	512	512	512	512
Max. Block List Rule	512	512	512	512
Max. Nebula Allow / Block List Rule (Org-wide)	100	100	100	100
Sandboxing				
Support protocol	HTTP/SMTP/POP3/FTP	HTTP/SMTP/POP3/FTP	HTTP/SMTP/POP3/FTP	HTTP/SMTP/POP3/FTP
Concurrent File Collect Capability	64	64	64	64
Upload File Size	Up to 10MB per file	Up to 10MB per file	Up to 10MB per file	Up to 10MB per file
Captive Portal (Web Authentication Policy)				
Max. Authentication Policy	10	10	10	10
Max. Exempt List per Auth. Policy	50	50	50	50
Max. Walled Garden (Domain) per Auth. Policy	30	30	30	30
AP Controller				
Default Managed AP Number	8	8	8	8
Max. Managed AP Number	12	12	24	24
Max. AP Group	8	8	8	8
Recommended max. AP in 1 AP Group	2	2	5	5
Max. Radio Profile	24	24	24	24
Max. SSID Profile	64	64	64	64
Max. Security Profile	64	64	64	64
Max. MAC Filter Profile	64	64	64	64
Max. MAC Entry per MAC Filter Profile	512	512	512	512

VERSION	1.39	1.39	1.39	1.39
MODEL NAME	USG FLEX 200H	USG FLEX 200HP	USG FLEX 500H	USG FLEX 700H
# Of MAC	8	8	12	14

VERSION	1.39	1.39	1.39	1.39
MODEL NAME	USG FLEX 200H	USG FLEX 200HP	USG FLEX 500H	USG FLEX 700H
Interface				
VLAN	32	32	64	128
Virtual (Alias)	4 per interface	4 per interface	4 per interface	4 per interface
PPP Interface Number	8	8	12	14
Bridge	4	4	6	7
LAG	4	4	4	4
Routing				
Static Route Rules	128	128	300	1000
Policy Route Rules	100	100	300	500
Reserved Sessions for Managed Devices	500	500	500	500
Trunk				
Max. Trunk Number (System Default)	1	1	1	1
Max. Trunk Number (User Define)	4	4	8	8
Max. Member Number Per Trunk	12	12	24	40
Sessions				
Max. TCP Concurrent Sessions (Forwarding, NAT/Firewall)	600,000	600,000	1,000,000	2,000,000
Max. UTM TCP Concurrent Sessions (CF, URL Threat Filter)	400,000	400,000	800,000	1,600,000
Session Rate	12,000	12,000	20,000	40,000
NAT				
Max. Virtual Server Number	128	128	256	512
Firewall (Secure Policy)				
Max Firewall ACL Rule Number = Secure Policy Number	2,000	2,000	5,000	10,000
Max Session Limit per Host Rules	100	100	100	100
DoS Prevention				
Max. DoS Prevention Profile Number	32	32	32	32
Max. DoS Prevention Rule Number	40	40	64	128
Source IP Spoofing Prevention				
Max. Interface	44	44	82	147
Max. Trusted IP/MAC Pairs	100	100	200	200
Max. Trusted IP	64	64	64	64
User Profile				
Max. Local User	128	128	256	512
Max. Admin User	5	5	5	10
Max. User Group	32	32	64	128
Max. User In One User Group	128	128	256	512
Max. Concurrent Device Login	200	200	500	2,000
On-Cloud Max. Concurrent Device Login	200	200	500	2,000
Max. Device Insight Entry	600	600	900	12,000
HTTPd				
Max. HTTPd Number	2	2	2	2
Objects				
Address Object	300	300	500	1,500
Address Group	50	50	200	400
Max. Address Object In One Group	128	128	128	256
Max. Multicast Address Reception	20	20	20	20
Service Object	500	500	1,000	1,000
Service Group	100	100	200	200
Max. Service Object In One Group	128	128	128	256
Schedule Object	32	32	32	32
Schedule Group	16	16	16	16
Max. Schedule Object In One Group	24	24	24	24
Application Object	500	500	1,000	1,000
Max. LDAP Server Object #	4	4	8	8
Max. RADIUS Server Object #	4	4	8	8
Max. AD Server Object #	4	4	8	8
Max. OIDC Server Object #	4	4	8	8

VERSION	1.39	1.39	1.39	1.39
MODEL NAME	USG FLEX 200H	USG FLEX 200HP	USG FLEX 500H	USG FLEX 700H
VPN				
Max. VTI / VPN Tunnels Number	100	100	300	1,000
Max. Remote Access VPN Tunnel Number	50	50	150	500
SSL VPN				
Max. SSL VPN Connections	50	50	150	500
Max. SSL VPN Network List	8	8	8	8
SSL VPN Max. Policy	32	32	64	128
Max. Profiles	32	32	64	128
Max. Profiles User List	32	32	32	32
Certificate				
Certificate Buffer Size	1024K	1024K	1024K	1024K
Built-In Service				
A Record	64	64	128	128
CNAME Record	8	8	8	8
NS Record (DNS Domain Zone Forward)	16	16	16	16
MX Record	8	8	8	8
Max. DHCP Network Pool (vlan+brg+ethernet)	44	44	82	147
Max. DHCP Host Pool (Static DHCP)	256	256	512	1,024
Max. DHCP User Defined (Custom) Extended Options (per Pool Server-Global)	5	5	5	5
Maximum DHCP options (pre-defined + User defined) (per pool)	15	15	15	15
Max. DDNS Profiles	10	10	10	10
DHCP Relay	2 per interface	2 per interface	2 per interface	2 per interface
Max. DHCP Relay Server	4	4	4	4
Max. DHCP Relay Interface per DHCP Relay Server	40	40	76	142
USB Storage				
Device Number	1	1	1	1
Centralized Log				
Log Entries	2,048	2,048	2,048	2,048
Debug Log Entries	1,024	1,024	1,024	1,024
Admin E-Mail Address	2	2	2	2
Syslog Server	4	4	4	4
BWM				
Max. BWM Rule	128	128	128	256
SIP Pinhole				
Maximum SIP concurrent call	100	100	100	200
Maximum SIP Signaling Port	8	8	8	8
Application Patrol				
Max. App Patrol Profile Number	32	32	64	96
Max. Nebula App Patrol Profile Number (Org-wide)	20	20	20	20
SSL Inspection				
Max. SSL Inspection Profile	8	8	16	16
Max. Exclude List	256	256	256	256
Content Filtering				
Max. Content Filtering Profile Number	16	16	32	32
Max. Nebula Content Filtering Profile Number (Org-wide)	16	16	16	16
Forbidden Domain Entry Number	256 per profile	256 per profile	512 per profile	512 per profile
Trusted Domain Entry Number	256 per profile	256 per profile	512 per profile	512 per profile
Keyword Blocking Number	128 per profile	128 per profile	256 per profile	256 per profile
Nebula Content Filtering Allow/Block Website Number (Org-wide)	100	100	100	100
URL Threat Filter				
Max. Statistic Number	1024	1024	1024	1024
Max. Allow List Rule	256	256	256	256
Max. Block List Rule	256	256	256	256

VERSION	1.39	1.39	1.39	1.39
MODEL NAME	USG FLEX 200H	USG FLEX 200HP	USG FLEX 500H	USG FLEX 700H
Max. Nebula Allow / Block List Rule (Org-wide)	100	100	100	100
IP Reputation				
Max. Statistic Number	1024	1024	1024	1024
Max. Allow List Rule	256	256	256	256
Max. Block List Rule	256	256	256	256
Max. Nebula Allow / Block List Rule (Org-wide)	100	100	100	100
DNS Threat Filter				
Max. Statistic Number	1024	1024	1024	1024
Max. Allow List Rule	256	256	256	256
Max. Block List Rule	256	256	256	256
Max. Nebula Allow / Block List Rule (Org-wide)	100	100	100	100
External Block List				
Max. External Block List DB Number	4	4	4	4
IP Exception				
Max. IP Exception Number	64	64	64	64
Anti-Malware				
Max. Statistic Number	1024	1024	1024	1024
Max. Allow List Rule	512	512	512	512
Max. Block List Rule	512	512	512	512
Max. Nebula Allow / Block List Rule (Org-wide)	100	100	100	100
Sandboxing				
Support protocol	HTTP/SMTP/POP3/FTP	HTTP/SMTP/POP3/FTP	HTTP/SMTP/POP3/FTP	HTTP/SMTP/POP3/FTP
Concurrent File Collect Capability	64	64	64	64
Upload File Size	Up to 10MB per file	Up to 10MB per file	Up to 10MB per file	Up to 10MB per file
Captive Portal (Web Authentication Policy)				
Max. Authentication Policy	10	10	10	10
Max. Exempt List per Auth. Policy	50	50	50	50
Max. Walled Garden (Domain) per Auth. Policy	30	30	30	30
AP Controller				
Default Managed AP Number	8	8	8	8
Max. Managed AP Number	40	40	72	520
Max. AP Group	8	8	16	64
Recommended max. AP in 1 AP Group	10	10	32	256
Max. Radio Profile	24	24	48	192
Max. SSID Profile	64	64	128	512
Max. Security Profile	64	64	128	512
Max. MAC Filter Profile	64	64	128	512
Max. MAC Entry per MAC Filter Profile	512	512	512	2048

APPENDIX D
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 (Class B)

Model List: USG FLEX 50H, USG FLEX 50HP, USG FLEX 100H, USG FLEX 100HP, USGFLEX 200H, USG FLEX 200HP

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

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)

Europe and the United Kingdom



The following information applies if you use the product within the European Union or United Kingdom.

List of National Codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Sweden	SE
Ireland	IE	Switzerland	CH
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not 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 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 battery)
- Fuse Warning! Replace a fuse only with a fuse of the same type and rating. (For devices with a fuse)
- To avoid possible eye injury, do not look into an operating fiber-optic module's connector. (For devices with fiber)
- 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)
- CLASS 1 LASER PRODUCT & "IEC 60825-1:2014" (For devices with fiber)
- APPAREIL À LASER DE CLASS 1 (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

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 *https://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.

Trademarks

ZyNOS (Zyxel Network Operating System) and ZON (Zyxel One Network) are registered trademarks of Zyxel Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Open Source Licenses

This product 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*

Regulatory Notice and Statement (Class A)

Model List: USG FLEX 500H, USG FLEX 700H

United States of America



The following information applies if you use the product within USA area.

Federal Communications Commission (FCC) EMC Statement

- This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

  (1) This device may not cause harmful interference.

  (2) This device must accept any interference received, including interference that may cause undesired operations.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canada

The following information applies if you use the product within Canada area

Innovation, Science and Economic Development Canada ICES statement

CAN ICES(A)/NMB(A)

Europe and the United Kingdom



The following information applies if you use the product within the European Union or United Kingdom.

EMC statement

WARNING: This equipment is compliant with Class A of EN55032. In a residential environment this equipment may cause radio interference.

List of National Codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Sweden	SE
Ireland	IE	Switzerland	CH
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not 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.
- Use ONLY power wires of the appropriate wire gauge for your device. Connect it to a power supply of the correct voltage.
- The POE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device.

  - For 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.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:

  - Install the power supply before connecting the power cable to the power supply.

  - Unplug the power cable before removing the power supply.

  - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supply.
- 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)

- This device must be grounded by qualified service personnel. Never defeat the ground conductor or operate the device in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

  - If your device has an earthing screw (frame ground), connect the screw to a ground terminal using an appropriate AWG ground wire. Do this before you make other connections.

  - If your device has no earthing screw, but has a 3-prong power plug, make sure to connect the plug to a 3-hole earthed socket.
- 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)
- Fuse Warning! Replace a fuse only with a fuse of the same type and rating. (For devices with a fuse)
- To avoid possible eye injury, do not look into an operating fiber-optic module's connector. (For devices with fiber)
- 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)
- CLASS 1 LASER PRODUCT & "IEC 60825-1:2014" (For devices with fiber)
- APPAREIL À LASER DE CLASS 1 (For devices with fiber)
- CLASS 1 CONSUMER LASER PRODUCT & "EN 50689:2021" (For devices with fiber)

Important Safety Instructions (For devices with a fan)

1 Warning! Energy Hazard. Remove all metal jewelry, watches, and so on from your hands and wrists before serving the Zyxel Device.
2 Caution! The RJ-45 jacks are not used for telephone line connection.
3  Hazardous Moving Parts. Keep body parts away from fan blades.
4  Hot Surface. Do not touch.
1 Avertissement: Risque de choc électrique. Retirer tout bijoux en métal et votre montre de vos mains et poignets avant de manipuler cet appareil.
2 Attention: Les câbles RJ-45 ne doivent pas être utilisés pour les connections téléphoniques.
3  Mobilité des pièces détachées. S'assurer que les pièces détachées ne sont pas en contact avec les pales du ventilateur.
4  Surface brûlante. Ne pas toucher.

Environment Statement

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.

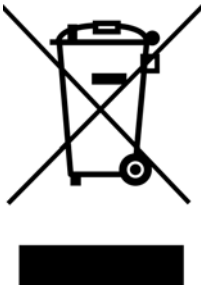
Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung 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

警告使用者

- 這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。
- 為避免電磁干擾，本產品不應安裝或使用於住宅環境。

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。
- 設備必須接地，接地導線不允許被破壞或沒有適當安裝接地導線，如果不確定接地方式是否符合要求可聯繫相應的電氣檢驗機構檢驗。
- 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 *https://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

1 Gbps 58
10 Gbps 58
100 Mbps 58
2.5 Gbps 58
3DES 222
5 Gbps 58

A

AAA
  Base DN 479
  Bind DN 479
  directory structure 478
  Distinguished Name, see DN
  DN 479
  port 492
AAA server 480
  and users 460
  local user database 478
  RADIUS 478, 480, 484
  RADIUS group 482, 485, 489, 491
  see also RADIUS
access 25
access control attacks 433
access users
  multiple logins 476
account
  user 459, 477
accounting server 480
active protocol 228
  AH 228
  and encapsulation 228
  ESP 228
active sessions 91
AD 479
  directory structure 478
  Distinguished Name, see DN
  port 492
address groups 324
  and content filtering 362
address objects 324
  and content filtering 362
  and NAT 186, 196
  and policy routes 186
  HOST 326
  RANGE 326
  SUBNET 326
  types of 324, 330
address record 585
admin users 459
  multiple logins 476
  see also users 459
ADP 296
  false negatives 298
  false positives 298
  inline profile 298
  monitor profile 298
Advanced Encryption Standard, see AES
AES 222
AES-GCM 242, 245, 252
AF 181
AH 228
  and transport mode 228
Airtime Fairness 504
alerts
  IDP 448
ALG 211
  and NAT 211
  and policy routes 211
  and security policy 211
  and trunks 211
  FTP 211, 212
  H.323 211
  see also VoIP pass through 211
  SIP 211
Anomaly Detection and Prevention, see ADP

Anonymizer 401, 407
Anonymous Proxies 394
anti-malware 412
  boot sector virus 412
  EICAR 415
  e-mail
    virus 412
  file infector 412
  file infector virus 412
  macro virus 412
  malware life cycle 412
  malware types 412
  mutation virus 412
  packet types 412
  polymorphic virus 412
  scanner types 420
  statistics 100
  virus 412
  worm 412
anti-virus
  EICAR 415
  e-mail virus 412
  polymorphic virus 412
  statistics 100, 101
  troubleshooting 710, 712
  updating signatures 127, 128
AP and SSID Tags 503
AP Group 503
AP Packet Capture 685
AP Roaming 503
Application Layer Gateway, see ALG
application patrol 350
  actions 350
  and security policy 350
  classification 351
  exceptions 350
  port-less 351
  ports 351
  service ports 351
  troubleshooting 710, 715, 719
asymmetrical routes 290
  allowing through the security policy 291
  vs virtual interfaces 290
attacks
  access control 433
  backdoor 433
  buffer overflow 432
  DoS/DDoS 433
  P2P 433
  scan 433
  trapdoor 433
  trojan 433
  virus 412, 433
  worm 433
authentication
  in IPSec 242, 245, 253
  server 480
authentication algorithms 222, 223
  and active protocol 222
  MD5 223
  SHA1 223
Authentication Header, see AH
authentication method objects
  and users 460
authentication server 601
Authentication, Authorization, Accounting servers, see AAA server
authorization server 480
auxiliary interfaces 131

B

backdoor attacks 433
backing up configuration files 657
bandwidth capacity
  cable types 59
bandwidth management 350
  maximize bandwidth usage 200
  see also application patrol 350
Base DN 479
Bind DN 479
BitTorrent 433
Blaster 437
Botnet 395
bridge interfaces 131, 133
  and virtual interfaces of members 134
  effect on routing table 134
  member interfaces 134
bridges 133
Brute Force Attack 395
buffer overflow 432
buffer overflow attacks 432

C

CA
  and certificates 610
CA (Certificate Authority), see certificates
cable types 59
Captive Portal 311
  Client Sign-In 321
  Redirect TCP Port 443 Traffic 312
  Walled Garden 311
capturing packets 675
CAT 5 cable 59
CAT 5e cable 58
CAT 6 cable 58
CAT 6a cable 58
CAT 7 cable 59
CEF (Common Event Format) 650
certificate
  troubleshooting 719
Certificate Authority (CA)
  see certificates
Certificate Revocation List (CRL) 610
certificates 609
  advantages of 610
  and CA 610
  and HTTPS 566
  and IKE SA 227
  certification path 610, 623
  expired 610
  factory-default 611
  file formats 611
  not used for encryption 610
  revoked 610
  self-signed 611, 617
  serial number 618, 623
  thumbprint algorithms 611
  thumbprints 611
  used for authentication 610
  verifying fingerprints 611
certification requests 617
certifications
  viewing 769, 774
CFRG 224
check 726
Chrome 25
CLI 24
CLI Script 669
commands 24
Common Event Format (CEF) 650
computer names 136
computer virus 412
  see also virus
configuration
  information 672
configuration files 656
  at restart 658
  backing up 657
  downloading 659
  editing 656
  lastgood.conf 657, 661, 664
  managing 657
  startup-config.conf 661, 664
  startup-config-bad.conf 657
  system-default.conf 661
  uploading 660
  use without restart 656
connection
  troubleshooting 715
connection monitor (in SSL) 116
connectivity check 149, 156, 163, 168
contact information 755, 760
content filter
  troubleshooting 710
content filtering 361, 362
  and address groups 362
  and address objects 362
  and schedules 361, 362
  and user groups 362
  and users 362
  by category 362, 364
  by keyword (in URL) 362
  by URL 362
  default policy 362
  filter list 362
  managed web pages 370
  policies 361, 362
  registration status 126
  URL for blocked access 366
cookies 25
copyright 766
Cross Site Scripting 395
current date/time 76, 565
  and schedules 344

setting manually 565
time server 565
current user list 116
customer support 755, 760

D

Data Encryption Standard, see DES
date 565
DDNS
backup mail exchanger 596
mail exchanger 596
service providers 581
troubleshooting 714
DDoS attacks 433
default
security policy behavior 288
Denial of Service (DoS) attacks 433
DES 222
device access
troubleshooting 708
Device HA 138, 570
Heartbeat 571
device High Availability see Device HA 570
DHCP 135
and DNS servers 136
and interfaces 136
pool 136
static DHCP 136
DHCP reservation 113
DHCP server 113
Diagnostics
AP Diagnostics 684
diagnostics 672
Diffie-Hellman 223
DiffServ 181
direct routes 182
directory service
file structure 478
Directory Service (LDAP/AD) 478
disclaimer 766
distance limitation
cable types 59
Distinguished Name (DN) 479
Distributed Denial of Service (DDoS) attacks 433
DN 479
DNS 581
address records 585
domain name forwarders 587
domain name to IP address 585
IP address to domain name 585
Mail eXchange (MX) records 587
pointer (PTR) records 585
DNS Filter 392, 399, 456
Priority 399
types of queries 399
DNS servers 582, 587
and interfaces 136
Domain Name System, see DNS
DoS 394
DoS (Denial of Service) attacks 433
DSCP 183, 185, 693, 699
Dynamic Host Configuration Protocol, see DHCP.
DynDNS 581
DynDNS see also DDNS 581
Dynu 581

E

ECP Brainpool 224
ECP NIST 224
Edge 25
e-Donkey 433
Egress Rate Limit 150
e-mail
daily statistics report 652
e-Mule 433
Encapsulating Security Payload, see ESP
encapsulation
and active protocol 228
transport mode 228
tunnel mode 228
VPN 228
encryption
IPSec 242, 245, 252
RSA 619
encryption algorithms 222
3DES 222

AES 222
and active protocol 222
DES 222
ESP 228
and transport mode 228
Ethernet interfaces 131
and routing protocols 142, 150
Exploits 394
External Block List
DNS/URL Threat Filter 456
IP Reputation 454

F

false negatives 298
false positives 298, 301, 302
file extensions
configuration files 656
shell scripts 656
file manager 656
Firefox 25
firmware
and restart 666
current version 76, 668
getting updated 666
uploading 667, 669
firmware upload
troubleshooting 720
Flash Memory 80
FQDN 585
FTP
ALG 211
signaling port 213
troubleshooting 715
full tunnel mode 268
Fully-Qualified Domain Name, see FQDN

G

Grace Period 21

H

Hash Value 412
host-based intrusions 436
HTTP
over SSL, see HTTPS
vs HTTPS 566
HTTP Strict Transport Security 311
HTTPS 566
and certificates 566
authenticating clients 566
vs HTTP 566
HyperText Transfer Protocol over Secure Socket Layer, see HTTPS

I

ICMP 334
IDP 426
alerts 448
log options 301, 302, 303, 448
service group 434
signatures 426
statistics 98
troubleshooting 710, 712
Iframe Injection 395
IGMP Proxy 215
IKE SA
aggressive mode 221, 226
and certificates 227
and to-ZyWALL security policy 716
authentication algorithms 222, 223
content 225
encryption algorithms 222
IP address, 221
IP address, remote IPSec router 221
local identity 225
main mode 221, 226
NAT traversal 227
negotiation mode 221
peer identity 225
pre-shared key 225
proposal 222
see also VPN
IM (Instant Messenger) 433
iMesh 433

Ingress Rate Limit 150
inline profile 298
installation
  desktop 67
installation scenarios 67
Instant Messenger (IM) 350, 433
  managing 350
interfaces 130
  and DNS servers 136
  and layer-3 virtualization 131
  and NAT 195
  and physical ports 131
  and policy routes 186
  and static routes 188
  and zones 131
  as DHCP relays 136
  as DHCP servers 136
  auxiliary, see also auxiliary interfaces.
  backup, see trunks
  bridge, see also bridge interfaces.
  DHCP clients 135
  Ethernet, see also Ethernet interfaces.
  gateway 135
  general characteristics 131
  IP address 134
  metric 135
  overlapping IP address and subnet mask 135
  port groups, see also port groups.
  PPPoE/PPTP, see also PPPoE/PPTP interfaces.
  prerequisites 132
  relationships between 132
  static DHCP 136
  subnet mask 134
  trunks, see also trunks.
  Tunnel, see also Tunnel interfaces.
  types 131
  virtual, see also virtual interfaces.
  VLAN, see also VLAN interfaces.
  WLAN, see also WLAN interfaces.
Internet access
  troubleshooting 708, 718
Internet Control Message Protocol, see ICMP
Internet Protocol Security, see IPSec
Intrusion, Detection and Prevention see IDP 426
intrusions
  host 436
  network 436
IP Fragment 302
IP policy routing, see policy routes
IP protocols 333
  and service objects 334
  ICMP, see ICMP
  TCP, see TCP
  UDP, see UDP
IP Reputation 391
  External Black List 399
IP static routes, see static routes
IP/MAC binding 303
IPSec 220
  authentication 242, 245, 253
  basic troubleshooting 716
  encryption 242, 245, 252
  established in two phases 231
  local network 220
  peer 220
  remote IPSec router 220
  remote network 220
  SA see also IPSec SA 227
  see also VPN
IPSec SA
  active protocol 228
  and security policy 716
  and to-ZyWALL security policy 716
  authentication algorithms 222, 223
  encapsulation 228
  encryption algorithms 222
  local policy 228
  Perfect Forward Secrecy (PFS) 229
  proposal 229
  remote policy 228
  Security Parameter Index (SPI) (manual keys) 231
  see also IPSec
  see also VPN
  transport mode 228
  tunnel mode 228
  when IKE SA is disconnected 227
IPSec VPN
  troubleshooting 715
IPSec VPN Tunnel 185

J

Java
  permissions 25

JavaScripts 25

K

key pairs 610

L

LAND Attack 302
lastgood.conf 657, 661, 664
LDAP
  and users 460
  Base DN 479
  Bind DN 479
  directory structure 478
  Distinguished Name, see DN
  DN 479
  port 492
least load first load balancing 169
LED troubleshooting 708
Let's Encrypt 625, 626
  DNS-01 625
  HTTP-01 625
level-4 inspection 351
level-7 inspection 351
licensing 123
Link 171
Link Sticking 171
load balancing 169
  algorithms 169, 174, 175
  least load first 169
  round robin 170
  see also trunks 169
  session-oriented 169
  spillover 171
  weighted round robin 170
Local Storage 80
local user database 478
log
  troubleshooting 720
log options
  (IDP) 301, 302, 303, 448
Login Name Attribute 484
logs
  and security policy 294
  e-mail profiles 647
  log consolidation 649
  settings 647
  syslog servers 647
  system 647
  types of 647

M

MAC address
  and VLAN 137
  Ethernet interface 147, 154, 160
  range 75
managed web pages 370
management access
  troubleshooting 720
Management Information Base (MIB) 597
managing the device
  using SNMP. See SNMP.
maximum distance
  cable types 59
MD5 223
mDNS
  mDNS Proxy 216, 218
  mDNS reflector 216
Message Digest 5, see MD5
MODP 223
monitor 116
  sessions 91
monitor profile
  ADP 298
mounting
  rack 23, 67
  wall 69
Multicast 215
  IGMP Proxy 215
My Certificates, see also certificates 612
MyDoom 437

N

NAT 181, 190

ALG, see ALG
and address objects 186
and address objects (HOST) 196
and ALG 211
and interfaces 195
and policy routes 180, 186
and security policy 290
and to-ZyWALL security policy 197
and VPN 226
loopback 192
port forwarding, see NAT
port translation, see NAT
traversal 227
NBNS 136
NCAS
authentication methods 461
number of users 461
NCAS (Nebula Cloud Authentication Server) 461
NetBIOS
Name Server, see NBNS.
network access mode
full tunnel 268
Network Address Translation, see NAT
network-based intrusions 436, 437
NID FS 462
NID FS (Nebula IDentity Federation Service) 272, 462
Nimda 437
No-IP 581

O

objects 269
AAA server 480
addresses and address groups 324
certificates 609
schedules 344
services and service groups 333
users, user groups 459, 477
OIDC 318
Google Workspace 489
Microsoft Entra ID 488
OIDC Server 487
OpenID Connect 478
OIDC Server 478
ommon 412
OSI (Open System Interconnection) 426
OSI level-4 351
OSI level-7 351

P

P Reputation
Priority 392
P2P (Peer-to-peer) 433
attacks 433
see also Peer-to-peer
packet
inspection signatures 428
packet capture 675
files 674, 678, 680
troubleshooting 720
packet captures
downloading files 674, 675
passkey
overview 727
Peer-to-peer (P2P) 433
managing 350
Perfect Forward Secrecy (PFS)
Diffie-Hellman key group 229
performance
troubleshooting 711, 712
PFS (Perfect Forward Secrecy) 229
Phishing 392, 395
pointer record 585
policy routes 179
actions 181
and address objects 186
and ALG 211
and interfaces 186
and NAT 180
and schedules 185
and service objects 334
and trunks 172, 186
and user groups 184, 185, 202, 205
and users 184, 185, 202, 205
and VPN connections 716
benefits 180
criteria 181
overriding direct routes 182
troubleshooting 711
pop-up windows 25
port forwarding, see NAT

port groups 131
port translation, see NAT
power off 705
PPP
  troubleshooting 711
PPP interfaces
  subnet mask 135
PPPoE 137
  and RADIUS 137
PPPoE/PPTP interfaces 131
PPTP
  as VPN 137
PRF 242, 245, 253
Protocol Anomaly Detection 302
PseudoRandom Function 223
PTR record 585
Public-Key Infrastructure (PKI) 610
public-private key pairs 609, 610

Q

QoS 180

R

rack-mounting 23, 67
RADIUS 478, 480
  advantages 480
  and PPPoE 137
  and users 460
RADIUS server 601
registration 123
Relative Distinguished Name (RDN) 479
Remote Authentication Dial-In User Service, see RADIUS
Remote Capture 688
remote management
  see also service control 565
  to-Device security policy 289
remote network 220
reports
  anti-virus 100, 101
  daily 652
  daily e-mail 652
  IDP 98
reputation filter
  anonymizers 392
  categories 392
  spyware adware keyloggers 392
  statistics 94
reset 724
RESET button 724
Restart 726
RFC
  1631 (NAT) 181
  2131 (DHCP) 135
  2132 (DHCP) 135
  2402 (AH) 228
  2406 (ESP) 228
Rogue AP Detection 558
round robin 170
routing
  troubleshooting 713
routing protocols
  and Ethernet interfaces 142, 150
RSA 619, 623
rubber feet 68

S

SAM Account Name 484
sandboxing
  action 424
  defend center 422
  EICAR test files 423
  log 424
  securirty mechanism 422
scan attacks 433
scanner types 420
Scanners 394
schedule
  troubleshooting 719
schedules 344
  and content filtering 361, 362
  and current date/time 344
  and policy routes 185
  and security policy 294
  one-time 344

recurring 344
types of 344
screen resolution 25
SecuExtender 253
Secure Hash Algorithm, see SHA1
Secure Socket Layer, see SSL
security associations, see IPSec
security policy 288
actions 294
and ALG 211
and application patrol 350
and IPSec VPN 716
and logs 294
and NAT 290
and schedules 294
and service groups 293
and service objects 334
and services 293
and user groups 294, 307
and users 294, 307
and zones 288, 292
asymmetrical routes 290, 291
global rules 289
priority 292
rule criteria 289
see also to-Device security policy 288
session limits 304, 305
triangle routes 290, 291
troubleshooting 711
security settings
troubleshooting 710
sensitivity level 301
serial number 75
service control 565
and to-ZyWALL security policy 565
and users 566
timeouts 565
service groups 334
and security policy 293
in IDP 434
service objects 333
and IP protocols 334
and policy routes 334
and security policy 334
service subscription status 126
services 333
and security policy 293
session limits 304, 305
sessions 91
SHA1 223
shell scripts 656
shutdown 705
signature categories
access control 433
backdoor/Trojan 433
buffer overflow 432
DoS/DDoS 433
P2P 433
scan 433
virus/worm 433
Web attack 432
signature ID 431
signatures
IDP 426
updating 123, 268, 277, 456, 458
Simple Network Management Protocol, see SNMP
SIP
ALG 211
Smurf Attack 302
SNAT 181, 251, 272, 274
troubleshooting 713
SNMP 24, 596, 597
agents 597
authentication 600
Get 597
GetNext 597
Manager 597
managers 597
MIB 597
network components 597
Set 597
Trap 597
traps 597
version 3 and security 597
versions 596
Source Network Address Translation, see SNAT
Spam Sources 394
Spam URLs 392
spillover (for load balancing) 171
SQL Injection 395
SQL slammer 437
SSH 566, 567
client requirements 567
encryption methods 567

versions 567
SSL 268, 566
access policy 269
connection monitor 116
see also SSL VPN 268
ssl certificate 273
SSL Inspection
Protocols 443
SSL inspection
Server Signed Certificate Keys 445
SSL policy
objects used 269
SSL VPN 116, 268
access policy 269
full tunnel mode 268
see also SSL 268
startup-config.conf 661, 664
if errors 657
missing at restart 657
present at restart 657
startup-config-bad.conf 657
static routes 180
and interfaces 188
metric 189
statistics
anti-virus 100, 101
daily e-mail report 652
IDP 98
status 74
Storage 79
streaming protocols management 350
subscription services
status 126
supported browsers 25
syslog servers, see also logs
system log, see logs
system name 569
system-default.conf 661

T

TCP 333
connections 333
port numbers 334
throughput rate
troubleshooting 720
time 565
to-Device security policy
and remote management 289
global rules 288
see also security policy 288
Top N APs 119
Top N Stations 121
Tor 395
to-ZyWALL security policy
and NAT 197
and NAT traversal (VPN) 716
and service control 565
and VPN 716
trademarks 769
Transmission Control Protocol, see TCP
transmission speed
cable types 59
trapdoor attacks 433
triangle routes 290
allowing through the security policy 291
vs virtual interfaces 290
Triple Data Encryption Standard, see 3DES
trojan attacks 433
troubleshooting 672, 708
anti-virus 710, 712
application patrol 710, 715, 719
certificate 719
connection resets 715
content filter 710
DDNS 714
device access 708
firmware upload 720
FTP 715
IDP 710, 712
Internet access 708, 718
IPSec VPN 715
LEDs 708
logs 720
management access 720
packet capture 720
performance 711, 712
policy routes 711
PPP 711
problems 708
routing 713
schedules 719
security policy 711

security settings 710
SNAT 713
throughput rate 720
VLAN 711
trunks 131, 169
and ALG 211
and policy routes 172, 186
member interface mode 175, 176
see also load balancing 169
Trusted Certificates, see also certificates 621
Tunnel interfaces 131

U

UDP 333
messages 333
port numbers 334
updating
anti-virus signatures 127, 128
signatures 123, 268, 277, 456, 458
upgrading
firmware 667, 669
Uplink and Downlink 506
uploading
configuration files 660
firmware 667, 669
UPN
userPrincipalName 484
URL Threat Filter 392, 405
Priority 405
user authentication 459
external 460
local user database 478
User Datagram Protocol, see UDP
user group objects 459, 477
user groups 459, 460, 477
and content filtering 362
and policy routes 184, 185, 202, 205
and security policy 294, 307
user name
rules 465
user objects 459, 477
user sessions, see sessions
users 459, 477
admin (type) 459
admin, see also admin users
and AAA servers 460
and authentication method objects 460
and content filtering 362
and LDAP 460
and policy routes 184, 185, 202, 205
and RADIUS 460
and security policy 294, 307
and service control 566
attributes for Ext-User 460
default lease time 475
default reauthentication time 475
default type for Ext-User 460
Ext-User (type) 460
ext-user (type) 459
groups, see user groups
lease time 471
lockout 476
reauthentication time 471
types of 459
user (type) 459
user names 465

V

ventilation holes 67
virtual interfaces 131
not DHCP clients 135
vs asymmetrical routes 290
vs triangle routes 290
Virtual Private Network, see VPN
virus 433
attack 412, 433
boot sector 412
e-mail 412
file infector 412
macro 412
mutation 412
polymorphic 412
VLAN
advantages 138
and MAC address 137
ID 137
troubleshooting 711
VLAN ID 138
VLAN interfaces 131, 138
and Ethernet interfaces 138, 711

VoIP pass through
see also ALG 211
VPN 220
active protocol 228
and NAT 226
basic troubleshooting 716
IKE SA, see IKE SA
IPSec 220
IPSec SA
proposal 222
security associations (SA) 231
see also IKE SA
see also IPSec 220
see also IPSec SA
VPN Algorithm 230
VPN connections
and policy routes 716
VPN gateways
and to-ZyWALL security policy 716

W

wall-mounting 69
warranty 769, 774
note 769, 774
Web attack 432
Web Configurator 23
access 25
requirements 25
supported browsers 25
weighted round robin (for load balancing) 170
WiFi Aid 531
WiFi Connection Log 534
WiFi Connection Stages 531
Windows Internet Naming Service, see WINS.
WINS 136
Wizard Setup 43
WLAN interfaces 131
worm 412, 433
attacks 433

Z

zones 340
and interfaces 340
and security policy 288, 292
and VPN 340
extra-zone traffic 341
inter-zone traffic 341
intra-zone traffic 341
types of traffic 341