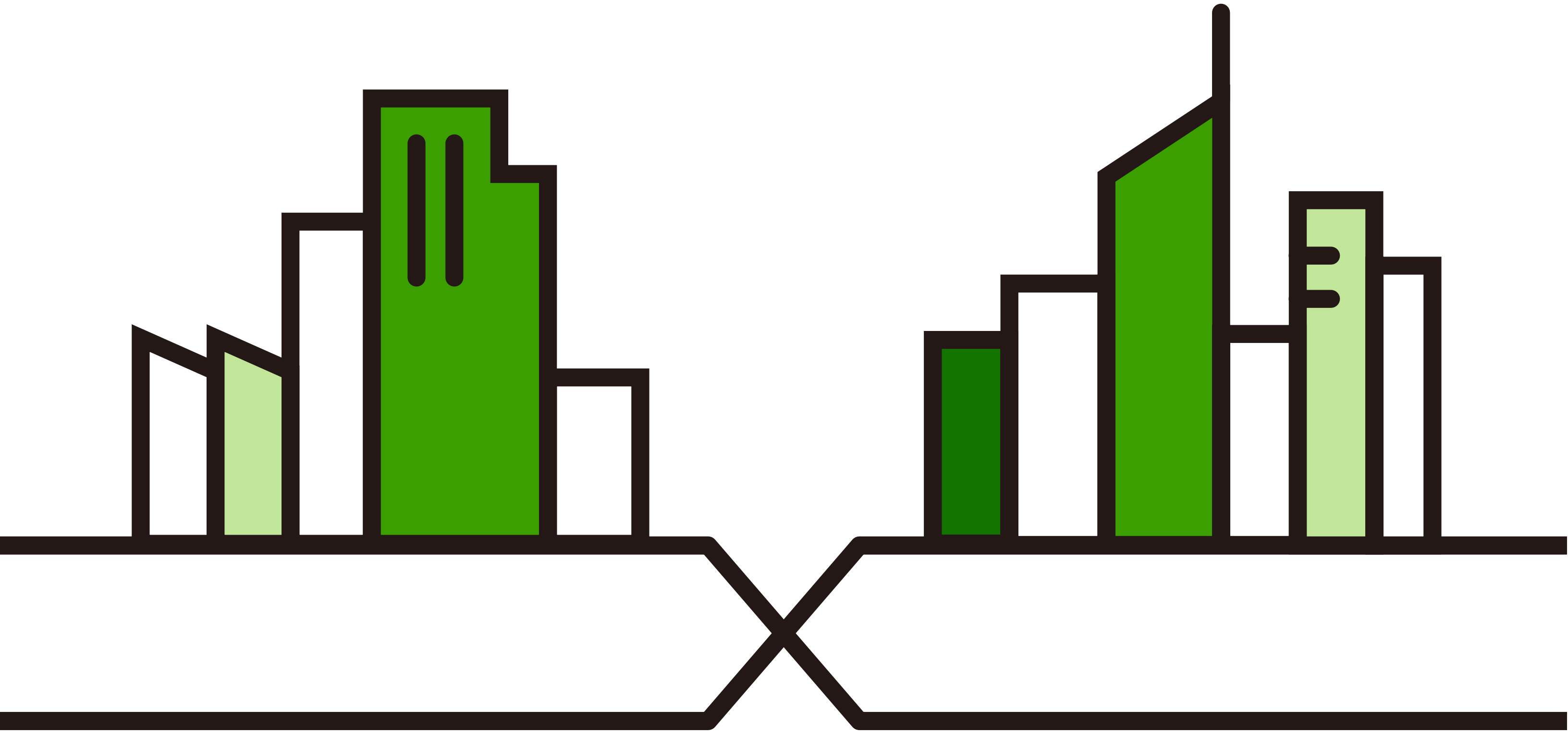
User's Guide

NWA/WAC/WAX/WBE Series

802.11 a/b/g/n/ac/ax/be Access Point

Default Login Details	
Management IP Address	http://DHCP-assigned IP OR http://192.168.1.2
User Name	admin
Password	1234

Version 6.70 Edition 2, 2/2024



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

This is a User's Guide for a series of products. Not all products support all firmware features. Screenshots and graphics in this book may differ slightly from your product due to differences in your product hardware, firmware, or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Some screens or options in this book may not be available for your product (see the product feature tables in Section 1.2 on page 14).

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the Zyxel Device and access the Web Configurator.
- CLI Reference Guide

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

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

- Web Configurator Online Help

  Click the help icon in any screen for help in configuring that screen and supplementary information.
- Nebula Control Center User's Guide

  This User's Guide shows how to manage the Zyxel Device remotely. The features of these devices can be managed through Nebula Control Center. It also offers features that are not available when the Zyxel Device is in standalone mode (see Section 2.1.2 on page 30).
- AC (AP Controller) User's Guide

  See the ZyWALL ATP, ZyWALL VPN, USG FLEX, or NXC User's Guide for instructions on using the gateways or NXC as an AP ConNWA/WAC/WAX/WBE Series User's Guidetroller (AC) for the Zyxel Device. This is used when the Zyxel Device is set to be managed by a Zyxel AC.
- More Information

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

Document Conventions

Warnings and Notes

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

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

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

Syntax Conventions

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

Icons Used in Figures

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

Zyxel Device	Router	Switch	Internet
Server	Desktop	Laptop	IP Phone
Printer	Smart T.V.		

Contents Overview

Introduction ... 13
AP Management ... 29
Hardware ... 40
Web Configurator ... 49

Standalone Configuration ... 60

Standalone Configuration ... 61
Dashboard ... 63
Setup Wizard ... 69
Getting Started ... 76
Monitor ... 90
Network ... 102
Wireless ... 115
Bluetooth ... 131
User ... 134
AP Profile ... 141
WDS Profile ... 187
Certificates ... 189
System ... 205
Log and Report ... 227
File Manager ... 239
Diagnostics ... 253
LEDs ... 256
Antenna Switch ... 259
Reboot ... 261

Local Configuration in Cloud Mode ... 263

Cloud Mode ... 264
Network ... 267
Maintenance ... 270

Appendices and Troubleshooting ... 277

Troubleshooting ... 278

Table of Contents

Document Conventions 3

Contents Overview 4

Table of Contents 5

Chapter 1
Introduction 13

1.1 Overview 13
1.2 Zyxel Device Product Feature Comparison 14
1.3 Zyxel Device Roles 18
1.3.1 Radio Frequency (RF) Monitor 26
1.4 Sample Feature Applications 26
1.4.1 MBSSID 26
1.4.2 Dual-Radio/Triple-Radio and BandFlex 27

Chapter 2
AP Management....................29

2.1 Management Mode 29
2.1.1 Standalone 29
2.1.2 Nebula Control Center 30
2.1.3 AP Controller (AC) 32
2.2 Switching Management Modes 32
2.3 Zyxel One Network (ZON) Utility 33
2.3.1 Requirements 33
2.3.2 Run the ZON Utility 34
2.4 Ways to Access the Zyxel Device 38
2.5 Good Habits for Managing the Zyxel Device 39

Chapter 3
Hardware 40

3.1 Grounding (WAC6552D-S, WAC6553D-E and WAX655E) 40
3.2 Zyxel Device Models With Single LEDs 41
3.3 Zyxel Device LED 41
3.4 Ports 46

Chapter 4
Web Configurator....................49

4.1 Overview 49
4.2 Accessing the Web Configurator 49

4.3 Navigating the Web Configurator 52
4.3.1 Title Bar 53
4.3.2 Navigation Panel 54
4.3.3 Standalone Mode Navigation Panel Menus 54
4.3.4 Cloud Mode Navigation Panel Menus 56
4.3.5 Tables and Lists 57

Part I: Standalone Configuration 60

Chapter 5
Standalone Configuration 61

5.1 Overview 61
5.2 Starting and Stopping the Zyxel Device 61

Chapter 6
Dashboard 63

6.1 Overview 63
6.1.1 CPU Usage 67
6.1.2 Memory Usage 68

Chapter 7
Setup Wizard 69

7.1 Accessing the Wizard 69
7.2 Using the Wizard 69
7.2.1 Step 1 Time Settings 69
7.2.2 Step 2 Password and Uplink Connection 70
7.2.3 Step 3 SSID 71
7.2.4 Step 4 Radio 73
7.2.5 Summary 74

Chapter 8
Getting Started 76

8.1 Getting Started Overview 76
8.2 Choose the Operation Mode 76
8.3 Set Up a WiFi Network 76
8.3.1 Configure a WiFi Network in AP Mode 77
8.3.2 Configure a WiFi Network in Root AP / Repeater Mode 78
8.4 Set Up Rogue AP Detection 79
8.4.1 Set Up a Friendly AP List 81
8.4.2 Import the Friendly AP List to Other APs 82
8.5 Set Up an Email Daily Report 83

8.6 Restrict Access to Specific Parts of Your Network 84
8.6.1 Scenario 84
8.6.2 Your Requirements 84
8.6.3 Setup 85
8.6.4 Configure the SERVER_1 Network 86
8.6.5 Configure the SERVER_2 Network 87
8.7 Check Your Settings and Test the Access Restrictions 88
8.7.1 Check Settings 88
8.7.2 Test the Access Restrictions 89

Chapter 9
Monitor 90

9.1 Overview 90
9.1.1 What You Can Do in this Chapter 90
9.2 What You Need to Know 90
9.3 Network Status 91
9.3.1 Port Statistics Graph 92
9.4 Radio List 93
9.4.1 AP Mode Radio Information 94
9.5 Station List 96
9.6 WDS Link Info 97
9.7 Detected Device 98
9.8 View Log 100

Chapter 10
Network 102

10.1 Overview 102
10.1.1 AP Controller Management 102
10.1.2 What You Can Do in this Chapter 104
10.2 IP Setting 105
10.3 VLAN 106
10.4 Storm Control 111
10.5 AC (AP Controller) Discovery 112
10.6 NCC Discovery 113

Chapter 11
Wireless 115

11.1 Overview 115
11.1.1 What You Can Do in this Chapter 115
11.1.2 What You Need to Know 116
11.2 AP Management 116
11.3 Rogue AP 122
11.3.1 Add/Edit Rogue/Friendly List 125

11.4 Load Balancing 126

11.4.1 Disassociating and Delaying Connections 127

11.5 DCS 128

11.6 Technical Reference 129

Chapter 12
Bluetooth........131

12.1 Overview 131

12.1.1 What You Need To Know 131

12.2 Bluetooth Advertising Settings 131

12.2.1 Edit Advertising Settings 132

Chapter 13
User........134

13.1 Overview 134

13.1.1 What You Can Do in this Chapter 134

13.1.2 What You Need To Know 134

13.2 User Summary 135

13.2.1 Add/Edit User 135

13.3 Setting 137

13.3.1 Edit User Authentication Timeout Settings 139

Chapter 14
AP Profile........141

14.1 Overview 141

14.1.1 What You Can Do in this Chapter 141

14.1.2 What You Need To Know 141

14.2 Radio 146

14.2.1 Add/Edit Radio Profile 147

14.3 SSID 154

14.3.1 SSID List 154

14.3.2 Add/Edit SSID Profile 156

14.3.3 Setting Up General and Guest WiFi Networks on Both Radios 158

14.4 Security List 163

14.4.1 Add/Edit Security Profile 164

14.4.2 Creating a Security Profile 180

14.5 MAC Filter List 181

14.5.1 Add/Edit MAC Filter Profile 182

14.6 Layer-2 Isolation List 183

14.6.1 Add/Edit Layer-2 Isolation Profile 185

Chapter 15
WDS Profile........187

15.1 Overview 187
15.1.1 What You Can Do in this Chapter 187
15.2 WDS Profile 187
15.2.1 Add/Edit WDS Profile 188

Chapter 16
Certificates 189

16.1 Overview 189
16.1.1 What You Can Do in this Chapter 189
16.1.2 What You Need to Know 189
16.1.3 Verifying a Certificate 191
16.2 My Certificates 192
16.2.1 Add My Certificates 193
16.2.2 Edit My Certificates 195
16.2.3 Import Certificates 198
16.3 Trusted Certificates 199
16.3.1 Edit Trusted Certificates 200
16.3.2 Import Trusted Certificates 203
16.4 Technical Reference 204

Chapter 17
System 205

17.1 Overview 205
17.1.1 What You Can Do in this Chapter 205
17.2 Host Name 205
17.3 Power Mode 206
17.4 Date and Time 207
17.4.1 Pre-defined NTP Time Servers List 209
17.4.2 Time Server Synchronization 209
17.5 WWW Overview 210
17.5.1 Service Access Limitations 210
17.5.2 System Timeout 210
17.5.3 HTTPS 211
17.5.4 Configuring WWW Service Control 211
17.5.5 HTTPS Example 213
17.6 SSH 218
17.6.1 How SSH Works 219
17.6.2 SSH Implementation on the Zyxel Device 220
17.6.3 Requirements for Using SSH 220
17.6.4 Configuring SSH 220
17.6.5 Examples of Secure Telnet Using SSH 221
17.7 FTP 222
17.8 SNMP 223

17.8.1 Supported MIBs 224
17.8.2 SNMP Traps 224
17.8.3 Configuring SNMP 224
17.8.4 Adding or Editing an SNMPv3 User Profile 225

Chapter 18
Log and Report........ 227

18.1 Overview 227
18.1.1 What You Can Do In this Chapter 227
18.2 Email Daily Report 227
18.3 Log Setting 229
18.3.1 Log Setting Screen 229
18.3.2 Edit System Log Settings 230
18.3.3 Edit Remote Server 234
18.3.4 Active Log Summary 235

Chapter 19
File Manager 239

19.1 Overview 239
19.1.1 What You Can Do in this Chapter 239
19.1.2 What you Need to Know 239
19.2 Configuration File 242
19.2.1 Example of Configuration File Download Using FTP 246
19.3 Firmware Package 247
19.3.1 Example of Firmware Upload Using FTP 250
19.4 Shell Script 251

Chapter 20
Diagnostics 253

20.1 Overview 253
20.1.1 What You Can Do in this Chapter 253
20.2 Diagnostics 253
20.3 Remote Capture 254

Chapter 21
LEDs 256

21.1 Overview 256
21.1.1 What You Can Do in this Chapter 256
21.2 Suppression Screen 256
21.3 Locator Screen 257

Chapter 22
Antenna Switch 259

22.1 Overview 259
22.1.1 What You Need To Know 259
22.2 Antenna Switch Screen 259

Chapter 23
Reboot 261

23.1 Overview 261
23.1.1 What You Need To Know 261
23.2 Reboot 261

Part II: Local Configuration in Cloud Mode 263

Chapter 24
Cloud Mode 264

24.1 Overview 264
24.2 Cloud Mode Web Configurator Screens 264
24.3 Dashboard 265

Chapter 25
Network 267

25.1 Overview 267
25.1.1 What You Can Do in this Chapter 267
25.2 IP Setting 267
25.3 VLAN 269

Chapter 26
Maintenance 270

26.1 Overview 270
26.1.1 What You Can Do in this Chapter 270
26.2 Shell Script 270
26.3 Diagnostics 273
26.4 Remote Capture 273
26.5 View Log 274

Part III: Appendices and Troubleshooting 277

Chapter 27
Troubleshooting 278

27.1 Overview 278
27.2 Power, Hardware Connections, and LED 278

27.3 Zyxel Device Management, Access, and Login 279
27.4 Internet Access 284
27.5 WiFi Network 285
27.6 Resetting the Zyxel Device 287
27.7 Getting More Troubleshooting Help 288

Appendix A Importing a Certificate 289

Appendix B IPv6 302

Appendix C Customer Support 310

Appendix D Legal Information 315

Index 327

CHAPTER 1
Introduction

1.1 Overview

This User's Guide covers the models listed in the following table. They can be managed in one of the following methods: remote management through Nebula Control Center (NCC) or an AP Controller (AC) such as the ZyWALL ATP, or local management in Standalone Mode. Each Zyxel Device runs in standalone mode by default, but it is recommended to use NCC management if it is available for your device.

NCC, AC or Standalone (NebulaFlex PRO)

- WAC500
- WAC500H
- WAX300H
- WAX510D
- WAX610D
- WAX620D-6E
- WAX630S
- WAX640S-6E
- WAX650S
- WAX655E
- WBE530
- WBE660S

NCC or Standalone (NebulaFlex)

- NWA110AX
- NWA1123ACv3
- NWA130BE
- NWA210AX
- NWA220AX-6E

For more information about Access Point (AP) management, see Section 2.1 on page 29.

When two or more APs are interconnected, this network is called a Wireless Distribution System (WDS). See Section 1.3 on page 18 for more information on root and repeater APs and how to set them up.

The screens you see in the Web Configurator may be different depending on the Zyxel Device model you are using.

1.2 Zyxel Device Product Feature Comparison

The following tables show the differences between each Zyxel Device model. You can find the feature introductions in the later sections.

Table 1 500/1000 Models Comparison Table

FEATURES	WAC500	WAC500H	NWA1123-ACv3
Supported WiFi Standards	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac
Supported Frequency Bands	2.4 GHz 5 GHz	2.4 GHz 5 GHz	2.4 GHz 5 GHz
Supported Channel Width	2.4G: 20/40 MHz 5G: 20/40/80 MHz	2.4G: 20/40 MHz 5G: 20/40/80 MHz	2.4G: 20/40 MHz 5G: 20/40/80 MHz
Available Security Modes	None / Enhanced-open / WEP/ WPA2-MIX / WPA3 - Personal & Enterprise	None / Enhanced-open / WEP/ WPA2-MIX / WPA3 - Personal & Enterprise	None/ Enhanced-open/ WEP / WPA2-MIX / WPA3 - Personal & Enterprise
Number of SSID Profiles	64	64	64
Number of WiFi Radios	2	2	2
Security Profile Radius Settings	Yes	Yes	Yes
Security Profile Enterprise Authentication Settings	Yes	Yes	Yes
Rogue AP Detection	Yes	Yes	Yes
WDS (Wireless Distribution System) - Root AP & Repeater Modes	Yes	Yes	Yes
Wireless Bridge	No	No	No
Tunnel Forwarding Mode	Yes	Yes	No
Layer-2 Isolation	Yes	Yes	Yes
Supported PoE Standards	IEEE 802.3af IEEE 802.3at	IEEE 802.3af IEEE 802.3at	IEEE 802.3af IEEE 802.3at
Power Detection	No	No	No
External Antennas	No	No	No
Internal Antennas	Yes	Yes	Yes
Antenna Switch	No	No	No
Smart Antenna	Yes	Yes	Yes
Console Port	4-Pin Serial	4-Pin Serial	4-Pin Serial
Reset Button	Yes	Yes	Yes
LED Locator	Yes	Yes	Yes
LED Suppression	Yes	Yes	Yes
AC (AP Controller) Discovery	Yes	Yes	No
NebulaFlex PRO	Yes	Yes	No
NCC Discovery	Yes	Yes	Yes
802.11r Fast Roaming Support	Yes	Yes	Yes
802.11k/v Assisted Roaming	Yes	Yes	Yes
Proxy ARP	Yes	Yes	Yes

Table 1 500/1000 Models Comparison Table (continued)

FEATURES	WAC500	WAC500H	NWA1123-ACv3
Bluetooth Low Energy (BLE)	No	No	No
Load Balancing	Yes	Yes	Yes
Ethernet Storm Control	Yes	Yes	Yes
Wireless Remote Capture	Yes	Yes	Yes
SNMP	Yes	Yes	Yes
Grounding	No	No	No
Power Jack	Yes	Yes	Yes
Maximum number of log messages	512 event logs		
Latest Firmware Version Supported	6.70	6.70	6.70

Table 2 WiFi 6 Models Comparison Table

FEATURES	WAX300H	WAX510D	WAX610D
Supported WiFi Standards	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax
Supported Frequency Bands	2.4 GHz 5 GHz	2.4 GHz 5 GHz	2.4 GHz 5 GHz
Supported Channel Width	2.4G: 20/40 MHz 5G: 20/40/80/160 MHz	2.4G: 20/40 MHz 5G: 20/40/80 MHz	2.4G: 20/40 MHz 5G: 20/40/80/160 MHz
Available Security Modes	None/ Enhanced-open / WEP / WPA2-MIX / WPA3 - Personal & Enterprise	None / Enhanced-open / WEP / WPA2-MIX / WPA3 - Personal & Enterprise	None / Enhanced-open / WEP / WPA2-MIX / WPA3 - Personal & Enterprise
Number of SSID Profiles	64	64	64
Number of WiFi Radios	2	2	2
Security Profile Radius Settings	Yes	Yes	Yes
Security Profile Enterprise Authentication Settings	Yes	Yes	Yes
Rogue AP Detection	No	Yes	Yes
WDS (Wireless Distribution System) - Root AP & Repeater Modes	Yes	Yes	Yes
Wireless Bridge	No	No	Yes
Tunnel Forwarding Mode	No	Yes	Yes
Layer-2 Isolation	Yes	Yes	Yes
Supported PoE Standards	IEEE 802.3af IEEE 802.3at	IEEE 802.3af IEEE 802.3at	IEEE 802.3af IEEE 802.3at
Power Detection	No	Yes	Yes
External Antennas	No	No	No
Internal Antennas	Yes	Yes	Yes
Antenna Switch	No	Yes (per AP)	Yes (per AP)
Smart Antenna	No	No	No
Console Port	4-Pin Serial	4-Pin Serial	4-Pin Serial

Table 2 WiFi 6 Models Comparison Table (continued)

FEATURES	WAX300H	WAX510D	WAX610D
Reset Button	Yes	Yes	Yes
LED Locator	Yes	Yes	Yes
LED Suppression	Yes	Yes	Yes
AC (AP Controller) Discovery	Yes	Yes	Yes
NebulaFlex PRO	Yes	Yes	Yes
NCC Discovery	Yes	Yes	Yes
802.11r Fast Roaming Support	Yes	Yes	Yes
802.11k/v Assisted Roaming	Yes	Yes	Yes
Proxy ARP	Yes	Yes	Yes
Bluetooth Low Energy (BLE)	No	No	No
Load Balancing	No	Yes	Yes
Ethernet Storm Control	Yes	Yes	Yes
Wireless Remote Capture	Yes	Yes	Yes
SNMP	No	Yes	Yes
Grounding	No	Yes	Yes
Power Jack	No	Yes	Yes
Maximum number of log messages	512 event logs		
Latest Firmware Version Supported	6.70	6.70	6.70

Table 3 WiFi 6 Models Comparison Table

FEATURES	WAX630S	WAX650S	WAX655E
Supported WiFi Standards	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax
Supported Frequency Bands	2.4 GHz 5 GHz	2.4 GHz 5 GHz	2.4 GHz 5 GHz
Supported Channel Width	2.4G: 20/40 MHz 5G: 20/40/80/160 MHz	2.4G: 20/40 MHz 5G: 20/40/80/160 MHz	2.4G: 20/40 MHz 5G: 20/40/80/160 MHz
Available Security Modes	None/ Enhanced-open / WEP /WPA2-MIX / WPA3 - Personal & Enterprise	None / Enhanced-open / WEP / WPA2-MIX / WPA3 - Personal & Enterprise	None / Enhanced-open / WEP / WPA2-MIX / WPA3 - Personal & Enterprise
Number of SSID Profiles	64	64	64
Number of WiFi Radios	2	2	2
Security Profile Radius Settings	Yes	Yes	Yes
Security Profile Enterprise Authentication Settings	Yes	Yes	Yes
Rogue AP Detection	Yes	Yes	Yes
WDS (Wireless Distribution System) - Root AP & Repeater Modes	Yes	Yes	Yes
Wireless Bridge	Yes	Yes	Yes

Table 3 WiFi 6 Models Comparison Table (continued)

FEATURES	WAX630S	WAX650S	WAX655E
Tunnel Forwarding Mode	Yes	Yes	Yes
Layer-2 Isolation	Yes	Yes	Yes
Supported PoE Standards	IEEE 802.3af IEEE 802.3at	IEEE 802.3at IEEE 802.3bt	IEEE 802.3af IEEE 802.3at
Power Detection	Yes	Yes	Yes
External Antennas	No	No	Yes
Internal Antennas	Yes	Yes	No
Antenna Switch	No	No	No
Smart Antenna	Yes	Yes	No
Console Port	4-Pin Serial	4-Pin Serial	4-Pin Serial
Reset Button	Yes	Yes	Yes
LED Locator	Yes	Yes	Yes
LED Suppression	Yes	Yes	Yes
AC (AP Controller) Discovery	Yes	Yes	Yes
NebulaFlex PRO	Yes	Yes	Yes
NCC Discovery	Yes	Yes	Yes
802.11r Fast Roaming Support	Yes	Yes	Yes
802.11k/v Assisted Roaming	Yes	Yes	Yes
Proxy ARP	Yes	Yes	Yes
Bluetooth Low Energy (BLE)	No	Yes	No
Load Balancing	Yes	Yes	Yes
Ethernet Storm Control	Yes	Yes	Yes
Wireless Remote Capture	Yes	Yes	Yes
SNMP	Yes	Yes	Yes
Grounding	Yes	Yes	Yes
Power Jack	Yes	Yes	Yes
Maximum number of log messages	512 event logs		
Latest Firmware Version Supported	6.70	6.70	6.70

1.3 Zyxel Device Roles

Table 4 WiFi 6 Models Comparison Table

FEATURES	NWA110AX	NWA210AX
Supported WiFi Standards	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax
Supported Frequency Bands	2.4 GHz 5 GHz	2.4 GHz 5 GHz
Supported Channel Width	2.4G: 20/40 MHz 5G: 20/40/80 MHz	2.4G: 20/40 MHz 5G: 20/40/80/160 MHz
Available Security Modes	None /Enhanced-open / WEP / WPA2-MIX / WPA3 - Personal & Enterprise	None /Enhanced-open / WEP / WPA2-MIX / WPA3 - Personal & Enterprise
Number of SSID Profiles	64	64
Number of WiFi Radios	2	2
Security Profile Radius Settings	Yes	Yes
Security Profile Enterprise Authentication Settings	Yes	Yes
Rogue AP Detection	Yes	Yes
WDS (Wireless Distribution System) - Root AP & Repeater Modes	Yes	Yes
Wireless Bridge	No	No
Tunnel Forwarding Mode	No	No
Layer-2 Isolation	Yes	Yes
Supported PoE Standards	IEEE 802.3af IEEE 802.3at	IEEE 802.3af IEEE 802.3at
Power Detection	Yes	Yes
External Antennas	No	No
Internal Antennas	Yes	Yes
Antenna Switch	No	No
Smart Antenna	No	No
Console Port	4-Pin Serial	4-Pin Serial
Reset Button	Yes	Yes
LED Locator	Yes	Yes
LED Suppression	Yes	Yes
AC (AP Controller) Discovery	No	No
NebulaFlex PRO	No	No
NCC Discovery	Yes	Yes
802.11r Fast Roaming Support	Yes	Yes
802.11k/v Assisted Roaming	Yes	Yes
Proxy ARP	Yes	Yes
Bluetooth Low Energy (BLE)	No	No
Load Balancing	Yes	Yes

Table 4 WiFi 6 Models Comparison Table (continued)

FEATURES	NWA110AX	NWA210AX
Ethernet Storm Control	Yes	Yes
Wireless Remote Capture	Yes	Yes
SNMP	Yes	Yes
Grounding	Yes	Yes
Power Jack	Yes	Yes
Maximum number of log messages	512 event logs	
Latest Firmware Version Supported	6.70	6.70

Table 5 WiFi 6E Models Comparison Table

FEATURES	WAX620D-6E	WAX640S-6E	NWA220AX-6E
Supported WiFi Standards	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax
Supported Frequency Bands	2.4 GHz 5 GHz 6 GHz	2.4 GHz 5 GHz 6 GHz	2.4 GHz 5 GHz 6 GHz
BandFlex (5 GHz/6 GHz)	Yes	No	Yes
Supported Channel Width	2.4G: 20/40 MHz 5G: 20/40/80/160 MHz 6G: 20/40/80/160 MHz	2.4G: 20/40 MHz 5G: 20/40/80/160 MHz 6G: 20/40/80/160 MHz	2.4G: 20/40 MHz 5G: 20/40/80/160 MHz 6G: 20/40/80/160 MHz
Available Security Modes	None / Enhanced-open / WEP / WPA2-MIX / WPA3 - Personal & Enterprise	None / Enhanced-open / WEP / WPA2-MIX / WPA3 - Personal & Enterprise	None / Enhanced-open / WEP / WPA2-MIX / WPA3 - Personal & Enterprise
Number of SSID Profiles	64	64	64
Number of WiFi Radios	2	3	2
Security Profile Radius Settings	Yes	Yes	Yes
Security Profile Enterprise Authentication Settings	Yes	Yes	Yes
Rogue AP Detection	Yes	Yes	Yes
WDS (Wireless Distribution System) - Root AP & Repeater Modes	Yes	Yes	Yes
Wireless Bridge	Yes	Yes	No
Tunnel Forwarding Mode	Yes	Yes	No
Layer-2 Isolation	Yes	Yes	Yes
Supported PoE Standards	IEEE 802.3af IEEE 802.3at	IEEE 802.3at IEEE 802.3bt	IEEE 802.3at IEEE 802.3af
Power Detection	Yes	Yes	Yes
External Antennas	No	No	No
Internal Antennas	Yes	Yes	Yes
Antenna Switch	Yes (per AP)	No	No
Smart Antenna	No	Yes	No
Console Port	4-Pin Serial	4-Pin Serial	4-Pin Serial

Table 5 WiFi 6E Models Comparison Table (continued)

FEATURES	WAX620D-6E	WAX640S-6E	NWA220AX-6E
Reset Button	Yes	Yes	Yes
LED Locator	Yes	Yes	Yes
LED Suppression	Yes	Yes	Yes
AC (AP Controller) Discovery	Yes	Yes	No
NebulaFlex PRO	Yes	Yes	No
NCC Discovery	Yes	Yes	Yes
802.11r Fast Roaming Support	Yes	Yes	Yes
802.11k/v Assisted Roaming	Yes	Yes	Yes
Proxy ARP	Yes	Yes	Yes
Bluetooth Low Energy (BLE)	No	Yes	No
Load Balancing	Yes	Yes	Yes
Ethernet Storm Control	Yes	Yes	Yes
Wireless Remote Capture	Yes	Yes	Yes
SNMP	Yes	Yes	Yes
Grounding	No	Yes	No
Power Jack	Yes	Yes	Yes
Maximum number of log messages	512 event logs		
Latest Firmware Version Supported	6.70	6.70	6.70

Table 6 WiFi 7 Models Comparison Table

FEATURES	NWA130BE	WBE530	WBE660S
Supported WiFi Standards	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax IEEE 802.11be	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax IEEE 802.11be	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax IEEE 802.11be
Supported Frequency Bands	2.4 GHz 5 GHz 6 GHz	2.4 GHz 5 GHz 6 GHz	2.4 GHz 5 GHz 6 GHz
BandFlex (5 GHz /6 GHz)	Yes	Yes	Yes
Supported Channel Width	2.4G: 20/40 MHz 5G: 20/40/80/160/240 MHz 6G: 80/160/320 MHz	2.4G: 20/40 MHz 5G: 20/40/80/160/240 MHz 6G: 80/160/320 MHz	2.4G: 20/40 MHz 5G: 20/40/80/160/240 MHz 6G: 80/160/320 MHz
Available Security Modes	None / Enhanced-open / WEP /WPA2-MIX / WPA3 - Personal & Enterprise	None / Enhanced-open / WEP /WPA2-MIX / WPA3 - Personal & Enterprise	None / Enhanced-open / WEP / WPA2-MIX / WPA3 - Personal & Enterprise
Number of SSID Profiles	64	64	64
Number of WiFi Radios	3	3	3
Security Profile Radius Settings	Yes	Yes	Yes
Security Profile Enterprise Authentication Settings	Yes	Yes	Yes
Rogue AP Detection	Yes	Yes	Yes

Table 6 WiFi 7 Models Comparison Table (continued)

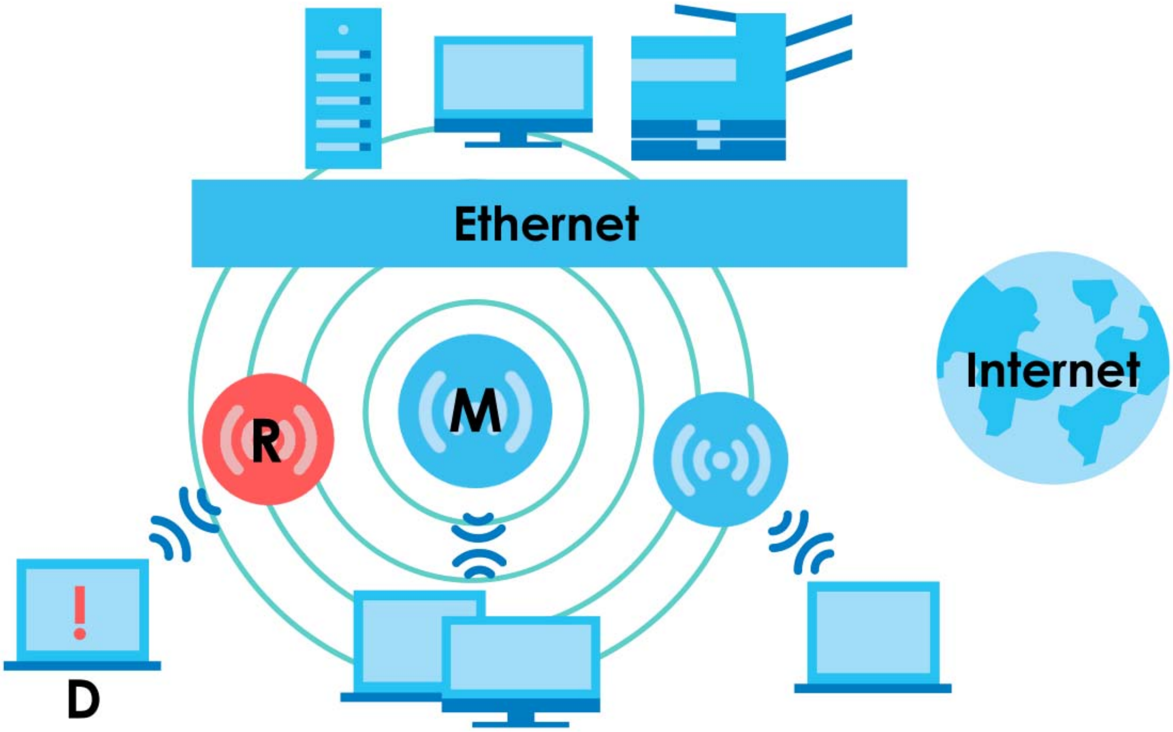
FEATURES	NWA130BE	WBE530	WBE660S
WDS (Wireless Distribution System) - Root AP & Repeater Modes	Yes	Yes	Yes
Wireless Bridge	Yes	Yes	Yes
Tunnel Forwarding Mode	Yes	Yes	Yes
Layer-2 Isolation	Yes	Yes	Yes
Supported PoE Standards	IEEE 802.3at IEEE 802.3af	IEEE 802.3at IEEE 802.3af	IEEE 802.3bt IEEE 802.3at
Power Detection	Yes	Yes	Yes
External Antennas	No	No	No
Internal Antennas	Yes	Yes	Yes
Antenna Switch	No	No	No
Smart Antenna	No	No	Yes
Console Port	4-Pin Serial	4-Pin Serial	4-Pin Serial
Reset Button	Yes	Yes	Yes
LED Locator	Yes	Yes	Yes
LED Suppression	Yes	Yes	Yes
AC (AP Controller) Discovery	No	No	Yes
NebulaFlex PRO	No	No	Yes
NCC Discovery	Yes	Yes	Yes
802.11r Fast Roaming Support	Yes	Yes	Yes
802.11k/v Assisted Roaming	Yes	Yes	Yes
Proxy ARP	Yes	Yes	Yes
Bluetooth Low Energy (BLE)	No	No	Yes
Load Balancing	Yes	Yes	Yes
Ethernet Storm Control	Yes	Yes	Yes
Wireless Remote Capture	Yes	Yes	Yes
SNMP	Yes	Yes	Yes
Grounding	No	No	No
Power Jack	Yes	Yes	USB-C
Maximum number of log messages	512 event logs	512 event logs	512 event logs
Latest Firmware Version Supported	6.70	6.70	6.70

This section describes some of the different roles that your Zyxel Device can take up within a network. Not all roles are supported by all models (see Section 1.2 on page 14). The Zyxel Device can serve as a:

- Access Point (AP) – This is used to allow WiFi clients to connect to the Internet.
- Radio Frequency (RF) monitor – If your Zyxel Device supports rogue APs detection, it can serve as an RF monitor and searches for rogue APs to help eliminate network threats. An RF monitor can simultaneously act as an AP.
- Root AP – A root AP connects to the gateway or switch through a wired Ethernet connection and has wireless repeaters connected to it to extend its range.
- WiFi Repeater – A WiFi repeater wirelessly connects to a root AP and extends the network's wireless range. A wireless repeater can also be a wireless bridge that connects to a root AP and extends the network to wired client devices.

If a client (**D**) tries to set up his own AP (**R**) with weak security settings, the network becomes exposed to threats. The RF monitor (**M**) scans the area to detect all APs, which can help the network administrator discover these rogue APs and remove them.

Figure 1 Zyxel Device Application in a Network

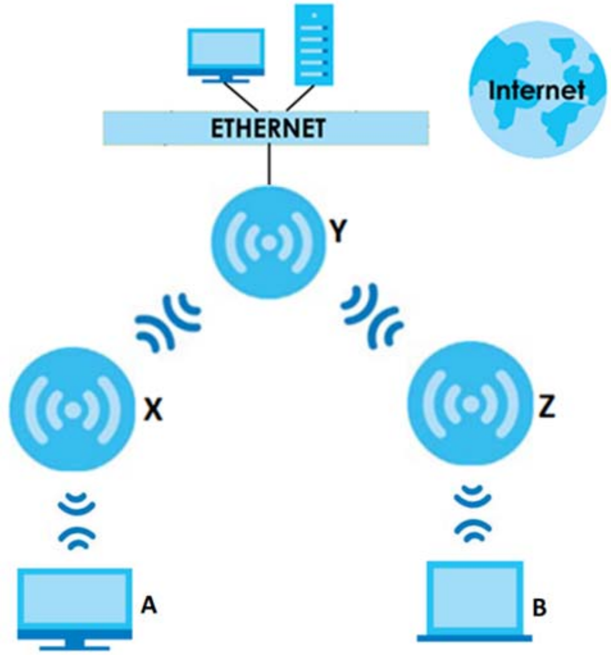


Wireless Distribution System (WDS)

Wireless Distribution System (WDS) is a network system that allows you to distribute the network to areas that require Internet connections. You can extend your network to unreachable areas with wireless repeaters.

The following figure shows you how to create a secure WDS with two wireless repeaters. The root AP (**Y**) is connected to a network with Internet access and has wireless repeaters (**X** and **Z**) connected to it to expand the WiFi network's range. Clients (**A** and **B**) can access the wired network through the wireless repeaters (**X** and **Z**) and/or root AP.

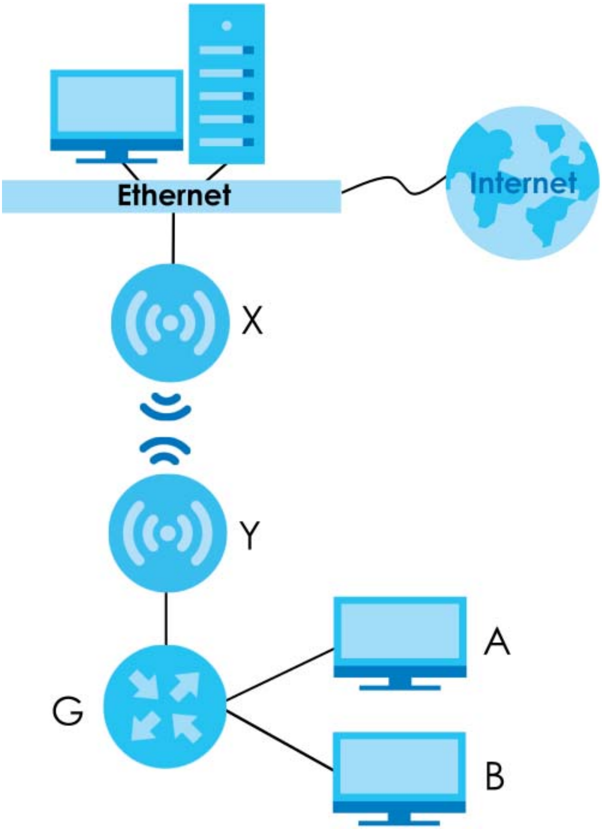
Figure 2 Wireless Distribution System Network Example



The Zyxel Device can also serve as a wireless bridge in Repeater mode. A wireless bridge connects two wired networks through a wireless connection. When the Zyxel Device is connected to a root AP, enable wireless bridge to allow traffic through the Ethernet port on the Zyxel Device to a wired network. Check Section 1.2 on page 14 for models that support wireless bridge.

The following figure shows an example of a WDS with a repeater acting as a wireless bridge. The root AP (**X**) is connected to a network with Internet access. The wireless repeater (**Y**) is connected to the root AP (**X**) to expand the network. Clients (**A** and **B**) are connected to the wireless repeater through the switch/ gateway/router (**G**). They can access the network with the extended wired network the wireless bridge (wireless repeater) provides.

Figure 3 Wireless Bridge Network Example

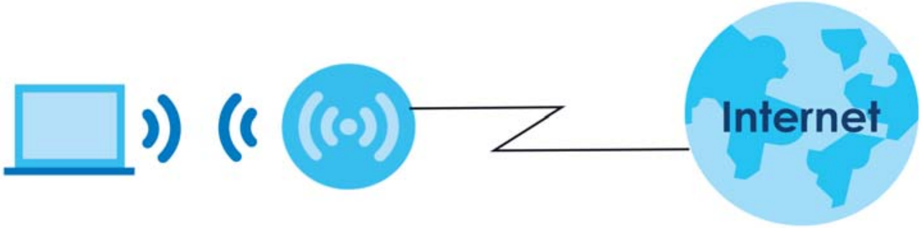


Access Point (AP)

the Zyxel Device can receive connections from WiFi clients and pass their data traffic through to the Zyxel Device to be managed (or subsequently passed on to an upstream gateway for managing).

In **AP Mode**, the Zyxel Device is connected to a broadband modem with Internet access and provides a WiFi network for users to use their notebooks or computers to wirelessly access the Internet.

Figure 4 AP Mode Application



Root AP

The Zyxel Device acts as an AP and also supports the WiFi connections with other APs (in repeater mode) to form a WDS to extend its WiFi network.

In **Root AP** mode, you can have multiple SSIDs active for regular WiFi connections and one SSID (WDS SSID) for the connection with a repeater. WiFi clients can use either SSID to associate with the Zyxel

Device in Root AP mode. A repeater must use the repeater SSID to connect to the Zyxel Device in **Root AP** mode. See Section 15.1 on page 187 for more details.

When the Zyxel Device is in **Root AP** mode, repeater security between the Zyxel Device and other repeaters is independent of the security between the WiFi clients and the AP or repeater. When repeater security is enabled, both APs and repeaters must use the same pre-shared key. See Section 11.2 on page 116 and Section 15.2 on page 187 for more details.

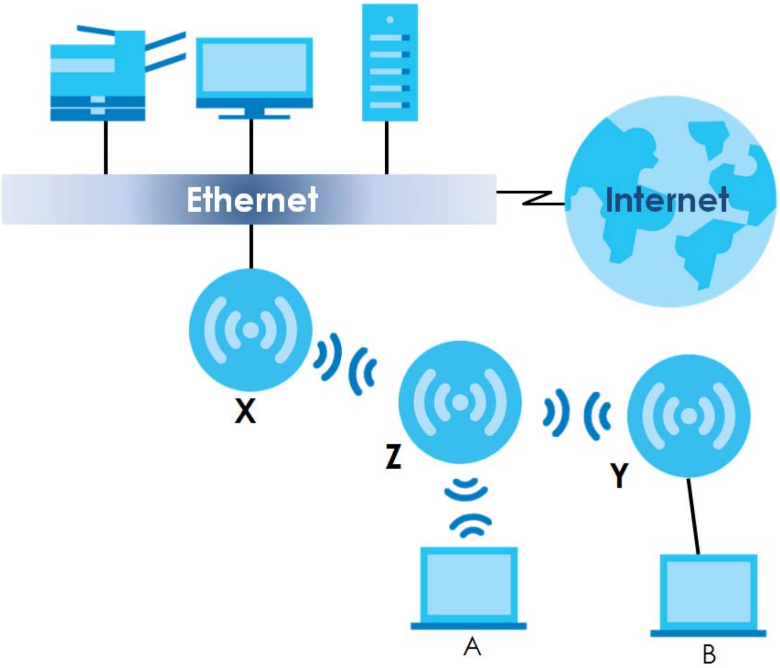
Unless specified, the term "security settings" refers to the traffic between the WiFi clients and the AP. At the time of writing, repeater security is compatible with the Zyxel Device only.

WiFi Repeater

The Zyxel Device can establish a WiFi connection with other APs (in either **Root AP** or **Repeater** mode) to form a WDS.

Using **Repeater** mode, your Zyxel Device can extend the range of the WLAN. In the figure below, the Zyxel Device in Repeater mode (**Z**) has a WiFi connection to the Zyxel Device in **Root AP** mode (**X**) which is connected to a wired network and also has a WiFi connection to another Zyxel Device in **Repeater** mode (**Y**) at the same time. **Z** acts as a repeater that forwards traffic between associated WiFi clients and the wired LAN. **Y** acts as a WiFi bridge (repeater with WDS wireless bridging enabled) that forwards traffic between wired clients and the wired LAN. Clients **A** and **B** access the AP and the wired network behind the AP through repeaters **Z** and **Y**.

Figure 5 Repeater Application



When the Zyxel Device is in **Repeater** mode, repeater security between the Zyxel Device and other repeater is independent of the security between the WiFi clients and the AP or repeater. When repeater security is enabled, both APs and repeaters must use the same pre-shared key. See Section 11.2 on page 116 and Section 15.2 on page 187 for more details.

For NCC managed devices, you only need to enable **AP Smart Mesh** to automatically create WiFi links between APs. See the NCC User's Guide for more details.

1.3.1 Radio Frequency (RF) Monitor

The Zyxel Device supports **Rogue AP Detection** (see Section 11.3 on page 122). **Rogue AP Detection** allows the Zyxel Device to be set to work as an RF monitor to discover nearby Access Points. The information it obtains from other APs is used to tag possible rogue APs and friendly APs. The Zyxel Device can still work as an AP while it scans the environment for wireless signals.

1.4 Sample Feature Applications

This section describes some possible scenarios and topologies that you can set up using your Zyxel Device.

1.4.1 MBSSID

A Basic Service Set (BSS) is the set of devices forming a single WiFi network (usually an access point and one or more WiFi clients). The Service Set IDentifier (SSID) is the name of a BSS. In Multiple BSS (MBSSID) mode, the Zyxel Device provides multiple virtual APs, each forming its own BSS and using its own individual SSID profile.

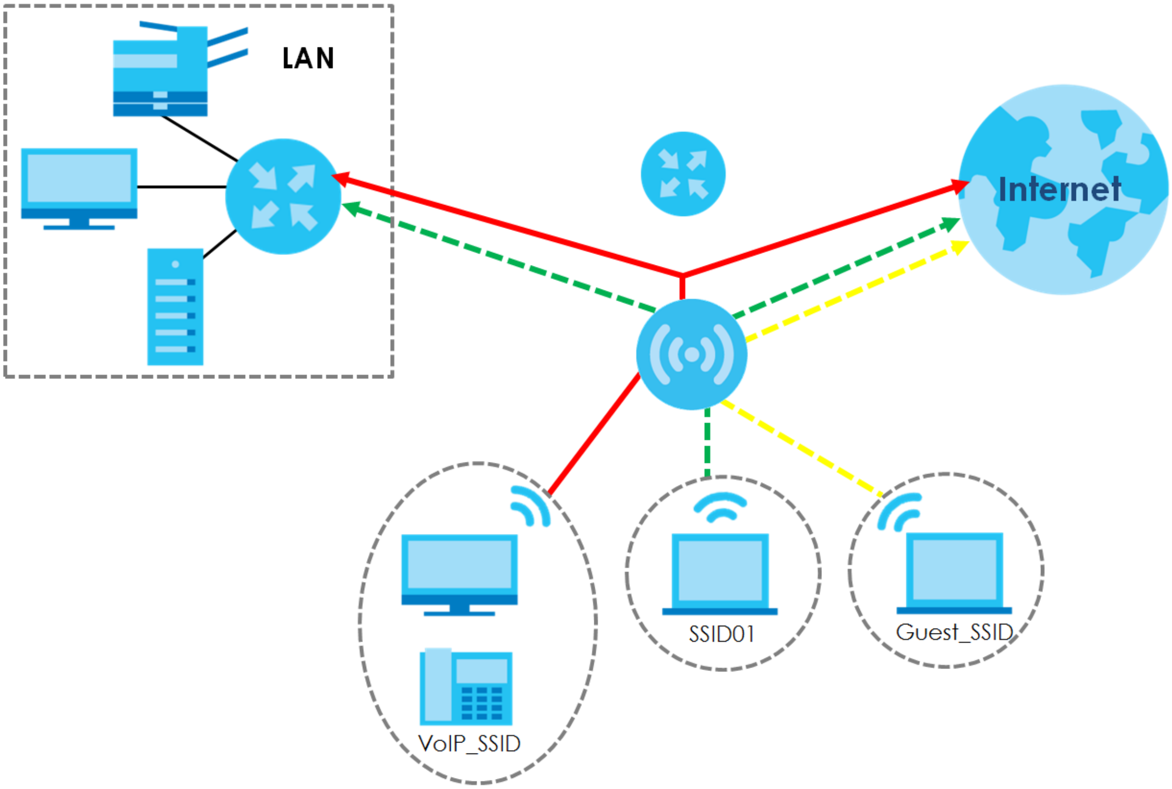
You can configure multiple SSID profiles, and have all of them active at any one time.

You can assign different wireless and security settings to each SSID profile. This allows you to compartmentalize groups of users, set varying access privileges, and prioritize network traffic to and from certain BSSs.

To the WiFi clients in the network, each SSID appears to be a different access point. As in any WiFi network, clients can associate only with the SSIDs for which they have the correct security settings.

For example, you might want to set up a WiFi network in your office where Internet telephony (VoIP) users have priority. You also want a regular WiFi network for standard users, as well as a ‘guest’ WiFi network for visitors. In the following figure, **VoIP_SSID** users have QoS priority, **SSID01** is the WiFi network for standard users, and **Guest_SSID** is the WiFi network for guest users. In this example, the guest user is forbidden access to the wired Local Area Network (LAN) behind the AP and can access only the Internet.

Figure 6 Multiple BSSs



1.4.2 Dual-Radio/Triple-Radio and BandFlex

The Zyxel Device models are equipped with two or even three WiFi radios. The Zyxel Device uses the WiFi radios to transmit WiFi signals. This means you can configure different WiFi networks on the 2.4G/5G/6G bands to operate simultaneously.

BandFlex allows you to select the frequency bands operating on the radios by configuration. A frequency band is a range of frequency divided into channels which carry the WiFi signals for data transmission. If your Zyxel Device supports BandFlex, you can configure the second radio on the Zyxel Device to use the 5 GHz or 6 GHz bands, while the first radio is always set to use the 2.4 GHz band. The 6 GHz band provides less coverage but has the highest amount of channels among the three frequency bands. Use the 6 GHz band for the most congestion-free transmission if your client devices supports WiFi 6E (see Section 14.1.2 on page 141).

Note: Due to each country's regulations on frequency band usage, the available radio bands (2.4 GHz, 5 GHz, and 6 GHz) may differ by countries or markets the Zyxel Device products are sold to.

Note: A different channel should be configured for each WLAN interface to reduce the effects of radio interference.

You could use the 2.4 GHz band for regular Internet surfing and downloading while using the 5 GHz or 6 GHz band for time sensitive traffic like high-definition video, music, and gaming.

See Section 1.2 on page 14 for the supported number of radios, frequency bands, and see if your Zyxel Device supports BandFlex.

Figure 7 Dual-Radio Application

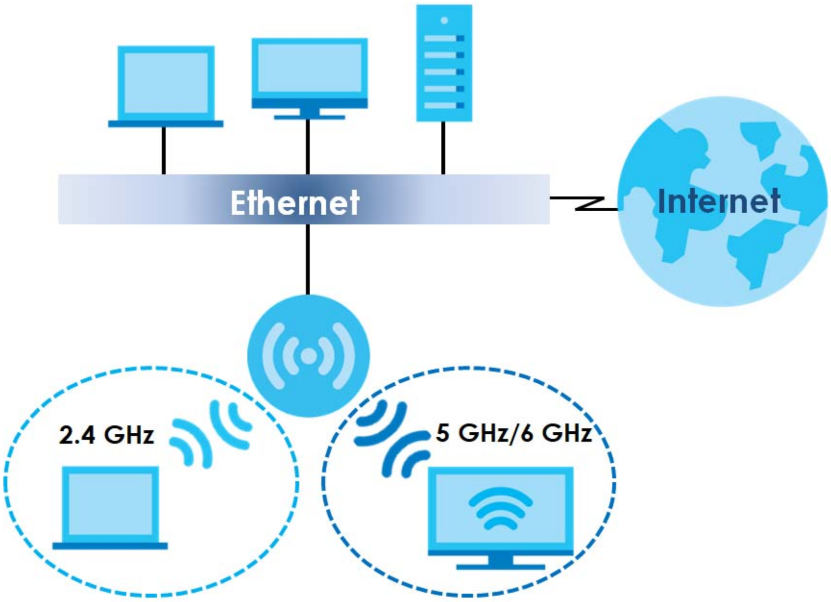
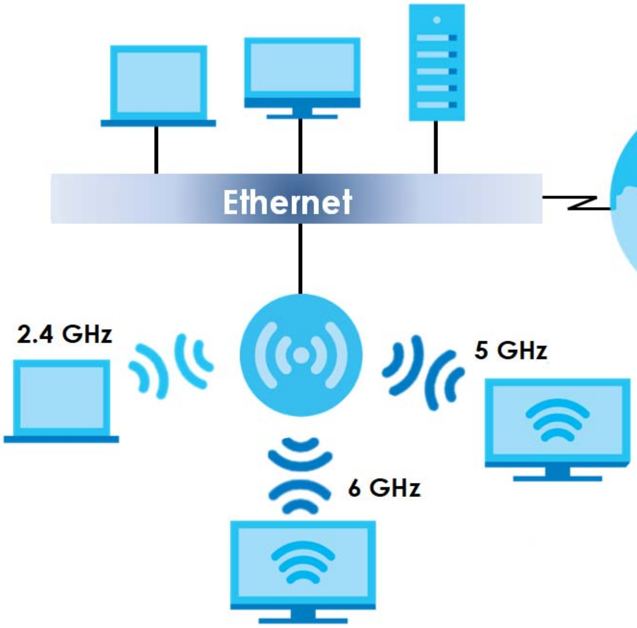


Figure 8 Triple-Radio Application



CHAPTER 2
AP Management

2.1 Management Mode

The Zyxel Device is a unified AP and can be managed by the NCC or an AP controller (AC), or work as a standalone device. We recommend you use NCC to manage multiple APs (see the NCC User's Guide). An AP Controller, such as the ZyWALL ATP/VPN, USG FLEX, or NXC, can only manage multiple APs in the same location.

Note: Not all models can be managed by NCC or an AC. See Section 1.2 on page 14 to check whether your product supports these.

The following table shows the default IP addresses and firmware upload methods for different management modes.

Table 7 Zyxel Device Management Mode Comparison

MANAGEMENT MODE	DEFAULT IP ADDRESS	UPLOAD FIRMWARE THROUGH
Nebula Control Center	Dynamic	NCC Portal
AP Controller	Dynamic	AP Controller using CAPWAP
Standalone	Dynamic or Static (192.168.1.2)	Built-in Web Configurator

When the Zyxel Device is in standalone mode and connects to a DHCP server, it uses the IP address assigned by the DHCP server. Otherwise, the Zyxel Device uses the default static management IP address (192.168.1.2). You can use the **NCC Discovery** or **AC Discovery** screen to allow the Zyxel Device to be managed by the NCC or an AC, respectively.

When the Zyxel Device is managed by the NCC or an AC, it acts as a DHCP client and obtains an IP address from the NCC/AC. It can be configured ONLY by the NCC/AC. To change the Zyxel Device back to standalone mode, use the **Reset** button to restore the default configuration. Alternatively, you need to check the NCC/AC for the Zyxel Device's IP address and use FTP to upload the default configuration file at conf/system-default.conf to the Zyxel Device and reboot the device.

2.1.1 Standalone

When working in standalone mode, the Zyxel Device is configured mainly with its built-in Web Configurator. You can only connect to and set up one Zyxel Device at a time in this mode.

See Chapter 5 on page 61 for detailed information about the standalone Web Configurator screens.

2.1.2 Nebula Control Center

In this mode, which is also called cloud mode, you can manage and monitor the Zyxel Device through the Zyxel Nebula cloud-based network management system. This means you can manage devices remotely without the need of connecting to each device directly. It offers many features to better manage and monitor not just the Zyxel Device, but your network as a whole, including supported switches and gateways. Your network can also be managed through your smartphone using the Nebula Mobile app. See Chapter 24 on page 264 for an example NCC managed network topology.

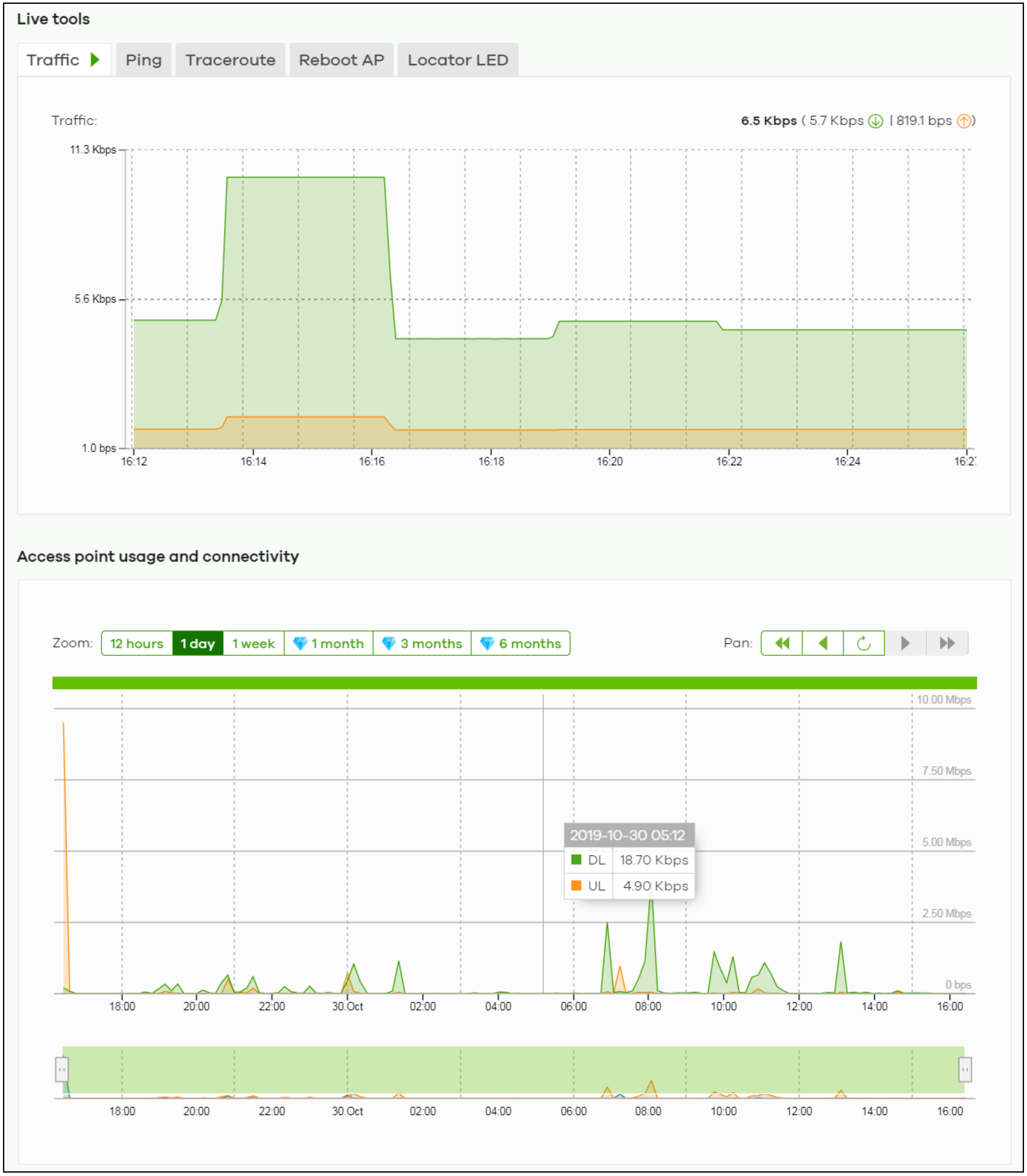
NCC allows different levels of management. You can configure each device on its own or configure a set of devices together as a site. You can also monitor groups of sites called organizations, as shown below.

Table 8 NCC Management Levels

Organization			
Site A		Site B	
Device A-1	Device A-2	Device B-1	Device B-2

It graphically presents your device/network statistics and shows an overview of your network topology, as shown in the following figure. It also sends reports, alerts, and notifications for events, such as when a site goes offline.

Figure 9 Traffic Monitoring Graph From NCC



See the NCC (Nebula Control Center) User's Guide for how to configure Nebula managed devices. See Chapter 25 on page 267 if you want to change the Zyxel Device's VLAN setting or manually set its IP address.

Note: Make sure your network firewall allows TCP ports 443, 4335, and 6667 as well as UDP port 123 so the device can connect to and sync with the NCC.

2.1.3 AP Controller (AC)

If the Zyxel Device supports management using an AC (see Section 10.1.1 on page 102) such as the ZyWALL ATP, ZyWALL VPN, USG FLEX, and the NXC series, and you have this AC in the same subnet, it will be managed by the controller automatically. To set the Zyxel Device to be managed by an AC in a different subnet or change between management modes, use the **AC Discovery** screen (see Section 10.5 on page 112 and Section 10.1.1 on page 102). You can use the AC to manage multiple Zyxel Devices. See Section 10.1.1 on page 102 for an example AC managed network topology.

Note: If the Zyxel Device is already registered to NCC, the controller will be unable to manage it.

An AC uses Control And Provisioning of Wireless Access Points (CAPWAP, see RFC 5415) to discover and configure multiple managed APs.

2.2 Switching Management Modes

The Zyxel Device is in standalone mode by default, with NCC and/or AC discovery enabled.

Standalone-to-NCC

Register the Zyxel Device at the NCC website and then turn on the Zyxel Device. Make sure that **NCC Discovery** is enabled (see Section 10.6 on page 113). The NCC manages the Zyxel Device automatically when it is discovered. Settings on the Zyxel Device will be overwritten with what you have configured on the NCC website.

Standalone-to-AC

By default, the Zyxel Device must be in the same subnet as the AC. See Section 10.1.1 on page 102 for setting it up in a different subnet. Make sure **AC Discovery** is enabled (see Section 10.5 on page 112). The AC manages the Zyxel Device automatically when it is discovered.

AC-to-NCC

Register the Zyxel Device at the NCC website. Make sure that **NCC Discovery** is enabled on your Zyxel Device (see Section 10.6 on page 113). In the AC Web Configurator, select the Zyxel Device and press the **Nebula** button. The NCC manages the Zyxel Device automatically when it is discovered.

NCC-to-AC

Unregister the Zyxel Device at the NCC portal. By default, the Zyxel Device must be in the same subnet as the AC. See Section 10.1.1 on page 102 for setting it up in a different subnet. Make sure **AC Discovery** is enabled (see Section 10.5 on page 112). The AC manages the Zyxel Device automatically when it is discovered.

NCC-to-Standalone

Back up your configurations first, then unregister the Zyxel Device from the NCC organization/site.

If the Zyxel Device is connected to NCC, the Zyxel Device will automatically reset to factory defaults and return to standalone mode.

If the Zyxel Device is not connected to NCC, press the reset button. The Zyxel Device will reset to factory defaults and return to standalone mode.

AC-to-Standalone

Use the **Reset** button to return the Zyxel Device to its factory default settings (see Section 27.6 on page 287).

2.3 Zyxel One Network (ZON) Utility

ZON Utility is a program designed to help you deploy and manage a network more efficiently. It detects devices automatically and allows you to do basic settings on devices in the network without having to be near it.

The ZON Utility issues requests via Zyxel Discovery Protocol (ZDP) and in response to the query, the device responds back with basic information including IP address, firmware version, location, system and model name in the same broadcast domain. The information is then displayed in the ZON Utility screen and you can perform tasks like basic configuration of the devices and batch firmware upgrade in it. You can download the ZON Utility at www.zyxel.com and install it on your computer (Windows operating system).

2.3.1 Requirements

Before installing the ZON Utility on your computer, please make sure it meets the requirements listed below.

Operating System

At the time of writing, the ZON Utility is compatible with:

- Windows 7 (both 32-bit / 64-bit versions)
- Windows 8 (both 32-bit / 64-bit versions)
- Windows 8.1 (both 32-bit / 64-bit versions)
- Window 10 (both 32-bit / 64-bit versions)
- Window 11 (64-bit version)

Note: To check for your Windows operating system version, right-click on **My Computer > Properties** on your computer. You should see this information in the **General** tab.

Note: It is suggested that you install Npcap, the packet capture library for Windows operating systems, and remove WinPcap or any other installed packet capture tools before you install the ZON utility.

Hardware

Here are the minimum hardware requirements to use the ZON Utility on your computer.

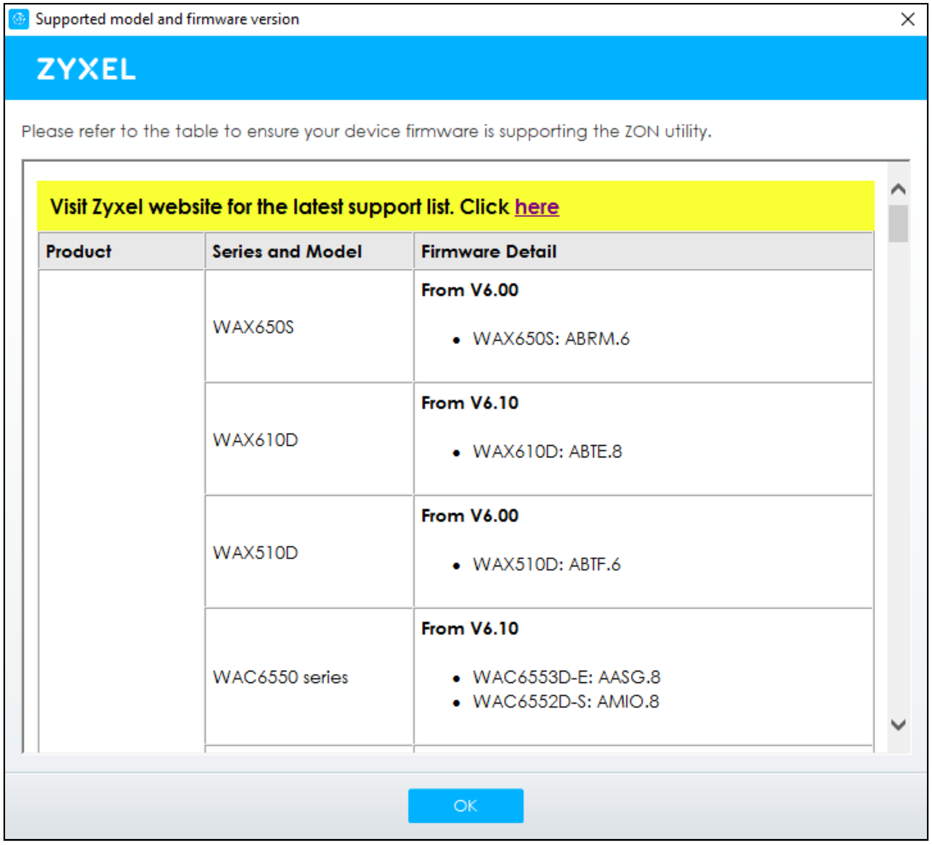
- Core i3 processor
- 2 GB RAM
- 100 MB free hard disk
- WXGA (Wide XGA 1280x800)

2.3.2 Run the ZON Utility

1 Double-click the ZON Utility to run it.

2 The first time you run the ZON Utility, you will see if your device and firmware version support the ZON Utility. Click the **OK** button to close this screen.

Figure 10 Supported Devices and Versions



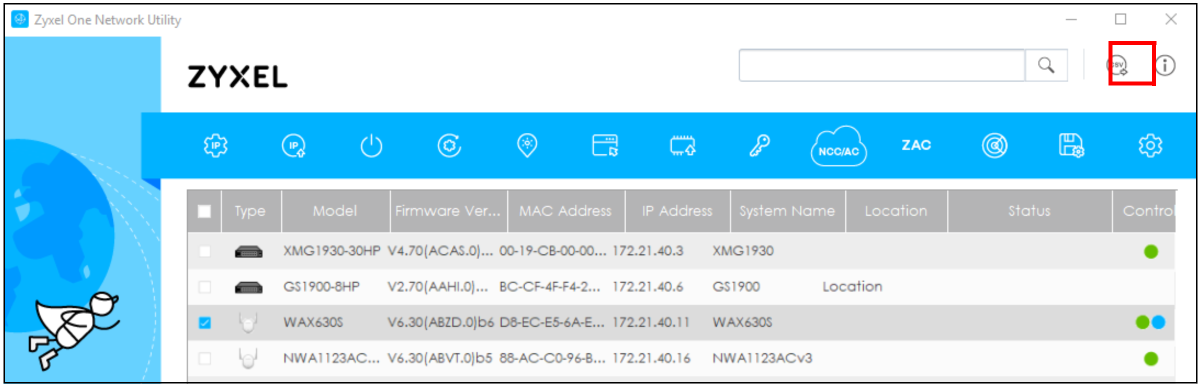
Please refer to the table to ensure your device firmware is supporting the ZON utility.

Visit Zyxel website for the latest support list. Click here

Product	Series and Model	Firmware Detail
	WAX650S	**From V6.00** • WAX650S: ABRM.6
	WAX610D	**From V6.10** • WAX610D: ABTE.8
	WAX510D	**From V6.00** • WAX510D: ABTF.6
	WAC6550 series	**From V6.10** • WAC6553D-E: AASG.8 • WAC6552D-S: AMIO.8

If you want to check the supported models and firmware versions later, you can click the **Show information about ZON** icon in the upper right hand corner of the screen. Then select the **Supported model and firmware version** link. If your device is not listed here, see the device release notes for ZON Utility support. The release notes are in the firmware zip file on the Zyxel web site.

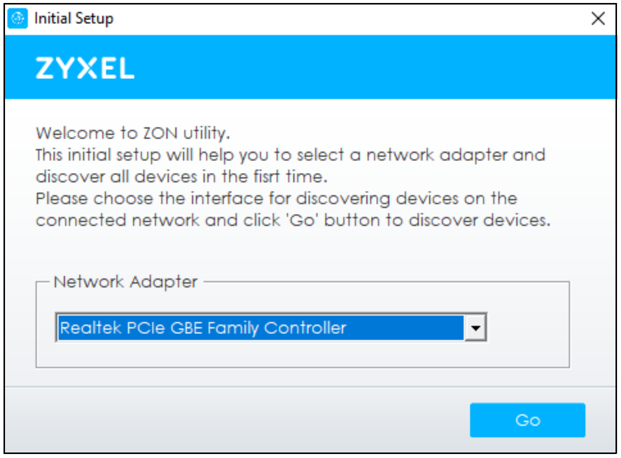
Figure 11 ZON Utility Screen



☐	Type	Model	Firmware Ver...	MAC Address	IP Address	System Name	Location	Status	Contro
☐		XMG1930-30HP	V4.70(ACAS.0)...	00-19-CB-00-00...	172.21.40.3	XMG1930			●
☐		GS1900-8HP	V2.70(AAHI.0)...	BC-CF-4F-F4-2...	172.21.40.6	GS1900	Location		
☑		WAX630S	V6.30(ABZD.0)b6	D8-EC-E5-6A-E...	172.21.40.11	WAX630S			●●
☐		NWA1123AC...	V6.30(ABVT.0)b5	88-AC-C0-96-B...	172.21.40.16	NWA1123ACv3			●

3 Select a network adapter to which your supported devices are connected.

Figure 12 Network Adapter

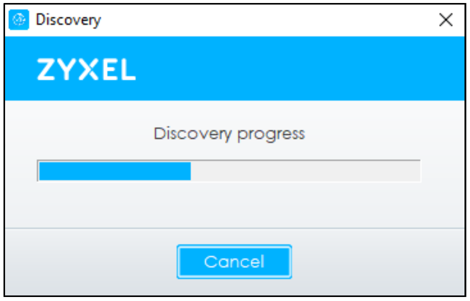


Welcome to ZON utility.
This initial setup will help you to select a network adapter and discover all devices in the fisrt time.
Please choose the interface for discovering devices on the connected network and click 'Go' button to discover devices.

Network Adapter: Realtek PCIe GBE Family Controller

4 Click the **Go** button for the ZON Utility to discover all supported devices in your network.

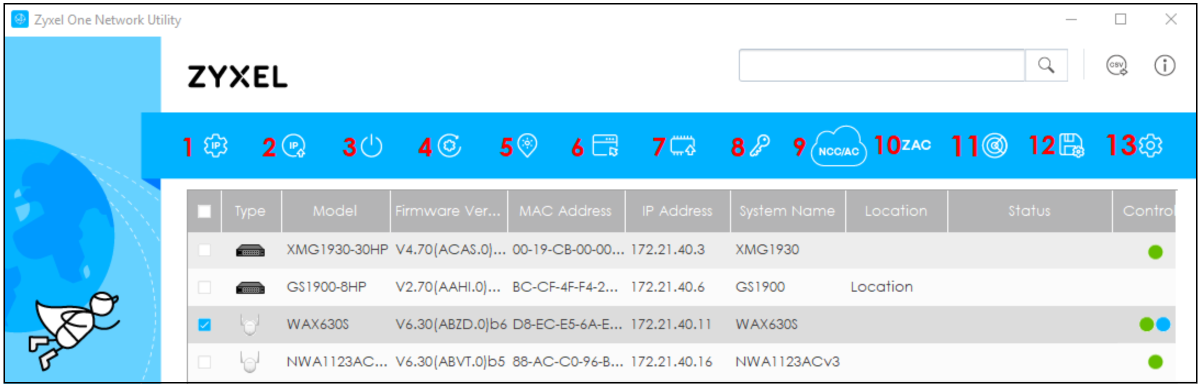
Figure 13 Discovery



Discovery progress

5 The ZON Utility screen shows the devices discovered.

Figure 14 ZON Utility Screen

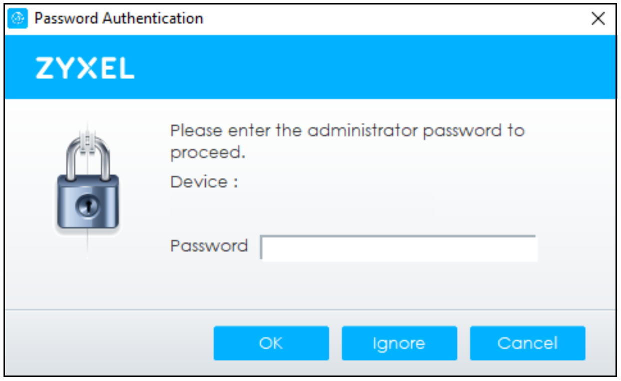


☐	Type	Model	Firmware Ver...	MAC Address	IP Address	System Name	Location	Status	Control
☐		XMG1930-30HP	V4.70(ACAS.0)...	00-19-CB-00-00...	172.21.40.3	XMG1930			●
☐		GS1900-8HP	V2.70(AAHI.0)...	BC-CF-4F-F4-2...	172.21.40.6	GS1900	Location		
☑		WAX630S	V6.30(ABZD.0)b6	D8-EC-E5-6A-E...	172.21.40.11	WAX630S			●●
☐		NWA1123AC...	V6.30(ABVT.0)b5	88-AC-C0-96-B...	172.21.40.16	NWA1123ACv3			●

6 Select a device and then use the icons to perform actions. Some functions may not be available for your devices.

Note: You must know the selected device admin password before taking actions on the device using the ZON Utility icons. If the selected device is being managed or has been managed by the NCC, check **Local credentials** in the NCC's **Site-wide > Configure > Site settings** screen for the selected device's current password.

Figure 15 Password Prompt



Password Authentication

Please enter the administrator password to proceed.

Device :

Password

The following table describes the icons numbered from left to right in the ZON Utility screen.

Table 9 ZON Utility Icons

ICON	DESCRIPTION
1 IP Configuration	Change the selected device's IP address.
2 Renew IP Address	Update a DHCP-assigned dynamic IP address.
3 Reboot Device	Use this icon to restart the selected device(s). This may be useful when troubleshooting or upgrading new firmware.
4 Reset Configuration to Default	Use this icon to reload the factory-default configuration file. This means that you will lose all previous configurations.
5 Locator LED	Use this icon to locate the selected device by causing its **Locator** LED to blink.
6 Web GUI	Use this to access the selected device Web Configurator from your browser. You will need a username and password to log in.

Table 9 ZON Utility Icons (continued)

ICON	DESCRIPTION
7 Firmware Upgrade	Use this icon to upgrade new firmware to selected device(s) of the same model. Make sure you have downloaded the firmware from the Zyxel website to your computer and unzipped it in advance. The ZON only supports a standalone mode AP for the firmware upgrade, it does not support to upgrade the firmware for a managed mode AP.
8 Change Password	Use this icon to change the admin password of the selected device. You must know the current admin password before changing to a new one.
9 Configure Controller Discovery and NCC Discovery	The option is available if the selected device supports AP controller discovery or Nebula Control Center (NCC) discovery. You must have Internet access to use this feature. Use this icon on the selected device to enable or disable the: • AP controller discovery feature • Nebula Control Center (NCC) discovery feature If the feature is enabled, the selected device will try to connect to the AP controller/ NCC. If the selected device has successfully connected to an AP controller, it will change to the AP controller managed mode. If the selected device has successfully connected to the NCC and is registered on the NCC, it will change to the Nebula cloud mode.
10 ZAC	Use this icon to run the Zyxel AP Configurator of the selected AP.
11 Clear and Rescan	Use this icon to clear the list and discover all devices on the connected network again.
12 Save Configuration	Use this icon to save configuration changes to permanent memory on a selected device.
13 Settings	Use this icon to select a network adapter for the computer on which the ZON utility is installed, and the utility language.

The following table describes the fields in the ZON Utility main screen.

Table 10 ZON Utility Fields

LABEL	DESCRIPTION
Type	This field displays an icon of the kind of device discovered.
Model	This field displays the model name of the discovered device.
Firmware Version	This field displays the firmware version of the discovered device.
MAC Address	This field displays the MAC address of the discovered device.
IP Address	This field displays the IP address of an internal interface on the discovered device that first received an ZDP discovery request from the ZON utility.
System Name	This field displays the system name of the discovered device.
Location	This field displays where the discovered device is.
Status	This field displays whether changes to the discovered device have been done successfully. As the Zyxel Device does not support **IP Configuration**, **Renew IP address** and **Flash Locator LED**, this field displays “Update failed”, “Not support Renew IP address” and “Not support Flash Locator LED” respectively.
Controller Discovery	This field displays if the discovered device supports the: • AP controller discovery feature. • Nebula Control Center (NCC) discovery feature. If the feature is enabled, the selected device will try to connect to the AP controller/ NCC. If the selected device has successfully connected to an AP controller, it will change to the AP controller managed mode. If the selected device has successfully connected to the NCC and is registered on the NCC, it will change to the Nebula cloud mode.
Serial Number	Enter the admin password of the discovered device to display its serial number.

Table 10 ZON Utility Fields (continued)

LABEL	DESCRIPTION
Hardware Version	This field displays the hardware version of the discovered device.
IPv6 Address	This field displays the IPv6 address of an internal interface on the discovered device that first received an ZDP discovery request from the ZON utility.

2.4 Ways to Access the Zyxel Device

You can use the following ways to configure the Zyxel Device.

Web Configurator

The Web Configurator allows easy Zyxel Device setup and management using an Internet browser. If your Zyxel Device is managed by the NCC or an AC, use this only for troubleshooting if you cannot connect to the Internet. This User's Guide provides information about the Web Configurator.

NCC

This is the primary means by which you manage the Zyxel Device in cloud (NCC) mode. With the NCC, you can remotely manage and monitor the Zyxel Device through a cloud-based network management system. See the NCC User's Guide for more information.

AP Controller (AC)

An AP controller lets you configure multiple APs through a single device. See the ZyWALL ATP, ZyWALL VPN, USG FLEX, or NXC Series User's Guide for more information.

ZON Utility

Zyxel One Network (ZON) Utility is a utility tool that assists you to set up and maintain network devices in a simple and efficient way. You can download the ZON Utility at *www.zyxel.com* and install it on your computer (Windows operating system). For more information on ZON Utility see Section 2.3 on page 33.

Command-Line Interface (CLI)

The CLI allows you to use text-based commands to configure the Zyxel Device. You can access it using remote management (SSH) or via the console port. See the Command Reference Guide for more information.

File Transfer Protocol (FTP)

This protocol can be used for firmware upgrades and configuration backup and restore.

Simple Network Management Protocol (SNMP)

The Zyxel Device can be monitored by an SNMP manager. See the SNMP chapter in this User's Guide.

2.5 Good Habits for Managing the Zyxel Device

Do the following things regularly to make the Zyxel Device more secure and to manage it more effectively.

- Change the password often. Use a password that is not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the Zyxel Device becomes unstable or even crashes. If you forget your password, you will have to reset the Zyxel Device to its factory default settings. If you backed up an earlier configuration file, you will not have to totally re-configure the Zyxel Device; you can simply restore your last configuration.

CHAPTER 3 Hardware

See the Quick Start Guide for hardware installation and connections.

3.1 Grounding (WAC6552D-S, WAC6553D-E and WAX655E)

Earth grounding helps protect against lightning and interference.

Note: The power installation must be performed by qualified service personnel and should conform to the National Electrical Code.

The Zyxel Device must be connected to earth ground to adequately ground the Zyxel Device and protect the operator from electrical hazards.

Qualified service personnel must confirm that the protective earthing terminal of the building is a valid terminal.

Before connecting the ground, ensure that a qualified service personnel has attached an appropriate ground lug to the ground cable.

1 Remove one of the ground screws from the Zyxel Device's rear panel.

2 Secure a green/yellow ground cable (18 AWG or smaller) to the Zyxel Device's rear panel using the ground screw.

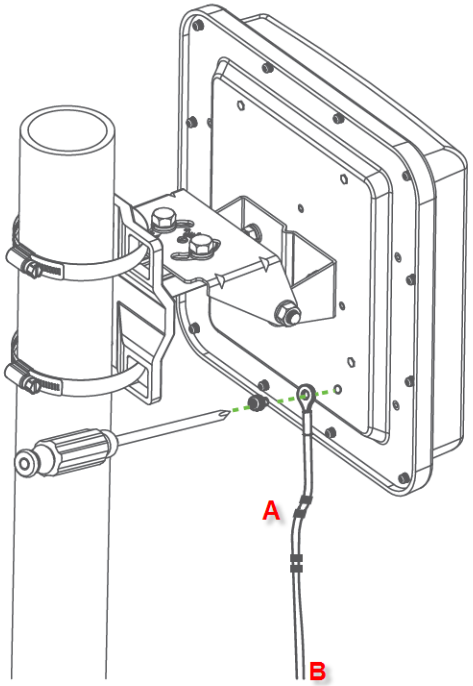
3 Attach the other end of the cable to the ground, either to the same ground electrode as the pole you installed the Zyxel Device on or to the main grounding electrode of the building.

Note: Follow your country's regulations and safety instructions to electrically ground the Zyxel Device properly. If you are uncertain that suitable grounding is available, contact the appropriate electrical inspection authority or an electrician.

Warning! Connect the ground cable before you connect any other cables or wiring.

The figure below illustrates how the ground cable (**A**) is attached to the Zyxel Device and goes to the earth ground (**B**).

Figure 16 Grounding Example



3.2 Zyxel Device Models With Single LEDs

The LEDs of some Zyxel Device models can be controlled by using the suppression feature such that the LEDs stay lit (ON) or OFF after the Zyxel Device is ready. Some Zyxel Device models also have Locator LED which allows you to see the actual location of the Zyxel Device among several devices in the network. See Section 1.2 on page 14 to check which models support these features. Refer to Section 21.1 on page 256 for the LED **Suppression** and **Locator** menus in standalone mode.

3.3 Zyxel Device LED

The LED of the Zyxel Device can be controlled by using the suppression feature such that the LED stays lit (ON) or OFF after the Zyxel Device is ready. Refer to Section 21.1 on page 256 for the LED **Suppression** and **Locator** menus in standalone mode.

Figure 17 WAC500, NWA1123Acv3, NWA110AX, NWA210AX, WAX510D, WAX610D, WAX630S and WAX650S LED

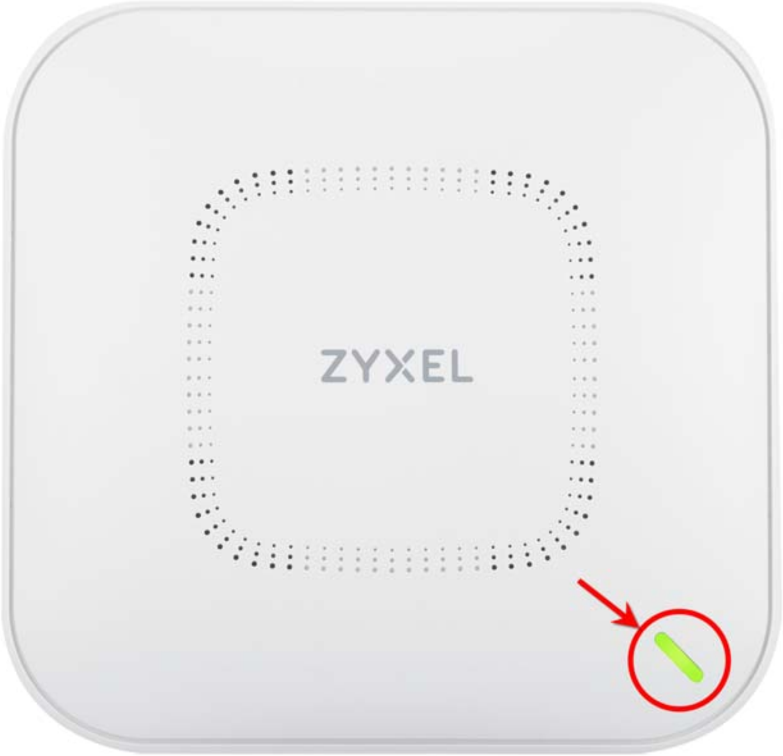


Figure 18 WAC500H / WAX300H LED

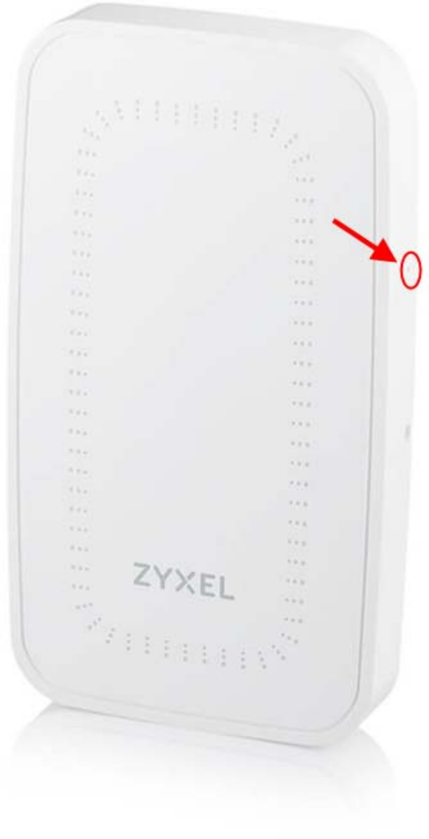


Figure 19 NWA220AX-6E, WAX620D-6E LED

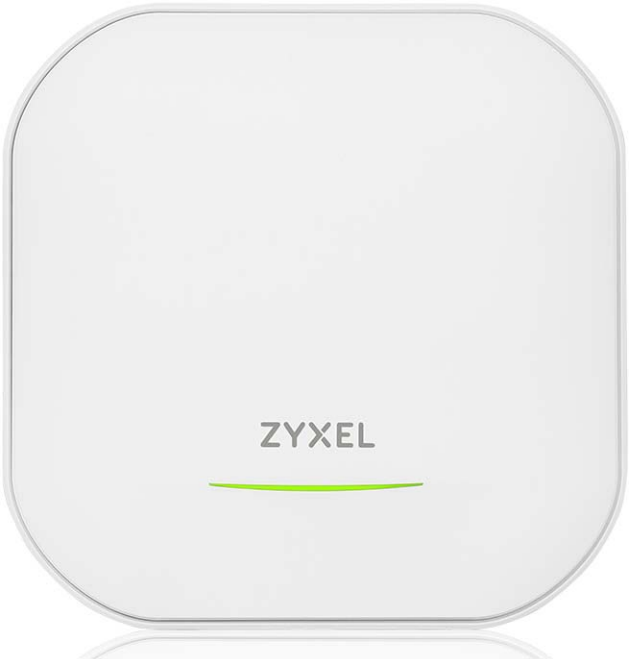


Figure 20 WAX640S-6E, WBE660S LED

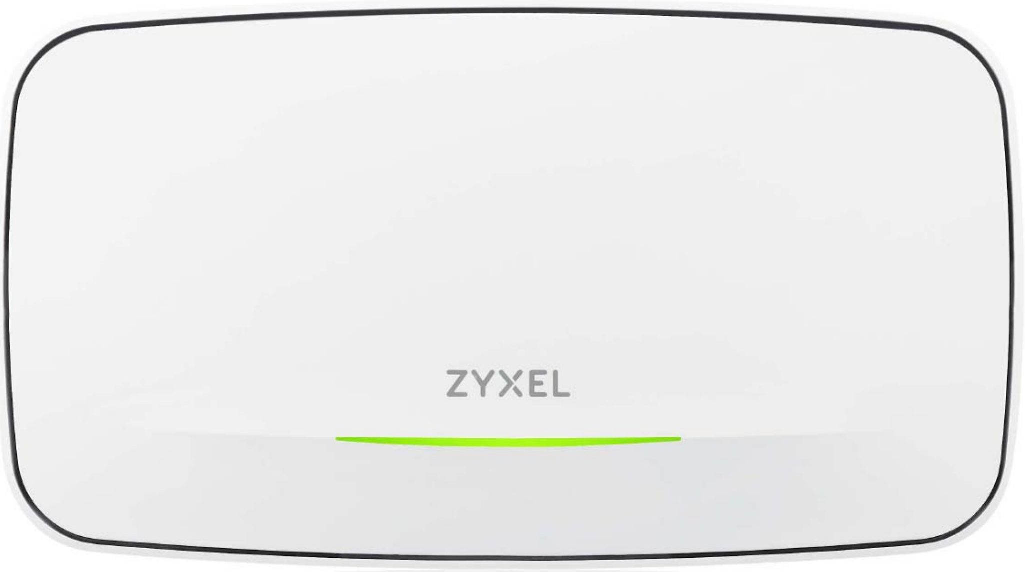
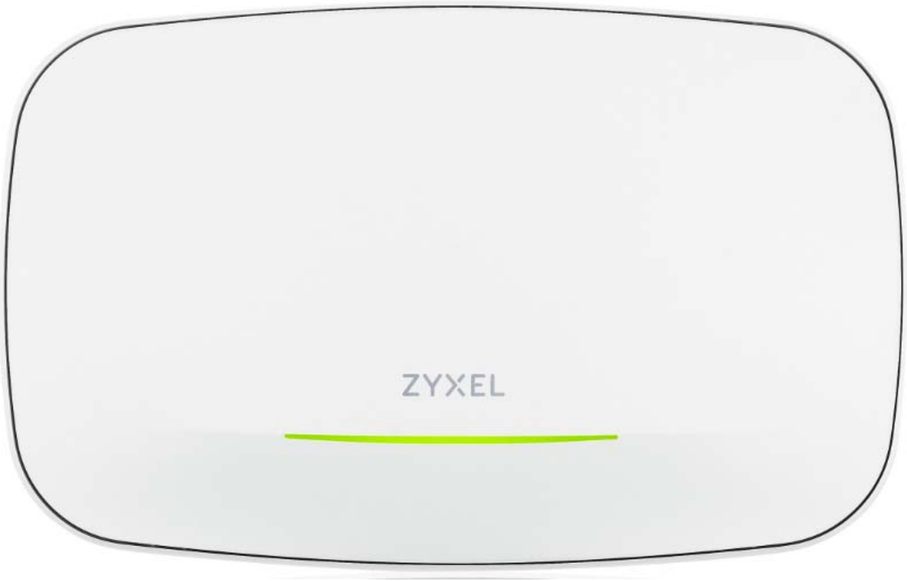


Figure 21 NWA130BE / WBE530 LED



The following are the LED descriptions for your Zyxel Device.

Table 11 Zyxel Device LED

COLOR		STATUS	DESCRIPTION
🟨 ↕ 🟩	Amber	Blinks between amber and green alternately (300 milliseconds interval).	The Zyxel Device is booting up.
	Green		
🟨 ↕ 🟩	Amber	Blinks between amber and green alternately (1 second interval).	The Zyxel Device is discovering the NCC.
	Green		

Table 11 Zyxel Device LED (continued)

COLOR		STATUS	DESCRIPTION
🟨 ↕ 🟩	Amber Green	Blinks between amber and green alternately 3 times and then turns solid green for 3 seconds.	The Zyxel Device is discovering an AC, or is managed by NCC but fails to connect with NCC, and is reconnecting with the NCC.
🟨 ↕ 🟩	Amber Green	Blinks between amber and green alternately 2 times and then turns solid green for 3 seconds.	The Zyxel Device is managed by an AC but the uplink is disconnected.
🟩	Green	Slow Blinking (On for 1 second, Off for 1 second)	The wireless module of the Zyxel Device is disabled or fails, the Zyxel Device is using default WiFi settings, or the Zyxel Device is configured to be managed by NCC but is not yet registered with the NCC. Note: WiFi networks on the WAX650S, NWA220AX-6E and WAX620D-6E are turned off automatically when it is connected to a device that supplies power using IEEE 802.3af PoE.
🟩	Green	Steady On	The Zyxel Device is ready for use, the Zyxel Device's wireless interface is activated, and/or WiFi clients are connected to the Zyxel Device in full power mode (see Table 21 on page 63).
🟨	Amber	Steady On	The Zyxel Device is ready for use in limited power mode (see Table 21 on page 63), the Zyxel Device's wireless interface is activated, and/or WiFi clients are connected to the Zyxel Device. Note: WiFi networks on the WAX650S, NWA220AX-6E, WAX620D-6E and WAX640S-6E are turned off automatically when it is connected to a device that supplies power using IEEE 802.3af PoE. Not all models support limited power mode. See Section 1.2 on page 14 for models that only support one PoE standard.
🟦	Bright Blue	Steady On	The Zyxel Device's wireless interface is activated, but there are no WiFi clients connected when it is in full power mode (see Table 21 on page 63).
⬜	White	Slow Blinking (On for 100ms per second)	Locator LED is on. It switches off automatically after the configured amount of time (1-60 min). Default duration is 10 minutes. Note: The color of the white LED may have slight differences (for example, very light purple) on different models.
🟦	Blue	Slow Blinking (Blink for 1 time, Off for 1 second)	The Zyxel Device is performing a Channel Availability Check (CAC) with Dynamic Frequency Selection (DFS) to monitor a channel for radar signals.
🟥	Red	On	The Zyxel Device failed to boot up or is experiencing system failure.
🟥		Fast Blinking (On for 50 milliseconds, Off for 50 milliseconds)	The Zyxel Device is undergoing firmware upgrade.
🟥		Slow Blinking (Blink for 3 times, Off for 3 seconds)	The uplink of the Zyxel Device is disconnected.

3.4 Ports

The following shows the Zyxel Device panels with connection ports.

Figure 22 NWA1123Acv3, WAC500 Ports

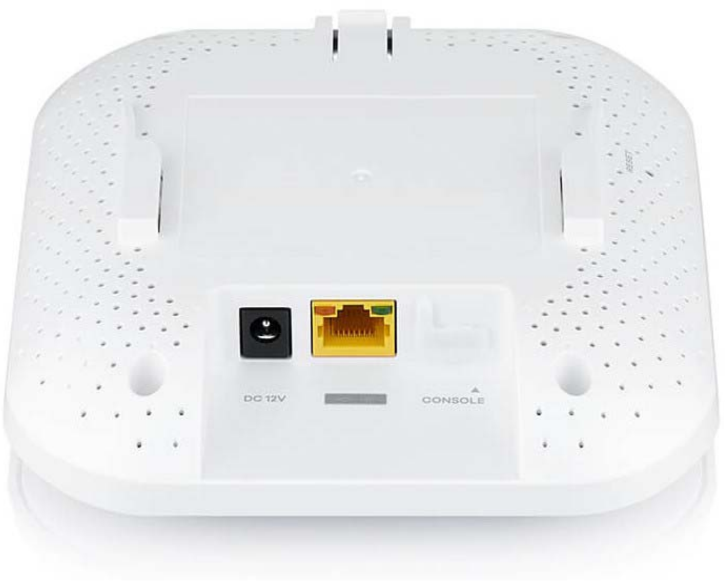


Figure 23 NWA210AX, NWA220AX-6E, WAX610D, WAX620D-6E, WAX630S, WAX650S Ports

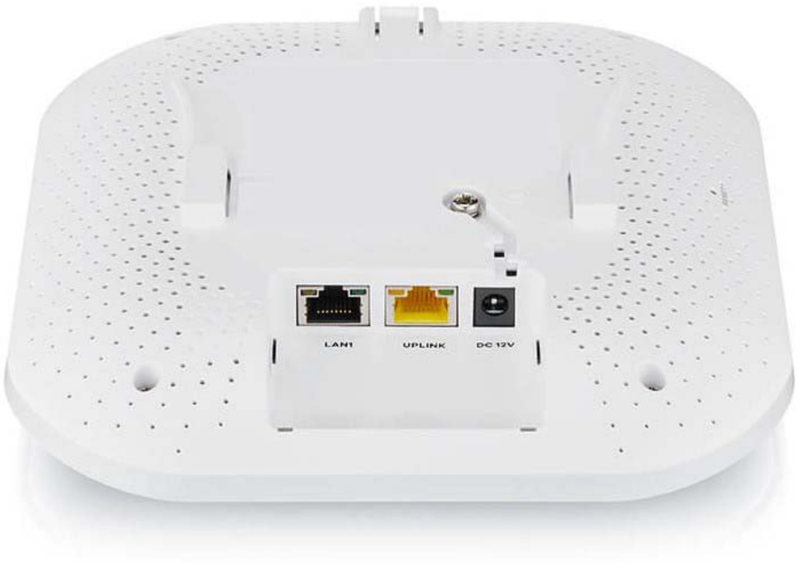


Figure 24 NWA110AX, WAX510D Ports

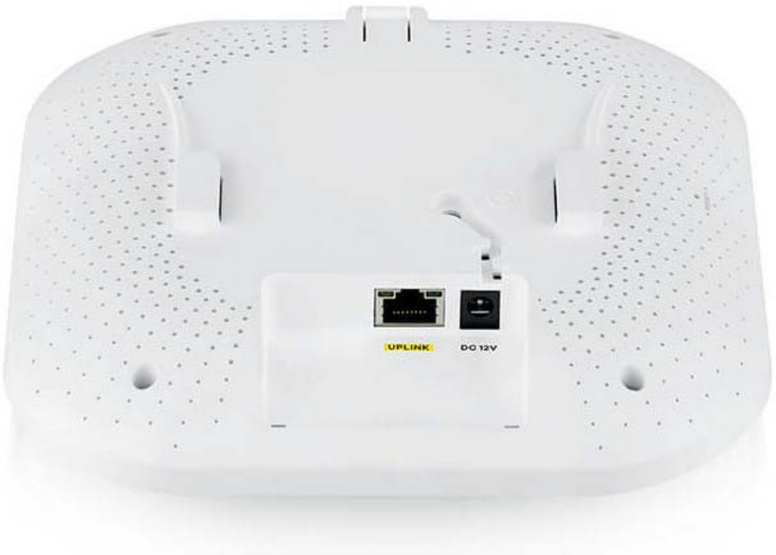


Figure 25 WAX640S-6E Ports

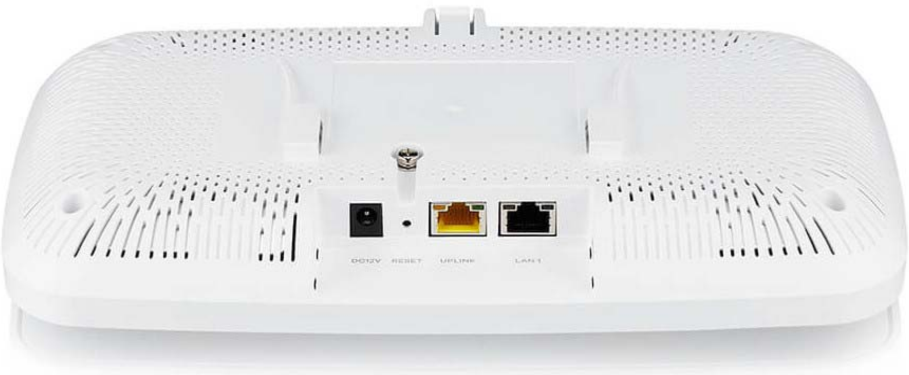


Figure 26 WBE660S Ports

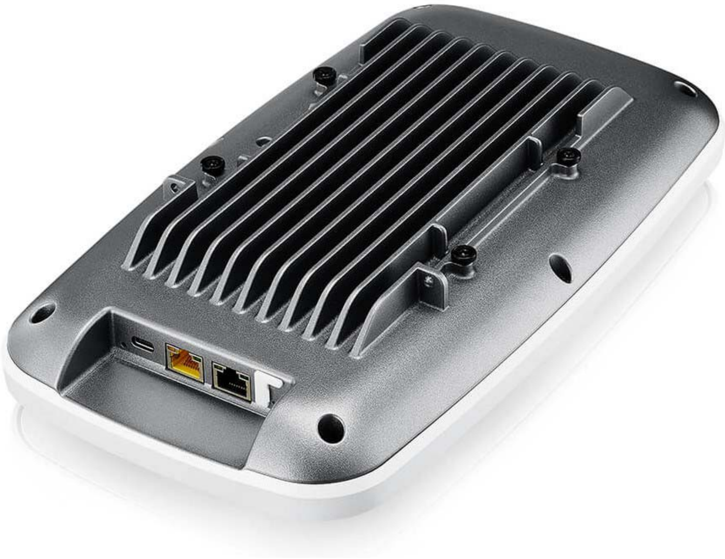


Figure 27 WAC500H, WAX300H Ports

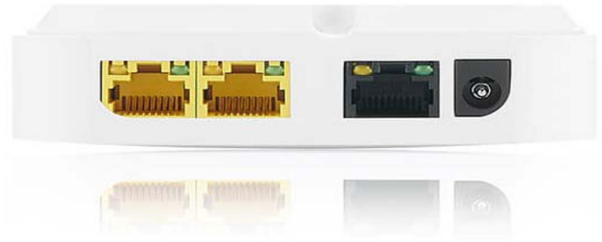
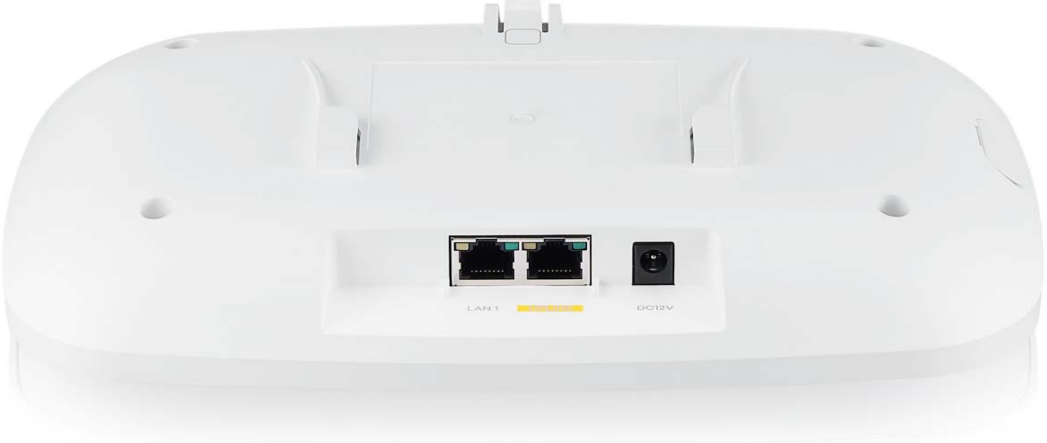


Figure 28 NWA130BE, WBE530 Ports



The following are the items on the ports panels for your Zyxel Device.

Table 12 Ports and Buttons

LABEL	DESCRIPTION
UPLINK	Connect the port to a router, a switch, or another access point (AP) to connect the Zyxel Device to the backbone of your network.
LAN	Connect computers or other Ethernet devices to Ethernet ports for Internet access.
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
RESET	Press the button for more than 5 seconds to return the Zyxel Device to the factory defaults.
POWER	Connect the power adapter and press the **ON/OFF** button to start the device

CHAPTER 4
Web Configurator

4.1 Overview

The Web Configurator is an HTML-based management interface that allows easy system setup and management through Internet browser. Use a browser that supports HTML5, such Mozilla Firefox, or Google Chrome, Microsoft Edge. The recommended screen resolution is 1024 by 768 pixels.

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

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

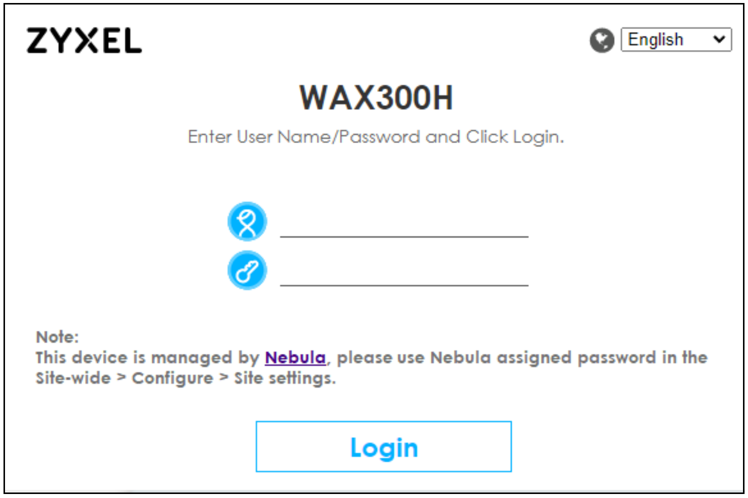
4.2 Accessing the Web Configurator

1 Make sure your Zyxel Device hardware is properly connected, and your computer is connected to the Zyxel Device through wired of WiFi connection. See the Quick Start Guide.

2 If the Zyxel Device and your computer are not connected to a DHCP server, make sure your computer's IP address is in the range between "192.168.1.3" and "192.168.1.254".

3 Browse to the Zyxel Device's DHCP-assigned IP address or http://192.168.1.2. The **Login** screen appears. If you are in cloud mode, check the NCC's **Site-wide > Devices > Access points** screen for the Zyxel Device's LAN IP address.

Figure 29 Login Page: Cloud mode



WAX300H

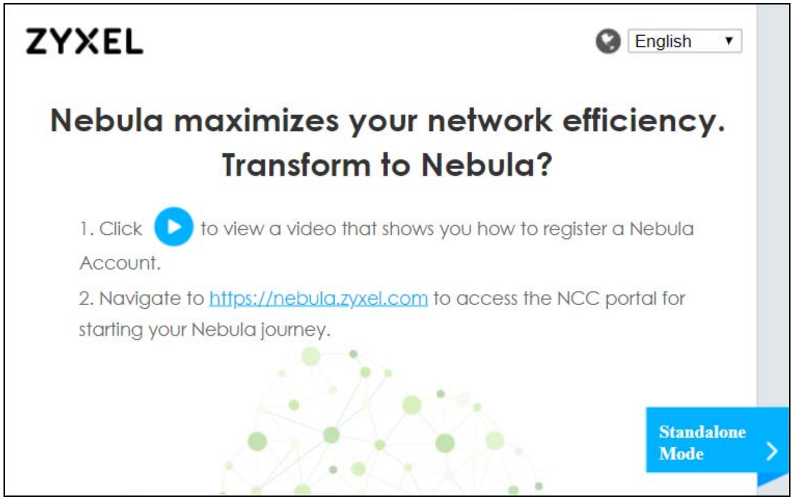
Enter User Name/Password and Click Login.

Note:
This device is managed by Nebula, please use Nebula assigned password in the Site-wide > Configure > Site settings.

If a Zyxel Device is in standalone mode and supports NCC, the following page displays.

Here, you can watch a tutorial for using the Zyxel Nebula Control Center (NCC) or access the link to the NCC, as shown in the following figure. Otherwise, continue with the next step. The NCC is a cloud-based network management system that allows you to remotely manage and monitor the Zyxel Device (see Section 2.1.2 on page 30)

Figure 30 Nebula Intro Page



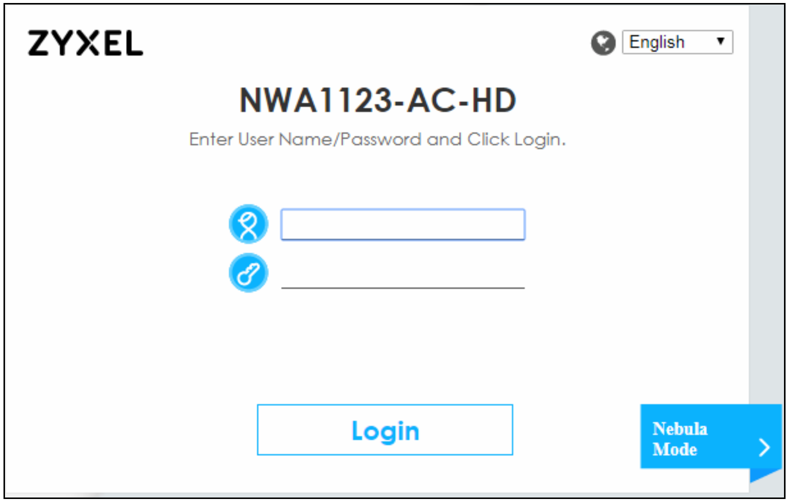
Nebula maximizes your network efficiency. Transform to Nebula?

1. Click ▶ to view a video that shows you how to register a Nebula Account.

2. Navigate to https://nebula.zyxel.com to access the NCC portal for starting your Nebula journey.

To go to the login page, click **Standalone Mode**. Login page displays as shown in the following figure.

Figure 31 Login Page in Standalone Mode



4 Enter the user name (default: “admin”) and password (default: “1234”).

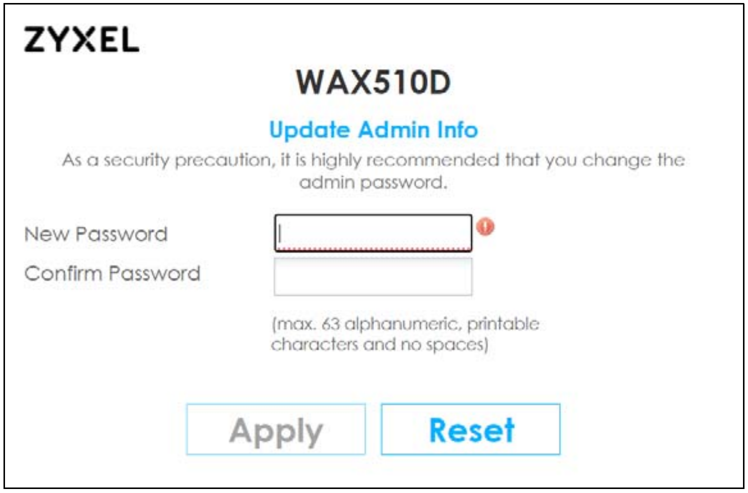
Note: If the Zyxel Device is being managed or has been managed by the NCC, check **Local credentials** in the NCC's **Site-wide > Configure > Site settings** screen for the Zyxel Device's current password.

5 Select the language you prefer for the Web Configurator. Click **Login**.

6 The wizard screen opens when the Zyxel Device is accessed for the first time or when you reset the Zyxel Device to its default factory settings.

7 If you logged in using the default user name and password, the **Update Admin Info** screen appears. Otherwise, the dashboard appears.

Figure 32 Update Admin Info Screen



As a security precaution, it is highly recommended that you change the admin password.

New Password

Confirm Password

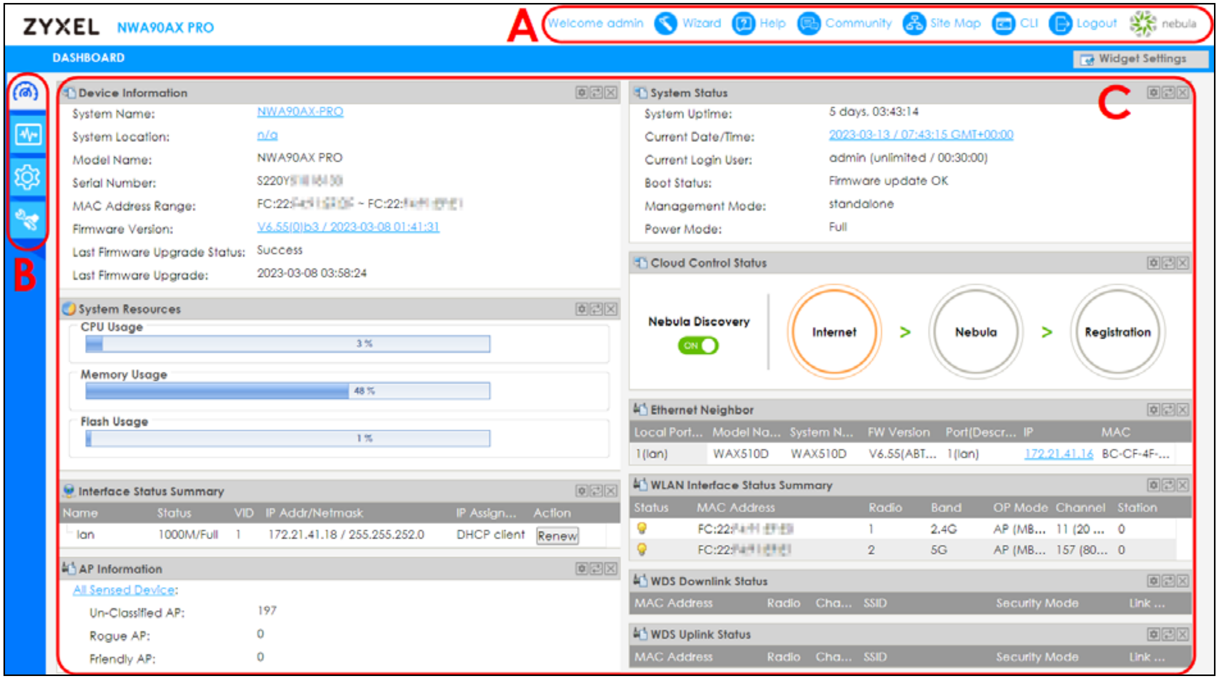
(max. 63 alphanumeric, printable characters and no spaces)

The **Update Admin Info** screen appears every time you log in using the default user name and default password. If you change the password for the default user account, this screen does not appear anymore.

4.3 Navigating the Web Configurator

The following summarizes how to navigate the Web Configurator from the **Dashboard** screen. The following figures show the **Dashboard** screen for standalone mode and for cloud (NCC) mode. The screen is different for standalone mode and cloud (NCC) mode and may vary slightly for different models.

Figure 33 The Web Configurator's Main Screen for Standalone Mode



Device Information

System Name:	NWA90AX-PRO
System Location:	n/a
Model Name:	NWA90AX PRO
Serial Number:	S220Y[redacted]
MAC Address Range:	FC:22:[redacted] ~ FC:22:[redacted]
Firmware Version:	V6.55(0)b3 / 2023-03-08 01:41:31
Last Firmware Upgrade Status:	Success
Last Firmware Upgrade:	2023-03-08 03:58:24

System Resources

CPU Usage 3 %

Memory Usage 48 %

Flash Usage 1 %

Interface Status Summary

Name	Status	VID	IP Addr/Netmask	IP Assign...	Action
lan	1000M/Full	1	172.21.41.18 / 255.255.252.0	DHCP client	Renew

AP Information

All Sensed Device:

Un-Classified AP:	197
Rogue AP:	0
Friendly AP:	0

System Status

System Uptime:	5 days, 03:43:14
Current Date/Time:	2023-03-13 / 07:43:15 GMT+00:00
Current Login User:	admin (unlimited / 00:30:00)
Boot Status:	Firmware update OK
Management Mode:	standalone
Power Mode:	Full

Cloud Control Status

Nebula Discovery ON

Internet > Nebula > Registration

Ethernet Neighbor

Local Port...	Model Na...	System N...	FW Version	Port(Descr...	IP	MAC
1(lan)	WAX510D	WAX510D	V6.55(ABT...	1(lan)	172.21.41.16	BC-CF-4F-...

WLAN Interface Status Summary

Status	MAC Address	Radio	Band	OP Mode	Channel	Station
●	FC:22:[redacted]	1	2.4G	AP (MB...	11 (20 ...	0
●	FC:22:[redacted]	2	5G	AP (MB...	157 (80...	0

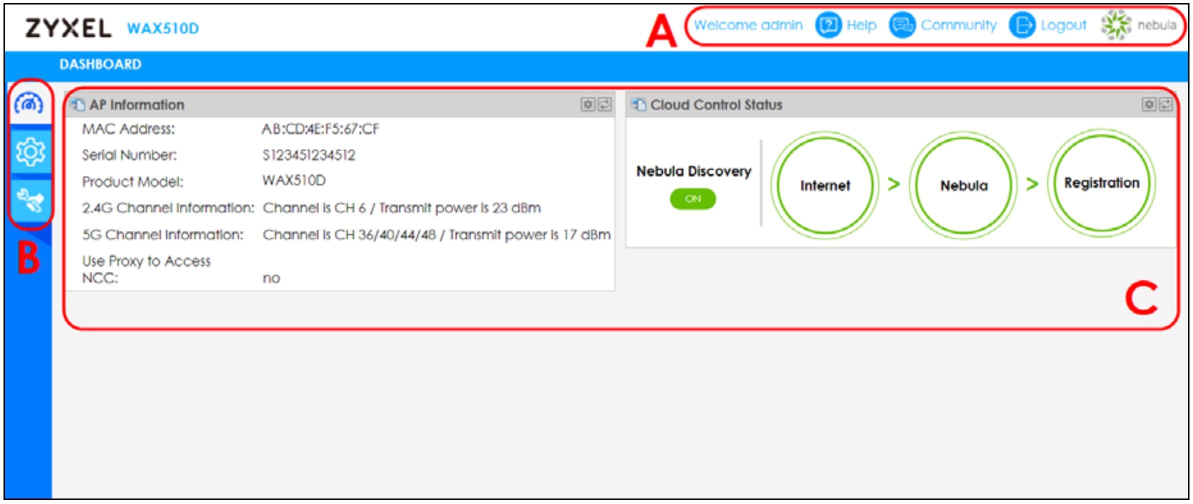
WDS Downlink Status

MAC Address	Radio	Cha...	SSID	Security Mode	Link ...

WDS Uplink Status

MAC Address	Radio	Cha...	SSID	Security Mode	Link ...

Figure 34 The Web Configurator's Main Screen for Cloud Mode



AP Information

MAC Address:	AB:CD:4E:F5:67:CF
Serial Number:	S123451234512
Product Model:	WAX510D
2.4G Channel Information:	Channel is CH 6 / Transmit power is 23 dBm
5G Channel Information:	Channel is CH 36/40/44/48 / Transmit power is 17 dBm
Use Proxy to Access NCC:	no

Cloud Control Status

Nebula Discovery ON

Internet > Nebula > Registration

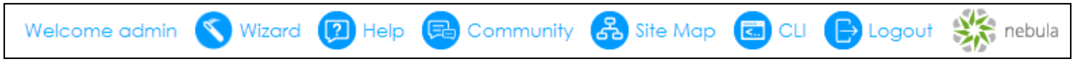
The Web Configurator's main screen is divided into these parts:

- **A** - Title Bar
- **B** - Navigation Panel
- **C** - Main Window

4.3.1 Title Bar

The title bar provides some useful links that always appear over the screens below, regardless of how deep into the Web Configurator you navigate. If your Zyxel Device is in NCC mode, not all icons will be available in the Title Bar.

Figure 35 Title Bar



The icons provide the following functions.

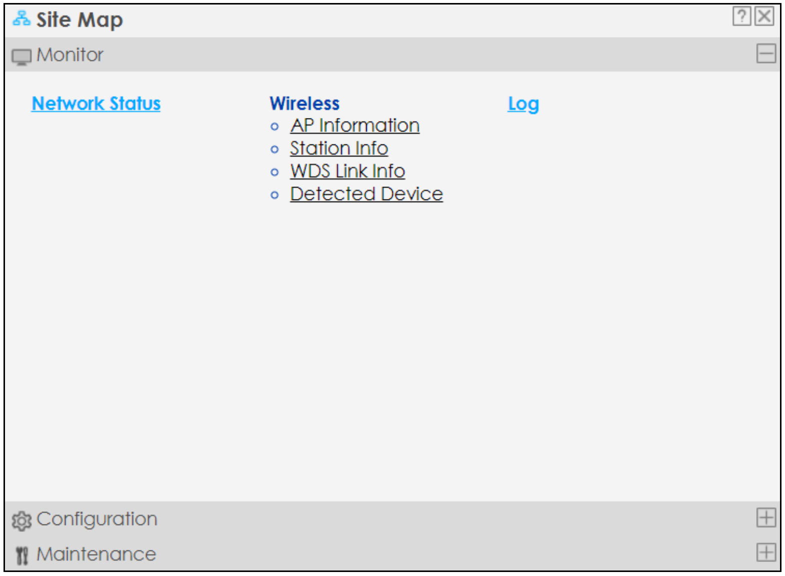
Table 13 Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
Wizard	Click this to open the wizard. See Section 7.1 on page 69 for more information.
Help	Click this to open the help page for the current screen.
Community	Click this to log into the Zyxel forum to post questions, contribute to a discussion and get feedback on Zyxel Device.
Site Map	Click this to see an overview of links to the Web Configurator screens.
CLI	Click this to open a popup window that displays the CLI commands sent by the Web Configurator.
Logout	Click this to log out of the Web Configurator.
nebula	Click this to open the NCC web site login page in a new tab or window.

Site Map

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

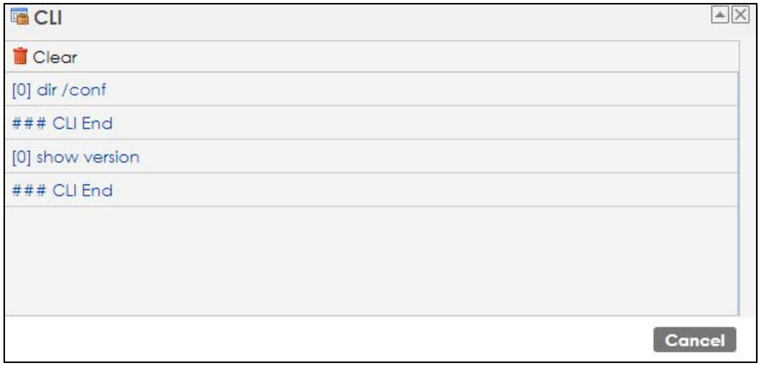
Figure 36 Site Map



CLI Messages

Click **CLI** to look at the CLI commands sent by the Web Configurator. These commands appear in a popup window, such as the following.

Figure 37 CLI Messages



```
[0] dir /conf
### CLI End
[0] show version
### CLI End
```

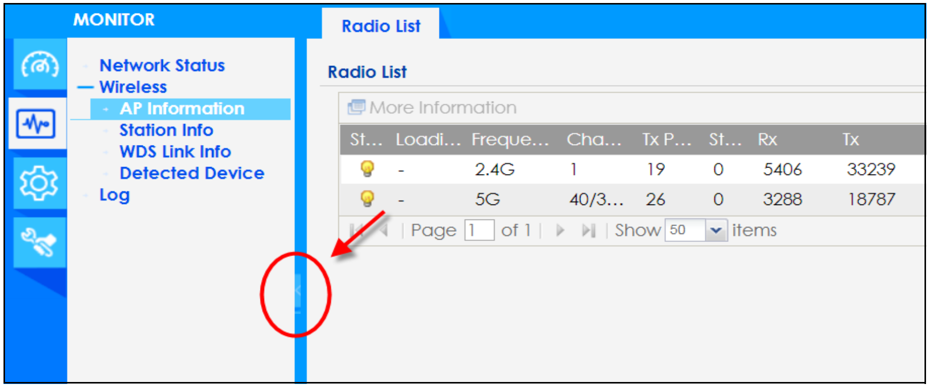
Click **Clear** to remove the currently displayed information.

Note: See the Command Reference Guide for information about the commands.

4.3.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure Zyxel Device features. Click the arrow in the middle of the right edge of the navigation panel to hide the navigation panel menus or drag it to resize them. The following sections introduce the Zyxel Device's navigation panel menus and their screens.

Figure 38 Navigation Panel



St...	Loadi...	Freque...	Cha...	Tx P...	St...	Rx	Tx
💡	-	2.4G	1	19	0	5406	33239
💡	-	5G	40/3...	26	0	3288	18787

Page 1 of 1 | Show 50 items

4.3.3 Standalone Mode Navigation Panel Menus

The following are the screens available in standalone mode. Note that some screens may not be available for your Zyxel Device model. See Section 1.2 on page 14 to see which features your Zyxel Device model supports.

Dashboard

The dashboard displays information such as general device information, system status, system resource usage, and interface status in widgets that you can re-arrange to suit your needs.

For details on the Dashboard's features, see Chapter 6 on page 63.

Monitor Menu

The monitor menu screens display status and statistics information.

Table 14 Monitor Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
Network Status	Network Status	Display general LAN interface information and packet statistics.
Wireless		
AP Information	Radio List	Display information about the radios of the connected APs.
Station Info	Station List	Display information about the connected stations.
WDS Link Info	WDS Link Info	Display statistics about the Zyxel Device's WDS (Wireless Distribution System) connections.
Detected Device	Detected Device	Display information about suspected rogue APs.
Log	View Log	Display log entries for the Zyxel Device.

Configuration Menu

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

Table 15 Configuration Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
Network	IP Setting	Configure the IP address for the Zyxel Device Ethernet interface.
	VLAN	Manage the Ethernet interface VLAN settings.
	Storm Control	Enable or disable the broadcast/multicast storm control feature.
	AC Discovery	Configure the Zyxel Device's AP Controller settings.
	NCC Discovery	Configure proxy server settings to access the NCC.
Wireless		
AP Management	WLAN Setting	Manage the Zyxel Device's general WiFi settings.
Rogue AP	Rogue/Friendly AP List	Configure how the Zyxel Device monitors for rogue APs.
Load Balancing	Load Balancing	Configure load balancing for traffic moving to and from WiFi clients.
DCS	DCS	Configure dynamic WiFi channel selection.
Bluetooth	Advertising Settings	Configure the beacon ID(s) to be included in the Bluetooth advertising packet.
Object		
User	User	Create and manage users.
	Setting	Manage default settings for all users, general settings for user sessions, and rules to force user authentication.

Table 15 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
AP Profile	Radio	Create and manage WiFi radio settings files that can be associated with different APs.
	SSID	Create and manage WiFi SSID, security, MAC filtering, and layer-2 isolation files that can be associated with different APs.
WDS Profile	WDS	Create and manage WDS profiles that can be used to connect to different APs in WDS.
Certificate	My Certificates	Create and manage th e Zyxel Device's certificates.
	Trusted Certificates	Import and manage certificates from trusted sources.
System		
Host Name	Host Name	Configure the system and domain name for the Zyxel Device.
Power Mode	Power Mode	Configure the Zyxel Device's power settings.
Date/Time	Date/Time	Configure the current date, time, and time zone in the Zyxel Device.
WWW	Service Control	Configure HTTP, HTTPS, and general authentication.
SSH	SSH	Configure SSH server and SSH service settings.
FTP	FTP	Configure FTP server settings.
SNMP	SNMP	Configure SNMP communities and services.
Log & Report		
Email Daily Report	Email Daily Report	Configure where and how to send daily reports and what reports to send.
Log Setting	Log Setting	Configure the system log and remote syslog servers.

Maintenance Menu

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

Table 16 Maintenance Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
File Manager	Configuration File	Manage and upload configuration files for the Zyxel Device.
	Firmware Package	View the current firmware version and to upload firmware.
	Shell Script	Manage and run shell script files for the Zyxel Device.
Diagnostics	Diagnostics	Collect diagnostic information.
	Remote Capture	Capture network traffic going through the Zyxel Device and output the captured packets to an analyzer.
LEDs	Suppression	Enable this feature to keep the LEDs off after the Zyxel Device starts.
	Locator	Enable this feature to see the actual location of the Zyxel Device between several devices in the network.
Antenna	Antenna Switch	Change antenna orientation for the radios.
Reboot	Reboot	Restart the Zyxel Device.

4.3.4 Cloud Mode Navigation Panel Menus

If your Zyxel Device is in cloud (NCC) mode, you only need to use the Web Configurator for troubleshooting if your Zyxel Device cannot connect to the Internet.

Dashboard

The dashboard displays general Zyxel Device information, and AP information in widgets that you can re-arrange to suit your needs.

For details on the Dashboard’s features, see Chapter 24 on page 265.

Configuration Menu

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

Table 17 Configuration Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
Network	IP Setting	Configure the IP address for the Zyxel Device Ethernet interface.
	VLAN	Manage the Ethernet interface VLAN settings.

Maintenance Menu

Use the maintenance menu screens to configure the Zyxel Device’s features.

Table 18 Maintenance Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
Shell Script	Shell Script	Manage and run shell script files for the Zyxel Device.
Diagnostics	Diagnostics	Collect diagnostic information.
	Remote Capture	Capture network traffic going through the Zyxel Device and output the captured packets to an analyzer.
Log	View Log	Displays the log when the Zyxel Device is not connected to the Nebula.

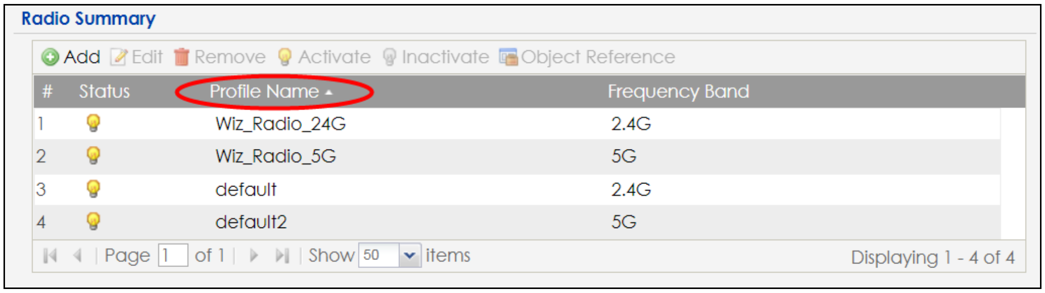
4.3.5 Tables and Lists

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

4.3.5.1 Manipulating Table Display

Here are some of the ways you can manipulate the Web Configurator tables.

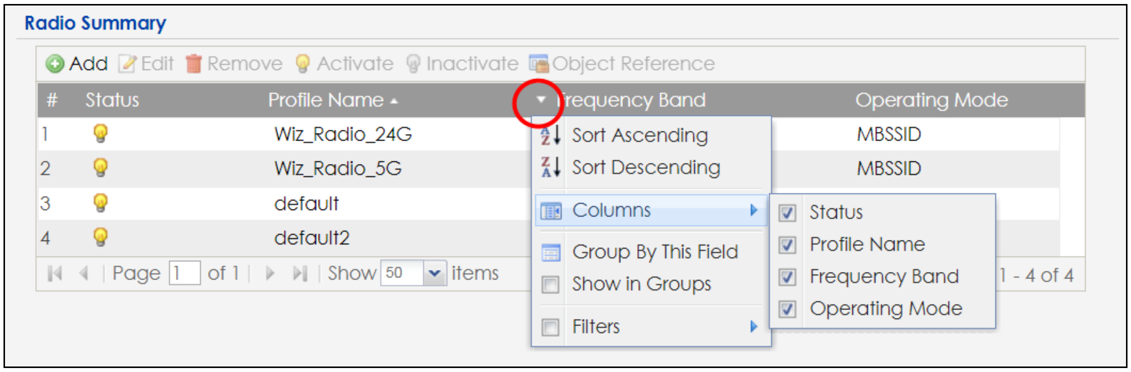
1 Click a column heading to sort the table’s entries according to that column’s criteria.



#	Status	Profile Name ▲	Frequency Band
1	💡	Wiz_Radio_24G	2.4G
2	💡	Wiz_Radio_5G	5G
3	💡	default	2.4G
4	💡	default2	5G

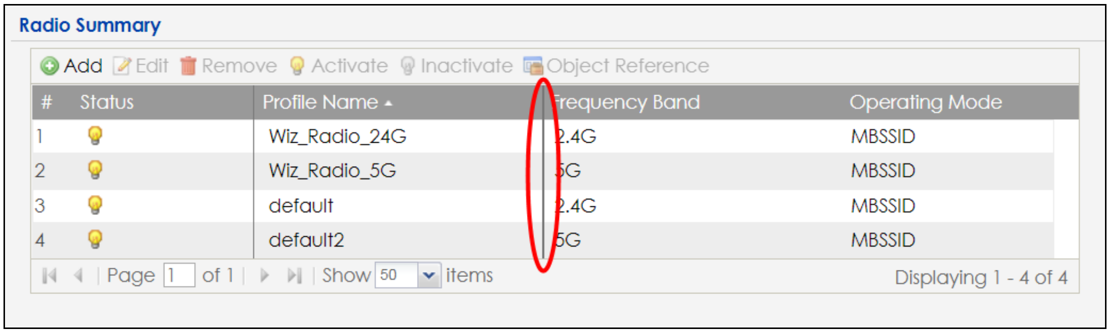
2 Click the down arrow next to a column heading for more options about how to display the entries. The options available vary depending on the type of fields in the column. Here are some examples of what you can do:

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



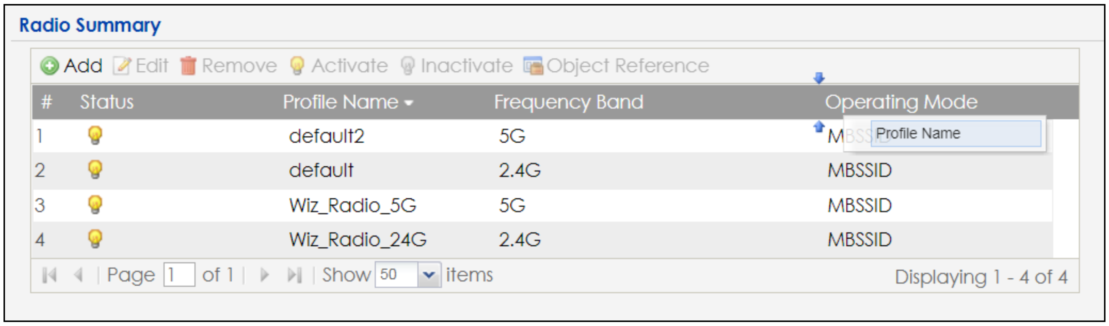
#	Status	Profile Name	Frequency Band	Operating Mode
1		Wiz_Radio_24G		MBSSID
2		Wiz_Radio_5G		MBSSID
3		default		
4		default2		

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



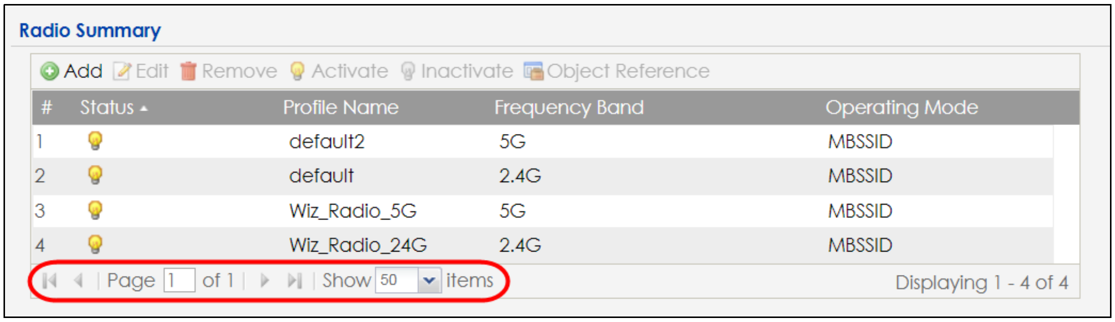
#	Status	Profile Name	Frequency Band	Operating Mode
1		Wiz_Radio_24G	2.4G	MBSSID
2		Wiz_Radio_5G	5G	MBSSID
3		default	2.4G	MBSSID
4		default2	5G	MBSSID

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



#	Status	Profile Name	Frequency Band	Operating Mode
1		default2	5G	M
2		default	2.4G	MBSSID
3		Wiz_Radio_5G	5G	MBSSID
4		Wiz_Radio_24G	2.4G	MBSSID

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



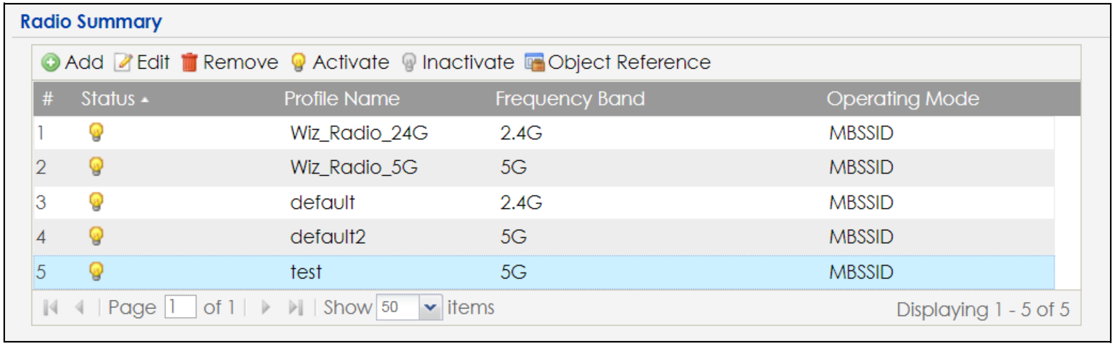
Radio Summary

#	Status ▴	Profile Name	Frequency Band	Operating Mode
1	💡	default2	5G	MBSSID
2	💡	default	2.4G	MBSSID
3	💡	Wiz_Radio_5G	5G	MBSSID
4	💡	Wiz_Radio_24G	2.4G	MBSSID

4.3.5.2 Working with Table Entries

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

Figure 39 Common Table Icons



Radio Summary

#	Status ▴	Profile Name	Frequency Band	Operating Mode
1	💡	Wiz_Radio_24G	2.4G	MBSSID
2	💡	Wiz_Radio_5G	5G	MBSSID
3	💡	default	2.4G	MBSSID
4	💡	default2	5G	MBSSID
5	💡	test	5G	MBSSID

Here are descriptions for the most common table icons.

Table 19 Common Table Icons

LABEL	DESCRIPTION
Add	Click this to create a new entry. For features where the entry's position in the numbered list is important (features where the Zyxel Device applies the table's entries in order like the firewall for example), you can select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings. In some tables you can just click a table entry and edit it directly in the table. For those types of tables small red triangles display for table entries with changes that you have not yet applied.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Object Reference	Select an entry and click **Object Reference** to open a screen that shows which settings use the entry.

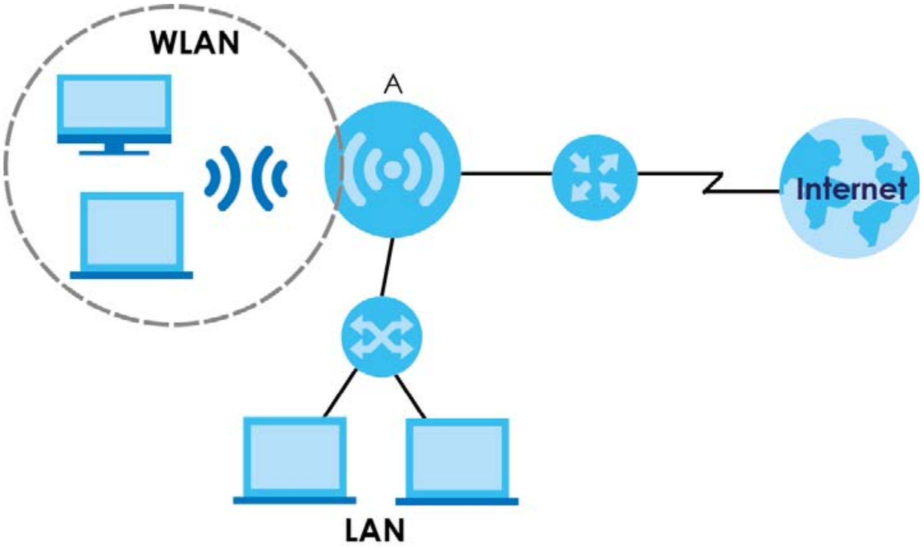
PART I

Standalone Configuration

CHAPTER 5
Standalone Configuration

5.1 Overview

The Zyxel Device is in standalone mode by default. Use the Web Configurator to manage and configure the Zyxel Device directly. As shown in the following figure, WiFi clients can connect to the Zyxel Device (**A**) to access network resources.



5.2 Starting and Stopping the Zyxel Device

Here are some of the ways to start and stop the Zyxel Device.

Table 20 Starting and Stopping the Zyxel Device

METHOD	DESCRIPTION
Turning on the power	A cold start occurs when you turn on the power to the Zyxel Device. The Zyxel Device powers up, checks the hardware, and starts the system processes.
Rebooting the Zyxel Device	A warm start (without powering down and powering up again) occurs when you use the **Reboot** button in the **Reboot** screen or when you use the `reboot` command. The Zyxel Device writes all cached data to the local storage, stops the system processes, and then does a warm start.

Table 20 Starting and Stopping the Zyxel Device (continued)

METHOD	DESCRIPTION
Using the **RESET** button	If you press the **RESET** button on the back of the Zyxel Device, the Zyxel Device sets the configuration to its default values and then reboots. See Section 27.6 on page 287 for more information. Note: Some models do not have a **RESET** button due to feature differences.
Disconnecting the power	Power off occurs when you turn off the power to the Zyxel Device. The Zyxel Device simply turns off. It does not stop the system processes or write cached data to local storage.

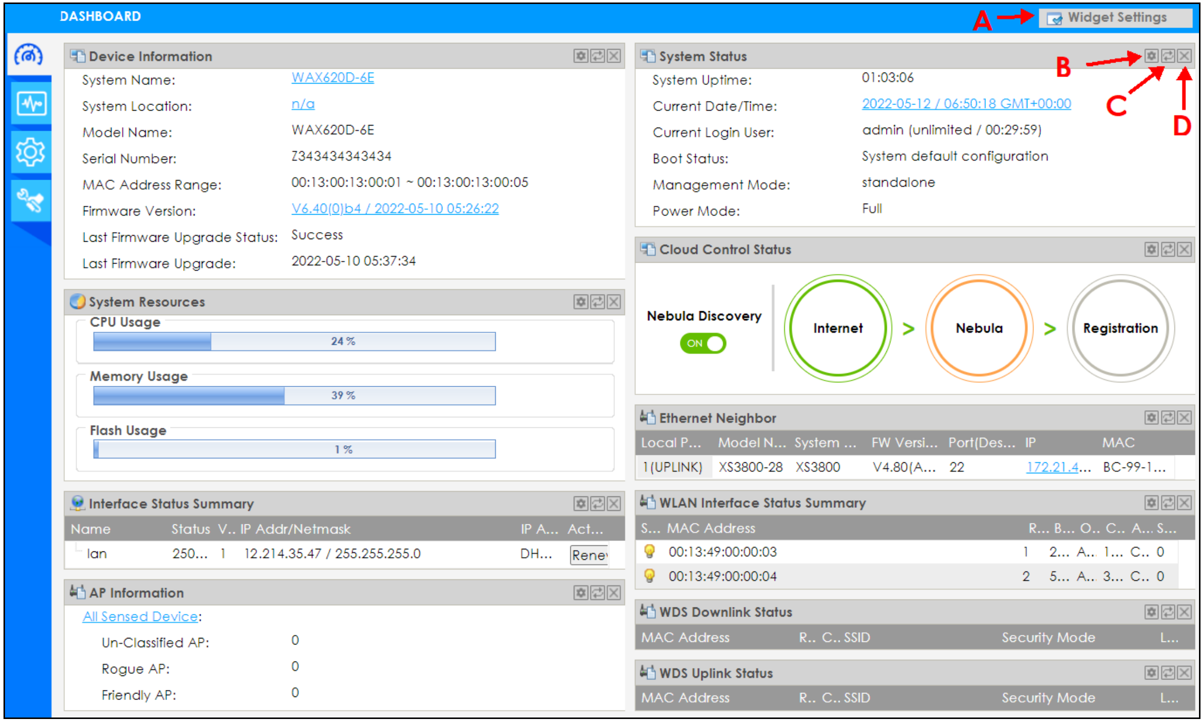
The Zyxel Device does not stop or start the system processes when you apply configuration files or run shell scripts although you may temporarily lose access to network resources.

CHAPTER 6
Dashboard

6.1 Overview

This screen displays general device information, system status, system resource usage, and interface status in widgets that you can re-arrange to suit your needs. You can also collapse, refresh, and close individual widgets. Fields in this screen may slightly differ by models.

Figure 40 Dashboard



Device Information

System Name: WAX620D-6E
System Location: n/a
Model Name: WAX620D-6E
Serial Number: Z343434343434
MAC Address Range: 00:13:00:13:00:01 ~ 00:13:00:13:00:05
Firmware Version: V6.40(0)b4 / 2022-05-10 05:26:22
Last Firmware Upgrade Status: Success
Last Firmware Upgrade: 2022-05-10 05:37:34

System Resources

CPU Usage 24 %
Memory Usage 39 %
Flash Usage 1 %

Interface Status Summary

Name	Status	V..	IP Addr/Netmask	IP A...	Act...
lan	250...	1	12.214.35.47 / 255.255.255.0	DH...	Rene

AP Information

All Sensed Device:
Un-Classified AP: 0
Rogue AP: 0
Friendly AP: 0

System Status

System Uptime: 01:03:06
Current Date/Time: 2022-05-12 / 06:50:18 GMT+00:00
Current Login User: admin (unlimited / 00:29:59)
Boot Status: System default configuration
Management Mode: standalone
Power Mode: Full

Cloud Control Status

Ethernet Neighbor

Local P...	Model N...	System ...	FW Versi...	Port(Des...	IP	MAC
1(UPLINK)	XS3800-28	XS3800	V4.80(A...	22	172.21.4...	BC-99-1...

WLAN Interface Status Summary

S...	MAC Address	R...	B...	O..	C..	A...	S...
💡	00:13:49:00:00:03	1	2...	A...	1...	C..	0
💡	00:13:49:00:00:04	2	5...	A...	3...	C..	0

WDS Downlink Status

MAC Address	R..	C..	SSID	Security Mode	L...

WDS Uplink Status

MAC Address	R..	C..	SSID	Security Mode	L...

The following table describes the labels in this screen.

Table 21 Dashboard

LABEL	DESCRIPTION
Widget Settings (A)	Use this link to re-open closed widgets. Widgets that are already open appear grayed out.
Refresh Time Setting (B)	Set the interval for refreshing the information displayed in the widget.
Refresh Now (C)	Click this to update the widget's information immediately.
Close Widget (D)	Click this to close the widget. Use **Widget Settings** to re-open it.
Device Information	
System Name	This field displays the name used to identify the Zyxel Device on any network. Click the icon to open the screen where you can change it.

Table 21 Dashboard (continued)

LABEL	DESCRIPTION
System Location	This field displays the location of the Zyxel Device. Click the icon to open the screen where you can change it.
Model Name	This field displays the model name of this Zyxel Device.
Serial Number	This field displays the serial number of this Zyxel Device.
MAC Address Range	This field displays the MAC addresses used by the Zyxel Device. Each physical port or WiFi radio has one MAC address. The first MAC address is assigned to the Ethernet LAN port, the second MAC address is assigned to the first radio, and so on.
Firmware Version	This field displays the version number and date of the firmware the Zyxel Device is currently running. Click the icon to open the screen where you can upload firmware.
Last Firmware Upgrade Status	This field displays whether the latest firmware update was successfully completed.
Last Firmware Upgrade	This field displays the date and time when the last firmware update was made.
System Resources	
CPU Usage	This field displays what percentage of the Zyxel Device's processing capability is currently being used. Hover your cursor over this field to display the **Show CPU Usage** icon that takes you to a chart of the Zyxel Device's recent CPU usage.
Memory Usage	This field displays what percentage of the Zyxel Device's RAM is currently being used. Hover your cursor over this field to display the **Show Memory Usage** icon that takes you to a chart of the Zyxel Device's recent memory usage.
Flash Usage	This field displays what percentage of the Zyxel Device's onboard flash memory is currently being used.
Ethernet Neighbor	
Local Port (Description)	This field displays the port of the Zyxel Device, on which the neighboring device is discovered.
Model Name	This field displays the model name of the discovered device.
System Name	This field displays the system name of the discovered device.
FW Version	This field displays the firmware version of the discovered device.
Port (Description)	This field displays the discovered device's port which is connected to the Zyxel Device.
IP	This field displays the IP address of the discovered device. Click the IP address to access and manage the discovered device using its Web Configurator.
MAC	This field displays the MAC address of the discovered device.
WDS (Wireless Distribution System) Uplink/Downlink Status	
MAC Address	This field displays the MAC address of the root AP or repeater to which the Zyxel Device is connected using WDS.
Radio	This field displays the radio number on the root AP or repeater to which the Zyxel Device is connected using WDS.
Channel	This field displays the channel number on the root AP or repeater to which the Zyxel Device is connected using WDS.
SSID	This field displays the name of the WiFi network to which the Zyxel Device is connected using WDS.
Security Mode	This field displays which secure encryption methods is being used by the Zyxel Device to connect to the root AP or repeater using WDS.
Link Status	This field displays the RSSI (Received Signal Strength Indicator) and transmission/reception rate of the wireless connection in WDS.
System Status	
System Uptime	This field displays how long the Zyxel Device has been running since it last restarted or was turned on.

Table 21 Dashboard (continued)

LABEL	DESCRIPTION
Current Date/ Time	This field displays the current date and time in the Zyxel Device. The format is yyyy-mm-dd hh:mm:ss.
Current Login User	This field displays the user name used to log in to the current session, the amount of reauthentication time remaining, and the amount of lease time remaining.
Boot Status	This field displays details about the Zyxel Device's startup state. **OK** - The Zyxel Device started up successfully. **Firmware update OK** - A firmware update was successful. **Problematic configuration after firmware update** - The application of the configuration failed after a firmware upgrade. **System default configuration** - The Zyxel Device successfully applied the system default configuration. This occurs when the Zyxel Device starts for the first time or you intentionally reset the Zyxel Device to the system default settings. **Fallback to lastgood configuration** - The Zyxel Device was unable to apply the startup-config.conf configuration file and fell back to the lastgood.conf configuration file. **Fallback to system default configuration** - The Zyxel Device was unable to apply the lastgood.conf configuration file and fell back to the system default configuration file (system-default.conf). **Booting in progress** - The Zyxel Device is still applying the system configuration.
Management Mode	This shows whether the Zyxel Device is set to work as a stand alone AP.
Power Mode	This displays the Zyxel Device's power status. **Full** - the Zyxel Device receives power using a power adapter and/or through a PoE switch/ injector using IEEE 802.3at PoE plus or IEEE 802.3bt (WAX650S only at the time of writing). **Limited** - the Zyxel Device receives power through a PoE switch/injector using IEEE 802.3af PoE or IEEE 802.3at PoE plus (WAX650S only at the time of writing) even when it is also connected to a power source using a power adapter. When the Zyxel Device is in limited power mode, the Zyxel Device throughput decreases and has just one transmitting radio chain. It always shows **Full** if the Zyxel Device does not support power detection. See Section 1.2 on page 14.
Bluetooth	This field displays the Zyxel Device'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. The Zyxel Device communicates with other BLE enabled devices using advertisements. **Unavailable** displays if the Zyxel Device supports Bluetooth, but there is no BLE USB dongle connected to the USB port of the Zyxel Device. Some Zyxel Devices, such as the WAC5302D-S, need to have a supported BLE USB dongle attached to act as a beacon to broadcast packets. **Available** displays if the Zyxel Device supports Bluetooth and detects a BLE device but advertising is inactive. **Advertising** displays if the Zyxel Device supports Bluetooth, detects a BLE device, and advertising is activated, which means the Zyxel Device can broadcast packets to every BLE device around it. Not all models support BLE, see Section 1.2 on page 14 for the supported model list.

Table 21 Dashboard (continued)

LABEL	DESCRIPTION
Cloud Control Status	This field displays: • The Zyxel Device Internet connection status. • The connection status between the Zyxel Device and NCC. • The Zyxel Device registration status on NCC. Mouse over the circles to display detailed information. To pass your Zyxel Device management to NCC, first make sure your Zyxel Device is connected to the Internet. Then go to NCC and register your Zyxel Device. You can also view this information in **Configuration > Network > NCC Discovery.** **1. Internet** Green - The Zyxel Device is connected to the Internet. Orange - The Zyxel Device is not connected to the Internet. **2. Nebula** Green - The Zyxel Device is connected to NCC. Orange - The Zyxel Device is not connected to NCC. **3. Registration** Green - The Zyxel Device is registered on NCC. Gray - The Zyxel Device is not registered on NCC. Note: All circles will gray out if you disable **Nebula Discovery**.
Nebula Discovery	Slide the switch to the right to enable NCC discovery on the Zyxel Device. The Zyxel Device will connect to NCC and change to the NCC management mode if it: • is connected to the Internet. • has been registered on NCC.
Interface Status Summary	If an Ethernet interface does not have any physical ports associated with it, its entry is displayed in light gray text. Click the **Detail** icon to go to a (more detailed) summary screen of interface statistics.
Name	This field displays the name of each interface.
Status	This field displays the current status of each interface. The possible values depend on what type of interface it is. **Inactive** - The Ethernet interface is disabled. **Down** - 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**).
VID	This field displays the VLAN ID to which the interface belongs.
IP Addr/Netmask	This field displays the current IP address and subnet mask assigned to the interface. If the IP address is 0.0.0.0, the interface is disabled or did not receive an IP address and subnet mask via DHCP.
IP Assignment	This field displays how the interface gets its IP address. **Static** - This interface has a static IP address. **DHCP Client** - This interface gets its IP address from a DHCP server.
Action	If the interface has a static IP address, this shows **n/a**. If the interface has a dynamic IP address, 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.

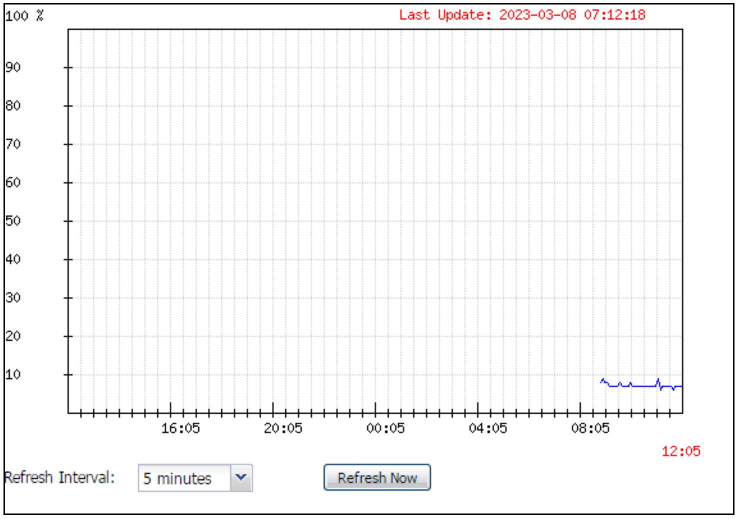
Table 21 Dashboard (continued)

LABEL	DESCRIPTION
WLAN Interface Status Summary	This displays status information for the WLAN interface.
Status	This displays whether or not the WLAN interface is activated.
MAC Address	This displays the MAC address of the radio.
Radio	This indicates the radio number on the Zyxel Device.
Band	This indicates the WiFi frequency band currently being used by the radio.
OP Mode	This indicates the radio's operating mode. Operating modes are **AP (MBSSID)**, **Root AP** or **Repeater**.
Channel	This indicates the channel number the radio is using.
Antenna	This indicates the antenna orientation for the radio (**Wall** or **Ceiling**). This field is not available if the Zyxel Device does not allow you to adjust antenna orientation for the Zyxel Device's radio(s) using the web configurator or a physical switch. Refer to Section 1.2 on page 14 to see if your Zyxel Device has an antenna switch.
Station	This displays the number of WiFi clients connected to the Zyxel Device.
AP Information	This shows a summary of connected wireless Access Points (APs).
All Sensed Device	This sections displays a summary of all wireless devices detected by the network. Click the link to go to the **Monitor > Wireless > Detected Device** screen.
Un-Classified AP	This displays the number of detected unclassified APs.
Rogue AP	This displays the number of detected rogue APs.
Friendly AP	This displays the number of detected friendly APs.

6.1.1 CPU Usage

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

Figure 41 Dashboard > CPU Usage



Last Update: 2023-03-08 07:12:18

Refresh Interval: 5 minutes

The following table describes the labels in this screen.

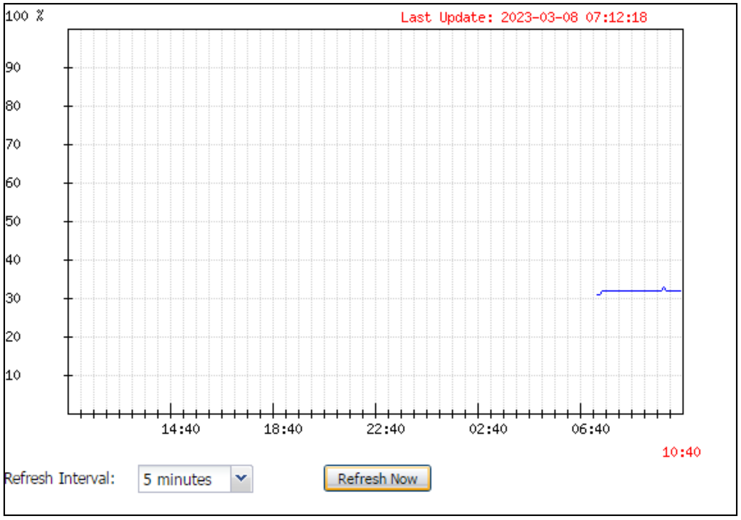
Table 22 Dashboard > CPU Usage

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

6.1.2 Memory Usage

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

Figure 42 Dashboard > Memory Usage



The following table describes the labels in this screen.

Table 23 Dashboard > Memory Usage

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

CHAPTER 7 Setup Wizard

7.1 Accessing the Wizard

When you log into the Web Configurator for the first time or when you reset the Zyxel Device to its default configuration, the wizard screen displays.

Note: If you have already configured the wizard screens and want to open it again, click the **Wizard** icon on the upper right corner of any Web Configurator screen.

7.2 Using the Wizard

This wizard helps you configure the Zyxel Device IP address, change time zone, daylight saving and radio settings, and edit an SSID profile to change general WiFi and WiFi security settings.

7.2.1 Step 1 Time Settings

Use this screen to configure the Zyxel Device's country code, time zone and daylight saving time.

- **Country**: Select the country where the Zyxel Device is located.

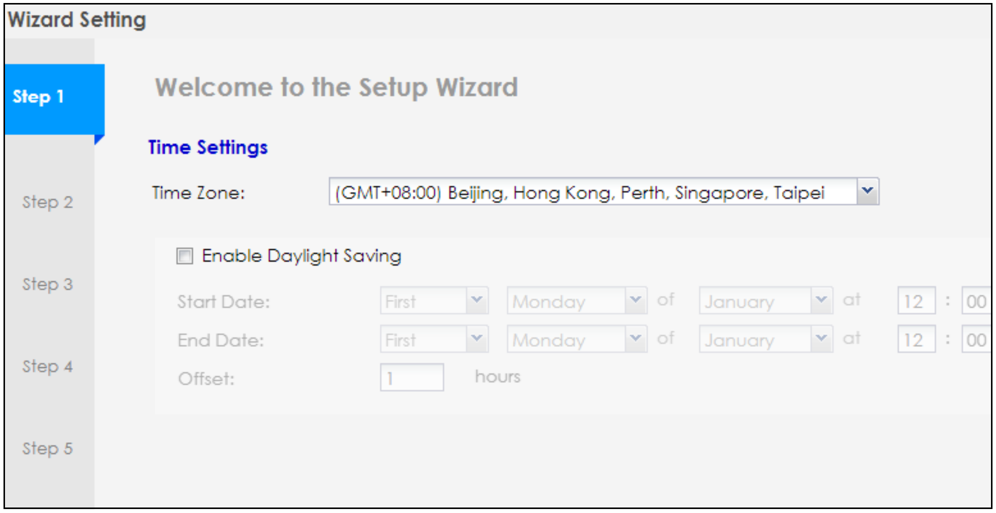
Note: The **Country** field is not available and you cannot change the country code if the Zyxel Device products comply with the U.S. laws, policies and regulations and are to be sold to the U.S. market.

Note: Due to each country's regulations on frequency band usage, the available radio bands (2.4 GHz, 5 GHz, and 6 GHz) may differ by the **Country** field you select here, or markets the Zyxel Device products are sold to.

- **Time Zone**: Select the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
- **Enable Daylight Saving**: Select the option if you use Daylight Saving Time. Configure the day and time when Daylight Saving Time starts and ends.
- **Offset** allows you to specify how much the clock changes when daylight saving begins and ends. Enter a number from 1 to 5.5 (by 0.5 increments).

Click **Next** to proceed. Click **Cancel** to close the wizard without saving.

Figure 43 Wizard: Time Settings



Welcome to the Setup Wizard

Time Settings

Time Zone: (GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei

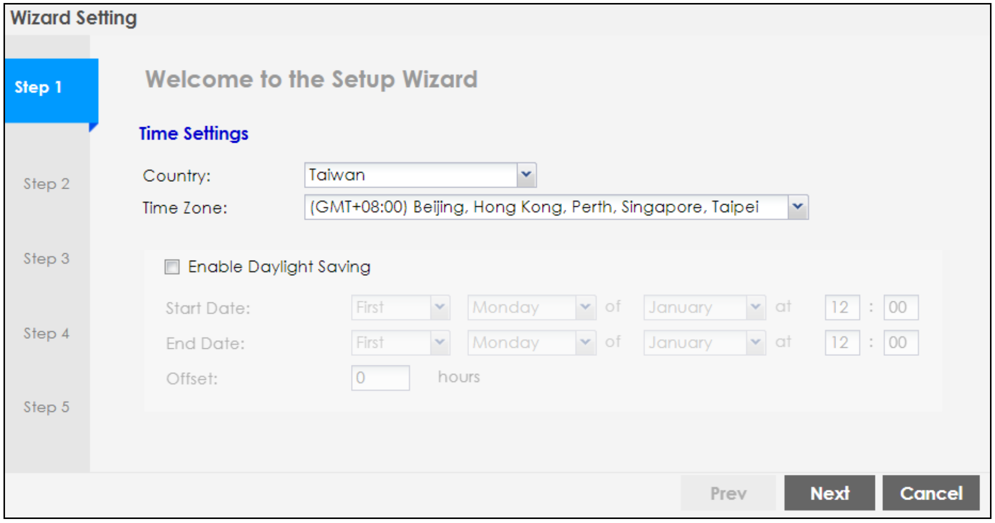
☐ Enable Daylight Saving

Start Date: First Monday of January at 12 : 00

End Date: First Monday of January at 12 : 00

Offset: 1 hours

Figure 44 Wizard: Time Settings (with **Country** option)



Welcome to the Setup Wizard

Time Settings

Country: Taiwan

Time Zone: (GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei

☐ Enable Daylight Saving

Start Date: First Monday of January at 12 : 00

End Date: First Monday of January at 12 : 00

Offset: 0 hours

7.2.2 Step 2 Password and Uplink Connection

Use this screen to configure the Zyxel Device's system password and IP address.

Change Password: Enter a new password and retype it to confirm.

Uplink Connection: Select **Auto (DHCP)** if the Zyxel Device is connected to a router with the DHCP server enabled. You then need to check the router for the IP address assigned to the Zyxel Device in order to access the Zyxel Device's Web Configurator again.

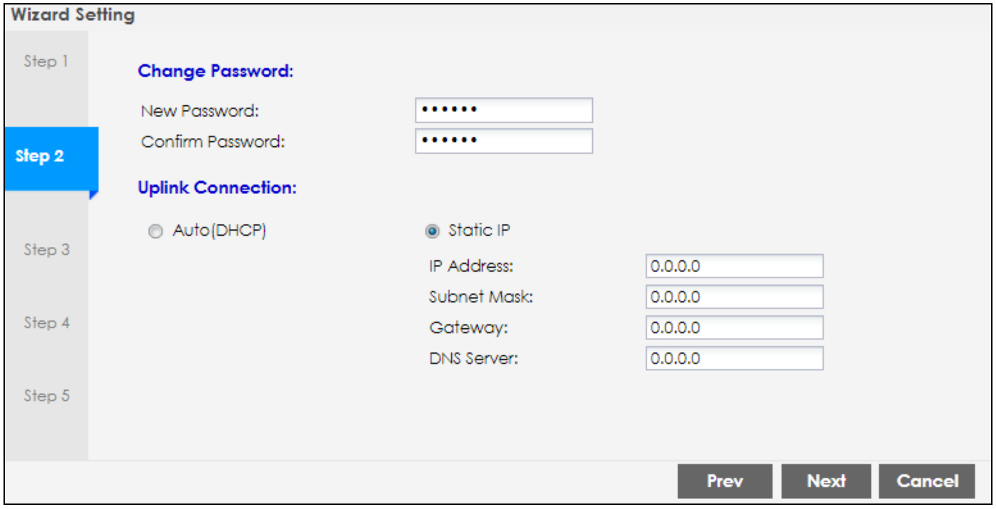
Otherwise, select **Static IP** when the Zyxel Device is NOT connected to a router or you want to assign it a fixed IP address. You will need to manually enter:

- the Zyxel Device's IP address and subnet mask.
- the IP address of the router that helps forward traffic.
- a DNS server's IP address. The Domain Name System (DNS) maps a domain name to an IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

Click **Prev** to return to the previous screen. Click **Next** to proceed. Click **Cancel** to close the wizard without saving.

Note: The number of characters shown is not an actual representation of your current password. If you click **Next** without changing password in the **New Password** and **Confirm Password** fields, your current password will not be changed.

Figure 45 Wizard: Change Password and Uplink Connection



Wizard Setting

Change Password:

New Password: ••••••

Confirm Password: ••••••

Uplink Connection:

○ Auto(DHCP) ● Static IP

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

DNS Server: 0.0.0.0

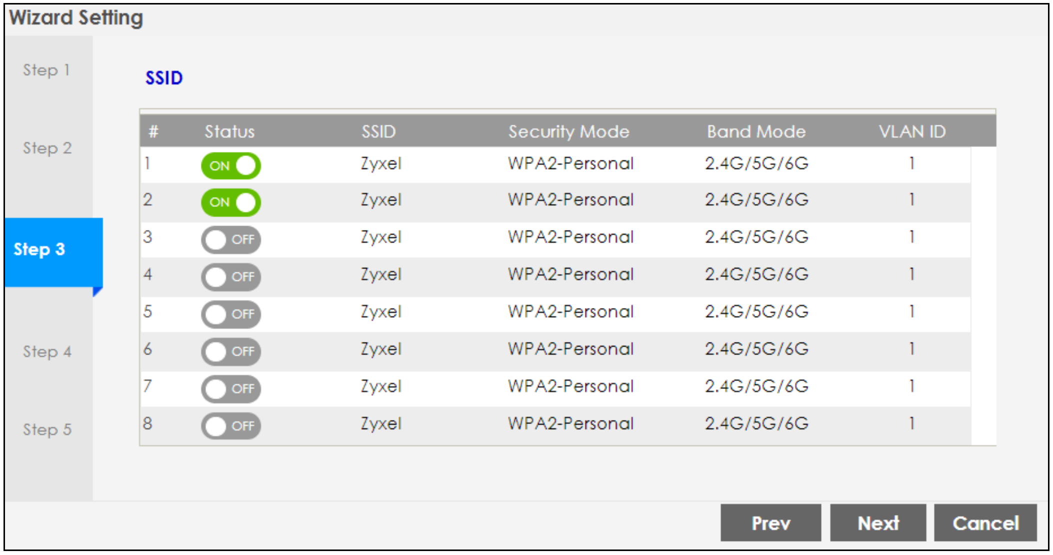
7.2.3 Step 3 SSID

Use this screen to enable, disable or edit an SSID profile.

Select an SSID profile and click the **Status** switch to turn it on or off. To change an SSID profile's settings, such as the SSID (WiFi network name) and WiFi password, double-click the SSID profile entry from the list. See Section 7.2.3.1 on page 72 for more information.

Note: You cannot add or remove an SSID profile after running the setup wizard.

Figure 46 Wizard: SSID



Wizard Setting

SSID

#	Status	SSID	Security Mode	Band Mode	VLAN ID
1	ON	Zyxel	WPA2-Personal	2.4G/5G/6G	1
2	ON	Zyxel	WPA2-Personal	2.4G/5G/6G	1
3	OFF	Zyxel	WPA2-Personal	2.4G/5G/6G	1
4	OFF	Zyxel	WPA2-Personal	2.4G/5G/6G	1
5	OFF	Zyxel	WPA2-Personal	2.4G/5G/6G	1
6	OFF	Zyxel	WPA2-Personal	2.4G/5G/6G	1
7	OFF	Zyxel	WPA2-Personal	2.4G/5G/6G	1
8	OFF	Zyxel	WPA2-Personal	2.4G/5G/6G	1

7.2.3.1 Edit SSID Profile

Use this screen to configure an SSID profile.

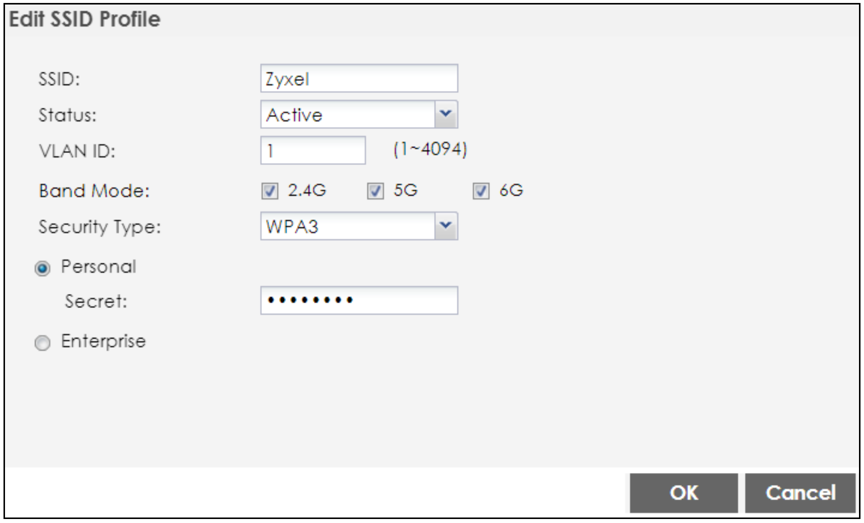
The screen varies depending on the security type you selected.

- **SSID**: Enter a descriptive name of up to 32 printable characters for the wireless LAN.
- **Status**: Select **Active** to apply this SSID profile on all the radios. Select **Inactive** to create the SSID profile without applying this SSID on any radio.
- **VLAN ID**: Enter a VLAN ID for the Zyxel Device to use to tag traffic originating from this SSID.
- **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.
- **Security Type**: Select **WPA2** or **WPA3** to add security on this WiFi network. Otherwise, select **OPEN** or **Enhanced-Open** to allow any WiFi client to associate this network without authentication.
- **Personal**: If you set **Security Type** to **WPA2** or **WPA3** and select **Personal**, enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
- **Enterprise**: Select this option and the **Primary / Secondary RADIUS Server** check box to have the Zyxel Device use the specified RADIUS server. You have to enter the IP address, port number and shared secret password of the RADIUS server to be used for authentication.

Note: See Section 1.2 on page 14 for models that support the 6 GHz band.

Click **OK** to proceed. Click **Cancel** to close the screen without saving.

Figure 47 Wizard: SSID: Edit (WPA3-Personal)



Edit SSID Profile

SSID: Zyxel

Status: Active

VLAN ID: 1 (1~4094)

Band Mode: ☑ 2.4G ☑ 5G ☑ 6G

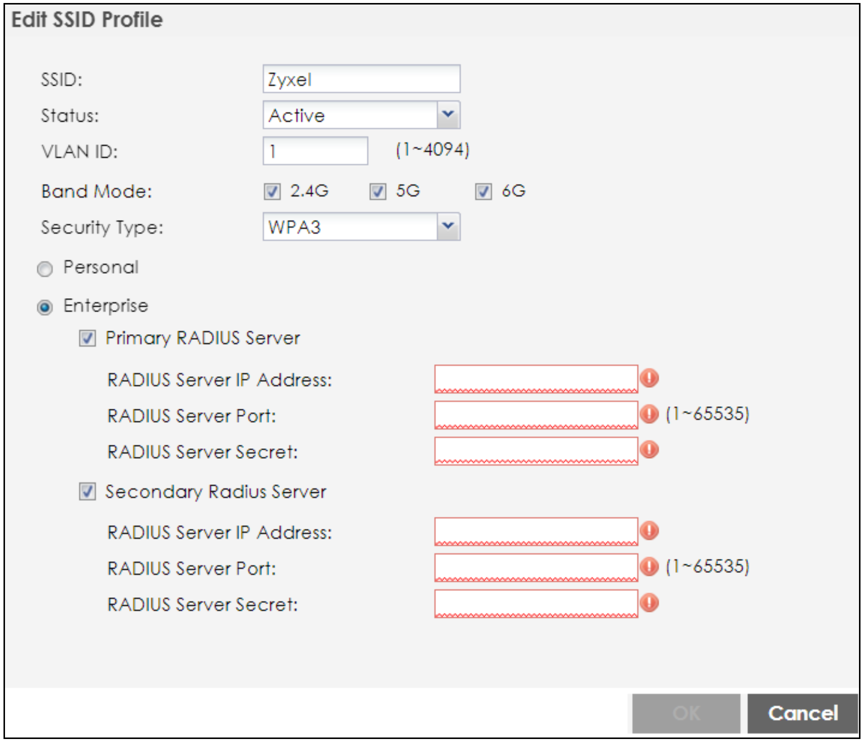
Security Type: WPA3

● Personal

Secret: ••••••••

○ Enterprise

Figure 48 Wizard: SSID: Edit (WPA3-Enterprise)



Edit SSID Profile

SSID: Zyxel

Status: Active

VLAN ID: 1 (1~4094)

Band Mode: ☑ 2.4G ☑ 5G ☑ 6G

Security Type: WPA3

○ Personal

● Enterprise

☑ Primary RADIUS Server

RADIUS Server IP Address:

RADIUS Server Port: (1~65535)

RADIUS Server Secret:

☑ Secondary Radius Server

RADIUS Server IP Address:

RADIUS Server Port: (1~65535)

RADIUS Server Secret:

7.2.4 Step 4 Radio

Use this screen to configure the Zyxel Device's radio transmitter(s).

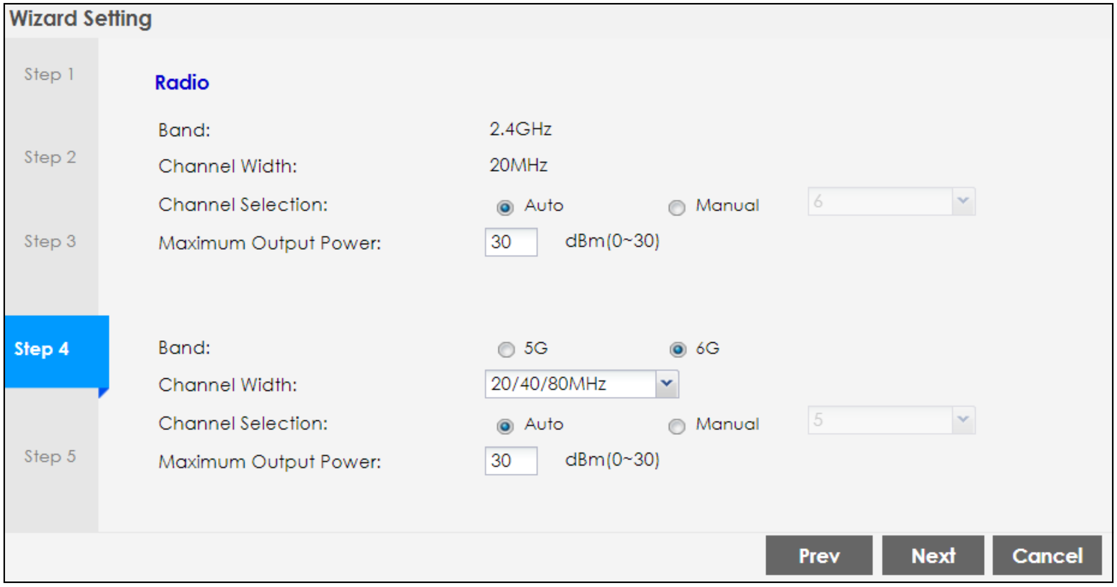
- **Band**: Select the radio band you want to use on this radio. The radio band is unconfigurable if the Zyxel Device does not support BandFlex (band selection on each radio). See Section 1.2 on page 14.
- **Channel Width**: Select the channel bandwidth list you want to use on this radio. The Zyxel Device will automatically choose the most suitable channel bandwidth from the bandwidth list you select based on your environment and client device type.
- **Channel Selection**: Select **Auto** to have the Zyxel Device automatically choose a radio channel that has least interference. Otherwise, select **Manual** and specify a channel the Zyxel Device will use in the 2.4 GHz or 5 GHz wireless LAN. The options vary depending on the frequency band and the country you are in.
- **Maximum Output Power**: Enter the maximum output power of the Zyxel Device. If there is a high density of APs in an area, decrease the output power of the Zyxel Device to reduce interference with other APs.

Note: Reducing the output power also reduces the Zyxel Device's effective broadcast radius.

Note: See Section 1.2 on page 14 for the supported band (2.4G/5G/6G) and channel bandwidth of your Zyxel Device model.

Click **Prev** to return to the previous screen. Click **Next** to proceed. Click **Cancel** to close the wizard without saving.

Figure 49 Wizard: Radio



Radio

Band: 2.4GHz

Channel Width: 20MHz

Channel Selection: ● Auto ○ Manual 6

Maximum Output Power: 30 dBm(0~30)

Band: ○ 5G ● 6G

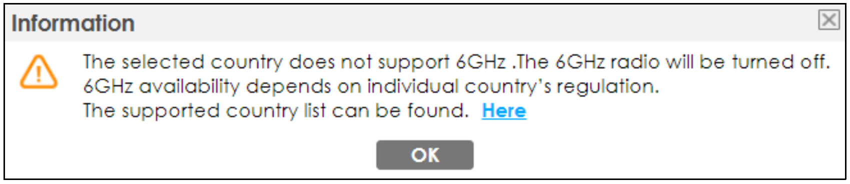
Channel Width: 20/40/80MHz

Channel Selection: ● Auto ○ Manual 5

Maximum Output Power: 30 dBm(0~30)

If the **Country** you select in **Step 1** does not support 6 GHz, the **6G** option will gray out, or a warning message will display when you select **6G**. Click **OK** to return to the previous page.

Figure 50 Wizard: Invalid Band Warning Message

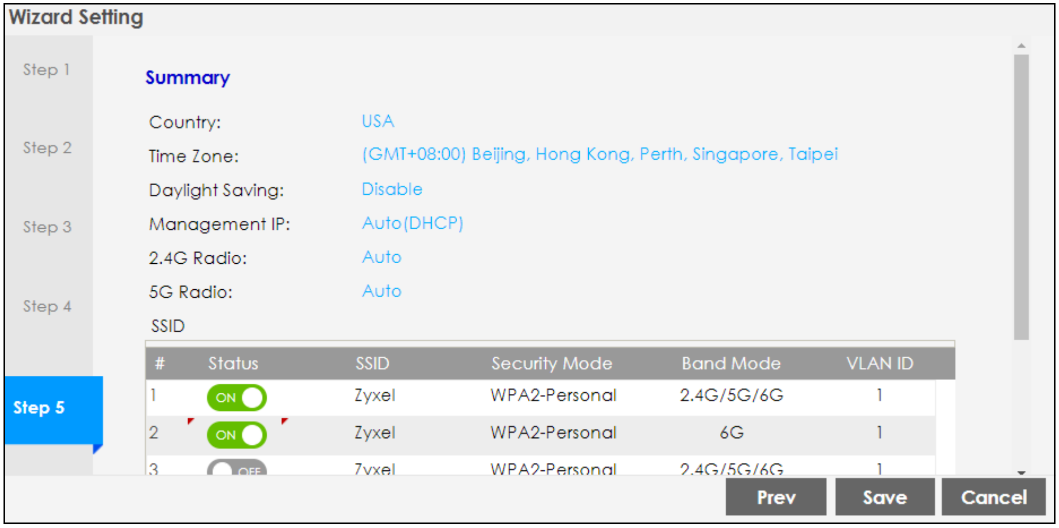


The selected country does not support 6GHz .The 6GHz radio will be turned off.
6GHz availability depends on individual country's regulation.
The supported country list can be found. Here

7.2.5 Summary

Use this screen to check whether what you have configured is correct. Click **Save** to apply your settings and complete the wizard setup. Otherwise, click **Prev** to return to the previous screen or click **Cancel** to close the wizard without saving.

Figure 51 Wizard: Summary



Wizard Setting

Summary

Country: USA

Time Zone: (GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei

Daylight Saving: Disable

Management IP: Auto(DHCP)

2.4G Radio: Auto

5G Radio: Auto

SSID

#	Status	SSID	Security Mode	Band Mode	VLAN ID
1	ON	Zyxel	WPA2-Personal	2.4G/5G/6G	1
2	ON	Zyxel	WPA2-Personal	6G	1
3	OFF	Zyxel	WPA2-Personal	2.4G/5G/6G	1

CHAPTER 8
Getting Started

8.1 Getting Started Overview

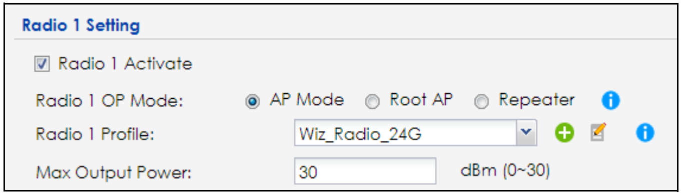
This chapter first provides a basic overview of how to configure the some basic items on your Zyxel Device.

- Choose the Operation Mode
- Set Up a WiFi Network
- Set Up Rogue AP Detection
- Set Up an Email Daily Report
- Restrict Access to Specific Parts of Your Network
- Check Your Settings and Test the Access Restrictions

8.2 Choose the Operation Mode

The Zyxel Device has different Operation Modes (OP modes) to act as different roles in a network. You can choose different OP modes for each radios. Not all OP modes are supported by all models. To choose the OP mode, go to **Configuration > Wireless > AP Management.**

Figure 52 OP Modes



Radio 1 Setting

☑ Radio 1 Activate

Radio 1 OP Mode: ● AP Mode ○ Root AP ○ Repeater

Radio 1 Profile: Wiz_Radio_24G

Max Output Power: 30 dBm (0~30)

The Zyxel Device supports the following OP modes:

- Choose **AP Mode** if you want WiFi clients to connect to the Zyxel Device.
- Choose **Root AP** Mode if you want the Zyxel Device to wirelessly extend your WiFi network and also allow WiFi clients to connect to the Zyxel Device.
- Choose **Repeater** Mode if you want the Zyxel Device to wirelessly extend your WiFi network (WDS).

8.3 Set Up a WiFi Network

In this section, we show you how to:

- Configure a WiFi Network in AP Mode

- Configure a WiFi Network in Root AP / Repeater Mode

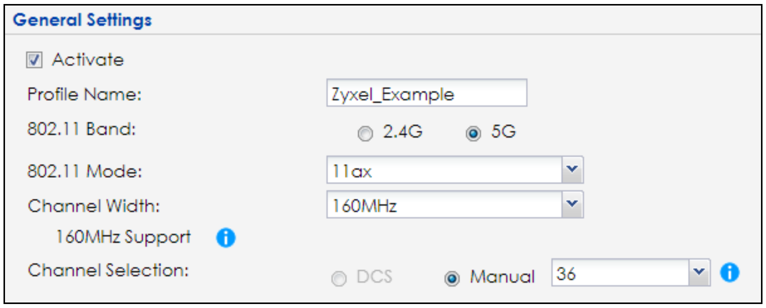
8.3.1 Configure a WiFi Network in AP Mode

This example uses the following parameters to set up a WiFi network.

Table 24 SSID Profile Settings Example

	PROFILE
SSID	Zyxel_Example
Channel Selection	36
Security Mode	Wpa2
Pre-Shared Key	zyxel1234
802.11 Mode	11ax

1 Go to **Configuration > Object > AP Profile > Radio**. Enter the profile name, select the 802.11 mode and select a channel that is not used by another AP (36 in this example). Click **Apply**.



General Settings

☑ Activate

Profile Name: Zyxel_Example

802.11 Band: ○ 2.4G ● 5G

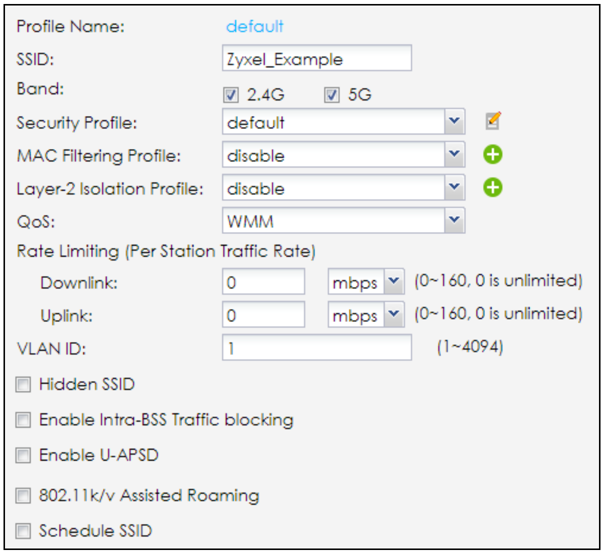
802.11 Mode: 11ax

Channel Width: 160MHz

160MHz Support

Channel Selection: ○ DCS ● Manual 36

2 Go to **Configuration > Object > AP Profile > SSID > SSID List**, select the **default** SSID profile and click **Edit** to configure the SSID settings. Click **Apply**.



Profile Name: default

SSID: Zyxel_Example

Band: ☑ 2.4G ☑ 5G

Security Profile: default

MAC Filtering Profile: disable

Layer-2 Isolation Profile: disable

QoS: WMM

Rate Limiting (Per Station Traffic Rate)

Downlink: 0 mbps (0~160, 0 is unlimited)

Uplink: 0 mbps (0~160, 0 is unlimited)

VLAN ID: 1 (1~4094)

□ Hidden SSID

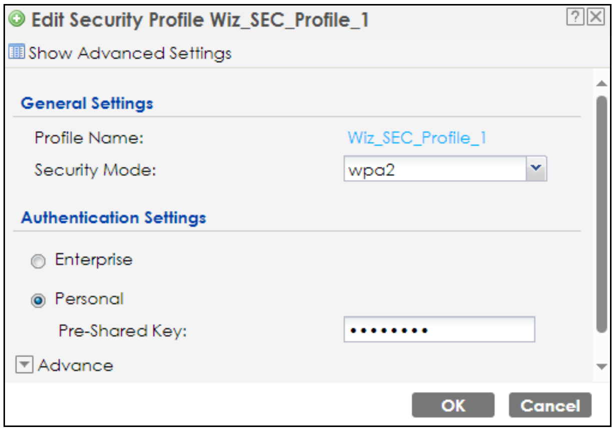
□ Enable Intra-BSS Traffic blocking

□ Enable U-APSD

□ 802.11k/v Assisted Roaming

□ Schedule SSID

3 Go to **Configuration > Object > AP Profile > SSID > Security List** to set the **Security Mode** and enter the **Pre-Shared Key**. Click **Apply**.



Edit Security Profile Wiz_SEC_Profile_1

Show Advanced Settings

General Settings

Profile Name:	Wiz_SEC_Profile_1
Security Mode:	wpa2

Authentication Settings

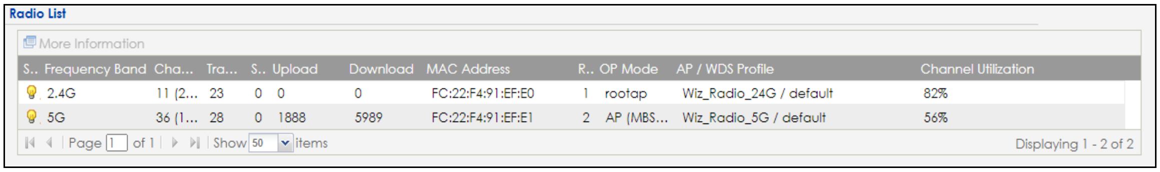
○ Enterprise

● Personal

Pre-Shared Key:	••••••••

Advance

4 To see your current WiFi settings and check if the WLAN connection is up, go to **Monitor > Wireless > AP Information**.



Radio List

More Information

S..	Frequency Band	Cha...	Tra...	S..	Upload	Download	MAC Address	R..	OP Mode	AP / WDS Profile	Channel Utilization
	2.4G	11 (2...	23	0	0	0	FC:22:F4:91:EF:E0	1	rootap	Wiz_Radio_24G / default	82%
	5G	36 (1...	28	0	1888	5989	FC:22:F4:91:EF:E1	2	AP (MBS...	Wiz_Radio_5G / default	56%

5 You can now allow your WiFi clients to search for the Zyxel Device's SSID and connect to the Zyxel Device's WiFi.

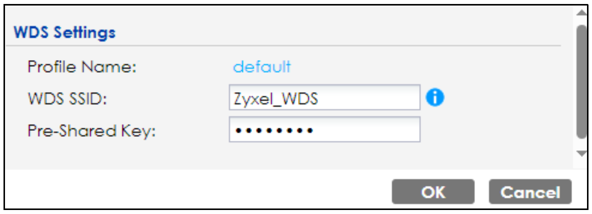
8.3.2 Configure a WiFi Network in Root AP / Repeater Mode

To wirelessly extend a WiFi network (WDS), you need two Zyxel Devices, one in **Repeater** mode and one in **Root AP** mode. You should already have the root AP set up.

Note: The Zyxel Device in **Root AP / Repeater** mode cannot connect with other company's APs.

1 Go to **Configuration > Object > WDS Profile** in your root AP Web Configurator and click **Add**.

2 Enter a profile name, a WDS SSID, and a pre-shared key.



WDS Settings

Profile Name:	default
WDS SSID:	Zyxel_WDS
Pre-Shared Key:	••••••••

3 Go to **Configuration > Wireless > AP Management**, select the **Radio WDS Profile** of the radio on which you are setting the WDS connection to use the WDS profile you set, and click **Apply**.

4 Do steps 1 and 3 for the Zyxel Device in **Repeater** mode using the same WDS SSID and pre-shared key.

5 Once the security settings of the Zyxel Device in **Root AP** and **Repeater** modes match one another, the connection between the two Zyxel Devices is made.

If your Zyxel Device supports wireless bridging, you can extend a wired network from the port on the WiFi repeater, do the following steps:

6 Go to **Configuration > Wireless > AP Management,** select **Setup WDS Wireless Bridging** to enable WiFi bridge on the Zyxel Device in **Repeater** mode.

7 Connect the client device to the Zyxel Device's LAN port with an Ethernet cable.

Note: Make sure the VLAN settings on both the root AP and the WiFi repeater are exactly the same so they can communicate.

Note: When wireless bridge is enabled, WiFi interfaces for client devices will be disabled. You can only transmit data through the ports of the Zyxel Device in **Repeater** mode.

To set up a WDS in AC (AP Controller)-managed Zyxel Devices, see the ZyWALL ATP, USG FLEX, or NCC User's Guide.

8.4 Set Up Rogue AP Detection

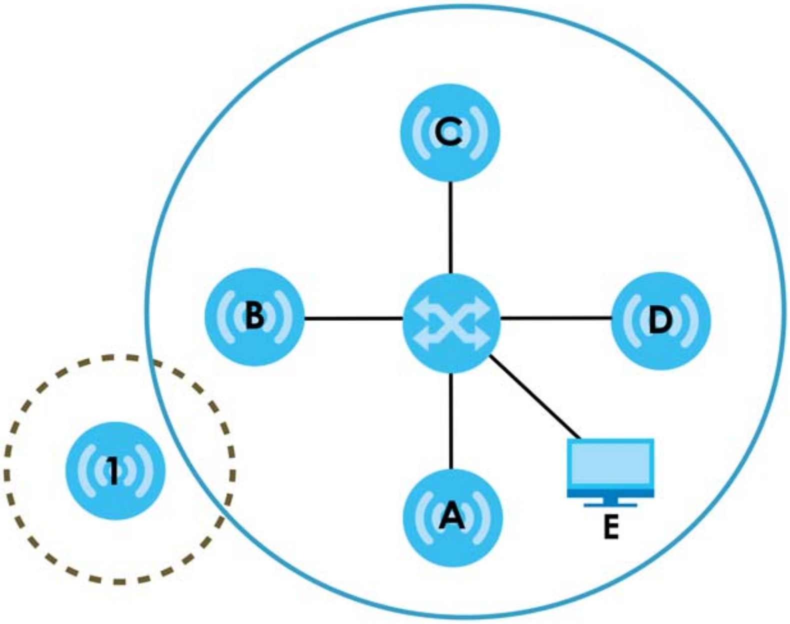
This example shows you how to configure the rogue AP detection feature on the Zyxel Device. A rogue AP is a WiFi access point operating in a network's coverage area that is not a sanctioned part of that network. See Section 11.3 on page 122 for background information on the rogue AP function and security considerations.

In this example, you want to ensure that your company's data is not accessible to an attacker gaining entry to your WiFi network through a rogue AP.

Your WiFi network operates in an office building. It consists of four Zyxel access points (all NWAs) and a variable number of WiFi clients. You also know that the coffee shop on the ground floor has a WiFi network consisting of a single access point (**AP 1**), which can be detected and accessed from your floor of the building. There are no other static WiFi networks in your coverage area.

The following diagram shows the WiFi networks in your area. Your access points are marked **A, B, C** and **D**. You also have a computer, marked **E**, connected to the wired network. The coffee shop's access point is marked **1**.

Figure 53 WiFi Network Example



In the figure, the solid circle represents the range of your WiFi network, and the dashed circle represents the extent of the coffee shop's WiFi network. Note that the two networks overlap. This means that one or more of your APs can detect the **AP 1** in the other WiFi network.

When configuring the rogue AP feature on your Zyxel Device in this example, you will need to use the information in the following table. You need the IP addresses of your APs to access their Web configurators, and you need the MAC address of each AP to configure the friendly AP list.

Table 25 Rogue AP Example Information

DEVICE	IP ADDRESS	MAC ADDRESS
Access Point **A**	192.168.1.1	00:AA:00:AA:00:AA
Access Point **B**	192.168.1.2	AA:00:AA:00:AA:00
Access Point **C**	192.168.1.3	A0:0A:A0:0A:A0:0A
Access Point **D**	192.168.1.4	0A:A0:0A:A0:0A:A0
Access Point **1**	Unknown	AF:AF:AF:FA:FA:FA

Note: You can detect the MAC addresses of other APs in the **Monitor > Wireless > Detected Device** screen. However, it is more secure to obtain the correct MAC addresses from another source and add them to the friendly AP list manually. For example, an attacker's AP mimicking the correct SSID could be placed on the friendly AP list by accident, if selected from the list of auto-detected APs.
In this example you have spoken to the coffee shop's owner, who has told you the correct MAC address of his **AP 1**.

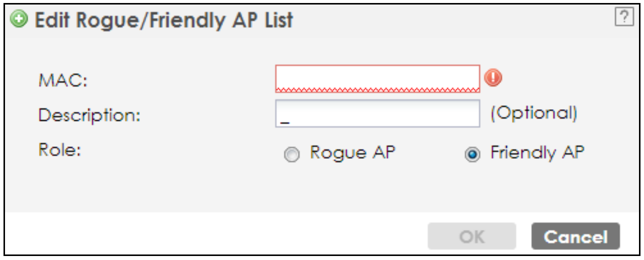
8.4.1 Set Up a Friendly AP List

To find rogue APs, create a list of known friendly APs, then scan for all APs in your coverage area. Check if other APs are known and if not add them to the Rogue AP list.

Take the following steps to set up and save a list of access points you want to allow in your network's coverage area.

1 On a computer connected to the wired network (**F** in the previous figure), open your Internet browser and enter the URL of access point **A** (192.168.1.1). Login to the Web Configurator, go to **Configuration** > **Rogue AP** > **Rogue/Friendly AP List** and then click **Add** in the **Rogue/Friendly AP list** field.

Figure 54 Getting Started: Add Rogue/Friendly AP



Edit Rogue/Friendly AP List

MAC:

Description: _ (Optional)

Role: ○ Rogue AP ● Friendly AP

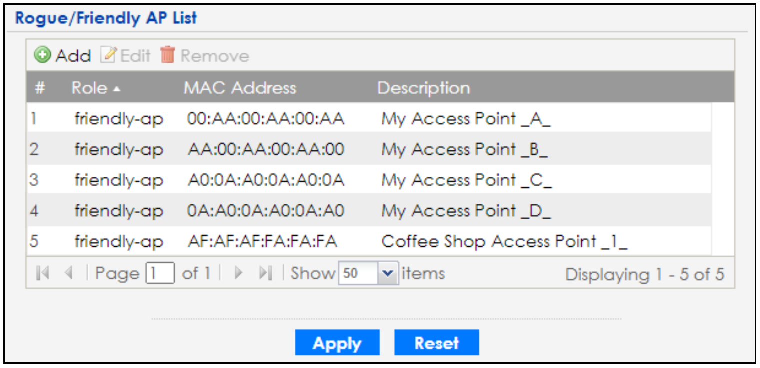
2 Fill in the **MAC Address** and **Description** fields as in the following table. Click **Add** after you enter the details of each AP to include it in the list.

MAC ADDRESS	DESCRIPTION
00:AA:00:AA:00:AA	My Access Point _A_
AA:00:AA:00:AA:00	My Access Point _B_
A0:0A:A0:0A:A0:0A	My Access Point _C_
0A:A0:0A:A0:0A:A0	My Access Point _D_
AF:AF:AF:FA:FA:FA	Coffee Shop Access Point _1_

Note: You can add APs that are not part of your network to the friendly AP list, as long as you know that they do not pose a threat to your network's security.

The Friendly AP screen now appears as follows.

Figure 55 Friendly AP List



Rogue/Friendly AP List

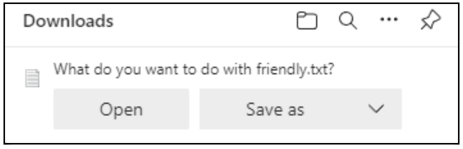
#	Role ▴	MAC Address	Description
1	friendly-ap	00:AA:00:AA:00:AA	My Access Point _A_
2	friendly-ap	AA:00:AA:00:AA:00	My Access Point _B_
3	friendly-ap	A0:0A:A0:0A:A0:0A	My Access Point _C_
4	friendly-ap	0A:A0:0A:A0:0A:A0	My Access Point _D_
5	friendly-ap	AF:AF:AF:FA:FA:FA	Coffee Shop Access Point _1_

Page 1 of 1 | Show 50 items Displaying 1 - 5 of 5

3 Next, click **Apply** to save the list of friendly APs in order to provide a backup and upload it to your other access points.

4 Click **Exporting** in the **Friendly AP List Importing/Exporting** field. If a window similar to the following appears, click **Save.**

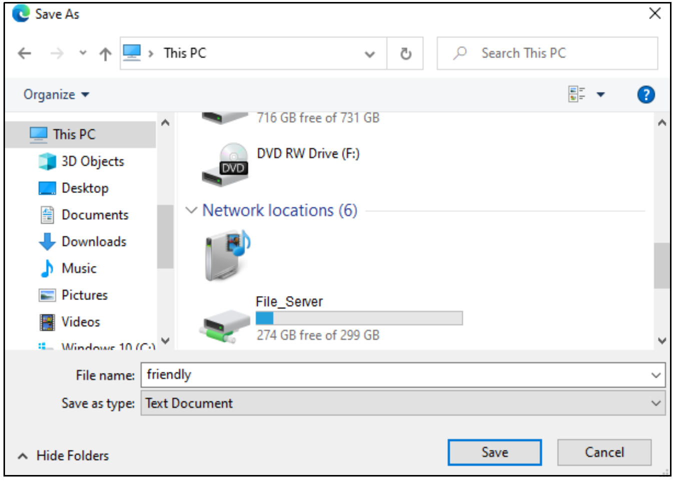
Figure 56 Getting Started: Export Friendly AP List



What do you want to do with friendly.txt?

5 Save the friendly AP list somewhere it can be accessed by all the other access points on the network. In this example, save it on the network file server. The default filename is “friendly”.

Figure 57 Getting Started: Save Friendly AP list



File name: friendly

Save as type: Text Document

8.4.2 Import the Friendly AP List to Other APs

Access point **A** is now configured to do the following.

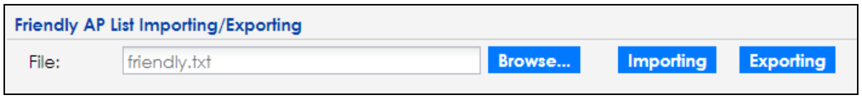
- Scan for access points in its coverage area
- Recognize friendly access points from a list

Now you need to configure the other WiFi access points in your network to do the same things.

For each access point, take the following steps.

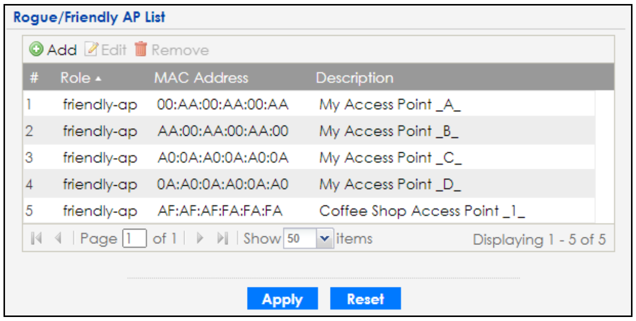
1 From a computer on the wired network, enter the access point’s IP address and log into its Web Configurator.

2 Import the friendly AP list. Click **Configuration > Wireless > Rogue AP > Rogue/Friendly AP List**, and click **Browse** in the **Friendly AP List Importing/Exporting** field**.** Find the “friendly” file where you previously saved it on the network and click **Open**.



File: friendly.txt

3 Click **Importing**. Check the **Configuration > Wireless > Rogue AP > Rogue/Friendly AP List** screen to ensure that the friendly AP list has been correctly uploaded.



Rogue/Friendly AP List

#	Role	MAC Address	Description
1	friendly-ap	00:AA:00:AA:00:AA	My Access Point _A_
2	friendly-ap	AA:00:AA:00:AA:00	My Access Point _B_
3	friendly-ap	A0:0A:A0:0A:A0:0A	My Access Point _C_
4	friendly-ap	0A:A0:0A:A0:0A:A0	My Access Point _D_
5	friendly-ap	AF:AF:AF:FA:FA:FA	Coffee Shop Access Point _1_

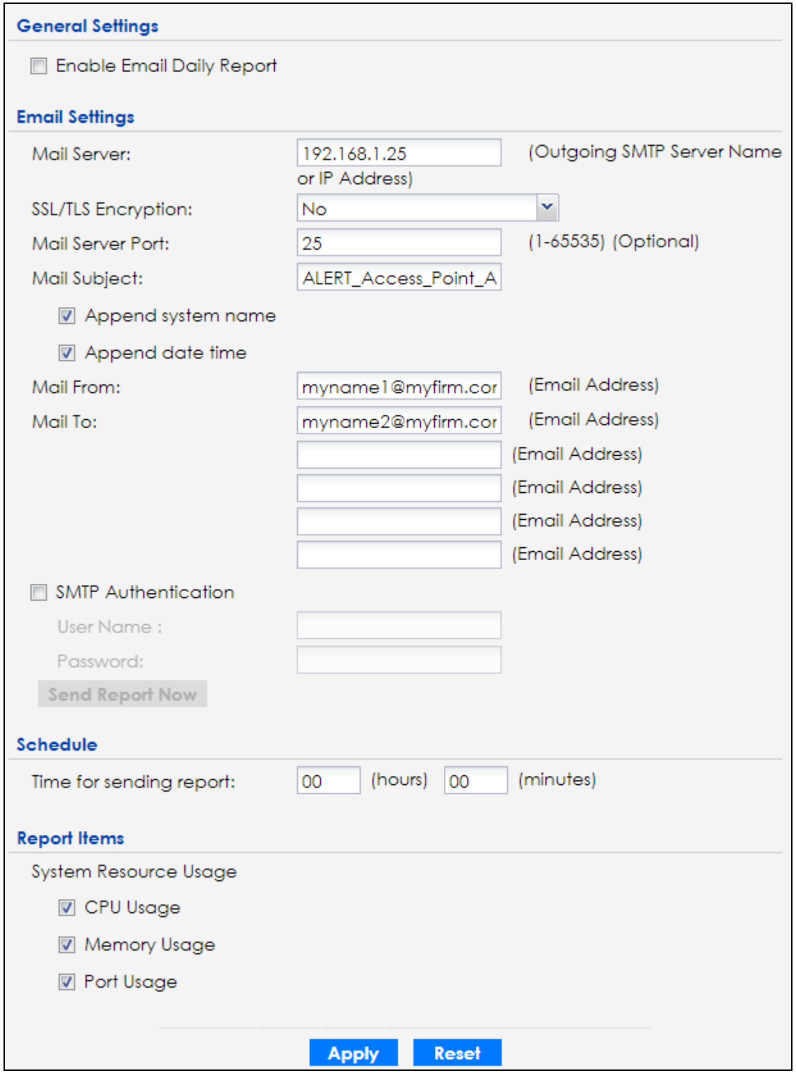
Page 1 of 1 | Show 50 items | Displaying 1 - 5 of 5

8.5 Set Up an Email Daily Report

In this example, you will configure the first of your APs to send a log message to your email inbox.

Click **Configuration** > **Log & Report > Email Daily Report**. The following screen appears.

Figure 58 Getting Started: Email Log Settings



General Settings

□ Enable Email Daily Report

Email Settings

Mail Server: 192.168.1.25 (Outgoing SMTP Server Name or IP Address)

SSL/TLS Encryption: No

Mail Server Port: 25 (1-65535) (Optional)

Mail Subject: ALERT_Access_Point_A

☑ Append system name

☑ Append date time

Mail From: myname1@myfirm.cor (Email Address)

Mail To: myname2@myfirm.cor (Email Address)

(Email Address)

(Email Address)

(Email Address)

(Email Address)

□ SMTP Authentication

User Name :

Password:

Schedule

Time for sending report: 00 (hours) 00 (minutes)

Report Items

System Resource Usage

☑ CPU Usage

☑ Memory Usage

☑ Port Usage

1 In this example, your mail server's IP address is **192.168.1.25**. Enter this IP address in the **Mail Server** field.

2 Enter a subject line for the alert emails in the **Mail Subject** field. Choose a subject that is eye-catching and identifies the access point - in this example, "ALERT_Access_Point_A".

3 Enter the email address to which you want alerts to be sent (**myname1@myfirm.com**, in this example).

4 Click **Apply**.

8.6 Restrict Access to Specific Parts of Your Network

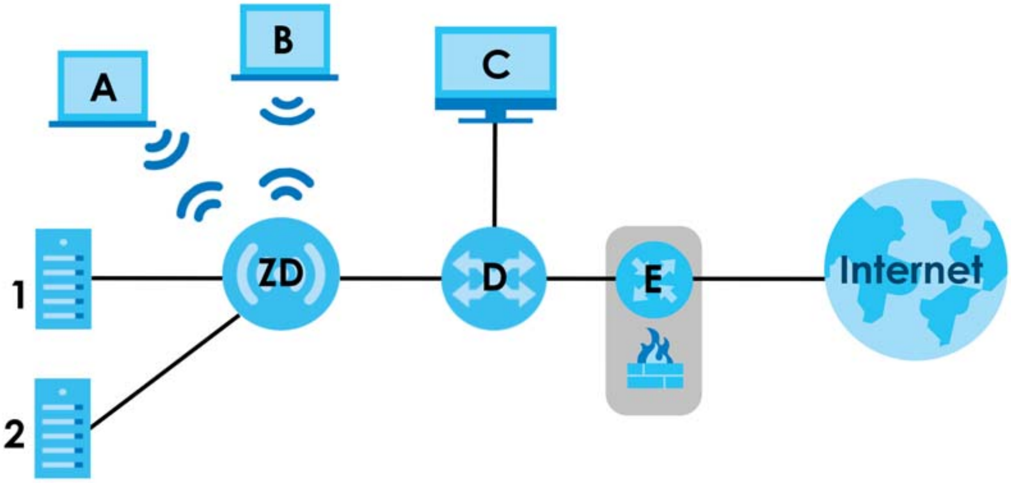
This example shows you how to allow certain users to access only specific parts of your network. You can do this by using multiple MAC filters and layer-2 isolation profiles.

8.6.1 Scenario

In this example, you run a company network in which certain employees must wirelessly access secure file servers containing valuable proprietary data.

You have two secure servers (**1** and **2** in the following figure). WiFi user "Alice" (**A**) needs to access server **1** (but should not access server **2**) and WiFi user "Bob" (**B**) needs to access server **2** (but should not access server **1**). Your Zyxel Device is marked **ZD**. **C** is a workstation on your wired network, **D** is your main network switch, and **E** is the security gateway you use to connect to the Internet.

Figure 59 Getting Started: Example Network



8.6.2 Your Requirements

1 You want to set up a WiFi network to allow only Alice to access server 1 and the Internet.

2 You want to set up a second WiFi network to allow only Bob to access server 1 and the Internet.

8.6.3 Setup

In this example, you have already set up the Zyxel Device in **AP Mode** (see Chapter 8 on page 76). It uses two SSID profiles simultaneously. You have configured each SSID profile as shown in the following table.

Table 26 SSID Profile Security Settings

SSID Profile Name	SERVER_1	SERVER_2
SSID	SSID_S1	SSID_S2
Security	Security Profile security03: WPA2-PSK Hide SSID	Security Profile security04: WPA2-PSK Hide SSID
Intra-BSS traffic blocking	Enabled	Enabled

Each SSID profile already uses a different pre-shared key.

In this example, you will configure access limitations for each SSID profile. To do this, you will take the following steps.

1. Configure the SERVER_1 network's SSID profile to use specific MAC filter and layer-2 isolation profiles.
2. Configure the SERVER_1 network's MAC filter profile.
3. Configure the SERVER_1 network's layer-2 isolation profile.
4. Repeat steps 1 to step 3 for the SERVER_2 network.
5. Check your settings and test the configuration.

To configure layer-2 isolation, you need to know the MAC addresses of the devices on your network, which are as follows.

Table 27 Getting Started: Example Network MAC Addresses

DEVICE	LABEL	MAC ADDRESS
Zyxel Device	ZD	BB:AA:99:88:77:66
Secure Server 1	1	AA:99:88:77:66:55
Secure Server 2	2	99:88:77:66:55:44
Workstation	C	88:77:66:55:44:33
Switch	D	77:66:55:44:33:22
Security gateway	E	66:55:44:33:22:11

To configure MAC filtering, you need to know the MAC addresses of the devices Alice and Bob use to connect to the network, which are as follows.

Table 28 Example User MAC Addresses

USER	MAC ADDRESS
Alice	11:22:33:44:55:66
Bob	22:33:44:55:66:77

8.6.4 Configure the SERVER_1 Network

First, you will set up the SERVER_1 network which allows Alice to access secure server 1 via the network switch.

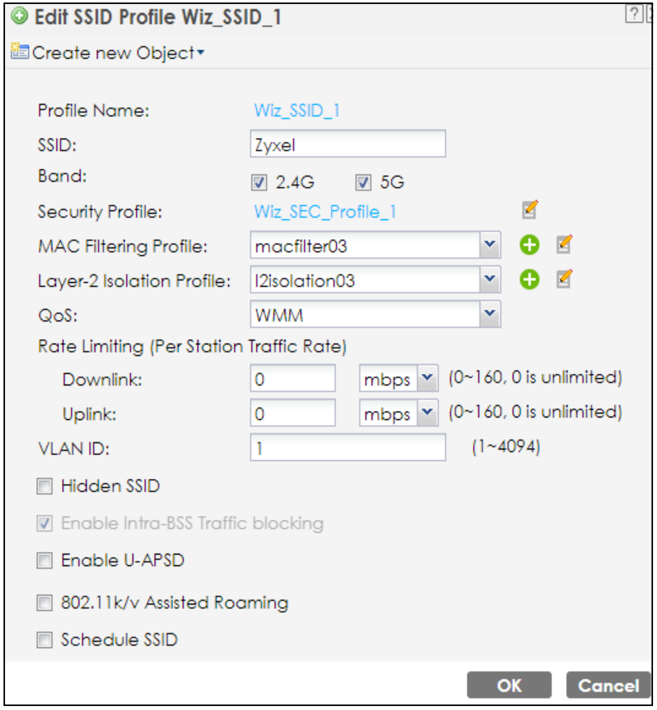
You will configure the MAC filter to restrict access to Alice alone, and then configure layer-2 isolation to allow her to access only the network router, the file server and the Internet security gateway.

Take the following steps to configure the SERVER_1 network.

1 Log into the Zyxel Device’s Web Configurator and go to **Configuration > Object > AP Profile > SSID > SSID List**. The following screen displays, showing the SSID profiles you already configured.

2 Select **SERVER_1**’s entry and click **Edit**. The following screen displays. Select **l2Isolation03** in the **L2 Isolation** field, and select **macfilter03** in the **MAC Filtering** field. Click **OK**.

Figure 60 SSID Edit Example



Edit SSID Profile Wiz_SSID_1

Create new Object

Profile Name:	Wiz_SSID_1	
SSID:	Zyxel	
Band:	☑ 2.4G ☑ 5G	
Security Profile:	Wiz_SEC_Profile_1	
MAC Filtering Profile:	macfilter03	
Layer-2 Isolation Profile:	l2isolation03	
QoS:	WMM	
Rate Limiting (Per Station Traffic Rate)		
Downlink:	0 mbps	(0~160, 0 is unlimited)
Uplink:	0 mbps	(0~160, 0 is unlimited)
VLAN ID:	1	(1~4094)

□ Hidden SSID

☑ Enable Intra-BSS Traffic blocking

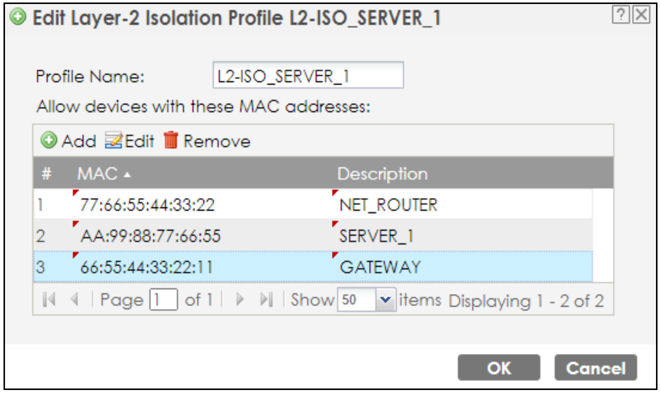
□ Enable U-APSD

□ 802.11k/v Assisted Roaming

□ Schedule SSID

3 Click the **Layer-2 Isolation** tab. When the **Layer-2 Isolation** screen appears, select **L2Isolation03**'s entry and click **Edit**. The following screen displays.

Figure 61 Layer-2 Isolation Edit



Edit Layer-2 Isolation Profile L2-ISO_SERVER_1

Profile Name: L2-ISO_SERVER_1

Allow devices with these MAC addresses:

#	MAC ▴	Description
1	77:66:55:44:33:22	NET_ROUTER
2	AA:99:88:77:66:55	SERVER_1
3	66:55:44:33:22:11	GATEWAY

4 Enter the network router's MAC Address and add a Description ("NET_ROUTER" in this case) in Set 1's entry.

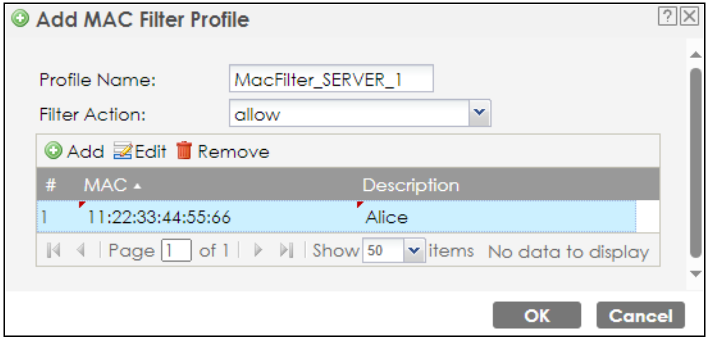
5 Enter server 1's MAC Address and add a Description ("SERVER_1" in this case) in Set 2's entry.

6 Change the Profile Name to "L2-ISO_SERVER_1" and click Apply. You have restricted users on the SERVER_1 network to access only the devices with the MAC addresses you entered.

7 Click the **MAC Filter** tab. When the **MAC Filter** screen appears, select **macfilter03**'s entry and click **Edit**.

8 Enter the MAC address of the device Alice uses to connect to the network in **Set 1**'s **MAC Address** field and enter her name in the **Description** field, as shown in the following figure. Change the **Profile Name** to "MacFilter_SERVER_1". Select **Allow** from the **Filter Action** field and click **Apply**.

Figure 62 MAC Filter Edit (SERVER_1)



Add MAC Filter Profile

Profile Name: MacFilter_SERVER_1

Filter Action: allow

#	MAC ▴	Description
1	11:22:33:44:55:66	Alice

You have restricted access to the SERVER_1 network to only the networking device whose MAC address you entered. The SERVER_1 network is now configured.

8.6.5 Configure the SERVER_2 Network

Next, you will configure the SERVER_2 network that allows Bob to access secure server 2 and the Internet.

To do this, repeat the procedure in Section 8.6.4 on page 86, substituting the following information.

Table 29 SERVER_2 Network Information

SSID Screen	
Index	4
Profile Name	SERVER_2
SSID Edit (SERVER_2) Screen	
L2 Isolation	L2Isolation04
MAC Filtering	macfilter04
Layer-2 Isolation (L2Isolation04) Screen	
Profile Name	L2-ISO_SERVER-2
Set 1	MAC Address: 77:66:55:44:33:22 Description: NET_ROUTER
Set 2	MAC Address: 99:88:77:66:55:44 Description: SERVER_2
Set 3	MAC Address: 66:55:44:33:22:11 Description: GATEWAY
MAC Filter (macfilter04) Edit Screen	
Profile Name	MacFilter_SERVER_2
Set 1	MAC Address: 22:33:44:55:66:77 Description: Bob

8.7 Check Your Settings and Test the Access Restrictions

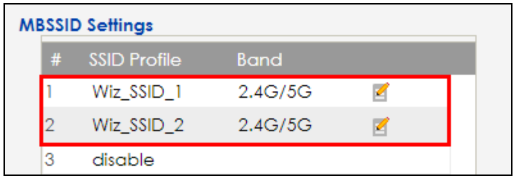
Use the following sections to ensure that your WiFi networks are set up correctly.

8.7.1 Check Settings

Take the following steps to check that the Zyxel Device is using the correct SSIDs, MAC filters and layer-2 isolation profiles.

1 Click **Configuration > Wireless**. Check that the correct SSID profiles are enabled, as shown in the following figure.

Figure 63 SSID Profiles Enabled

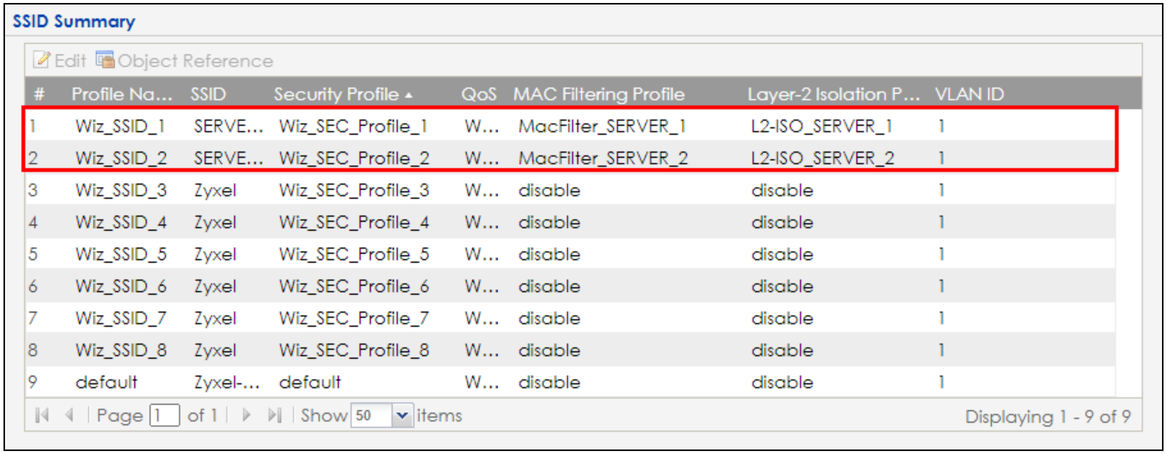


MBSSID Settings

#	SSID Profile	Band
1	Wiz_SSID_1	2.4G/5G
2	Wiz_SSID_2	2.4G/5G
3	disable	

2 Next, go to **Configuration > Object > AP Profile**. Check that each configured SSID profile uses the correct **Security**, **Layer-2 Isolation** and **MAC Filter** profiles, as shown in the following figure.

Figure 64 SSID Tab Correct Settings



SSID Summary

#	Profile Na...	SSID	Security Profile ▴	QoS	MAC Filtering Profile	Layer-2 Isolation P...	VLAN ID
1	Wiz_SSID_1	SERVE...	Wiz_SEC_Profile_1	W...	MacFilter_SERVER_1	L2-ISO_SERVER_1	1
2	Wiz_SSID_2	SERVE...	Wiz_SEC_Profile_2	W...	MacFilter_SERVER_2	L2-ISO_SERVER_2	1
3	Wiz_SSID_3	Zyxel	Wiz_SEC_Profile_3	W...	disable	disable	1
4	Wiz_SSID_4	Zyxel	Wiz_SEC_Profile_4	W...	disable	disable	1
5	Wiz_SSID_5	Zyxel	Wiz_SEC_Profile_5	W...	disable	disable	1
6	Wiz_SSID_6	Zyxel	Wiz_SEC_Profile_6	W...	disable	disable	1
7	Wiz_SSID_7	Zyxel	Wiz_SEC_Profile_7	W...	disable	disable	1
8	Wiz_SSID_8	Zyxel	Wiz_SEC_Profile_8	W...	disable	disable	1
9	default	Zyxel-...	default	W...	disable	disable	1

8.7.2 Test the Access Restrictions

Before you allow employees to use the network, you need to thoroughly test whether the setup behaves as it should. Take the following steps to do this.

1 Test the SERVER_1 network.

- Using Alice's computer and WiFi client, and the correct security settings, do the following.

  Attempt to access Server 1. You should be able to do so.

  Attempt to access the Internet. You should be able to do so.

  Attempt to access Server 2. You should be unable to do so. If you can do so, layer-2 isolation is misconfigured.

- Using Alice's computer and WiFi client, and incorrect security settings, attempt to associate with the SERVER_1 network. You should be unable to do so. If you can do so, security is misconfigured.
- Using another computer and WiFi client, but with the correct security settings, attempt to associate with the SERVER_1 network. You should be unable to do so. If you can do so, MAC filtering is misconfigured.

2 Test the SERVER_2 network.

- Using Bob's computer and WiFi client, and the correct security settings, do the following.

  Attempt to access Server 2. You should be able to do so.

  Attempt to access the Internet. You should be able to do so.

  Attempt to access Server 1. You should be unable to do so. If you can do so, layer-2 isolation is misconfigured.

- Using Bob's computer and WiFi client, and incorrect security settings, attempt to associate with the SERVER_2 network. You should be unable to do so. If you can do so, security is misconfigured.
- Using another computer and WiFi client, but with the correct security settings, attempt to associate with the SERVER_2 network. You should be unable to do so. If you can do so, MAC filtering is misconfigured.

If you cannot do something that you should be able to do, check the settings as described in Section 8.7.1 on page 88, and in the individual Security, layer-2 isolation and MAC filter profiles for the relevant network. If this does not help, see the Troubleshooting chapter in this User's Guide.

CHAPTER 9 Monitor

9.1 Overview

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

9.1.1 What You Can Do in this Chapter

- The **Network Status** screen (Section 9.3 on page 91) displays general LAN interface information and packet statistics.
- The **AP Information** > **Radio List** screen (Section 9.4 on page 93) displays statistics about the WiFi radio transmitters in the Zyxel Device.
- The **Station Info** screen (Section 9.5 on page 96) displays statistics pertaining to the associated stations.
- The **WDS Link Info** screen (Section 9.6 on page 97) displays statistics about the Zyxel Device's WDS (Wireless Distribution System) connections.
- The **Detected Device** screen (Section 9.7 on page 98) displays information about suspected rogue APs.
- The **View Log** screen (Section 9.8 on page 100) displays the Zyxel Device's current log messages. You can change the way the log is displayed, you can email the log, and you can also clear the log in this screen.

9.2 What You Need to Know

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

Rogue AP

Rogue APs are wireless access points operating in a network's coverage area that are not under the control of the network's administrators, and can open up holes in a network's security.

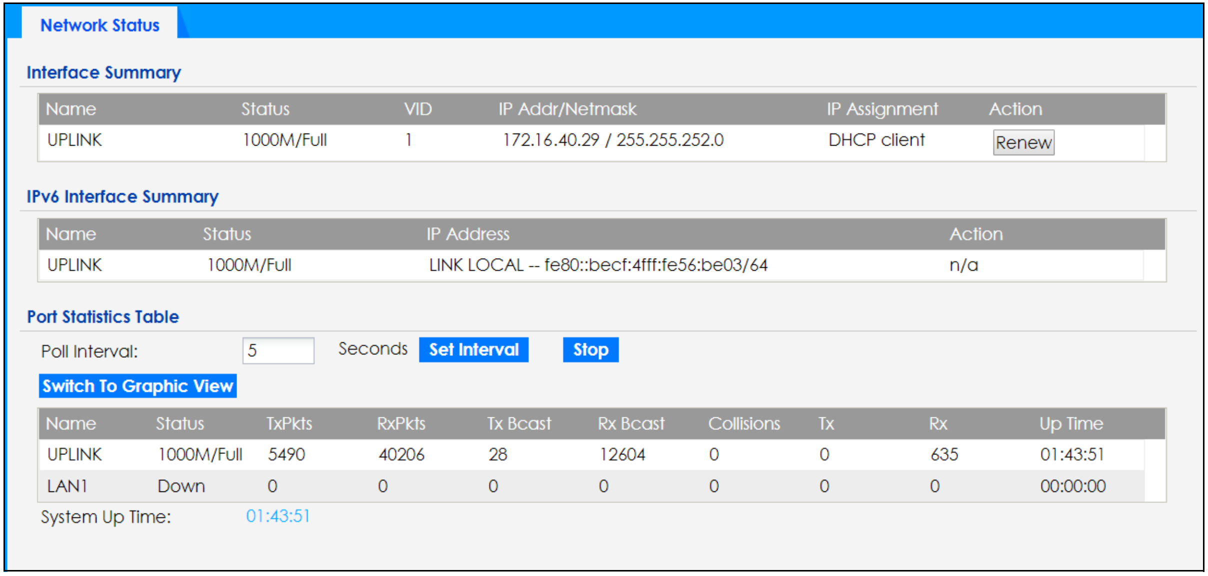
Friendly AP

Friendly APs are other wireless access points that are detected in your network, as well as any others that you know are not a threat (those from neighboring networks, for example).

9.3 Network Status

Use this screen to look at general Ethernet interface information and packet statistics. To access this screen, click **Monitor > Network Status**.

Figure 65 Monitor > Network Status



Network Status

Interface Summary

Name	Status	VID	IP Addr/Netmask	IP Assignment	Action
UPLINK	1000M/Full	1	172.16.40.29 / 255.255.252.0	DHCP client	Renew

IPv6 Interface Summary

Name	Status	IP Address	Action
UPLINK	1000M/Full	LINK LOCAL -- fe80::becf:4fff:fe56:be03/64	n/a

Port Statistics Table

Poll Interval: 5 Seconds

Name	Status	TxPkts	RxPkts	Tx Bcast	Rx Bcast	Collisions	Tx	Rx	Up Time
UPLINK	1000M/Full	5490	40206	28	12604	0	0	635	01:43:51
LAN1	Down	0	0	0	0	0	0	0	00:00:00

System Up Time: 01:43:51

The following table describes the labels in this screen.

Table 30 Monitor > Network Status

LABEL	DESCRIPTION
Interface Summary/IPv6 Interface Summary Use the **Interface Summary** section for IPv4 network settings. Use the **IPv6 Interface Summary** section for IPv6 network settings if you connect your Zyxel Device to an IPv6 network. Both sections have similar fields as described below.	
Name	This field displays the name of the physical Ethernet port on the Zyxel Device.
Status	This field displays the current status of each physical port on the Zyxel Device. **Down** - The port is not connected. **Speed / Duplex** - The port is connected. This field displays the port speed and duplex setting (**Full** or **Half**).
VID	This field displays the VLAN ID to which the port belongs.
IP Addr/ Netmask IP Address	This field displays the current IP address (and subnet mask) of the interface. If the IP address is 0.0.0.0 (in the IPv4 network) or :: (in the IPv6 network), the interface does not have an IP address yet.
IP Assignment	This field displays how the interface gets its IPv4 address. **Static** - This interface has a static IPv4 address. **DHCP Client** - This interface gets its IPv4 address from a DHCP server.
Action	Use this field to get or to update the IP address for the interface. Click **Renew** to send a new DHCP request to a DHCP server. If the interface cannot use one of these ways to get or to update its IP address, this field displays **n/a**.
Port Statistics Table	
Poll Interval	Enter how often you want this window to be updated automatically, and click **Set Interval**.

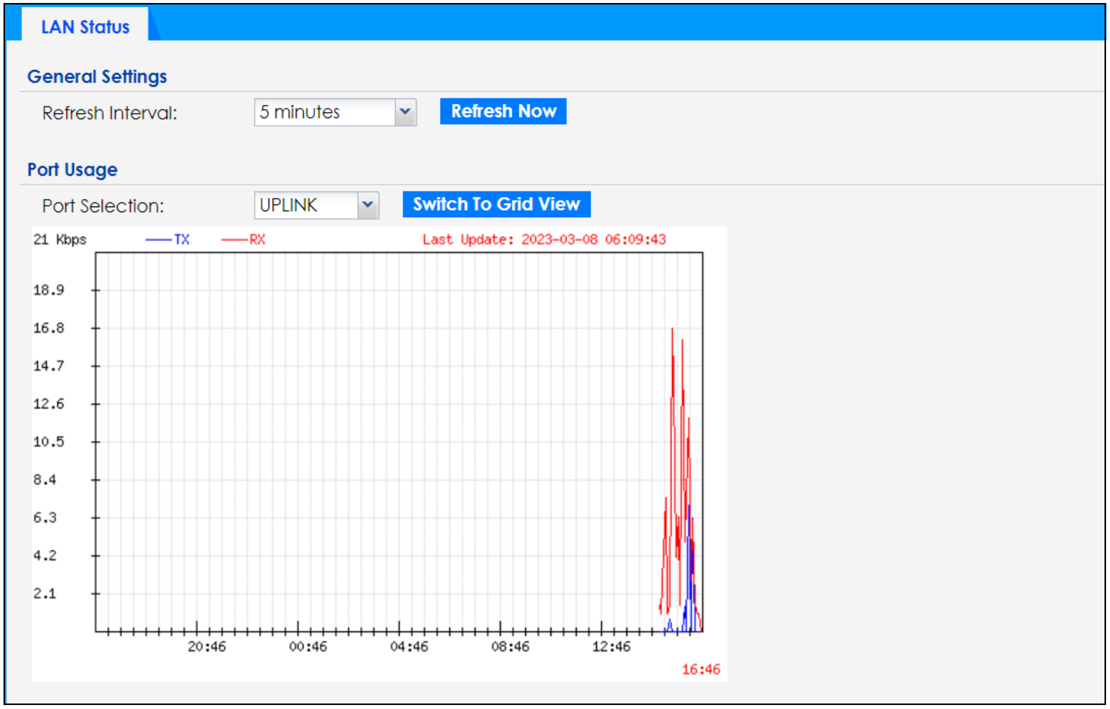
Table 30 Monitor > Network Status (continued)

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

9.3.1 Port Statistics Graph

Use the port statistics graph to look at a line graph of packet statistics for the Ethernet port. To view, click **Monitor > Network Status** and then the **Switch to Graphic View** button.

Figure 66 Monitor > Network Status > Switch to Graphic View



LAN Status

General Settings

Refresh Interval: 5 minutes

Refresh Now

Port Usage

Port Selection: UPLINK

Switch To Grid View

The following table describes the labels in this screen.

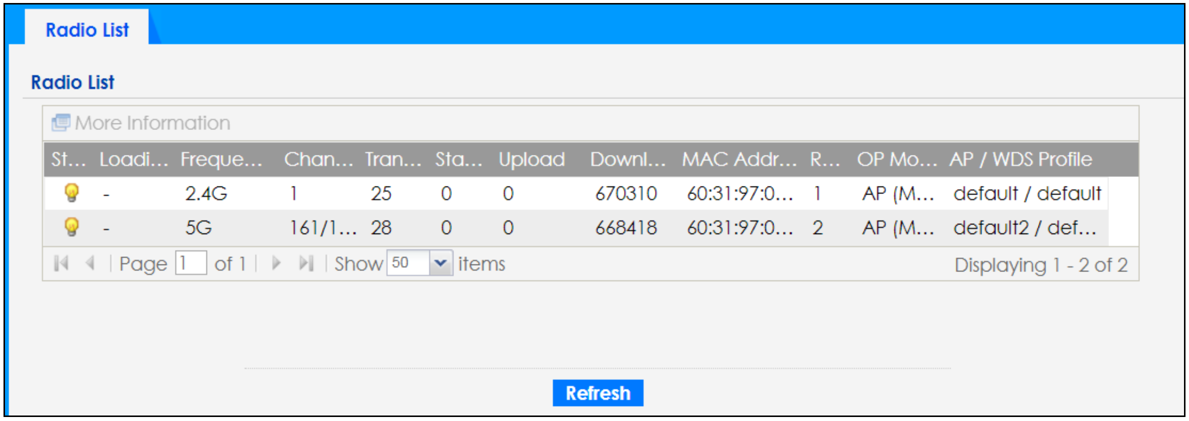
Table 31 Monitor > Network Status > Switch to Graphic View

LABEL	DESCRIPTION
General Settings	
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh Now	Click this to update the information in the window right away.
Port Usage	
Port Selection	Select the Ethernet port for which you want to view the packet statistics. This is only available for Zyxel Device models that support more than one Ethernet port.
Switch to Grid View	Click this to display the port statistics as a table.
Kbps/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.
TX	This line represents traffic transmitted from the Zyxel Device on the physical port since it was last connected.
RX	This line represents the traffic received by the Zyxel Device on the physical port since it was last connected.
Last Update	This field displays the date and time the information in the window was last updated.

9.4 Radio List

Use this screen to view statistics for the Zyxel Device's WiFi radio transmitters. To access this screen, click **Monitor > Wireless > AP Information > Radio List**.

Figure 67 Monitor > Wireless > AP Information > Radio List



Radio List

Radio List

More Information

St...	Loadi...	Freque...	Chan...	Tran...	Sta...	Upload	Downl...	MAC Addr...	R...	OP Mo...	AP / WDS Profile
💡	-	2.4G	1	25	0	0	670310	60:31:97:0...	1	AP (M...	default / default
💡	-	5G	161/1...	28	0	0	668418	60:31:97:0...	2	AP (M...	default2 / def...

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

Refresh

The following table describes the labels in this screen.

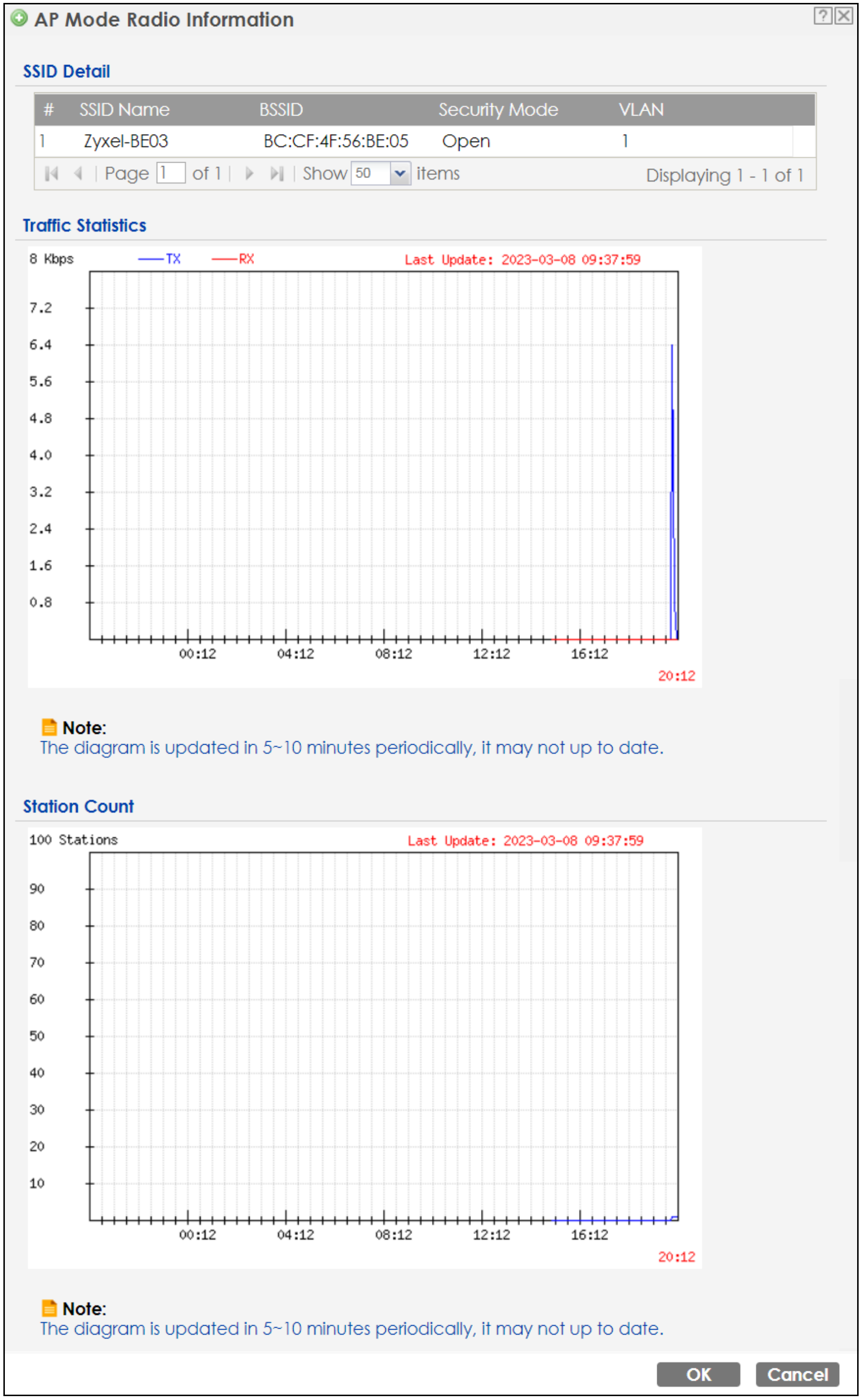
Table 32 Monitor > Wireless > AP Information > Radio List

LABEL	DESCRIPTION
More Information	Click this to view additional information about the selected radio's wireless traffic and station count. Information spans a 24 hour period.
Status	This displays whether or not the radio is enabled.
Frequency Band	This indicates the wireless frequency band currently being used by the radio.
Channel	This indicates the radio's channel ID.
Transmit Power	This displays the output power of the radio.
Station	This displays the number of WiFi clients connected to this radio on the Zyxel Device.
Upload	This displays the total number of packets received by the radio.
Download	This displays the total number of packets transmitted by the radio.
Loading	This indicates the AP's load balance status (**UnderLoad** or **OverLoad**) when load balancing is enabled on the Zyxel Device. Otherwise, it shows **-** when load balancing is disabled. This is only available if your Zyxel Device supports **Load Balancing**. See Section 1.2 on page 14 for the supported models list.
MAC Address	This displays the MAC address of the radio.
Radio	This indicates the radio number on the Zyxel Device to which it belongs.
OP Mode	This indicates the radio's operating mode. Operating modes are **AP (MBSSID)**, **Root AP** or **Repeater**.
AP/WDS Profile	This indicates the AP profile name and WDS profile name to which the radio belongs.
Channel Utilization	This indicates 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.

9.4.1 AP Mode Radio Information

This screen allows you to view a selected radio's SSID details, wireless traffic statistics and station count for the preceding 24 hours. To access this window, select a radio and click the **More Information** button in the **Radio List** screen.

Figure 68 Monitor > Wireless > AP Information > Radio List > More Information



SSID Detail

#	SSID Name	BSSID	Security Mode	VLAN
1	Zyxel-BE03	BC:CF:4F:56:BE:05	Open	1

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

Traffic Statistics

Last Update: 2023-03-08 09:37:59

Note:
The diagram is updated in 5~10 minutes periodically, it may not up to date.

Station Count

Last Update: 2023-03-08 09:37:59

Note:
The diagram is updated in 5~10 minutes periodically, it may not up to date.

The following table describes the labels in this screen.

Table 33 Monitor > Wireless > AP Information > Radio List > More Information

LABEL	DESCRIPTION
SSID Detail	This list shows information about all the WiFi clients that have connected to the specified radio over the preceding 24 hours.
#	This is the items sequential number in the list. It has no bearing on the actual data in this list.

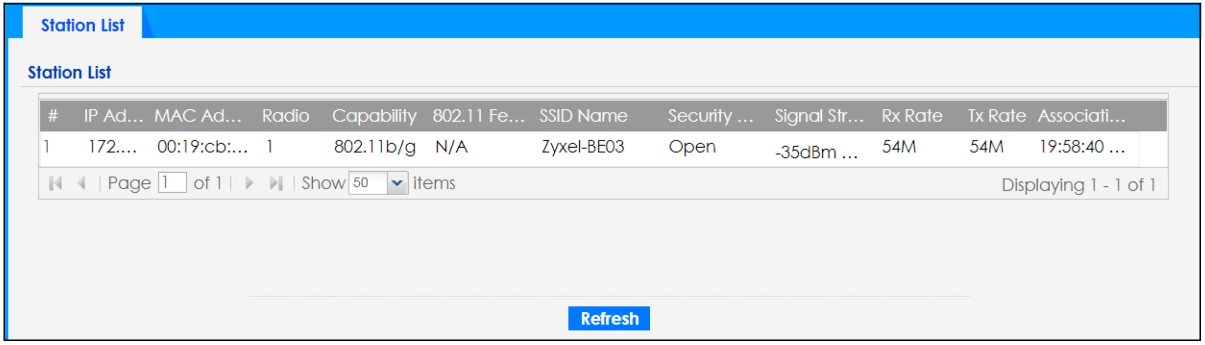
Table 33 Monitor > Wireless > AP Information > Radio List > More Information (continued)

LABEL	DESCRIPTION
SSID Name	This displays an SSID associated with this radio. There can be up to eight maximum.
BSSID	This displays a BSSID associated with this radio. The BSSID is tied to the SSID.
Security Mode	This displays the security mode in which the SSID is operating.
VLAN	This displays the VLAN ID associated with the SSID.
Traffic Statistics	This graph displays the overall traffic information of the radio over the preceding 24 hours.
Kbps/Mbps	This y-axis represents the amount of data moved across this radio in megabytes per second.
Time	This x-axis represents the amount of time over which the data moved across this radio.
TX	This line represents traffic transmitted from the Zyxel Device on this radio.
RX	This line represents the traffic received by the Zyxel Device on this radio.
Station Count	This graph displays the connected station information of the radio over the preceding 24 hours
Stations	The y-axis represents the number of connected stations.
Time	The x-axis shows the time period over which a station was connected.
Last Update	This field displays the date and time the information in the window was last updated.
OK	Click this to close this window.
Cancel	Click this to close this window.

9.5 Station List

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

Figure 69 Monitor > Wireless > Station Info



Station List

#	IP Ad...	MAC Ad...	Radio	Capability	802.11 Fe...	SSID Name	Security ...	Signal Str...	Rx Rate	Tx Rate	Associati...
1	172....	00:19:cb:...	1	802.11b/g	N/A	Zyxel-BE03	Open	-35dBm ...	54M	54M	19:58:40 ...

The following table describes the labels in this screen.

Table 34 Monitor > Wireless > Station Info

LABEL	DESCRIPTION
#	This is the station’s index number in this list.
IP Address	This is the station’s IP address.
Band	This is the frequency band to which the station is connected.
MAC Address	This is the station’s MAC address.
Radio	This is the radio number on the Zyxel Device to which the station is connected.

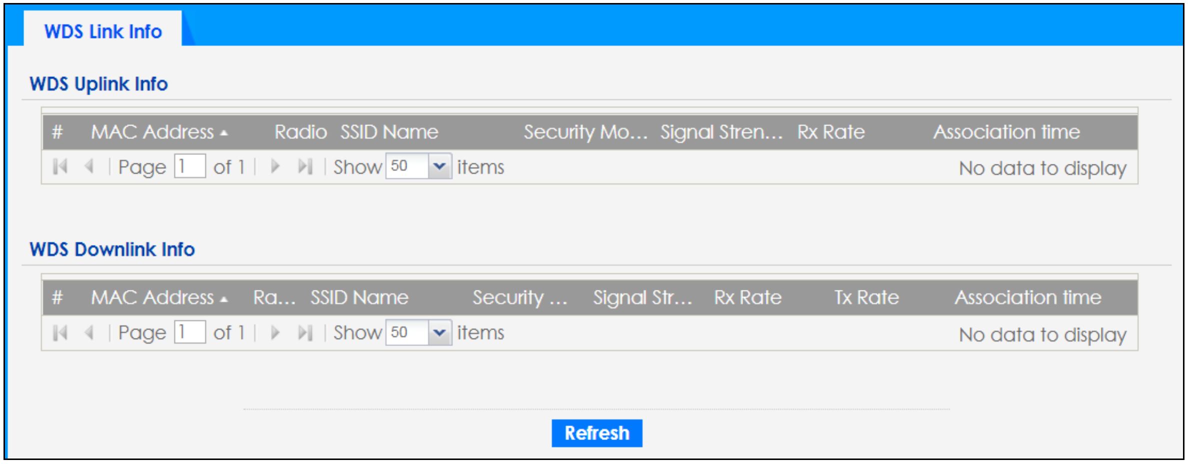
Table 34 Monitor > Wireless > Station Info (continued)

LABEL	DESCRIPTION
802.11 Features	This displays whether the station supports IEEE802.11r, IEEE 802.11k, IEEE 802.11v or none of the above (**N/A**).
Capability	This displays the supported standard currently being used by the station or the standards supported by the station.
SSID Name	This indicates the name of the WiFi network to which the station is connected. A single AP can have multiple SSIDs or networks.
Security Mode	This indicates which secure encryption methods is being used by the station to connect to the network.
Signal Strength	This is the RSSI (Received Signal Strength Indicator) of the station's WiFi connection.
Rx Rate	This is the maximum reception rate of the station.
Tx Rate	This is the maximum transmission rate of the station.
Association Time	This displays the time the station first associated with the Zyxel Device's WiFi network.
Refresh	Click this to refresh the items displayed on this page.

9.6 WDS Link Info

Use this screen to view the WDS traffic statistics between the Zyxel Device and a root AP or repeaters. See Section 1.3 on page 18 to know more about WDS. Click **Monitor > Wireless > WDS Link Info** to access this screen.

Figure 70 Monitor > Wireless > WDS Link Info


WDS Link Info
WDS Uplink Info
# MAC Address Radio SSID Name Security Mo... Signal Stren... Rx Rate Association time
Page 1 of 1 Show 50 items
No data to display
WDS Downlink Info
# MAC Address Ra... SSID Name Security ... Signal Str... Rx Rate Tx Rate Association time
Page 1 of 1 Show 50 items
No data to display
Refresh

The following table describes the labels in this screen.

Table 35 Monitor > Wireless > WDS Link Info

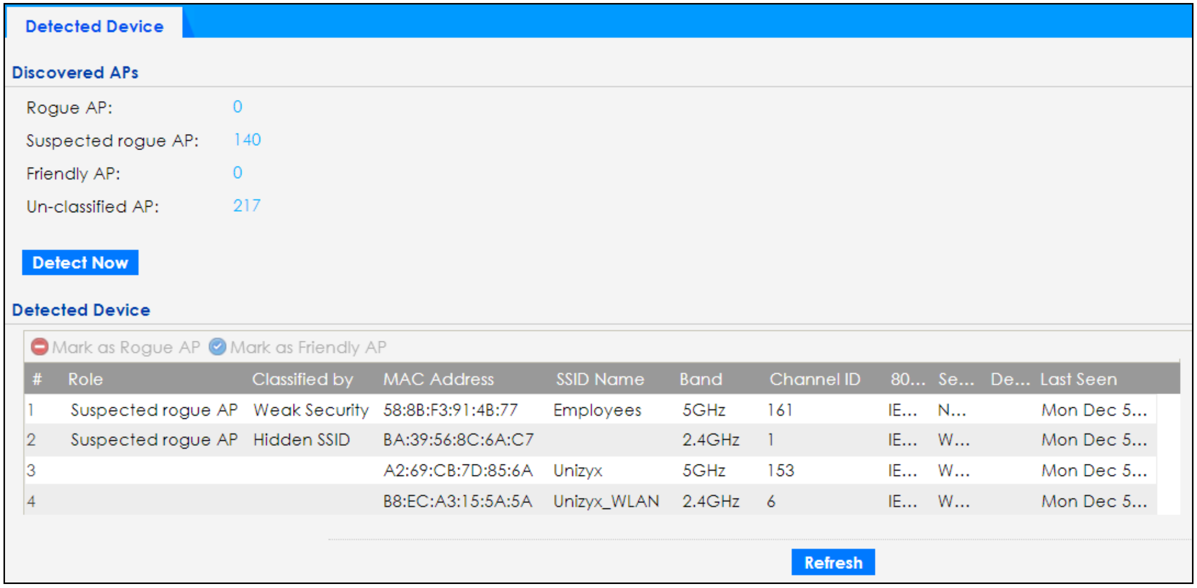
LABEL	DESCRIPTION
WDS Uplink/ Downlink Info	**Uplink** refers to the WDS link from the repeaters to the root AP. **Downlink** refers to the WDS link from the root AP to the repeaters. When the Zyxel Device is in root AP mode and connected to a repeater, only the downlink information is displayed. When the Zyxel Device is in repeater mode and connected to a root AP directly or via another repeater, the uplink information is displayed. When the Zyxel Device is in repeater mode and connected to a root AP and other repeater(s), both the uplink and downlink information would be displayed.
#	This is the index number of the root AP or repeater in this list.
MAC Address	This is the MAC address of the root AP or repeater to which the Zyxel Device is connected using WDS.
Band	This is the frequency band of the WiFi network to which the Zyxel Device is connected using WDS.
Radio	This is the radio number on the root AP or repeater to which the Zyxel Device is connected using WDS.
SSID Name	This indicates the name of the WiFi network to which the Zyxel Device is connected using WDS.
Security Mode	This indicates which secure encryption methods is being used by the Zyxel Device to connect to the root AP or repeater using WDS.
Signal Strength	This is the RSSI (Received Signal Strength Indicator) of the wireless connection in WDS.
Tx Rate	This is the maximum transmission rate of the root AP or repeater to which the Zyxel Device is connected using WDS.
Rx Rate	This is the maximum reception rate of the root AP or repeater to which the Zyxel Device is connected using WDS.
Association Time	This displays the time the Zyxel Device first associated with the wireless network using WDS.
Refresh	Click this to refresh the items displayed on this page.

9.7 Detected Device

Use this screen to view information about surrounding APs which you could mark as **Rogue** or **Friendly**. Click **Monitor > Wireless > Detected Device** to access this screen. For more information about Rogue APs, see Section 11.3 on page 122.

Note: Turn on **Enable Rogue AP Detection** in the **Configuration > Wireless > Rogue AP** screen to detect other APs.

Figure 71 Monitor > Wireless > Detected Device



Discovered APs

Rogue AP:	0
Suspected rogue AP:	140
Friendly AP:	0
Un-classified AP:	217

Detected Device

#	Role	Classified by	MAC Address	SSID Name	Band	Channel ID	80...	Se...	De...	Last Seen
1	Suspected rogue AP	Weak Security	58:8B:F3:91:4B:77	Employees	5GHz	161	IE...	N...		Mon Dec 5...
2	Suspected rogue AP	Hidden SSID	BA:39:56:8C:6A:C7		2.4GHz	1	IE...	W...		Mon Dec 5...
3			A2:69:CB:7D:85:6A	Unizyx	5GHz	153	IE...	W...		Mon Dec 5...
4			B8:EC:A3:15:5A:5A	Unizyx_WLAN	2.4GHz	6	IE...	W...		Mon Dec 5...

The following table describes the labels in this screen.

Table 36 Monitor > Wireless > Detected Device

LABEL	DESCRIPTION
Discovered APs	
Rogue AP	This shows how many devices are detected as rogue APs.
Suspected rogue AP	This shows how many devices are detected as possible rogue APs based on the classification rule(s) in Section 11.3 on page 122.
Friendly AP	This shows how many devices are detected as friendly APs.
Un-classified AP	This shows how many devices are detected, but have not been classified as either Rogue or Friendly by the Zyxel Device.
Detect Now	Click this button for the Zyxel Device to scan for APs in the network.
Detected Device	
Mark as Rogue AP	Click this button to mark the selected AP as a rogue AP. For more on managing rogue APs, see the **Configuration > Wireless > Rogue AP** screen (Section 11.3 on page 122).
Mark as Friendly AP	Click this button to mark the selected AP as a friendly AP. For more on managing friendly APs, see the **Configuration > Wireless > Rogue AP** screen (Section 11.3 on page 122).
#	This is the detected device's index number in this list.
Role	This indicates the detected device's role (such as friendly or rogue).
Classified by	This indicates the detected device's classification rule.
MAC Address	This indicates the detected device's MAC address.
SSID Name	This indicates the detected device's SSID.
Band	This is the frequency band to which the station is connected.
Channel ID	This indicates the detected device's channel ID.
802.11 Mode	This indicates the 802.11 mode (a/b/g/n/ac/ax) transmitted by the detected device.
Security	This indicates the encryption method (if any) used by the detected device.
Description	This displays the detected device's description. For more on managing friendly and rogue APs, see the **Configuration > Wireless > Rogue AP** screen (Section 11.3 on page 122).

Table 36   Monitor > Wireless > Detected Device (continued)

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

9.8 View Log

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

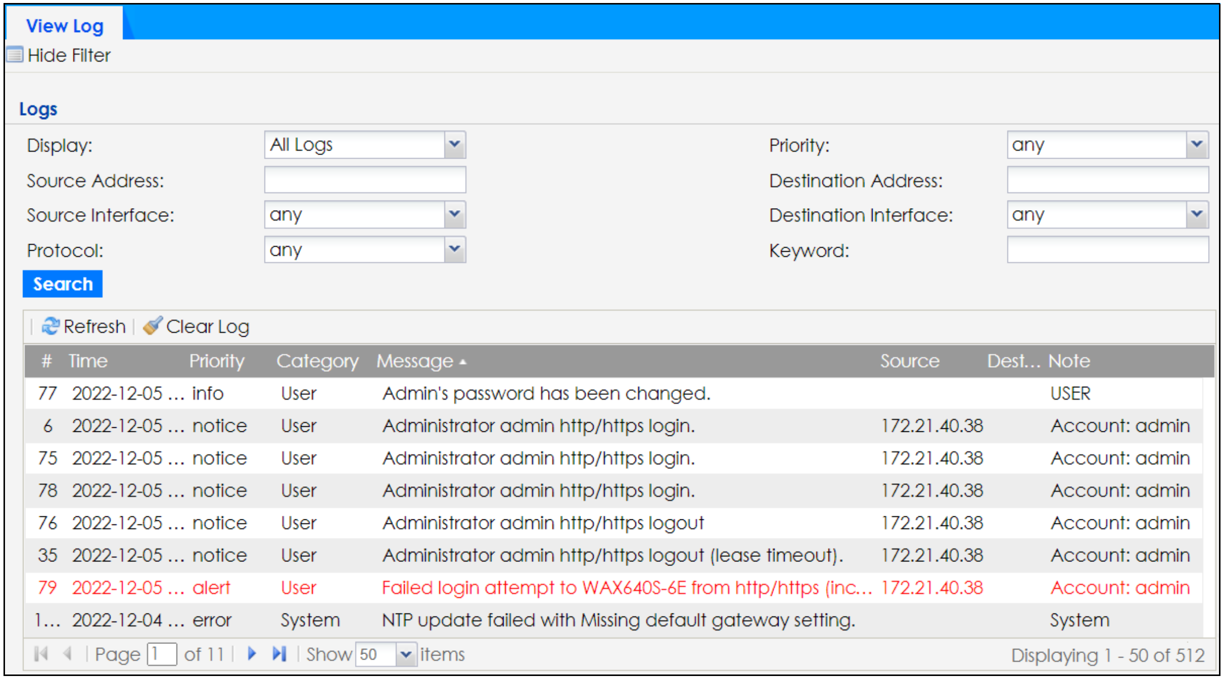
To access this screen, click **Monitor > Log**. The log is displayed in the following screen.

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

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 once you click **Search**. If you leave the **View Log** screen and return to it later, the last filter settings would still apply.

Figure 72   Monitor > Log > View Log



Logs

Display:	All Logs	Priority:	any
Source Address:		Destination Address:	
Source Interface:	any	Destination Interface:	any
Protocol:	any	Keyword:	

#	Time	Priority	Category	Message ▴	Source	Dest...	Note
77	2022-12-05 ...	info	User	Admin's password has been changed.			USER
6	2022-12-05 ...	notice	User	Administrator admin http/https login.	172.21.40.38		Account: admin
75	2022-12-05 ...	notice	User	Administrator admin http/https login.	172.21.40.38		Account: admin
78	2022-12-05 ...	notice	User	Administrator admin http/https login.	172.21.40.38		Account: admin
76	2022-12-05 ...	notice	User	Administrator admin http/https logout	172.21.40.38		Account: admin
35	2022-12-05 ...	notice	User	Administrator admin http/https logout (lease timeout).	172.21.40.38		Account: admin
79	2022-12-05 ...	alert	User	Failed login attempt to WAX640S-6E from http/https (inc...	172.21.40.38		Account: admin
1...	2022-12-04 ...	error	System	NTP update failed with Missing default gateway setting.			System

Page 1 of 11 | Show 50 items   Displaying 1 - 50 of 512

The following table describes the labels in this screen.

Table 37 Monitor > Log > View Log

LABEL	DESCRIPTION
Show Filter / Hide Filter	Click this button to show or hide the filter settings. The **Priority**, **Source Address**, **Destination Address**, **Source Interface**, **Destination Interface**, **Protocol**, **Keyword**, and **Search** fields are only available if the filter settings are shown.
Display	Select the category of log message(s) you want to view. You can also view **All Logs** at one time, or you can view the **Debug Log**.
Priority	This displays when you show the filter. Select the priority of log messages to display. The log displays the log messages with this priority or higher. Choices are: **any**, **emerg**, **alert**, **crit**, **error**, **warn**, **notice**, and **info**, from highest priority to lowest priority. This field is read-only if the **Category** is **Debug Log**.
Source Address	This displays when you show the filter. Type the source IP address of the incoming packet that generated the log message. Do not include the port in this filter.
Destination Address	This displays when you show the filter. Type the IP address of the destination of the incoming packet when the log message was generated. Do not include the port in this filter.
Source Interface	This displays when you show the filter. Select the source interface of the packet that generated the log message.
Destination Interface	This displays when you show the filter. Select the destination interface of the packet that generated the log message.
Protocol	This displays when you show the filter. Select a service protocol whose log messages you would like to see.
Keyword	This displays when you show the filter. Type a keyword to look for in the **Message**, **Source**, **Destination** and **Note** fields. If a match is found in any field, the log message is displayed. You can use up to 63 alphanumeric characters and the underscore, as well as punctuation marks ()' ,:;?! +-*/= #$% @ ; the period, double quotes, and brackets are not allowed.
Search	This displays when you show the filter. Click this button to update the log using the current filter settings.
Email Log Now	Click this button to send log messages to the **Active** email addresses specified in the **Send Log To** field on the **Configuration > Log & Report > Log Settings** screen.
Refresh	Click this to update the list of logs.
Clear Log	Click this button to clear the whole log, regardless of what is currently displayed on the screen.
#	This field is a sequential value, and it is not associated with a specific log message.
Time	This field displays the time the log message was recorded.
Priority	This field displays the priority of the log message. It has the same range of values as the **Priority** field above.
Category	This field displays the log that generated the log message. It is the same value used in the **Display** and (other) **Category** fields.
Message	This field displays the reason the log message was generated. The text "[count=*x*]", where *x* is a number, appears at the end of the **Message** field if log consolidation is turned on and multiple entries were aggregated to generate into this one.
Source	This field displays the source IP address and the port number in the event that generated the log message.
Source Interface	This field displays the source interface of the packet that generated the log message.
Destination	This field displays the destination IP address and the port number of the event that generated the log message.
Destination Interface	This field displays the destination interface of the packet that generated the log message.
Protocol	This field displays the service protocol in the event that generated the log message.
Note	This field displays any additional information about the log message.

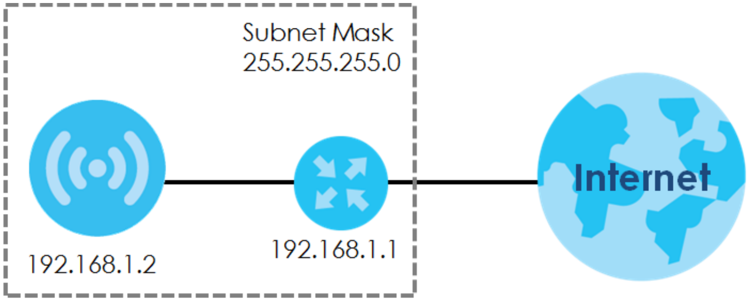
CHAPTER 10
Network

10.1 Overview

This chapter describes how you can configure the management IP address and VLAN settings of your Zyxel Device.

The Internet Protocol (IP) address identifies a device on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Figure 73 IP Setup



The figure above illustrates one possible setup of your Zyxel Device. The gateway IP address is 192.168.1.1 and the managed IP address of the Zyxel Device is 192.168.1.2 (default), but if the Zyxel Device is assigned an IP address by a DHCP server, the default (192.168.1.2) will not be used. The gateway and the Zyxel Device must belong in the same IP subnet to be able to communicate with each other.

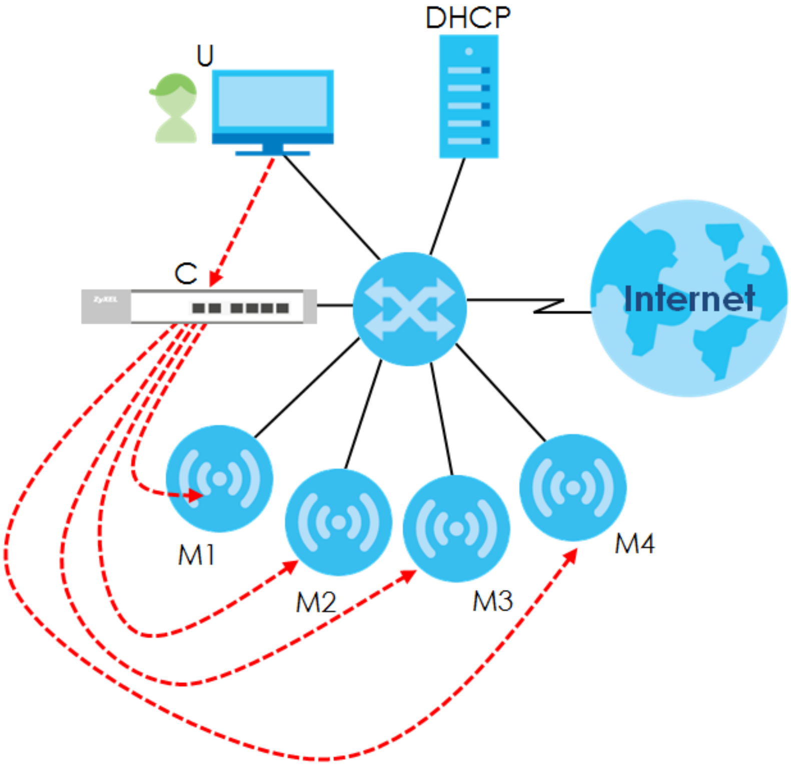
10.1.1 AP Controller Management

This discusses using the Zyxel Device with an AP Controller. AP Controllers, such as the ZyWALL ATP, ZyWALL VPN, USG FLEX, and NXC, use Control And Provisioning of Wireless Access Points (CAPWAP) to push firmware and/or configurations to the APs that they manage.

Note: Not all models support AC management. See Section 1.1 on page 13 for more information.

The following figure illustrates a wireless network managed by an AC. You (**U**) configure the AC (**C**), which then automatically updates the configurations of the managed APs (**M1** ~ **M4**).

Figure 74 AC managed Network Example



Note: The Zyxel Device can be a standalone device or be managed by an AC.

AC Discovery and Management

The link between AC Discovery-enabled access points proceeds as follows:

1. A Zyxel Device with **AC Discovery** enabled joins a wired network (receives a dynamic IP address).
2. The Zyxel Device sends out a discovery request, looking for an AC.
3. If there is an AC on the network, it receives the discovery request. If the AC, for example, a ZyWALL ATP, is in **Manual** mode, it adds the details of the Zyxel Device to its **Unmanaged Access Points** list, and you decide which available APs to manage. If the AC is in **Always Accept** mode, it automatically adds the Zyxel Device to its **Managed Access Points** list and provides the managed Zyxel Device with default configuration information, as well as securely transmitting the DTLS pre-shared key. The managed Zyxel Device is ready for association with WiFi clients.

Managed AP Finds the Controller

A managed Zyxel Device can find the controller in one of the following ways:

- Manually specify the controller's IP address in the Web Configurator's **AC Discovery** screen.
- Get the controller's IP address from a DHCP server with the controller's IP address configured as option 138.
- Get the controller's IP address from a DNS server SRV (Service) record.
- Broadcasting to discover the controller within the broadcast domain.

Note: The AC needs to have a static IP address. If it is a DHCP client, set the DHCP server to reserve an IP address for the AC.

AC management and IP Subnets

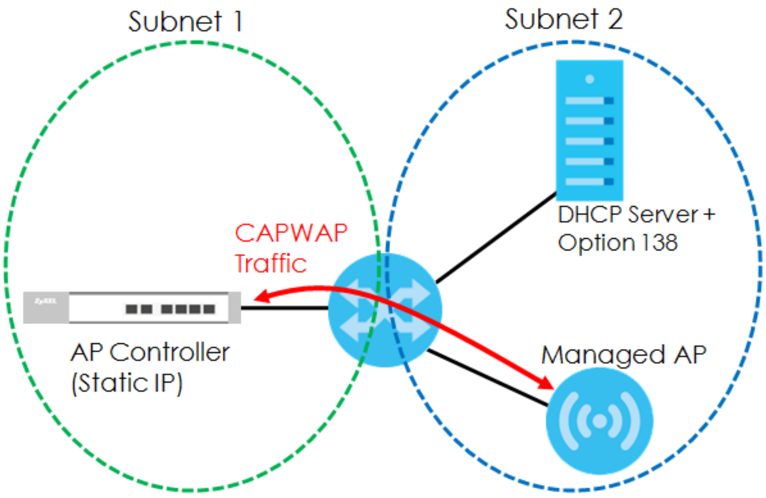
By default, CAPWAP works only between Zyxel Devices with IP addresses in the same subnet.

However, you can configure the Zyxel Device and the AC to use CAPWAP with IP addresses in different subnets by doing the following.

- Activate DHCP. Your network's DHCP server must support option 138 defined in RFC 5415.
- Configure DHCP option 138 with the IP address of the AC on your network.

DHCP Option 138 allows the management request (from the Zyxel Device) to reach the AC in a different subnet, as shown in the following figure.

Figure 75 CAPWAP and DHCP Option 138



Notes on AC Management

This section lists some additional features of Zyxel's implementation of the CAPWAP protocol.

- When the AC uses its internal Remote Authentication Dial In User Service (RADIUS) server, managed Zyxel Devices also use the AC's authentication server to authenticate WiFi clients.
- If an Zyxel Device's link to the AC is broken, the Zyxel Device continues to use the WiFi settings with which it was last provided.

10.1.2 What You Can Do in this Chapter

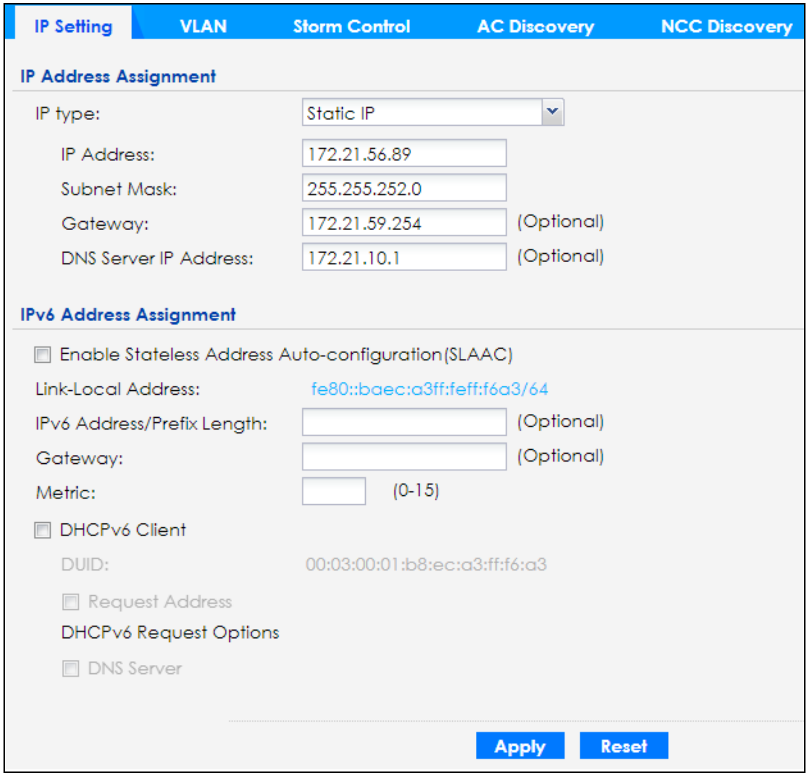
- The **IP Setting** screen (Section 10.2 on page 105) configures the Zyxel Device's LAN IP address.
- The **VLAN** screen (Section 10.3 on page 106) configures the Zyxel Device's VLAN settings.
- The **Storm Control** screen (Section 10.4 on page 111) turns on or off the traffic storm control feature on the Zyxel Device.
- The **AC Discovery** screen (Section 10.5 on page 112) configures the Zyxel Device's AP Controller (AC) settings.

- The **NCC Discovery** screen (Section 10.6 on page 113) configures the Zyxel Device's Nebula Control Center (NCC) discovery settings.

10.2 IP Setting

Use this screen to configure the IP address for your Zyxel Device. To access this screen, click **Configuration > Network > IP Setting**.

Figure 76 Configuration > Network > IP Setting



IP Address Assignment

IP type: Static IP

IP Address: 172.21.56.89

Subnet Mask: 255.255.252.0

Gateway: 172.21.59.254 (Optional)

DNS Server IP Address: 172.21.10.1 (Optional)

IPv6 Address Assignment

□ Enable Stateless Address Auto-configuration(SLAAC)

Link-Local Address: fe80::baec:a3ff:feff:f6a3/64

IPv6 Address/Prefix Length: (Optional)

Gateway: (Optional)

Metric: (0-15)

□ DHCPv6 Client

DUID: 00:03:00:01:b8:ec:a3:ff:f6:a3

□ Request Address

DHCPv6 Request Options

□ DNS Server

Each field is described in the following table.

Table 38 Configuration > Network > IP Setting

LABEL	DESCRIPTION
IP Address Assignment	
IP Type	Select **DHCP** to make the interface a DHCP client and automatically get the IP address, subnet mask, gateway and DNS Server IP Address from a DHCP server. Select **Static IP** to specify the IP address, subnet mask, gateway and DNS server IP address manually.
Use Fixed DNS Server IP Address	Select this if you have a preferred DNS server that you want to specify manually even if the IP type is DHCP. Setting a fixed DNS server IP address may help if you experience unreliable DNS resolution.
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.

Table 38 Configuration > Network > IP Setting (continued)

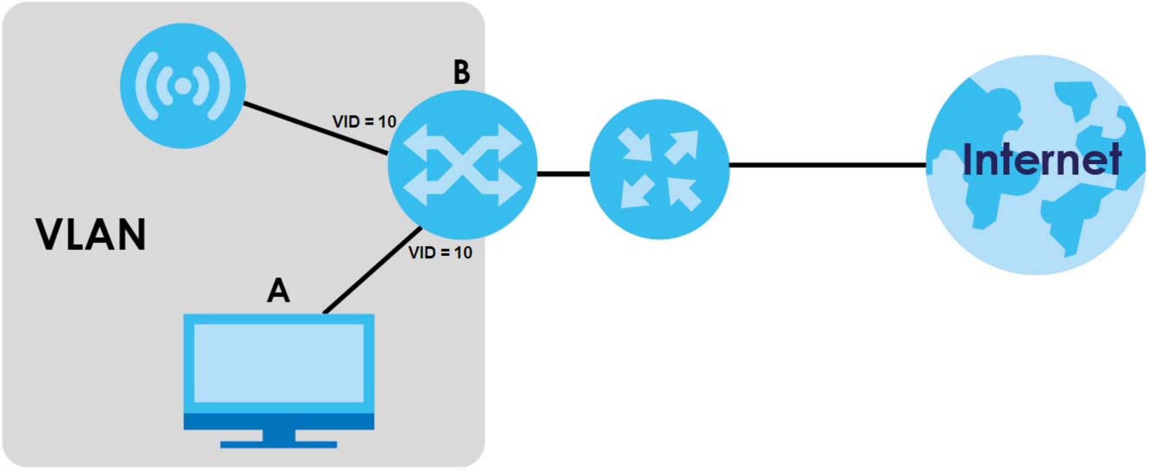
LABEL	DESCRIPTION
Gateway	Enter the IP address of the gateway. The Zyxel Device sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
DNS Server IP Address	Enter the IP address of the DNS server.
IPv6 Address Assignment	
Enable Stateless Address Auto-configuration (SLAAC)	Select this to enable IPv6 stateless auto-configuration on the Zyxel Device. The Zyxel Device will generate an IPv6 address itself from a prefix obtained from an IPv6 router in the network.
Link-Local Address	This displays the IPv6 link-local address and the network prefix that the Zyxel Device generates itself for the LAN interface.
IPv6 Address/Prefix Length	Enter the IPv6 address and the prefix length for the LAN interface if you want to use a static IP address. This field is optional. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Gateway	Enter the IPv6 address of the default outgoing gateway using colon (:) hexadecimal notation.
Metric	Enter the priority of the gateway (if any) on the LAN interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first. Enter zero to set the metric to 1024 for IPv6.
DHCPv6 Client	Select this option to set the Zyxel Device to act as a DHCPv6 client.
DUID	This field displays the DHCP Unique IDentifier (DUID) of the Zyxel Device, which is unique and used for identification purposes when the Zyxel Device is exchanging DHCPv6 messages with others. See Appendix B on page 302 for more information.
Request Address	Select this option to get an IPv6 address from the DHCPv6 server.
DHCPv6 Request Options	Select the following DHCPv6 options to determine what additional information to get from the DHCPv6 server.
DNS Server	Select this option to obtain the IP address of the DNS server.
NTP Server	Select this option to obtain the IP address of the NTP server.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

10.3 VLAN

This section discusses how to configure the Zyxel Device's VLAN settings.

Note: Mis-configuring the management VLAN settings on your Zyxel Device can make it inaccessible. If this happens, you will have to reset the Zyxel Device.

Figure 77 Management VLAN Setup



In the figure above, to access and manage the Zyxel Device from computer **A**, the Zyxel Device and switch **B**'s ports to which computer **A** and the Zyxel Device are connected should be in the same VLAN.

A Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

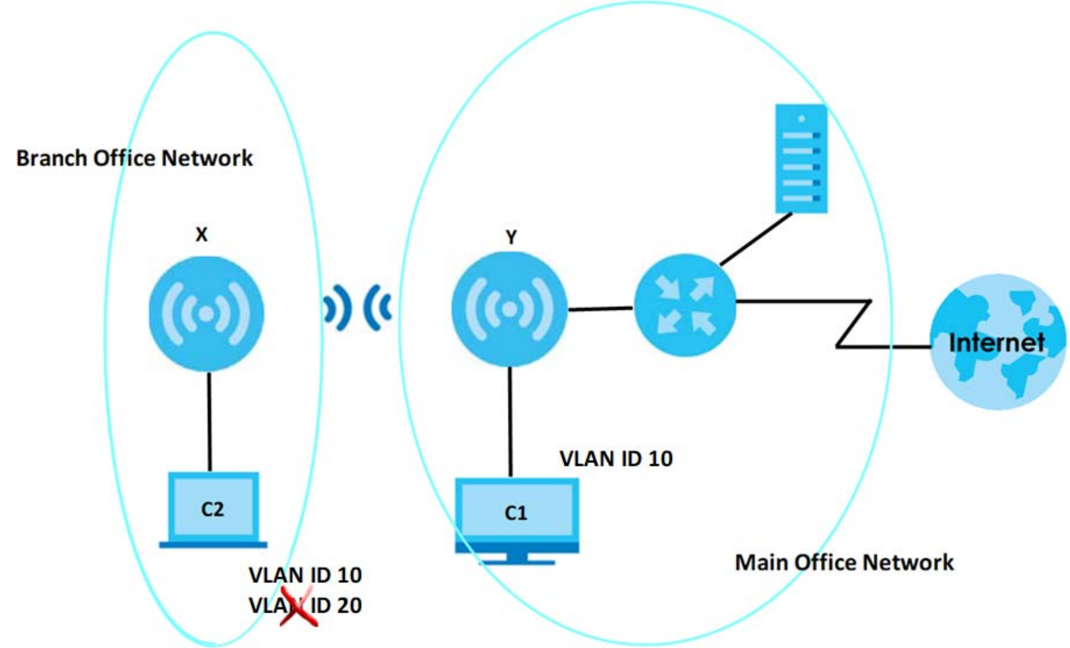
VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Wireless Bridge VLAN ID

Wireless bridge VLAN allows you to have clients in different WiFi networks appear to be in the same virtual network using VLAN IDs. VLAN IDs are sent across the wireless bridge so that only clients with the same VLAN ID receive that network traffic. See Section 1.3 on page 18 for more information on the wireless bridge.

In the figure below, a client (**C2**) in the branch office wants to connect to the main office (**Y**). The branch office client (**C2**) can connect to the main office network using the **VLAN ID 10**. However, the branch office client (**C2**) cannot connect to the to the main office network using the **VLAN ID 20** because that VLAN ID does not exist in the main office network. To bridge the branch office network and the main office network, the VLAN IDs you set on the Zyxel Device (**X**) should be the same as the VLAN IDs you set on the root AP (**Y**).

Figure 78 Wireless Bridge VLAN ID Example

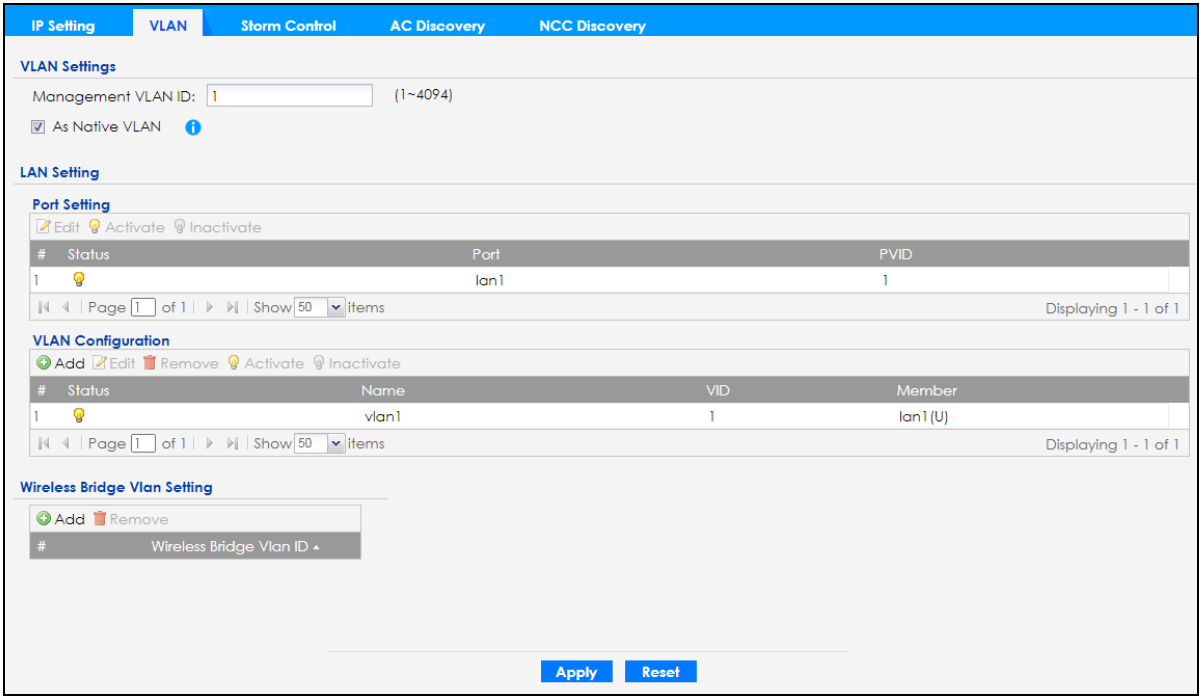


IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

Use this screen to configure the VLAN settings for your Zyxel Device. To access this screen, click **Configuration > Network > VLAN**.

Figure 79 Configuration > Network > VLAN (for Zyxel Device with multiple Ethernet ports)



VLAN Settings

Management VLAN ID: 1 (1~4094)

☑ As Native VLAN

LAN Setting

Port Setting

#	Status	Port	PVID
1	💡	lan1	1

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

VLAN Configuration

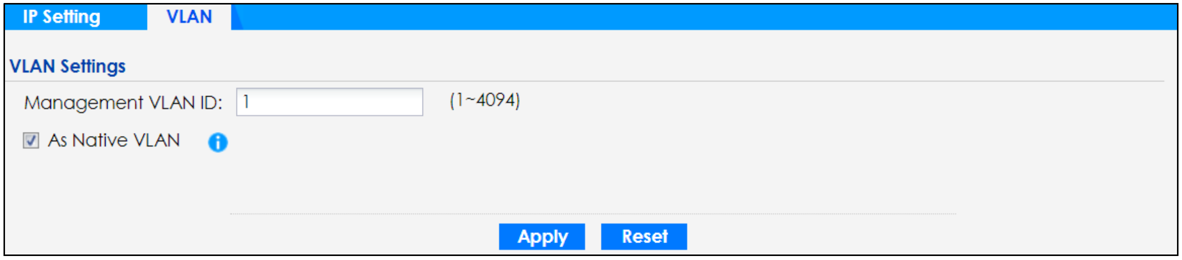
#	Status	Name	VID	Member
1	💡	vlan1	1	lan1(U)

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

Wireless Bridge Vlan Setting

#	Wireless Bridge Vlan ID ▴

Figure 80 Configuration > Network > VLAN (for Zyxel Device with one Ethernet port)



VLAN Settings

Management VLAN ID: 1 (1~4094)

☑ As Native VLAN

Each field is described in the following table.

Table 39 Configuration > Network > VLAN

LABEL	DESCRIPTION
VLAN Settings	
Management VLAN ID	Enter a VLAN ID for the Zyxel Device. The range is 1–4094.
As Native VLAN	Select this option to treat the **Management VLAN ID** as a VLAN created on the Zyxel Device and not one assigned to it from outside the network. Outbound traffic transmitted through the Zyxel Device Ethernet port will NOT be tagged with the **Management VLAN ID**. Clear this option to have the Zyxel Device add the **Management VLAN ID** tag to outbound traffic transmitted through the Zyxel Device Ethernet port. The uplink device connected to the Zyxel Device Ethernet port needs to have the same VLAN ID configured to receive traffic from the Zyxel Device.
LAN Setting Note: The following settings are only available if your Zyxel Device supports wireless bridge and have more than one Ethernet port. See the feature comparison table in Section 1.2 on page 14.	
Port Setting	

Table 39 Configuration > Network > VLAN (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. In some tables you can just click a table entry and edit it directly in the table. For those types of tables small red triangles display for table entries with changes that you have not yet applied.
Activate/ Inactivate	To turn on an entry, select it and click **Activate**. To turn off an entry, select it and click **Inactivate**.
#	This is the index number of the port.
Status	This field indicates whether the port is enabled (a yellow bulb) or not (a gray bulb).
Port	This field displays the name of the port.
PVID	This field displays the PVID of a port. You can click **Edit** to set the PVID in the **Edit Port** screen. This only governs the incoming untagged packets. The Zyxel Device will tag packets received on the port with the specified PVID. The packets will then be sent to the VLANs they belong to accordingly.
VLAN Configuration	
Add	Click this to create a new entry. For features where the entry's position in the numbered list is important (features where the Zyxel Device applies the table's entries in order like the SSID for example), you can select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings. In some tables you can just click a table entry and edit it directly in the table. For those types of tables small red triangles display for table entries with changes that you have not yet applied.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Activate/ Inactivate	To turn on an entry, select it and click **Activate**. To turn off an entry, select it and click **Inactivate**.
#	This is the index number of the VLAN ID.
Status	This field indicates whether the VLAN is enabled (a yellow bulb) or not (a gray bulb).
Name	This field displays the name of each VLAN.
VID	This field displays the VLAN ID. Note: The VLAN ID you set here will be added as an entry in the **Wireless Bridge VLAN Settings** table.
Member	This field displays the VLAN membership to which the port belongs. This also displays if outgoing packets from the port are tagged or not. **(T)** means the packets going out from the port are tagged. **(U)** means the packets going out from the port are untagged. Note: For WAX620D-6E, WAX640S-6E, and NWA220AX-6E, the Tx-tagging settings are unconfigurable. The Tx-tagging settings will be synced with the **PVID** settings in the **Port Settings** table. If the VID is the same as the PVID set on the port, the outgoing traffic will be untagged, the member port will display **(U)**. Otherwise, the outgoing packets will be tagged with the VID, the member port will display **(T)**.
Wireless Bridge Vlan Setting This section appears if your Zyxel Device supports wireless bridge. See the feature comparison table in Section 1.2 on page 14.	
Add	Click this to add an entry in the table.

Table 39 Configuration > Network > VLAN (continued)

LABEL	DESCRIPTION
Remove	Select an entry and click this to remove the selected entry.
#	This field is a sequential value. It is not associated with any VLAN ID.
Wireless Bridge Vlan ID (1-4094)	Enter a VLAN ID for the wireless bridge. Duplicate VLAN IDs are not allowed. The VLAN IDs you set on your root AP should be the same as the VLAN IDs you set here. See Section on page 14 for more information on wireless bridge. Note: The VLAN ID you set here will be added as an entry in the **VLAN Configuration** table.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

10.4 Storm Control

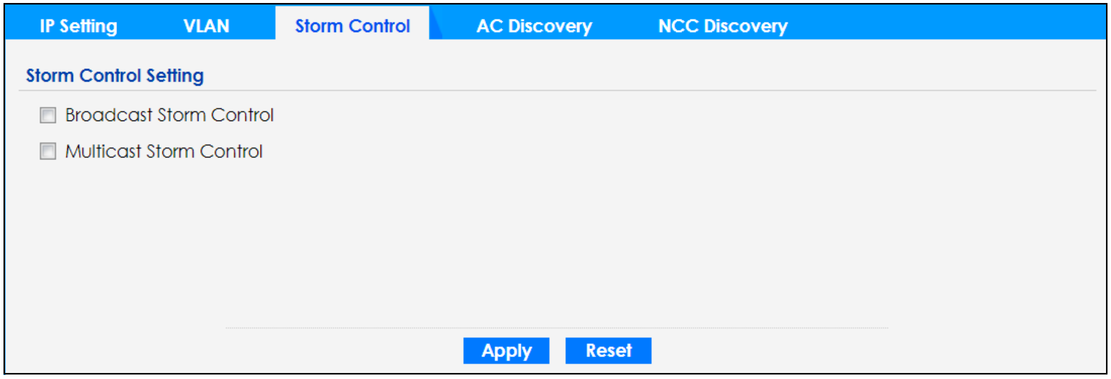
Traffic storm control limits the number of broadcast and/or multicast packets the Zyxel Device receives on the ports. When the maximum number of allowable broadcast and/or multicast packets is reached, the subsequent packets are discarded. Enable this feature to reduce broadcast and/or multicast packets in your network.

Note: Not all Zyxel Device models support the storm control feature. See the feature comparison table in Section 1.2 on page 14.

Note: The maximum traffic rate can be changed using the CLI (see the CLI Reference Guide).

To access this screen, click **Configuration** > **Network** > **Storm Control**.

Figure 81 Configuration > Network > Storm Control



Storm Control Setting

☐ Broadcast Storm Control

☐ Multicast Storm Control

Each field is described in the following table.

Table 40 Configuration > Network > Storm Control

LABEL	DESCRIPTION
Broadcast Storm Control	Select the check box to enable broadcast storm control on the Zyxel Device. Enabling this will drop ingress broadcast traffic in the physical Ethernet port if it exceeds the maximum traffic rate.
Multicast Storm Control	Select the check box to enable multicast storm control on the Zyxel Device. Enabling this will drop ingress multicast traffic in the physical Ethernet port if it exceeds the maximum traffic rate.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

10.5 AC (AP Controller) Discovery

This section discusses how to configure the Zyxel Device's AC Discovery settings. You can have the Zyxel Device managed by an AC on your network. When you do this, the Zyxel Device can be configured ONLY by the AC. See Section 10.1.1 on page 102 for more information on AC management.

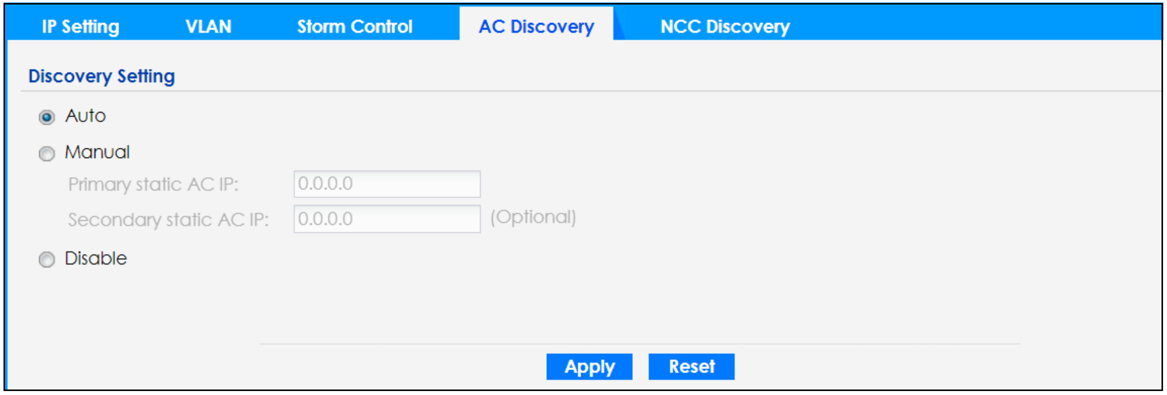
Note: The AC Discovery settings are not available in all Zyxel Devices. See Section 1.2 on page 14 for more information.

If you want to return the Zyxel Device to function in standalone mode, you can do one of the two following options:

- Press the Reset button.
- Check the AC for the Zyxel Device's IP address and use FTP to upload the default configuration file to the Zyxel Device. You can get the configuration file at conf/system-default.conf. You must reboot the Zyxel Device after uploading the configuration file.

To access the Controller Discover screen, click **Configuration** > **Network** > **AC Discovery**.

Figure 82 Configuration > Network > AC Discovery



Discovery Setting

● Auto

○ Manual

Primary static AC IP: 0.0.0.0

Secondary static AC IP: 0.0.0.0 (Optional)

○ Disable

Each field is described in the following table.

Table 41 Configuration > Network > AC Discovery

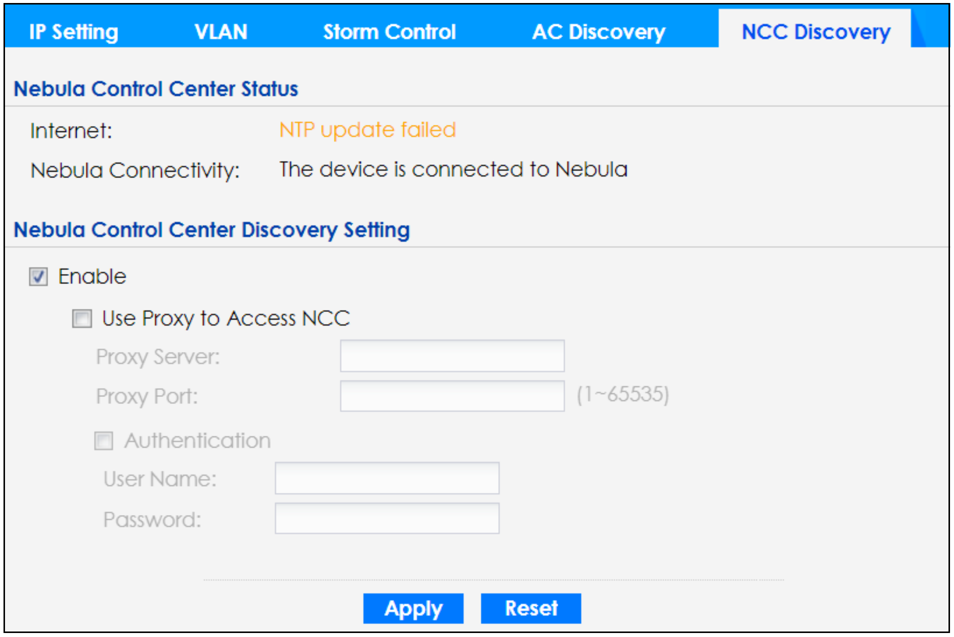
LABEL	DESCRIPTION
Discovery Setting	
Auto	Select this option to use DHCP option 138/DNS SRV record/Broadcast to get the AC's IP address. If the Zyxel Device and a Zyxel AC, such as a ZyWALL ATP, are in the same subnet, it will be managed by the controller automatically.
Manual	Select this option and enter the IP address of the AC manually. This is necessary when the AP Controller is not in the same subnet and you want it to manage the Zyxel Device.
Primary / Secondary Static AC IP	Specify the primary and secondary IP address of the AC to which the Zyxel Device connects.
Disable	Select this to manage the Zyxel Device using its own Web Configurator, neither managing nor being managed by other devices. Please note if an AP Controller is in the same subnet, you will need to click **Disable** if you do not want the Zyxel Device to be managed.
Apply	Click **Apply** to save the information entered in this screen. If you select **Auto** or **Manual**, the AC uploads the firmware package for managed AP mode to the Zyxel Device and you cannot log in as the web configurator is disabled; you must manage the Zyxel Device through the AC on your network.
Reset	Click **Reset** to return the screen to its last-saved settings.

10.6 NCC Discovery

You can manage the Zyxel Device through the Zyxel Nebula Control Center (NCC). Use this screen to configure the proxy server settings if the Zyxel Device is behind a proxy server.

To access this screen, click **Configuration** > **Network** > **NCC Discovery**.

Figure 83 Configuration > Network > NCC Discovery



Nebula Control Center Status

Internet: NTP update failed

Nebula Connectivity: The device is connected to Nebula

Nebula Control Center Discovery Setting

☑ Enable

□ Use Proxy to Access NCC

Proxy Server:

Proxy Port: (1~65535)

□ Authentication

User Name:

Password:

Each field is described in the following table.

Table 42 Configuration > Network > NCC Discovery

LABEL	DESCRIPTION
Nebula Control Center Status	
Internet	This field displays whether the Zyxel Device can connect to the Internet.
Nebula Connectivity	This field displays whether the Zyxel Device can connect to the Zyxel Nebula Control Center (NCC).
Nebula Control Center Discovery Setting	
Enable	Select this option to turn on NCC discovery on the Zyxel Device. The Zyxel Device will try to discover the NCC and go into NCC management mode when it is connected to the Internet and has been registered in the NCC. If NCC discovery is disabled, the Zyxel Device will not discover the NCC and remain in standalone operation.
Use Proxy to Access NCC	If the Zyxel Device is behind a proxy server, you need to select this option and configure the proxy server settings so that the Zyxel Device can access the NCC through the proxy server.
Proxy Server	Enter the IP address of the proxy server.
Proxy Port	Enter the service port number used by the proxy server.
Authentication	Select this option if the proxy server requires authentication before it grants access to the NCC.
User Name	Enter your proxy user name.
Password	Enter your proxy password.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

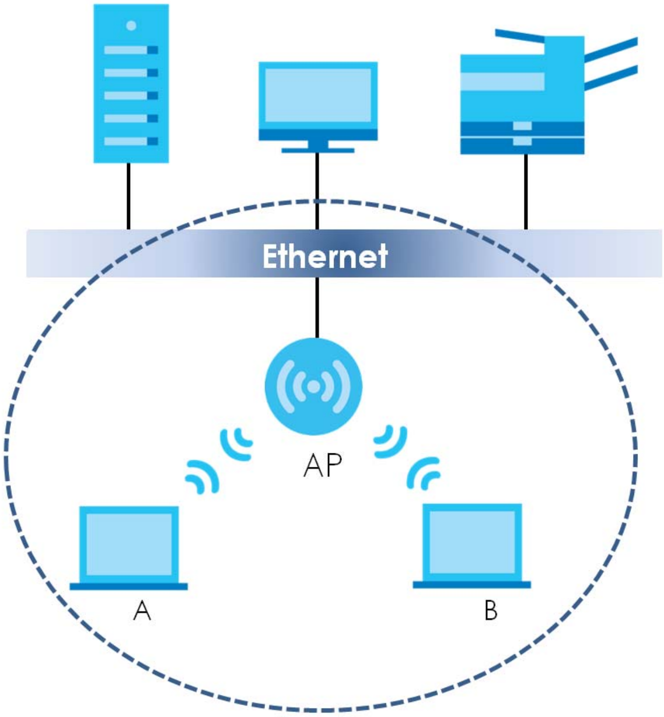
CHAPTER 11 Wireless

11.1 Overview

This chapter discusses how to configure the WiFi network settings in your Zyxel Device.

The following figure provides an example of a WiFi network.

Figure 84 Example of a WiFi Network



The WiFi network is the part in the blue circle. In this WiFi network, devices **A** and **B** are called WiFi clients. The WiFi clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet. Your Zyxel Device is the AP.

11.1.1 What You Can Do in this Chapter

- The **AP Management** screen (Section 11.2 on page 116) allows you to manage the Zyxel Device's general WiFi settings.
- The **Rogue AP** screen (Section 11.3 on page 122) allows you to assign APs either to the rogue AP list or the friendly AP list.
- The **Load Balancing** screen (Section 11.4 on page 126) allows you to configure network traffic load balancing between the APs and the Zyxel Device.
- The **DCS** screen (Section 11.5 on page 128) allows you to configure dynamic radio channel selection.

11.1.2 What You Need to Know

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

Station / WiFi Client

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

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 Section 11.6 on page 129.

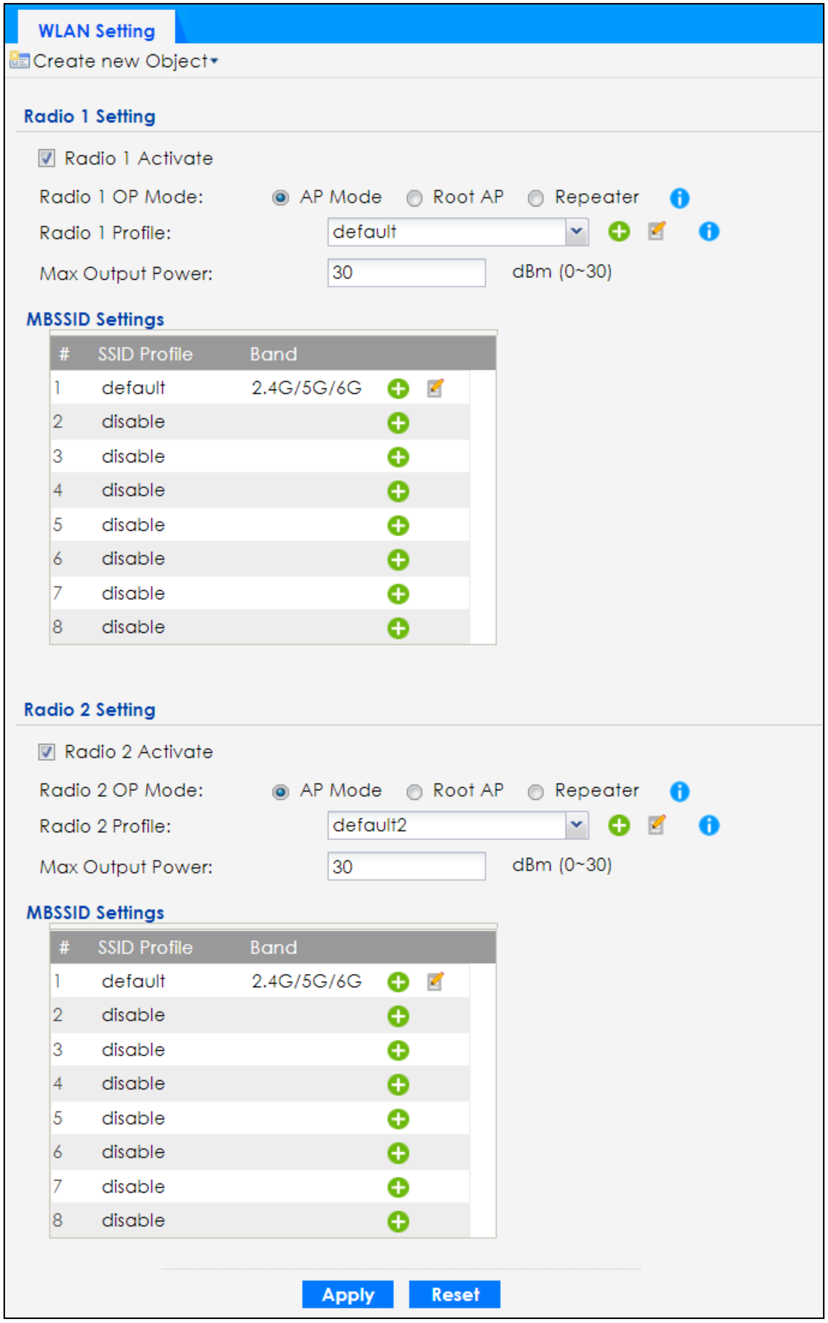
Load Balancing (Wireless)

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

11.2 AP Management

Use this screen to manage the Zyxel Device’s general WiFi settings. Click **Configuration > Wireless > AP Management** to access this screen.

Figure 85 Configuration > Wireless > AP Management



Radio 1 Setting

☑ Radio 1 Activate

Radio 1 OP Mode: ● AP Mode ○ Root AP ○ Repeater

Radio 1 Profile: default

Max Output Power: 30 dBm (0~30)

MBSSID Settings

#	SSID Profile	Band
1	default	2.4G/5G/6G
2	disable	
3	disable	
4	disable	
5	disable	
6	disable	
7	disable	
8	disable	

Radio 2 Setting

☑ Radio 2 Activate

Radio 2 OP Mode: ● AP Mode ○ Root AP ○ Repeater

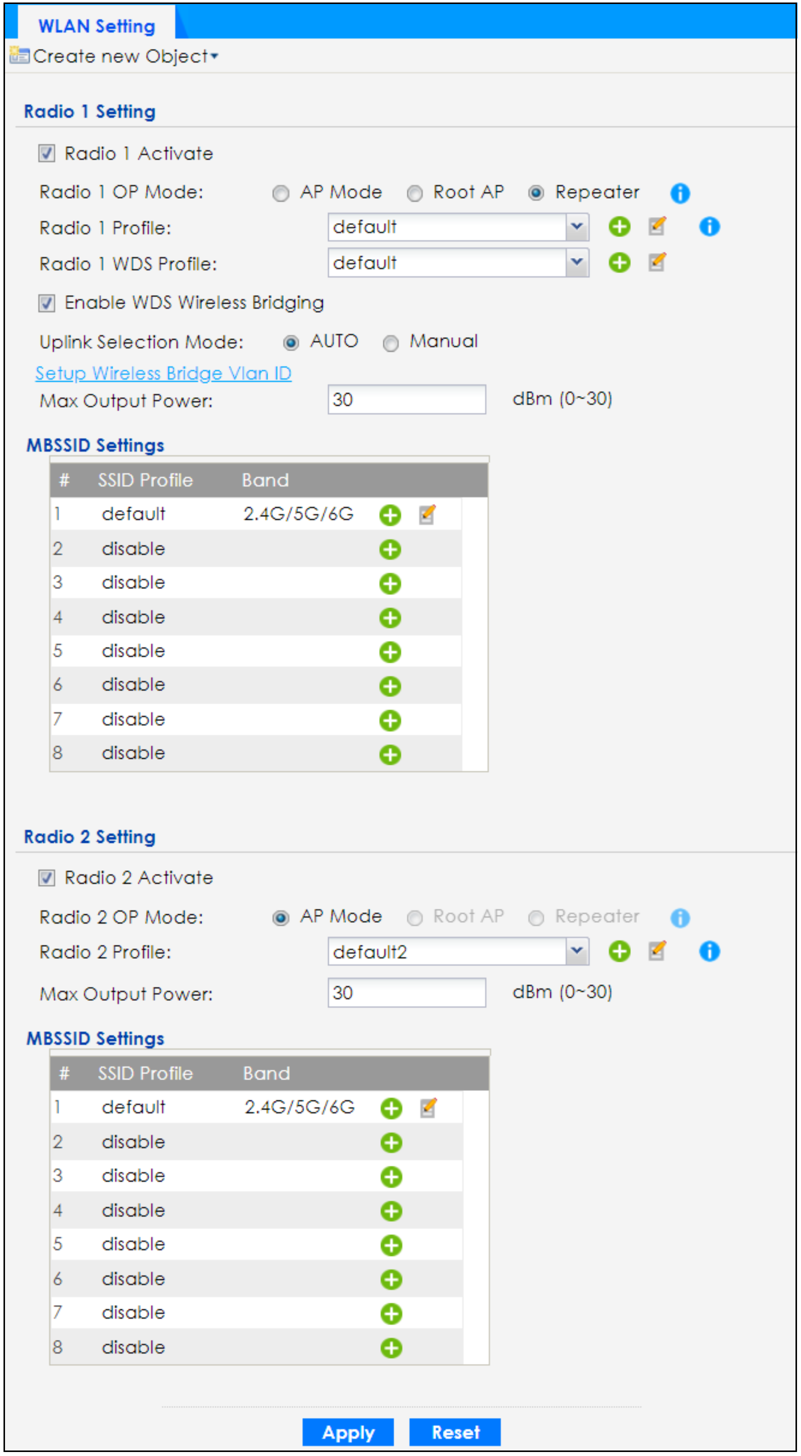
Radio 2 Profile: default2

Max Output Power: 30 dBm (0~30)

MBSSID Settings

#	SSID Profile	Band
1	default	2.4G/5G/6G
2	disable	
3	disable	
4	disable	
5	disable	
6	disable	
7	disable	
8	disable	

Figure 86 Configuration > Wireless > AP Management (for Zyxel Device with multiple Ethernet ports - in Repeater mode)



Radio 1 Setting

☑ Radio 1 Activate

Radio 1 OP Mode: ○ AP Mode ○ Root AP ● Repeater

Radio 1 Profile: default

Radio 1 WDS Profile: default

☑ Enable WDS Wireless Bridging

Uplink Selection Mode: ● AUTO ○ Manual

Setup Wireless Bridge Vlan ID

Max Output Power: 30 dBm (0~30)

MBSSID Settings

#	SSID Profile	Band
1	default	2.4G/5G/6G
2	disable	
3	disable	
4	disable	
5	disable	
6	disable	
7	disable	
8	disable	

Radio 2 Setting

☑ Radio 2 Activate

Radio 2 OP Mode: ● AP Mode ○ Root AP ○ Repeater

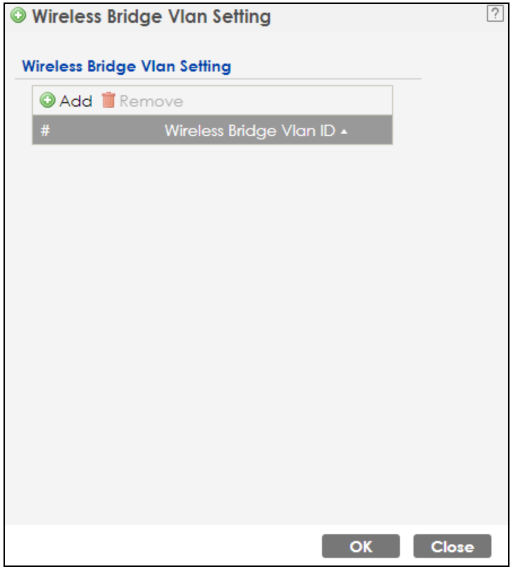
Radio 2 Profile: default2

Max Output Power: 30 dBm (0~30)

MBSSID Settings

#	SSID Profile	Band
1	default	2.4G/5G/6G
2	disable	
3	disable	
4	disable	
5	disable	
6	disable	
7	disable	
8	disable	

Figure 87 Configuration > Wireless > AP Management > Setup Wireless Bridge Vlan ID: Wireless Bridge Vlan Setting (for Zyxel Device with multiple Ethernet ports)



Each field is described in the following table.

Table 43 Configuration > Wireless > AP Management

LABEL	DESCRIPTION
Radio 1 Setting	
Radio 1 Activate	Select the check box to enable the Zyxel Device's first (default) radio.
Radio 1 OP Mode	Select the operating mode for radio 1. **AP Mode** means the radio can receive connections from WiFi clients and pass their data traffic through to the Zyxel Device to be managed (or subsequently passed on to an upstream gateway for managing). **Root AP** means the radio acts as an AP and also supports the wireless connections with other APs (in repeater mode) to form a WDS (Wireless Distribution System) to extend its wireless network. **Repeater** means the radio can establish a wireless connection with other APs (in either root AP or repeater mode) to form a WDS.
Radio 1 Profile	Select the radio profile the radio uses. Note: You can only apply a 2.4G AP radio profile to radio 1. Otherwise, the first radio will not be working.
Radio 1 WDS Profile	This field is available only when the radio is in **Root AP** or **Repeater** mode. Select the WDS profile the radio uses to connect to a root AP or repeater.

Table 43 Configuration > Wireless > AP Management (continued)

LABEL	DESCRIPTION
Enable WDS Wireless Bridging	Not all models support this feature. See Section 1.2 on page 14 for models that support wireless bridge. If you set the Zyxel Device as a root AP, the radio that's bridging with the Zyxel Device should be in repeater mode. Be careful to avoid bridge loops. For example, if your root AP and the Zyxel Device are connected to a switch, and they're also connected to each other using a WiFi connection. This will create bridge loops. This field is available only when the radio is in **Repeater** mode. Select this to enable WDS wireless bridging on the Zyxel Device to establish wireless links with other APs. See Section on page 14 for more information on Wireless Distribution System (WDS). Note: You must enable the same WiFi security settings on the Zyxel Device and on all WiFi clients that you want to associate with it.
Uplink Selection Mode	This field is available only when the radio is in **Repeater** mode. Select **AUTO** to have the Zyxel Device automatically use the settings in the applied WDS profile to connect to a root AP or repeater. Select **Manual** to have the Zyxel Device connect to the root AP or repeater with the MAC address specified in the **Radio 1 Uplink MAC Address** field.
Setup Wireless Bridge Vlan ID	This appears if you select **Enable WDS Wireless Bridging**. Click this to show the **Wireless Bridge Vlan Setting** pop-up window. This link is available only when the radio is in **Root AP** or **Repeater** mode.
Wireless Bridge Vlan Setting	
Add	Click this to add an entry in the table.
Remove	Select an entry and click this to remove the selected entry.
#	This field is a sequential value. It is not associated with any VLAN ID.
Wireless Bridge Vlan ID	Enter a VLAN ID for the wireless bridge. The VLAN IDs you set on your root AP should be the same as the VLAN ID you set here. See Section 1.3 on page 18 for more information on wireless bridge.
OK	Click **OK** to save your changes back to the Zyxel Device.
Close	Click **Close** to close the pop-up window without saving your changes.
Max Output Power	Enter the maximum output power (between 0 to 30 dBm) of the Zyxel Device in this field. If there is a high density of APs in an area, decrease the output power of the Zyxel Device to reduce interference with other APs. Note: Reducing the output power also reduces the Zyxel Device's effective broadcast radius.
MBSSID Settings	
Add ➕	This button is not available after you configure the Zyxel Device using the wizard. Click the **Add** icon (➕)to open a screen where you can create a new entry. For features where the entry's position in the numbered list is important (features where the Zyxel Device applies the table's entries in order like the SSID for example), you can select an entry and click **Add** to create a new entry after the selected entry.
Edit ✎	Click the **Edit** icon (✎)to open a screen where you can modify the entry's settings. In some tables you can just click a table entry and edit it directly in the table. For those types of tables small red triangles display for table entries with changes that you have not yet applied.
#	This field shows the index number of the SSID
SSID Profile	This field displays the SSID profile that is associated with the radio profile.

Table 43 Configuration > Wireless > AP Management (continued)

LABEL	DESCRIPTION
Band	This field displays the frequency bands to which the SSID profile is applicable. If the SSID profile is not applicable to the current radio, the SSID profile will not be enabled. You can configure the SSID profile's applicable frequency bands in the **Edit SSID Profile** screen (click the **Edit** button next to the profile).
Radio 2/3 Setting The **Radio 3 Setting** fields are only available for Zyxel Device models that support triple radios.	
Radio 2/3 Activate	This displays if the Zyxel Device has a second radio. Select the check box to enable the Zyxel Device's second radio.
Radio 2/3 OP Mode	This displays if the Zyxel Device has a second radio. Select the operating mode for radio 2. **AP Mode** means the radio can receive connections from WiFi clients and pass their data traffic through to the Zyxel Device to be managed (or subsequently passed on to an upstream gateway for managing). **Root AP** means the radio acts as an AP and also supports the wireless connections with other APs (in repeater mode) to form a WDS to extend its wireless network. **Repeater** means the radio can establish a wireless connection with other APs (in either root AP or repeater mode) to form a WDS.
Radio 2/3 Profile	This displays if the Zyxel Device has a second/third radio. Select the radio profile the radio uses. Note: For models that do not support BandFlex, you can only apply a 5G AP radio profile to radio 2. Otherwise, the second radio will not be working. See Section on page 14 for more information.
Radio 2/3 WDS Profile	This field is available only when the radio is in **Root AP** or **Repeater** mode. Select the WDS profile the radio uses to connect to a root AP or repeater.
Enable WDS Wireless Bridging	Not all models support this feature. See Section 1.2 on page 14 for models that support wireless bridge. If you set the Zyxel Device as a root AP, the radio that's bridging with the Zyxel Device should be in repeater mode. Be careful to avoid bridge loops. For example, if your root AP and the Zyxel Device are connected to a switch, and they're also connected to each other using a WiFi connection. This will create bridge loops. This field is available only when the radio is in **Repeater** mode. Select this to enable WDS wireless bridging on the Zyxel Device to establish wireless links with other APs. See Section on page 14 for more information on Wireless Distribution System (WDS). Note: You must enable the same WiFi security settings on the Zyxel Device and on all WiFi clients that you want to associate with it.
Uplink Selection Mode	This field is available only when the radio is in **Repeater** mode. Select **AUTO** to have the Zyxel Device automatically use the settings in the applied WDS profile to connect to a root AP or repeater. Select **Manual** to have the Zyxel Device connect to the root AP or repeater with the MAC address specified in the **Radio 1 Uplink MAC Address** field.
Setup Wireless Bridge Vlan ID	Click this to show the **Wireless Bridge Vlan Setting** pop-up window. This link is available only when the radio is in **Root AP** or **Repeater** mode.
Wireless Bridge Vlan Setting	
Add	Click this to add an entry in the table.
Remove	Select an entry and click this to remove the selected entry.

Table 43 Configuration > Wireless > AP Management (continued)

LABEL	DESCRIPTION
#	This field is a sequential value. It is not associated with any VLAN ID.
Wireless Bridge Vlan ID	Enter a VLAN ID for the wireless bridge. The VLAN IDs you set on your root AP should be the same as the VLAN ID you set here. See Section 1.3 on page 18 for more information on wireless bridge.
OK	Click **OK** to save your changes back to the Zyxel Device.
Close	Click **Close** to close the pop-up window without saving your changes.
Max Output Power	Enter the maximum output power (between 0 to 30 dBm) of the Zyxel Device in this field. If there is a high density of APs in an area, decrease the output power of the Zyxel Device to reduce interference with other APs. Note: Reducing the output power also reduces the Zyxel Device's effective broadcast radius.
MBSSID Settings	
Add ⊕	This button is not available after you configure the Zyxel Device using the wizard. Click the **Add** icon (⊕)to open a screen where you can create a new entry. For features where the entry's position in the numbered list is important (features where the Zyxel Device applies the table's entries in order like the SSID for example), you can select an entry and click **Add** to create a new entry after the selected entry.
Edit ✎	Click **Edit** (✎)to open a screen where you can modify the entry's settings. In some tables you can just click a table entry and edit it directly in the table. For those types of tables small red triangles display for table entries with changes that you have not yet applied.
#	This field shows the index number of the SSID
SSID Profile	This field shows the SSID profile that is associated with the radio profile.
Band	This field displays the radio bands to which the SSID profile is applicable. If the SSID profile is not applicable to the current radio, the SSID profile will not be enabled. You can configure the SSID profile's applicable radio bands in the **Edit SSID Profile** screen (click the **Edit** button next to the profile).
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

11.3 Rogue AP

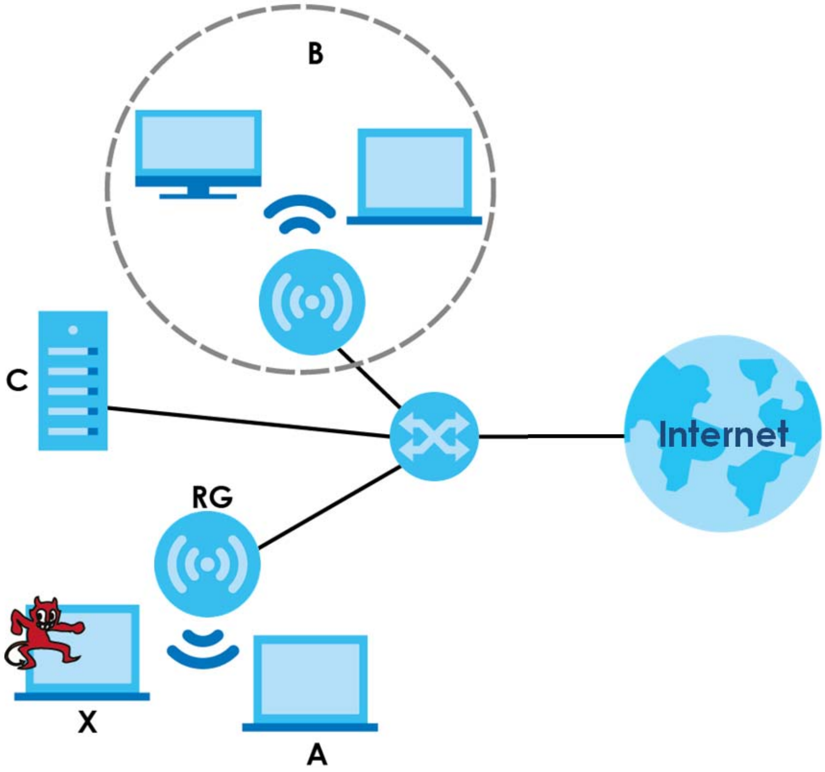
Use this screen to enable **Rogue AP Detection** and import/export a rogue or friendly AP list in a txt file. Click **Configuration > Wireless > Rogue AP** to access this screen.

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 (the dashed ellipse **B**) is well-secured, but the rogue AP uses inferior security that is easily broken by an attacker (**X**) running readily available encryption-cracking software. In this example, the attacker now has access to the company network, including sensitive data stored on the file server (**C**).

Figure 88 Rogue AP Example



Friendly APs

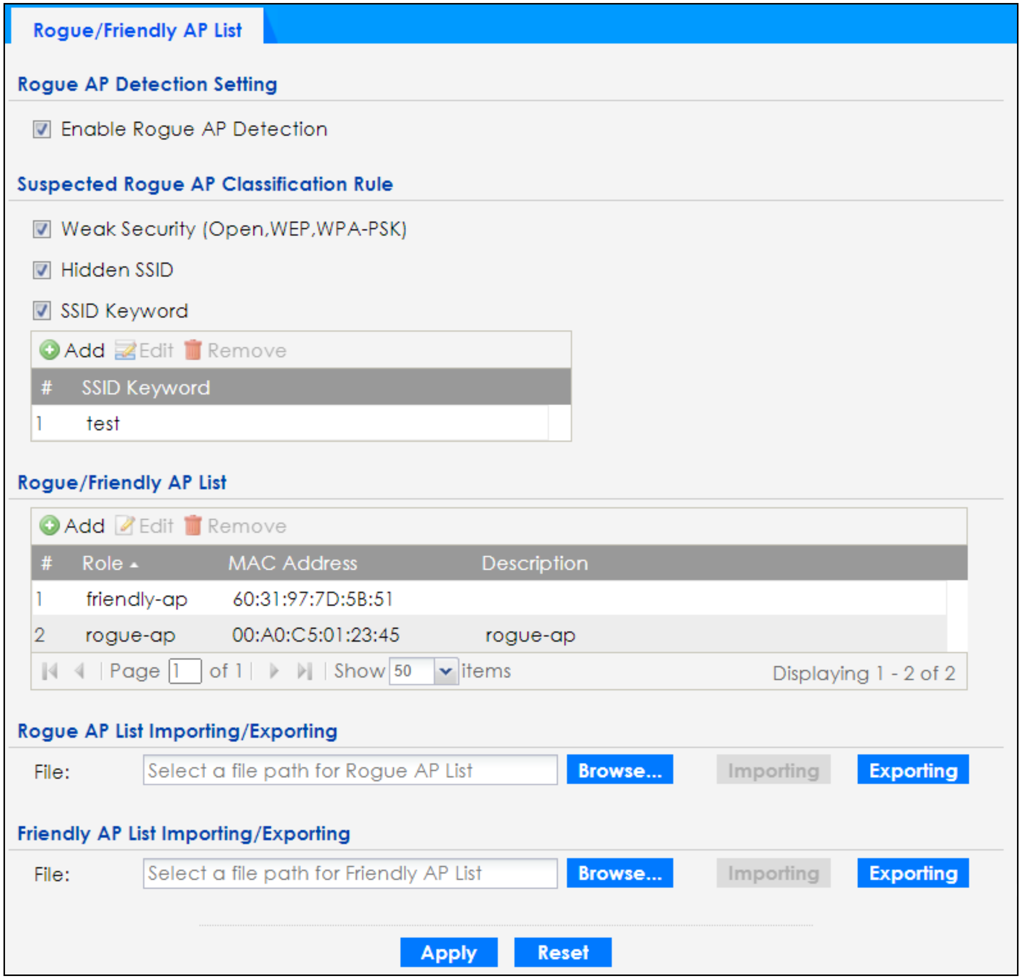
If you have more than one AP in your WiFi network, you should also configure a list of “friendly” APs. Friendly APs are wireless access points that you know are not a threat. It is recommended that you export (save) your list of friendly APs often, especially if you have a network with a large number of access points. Exported lists show MAC addresses in txt file format separated by line breaks.

Rogue AP Detection

This feature allows the Zyxel Device to monitor the WiFi signals for other wireless APs (see also Section 1.3.1 on page 26). Detected APs will appear in the **Monitor > Wireless > Detected Device** screen, where the Zyxel Device will label APs with the criteria you select in **Suspected Rogue AP Classification Rule** as a suspected rogue. The APs which you mark as either rogue or friendly APs in the **Monitor > Wireless > Detected Device** screen will appear in the **Wireless > Rogue AP** screen. See Section 1.2 on page 14 to know which models support **Rogue AP Detection**.

Note: Enabling **Rogue AP Detection** might affect the performance of WiFi clients associated with the Zyxel Device.

Figure 89 Configuration > Wireless > Rogue AP



Rogue/Friendly AP List
Rogue AP Detection Setting
☑ Enable Rogue AP Detection
Suspected Rogue AP Classification Rule
☑ Weak Security (Open,WEP,WPA-PSK)
☑ Hidden SSID
☑ SSID Keyword
Add Edit Remove
Rogue/Friendly AP List
Add Edit Remove
Page 1 of 1 Show 50 items Displaying 1 - 2 of 2
Rogue AP List Importing/Exporting
File: Select a file path for Rogue AP List Browse... Importing Exporting
Friendly AP List Importing/Exporting
File: Select a file path for Friendly AP List Browse... Importing Exporting
Apply Reset

#	SSID Keyword
1	test

#	Role	MAC Address	Description
1	friendly-ap	60:31:97:7D:5B:51	
2	rogue-ap	00:A0:C5:01:23:45	rogue-ap

Each field is described in the following table.

Table 44 Configuration > Wireless > Rogue AP

LABEL	DESCRIPTION
Rogue AP Detection Setting	
Enable Rogue AP Detection	Select this check box to detect Rogue APs in the network.
Suspected Rogue AP Classification Rule	Select the check boxes (**Weak Security (Open, WEP, WPA-PSK)**, **Hidden SSID**, **SSID Keyword**) of the characteristics an AP should have for the Zyxel Device to mark it as a Rogue AP.
Add	Click this to add an SSID Keyword.
Edit	Select an SSID Keyword and click this button to modify it.
Remove	Select an existing SSID keyword and click this button to delete it.
#	This is the SSID Keyword's index number in this list.
SSID Keyword	This field displays the SSID Keyword.
Rogue/Friendly AP List	
Add	Click this button to add an AP to the list and assign it either friendly or rogue status.
Edit	Select an AP in the list to edit and reassign its status.
Remove	Select an AP in the list to remove.

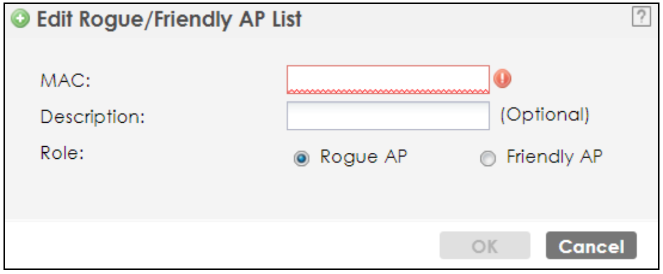
Table 44 Configuration > Wireless > Rogue AP (continued)

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with any interface.
Role	This field indicates whether the selected AP is a **rogue-ap** or a **friendly-ap**. To change the AP's role, click the **Edit** button.
MAC Address	This field indicates the AP's radio MAC address.
Description	This field displays the AP's description. You can modify this by clicking the **Edit** button.
Rogue/Friendly AP List Importing/Exporting	These controls allow you to export the current list of rogue and friendly APs or import existing lists.
File Path / Browse / Importing	Enter the file name and path of the list you want to import or click the **Browse** button to locate it. Once the **File Path** field has been populated, click **Importing** to bring the list into the Zyxel Device. You need to wait a while for the importing process to finish.
Exporting	Click this button to export the current list of either rogue APs or friendly APS.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

11.3.1 Add/Edit Rogue/Friendly List

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

Figure 90 Configuration > Wireless > Rogue AP > Add/Edit Rogue/Friendly AP List



Edit Rogue/Friendly AP List

MAC:

Description: (Optional)

Role: ● Rogue AP ○ Friendly AP

Each field is described in the following table.

Table 45 Configuration > Wireless > Rogue AP > Add/Edit Rogue/Friendly AP List

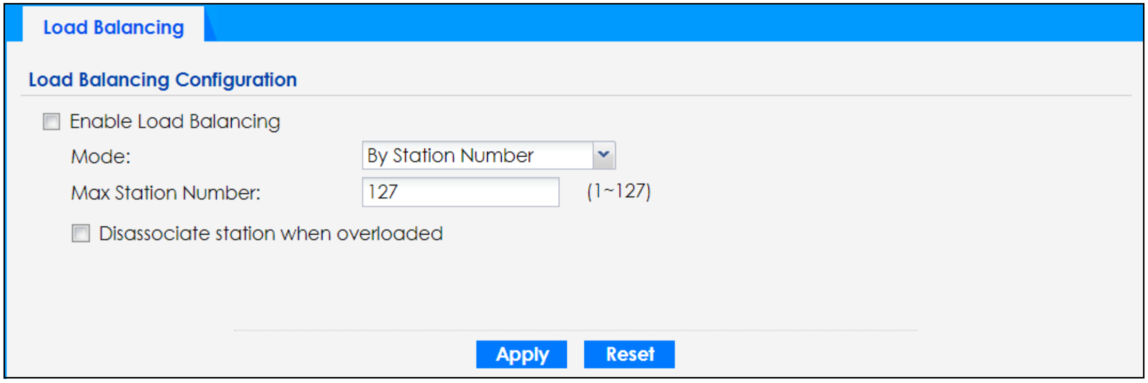
LABEL	DESCRIPTION
MAC	Enter the MAC address of the AP you want to add to the list. A MAC address is a unique hardware identifier in the following hexadecimal format: xx:xx:xx:xx:xx:xx where xx is a hexadecimal number separated by colons.
Description	Enter up to 60 characters for the AP's description.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

11.4 Load Balancing

Use this screen to configure wireless network traffic load balancing between the APs on your network (see Load Balancing on page 130). Click **Configuration > Wireless > Load Balancing** to access this screen.

Note: This screen is only available on Zyxel Device models that support load balancing. See the feature comparison table in Section 1.2 on page 14.

Figure 91 Configuration > Wireless > Load Balancing



□ Enable Load Balancing

Mode: By Station Number

Max Station Number: 127 (1~127)

□ Disassociate station when overloaded

Each field is described in the following table.

Table 46 Configuration > Wireless > Load Balancing

LABEL	DESCRIPTION
Enable Load Balancing	Select this to enable load balancing on the Zyxel Device. Use this section to configure wireless network traffic load balancing between the managed APs in this group.
Mode	Select a mode by which load balancing is carried out. Select **By Station Number** to balance network traffic based on the number of specified stations connected to the Zyxel Device. Select **By Traffic Level** to balance network traffic based on the volume generated by the stations connected to the Zyxel Device. Select **By Smart Classroom** to balance network traffic based on the number of specified stations connected to the Zyxel Device. The Zyxel Device ignores association request and authentication request packets from any new station when the maximum number of stations is reached. If you select **By Station Number** or **By Traffic Level**, once the threshold is crossed (either the maximum station numbers or with network traffic), the Zyxel Device delays association request and authentication request packets from any new station that attempts to make a connection. This allows the station to automatically attempt to connect to another, less burdened AP if one is available.
Max Station Number	Enter the threshold number of stations at which the Zyxel Device begins load balancing its connections.
Traffic Level	Select the threshold traffic level at which the Zyxel Device begins load balancing its connections (**Low**, **Medium**, **High**). The maximum bandwidth allowed for each level is: • **Low** - 11 Mbps • **Medium** - 23 Mbps • **High** - 35 Mbps

Table 46 Configuration > Wireless > Load Balancing (continued)

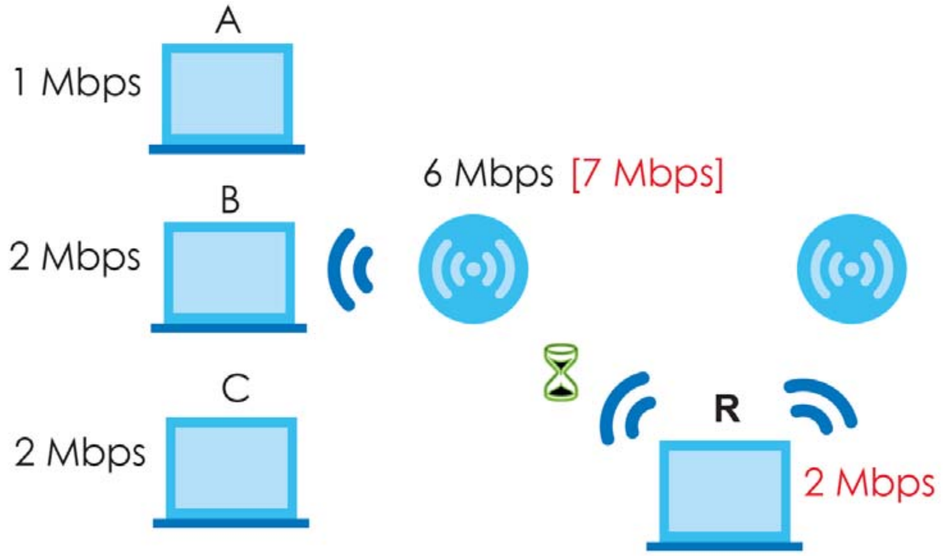
LABEL	DESCRIPTION
Disassociate station when overloaded	This function is enabled by default and the disassociation priority is always **Signal Strength** when you set **Mode** to **By Smart Classroom**. Select this option to disassociate WiFi clients connected to the AP when it becomes overloaded. If you do not enable this option, then the AP simply delays the connection until it can afford the bandwidth it requires, or it transfers the connection to another AP within its broadcast radius. The disassociation priority is determined automatically by the Zyxel Device and is as follows: • **Idle Timeout** - Devices that have been idle the longest will be kicked first. If none of the connected devices are idle, then the priority shifts to **Signal Strength**. • **Signal Strength** - Devices with the weakest signal strength will be kicked first. Note: If you enable this function, you should ensure that there are multiple APs within the broadcast radius that can accept any rejected or kicked WiFi clients; otherwise, a WiFi client attempting to connect to an overloaded AP will be disassociated permanently and never be allowed to connect.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

11.4.1 Disassociating and Delaying Connections

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

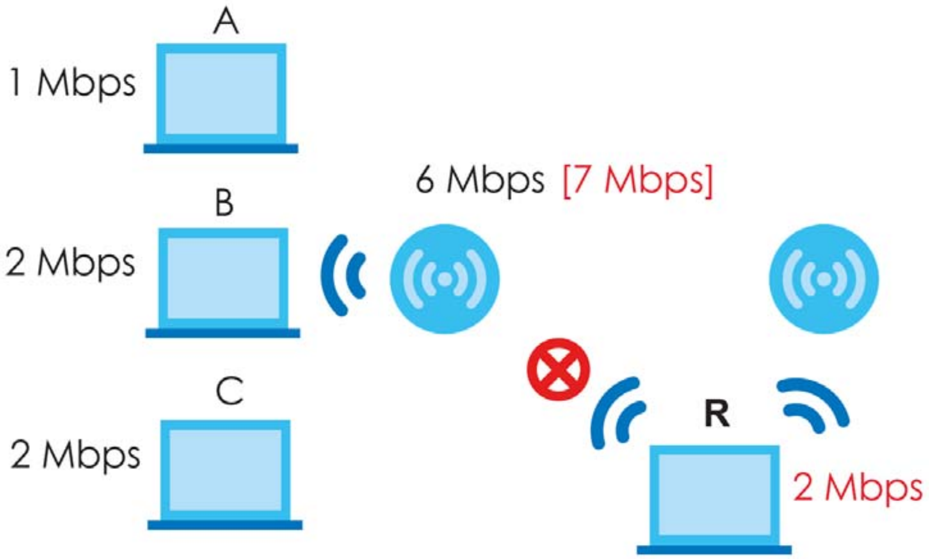
For example, here the AP has a balanced bandwidth allotment of 6 Mbps. If laptop **R** connects and it pushes the AP over its allotment, say to 7 Mbps, then the AP delays the red laptop’s connection until it can afford the bandwidth or the laptop is picked up by a different AP with bandwidth to spare.

Figure 92 Delaying a Connection



The second response your AP can take is to disassociate with clients that are pushing it over its balanced bandwidth allotment.

Figure 93 Disassociating with a Client

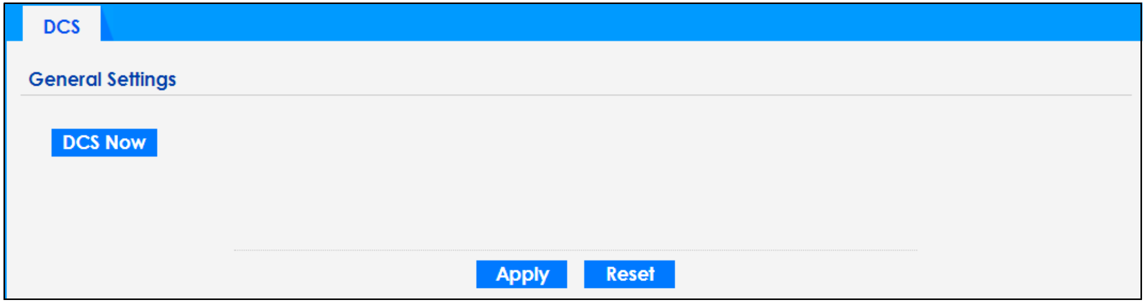


Connections are cut based on either **idle timeout** or **signal strength**. The Zyxel Device first looks to see which devices have been idle the longest, then starts kicking them in order of highest idle time. If no connections are idle, the next criteria the Zyxel Device analyzes is signal strength.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

11.5 DCS

Use this screen to configure dynamic radio channel selection (see Dynamic Channel Selection (DCS) on page 116). Click **Configuration > Wireless > DCS** to access this screen.

Figure 94 Configuration > Wireless > DCS



Each field is described in the following table.

Table 47 Configuration > Wireless > DCS

LABEL	DESCRIPTION
DCS Now	Click this to have the Zyxel Device scan for and select an available channel immediately.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

11.6 Technical Reference

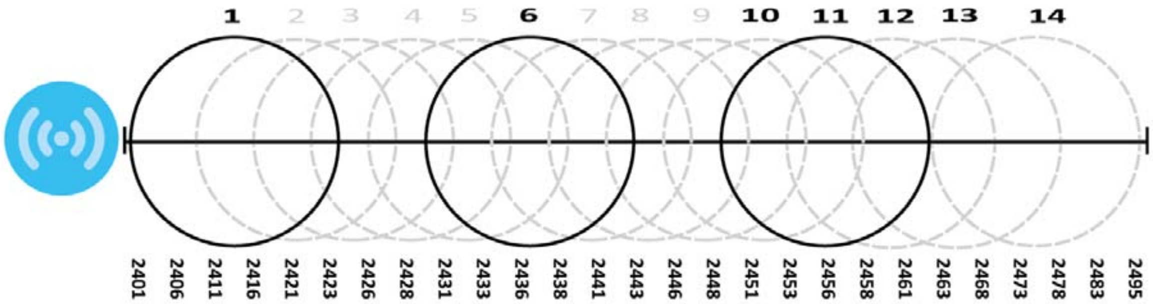
The following section contains additional technical information about the features described in this chapter.

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.

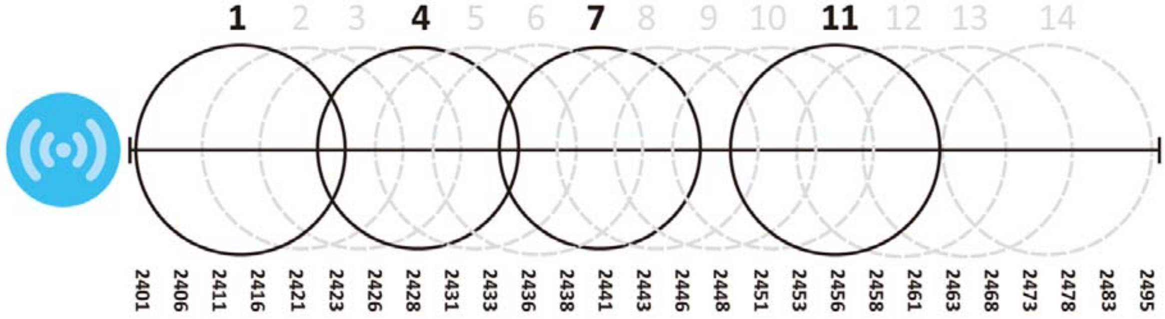
In the 2.4 GHz spectrum, each channel from 1 to 13 is broken up into discrete 22 MHz segments that are spaced 5 MHz apart. Channel 1 is centered on 2.412 GHz while channel 13 is centered on 2.472 GHz.

Figure 95 An Example Three-Channel Deployment



Three channels are situated in such a way as to create almost no interference with one another if used exclusively: 1, 6 and 11. When an AP broadcasts on any of these 3 channels, it should not interfere with neighboring APs as long as they are also limited to same trio.

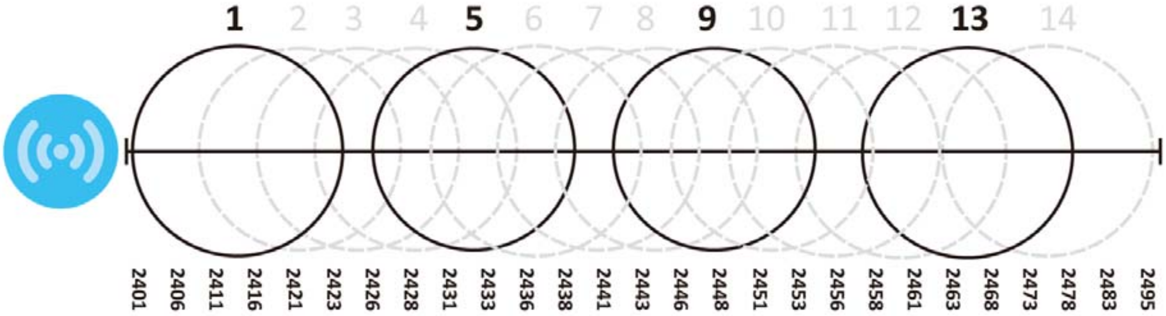
Figure 96 An Example Four-Channel Deployment



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

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

Figure 97 An Alternative Four-Channel Deployment



Load Balancing

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

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

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

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

Load balancing by smart classroom also limits the number of devices allowed to connect to your AP. But any new connections will be just rejected when the AP is overloaded.

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

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

CHAPTER 12 Bluetooth

12.1 Overview

Use this screen to configure the iBeacon advertising settings for the Zyxel Device that supports Bluetooth Low Energy (BLE). Bluetooth Low Energy, which is also known as Bluetooth Smart, transmits less data over a shorter distance but consumes less power than classic Bluetooth.

Note: Check the feature comparison table in Section 1.2 on page 14 to see which Zyxel Device models that support BLE.

12.1.1 What You Need To Know

Beacon is Apple's communication protocol on top of Bluetooth Low Energy wireless technology. Beacons (Bluetooth radio transmitters) or BLE enabled devices broadcast packets to every device around it to announce their presence. Advertising packets contain their iBeacon ID, which consists of the Universally Unique Identifier (UUID), major number, and minor number. These packets also contain a TX (transmit) power measured at a reference point, which is used to approximate a device's distance from the beacon. The UUID can be used to identify a service, a device, a manufacturer or an owner. The 2-byte major number is to identify and distinguish a group, and the 2-byte minor number is to identify and distinguish an individual.

For example, a company can set all its beacons to share the same UUID. The beacons in a particular branch uses the same major number, and each beacon in a branch can have its own minor number.

	COMPANY A		
	BRANCH X		**BRANCH Y**
	BEACON 1	**BEACON 2**	**BEACON 3**
UUID	EBAECFAF-DFE0-4039-BE5A-F030EED4303C		
Major	10	10	20
Minor	1	2	1

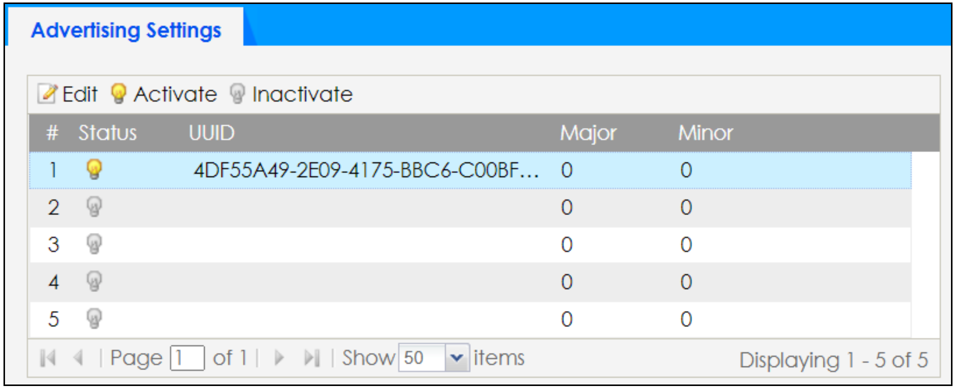
Developers can create apps that respond to the iBeacon ID that your Zyxel Device broadcasts. An app that is associated with the Zyxel Device's iBeacon ID can measure the proximity of a customer to a beacon. This app can then push messages or trigger prompts and actions based on this information. This allows you to send highly contextual and highly localized advertisements to customers.

12.2 Bluetooth Advertising Settings

The Zyxel Device communicates with another BLE enabled device for advertisements. Use this screen to configure up to five beacon IDs to be included in the advertising packet.

To access this screen, click **Configuration > Bluetooth > Advertising Settings**.

Figure 98 Configuration > Bluetooth > Advertising Settings



#	Status	UUID	Major	Minor
1	●	4DF55A49-2E09-4175-BBC6-C00BF…	0	0
2	○		0	0
3	○		0	0
4	○		0	0
5	○		0	0

The following table describes the labels in this screen.

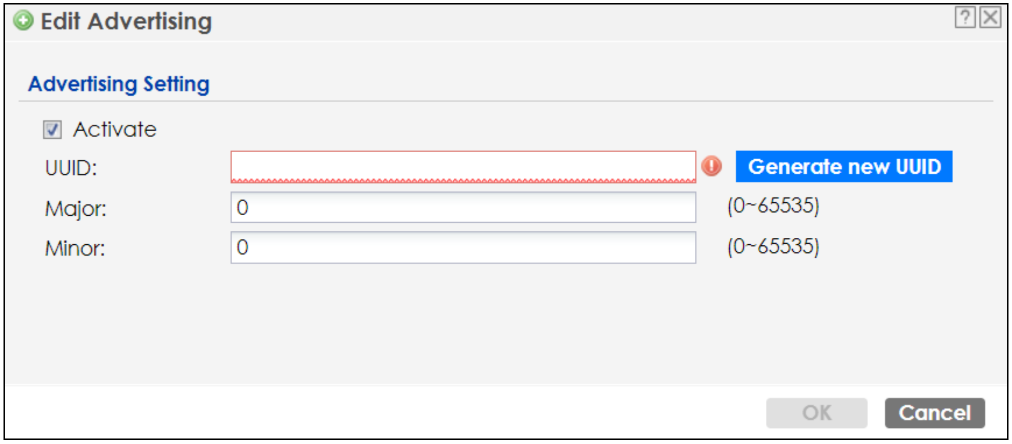
Table 48 Configuration > Bluetooth > Advertising Settings

LABEL	DESCRIPTION
Edit	Click this to edit the selected entry.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
#	This field is a sequential value, and it is not associated with a specific entry.
Status	This field shows whether or not the entry is activated. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
UUID	This field indicates the UUID to be included in the Bluetooth advertising packets.
Major	This field indicates the major number to be included in the Bluetooth advertising packets.
Minor	This field indicates the minor number to be included in the Bluetooth advertising packets.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

12.2.1 Edit Advertising Settings

Select an entry in the **Configuration > Bluetooth > Advertising Settings** screen and click the **Edit** icon to open the **Edit Advertising** screen. Use this screen to configure the beacon ID in the Bluetooth advertising packets.

Figure 99 Configuration > Bluetooth > Advertising Settings > Edit



The following table describes the labels in this screen.

Table 49 Configuration > Bluetooth > Advertising Settings > Edit

LABEL	DESCRIPTION
Activate	Select this option to enable the advertising settings.
UUID	To specify a UUID for the Zyxel Device's beacon ID, enter 32 hexadecimal digits in the range of "A-F", "a-f" and "0-9", split into five groups separated by hyphens (-). The UUID format is as follows: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx (8-4-4-4-12)
Generate new UUID	Click this button to have the Zyxel Device generate a new UUID automatically.
Major	Enter an integer from 0 to 65535 as the major value to identify the group to which the beacon belongs.
Minor	Enter an integer from 0 to 65535 as the minor value to identify the individual beacon.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

CHAPTER 13
User

13.1 Overview

This chapter describes how to set up user accounts and user settings for the Zyxel Device.

13.1.1 What You Can Do in this Chapter

- The **User** screen (see Section 13.2 on page 135) provides a summary of all user accounts.
- The **Setting** screen (see Section 13.3 on page 137) controls default settings, login settings, lockout settings, and other user settings for the Zyxel Device.

13.1.2 What You Need To Know

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

User Account

A user account defines the privileges of a user logged into the Zyxel Device. User accounts are used in controlling access to configuration and services in the Zyxel Device.

User Types

These are the types of user accounts the Zyxel Device uses.

Table 50 Types of User Accounts

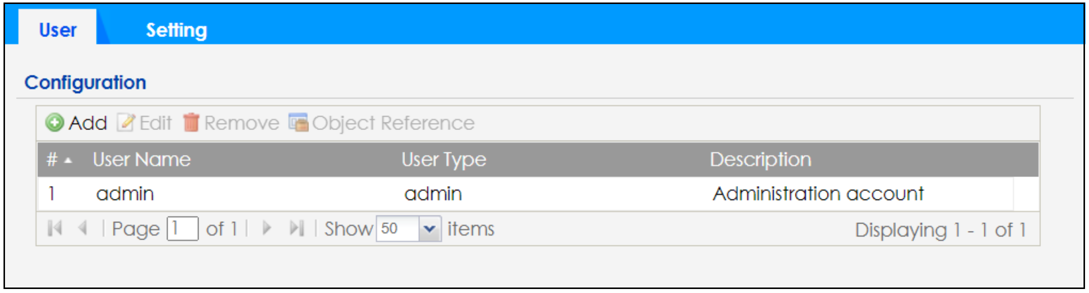
TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
admin	Change Zyxel Device configuration (web, CLI)	WWW, SSH, FTP
limited-admin	Look at Zyxel Device configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, SSH
Access Users		
user	Used for the embedded RADIUS server and SNMPv3 user access Browse user-mode commands (CLI)	

Note: The default **admin** account is always authenticated locally, regardless of the authentication method setting.

13.2 User Summary

The **User** screen provides a summary of all user accounts. To access this screen click **Configuration > Object > User**.

Figure 100 Configuration > Object > User



#	User Name	User Type	Description
1	admin	admin	Administration account

The following table describes the labels in this screen.

Table 51 Configuration > Object > User

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Object Reference	Select an entry and click **Object Reference** to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific user.
User Name	This field displays the user name of each user.
User Type	This field displays type of user this account was configured as. • **admin** - this user can look at and change the configuration of the Zyxel Device • **limited-admin** - this user can look at the configuration of the Zyxel Device but not to change it • **user** - this user has access to the Zyxel Device's services but cannot look at the configuration
Description	This field displays the description for each user.

13.2.1 Add/Edit User

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

13.2.1.1 Rules for User Names

Enter a user name from 1 to 31 characters.

The user name can only contain the following characters:

- Alphanumeric A-z 0-9 (there is no unicode support)
- _ [underscores]
- - [dashes]

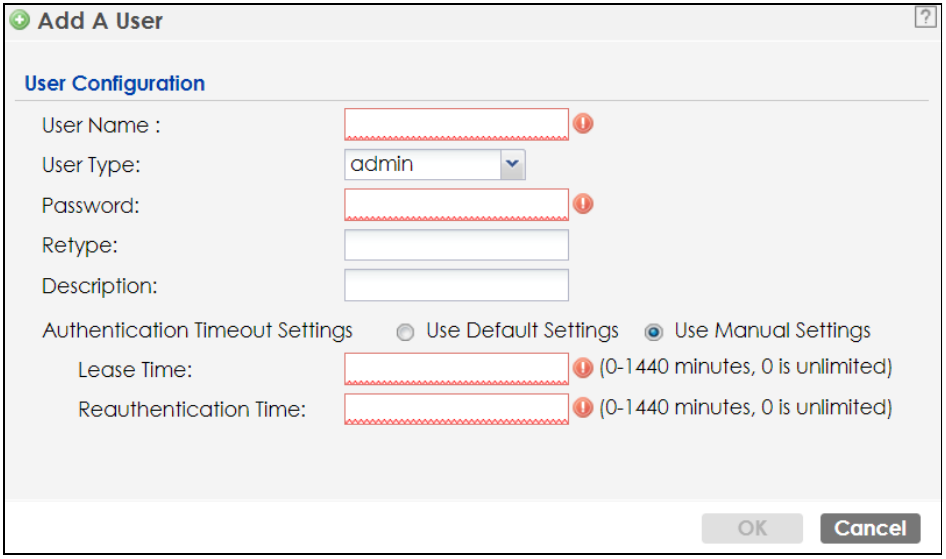
The first character must be alphabetical (A-Z a-z), an underscore (_), or a dash (-). Other limitations on user names are:

- User names are case-sensitive. If you enter a user 'bob' but use 'BOB' when connecting via CIFS or FTP, it will use the account settings used for 'BOB' not ‘bob’.
- User names have to be different than user group names.
- Here are the reserved user names:

• adm	• admin	• any	• bin	• daemon
• debug	• devicehaecived	• ftp	• games	• halt
• ldap-users	• lp	• mail	• news	• nobody
• operator	• radius-users	• root	• shutdown	• sshd
• sync	• uucp	• zyxel		

To access this screen, go to the **User** screen, and click **Add** or **Edit**.

Figure 101 Configuration > Object > User > Add/Edit A User



Add A User

User Configuration

User Name :

User Type: admin

Password:

Retype:

Description:

Authentication Timeout Settings ○ Use Default Settings ● Use Manual Settings

Lease Time: (0-1440 minutes, 0 is unlimited)

Reauthentication Time: (0-1440 minutes, 0 is unlimited)

The following table describes the labels in this screen.

Table 52 Configuration > User > User > Add/Edit A User

LABEL	DESCRIPTION
User Name	Type the user name for this user account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User names have to be different than user group names, and some words are reserved.
User Type	Select what type of user this is. Choices are: • **admin** - this user can look at and change the configuration of the Zyxel Device • **limited-admin** - this user can look at the configuration of the Zyxel Device but not to change it • **user** - this is used for embedded RADIUS server and SNMPv3 user access
Password	Enter the password of this user account. It can consist of 4 - 63 alphanumeric characters.
Retype	Re-enter the password to make sure you have entered it correctly.
Description	Enter the description of each user, if any. You can use up to 60 printable ASCII characters. Default descriptions are provided.

Table 52 Configuration > User > User > Add/Edit A User (continued)

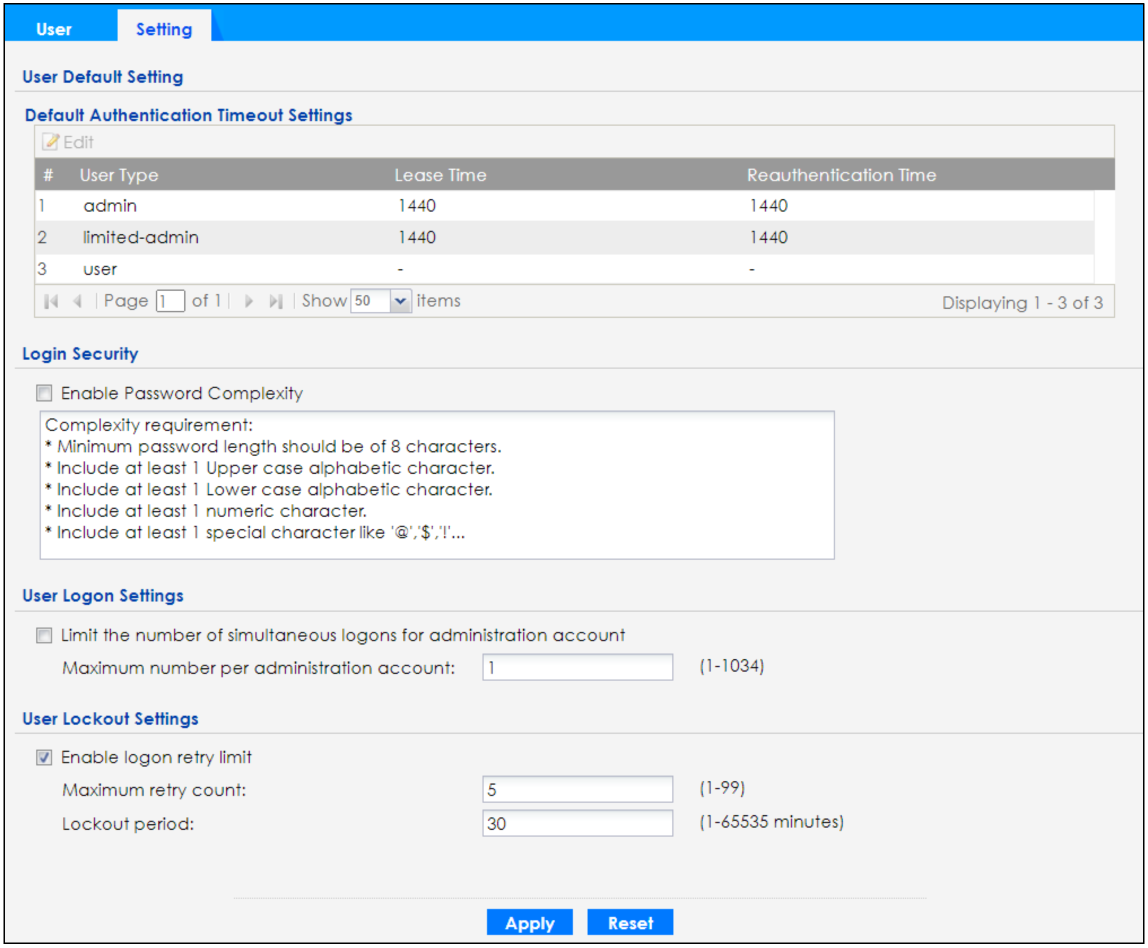
LABEL	DESCRIPTION
Authentication Timeout Settings	This field is not available if the user type is **user**. If you want to set authentication timeout to a value other than the default settings, select **Use Manual Settings** then fill your preferred values in the fields that follow. Otherwise, select **Use Default Settings** to use the default settings displayed below.
Lease Time	This field is not available if the user type is **user**. 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.
Reauthentication Time	This field is not available if the user type is **user**. 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.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

13.3 Setting

This screen controls default settings, login settings, lockout settings, and other user settings for the Zyxel Device.

To access this screen, login to the Web Configurator, and click **Configuration > Object > User > Setting**.

Figure 102 Configuration > Object > User > Setting



User Default Setting

Default Authentication Timeout Settings

#	User Type	Lease Time	Reauthentication Time
1	admin	1440	1440
2	limited-admin	1440	1440
3	user	-	-

Page 1 of 1 | Show 50 items | Displaying 1 - 3 of 3

Login Security

□ Enable Password Complexity

Complexity requirement:
* Minimum password length should be of 8 characters.
* Include at least 1 Upper case alphabetic character.
* Include at least 1 Lower case alphabetic character.
* Include at least 1 numeric character.
* Include at least 1 special character like '@','$','!'...

User Logon Settings

□ Limit the number of simultaneous logons for administration account

Maximum number per administration account: 1 (1-1034)

User Lockout Settings

☑ Enable logon retry limit

Maximum retry count: 5 (1-99)

Lockout period: 30 (1-65535 minutes)

The following table describes the labels in this screen.

Table 53 Configuration > Object > User > Setting

LABEL	DESCRIPTION
User Default Setting	
Default Authentication Timeout Settings	These authentication timeout settings are used by default when you create a new user account. They also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentication timeout settings.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
#	This field is a sequential value, and it is not associated with a specific entry.
User Type	These are the kinds of user account the Zyxel Device supports. • **admin** - this user can look at and change the configuration of the Zyxel Device • **limited-admin** - this user can look at the configuration of the Zyxel Device but not to change it • **user** - this is used for embedded RADIUS server and SNMPv3 user access
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.

Table 53   Configuration > Object > User > Setting (continued)

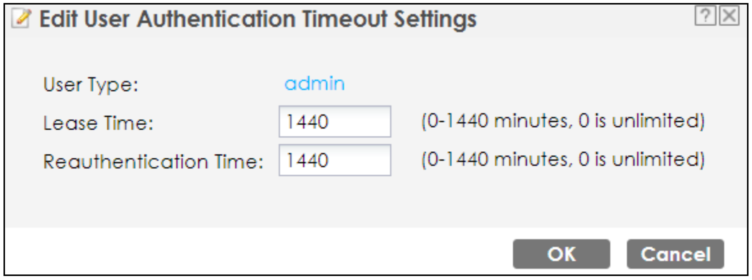
LABEL	DESCRIPTION
Reauthentication Time	This is the default reauthentication time in minutes for each type of user account. It defines the number of minutes the user can be logged into the Zyxel Device in one session before having to log in again. Unlike **Lease Time**, the user has no opportunity to renew the session without logging out.
Login Security	
Enable Password Complexity	Select this to enforce the following conditions in a user password. New user accounts will have to set passwords following this complexity rule. The password must consist of at least 8 characters and should include at least: • 1 uppercase alphabetic character. • 1 lowercase alphabetic character. • 1 numeric character. • 1 special character like '@','$','!'... Note: This does not affect the existing accounts.
User Logon Settings	
Limit the number of simultaneous logons for administration account	Select this check box if you want to set a limit on the number of simultaneous logins by admin users. If you do not select this, admin users can login as many times as they want at the same time using the same or different IP addresses.
Maximum number per administration account	This field is effective when **Limit ... for administration account** is checked. Type the maximum number of simultaneous logins by each admin user.
User Lockout Settings	
Enable logon retry limit	Select this check box to set a limit on the number of times each user can login unsuccessfully (for example, wrong password) before the IP address is locked out for a specified amount of time.
Maximum retry count	This field is effective when **Enable logon retry limit** is checked. Type the maximum number of times each user can login unsuccessfully before the IP address is locked out for the specified **lockout period**. The number must be between 1 and 99.
Lockout period	This field is effective when **Enable logon retry limit** is checked. Type the number of minutes the user must wait to try to login again, if **logon retry limit** is enabled and the **maximum retry count** is reached. This number must be between 1 and 65,535 (about 45.5 days).
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to return the screen to its last-saved settings.

13.3.1 Edit User Authentication Timeout Settings

This screen allows you to set the default authentication timeout settings for the selected type of user account. These default authentication timeout settings also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account’s authentication timeout settings.

To access this screen, go to the **Configuration > Object > User > Setting** screen, select one of the **Default Authentication Timeout Settings** entry and click the **Edit** icon.

Figure 103 User > Setting > Edit User Authentication Timeout Settings



Edit User Authentication Timeout Settings

User Type:	admin	
Lease Time:	1440	(0-1440 minutes, 0 is unlimited)
Reauthentication Time:	1440	(0-1440 minutes, 0 is unlimited)

The following table describes the labels in this screen.

Table 54 User > Setting > Edit User Authentication Timeout Settings

LABEL	DESCRIPTION
User Type	This read-only field identifies the type of user account for which you are configuring the default settings. • **admin** - this user can look at and change the configuration of the Zyxel Device. • **limited-admin** - this user can look at the configuration of the Zyxel Device but not to change it.
Lease Time	Enter the number of minutes this type of user account has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the **Renew** button on their screen. If you allow access users to renew time automatically, 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	Type the number of minutes this type of user account can be logged into the Zyxel Device in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike **Lease Time**, the user has no opportunity to renew the session without logging out.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

CHAPTER 14
AP Profile

14.1 Overview

This chapter shows you how to configure preset profiles for the Zyxel Device.

14.1.1 What You Can Do in this Chapter

- The **Radio** screen (Section 14.2 on page 146) creates radio configurations that can be used by the APs.
- The **SSID** screen (Section 14.3 on page 154) configures three different types of profiles for your networked APs.

14.1.2 What You Need To Know

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

Wireless Profiles

At the heart of all wireless AP configurations on the Zyxel Device are profiles. A profile represents a group of saved settings that you can use across any number of connected APs. You can set up the following wireless profile types:

- **Radio** - This profile type defines the properties of an AP's radio transmitter. You can have a maximum of 64 radio profiles on the Zyxel Device.
- **SSID** - This profile type defines the properties of a single WiFi network signal broadcast by an AP. Each radio on a single AP can broadcast up to 8 SSIDs. You can have a maximum of 64 SSID profiles on the Zyxel Device.
- **Security** - This profile type defines the security settings used by a single SSID. It controls the encryption method required for a WiFi client to associate itself with the SSID. You can have a maximum of 64 security profiles on the Zyxel Device.
- **MAC Filtering** - This profile provides an additional layer of security for an SSID, allowing you to block access or allow access to that SSID based on WiFi client MAC addresses. If a client's MAC address is on the list, then it is either allowed or denied, depending on how you set up the MAC Filter profile. You can have a maximum of 64 MAC filtering profiles on the Zyxel Device.
- **Layer-2 Isolation** - This profile defines the MAC addresses of the devices that you want to allow the associated WiFi clients to have access to when layer-2 isolation is enabled.

SSID

The SSID (Service Set IDentifier) is the name that identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. In other words, it is the name of the WiFi network that clients use to connect to it.

WEP

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the AP and the wireless stations associated with it in order to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

WPA2

WPA2 (IEEE 802.11i) is a WiFi security standard that defines stronger encryption, authentication and key management than WPA. Key differences between WPA2 and WEP are improved data encryption and user authentication.

WPA3

WPA3 is a WiFi security standard based on IEEE 802.11i, with security improvements like adopting enhanced PSK (Pre-Shared Key) authentication mechanism.

Personal vs Enterprise

A secure WiFi connection relies on WiFi encryption and authentication. There are two authentication modes: Personal and Enterprise.

Personal mode requires a password called Pre-Shared Key (PSK). Users enter the same PSK to connect to the WiFi network.

Enterprise mode requires an external RADIUS server for authentication. Authentication of user identity is required to connect to the WiFi network.

IEEE 802.1X

The IEEE 802.1X standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication is done using an external RADIUS server.

IEEE 802.11k/v Assisted Roaming

IEEE 802.11k is a standard for radio resource management of wireless LANs, which allows clients to request neighbor lists from the connected AP and discover the best available AP when roaming. An 802.11k neighbor list can contain up to six BSSIDs with the highest RCPI (Received Channel Power Indicator) value in both bands (5 GHz and 2.4 GHz, in the ratio of 4:2).

The IEEE 802.11v BSS Transition Management feature lets an AP automatically provide load information of the neighbor APs to clients. It helps the Zyxel Device steer clients to a suitable AP for better performance or load balancing.

WiFi 6 (IEEE 802.11ax)

WiFi 6 (802.11ax) is a WiFi standard that supports both 2.4 GHz and 5 GHz frequency bands and brings the following improvements over WiFi 5:

Faster Data Transmission

WiFi 6 allows faster data transmission using:

- 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, such as a campus or a company office that have multiple client devices using:

- OFDMA (Orthogonal Frequency-Division Multiple Access) – allows multiple WiFi clients to transmit data simultaneously on a single OFDM symbol by dividing sub-carriers into groups as transmission units called Resource Units (RUs). The AP then allocates RUs to different WiFi clients for data transmissions at the same time.
- BSS Coloring – tags traffic by Basic Service Set (BSS) 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 downlink/uplink 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

TWT (Target Wake Time) – The AP negotiates with client devices so client devices only wake up and communicate with the AP in specific periods. This conserves the battery life of client devices.

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.

Below is a comparison table that shows the main differences between WiFi 6 and WiFi 6E.

Table 55 WiFi 6 and WiFi 6E Comparison

FEATURES	WIFI 6	WIFI 6E
Theoretical Maximum Speed (Up-to)	The same (9.6 Gbps).	
Supported Frequency Bands	2.4 GHz/5 GHz	2.4 GHz/5 GHz/6 GHz
Supported Channel Bandwidth	20/40/80/160 MHz	20/40/80/160 MHz

Table 55 WiFi 6 and WiFi 6E Comparison

FEATURES		WIFI 6	WIFI 6E
Total Spectrum (Up-to)	2.4 GHz	80 MHz	
	5 GHz	500 MHz	
	6 GHz	Not supported.	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 6E MBSSID Beacon Management

The Zyxel Device supports MBSSID (see Section 1.4.1 on page 26), which allows you to create multiple virtual WiFi networks (SSIDs) on the Zyxel Device. With the WiFi 6E (802.11ax-extended) standard, the Zyxel Device 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 56 WiFi 6, WiFi 6E and WiFi 7 Comparison

FEATURES	WIFI 6	WIFI 6E	WIFI 7
Theoretical Maximum Speed (Up-to)	The same (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

Table 56 WiFi 6, WiFi 6E and WiFi 7 Comparison

FEATURES		WIFI 6	WIFI 6E	WIFI 7
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

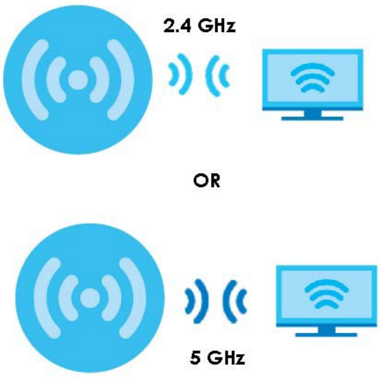
WiFi 7 allows faster data transmission using:

- 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 104 Without Multi-Link Operation

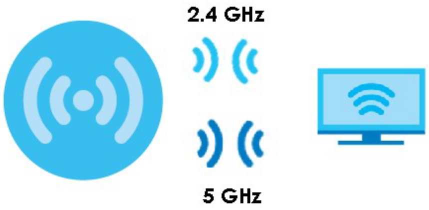


WiFi 7 MLO allows a WiFi client to connect to the AP using multiple frequency bands simultaneously. This increases speed and improves reliability of the WiFi connection. MLO makes WiFi 7 ideal for streaming 4K/8K videos, using augmented reality (AR), virtual reality (VR) applications and playing online games.

To use MLO, both the AP and the WiFi client have to support MLO.

Note: The Zyxel Device does not support MLO at the time of writing.

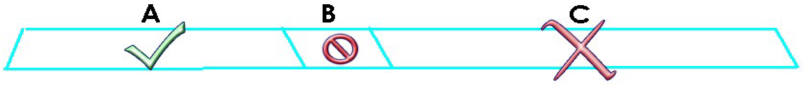
Figure 105 Multi-Link Operation Example



Preamble Puncturing

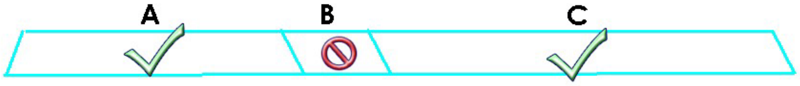
In WiFi 6 and earlier, any interference would cause the entire WiFi channel to become unavailable. In the figure below, if part of the WiFi channel (**B**) experiences interference, the rest of the WiFi channel (**C**) becomes unavailable.

Figure 106 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 107 Preamble Puncturing Example

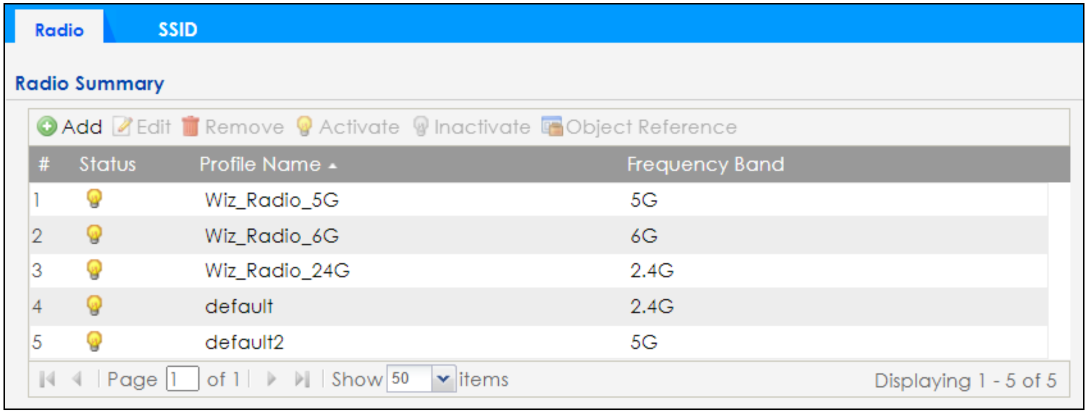


14.2 Radio

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

Note: You can have a maximum of 32 radio profiles on the Zyxel Device.

Figure 108 Configuration > Object > AP Profile > Radio



#	Status	Profile Name	Frequency Band
1	●	Wiz_Radio_5G	5G
2	●	Wiz_Radio_6G	6G
3	●	Wiz_Radio_24G	2.4G
4	●	default	2.4G
5	●	default2	5G

The following table describes the labels in this screen.

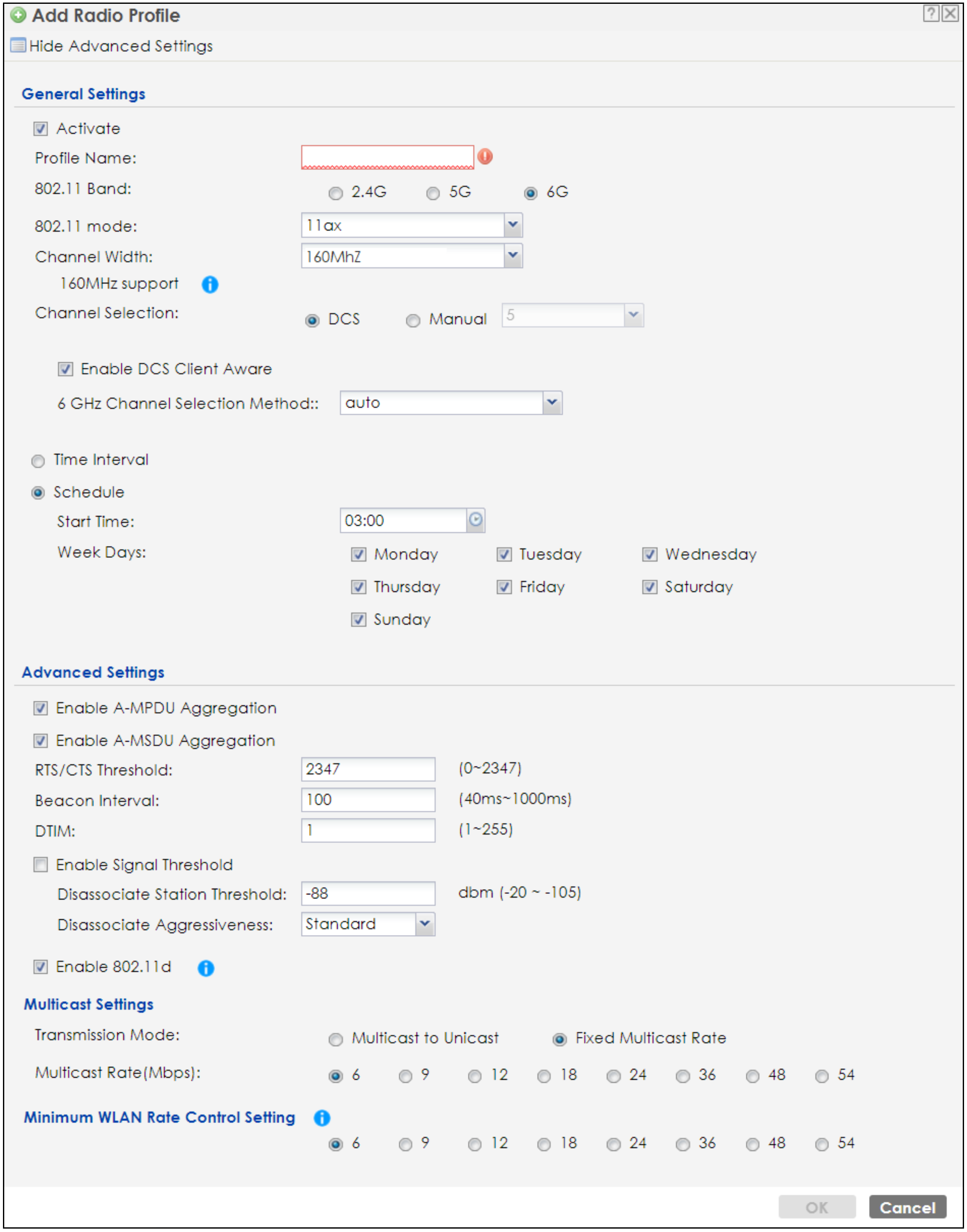
Table 57 Configuration > Object > AP Profile > Radio

LABEL	DESCRIPTION
Add	Click this to add a new radio profile.
Edit	Click this to edit the selected radio profile.
Remove	Click this to remove the selected radio profile.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Object Reference	Click this to view which other objects are linked to the selected radio profile.
#	This field is a sequential value, and it is not associated with a specific user.
Status	This field shows whether or not the entry is activated. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Profile Name	This field indicates the name assigned to the radio profile.
Frequency Band	This field indicates the frequency band which this radio profile is configured to use.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

14.2.1 Add/Edit Radio Profile

This screen allows you to create a new radio profile or edit an existing one. To access this screen, click the **Add** button or select a radio profile from the list and click the **Edit** button.

Figure 109 Configuration > Object > AP Profile > Radio > Add/Edit



Add Radio Profile

Hide Advanced Settings

General Settings

☑ Activate

Profile Name:

802.11 Band: ○ 2.4G ○ 5G ● 6G

802.11 mode: 11ax

Channel Width: 160MhZ

160MHz support

Channel Selection: ● DCS ○ Manual 5

☑ Enable DCS Client Aware

6 GHz Channel Selection Method:: auto

○ Time Interval

● Schedule

Start Time: 03:00

Week Days: ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

Advanced Settings

☑ Enable A-MPDU Aggregation

☑ Enable A-MSDU Aggregation

RTS/CTS Threshold: 2347 (0~2347)

Beacon Interval: 100 (40ms~1000ms)

DTIM: 1 (1~255)

□ Enable Signal Threshold

Disassociate Station Threshold: -88 dbm (-20 ~ -105)

Disassociate Aggressiveness: Standard

☑ Enable 802.11d

Multicast Settings

Transmission Mode: ○ Multicast to Unicast ● Fixed Multicast Rate

Multicast Rate(Mbps): ● 6 ○ 9 ○ 12 ○ 18 ○ 24 ○ 36 ○ 48 ○ 54

Minimum WLAN Rate Control Setting

● 6 ○ 9 ○ 12 ○ 18 ○ 24 ○ 36 ○ 48 ○ 54

The following table describes the labels in this screen.

Table 58 Configuration > Object > AP Profile > Radio > Add/Edit

LABEL	DESCRIPTION
Hide / Show Advanced Settings	Click this to hide or show the **Advanced Settings** in this window.
General Settings	
Activate	Select this option to make this profile active.
Profile Name	Enter up to 31 alphanumeric characters to be used as this profile's name. Spaces and underscores are allowed.
802.11 Band	Select whether this radio will use the 2.4 GHz, 5 GHz, or 6 GHz band.
802.11 Mode	Select how to let WiFi clients connect to the AP. If **802.11 Band** is set to **2.4G**: • **11b/g**: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the Zyxel Device. The Zyxel Device adjusts the transmission rate automatically according to the WiFi standard supported by the wireless devices. • **11n**: allows IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the Zyxel Device. • **11ax**: allows IEEE802.11b, IEEE802.11g, IEEE802.11n, and IEEE802.11ax compliant WLAN devices to associate with the Zyxel Device. If the WLAN device isn't compatible with 802.11ax, the Zyxel Device will communicate with the WLAN device using 802.11n, and so on. • **11be:** allows IEEE802.11b, IEEE802.11g, IEEE802.11n, IEEE802.11ax and IEEE802.11be compliant WLAN devices to associate with the Zyxel Device. If the WLAN device isn't compatible with 802.11be, the Zyxel Device will communicate with the WLAN device using 802.11ax, and so on. If **802.11 Band** is set to **5G**: • **11a**: allows only IEEE 802.11a compliant WLAN devices to associate with the Zyxel Device. • **11n**: allows both IEEE802.11n and IEEE802.11a compliant WLAN devices to associate with the Zyxel Device. • **11ac**: allows IEEE802.11n, IEEE802.11a, and IEEE802.11ac compliant WLAN devices to associate with the Zyxel Device. If the WLAN device isn't compatible with 802.11ac, the Zyxel Device will communicate with the WLAN device using 802.11n, and so on. • **11ax**: allows IEEE802.11n, IEEE802.11a, IEEE802.11ac, and IEEE802.11ax compliant WLAN devices to associate with the Zyxel Device. If the WLAN device isn't compatible with 802.11ax, the Zyxel Device will communicate with the WLAN device using 802.11ac, and so on. • **11be:** allows IEEE802.11a, IEEE802.11n, IEEE802.11ac, IEEE802.11ax and IEEE802.11be compliant WLAN devices to associate with the Zyxel Device. If the WLAN device isn't compatible with 802.11be, the Zyxel Device will communicate with the WLAN device using 802.11ax, and so on. If **802.11 Band** is set to **6G**: • **11ax**: allows IEEE802.11ax compliant WLAN devices to associate with the Zyxel Device. • **11be**: allows IEEE802.11be compliant WLAN devices to associate with the Zyxel Device. If the WLAN device isn't compatible with 802.11be, the Zyxel Device will communicate with the WLAN device using 802.11ax.