ZYXEL
Your Networking Ally

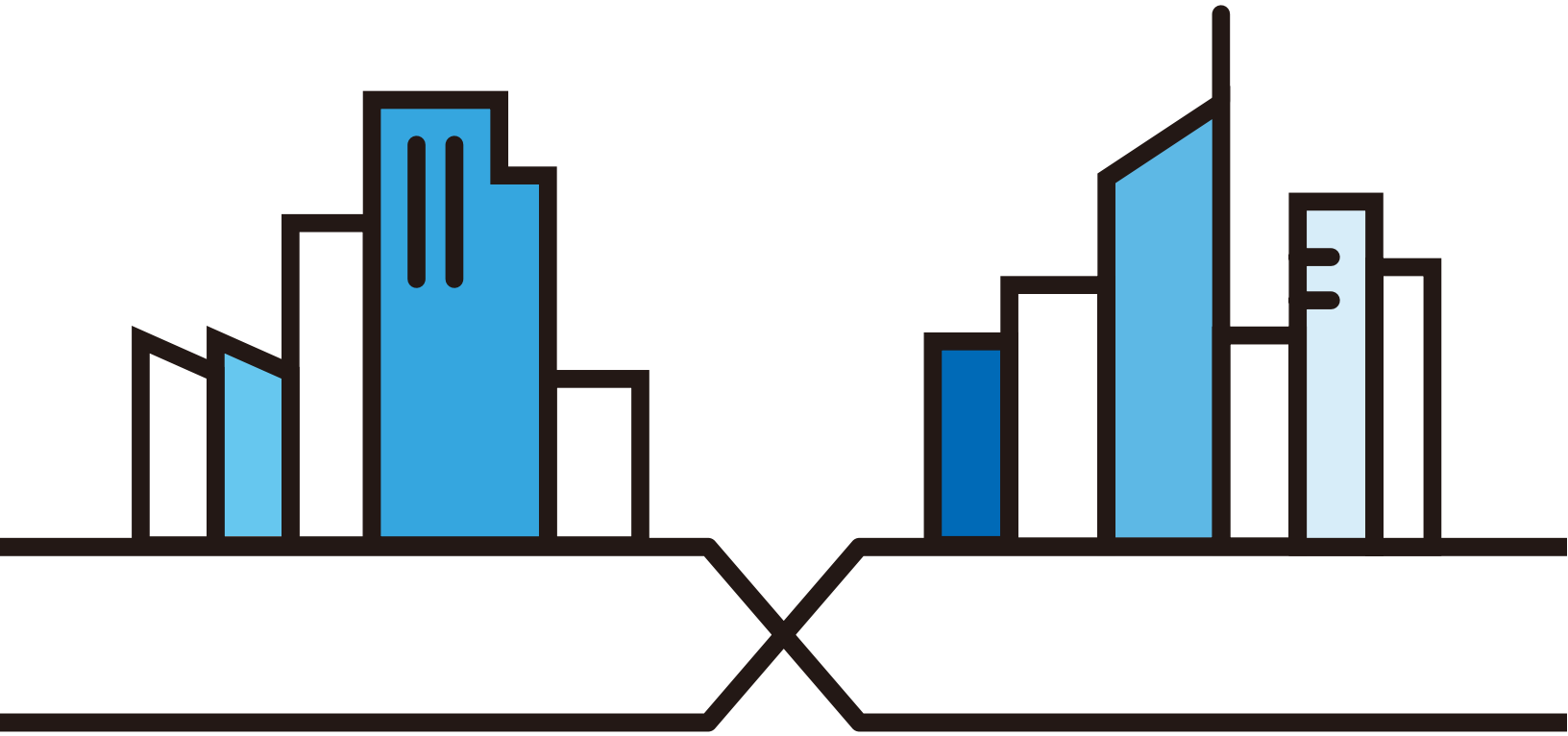
User's Guide

NWA/WAC/WAX Series

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

Version 6.00 Edition 1, 12/2019

Default Login Details	
LAN IP Address	DHCP-assigned IP OR 192.168.1.2
User Name	admin
Password	1234



Copyright © 2019 Zyxel Communications Corporation

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

This is a User's Guide for a series of products. Not all products support all firmware features. Screenshots and graphics in this book may differ slightly from your product due to differences in 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 1.4 on page 19).

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 24).

- NXC Series User's Guide

  See this User's Guide for instructions on using the NXC as an AP Controller (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	AP Controller
Printer	Nebula Switch	Nebula Gateway	Smart T.V.
IP Phone			

Contents Overview

Introduction 13
AP Management 24
Hardware 33
The Web Configurator 53

Standalone Configuration 64

Standalone Configuration 65
Dashboard 67
Setup Wizard 73
Monitor 79
Network 94
Wireless 105
Bluetooth 120
User 123
AP Profile 130
MON Profile 150
WDS Profile 153
Certificates 155
System 171
Log and Report 194
File Manager 206
Diagnostics 217
LEDs 219
Antenna Switch 222
Reboot 224
Shutdown 225

Local Configuration in Cloud Mode 226

Cloud Mode 227
Dashboard 229
Network 231
Maintenance 234

Appendices and Troubleshooting 239

Troubleshooting 240

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 Roles 13
1.2.1 Root AP 14
1.2.2 Wireless Repeater 14
1.2.3 Radio Frequency (RF) Monitor 15
1.3 Sample Feature Applications 17
1.3.1 MBSSID 17
1.3.2 Dual-Radio 18
1.4 Zyxel Device Product Feature Comparison 19

Chapter 2
AP Management 24

2.1 Management Mode 24
2.1.1 Standalone 24
2.1.2 Nebula Control Center 24
2.1.3 AP Controller (AC) 26
2.2 Switching Management Modes 26
2.3 Zyxel One Network (ZON) Utility 27
2.3.1 Requirements 27
2.3.2 Run the ZON Utility 28
2.4 Ways to Access the Zyxel Device 31
2.5 Good Habits for Managing the Zyxel Device 32

Chapter 3
Hardware 33

3.1 Grounding (WAC6552D-S and WAC6553D-E) 33
3.2 Zyxel Device Models With Single LEDs 34
3.2.1 NWA1123-ACv2 34
3.2.2 WAC6303D-S and NWA5123-AC HD 36
3.2.3 NWA1123-AC HD 37
3.2.4 NWA5123-AC 39
3.2.5 NWA110AX, WAX510D and WAX650S 40

3.3 Zyxel Device Models With Multiple LEDs 42
3.3.1 NWA1123-AC PRO 42
3.3.2 NWA1302-AC 44
3.3.3 WAC6502D-E, WAC6502D-S, and WAC6503D-S 46
3.3.4 WAC6103D-I 48
3.3.5 WAC5302D-S 50

Chapter 4
The Web Configurator 53

4.1 Overview 53
4.2 Accessing the Web Configurator 53
4.3 Navigating the Web Configurator 55
4.3.1 Title Bar 56
4.3.2 Navigation Panel 58
4.3.3 Standalone Mode Navigation Panel Menus 58
4.3.4 Cloud Mode Navigation Panel Menus 60
4.3.5 Tables and Lists 61

Part I: Standalone Configuration 64

Chapter 5
Standalone Configuration 65

5.1 Overview 65
5.2 Starting and Stopping the Zyxel Device 65

Chapter 6
Dashboard 67

6.1 Overview 67
6.1.1 CPU Usage 70
6.1.2 Memory Usage 71

Chapter 7
Setup Wizard 73

7.1 Accessing the Wizard 73
7.2 Using the Wizard 73
7.2.1 Step 1 Time Settings 73
7.2.2 Step 2 Password and Uplink Connection 74
7.2.3 Step 3 Radio 75
7.2.4 Step 4 SSID 76
7.2.5 Summary 78

Chapter 8
Monitor 79

8.1 Overview 79
8.1.1 What You Can Do in this Chapter 79
8.2 What You Need to Know 79
8.3 Network Status 80
8.3.1 Port Statistics Graph 81
8.4 Radio List 82
8.4.1 AP Mode Radio Information 84
8.5 Station List 86
8.6 WDS Link Info 87
8.7 Detected Device 88
8.8 View Log 91

Chapter 9
Network 94

9.1 Overview 94
9.1.1 AP Controller Management 94
9.1.2 What You Can Do in this Chapter 96
9.2 IP Setting 97
9.3 VLAN 98
9.4 Storm Control 101
9.5 AC (AP Controller) Discovery 102
9.6 NCC Discovery 103

Chapter 10
Wireless 105

10.1 Overview 105
10.1.1 What You Can Do in this Chapter 105
10.1.2 What You Need to Know 106
10.2 AP Management 106
10.3 Rogue AP 109
10.3.1 Add/Edit Rogue/Friendly List 113
10.4 Load Balancing 114
10.4.1 Disassociating and Delaying Connections 115
10.5 DCS 116
10.6 Technical Reference 117

Chapter 11
Bluetooth 120

11.1 Overview 120
11.1.1 What You Need To Know 120
11.2 Bluetooth Advertising Settings 121

11.2.1 Edit Advertising Settings 121

Chapter 12
User 123

12.1 Overview 123
12.1.1 What You Can Do in this Chapter 123
12.1.2 What You Need To Know 123
12.2 User Summary 124
12.2.1 Add/Edit User 124
12.3 Setting 126
12.3.1 Edit User Authentication Timeout Settings 128

Chapter 13
AP Profile 130

13.1 Overview 130
13.1.1 What You Can Do in this Chapter 130
13.1.2 What You Need To Know 130
13.2 Radio 131
13.2.1 Add/Edit Radio Profile 132
13.3 SSID 137
13.3.1 SSID List 137
13.3.2 Add/Edit SSID Profile 139
13.4 Security List 141
13.4.1 Add/Edit Security Profile 142
13.5 MAC Filter List 146
13.5.1 Add/Edit MAC Filter Profile 146
13.6 Layer-2 Isolation List 147
13.6.1 Add/Edit Layer-2 Isolation Profile 149

Chapter 14
MON Profile 150

14.1 Overview 150
14.1.1 What You Can Do in this Chapter 150
14.2 MON Profile 150
14.2.1 Add/Edit MON Profile 151

Chapter 15
WDS Profile 153

15.1 Overview 153
15.1.1 What You Can Do in this Chapter 153
15.2 WDS Profile 153
15.2.1 Add/Edit WDS Profile 154

Chapter 16
Certificates 155

16.1 Overview 155
16.1.1 What You Can Do in this Chapter 155
16.1.2 What You Need to Know 155
16.1.3 Verifying a Certificate 157
16.2 My Certificates 158
16.2.1 Add My Certificates 159
16.2.2 Edit My Certificates 161
16.2.3 Import Certificates 164
16.3 Trusted Certificates 165
16.3.1 Edit Trusted Certificates 166
16.3.2 Import Trusted Certificates 169
16.4 Technical Reference 170

Chapter 17
System 171

17.1 Overview 171
17.1.1 What You Can Do in this Chapter 171
17.2 Host Name 171
17.3 Power Mode 172
17.4 Date and Time 173
17.4.1 Pre-defined NTP Time Servers List 175
17.4.2 Time Server Synchronization 175
17.5 WWW Overview 176
17.5.1 Service Access Limitations 176
17.5.2 System Timeout 176
17.5.3 HTTPS 177
17.5.4 Configuring WWW Service Control 177
17.5.5 HTTPS Example 178
17.6 SSH 184
17.6.1 How SSH Works 185
17.6.2 SSH Implementation on the Zyxel Device 186
17.6.3 Requirements for Using SSH 186
17.6.4 Configuring SSH 186
17.6.5 Examples of Secure Telnet Using SSH 187
17.7 Telnet 188
17.8 FTP 189
17.9 SNMP 190
17.9.1 Supported MIBs 191
17.9.2 SNMP Traps 191
17.9.3 Configuring SNMP 191
17.9.4 Adding or Editing an SNMPv3 User Profile 192

Chapter 18
Log and Report 194

18.1 Overview 194
18.1.1 What You Can Do In this Chapter 194
18.2 Email Daily Report 194
18.3 Log Setting 196
18.3.1 Log Setting Screen 197
18.3.2 Edit System Log Settings 198
18.3.3 Edit Remote Server 202
18.3.4 Active Log Summary 203

Chapter 19
File Manager 206

19.1 Overview 206
19.1.1 What You Can Do in this Chapter 206
19.1.2 What you Need to Know 206
19.2 Configuration File 207
19.2.1 Example of Configuration File Download Using FTP 211
19.3 Firmware Package 212
19.3.1 Example of Firmware Upload Using FTP 213
19.4 Shell Script 214

Chapter 20
Diagnostics 217

20.1 Overview 217
20.1.1 What You Can Do in this Chapter 217
20.2 Diagnostics 217

Chapter 21
LEDs 219

21.1 Overview 219
21.1.1 What You Can Do in this Chapter 219
21.2 Suppression Screen 219
21.3 Locator Screen 220

Chapter 22
Antenna Switch 222

22.1 Overview 222
22.1.1 What You Need To Know 222
22.2 Antenna Switch Screen 222

Chapter 23
Reboot 224

23.1 Overview 224
23.1.1 What You Need To Know 224
23.2 Reboot 224

Chapter 24
Shutdown 225

24.1 Overview 225
24.1.1 What You Need To Know 225
24.2 Shutdown 225

Part II: Local Configuration in Cloud Mode 226

Chapter 25
Cloud Mode 227

25.1 Overview 227
25.2 Cloud Mode Web Configurator Screens 227

Chapter 26
Dashboard 229

Chapter 27
Network 231

27.1 Overview 231
27.1.1 What You Can Do in this Chapter 231
27.2 IP Setting 231
27.3 VLAN 233

Chapter 28
Maintenance 234

28.1 Overview 234
28.1.1 What You Can Do in this Chapter 234
28.2 Shell Script 234
28.3 Diagnostics 235
28.4 View Log 236

Part III: Appendices and Troubleshooting 239

Chapter 29
Troubleshooting 240

29.1 Overview 240

29.2 Power, Hardware Connections, and LED 240
29.3 Zyxel Device Management, Access, and Login 241
29.4 Internet Access 245
29.5 WiFi Network 246
29.6 Resetting the Zyxel Device 247
29.7 Getting More Troubleshooting Help 248

Appendix A Importing Certificates 249

Appendix B IPv6 273

Appendix C Customer Support 281

Appendix D Legal Information 287

Index 300

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 NXC, 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)

- NWA5123-AC HD
- WAC6103D-I
- WAC6303D-S
- WAC6502D-E
- WAC6502D-S
- WAC6503D-S
- WAC6552D-S
- WAC6553D-E
- WAX510D
- WAX650S

NCC or Standalone (NebulaFlex)

- NWA1123-ACv2
- NWA1123-AC PRO
- NWA1123-AC HD
- NWA1302-AC
- NWA110AX

AC or Standalone

- NWA5123-AC
- WAC5302D-S

For more information about Access Point (AP) management, see Section 2.1 on page 24.

Use the Zyxel Device to set up a wireless network with other IEEE 802.11a/b/g/n/ac/ax compatible devices in either 2.4GHz and 5GHz networks or both at the same time.

When two or more APs are interconnected, this network is called a Wireless Distribution System (WDS). See Section 1.2.2 on page 14 for more information on root and repeater APs and how to set them up.

1.2 Zyxel Device Roles

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 1.4 on page 19). The Zyxel Device can serve as a:

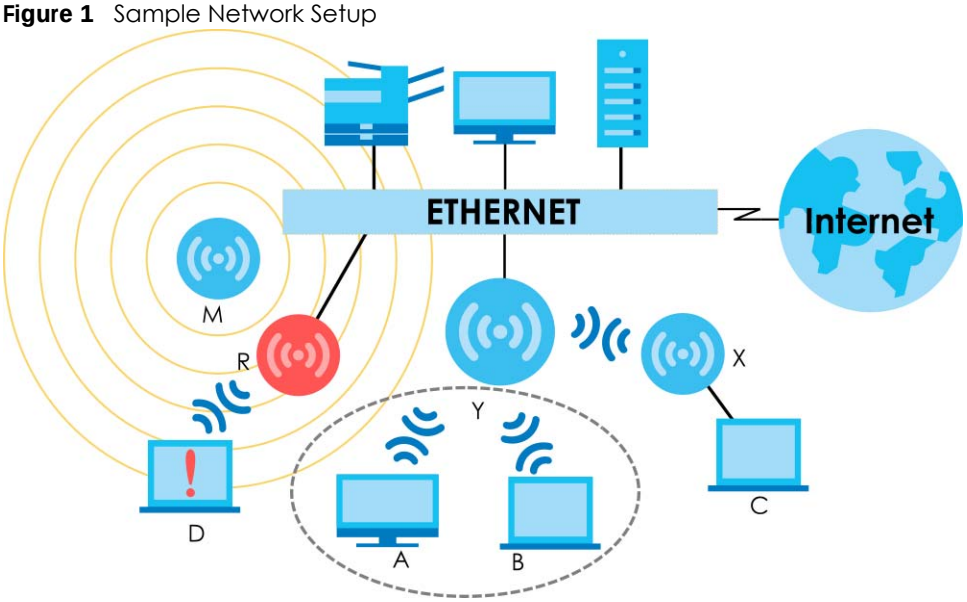
- Access Point (AP) - This is used to allow wireless clients to connect to the Internet.
- Radio Frequency (RF) monitor - An RF monitor searches for rogue APs to help eliminate network threats if it supports monitor mode and rogue APs detection/containment. An RF monitor cannot simultaneously act as 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.

- Wireless repeater - A wireless repeater wirelessly connects to a root AP and extends the network's wireless range.

The following figure shows a network setup that uses these different roles to create a secure Wireless Distribution System (WDS). The root AP (**Y**) is connected to a network with Internet access and has a wireless repeater (**X**) connected to it to expand the wireless network's range. Clients (**A, B,** and **C**) can access the wired network through the wireless repeater and/or root AP.

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 or use the NXC to quarantine them.

Figure 1 Sample Network Setup



1.2.1 Root AP

In Root AP mode, you can have multiple SSIDs active for regular wireless connections and one SSID for the connection with a repeater (repeater SSID). Wireless 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.

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 wireless clients and the AP or repeater. When repeater security is enabled, both APs and repeaters must use the same pre-shared key. See Section 10.2 on page 106 and Section 15.2 on page 153 for more details.

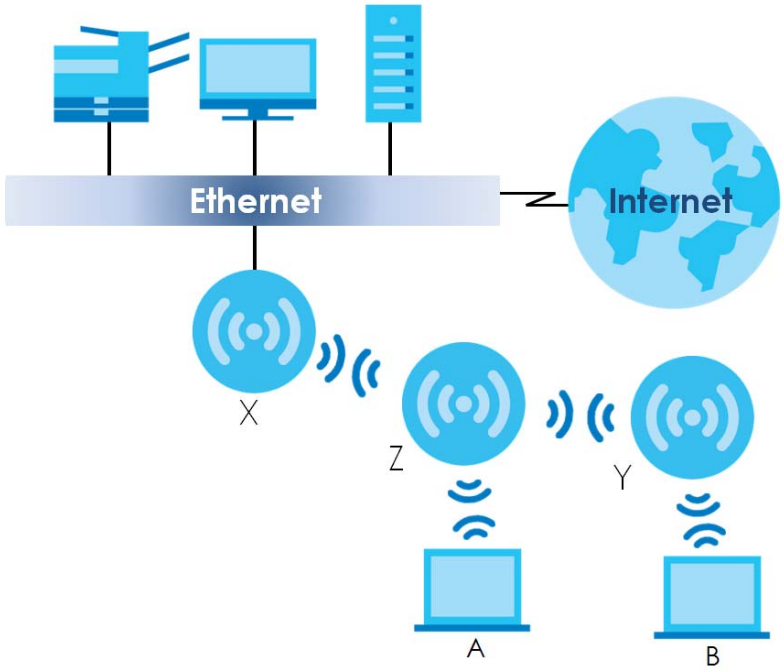
Unless specified, the term "security settings" refers to the traffic between the wireless clients and the AP. At the time of writing, repeater security is compatible with the Zyxel Device only.

1.2.2 Wireless Repeater

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 wireless connection to the Zyxel Device in Root AP mode (**X**) which is connected to a wired network and also has a wireless connection to another Zyxel Device in Repeater mode (**Y**) at the same time. **Z** and **Y** act as repeaters that forward traffic between associated

wireless 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 2 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 wireless clients and the AP or repeater. When repeater security is enabled, both APs and repeaters must use the same pre-shared key. See Section 10.2 on page 106 and Section 15.2 on page 153 for more details.

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

To set up a WDS in standalone mode APs, do the following steps. You should already have the root AP set up (see the Quick Start Guide for hardware connections).

1. Go to **Configuration > Object > WDS Profile** in your root AP web configurator and click **Add**.
2. Enter a profile name, an SSID for the WDS, and a pre-shared key.
3. Do steps 1 and 2 for the wireless repeater using the same SSID and pre-shared key.
4. Once the security settings of peer sides match one another, the connection between the root and repeater Zyxel Devices is made.

To set up a WDS in NXC managed Zyxel Devices, see the NXC User's Guide.

1.2.3 Radio Frequency (RF) Monitor

The Zyxel Device can 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 quarantine them if the Zyxel Device is

managed by the NXC (see Section 2.1.3 on page 26). If the Zyxel Device's radio setting is set to **MON Mode** (RF Monitor mode), it will serve as a dedicated RF monitor and its AP clients are disconnected.

The models that do not support **MON Mode** support **Rogue AP Detection** (see Section 10.3 on page 109). **Rogue AP Detection** allows the AP to scan all channels similar to **MON Mode** except that the Zyxel Device still works as an AP while it scans the environment for wireless signals. To see which Zyxel Devices support the RF Monitor feature, see Section 1.4 on page 19.

The Zyxel Device in **MON Mode** scans a range of WiFi channels that you specify in a **MON Profile**, either in the 2.4 GHz or 5 GHz band. To scan both bands, you need to set both radio 1 and radio 2 in **MON Mode**. Once a rogue AP is detected, the network administrator can manually change the network settings to limit its access to the network using its MAC address or have the device physically removed. If the Zyxel Device is managed by an NXC, the network administrator can also use **Rogue AP Containment** through the NXC.

MON Mode in Standalone Mode

To use an RF monitor in standalone mode, do the following steps:

1. Create a **MON Profile** in **Configuration > Object > MON Profile > Add**. Specify a **Channel dwell time** to determine how long the RF monitor scans a specific channel before moving to the next one.
2. To scan all 2.4 GHz and 5 GHz channels, select **auto** in **Scan Channel Mode**. Make sure that the **Activate** check box is selected and click **OK**.
3. Go to the **Configuration > Wireless > AP Management** screen and set **Radio 1 OP Mode** (2.4 GHz) and/or **Radio 2 OP Mode** (5 GHz) to **MON Mode**.
4. Select the **Radio 1(2) Profile** that you created in the previous step. Make sure that the **Radio 1(2) Activate** check box is selected and click **Apply**.
5. Go to **Monitor > Wireless > Detected Device** to see a list of APs scanned by the RF monitor.
6. Select an AP or APs in the list and click **Mark as Rogue AP** or **Mark as Friendly AP**.

MON Mode in NXC-Managed Zyxel Devices

For NXC-managed Zyxel Devices, do the following steps in the NXC web configurator:

1. Create a **MON Profile** in **CONFIGURATION > Object > MON Profile > Add**. Specify a **Channel dwell time** to determine how long the RF monitor scans a specific channel before moving to the next one.
2. To scan all 2.4 GHz and 5 GHz channels, select **auto** in **Scan Channel Mode**. Make sure that the **Activate** check box is selected and click **OK**.
3. Go to the **CONFIGURATION > Wireless > AP Management > Mgmt. AP List > Edit** screen and/or set **Radio 1 OP Mode** (2.4 GHz) and **Radio 2 OP Mode** (5 GHz) to **MON Mode**.
4. Select the **Radio 1(2) Profile** that you created in the previous step. Select **Override Group Radio Setting** and click **OK**.
5. Go to **MONITOR > Wireless > Detected Device** to see a list of APs scanned by the RF monitor.

6 Select an AP or APs in the list and click **Mark as Rogue AP** or **Mark as Friendly AP**.

7 To quarantine a rogue AP, go to **CONFIGURATION > Wireless > Rogue AP**, select the APs you want to quarantine, and click **Containment**. Make sure the **Enable Rogue AP Containment** check box is selected, and click **Apply**.

1.3 Sample Feature Applications

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

1.3.1 MBSSID

A Basic Service Set (BSS) is the set of devices forming a single wireless network (usually an access point and one or more wireless 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.

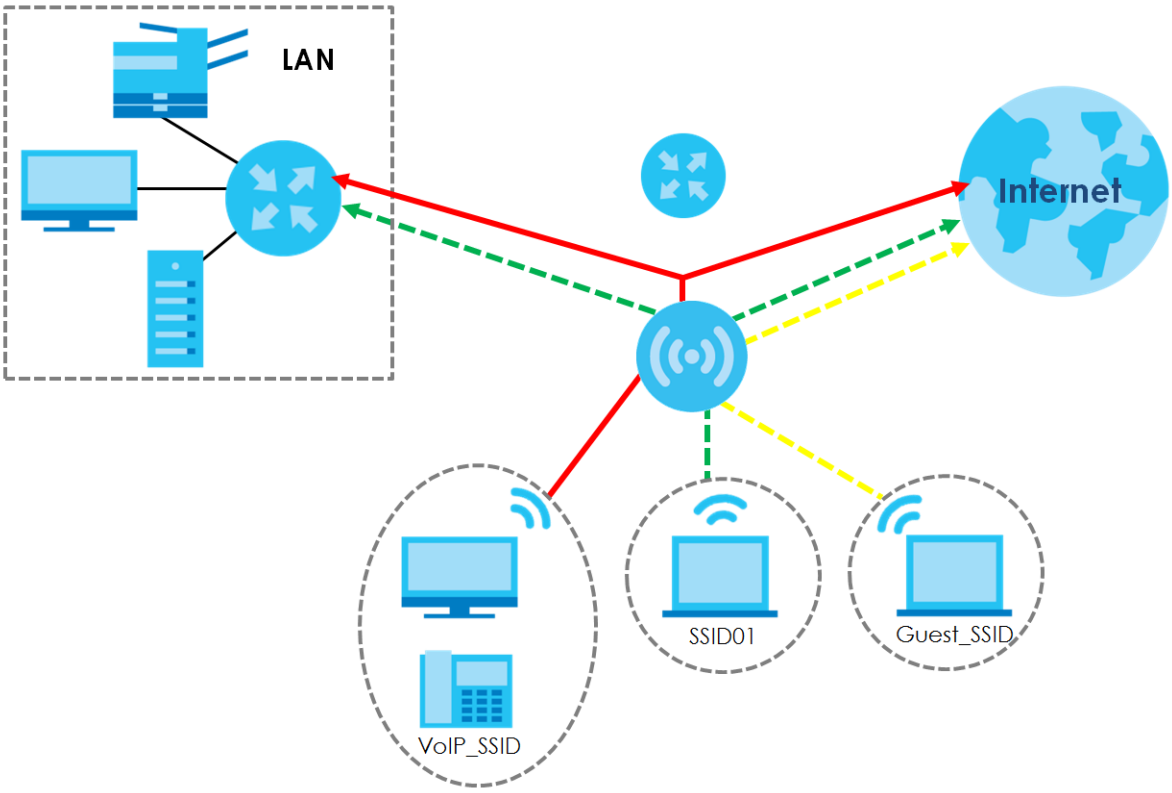
You can configure multiple SSID profiles, and have all of them active at any one time.

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 wireless clients in the network, each SSID appears to be a different access point. As in any wireless 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 wireless network in your office where Internet telephony (VoIP) users have priority. You also want a regular wireless network for standard users, as well as a 'guest' wireless network for visitors. In the following figure, **VoIP_SSID** users have QoS priority, **SSID01** is the wireless network for standard users, and **Guest_SSID** is the wireless network for guest users. In this example, the guest user is forbidden access to the wired Land Area Network (LAN) behind the AP and can access only the Internet.

Figure 3 Multiple BSSs



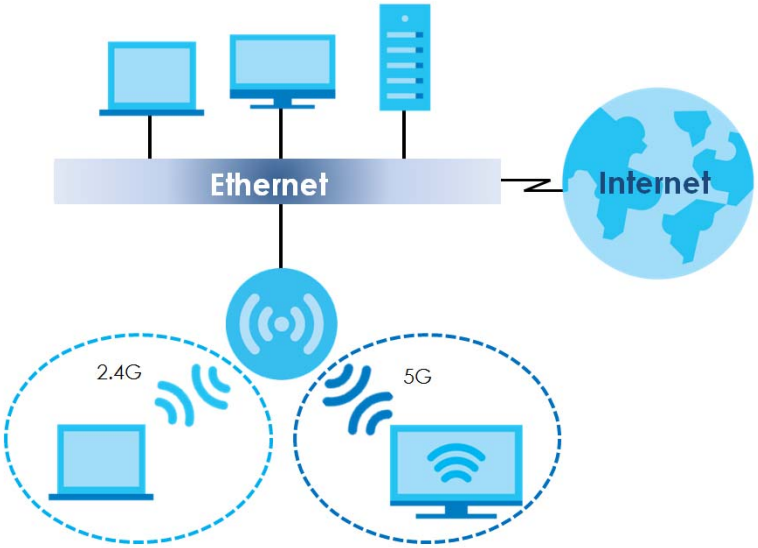
1.3.2 Dual-Radio

Some of the Zyxel Device models are equipped with dual wireless radios. This means you can configure two different wireless networks to operate simultaneously.

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 band for time sensitive traffic like high-definition video, music, and gaming.

Figure 4 Dual-Radio Application



1.4 Zyxel Device Product Feature Comparison

The following tables show the differences between each Zyxel Device model.

Table 1 Zyxel Device 1000/5000 Series Comparison Table

FEATURES	NWA1123-ACv2	NWA1123-AC PRO	NWA1123-AC HD	NWA110AX	NWA1302-AC	NWA5123-AC	NWA5123-AC HD	WAC5302D-S
Supported Wireless 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	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 802.11a 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	2.4 GHz 5 GHz	2.4 GHz 5 GHz	2.4 GHz 5 GHz	2.4 GHz 5 GHz	2.4 GHz 5 GHz
Available Security Modes	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX Enhanced-open WPA3-enterprise WPA3-personal	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX
Number of SSID Profiles	64	64	64	64	64	64	64	64
Number of Wireless Radios	2	2	2	2	2	2	2	2

Table 1 Zyxel Device 1000/5000 Series Comparison Table

FEATURES	NWA1123-ACv2	NWA1123-AC PRO	NWA1123-AC HD	NWA110AX	NWA1302-AC	NWA5123-AC	NWA5123-AC HD	WAC5302D-S
Monitor Mode & Rogue APs Containment[A]	No	No	No	No	No	Yes	No	No
Rogue AP Detection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WDS (Wireless Distribution System) - Root AP & Repeater Modes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Tunnel Forwarding Mode	No	No	No	No	No	No	No	No
Layer-2 Isolation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Supported PoE Standards	IEEE 802.3af IEEE 802.3at	IEEE 802.3af IEEE 802.3at	IEEE 802.3af IEEE 802.3at	IEEE 802.3af IEEE 802.3at	IEEE 802.3af IEEE 802.3at	IEEE 802.3af IEEE 802.3at	IEEE 802.3af IEEE 802.3at	IEEE 802.3af IEEE 802.3at
Power Detection	No	No	Yes	Yes	Yes	No	Yes	Yes
External Antennas	No	No	No	No	No	No	No	No
Internal Antennas	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Antenna Switch	No	Yes (per radio + physical switch)	No	No	No	No	No	No
Console Port	4-Pin Serial	4-Pin Serial	4-Pin Serial	4-Pin Serial	4-Pin Serial	4-Pin Serial	4-Pin Serial	4-Pin Serial
LED Locator	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LED Suppression	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AC (AP Controller) Discovery	No	No	No	No	No	Yes	Yes	Yes
NebulaFlex PRO	No	No	No	No	No	No	Yes	No
NCC Discovery	Yes	Yes	Yes	Yes	Yes	No	Yes	No
802.11r Fast Roaming Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
802.11k/v Assisted Roaming	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Bluetooth Low Energy (BLE)	No	No	No	No	No	No	No	Yes
USB Port for BLE	No	No	No	No	No	No	No	Yes
Ethernet Storm Control	No	No	Yes	Yes	No	No	Yes	No

Table 1 Zyxel Device 1000/5000 Series Comparison Table

FEATURES	NWA1123-ACv2	NWA1123-AC PRO	NWA1123-AC HD	NWA110AX	NWA1302-AC	NWA5123-AC	NWA5123-AC HD	WAC5302D-S
Grounding	No	No	Yes	Yes	No	No	Yes	No
Maximum number of log messages	512 event logs and 1024 debug logs							256 event logs and 1 debug logs

A. For NXC managed devices only. See the NXC User's Guide for details.

Table 2 WAC 6000 Series Comparison Table

FEATURES	WAC6103D-I	WAC6303D-S	WAC6502D-E	WAC6502D-S	WAC6503D-S	WAC6552D-S	WAC6553D-E
Supported Wireless 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	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	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	2.4 GHz 5 GHz	2.4 GHz 5 GHz	2.4 GHz 5 GHz	2.4 GHz 5 GHz
Available Security Modes	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX
Number of SSID Profiles	64	64	64	64	64	64	64
Number of Wireless Radios	2	2	2	2	2	2	2
Monitor Mode & Rogue APs Containment[A]	Yes	No	Yes	Yes	Yes	Yes	Yes
Rogue AP Detection	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WDS (Wireless Distribution System) - Root AP & Repeater Modes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tunnel Forwarding Mode	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Layer-2 Isolation	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Supported PoE Standards	IEEE 802.3af IEEE 802.3at	IEEE 802.3af IEEE 802.3at	IEEE 802.3af IEEE 802.3at	IEEE 802.3af IEEE 802.3at	IEEE 802.3af IEEE 802.3at	IEEE 802.3af IEEE 802.3at	IEEE 802.3af IEEE 802.3at
Power Detection	No	Yes	Yes	Yes	Yes	Yes	Yes
External Antennas	No	No	Yes	No	No	No	Yes
Internal Antennas	Yes	Yes	No	Yes	Yes	Yes	No
Antenna Switch	Yes (per radio + physical switch)	No	No	No	No	No	No
Console Port	4-Pin Serial	4-Pin Serial	RJ-45 serial	RJ-45 serial	RJ-45 serial	RJ-45 serial	RJ-45 serial
LED Locator	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LED Suppression	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AC (AP Controller) Discovery	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 2 WAC 6000 Series Comparison Table

FEATURES	WAC6103D -I	WAC6303D -S	WAC6502D -E	WAC6502D -S	WAC6503D -S	WAC6552D -S	WAC6553D -E
NebulaFlex PRO	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NCC Discovery	Yes	Yes	Yes	Yes	Yes	Yes	Yes
802.11r Fast Roaming Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes
802.11k/v Assisted Roaming	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Bluetooth Low Energy (BLE)	No	Yes	No	No	No	No	No
USB Port for BLE	No	No	No	No	No	No	No
Ethernet Storm Control	No	Yes	No	No	No	No	No
Grounding	No	Yes	Yes	Yes	No	Yes	Yes
Maximum number of log messages	512 event logs and 1024 debug logs						

A. For NXC managed devices only. See the NXC User's Guide for details.

Table 3 WAX 500/600 Series Comparison Table

FEATURES	WAX510D	WAX650S
Supported Wireless 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
Available Security Modes	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX Enhanced-open WPA3-enterprise WPA3-personal	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX Enhanced-open WPA3-enterprise WPA3-personal
Number of SSID Profiles	64	64
Number of Wireless Radios	2	2
Monitor Mode & Rogue APs Containment[A]	No	No
Rogue AP Detection	Yes	Yes
WDS (Wireless Distribution System) - Root AP & Repeater Modes	No	No
Tunnel Forwarding Mode	Yes	Yes
Layer-2 Isolation	Yes	Yes
Supported PoE Standards	IEEE 802.3af IEEE 802.3at	IEEE 802.3at IEEE 802.3bt
Power Detection	Yes	Yes
External Antennas	No	No
Internal Antennas	Yes	Yes

Table 3 WAX 500/600 Series Comparison Table

FEATURES	WAX510D	WAX650S
Antenna Switch	Yes (per AP)	No
Console Port	4-Pin Serial	4-Pin Serial
LED Locator	Yes	Yes
LED Suppression	Yes	Yes
AC (AP Controller) Discovery	Yes	Yes
NebulaFlex PRO	Yes	Yes
NCC Discovery	Yes	Yes
802.11r Fast Roaming Support	Yes	Yes
802.11k/v Assisted Roaming	Yes	Yes
Bluetooth Low Energy (BLE)	No	Yes
USB Port for BLE	No	No
Ethernet Storm Control	Yes	Yes
Grounding	Yes	Yes
Maximum number of log messages	512 event logs and 1024 debug logs	

A. For NXC managed devices only. See the NXC User's Guide for details.

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 NXC can only manage multiple APs in the same location.

Note: Not all models can be managed by NCC or an AC. See Section 1.4 on page 19 to check whether your product supports these.

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

Table 4 Zyxel Device Management Mode Comparison

MANAGEMENT MODE	DEFAULT IP ADDRESS	UPLOAD FIRMWARE VIA
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 65 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 Section 25.1 on page 227 for an example NCC managed network topology.

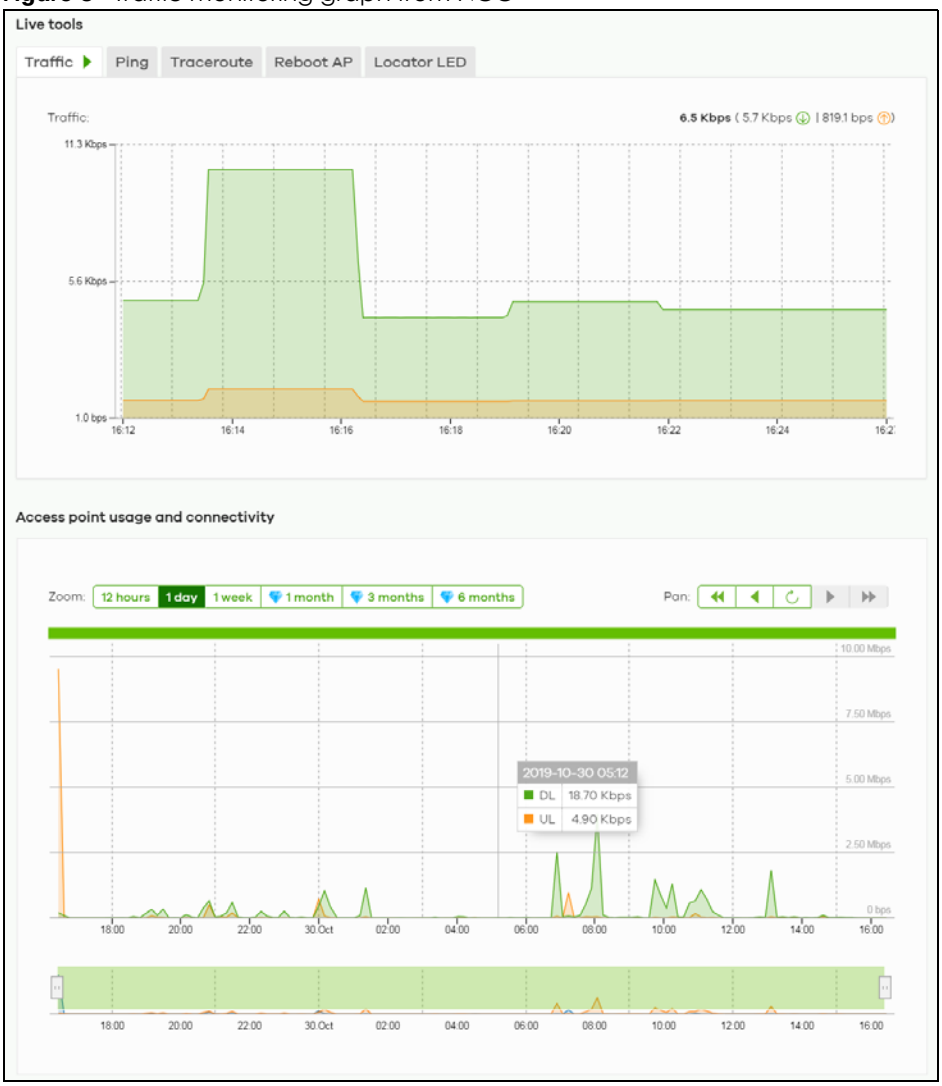
NCC allows different levels of management. You can configure each device on its own or configure a set of devices together as a site. You can also monitor groups of sites called organizations, as shown below.

Table 5 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 5 Traffic monitoring graph from NCC



See the NCC (Nebula Control Center) User's Guide for how to configure Nebula managed devices. See Chapter 27 on page 231 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 9.1.1 on page 94) such as the NXC2500 or NXC5500, 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 9.5 on page 102 and Section 9.1.1 on page 94). You can use the AC to manage multiple Zyxel Devices. See Section 9.1.1 on page 94 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 9.6 on page 103). The NCC manages the Zyxel Device automatically when it is discovered.

Standalone-to-AC (NXC)

By default, the Zyxel Device must be in the same subnet as the NXC. See Section 9.1.1 on page 94 for setting it up in a different subnet. Make sure **AC Discovery** is enabled (see Section 9.5 on page 102). The NXC manages the Zyxel Device automatically when it is discovered.

NXC-to-NCC

Register the Zyxel Device at the NCC website. Make sure that **NCC Discovery** is enabled on your Zyxel Device (see Section 9.6 on page 103). In the NXC web configurator, select the Zyxel Device and press the **Nebula** button. The NCC manages the Zyxel Device automatically when it is discovered.

NCC-to-NXC

Unregister the Zyxel Device at the NCC portal. By default, the Zyxel Device must be in the same subnet as the NXC. See Section 9.1.1 on page 94 for setting it up in a different subnet. Make sure **AC Discovery**

is enabled (see Section 9.5 on page 102). The NXC manages the Zyxel Device automatically when it is discovered.

NCC-to-Standalone

Unregister the Zyxel Device from the NCC organization/site. Reset the Zyxel Device to factory defaults (see Section 29.6 on page 247).

AC-to-Standalone

Use the **Reset** button to return the Zyxel Device to its factory default settings (see Section 29.6 on page 247).

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 PC, please make sure it meets the requirements listed below.

Operating System

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

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

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

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 PC.

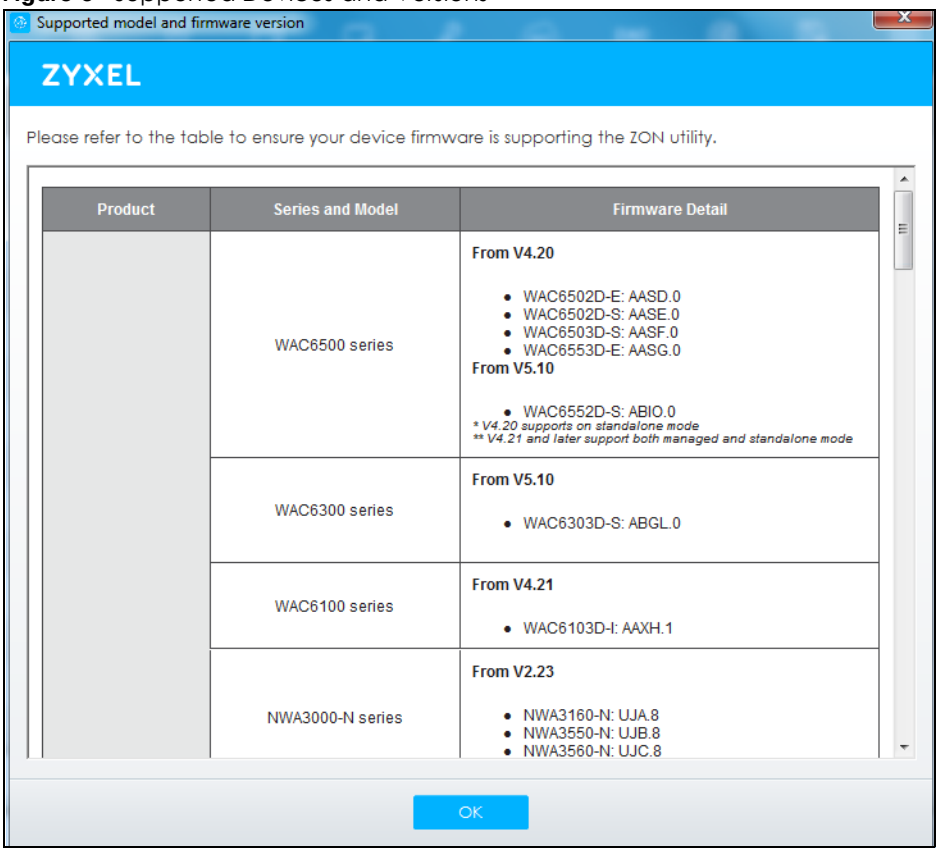
- Core i3 processor
- 2GB RAM
- 100MB free hard disk
- WXGA (Wide XGA 1280x800)

2.3.2 Run the ZON Utility

1 Double-click the ZON Utility to run it.

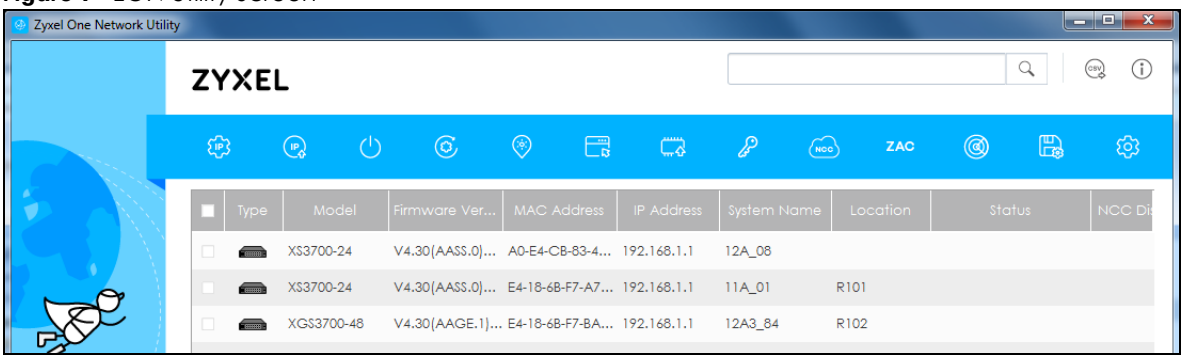
2 The first time you run the ZON Utility, you will see if your device and firmware version support the ZON Utility. Click the **OK** button to close this screen.

Figure 6 Supported Devices and Versions



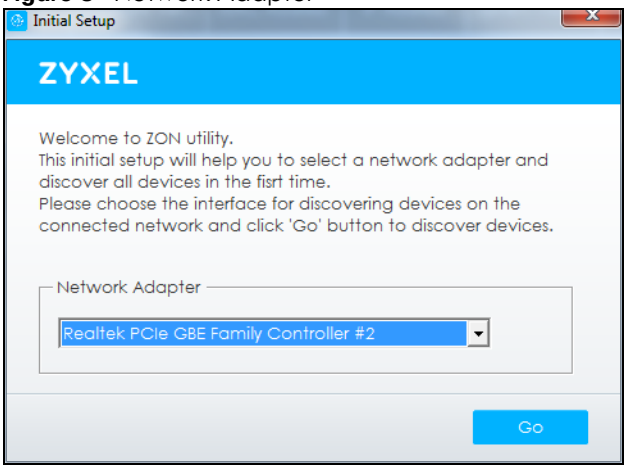
If you want to check the supported models and firmware versions later, you can click the **Show information about ZON** icon in the upper right hand corner of the screen. Then select the **Supported model and firmware version** link. If your device is not listed here, see the device release notes for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

Figure 7 ZON Utility Screen



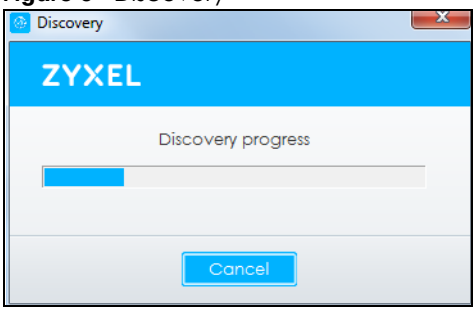
3 Select a network adapter to which your supported devices are connected.

Figure 8 Network Adapter



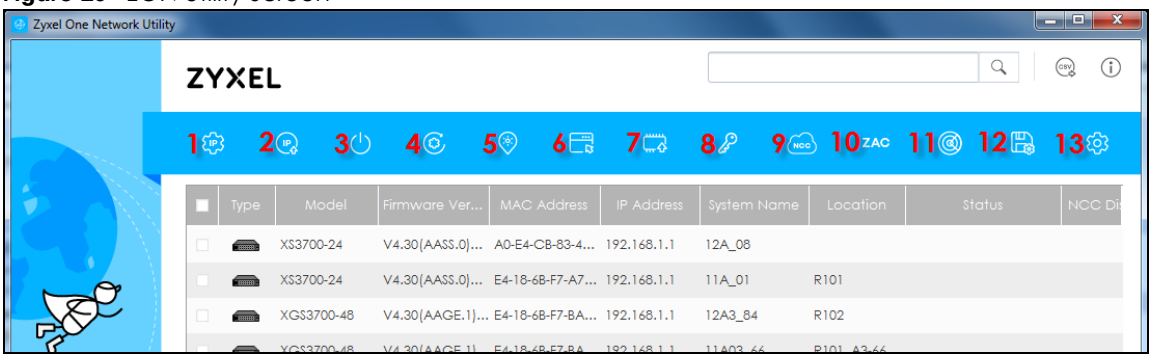
4 Click the **Go** button for the ZON Utility to discover all supported devices in your network.

Figure 9 Discovery



5 The ZON Utility screen shows the devices discovered.

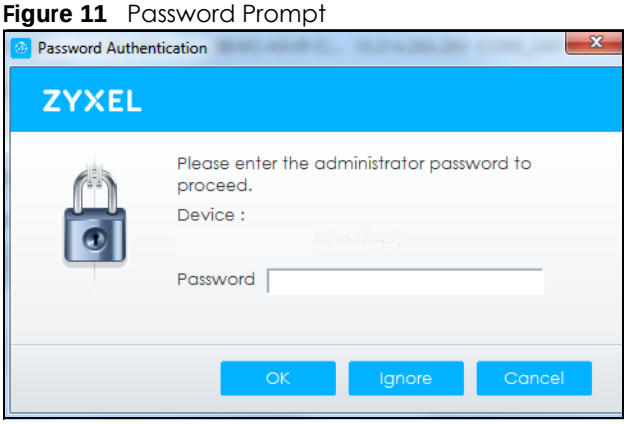
Figure 10 ZON Utility Screen



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.

Figure 11 Password Prompt



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

Table 6 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.
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.
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.

Table 6 ZON Utility Icons

ICON	DESCRIPTION
9 Configure NCC Discovery	You must have Internet access to use this feature. Use this icon to enable or disable the Nebula Control Center (NCC) discovery feature on the selected device. If it's enabled, the selected device will try to connect to the NCC. Once the selected device is connected to and has registered in the NCC, it'll go into the Nebula cloud management mode.
10 ZAC	Use this icon to run the Zyxel AP Configurator of the selected AP.
11 Clear and Rescan	Use this icon to clear the list and discover all devices on the connected network again.
12 Save Configuration	Use this icon to save configuration changes to permanent memory on a selected device.
13 Settings	Use this icon to select a network adaptor for the computer on which the ZON utility is installed, and the utility language.

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

Table 7 ZON Utility Fields

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

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.

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 27.

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 (for example, SSH or Telnet) 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's 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 won't 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 and WAC6553D-E)

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.

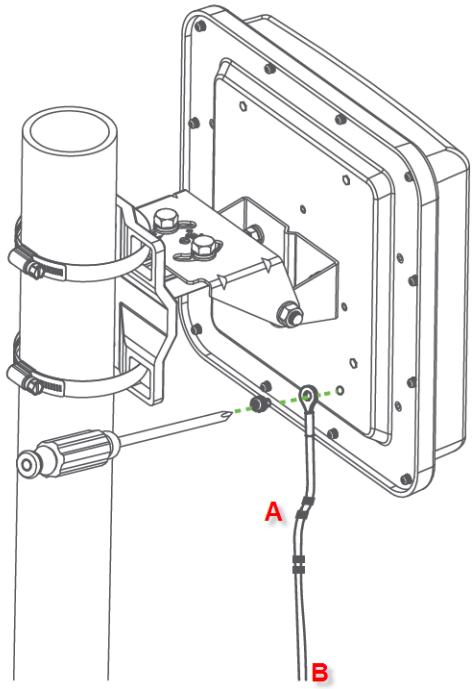
1. Remove one of the ground screws from the Zyxel Device's rear panel.
2. Secure a green/yellow ground cable (18 AWG or smaller) to the Zyxel Device's rear panel using the ground screw.
3. Attach the other end of the cable to the ground, either to the same ground electrode as the pole you installed the 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 12 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 has Locator LED which allows you to see the actual location of the Zyxel Device among several devices in the network. See Section 1.4 on page 19 to check which models support these features. Refer to Chapter 21 on page 219 for the LED **Suppression** and **Locator** menus in standalone mode.

The following models have single LEDs: NWA1123-ACv2, NWA1123-AC HD, NWA5123AC, NWA5123-AC HD, WAC6303D-S, NWA110AX, WAX510D and WAX650S.

3.2.1 NWA1123-ACv2

The following are the LED descriptions for your NWA1123-ACv2.

Figure 13 NWA1123-ACv2 LED

The following are the LED descriptions for your NWA1123-ACv2.

Table 8 NWA1123-ACv2 LED

COLOR		STATUS	DESCRIPTION
	Amber Green	Blinks amber for 1 second and green for 1 second alternatively.	The LED blinks amber and green alternatively when the Zyxel Device is booting up or is connecting to the NCC.
	Amber Green	Blinks amber and green alternatively 3 times and then turns solid green for 3 seconds.	The Zyxel Device is discovering the NCC.
	Green	On	The Zyxel Device is ready for use and its wireless interface is activated.
		Slow Blinking (On for 1s, Off for 1s)	The wireless module of the Zyxel Device is disabled or failed, the Zyxel Device is using default wireless settings, or the Zyxel Device is connected to the NCC but is unregistered with the NCC.
		Fast Blinking (On for 50ms, Off for 50ms)	The Locator LED is on.
	Amber	On	The Zyxel Device is powered up.

Table 8 NWA1123-ACv2 LED (continued)

COLOR		STATUS	DESCRIPTION
	Red	Steady On	The Zyxel Device failed to boot up or is experiencing system failure.
		Slow Blinking (Blink for 3 times, Off for 3s)	The Uplink interface is down.
		Fast Blinking (On for 50ms, Off for 50ms)	The Zyxel Device is undergoing firmware upgrade.

3.2.2 WAC6303D-S and NWA5123-AC HD

The following are the LED descriptions for your WAC6303D-S or NWA5123-AC HD.

Figure 14 WAC6303D-S LED

The following are the LED descriptions for your WAC6303D-S or NWA5123-AC HD.

Table 9 WAC6303D-S and NWA5123-AC HD LED

COLOR		STATUS	DESCRIPTION
	Amber Green	Blinks amber for 1 second and green for 1 second alternatively.	The Zyxel Device is booting up or is connecting with NCC.
	Amber Green	Blinks amber and green alternatively 3 times and then turns solid green for 3 seconds.	The Zyxel Device is discovering the NCC or an AC.

Table 9 WAC6303D-S and NWA5123-AC HD LED (continued)

COLOR		STATUS	DESCRIPTION
	Amber Green	Blinks amber and green alternatively 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 wireless settings, or the Zyxel Device is configured to be managed by NCC but is not yet registered with the NCC.
	Green	Steady On	The Zyxel Device is ready for use, the Zyxel Device's wireless interface is activated, and/or wireless clients are connected to the Zyxel Device in full power mode (see Table 26 on page 67).
	Amber	Steady On	The Zyxel Device is ready for use, the Zyxel Device's wireless interface is activated, and/or wireless clients are connected to the Zyxel Device in limited power mode (see Table 26 on page 67).
	Bright Blue	Steady On	The Zyxel Device's wireless interface is activated, but there are no wireless clients connected when it is in full power mode (see Table 26 on page 67).
	White	Steady On	The Zyxel Device's wireless interface is activated, but there are no wireless clients connected when it is in limited power mode (see Table 26 on page 67).
		Slow Blinking (On for 100ms per second)	Locator LED is on. It switches off automatically after the configured amount of time (1-60min). Default duration is 10 minutes.
	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 port of the Zyxel Device in standalone mode is disconnected.

3.2.3 NWA1123-AC HD

The following are the LED descriptions for your NWA1123-AC HD.

Figure 15 NWA1123-AC HD LED

The following are the LED descriptions for your NWA1123-AC HD.

Table 10 NWA1123-AC HD LED

COLOR		STATUS	DESCRIPTION
	Amber Green	Blinks amber for 1 second and green for 1 second alternatively.	The Zyxel Device is booting up or connecting with NCC.
	Amber Green	Blinks amber and green alternatively 3 times and then turns solid green for 3 seconds.	The Zyxel Device is discovering the NCC.
	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 wireless settings, or the Zyxel Device is configured to be managed by NCC but is not yet registered with the NCC.
	Green	Steady On	The Zyxel Device is ready for use, the Zyxel Device's wireless interface is activated, and/or wireless clients are connected to the Zyxel Device in full power mode (see Table 26 on page 67).
	Amber	Steady On	The Zyxel Device is ready for use, the Zyxel Device's wireless interface is activated, and/or wireless clients are connected to the Zyxel Device in limited power mode (see Table 26 on page 67).
	Bright Blue	Steady On	The Zyxel Device's wireless interface is activated, but there are no wireless clients connected when it is in full power mode (see Table 26 on page 67).

Table 10 NWA1123-AC HD LED (continued)

COLOR		STATUS	DESCRIPTION
	White	Steady On	The Zyxel Device's wireless interface is activated, but there are no wireless clients connected when it is in limited power mode (see Table 26 on page 67).
		Slow Blinking (On for 100ms per second)	Locator LED is on. It switches off automatically after the configured amount of time (1-60min). Default duration is 10 minutes.
	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 interface of the Zyxel Device is down.

3.2.4 NWA5123-AC

The following are the LED descriptions for your NWA5123-AC.

Figure 16 NWA5123-AC LED

The following are the LED descriptions for your NWA5123-AC.

Table 11 NWA5123-AC LED

COLOR		STATUS	DESCRIPTION
	Amber Green	Blinks amber for 1 second and green for 1 second alternatively.	The Zyxel Device is booting up.
	Amber Green	Blinks amber and green alternatively 3 times and then turns solid green for 3 seconds.	The Zyxel Device is discovering an AC.
	Amber Green	Blinks amber and green alternatively 2 times and then turns solid green for 3 seconds.	The Zyxel Device is managed by an AC and the uplink interface is down.
	Green	On	The Zyxel Device is ready for use and its wireless interface is activated.
		Slow Blinking (On for 1s, Off for 1s)	The wireless module of the Zyxel Device is disabled or failed, or the Zyxel Device is using default wireless settings.
		Fast Blinking (On for 50ms, Off for 50ms)	The Locator LED is on.
	Amber	On	The Zyxel Device is powered up.
	Red	Steady On	The Zyxel Device failed to boot up or is experiencing system failure.
		Slow Blinking (Blink for 3 times, Off for 3s)	The Uplink interface is down.
		Fast Blinking (On for 50ms, Off for 50ms)	The Zyxel Device is undergoing firmware upgrade.

3.2.5 NWA110AX, WAX510D and WAX650S

The following are the LED descriptions for your NWA110AX, WAX510D and WAX650S.

Figure 17 NWA110AX, WAX510D and WAX650S LED

The following are the LED descriptions for your NWA110AX, WAX510D and WAX650S.

Table 12 NWA110AX, WAX510D and WAX650S LED

COLOR		STATUS	DESCRIPTION
	Amber Green	Blinks amber for 1 second and green for 1 second alternatively.	The Zyxel Device is booting up or is connecting with NCC.
	Amber Green	Blinks amber and green alternatively 3 times and then turns solid green for 3 seconds.	The Zyxel Device is discovering the NCC or an AC.
	Amber Green	Blinks amber and green alternatively 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 wireless 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 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 wireless clients are connected to the Zyxel Device in full power mode (see Table 26 on page 67).

Table 12 NWA110AX, WAX510D and WAX650S LED (continued)

COLOR		STATUS	DESCRIPTION
	Amber	Steady On	The Zyxel Device is ready for use, the Zyxel Device's wireless interface is activated, and/or wireless clients are connected to the Zyxel Device in limited power mode (see Table 26 on page 67).
	Bright Blue	Steady On	The Zyxel Device's wireless interface is activated, but there are no wireless clients connected when it is in full power mode (see Table 26 on page 67).
	White	Steady On	The Zyxel Device's wireless interface is activated, but there are no wireless clients connected when it is in limited power mode (see Table 26 on page 67).
		Slow Blinking (On for 100ms per second)	Locator LED is on. It switches off automatically after the configured amount of time (1-60min). Default duration is 10 minutes.
	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 port of the Zyxel Device in standalone mode is disconnected.

3.3 Zyxel Device Models With Multiple 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 has Locator LED which allows you to see the actual location of the Zyxel Device among several devices in the network. See Section 1.4 on page 19 to check which models support these features. Refer to Chapter 21 on page 219 for the LED **Suppression** and **Locator** menus in standalone mode.

The following models have multiple LEDs: NWA1123-AC PRO, NWA1302-AC, WAC6103D-I, WAC5302D-S, WAC6502D-E, WAC6502D-S, WAC6503D-S.

3.3.1 NWA1123-AC PRO

The following are the LED descriptions for your NWA1123-AC PRO.

Figure 18 NWA1123-AC PRO LEDs

The following table describes the LEDs.

Table 13 NWA1123-AC PRO LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR/SYS ⏻	Amber	Blinks amber for 1 second and green for 1 second alternatively.	The LED blinks amber and green alternatively when the Zyxel Device is booting up.
	Green		
	Green	On	The Zyxel Device is ready for use.
		Slow Blinking (On for 1 sec, Off for 1 sec)	The wireless module of the Zyxel Device is disabled or failed.
	Red	On	There is a system error and the Zyxel Device cannot boot up, or the Zyxel Device suffered a system failure.
		Fast Blinking (On for 50 ms, Off for 50 ms)	The Zyxel Device is undergoing firmware upgrade.
		Slow Blinking (Blink for 3 times, Off for 3 sec)	The Uplink interface is down.

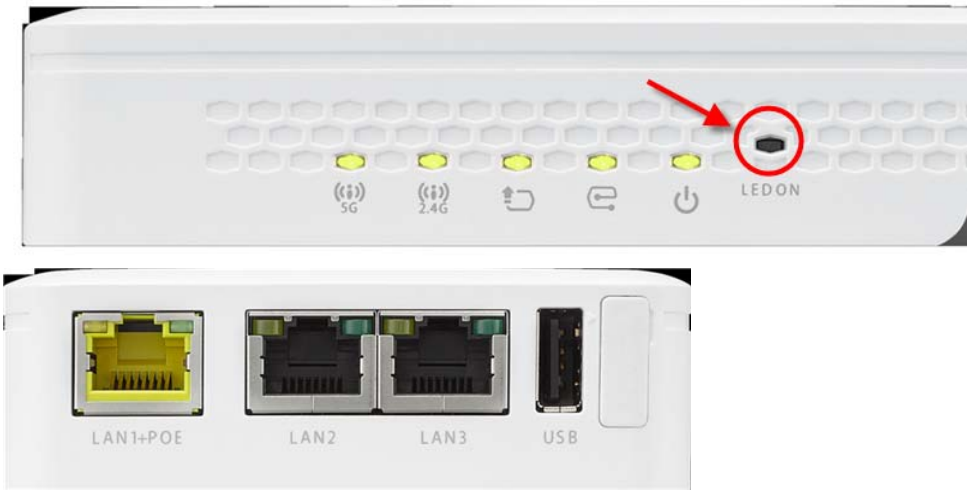
Table 13 NWA1123-AC PRO LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
Management	Green	On	The Zyxel Device is managed by the NCC.
		Slow Blinking (On for 1 sec, Off for 1 sec)	The Zyxel Device is using default wireless settings, or the Zyxel Device is connected to the NCC but is unregistered with the NCC.
	Amber Green	Blinks amber for 1 second and green for 1 second alternatively	The Zyxel Device is searching for (discovering) the NCC.
	Amber Green	Blinks amber and green alternatively 3 times and then turns solid green for 3 seconds.	The NCC is connecting to the registered Zyxel Device.
		Off	The Zyxel Device is in standalone mode.
WLAN 2.4G	Green	On	The 2.4 GHz radio is set to “Ceiling” and is active
	Amber	On	The 2.4 GHz radio is set to “Wall” and is active
		Off	The 2.4 GHz WLAN is not active.
WLAN 5G	Green	On	The 5 GHz radio is set to “Ceiling” and is active
	Amber	On	The 5 GHz radio is set to “Wall” and is active
		Off	The 5 GHz WLAN is not active.
UPLINK	Amber	On	The port is operating as a 100 Mbps connection.
		Blinking	The Zyxel Device is sending/receiving data through the port at 100 Mbps.
	Green	On	The port is operating as a Gigabit connection (1000 Mbps).
		Blinking	The Zyxel Device is sending/receiving data through the port at 1 Gbps.
		Off	The port is not connected.
LAN	Amber	On	The port is operating as a 100 Mbps connection.
		Blinking	The LAN port is sending/receiving data at 100 Mbps.
	Green	On	The port is operating as a Gigabit connection (1000 Mbps).
		Blinking	The LAN port is sending/receiving data at 1 Gbps.
		Off	The LAN port is not connected.
Locator	White	Blinking	The Locator is activated and will blink to show the actual location of the Zyxel Device between several devices in the network.
		Off	The Locator function is off.

3.3.2 NWA1302-AC

By default, the LEDs automatically turn on when the NWA1302-AC is ready. If the LEDs are turned off by the NCC, you can press the **LED ON** button for one second to turn on the LEDs again. The LEDs will blink and turn off after two minutes.

Figure 19 NWA1302-AC LEDs



The following table describes the LEDs.

Table 14 NWA1302-AC LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR/SYS	Amber	Blinks amber for 1 second and green for 1 second alternatively.	The LED blinks amber and green alternatively when the Zyxel Device is booting up.
	Green		
	Green	On	The Zyxel Device is ready for use.
		Slow Blinking (On for 1 sec, Off for 1 sec)	The wireless module of the Zyxel Device is disabled or failed.
		Fast Blinking (On 50ms, Off 50ms)	The Locator LED is on.
	Red	On	There is a system error and the Zyxel Device cannot boot up, or the Zyxel Device suffered a system failure.
		Fast Blinking (On for 50 ms, Off for 50 ms)	The Zyxel Device is doing firmware upgrade.
		Slow Blinking (Blink for 3 times, Off for 3 sec)	The **Uplink** interface is down.
Management	Green	On	The Zyxel Device is managed by the NCC.
		Slow Blinking (On for 1 sec, Off for 1 sec)	The Zyxel Device is using default wireless settings, or the Zyxel Device is connected to the NCC but is unregistered with the NCC.
	Amber	Blinks amber for 1 second and green for 1 second alternatively	The Zyxel Device is searching for (discovering) the NCC.
	Green		
	Amber	Blinks amber and green alternatively 3 times and then turns solid green for 3 seconds.	The NCC is connecting to the registered Zyxel Device.
	Green		
	Off		The Zyxel Device is in standalone mode.

Table 14 NWA1302-AC LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
UPLINK	Amber	On	The port is operating as a 10/100 Mbps connection.
		Blinking	The Zyxel Device is sending/receiving data through the port at 10/100 Mbps.
	Green	On	The port is operating as a Gigabit connection (1000 Mbps).
		Blinking	The Zyxel Device is sending/receiving data through the port at 1Gbps.
		Off	The port is not connected.
WLAN 2.4G	Green	On	The 2.4 GHz WLAN is active.
		Off	The 2.4 GHz WLAN is not active.
WLAN 5G	Green	On	The 5 GHz WLAN is active.
		Off	The 5 GHz WLAN is not active.
LAN	Amber	On	The port is operating as a 10/100 Mbps connection.
		Blinking	The LAN port is sending/receiving data through the port at 10/100 Mbps.
	Green	On	The port is operating as a Gigabit connection (1000 Mbps).
		Blinking	The LAN port is sending/receiving data through the port at 1 Gbps.
	Off		The LAN port is not connected.

3.3.3 WAC6502D-E, WAC6502D-S, and WAC6503D-S

The following are the LED descriptions for your WAC6502D-E, WAC6502D-S, or WAC6503D-S.

Figure 20 WAC6502D-E, WAC6502D-S, or WAC6503D-S LEDs

The following table describes the LEDs.

Table 15 WAC6502D-E, WAC6502D-S, or WAC6503D-S LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR/SYS ⏻	Amber	Blinks amber for 1 second and green for 1 second alternatively.	The Zyxel Device is booting up or is connecting to the NCC or to an AC.
	Green		
	Green	On	The Zyxel Device is ready for use.
		Slow Blinking (On for 1s, Off for 1ss)	The wireless module of the Zyxel Device is disabled or failed.
	Red	On	There is system error and the Zyxel Device cannot boot up, or the Zyxel Device suffered a system failure.
		Fast Blinking (On for 50ms, Off for 50ms)	The Zyxel Device is doing firmware upgrade.
		Slow Blinking (Blink for 3 times, Off for 3s)	The Uplink interface is down.
		Slow Blinking (Blink for 2 times, Off for 3s)	The Zyxel Device is managed by an AC and the uplink is disconnected.

Table 15 WAC6502D-E, WAC6502D-S, or WAC6503D-S LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
Management	Green	On	The Zyxel Device is managed by a the NCC or an AC.
		Slow Blinking (Blink for 3 times, Off for 3s)	The Zyxel Device is searching (discovery) for an AC.
		Slow Blinking (On for 1s, Off for 1s)	The Zyxel Device is using default wireless settings, or the Zyxel Device is connected to the NCC but is unregistered with the NCC.
		Off	The Zyxel Device is in standalone mode.
	Amber Green	Blinks amber for 1 second and green for 1 second alternatively	The Zyxel Device is searching (discovery) for the NCC.
	Amber Green	Blinks amber and green alternatively 3 times and then turns solid green for 3 seconds.	The NCC is connecting to the registered Zyxel Device.
WLAN 2.4G	Green	On	The 2.4 GHz WLAN is active.
		Off	The 2.4 GHz WLAN is not active.
WLAN 5G	Green	On	The 5 GHz WLAN is active.
		Off	The 5 GHz WLAN is not active.
UPLINK	Amber	On	The port is operating as a 100 Mbps connection.
		Blinking	The Zyxel Device is sending/receiving data through the port at 100 Mbps.
	Green	On	The port is operating as a Gigabit connection (1000 Mbps).
		Blinking	The Zyxel Device is sending/receiving data through the port at 1 Gbps.
		Off	The port is not connected.
LAN	Amber	On	The port is operating as a 100 Mbps connection.
		Blinking	The LAN port is sending/receiving data through the port at 100 Mbps.
	Green	On	The port is operating as a Gigabit connection (1000 Mbps).
		Blinking	The LAN port is sending/receiving data through the port at 1 Gbps.
		Off	The LAN port is not connected.
Locator	White	Blinking	The Locator is activated and will blink to show the actual location of the Zyxel Device between several devices in the network.
		Off	The Locator function is off.

3.3.4 WAC6103D-I

The following are the LED descriptions for your WAC6103D-I.

Figure 21 WAC6103D-I LEDs

The following table describes the LEDs.

Table 16 WAC6103D-I LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR/SYS	Amber	Blinks amber for 1 second and green for 1 second alternatively.	The Zyxel Device is booting up.
	Green		
	Green	On	The Zyxel Device is ready for use.
		Slow Blinking (On for 1s, Off for 1s)	The wireless module of the Zyxel Device is disabled or failed.
	Red	On	There is system error and the Zyxel Device cannot boot up, or the Zyxel Device suffered a system failure.
		Fast Blinking (On for 50ms, Off for 50ms)	The Zyxel Device is doing firmware upgrade.
		Slow Blinking (Blink for 3 times, Off for 3s)	The **Uplink** port is disconnected.

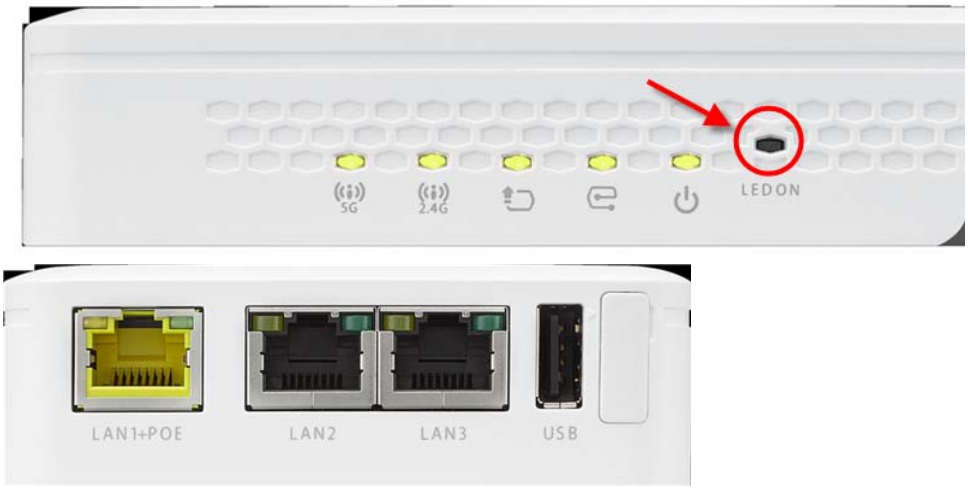
Table 16 WAC6103D-I LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
Management	Green	On	The Zyxel Device is managed by an AC or the NCC.
		Slow Blinking (Blink for 3 times, Off for 3s)	The Zyxel Device is searching (discovery) for an AC.
		Slow Blinking (On for 1s, Off for 1s)	The Zyxel Device is using default wireless settings, or the Zyxel Device is connected to the NCC but is unregistered with the NCC.
		Off	The Zyxel Device is in standalone mode.
	Amber Green	Blinks amber for 1 second and green for 1 second alternatively	The Zyxel Device is searching (discovery) for the NCC.
	Amber Green	Blinks amber and green alternatively 3 times and then turns solid green for 3 seconds.	The NCC is connecting to the registered Zyxel Device.
WLAN 2.4G	Green	On	The 2.4 GHz radio is set to “Ceiling” and is active
	Amber	On	The 2.4 GHz radio is set to “Wall” and is active
		Off	The 2.4 GHz WLAN is not active.
WLAN 5G	Green	On	The 5 GHz radio is set to “Ceiling” and is active
	Amber	On	The 5 GHz radio is set to “Wall” and is active
		Off	The 5 GHz WLAN is not active.
UPLINK	Amber	On	The port is operating as a 100 Mbps connection.
		Blinking	The Zyxel Device is sending/receiving data through the port at 100 Mbps.
	Green	On	The port is operating as a Gigabit connection (1000 Mbps).
		Blinking	The Zyxel Device is sending/receiving data through the port at 1 Gbps.
		Off	The port is not connected.
LAN	Amber	On	The port is operating as a 100 Mbps connection.
		Blinking	The LAN port is sending/receiving data through the port at 100 Mbps.
	Green	On	The port is operating as a Gigabit connection (1000 Mbps).
		Blinking	The LAN port is sending/receiving data through the port at 1 Gbps.
		Off	The LAN port is not connected.
Locator	White	Blinking	The Locator is activated and will blink to show the actual location of the Zyxel Device between several devices in the network.
		Off	The Locator function is off.

3.3.5 WAC5302D-S

The LEDs automatically turn off when the WAC5302D-S is ready. You can press the **LED ON** button for one second to turn on the LEDs again. The LEDs will blink and turn off after two minutes.

Figure 22 WAC5302D-S LEDs



The following table describes the LEDs.

Table 17 WAC5302D-S LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR/SYS	Amber	Blinks amber for 1 second and green for 1 second alternatively.	The LED blinks amber and green alternatively when the WAC is booting up.
	Green		
	Green	On	The Zyxel Device is ready for use.
		Slow Blinking (On for 1s, Off for 1s)	The wireless module of the Zyxel Device is disabled or failed.
		Fast Blinking (On 50ms, Off 50ms)	The Locator LED is on.
	Red	On	There is system error and the Zyxel Device cannot boot up, or the Zyxel Device suffered a system failure.
		Fast Blinking (On for 50ms, Off for 50ms)	The Zyxel Device is doing firmware upgrade.
		Slow Blinking (Blink for 3 times, Off for 3s)	The Uplink interface is down.
		Slow Blinking (Blink for 2 times, Off for 3s)	The Zyxel Device is managed by an AC and the uplink is disconnected.
Management	Green	On	The Zyxel Device is managed by a controller.
		Slow Blinking (Blink for 3 times, Off for 3s)	The Zyxel Device is searching (discovery) for a controller.
		Slow Blinking (On for 1s, Off for 1s)	The Zyxel Device is using default wireless settings, or the Zyxel Device is connected to the NCC but is unregistered with the NCC.
		Off	The Zyxel Device is in standalone mode.

Table 17 WAC5302D-S LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
UPLINK	Amber	On	The port is operating as a 10/100 Mbps connection.
		Blinking	The Zyxel Device is sending/receiving data through the port at 10/100 Mbps.
	Green	On	The port is operating as a Gigabit connection (1000 Mbps).
		Blinking	The Zyxel Device is sending/receiving data through the port at 1 Gbps.
		Off	The port is not connected.
WLAN 2.4G	Green	On	The 2.4 GHz WLAN is active.
		Off	The 2.4 GHz WLAN is not active.
WLAN 5G	Green	On	The 5 GHz WLAN is active.
		Off	The 5 GHz WLAN is not active.
LAN	Amber	On	The port is operating as a 10/100 Mbps connection.
		Blinking	The LAN port is sending/receiving data through the port at 10/100 Mbps.
	Green	On	The port is operating as a Gigabit connection (1000 Mbps).
		Blinking	The LAN port is sending/receiving data through the port at 1 Gbps.
		Off	The LAN port is not connected.

CHAPTER 4
The Web Configurator

4.1 Overview

The Zyxel Device Web Configurator allows management using an Internet browser.

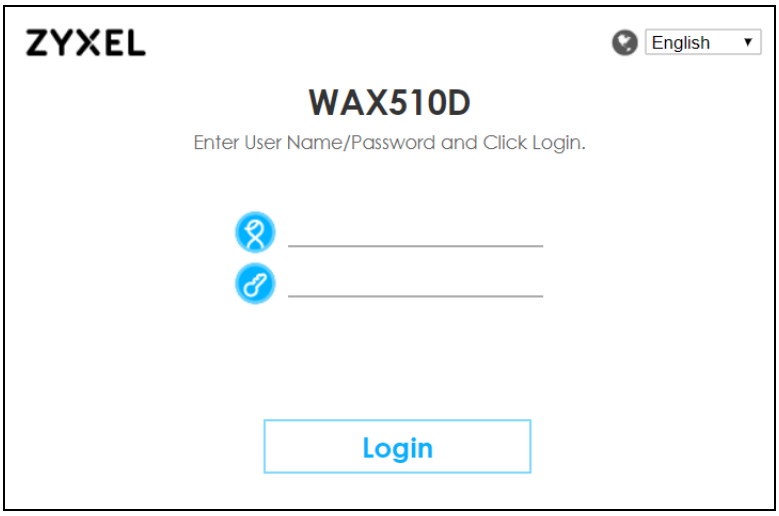
In order to use the Web Configurator, you must:

- Use Internet Explorer 10.0 and later versions, Mozilla Firefox 36.0 and later versions, Safari 9.0 and later versions, or Google Chrome 38.0 and later versions.
- Allow pop-up windows.
- Enable JavaScript (enabled by default).
- Enable Java permissions (enabled by default).
- Enable cookies.

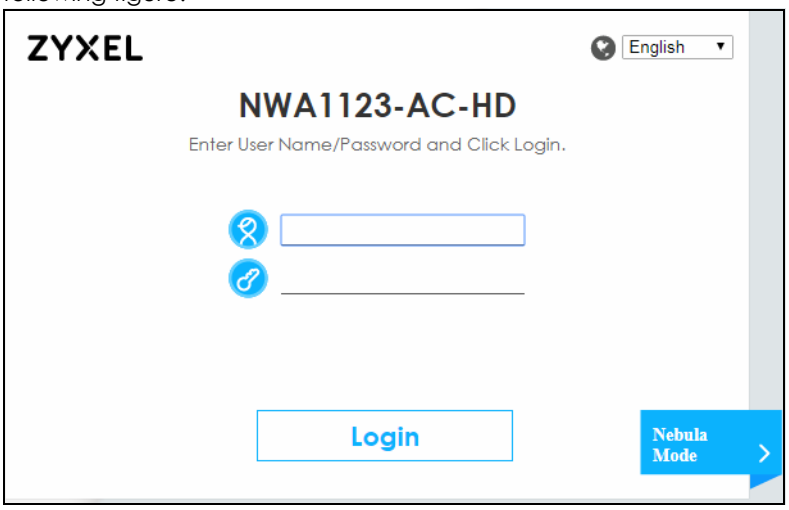
The recommended screen resolution is 1024 x 768 pixels and higher.

4.2 Accessing the Web Configurator

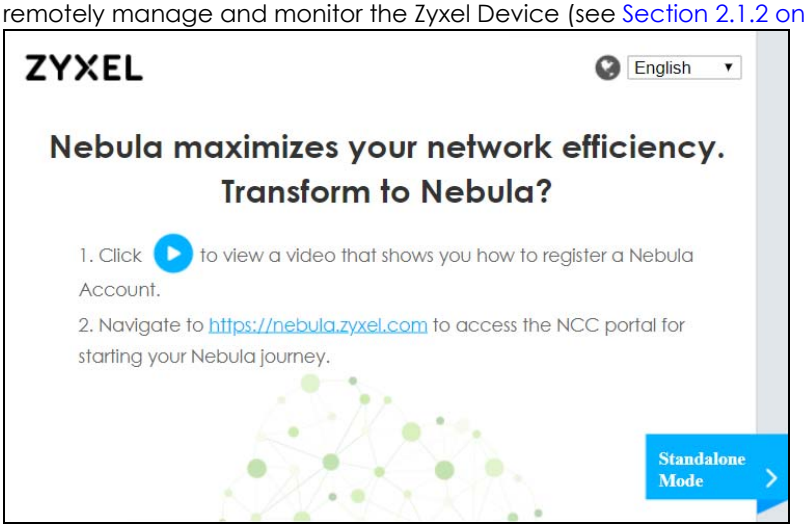
1. Make sure your Zyxel Device hardware is properly connected. See the Quick Start Guide.
2. If the Zyxel Device and your computer are not connected to a DHCP server, make sure your computer's IP address is in the range between "192.168.1.3" and "192.168.1.254".
3. Browse to the Zyxel Device's DHCP-assigned IP address or http://192.168.1.2. The **Login** screen appears. If you are in NCC mode, check the NCC's **AP > Monitor > Access Point** screen for the Zyxel Device's LAN IP address.



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



Click **Nebula Mode** to show the following screen. 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 24).



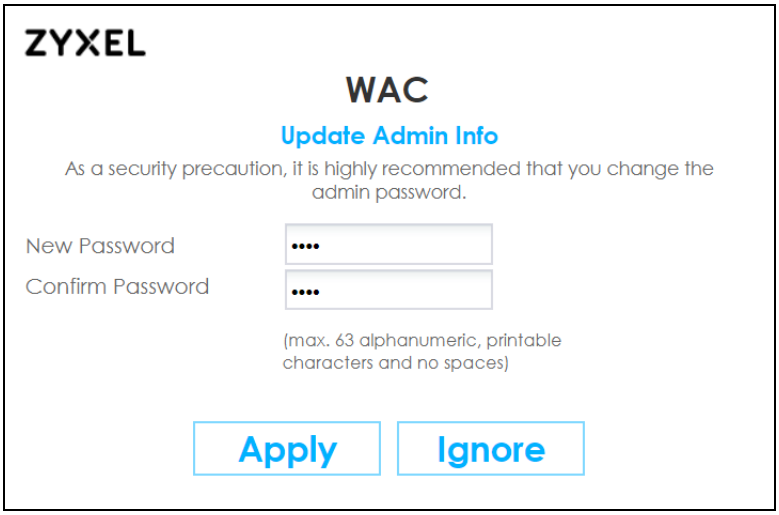
If you want to return to the login page, click **Standalone Mode** and follow the next steps.

4 Enter the user name (default: "admin") and password (default: "1234"). If the Zyxel Device is being managed or has been managed by the NCC, check the NCC's **Site-Wide > Configure > General setting** 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.



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 23 The Web Configurator's Main Screen for Standalone Mode

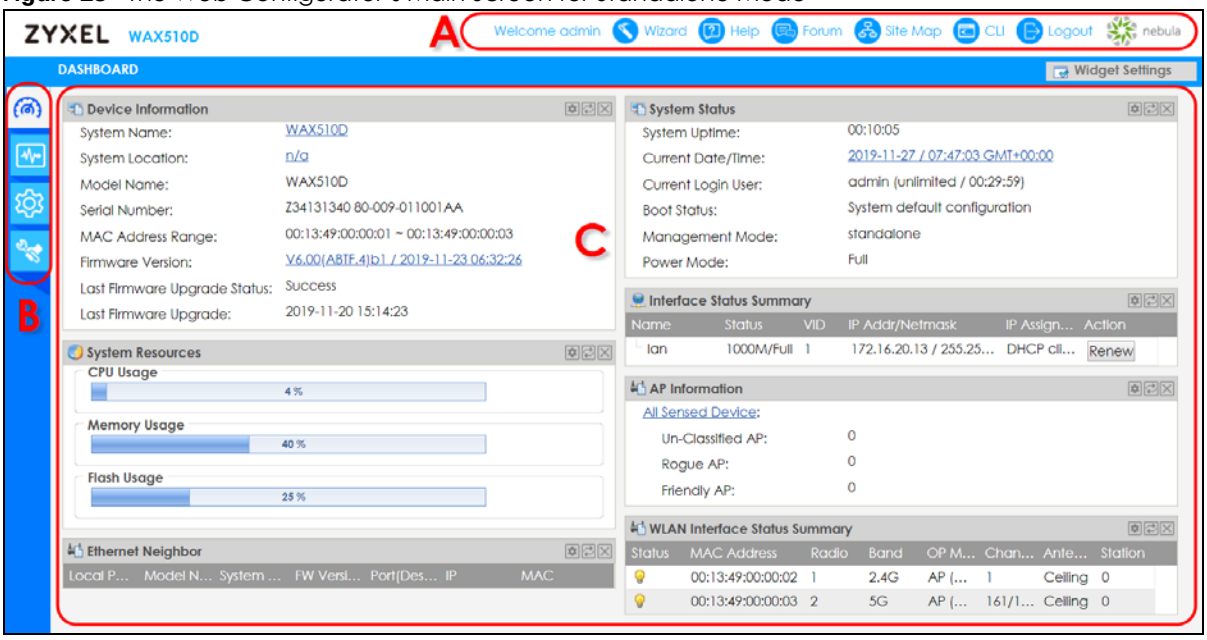
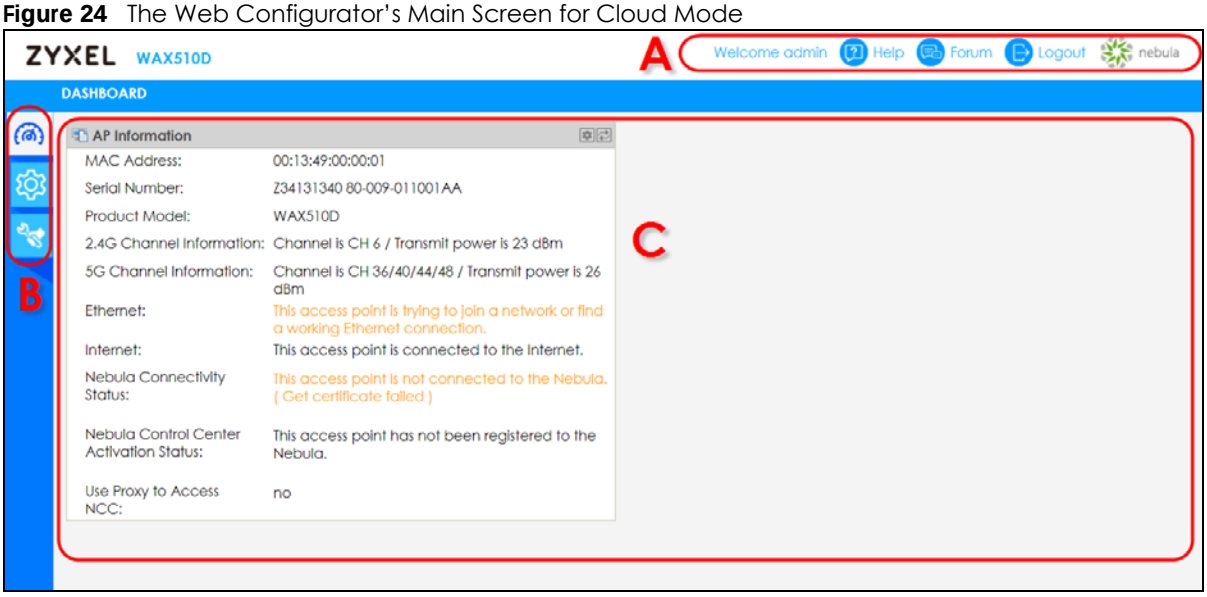


Figure 24 The Web Configurator's Main Screen for Cloud Mode



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 (see Figure 24 on page 56).

Figure 25 Title Bar

The icons provide the following functions.

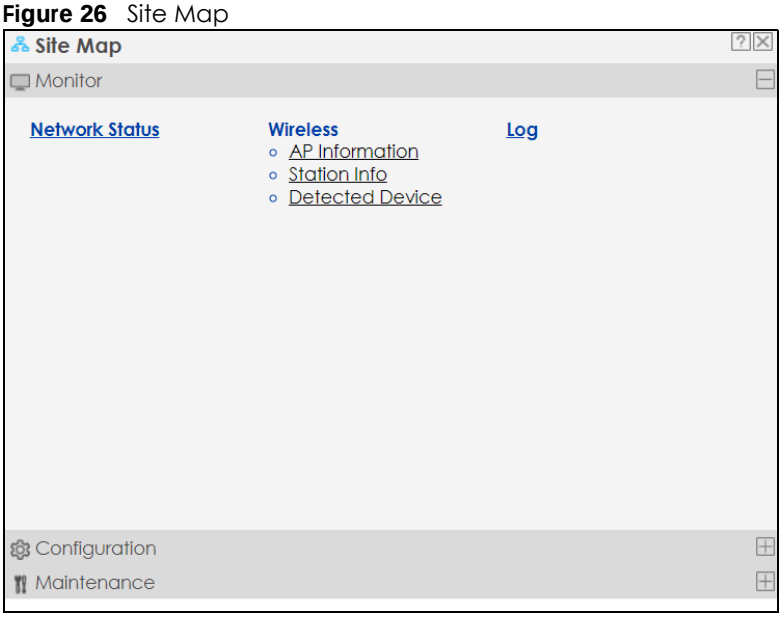
Table 18 Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
Wizard	Click this to open the wizard. See Chapter 7 on page 73 for more information.
Help	Click this to open the help page for the current screen.
Forum	Click this to go to Zyxel Biz User Forum, where you can get the latest Zyxel Device information and have conversations with other people by posting your messages.
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.

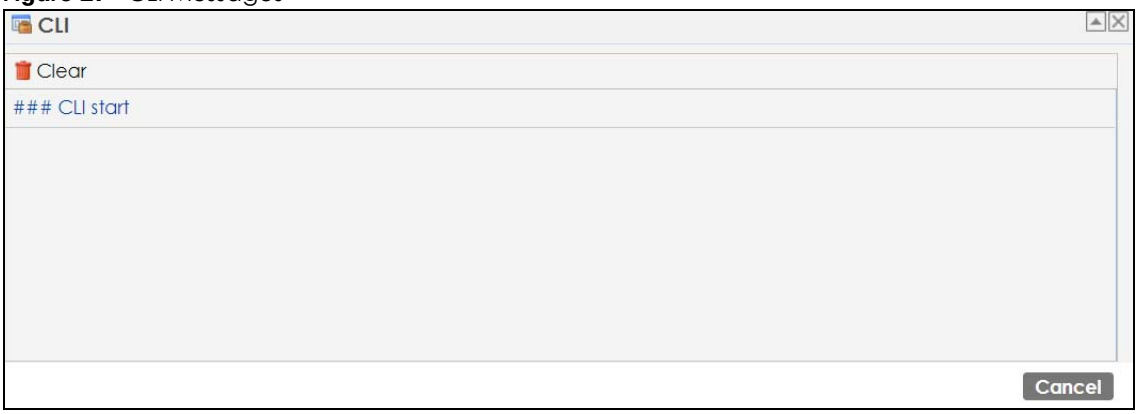
Figure 26 Site Map



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 27 CLI Messages



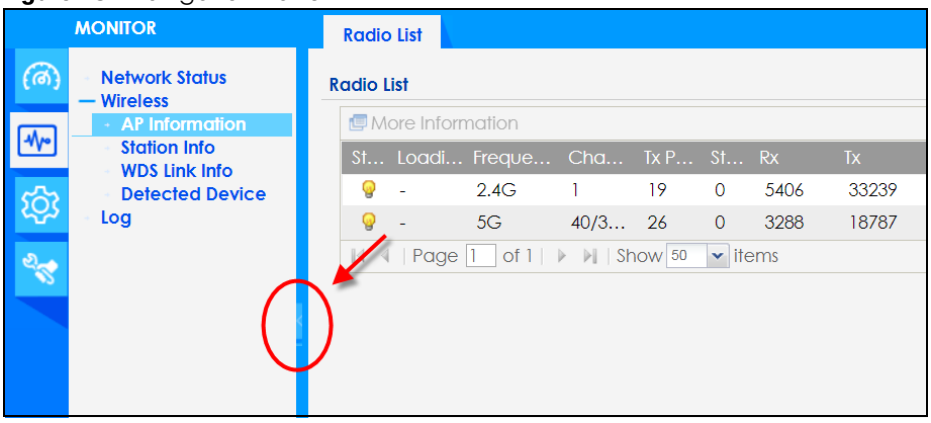
Click **Clear** to remove the currently displayed information.

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 28 Navigation Panel



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 1.4 on page 19 to see which features your Zyxel Device model supports.

Dashboard

The dashboard displays 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 67.

Monitor Menu

The monitor menu screens display status and statistics information.

Table 19 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 20 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 wireless 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 wireless clients.
DCS	DCS	Configure dynamic wireless 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.
AP Profile	Radio	Create and manage wireless radio settings files that can be associated with different APs.
	SSID	Create and manage wireless SSID, security, MAC filtering, and layer-2 isolation files that can be associated with different APs.
MON Profile	MON Profile	Create and manage rogue AP monitoring files that can be associated with different APs.

Table 20 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
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.
TELNET	TELNET	Configure telnet server settings for the Zyxel Device.
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, e-mail logs, and remote syslog servers.

Maintenance Menu

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

Table 21 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.
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.
Shutdown	Shutdown	Turn off the Zyxel Device.

4.3.4 Cloud Mode Navigation Panel Menus

If your Zyxel Device is in 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 26 on page 229.

Configuration Menu

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

Table 22 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.

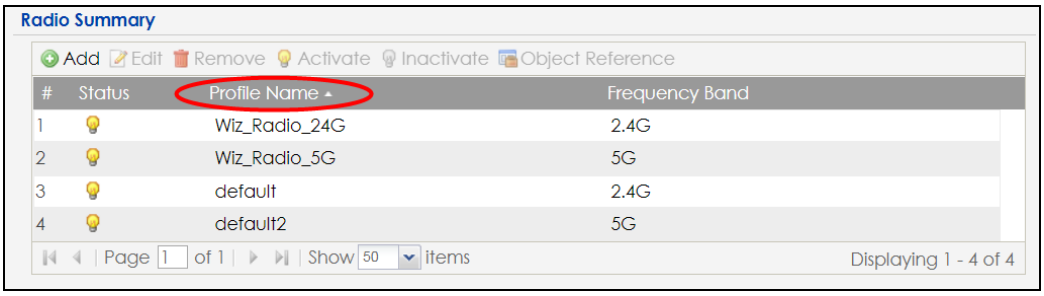
4.3.5 Tables and Lists

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

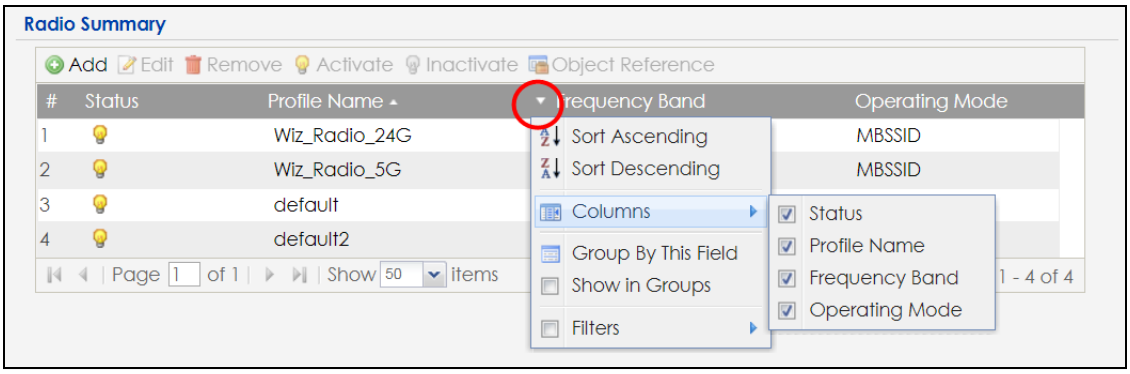
Here are some of the ways you can manipulate the Web Configurator tables.

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

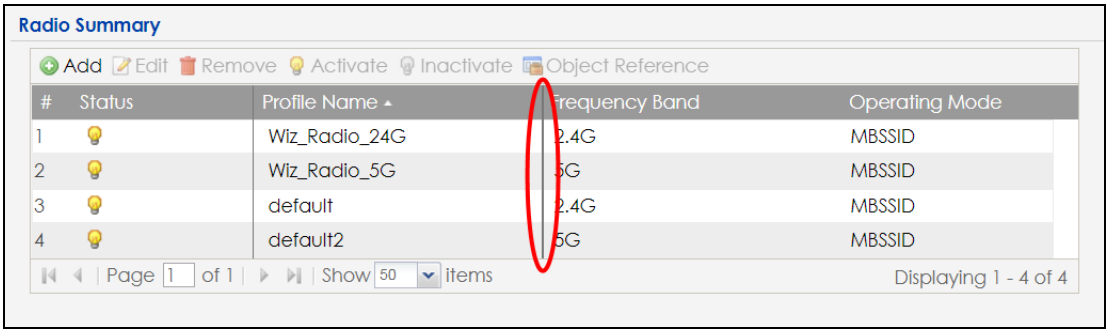


2 Click the down arrow next to a column heading for more options about how to display the entries. The options available vary depending on the type of fields in the column. Here are some examples of what you can do:

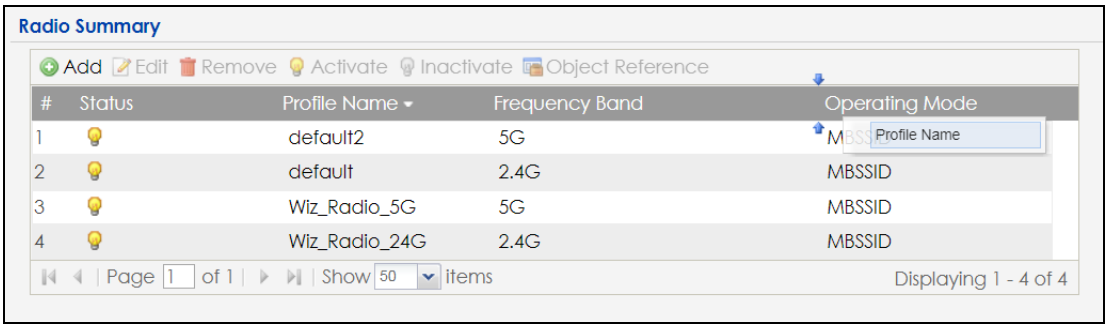
- Sort in ascending alphabetical order
- Sort in descending (reverse) alphabetical order
- Select which columns to display
- Group entries by field
- Show entries in groups
- Filter by mathematical operators (<, >, or =) or searching for text.



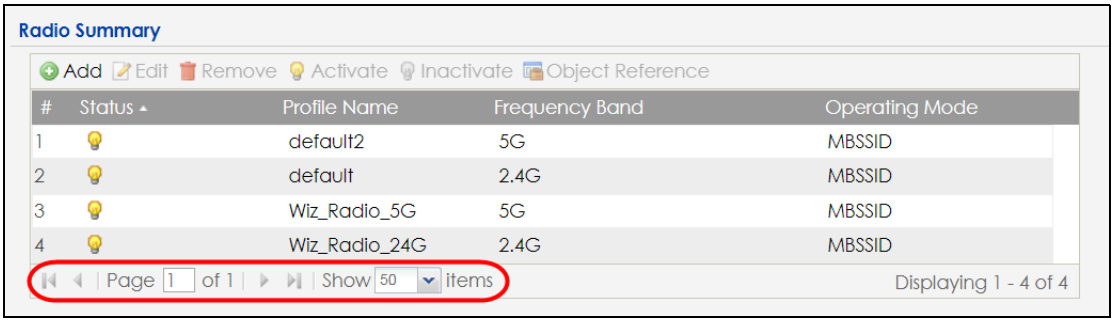
3 Select a column heading cell's right border and drag to re-size the column.



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.



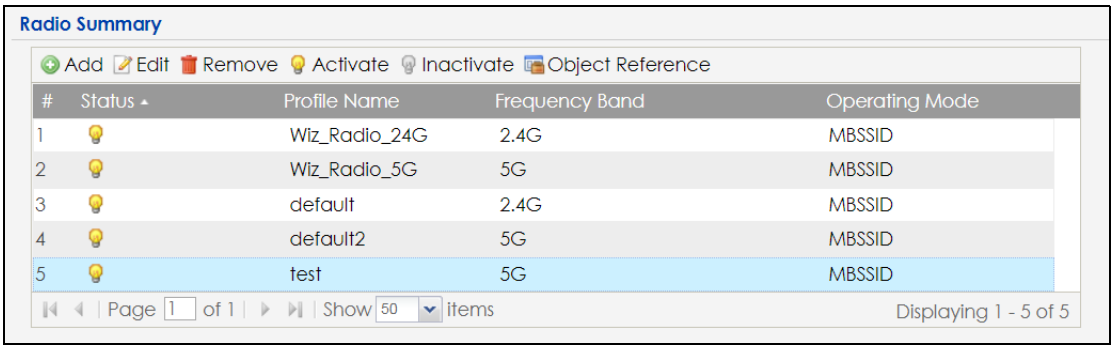
5 Use the icons and fields at the bottom of the table to navigate to different pages of entries and control how many entries display at a time.



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.

Table 23 Common Table Icons



Here are descriptions for the most common table icons.

Table 24 Common Table Icons

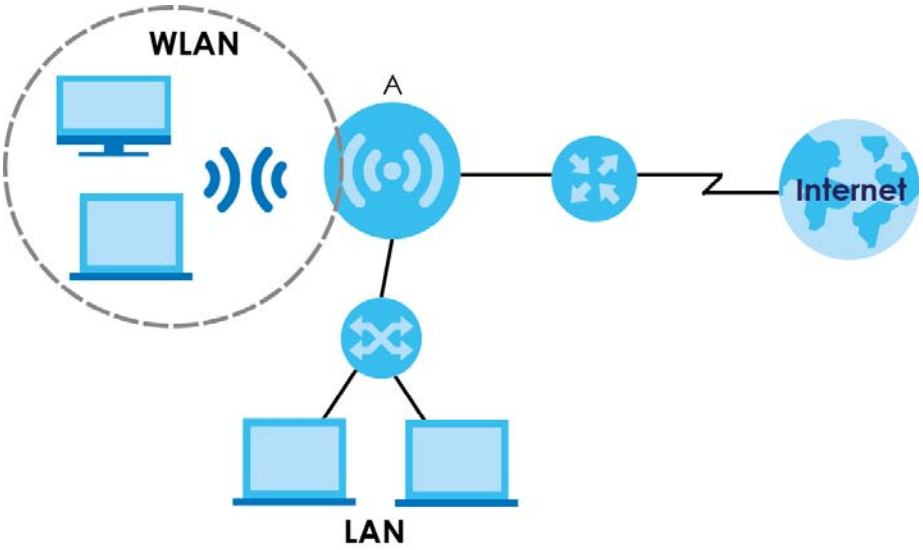
LABEL	DESCRIPTION
Add	Click this to create a new entry. For features where the entry's position in the numbered list is important (features where the Zyxel Device applies the table's entries in order like the firewall for example), you can select an entry and click **Add** to create a new entry after 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, wireless 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.

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

Table 25 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 25 Starting and Stopping the Zyxel Device

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 29.6 on page 247 for more information.
Clicking **Maintenance > Shutdown > Shutdown** or using the `shutdown` command	Clicking **Maintenance > Shutdown > Shutdown** or using the `shutdown` command writes all cached data to the local storage and stops the system processes. Wait for the Zyxel Device to shut down and then manually turn off or remove the power. It does not turn off the power.
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.

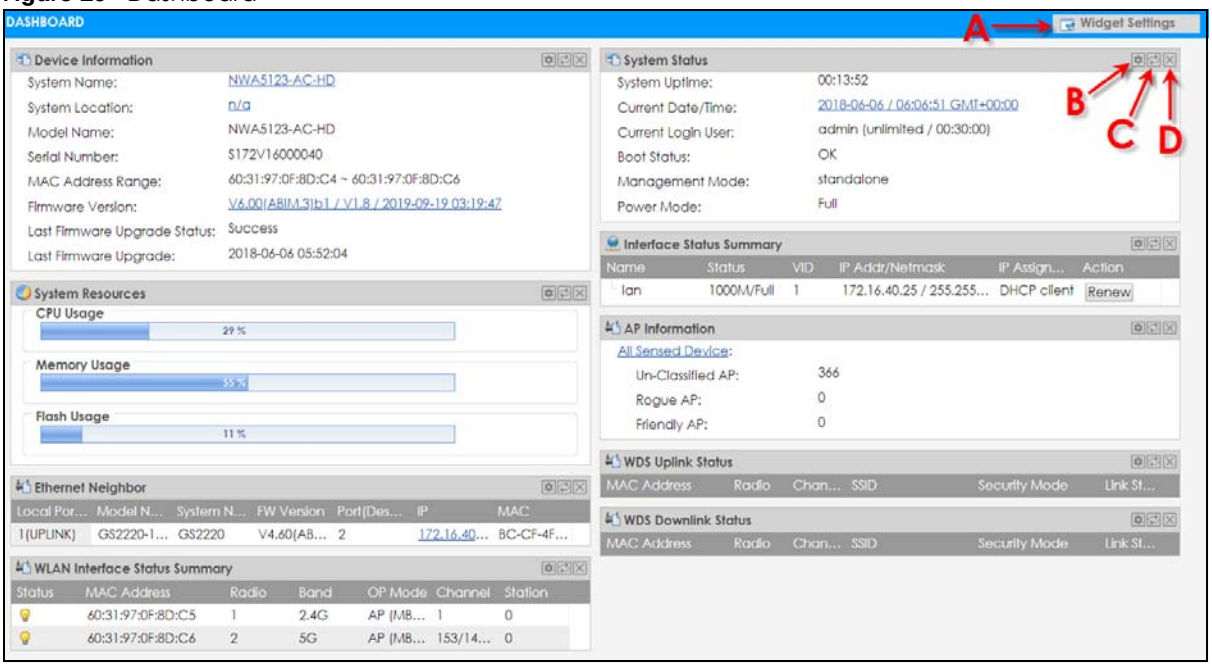
The Zyxel Device does not stop or start the system processes when you apply configuration files or run shell scripts although you may temporarily lose access to network resources.

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.

Figure 29 Dashboard



The following table describes the labels in this screen.

Table 26 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.
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.

Table 26 Dashboard (continued)

LABEL	DESCRIPTION
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 wireless 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 wireless 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.
Current Date/ Time	This field displays the current date and time in the Zyxel Device. The format is yyyy-mm-dd hh:mm:ss.

Table 26 Dashboard (continued)

LABEL	DESCRIPTION
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 1.4 on page 19.
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. **N/A** displays if the Zyxel Device does not support BLE. **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.
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.

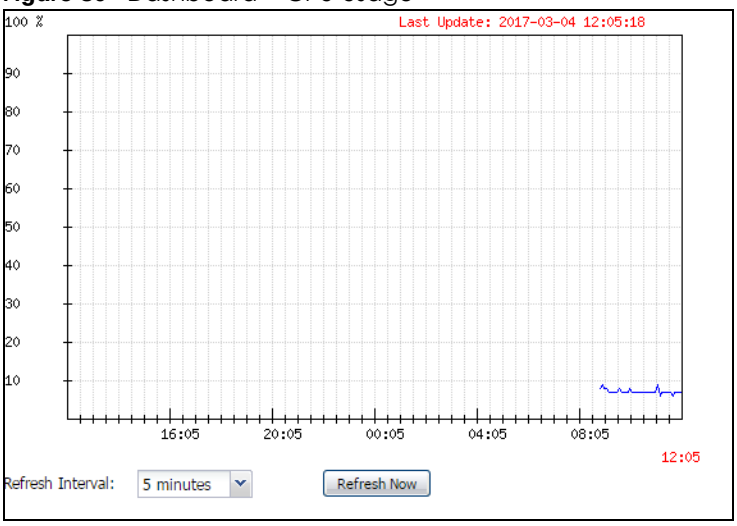
Table 26 Dashboard (continued)

LABEL	DESCRIPTION
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.
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 wireless frequency band currently being used by the radio. This shows **-** when the radio is in monitor mode.
OP Mode	This indicates the radio's operating mode. Operating modes are **AP (MBSSID)**, **MON** (monitor), **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 1.4 on page 19 to see if your Zyxel Device has an antenna switch.
Station	This displays the number of wireless 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 30 Dashboard > CPU Usage



The following table describes the labels in this screen.

Table 27 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 31 Dashboard > Memory Usage

The following table describes the labels in this screen.

Table 28 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 wireless and wireless 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.

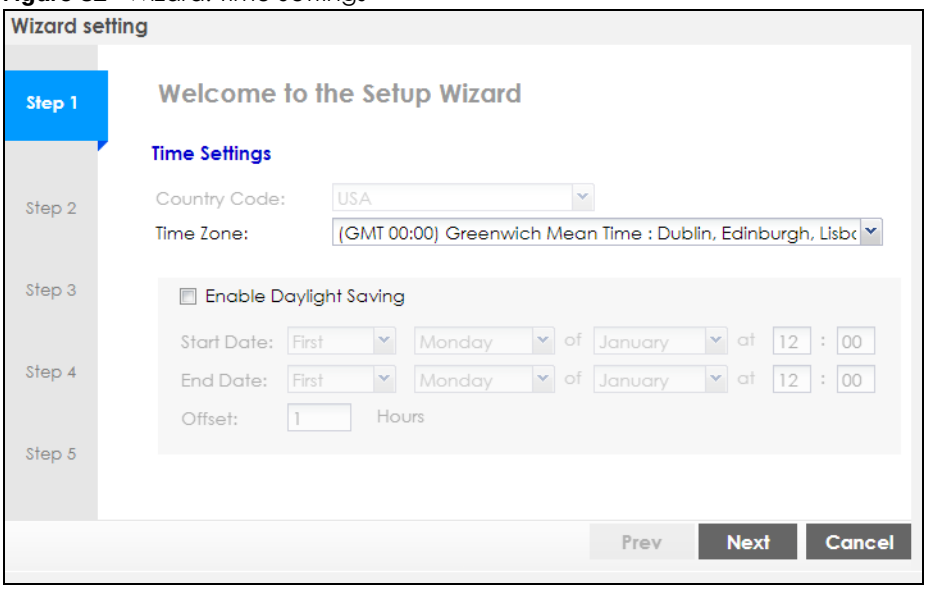
- **Country Code**: Select the country where the Zyxel Device is located.

Note: The country code 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.

- **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 32 Wizard: Time Settings



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.

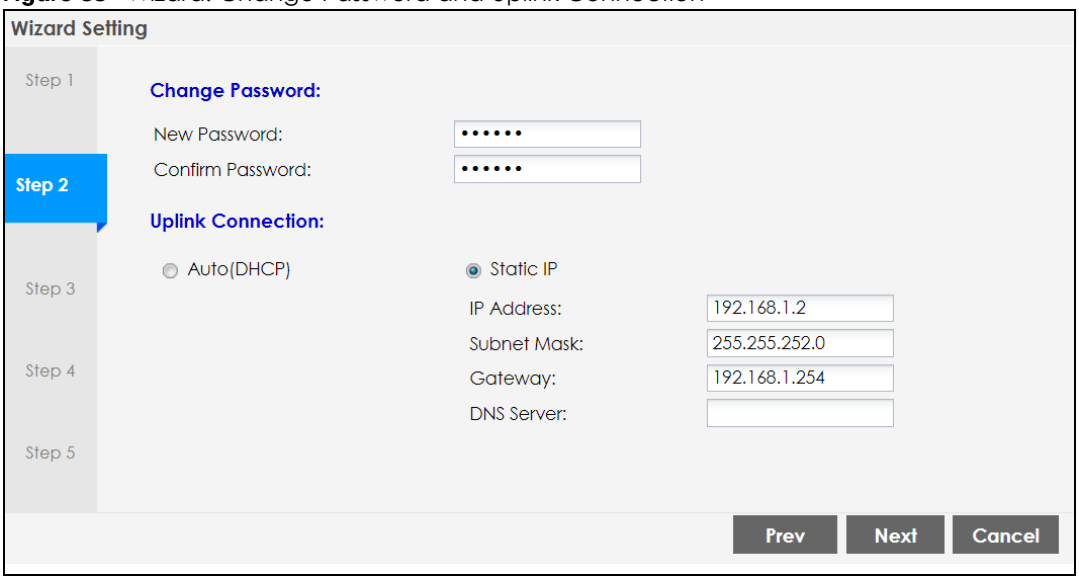
Uplink Connection: Select **Auto (DHCP)** if the Zyxel Device is connected to a router with the DHCP server enabled. You then need to check the router for the IP address assigned to the Zyxel Device in order to access the Zyxel Device's web configurator again.

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.

Figure 33 Wizard: Change Password and Uplink Connection



7.2.3 Step 3 Radio

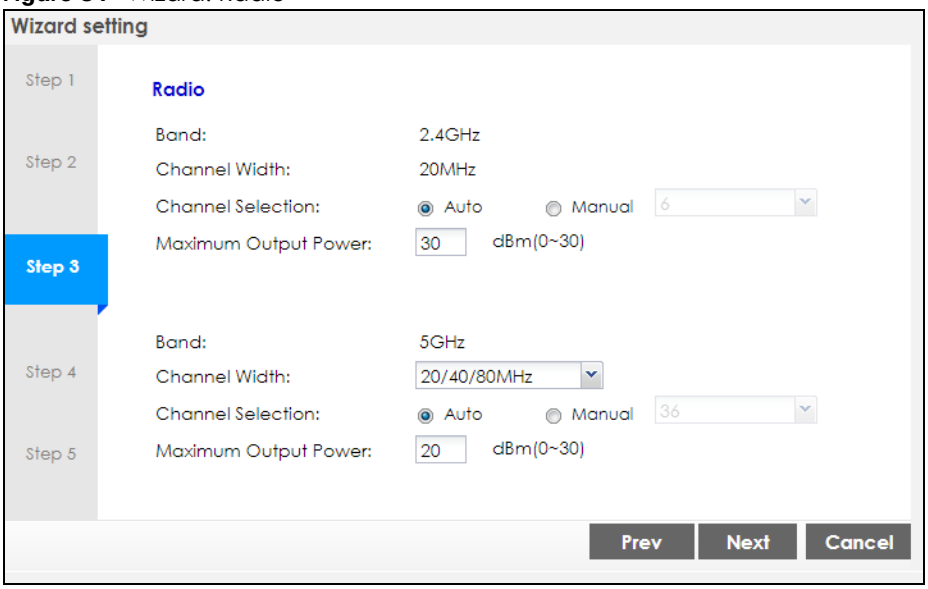
Use this screen to configure the Zyxel Device's radio transmitter(s).

- **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 2.4GHz or 5GHz 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.

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

Figure 34 Wizard: Radio



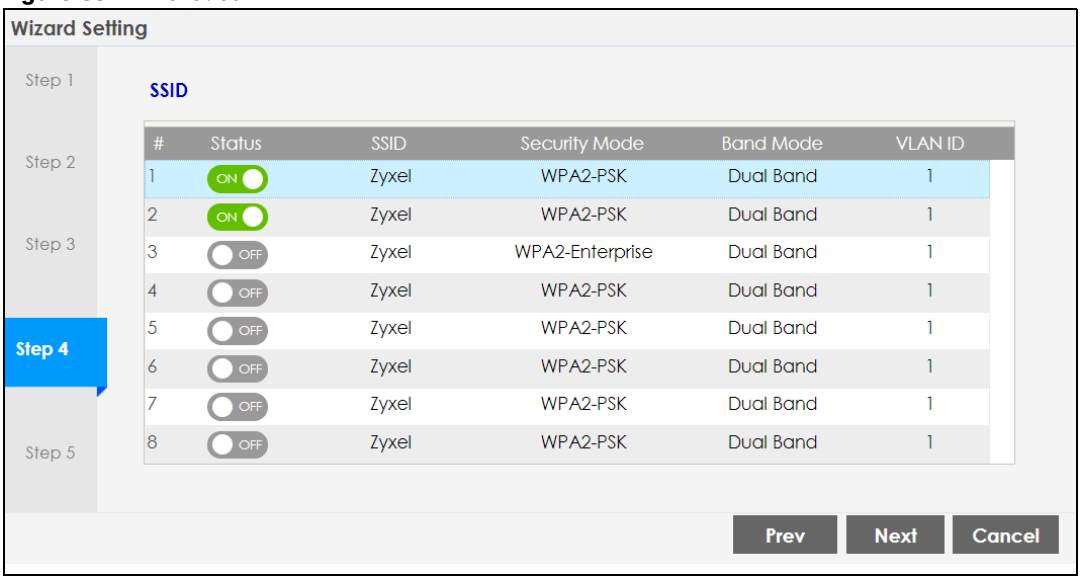
7.2.4 Step 4 SSID

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 7.2.4.1 on page 76 for more information.

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

Figure 35 Wizard: SSID



7.2.4.1 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.
- **VLAN ID**: Enter a VLAN ID for the Zyxel Device to use to tag traffic originating from this SSID.

  Band Mode: Select the wireless band which this profile should use. 2.4 GHz is the frequency used by IEEE 802.11b/g/n wireless clients. 5 GHz is the frequency used by IEEE 802.11ac/a/n wireless clients.
- **Security Type**: Select **WPA2** to add security on this wireless network. Otherwise, select **OPEN** to allow any wireless client to associate this network without authentication.
- **Personal**: If you set **Security Type** to **WPA2** 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.

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

Figure 36 Wizard: SSID: Edit (WPA2-Personal)

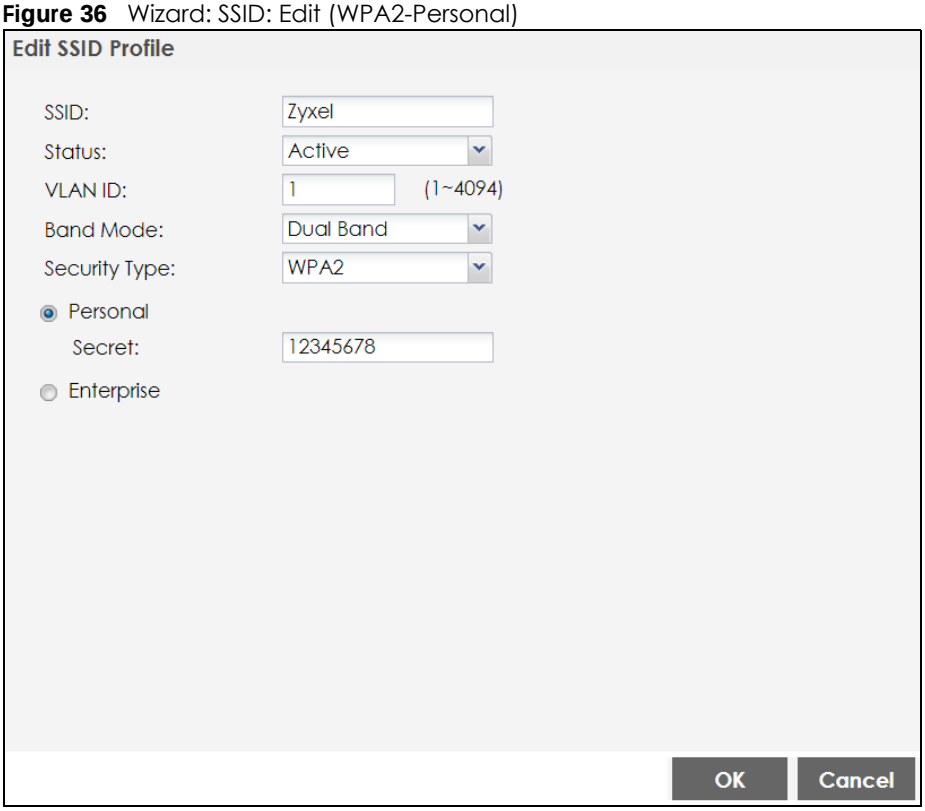
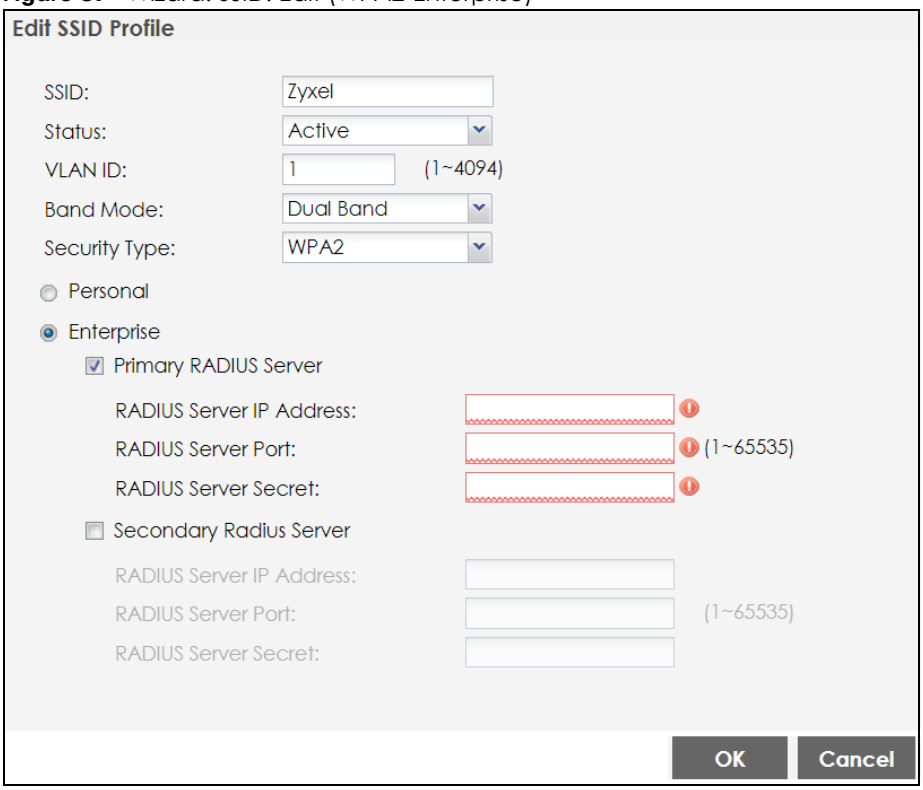


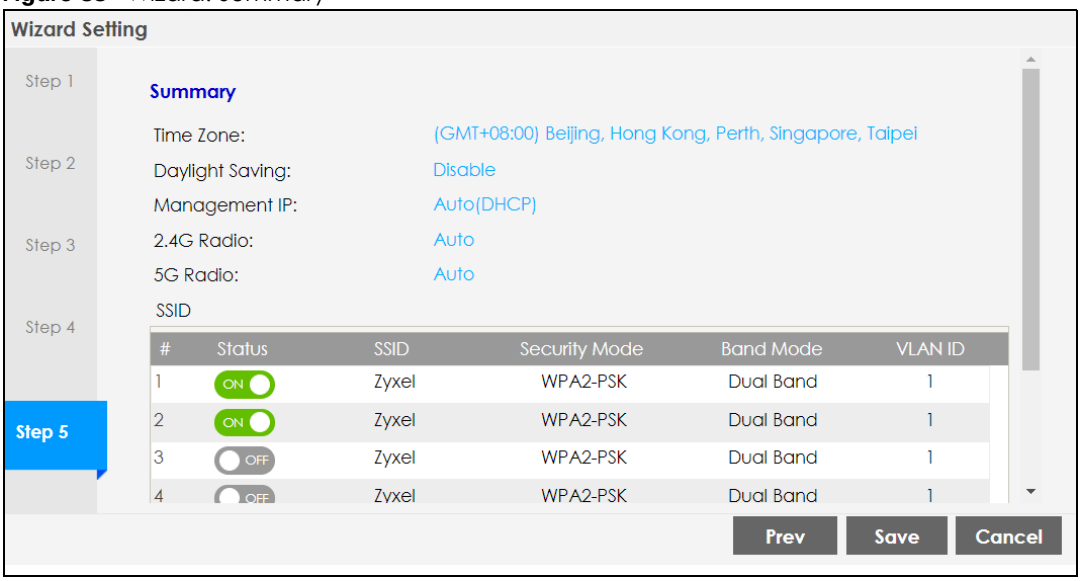
Figure 37 Wizard: SSID: Edit (WPA2-Enterprise)



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 38 Wizard: Summary



CHAPTER 8
Monitor

8.1 Overview

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

8.1.1 What You Can Do in this Chapter

- The **Network Status** screen (Section 8.3 on page 80) displays general LAN interface information and packet statistics.
- The **AP Information** > **Radio List** screen (Section 8.4 on page 82) displays statistics about the wireless radio transmitters in the Zyxel Device.
- The **Station Info** screen (Section 8.5 on page 86) displays statistics pertaining to the associated stations.
- The **WDS Link Info** screen (Section 8.6 on page 87) displays statistics about the Zyxel Device's WDS (Wireless Distribution System) connections.
- The **Detected Device** screen (Section 8.7 on page 88) displays information about suspected rogue APs.
- The **View Log** screen (Section 8.8 on page 91) displays the Zyxel Device's current log messages. You can change the way the log is displayed, you can e-mail the log, and you can also clear the log in this screen.

8.2 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. See Chapter 14 on page 150 for details.

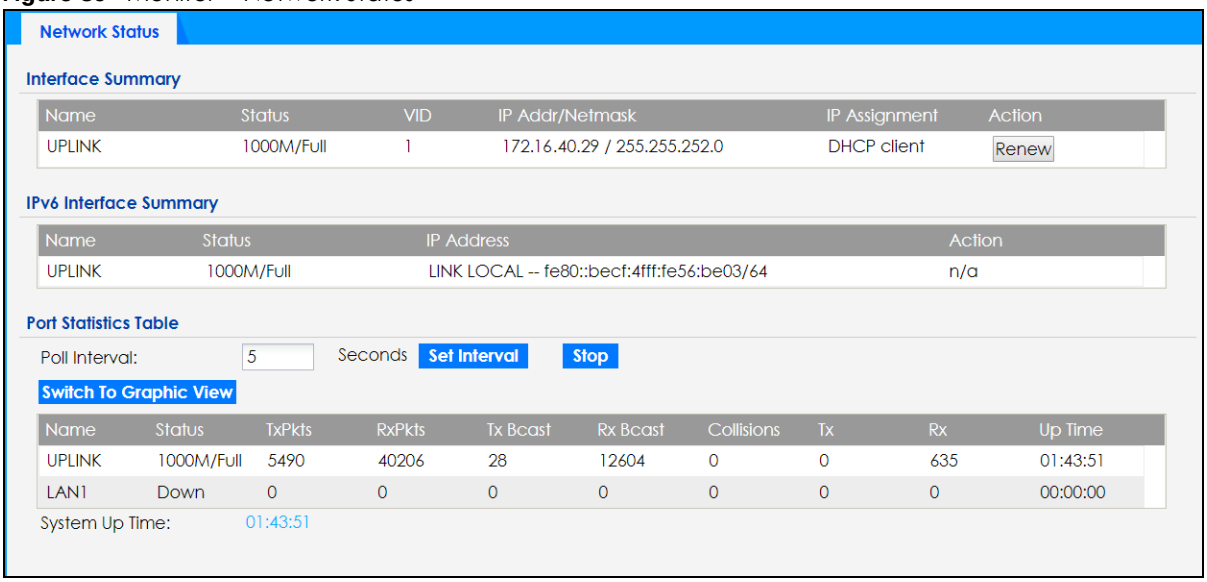
Friendly AP

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). See Chapter 14 on page 150 for details.

8.3 Network Status

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

Figure 39 Monitor > Network Status



The following table describes the labels in this screen.

Table 29 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**.

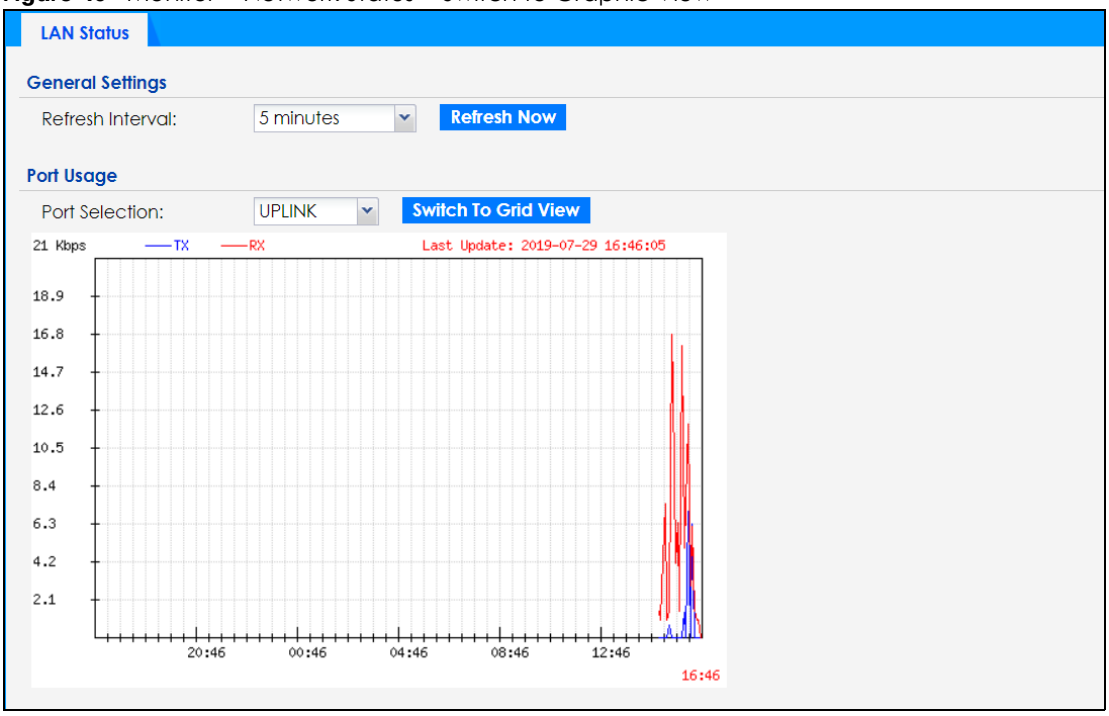
Table 29 Monitor > Network Status (continued)

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.

8.3.1 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 40 Monitor > Network Status > Switch to Graphic View



The following table describes the labels in this screen.

Table 30 Monitor > Network Status > Switch to Graphic View

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want this window to be automatically updated.
Refresh Now	Click this to update the information in the window right away.
Port Selection	Select the Ethernet port for which you want to view the packet statistics.
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.

8.4 Radio List

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

Figure 41 Monitor > Wireless > AP Information > Radio List (for Zyxel Device that supports WDS)

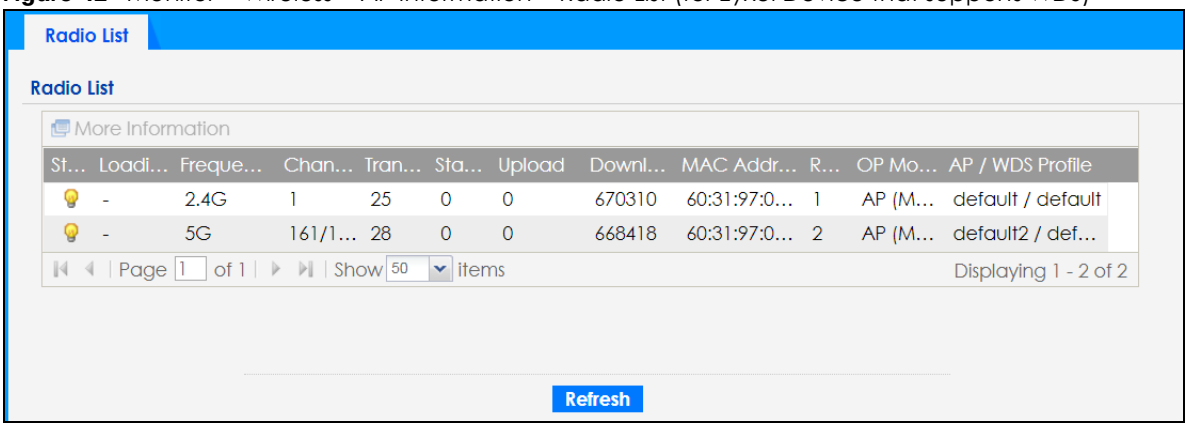
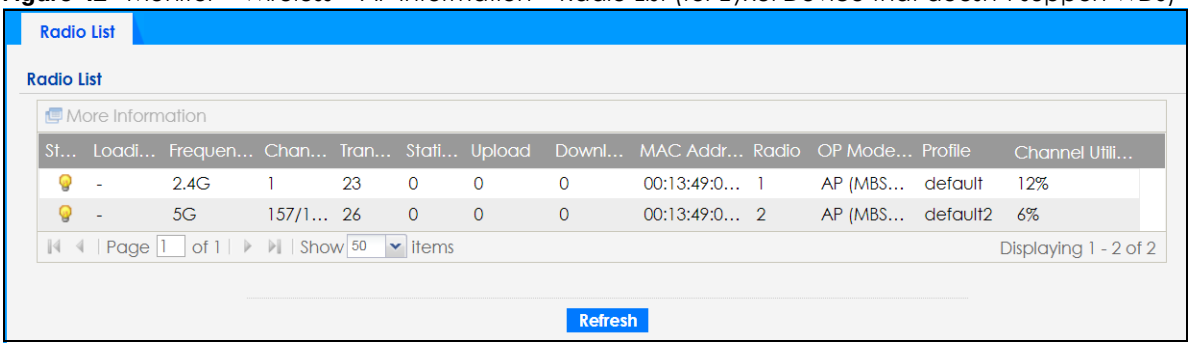


Figure 42 Monitor > Wireless > AP Information > Radio List (for Zyxel Device that doesn't support WDS)



The following table describes the labels in this screen.

Table 31 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.
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 or the radio is in monitor mode.
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)**, **MONITOR**, **Root AP** or **Repeater**
AP/WDS Profile	This indicates the AP profile name and WDS profile name to which the radio belongs. This field is available only on the Zyxel Device that supports WDS.
Profile	This indicates the AP profile name to which the radio belongs. This field is available only on the Zyxel Device that doesn't support WDS.
Frequency Band	This indicates the wireless frequency band currently being used by the radio. This shows **-** when the radio is in monitor mode.
Channel	This indicates the radio's channel ID.
Transmit Power	This displays the output power of the radio.
Station	This displays the number of wireless clients connected to this radio on the Zyxel Device.

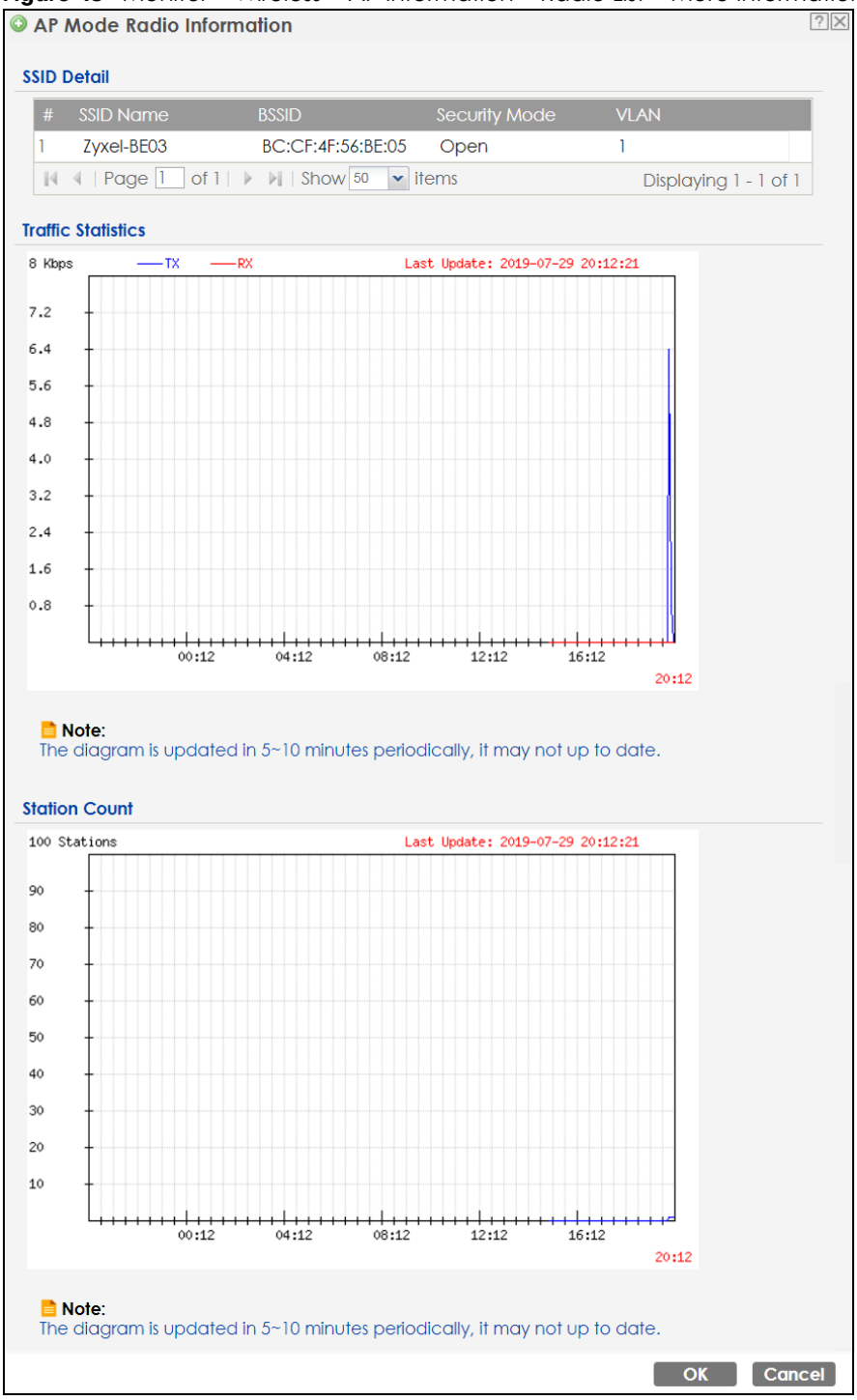
Table 31 Monitor > Wireless > AP Information > Radio List (continued)

LABEL	DESCRIPTION
Upload	This displays the total number of packets received by the radio.
Download	This displays the total number of packets transmitted by the radio.
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.

8.4.1 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 43 Monitor > Wireless > AP Information > Radio List > More Information



The following table describes the labels in this screen.

Table 32 Monitor > Wireless > AP Information > Radio List > More Information

LABEL	DESCRIPTION
SSID Detail	This list shows information about all the wireless 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.

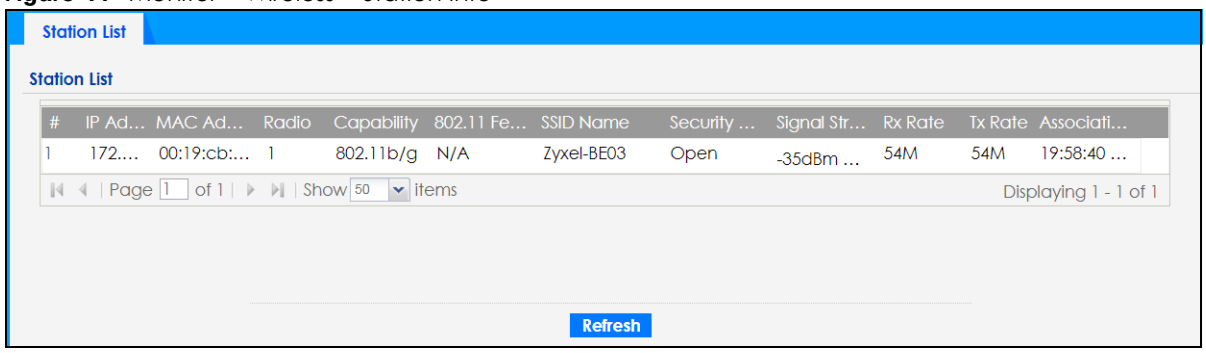
Table 32 Monitor > Wireless > AP Information > Radio List > More Information (continued)

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.
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.

8.5 Station List

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

Figure 44 Monitor > Wireless > Station Info



The following table describes the labels in this screen.

Table 33 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.
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.
Capability	This displays the supported standard currently being used by the station or the standards supported by the station.
802.11 Features	This displays whether the station supports IEEE802.11r, IEEE 802.11k, IEEE 802.11v or none of the above (**N/A**).

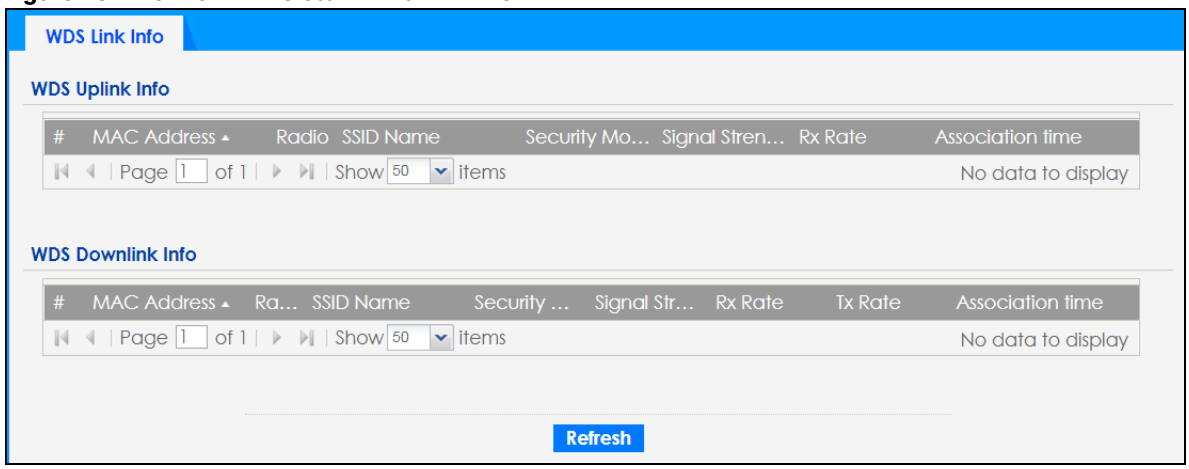
Table 33 Monitor > Wireless > Station Info (continued)

LABEL	DESCRIPTION
SSID Name	This indicates the name of the wireless network to which the station is connected. A single AP can have multiple SSIDs or networks.
Security Mode	This indicates which secure encryption methods is being used by the station to connect to the network.
Signal Strength	This is the RSSI (Received Signal Strength Indicator) of the station's wireless connection.
Tx Rate	This is the maximum transmission rate of the station.
Rx Rate	This is the maximum reception rate of the station.
Association Time	This displays the time the station first associated with the Zyxel Device's wireless network.
Refresh	Click this to refresh the items displayed on this page.

8.6 WDS Link Info

Use this screen to view the WDS traffic statistics between the Zyxel Device and a root AP or repeaters. See Section 1.2 on page 13 to know more about WDS. Click **Monitor > Wireless > WDS Link Info** to access this screen.

Figure 45 Monitor > Wireless > WDS Link Info



The following table describes the labels in this screen.

Table 34 Monitor > Wireless > WDS Link Info

LABEL	DESCRIPTION
WDS Uplink Info WDS 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.

Table 34 Monitor > Wireless > WDS Link Info (continued)

LABEL	DESCRIPTION
MAC Address	This is the MAC address of the root AP or repeater 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 wireless 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.

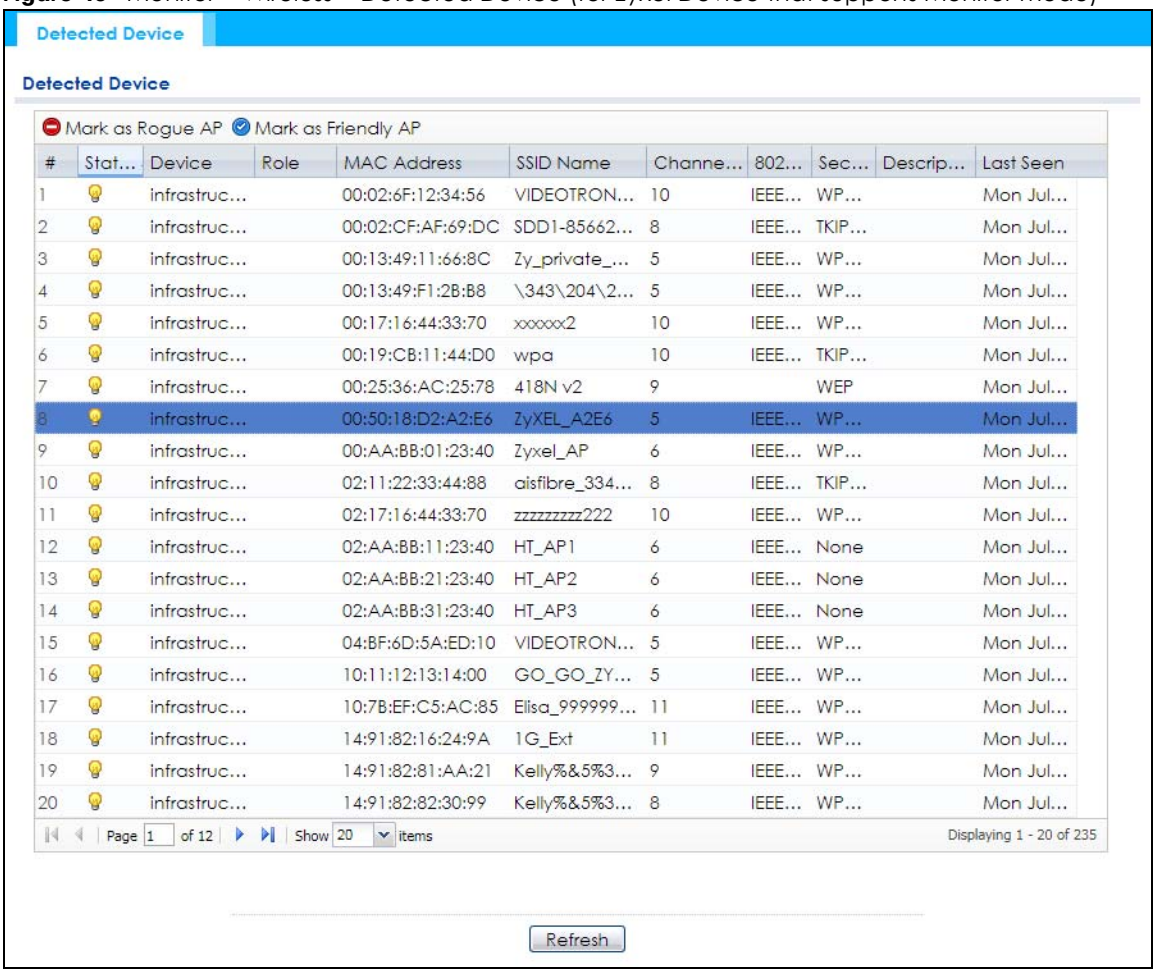
8.7 Detected Device

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. Not all Zyxel Devices support monitor mode (see Section 1.4 on page 19). For more information about Rogue APs, see Section 10.3 on page 109.

Note: If the Zyxel Device supports monitor mode, the radio or at least one of the Zyxel Device's radio must be set to monitor mode (in the **Wireless > AP Management** screen) in order to detect other wireless devices in its vicinity.

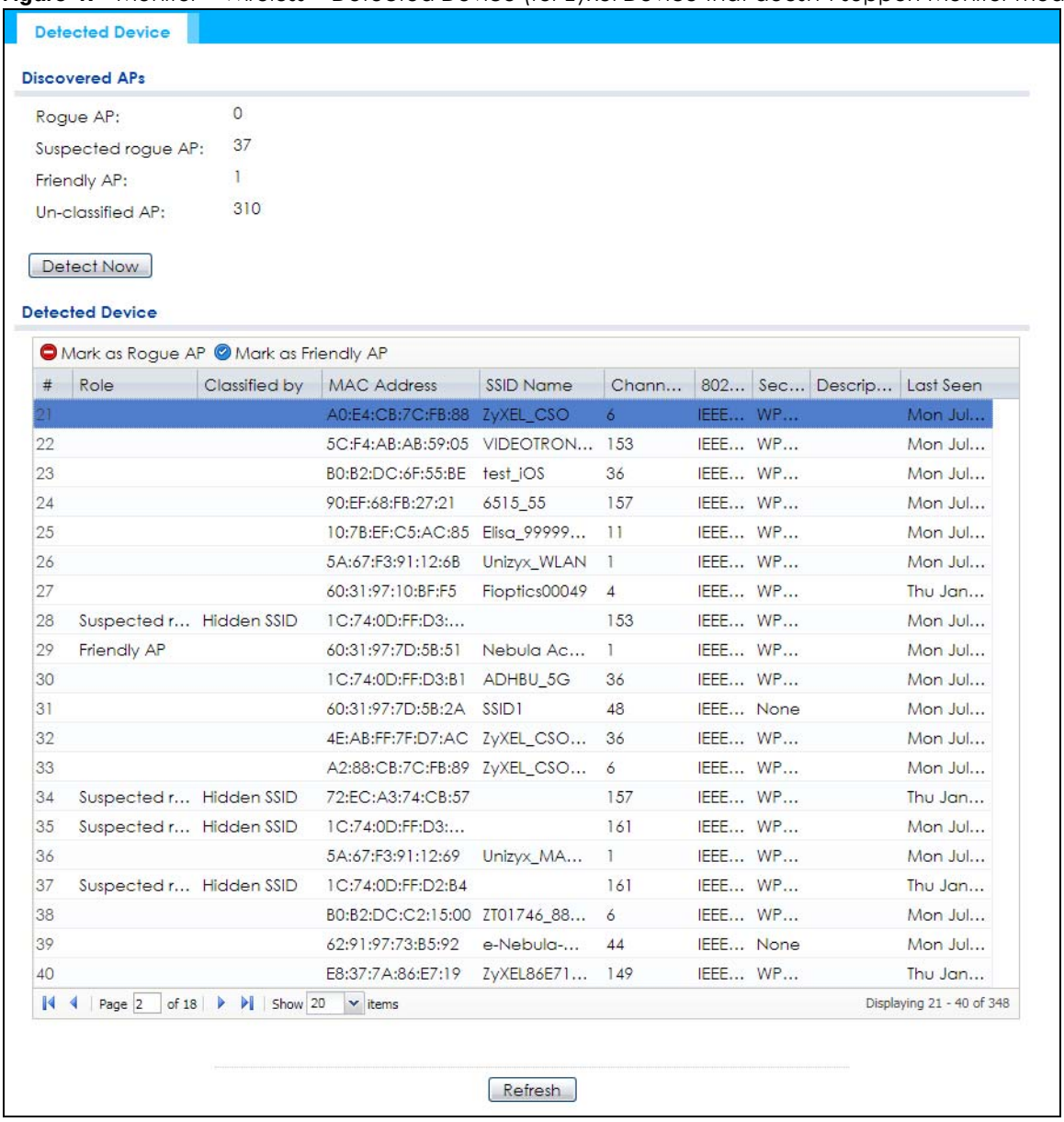
If the Zyxel Device doesn't support monitor mode, turn on rogue AP detection in the **Configuration > Wireless > Rogue AP** screen to detect other APs.

Figure 46 Monitor > Wireless > Detected Device (for Zyxel Device that supports Monitor mode)



#	Stat...	Device	Role	MAC Address	SSID Name	Channe...	802...	Sec...	Descrip...	Last Seen
1		infrastruc...		00:02:6F:12:34:56	VIDEOTRON...	10	IEEE...	WP...		Mon Jul...
2		infrastruc...		00:02:CF:AF:69:DC	SDD1-85662...	8	IEEE...	TKIP...		Mon Jul...
3		infrastruc...		00:13:49:11:66:8C	Zy_private_...	5	IEEE...	WP...		Mon Jul...
4		infrastruc...		00:13:49:F1:2B:B8	\343\204\2...	5	IEEE...	WP...		Mon Jul...
5		infrastruc...		00:17:16:44:33:70	xxxxxx2	10	IEEE...	WP...		Mon Jul...
6		infrastruc...		00:19:CB:11:44:D0	wpa	10	IEEE...	TKIP...		Mon Jul...
7		infrastruc...		00:25:36:AC:25:78	418N v2	9		WEP		Mon Jul...
8		infrastruc...		00:50:18:D2:A2:E6	ZyXEL_A2E6	5	IEEE...	WP...		Mon Jul...
9		infrastruc...		00:AA:BB:01:23:40	Zyxel_AP	6	IEEE...	WP...		Mon Jul...
10		infrastruc...		02:11:22:33:44:88	aisfibre_334...	8	IEEE...	TKIP...		Mon Jul...
11		infrastruc...		02:17:16:44:33:70	zzzzzzzzz222	10	IEEE...	WP...		Mon Jul...
12		infrastruc...		02:AA:BB:11:23:40	HT_AP1	6	IEEE...	None		Mon Jul...
13		infrastruc...		02:AA:BB:21:23:40	HT_AP2	6	IEEE...	None		Mon Jul...
14		infrastruc...		02:AA:BB:31:23:40	HT_AP3	6	IEEE...	None		Mon Jul...
15		infrastruc...		04:BF:6D:5A:ED:10	VIDEOTRON...	5	IEEE...	WP...		Mon Jul...
16		infrastruc...		10:11:12:13:14:00	GO_GO_ZY...	5	IEEE...	WP...		Mon Jul...
17		infrastruc...		10:7B:EF:C5:AC:85	Elisa_999999...	11	IEEE...	WP...		Mon Jul...
18		infrastruc...		14:91:82:16:24:9A	1G_Ext	11	IEEE...	WP...		Mon Jul...
19		infrastruc...		14:91:82:81:AA:21	Kelly%&5%3...	9	IEEE...	WP...		Mon Jul...
20		infrastruc...		14:91:82:82:30:99	Kelly%&5%3...	8	IEEE...	WP...		Mon Jul...

Figure 47 Monitor > Wireless > Detected Device (for Zyxel Device that doesn't support Monitor mode)



The following table describes the labels in this screen.

Table 35 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 10.3 on page 109.
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	

Table 35 Monitor > Wireless > Detected Device (continued)

LABEL	DESCRIPTION
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 10.3 on page 109).
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 10.3 on page 109).
#	This is the detected device's index number in this list.
Status	This indicates the detected device's status.
Device	This indicates the type of device detected.
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.
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 10.3 on page 109).
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.

8.8 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.

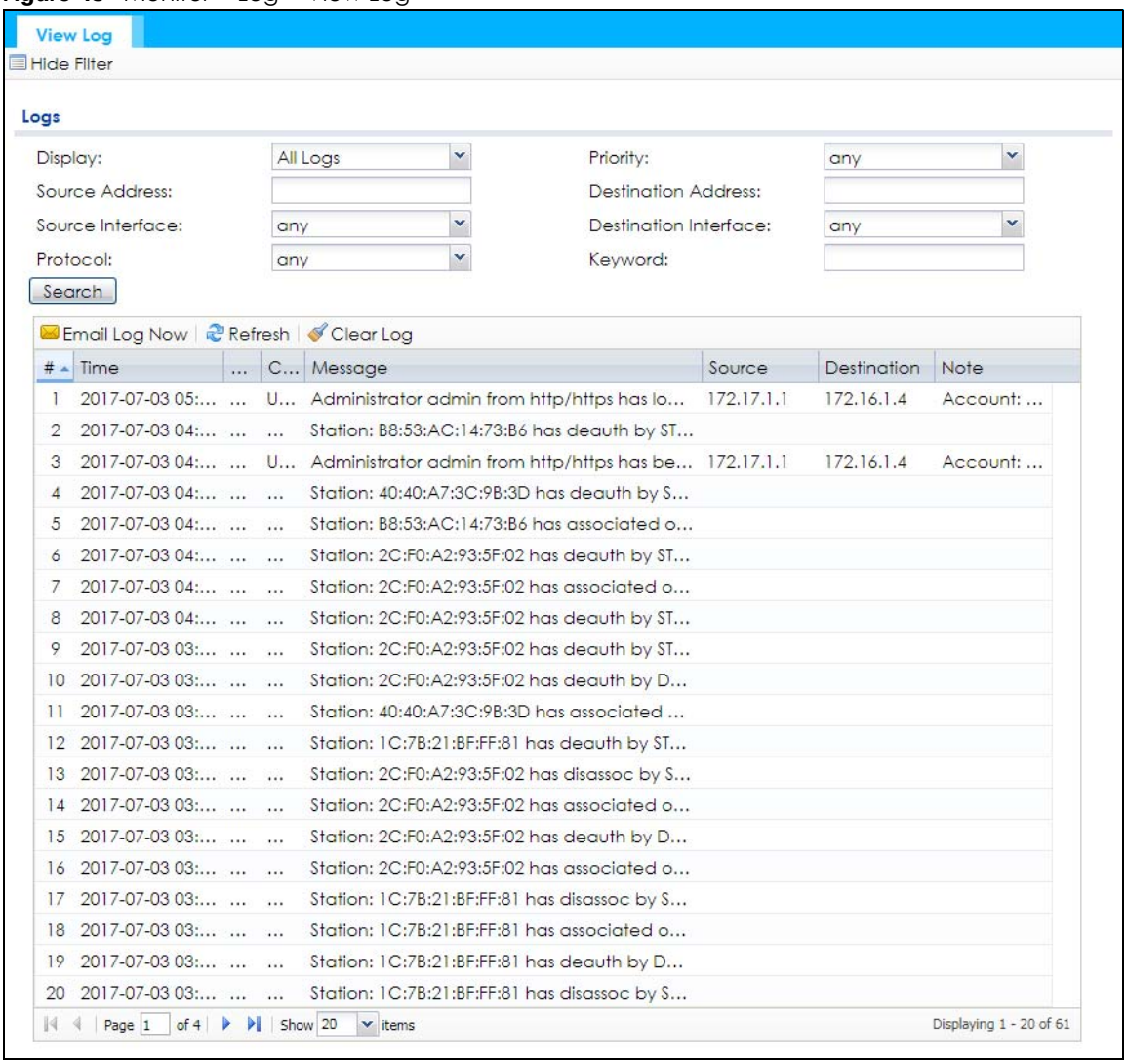
To access this screen, click **Monitor > Log**. The log is displayed in the following screen.

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 48 Monitor > Log > View Log



The following table describes the labels in this screen.

Table 36 Monitor > Log > View Log

LABEL	DESCRIPTION
Show Filter / Hide Filter	Click this button to show or hide the filter settings. If the filter settings are hidden, the **Display**, **Email Log Now**, **Refresh**, and **Clear Log** fields are available. If the filter settings are shown, the **Display**, **Priority**, **Source Address**, **Destination Address**, **Source Interface**, **Destination Interface**, **Protocol**, **Keyword**, and **Search** fields are available.
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.

Table 36 Monitor > Log > View Log (continued)

LABEL	DESCRIPTION
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** e-mail 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.

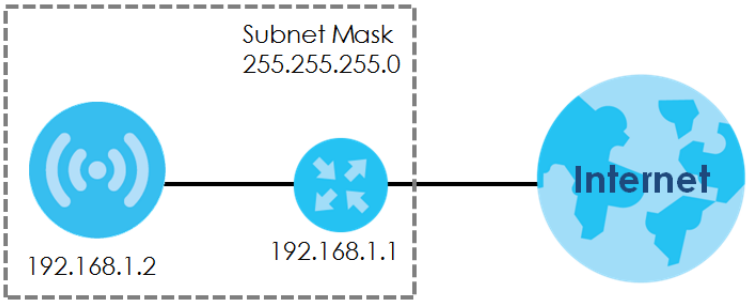
CHAPTER 9
Network

9.1 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 49 IP Setup



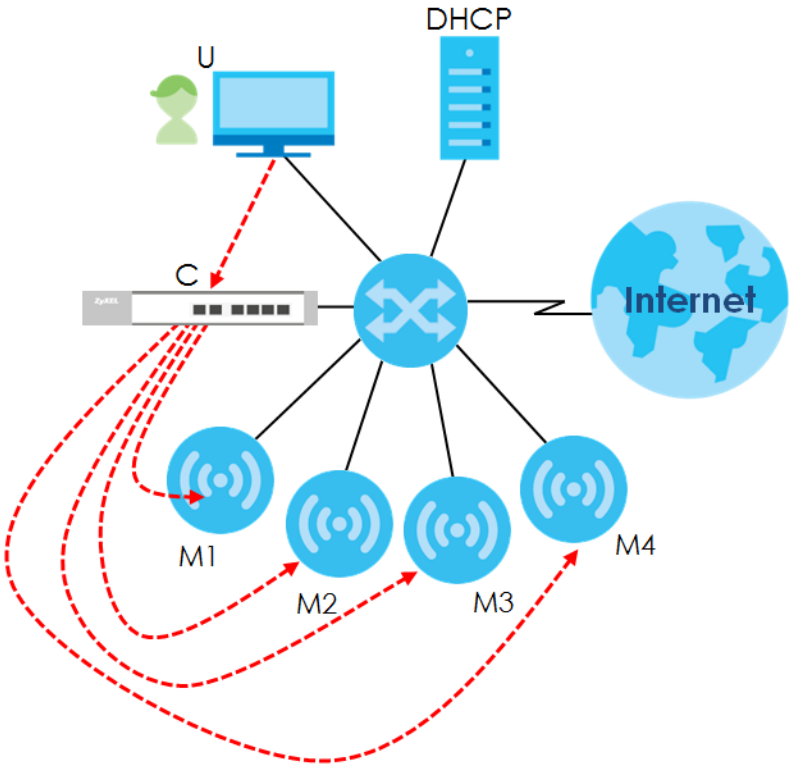
The figure above illustrates one possible setup of your Zyxel Device. The gateway IP address is 192.168.1.1 and the managed IP address of the Zyxel Device is 192.168.1.2 (default), but if the Zyxel Device is assigned an IP address by a DHCP server, the default (192.168.1.2) will not be used. The gateway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

9.1.1 AP Controller Management

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

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 50 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. An 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, such as NXC, 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 wireless 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

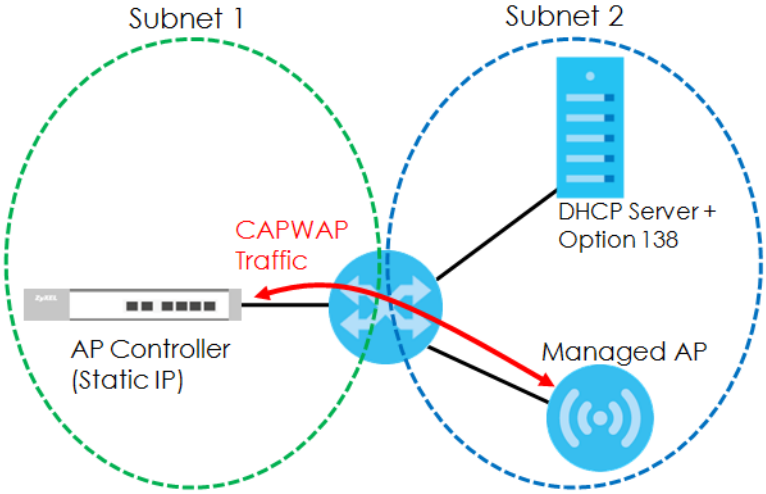
By default, CAPWAP works only between Zyxel Devices with IP addresses in the same subnet.

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 51 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 wireless clients.
- If an Zyxel Device's link to the ACis broken, the Zyxel Device continues to use the wireless settings with which it was last provided.

9.1.2 What You Can Do in this Chapter

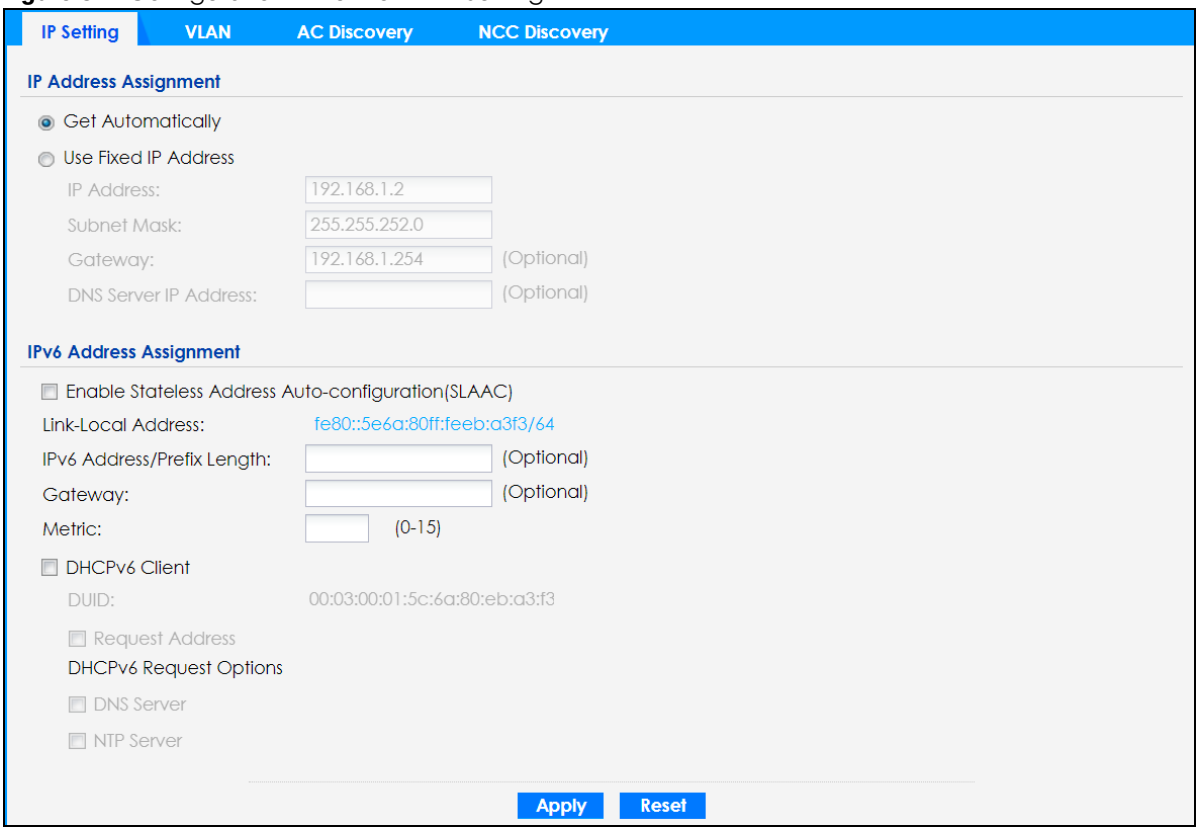
- The **IP Setting** screen (Section 9.2 on page 97) configures the Zyxel Device's LAN IP address.
- The **VLAN** screen (Section 9.3 on page 98) configures the Zyxel Device's VLAN settings.
- The **Storm Control** screen (Section 9.4 on page 101) turns on or off the traffic storm control feature on the Zyxel Device.
- The **AC Discovery** screen (Section 9.5 on page 102) configures the Zyxel Device's AP Controller (AC) settings.

- The **NCC Discovery** screen (Section 9.6 on page 103) configures the Zyxel Device's Nebula Control Center (NCC) discovery settings.

9.2 IP Setting

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

Figure 52 Configuration > Network > IP Setting



Each field is described in the following table.

Table 37 Configuration > Network > IP Setting

LABEL	DESCRIPTION
IP Address Assignment	
Get Automatically	Select this to make the interface a DHCP client and automatically get the IP address, subnet mask, and gateway address from a DHCP server.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	Enter the IP address of the gateway. The 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.

Table 37 Configuration > Network > IP Setting (continued)

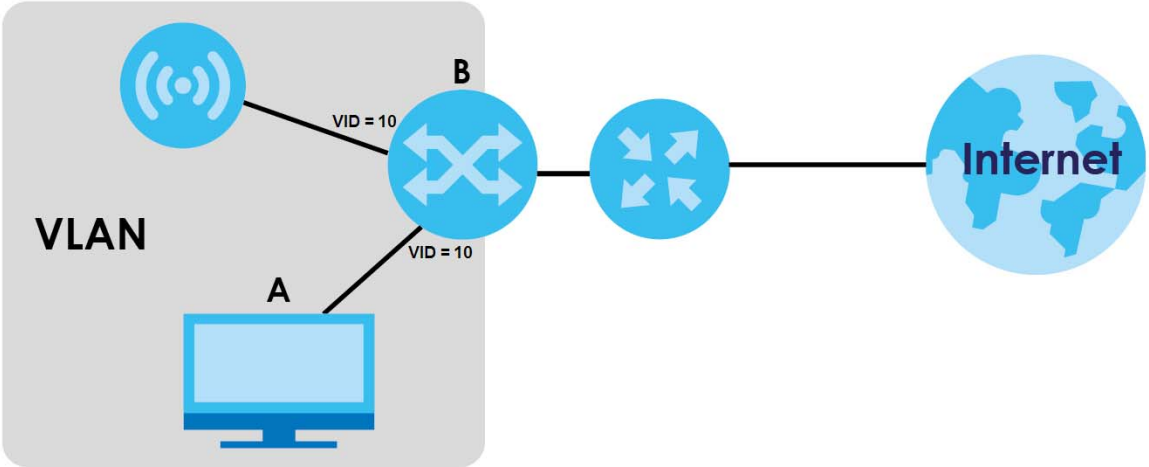
LABEL	DESCRIPTION
DNS Server IP Address	Enter the IP address of the DNS server.
IPv6 Address Assignment	
Enable Stateless Address Auto-configuration (SLAAC)	Select this to enable IPv6 stateless auto-configuration on the Zyxel Device. The Zyxel Device will generate an IPv6 address itself from a prefix 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 273 for more information.
Request Address	Select this option to get an IPv6 address from the DHCPv6 server.
DHCPv6 Request Options	Select this option 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.

9.3 VLAN

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

Note: Misconfiguring the management VLAN settings in your Zyxel Device can make it inaccessible. If this happens, you will have to reset the Zyxel Device.

Figure 53 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.

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**.

The screen varies depending on whether the Zyxel Device has an extra Ethernet port (except the uplink port).

Figure 54 Configuration > Network > VLAN (for Zyxel Device with multiple Ethernet ports)

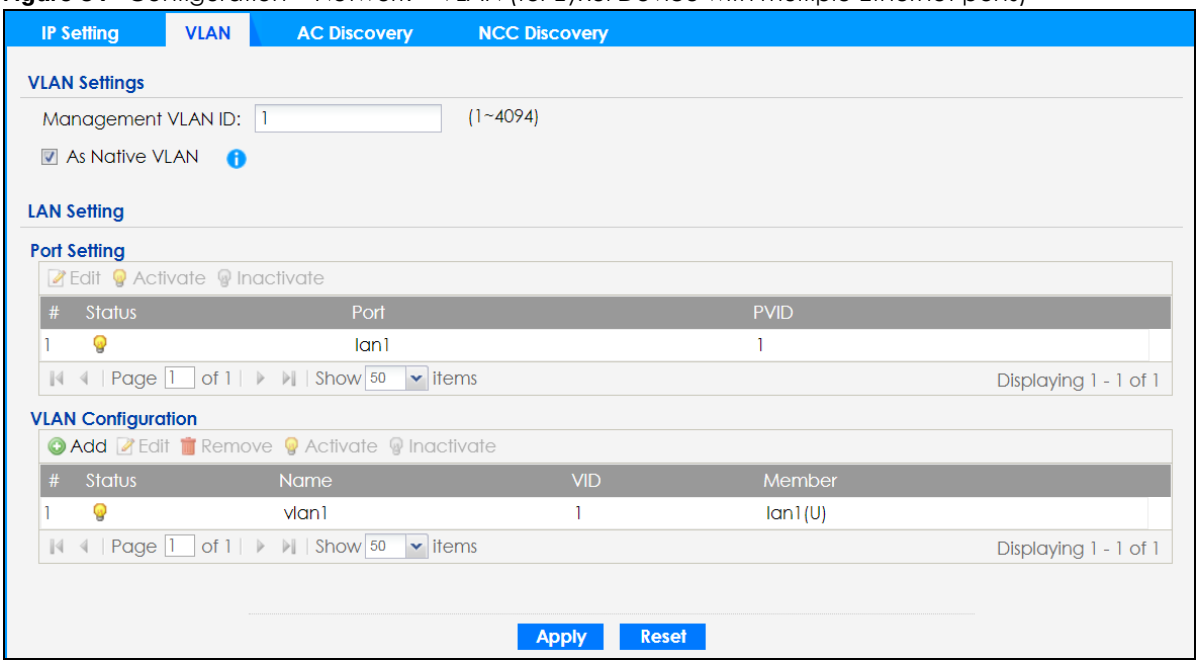
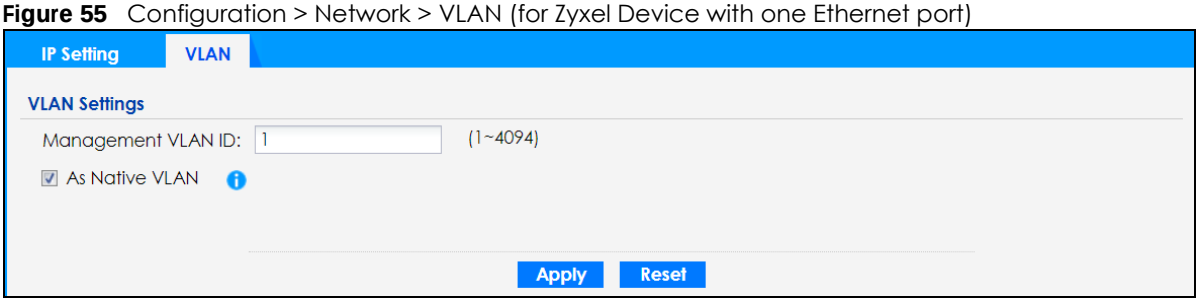


Figure 55 Configuration > Network > VLAN (for Zyxel Device with one Ethernet port)



Each field is described in the following table.

Table 38 Configuration > Network > VLAN

LABEL	DESCRIPTION
VLAN Settings	
Management VLAN ID	Enter a VLAN ID for the Zyxel Device.
As Native VLAN	Select this option to treat this VLAN ID as a VLAN created on the Zyxel Device and not one assigned to it from outside the network.
LAN Setting	
Port Setting	
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.

Table 38 Configuration > Network > VLAN (continued)

LABEL	DESCRIPTION
PVID	This field displays the port number of the VLAN ID.
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.
Member	This field displays the VLAN membership to which the port belongs.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

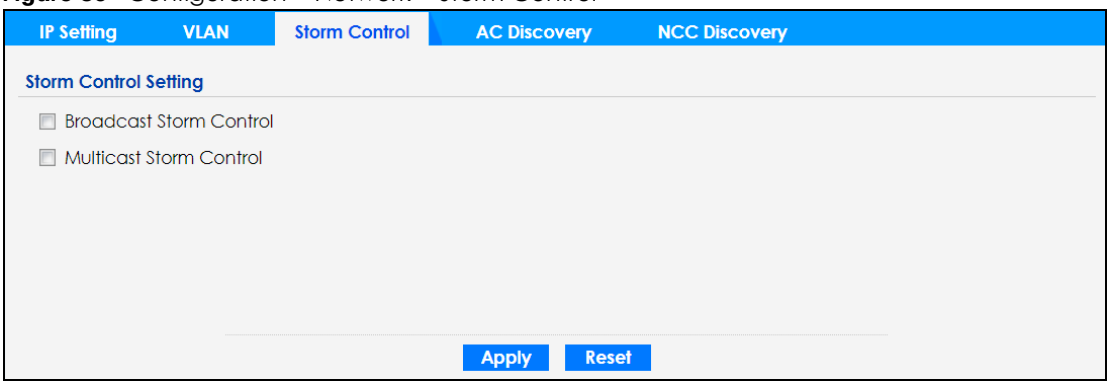
9.4 Storm Control

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: 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 56 Configuration > Network > Storm Control



Each field is described in the following table.

Table 39 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.

9.5 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 9.1.1 on page 94 for more information on AC management.

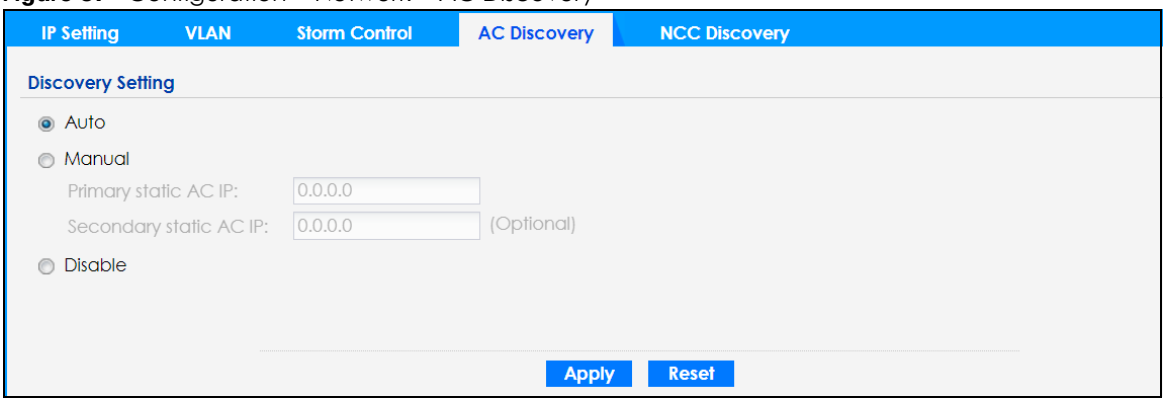
Note: The AC Discovery settings are not available in all Zyxel Devices. See Section 1.4 on page 19 for more information.

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 57 Configuration > Network > AC Discovery



Each field is described in the following table.

Table 40 Configuration > Network > AC Discovery

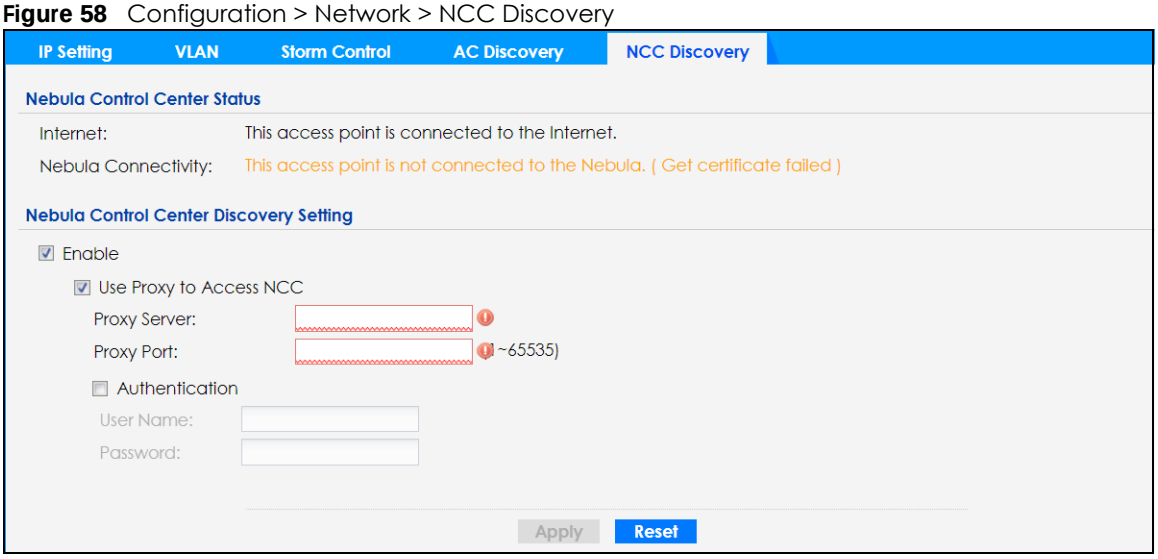
LABEL	DESCRIPTION
Discovery Setting	
Auto	Select this option to use DHCP option 138/DNS SRV record/Broadcast to get the AC's IP address. If the Zyxel Device and a Zyxel AC, such as the NXC2500 or NXC5500, are in the same subnet, it will be managed by the controller automatically.
Manual	Select this option 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.

9.6 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 58 Configuration > Network > NCC Discovery



Each field is described in the following table.

Table 41 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.

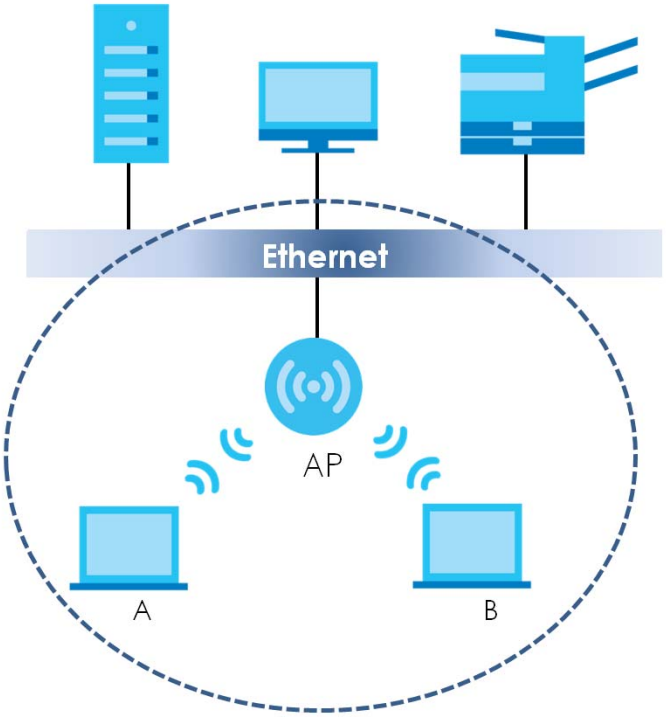
CHAPTER 10
Wireless

10.1 Overview

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

The following figure provides an example of a wireless network.

Figure 59 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** are called wireless clients. The wireless 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.

10.1.1 What You Can Do in this Chapter

- The **AP Management** screen (Section 10.2 on page 106) allows you to manage the Zyxel Device's general wireless settings.
- The **Rogue AP** screen (Section 10.3 on page 109) allows you to assign APs either to the rogue AP list or the friendly AP list.
- The **Load Balancing** screen (Section 10.4 on page 114) allows you to configure network traffic load balancing between the APs and the Zyxel Device.
- The **DCS** screen (Section 10.5 on page 116) allows you to configure dynamic radio channel selection.

10.1.2 What You Need to Know

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

Station / Wireless Client

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

Dynamic Channel Selection (DCS)

Dynamic Channel Selection (DCS) is a feature that allows an AP to automatically select the radio channel which it broadcasts. For more information, see Section 10.6 on page 117.

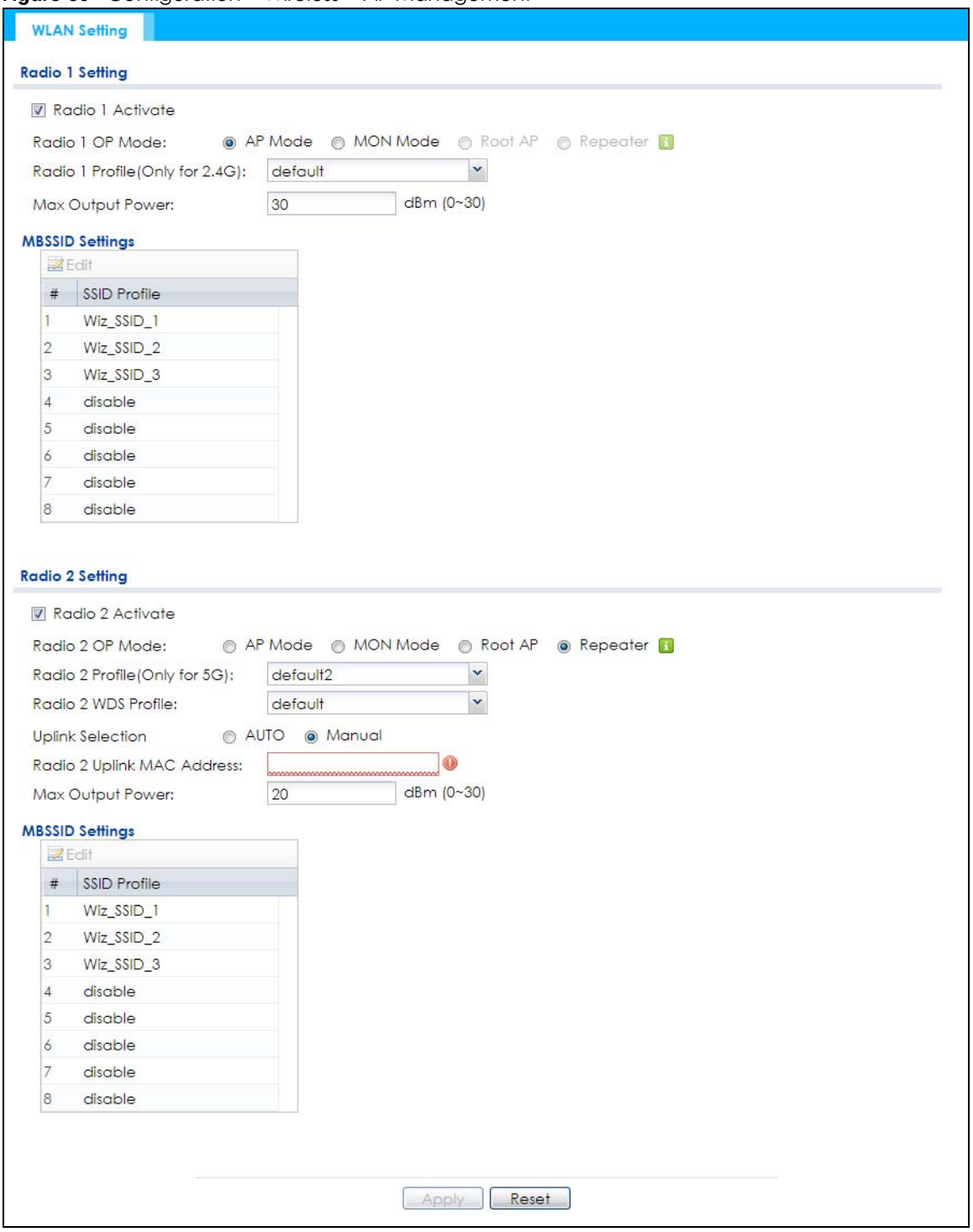
Load Balancing (Wireless)

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.

10.2 AP Management

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

Figure 60 Configuration > Wireless > AP Management



Each field is described in the following table.

Table 42 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.

Table 42 Configuration > Wireless > AP Management (continued)

LABEL	DESCRIPTION
Radio 1 OP Mode	Select the operating mode for radio 1. **AP Mode** means the radio can receive connections from wireless clients and pass their data traffic through to the Zyxel Device to be managed (or subsequently passed on to an upstream gateway for managing). **MON Mode** means the radio monitors the broadcast area for other APs, then passes their information on to the Zyxel Device where it can be determined if those APs are friendly or rogue. If a radio is set to this mode it cannot receive connections from wireless clients (see Section 1.2.3 on page 15). **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.
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.
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	
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.
#	This field shows the index number of the SSID
SSID Profile	This field displays the SSID profile that is associated with the radio profile.
Radio 2 Setting	
Radio 2 Activate	This displays if the Zyxel Device has a second radio. Select the check box to enable the Zyxel Device's second radio.

Table 42 Configuration > Wireless > AP Management (continued)

LABEL	DESCRIPTION
Radio 2 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 wireless clients and pass their data traffic through to the Zyxel Device to be managed (or subsequently passed on to an upstream gateway for managing). **MON Mode** means the radio monitors the broadcast area for other APs, then passes their information on to the Zyxel Device where it can be determined if those APs are friendly or rogue. If a radio is set to this mode it cannot receive connections from wireless clients (see Section 1.2.3 on page 15). **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 Profile	This displays if the Zyxel Device has a second radio. Select the radio profile the radio uses. Note: You can only apply a 5G AP radio profile to radio 2. Otherwise, the second radio will not be working.
Radio 2 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.
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 tbe MAC address specified in the **Radio 2 Uplink MAC Address** field.
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	
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.
#	This field shows the index number of the SSID
SSID Profile	This field shows the SSID profile that is associated with the radio 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.

10.3 Rogue AP

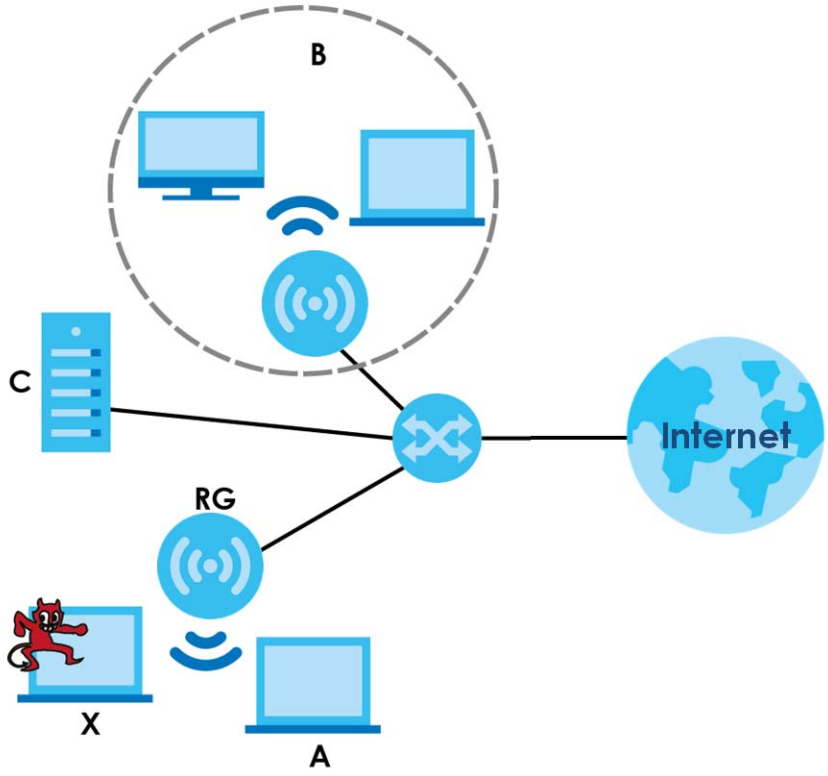
Use this screen to enable **Rogue AP Detection** and import/export a rogue or friendly AP list in a txt file. Click **Configuration > Wireless > Rogue AP** to access this screen.

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

Figure 61 Rogue AP Example



Friendly APs

If you have more than one AP in your wireless network, you should also configure a list of "friendly" APs. Friendly APs are 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 1.2.3 on page 15). 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 1.4 on page 19 to know which models support **Rogue AP Detection**.

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

Figure 62 Configuration > Wireless > Rogue AP (for Zyxel Devices that support Monitor mode)

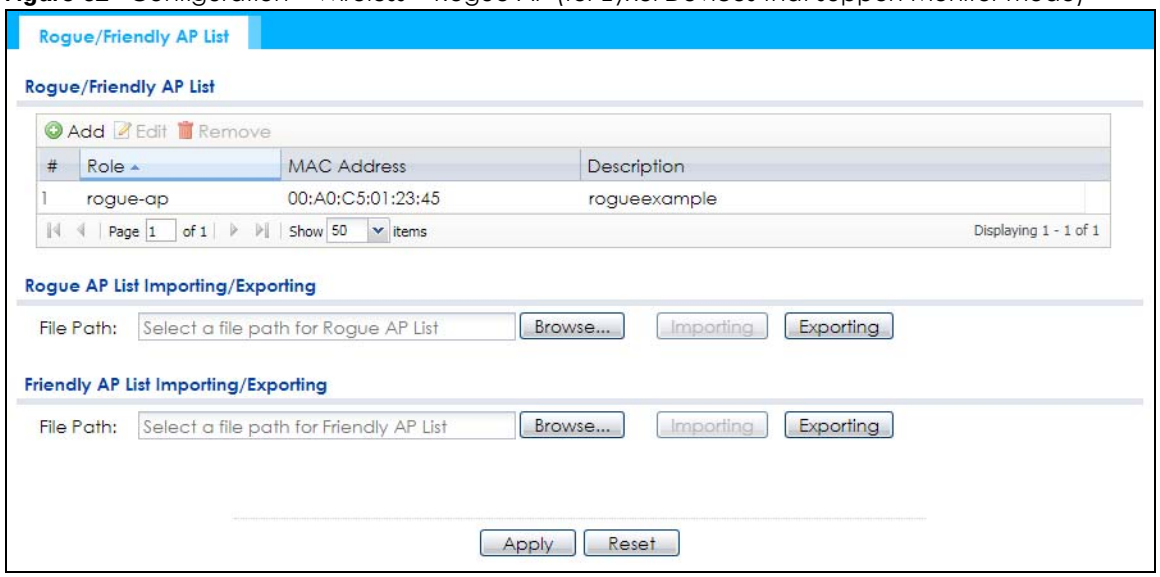
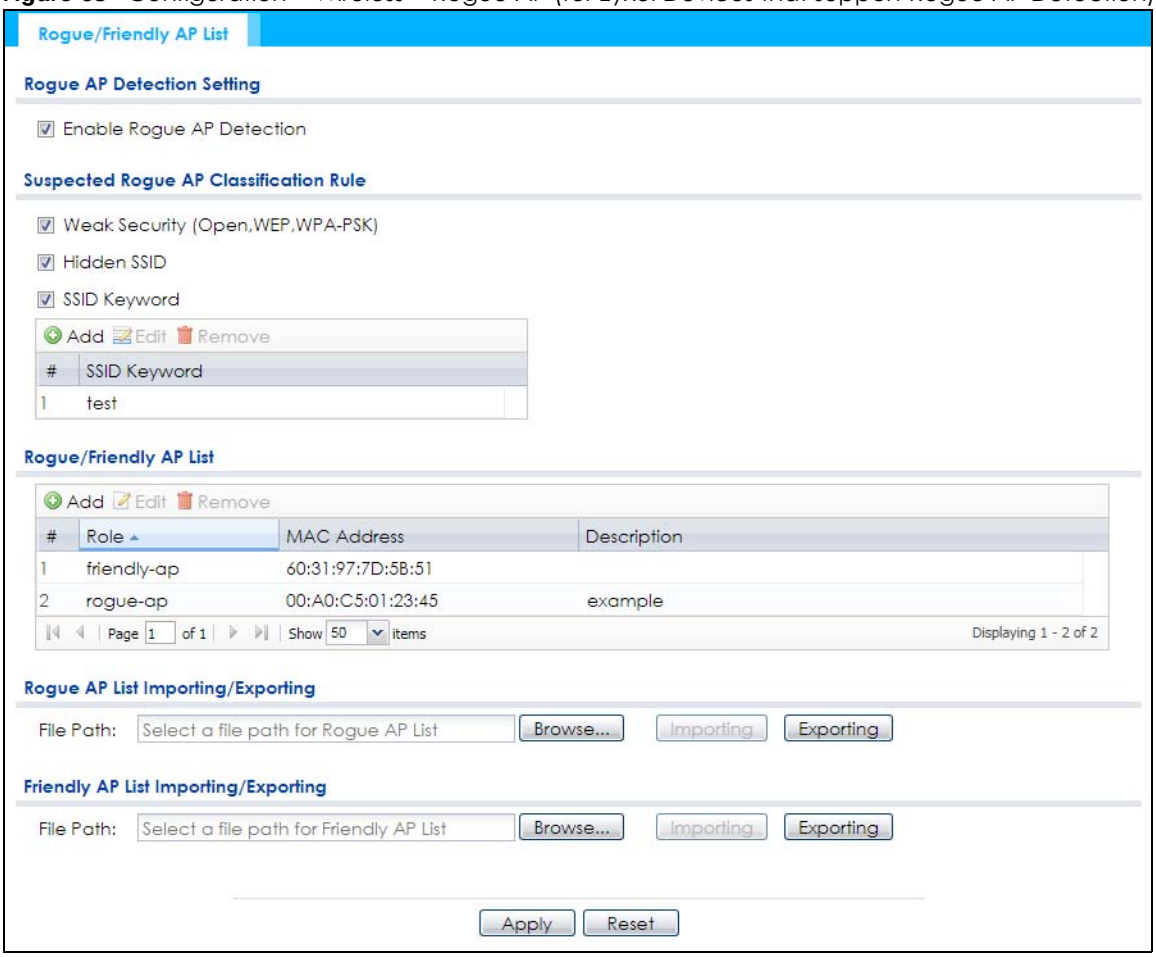


Figure 63 Configuration > Wireless > Rogue AP (for Zyxel Devices that support Rogue AP Detection)



Each field is described in the following table.

Table 43 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.
#	This field is a sequential value, and it is not associated with any interface.

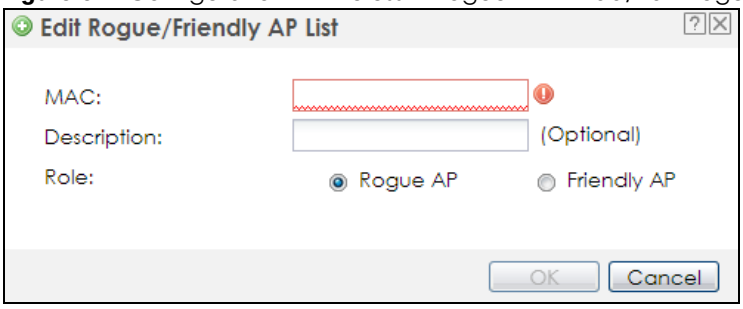
Table 43 Configuration > Wireless > Rogue AP (continued)

LABEL	DESCRIPTION
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.

10.3.1 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 64 Configuration > Wireless > Rogue AP > Add/Edit Rogue/Friendly AP List



Each field is described in the following table.

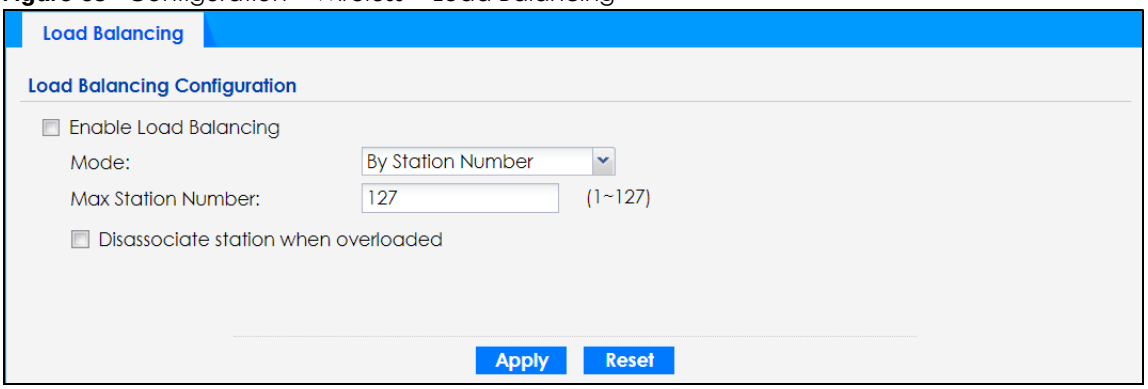
Table 44 Configuration > Wireless > Rogue AP > Add/Edit Rogue/Friendly AP List

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.

10.4 Load Balancing

Use this screen to configure wireless network traffic load balancing between the APs on your network (see Load Balancing on page 118). Click **Configuration > Wireless > Load Balancing** to access this screen.

Figure 65 Configuration > Wireless > Load Balancing



Each field is described in the following table.

Table 45 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** - 35M bps

Table 45 Configuration > Wireless > Load Balancing (continued)

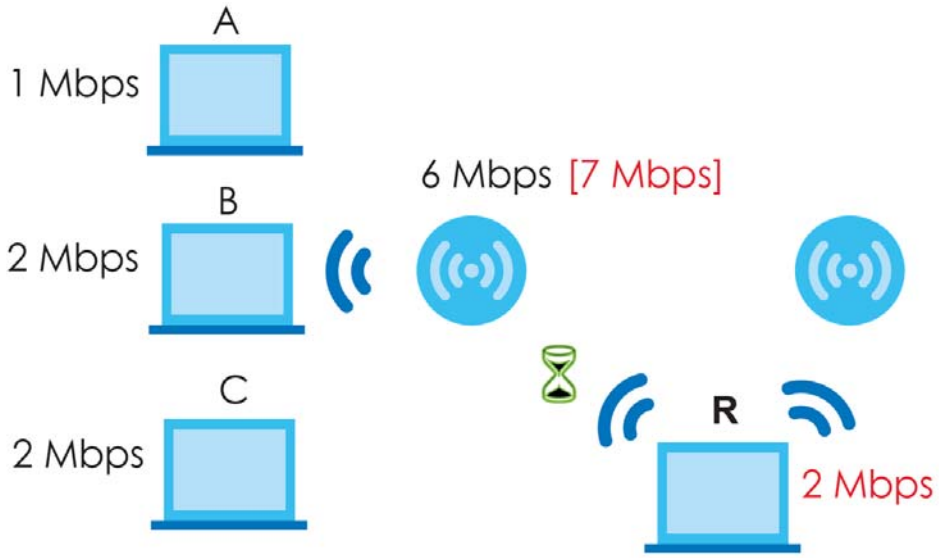
LABEL	DESCRIPTION
Disassociate station when overloaded	This function is enabled by default and the disassociation priority is always **Signal Strength** when you set **Mode** to **By Smart Classroom**. Select this option to disassociate wireless clients connected to the AP when it becomes overloaded. If you do not enable this option, then the AP simply delays the connection until it can afford the bandwidth it requires, or it transfers the connection to another AP within its broadcast radius. The disassociation priority is determined automatically by the Zyxel Device and is as follows: • **Idle Timeout** - Devices that have been idle the longest will be 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 wireless clients; otherwise, a wireless 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.

10.4.1 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.

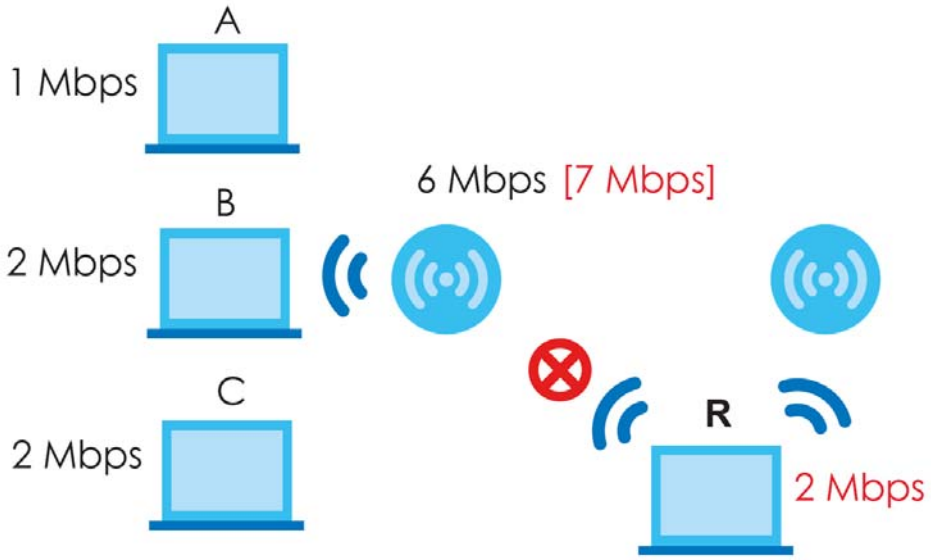
For example, here the AP has a balanced bandwidth allotment of 6 Mbps. If laptop **R** connects and it pushes the AP over its allotment, say to 7 Mbps, then the AP delays the red laptop's connection until it can afford the bandwidth or the laptop is picked up by a different AP with bandwidth to spare.

Figure 66 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 67 Disassociating with a client

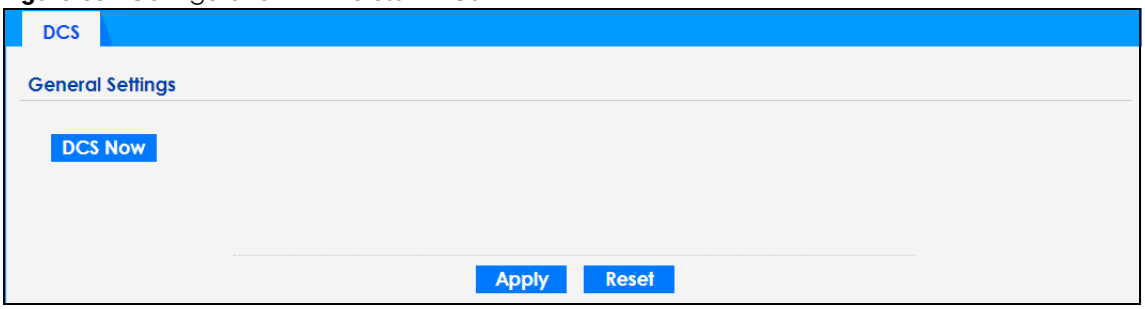


Connections are cut based on either **idle timeout** or **signal strength**. The Zyxel Device first looks to see which devices have been idle the longest, then starts kicking them in order of highest idle time. If no connections are idle, the next criteria the Zyxel Device analyzes is signal strength.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

10.5 DCS

Use this screen to configure dynamic radio channel selection (see Dynamic Channel Selection (DCS) on page 106). Click **Configuration > Wireless > DCS** to access this screen.

Figure 68 Configuration > Wireless > DCS



Each field is described in the following table.

Table 46 Configuration > Wireless > DCS

LABEL	DESCRIPTION
DCS Now	Click this to have the Zyxel Device scan for and select an available channel immediately.

Table 46 Configuration > Wireless > DCS (continued)

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

10.6 Technical Reference

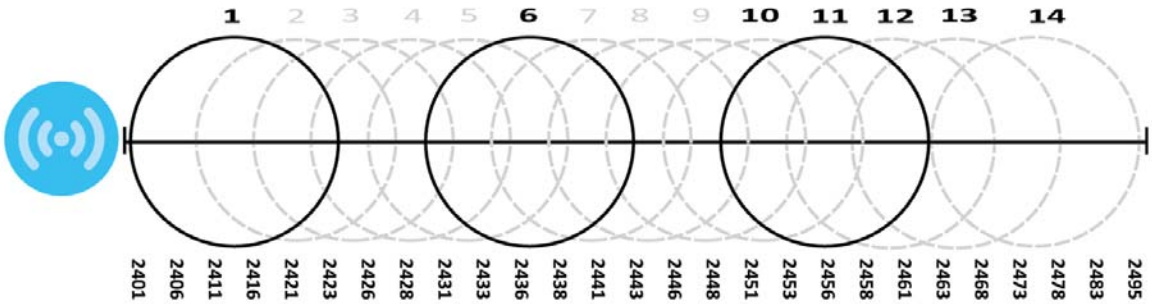
The following section contains additional technical information about the features described in this chapter.

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.

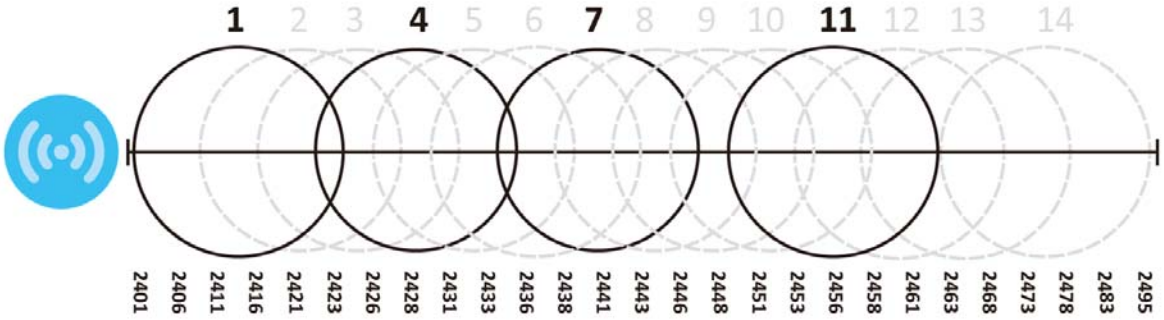
In the 2.4 GHz spectrum, each channel from 1 to 13 is broken up into discrete 22 MHz segments that are spaced 5 MHz apart. Channel 1 is centered on 2.412 GHz while channel 13 is centered on 2.472 GHz.

Figure 69 An Example Three-Channel Deployment



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

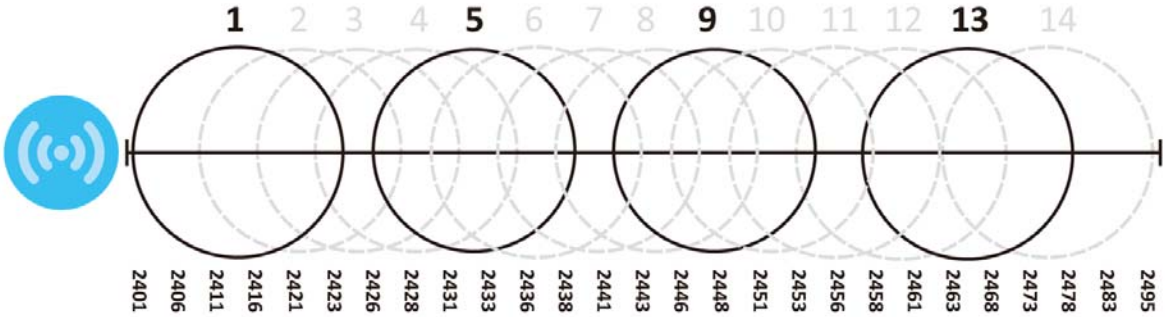
Figure 70 An Example Four-Channel Deployment



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 71 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 11
Bluetooth

11.1 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.

On the WAC5302D-S, you need to attach a supported BLE USB dongle to its USB port to have the AP act as a beacon to broadcast packets. Contact Zyxel customer support if you are not sure whether your BLE USB dongle is compatible with the Zyxel Device.

11.1.1 What You Need To Know

iBeacon 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

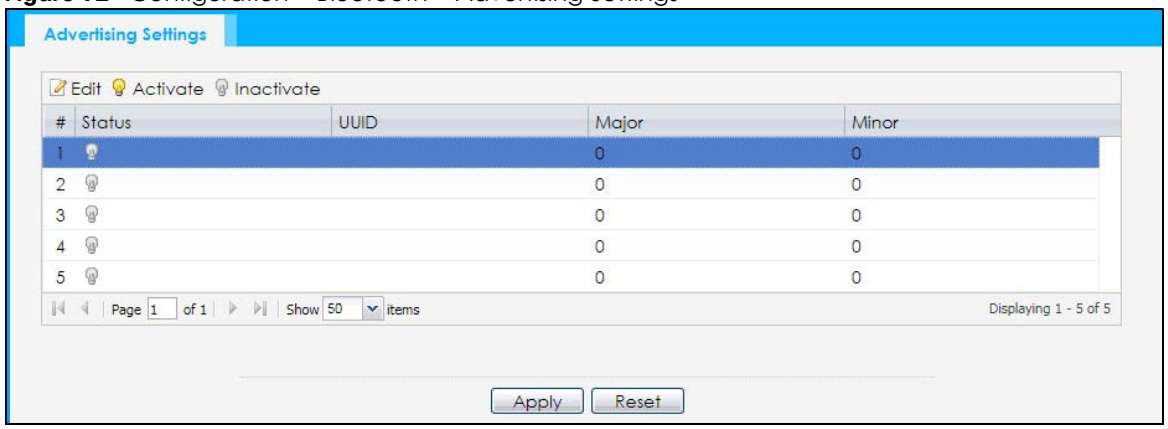
Developers can create apps that respond to the iBeacon ID that your Zyxel Device broadcasts. An app that is associated with the Zyxel Device's iBeacon ID can measure the proximity of a customer to a beacon. This app can then push messages or trigger prompts and actions based on this information. This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

11.2 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 72 Configuration > Bluetooth > Advertising Settings



The following table describes the labels in this screen.

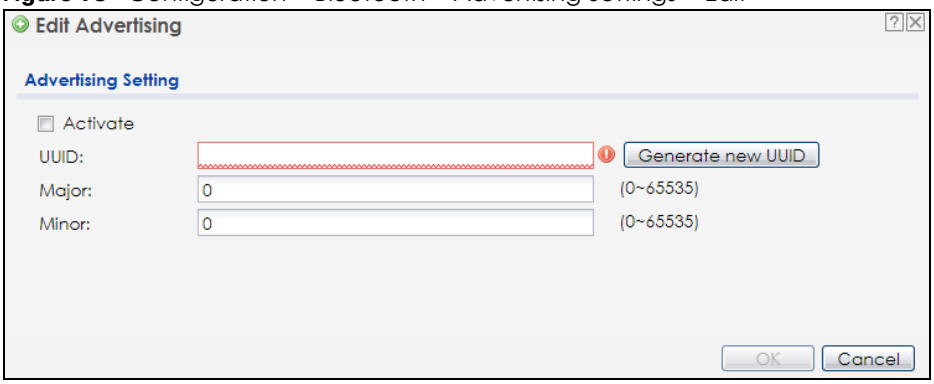
Table 47 Configuration > Bluetooth > Advertising Settings

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.

11.2.1 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 73 Configuration > Bluetooth > Advertising Settings > Edit



The following table describes the labels in this screen.

Table 48 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 12
User

12.1 Overview

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

12.1.1 What You Can Do in this Chapter

- The **User** screen (see Section 12.2 on page 124) provides a summary of all user accounts.
- The **Setting** screen (see Section 12.3 on page 126) controls default settings, login settings, lockout settings, and other user settings for the Zyxel Device.

12.1.2 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 49 Types of User Accounts

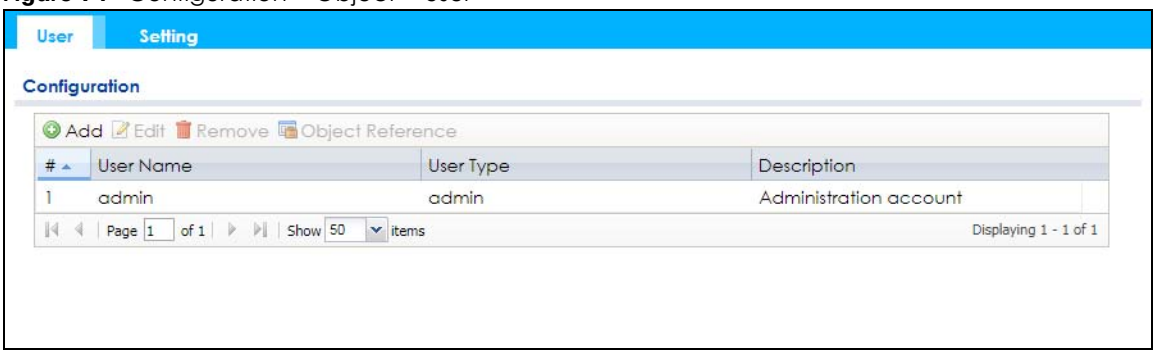
TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
admin	Change Zyxel Device configuration (web, CLI)	WWW, TELNET, SSH, FTP
limited-admin	Look at Zyxel Device configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, TELNET, SSH
Access Users		
user	Used for the embedded RADIUS server and SNMPv3 user access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

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

12.2 User Summary

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

Figure 74 Configuration > Object > User



The following table describes the labels in this screen.

Table 50 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.

12.2.1 Add/Edit User

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

12.2.1.1 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]

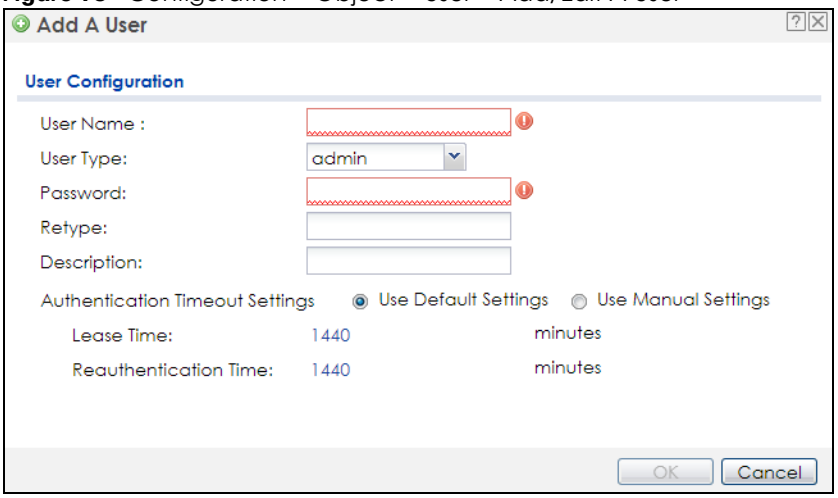
The first character must be alphabetical (A-Z a-z), an underscore (_), or a dash (-). Other limitations on user names are:

- 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 75 Configuration > Object > User > Add/Edit A User



The following table describes the labels in this screen.

Table 51 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 51 Configuration > User > User > Add/Edit A User (continued)

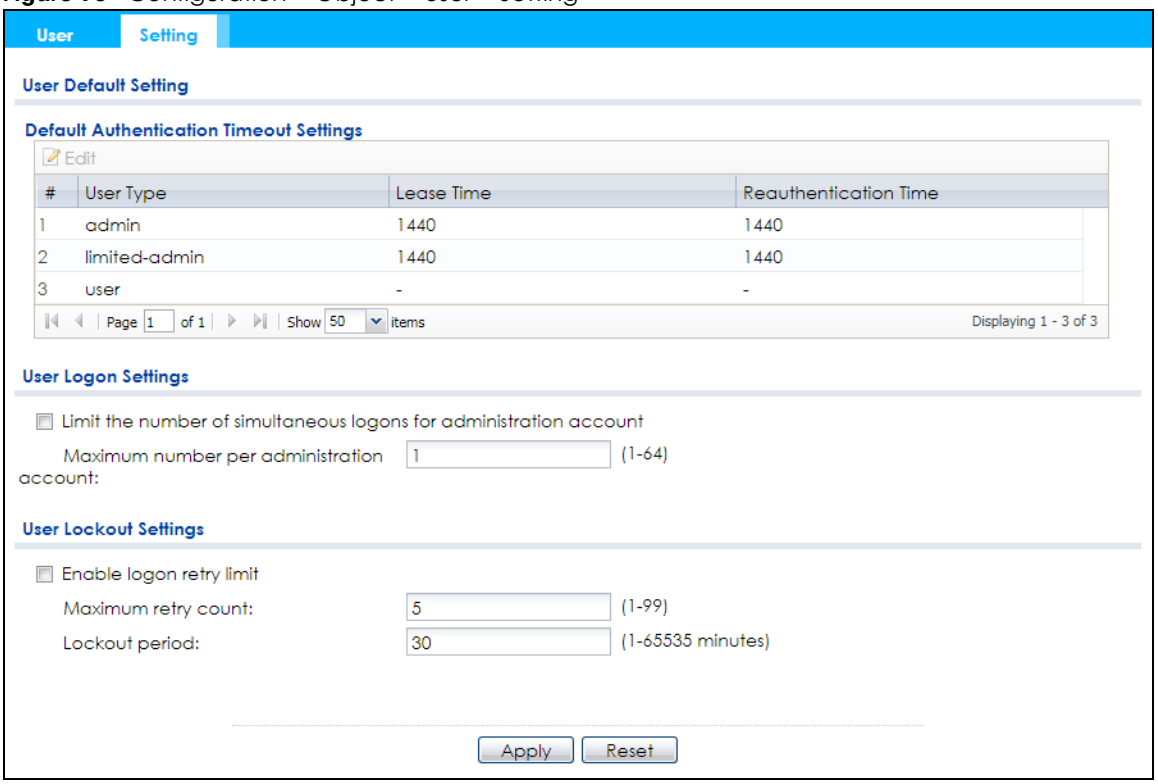
LABEL	DESCRIPTION
Authentication Timeout Settings	This field is not available if the user type is **user**. If you want to set authentication timeout to a value other than the default settings, select **Use Manual Settings** then fill your preferred values in the fields that follow.
Lease Time	This field 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.

12.3 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 76 Configuration > Object > User > Setting



The following table describes the labels in this screen.

Table 52 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.
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.
User Logon Settings	

Table 52 Configuration > Object > User > Setting (continued)

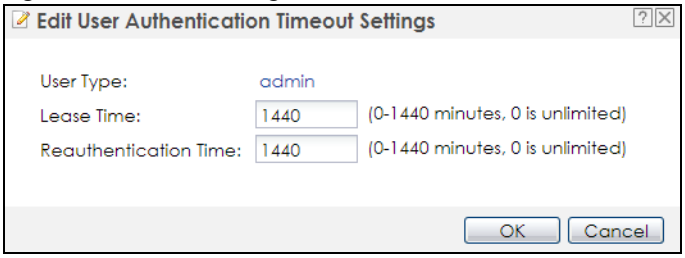
LABEL	DESCRIPTION
Limit the number of simultaneous logons for administration account	Select this check box if you want to set a limit on the number of simultaneous logins by admin users. If you do not select this, admin users can login as many times as they want at the same time using the same or different 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.

12.3.1 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 77 User > Setting > Edit User Authentication Timeout Settings



The following table describes the labels in this screen.

Table 53 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 13
AP Profile

13.1 Overview

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

13.1.1 What You Can Do in this Chapter

- The **Radio** screen (Section 13.2 on page 131) creates radio configurations that can be used by the APs.
- The **SSID** screen (Section 13.3 on page 137) configures three different types of profiles for your networked APs.

13.1.2 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 wireless network signal broadcast by an AP. Each radio on a single AP can broadcast up to 8 SSIDs. You can have a maximum of 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 wireless 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 wireless client MAC addresses. If a client's MAC address is on the list, then it is either allowed or denied, depending on how you set up the MAC Filter profile. You can have a maximum of 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 wireless 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 wireless network that clients use to connect to it.

WEP

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

WPA2

WPA2 (IEEE 802.11i) is a wireless 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.

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).

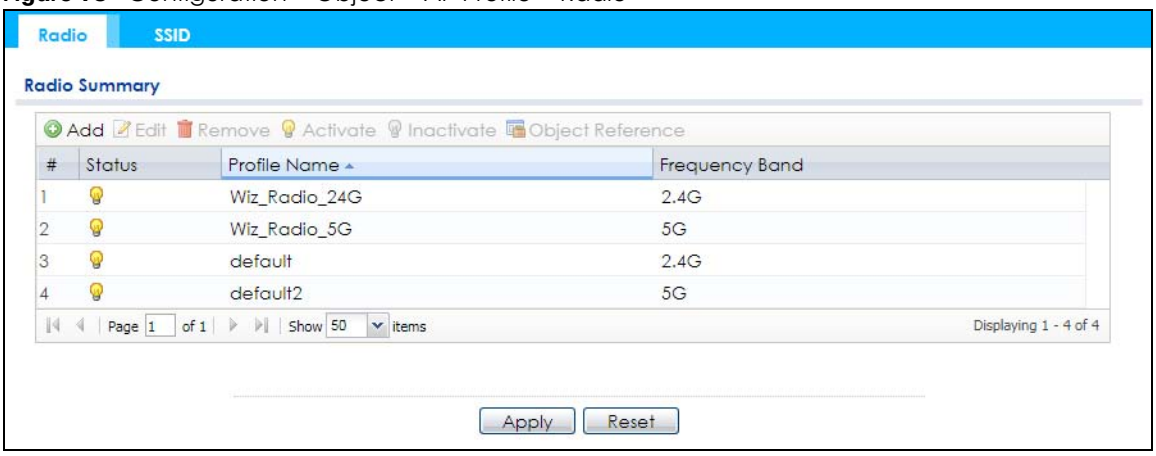
The IEEE 802.11v BSS Transition Management feature lets an AP automatically provide load information of the neighbor APs to clients. It helps the Zyxel Device steer clients to a suitable AP for better performance or load balancing.

13.2 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 78 Configuration > Object > AP Profile > Radio



The following table describes the labels in this screen.

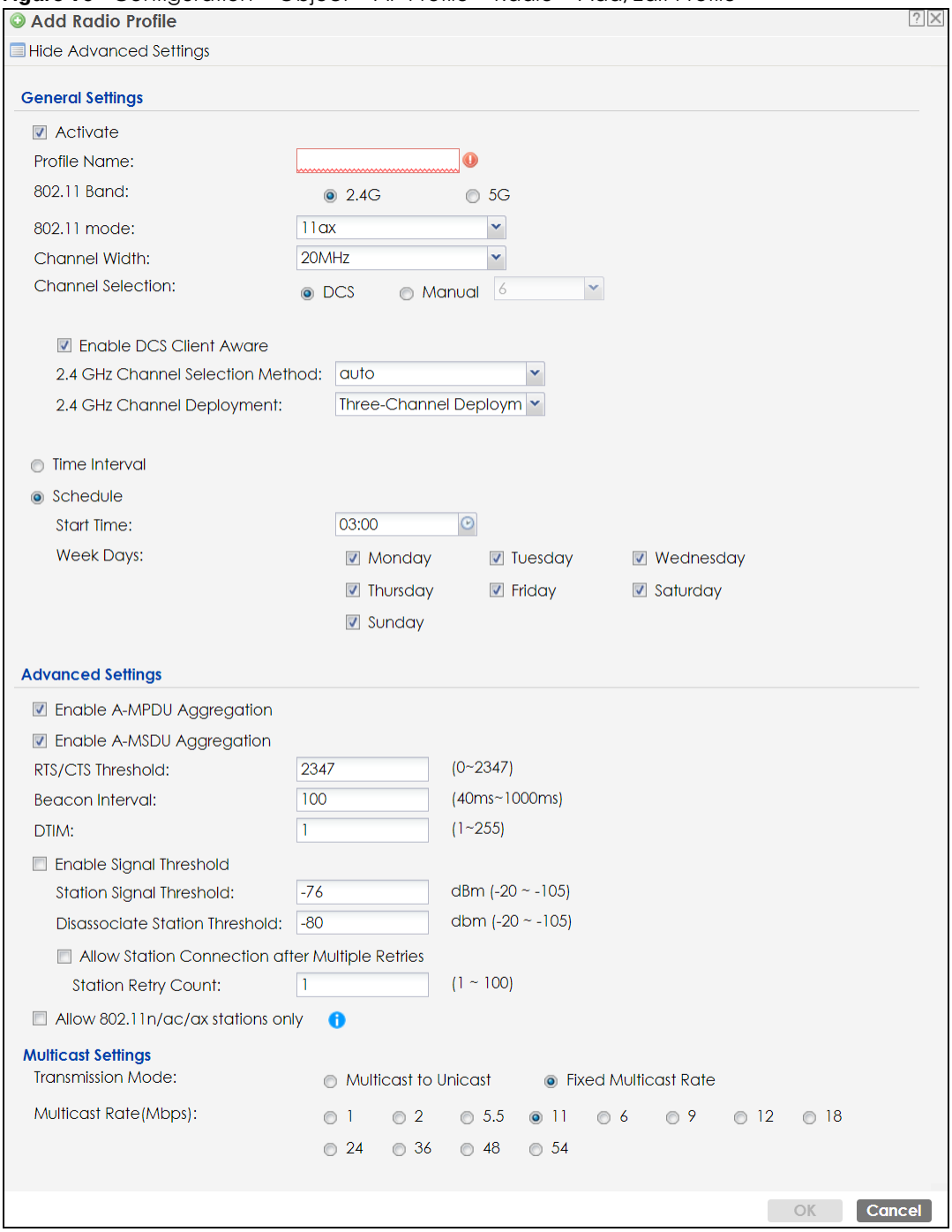
Table 54 Configuration > Object > AP Profile > Radio

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.

13.2.1 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 79 Configuration > Object > AP Profile > Radio > Add/Edit Profile



The following table describes the labels in this screen.

Table 55 Configuration > Object > AP Profile > Radio > Add/Edit Profile

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.

Table 55 Configuration > Object > AP Profile > Radio > Add/Edit Profile (continued)

LABEL	DESCRIPTION
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 would use the 2.4 GHz or 5 GHz band.
802.11 Mode	Select how to let wireless 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 wireless 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. 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.
Channel Width	Select the channel bandwidth you want to use for your wireless network. Select **20 MHz** if you want to lessen radio interference with other wireless devices in your neighborhood. Select **20/40 MHz** to allow the Zyxel Device to choose the channel bandwidth (20 or 40 MHz) that has least interference. Select **20/40/80 MHz** to allow the Zyxel Device to choose the channel bandwidth (20 or 40 or 80 MHz) that has least interference. This option is available only when you select **11ac** or **11ax** in the **802.11 Mode** field. Note: If the environment has poor signal-to-noise ratio (SNR), the Zyxel Device will switch to a lower bandwidth.
Channel Selection	This is the radio channel which the signal will use for broadcasting by this radio profile. • **DCS**: Choose Dynamic Channel Selection to have the Zyxel Device choose a radio channel that has least interference. • **Manual**: Choose from the available radio channels in the list. If your Zyxel Device is outdoor type, be sure to choose non-indoors channels.
Enable DCS Client Aware	Select this to have the Zyxel Device switch channels only when there are no clients connected to it. If there is a client connected, the Zyxel Device will not switch channels but generate a log. The Zyxel Device tries to scan and switch channels again at the end of the specified time interval or at the scheduled time. If you disable this then the Zyxel Device switches channels immediately regardless of any client connections. In this instance, clients that are connected to the Zyxel Device when it switches channels are dropped.
Blacklist DFS channels in presence of radar	This field is available if **802.11 Band** is set to **5G** and **Channel Selection** is set to **DCS**. Enable this to temporarily blacklist the wireless channels in the Dynamic Frequency Selection (DFS) range whenever a radar signal is detected by the Zyxel Device.

Table 55 Configuration > Object > AP Profile > Radio > Add/Edit Profile (continued)

LABEL	DESCRIPTION
Enable DCS Client Aware	This field is available when you set **Channel Selection** to **DCS**. Select this to have the Zyxel Device switch channels only when there are no clients connected to it. If there is a client connected, the Zyxel Device will not switch channels but generate a log. The Zyxel Device tries to scan and switch channels again at the end of the specified time interval or at the scheduled time. If you disable this then the Zyxel Device switches channels immediately regardless of any client connections. In this instance, clients that are connected to the Zyxel Device when it switches channels are dropped.
2.4 GHz Channel Selection Method	This field is available when you set **Channel Selection** to **DCS**. Select how you want to specify the channels the Zyxel Device switches between for 2.4 GHz operation. Select **auto** to have the Zyxel Device display a **2.4 GHz Channel Deployment** field you can use to limit channel switching to 3 or 4 channels. Select **manual** to select the individual channels the Zyxel Device switches between. Note: The method is automatically set to **auto** when no channel is selected or any one of the previously selected channels is not supported.
Channel ID	This field is available only when you set **Channel Selection** to **DCS** and set **2.4 GHz Channel Selection Method** to **manual**. Select the channels that you want the Zyxel Device to use.
2.4 GHz Channel Deployment	This is available when you set **Channel Selection** to **DCS** and the **2.4 GHz Channel Selection Method** is set to **auto**. Select **Three-Channel Deployment** to limit channel switching to channels 1,6, and 11, the three channels that are sufficiently attenuated to have almost no impact on one another. In other words, this allows you to minimize channel interference by limiting channel-hopping to these three "safe" channels. Select **Four-Channel Deployment** to limit channel switching to four channels. Depending on the country domain, if the only allowable channels are 1-11 then the Zyxel Device uses channels 1, 4, 7, 11 in this configuration; otherwise, the Zyxel Device uses channels 1, 5, 9, 13 in this configuration. Four channel deployment expands your pool of possible channels while keeping the channel interference to a minimum.
Enable 5 GHz DFS Aware	This field is available only when you select **5G** in the **802.11 Band** field, set **Channel Selection** to **DCS** and set **5 GHz Channel Selection Method** to **auto**. Select this if your APs are operating in an area known to have RADAR devices. This allows the Zyxel Device to downgrade its frequency to below 5 GHz in the event RADAR signal is detected, thus preventing it from interfering with that signal. Enabling this forces the AP to select a non-DFS channel.
5 GHz Channel Selection Method	Select how you want to specify the channels the Zyxel Device switches between for 5 GHz operation. Select **Auto** to have the Zyxel Device automatically select the best channel. Select **manual** to select the individual channels the Zyxel Device switches between. Note: The method is automatically set to **auto** when no channel is selected or any one of the previously selected channels is not supported.
Channel ID	This field is available only when you set **Channel Selection** to **DCS** and set **5 GHz Channel Selection Method** to **manual**. Select the channels that you want the Zyxel Device to use.

Table 55 Configuration > Object > AP Profile > Radio > Add/Edit Profile (continued)

LABEL	DESCRIPTION
Time Interval	Select this option to have the Zyxel Device survey the other APs within its broadcast radius at the end of the specified time interval.
DCS Time Interval	This field is available when you set **Channel Selection** to **DCS** and select the **Time Interval** option. Enter a number of minutes. This regulates how often the Zyxel Device surveys the other APs within its broadcast radius. If the channel on which it is currently broadcasting suddenly comes into use by another AP, the Zyxel Device will then dynamically select the next available clean channel or a channel with lower interference.
Schedule	Select this option to have the Zyxel Device survey the other APs within its broadcast radius at a specific time on selected days of the week.
Start Time	Specify the time of the day (in 24-hour format) to have the Zyxel Device use DCS to automatically scan and find a less-used channel.
Week Days	Select each day of the week to have the Zyxel Device use DCS to automatically scan and find a less-used channel.
Advanced Settings	
Guard Interval	This field is available only when the channel width is **20/40MHz** or **20/40/80MHz** and the **802.11 Mode** is either **11n** or **11ac**. Set the guard interval for this radio profile to either **short** or **long**. The guard interval is the gap introduced between data transmission from users in order to reduce interference. Reducing the interval increases data transfer rates but also increases interference. Increasing the interval reduces data transfer rates but also reduces interference.
Enable A-MPDU Aggregation	This field is not available when you set **802.11 Mode** to **11a** or **11b/g**. Select this to enable A-MPDU aggregation. Message Protocol Data Unit (MPDU) aggregation collects Ethernet frames along with their 802.11n headers and wraps them in a 802.11n MAC header. This method is useful for increasing bandwidth throughput in environments that are prone to high error rates.
Enable A-MSDU Aggregation	This field is not available when you set **802.11 Mode** to **11a** or **11b/g**. Select this to enable A-MSDU aggregation. Mac Service Data Unit (MSDU) aggregation collects Ethernet frames without any of their 802.11n headers and wraps the header-less payload in a single 802.11n MAC header. This method is useful for increasing bandwidth throughput. It is also more efficient than A-MPDU except in environments that are prone to high error rates.
RTS/CTS Threshold	Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions). A wireless client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS/CTS equal to or higher than the fragmentation threshold to turn RTS/CTS off.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the Zyxel Device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. A high value helps save current consumption of the access point.
DTIM	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255.

Table 55 Configuration > Object > AP Profile > Radio > Add/Edit Profile (continued)

LABEL	DESCRIPTION
Enable Signal Threshold	Select the check box to use the signal threshold to ensure wireless clients receive good throughput. This allows only wireless clients with a strong signal to connect to the AP. Clear the check box to not require wireless clients to have a minimum signal strength to connect to the AP.
Station Signal Threshold	Set a minimum client signal strength. A wireless client is allowed to connect to the AP only when its signal strength is stronger than the specified threshold. -20 dBm is the strongest signal you can require and -105 is the weakest.
Disassociate Station Threshold	Set a minimum kick-off signal strength. When a wireless client's signal strength is lower than the specified threshold, the Zyxel Device disconnects the wireless client from the AP. -20 dBm is the strongest signal you can require and -105 is the weakest.
Allow Station Connection after Multiple Retries	Select this option to allow a wireless client to try to associate with the AP again after it is disconnected due to weak signal strength.
Station Retry Count	Set the maximum number of times a wireless client can attempt to re-connect to the AP
Allow 802.11n/ ac/ax stations only	Select this option to allow only 802.11 n/ac/ax clients to connect, and reject 802.11a/b/g clients.
Multicast Settings	
Transmission Mode	Specify how the Zyxel Device handles wireless multicast traffic. Select **Multicast to Unicast** to broadcast wireless multicast traffic to all of the wireless clients as unicast traffic. Unicast traffic dynamically changes the data rate based on the application's bandwidth requirements. The retransmit mechanism of unicast traffic provides more reliable transmission of the multicast traffic, although it also produces duplicate packets. Select **Fixed Multicast Rate** to send multicast traffic to all wireless clients at a single data rate. You must know the multicast application's bandwidth requirements and set it in the following field.
Multicast Rate(Mbps)	If you set **Transmission Mode** to **Fixed Multicast Rate**, select a data rate at which the Zyxel Device transmits multicast packets to wireless clients. For example, to deploy 4 Mbps video, select a fixed multicast rate higher than 4 Mbps.
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 SSID

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

13.3.1 SSID List

This screen allows you to create and manage SSID configurations that can be used by the APs. An SSID, or Service Set IDentifier, is basically the name of the wireless network to which a wireless client can connect. The SSID appears as readable text to any device capable of scanning for wireless frequencies

(such as the WiFi adapter in a laptop), and is displayed as the wireless network name when a person makes a connection to it.

To access this screen click **Configuration > Object > AP Profile > SSID > SSID List**.

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

Figure 80 Configuration > Object > AP Profile > SSID > SSID List (Default)

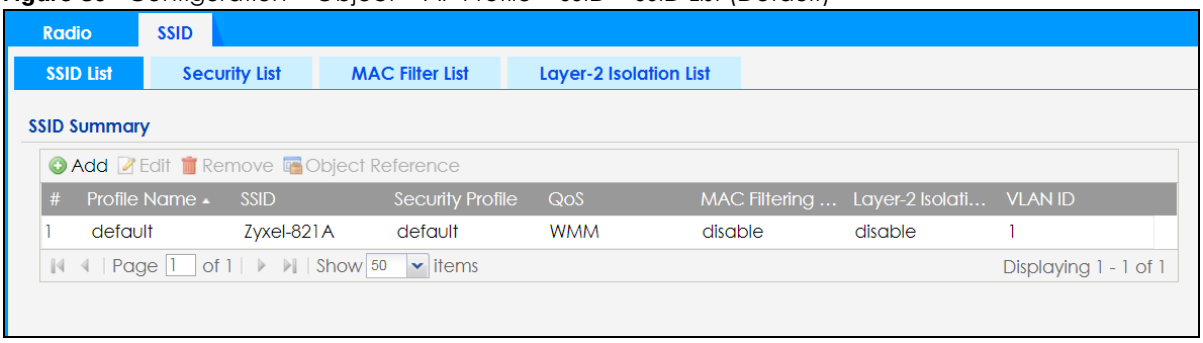
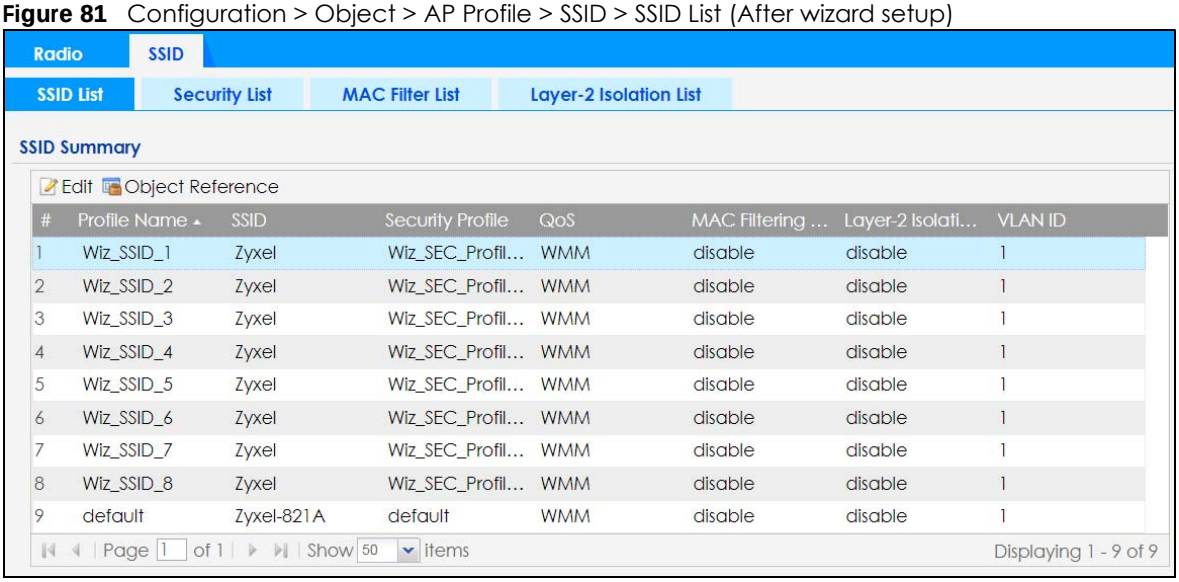


Figure 81 Configuration > Object > AP Profile > SSID > SSID List (After wizard setup)



The following table describes the labels in this screen.

Table 56 Configuration > Object > AP Profile > SSID > SSID List

LABEL	DESCRIPTION
Add	Click this to add a new SSID profile. This button is not available after you configure the Zyxel Deviceusing the wizard.
Edit	Click this to edit the selected SSID profile.
Remove	Click this to remove the selected SSID profile. This button is not available after you configure the Zyxel Deviceusing the wizard.
Object Reference	Click this to view which other objects are linked to the selected SSID profile (for example, radio profile).
#	This field is a sequential value, and it is not associated with a specific user.
Profile Name	This field indicates the name assigned to the SSID profile.
SSID	This field indicates the SSID name as it appears to wireless clients.

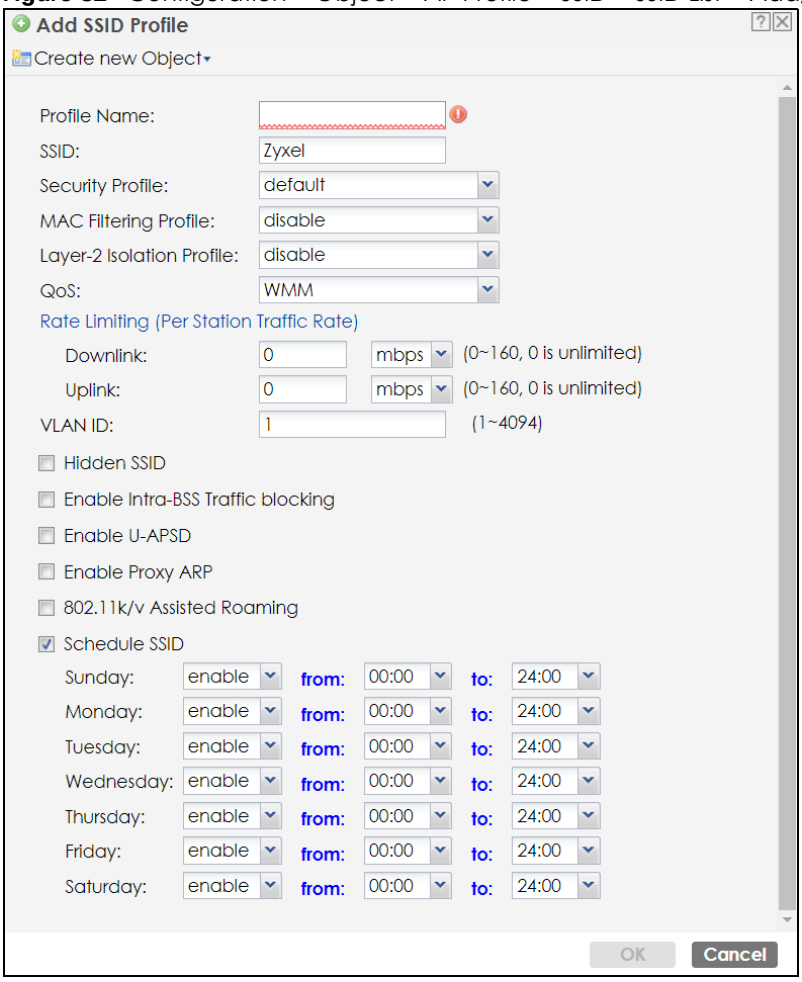
Table 56 Configuration > Object > AP Profile > SSID > SSID List (continued)

LABEL	DESCRIPTION
Security Profile	This field indicates which (if any) security profile is associated with the SSID profile.
QoS	This field indicates the QoS type associated with the SSID profile.
MAC Filtering Profile	This field indicates which (if any) MAC filter Profile is associated with the SSID profile.
Layer-2 Isolation Profile	This field indicates which (if any) layer-2 isolation Profile is associated with the SSID profile.
VLAN ID	This field indicates the VLAN ID associated with the SSID profile.

13.3.2 Add/Edit SSID Profile

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

Figure 82 Configuration > Object > AP Profile > SSID > SSID List > Add/Edit SSID Profile



The following table describes the labels in this screen.

Table 57 Configuration > Object > AP Profile > SSID > SSID List > Add/Edit SSID Profile

LABEL	DESCRIPTION
Create new Object	Select an object type from the list to create a new one associated with this SSID profile.
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
SSID	Enter the SSID name for this profile. This is the name visible on the network to wireless clients. Enter up to 32 characters, spaces and underscores are allowed.
Security Profile	Select a security profile from this list to associate with this SSID. If none exist, you can use the **Create new Object** menu to create one. Note: It is highly recommended that you create security profiles for all of your SSIDs to enhance your network security.
MAC Filtering Profile	Select a MAC filtering profile from the list to associate with this SSID. If none exist, you can use the **Create new Object** menu to create one. MAC filtering allows you to limit the wireless clients connecting to your network through a particular SSID by wireless client MAC addresses. Any clients that have MAC addresses not in the MAC filtering profile of allowed addresses are denied connections. The **disable** setting means no MAC filtering is used.
Layer-2 Isolation Profile	Select a layer-2 isolation profile from the list to associate with this SSID. If none exist, you can use the **Create new Object** menu to create one. Layer-2 isolation allows you to prevent wireless clients associated with your Zyxel Device from communicating with other wireless clients, APs, computers or routers in a network. The **disable** setting means no layer-2 isolation is used.
QoS	Select a Quality of Service (QoS) access category to associate with this SSID. Access categories minimize the delay of data packets across a wireless network. Certain categories, such as video or voice, are given a higher priority due to the time sensitive nature of their data packets. QoS access categories are as follows: **disable**: Turns off QoS for this SSID. All data packets are treated equally and not tagged with access categories. **WMM**: Enables automatic tagging of data packets. The Zyxel Device assigns access categories to the SSID by examining data as it passes through it and making a best guess effort. If something looks like video traffic, for instance, it is tagged as such. **WMM_VOICE**: All wireless traffic to the SSID is tagged as voice data. This is recommended if an SSID is used for activities like placing and receiving VoIP phone calls. **WMM_VIDEO**: All wireless traffic to the SSID is tagged as video data. This is recommended for activities like video conferencing. **WMM_BEST_EFFORT**: All wireless traffic to the SSID is tagged as "best effort," meaning the data travels the best route it can without displacing higher priority traffic. This is good for activities that do not require the best bandwidth throughput, such as surfing the Internet. **WMM_BACKGROUND**: All wireless traffic to the SSID is tagged as low priority or "background traffic", meaning all other access categories take precedence over this one. If traffic from an SSID does not have strict throughput requirements, then this access category is recommended. For example, an SSID that only has network printers connected to it.
Rate Limiting	
Downlink	Define the maximum incoming transmission data rate (either in mbps or kbps) on a per-station basis.

Table 57 Configuration > Object > AP Profile > SSID > SSID List > Add/Edit SSID Profile (continued)

LABEL	DESCRIPTION
Uplink	Define the maximum outgoing transmission data rate (either in mbps or kbps) on a per-station basis.
VLAN ID	Enter a VLAN ID for the Zyxel Device to use to tag traffic originating from this SSID.
Hidden SSID	Select this if you want to "hide" your SSID from wireless clients. This tells any wireless clients in the vicinity of the AP using this SSID profile not to display its SSID name as a potential connection. Not all wireless clients respect this flag and display it anyway. When a SSID is "hidden" and a wireless client cannot see it, the only way you can connect to the SSID is by manually entering the SSID name in your wireless connection setup screen(s) (these vary by client, client connectivity software, and operating system).
Enable Intra-BSS Traffic Blocking	Select this option to prevent crossover traffic from within the same SSID on the Zyxel Device.
Enable U-APSD	Select this option to enable Unscheduled Automatic Power Save Delivery (U-APSD), which is also known as WMM-Power Save. This helps increase battery life for battery-powered wireless clients connected to the Zyxel Device using this SSID profile.
Enable Proxy ARP	The Address Resolution Protocol (ARP) is a protocol for mapping an IP address to a MAC address. An ARP broadcast is sent to all devices in the same Ethernet network to request the MAC address of a target IP address. Select this option to allow the Zyxel Device to answer ARP requests for an IP address on behalf of a client associated with this SSID. This can reduce broadcast traffic and improve network performance.
802.11k/v Assisted Roaming	Select this option to enable IEEE 802.11k/v assisted roaming on the Zyxel Device. When the connected clients request 802.11k neighbor lists, the Zyxel Device will response with a list of neighbor APs that can be candidates for roaming.
Schedule SSID	Select this option and set whether the SSID is enabled or disabled on each day of the week. You also need to select the hour and minute (in 24-hour format) to specify the time period of each day during which the SSID is enabled/enabled.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

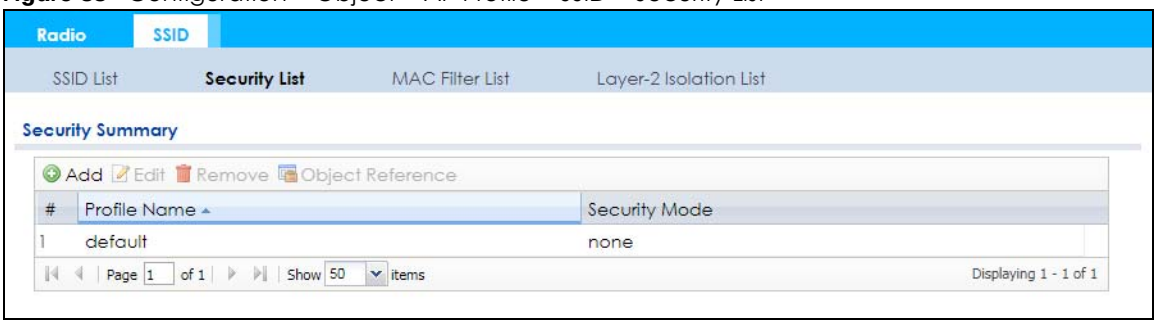
13.4 Security List

This screen allows you to manage wireless security configurations that can be used by your SSIDs. Wireless security is implemented strictly between the AP broadcasting the SSID and the stations that are connected to it.

To access this screen click **Configuration > Object > AP Profile > SSID > Security List**.

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

Figure 83 Configuration > Object > AP Profile > SSID > Security List



The following table describes the labels in this screen.

Table 58 Configuration > Object > AP Profile > SSID > Security List

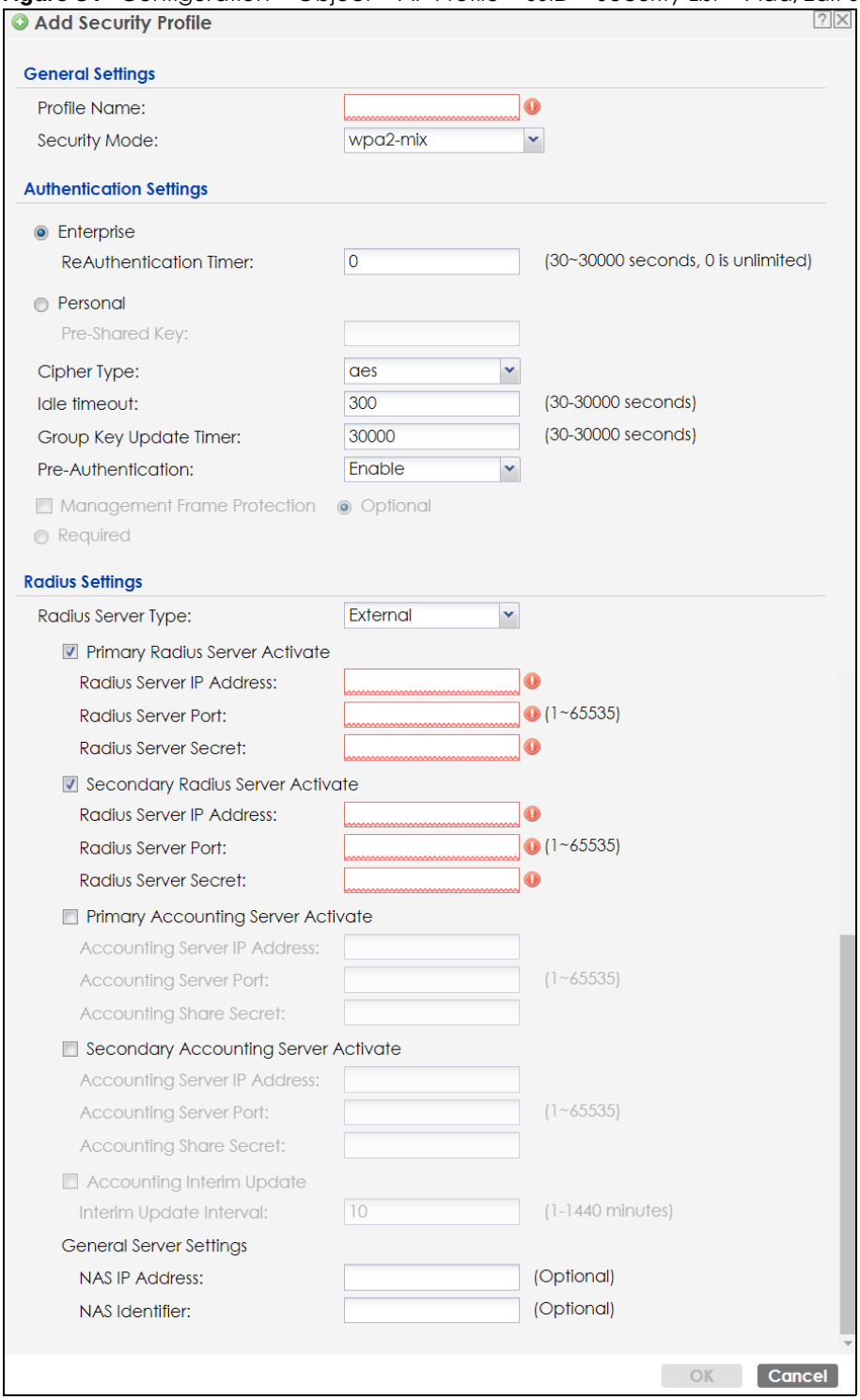
LABEL	DESCRIPTION
Add	Click this to add a new security profile.
Edit	Click this to edit the selected security profile.
Remove	Click this to remove the selected security profile.
Object Reference	Click this to view which other objects are linked to the selected security profile (for example, SSID profile).
#	This field is a sequential value, and it is not associated with a specific user.
Profile Name	This field indicates the name assigned to the security profile.
Security Mode	This field indicates this profile's security mode (if any).

13.4.1 Add/Edit Security Profile

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

Note: This screen's options change based on the **Security Mode** selected. Only the default screen is displayed here.

Figure 84 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile



The following table describes the labels in this screen.

Table 59 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile

LABEL	DESCRIPTION
General Settings	
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
Security Mode	Select a security mode from the list: **none**, **enhanced-open**, **wep**, **wpa2**, **wpa2-mix** or **wpa3**. **enhanced-open** uses Opportunistic Wireless Encryption (OWE) which encrypts the wireless connection when possible.
Authentication Settings	
Enterprise	Select this to enable 802.1x secure authentication with a RADIUS server.
ReAuthentication Timer	Enter the interval (in seconds) between authentication requests. Enter a 0 for unlimited time.
Personal	This field is available when you select the **wpa2**, **wpa2-mix** or **wpa3** security mode. Select this option to use a Pre-Shared Key (PSK) with WPA2 encryption or Simultaneous Authentication of Equals (SAE) with WPA3 encryption.
Pre-Shared Key	Enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
Transition Mode	Enable this for backwards compatibility. This option is only available if the **Security Mode** is **wpa3** or **enhanced-open**. This creates two virtual APs (VAPs) with a primary (**wpa3** or **enhanced-open**) and fallback (**wpa2** or **none**) security method. If the **Security Mode** is **wpa3**, enabling this will force **Management Frame Protection** to be set to **Optional**. If this is disabled or if the **Security Mode** is **enhanced-open**, **Management Frame Protection** will be set to **Required**.
Cipher Type	Select an encryption cipher type from the list. • **auto** - This automatically chooses the best available cipher based on the cipher in use by the wireless client that is attempting to make a connection. • **aes** - This is the Advanced Encryption Standard encryption method. It is a more recent development over TKIP and considerably more robust. Not all wireless clients may support this.
Idle Timeout	Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued.
Authentication Type	Select a WEP authentication method. Choices are **Open** or **Share** key.
Key Length	Select the bit-length of the encryption key to be used in WEP connections. If you select **WEP-64**: • Enter 10 hexadecimal digits in the range of “A-F”, “a-f” and “0-9” (for example, 0x11AA22BB33) for each **Key** used. or • Enter 5 ASCII characters (case sensitive) ranging from “a-z”, “A-Z” and “0-9” (for example, MyKey) for each **Key** used. If you select **WEP-128**: • Enter 26 hexadecimal digits in the range of “A-F”, “a-f” and “0-9” (for example, 0x00112233445566778899AABBCC) for each **Key** used. or • Enter 13 ASCII characters (case sensitive) ranging from “a-z”, “A-Z” and “0-9” (for example, MyKey12345678) for each **Key** used.

Table 59 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile (continued)

LABEL	DESCRIPTION
Key 1~4	Based on your **Key Length** selection, enter the appropriate length hexadecimal or ASCII key.
Group Key Update Timer	Enter the interval (in seconds) at which the AP updates the group WPA2 encryption key.
Management Frame Protection	This field is available only when you select **wpa2** in the **Security Mode** field and set **Cipher Type** to **aes**. Data frames in 802.11 WLANs can be encrypted and authenticated with WEP, WPA or WPA2. But 802.11 management frames, such as beacon/probe response, association request, association response, de-authentication and disassociation are always unauthenticated and unencrypted. IEEE 802.11w Protected Management Frames allows APs to use the existing security mechanisms (encryption and authentication methods defined in IEEE 802.11i WPA/WPA2) to protect management frames. This helps prevent wireless DoS attacks. Select the check box to enable management frame protection (MFP) to add security to 802.11 management frames. Select **Optional** if you do not require the wireless clients to support MFP. Management frames will be encrypted if the clients support MFP. Select **Required** and wireless clients must support MFP in order to join the Zyxel Device's wireless network.
Radius Settings	
Radius Server Type	This shows **External** and the Zyxel Device uses an external RADIUS server for authentication.
Primary / Secondary Radius Server Activate	Select this to have the Zyxel Device use the specified RADIUS server.
Radius Server IP Address	Enter the IP address of the RADIUS server to be used for authentication.
Radius Server Port	Enter the port number of the RADIUS server to be used for authentication.
Radius Server Secret	Enter the shared secret password of the RADIUS server to be used for authentication.
Primary / Secondary Accounting Server Activate	Select the check box to enable user accounting through an external authentication server.
Accounting Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Accounting Server Port	Enter the port number of the external accounting server. The default port number is 1813. You need not change this value unless your network administrator instructs you to do so with additional information.
Accounting Share Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external accounting server and the Zyxel Device. The key must be the same on the external accounting server and your Zyxel Device. The key is not sent over the network.
Accounting Interim Update	This field is available only when you enable user accounting through an external authentication server. Select this to have the Zyxel Device send subscriber status updates to the accounting server at the interval you specify.
Interim Update Interval	Specify the time interval for how often the Zyxel Device is to send a subscriber status update to the accounting server.
General Server Settings	
NAS IP Address	If the RADIUS server requires the Zyxel Device to provide the NAS (Network Access Server) IP address attribute, enter it here.

Table 59 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile (continued)

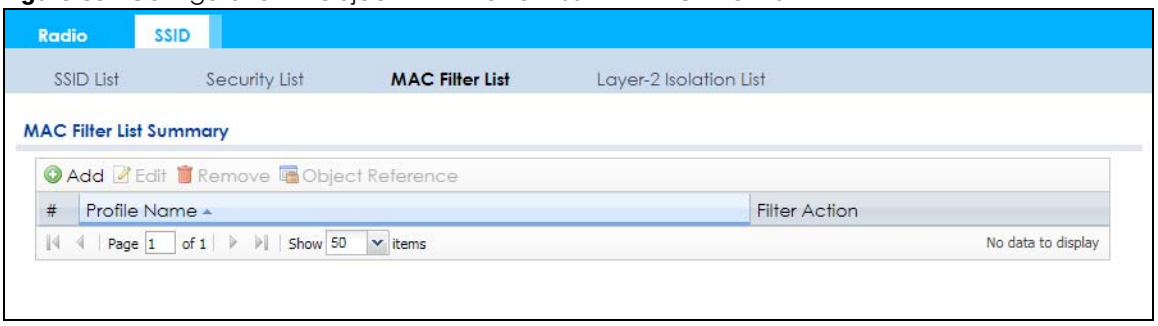
LABEL	DESCRIPTION
NAS Identifier	If the RADIUS server requires the Zyxel Device to provide the NAS (Network Access Server) identifier attribute, enter it here. The NAS identifier is to identify the source of access request. It could be the NAS's fully qualified domain name.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

13.5 MAC Filter List

This screen allows you to create and manage security configurations that can be used by your SSIDs. To access this screen click **Configuration > Object > AP Profile > SSID > MAC Filter List**.

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

Figure 85 Configuration > Object > AP Profile > SSID > MAC Filter List



The following table describes the labels in this screen.

Table 60 Configuration > Object > AP Profile > SSID > MAC Filter List

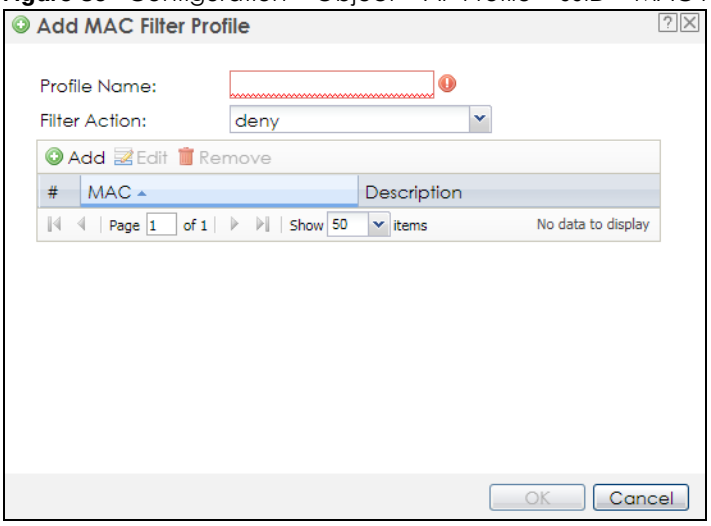
LABEL	DESCRIPTION
Add	Click this to add a new MAC filtering profile.
Edit	Click this to edit the selected MAC filtering profile.
Remove	Click this to remove the selected MAC filtering profile.
Object Reference	Click this to view which other objects are linked to the selected MAC filtering profile (for example, SSID profile).
#	This field is a sequential value, and it is not associated with a specific user.
Profile Name	This field indicates the name assigned to the MAC filtering profile.
Filter Action	This field indicates this profile's filter action (if any).

13.5.1 Add/Edit MAC Filter Profile

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

Note: Each MAC filtering profile can include a maximum of 512 MAC addresses.

Figure 86 Configuration > Object > AP Profile > SSID > MAC Filter List > Add/Edit MAC Filter Profile



The following table describes the labels in this screen.

Table 61 Configuration > Object > AP Profile > SSID > MAC Filter List > Add/Edit MAC Filter Profile

LABEL	DESCRIPTION
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
Filter Action	Select **allow** to permit the wireless client with the MAC addresses in this profile to connect to the network through the associated SSID; select **deny** to block the wireless clients with the specified MAC addresses.
Add	Click this to add a MAC address to the profile's list.
Edit	Click this to edit the selected MAC address in the profile's list.
Remove	Click this to remove the selected MAC address from the profile's list.
#	This field is a sequential value, and it is not associated with a specific user.
MAC	This field specifies a MAC address associated with this profile. You can click the MAC address to make it editable.
Description	This field displays a description for the MAC address associated with this profile. You can click the description to make it editable. Enter up to 60 characters, spaces and underscores allowed.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

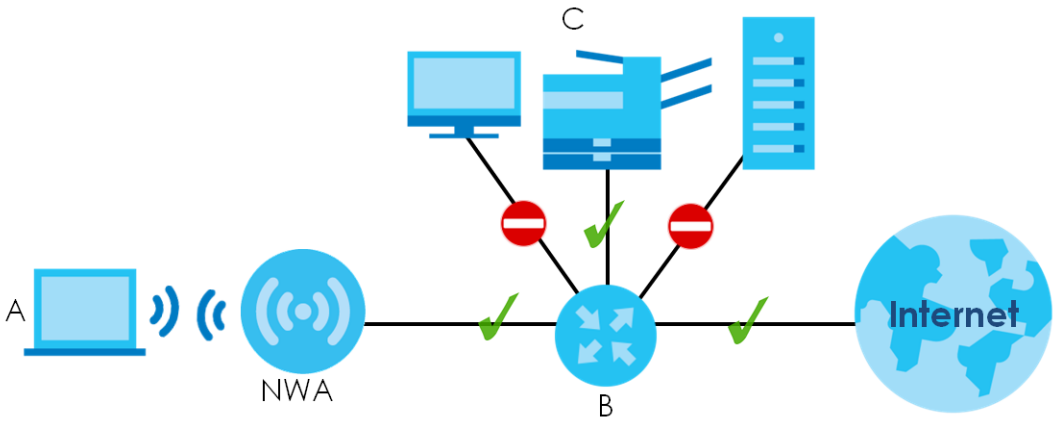
13.6 Layer-2 Isolation List

Layer-2 isolation is used to prevent wireless clients associated with your Zyxel Device from communicating with other wireless clients, APs, computers or routers in a network.

In the following example, layer-2 isolation is enabled on the Zyxel Device to allow a guest wireless client (**A**) to access the main network router (**B**). The router provides access to the Internet and the network printer (**C**) while preventing the client from accessing other computers and servers on the network. The client can communicate with other wireless clients only if Intra-BSS Traffic blocking is disabled.

Note: Intra-BSS Traffic Blocking is activated when you enable layer-2 isolation.

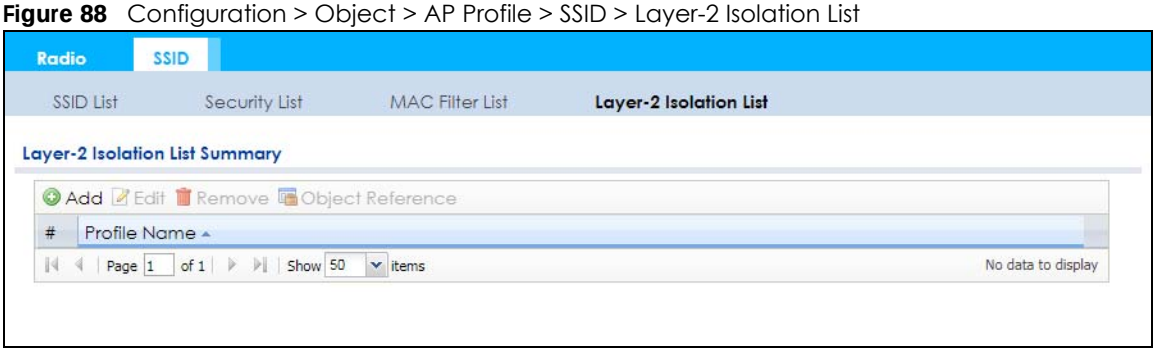
Figure 87 Layer-2 Isolation Application



MAC addresses that are not listed in the layer-2 isolation table are blocked from communicating with the Zyxel Device's wireless clients except for broadcast packets. Layer-2 isolation does not check the traffic between wireless clients that are associated with the same AP. Intra-BSS traffic allows wireless clients associated with the same AP to communicate with each other.

This screen allows you to specify devices you want the users on your wireless networks to access. To access this screen click **Configuration > Object > AP Profile > SSID > Layer-2 Isolation List**.

Figure 88 Configuration > Object > AP Profile > SSID > Layer-2 Isolation List



The following table describes the labels in this screen.

Table 62 Configuration > Object > AP Profile > SSID > Layer-2 Isolation List

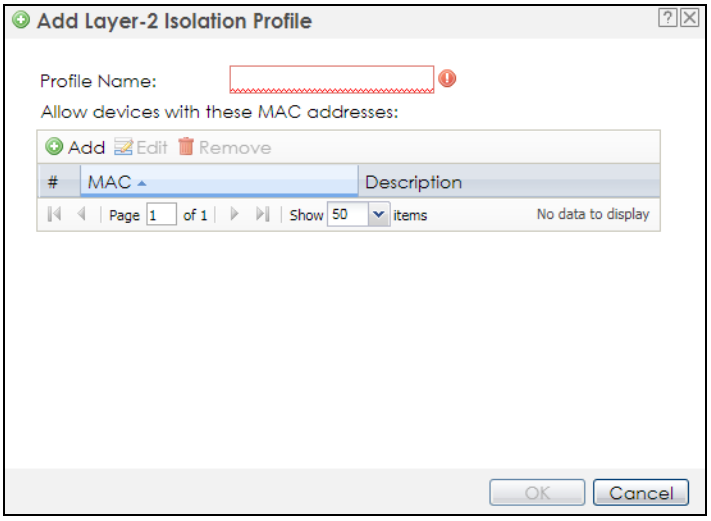
LABEL	DESCRIPTION
Add	Click this to add a new layer-2 isolation profile.
Edit	Click this to edit the selected layer-2 isolation profile.
Remove	Click this to remove the selected layer-2 isolation profile.
Object Reference	Click this to view which other objects are linked to the selected layer-2 isolation profile (for example, SSID profile).
#	This field is a sequential value, and it is not associated with a specific user.
Profile Name	This field indicates the name assigned to the layer-2 isolation profile.

13.6.1 Add/Edit Layer-2 Isolation Profile

This screen allows you to create a new layer-2 isolation profile or edit an existing one. To access this screen, click the **Add** button or select a layer-2 isolation profile from the list and click the **Edit** button.

Note: You need to know the MAC address of each wireless client, AP, computer or router that you want to allow to communicate with the Zyxel Device's wireless clients.

Figure 89 Configuration > Object > AP Profile > SSID > Layer-2 Isolation List > Add/Edit Layer-2 Isolation Profile



The following table describes the labels in this screen.

Table 63 Configuration > Object > AP Profile > SSID > Layer-2 Isolation List > Add/Edit Layer-2 Isolation Profile

LABEL	DESCRIPTION
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
Add	Click this to add a MAC address to the profile's list.
Edit	Click this to edit the selected MAC address in the profile's list.
Remove	Click this to remove the selected MAC address from the profile's list.
#	This field is a sequential value, and it is not associated with a specific user.
MAC	This field specifies a MAC address associated with this profile. You can click the MAC address to make it editable.
Description	This field displays a description for the MAC address associated with this profile. You can click the description to make it editable. Enter up to 60 characters, spaces and underscores allowed.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

CHAPTER 14
MON Profile

14.1 Overview

This screen allows you to set up monitor mode configurations that allow your Zyxel Device to scan for other wireless devices in the vicinity. Once detected, you can use the **Wireless > MON Mode** screen (Section 10.3 on page 109) to classify them as either rogue or friendly.

Not all Zyxel Devices support monitor mode and rogue APs detection.

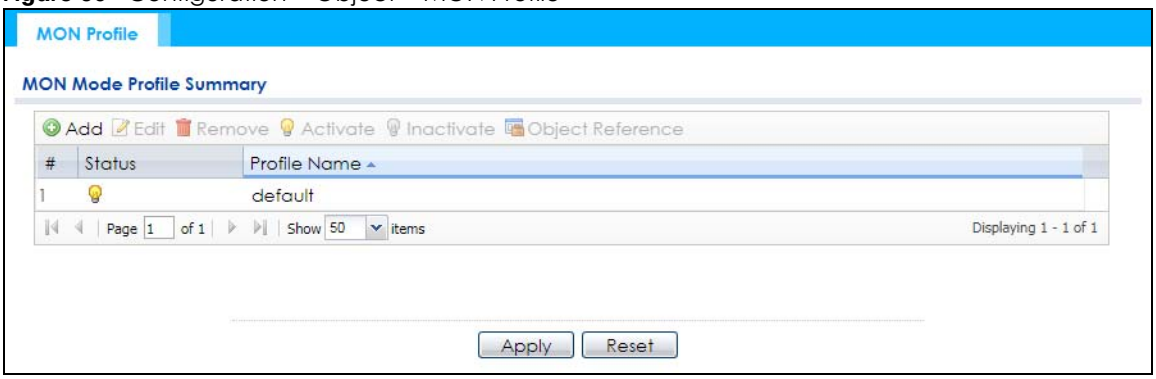
14.1.1 What You Can Do in this Chapter

The **MON Profile** screen (Section 14.2 on page 150) creates preset monitor mode configurations that can be used by the Zyxel Device.

14.2 MON Profile

This screen allows you to create monitor mode configurations that can be used by the APs. To access this screen, log into the Web Configurator, and click **Configuration > Object > MON Profile**.

Figure 90 Configuration > Object > MON Profile



The following table describes the labels in this screen.

Table 64 Configuration > Object > MON Profile

LABEL	DESCRIPTION
Add	Click this to add a new monitor mode profile.
Edit	Click this to edit the selected monitor mode profile.
Remove	Click this to remove the selected monitor mode profile.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.