ZYXEL
NETWORKS

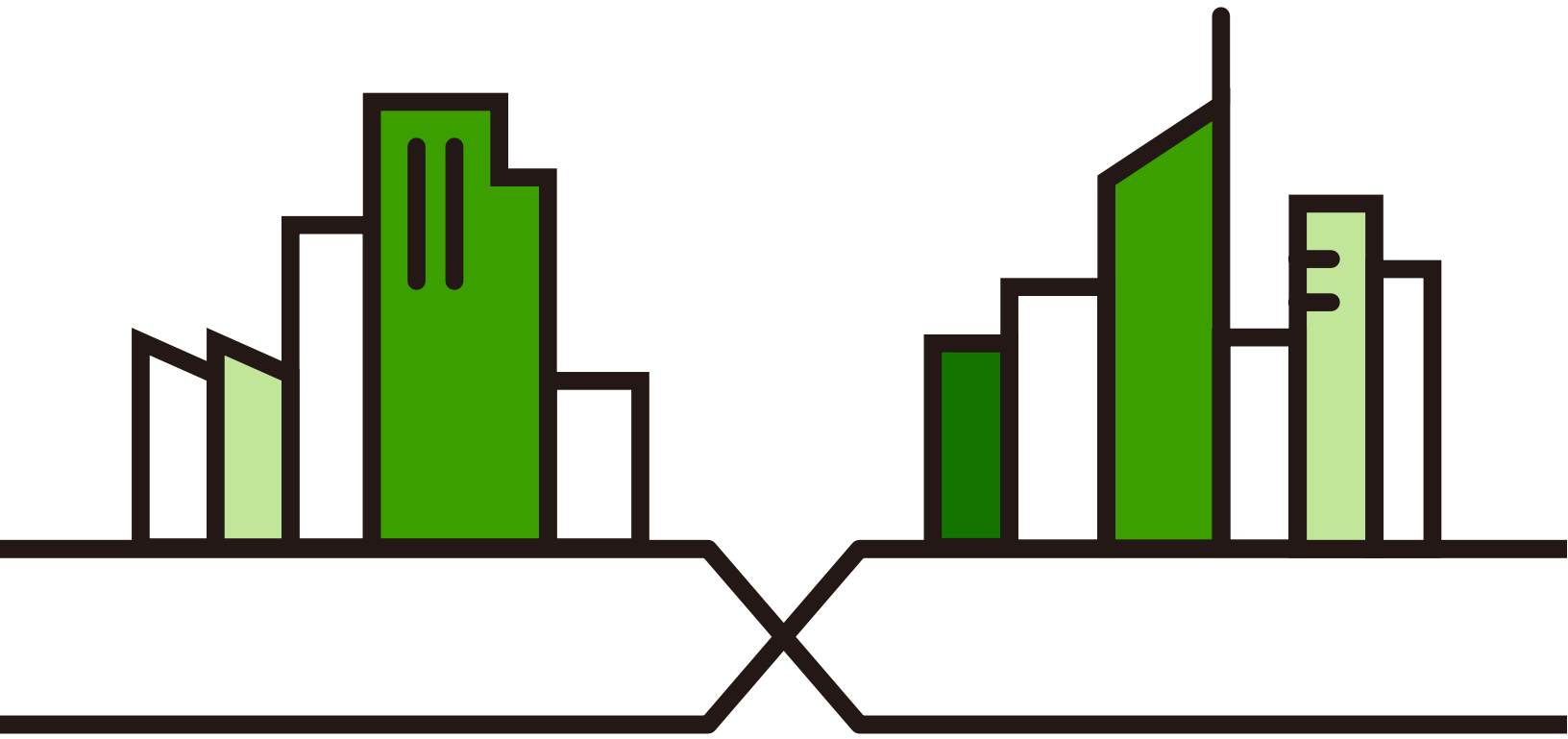
User's Guide

NWA/WAC/WAX/WBE Series

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

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

Version 6.70-7.10 Edition 1, 12/2024



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

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

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

Related Documentation

- Quick Start Guide

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

- CLI Reference Guide

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

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

- Web Configurator Online Help

  Click the help icon in any screen for help in configuring that screen and supplementary information.

- Nebula Control Center User's Guide

  This User's Guide shows how to manage the Zyxel Device remotely. The features of these devices can be managed through Nebula Control Center. It also offers features that are not available when the Zyxel Device is in standalone mode (see Section 2.1.2 on page 33).

- AC (AP Controller) User's Guide

  See the ZyWALL ATP, ZyWALL VPN, or USG FLEX User's Guide for instructions on using the gateways 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 	IP Phone 
Printer 	Smart TV. 		

Contents Overview

Table of Contents

CHAPTER 1 Introduction

1.1 Overview

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

NCC, AC or Standalone (NebulaFlex PRO)

- WAC500
- WAC500H
- WAX300H
- WAX510D
- WAX610D
- WAX620D-6E
- WAX630S
- WAX640S-6E
- WAX650S
- WAX655E
- WBE510D
- WBE530
- WBE630S
- WBE660S

NCC or Standalone (NebulaFlex)

- NWA110AX
- NWA110BE
- NWA1123ACv3
- NWA130BE
- NWA210AX
- NWA210BE
- NWA220AX-6E

For more information about Access Point (AP) management, see Section 2.1 on page 32.

When two or more APs are interconnected, this network is called a Wireless Distribution System (WDS). See Section on page 17 for more information on root and repeater APs and how to set them up.

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

1.2 Zyxel Device Product Feature Comparison

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

Table 1 500/1000 Models Comparison Table

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

Table 1 500/1000 Models Comparison Table (continued)

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

Table 2 WiFi 6 Models Comparison Table

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

Table 2 WiFi 6 Models Comparison Table (continued)

FEATURES	WAX300H	WAX510D	WAX610D
Reset Button	Yes	Yes	Yes
LED Locator	Yes	Yes	Yes
LED Suppression	Yes	Yes	Yes
AC (AP Controller) Discovery	Yes	Yes	Yes
NebulaFlex PRO	Yes	Yes	Yes
NCC Discovery	Yes	Yes	Yes
802.11r Fast Roaming Support	Yes	Yes	Yes
802.11k/v Assisted Roaming	Yes	Yes	Yes
Proxy ARP	Yes	Yes	Yes
Bluetooth Low Energy (BLE)	No	No	No
Load Balancing	No	Yes	Yes
Ethernet Storm Control	Yes	Yes	Yes
Wireless Remote Capture	Yes	Yes	Yes
SNMP	No	Yes	Yes
Grounding	No	Yes	Yes
Power Jack	No	Yes	Yes
Maximum number of log messages	512 event logs		
Latest Firmware Version Supported	7.00	7.00	7.00

Table 3 WiFi 6 Models Comparison Table

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

Table 3 WiFi 6 Models Comparison Table (continued)

FEATURES	WAX630S	WAX650S	WAX655E
Tunnel Forwarding Mode	Yes	Yes	Yes
Layer-2 Isolation	Yes	Yes	Yes
Supported PoE Standards	IEEE 802.3af IEEE 802.3at	IEEE 802.3at IEEE 802.3bt	IEEE 802.3af IEEE 802.3at
Power Detection	Yes	Yes	Yes
External Antennas	No	No	Yes
Internal Antennas	Yes	Yes	No
Antenna Switch	No	No	No
Smart Antenna	Yes	Yes	No
Console Port	4-Pin Serial	4-Pin Serial	4-Pin Serial
Reset Button	Yes	Yes	Yes
LED Locator	Yes	Yes	Yes
LED Suppression	Yes	Yes	Yes
AC (AP Controller) Discovery	Yes	Yes	Yes
NebulaFlex PRO	Yes	Yes	Yes
NCC Discovery	Yes	Yes	Yes
802.11r Fast Roaming Support	Yes	Yes	Yes
802.11k/v Assisted Roaming	Yes	Yes	Yes
Proxy ARP	Yes	Yes	Yes
Bluetooth Low Energy (BLE)	No	Yes	No
Load Balancing	Yes	Yes	Yes
Ethernet Storm Control	Yes	Yes	Yes
Wireless Remote Capture	Yes	Yes	Yes
SNMP	Yes	Yes	Yes
Grounding	Yes	Yes	Yes
Power Jack	Yes	Yes	Yes
Maximum number of log messages	512 event logs		
Latest Firmware Version Supported	7.00	7.00	7.00

Table 4 WiFi 6 Models Comparison Table

FEATURES	NWA110AX	NWA210AX
Supported WiFi Standards	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax
Supported Frequency Bands	2.4 GHz 5 GHz	2.4 GHz 5 GHz
Supported Channel Width	2.4G: 20/40 MHz 5G: 20/40/80 MHz	2.4G: 20/40 MHz 5G: 20/40/80/160 MHz
Available Security Modes	None /Enhanced-open / WEP / WPA2-MIX / WPA3 - Personal & Enterprise	None /Enhanced-open / WEP / WPA2-MIX / WPA3 - Personal & Enterprise

Table 4 WiFi 6 Models Comparison Table (continued)

FEATURES	NWA110AX	NWA210AX
Number of SSID Profiles	64	64
Number of WiFi Radios	2	2
Security Profile Radius Settings	Yes	Yes
Security Profile Enterprise Authentication Settings	Yes	Yes
Rogue AP Detection	Yes	Yes
WDS (Wireless Distribution System) - Root AP & Repeater Modes	Yes	Yes
Wireless Bridge	No	No
Tunnel Forwarding Mode	No	No
Layer-2 Isolation	Yes	Yes
Supported PoE Standards	IEEE 802.3af IEEE 802.3at	IEEE 802.3af IEEE 802.3at
Power Detection	Yes	Yes
External Antennas	No	No
Internal Antennas	Yes	Yes
Antenna Switch	No	No
Smart Antenna	No	No
Console Port	4-Pin Serial	4-Pin Serial
Reset Button	Yes	Yes
LED Locator	Yes	Yes
LED Suppression	Yes	Yes
AC (AP Controller) Discovery	No	No
NebulaFlex PRO	No	No
NCC Discovery	Yes	Yes
802.11r Fast Roaming Support	Yes	Yes
802.11k/v Assisted Roaming	Yes	Yes
Proxy ARP	Yes	Yes
Bluetooth Low Energy (BLE)	No	No
Load Balancing	Yes	Yes
Ethernet Storm Control	Yes	Yes
Wireless Remote Capture	Yes	Yes
SNMP	Yes	Yes
Grounding	Yes	Yes
Power Jack	Yes	Yes
Maximum number of log messages	512 event logs	
Latest Firmware Version Supported	7.00	7.00

Table 5 WiFi 6E Models Comparison Table

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

Table 5 WiFi 6E Models Comparison Table (continued)

FEATURES	WAX620D-6E	WAX640S-6E	NWA220AX-6E
Load Balancing	Yes	Yes	Yes
Ethernet Storm Control	Yes	Yes	Yes
Wireless Remote Capture	Yes	Yes	Yes
SNMP	Yes	Yes	Yes
Grounding	No	Yes	No
Power Jack	Yes	Yes	Yes
Maximum number of log messages	512 event logs		
Latest Firmware Version Supported	7.00	7.00	7.00

Table 6 WiFi 7 Models Comparison Table (Part 1)

FEATURES	NWA110BE	NWA130BE	NWA210BE
Supported WiFi Standards	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax IEEE 802.11be	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax IEEE 802.11be	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax IEEE 802.11be
Supported Frequency Bands	2.4 GHz 5 GHz 6 GHz	2.4 GHz 5 GHz 6 GHz	2.4 GHz 5 GHz 6 GHz
BandFlex (5 GHz /6 GHz)	Yes	Yes	Yes
Supported Channel Width	2.4G: 20/40 MHz 5G: 20/40/80/160/240 MHz 6G: 80/160/320 MHz	2.4G: 20/40 MHz 5G: 20/40/80/160/240 MHz 6G: 80/160/320 MHz	2.4G: 20/40 MHz 5G: 20/40/80/160/240 MHz 6G: 80/160/320 MHz
Available Security Modes	None / Enhanced-open / WEP /WPA2-MIX / WPA3 - Personal & Enterprise	None / Enhanced-open / WEP /WPA2-MIX / WPA3 - Personal & Enterprise	None / Enhanced-open / WEP / WPA2-MIX / WPA3 - Personal & Enterprise
Number of SSID Profiles	64	64	64
Number of WiFi Radios	2	3	2
Security Profile Radius Settings	Yes	Yes	Yes
Security Profile Enterprise Authentication Settings	Yes	Yes	Yes
Rogue AP Detection	Yes	Yes	Yes
WDS (Wireless Distribution System) - Root AP & Repeater Modes	Yes	Yes	Yes
Wireless Bridge	Yes	Yes	Yes
Tunnel Forwarding Mode	Yes	Yes	Yes
Layer-2 Isolation	Yes	Yes	Yes
Supported PoE Standards	IEEE 802.3at IEEE 802.3af	IEEE 802.3at IEEE 802.3af	IEEE 802.3at IEEE 802.3af
Power Detection	Yes	Yes	Yes
External Antennas	No	No	No
Internal Antennas	Yes	Yes	Yes
Antenna Switch	No	No	No

Table 6 WiFi 7 Models Comparison Table (Part 1) (continued)

FEATURES	NWA110BE	NWA130BE	NWA210BE
Smart Antenna	No	No	No
Console Port	4-Pin Serial	4-Pin Serial	4-Pin Serial
Reset Button	Yes	Yes	Yes
LED Locator	Yes	Yes	Yes
LED Suppression	Yes	Yes	Yes
AC (AP Controller) Discovery	No	No	No
NebulaFlex PRO	No	No	No
NCC Discovery	Yes	Yes	Yes
802.11r Fast Roaming Support	Yes	Yes	Yes
802.11k/v Assisted Roaming	Yes	Yes	Yes
Proxy ARP	Yes	Yes	Yes
Bluetooth Low Energy (BLE)	No	No	No
Load Balancing	Yes	Yes	Yes
Ethernet Storm Control	Yes	Yes	Yes
Wireless Remote Capture	Yes	Yes	Yes
SNMP	Yes	Yes	Yes
Grounding	No	No	No
Power Jack	USB-C	Yes	USB-C
Maximum number of log messages	512 event logs		
Latest Firmware Version Supported	7.10	7.00	7.10

Table 7 WiFi 7 Models Comparison Table (Part 2)

FEATURES	WBE510D	WBE530	WBE630S
Supported WiFi Standards	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax IEEE 802.11be	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax IEEE 802.11be	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax IEEE 802.11be
Supported Frequency Bands	2.4 GHz 5 GHz 6 GHz	2.4 GHz 5 GHz 6 GHz	2.4 GHz 5 GHz 6 GHz
BandFlex (5 GHz /6 GHz)	Yes	Yes	Yes
Supported Channel Width	2.4G: 20/40 MHz 5G: 20/40/80/160/240 MHz 6G: 80/160/320 MHz	2.4G: 20/40 MHz 5G: 20/40/80/160/240 MHz 6G: 80/160/320 MHz	2.4G: 20/40 MHz 5G: 20/40/80/160/240 MHz 6G: 80/160/320 MHz
Available Security Modes	None / Enhanced-open / WEP /WPA2-MIX / WPA3 - Personal & Enterprise	None / Enhanced-open / WEP /WPA2-MIX / WPA3 - Personal & Enterprise	None / Enhanced-open / WEP /WPA2-MIX / WPA3 - Personal & Enterprise
Number of SSID Profiles	64	64	64
Number of WiFi Radios	2	3	2
Security Profile Radius Settings	Yes	Yes	Yes
Security Profile Enterprise Authentication Settings	Yes	Yes	Yes
Rogue AP Detection	Yes	Yes	Yes

Table 7 WiFi 7 Models Comparison Table (Part 2) (continued)

FEATURES	WBE510D	WBE530	WBE630S
WDS (Wireless Distribution System) - Root AP & Repeater Modes	Yes	Yes	Yes
Wireless Bridge	Yes	Yes	Yes
Tunnel Forwarding Mode	Yes	Yes	Yes
Layer-2 Isolation	Yes	Yes	Yes
Supported PoE Standards	IEEE 802.3at IEEE 802.3af	IEEE 802.3at IEEE 802.3af	IEEE 802.3at IEEE 802.3af
Power Detection	Yes	Yes	Yes
External Antennas	No	No	No
Internal Antennas	Yes	Yes	Yes
Antenna Switch	Yes (per AP)	No	No
Smart Antenna	No	No	Yes
Console Port	4-Pin Serial	4-Pin Serial	4-Pin Serial
Reset Button	Yes	Yes	Yes
LED Locator	Yes	Yes	Yes
LED Suppression	Yes	Yes	Yes
AC (AP Controller) Discovery	Yes	No	Yes
NebulaFlex PRO	Yes	Yes	Yes
NCC Discovery	Yes	Yes	Yes
802.11r Fast Roaming Support	Yes	Yes	Yes
802.11k/v Assisted Roaming	Yes	Yes	Yes
Proxy ARP	Yes	Yes	Yes
Bluetooth Low Energy (BLE)	No	No	No
Load Balancing	Yes	Yes	Yes
Ethernet Storm Control	Yes	Yes	Yes
Wireless Remote Capture	Yes	Yes	Yes
SNMP	Yes	Yes	Yes
Grounding	No	No	No
Power Jack	USB-C	Yes	USB-C
Maximum number of log messages	512 event logs		
Latest Firmware Version Supported	7.10	7.00	7.10

Table 8 WiFi 7 Models Comparison Table (Part 3)

FEATURES	WBE660S
Supported WiFi Standards	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax IEEE 802.11be
Supported Frequency Bands	2.4 GHz 5 GHz 6 GHz
BandFlex (5 GHz /6 GHz)	Yes
Supported Channel Width	2.4G: 20/40 MHz 5G: 20/40/80/160/240 MHz 6G: 80/160/320 MHz
Available Security Modes	None / Enhanced-open / WEP /WPA2-MIX / WPA3 - Personal & Enterprise
Number of SSID Profiles	64
Number of WiFi Radios	3
Security Profile Radius Settings	Yes
Security Profile Enterprise Authentication Settings	Yes
Rogue AP Detection	Yes
WDS (Wireless Distribution System) - Root AP & Repeater Modes	Yes
Wireless Bridge	Yes
Tunnel Forwarding Mode	Yes
Layer-2 Isolation	Yes
Supported PoE Standards	IEEE 802.3bt IEEE 802.3at
Power Detection	Yes
External Antennas	No
Internal Antennas	Yes
Antenna Switch	No
Smart Antenna	Yes
Console Port	4-Pin Serial
Reset Button	Yes
LED Locator	Yes
LED Suppression	Yes
AC (AP Controller) Discovery	Yes
NebulaFlex PRO	Yes
NCC Discovery	Yes
802.11r Fast Roaming Support	Yes
802.11k/v Assisted Roaming	Yes
Proxy ARP	Yes

Table 8 WiFi 7 Models Comparison Table (Part 3) (continued)

FEATURES	WBE660S
Bluetooth Low Energy (BLE)	Yes
Load Balancing	Yes
Ethernet Storm Control	Yes
Wireless Remote Capture	Yes
SNMP	Yes
Grounding	No
Power Jack	USB-C
Maximum number of log messages	512 event logs
Latest Firmware Version Supported	7.00

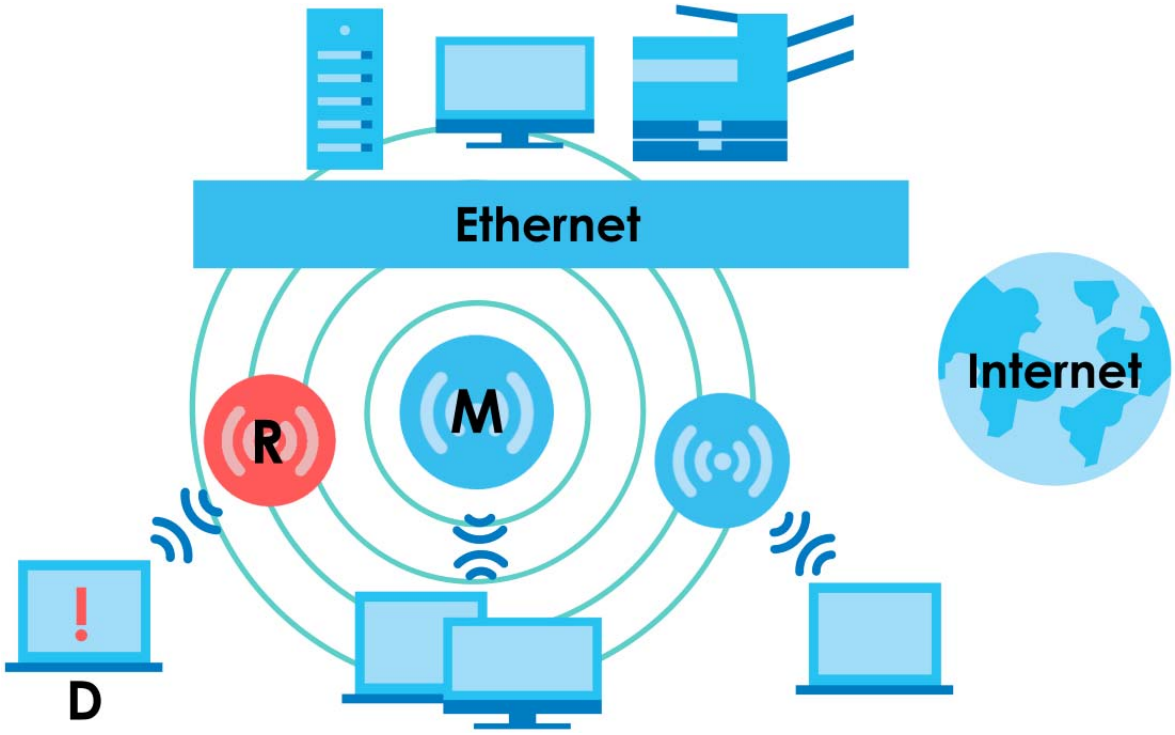
1.3 Zyxel Device Roles

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 1.2 on page 14). The Zyxel Device can serve as a:

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

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

Figure 1 Zyxel Device Application in a Network

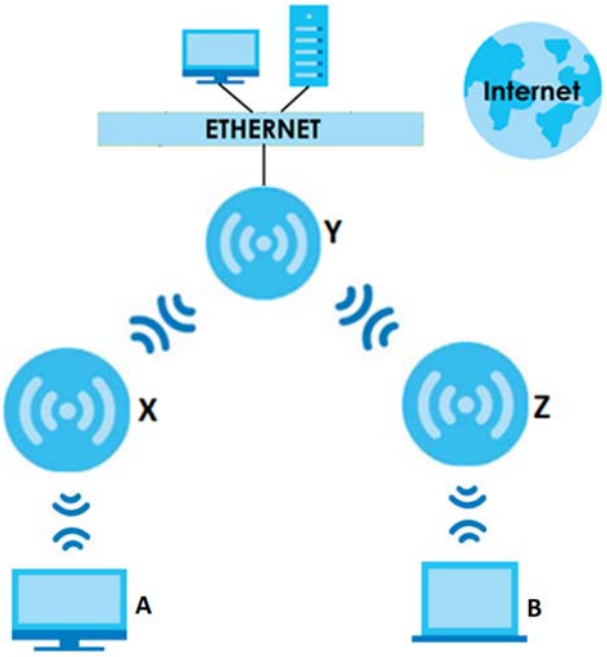


Wireless Distribution System (WDS)

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

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

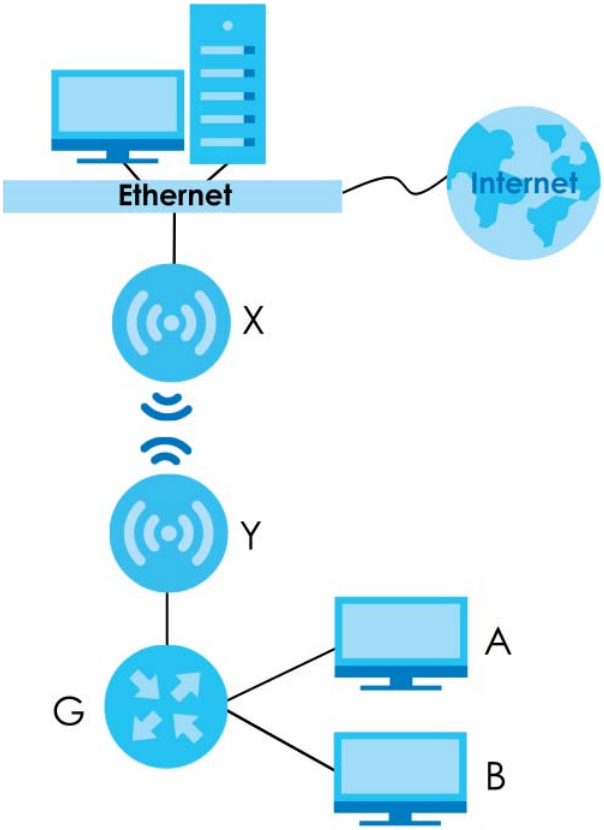
Figure 2 Wireless Distribution System Network Example



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

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

Figure 3 Wireless Bridge Network Example

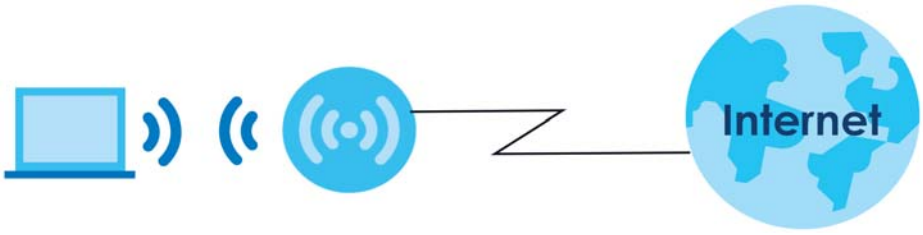


Access Point (AP)

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

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

Figure 4 AP Mode Application



Root AP

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

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

Device in Root AP mode. A repeater must use the repeater SSID to connect to the Zyxel Device in **Root AP** mode. See Section 15.1 on page 204 for more details.

When the Zyxel Device is in **Root AP** mode, repeater security between the Zyxel Device and other repeaters is independent of the security between the WiFi clients and the AP or repeater. When repeater security is enabled, both APs and repeaters must use the same pre-shared key. See Section 11.2 on page 138 and Section 15.2 on page 204 for more details.

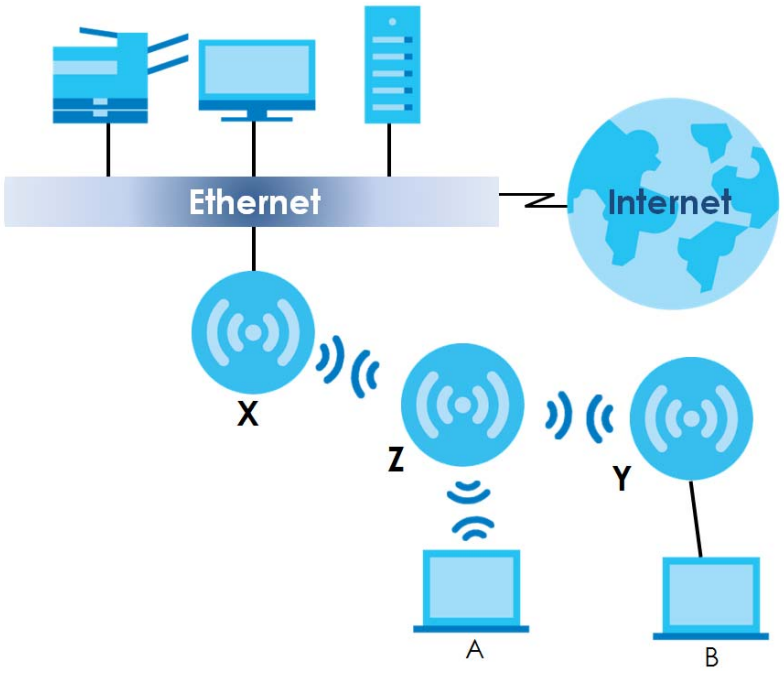
Unless specified, the term "security settings" refers to the traffic between the WiFi clients and the AP. At the time of writing, repeater security is compatible with the Zyxel Device only.

WiFi Repeater

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

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

Figure 5 Repeater Application



When the Zyxel Device is in **Repeater** mode, repeater security between the Zyxel Device and other repeater is independent of the security between the WiFi clients and the AP or repeater. When repeater security is enabled, both APs and repeaters must use the same pre-shared key. See Section 11.2 on page 138 and Section 15.2 on page 204 for more details.

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

1.3.1 Radio Frequency (RF) Monitor

The Zyxel Device supports **Rogue AP Detection** (see Section 11.3 on page 144). **Rogue AP Detection** allows the Zyxel Device to be set to work as an RF monitor to discover nearby Access Points. The information it obtains from other APs is used to tag possible rogue APs and friendly APs. The Zyxel Device can still work as an AP while it scans the environment for wireless signals.

1.4 Sample Feature Applications

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

1.4.1 MBSSID

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

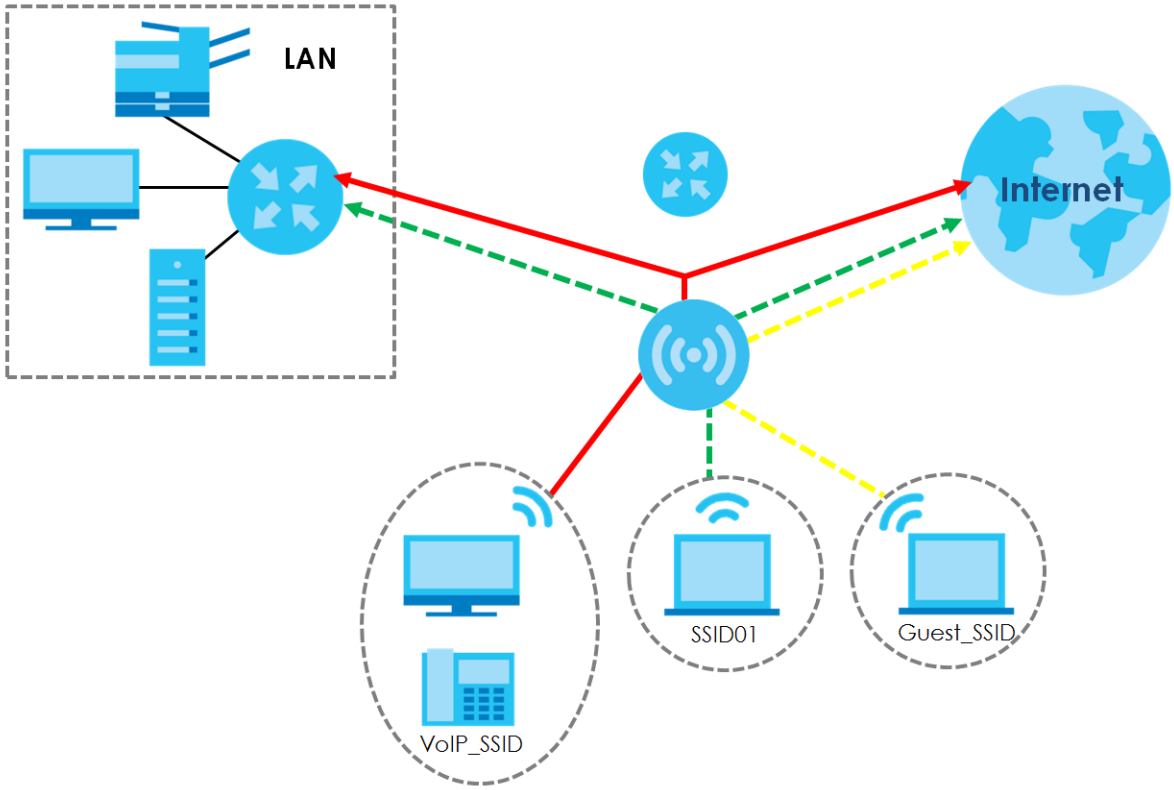
You can configure multiple SSID profiles, and have all of them active at any one time.

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

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

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

Figure 6 Multiple BSSs



1.4.2 Dual-Radio/Triple-Radio and BandFlex

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

BandFlex allows you to select the frequency bands operating on the radios by configuration. A frequency band is a range of frequency divided into channels which carry the WiFi signals for data transmission. If your Zyxel Device supports BandFlex, you can configure the second radio on the Zyxel Device to use the 5 GHz or 6 GHz bands, while the first radio is always set to use the 2.4 GHz band. The 6 GHz band provides less coverage but has the highest amount of channels among the three frequency bands. Use the 6 GHz band for the most congestion-free transmission if your client devices supports WiFi 6E (see Section 14.1.2 on page 163).

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

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

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

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

Figure 7 Dual-Radio Application

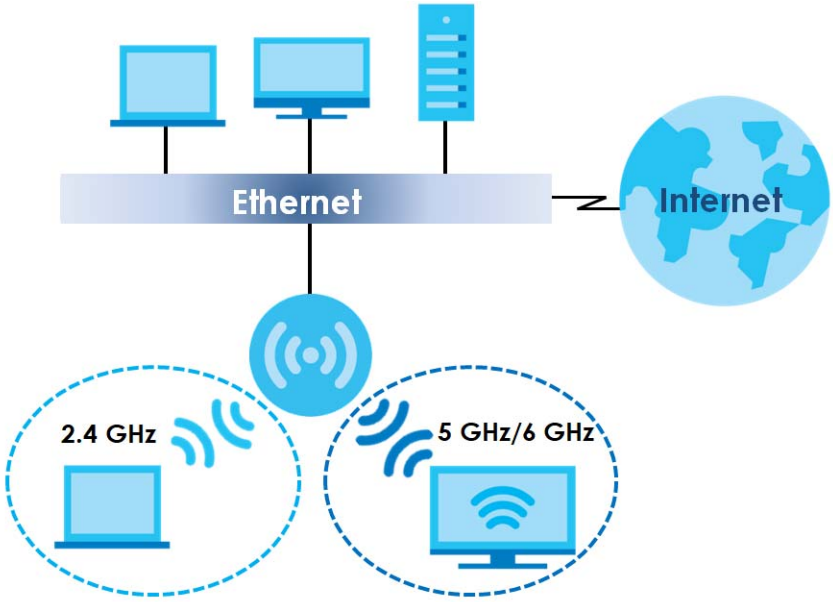
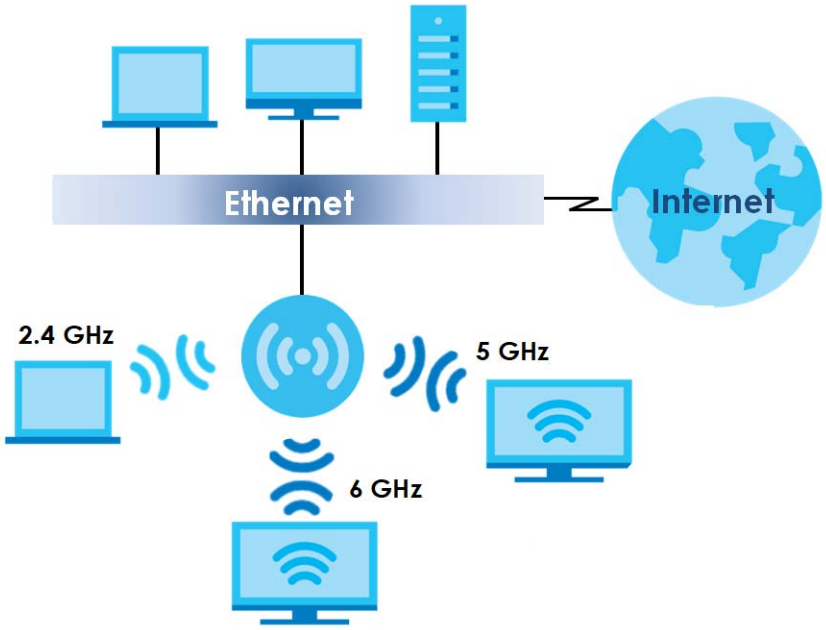


Figure 8 Triple-Radio Application



CHAPTER 2
AP Management

2.1 Management Mode

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

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

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

Table 9 Zyxel Device Management Mode Comparison

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

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

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

2.1.1 Standalone

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

See Chapter 5 on page 67 for detailed information about the standalone Web Configurator screens.

2.1.2 Nebula Control Center

In this mode, which is also called cloud mode, you can manage and monitor the Zyxel Device through the Zyxel Nebula cloud-based network management system. This means you can manage devices remotely without the need of connecting to each device directly. It offers many features to better manage and monitor not just the Zyxel Device, but your network as a whole, including supported switches and gateways. Your network can also be managed through your smartphone using the Nebula Mobile app. See Chapter 24 on page 280 for an example NCC managed network topology.

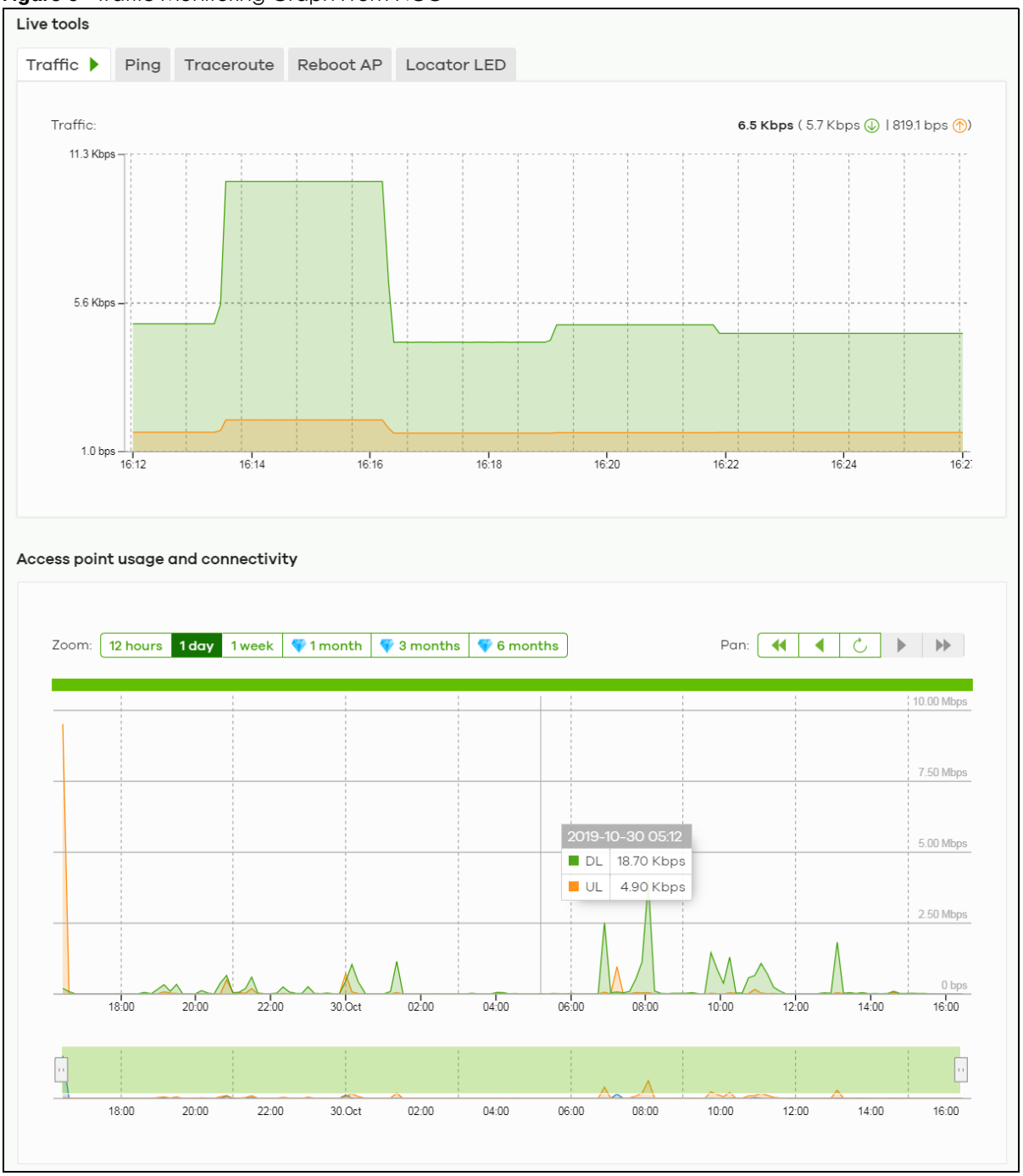
NCC allows different levels of management. You can configure each device on its own or configure a set of devices together as a site. You can also monitor groups of sites called organizations, as shown below.

Table 10 NCC Management Levels

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

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

Figure 9 Traffic Monitoring Graph From NCC



See the NCC (Nebula Control Center) User's Guide for how to configure Nebula managed devices. See Chapter 25 on page 283 if you want to change the Zyxel Device's VLAN setting or manually set its IP address.

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

2.1.3 AP Controller (AC)

If the Zyxel Device supports management using an AC (see Section 10.1.1 on page 124) such as the ZyWALL ATP, ZyWALL VPN, and the USG FLEX series, and you have this AC in the same subnet, it will be managed by the controller automatically. To set the Zyxel Device to be managed by an AC in a different subnet or change between management modes, use the **AC Discovery** screen (see Section 10.5 on page 134 and Section 10.1.1 on page 124). You can use the AC to manage multiple Zyxel Devices. See Section 10.1.1 on page 124 for an example AC managed network topology.

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

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

2.2 Switching Management Modes

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

Standalone-to-NCC

Register the Zyxel Device at the NCC website and then turn on the Zyxel Device. Make sure that **NCC Discovery** is enabled (see Section 10.6 on page 135). The NCC manages the Zyxel Device automatically when it is discovered. Settings on the Zyxel Device will be overwritten with what you have configured on the NCC website.

Standalone-to-AC

By default, the Zyxel Device must be in the same subnet as the AC. See Section 10.1.1 on page 124 for setting it up in a different subnet. Make sure **AC Discovery** is enabled (see Section 10.5 on page 134). The AC manages the Zyxel Device automatically when it is discovered.

AC-to-NCC

Register the Zyxel Device at the NCC website. Make sure that **NCC Discovery** is enabled on your Zyxel Device (see Section 10.6 on page 135). In the AC Web Configurator, select the Zyxel Device and press the **Nebula** button. The NCC manages the Zyxel Device automatically when it is discovered.

NCC-to-AC

Unregister the Zyxel Device at the NCC portal. By default, the Zyxel Device must be in the same subnet as the AC. See Section 10.1.1 on page 124 for setting it up in a different subnet. Make sure **AC Discovery** is enabled (see Section 10.5 on page 134). The AC manages the Zyxel Device automatically when it is discovered.

NCC-to-Standalone

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

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

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

AC-to-Standalone

Use the **Reset** button to return the Zyxel Device to its factory default settings (see Section 27.6 on page 304).

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

2.3.1 Requirements

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

Operating System

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

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

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

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

Hardware

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

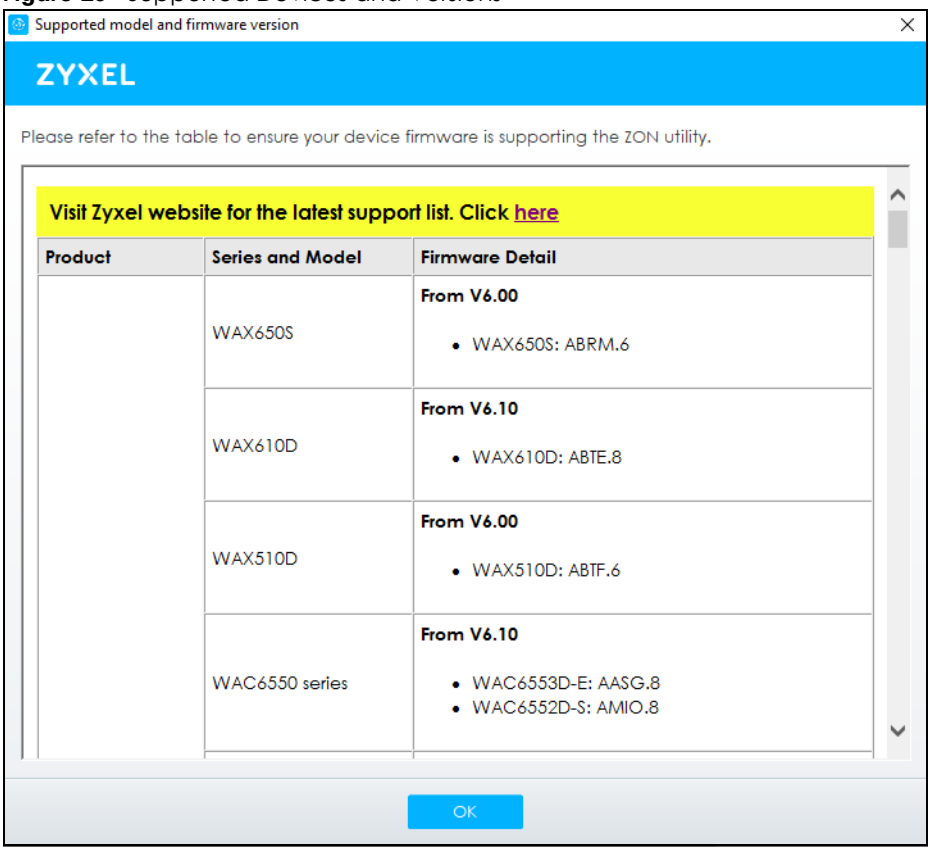
- Core i3 processor
- 2 GB RAM
- 100 MB free hard disk
- WXGA (Wide XGA 1280x800)

2.3.2 Run the ZON Utility

1 Double-click the ZON Utility to run it.

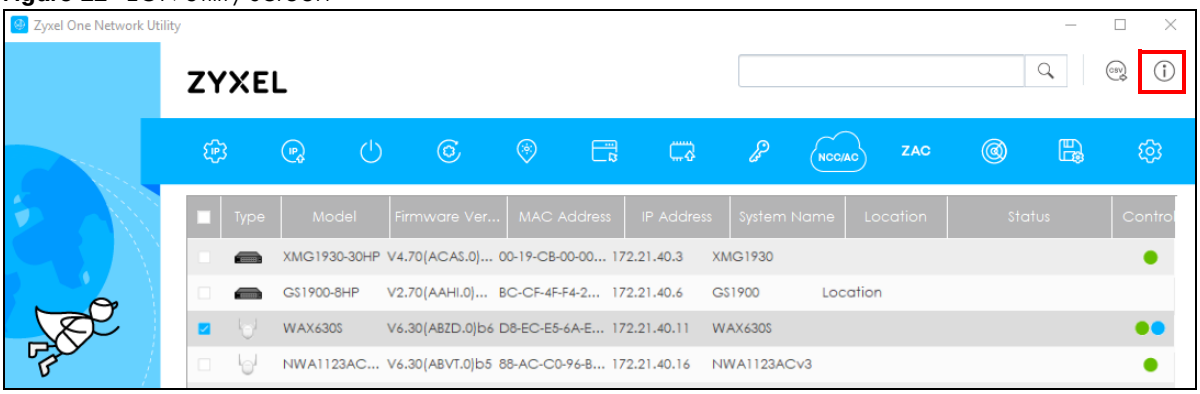
2 The first time you run the ZON Utility, you will see if your device and firmware version support the ZON Utility. Click the **OK** button to close this screen.

Figure 10 Supported Devices and Versions



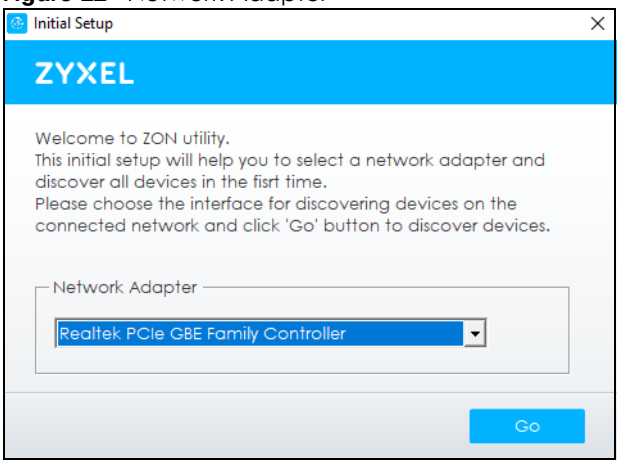
If you want to check the supported models and firmware versions later, you can click the **Show information about ZON** icon in the upper right hand corner of the screen. Then select the **Supported model and firmware version** link. If your device is not listed here, see the device release notes for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

Figure 11 ZON Utility Screen



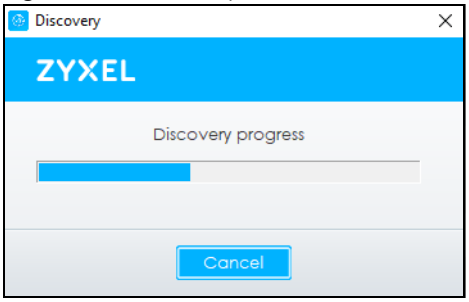
3 Select a network adapter to which your supported devices are connected.

Figure 12 Network Adapter



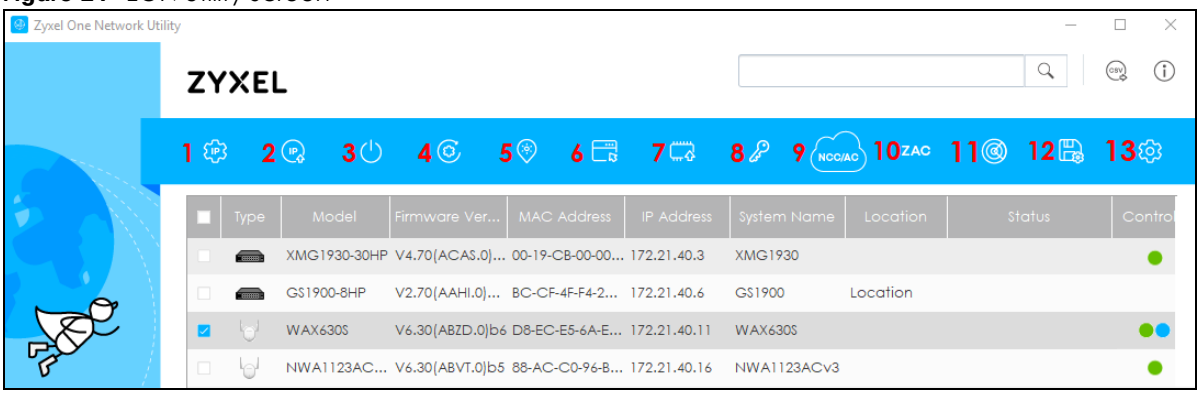
4 Click the **Go** button for the ZON Utility to discover all supported devices in your network.

Figure 13 Discovery



5 The ZON Utility screen shows the devices discovered.

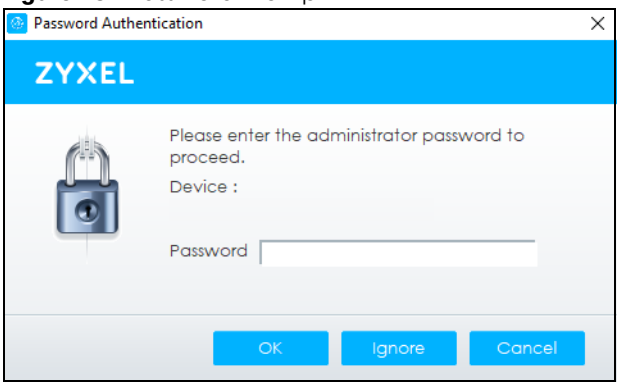
Figure 14 ZON Utility Screen



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

Figure 15 Password Prompt



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

Table 11 ZON Utility Icons

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

Table 11 ZON Utility Icons (continued)

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

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

Table 12 ZON Utility Fields

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

Table 12 ZON Utility Fields (continued)

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

2.4 Ways to Access the Zyxel Device

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

Web Configurator

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

NCC

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

AP Controller (AC)

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

ZON Utility

Zyxel One Network (ZON) Utility is a utility tool that assists you to set up and maintain network devices in a simple and efficient way. You can download the ZON Utility at *www.zyxel.com* and install it on your computer (Windows operating system). For more information on ZON Utility see Section 2.3 on page 36.

Command-Line Interface (CLI)

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

File Transfer Protocol (FTP)

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

Simple Network Management Protocol (SNMP)

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

2.5 Good Habits for Managing the Zyxel Device

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

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

CHAPTER 3 Hardware

See the Quick Start Guide for hardware installation and connections.

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

Earth grounding helps protect against lightning and interference.

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

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

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

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

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

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

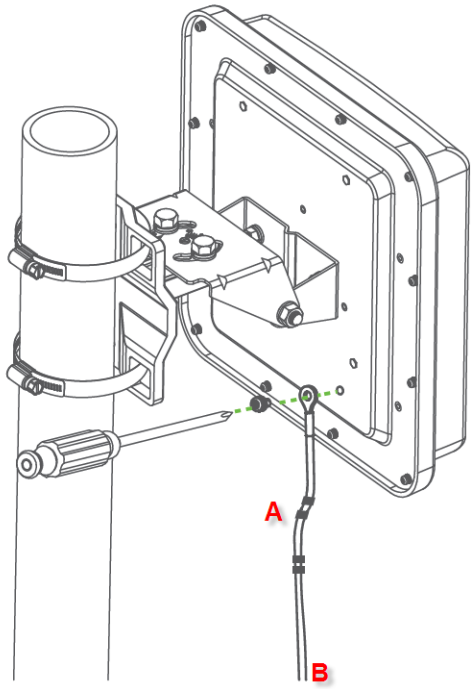
3 Attach the other end of the cable to the ground, either to the same ground electrode as the pole you installed the Zyxel Device on or to the main grounding electrode of the building.

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

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

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

Figure 16 Grounding Example



3.2 Zyxel Device Models With Single LEDs

The LEDs of some Zyxel Device models can be controlled by using the suppression feature such that the LEDs stay lit (ON) or OFF after the Zyxel Device is ready. Some Zyxel Device models also have Locator LED which allows you to see the actual location of the Zyxel Device among several devices in the network. See Section 1.2 on page 14 to check which models support these features. Refer to Section 21.1 on page 272 for the LED **Suppression** and **Locator** menus in standalone mode.

3.3 Zyxel Device LED

The LED of the Zyxel Device can be controlled by using the suppression feature such that the LED stays lit (ON) or OFF after the Zyxel Device is ready. Refer to Section 21.1 on page 272 for the LED **Suppression** and **Locator** menus in standalone mode.

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

Figure 18 WAC500H, WAX300H LED

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

Figure 20 WAX640S-6E, WBE660S LED

Figure 21 NWA130BE / WBE530 / WBE630S / WBE510D / NWA210BE / NWA110BE LED

The following are the LED descriptions for your Zyxel Device.

Table 13 Zyxel Device LED

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

Table 13 Zyxel Device LED (continued)

COLOR		STATUS	DESCRIPTION
	Amber Green	Blinks between amber and green alternately 3 times and then turns solid green for 3 seconds.	The Zyxel Device is discovering an AC, or is managed by NCC but fails to connect with NCC, and is reconnecting with the NCC.
	Amber Green	Blinks between amber and green alternately 2 times and then turns solid green for 3 seconds.	The Zyxel Device is managed by an AC but the uplink is disconnected.
	Green	Slow Blinking (On for 1 second, Off for 1 second)	The wireless module of the Zyxel Device is disabled or fails, the Zyxel Device is using default WiFi settings, or the Zyxel Device is configured to be managed by NCC but is not yet registered with the NCC. Note: WiFi networks on the WAX650S, NWA220AX-6E and WAX620D-6E are turned off automatically when it is connected to a device that supplies power using IEEE 802.3af PoE.
	Green	Steady On	The Zyxel Device is ready for use, the Zyxel Device's wireless interface is activated, and/or WiFi clients are connected to the Zyxel Device in full power mode (see Table 23 on page 69).
	Amber	Steady On	The Zyxel Device is ready for use in limited power mode (see Table 23 on page 69), the Zyxel Device's wireless interface is activated, and/or WiFi clients are connected to the Zyxel Device. Note: WiFi networks on the WAX650S, NWA220AX-6E, WAX620D-6E and WAX640S-6E are turned off automatically when it is connected to a device that supplies power using IEEE 802.3af PoE. Not all models support limited power mode. See Section 1.2 on page 14 for models that only support one PoE standard.
	Bright Blue	Steady On	The Zyxel Device's wireless interface is activated, but there are no WiFi clients connected when it is in full power mode (see Table 23 on page 69).
	White	Slow Blinking (On for 100 ms per second)	Locator LED is on. It switches off automatically after the configured amount of time (1-60 min). Default duration is 10 minutes. Note: The color of the white LED may have slight differences (for example, very light purple) on different models.
	Blue	Slow Blinking (Blink for 1 time, Off for 1 second)	The Zyxel Device is performing a Channel Availability Check (CAC) with Dynamic Frequency Selection (DFS) to monitor a channel for radar signals.
	Red	On	The Zyxel Device failed to boot up or is experiencing system failure.
		Fast Blinking (On for 50 milliseconds, Off for 50 milliseconds)	The Zyxel Device is undergoing firmware upgrade.
		Slow Blinking (Blink for 3 times, Off for 3 seconds)	The uplink of the Zyxel Device is disconnected.

3.4 Ports

The following shows the Zyxel Device panels with connection ports.

Figure 22 NWA1123Acv3, WAC500 Ports

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

Figure 24 NWA110AX, WAX510D Ports

Figure 25 WAX640S-6E Ports

Figure 26 WBE660S Ports

Figure 27 WAC500H Ports

Figure 28 WAX300H Ports

Figure 29 NWA130BE, WBE530, WBE630S, NWA210BE Ports

Figure 30 WBE510D, NWA110BE Ports

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

Table 14 Ports and Buttons

LABEL	DESCRIPTION
UPLINK	Connect the port to a router, a switch, or another access point (AP) to connect the Zyxel Device to the backbone of your network.
LAN	Connect computers or other Ethernet devices to Ethernet ports for Internet access.
CONSOLE	You can use the console port to manage the Zyxel Device using CLI commands. You will be prompted to enter your user name and password. See the Command Reference Guide for more information about the CLI. When configuring using the console port, you need a computer equipped with communications software configured to the following parameters: • Speed 115200 bps • Data Bits 8 • Parity None • Stop Bit 1 • Flow Control Off
RESET	Press the button for more than 5 seconds to return the Zyxel Device to the factory defaults.
POWER	Connect the power adapter and press the **ON/OFF** button to start the device

3.4.1 Ways to Reset a Zyxel Device without a Reset Button

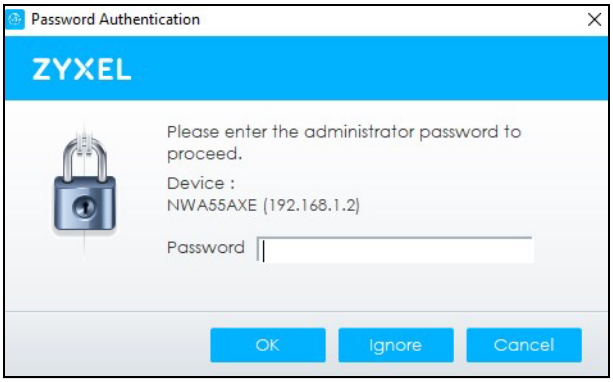
You can use the following ways to reset a Zyxel Device without a reset button to its factory default settings.

ZON Utility

1 Open the ZON Utility and click the **Clear and rescan** icon to scan for the Zyxel Device you want to reset.

2 Select the device and click the **Reset Configuration to Default** icon.

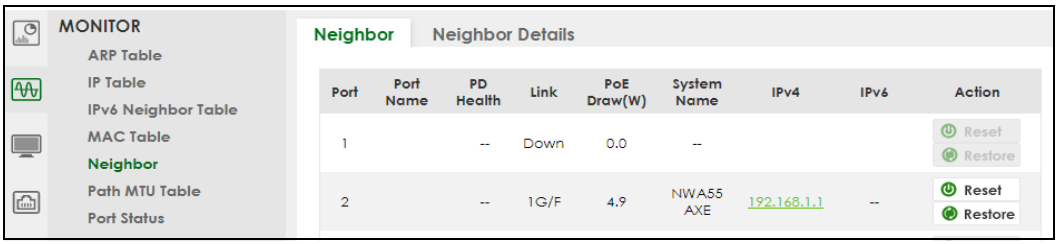
3 Enter the administrator password in the **Password** field on the pop-up screen and click **OK** to start the reset.



Web Configurator of the Zyxel Device Gateway

You can use this method if the Zyxel Device is connected to a Zyxel Switch with a Neighbor Reset function.

1 Log into the Zyxel switch's Web Configurator. Go to **Monitor** > **Neighbor,** and then click the **Restore** button to reset the Zyxel Device to its factory default settings.



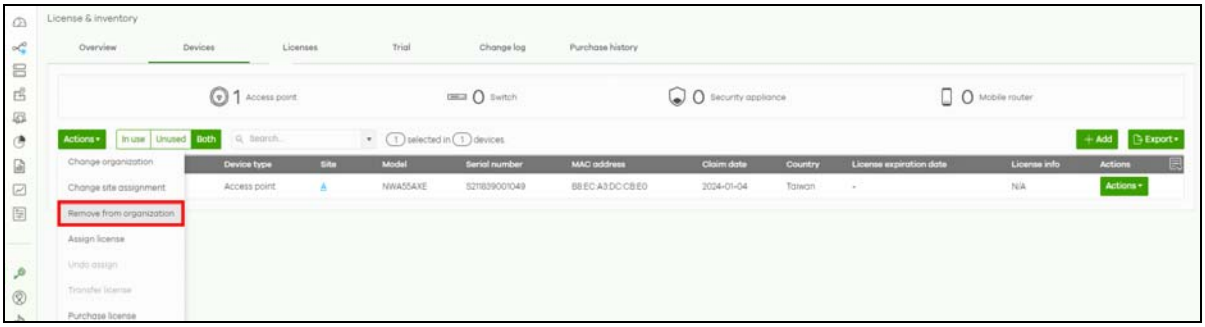
2 A pop-up window asks you to confirm that you want to reset the Zyxel Device to factory default. Click **OK** to proceed with reset. A count down starts.

Nebula Control Center

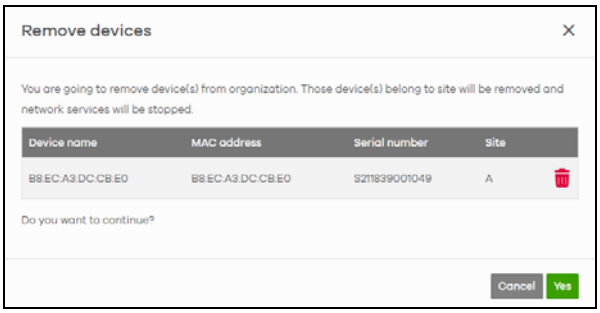
If your Zyxel Device is registered with NCC, you can unregister it to reset it to its factory default settings.

1 Go to **Organization-wide** > **License & inventory** > **Devices** tab in the NCC portal.

2 Select the Zyxel Device you want to remove, then click **Actions** > **Remove from organization**.



3 Click the **Yes** button to confirm.



CHAPTER 4
Web Configurator

4.1 Overview

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

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

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

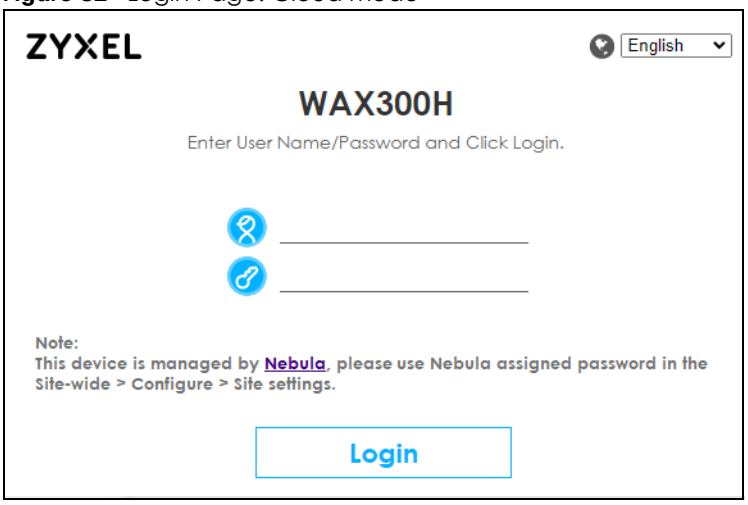
4.2 Accessing the Web Configurator

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

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

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

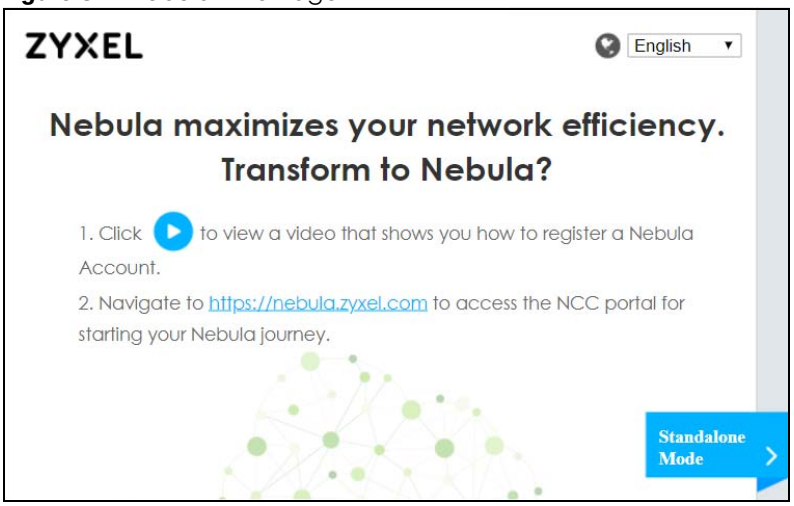
Figure 31 Login Page: Cloud mode



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

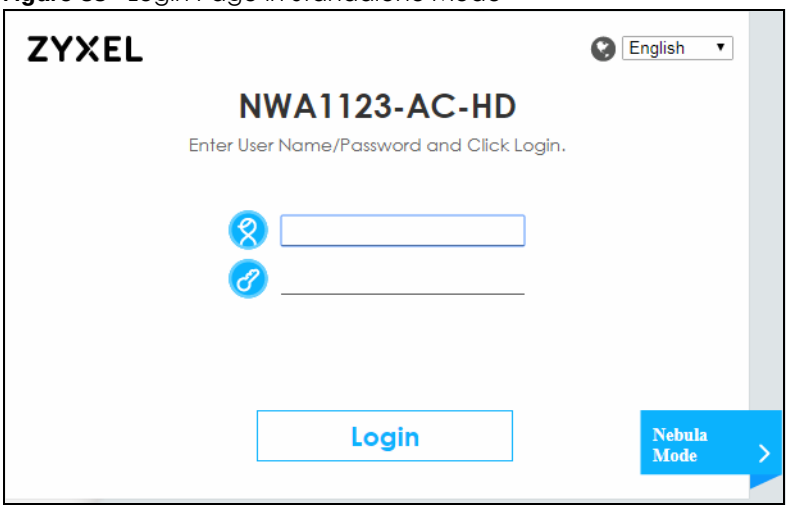
Here, you can watch a tutorial for using the Zyxel Nebula Control Center (NCC) or access the link to the NCC, as shown in the following figure. Otherwise, continue with the next step. The NCC is a cloud-based network management system that allows you to remotely manage and monitor the Zyxel Device (see Section 2.1.2 on page 33)

Figure 32 Nebula Intro Page



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

Figure 33 Login Page in Standalone Mode



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

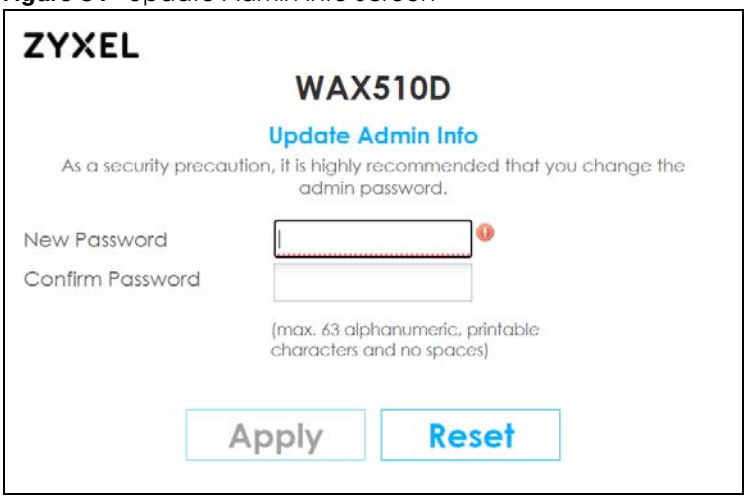
Note: If the Zyxel Device is being managed or has been managed by the NCC, check **Local credentials** in the NCC's **Site-wide > Configure > Site settings** screen for the Zyxel Device's current password.

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

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

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

Figure 34 Update Admin Info Screen



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 35 The Web Configurator's Main Screen for Standalone Mode

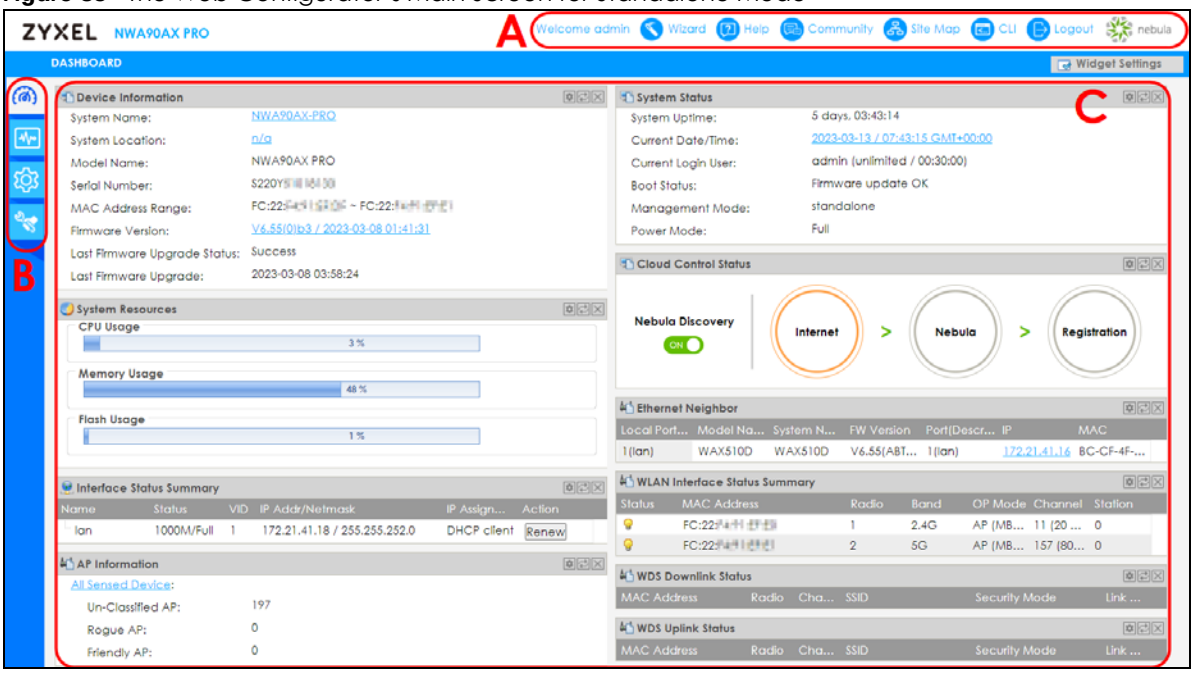
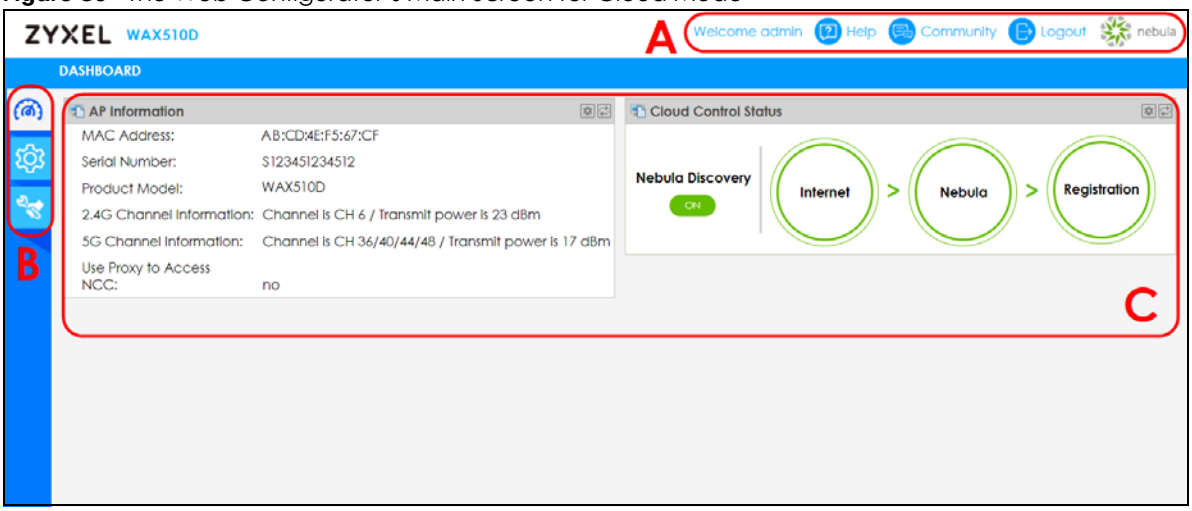


Figure 36 The Web Configurator's Main Screen for Cloud Mode



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.

Figure 37 Title Bar

The icons provide the following functions.

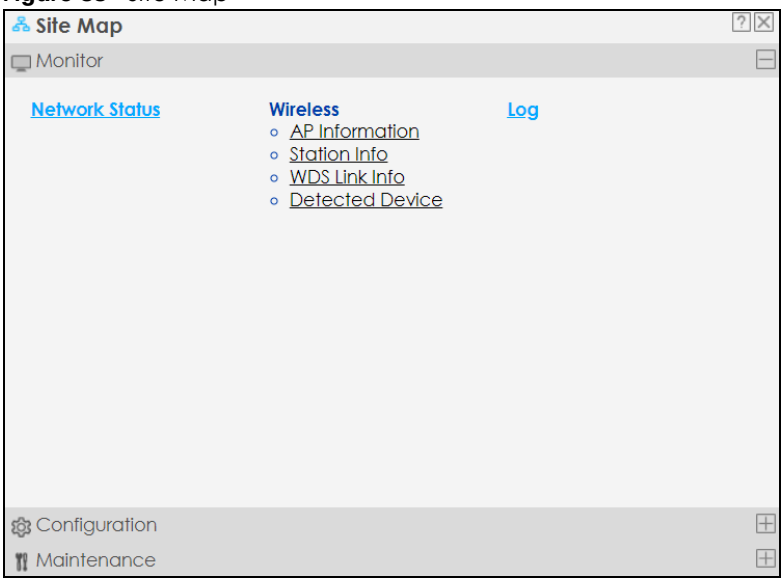
Table 15 Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
Wizard	Click this to open the wizard. See Section 7.1 on page 75 for more information.
Help	Click this to open the help page for the current screen.
Community	Click this to log into the Zyxel forum to post questions, contribute to a discussion and get feedback on Zyxel Device.
Site Map	Click this to see an overview of links to the Web Configurator screens.
CLI	Click this to open a popup window that displays the CLI commands sent by the Web Configurator.
Logout	Click this to log out of the Web Configurator.
nebula	Click this to open the NCC web site login page in a new tab or window.

Site Map

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

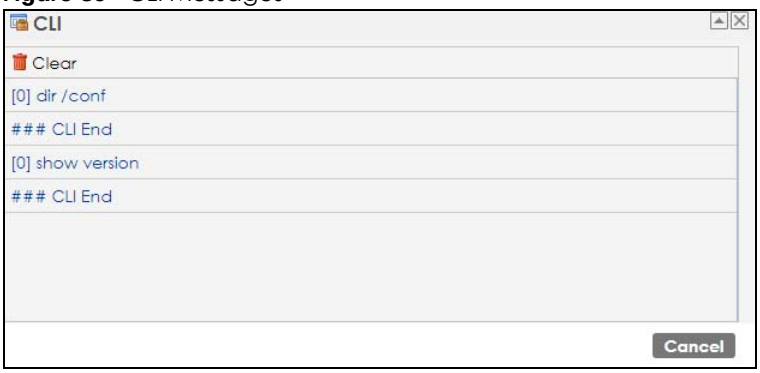
Figure 38 Site Map



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 39 CLI Messages



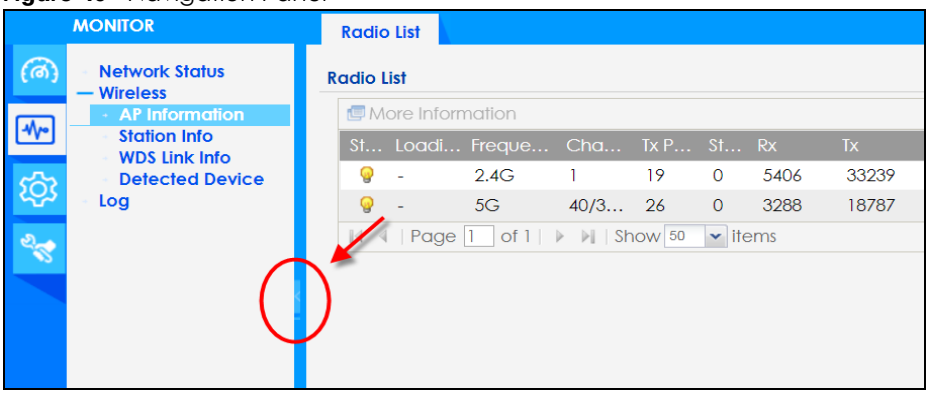
Click **Clear** to remove the currently displayed information.

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 40 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 1.2 on page 14 to see which features your Zyxel Device model supports.

Dashboard

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

For details on the Dashboard's features, see Chapter 6 on page 69.

Monitor Menu

The monitor menu screens display status and statistics information.

Table 16 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 17 Configuration Menu Screens Summary

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

Table 17 Configuration Menu Screens Summary (continued)

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

Maintenance Menu

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

Table 18 Maintenance Menu Screens Summary

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

4.3.4 Cloud Mode Navigation Panel Menus

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

Dashboard

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

For details on the Dashboard's features, see Chapter 24 on page 281.

Configuration Menu

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

Table 19 Configuration Menu Screens Summary

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

Maintenance Menu

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

Table 20 Maintenance Menu Screens Summary

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

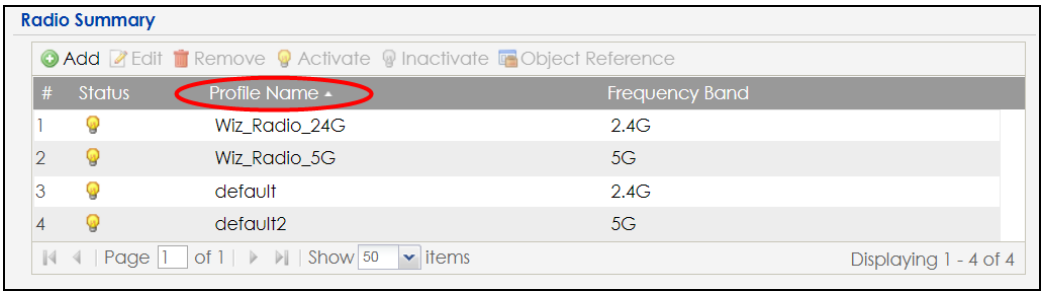
4.3.5 Tables and Lists

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

4.3.5.1 Manipulating Table Display

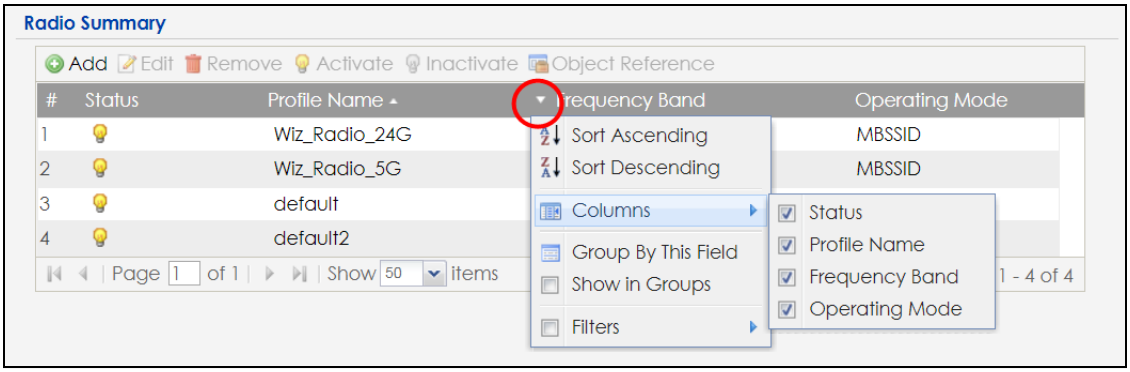
Here are some of the ways you can manipulate the Web Configurator tables.

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

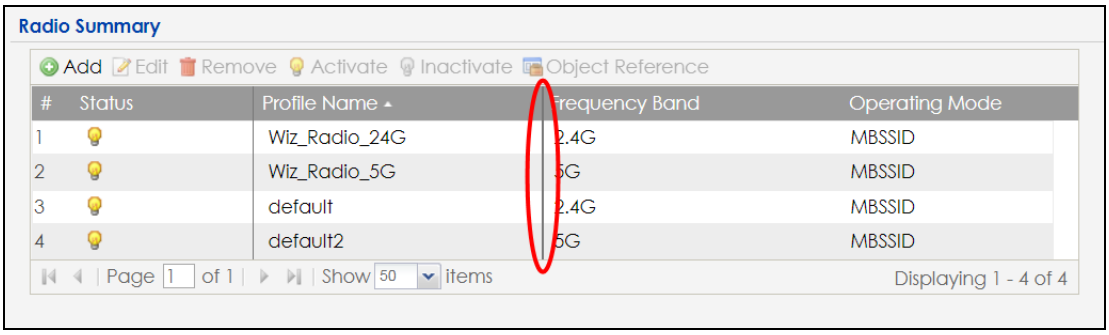


2 Click the down arrow next to a column heading for more options about how to display the entries. The options available vary depending on the type of fields in the column. Here are some examples of what you can do:

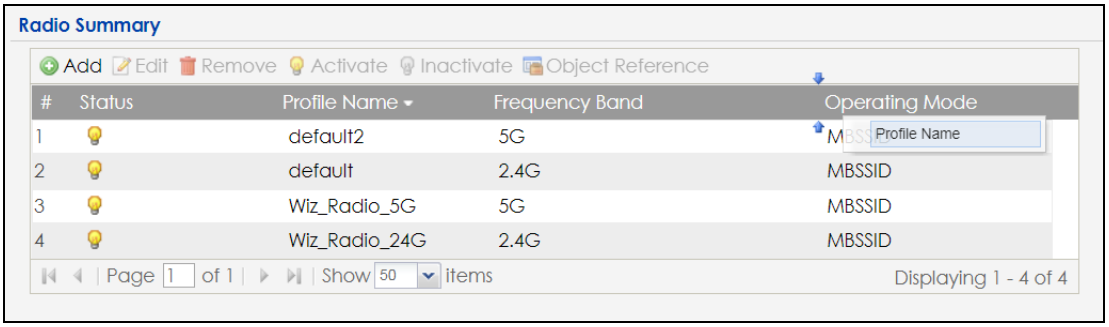
- Sort in ascending alphabetical order
- Sort in descending (reverse) alphabetical order
- Select which columns to display
- Group entries by field
- Show entries in groups
- Filter by mathematical operators (<, >, or =) or searching for text.



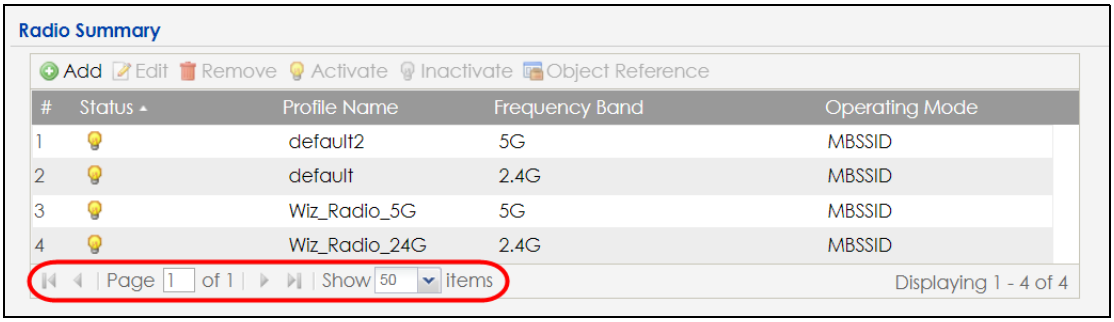
3 Select a column heading cell's right border and drag to re-size the column.



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.



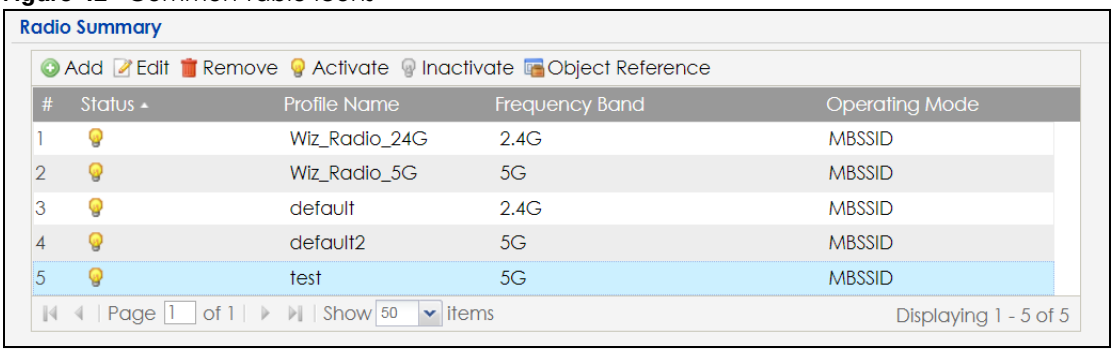
5 Use the icons and fields at the bottom of the table to navigate to different pages of entries and control how many entries display at a time.



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.

Figure 41 Common Table Icons



Here are descriptions for the most common table icons.

Table 21 Common Table Icons

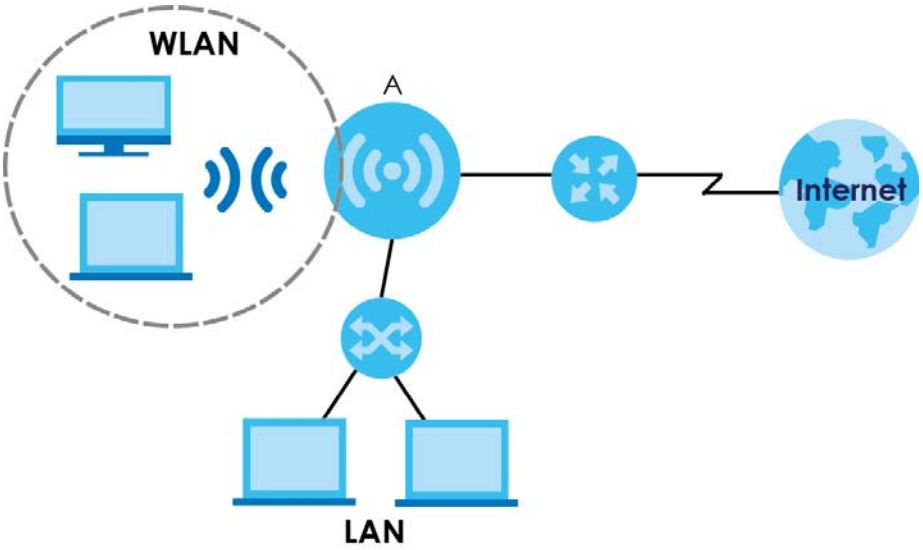
LABEL	DESCRIPTION
Add	Click this to create a new entry. For features where the entry's position in the numbered list is important (features where the Zyxel Device applies the table's entries in order like the firewall for example), you can select an entry and click **Add** to create a new entry after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

PART I
Standalone Configuration

CHAPTER 5
Standalone Configuration

5.1 Overview

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



5.2 Starting and Stopping the Zyxel Device

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

Table 22 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 22 Starting and Stopping the Zyxel Device (continued)

METHOD	DESCRIPTION
Using the **RESET** button	If you press the **RESET** button on the back of the Zyxel Device, the Zyxel Device sets the configuration to its default values and then reboots. See Section 27.6 on page 304 for more information. Note: Some models do not have a **RESET** button due to feature differences.
Disconnecting the power	Power off occurs when you turn off the power to the Zyxel Device. The Zyxel Device simply turns off. It does not stop the system processes or write cached data to local storage.

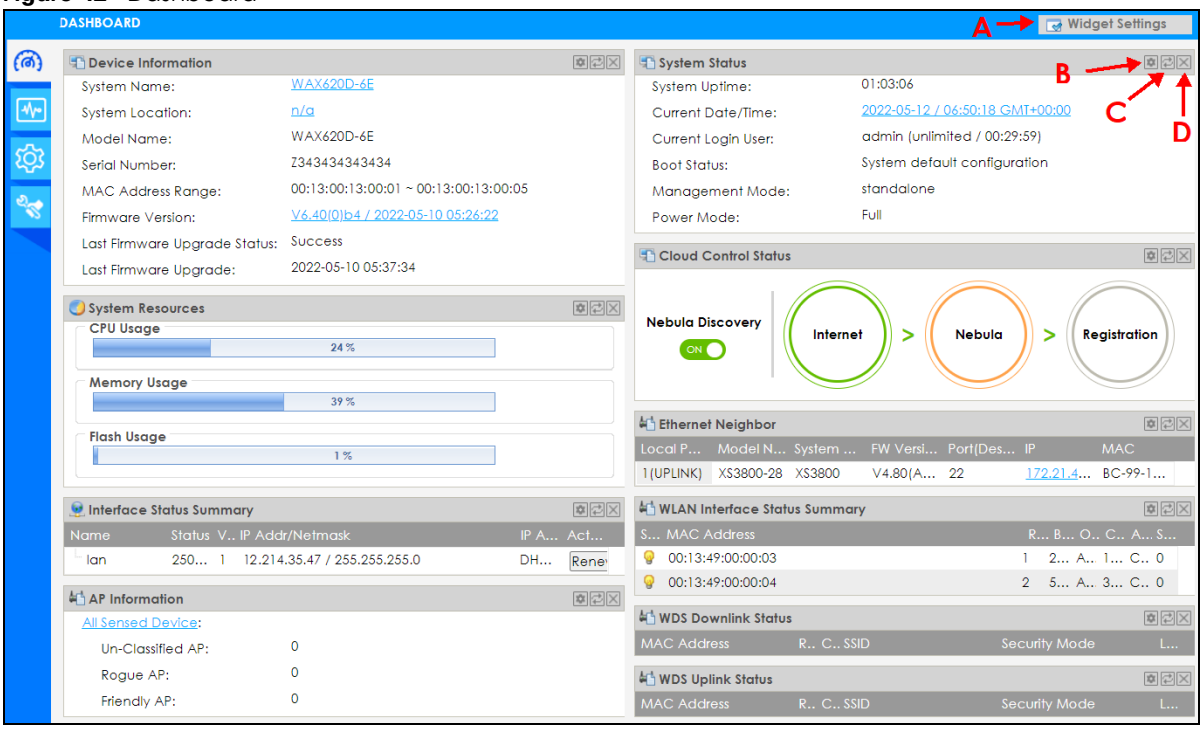
The Zyxel Device does not stop or start the system processes when you apply configuration files or run shell scripts although you may temporarily lose access to network resources.

CHAPTER 6
Dashboard

6.1 Overview

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

Figure 42 Dashboard



The following table describes the labels in this screen.

Table 23 Dashboard

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

Table 23 Dashboard (continued)

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

Table 23 Dashboard (continued)

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

Table 23 Dashboard (continued)

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

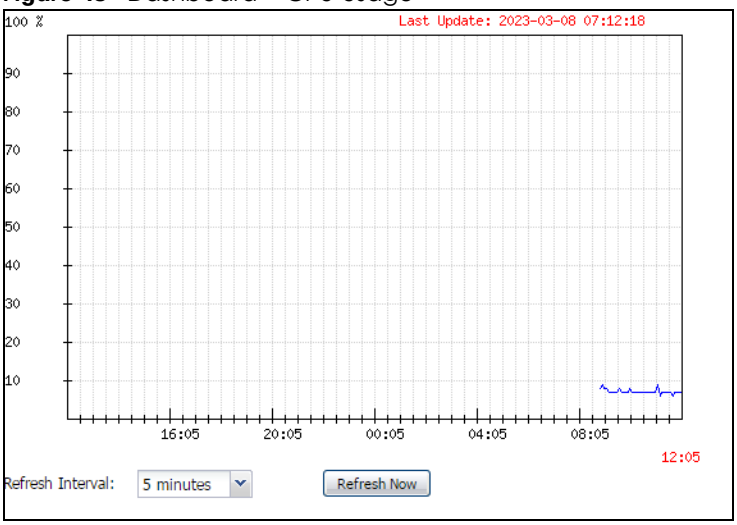
Table 23 Dashboard (continued)

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

6.1.1 CPU Usage

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

Figure 43 Dashboard > CPU Usage



The following table describes the labels in this screen.

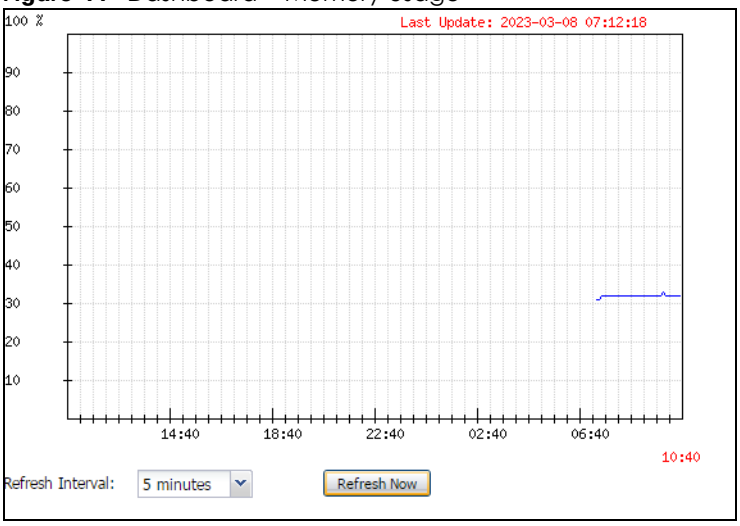
Table 24 Dashboard > CPU Usage

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 44 Dashboard > Memory Usage



The following table describes the labels in this screen.

Table 25 Dashboard > Memory Usage

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

CHAPTER 7
Setup Wizard

7.1 Accessing the Wizard

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

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

7.2 Using the Wizard

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

7.2.1 Step 1 Time Settings

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

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

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

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

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

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

Figure 45 Wizard: Time Settings

Figure 46 Wizard: Time Settings (with **Country** option)

7.2.2 Step 2 Password and Uplink Connection

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

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

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

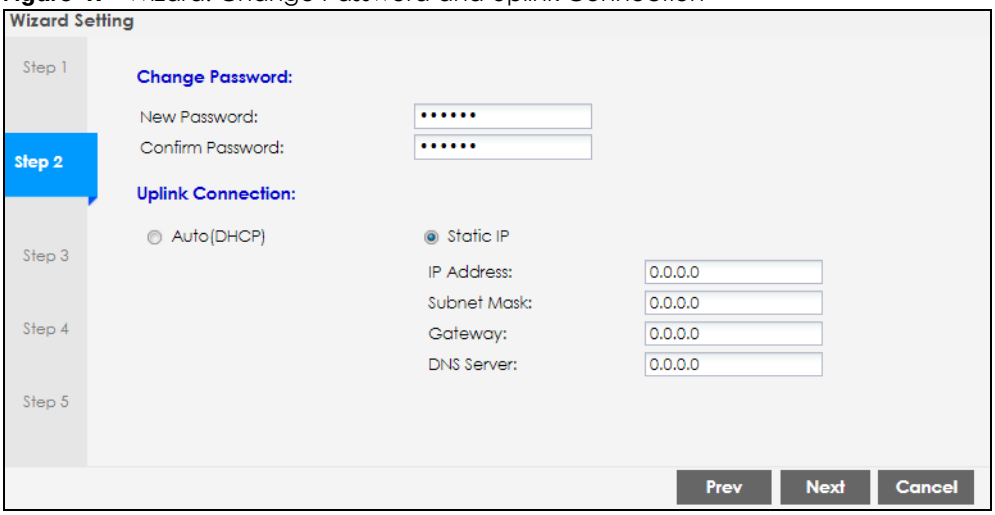
Otherwise, select **Static IP** when the Zyxel Device is NOT connected to a router or you want to assign it a fixed IP address. You will need to manually enter:

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

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

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

Figure 47 Wizard: Change Password and Uplink Connection



7.2.3 Step 3 SSID

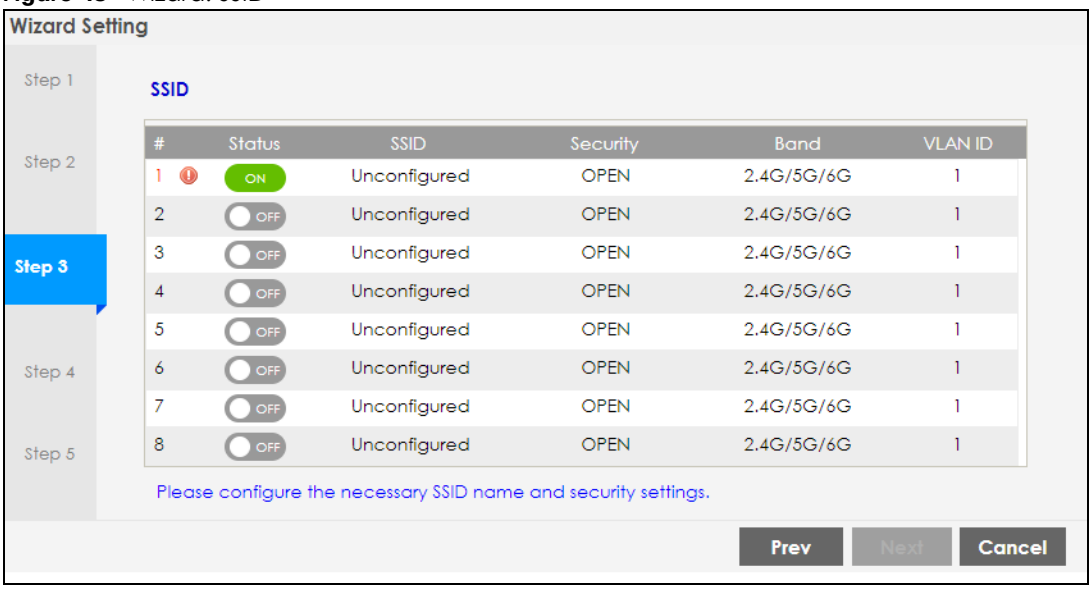
Use this screen to enable, disable or edit an SSID profile.

Select an SSID profile and click the **Status** switch to turn it on or off. To change an SSID profile's settings, such as the SSID (WiFi network name) and WiFi password, double-click the SSID profile entry from the list. See Section 7.2.3.1 on page 78 for more information.

Note: You must configure an SSID to continue.

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

Figure 48 Wizard: SSID



7.2.3.1 Edit SSID Profile

Use this screen to configure an SSID profile.

The screen varies depending on the security type you selected.

- **SSID**: Enter a descriptive name of up to 32 printable characters for the wireless LAN.
- **Status**: Select **Active** to apply this SSID profile on all the radios. Select **Inactive** to create the SSID profile without applying this SSID on any radio.
- **VLAN ID**: Enter a VLAN ID for the Zyxel Device to use to tag traffic originating from this SSID.
- **Band Mode**: Select the WiFi band which this profile should use. 2.4 GHz is the frequency used by IEEE 802.11b/g/n/ax WiFi clients. 5 GHz is the frequency used by IEEE 802.11a/n/ac/ax WiFi clients. 6 GHz is the frequency used by IEEE 802.11ax WiFi clients.
- **Security Type**: Select **WPA2** or **WPA3** to add security on this WiFi network. Otherwise, select **OPEN** or **Enhanced-Open** to allow any WiFi client to associate this network without authentication.
- **Personal**: If you set **Security Type** to **WPA2** or **WPA3** and select **Personal**, enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
- **Enterprise**: Select this option and the **Primary / Secondary RADIUS Server** checkbox to have the Zyxel Device use the specified RADIUS server. You have to enter the IP address, port number and shared secret password of the RADIUS server to be used for authentication.

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

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

Figure 49 Wizard: SSID: Edit (WPA2-Personal)

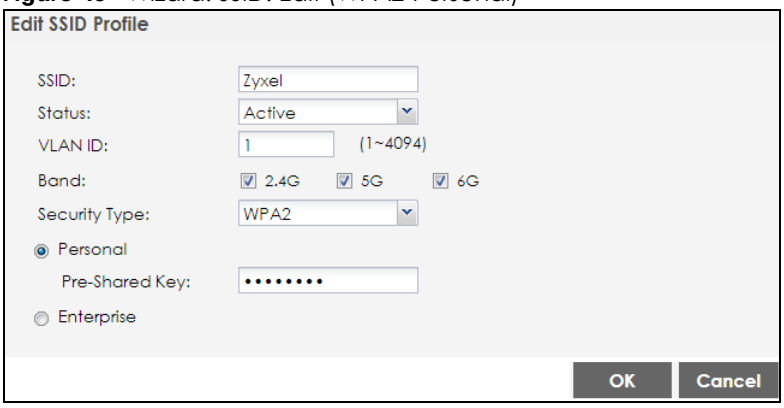
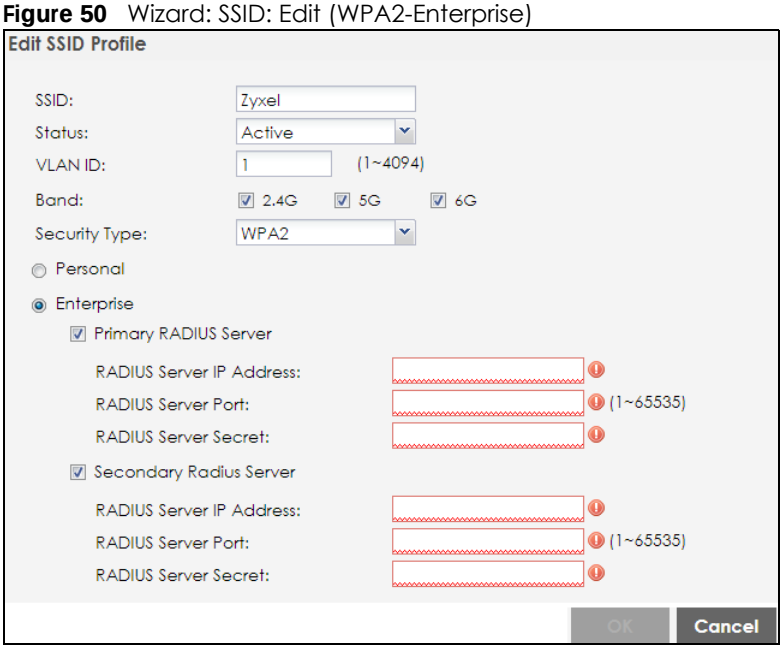


Figure 50 Wizard: SSID: Edit (WPA2-Enterprise)



7.2.4 Step 4 Radio

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

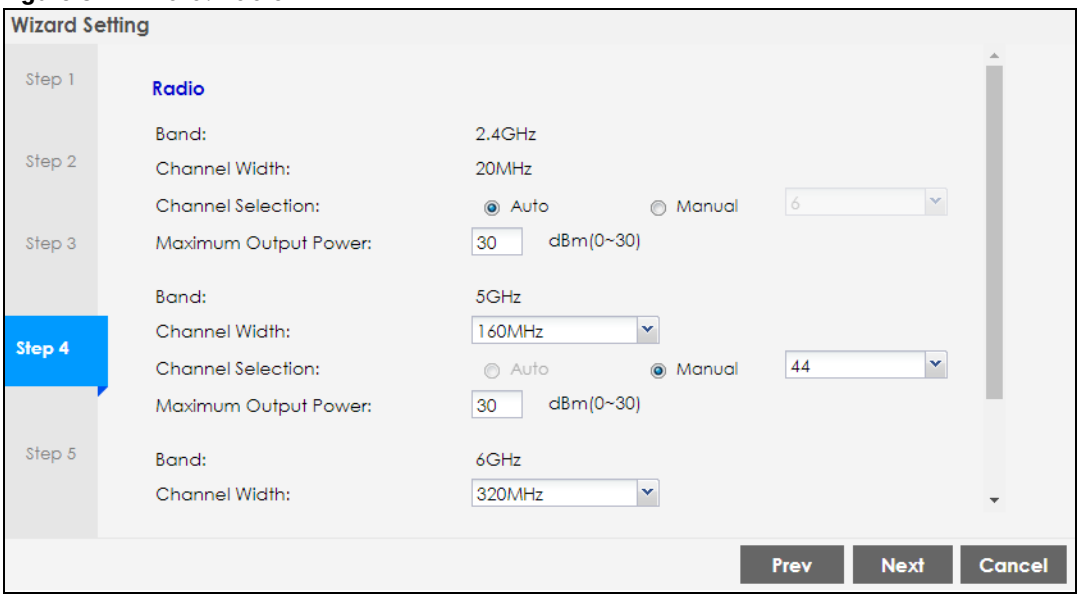
- **Band**: Select the radio band you want to use on this radio. The radio band is unconfigurable if the Zyxel Device does not support BandFlex (band selection on each radio). See Section 1.2 on page 14.
- **Channel Width**: Select the channel bandwidth list you want to use on this radio. The Zyxel Device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

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

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

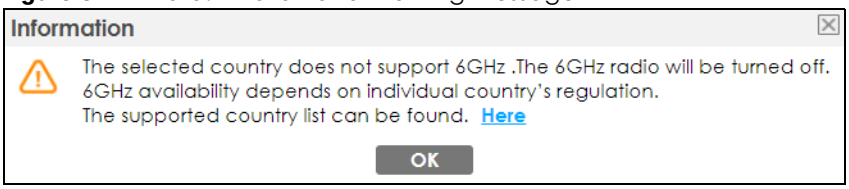
Click **Prev** to return to the previous screen. Click **Next** to proceed. Click **Cancel** to close the wizard without saving.

Figure 51 Wizard: Radio



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

Figure 52 Wizard: Invalid Band Warning Message



7.2.5 Step 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 53 Wizard: Summary

CHAPTER 8
Getting Started

8.1 Getting Started Overview

This chapter shows you how to use the Zyxel Device's various features.

- WiFi Network Setup - Choose the operation mode and set up a WiFi network.
- Limit Network Bandwidth for Each WiFi Client - Restrict the network bandwidth on a WiFi client.
- Network Security - Change the WiFi security, set up a RADIUS server, a rogue AP list, a friendly AP list, and a MAC filter list, and restrict users' access on the network.
- Device Settings - Change the management IP address, the login password, and the system name.
- Device Maintenance - Upgrade firmware, download and restore the device configuration.
- Log and Report - Set up a daily email report and back up the logs to a remote server.
- Access to the Zyxel Device - Configure ways to access the Zyxel Device.

8.2 WiFi Network Setup

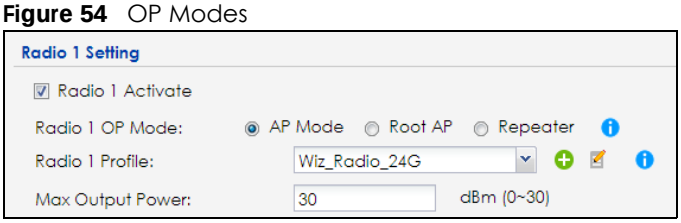
In this section, we show you how to:

- Choose the Operation Mode
- Set Up a WiFi Network in AP Mode
- Set Up a WiFi Network in Root AP/Repeater Mode
- Set Up General and Guest WiFi Networks on Both Radios

8.2.1 Choose the Operation Mode

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

Figure 54 OP Modes



The Zyxel Device supports the following OP modes:

- Choose **AP Mode** if you want WiFi clients to connect to the Zyxel Device.

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

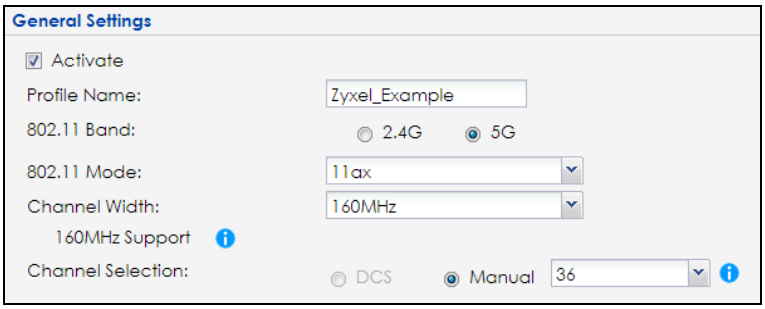
8.2.2 Set Up a WiFi Network in AP Mode

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

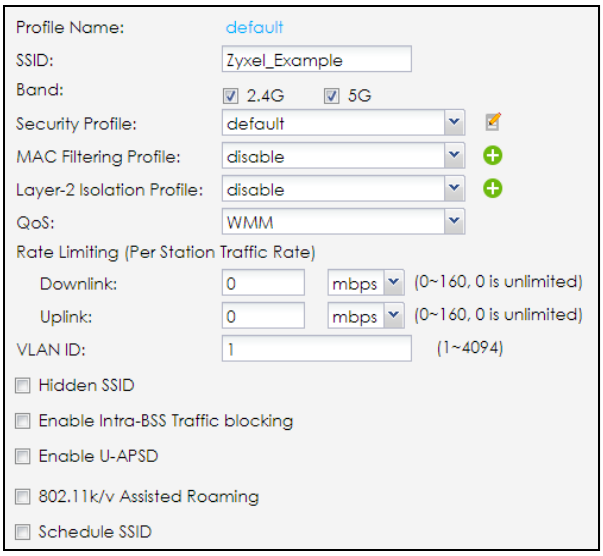
Table 26 SSID Profile Settings Example

	PROFILE
SSID	Zyxel_Example
Channel Selection	36
Security Mode	wpa2
Pre-Shared Key	zyxel1234
802.11 Mode	11ax

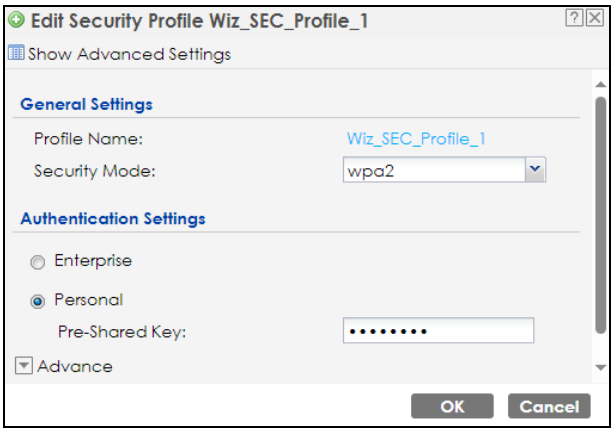
1 Go to **Configuration** > **Object** > **AP Profile** > **Radio** > **Add**. Enter the profile name, select the 802.11 mode and select a channel (36 in this example) that is not used by another AP. Click **OK**.



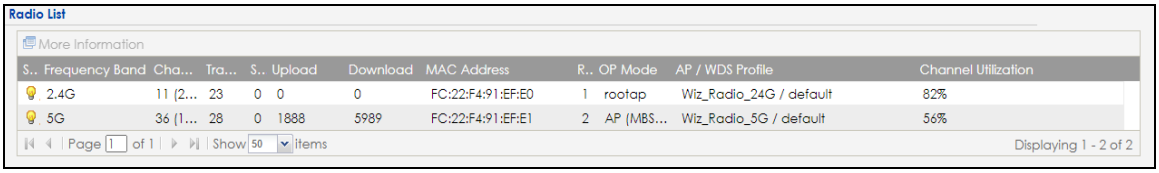
2 Go to **Configuration** > **Object** > **AP Profile** > **SSID** > **SSID List**, select the **default** SSID profile and click **Edit** to configure the SSID settings. Click **OK**.



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



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



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

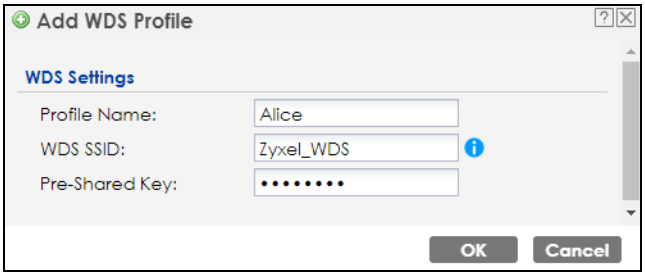
8.2.3 Set Up a WiFi Network in Root AP/Repeater Mode

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

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

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

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



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

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

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

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

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

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

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

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

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

8.2.4 Set Up General and Guest WiFi Networks on Both Radios

The following example shows you how to create two WiFi networks (**Zyxel_General** and **Zyxel_Guest**) using the following settings for both **Radio 1** (2.4 GHz) and **Radio 2** (5 GHz). You should have already created two security profiles, **Security_Profile1** and **Security_Profile2,** on the **Configuration > Object > AP Profile > SSID > Security List** screen. See Section 14.4.2 on page 197 for a tutorial on creating security profiles.

For the Guest WiFi, enable **Enable Intra-BSS Traffic blocking** to prohibit Guest WiFi clients from directly connecting to each other. To separate the **Guest** WiFi network from the **General** internal WiFi network, create two VLANs, **VLAN 10** and **VLAN 20**, on your firewall (**F**), such as ZyWALL. Set the **General** WiFi network to be in **VLAN 10**, where your internal network is. Set the **Guest** WiFi network to be in **VLAN 20.** This way, Guest WiFi clients will not be able to access the wired LAN network of the firewall (**F**) in **VLAN 10** while still able to access the Internet.

Figure 55 General and Guest WiFi Networks

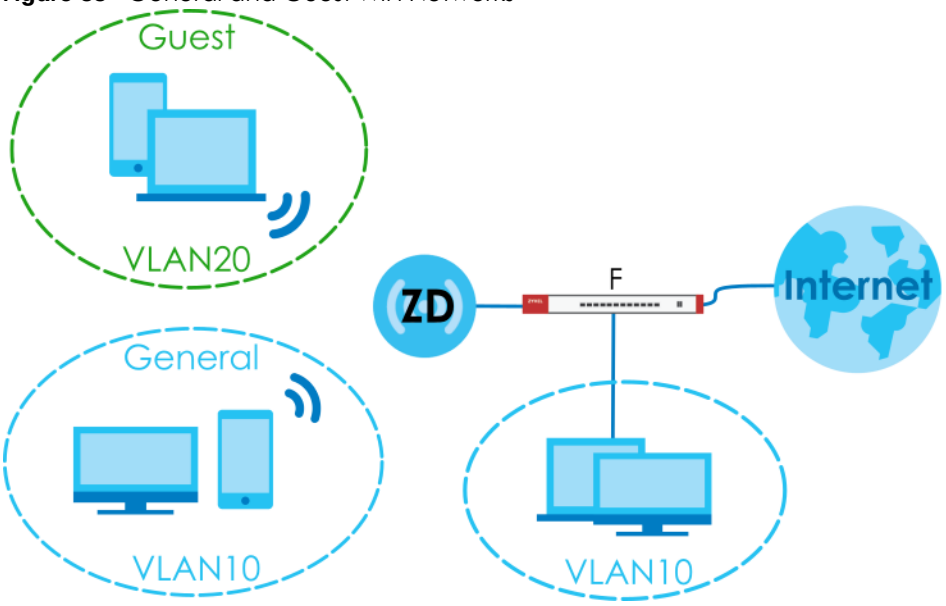
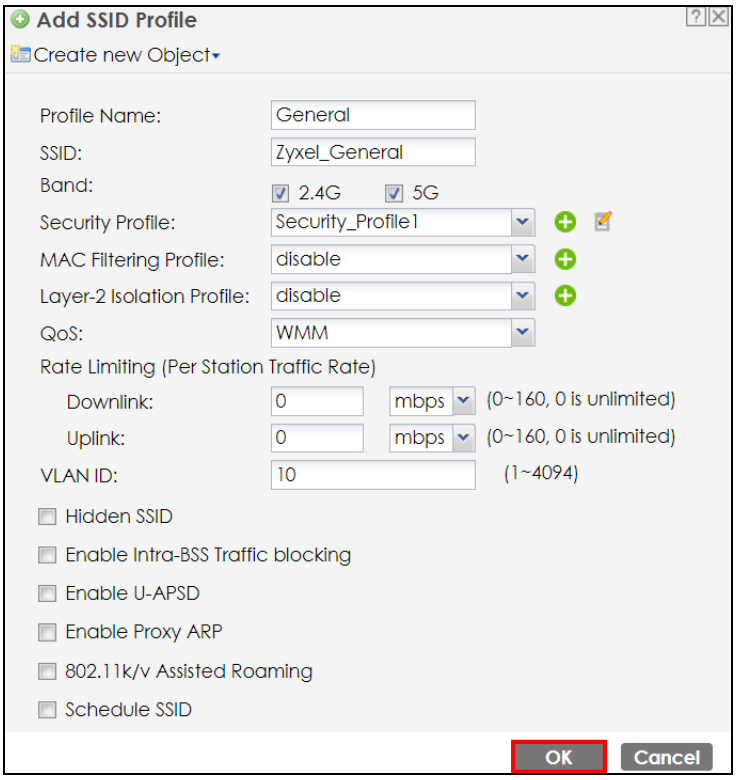


Table 27 General and Guest SSID Profiles

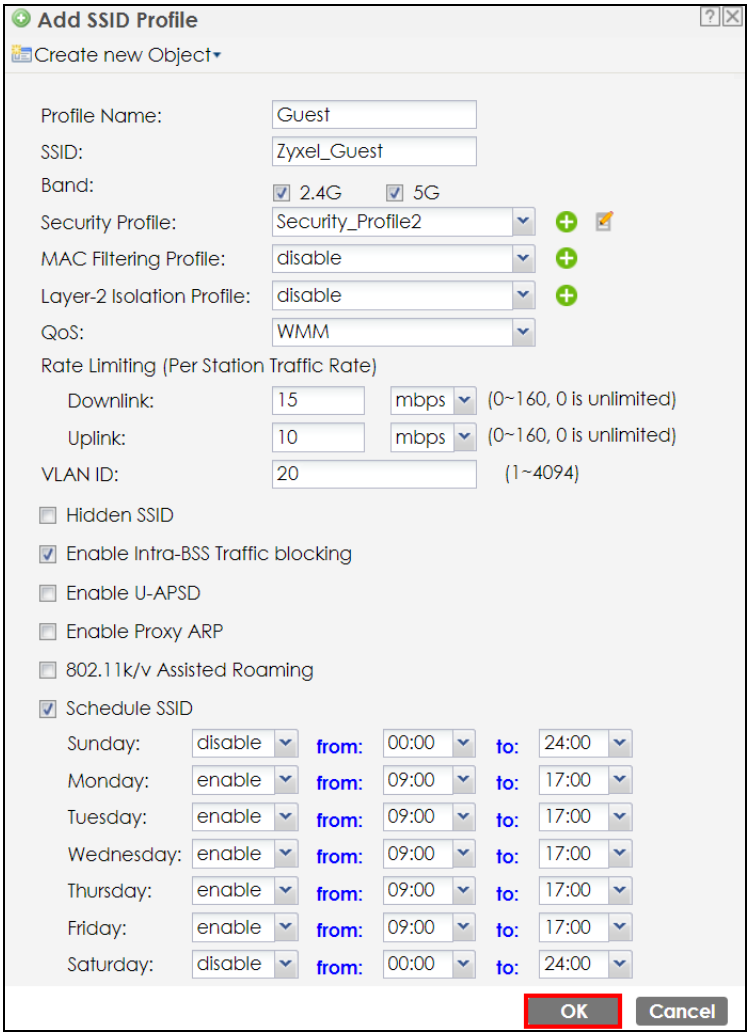
	GENERAL	GUEST
Profile Name	General	Guest
SSID	Zyxel_General	Zyxel_Guest
Band	2.4 GHz/5 GHz	2.4 GHz/5 GHz
Security Profile	Security_Profile1 **Security Mode**: WPA3 **Authentication**: Personal **Pre-Shared Key**: zyxel1234	Security_Profile2 **Security Mode**: WPA3 **Authentication**: Personal **Pre-Shared Key**: guest1234
VLAN ID	10	20
Rate Limiting	0 (unlimited)	Downlink: Up to 15 Mbps Uplink: Up to 10 Mbps
Enable Intra-BSS Traffic Blocking	Disabled	Enabled
Schedule SSID	No schedule	Monday-Friday: 09:00-17:00

1 Go to **Configuration** > **Object** > **AP Profile** > **SSID** > **SSID List**, click **Add** to create an SSID profile.

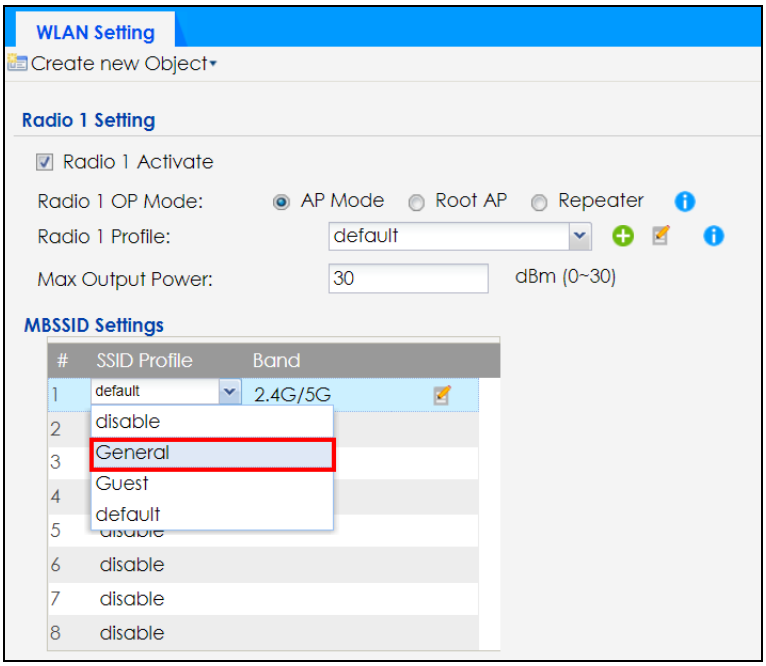
2 Configure the first SSID – **Zyxel_General** using the parameters given above, and then click **OK**.



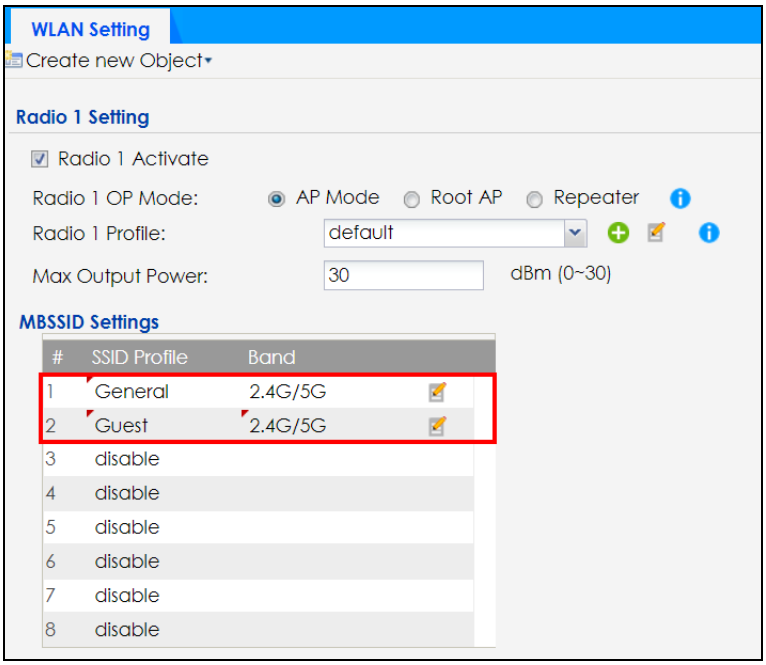
3 Configure the second SSID – **Zyxel_Guest** using the parameters given above, and then click **OK**.



4 Go to **Configuration** > **Wireless** > **AP Management**. Click the first **SSID Profile** of **Radio 1** (2.4 GHz). A drop-down list appears. Select the **General** SSID profile you just configured.



5 Click the second **SSID Profile** and select the **Guest** SSID profile.



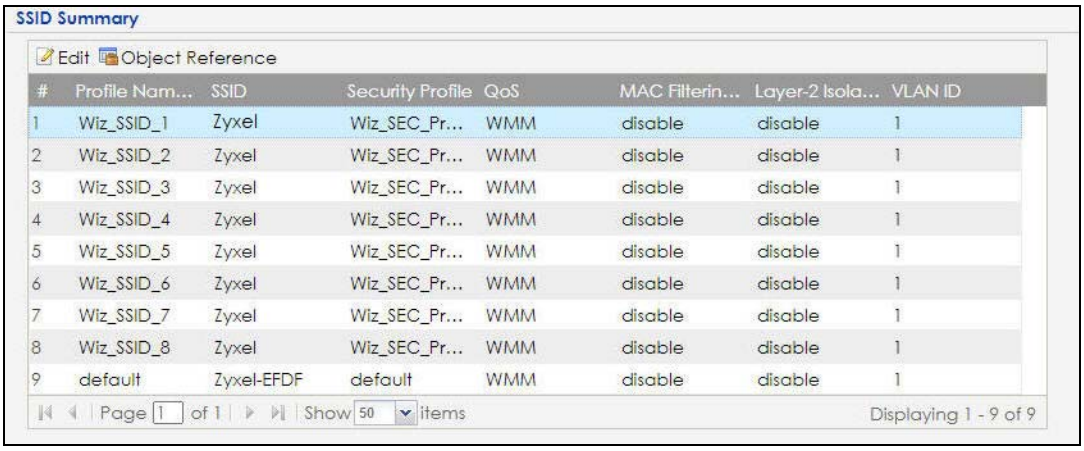
6 Click the first **SSID Profile** of **Radio 2** (5 GHz). A drop-down list appears. Select the **General** SSID profile you just configured. Click the second **SSID Profile** and select the **Guest** SSID profile.

7 Click **Apply** on the bottom of the screen. The **General** and **Guest** SSID profiles are now applied on **Radio 1** and **Radio 2**. You should now be able to see the **Zyxel_General** and **Zyxel_Guest** SSIDs on your WiFi devices for both 2.4 GHz and 5 GHz radio bands. General WiFi users can access the Internet and your local network. Guest users can only access the Internet.

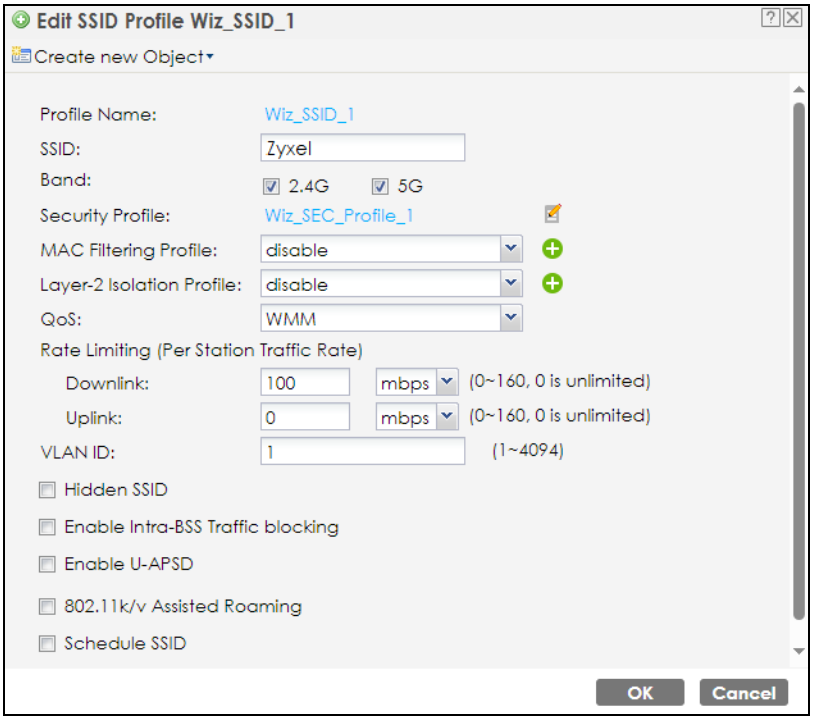
8.3 Limit Network Bandwidth for Each WiFi Client

Restricting network bandwidth for each WiFi client ensures that all clients have equitable access to the network, preventing a few WiFi clients from monopolizing the bandwidth.

1 Go to **Configuration** > **Object** > **AP Profile** > **SSID** > **SSID List**, select a profile and click **Edit**.



2 Enter the maximum transmission data rate (either in Mbps or Kbps) for each WiFi client in the **Downlink** field.



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

8.4 Network Security

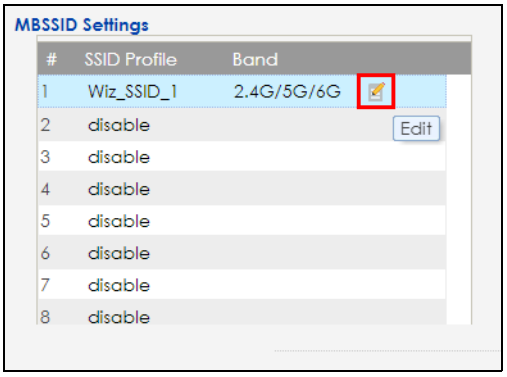
In this section, we show you how to:

- Change Security for a WiFi Network
- RADIUS Server Setup
- Set Up Rogue AP Detection
- Set Up a Friendly AP List
- Set Up a MAC Filter List
- Restrict Users' Access to Specific Parts of Your Network
- Test Your WiFi Access Restrictions

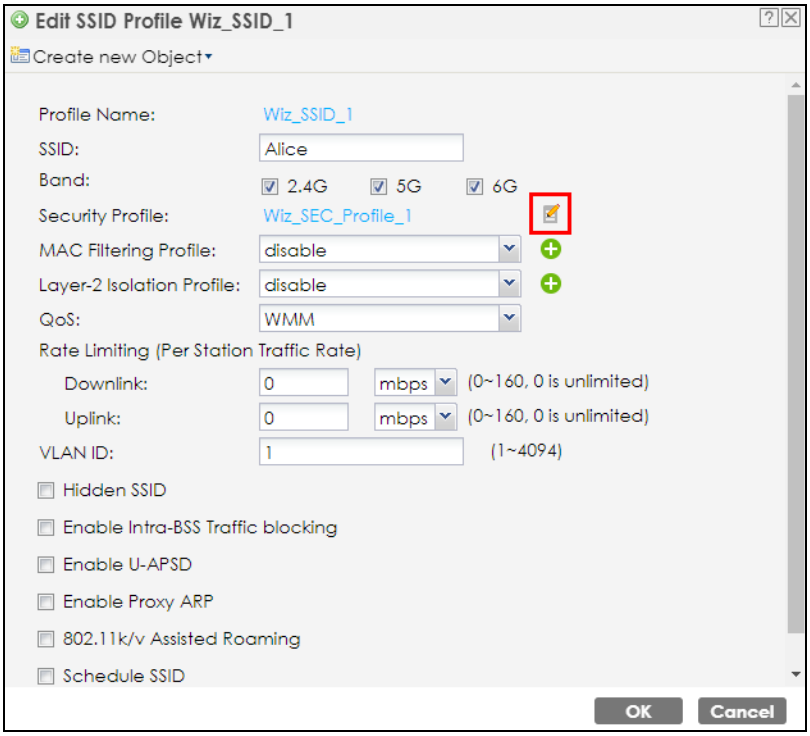
8.4.1 Change Security for a WiFi Network

Changing the security settings on a WiFi network enhances protection by blocking unauthorized client devices. This option is ideal for small WiFi networks with a few WiFi clients. For WiFi networks with a lot of clients, see Section 8.4.2 on page 92 for more information.

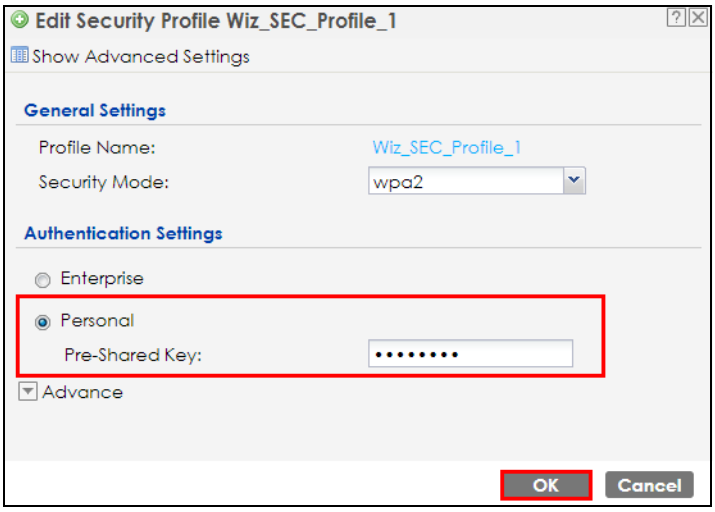
1 Go to the **Configuration** > **Wireless** > **AP Management** > **WLAN Setting** screen. Click **Edit** under the SSID profile to change the WiFi security.



2 The following screen appears, click the **Edit** icon next to **Security Profile**.



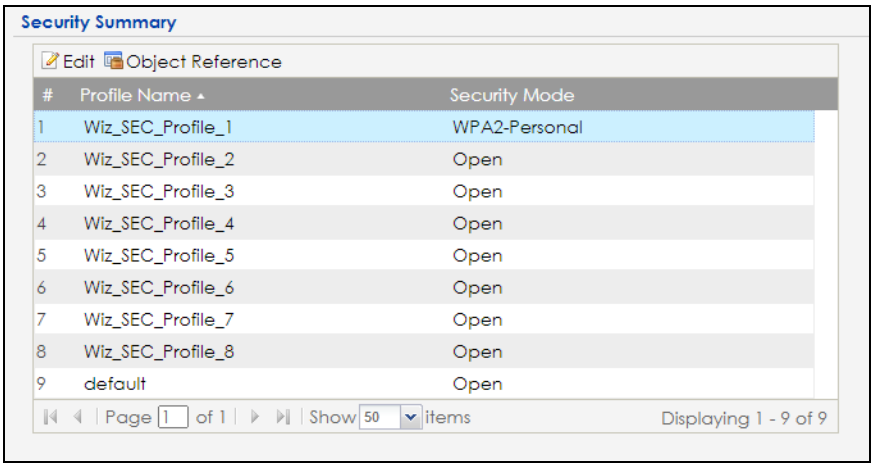
3 The following screen appears, select **Personal** and enter a pre-shared key from 8 to 63 case-sensitive keyboard characters in **Pre-Shared Key**. Click **OK** to save your changes.



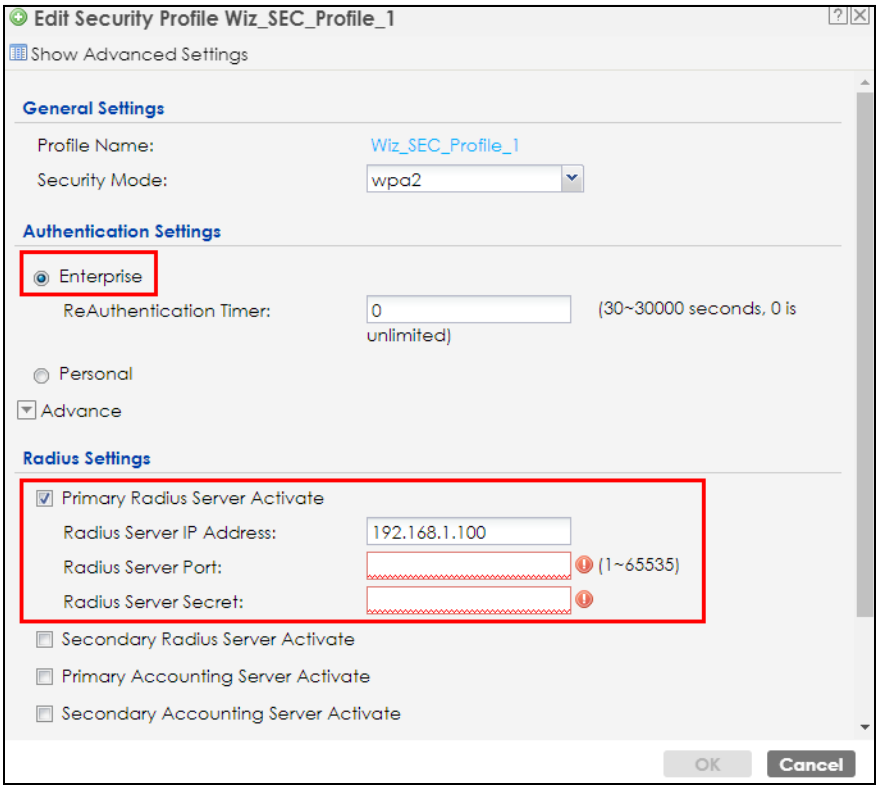
8.4.2 RADIUS Server Setup

Setting up a RADIUS server on your Zyxel Device allows centralized user authentication and authorization, which enhances network security. This option is ideal for enterprise users who need to manage many WiFi clients.

1 Go to the **Configuration** > **Object** > **AP Profile** > **SSID** > **Security List** screen. Select a profile you want to configure for the RADIUS server and click **Edit**.



2 Set **Authentication Settings** to **Enterprise** to configure the RADIUS server. Enter the RADIUS server's IP address, port number and secret. The **Radius Server Secret** must match the secret on the RADIUS server client. Click **OK** to save your changes.



8.4.3 Set Up Rogue AP Detection

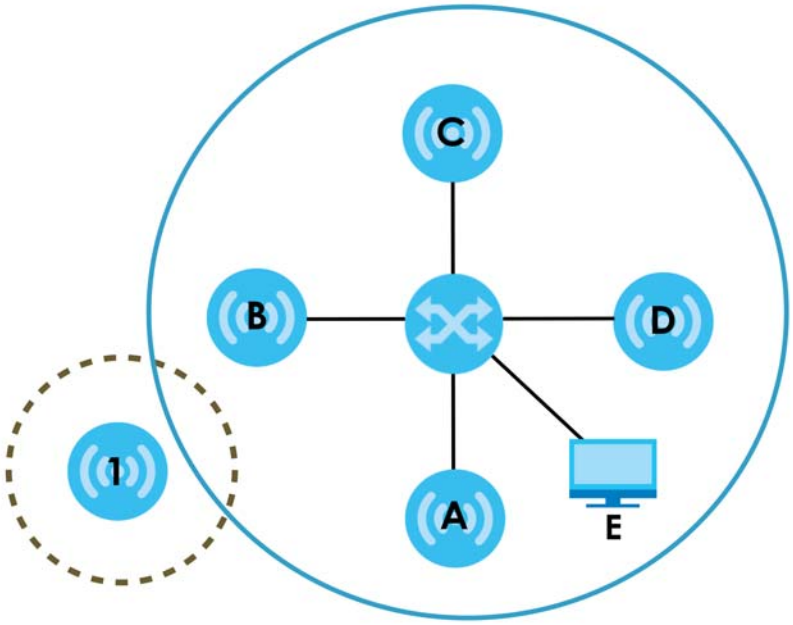
This example shows you how to configure the rogue AP detection feature on the Zyxel Device. A rogue AP is a WiFi access point operating in a network's coverage area that is not a sanctioned part of that network. See Section 11.3 on page 144 for background information on the rogue AP function and security considerations.

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

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

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

Figure 56 WiFi Network Example



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

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

Table 28 Rogue AP Example Information

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

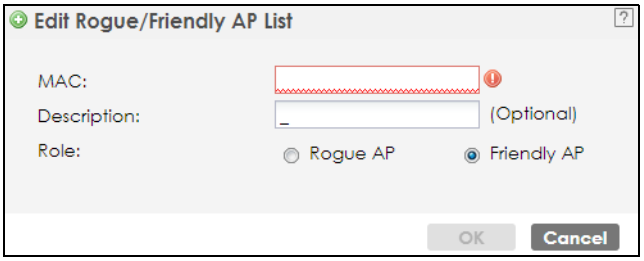
Note: You can detect the MAC addresses of other APs in the **Monitor > Wireless > Detected Device** screen. However, it is more secure to obtain the correct MAC addresses from another source and add them to the friendly AP list manually. For example, an attacker's AP mimicking the correct SSID could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

8.4.4 Set Up a Friendly AP List

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

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

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

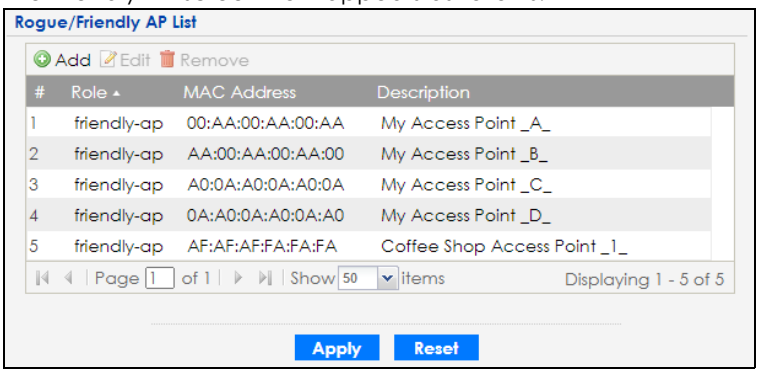


2 Fill in the **MAC** and **Description** fields as in the following table. Click **Add** after you enter the details of each AP to include it in the list.

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

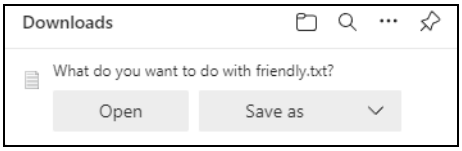
Note: You can add APs that are not part of your network to the friendly AP list, as long as you know that they do not pose a threat to your network's security.

The Friendly AP screen now appears as follows.

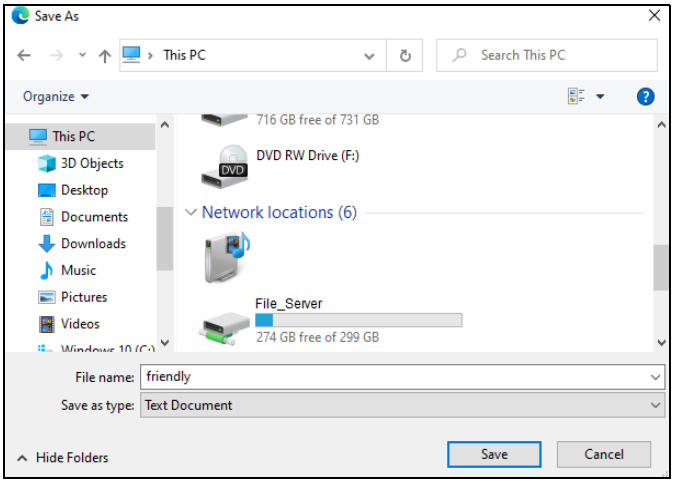


3 Next, click **Apply** to save the list of friendly APs in order to provide a backup and upload it to your other access points.

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



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



8.4.4.1 Import the Friendly AP List to Other APs

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

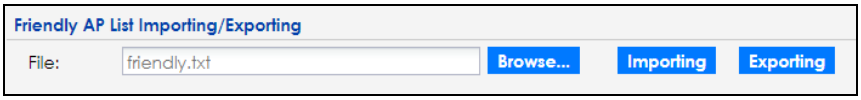
- Scan for access points in its coverage area
- Recognize friendly access points from a list

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

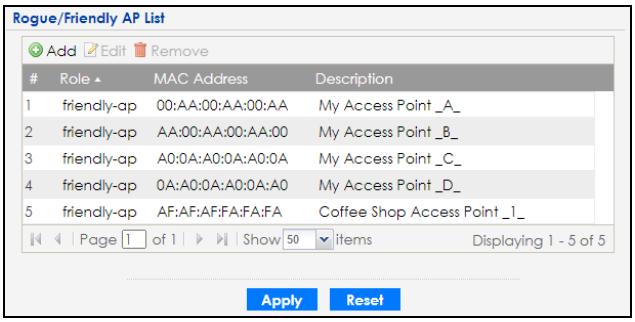
For each access point, take the following steps.

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

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



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

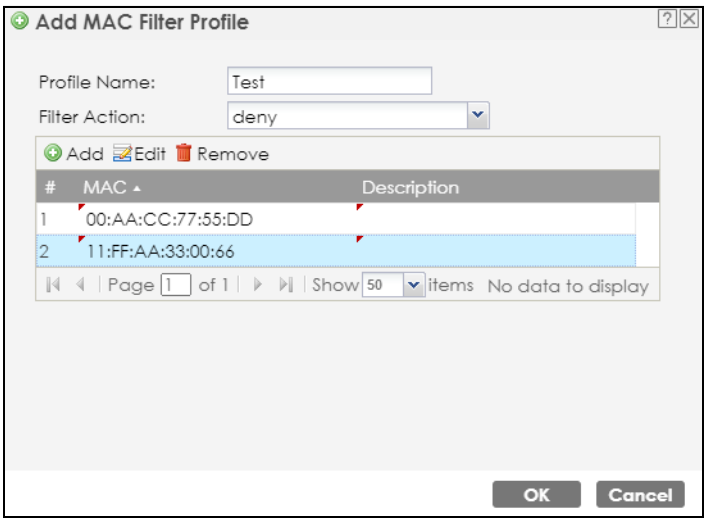


8.4.5 Set Up a MAC Filter List

A MAC filter list blocks or allows a list of clients based on their MAC addresses, ensuring only authorized clients can access the network. This example shows how to block certain clients based on their MAC addresses.

1 Go to **Configuration** > **Object** > **AP Profile** > **SSID** > **MAC Filter List** and then click **Add**.

2 Fill in the **Profile Name** and select **deny** for **Filter Action.** Click **Add** to add a new MAC address to block. Enter the MAC addresses of the clients you want to block under the **MAC** field and then click **OK**.



8.4.6 Restrict Users' Access to Specific Parts of Your Network

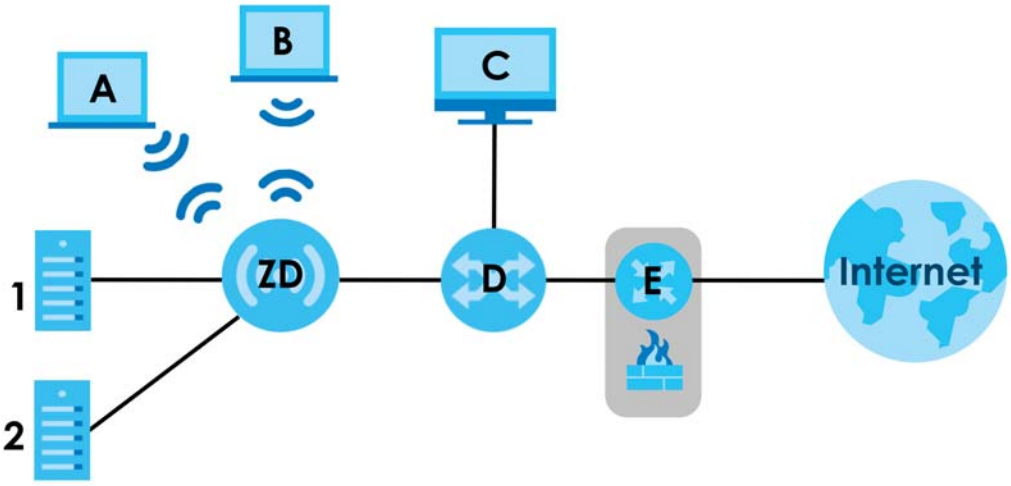
This example shows you how to allow certain users to access only specific parts of your network. You can do this by using multiple MAC filters and layer-2 isolation profiles.

8.4.6.1 Scenario

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

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

Figure 57 Getting Started: Example Network



8.4.6.2 Your Requirements

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

8.4.6.3 Setup

In this example, you have already set up the Zyxel Device in **AP Mode** (see Chapter 8 on page 82). It uses two SSID profiles simultaneously. You have configured each SSID profile as shown in the following table.

Table 29 SSID Profile Security Settings

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

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

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

1 Configure the SERVER_1 network's SSID profile to use specific MAC filter and layer-2 isolation profiles.

2 Configure the SERVER_1 network's MAC filter profile.

3 Configure the SERVER_1 network's layer-2 isolation profile.

4 Repeat steps 1 to step 3 for the SERVER_2 network.

5 Check your settings and test the configuration.

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

Table 30 Getting Started: Example Network MAC Addresses

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

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

Table 31 Example User MAC Addresses

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

8.4.6.4 Configure the SERVER_1 Network

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

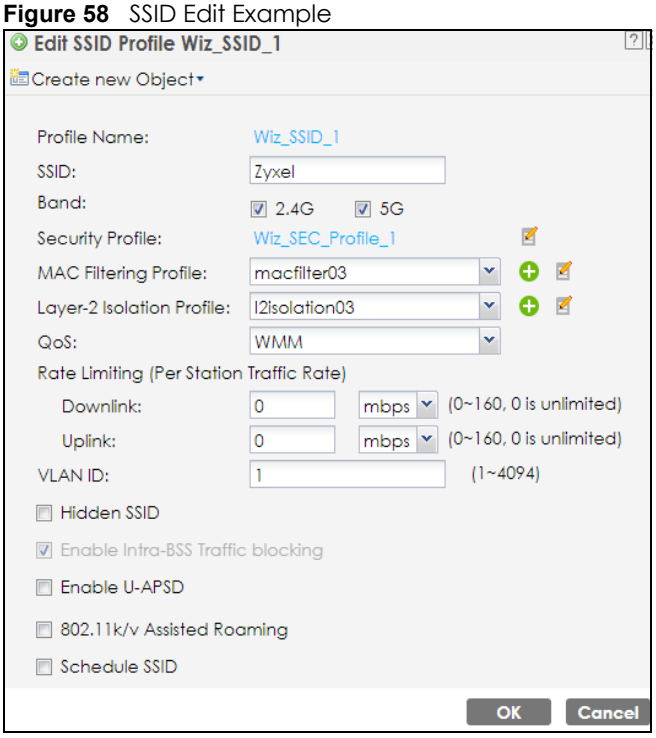
You will configure the MAC filter to restrict access to Alice alone, and then configure layer-2 isolation to allow her to access only the network router, the file server and the Internet security gateway.

Take the following steps to configure the SERVER_1 network.

1 Go to **Configuration** > **Object** > **AP Profile** > **SSID** > **SSID List**. The following screen displays, showing the SSID profiles you already configured. Select **SERVER_1**'s entry and click **Edit**.

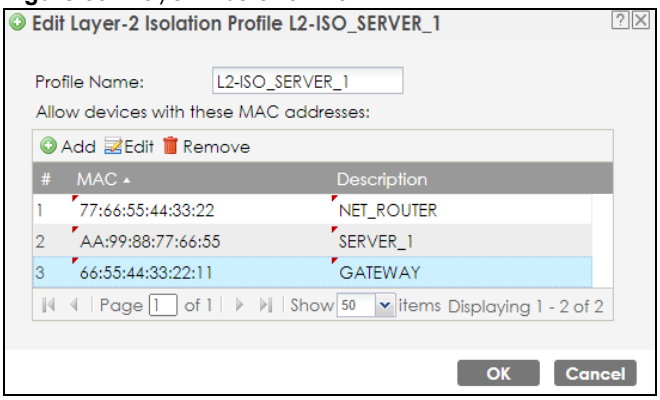
2 The following screen appears. Select **l2Isolation03** for **Layer-2 Isolation Profile**, and select **macfilter03** for **MAC Filtering Profile**. Click **OK**.

Figure 58 SSID Edit Example



3 Click the **Layer-2 Isolation List** tab. Select the **l2Isolation03**'s entry and click **Edit**. The following screen displays.

Figure 59 Layer-2 Isolation Edit



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

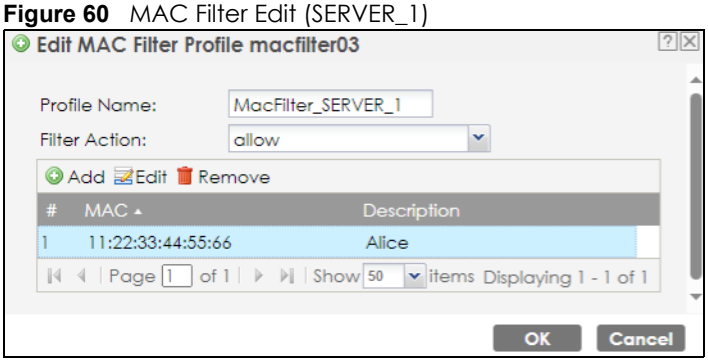
5 Enter server 1's MAC Address and add a Description ("SERVER_1" in this case) in Set 2's entry.

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

7 Go to the **MAC Filter List** tab. Then, select **macfilter03**'s entry and click **Edit**.

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

Figure 60 MAC Filter Edit (SERVER_1)



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

8.4.6.5 Configure the SERVER_2 Network

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

To do this, repeat the procedure in Section 8.4.6.4 on page 99, substituting the following information.

Table 32 SERVER_2 Network Information

SSID Screen	
Index	4
Profile Name	SERVER_2
SSID Edit (SERVER_2) Screen	
L2 Isolation	l2Isolation04
MAC Filtering	macfilter04
Layer-2 Isolation (l2Isolation04) Screen	
Profile Name	L2-ISO_SERVER-2
Set 1	MAC Address: 77:66:55:44:33:22 Description: NET_ROUTER
Set 2	MAC Address: 99:88:77:66:55:44 Description: SERVER_2
Set 3	MAC Address: 66:55:44:33:22:11 Description: GATEWAY
MAC Filter (macfilter04) Edit Screen	
Profile Name	MacFilter_SERVER_2
Set 1	MAC Address: 22:33:44:55:66:77 Description: Bob

8.4.7 Test Your WiFi Access Restrictions

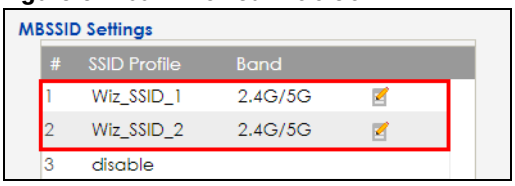
Use the following sections to ensure that your WiFi networks are set up correctly.

8.4.7.1 Check Settings

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

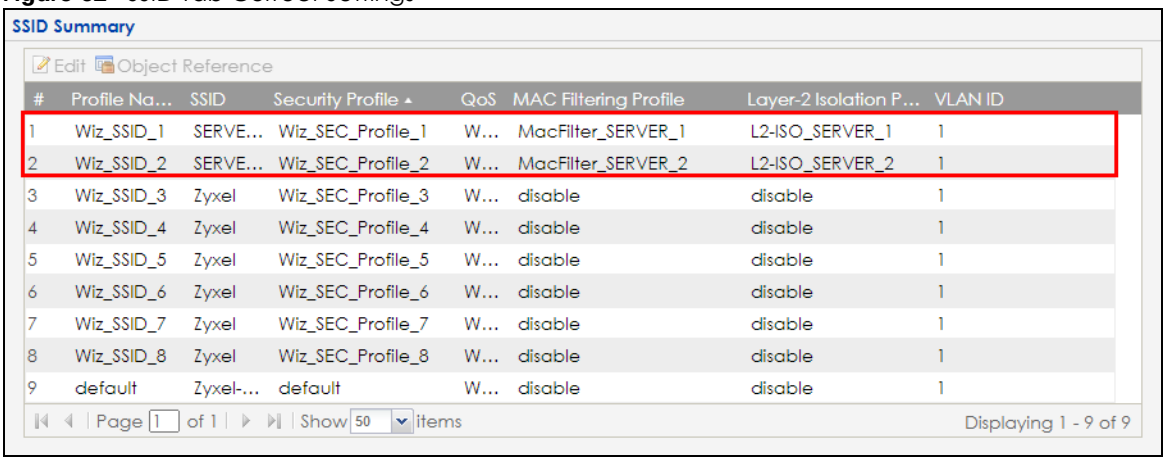
1 Click **Configuration > Wireless > AP Management**. Check that the correct SSID profiles are enabled, as shown in the following figure.

Figure 61 SSID Profiles Enabled



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

Figure 62 SSID Tab Correct Settings



8.4.7.2 Testing the Access Restrictions

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

1 Test the SERVER_1 network.

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

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

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

  Attempt to access Server 2. You should be unable to do so. If you can do so, layer-2 isolation is misconfigured.
- Using Alice's computer and WiFi client, and incorrect security settings, attempt to associate with the SERVER_1 network. You should be unable to do so. If you can do so, security is misconfigured.
- Using another computer and WiFi client, but with the correct security settings, attempt to associate with the SERVER_1 network. You should be unable to do so. If you can do so, MAC filtering is misconfigured.

2 Test the SERVER_2 network.

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

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

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

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

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

If you cannot do something that you should be able to do, check the settings as described in Section 8.4.7.1 on page 102, and in the individual Security, layer-2 isolation and MAC filter profiles for the relevant network. If this does not help, see the Troubleshooting chapter in this User's Guide.

8.5 Device Settings

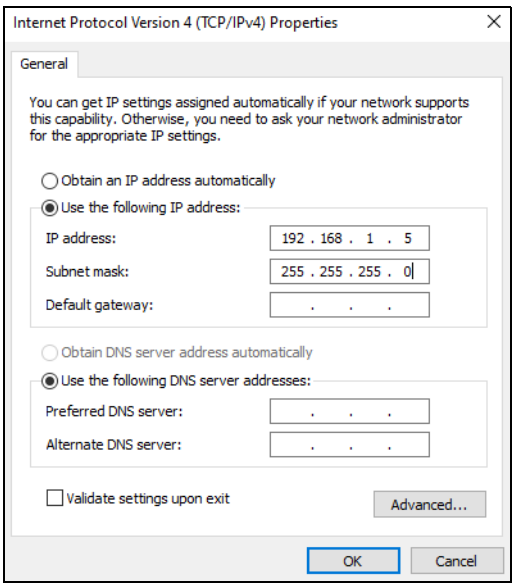
In this section, we show you how to:

- Change the Management IP Address
- Change the System Name
- Change the Login Password

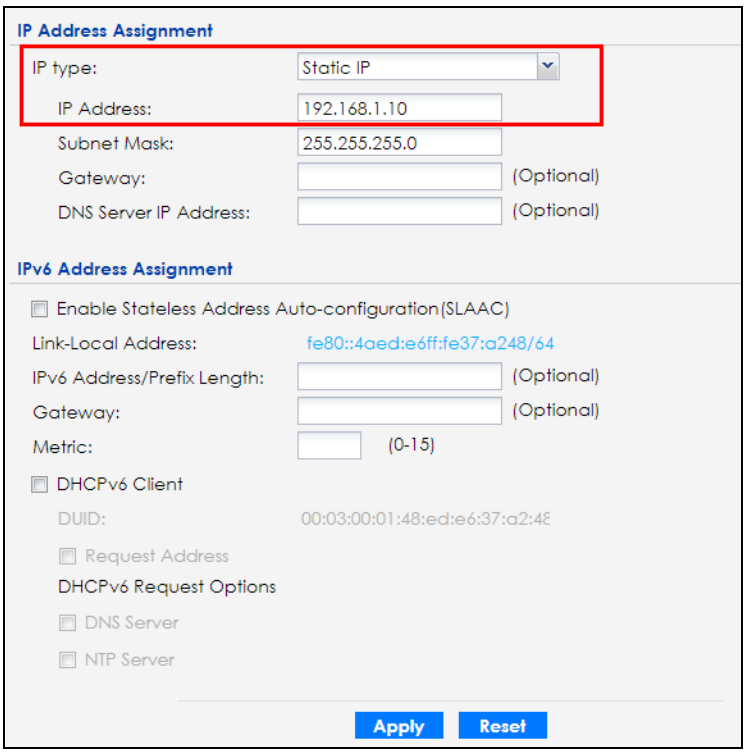
8.5.1 Change the Management IP Address

Change the management IP address of the Zyxel Device to ensure it does not duplicate the IP address of any other device on the network. If IP addresses are duplicated, you may be unable to access the Zyxel Device.

1 Set the computer's IP address to be in the same subnet as the Zyxel Device. For example, the default static management IP address of the Zyxel Device is 192.168.1.2. Make sure your computer's IP address is from 192.168.1.3~192.168.1.254.



2 Go to the **Configuration** > **Network** > **IP Setting** screen in the Web Configurator. Select the **IP type** to **Static IP** and specify a preferred IPv4 address in the **IP Address** field, for example, "192.168.1.10**"**. After clicking **Apply**, you will be disconnected from the Web Configurator due to the IP address change.

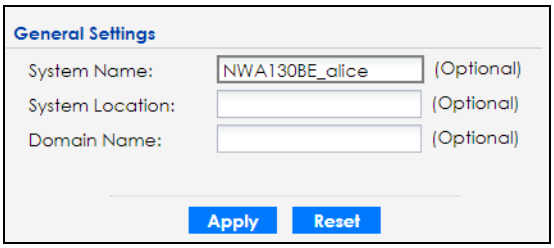


3 To check if the IP address of the Zyxel Device has been changed to "192.168.1.10", enter the new IP address "192.168.1.10" in the address bar and see if you can log in to the Web Configurator successfully. Ensure that your computer's IP address is in the same subnet as the Zyxel Device. For example, if the management IP address of the Zyxel Device is "192.168.1.10", your computer's IP address should be from 192.168.1.3~192.168.1.254.

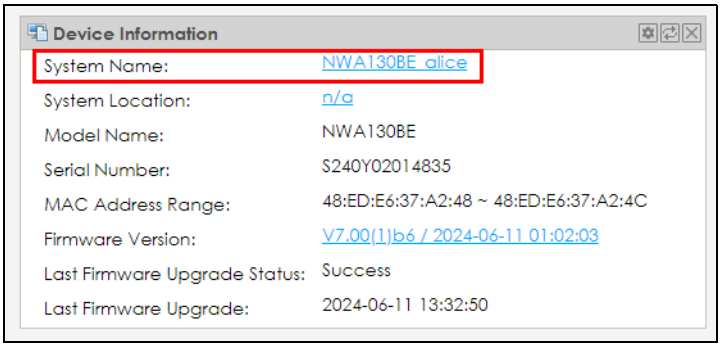
8.5.2 Change the System Name

Changing the system name ensures that the Zyxel Device's name is not duplicated with other devices on the network, which may otherwise cause confusion for network administrators.

1 Go to the **Configuration** > **System** > **Host Name** screen and enter a new name with 1 to 64 alphanumeric characters in the **System Name** field. Spaces are not allowed. Click **Apply** to save your changes.



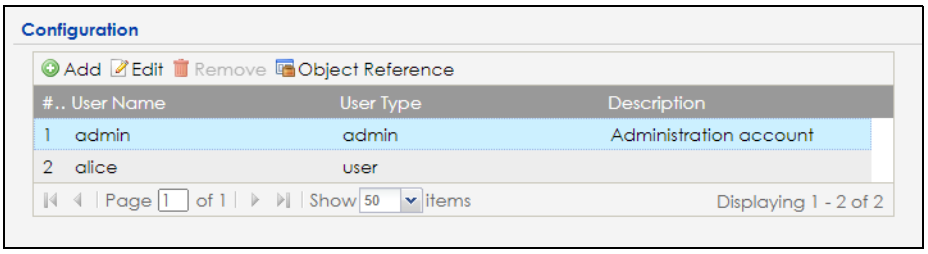
2 See the **System Name** field in the **Dashboard** screen to check if the new system name has been applied.



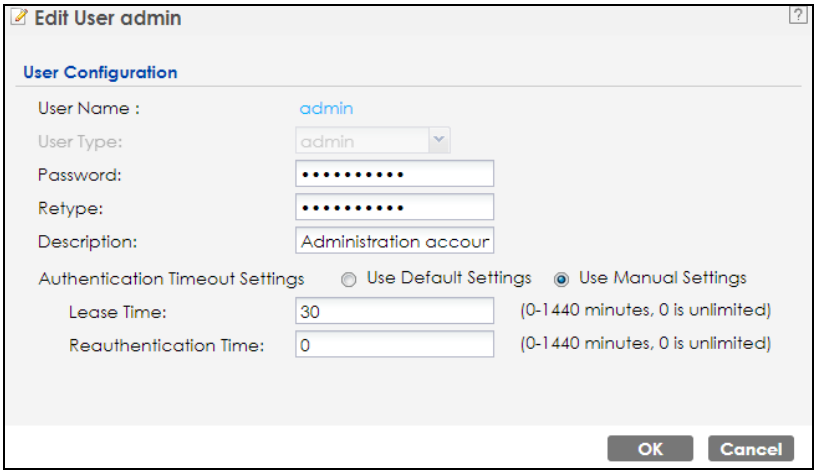
8.5.3 Change the Login Password

Change the Web Configuration login password to help secure your account.

1 Go to the **Configuration** > **Object** > **User** screen. Select an account and click the **Edit** icon.



2 The **Edit User admin** screen appears. Enter the new password with 4 to 63 alphanumeric characters. Retype the new password and click **OK**.



8.6 Device Maintenance

In this section, we show you how to:

- Upgrade the Firmware

- Restore the Zyxel Device Configuration

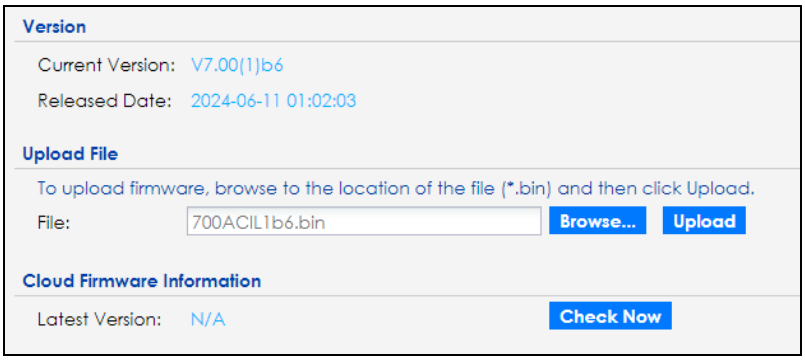
8.6.1 Upgrade the Firmware

Upload the firmware to the Zyxel Device for feature enhancements.

1 Download the correct firmware from the download library at the Zyxel website. The model code for the Zyxel Device in this example is ACIL. Unzip the file.

2 Go to **Maintenance** > **File Manager** > **Firmware Package** screen.

3 Click **Browse...** and select the file with a ".bin" extension to upload. Click **Upload**.



4 This process may take up to 2 minutes to finish. After 2 minutes, log on again and check your firmware version in the **Dashboard** screen.

8.6.2 Restore the Zyxel Device Configuration

The section shows you how to restore the configuration. You need to download and upload the configuration file to restore the configuration on the Zyxel Device.

Table 33 Configuration File Types

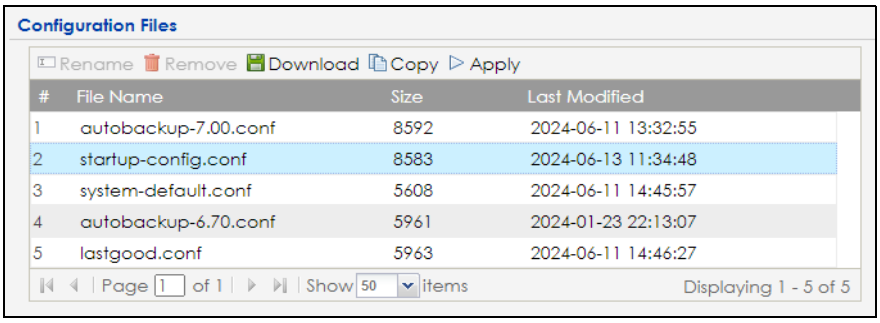
FILENAME	DESCRIPTION
autobackup-x.xx.conf	This is the configuration file that the Zyxel Device automatically backs up when upgrading the firmware.
startup-config.conf	This is the configuration file that the Zyxel Device is currently using.
system-default.conf	This is the Zyxel Device's default settings.
lastgood.conf	This is the most recently used (valid) configuration file that was saved when the Zyxel Device last restarted.

8.6.2.1 Download the Zyxel Device Configuration

You should regularly download your configuration especially before you make major configuration changes.

1 Go to the **Maintenance** > **File Manager** > **Configuration File** screen.

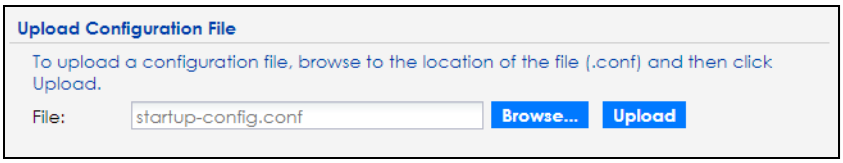
2 Under the **Configuration Files**, select **startup-config.conf** and click **Download**. The current configuration file that the Zyxel Device is using is saved to your computer. You can rename the configuration file to include the date you downloaded it. For example, **startup-config.conf_20240716**.



8.6.2.2 Upload the Zyxel Device Configuration

This section shows how to upload a previously saved configuration file from your computer to the Zyxel Device. You might need to do this to recover settings after a reset or to fix problems after configuration changes.

1 Go to the **Maintenance** > **File Manager** > **Configuration File** screen. Under **Upload Configuration File**, click **Browse...** and then select the configuration file that you saved. Click **Upload**.



2 You are logged out of the Web Configurator after the configuration file is successfully uploaded. Wait for one minute before logging into the Zyxel Device again.

8.7 Log and Report

In this section, we show you how to:

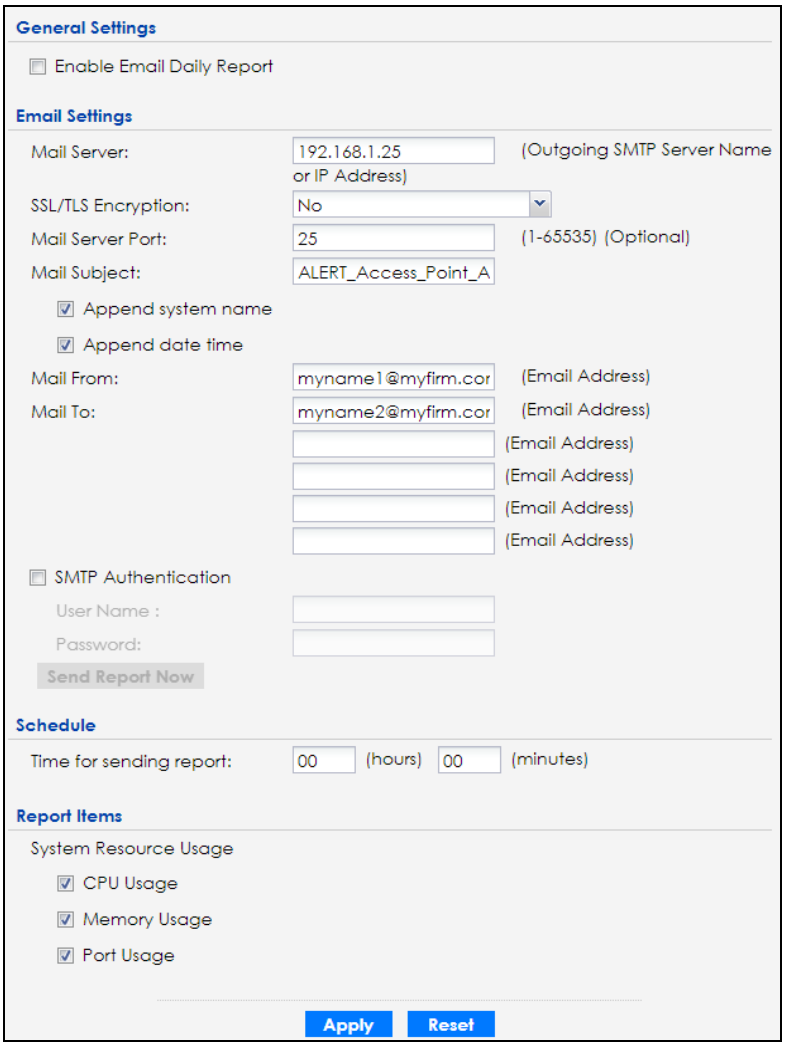
- Daily Email Report Setup
- Back Up Logs to a Remote Server

8.7.1 Daily Email Report Setup

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

Note: Some models do not support the email daily report feature.

1 Go to **Configuration** > **Log & Report > Log Setting**. Select the item and click **Edit**.The following screen appears. In this example, your mail server's IP address is **192.168.1.25**. Enter this IP address in the **Mail Server** field.



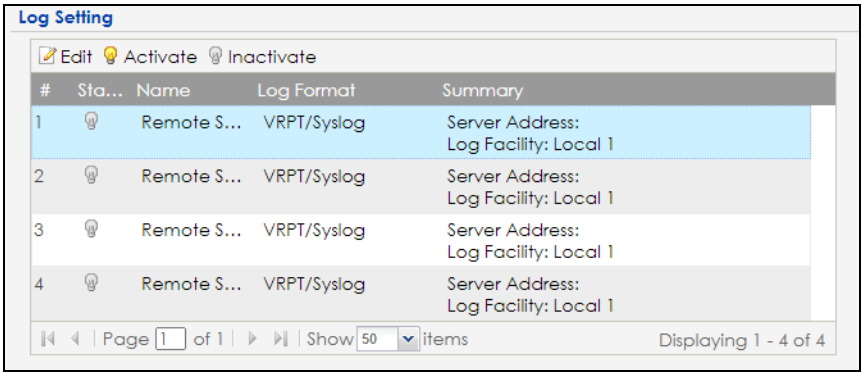
2 Enter a subject line for the alert emails in the **Mail Subject** field. Choose a subject that is eye-catching and identifies the access point - in this example, "ALERT_Access_Point_A".

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

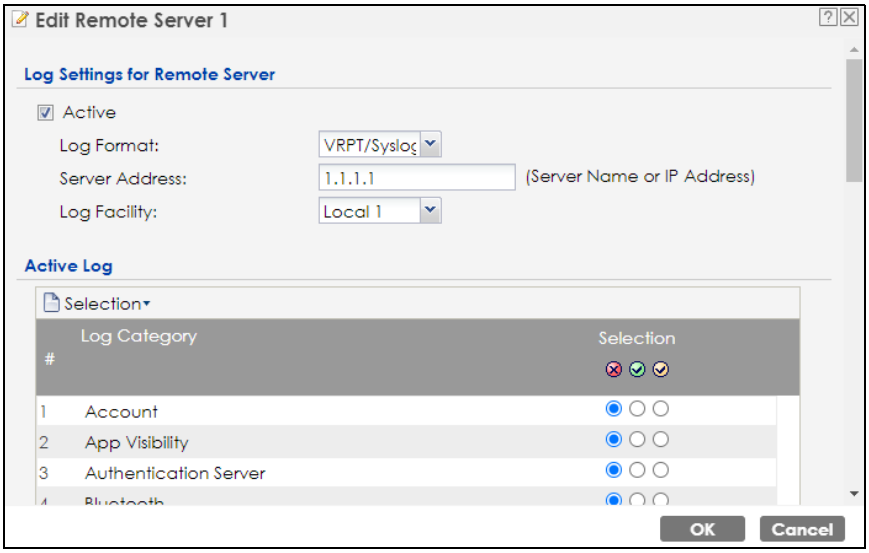
8.7.2 Back Up Logs to a Remote Server

Backing up logs to a remote server allows you to store large amounts of log data and prevent log data lost on your Zyxel Device. The Zyxel Device can keep at most 512 logs. If the logs exceed this number, the oldest logs will be lost.

1 Go to **Configuration** > **Log & Report** > **Log Setting**. Select a remote server to configure, and then click **Edit**.

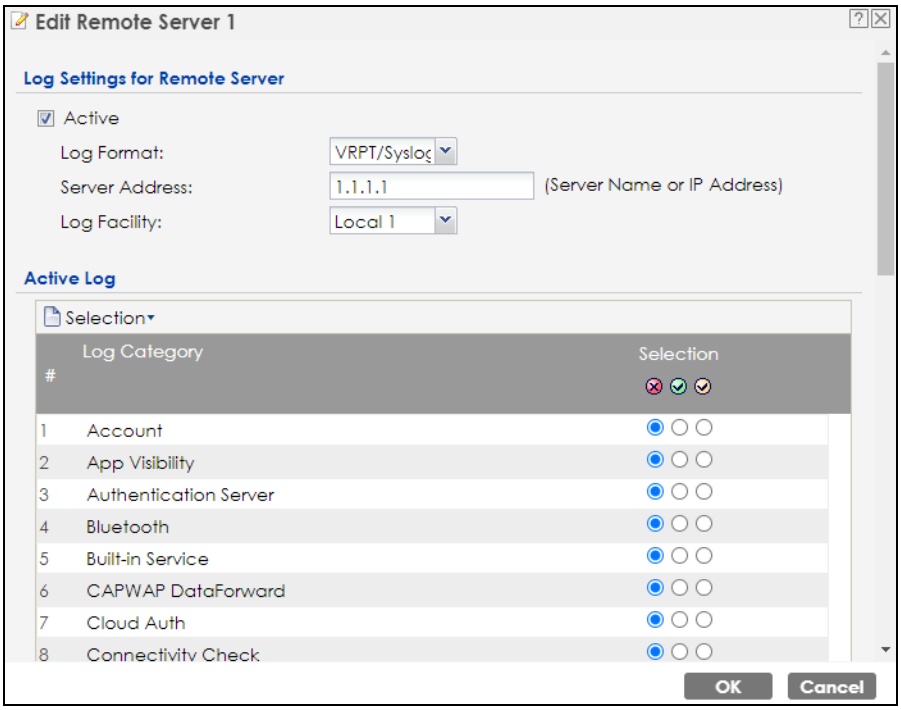


2 The following screen appears. Select **Active** and enter the IPv4 address or name of the remote server in the **Server Address** field to send the logs. Then, select a log facility. The log facility allows you to log the messages to different files in the syslog server. Please see the documentation for your syslog program for more information.



3 Select the type of logs you want to back up on the remote server. The following are the log settings represented by the icons.

- Red X - Do not send the remote server logs for any log category.
- Green checkmark - Send the remote server log messages and alerts for all log categories.
- Yellow checkmark - Send the remote server log messages, alerts, and debugging information for all log categories.



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

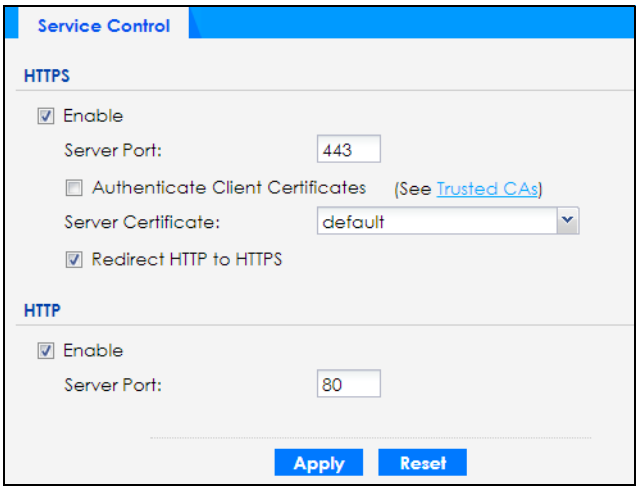
8.8 Access to the Zyxel Device

This section shows you how to configure WAN access for a specific trusted computer through HTTPS, HTTP or SSH to the Zyxel Device. Remote management determines which interface and web services are allowed to access the Zyxel Device.

Perform the following to find the options to configure remote access to your Zyxel Device.

HTTPS / HTTP

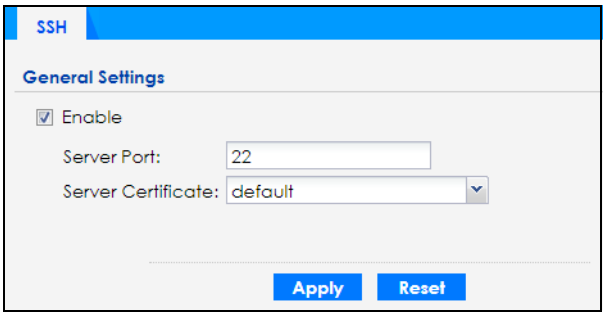
1 Go to the **Configuration** > **System** > **WWW** screen. Select whether you want to access the Zyxel Device remotely through HTTPS or HTTP. Click **Apply** to save your changes.



Note: The HTTPS server listens on port 443 by default. If you change the HTTPS server port to a different number on the Zyxel Device, for example 8443, then you must notify people who need to access the Zyxel Device Web Configurator to use "https://Zyxel Device IP Address:8443" as the URL.

SSH

1 Go to the **Configuration** > **System** > **SSH** screen. Select whether you want to access the Zyxel Device remotely through SSH. Click **Apply** to save your changes. You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.



CHAPTER 9
Monitor

9.1 Overview

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

9.1.1 What You Can Do in this Chapter

- The **Network Status** screen (Section 9.3 on page 113) displays general LAN interface information and packet statistics.
- The **AP Information** > **Radio List** screen (Section 9.4 on page 115) displays statistics about the WiFi radio transmitters in the Zyxel Device.
- The **Station Info** screen (Section 9.5 on page 118) displays statistics pertaining to the associated stations.
- The **WDS Link Info** screen (Section 9.6 on page 119) displays statistics about the Zyxel Device's WDS (Wireless Distribution System) connections.
- The **Detected Device** screen (Section 9.7 on page 120) displays information about suspected rogue APs.
- The **View Log** screen (Section 9.8 on page 122) displays the Zyxel Device's current log messages. You can change the way the log is displayed, you can email the log, and you can also clear the log in this screen.

9.2 What You Need to Know

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

Rogue AP

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

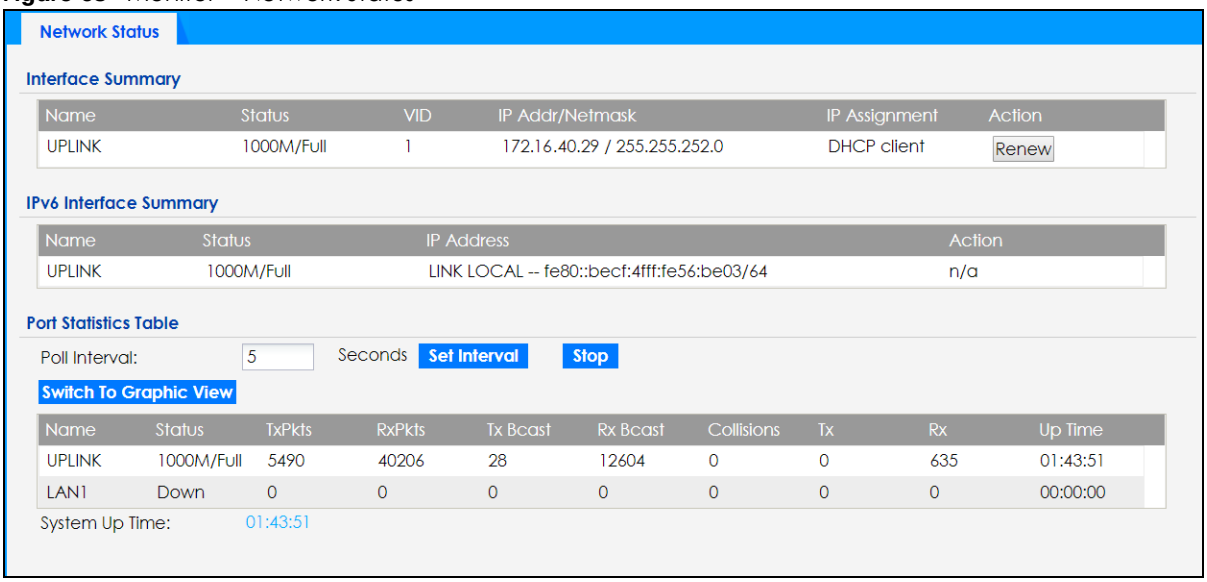
Friendly AP

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

9.3 Network Status

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

Figure 63 Monitor > Network Status



The following table describes the labels in this screen.

Table 34 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**.

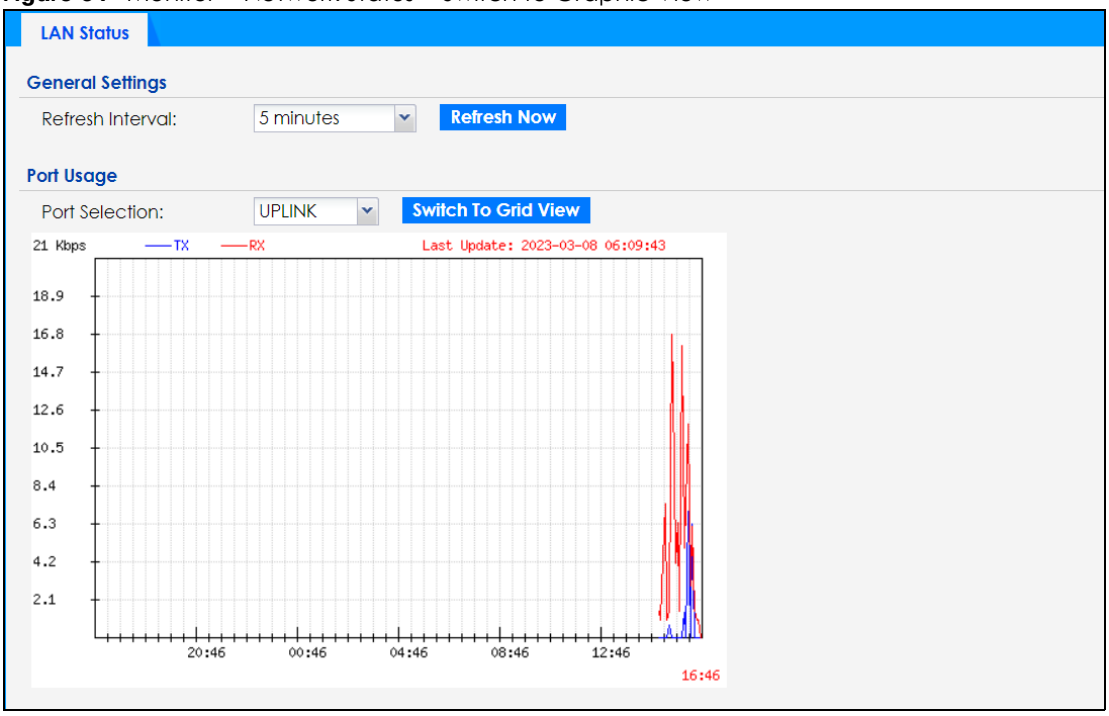
Table 34 Monitor > Network Status (continued)

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

9.3.1 Port Statistics Graph

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

Figure 64 Monitor > Network Status > Switch to Graphic View



The following table describes the labels in this screen.

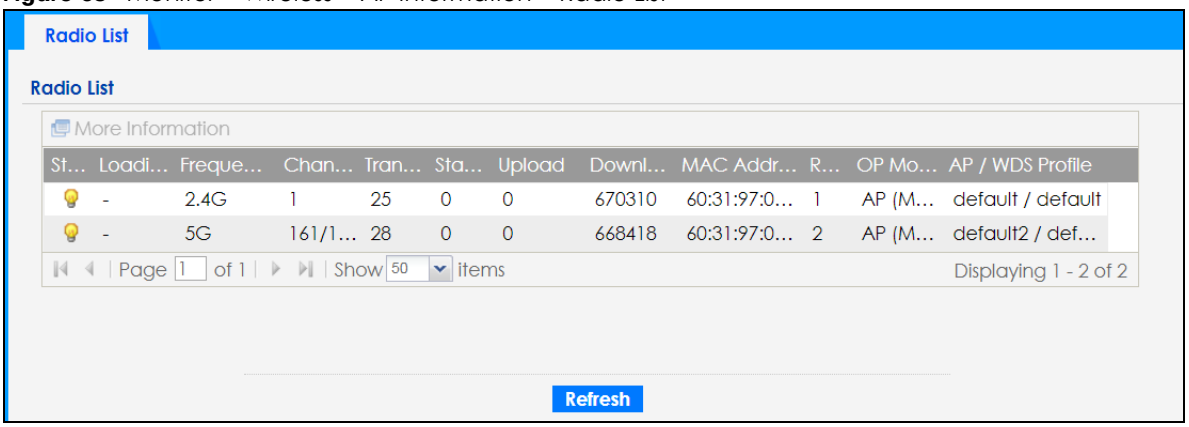
Table 35 Monitor > Network Status > Switch to Graphic View

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

9.4 Radio List

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

Figure 65 Monitor > Wireless > AP Information > Radio List



The following table describes the labels in this screen.

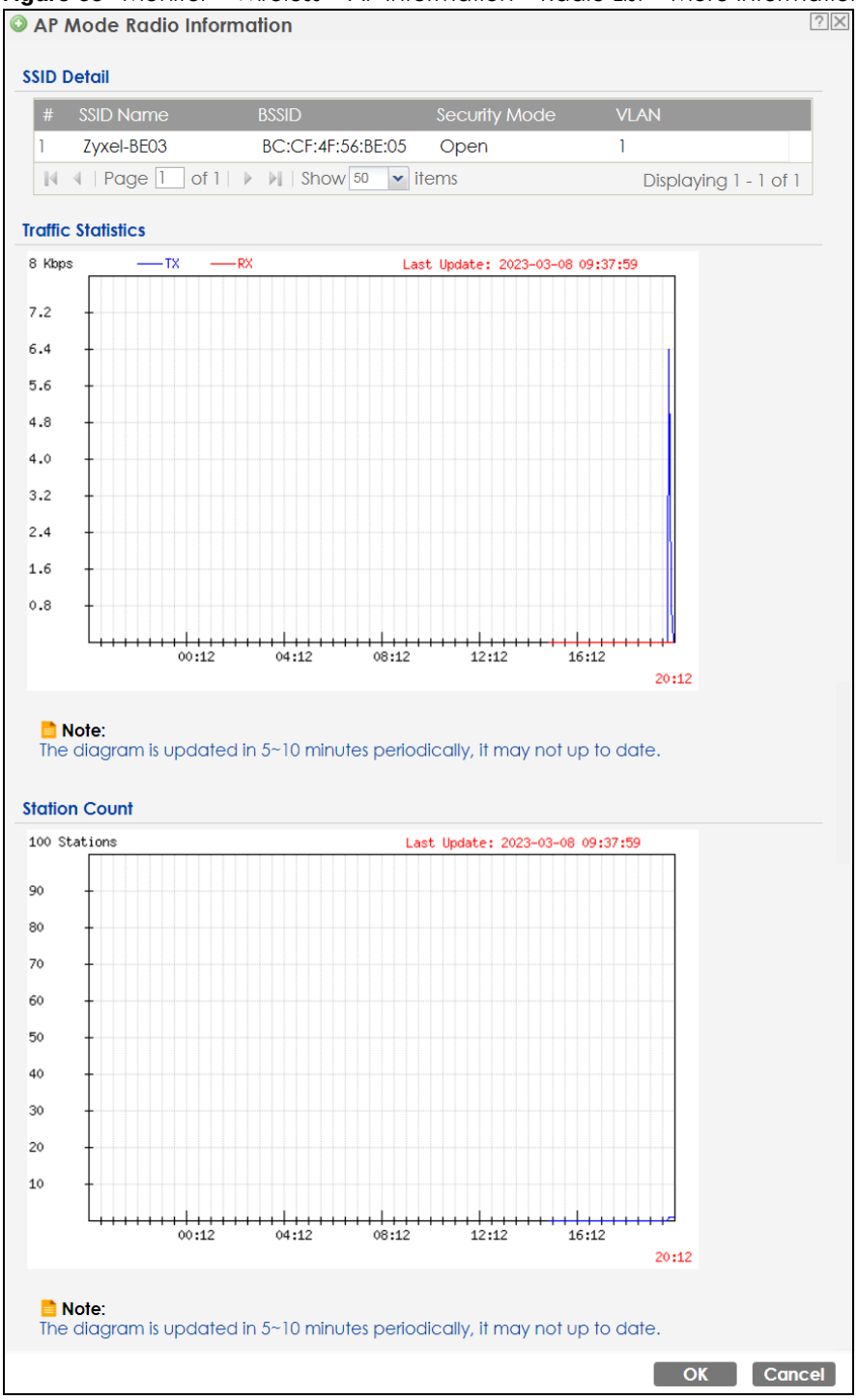
Table 36 Monitor > Wireless > AP Information > Radio List

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. This is only available if your Zyxel Device supports **Load Balancing**. See Section 1.2 on page 14 for the supported models list.
Frequency Band	This indicates the wireless frequency band currently being used by the radio.
Channel	This indicates the radio's channel ID.
Transmit Power	This displays the output power of the radio.
Station	This displays the number of WiFi clients connected to this radio on the Zyxel Device.
Upload	This displays the total number of packets received by the radio.
Download	This displays the total number of packets transmitted by the radio.
MAC Address	This displays the MAC address of the radio.
Radio	This indicates the radio number on the Zyxel Device to which it belongs.
OP Mode	This indicates the radio's operating mode. Operating modes are **AP (MBSSID)**, **Root AP** or **Repeater**.
AP/WDS Profile	This indicates the AP profile name and WDS profile name to which the radio belongs.
Channel Utilization	This indicates how much IEEE 802.11 traffic the radio can receive on the channel. It displays what percentage of the radio's channel is currently being used.

9.4.1 AP Mode Radio Information

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

Figure 66 Monitor > Wireless > AP Information > Radio List > More Information



The following table describes the labels in this screen.

Table 37 Monitor > Wireless > AP Information > Radio List > More Information

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

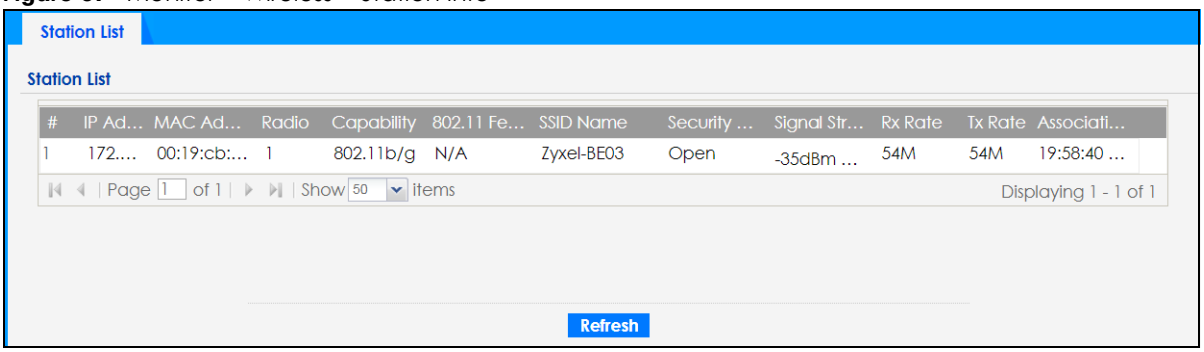
Table 37 Monitor > Wireless > AP Information > Radio List > More Information (continued)

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

9.5 Station List

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

Figure 67 Monitor > Wireless > Station Info



The following table describes the labels in this screen.

Table 38 Monitor > Wireless > Station Info

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

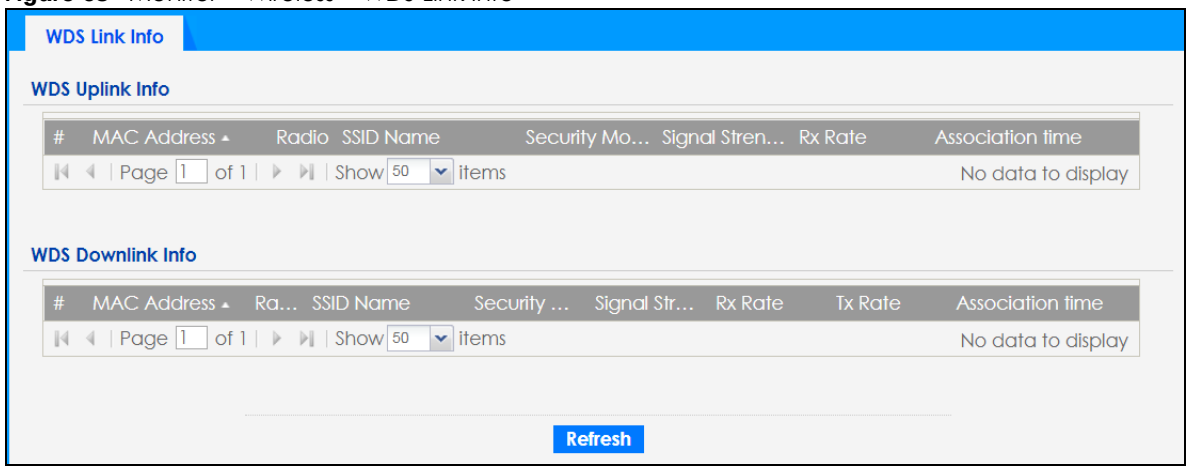
Table 38 Monitor > Wireless > Station Info (continued)

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

9.6 WDS Link Info

Use this screen to view the WDS traffic statistics between the Zyxel Device and a root AP or repeaters. See Section 1.3 on page 24 to know more about WDS. Click **Monitor > Wireless > WDS Link Info** to access this screen.

Figure 68 Monitor > Wireless > WDS Link Info



The following table describes the labels in this screen.

Table 39 Monitor > Wireless > WDS Link Info

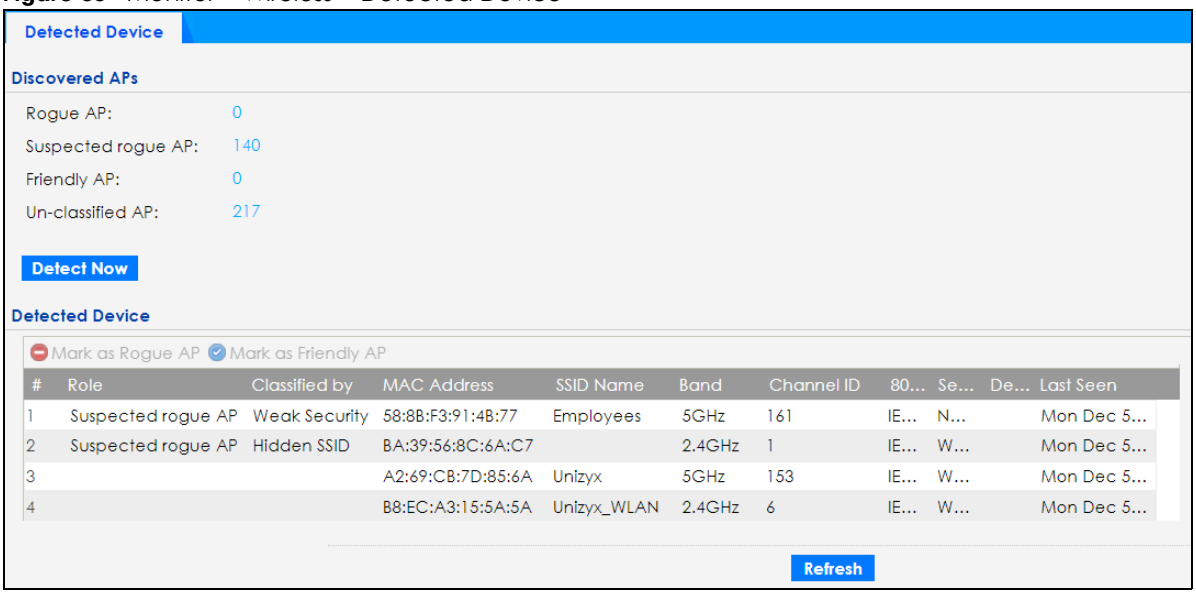
LABEL	DESCRIPTION
WDS Uplink/ Downlink Info	**Uplink** refers to the WDS link from the repeaters to the root AP. **Downlink** refers to the WDS link from the root AP to the repeaters. When the Zyxel Device is in root AP mode and connected to a repeater, only the downlink information is displayed. When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

9.7 Detected Device

Use this screen to view information about surrounding APs which you could mark as **Rogue** or **Friendly**. Click **Monitor > Wireless > Detected Device** to access this screen. For more information about Rogue APs, see Section 11.3 on page 144.

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

Figure 69 Monitor > Wireless > Detected Device



The following table describes the labels in this screen.

Table 40 Monitor > Wireless > Detected Device

LABEL	DESCRIPTION
Discovered APs	
Rogue AP	This shows how many devices are detected as rogue APs.
Suspected rogue AP	This shows how many devices are detected as possible rogue APs based on the classification rule(s) in Section 11.3 on page 144.
Friendly AP	This shows how many devices are detected as friendly APs.
Un-classified AP	This shows how many devices are detected, but have not been classified as either Rogue or Friendly by the Zyxel Device.
Detect Now	Click this button for the Zyxel Device to scan for APs in the network.
Detected Device	
Mark as Rogue AP	Click this button to mark the selected AP as a rogue AP. For more on managing rogue APs, see the **Configuration > Wireless > Rogue AP** screen (Section 11.3 on page 144).
Mark as Friendly AP	Click this button to mark the selected AP as a friendly AP. For more on managing friendly APs, see the **Configuration > Wireless > Rogue AP** screen (Section 11.3 on page 144).
#	This is the detected device's index number in this list.
Role	This indicates the detected device's role (such as friendly or rogue).
Classified by	This indicates the detected device's classification rule.
MAC Address	This indicates the detected device's MAC address.
SSID Name	This indicates the detected device's SSID.
Band	This is the frequency band to which the station is connected.
Channel ID	This indicates the detected device's channel ID.
802.11 Mode	This indicates the 802.11 mode (a/b/g/n/ac/ax) transmitted by the detected device.
Security	This indicates the encryption method (if any) used by the detected device.
Description	This displays the detected device's description. For more on managing friendly and rogue APs, see the **Configuration > Wireless > Rogue AP** screen (Section 11.3 on page 144).

Table 40 Monitor > Wireless > Detected Device (continued)

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

9.8 View Log

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

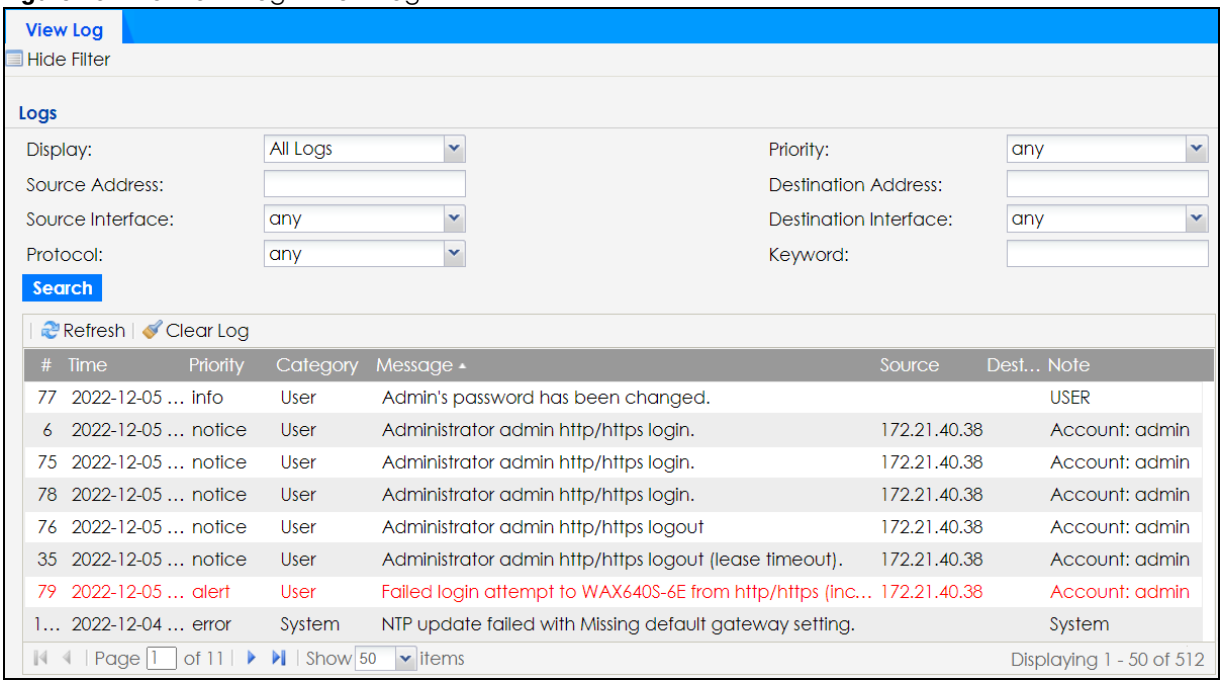
To access this screen, click **Monitor > Log**. The log is displayed in the following screen.

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

Events that generate an alert (as well as a log message) display in red. Regular logs display in black. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

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

Figure 70 Monitor > Log > View Log



The following table describes the labels in this screen.

Table 41 Monitor > Log > View Log

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

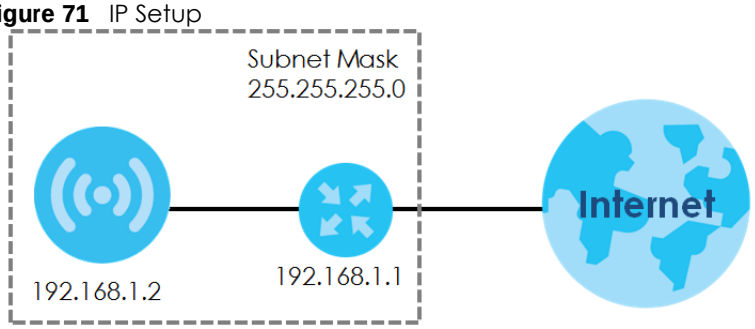
CHAPTER 10
Network

10.1 Overview

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

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

Figure 71 IP Setup



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

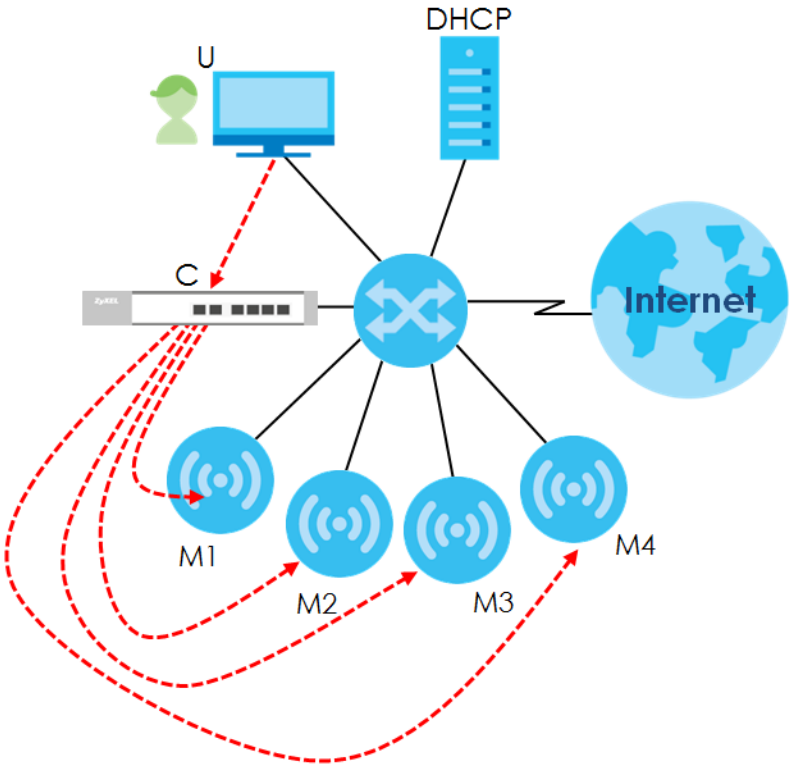
10.1.1 AP Controller Management

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

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

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

Figure 72 AC managed Network Example



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

AC Discovery and Management

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

1 A Zyxel Device with **AC Discovery** enabled joins a wired network (receives a dynamic IP address).

2 The Zyxel Device sends out a discovery request, looking for an AC.

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

Managed AP Finds the Controller

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

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

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

AC management and IP Subnets

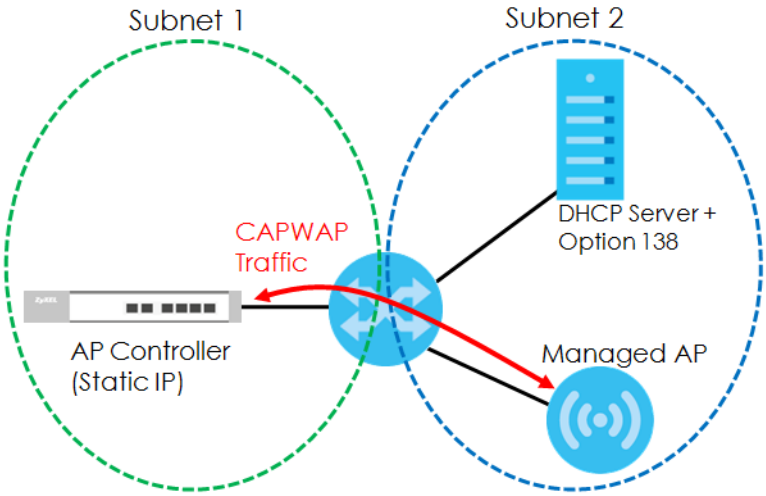
By default, CAPWAP works only between Zyxel Devices with IP addresses in the same subnet.

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

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

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

Figure 73 CAPWAP and DHCP Option 138



Notes on AC Management

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

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

10.1.2 What You Can Do in this Chapter

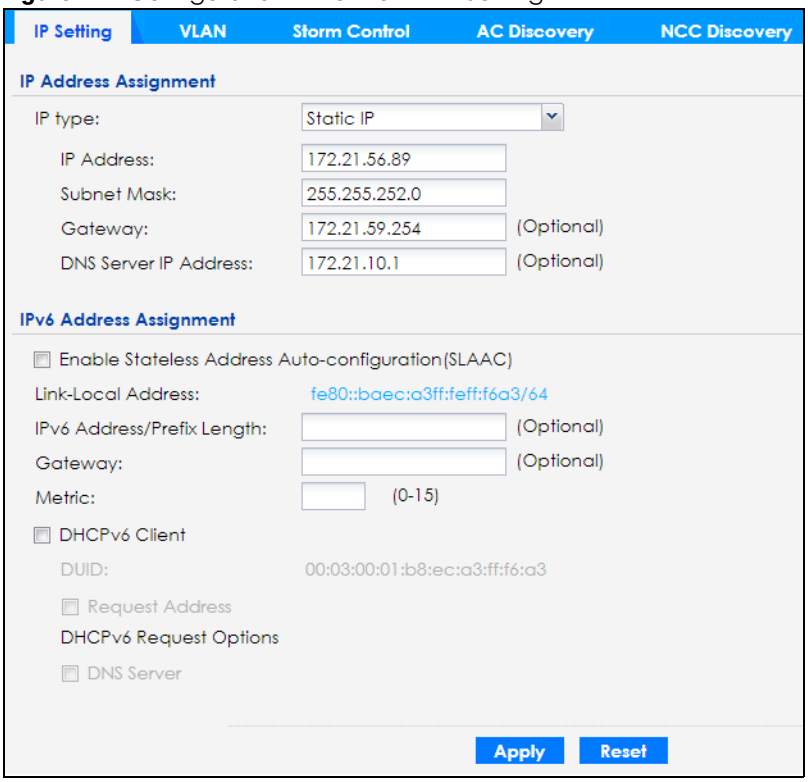
- The **IP Setting** screen (Section 10.2 on page 127) configures the Zyxel Device's LAN IP address.
- The **VLAN** screen (Section 10.3 on page 128) configures the Zyxel Device's VLAN settings.
- The **Storm Control** screen (Section 10.4 on page 133) turns on or off the traffic storm control feature on the Zyxel Device.
- The **AC Discovery** screen (Section 10.5 on page 134) configures the Zyxel Device's AP Controller (AC) settings.

- The **NCC Discovery** screen (Section 10.6 on page 135) configures the Zyxel Device's Nebula Control Center (NCC) discovery settings.

10.2 IP Setting

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

Figure 74 Configuration > Network > IP Setting



Each field is described in the following table.

Table 42 Configuration > Network > IP Setting

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

Table 42 Configuration > Network > IP Setting (continued)

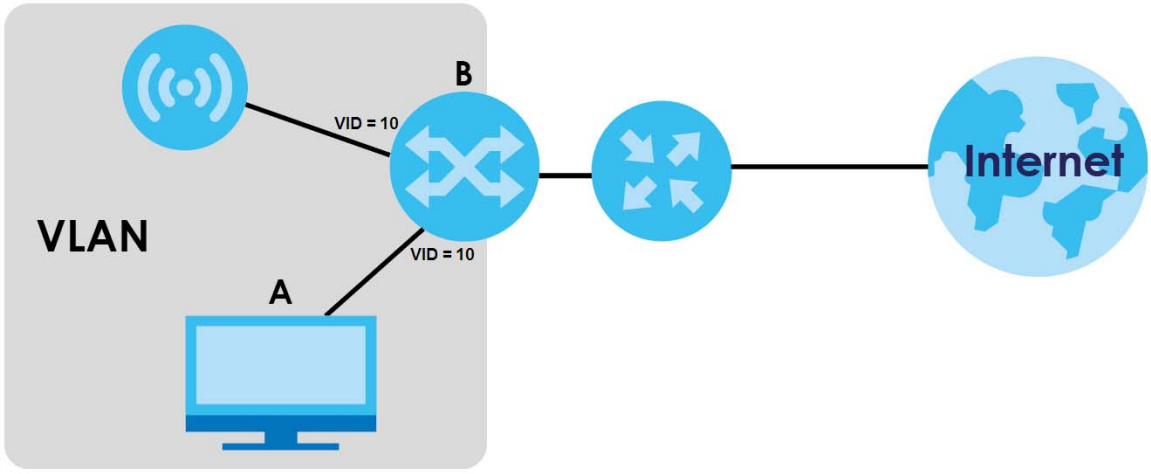
LABEL	DESCRIPTION
Gateway	Enter the IP address of the gateway. The Zyxel Device sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
DNS Server IP Address	Enter the IP address of the DNS server.
IPv6 Address Assignment	
Enable Stateless Address Auto-configuration (SLAAC)	Select this to enable IPv6 stateless auto-configuration on the Zyxel Device. The Zyxel Device will generate an IPv6 address itself from a prefix obtained from an IPv6 router in the network.
Link-Local Address	This displays the IPv6 link-local address and the network prefix that the Zyxel Device generates itself for the LAN interface.
IPv6 Address/Prefix Length	Enter the IPv6 address and the prefix length for the LAN interface if you want to use a static IP address. This field is optional. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Gateway	Enter the IPv6 address of the default outgoing gateway using colon (:) hexadecimal notation.
Metric	Enter the priority of the gateway (if any) on the LAN interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first. Enter zero to set the metric to 1024 for IPv6.
DHCPv6 Client	Select this option to set the Zyxel Device to act as a DHCPv6 client.
DUID	This field displays the DHCP Unique IDentifier (DUID) of the Zyxel Device, which is unique and used for identification purposes when the Zyxel Device is exchanging DHCPv6 messages with others. See Appendix B on page 318 for more information.
Request Address	Select this option to get an IPv6 address from the DHCPv6 server.
DHCPv6 Request Options	Select the following DHCPv6 options to determine what additional information to get from the DHCPv6 server.
DNS Server	Select this option to obtain the IP address of the DNS server.
NTP Server	Select this option to obtain the IP address of the NTP server.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

10.3 VLAN

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

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

Figure 75 Management VLAN Setup



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

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

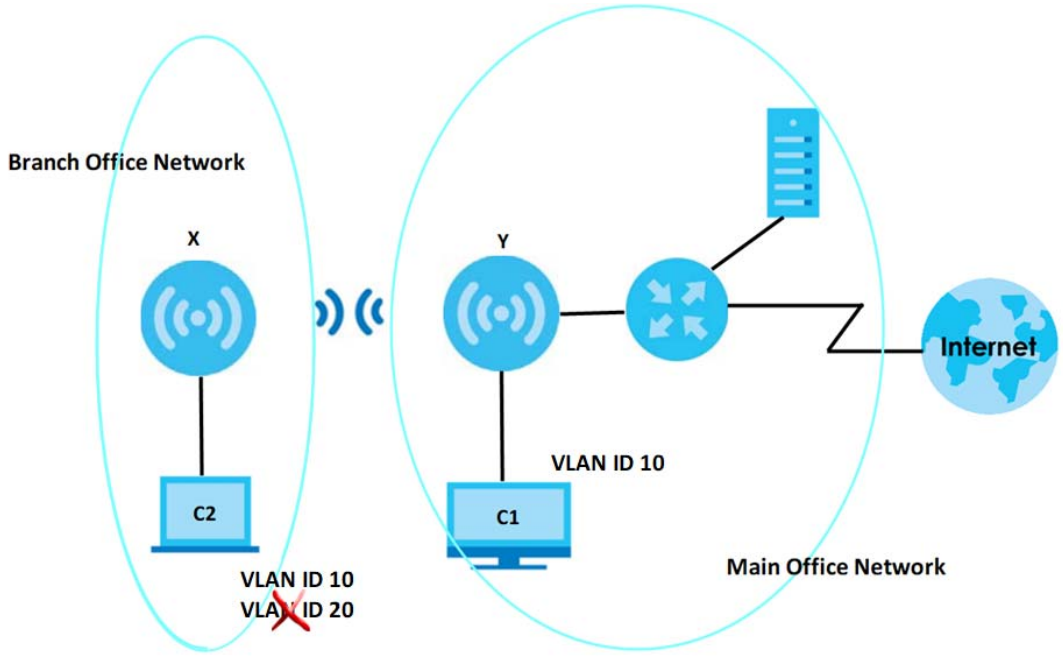
VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Wireless Bridge VLAN ID

Wireless bridge VLAN allows you to have clients in different WiFi networks appear to be in the same virtual network using VLAN IDs. VLAN IDs are sent across the wireless bridge so that only clients with the same VLAN ID receive that network traffic. See Section 1.3 on page 24 for more information on the wireless bridge.

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

Figure 76 Wireless Bridge VLAN ID Example



IEEE 802.1Q Tag

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

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

Figure 77 Configuration > Network > VLAN (for Zyxel Device with multiple Ethernet ports)

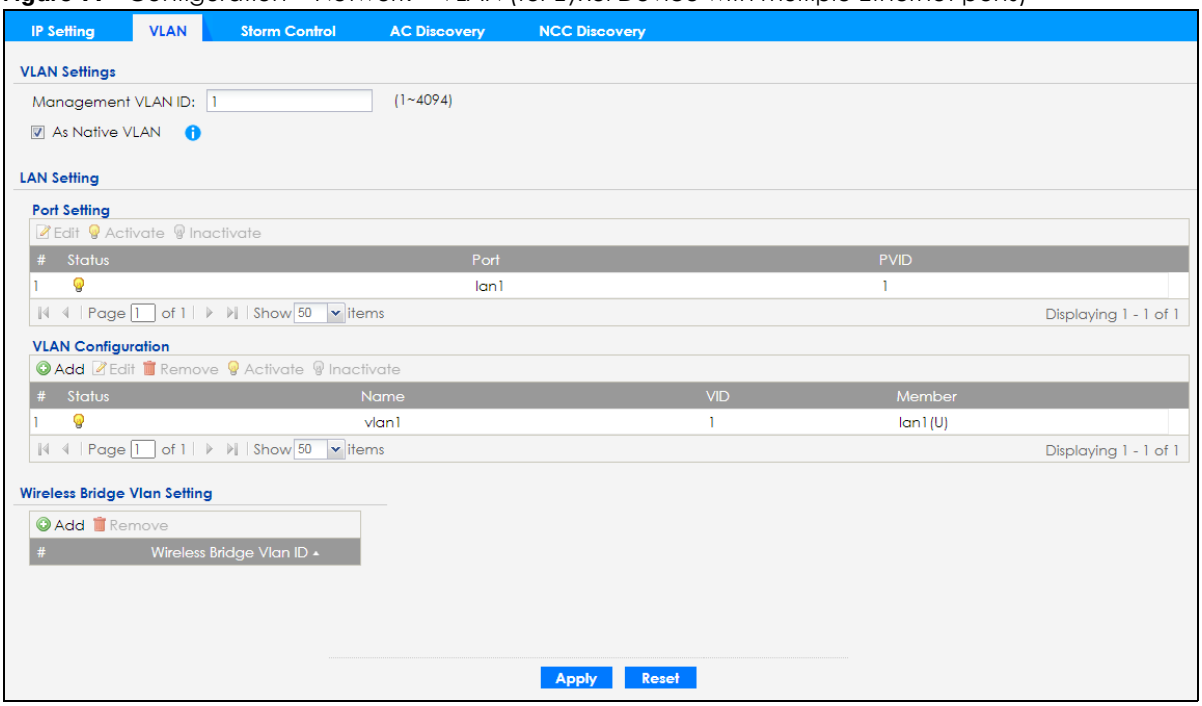
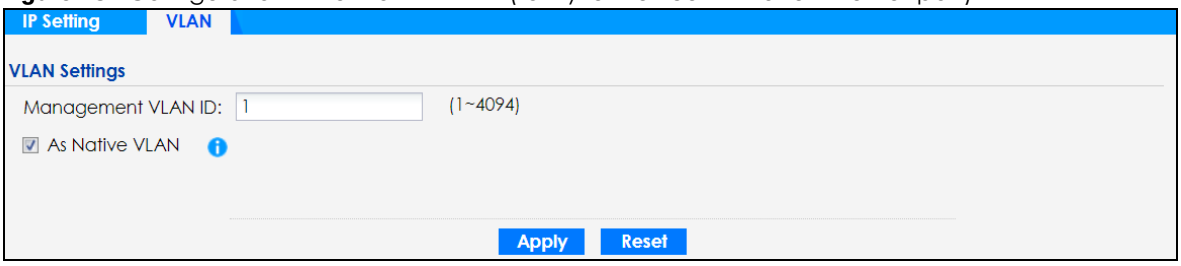


Figure 78 Configuration > Network > VLAN (for Zyxel Device with one Ethernet port)



Each field is described in the following table.

Table 43 Configuration > Network > VLAN

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

Table 43 Configuration > Network > VLAN (continued)

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

Table 43 Configuration > Network > VLAN (continued)

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

10.4 Storm Control

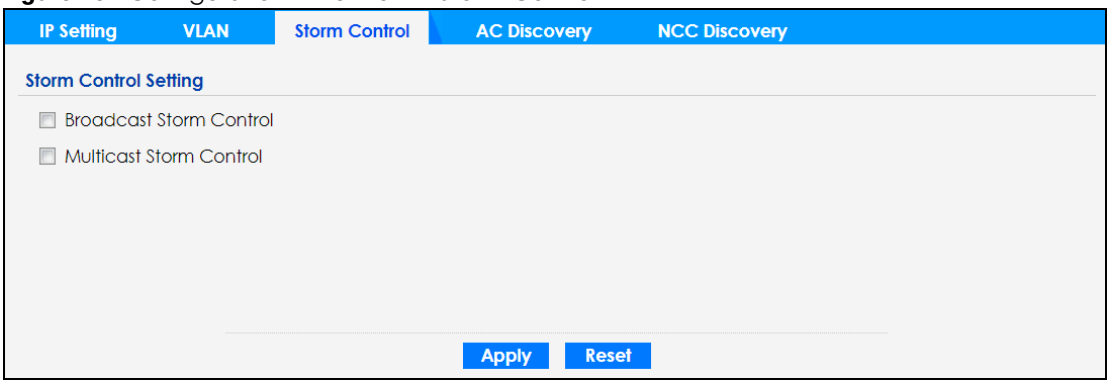
Traffic storm control limits the number of broadcast and/or multicast packets the Zyxel Device receives on the ports. When the maximum number of allowable broadcast and/or multicast packets is reached, the subsequent packets are discarded. Enable this feature to reduce broadcast and/or multicast packets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

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

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

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

Figure 79 Configuration > Network > Storm Control



Each field is described in the following table.

Table 44 Configuration > Network > Storm Control

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

10.5 AC (AP Controller) Discovery

This section discusses how to configure the Zyxel Device's AC Discovery settings. You can have the Zyxel Device managed by an AC on your network. When you do this, the Zyxel Device can be configured ONLY by the AC. See Section 10.1.1 on page 124 for more information on AC management.

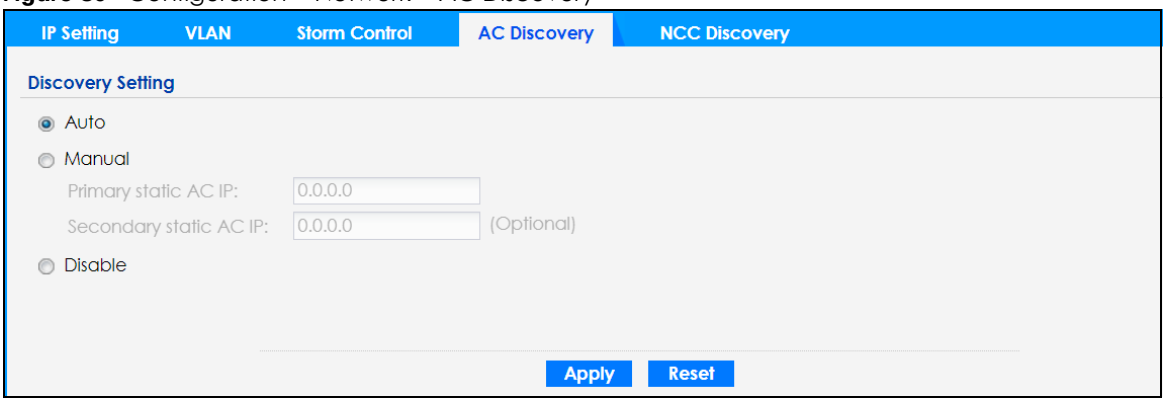
Note: The AC Discovery settings are not available in all Zyxel Devices. See Section 1.2 on page 14 for more information.

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

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

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

Figure 80 Configuration > Network > AC Discovery



Each field is described in the following table.

Table 45 Configuration > Network > AC Discovery

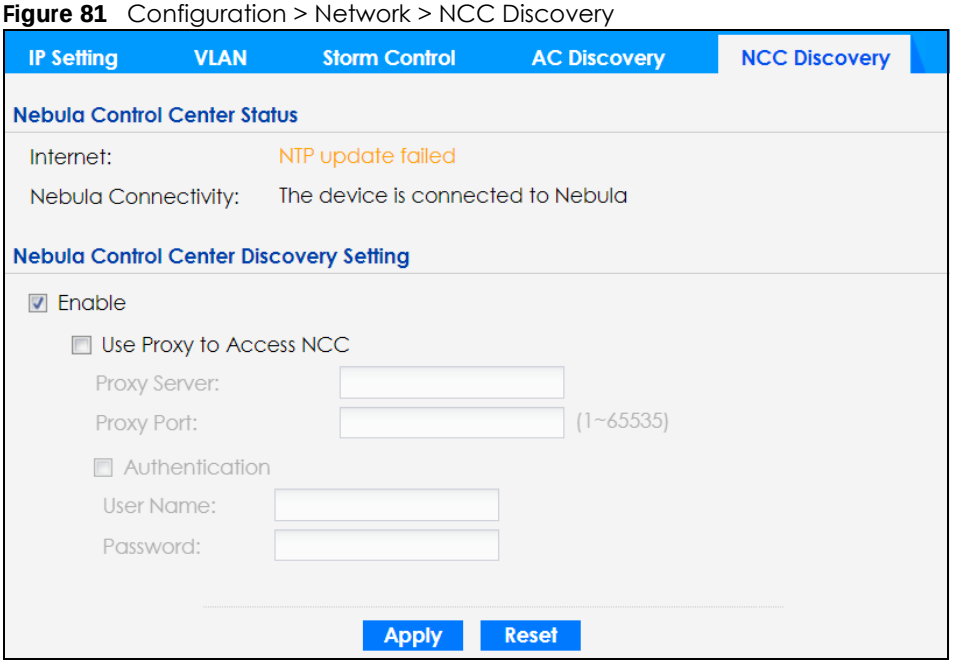
LABEL	DESCRIPTION
Discovery Setting	
Auto	Select this option to use DHCP option 138/DNS SRV record/Broadcast to get the AC's IP address. If the Zyxel Device and a Zyxel AC, such as a ZyWALL ATP, are in the same subnet, it will be managed by the controller automatically.
Manual	Select this option and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

10.6 NCC Discovery

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

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

Figure 81 Configuration > Network > NCC Discovery



Each field is described in the following table.

Table 46 Configuration > Network > NCC Discovery

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

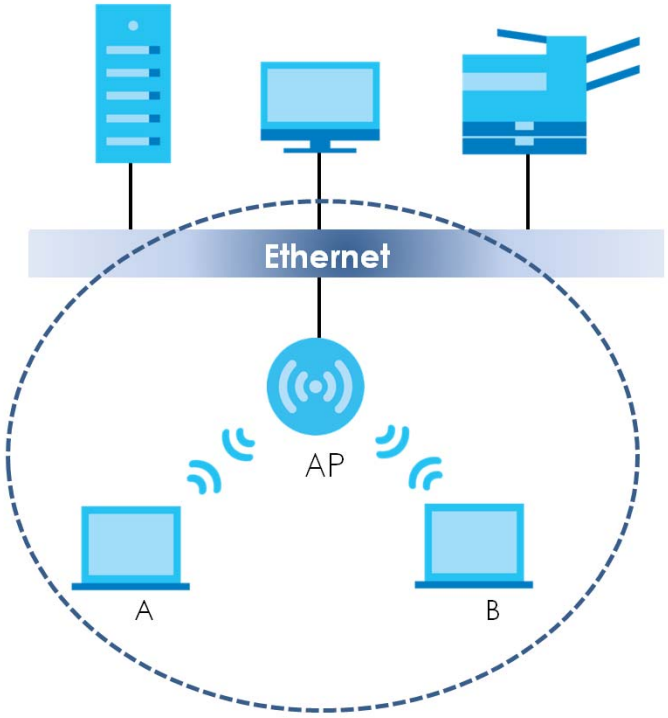
CHAPTER 11
Wireless

11.1 Overview

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

The following figure provides an example of a WiFi network.

Figure 82 Example of a WiFi Network



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

11.1.1 What You Can Do in this Chapter

- The **AP Management** screen (Section 11.2 on page 138) allows you to manage the Zyxel Device's general WiFi settings.
- The **Rogue AP** screen (Section 11.3 on page 144) allows you to assign APs either to the rogue AP list or the friendly AP list.
- The **Load Balancing** screen (Section 11.4 on page 148) allows you to configure network traffic load balancing between the APs and the Zyxel Device.
- The **DCS** screen (Section 11.5 on page 150) allows you to configure dynamic radio channel selection.

11.1.2 What You Need to Know

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

Station / WiFi Client

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

Dynamic Channel Selection (DCS)

Dynamic Channel Selection (DCS) is a feature that allows an AP to automatically select the radio channel which it broadcasts. For more information, see Section 11.6 on page 151.

Load Balancing (Wireless)

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

11.2 AP Management

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

Figure 83 Configuration > Wireless > AP Management

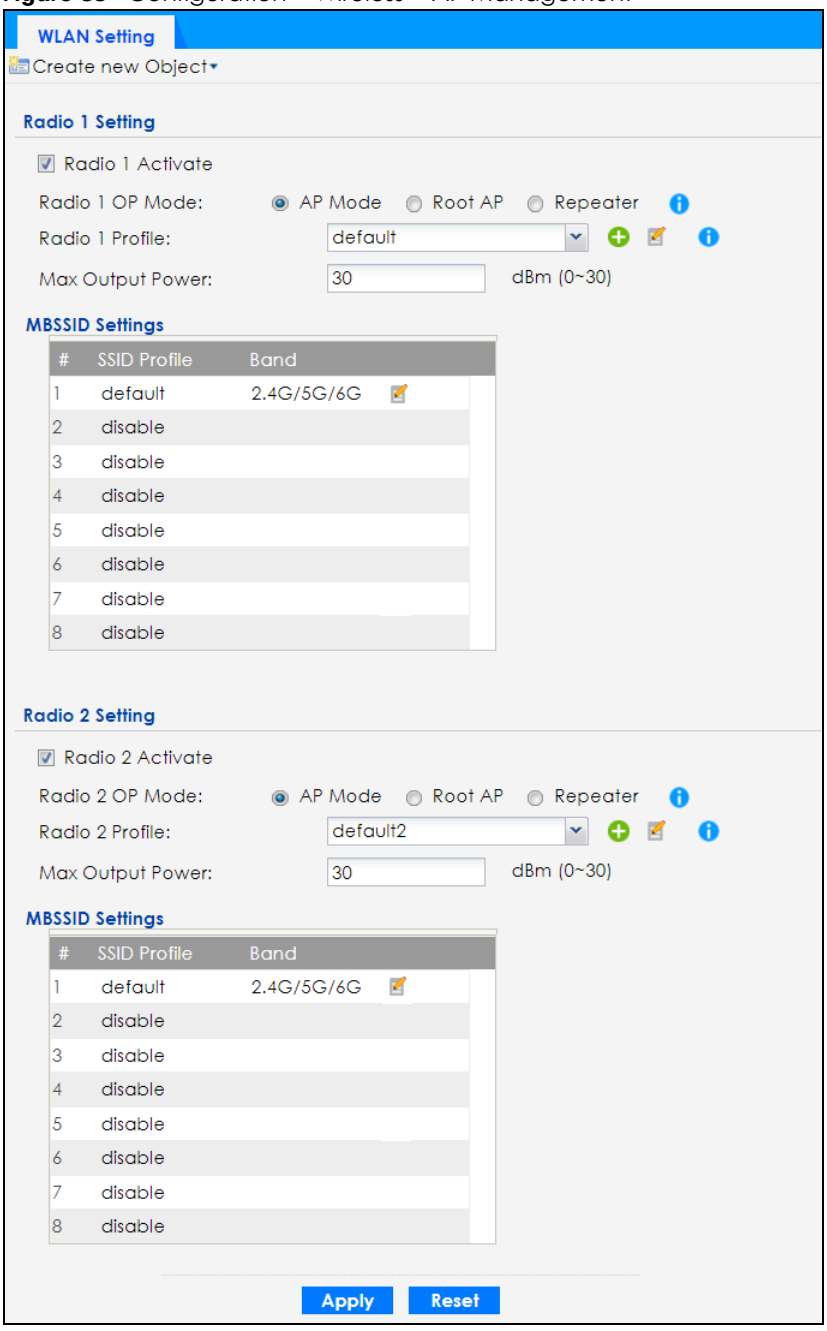


Figure 84 Configuration > Wireless > AP Management (for Zyxel Device with multiple Ethernet ports - in Repeater mode)

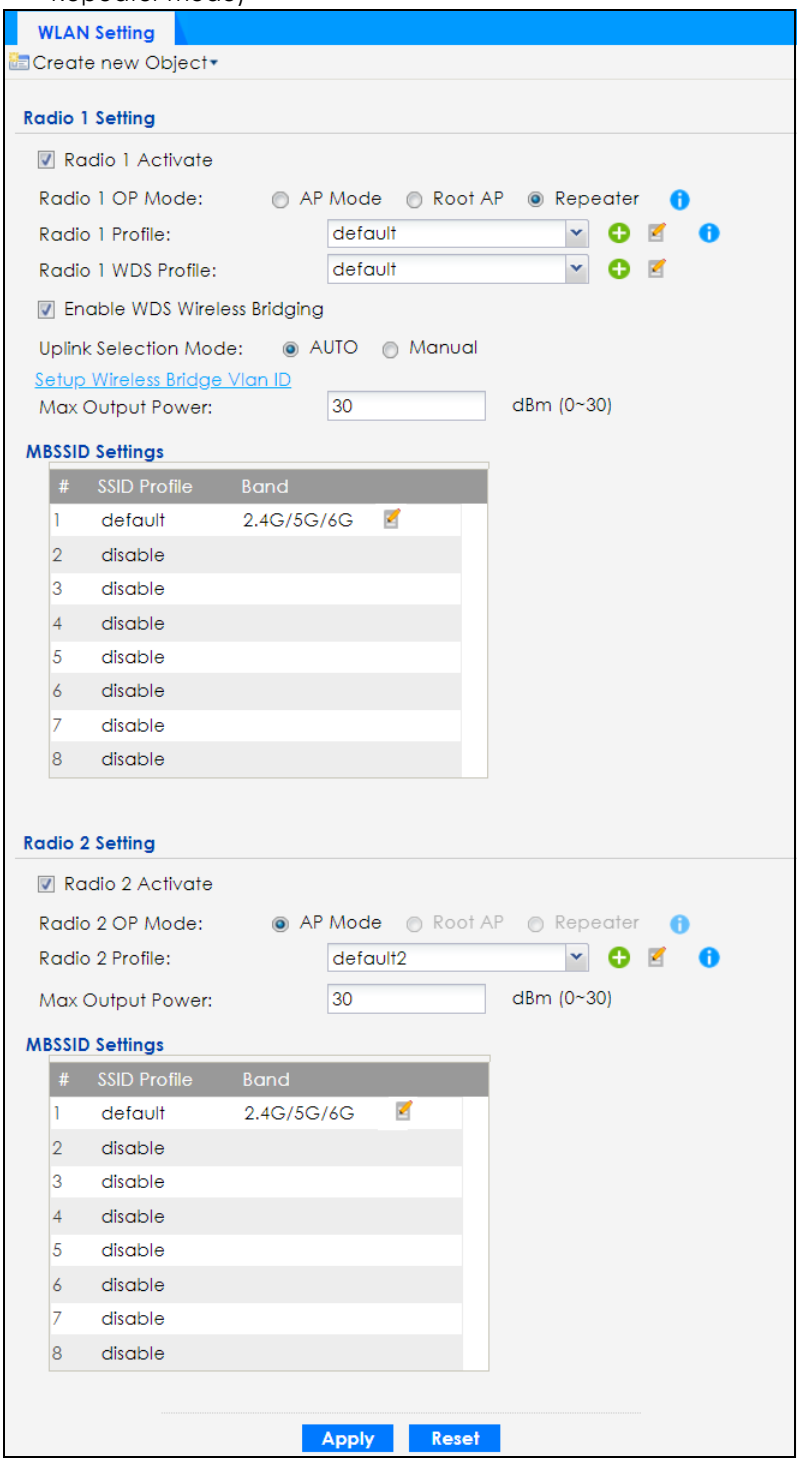
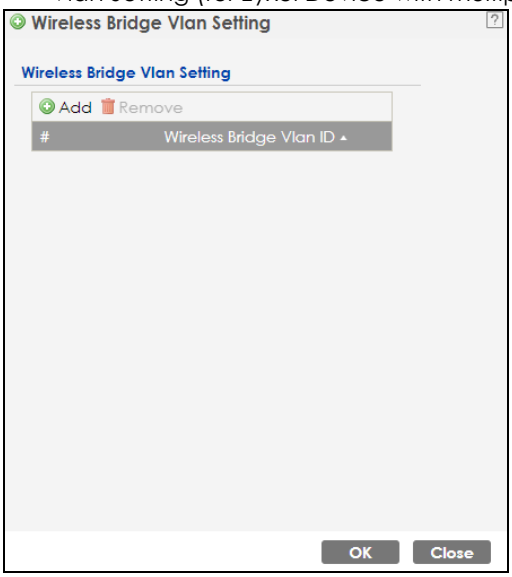


Figure 85 Configuration > Wireless > AP Management > Setup Wireless Bridge Vlan ID: Wireless Bridge Vlan Setting (for Zyxel Device with multiple Ethernet ports)



Each field is described in the following table.

Table 47 Configuration > Wireless > AP Management

LABEL	DESCRIPTION
Radio 1 Setting	
Radio 1 Activate	Select the checkbox to enable the Zyxel Device's first (default) radio.
Radio 1 OP Mode	Select the operating mode for radio 1. **AP Mode** means the radio can receive connections from WiFi clients and pass their data traffic through to the Zyxel Device to be managed (or subsequently passed on to an upstream gateway for managing). **Root AP** means the radio acts as an AP and also supports the wireless connections with other APs (in repeater mode) to form a WDS (Wireless Distribution System) to extend its wireless network. **Repeater** means the radio can establish a wireless connection with other APs (in either root AP or repeater mode) to form a WDS.
Radio 1 Profile	Select the radio profile the radio uses. Note: You can only apply a 2.4G AP radio profile to radio 1. Otherwise, the first radio will not be working.
Add	This button is not available after you configure the Zyxel Device using the wizard. Click the **Add** icon ( )to open a screen where you can create a new entry. For features where the entry's position in the numbered list is important (features where the Zyxel Device applies the table's entries in order like the SSID for example), you can select an entry and click **Add** to create a new entry after the selected entry.
Radio 1 WDS Profile	This field is available only when the radio is in **Root AP** or **Repeater** mode. Select the WDS profile the radio uses to connect to a root AP or repeater.

Table 47 Configuration > Wireless > AP Management (continued)

LABEL	DESCRIPTION
Enable WDS Wireless Bridging	Not all models support this feature. See Section 1.2 on page 14 for models that support wireless bridge. If you set the Zyxel Device as a root AP, the radio that's bridging with the Zyxel Device should be in repeater mode. Be careful to avoid bridge loops. For example, if your root AP and the Zyxel Device are connected to a switch, and they're also connected to each other using a WiFi connection. This will create bridge loops. This field is available only when the radio is in **Repeater** mode. Select this to enable WDS wireless bridging on the Zyxel Device to establish wireless links with other APs. See Section 1.3 on page 24 for more information on Wireless Distribution System (WDS). Note: You must enable the same WiFi security settings on the Zyxel Device and on all WiFi clients that you want to associate with it.
Uplink Selection Mode	This field is available only when the radio is in **Repeater** mode. Select **AUTO** to have the Zyxel Device automatically use the settings in the applied WDS profile to connect to a root AP or repeater. Select **Manual** to have the Zyxel Device connect to the root AP or repeater with the MAC address specified in the **Radio 1 Uplink MAC Address** field.
Setup Wireless Bridge Vlan ID	This appears if you select **Enable WDS Wireless Bridging**. Click this to show the **Wireless Bridge Vlan Setting** pop-up window. This link is available only when the radio is in **Root AP** or **Repeater** mode.
Wireless Bridge Vlan Setting	
Add	Click this to add an entry in the table.
Remove	Select an entry and click this to remove the selected entry.
#	This field is a sequential value. It is not associated with any VLAN ID.
Wireless Bridge Vlan ID	Enter a VLAN ID for the wireless bridge. The VLAN IDs you set on your root AP should be the same as the VLAN ID you set here. See Section 1.3 on page 24 for more information on wireless bridge.
OK	Click **OK** to save your changes back to the Zyxel Device.
Close	Click **Close** to close the pop-up window without saving your changes.
Max Output Power	Enter the maximum output power (between 0 to 30 dBm) of the Zyxel Device in this field. If there is a high density of APs in an area, decrease the output power of the Zyxel Device to reduce interference with other APs. Note: Reducing the output power also reduces the Zyxel Device's effective broadcast radius.
MBSSID Settings	
Edit	Click the **Edit** icon ( )to open a screen where you can modify the entry's settings. In some tables you can just click a table entry and edit it directly in the table. For those types of tables small red triangles display for table entries with changes that you have not yet applied.
#	This field shows the index number of the SSID
SSID Profile	This field displays the SSID profile that is associated with the radio profile.
Band	This field displays the frequency bands to which the SSID profile is applicable. If the SSID profile is not applicable to the current radio, the SSID profile will not be enabled. You can configure the SSID profile's applicable frequency bands in the **Edit SSID Profile** screen (click the **Edit** button next to the profile).

Table 47 Configuration > Wireless > AP Management (continued)

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

Table 47 Configuration > Wireless > AP Management (continued)

LABEL	DESCRIPTION
Remove	Select an entry and click this to remove the selected entry.
#	This field is a sequential value. It is not associated with any VLAN ID.
Wireless Bridge Vlan ID	Enter a VLAN ID for the wireless bridge. The VLAN IDs you set on your root AP should be the same as the VLAN ID you set here. See Section 1.3 on page 24 for more information on wireless bridge.
OK	Click **OK** to save your changes back to the Zyxel Device.
Close	Click **Close** to close the pop-up window without saving your changes.
Max Output Power	Enter the maximum output power (between 0 to 30 dBm) of the Zyxel Device in this field. If there is a high density of APs in an area, decrease the output power of the Zyxel Device to reduce interference with other APs. Note: Reducing the output power also reduces the Zyxel Device's effective broadcast radius.
MBSSID Settings	
Edit	Click **Edit** ( )to open a screen where you can modify the entry's settings. In some tables you can just click a table entry and edit it directly in the table. For those types of tables small red triangles display for table entries with changes that you have not yet applied.
#	This field shows the index number of the SSID
SSID Profile	This field shows the SSID profile that is associated with the radio profile.
Band	This field displays the radio bands to which the SSID profile is applicable. If the SSID profile is not applicable to the current radio, the SSID profile will not be enabled. You can configure the SSID profile's applicable radio bands in the **Edit SSID Profile** screen (click the **Edit** button next to the profile).
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

11.3 Rogue AP

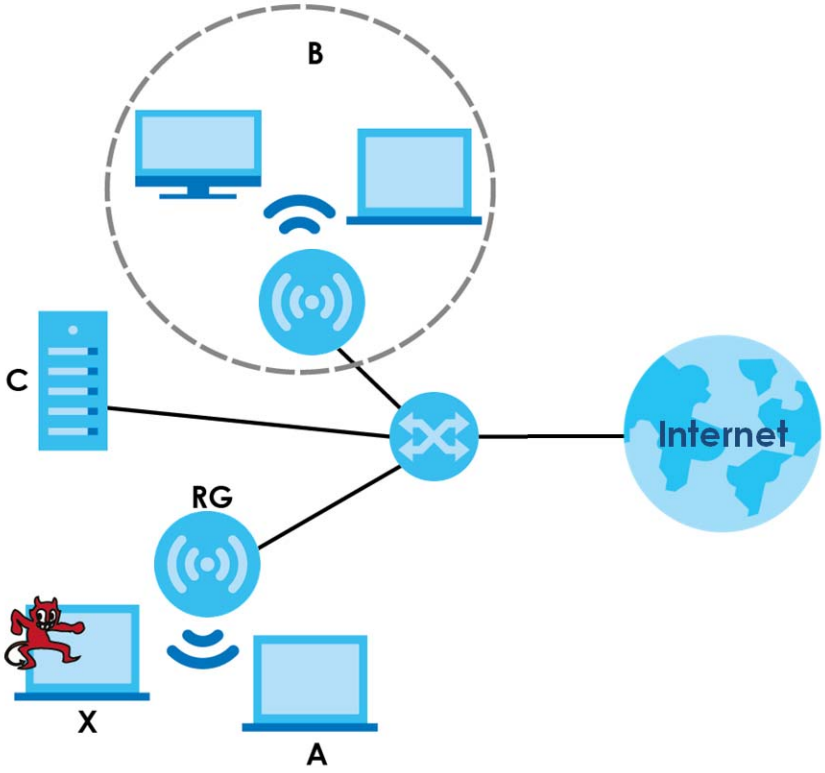
Use this screen to enable **Rogue AP Detection** and import/export a rogue or friendly AP list in a txt file. Click **Configuration > Wireless > Rogue AP** to access this screen.

Rogue APs

A rogue AP is a wireless access point operating in a network's coverage area that is not under the control of the network administrator, and which can potentially open up holes in a network's security.

In the following example, a corporate network's security is compromised by a rogue AP (**RG**) set up by an employee at his workstation in order to allow him to connect his notebook computer wirelessly (**A**). The company's legitimate WiFi network (the dashed ellipse **B**) is well-secured, but the rogue AP uses inferior security that is easily broken by an attacker (**X**) running readily available encryption-cracking software. In this example, the attacker now has access to the company network, including sensitive data stored on the file server (**C**).

Figure 86 Rogue AP Example



Friendly APs

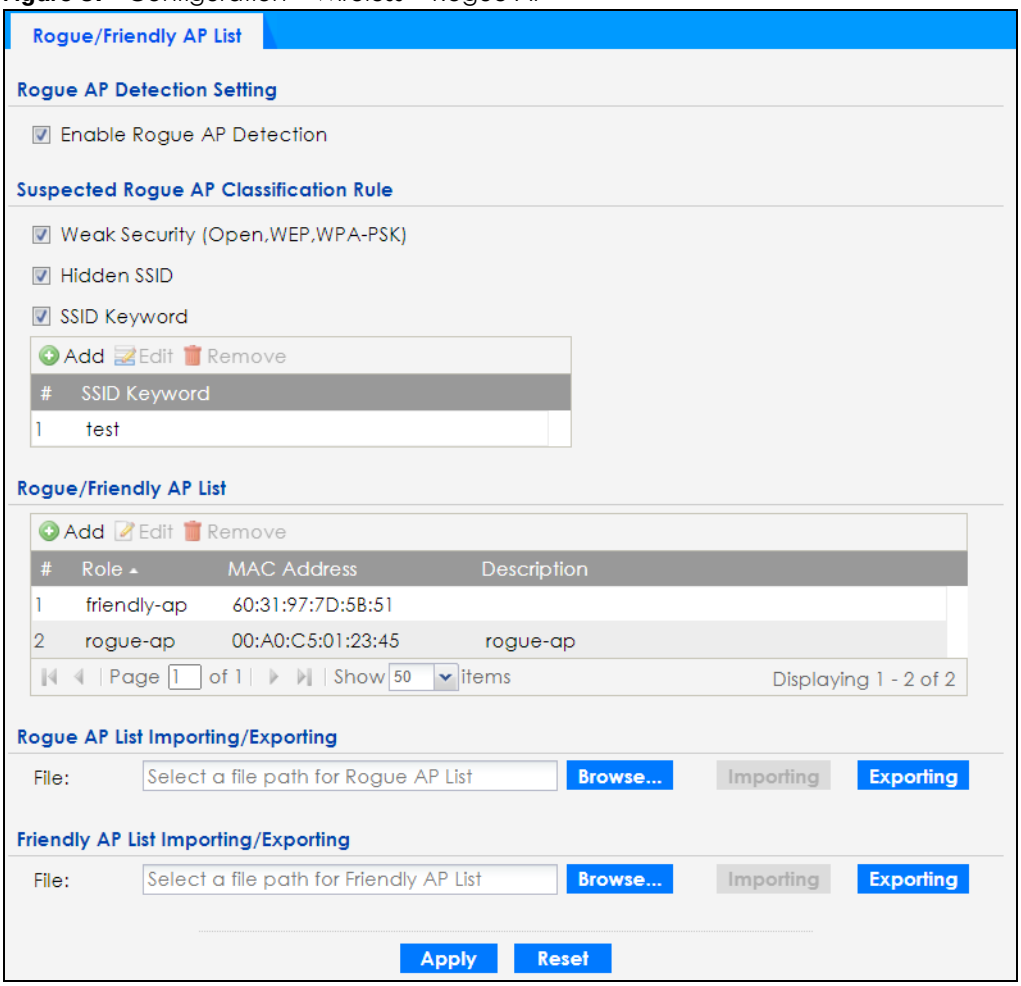
If you have more than one AP in your WiFi network, you should also configure a list of "friendly" APs. Friendly APs are wireless access points that you know are not a threat. It is recommended that you export (save) your list of friendly APs often, especially if you have a network with a large number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

Rogue AP Detection

This feature allows the Zyxel Device to monitor the WiFi signals for other wireless APs (see also Section 1.3.1 on page 29). Detected APs will appear in the **Monitor > Wireless > Detected Device** screen, where the Zyxel Device will label APs with the criteria you select in **Suspected Rogue AP Classification Rule** as a suspected rogue. The APs which you mark as either rogue or friendly APs in the **Monitor > Wireless > Detected Device** screen will appear in the **Wireless > Rogue AP** screen. See Section 1.2 on page 14 to know which models support **Rogue AP Detection**.

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

Figure 87 Configuration > Wireless > Rogue AP



Each field is described in the following table.

Table 48 Configuration > Wireless > Rogue AP

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

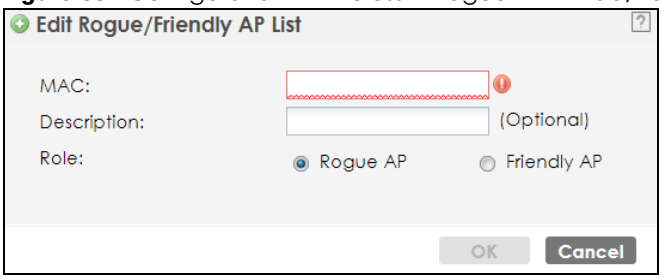
Table 48 Configuration > Wireless > Rogue AP (continued)

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

11.3.1 Add/Edit Rogue/Friendly List

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

Figure 88 Configuration > Wireless > Rogue AP > Add/Edit Rogue/Friendly AP List



Each field is described in the following table.

Table 49 Configuration > Wireless > Rogue AP > Add/Edit Rogue/Friendly AP List

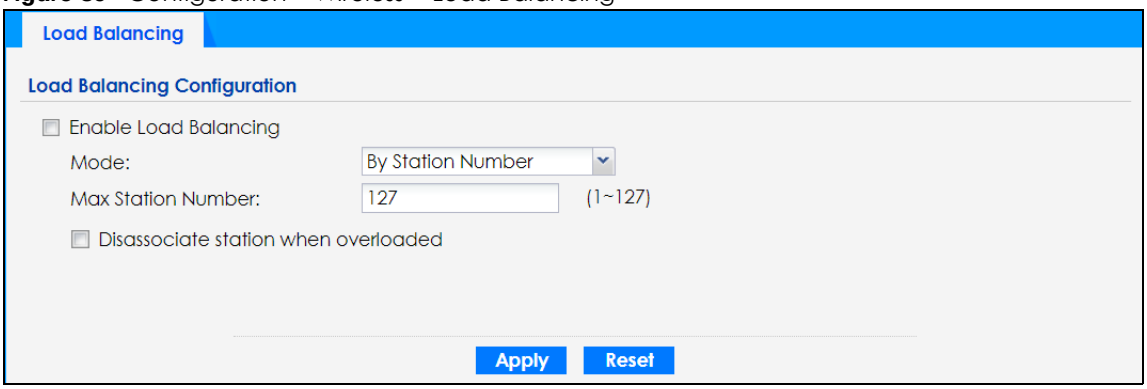
LABEL	DESCRIPTION
MAC	Enter the MAC address of the AP you want to add to the list. A MAC address is a unique hardware identifier in the following hexadecimal format: xx:xx:xx:xx:xx:xx where xx is a hexadecimal number separated by colons.
Description	Enter up to 60 characters for the AP's description.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

11.4 Load Balancing

Use this screen to configure wireless network traffic load balancing between the APs on your network (see Load Balancing on page 152). Click **Configuration > Wireless > Load Balancing** to access this screen.

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

Figure 89 Configuration > Wireless > Load Balancing



Each field is described in the following table.

Table 50 Configuration > Wireless > Load Balancing

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

Table 50 Configuration > Wireless > Load Balancing (continued)

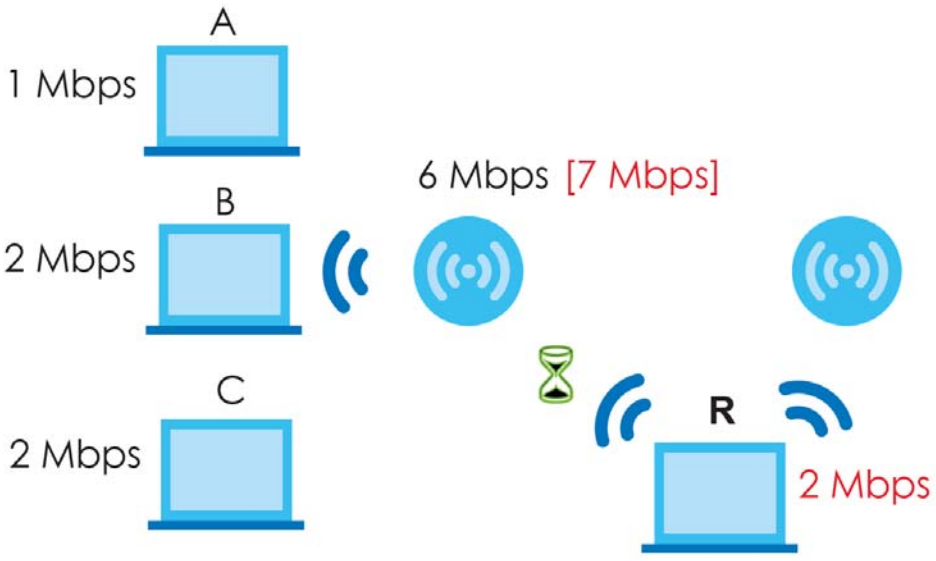
LABEL	DESCRIPTION
Disassociate station when overloaded	This function is enabled by default and the disassociation priority is always **Signal Strength** when you set **Mode** to **By Smart Classroom**. Select this option to disassociate WiFi clients connected to the AP when it becomes overloaded. If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

11.4.1 Disassociating and Delaying Connections

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

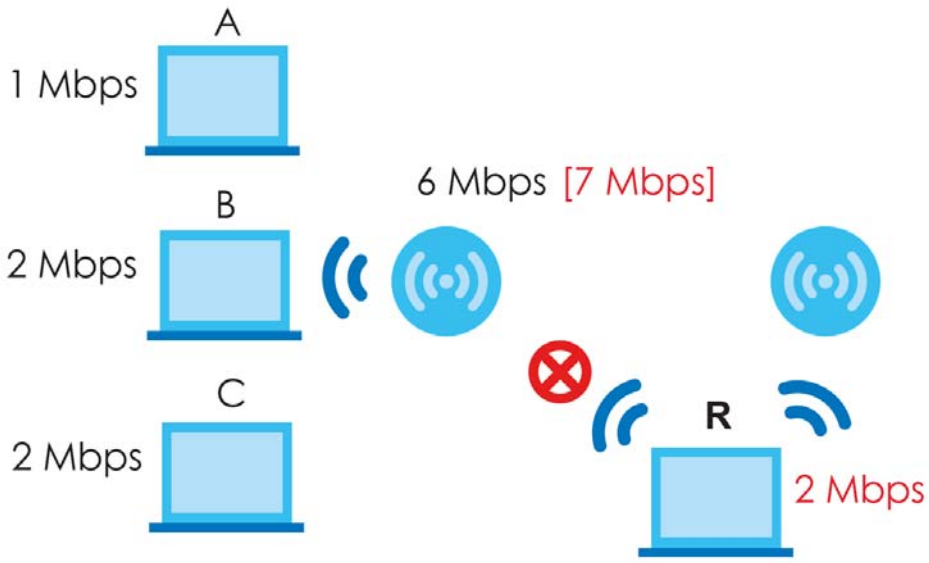
For example, here the AP has a balanced bandwidth allotment of 6 Mbps. If laptop **R** connects and it pushes the AP over its allotment, say to 7 Mbps, then the AP delays the red laptop's connection until it can afford the bandwidth or the laptop is picked up by a different AP with bandwidth to spare.

Figure 90 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 91 Disassociating with a Client

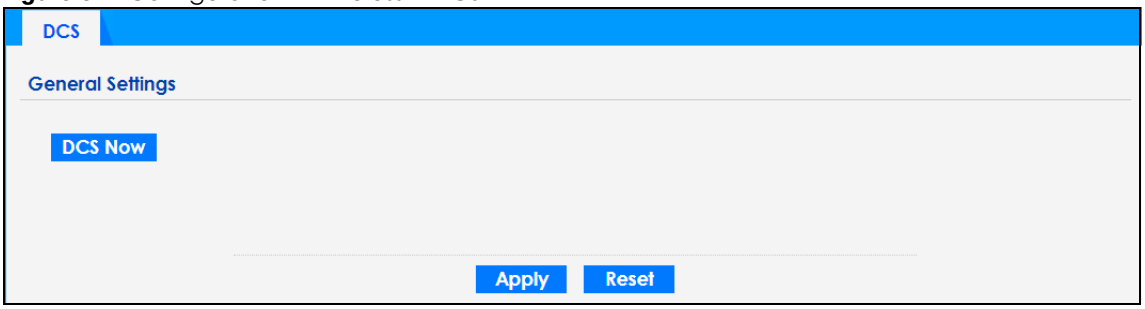


Connections are cut based on either **idle timeout** or **signal strength**. The Zyxel Device first looks to see which devices have been idle the longest, then starts kicking them in order of highest idle time. If no connections are idle, the next criteria the Zyxel Device analyzes is signal strength.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

11.5 DCS

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

Figure 92 Configuration > Wireless > DCS



Each field is described in the following table.

Table 51 Configuration > Wireless > DCS

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

11.6 Technical Reference

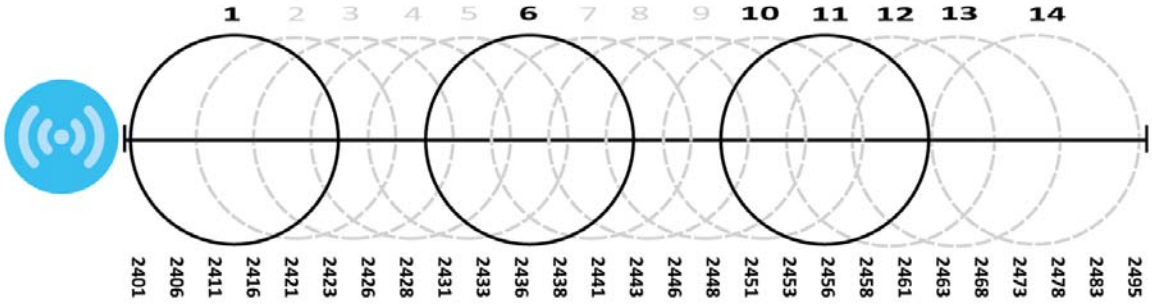
The following section contains additional technical information about the features described in this chapter.

Dynamic Channel Selection

When numerous APs broadcast within a given area, they introduce the possibility of heightened radio interference, especially if some or all of them are broadcasting on the same radio channel. If the interference becomes too great, then the network administrator must open his AP configuration options and manually change the channel to one that no other AP is using (or at least a channel that has a lower level of interference) in order to give the connected stations a minimum degree of interference. Dynamic channel selection frees the network administrator from this task by letting the AP do it automatically. The AP can scan the area around it looking for the channel with the least amount of interference.

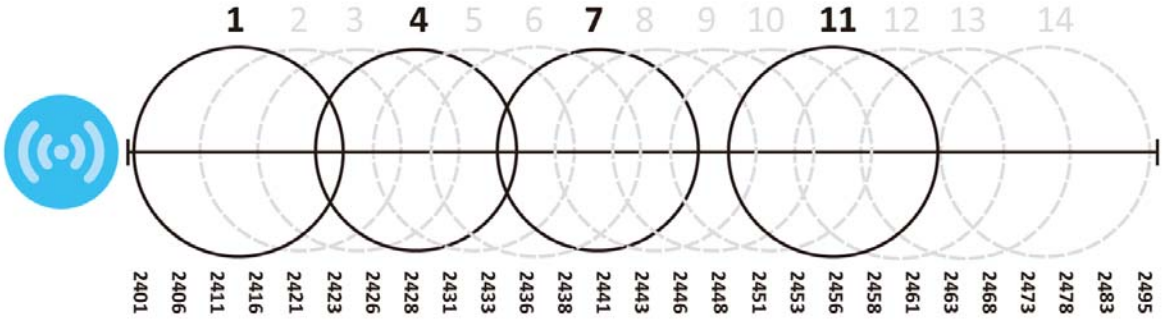
In the 2.4 GHz spectrum, each channel from 1 to 13 is broken up into discrete 22 MHz segments that are spaced 5 MHz apart. Channel 1 is centered on 2.412 GHz while channel 13 is centered on 2.472 GHz.

Figure 93 An Example Three-Channel Deployment



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

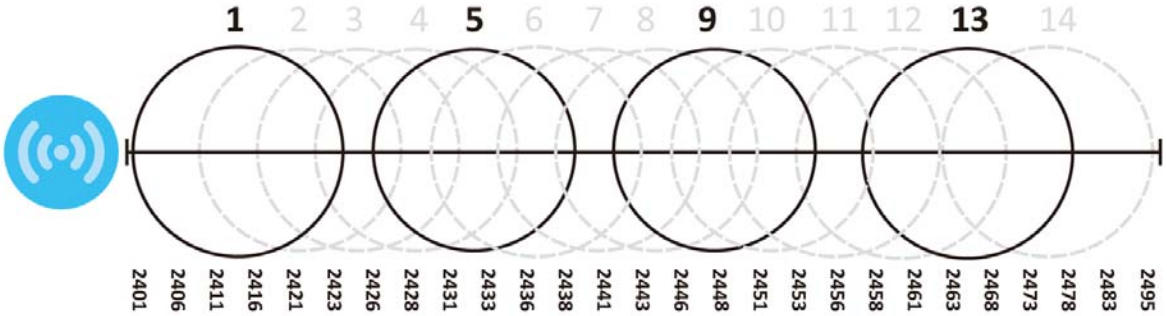
Figure 94 An Example Four-Channel Deployment



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 95 An Alternative Four-Channel Deployment



Load Balancing

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

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

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

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

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

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

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

CHAPTER 12
Bluetooth

12.1 Overview

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

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

12.1.1 What You Need To Know

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

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

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

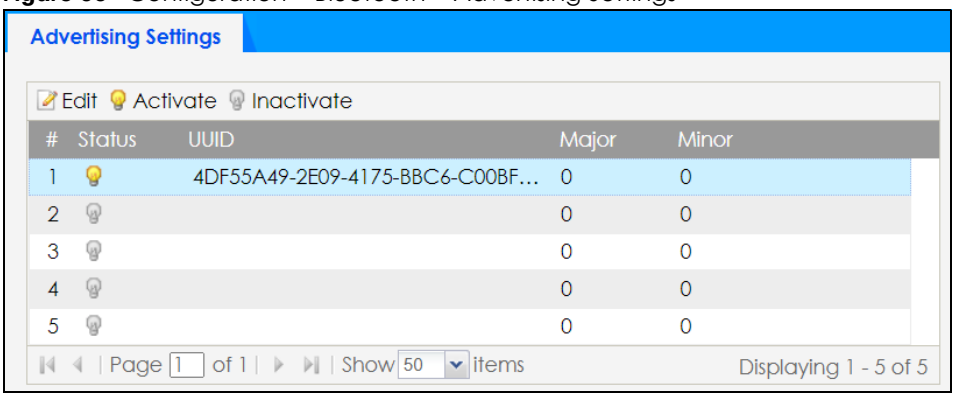
Developers can create apps that respond to the iBeacon ID that your Zyxel Device broadcasts. An app that is associated with the Zyxel Device's iBeacon ID can measure the proximity of a customer to a beacon. This app can then push messages or trigger prompts and actions based on this information. This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

12.2 Bluetooth Advertising Settings

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

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

Figure 96 Configuration > Bluetooth > Advertising Settings



The following table describes the labels in this screen.

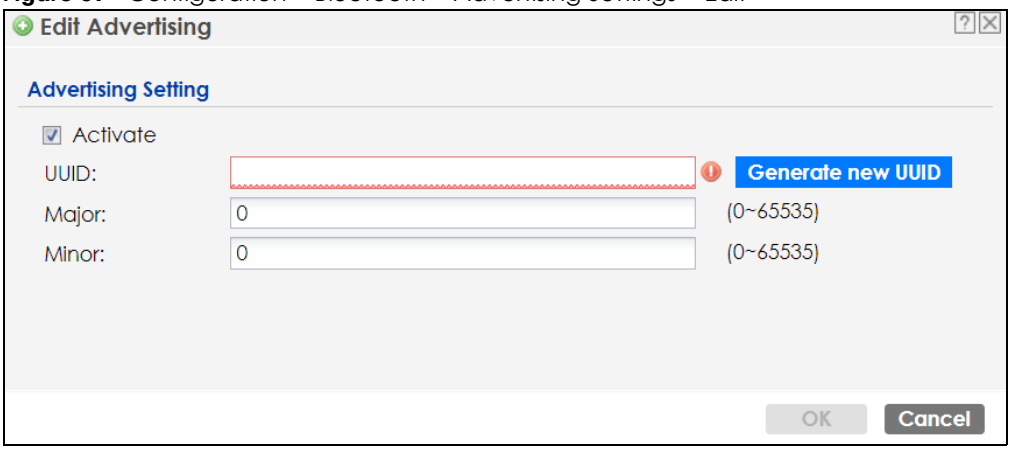
Table 52 Configuration > Bluetooth > Advertising Settings

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

12.2.1 Edit Advertising Settings

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

Figure 97 Configuration > Bluetooth > Advertising Settings > Edit



The following table describes the labels in this screen.

Table 53 Configuration > Bluetooth > Advertising Settings > Edit

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

CHAPTER 13
User

13.1 Overview

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

13.1.1 What You Can Do in this Chapter

- The **User** screen (see Section 13.2 on page 157) provides a summary of all user accounts.
- The **Setting** screen (see Section 13.3 on page 159) controls default settings, login settings, lockout settings, and other user settings for the Zyxel Device.

13.1.2 What You Need To Know

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

User Account

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

User Types

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

Table 54 Types of User Accounts

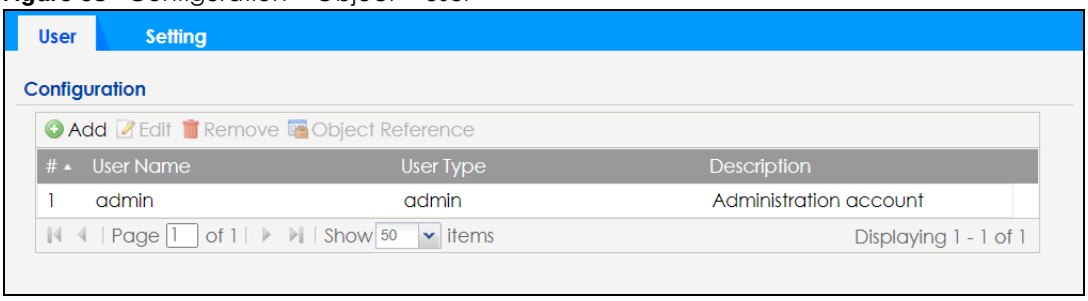
TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
admin	Change Zyxel Device configuration (web, CLI)	WWW, SSH, FTP
limited-admin	Look at Zyxel Device configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, SSH
Access Users		
user	Used for the embedded RADIUS server and SNMPv3 user access Browse user-mode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

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

13.2 User Summary

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

Figure 98 Configuration > Object > User



The following table describes the labels in this screen.

Table 55 Configuration > Object > User

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

13.2.1 Add/Edit User

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

13.2.1.1 Rules for User Names

Enter a user name from 1 to 31 characters.

The user name can only contain the following characters:

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

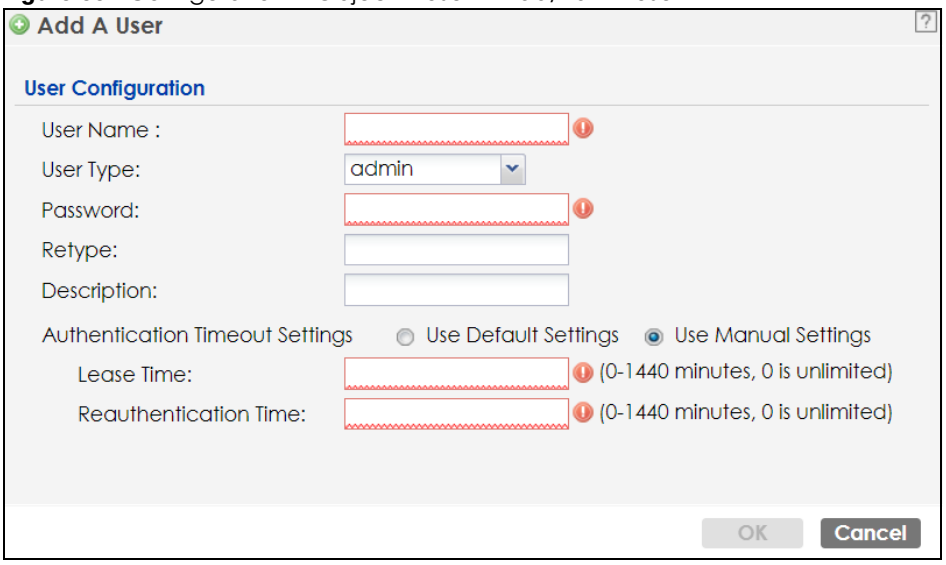
The first character must be alphabetical (A-Z a-z), an underscore (_), or a dash (-). Other limitations on user names are:

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

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

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

Figure 99 Configuration > Object > User > Add/Edit A User



The following table describes the labels in this screen.

Table 56 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 56 Configuration > User > User > Add/Edit a User (continued)

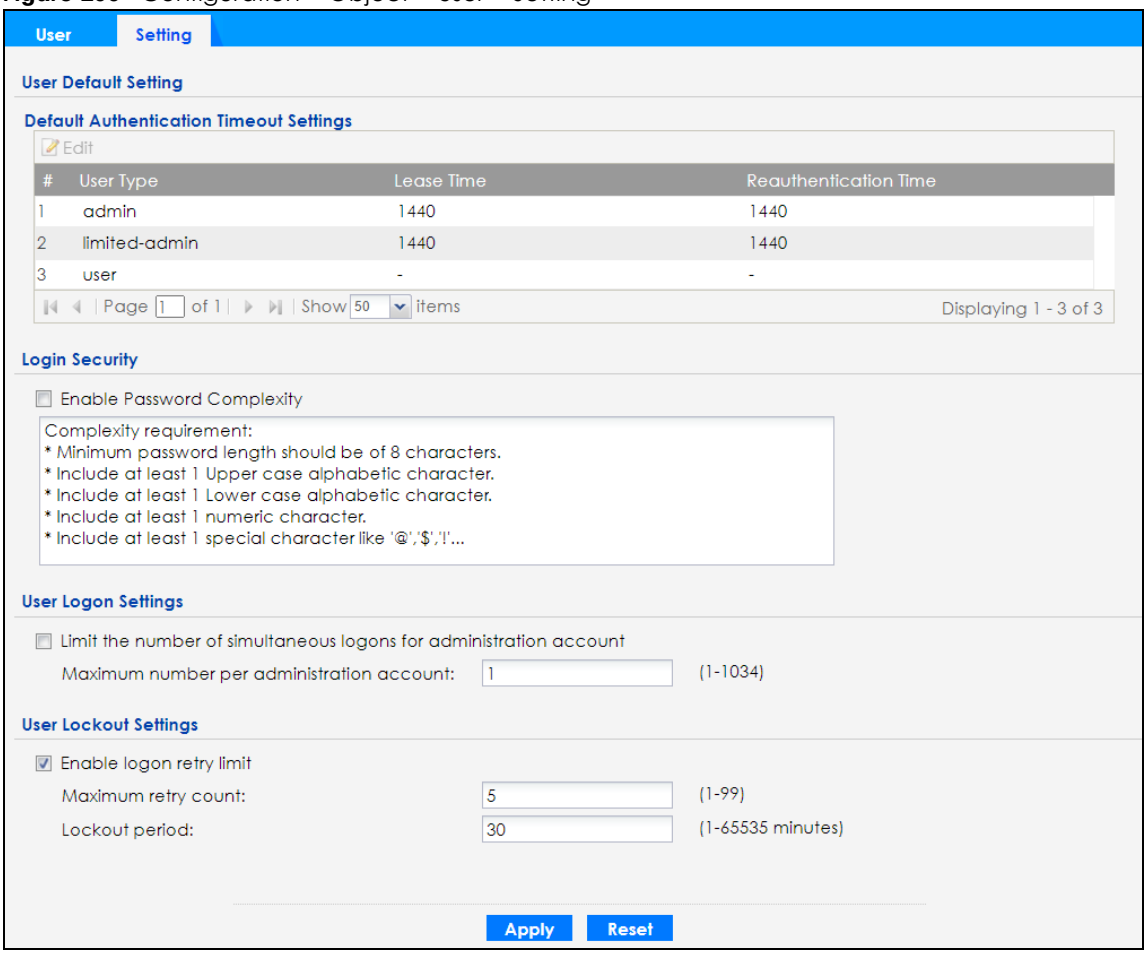
LABEL	DESCRIPTION
Authentication Timeout Settings	This field is not available if the user type is **user**. If you want to set authentication timeout to a value other than the default settings, select **Use Manual Settings** then fill your preferred values in the fields that follow. Otherwise, select **Use Default Settings** to use the default settings displayed below.
Lease Time	This field is not available if the user type is **user**. Enter the number of minutes this user has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Admin users renew the session every time the main screen refreshes in the Web Configurator.
Reauthentication Time	This field is not available if the user type is **user**. Type the number of minutes this user can be logged into the Zyxel Device in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike **Lease Time**, the user has no opportunity to renew the session without logging out.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

13.3 Setting

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

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

Figure 100 Configuration > Object > User > Setting



The following table describes the labels in this screen.

Table 57 Configuration > Object > User > Setting

LABEL	DESCRIPTION
User Default Setting	
Default Authentication Timeout Settings	These authentication timeout settings are used by default when you create a new user account. They also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentication timeout settings.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
#	This field is a sequential value, and it is not associated with a specific entry.
User Type	These are the kinds of user account the Zyxel Device supports. • **admin** - this user can look at and change the configuration of the Zyxel Device • **limited-admin** - this user can look at the configuration of the Zyxel Device but not to change it • **user** - this is used for embedded RADIUS server and SNMPv3 user access
Lease Time	This is the default lease time in minutes for each type of user account. It defines the number of minutes the user has to renew the current session before the user is logged out. Admin users renew the session every time the main screen refreshes in the Web Configurator.

Table 57 Configuration > Object > User > Setting (continued)

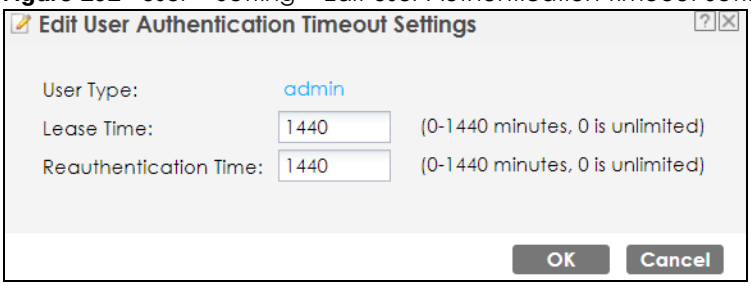
LABEL	DESCRIPTION
Reauthentication Time	This is the default reauthentication time in minutes for each type of user account. It defines the number of minutes the user can be logged into the Zyxel Device in one session before having to log in again. Unlike **Lease Time**, the user has no opportunity to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

13.3.1 Edit User Authentication Timeout Settings

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

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

Figure 101 User > Setting > Edit User Authentication Timeout Settings



The following table describes the labels in this screen.

Table 58 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 checkbox on their screen as well. In this case, the session is automatically renewed before the lease time expires.
Reauthentication Time	Type the number of minutes this type of user account can be logged into the Zyxel Device in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike **Lease Time**, the user has no opportunity to renew the session without logging out.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

CHAPTER 14
AP Profile

14.1 Overview

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

14.1.1 What You Can Do in this Chapter

- The **Radio** screen (Section 14.2 on page 168) creates radio configurations that can be used by the APs.
- The **SSID** screen (Section 14.3 on page 176) configures three different types of profiles for your networked APs.

14.1.2 What You Need To Know

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

Wireless Profiles

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

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

SSID

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

WEP

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

WPA2

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

WPA3

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

Personal vs Enterprise

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

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

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

IEEE 802.1X

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

IEEE 802.11k/v Assisted Roaming

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

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

WiFi 6 (IEEE 802.11ax)

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

Faster Data Transmission

WiFi 6 allows faster data transmission using:

- 1024-QAM (Quadrature Amplitude Modulation) – enhances the data capacity of each transmission unit.
- 160 MHz Channel Bandwidth – extends the supported channel bandwidth to 160 MHz, providing higher data throughput.

Enhanced Air Time Utilization

WiFi 6 increases transmission performance in high-density environments, such as a campus or a company office that have multiple client devices using:

- OFDMA (Orthogonal Frequency-Division Multiple Access) – allows multiple WiFi clients to transmit data simultaneously on a single OFDM symbol by dividing sub-carriers into groups as transmission units called Resource Units (RUs). The AP then allocates RUs to different WiFi clients for data transmissions at the same time.
- BSS Coloring – tags traffic by Basic Service Set (BSS) and identifies traffic from overlapping BSSs. The AP can ignore traffic of unrelated BSSs and transmit data when a channel is occupied.
- MU-MIMO (Multiple User-Multiple Input Multiple Output) – enables multiple users to connect to the AP and downlink/uplink traffic simultaneously.

Extended Signal Range

Beamforming – forms the radiating signals into one direction. This enhances the signal strength and extends the signal transmission range.

Extended Battery Life

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

WiFi 6E (IEEE 802.11ax - Extended Standard)

WiFi 6E is an extended standard of WiFi 6 (IEEE 802.11ax). WiFi 6E inherits all the WiFi 6 features and brings with an additional 6 GHz band. The 6 GHz band allows you to avoid possible congested traffic in the lower 2.4 GHz and 5 GHz bands. WiFi clients must support WiFi 6E to connect to an AP using the 6 GHz band.

You must use WPA3 for security with WiFi 6E.

Note: Check your client device's product specification to see if your client device supports the 6 GHz band (WiFi 6E). If not, you should still use the 2.4/5 GHz bands for connection.

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

Table 59 WiFi 6 and WiFi 6E Comparison

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

Table 59 WiFi 6 and WiFi 6E Comparison

FEATURES		WIFI 6	WIFI 6E
Total Spectrum (Up-to)	2.4 GHz	80 MHz	
	5 GHz	500 MHz	
	6 GHz	Not supported.	1200 MHz
Other Features (OFDMA/BSS Coloring/TWT/Two-Way MU-MIMO/ Beamforming/1024-QAM)		The same (WiFi 6E inherits all the features from WiFi 6).	

WiFi 6E MBSSID Beacon Management

The Zyxel Device supports MBSSID (see Section 1.4.1 on page 29), which allows you to create multiple virtual WiFi networks (SSIDs) on the Zyxel Device. With the WiFi 6E (802.11ax-extended) standard, the Zyxel Device divides SSIDs into groups, and includes information of all SSIDs in a group in one SSID beacon. Therefore, the Zyxel Device doesn't need to send beacons for individual SSIDs, which improves air time efficiency.

Note: If you disable a virtual WiFi network (SSID) whose beacon contains the group SSID information, WiFi clients of that group will be disconnected until the AP reselects another SSID to send the beacon.

Out-of-Band Discovery

Out-of-band discovery allows the AP to include information of the 6 GHz band in management frames sent over the 2.4 GHz /5 GHz bands. WiFi 6E clients only need to scan the lower bands (2.4 GHz/5 GHz) to connect to the AP in the 6 GHz band, reducing the discovery time.

PSC Channel (In-Band Discovery)

PSCs (Preferred Scanning Channels) are dedicated channels for WiFi 6E clients to send probe requests on to discover a compatible AP, instead of scanning the entire 6 GHz band. In this way, WiFi 6E clients are able to efficiently discover and connect to the AP within the 6 GHz band.

Note: The available PSCs differ by country for the unlicensed use in the 6 GHz band.

Resource Unit

A resource unit is a portion of a channel bandwidth. For example, a 20 MHz channel can be divided into several resource units. Each resource unit can be allocated to a specified WiFi client, allowing simultaneous data transmission.

WiFi 7 (IEEE802.11be)

WiFi 7 (802.11be) is backward-s compatible with WiFi 6 and WiFi 6E. WiFi 7 is a WiFi standard that supports 2.4 GHz, 5 GHz and 6 GHz frequency bands with the following improvements over WiFi 6 and WiFi 6E.

Table 60 WiFi 6, WiFi 6E and WiFi 7 Comparison

FEATURES	WIFI 6	WIFI 6E	WIFI 7
Theoretical Maximum Speed (Up-to)	The same (9.6 Gbps).		46 Gbps
Supported Frequency Bands	2.4 GHz/5 GHz	2.4 GHz/5 GHz/6 GHz	2.4 GHz/5 GHz/6 GHz
Supported Channel Bandwidth	20/40/80/160 MHz	20/40/80/160 MHz	20/40/80/160/320 MHz

Table 60 WiFi 6, WiFi 6E and WiFi 7 Comparison

FEATURES		WIFI 6	WIFI 6E	WIFI 7
Total Spectrum (Up-to)	2.4 GHz	80 MHz		80 MHz
	5 GHz	500 MHz		500 MHz
	6 GHz	Not supported.	1200 MHz	1200 MHz
Other Features (OFDMA/BSS Coloring/TWT/Two-Way MU-MIMO/ Beamforming/1024-QAM)		The same (WiFi 6E inherits all the features from WiFi 6).		WiFi 7 inherits all the features from WiFi 6 and WiFi 6E, with the addition of multi-link operation and preamble puncturing.

Faster Data Transmission

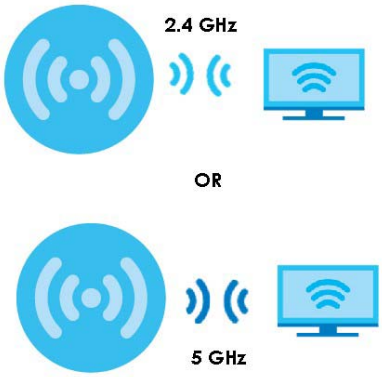
WiFi 7 allows faster data transmission using:

- 4096 QAM (Quadrature Amplitude Modulation)- enhances the amount of data transmitted over the available bandwidth.
- 320 MHz Channel Bandwidth- enlarges the supported channel bandwidth to 320 MHz, allowing higher data throughput.
- Multiple Resource Units (RUs)- allows an AP to allocate multiple RUs to a WiFi client.

Multi-Link Operation (MLO)

An AP can support multiple frequency bands (2.4 GHz, 5 GHz and 6 GHz), but a WiFi client can only connect to the AP using one of these frequency bands. The other frequency bands are unused. The client's data transmission speed depends on the frequency band they are connected to.

Figure 102 Without Multi-Link Operation



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

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

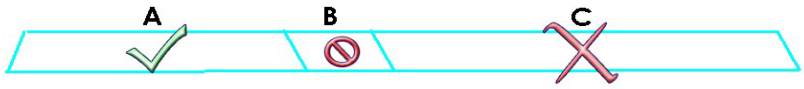
Note: The Zyxel Device does not support MLO at the time of writing.

Figure 103 Multi-Link Operation Example

Preamble Puncturing

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

Figure 104 Without Preamble Puncturing



WiFi 7 preamble puncturing allows you to block the specific portion of the channel that is experiencing interference while continuing to use the rest of the WiFi channel. In the figure below, if part of the WiFi channel (**B**) experiences interference, the rest of the WiFi channel (**C**) is still available.

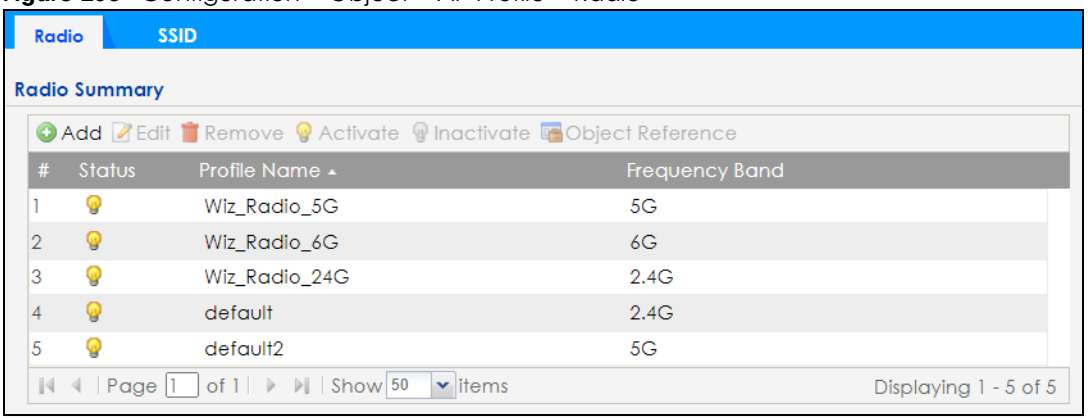
Figure 105 Preamble Puncturing Example

14.2 Radio

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

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

Figure 106 Configuration > Object > AP Profile > Radio



The following table describes the labels in this screen.

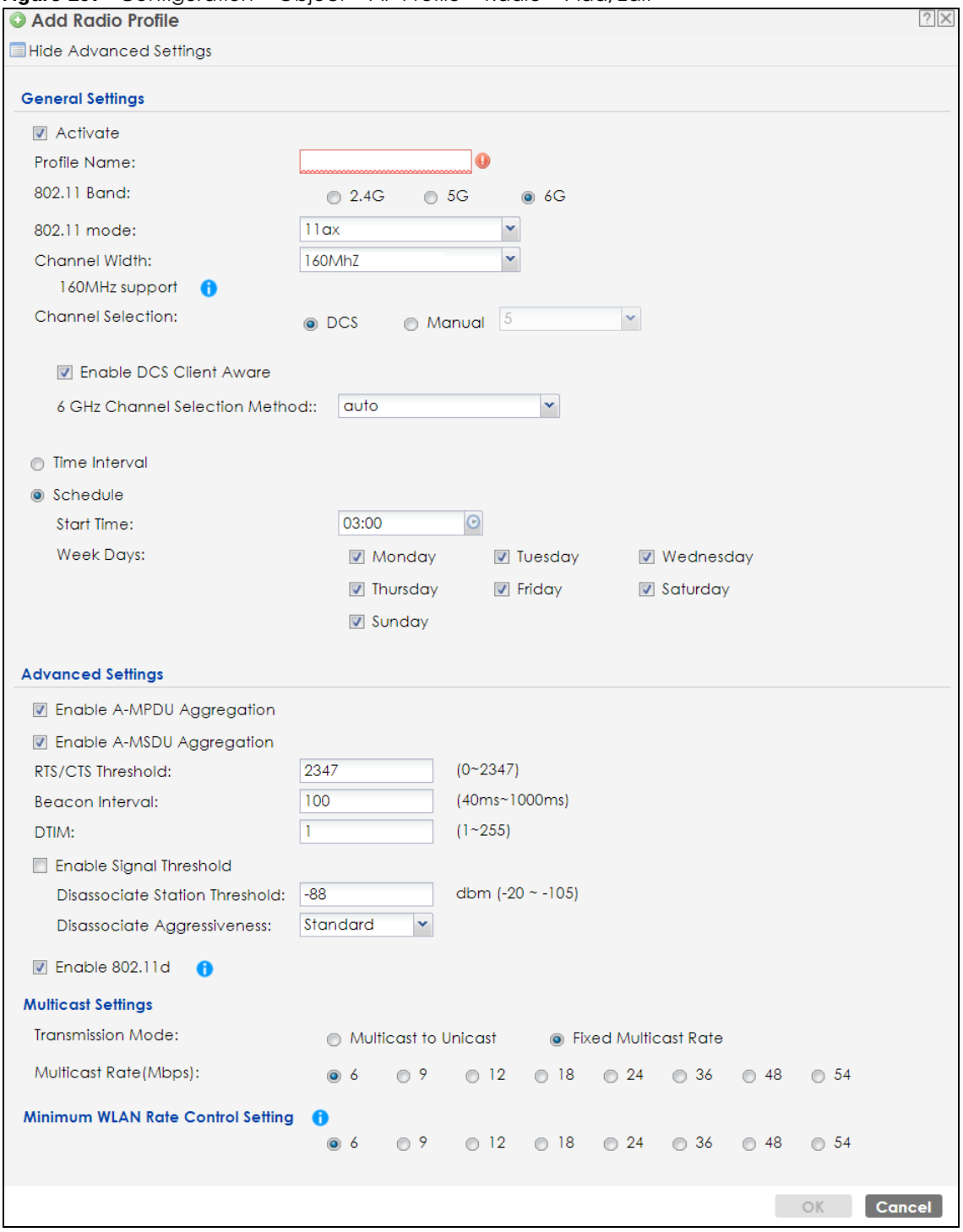
Table 61 Configuration > Object > AP Profile > Radio

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.
Operating Mode	This indicates the radio's operating mode. Operating modes are **AP (MBSSID)**, **Root AP** or **Repeater**.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

14.2.1 Add/Edit Radio Profile

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

Figure 107 Configuration > Object > AP Profile > Radio > Add/Edit



The following table describes the labels in this screen.

Table 62 Configuration > Object > AP Profile > Radio > Add/Edit

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

Table 62 Configuration > Object > AP Profile > Radio > Add/Edit (continued)

LABEL	DESCRIPTION
Channel Width	Select the channel bandwidth you want to use for your WiFi network. See Section 1.2 on page 14 to see the channel bandwidth your Zyxel Device supports. Select **20MHz** if you want to lessen radio interference with other wireless devices in your neighborhood. Select **40MHz** to allow the Zyxel Device to choose the channel bandwidth (20 or 40 MHz) that has least interference. Select **80MHZ** to allow the Zyxel Device to choose the channel bandwidth (20, 40 or 80) that has least interference. This option is available only when you select **11ac** or **11ax** in the **802.11 Mode** field. Select **160MHZ** to allow the Zyxel Device to choose the channel bandwidth (20, 40, 80 or 160MHz) that has least interference. This option is available only when you select **11ax** or **11be** in the **802.11 Mode** field. Select **240MHz** to allow the Zyxel Device to choose the channel bandwidth (20, 40, 80, 160 or 240MHz) that has least interference. This option is available only when you set **802.11 Band** to **5G**, and select **11ax** or **11be** in the **802.11 Mode** field. Select **320MHz** to allow the Zyxel Device to choose the channel bandwidth (20, 40, 80, 160, 240 or 320 MHz) that has least interference. This option is available only when you set **802.11 Band** to **6G**, and select **11be** 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. Note: The available SSID broadcast channels in the 6 GHz band are PSCs (Preferred Scanning Channels). See Section 14.1.2 on page 163.
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 are dropped when it switches channels.
2.4 GHz Channel Selection Method	This field is available when you set **802.11 Band** to **2.4G** and **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.

Table 62 Configuration > Object > AP Profile > Radio > Add/Edit (continued)

LABEL	DESCRIPTION
2.4 GHz Channel Deployment	This is available when you set **802.11 Band** to **2.4G, Channel Selection** to **DCS,** and **2.4 GHz Channel Selection Method** to **auto**. Select **Three-Channel Deployment** to limit channel switching to channels 1,6, and 11, the three channels that are sufficiently attenuated to have almost no impact on one another. In other words, this allows you to minimize channel interference by limiting channel-hopping to these three "safe" channels. Select **Four-Channel Deployment** to limit channel switching to four channels. Depending on the country domain, if the only allowable channels are 1-11 then the Zyxel Device uses channels 1, 4, 7, 11 in this configuration; otherwise, the Zyxel Device uses channels 1, 5, 9, 13 in this configuration. Four channel deployment expands your pool of possible channels while keeping the channel interference to a minimum.
Avoid 5G DFS Channel	This field is available only when you set **802.11 Band** to **5G**, **Channel Selection** to **DCS** and **5 GHz Channel Selection Method** to **auto**. Dynamic Frequency Selection (DFS) is a WiFi channel allocation scheme that allows APs to use channels in the 5 GHz band normally reserved for radar. Before using a DFS channel, an AP must ensure there is no radar present by performing a Channel Availability Check (CAC). This check takes 1-10 minutes, depending on the country in which the AP is located. Select this if you don't want to wait for the Zyxel Device to perform a CAC before using a channel by forcing the Zyxel Device to only use the non-DFS channels. Clear this to allow the Zyxel Device to use the DFS channels for more channel options. The Zyxel Device only switches to a DFS channel when a nearby AP is broadcasting the same SSID the Zyxel Device uses. This allows WiFi clients to switch to connect to the same SSID on another AP when the Zyxel Device is under the CAC process before switching to a 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.
6 GHz Channel Selection Method	This field is available only when you set **802.11 Band** to **6G**, **Channel Selection** to **DCS**. Select how you want to specify the channels the Zyxel Device switches between for 6 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 **6 GHz Channel Selection Method** to **manual**. Select the channels that you want the Zyxel Device to use.
Time Interval	Select this option to have the Zyxel Device survey the other APs within its broadcast radius at the end of the specified time interval.

Table 62 Configuration > Object > AP Profile > Radio > Add/Edit (continued)

LABEL	DESCRIPTION
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 MHz**, **20/40 MHz** or **20/40/80 MHz** 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 WiFi network if you have WiFi clients that are associated with the same AP but out of range of one another. When enabled, a WiFi client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops WiFi clients from transmitting packets at the same time (and causing data collisions). A WiFi 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.
Fragmentation Threshold	This field is only available when you set **802.11 Mode** to **11a** or **11b/g**. A fragmentation threshold is the maximum data fragment size (between 256 and 2436 bytes) that can be sent in the WiFi network before the AP will fragment the packet into smaller data frames. A large fragmentation threshold is recommended for networks not prone to interference. A smaller threshold is recommended for busy networks or networks that are prone to interference.

Table 62 Configuration > Object > AP Profile > Radio > Add/Edit (continued)

LABEL	DESCRIPTION
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.
Enable Signal Threshold	Select the checkbox to use the signal threshold to ensure WiFi clients receive good throughput. This allows only WiFi clients with strong signals to connect to the Zyxel Device. The Zyxel Device will disconnect WiFi clients with signal strengths lower than the **Disassociate Station Threshold** you specify. Clear the checkbox to not require WiFi clients to have a minimum signal strength to keep their connections with the Zyxel Device.
Disassociate Station Threshold	Set a minimum kick-off signal strength. You can set from -20dBm (the strongest signal) to -105dBm (the weakest signal). When a WiFi client's signal strength is lower than the specified threshold, the Zyxel Device checks the traffic between the Zyxel Device and the WiFi client. The Zyxel Device will only disconnect the WiFi client when • the WiFi client signal strength falls below the kick-off strength and • the WiFi client's traffic throughput is below a minimum threshold. You can set the WiFi client's minimum traffic throughput threshold in **Disassociate Aggressiveness**.
Disassociate Aggressiveness	Set the minimum traffic throughput threshold here. **High**: Select this if you don't want the Zyxel Device to disconnect a WiFi client with a weak signal strength (below the kick-off threshold) when the traffic between the Zyxel Device and the WiFi client is heavy. The Zyxel Device will disconnect the WiFi client if the traffic between the Zyxel Device and the WiFi client is medium or low. **Standard**: Select this if you don't want the Zyxel Device to disconnect a WiFi client with a weak signal strength (below the kick-off threshold) when the traffic between the Zyxel Device and the WiFi client is medium. The Zyxel Device will disconnect the WiFi client if the traffic between the Zyxel Device and the WiFi client is low. **Low**: Select this if you don't want the Zyxel Device to disconnect a WiFi client with a weak signal strength (below the kick-off threshold) when the traffic between the Zyxel Device and the WiFi client is low. At the time of writing, the Zyxel Device will disconnect the WiFi client if there's no packet sent between the Zyxel Device and the WiFi client in one second.
Allow 802.11n/ ac/ax stations only	This is not available if **802.11 Band** is set to **6G.** Select this option to allow only 802.11 n/ac/ax clients to connect, and reject 802.11a/b/g clients.
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.
Enable 802.11d	Clear the checkbox to prevent the AP from broadcasting a country code, also called a country Information Element (IE), in beacon frames. This makes the AP incompatible with 802.11d networks and devices. 802.11d is a WiFi network specification that allows the AP to broadcast a country code to WiFi client. The country code indicates where the AP is located. If WiFi clients are unable to connect to the AP due to an incompatible country code, you should disable 802.11d.
Multicast Settings	

Table 62 Configuration > Object > AP Profile > Radio > Add/Edit (continued)

LABEL	DESCRIPTION
Transmission Mode	Specify how the Zyxel Device handles wireless multicast traffic. Select **Multicast to Unicast** to broadcast wireless multicast traffic to all of the WiFi 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 WiFi 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 WiFi clients. For example, to deploy 4 Mbps video, select a fixed multicast rate higher than 4 Mbps.
Minimum WLAN Rate Control Setting	Sets the minimum data rate that 2.4 Ghz WiFi clients can connect at. At the time of writing, the allowed values are: 1, 2, 5. 5, 6, 9, 11, 12, 18, 24, 36, 48, 54 (Mbps). Sets the minimum data rate that 5 Ghz WiFi clients can connect at. At the time of writing, the allowed values are: 6, 9, 12, 18, 24, 36, 48, 54 (Mbps). Sets the minimum data rate that 6 Ghz WiFi clients can connect. At the time of writing, the allowed values are: 6, 9, 12, 18, 24, 36, 48, 54 (Mbps). Increasing the minimum data rate can reduce network overhead and improve WiFi network performance in high density environments. However, WiFi clients that do not support the minimum data rate will not be able to connect to the AP.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

14.3 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 WiFi clients to connect to them; and a MAC filter list, which can limit connections to an AP based on WiFi clients MAC addresses.

14.3.1 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 WiFi network to which a WiFi 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 WiFi 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 108 Configuration > Object > AP Profile > SSID > SSID List (Default)

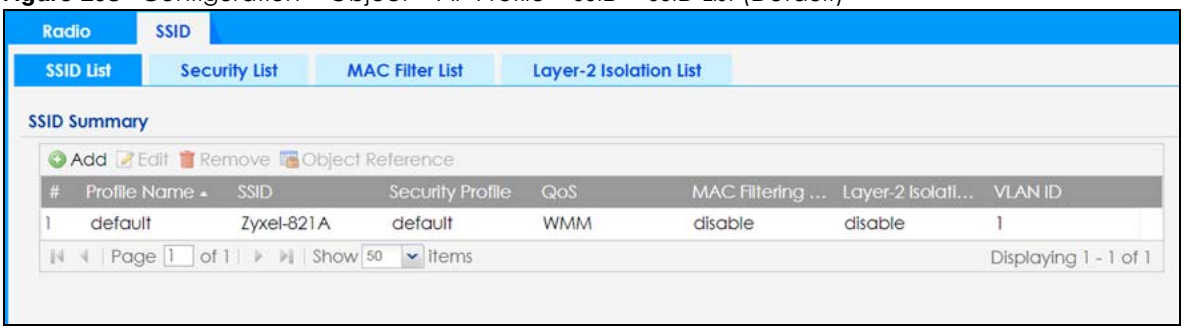
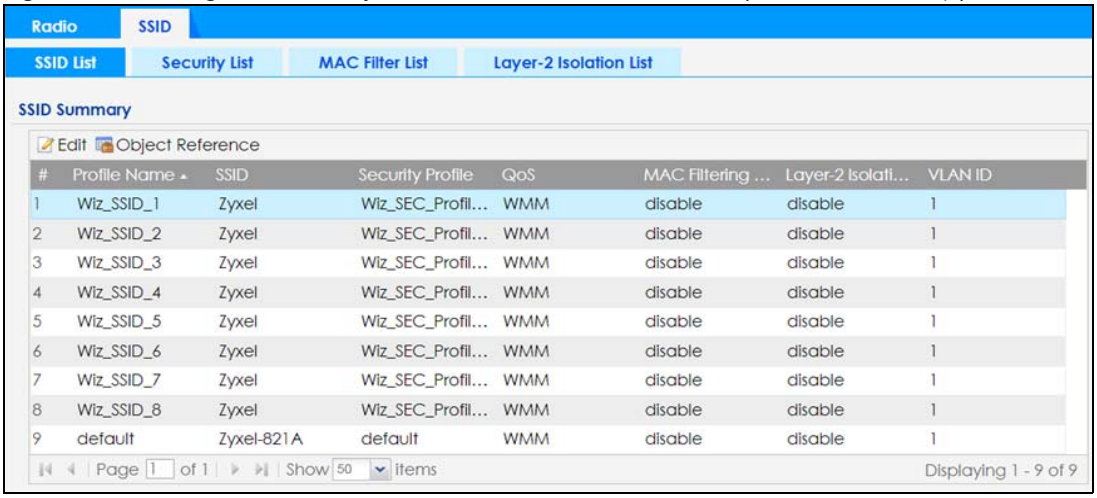


Figure 109 Configuration > Object > AP Profile > SSID > SSID List (After wizard setup)



The following table describes the labels in this screen.

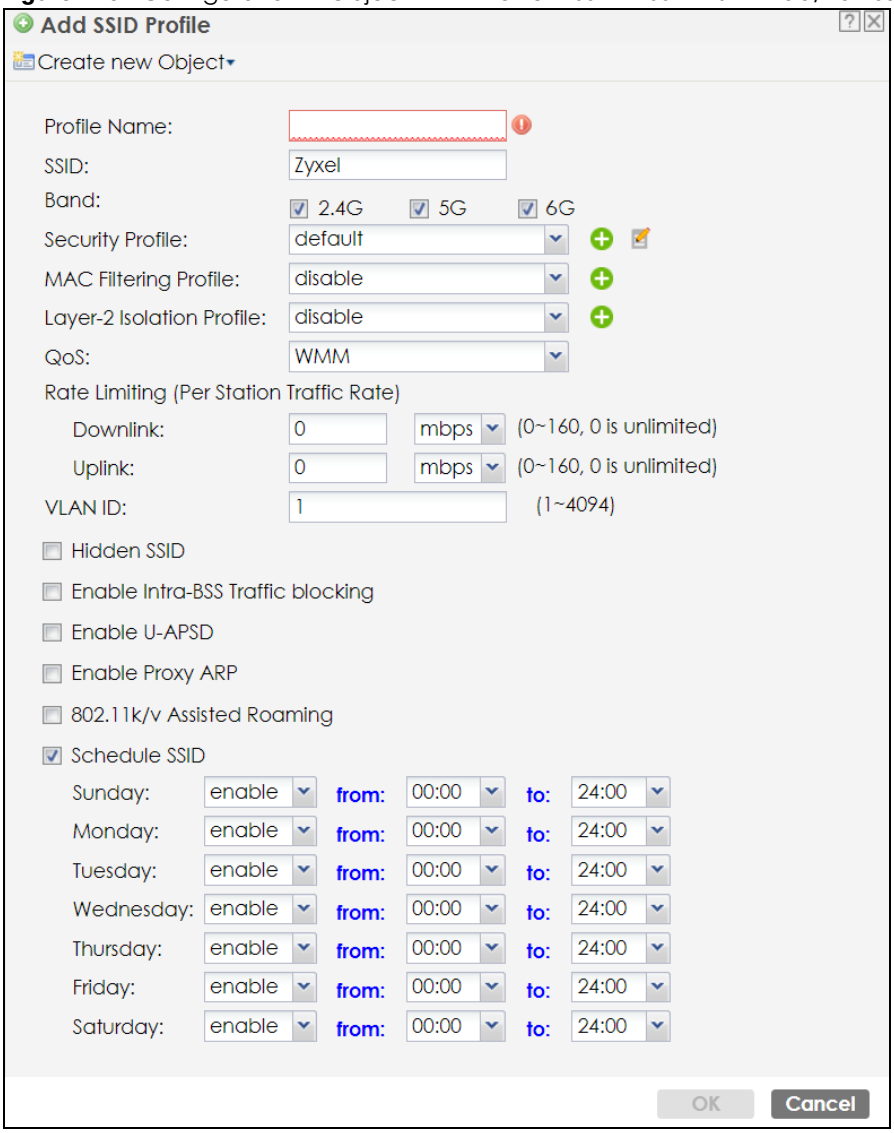
Table 63 Configuration > Object > AP Profile > SSID > SSID List

LABEL	DESCRIPTION
Add	Click this to add a new SSID profile. This button is not available after you configure the Zyxel Device using 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 Device using 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 WiFi clients.
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.

14.3.2 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 110 Configuration > Object > AP Profile > SSID > SSID List > Add/Edit SSID Profile



The following table describes the labels in this screen.

Table 64 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 WiFi clients. Enter up to 32 characters, spaces and underscores are allowed.

Table 64 Configuration > Object > AP Profile > SSID > SSID List > Add/Edit SSID Profile (continued)

LABEL	DESCRIPTION
Band	Select the radio bands to which the SSID profile is applicable. The profile will only work on the radio bands you select. For example, you select **5G** for the SSID profile "Wiz_SSID_1", and apply it on radio 2 (with a radio profile using the 6 GHz band). The SSID profile will not take effect until you set radio 2 to use the 5 GHz band.
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. 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 WiFi clients connecting to your network through a particular SSID by WiFi 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 WiFi clients associated with your Zyxel Device from communicating with other WiFi 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 WiFi 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: **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 (Per Station Traffic Rate)	
Downlink	Define the maximum incoming transmission data rate (either in mbps or kbps) on a per-station basis. The range is from 0–160. Enter 0 to set the maximum rate to unlimited.
Uplink	Define the maximum outgoing transmission data rate (either in mbps or kbps) on a per-station basis. The range is from 0–160. Enter 0 to set the maximum rate to unlimited.
VLAN ID	Enter a VLAN ID for the Zyxel Device to use to tag traffic originating from this SSID. The range is from 1–4094.

Table 64 Configuration > Object > AP Profile > SSID > SSID List > Add/Edit SSID Profile (continued)

LABEL	DESCRIPTION
Hidden SSID	Select this if you want to "hide" your SSID from WiFi clients. This tells any WiFi clients in the vicinity of the AP using this SSID profile not to display its SSID name as a potential connection. Not all WiFi clients respect this flag and display it anyway. When a SSID is "hidden" and a WiFi client cannot see it, the only way you can connect to the SSID is by manually entering the SSID name in your WiFi 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 BSSID 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 WiFi 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.

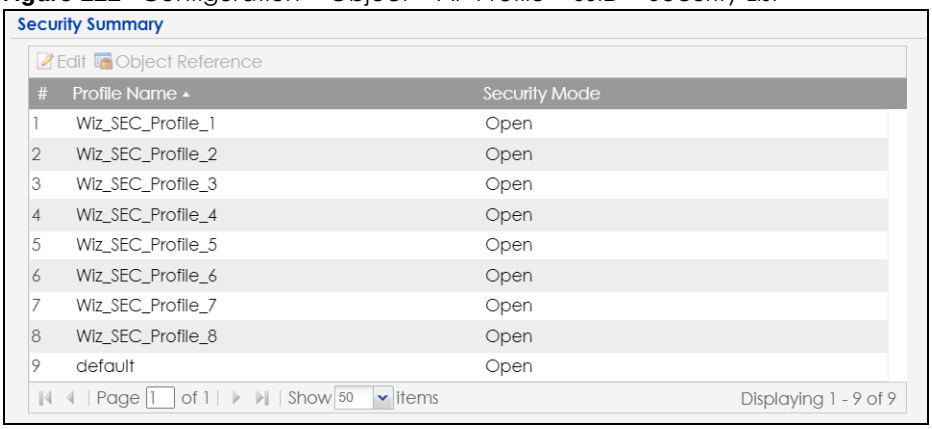
14.4 Security List

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 111 Configuration > Object > AP Profile > SSID > Security List



The following table describes the labels in this screen.

Table 65 Configuration > Object > AP Profile > SSID > Security List

LABEL	DESCRIPTION
Add	Click this to add a new security profile. This button is not available after you configure the Zyxel Device using the wizard.
Edit	Click this to edit the selected security profile.
Remove	Click this to remove the selected security profile. This button is not available after you configure the Zyxel Device using the wizard.
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).

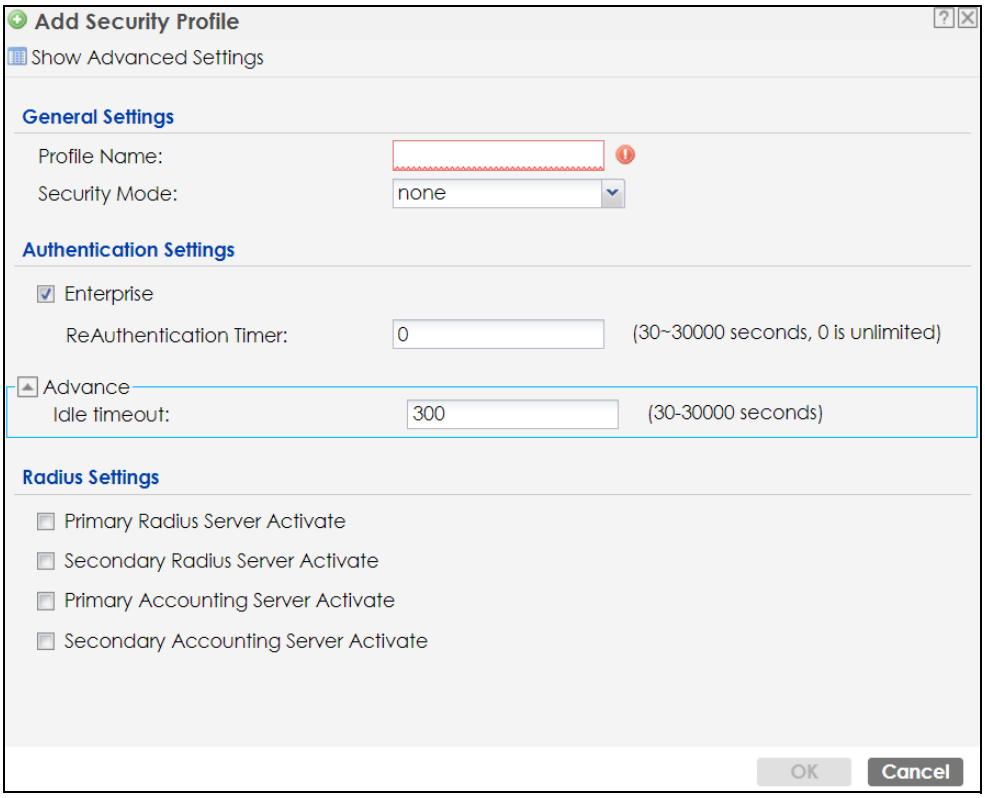
14.4.1 Add/Edit Security Profile

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.

These screens' options change based on the **Security Mode** selected.

Note: 6 GHz SSIDs only support WPA3 encryption. The Zyxel Device will automatically use WPA3 encryption for 6 GHz SSIDs (SSIDs used by the 6 GHz radio) regardless of the **Security Mode** you select here.

Figure 112 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: none



The following table describes the labels in this screen.

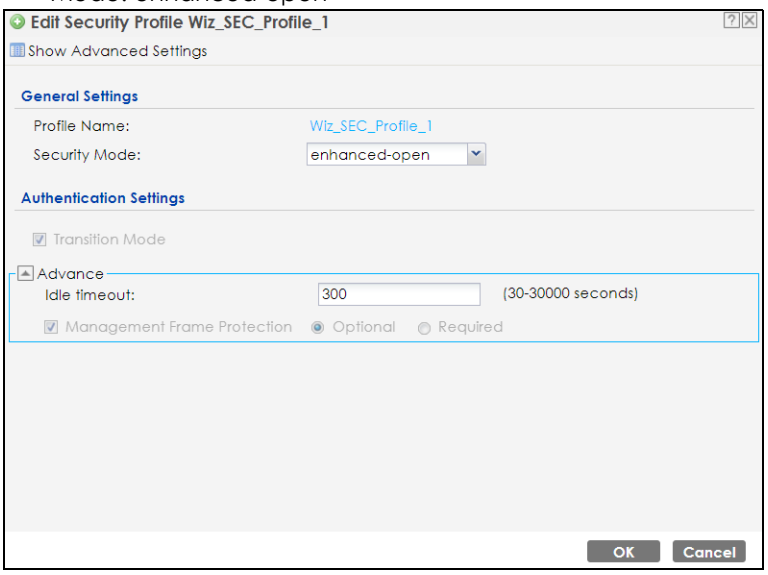
Table 66 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile > Security Mode: none

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. Select **wpa2-mix** if you want the Zyxel Device WiFi network to use WPA2 security mode and provide a fallback WPA security mode for clients that only support WPA connections.
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.
Advance Note: Click on the **Show Advanced Settings** button to show the fields describe below.	
Idle timeout	Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued.

Table 66 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile > Security Mode: none (continued)

LABEL	DESCRIPTION
Radius Settings The **Radius Settings** fields are only available when you set **Authentication Settings** to **Enterprise**.	
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 checkbox 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.
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.

Figure 113 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile > Security Mode: enhanced-open



The following table describes the labels in this screen.

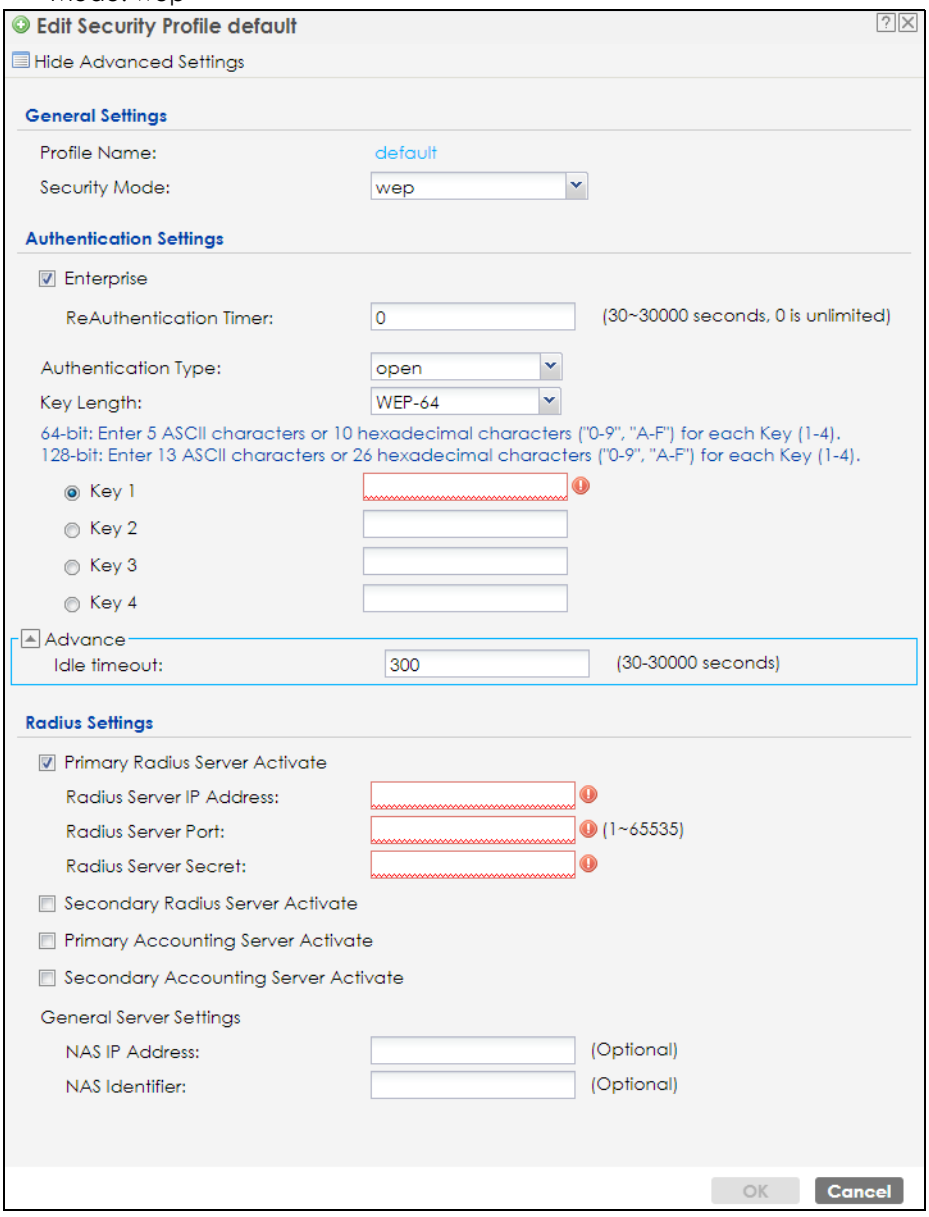
Table 67 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: enhanced-open

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. Select **wpa2-mix** if you want the Zyxel Device WiFi network to use WPA2 security mode and provide a fallback WPA security mode for clients that only support WPA connections.
Authentication Settings	
Transition Mode	This option only displays if you set the **Security Mode** to **wpa3** or **enhanced-open**. This option is always enabled for backwards compatibility. This creates two virtual APs (VAPs) with a primary (**wpa3** or **enhanced-open**) and fallback (**wpa2** or **none**) security method.
Advance Note: Click on the **Show Advanced Settings** button to show the fields described below.	
Idle timeout	Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued.

Table 67 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: enhanced-open (continued)

LABEL	DESCRIPTION
Management Frame Protection	This field is configurable only when you select **wpa2** in the **Security Mode** field and set **Cipher Type** to **aes**. Data frames in 802.11 WLANs can be encrypted and authenticated with WEP, WPA or WPA2. But 802.11 management frames, such as beacon/probe response, association request, association response, de-authentication and disassociation are always unauthenticated and unencrypted. IEEE 802.11w Protected Management Frames allows APs to use the existing security mechanisms (encryption and authentication methods defined in IEEE 802.11i WPA/WPA2) to protect management frames. This helps prevent wireless DoS attacks. Select the checkbox to enable management frame protection (MFP) to add security to 802.11 management frames. This option is always enabled if you select **enhanced-open** or **WPA3** as the **Security Mode.** If **Optional** is selected, WiFi clients will not be not required to support MFP. Management frames will be encrypted if the clients support MFP. If **Required** is selected, WiFi clients must support MFP in order to join the Zyxel Device's WiFi network.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

Figure 114 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wep



The following table describes the labels in this screen.

Table 68 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wep

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.

Table 68 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wep (continued)

LABEL	DESCRIPTION
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. Select **wpa2-mix** if you want the Zyxel Device WiFi network to use WPA2 security mode and provide a fallback WPA security mode for clients that only support WPA connections.
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.
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.
Key 1~4	Based on your **Key Length** selection, enter the appropriate length hexadecimal or ASCII key.
Advance Note: Click on the **Show Advanced Settings** button to show the fields describe below.	
Idle timeout	Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued.
Radius Settings The **Radius Settings** fields are only available when you set **Authentication Settings** to **Enterprise**.	
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 checkbox 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.

Table 68 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wep (continued)

LABEL	DESCRIPTION
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.
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.