ZYXEL
NETWORKS

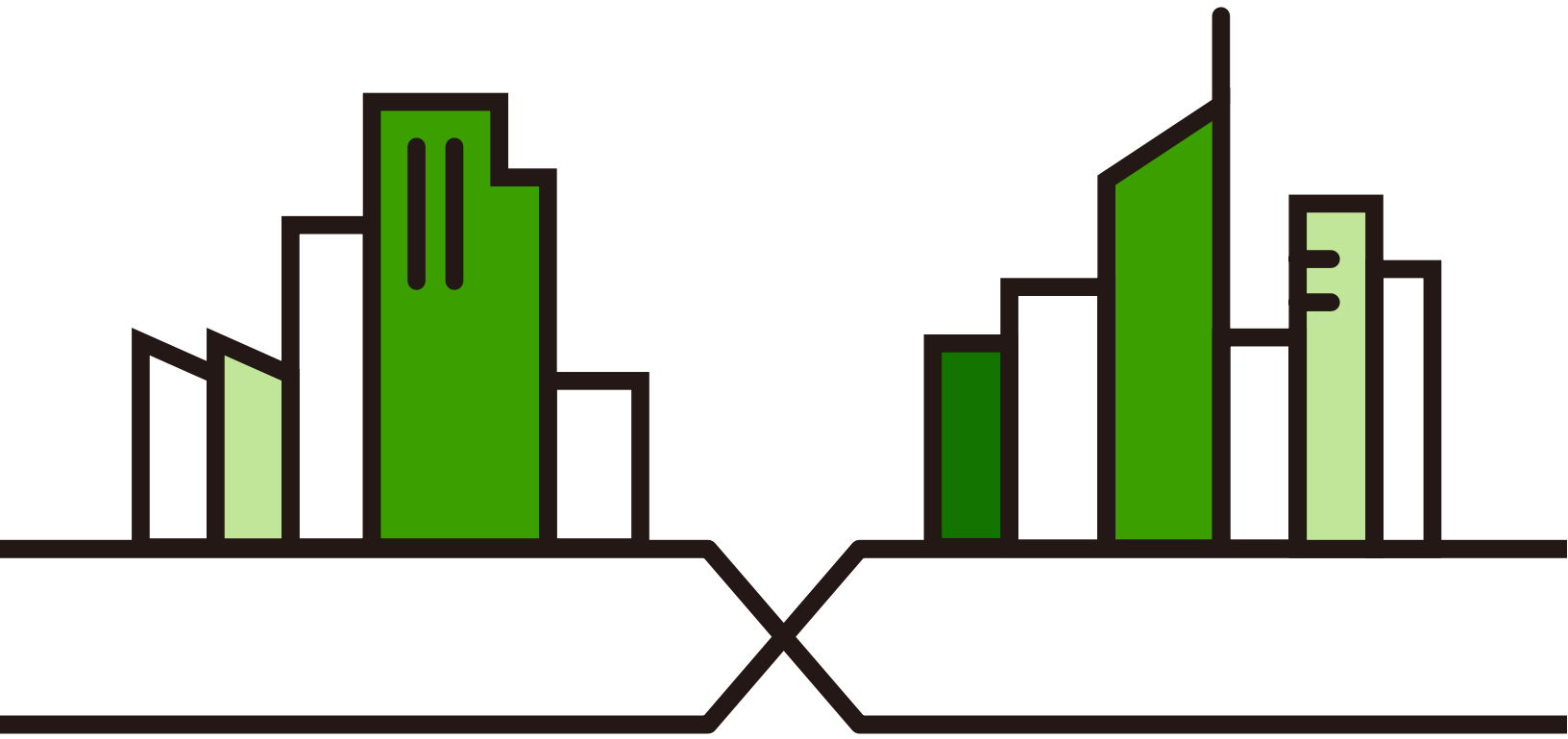
User's Guide

NWA50/90/55 Series

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

Default Login Details	
Management IP Address	http://DHCP-assigned IP OR http://192.168.1.2
User Name	admin
Password	See Zyxel Device label or 1234

Version 7.10 Edition 2, 3/2025



Copyright © 2025 Zyxel and/or its affiliates. All rights reserved.

Document Conventions

Warnings and Notes

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

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

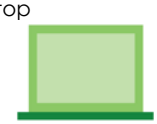
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- All models in this series may be referred to as the "Zyxel Device" in this guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **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 below:

- NWA50AX
- NWA90AX
- NWA55AXE
- NWA50AX PRO
- NWA90AX PRO

The Zyxel Device can be managed in one of the following methods: remote management through Nebula Control Center (NCC) or local management in Standalone Mode. The Zyxel Device runs in standalone mode by default, but it is recommended to use NCC management if it is available for your device. For more information about Access Point (AP) management, see Section 2.1 on page 20.

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

When two or more APs are interconnected, this network is called a Wireless Distribution System (WDS). See Section 1.3 on page 13 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're using.

1.2 Zyxel Device Product Feature Comparison

The following table lists the features of the Zyxel Device.

Table 1 WiFi 6 Models Comparison Table

FEATURES	NWA50AX	NWA90AX	NWA55AXE
Supported WiFi Standards	IEEE 802.11a IEEE802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE802.11ax	IEEE 802.11a IEEE802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE802.11ax	IEEE 802.11a IEEE802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE802.11ax
Multi-Link Operation (MLO)	No	No	No
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

Table 1 WiFi 6 Models Comparison Table (continued)

FEATURES	NWA50AX	NWA90AX	NWA55AXE
Available Security Modes	None / Enhanced-open / WEP / WPA2-MIX-Personal / WPA3-Personal	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	No	Yes	Yes
Security Profile Enterprise Authentication Settings	No	Yes	Yes
Rogue AP Detection	Yes	Yes	Yes
WDS (Wireless Distribution System) - Root AP & Repeater Modes	Yes	Yes	Yes
Wireless Bridge	No	No	Yes
Layer-2 Isolation	Yes	Yes	Yes
Supported PoE Standards	IEEE 802.3at	IEEE 802.3at	IEEE 802.3at
Power Detection	No	No	No
External Antennas	No	No	Yes
Internal Antennas	Yes	Yes	No
Console Port	4-Pin Serial	4-Pin Serial	No
Reset button	Yes	Yes	No
LED Locator	Yes	Yes	No
LED Suppression	Yes	Yes	Yes
APC (AP Controller) Discovery	No	No	No
NCC Discovery	Yes	Yes	Yes
802.11r Fast Roaming Support	Yes	Yes	Yes
802.11k/v Assisted Roaming	Yes	Yes	Yes
Ethernet Storm Control	No	No	No
Grounding	No	No	No
Power Jack	Yes	Yes	No
Maximum number of log messages	512 event logs		
Latest Firmware Version Supported	7.10	7.10	7.10

Table 2 WiFi 6 PRO Models Comparison Table

FEATURES	NWA50AX PRO	NWA90AX PRO
Supported WiFi Standards	IEEE 802.11a IEEE802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE802.11ax	IEEE 802.11a IEEE802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE802.11ax
Multi-Link Operation (MLO)	No	No
Supported Frequency Bands	2.4 GHz 5 GHz	2.4 GHz 5 GHz
Supported Channel Width	2.4G: 20/40 MHz 5G: 20/40/80/160 MHz	2.4G: 20/40 MHz 5G: 20/40/80/160 MHz

Table 2 WiFi 6 PRO Models Comparison Table (continued)

FEATURES	NWA50AX PRO	NWA90AX PRO
Available Security Modes	None / Enhanced-open / WEP / WPA2-MIX-Personal / WPA3-Personal	None / Enhanced-open / WEP / WPA2-MIX / WPA3 -Personal & Enterprise
Number of SSID Profiles	64	64
Number of WiFi Radios	2	2
Security Profile Radius Settings	No	Yes
Security Profile Enterprise Authentication Settings	No	Yes
Rogue AP Detection	Yes	Yes
WDS (Wireless Distribution System) - Root AP & Repeater Modes	Yes	Yes
Wireless Bridge	No	No
Layer-2 Isolation	Yes	Yes
Supported PoE Standards	IEEE 802.3at	IEEE 802.3at
Power Detection	No	No
External Antennas	No	No
Internal Antennas	Yes	Yes
Console Port	4-Pin Serial	4-Pin Serial
Reset Button	Yes	Yes
LED Locator	Yes	Yes
LED Suppression	Yes	Yes
APC (AP Controller) Discovery	No	No
NCC Discovery	Yes	Yes
802.11r Fast Roaming Support	Yes	Yes
802.11k/v Assisted Roaming	Yes	Yes
Ethernet Storm Control	No	No
Grounding	No	No
Power Jack	Yes	Yes
Maximum number of log messages	512 event logs	
Latest Firmware Version Supported	7.10	7.10

1.3 Zyxel Device Roles

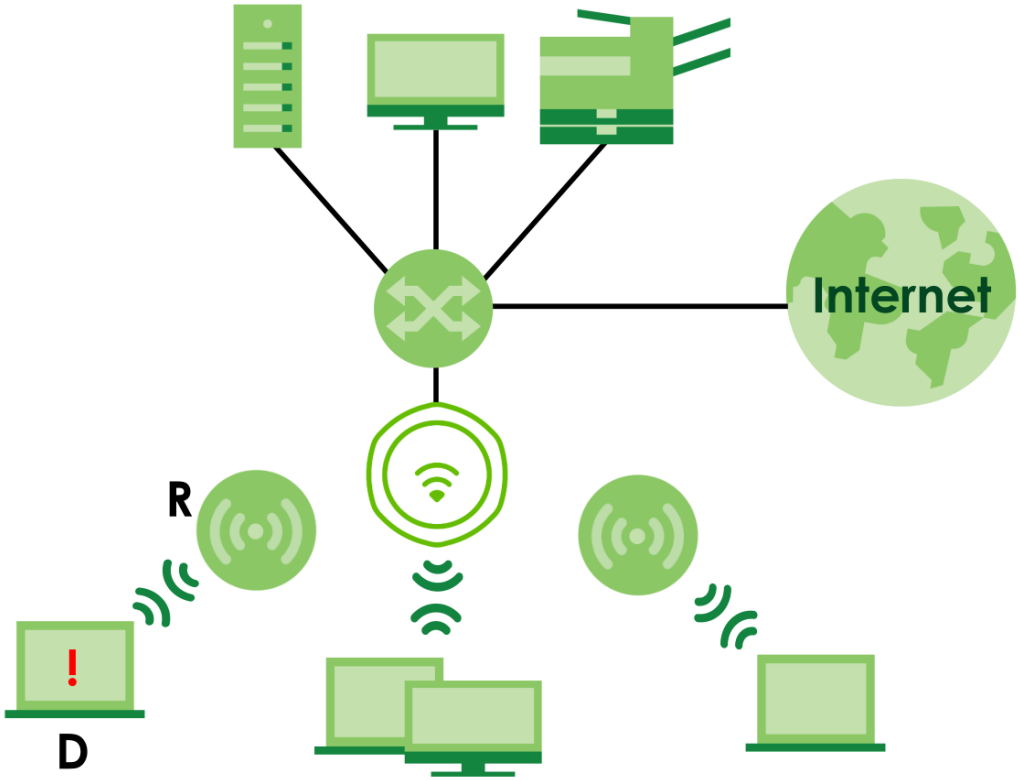
This section describes some of the different roles that your Zyxel Device can take up within a network. Not all roles are supported by all models (see Section 1.2 on page 11). The Zyxel Device can serve as a:

- 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.

Figure 1 Zyxel Device Application in a Network

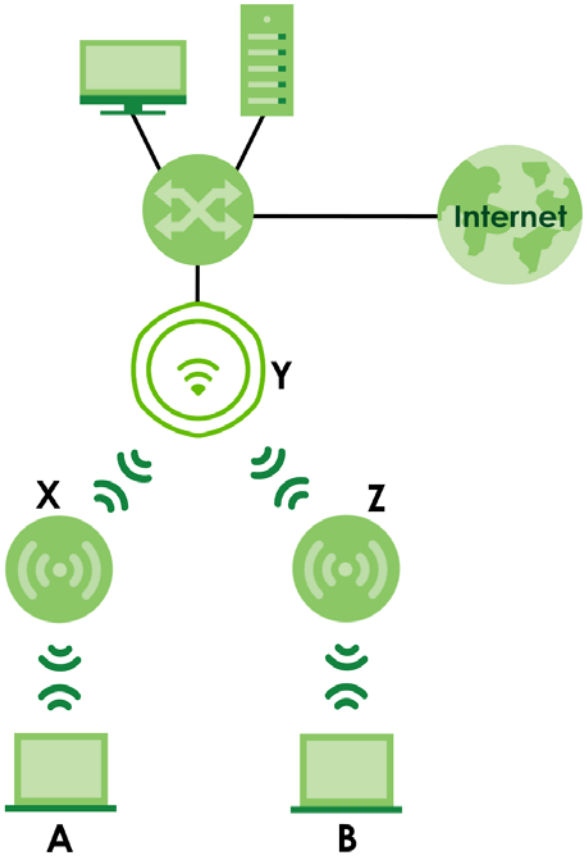


Wireless Distribution System (WDS)

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.

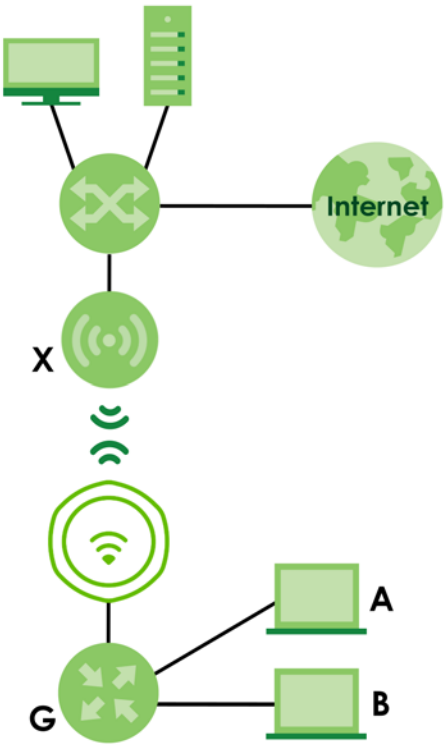
Figure 2 Wireless Distribution System Network Example



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 11 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 14.1 on page 168 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 113 and Section 14.2 on page 168 for more details.

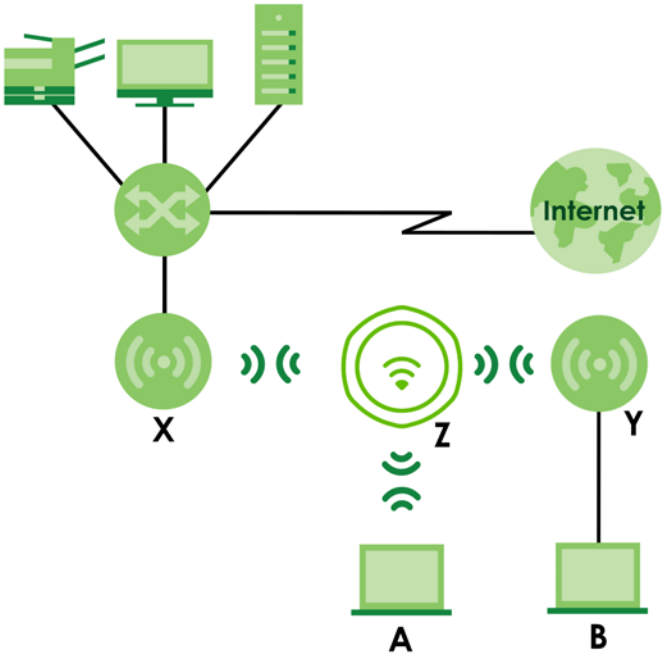
Unless specified, the term "security settings" refers to the traffic between the WiFi clients and the AP. At the time of writing, repeater security is compatible with the Zyxel Device only.

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 113 and Section 14.2 on page 168 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 119). **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.

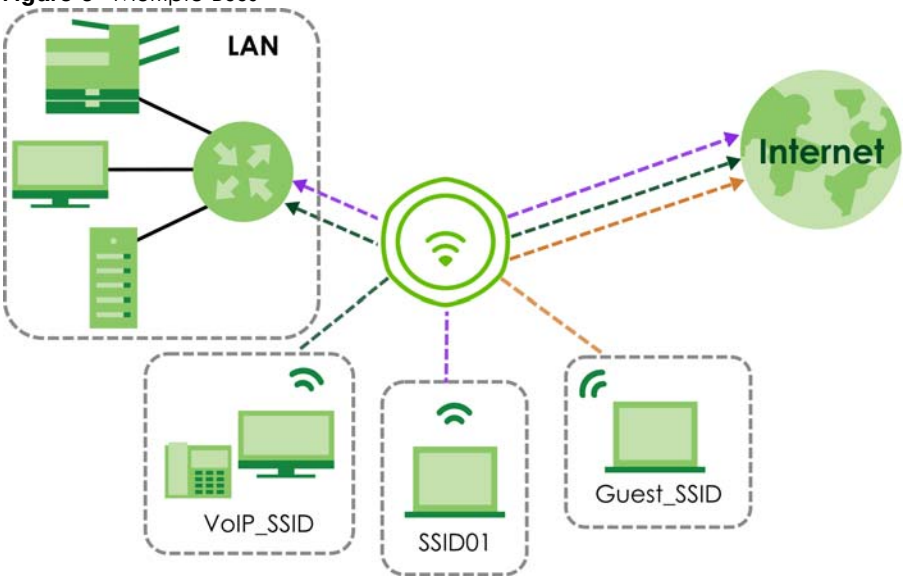
You can configure multiple SSID profiles, and have all of them active at any one time.

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



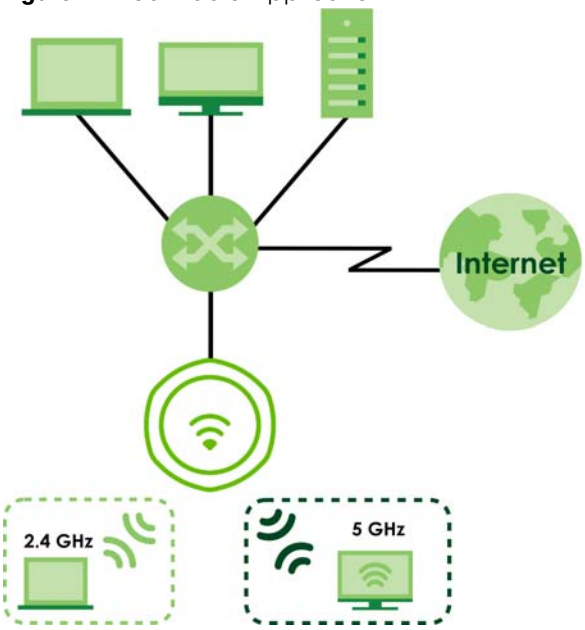
1.4.2 Dual-Radio

Some of the Zyxel Device models are equipped with dual WiFi radios. This means you can configure different WiFi networks on the 2.4G and 5G bands to operate simultaneously.

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

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

Figure 7 Dual-Radio Application



CHAPTER 2
AP Management

2.1 Management Mode

The Zyxel Device is a unified AP and can be managed by NCC, or work as a standalone device. We recommend you use NCC to manage multiple APs (see the NCC User's Guide).

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

Table 3 Zyxel Device Management Mode Comparison

MANAGEMENT MODE	DEFAULT IP ADDRESS	UPDATE FIRMWARE THROUGH
Nebula Control Center	Dynamic	NCC Portal / Built-in Web Configurator
Standalone	Dynamic or Static (192.168.1.2)	Built-in Web Configurator

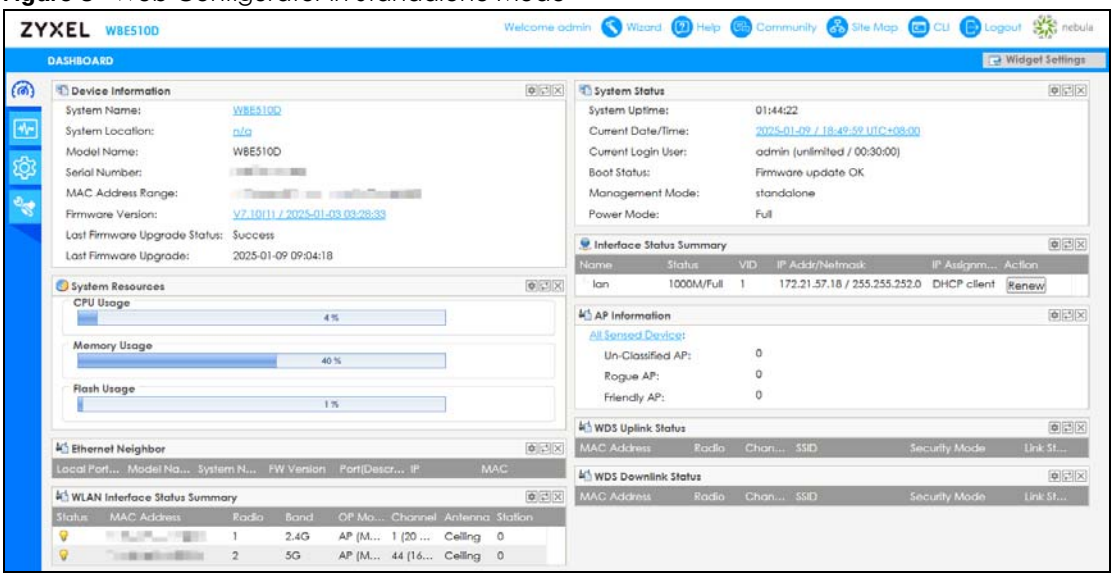
When the Zyxel Device is in standalone mode and connects to a DHCP server, it uses the IP address assigned by the DHCP server. Otherwise, the Zyxel Device uses the default static management IP address (192.168.1.2).

When the Zyxel Device is managed by the NCC, it acts as a DHCP client and obtains an IP address from NCC. You can configure the Zyxel Device using the web configurator when the Zyxel Device is not connected to NCC. Refer to Section 2.2 on page 22 if you need to change the Zyxel Device's management mode.

2.1.1 Standalone

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

Figure 8 Web Configurator in Standalone Mode

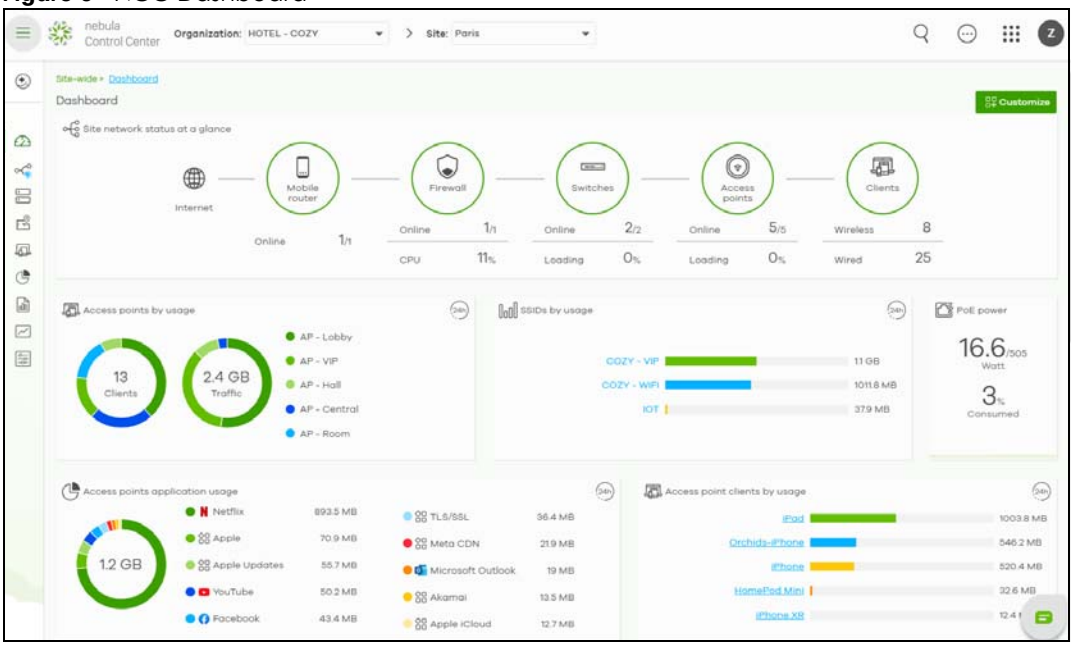


See Chapter 5 on page 49 for detailed information about the standalone Web Configurator screens.

2.1.2 Nebula Control Center

In this mode, which is also called cloud managed 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 22 on page 231 for an example NCC managed network topology.

Figure 9 NCC Dashboard



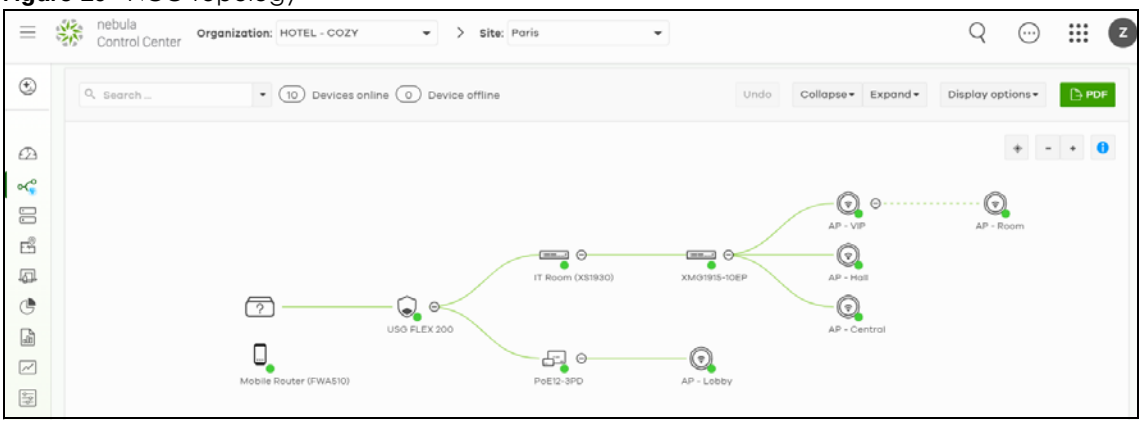
Each Zyxel Device must belong to a site which must be in an organization. You can configure each Zyxel Device on its own or configure a set of Zyxel Devices together in a site. You can also monitor groups of sites in organizations.

Table 4 Sites and Organizations

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

You can use the **Topology** in NCC which graphically presents your device and network statistics. It shows an overview of your network topology, as shown in the following figure. See the NCC User's Guide for how to configure Nebula managed devices.

Figure 10 NCC Topology



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

2.2 Switching Management Modes

This section shows you how to switch the Zyxel Device's management mode between standalone and cloud managed mode.

To change the Zyxel Device management mode, use the **Reset** button to restore the default configuration (see Section 25.6 on page 258). Alternatively, you need to check NCC 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 it.

Standalone-to-NCC

Register the Zyxel Device on the NCC website and then turn on the Zyxel Device. 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.

NCC-to-Standalone

Back up your configurations first, then unregister the Zyxel Device from NCC. Press the **Reset** button. The Zyxel Device will reset to factory defaults. See Section 4.2 on page 37 to log in to the Web Configurator and select standalone mode.

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

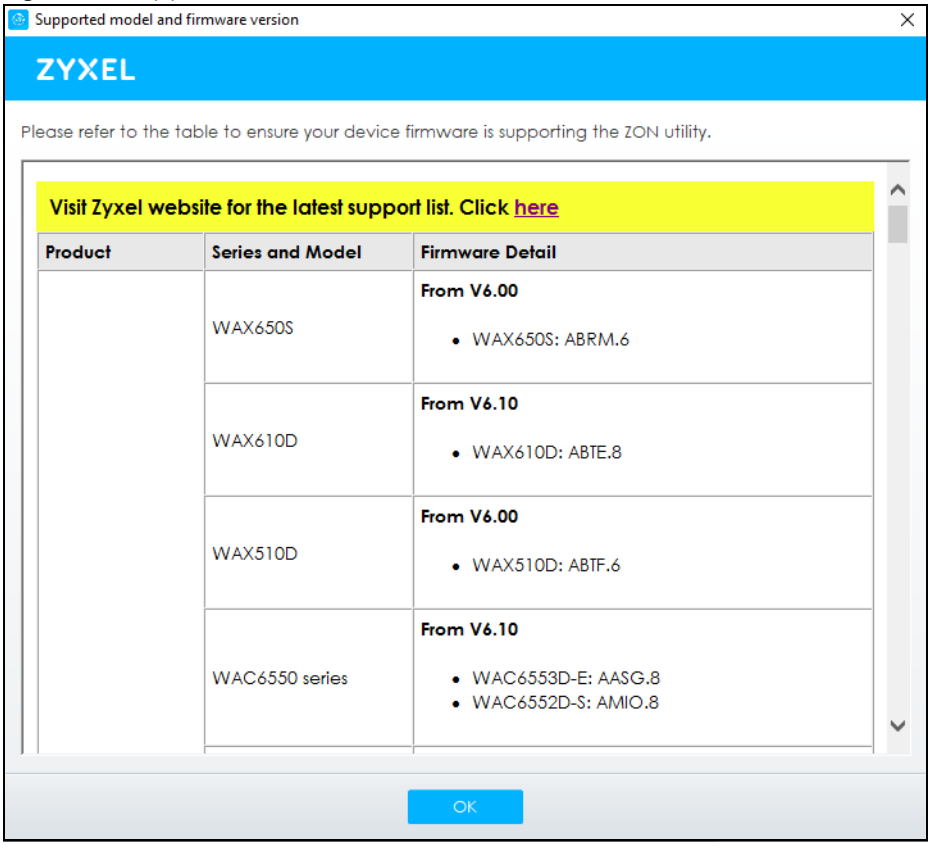
- WXGA (Wide XGA 1280x800)

2.3.2 Run the ZON Utility

1 Double-click the ZON Utility to run it.

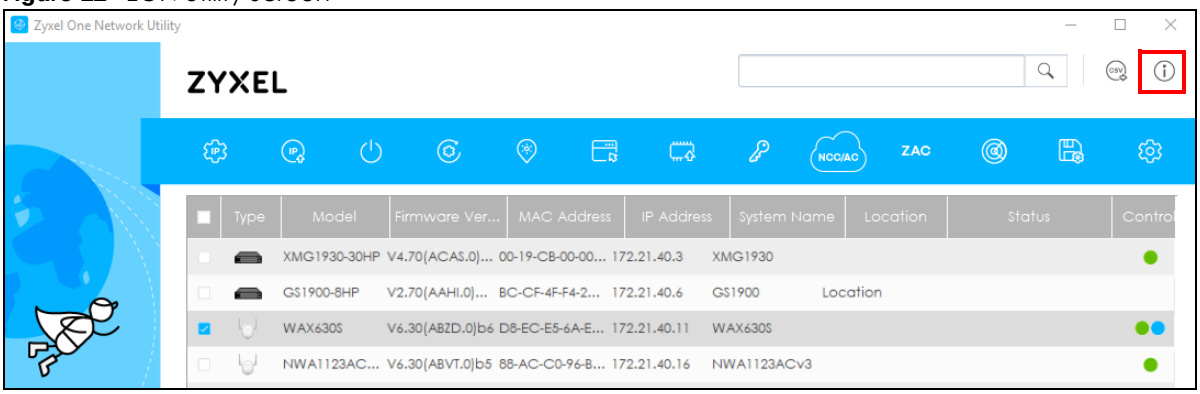
2 The first time you run the ZON Utility, you will see if your device and firmware version support the ZON Utility. Click the **OK** button to close this screen.

Figure 11 Supported Devices and Versions



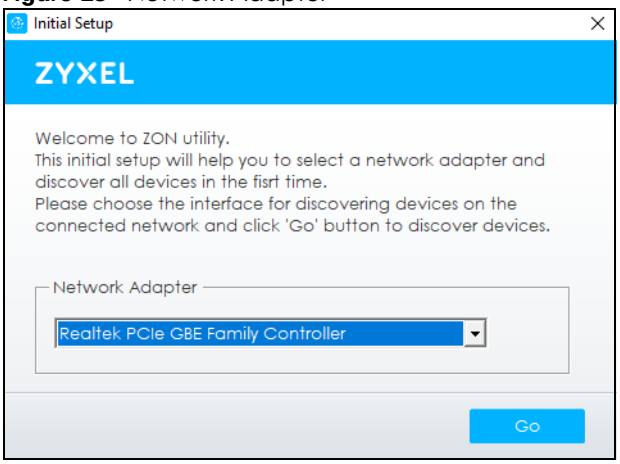
If you want to check the supported models and firmware versions later, you can click the **Show information about ZON** icon in the upper right hand corner of the screen. Then select the **Supported model and firmware version** link. If your device is not listed here, see the device release notes for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

Figure 12 ZON Utility Screen



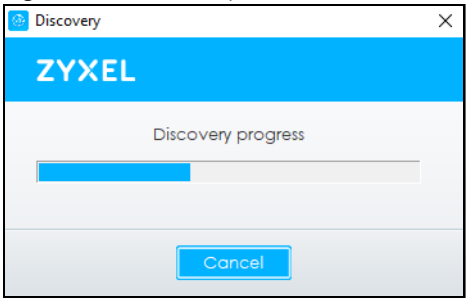
3 Select a network adapter to which your supported devices are connected.

Figure 13 Network Adapter



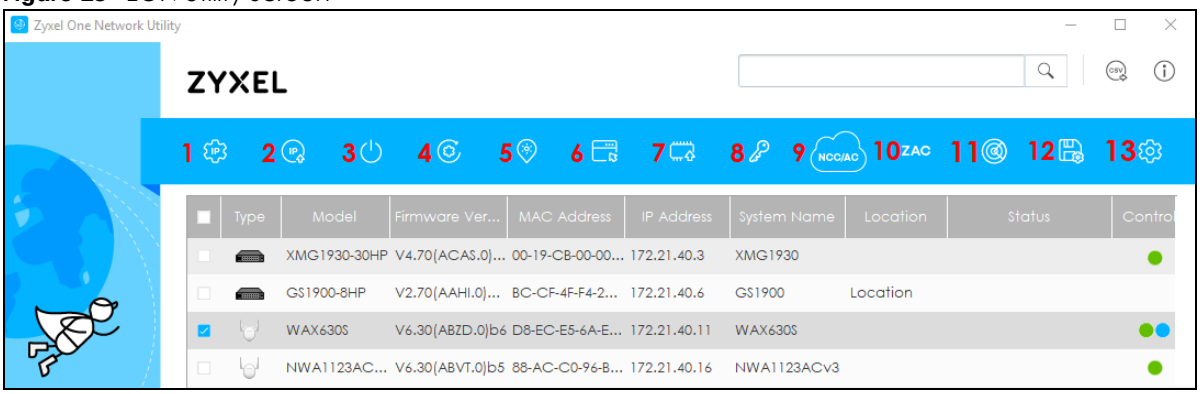
4 Click the **Go** button for the ZON Utility to discover all supported devices in your network.

Figure 14 Discovery



5 The ZON Utility screen shows the devices discovered.

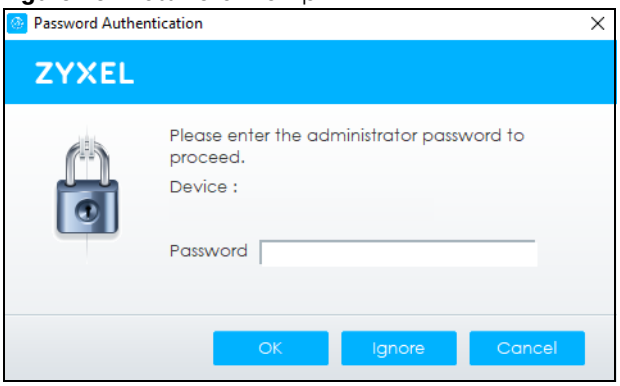
Figure 15 ZON Utility Screen



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 16 Password Prompt



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

Table 5 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 5 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 NCC Discovery	The option is available if the selected device supports 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 Nebula Control Center (NCC) discovery feature. If the feature is enabled, the selected device will try to connect to the NCC. 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 6 ZON Utility Fields

LABEL	DESCRIPTION
Type	This field displays an icon of the kind of device discovered.
Model	This field displays the model name of the discovered device.
Firmware Version	This field displays the firmware version of the discovered device.
MAC Address	This field displays the MAC address of the discovered device.
IP Address	This field displays the IP address of an internal interface on the discovered device that first received an ZDP discovery request from the ZON utility.
System Name	This field displays the system name of the discovered device.
Location	This field displays where the discovered device is.
Status	This field displays whether changes to the discovered device have been done successfully. As the Zyxel Device does not support **IP Configuration**, **Renew IP address** and **Flash Locator LED**, this field displays "Update failed", "Not support Renew IP address" and "Not support Flash Locator LED" respectively.
NCC Discovery	This field displays if the discovered device supports the Nebula Control Center (NCC) discovery feature. If the feature is enabled, the selected device will try to connect to the NCC. 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.
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, 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 managed mode (NCC). With the NCC, you can remotely manage and monitor the Zyxel Device through a cloud-based network management system. See the NCC User's Guide for more information.

ZON Utility

Zyxel One Network (ZON) Utility is a utility tool that assists you to set up and maintain network devices in a simple and efficient way. You can download the ZON Utility at *www.zyxel.com* and install it on your computer (Windows operating system). For more information on ZON Utility see Section 2.3 on page 23.

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.

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.

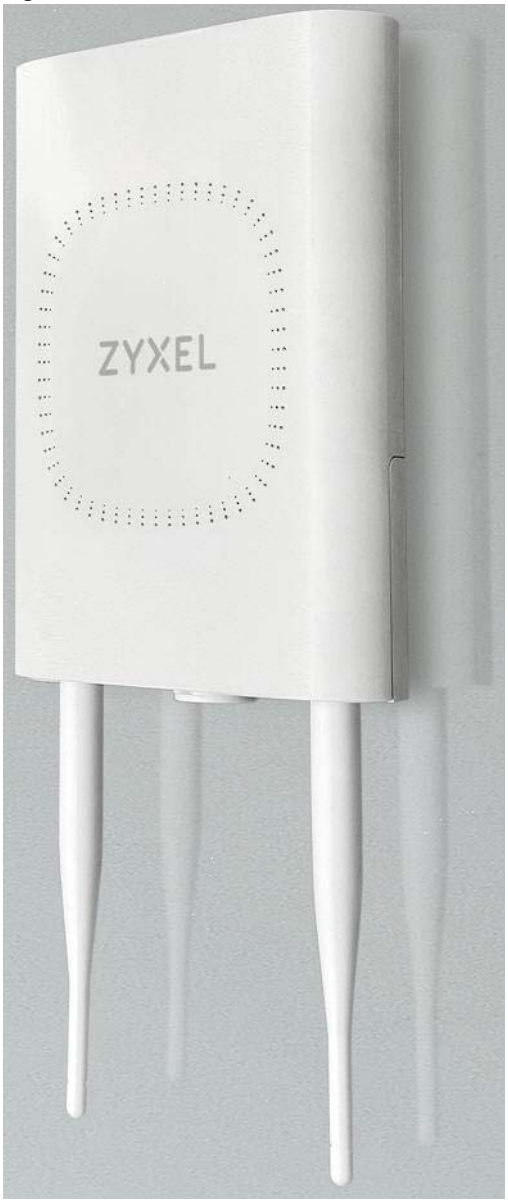
3.1 Zyxel Device Models With Single LEDs

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 11 to check which models support these features. Refer to Section 20.1 on page 225 for the LED **Suppression** and **Locator** menus in standalone mode.

3.2 Zyxel Device LED

Figure 17 NWA50AX/NWA90AX/NWA50AX PRO/NWA90AX PRO LED

Figure 18 NWA55AXE



Note: The NWA55AXE does not have LEDs.

The following are the LED descriptions for the Zyxel Device.

Table 7 Zyxel Device LED

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

Table 7 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 managed by the NCC but fails to connect with NCC, and is reconnecting with the NCC.
	Green	Slow Blinking (On for 1 second, Off for 1 second)	The wireless module of the Zyxel Device is disabled or fails, the Zyxel Device is using default WiFi settings, and/or the Zyxel Device is configured to be managed by the NCC but is not yet registered with the NCC.
	Green	Steady On	The Zyxel Device is ready for use, the Zyxel Device's wireless interface is activated, and WiFi clients are connected to the Zyxel Device.
	Bright Blue	Steady On	The Zyxel Device's wireless interface is activated, but there are no WiFi clients connected.
	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.

3.3 Ports

The following shows the Zyxel Device panels with connection ports.

Figure 19 NWA50AX/NWA90AX/NWA50AX PRO/NWA90AX PRO

Figure 20 NWA55AXE

Note: The NWA55AXE does not have a reset button. Refer to Section 3.3.1 on page 33 to see how to reset your Zyxel Device to its factory default settings.

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

Table 8 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.

Table 8 Ports and Buttons

LABEL	DESCRIPTION
CONSOLE	You can use the console port to manage the Zyxel Device using CLI commands. You will be prompted to enter your user name and password. See the Command Reference Guide for more information about the CLI. When configuring using the console port, you need a computer equipped with communications software configured to the following parameters: • Speed 115200 bps • Data Bits 8 • Parity None • Stop Bit 1 • Flow Control Off
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

3.3.1 Ways to Reset a Zyxel Device without a Reset Button

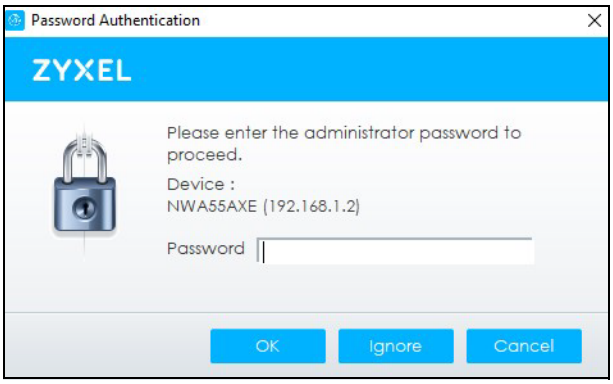
You can use the following ways to reset a Zyxel Device without a reset button to its factory default settings.

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.

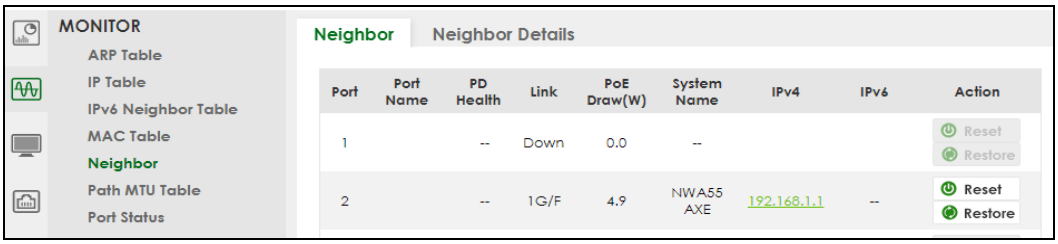
3 Enter the administrator password in the **Password** field on the pop-up screen and click **OK** to start the reset.



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.



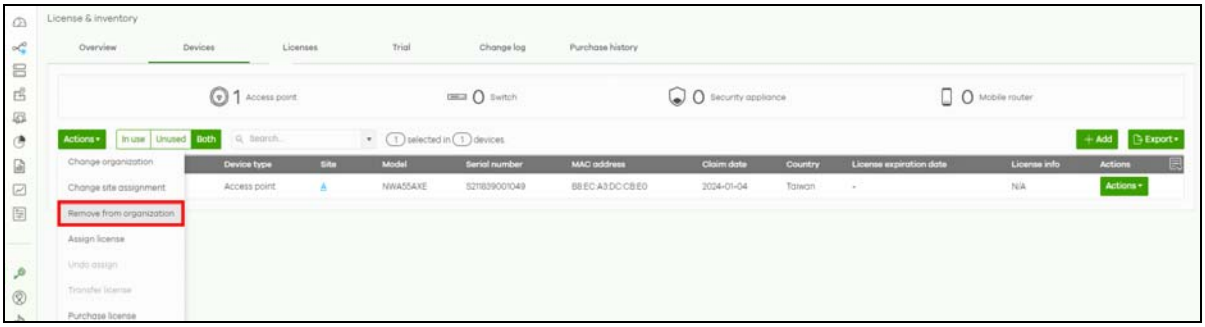
2 A pop-up window asks you to confirm that you want to reset the Zyxel Device to factory default. Click **OK** to proceed with reset. A count down starts.

Nebula Control Center

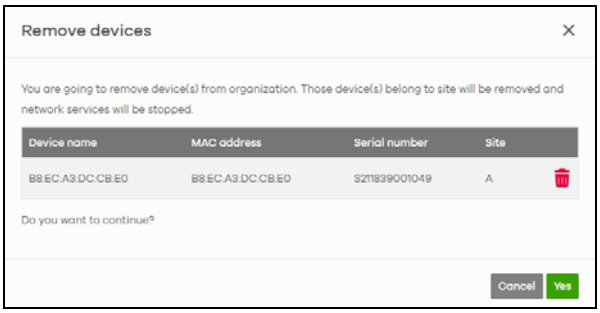
If your Zyxel Device is registered with NCC, you can unregister it to reset it to its factory default settings.

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.

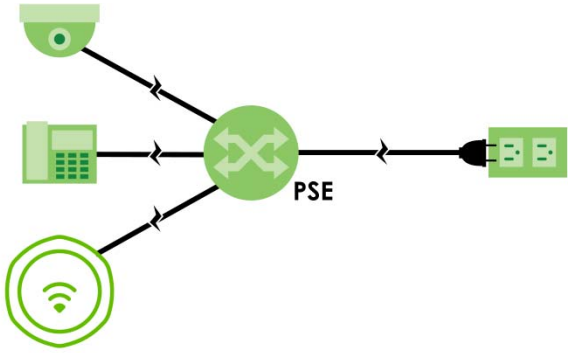


3.4 PoE

Power Over Ethernet (PoE) is a technology that allows Ethernet cables to supply power and transmit data simultaneously through a single Ethernet cable. You can use PoE when the Zyxel Device is hard to reach a power outlet or to simplify cabling.

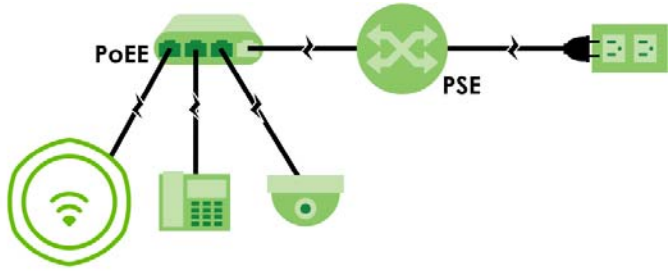
The following example shows a Power Sourcing Equipment (**PSE**) supplying power and transmitting data to the Zyxel Device, along with other Powered Devices (PDs) such as an IP camera and an IP telephone.

Figure 21 PoE Example Application - PSE



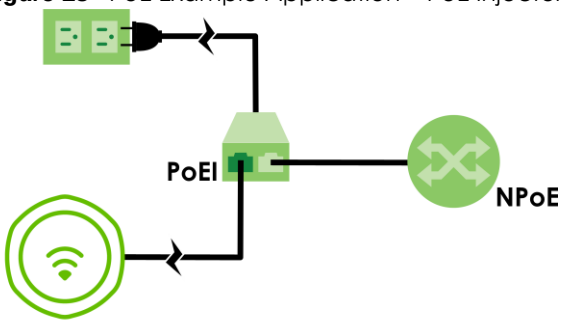
The following example shows a **PSE** using a PoE Extender (**PoEE**) to supply power and transmit data to the Zyxel Device, along with other PDs such as an IP camera and an IP telephone.

Figure 22 PoE Example Application - PSE with PoE Extender



The following example shows the PoE Injector (**PoEI**) delivering power from the power outlet and transmitting data from the non-PoE (**NPoE**) device to the Zyxel Device.

Figure 23 PoE Example Application - PoE Injector



To view the Zyxel Device's supported PoE standards, see Section 1.2 on page 11. Use Ethernet cables that correspond to the PoE standard your Zyxel Device supports (see Table 9 on page 36).

PoE standards are:

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

The following table describes the PoE standards.

Table 9 PoE Standards

PoE FEATURES	PoE	PoE+	PoE++
IEEE Standard	IEEE 802.3af	IEEE 802.3at	IEEE 802.3bt
PoE Type	Type 1	Type 2	Type 3
PSE Port Power			
IEEE Power Classification	Class 0, 1, 2, 3	Class 4	Class 5, 6
Maximum Power Per Port	15.4 W	30 W	60 W
Port Voltage Range	44 – 57 V	50 – 57 V	50 – 57 V
Cables			
Twisted Pairs Used	2-pair	2-pair	4-pair
Supported Cables	Cat3 or better	Cat5 or better	Cat5 or better

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

This section shows how to access the Web Configurator for the first time.

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

2 Access the web configurator login screen through a WiFi or wired connection.

2a WiFi connection

From a WiFi-enabled device, search for the Zyxel Device's initial SSID (Zyxel-xxxx, where xxxx is the last four characters of the MAC address on the device label.) and connect to it. The web configurator appears once your computer connects to the initial SSID. If the web configurator does not appear automatically, open your web browser and enter "https://1.1.1.1" or "https://setup.zyxel.com".

Note: If the Zyxel Device cannot connect to the Internet, use the Zyxel Device's DHCP-assigned IP address to access its web configurator. Check the connected router or DHCP server for the IP address of the Zyxel Device.

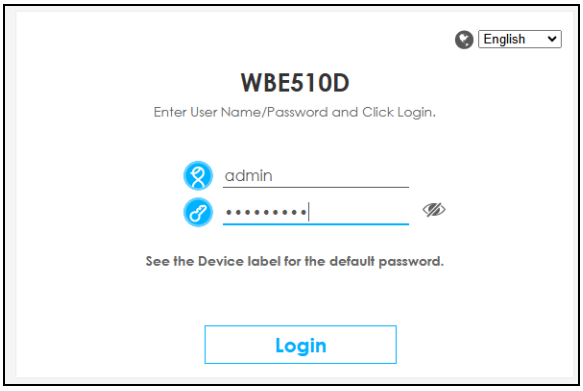
Note: The default security mode for the Zyxel Device's initial SSID is enhanced-open. Client devices without enhanced-open support cannot connect to the initial SSID. Alternatively, you can use a wired connection to access the web configurator.

Init (initial) SSID (Service Set IDentifier) is the default WiFi network name of the Zyxel Device. The default forwarding mode of the Zyxel Device is NAT (Network Address Translation) mode. This allows the Init SSID to be visible to your WiFi-enabled device and connect to the Zyxel Device. (see Section on page 133 for more information about forwarding mode.)

2b Wired connection

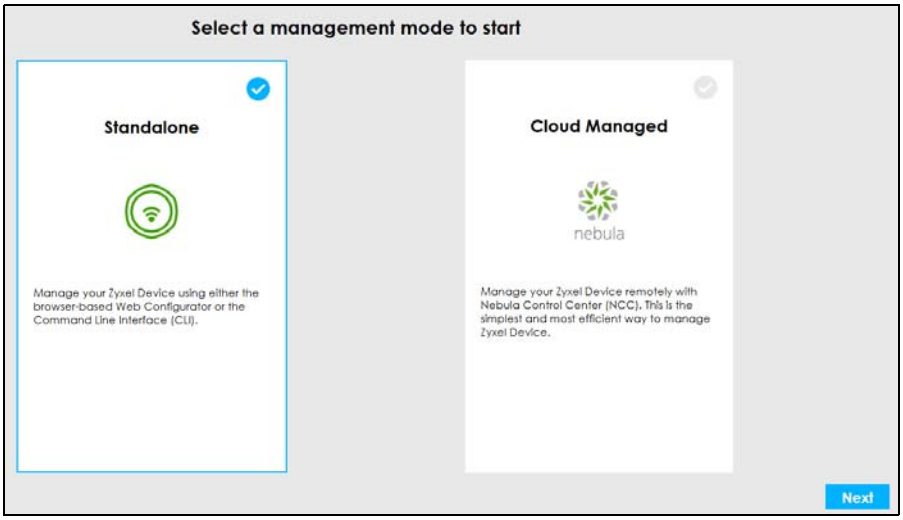
Use an Ethernet cable to connect your computer to the Zyxel Device. Open your web browser and enter the Zyxel Device's DHCP-assigned IP address or http://192.168.1.2. If the Zyxel Device and your computer are not connected to a DHCP server, ensure your computer's IP address is between "192.168.1.3" and "192.168.1.254".

3 Enter the user name (default: "admin") and default password. The default password is unique to each Zyxel Device and shown on the label. If your Zyxel Device does not have a password on the label, use "1234".

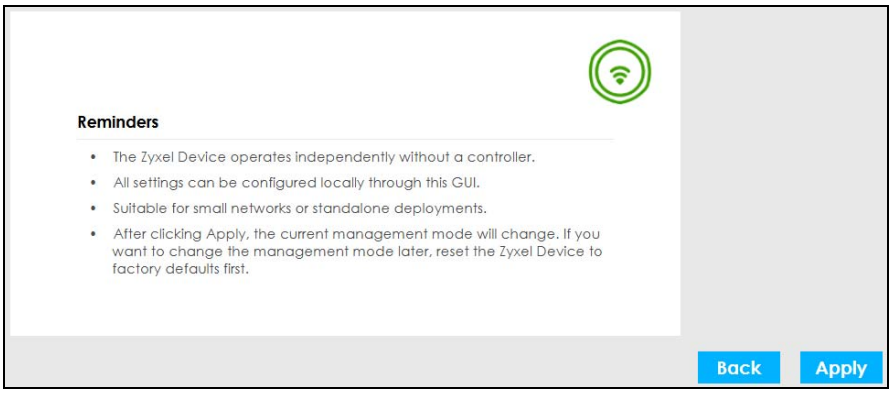


4 Select the language you prefer for the Web Configurator. Click **Login**.

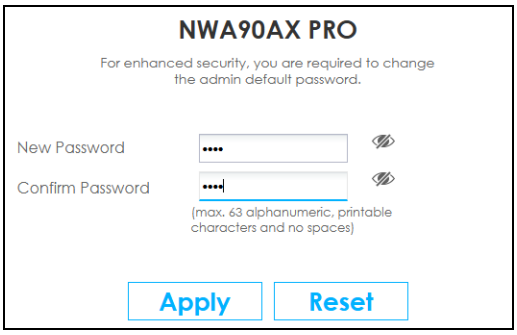
5 Select a management mode. Select **Standalone** if you use the Web Configurator to manage your Zyxel Device. Select **Could Managed** if you use NCC to manage your Zyxel Device. Refer to Section 2.1 on page 20 for more information about management mode. Click **Next**.



6 Check the **Reminders** on the screen. Click **Apply**. If you select **Cloud Managed**, refer to Nebula Control Center (NCC) to manage your Zyxel Device (see Section 2.4 on page 28 for more information). If you select **Standalone**, continue with the steps below.



7 Set up a new password containing 4 to 63 printable characters. Spaces are not allowed. Click **Apply**.



8 Log in again with the user name (default: "admin") and the new password. Click **Login**.

9 The wizard screen appears. Please refer to Section 7.1 on page 77 for wizard setup steps.

4.3 Navigating the Web Configurator

The following summarizes how to navigate the Web Configurator from the **Dashboard** screen. The figures below show the **Dashboard** screen in standalone mode and cloud managed mode. The screen layout may differ slightly depending on the mode and device model.

Figure 24 The Web Configurator's Dashboard for Standalone Mode

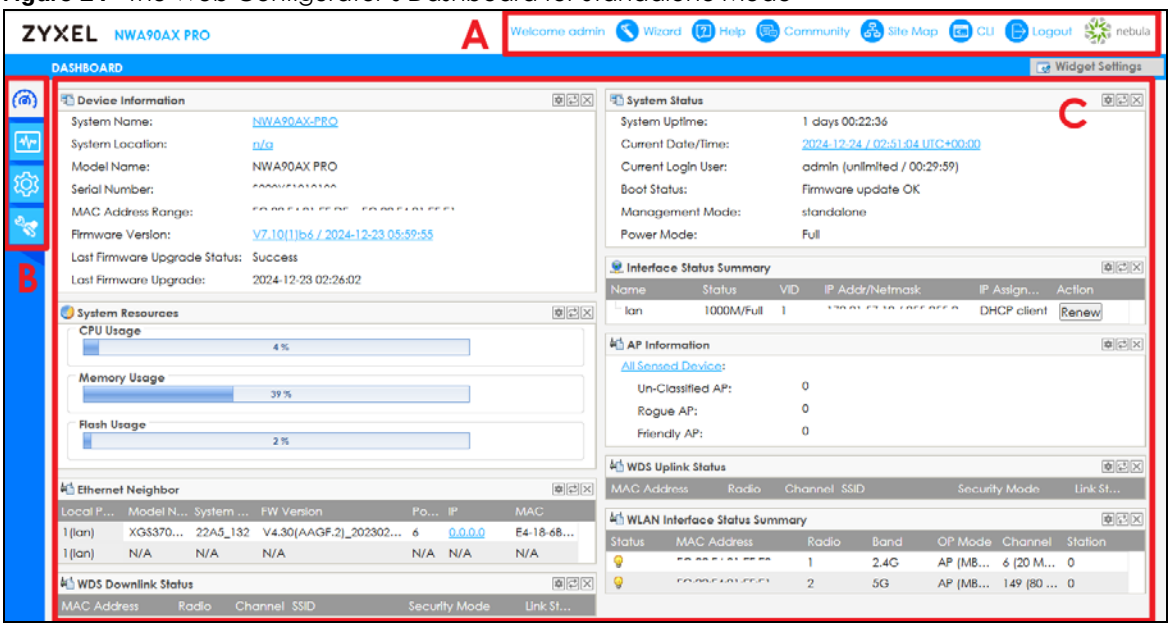
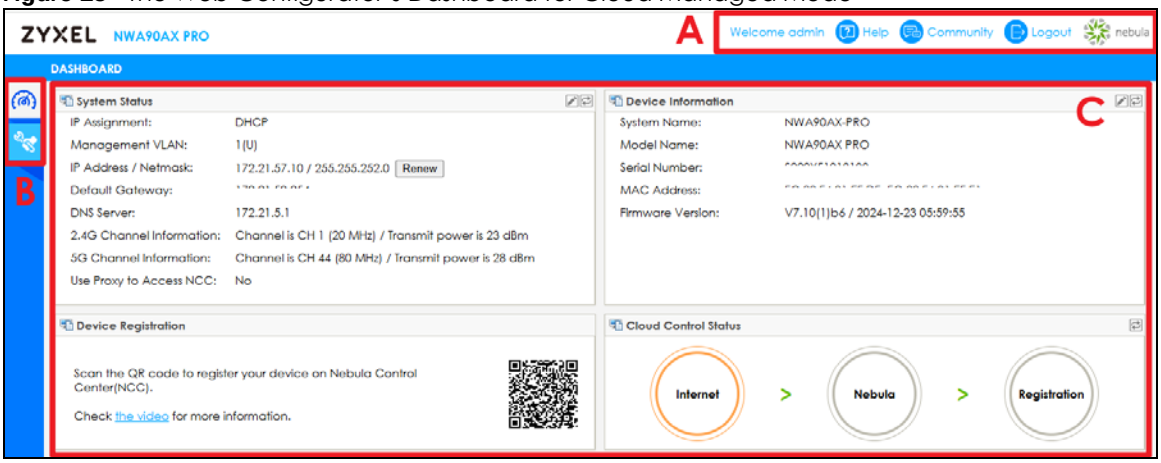


Figure 25 The Web Configurator's Dashboard for Cloud Managed Mode



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 cloud managed mode, not all icons will be available in the title Bar.

Figure 26 Title Bar

The icons provide the following functions.

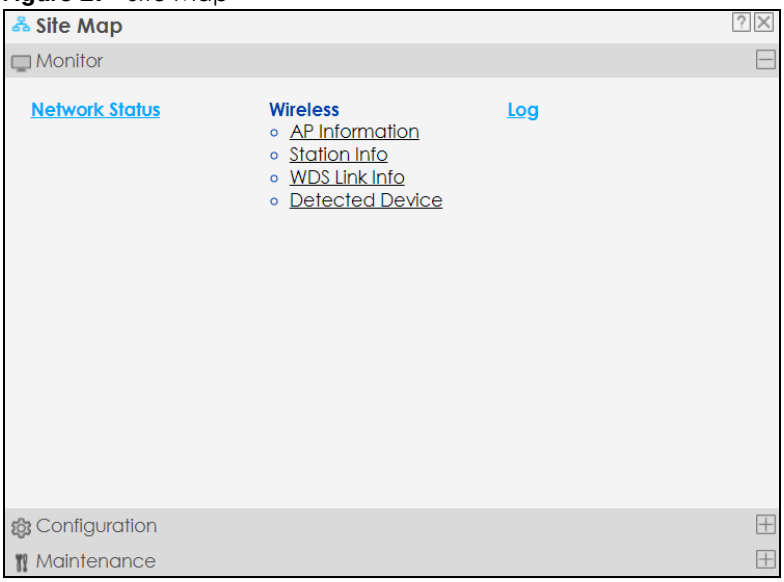
Table 10 Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
Wizard	Click this to open the wizard. See Section 7.1 on page 57 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.

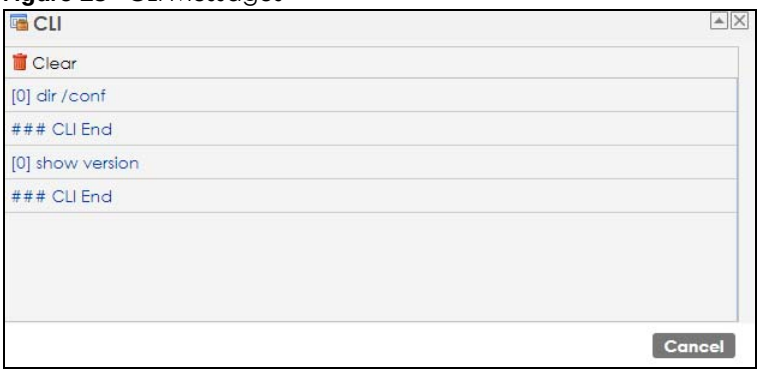
Figure 27 Site Map



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 28 CLI Messages



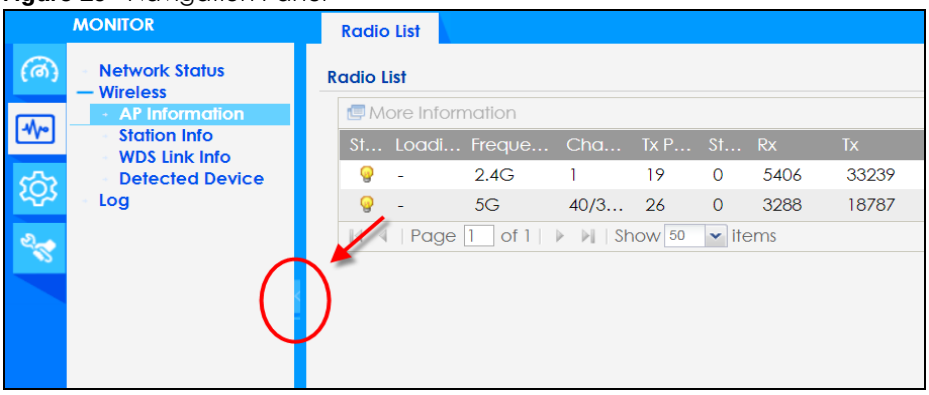
Click **Clear** to remove the currently displayed information.

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 29 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 11 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 rearrange to suit your needs.

For details on the Dashboard's features, see Chapter 5 on page 49.

Monitor Menu

The monitor menu screens display status and statistics information.

Table 11 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 12 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.
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.
DCS	DCS	Configure dynamic WiFi channel selection.
Object		
User	User	Create and manage users.
	Setting	Manage default settings for all users, general settings for user sessions, and rules to force user authentication.
AP Profile	Radio	Create and manage 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.
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.

Table 12 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
FTP	FTP	Configure FTP server settings.
Log & Report		
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 13 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.
Reboot	Reboot	Restart the Zyxel Device.

4.3.4 Cloud Managed Mode Navigation Panel Menus

If your Zyxel Device is in cloud managed mode, you can 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 rearrange to suit your needs.

For details on the Dashboard's features, see Section 23.1 on page 233.

Maintenance Menu

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

Table 14 Maintenance Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
File Manager	Firmware Package	View the current firmware version and to upload firmware.
	Shell Script	Manage and run shell script files for the Zyxel Device.
Legal and Regulatory	Legal and Regulatory	View the regulatory information.

Table 14 Maintenance Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
Diagnostics	Diagnostics	Collect diagnostic information.
	Remote Capture	Capture network traffic going through the Zyxel Device and output the captured packets to an analyzer.
Reboot	Reboot	Restart the Zyxel Device.

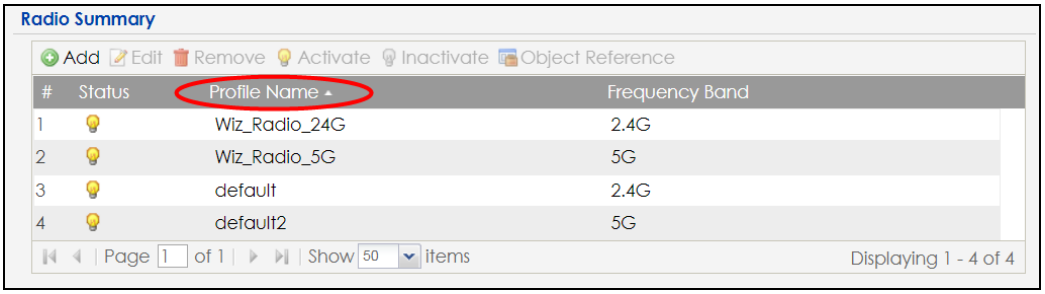
4.3.5 Tables and Lists

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

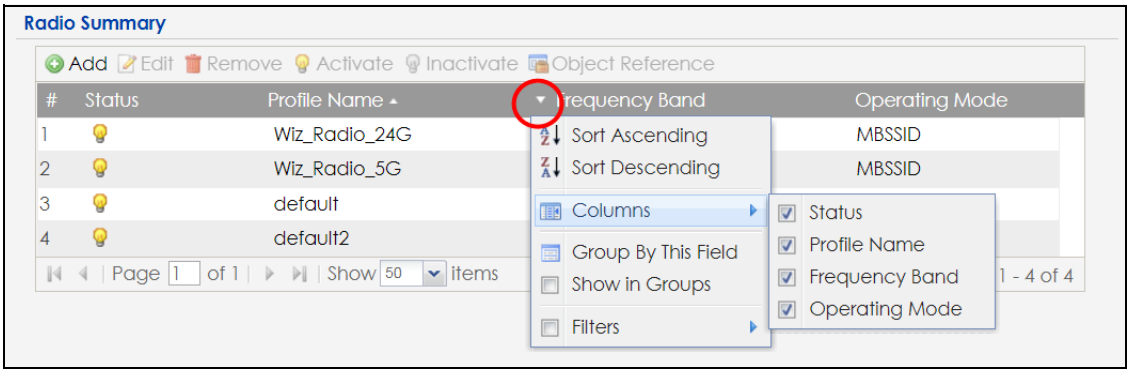
Here are some of the ways you can manipulate the Web Configurator tables.

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

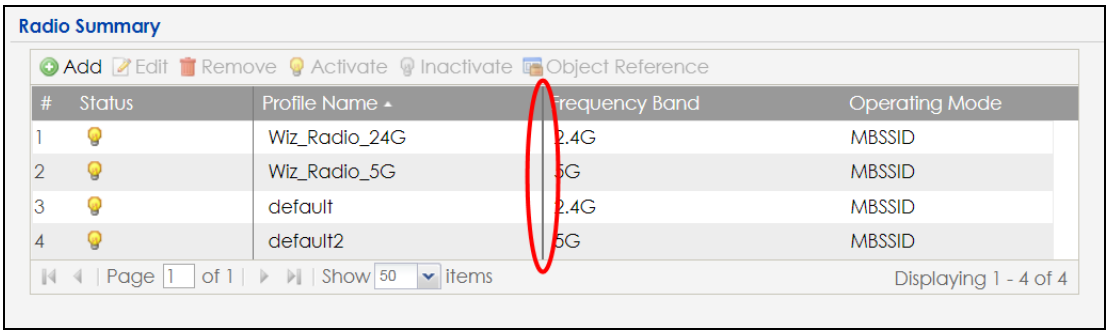


2 Click the down arrow next to a column heading for more options about how to display the entries. The options available vary depending on the type of fields in the column. Here are some examples of what you can do:

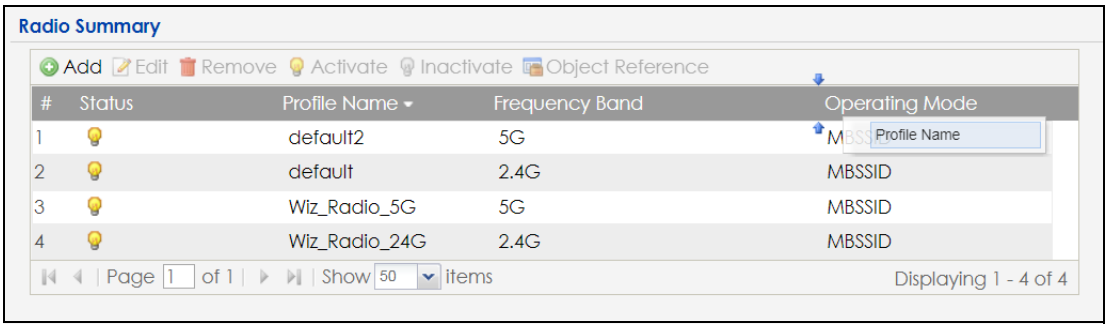
- Sort in ascending alphabetical order
- Sort in descending (reverse) alphabetical order
- Select which columns to display
- Group entries by field
- Show entries in groups
- Filter by mathematical operators (<, >, or =) or searching for text.



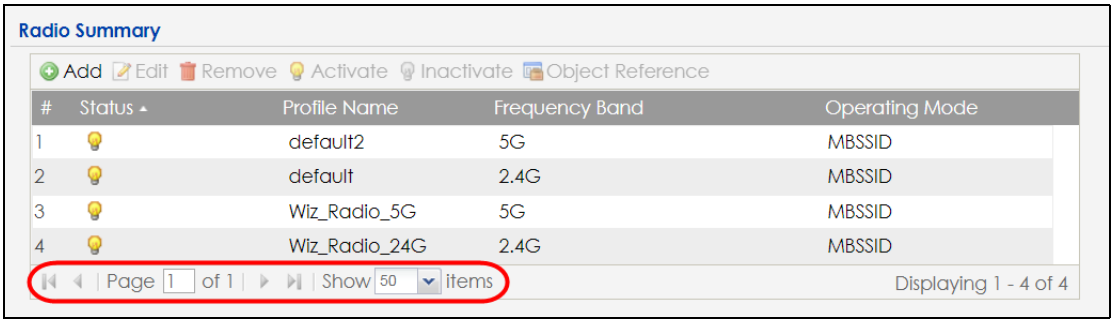
3 Select a column heading cell's right border and drag to re-size the column.



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.



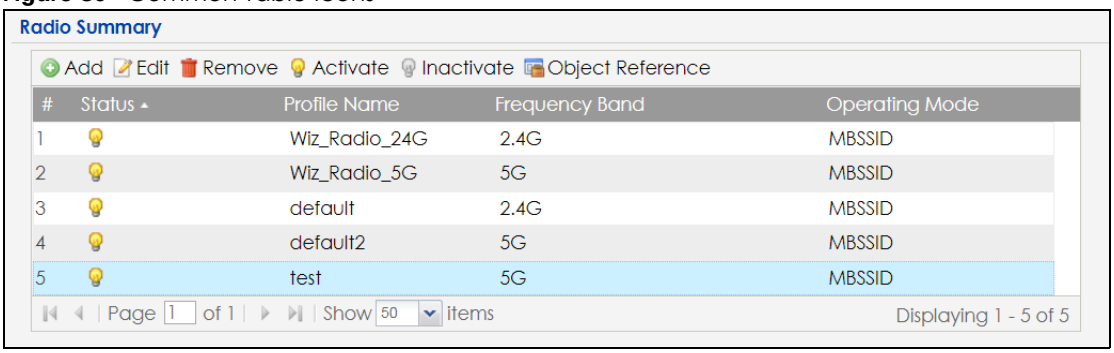
5 Use the icons and fields at the bottom of the table to navigate to different pages of entries and control how many entries display at a time.



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 30 Common Table Icons



Here are descriptions for the most common table icons.

Table 15 Common Table Icons

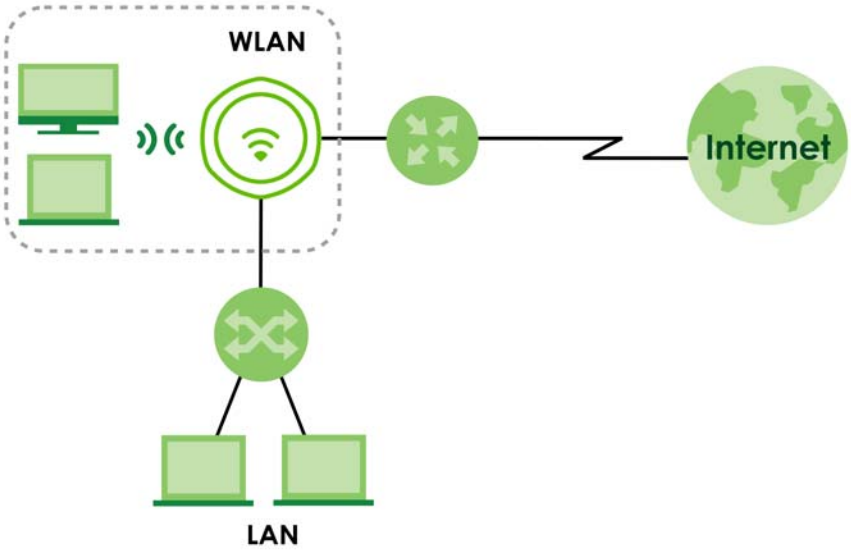
LABEL	DESCRIPTION
Add	Click this to create a new entry. For features where the entry's position in the numbered list is important (features where the Zyxel Device applies the table's entries in order like the firewall for example), you can select an entry and click **Add** to create a new entry after 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 16 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 16 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 25.6 on page 258 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.

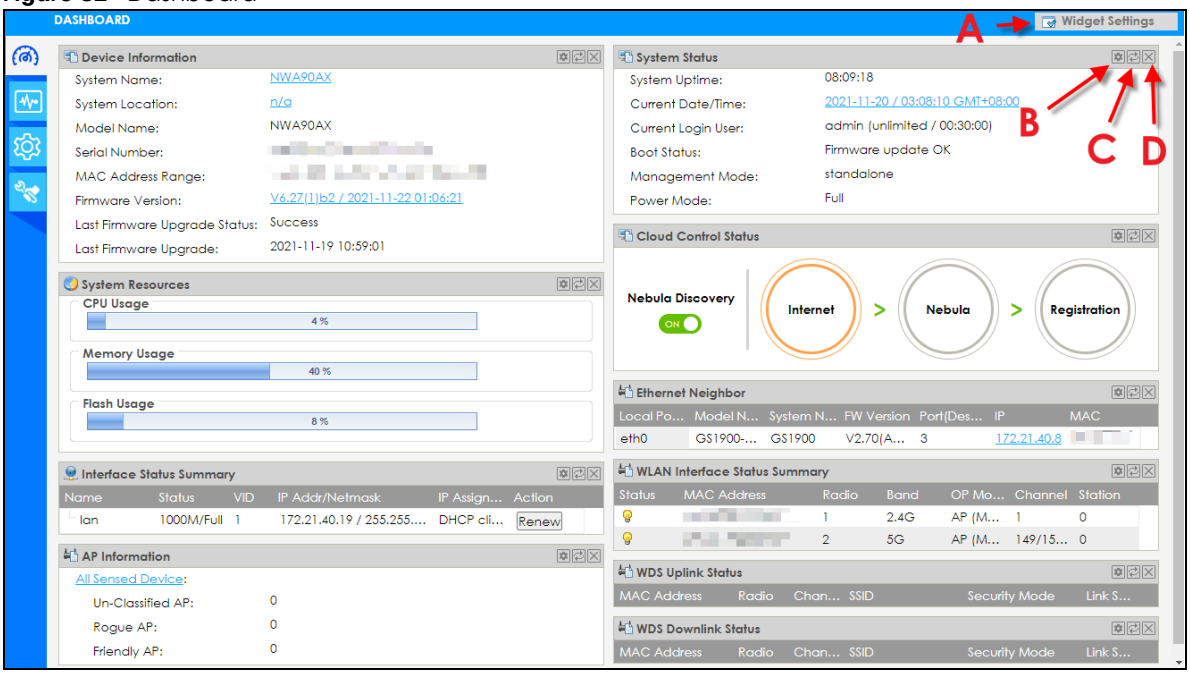
The Zyxel Device does not stop or start the system processes when you apply configuration files or run shell scripts although you may temporarily lose access to network resources.

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 rearrange to suit your needs. You can also collapse, refresh, and close individual widgets. Fields in this screen may slightly differ by models.

Figure 31 Dashboard



The following table describes the labels in this screen.

Table 17 Dashboard

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

Table 17 Dashboard (continued)

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

Table 17 Dashboard (continued)

LABEL	DESCRIPTION
Current Login User	This field displays the user name used to log in to the current session, the amount of reauthentication time remaining, and the amount of lease time remaining.
Boot Status	This field displays details about the Zyxel Device's startup state. **OK** - The Zyxel Device started up successfully. **Firmware update OK** - A firmware update was successful. **Problematic configuration after firmware update** - The application of the configuration failed after a firmware upgrade. **System default configuration** - The Zyxel Device successfully applied the system default configuration. This occurs when the Zyxel Device starts for the first time or you intentionally reset the Zyxel Device to the system default settings. **Fallback to lastgood configuration** - The Zyxel Device was unable to apply the startup-config.conf configuration file and fell back to the lastgood.conf configuration file. **Fallback to system default configuration** - The Zyxel Device was unable to apply the lastgood.conf configuration file and fell back to the system default configuration file (system-default.conf). **Booting in progress** - The Zyxel Device is still applying the system configuration.
Management Mode	This shows whether the Zyxel Device is set to work as a 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 11.

Table 17 Dashboard (continued)

LABEL	DESCRIPTION
Cloud Control Status	This field displays only in cloud managed mode: • 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. **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.
Interface Status Summary	If an Ethernet interface does not have any physical ports associated with it, its entry is displayed in light gray text.
Name	This field displays the name of each interface.
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.
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.

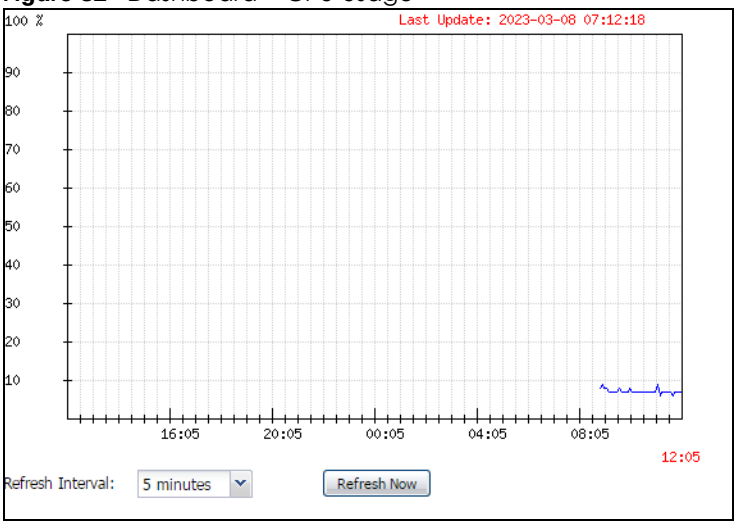
Table 17 Dashboard (continued)

LABEL	DESCRIPTION
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.
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 32 Dashboard > CPU Usage



The following table describes the labels in this screen.

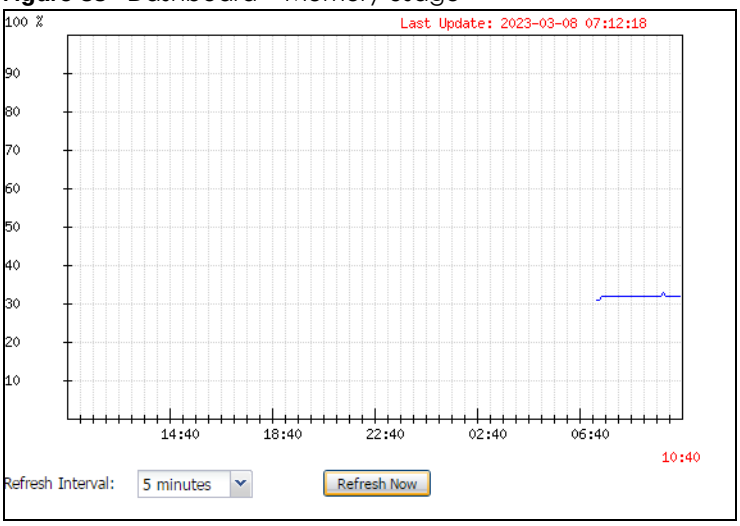
Table 18 Dashboard > CPU Usage

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 33 Dashboard > Memory Usage



The following table describes the labels in this screen.

Table 19 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 for the USA in order to comply with the U.S. laws, policies and regulations.

- **Time Zone**: Select the time zone of your Zyxel Device's location. This will set the time difference between your time zone and Coordinated Universal Time (UTC). UTC is a standard time for use around the world (formerly known as Greenwich Mean Time or GMT). UTC is an international abbreviation that is neither French nor English. It means both "Temps Universel Coordonné" and "Coordinated Universal Time".
- **Enable Daylight Saving**: Select this option if the location in which your Zyxel Device is uses Daylight Saving Time. Configure the date 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 **Exit** to close the wizard without saving.

Figure 34 Wizard: Time Settings

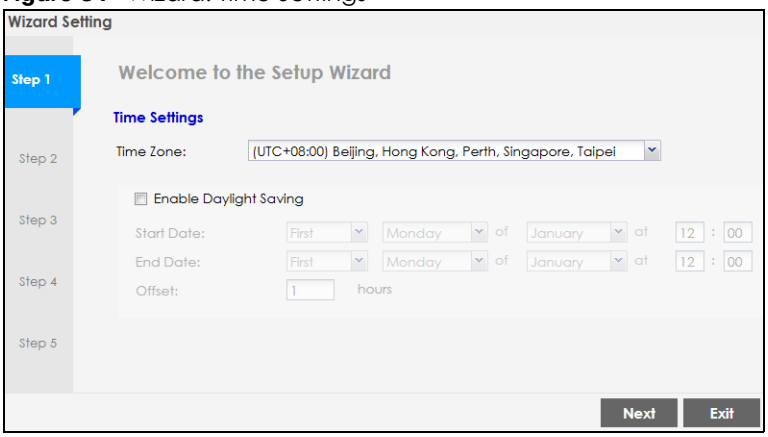
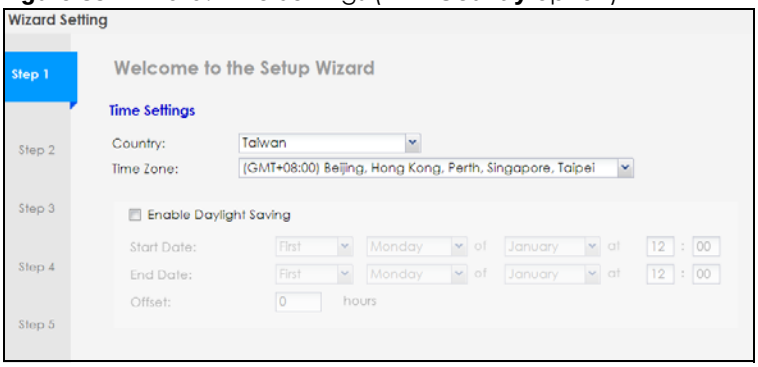


Figure 35 Wizard: Time Settings (with **Country** option)



7.2.2 Step 2 Password and Uplink Connection

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

Uplink Connection: Select **Auto (DHCP)** if the Zyxel Device is connected to a router with 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.

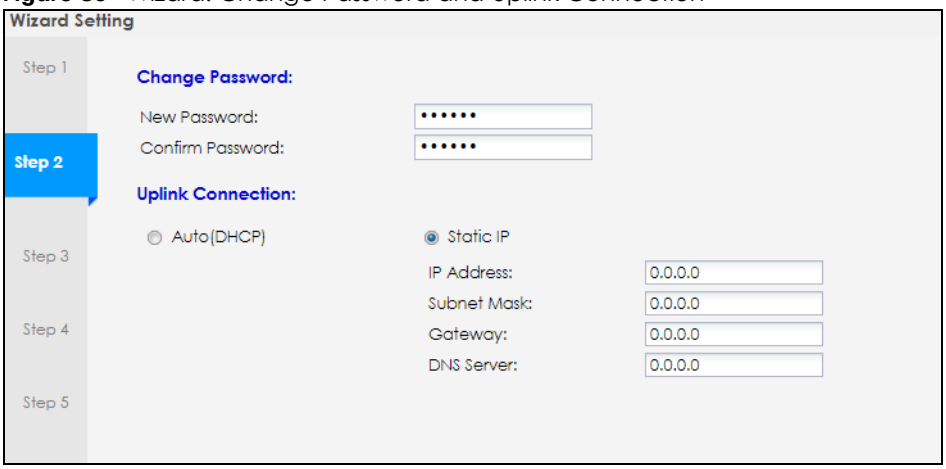
Otherwise, select **Static IP** when the Zyxel Device is NOT connected to a router or you want to assign it a fixed IP address. You will need to manually enter:

- 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 **Back** to return to the previous screen. Click **Next** to proceed. Click **Exit** 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 36 Wizard: Change Password and Uplink Connection



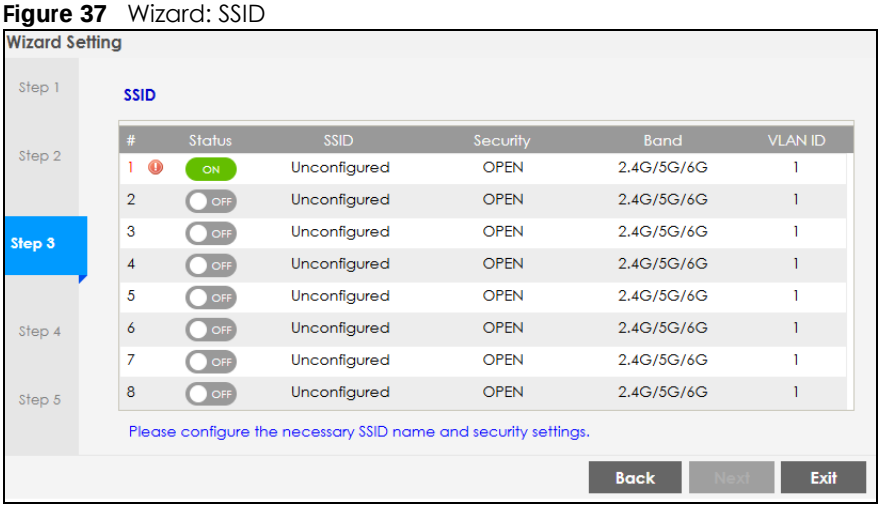
7.2.3 Step 3 SSID

Use this screen to enable, disable or edit an SSID profile. An SSID profile is a configuration template for SSID (Service Set IDentifier). It allows you to configure the SSID settings such as WiFi network name, VLAN ID, frequency band and security. You can configure multiple SSID profiles to provide different network access for various user groups.

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 59 for more information.

Note: You must configure the first SSID in the list (default SSID).

Figure 37 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.

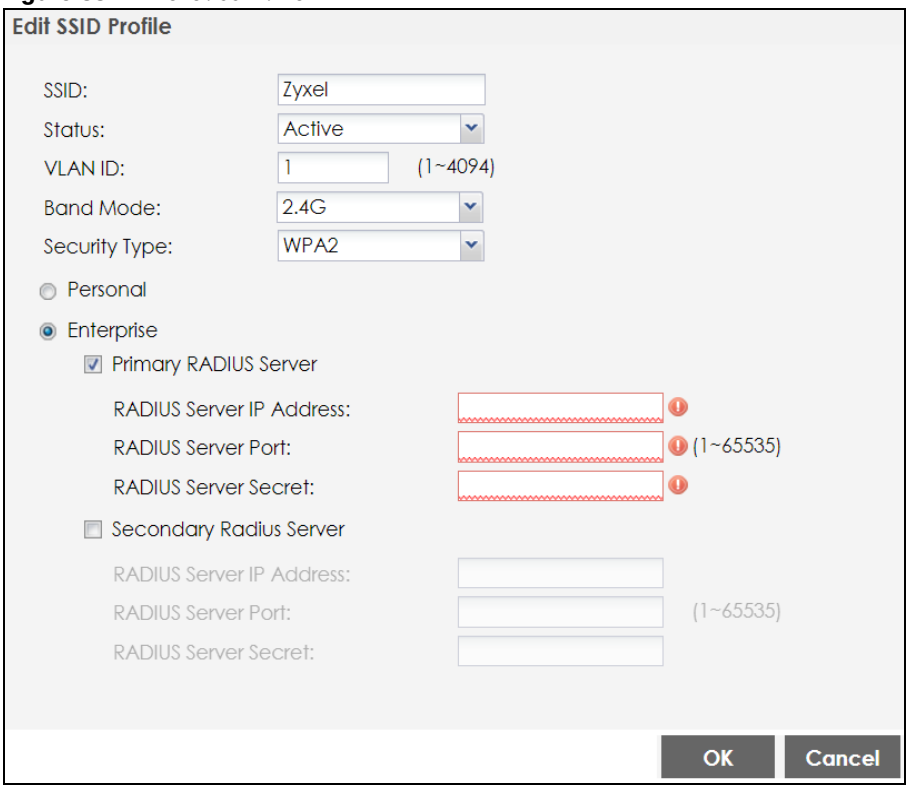
- **SSID**: Enter a descriptive name of up to 32 printable characters for the WiFi network.

- **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 (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.
- **Security Type (Security Mode)**: Select **WPA2** or **WPA3** to add security on this WiFi network (recommended). Select **OPEN** or **Enhanced-Open** to allow any WiFi client to associate this network without authentication.
- **Personal**: Select this to store passwords for users on the Zyxel Device. 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 to store passwords for users on an external RADIUS authentication server. Select **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: Not all Zyxel Devices support the enterprise authentication settings; see Section 1.2 on page 11 for more information.

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

Figure 38 Wizard: SSID: Edit



7.2.4 Step 4 Radio

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

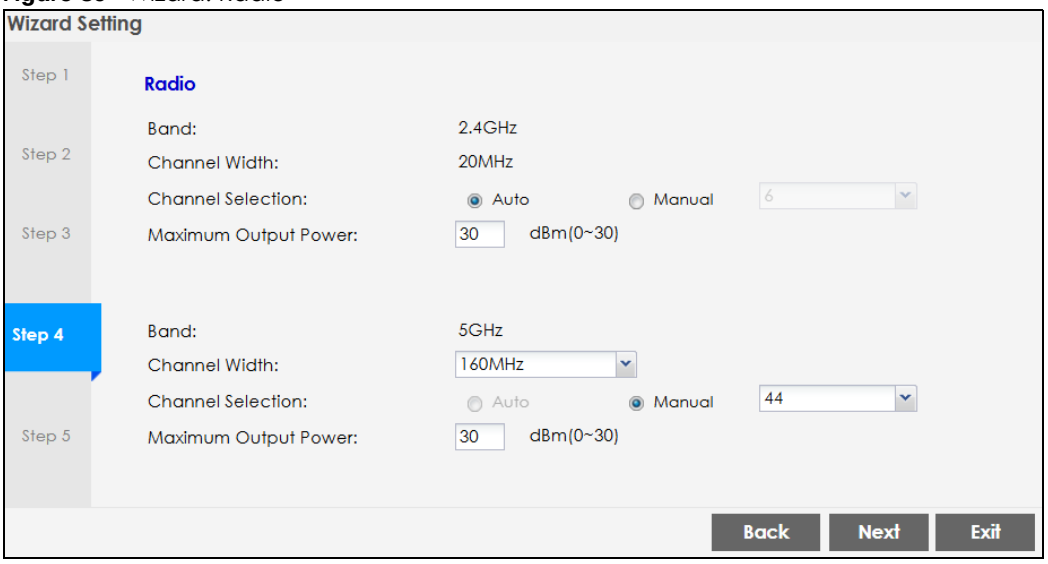
- **Band**: This displays the radio band.

- **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. See Section 13.2.1 on page 136.
- **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.

Click **Back** to return to the previous screen. Click **Next** to proceed. Click **Exit** to close the wizard without saving.

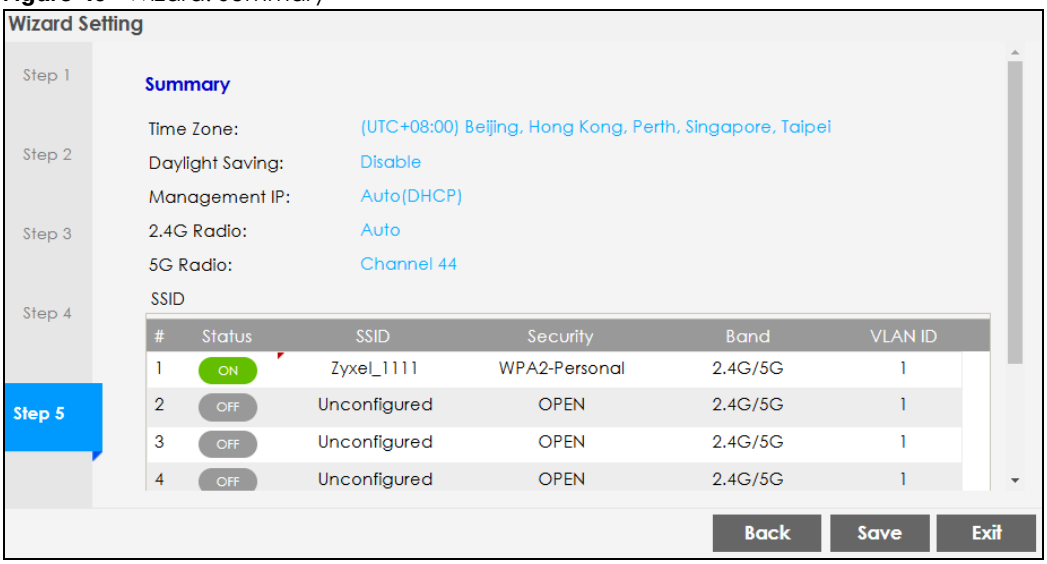
Figure 39 Wizard: Radio



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 **Back** to return to the previous screen or click **Exit** to close the wizard without saving.

Figure 40 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

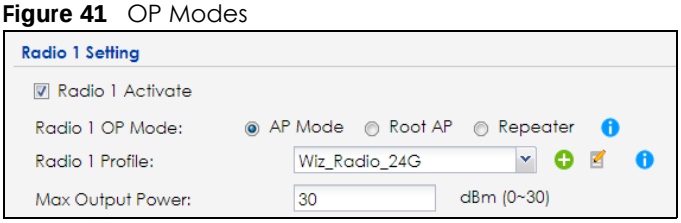
In this section, we show you how to:

- 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 41 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).

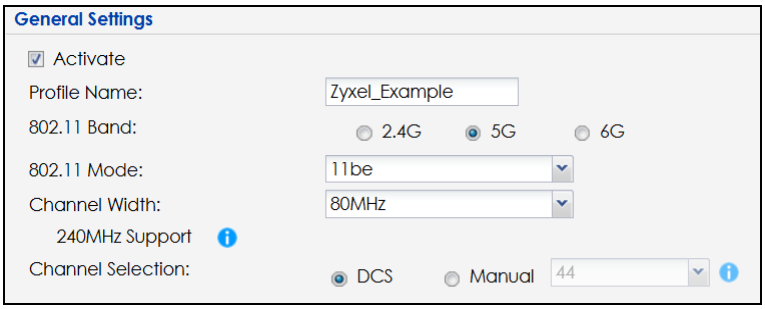
8.2.2 Set Up a WiFi Network in AP Mode

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

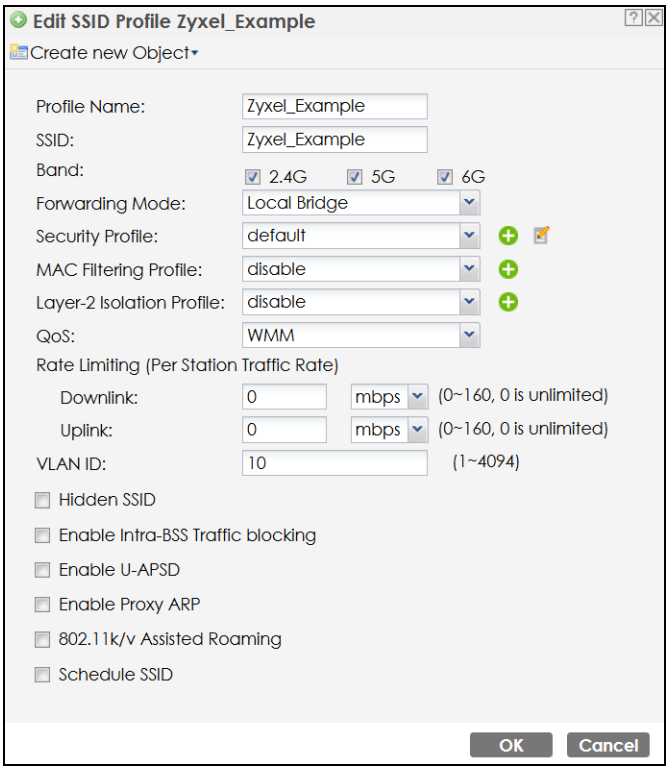
Table 20 SSID Profile Settings Example

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

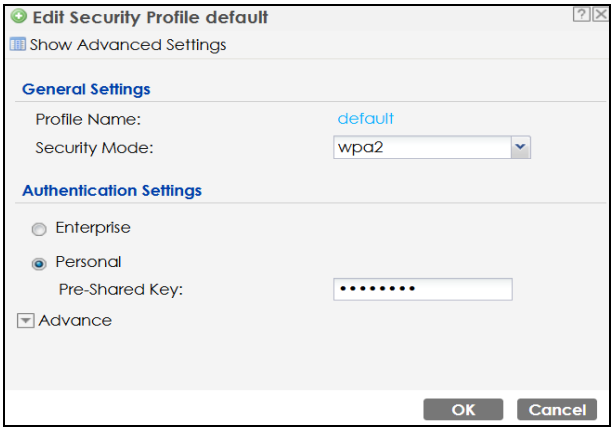
1 Go to **Configuration** > **Object** > **AP Profile** > **Radio** > **Add**. Enter the profile name, select the 802.11 mode and select a channel (36 in this example) that is not used by another AP. Click **OK**.



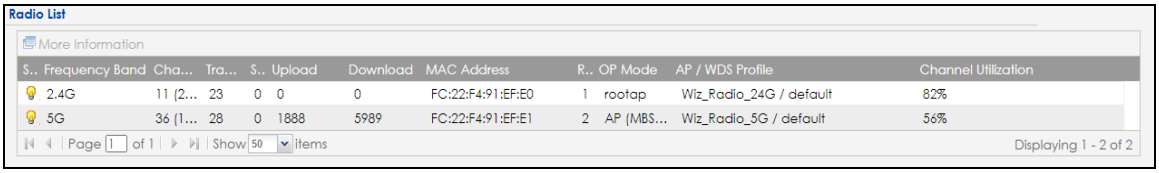
2 Go to **Configuration** > **Object** > **AP Profile** > **SSID** > **SSID List**, select a SSID profile and click **Edit** to configure the SSID settings. Click **OK**.



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.

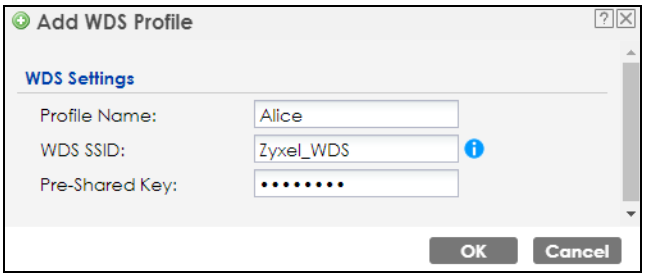
8.2.3 Set Up a WiFi Network in Root AP/Repeater Mode

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 APC-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 13.4.2 on page 162 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 42 General and Guest WiFi Networks

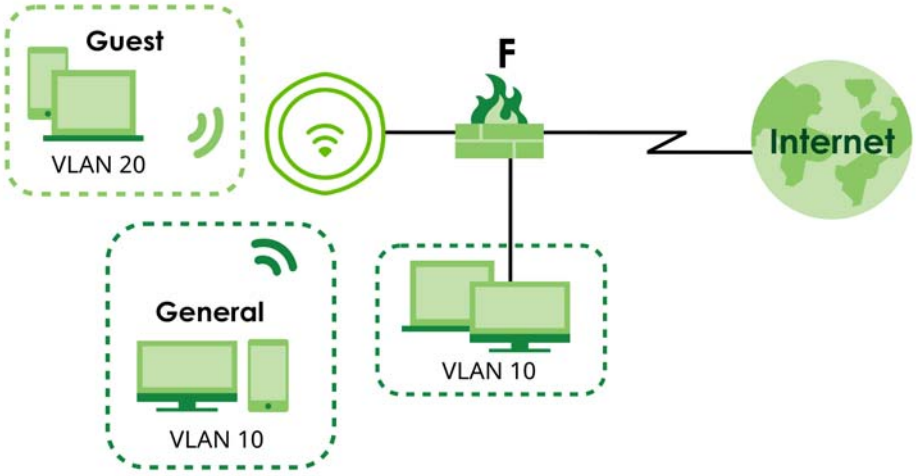
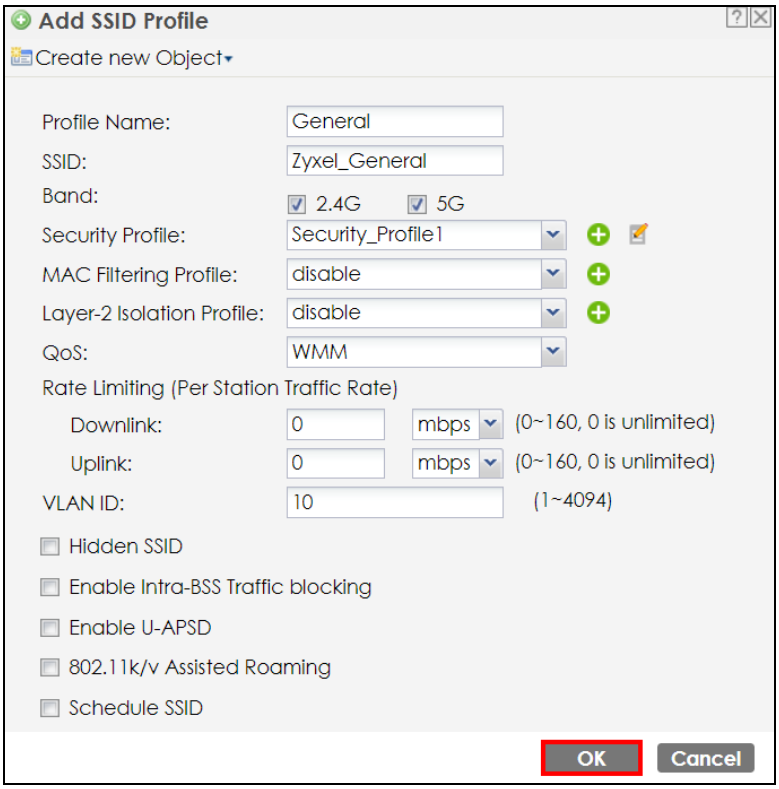


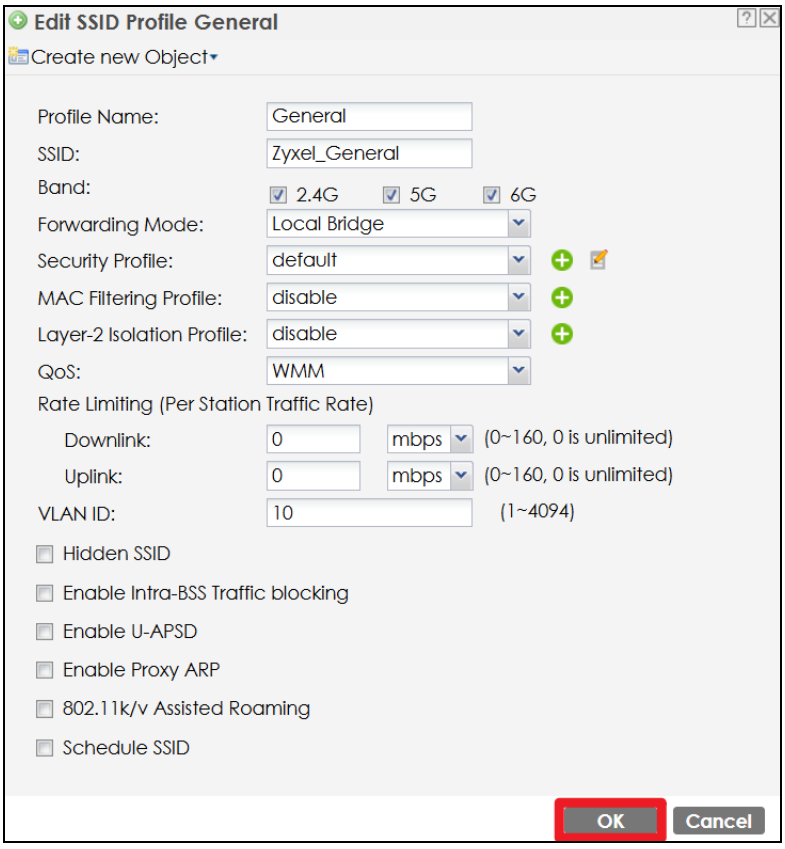
Table 21 General and Guest SSID Profiles

	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

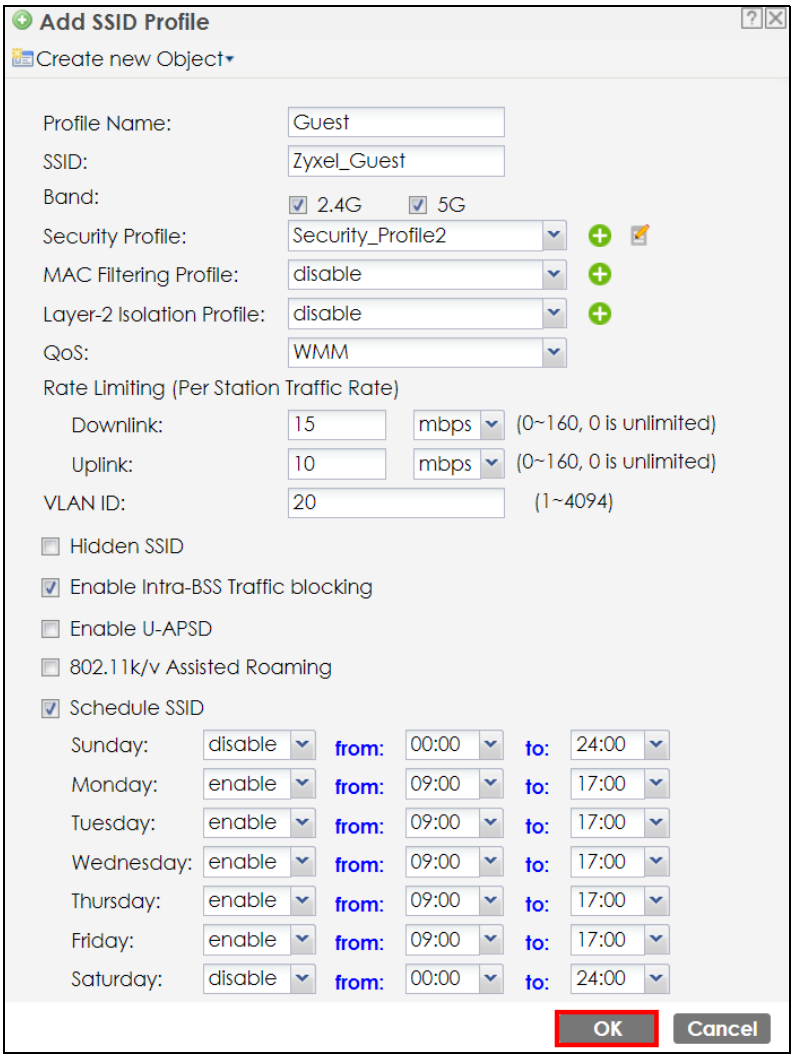
1 Go to **Configuration** > **Object** > **AP Profile** > **SSID** > **SSID List**, click **Add** to create an SSID profile.

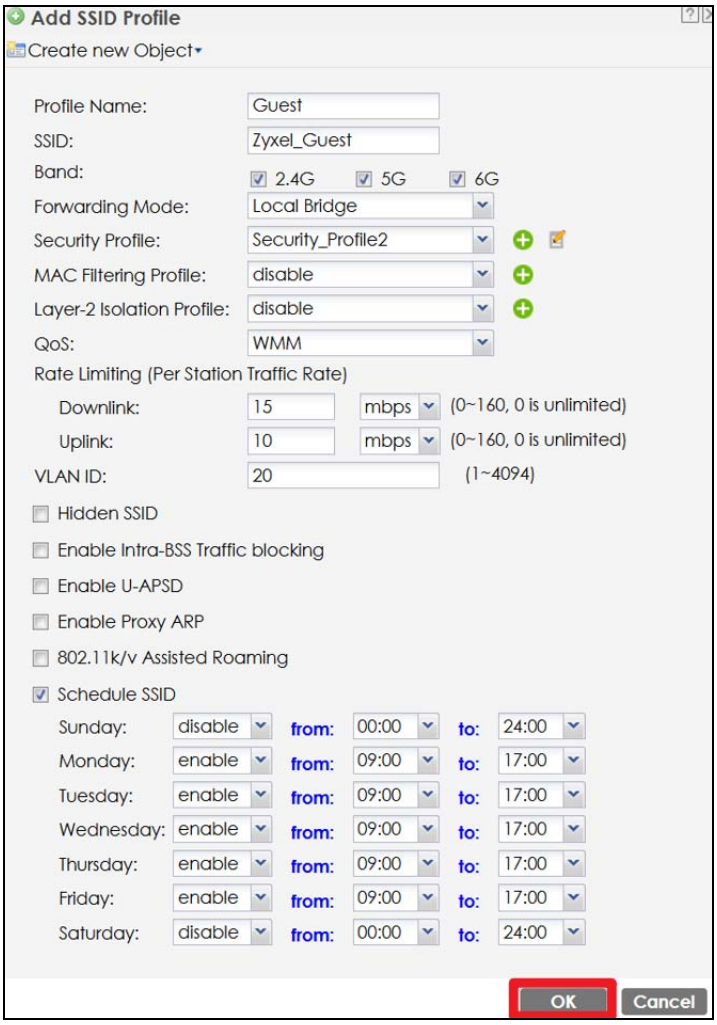
2 Configure the first SSID – **Zyxel_General** using the parameters given above, and then click **OK**.



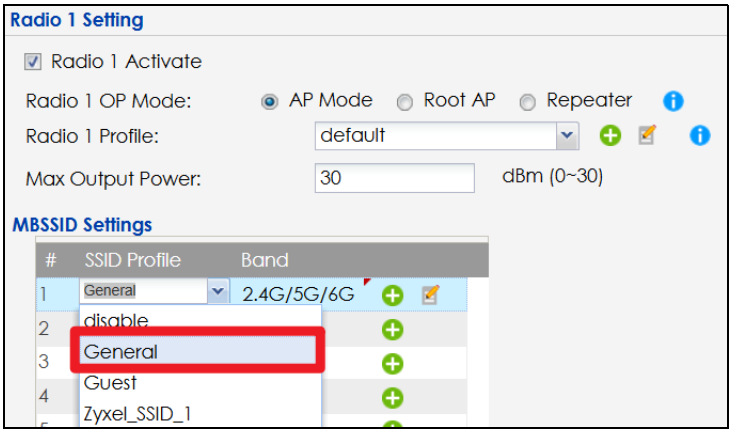


3 Configure the second SSID – **Zyxel_Guest** using the parameters given above, and then click **OK**.

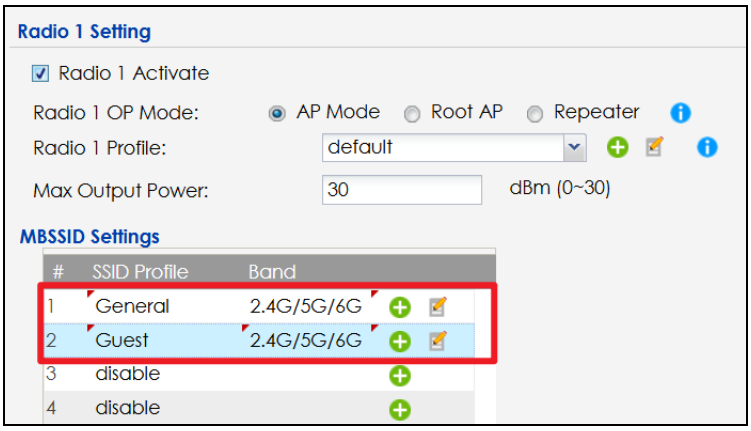

Add SSID Profile
Create new Object
Profile Name: Guest
SSID: Zyxel_Guest
Band: 2.4G 5G
Security Profile: Security_Profile2
MAC Filtering Profile: disable
Layer-2 Isolation Profile: disable
QoS: WMM
Rate Limiting (Per Station Traffic Rate)
Downlink: 15 mbps (0~160, 0 is unlimited)
Uplink: 10 mbps (0~160, 0 is unlimited)
VLAN ID: 20 (1~4094)
Hidden SSID
Enable Intra-BSS Traffic blocking
Enable U-APSD
802.11k/v Assisted Roaming
Schedule SSID
Sunday: disable from: 00:00 to: 24:00
Monday: enable from: 09:00 to: 17:00
Tuesday: enable from: 09:00 to: 17:00
Wednesday: enable from: 09:00 to: 17:00
Thursday: enable from: 09:00 to: 17:00
Friday: enable from: 09:00 to: 17:00
Saturday: disable from: 00:00 to: 24:00
OK
Cancel



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.



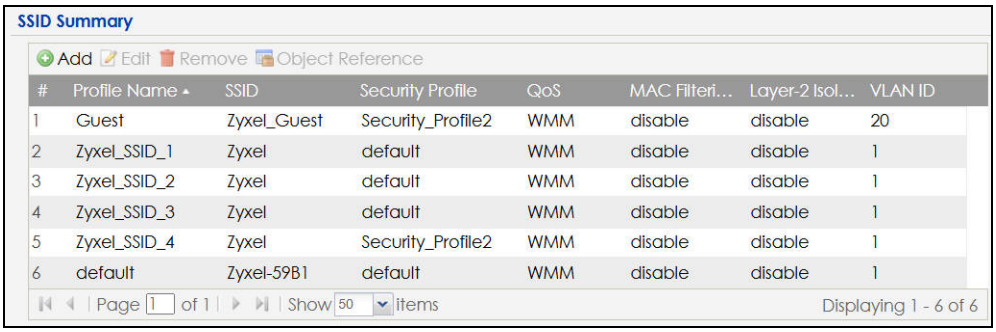
6 Click the first **SSID Profile** of **Radio 2** (5 GHz). A drop-down list appears. Select the **General** SSID profile you just configured. Click the second **SSID Profile** and select the **Guest** SSID profile.

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.

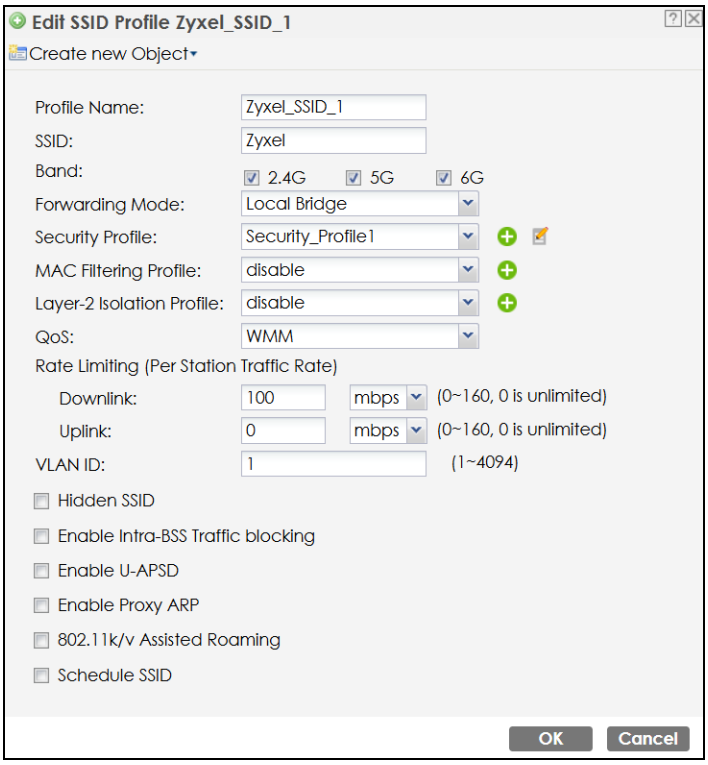
8.3 Limit Network Bandwidth for Each WiFi Client

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

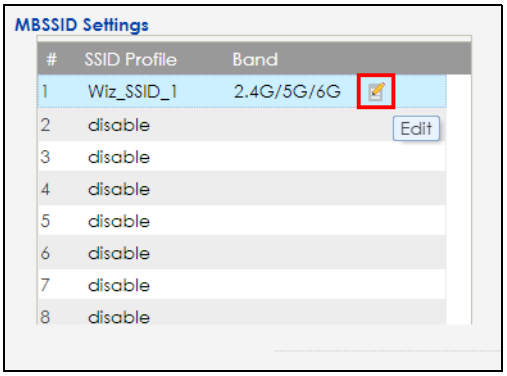
In this section, we show you how to:

- 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

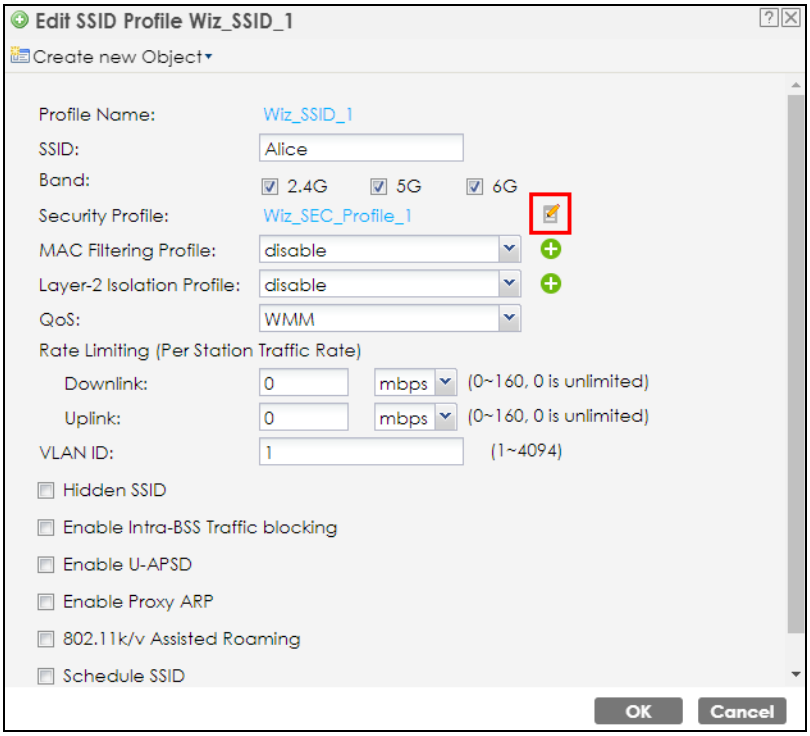
8.4.1 Change Security for a WiFi Network

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 74 for more information.

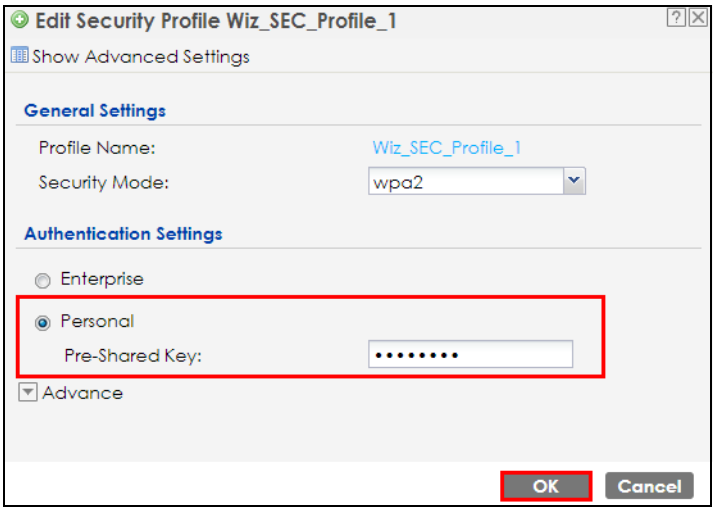
1 Go to the **Configuration** > **Wireless** > **AP Management** > **WLAN Setting** screen. Click **Edit** under the SSID profile to change the WiFi security.



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



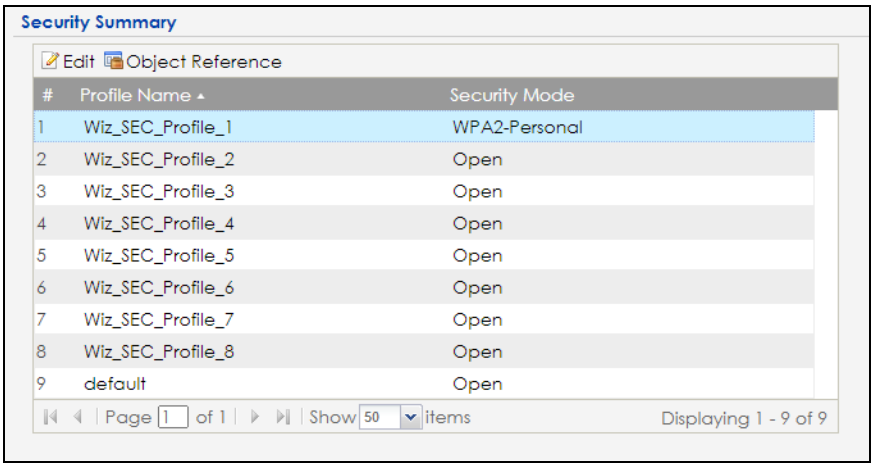
3 The following screen appears, select **Personal** and enter a pre-shared key from 8 to 63 case-sensitive keyboard characters in **Pre-Shared Key**. Click **OK** to save your changes.



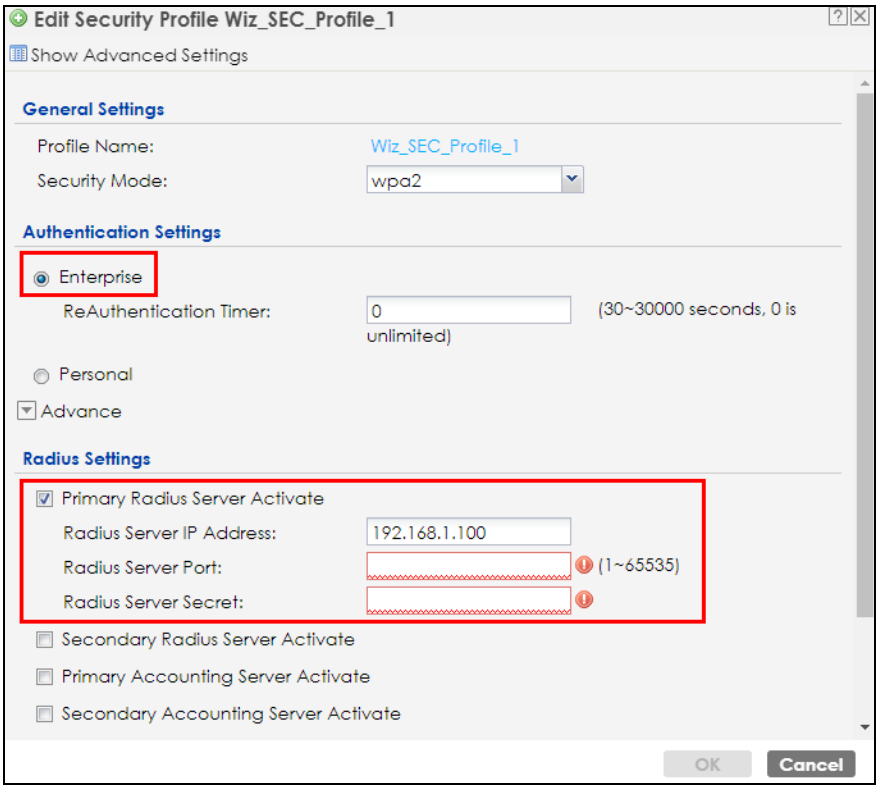
8.4.2 RADIUS Server Setup

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

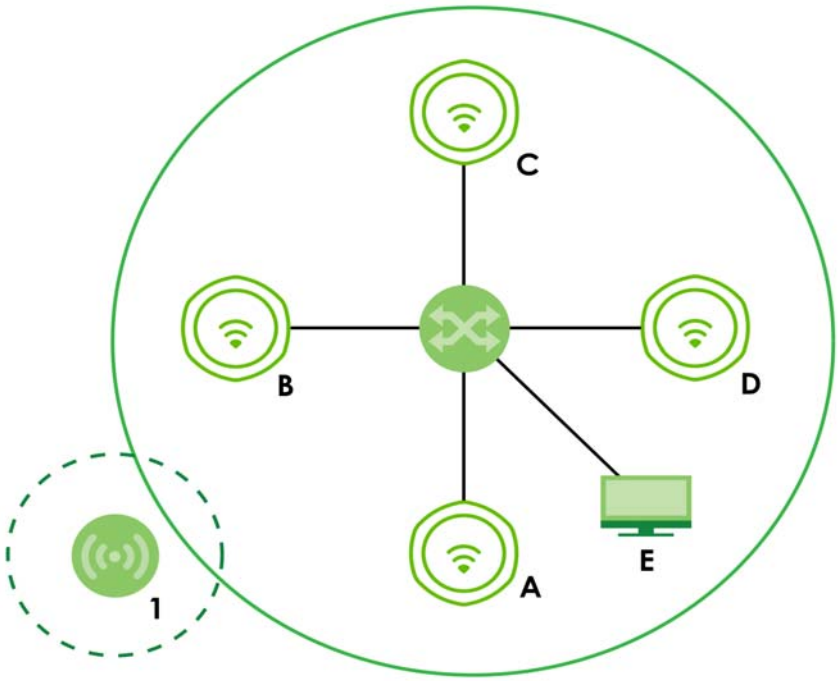
This example shows you how to configure the rogue AP detection feature on the Zyxel Device. A rogue AP is a WiFi access point operating in a network's coverage area that is not a sanctioned part of that network. See Section 11.3 on page 119 for background information on the rogue AP function and security 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 43 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 22 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

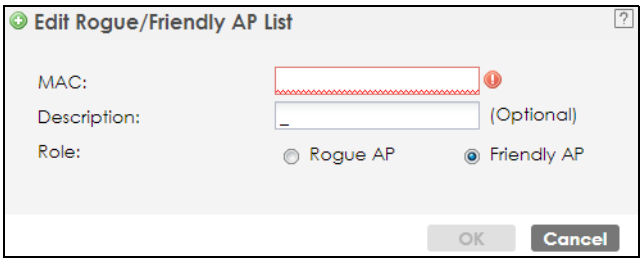
Note: You can detect the MAC addresses of other APs in the **Monitor > Wireless > Detected Device** screen. However, it is more secure to obtain the correct MAC addresses from another source and add them to the friendly AP list manually. For example, an attacker's AP mimicking the correct SSID could 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.

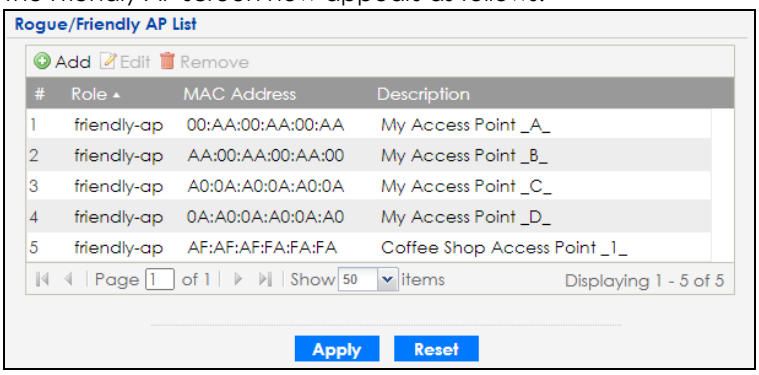


2 Fill in the **MAC** and **Description** fields as in the following table. Click **Add** after you enter the details of each AP to include it in the list.

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_

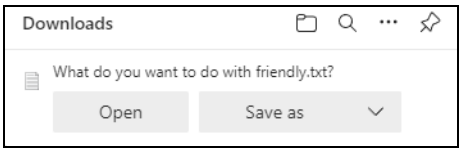
Note: You can add APs that are not part of your network to the friendly AP list, as long as you know that they do not pose a threat to your network's security.

The Friendly AP screen now appears as follows.

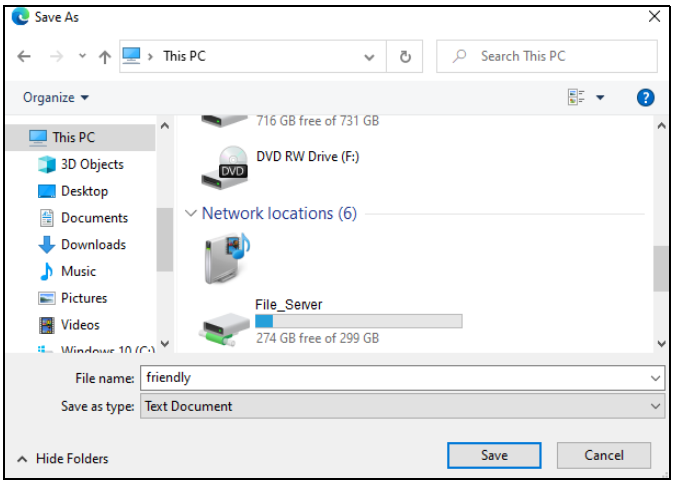


3 Next, click **Apply** to save the list of friendly APs in order to provide a backup and upload it to your other access points.

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.

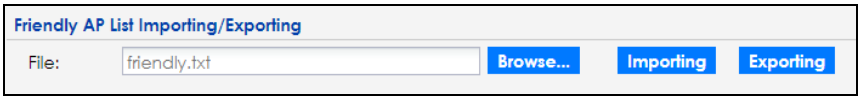
- Scan for access points in its coverage area
- Recognize friendly access points from a list

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

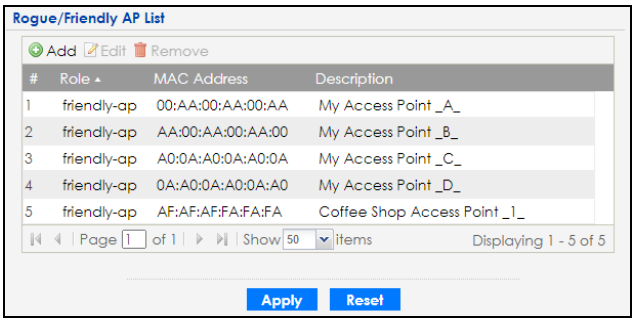
For each access point, take the following steps.

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.

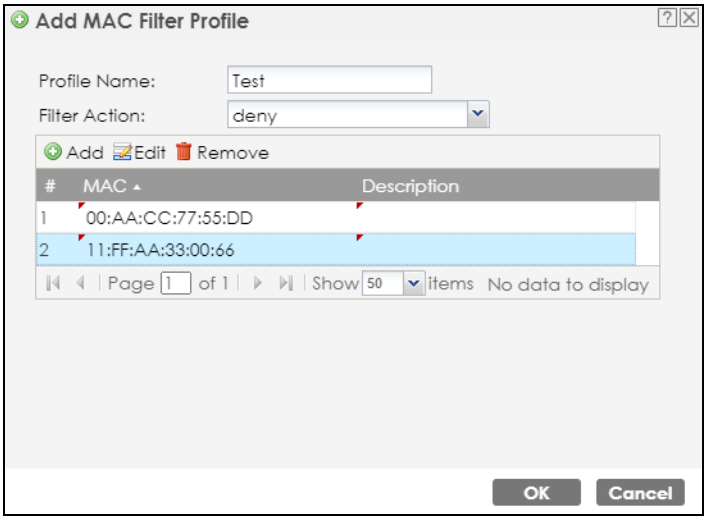


8.4.5 Set Up a MAC Filter List

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.

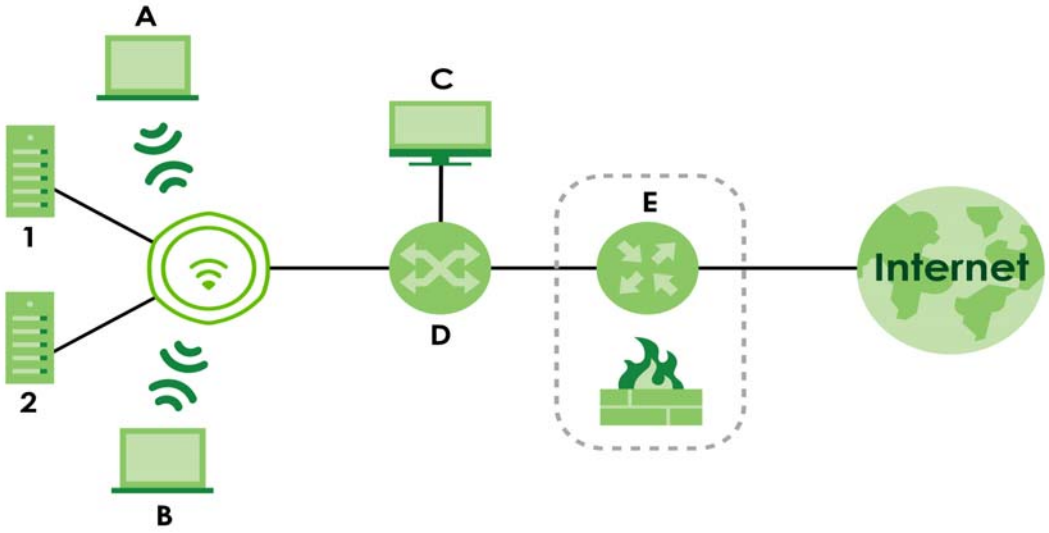
8.4.6.1 Scenario

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 44 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 63). It uses two SSID profiles simultaneously. You have configured each SSID profile as shown in the following table.

Table 23 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 24 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 25 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.

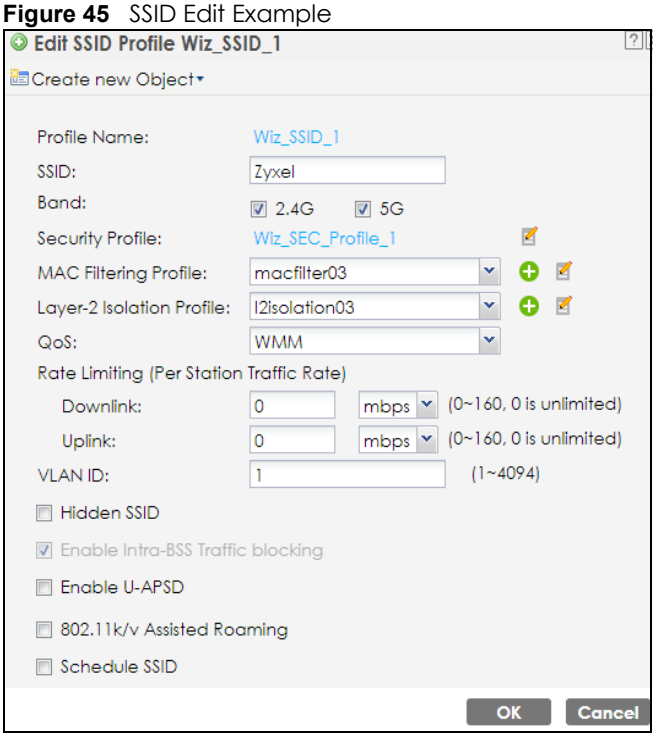
You will configure the MAC filter to restrict access to Alice alone, and then configure layer-2 isolation to allow her to access only the network router, the file server and the Internet security gateway.

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**.

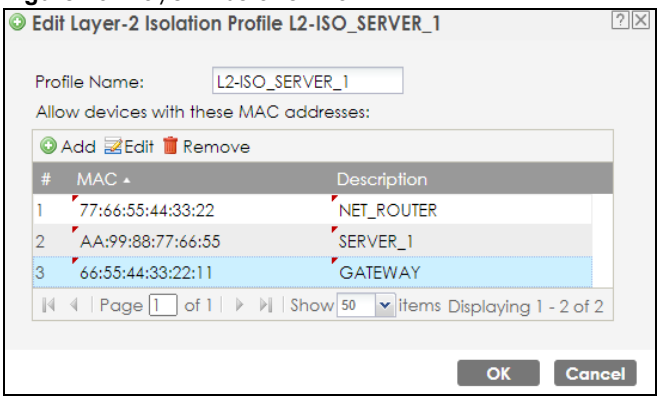
2 The following screen appears. Select **l2Isolation03** for **Layer-2 Isolation Profile**, and select **macfilter03** for **MAC Filtering Profile**. Click **OK**.

Figure 45 SSID Edit Example



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

Figure 46 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.

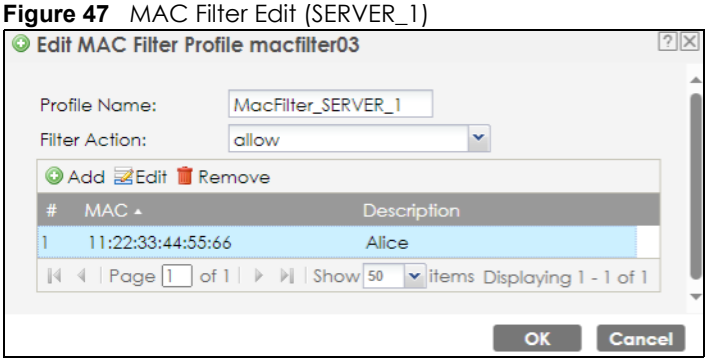
5 Enter server 1's MAC Address and add a Description ("SERVER_1" in this case) in Set 2's entry.

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 47 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 81, substituting the following information.

Table 26 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

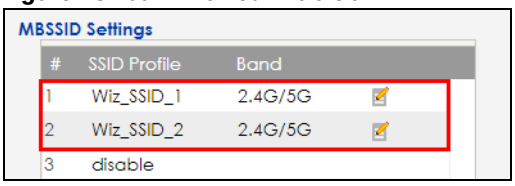
Use the following sections to ensure that your WiFi networks are set up correctly.

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.

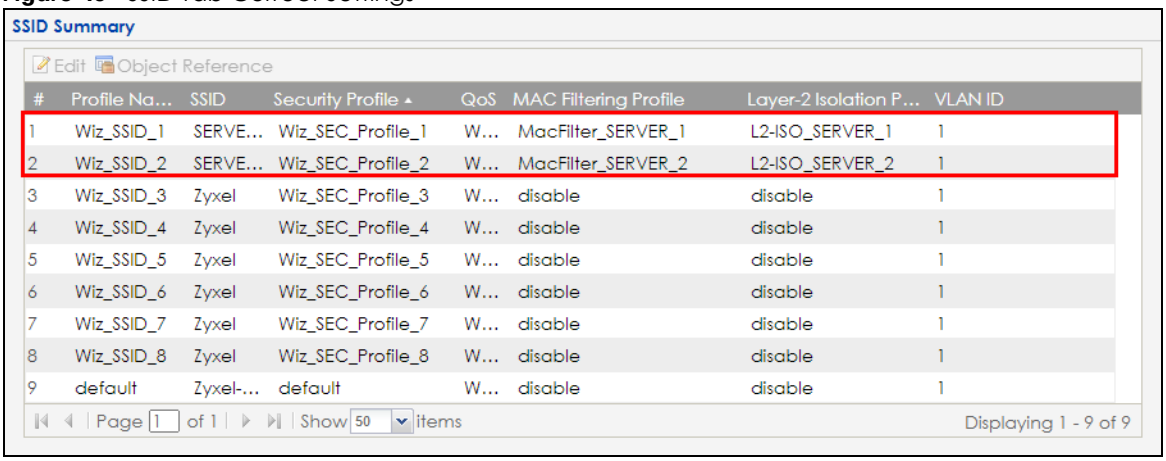
1 Click **Configuration > Wireless > AP Management**. Check that the correct SSID profiles are enabled, as shown in the following figure.

Figure 48 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 49 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 84, 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

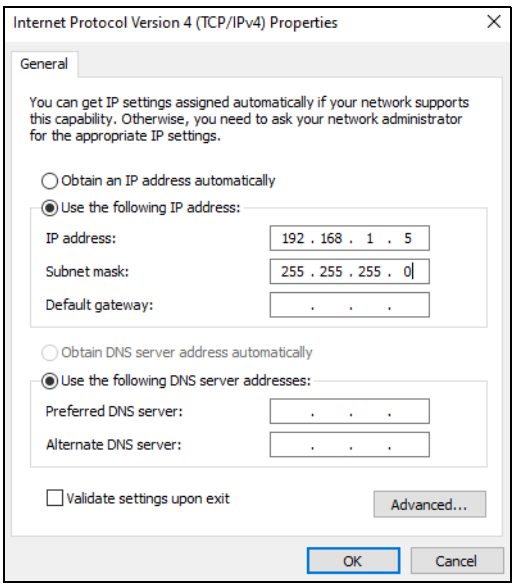
In this section, we show you how to:

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

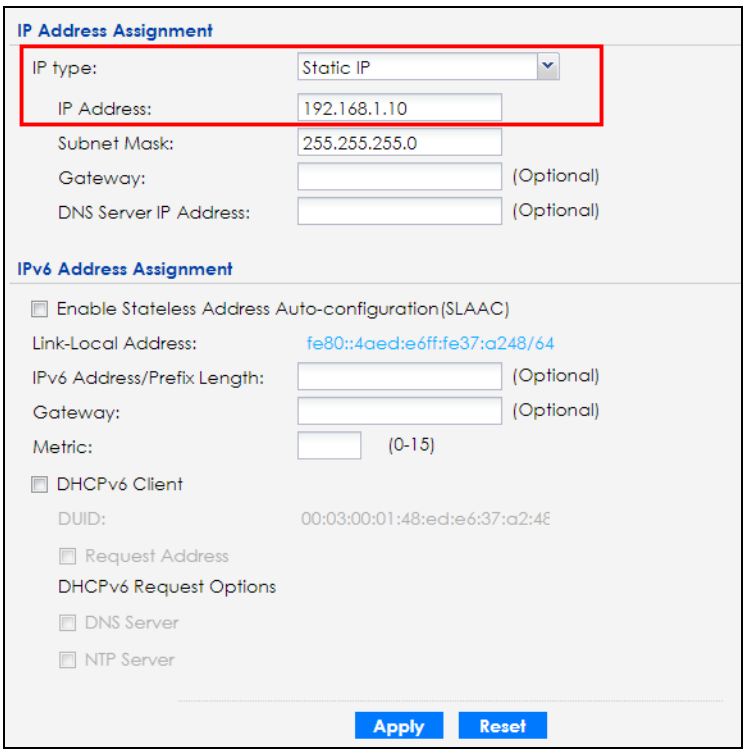
8.5.1 Change the Management IP Address

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.

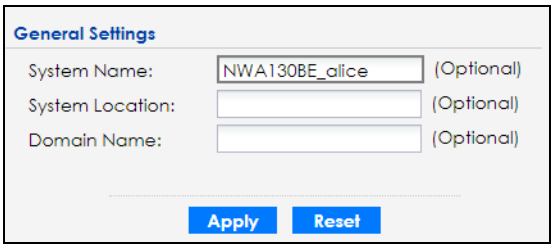


3 To check if the IP address of the Zyxel Device has been changed to "192.168.1.10", enter the new IP address "192.168.1.10" in the address bar and see if you can log in to the Web Configurator successfully. Ensure that your computer's IP address is in the same subnet as the Zyxel Device. For example,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

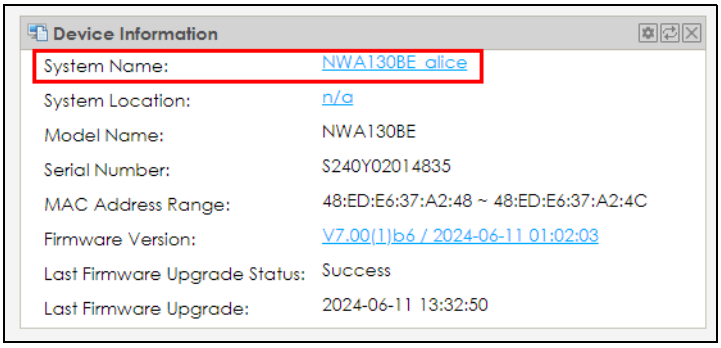
8.5.2 Change the System Name

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.



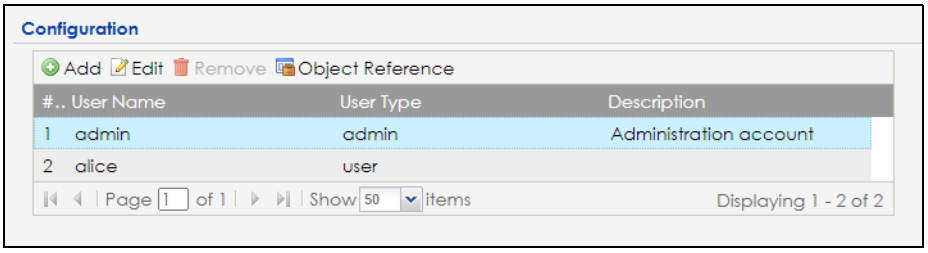
2 See the **System Name** field in the **Dashboard** screen to check if the new system name has been applied.



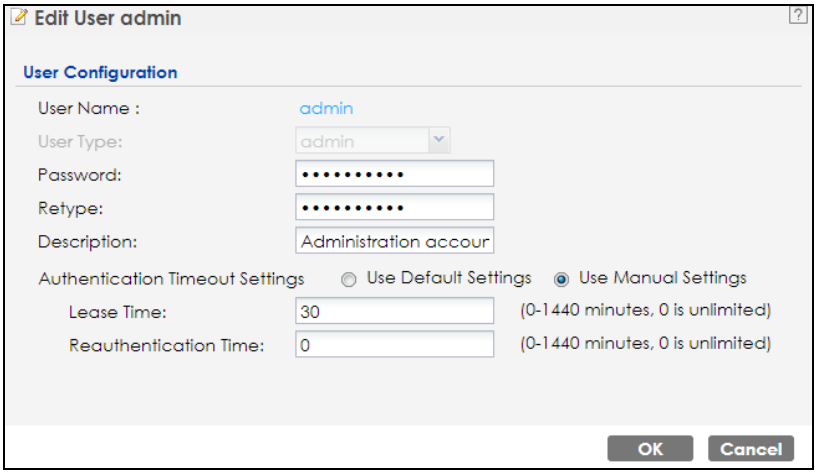
8.5.3 Change the Login Password

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 characters. Spaces are not allowed. Reenter 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

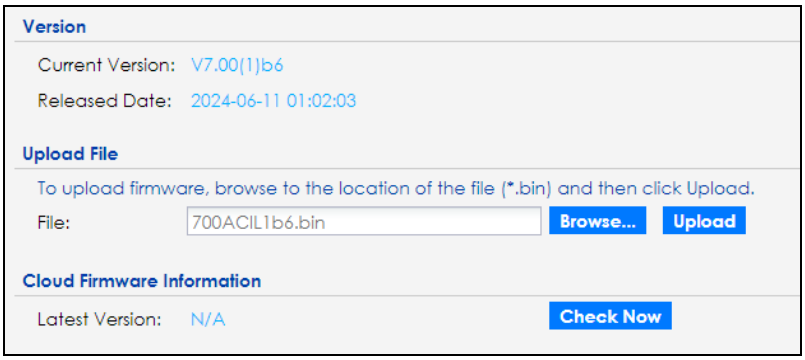
8.6.1 Upgrade the Firmware

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 27 Configuration File Types

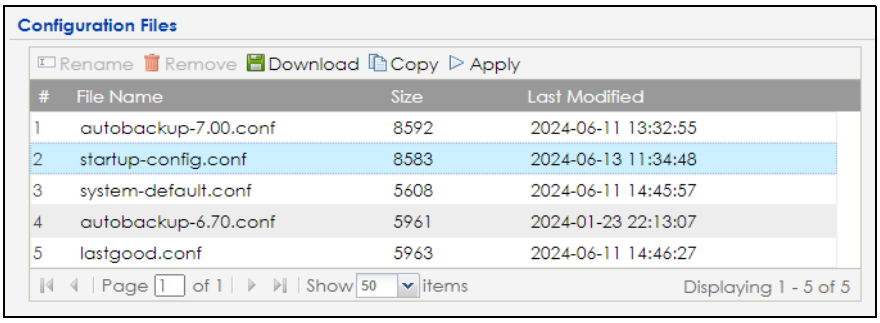
FILENAME	DESCRIPTION
autobackup-x.xx.conf	This is the configuration file that the Zyxel Device automatically backs up when upgrading the firmware.
startup-config.conf	This is the configuration file that the Zyxel Device is currently using.
system-default.conf	This is the Zyxel Device's default settings.
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.

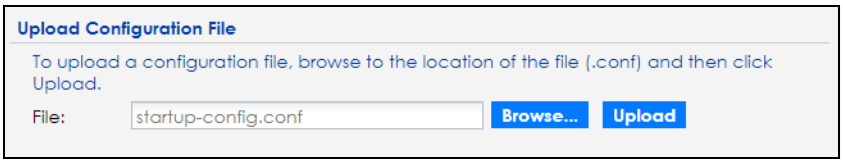
2 Under the **Configuration Files**, select **startup-config.conf** and click **Download**. The current configuration file that the Zyxel Device is using is saved to your computer. You can rename the configuration file to include the date you downloaded it. For example, **startup-config.conf_20240716**.



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:

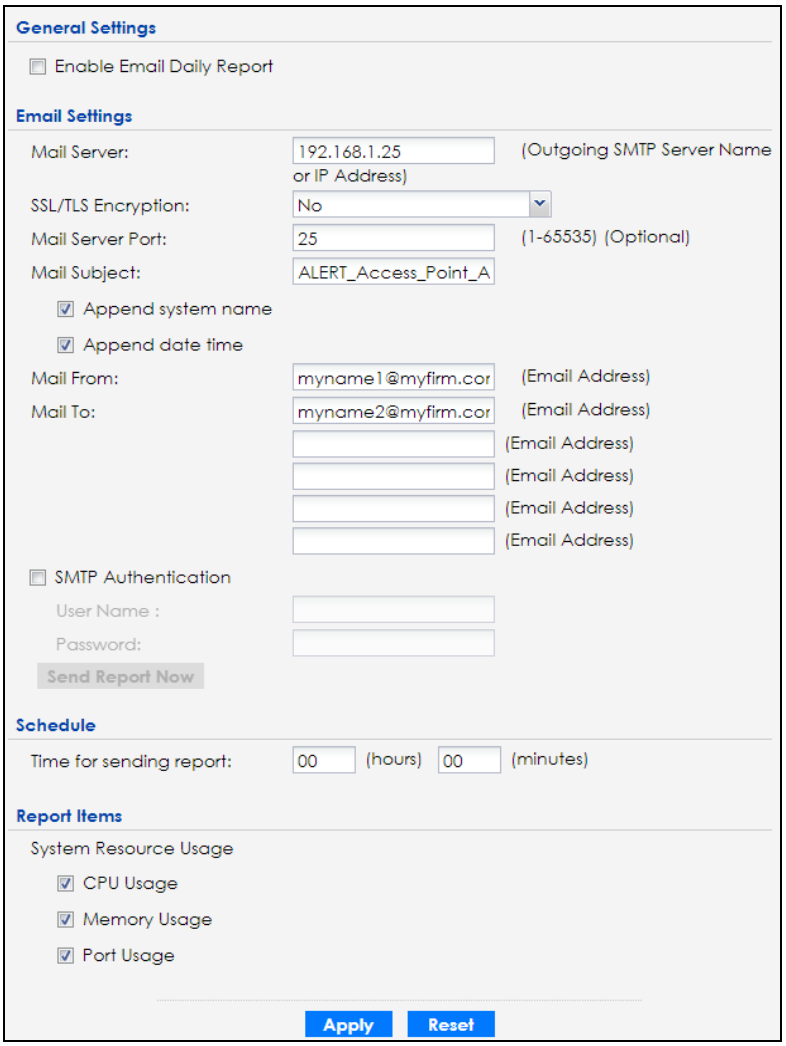
- Daily Email Report Setup
- Back Up Logs to a Remote Server

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.



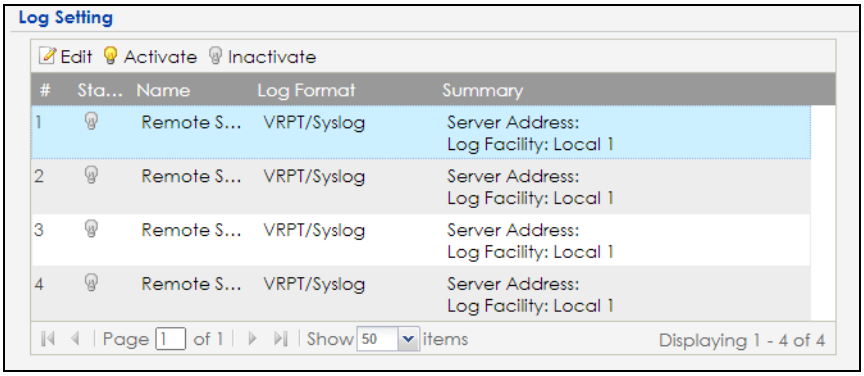
2 Enter a subject line for the alert emails in the **Mail Subject** field. Choose a subject that is eye-catching and identifies the access point - in this example, "ALERT_Access_Point_A".

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

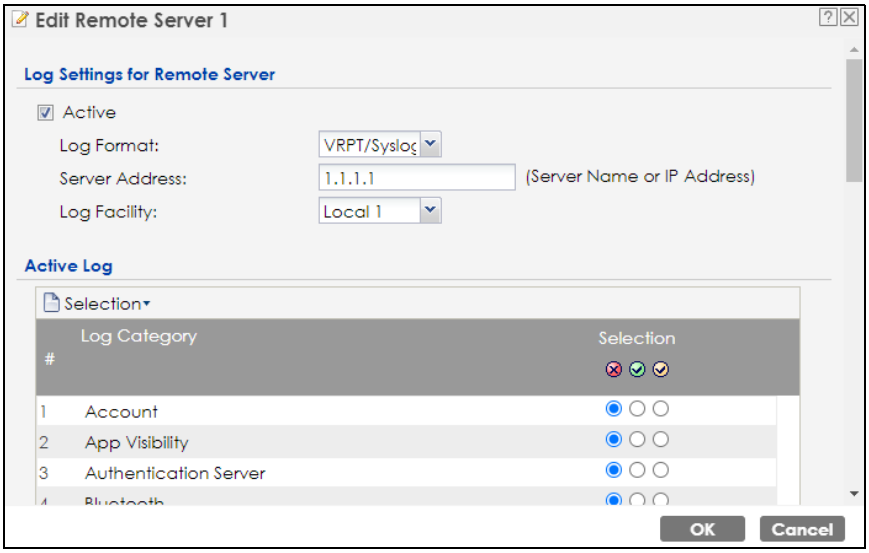
8.7.2 Back Up Logs to a Remote Server

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**.

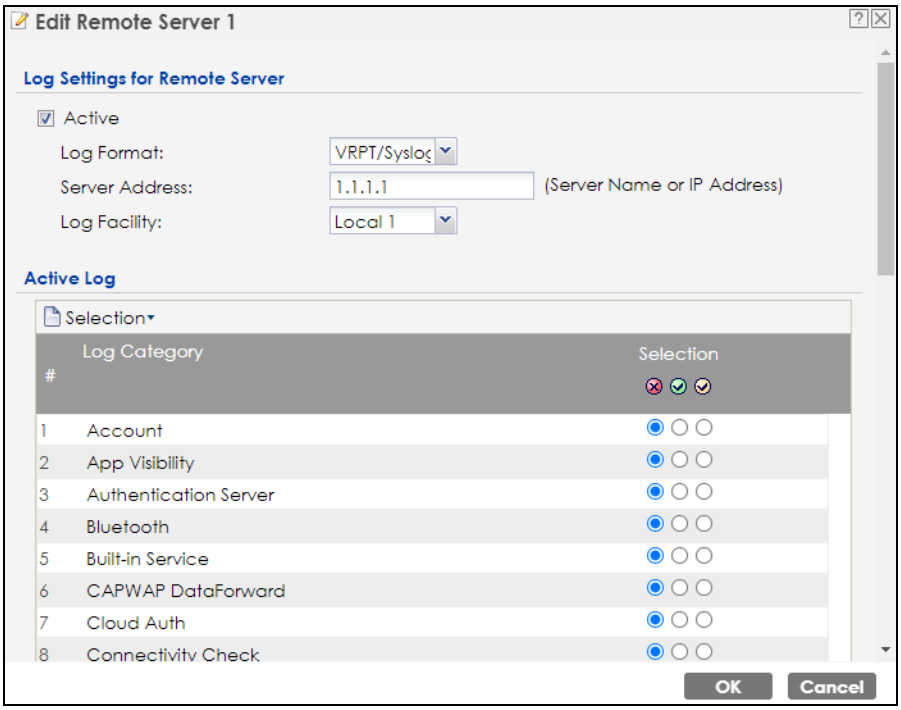


2 The following screen appears. Select **Active** and enter the IPv4 address or name of the remote server in the **Server Address** field to send the logs. Then, select a log facility. The log facility allows you to log the messages to different files in the syslog server. Please see the documentation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

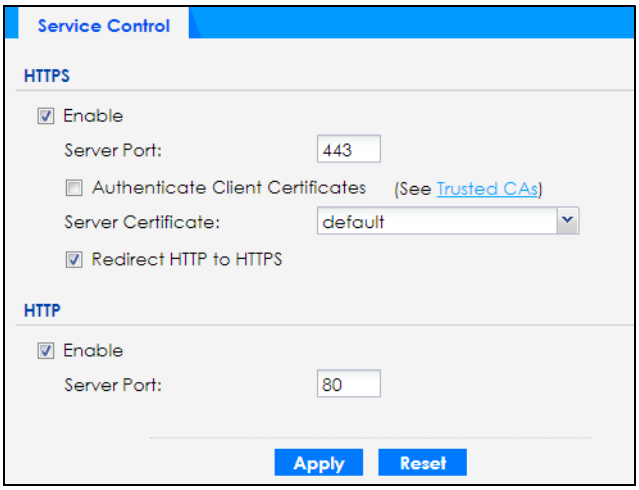
8.8 Access to the Zyxel Device

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

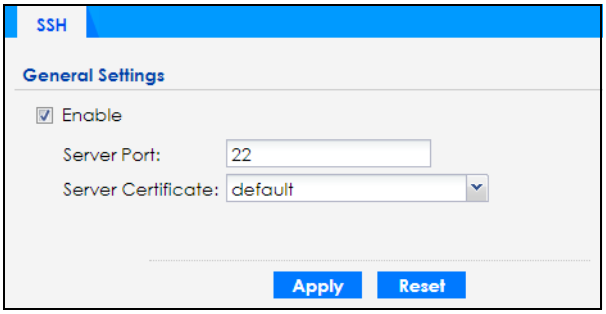
1 Go to the **Configuration** > **System** > **WWW** screen. Select whether you want to access the Zyxel Device remotely through HTTPS or HTTP. Click **Apply** to save your changes.



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

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 95) displays general LAN interface information and packet statistics.
- The **AP Information** > **Radio List** screen (Section 9.4 on page 97) displays statistics about the WiFi radio transmitters in the Zyxel Device.
- The **Station Info** screen (Section 9.5 on page 100) displays statistics pertaining to the associated stations.
- The **WDS Link Info** screen (Section 9.6 on page 101) displays statistics about the Zyxel Device's WDS (Wireless Distribution System) connections.
- The **Detected Device** screen (Section 9.7 on page 102) displays information about suspected rogue APs.
- The **View Log** screen (Section 9.8 on page 104) 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.

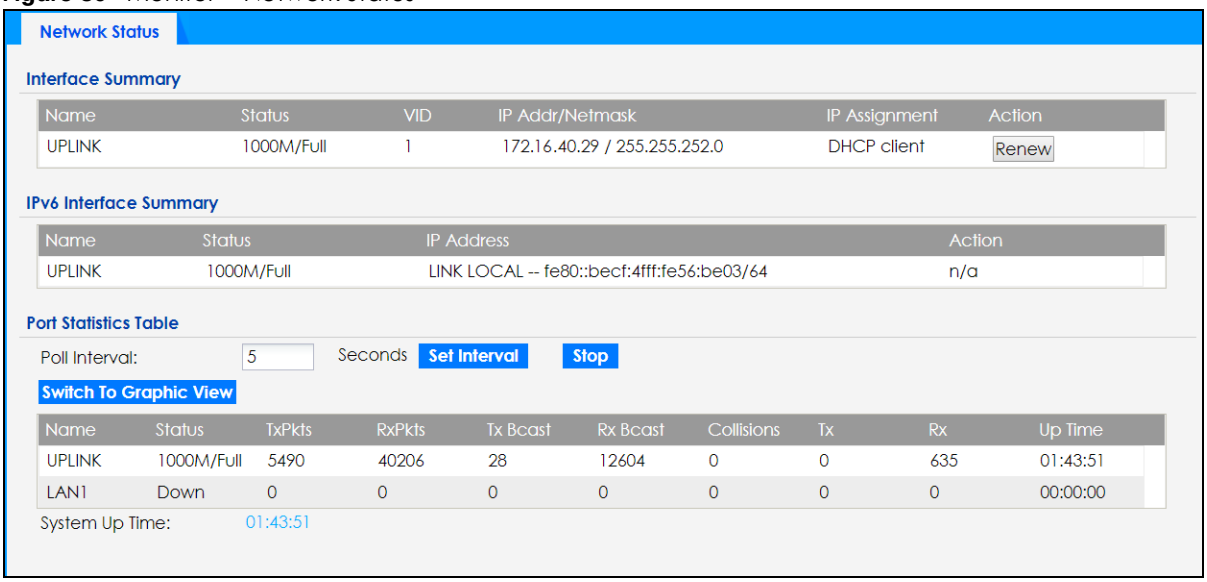
Friendly AP

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 50 Monitor > Network Status



The following table describes the labels in this screen.

Table 28 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**.

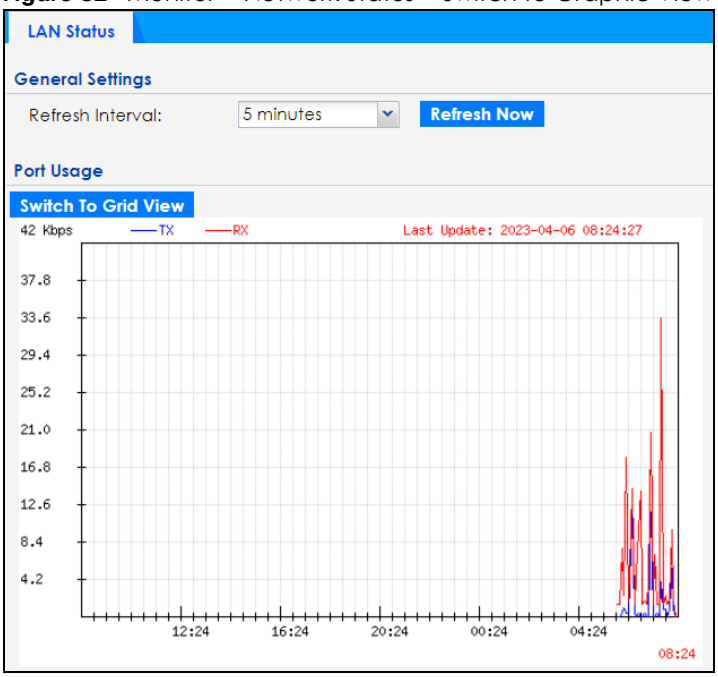
Table 28 Monitor > Network Status (continued)

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 51 Monitor > Network Status > Switch to Graphic View



The following table describes the labels in this screen.

Table 29 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	
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 52 Monitor > Wireless > AP Information > Radio List (for Zyxel Device that supports WDS)

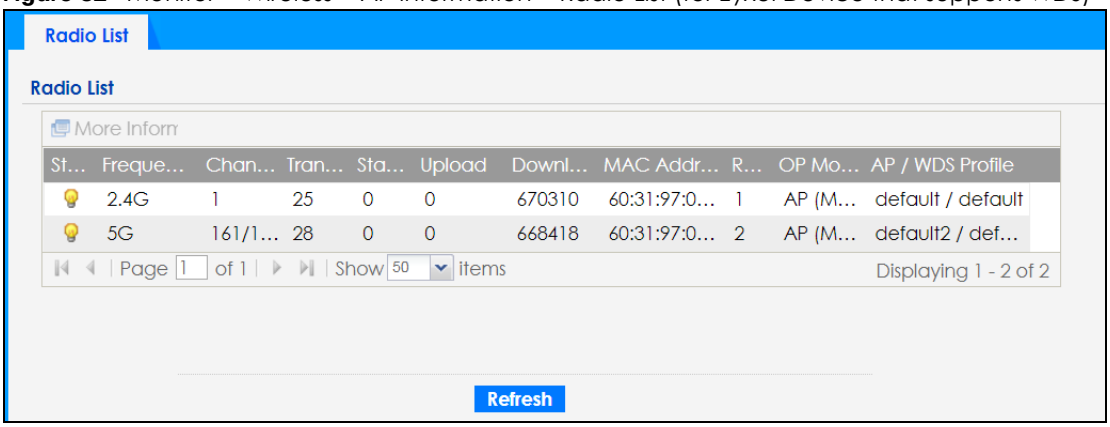
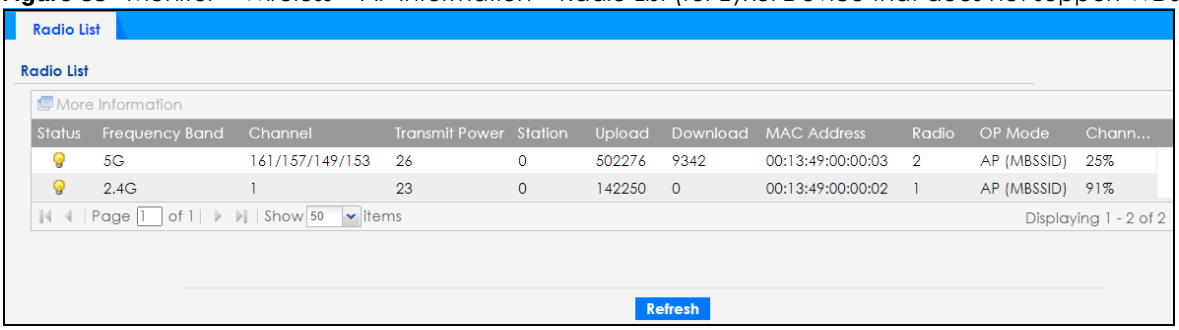


Figure 53 Monitor > Wireless > AP Information > Radio List (for Zyxel Device that does not support WDS)



The following table describes the labels in this screen.

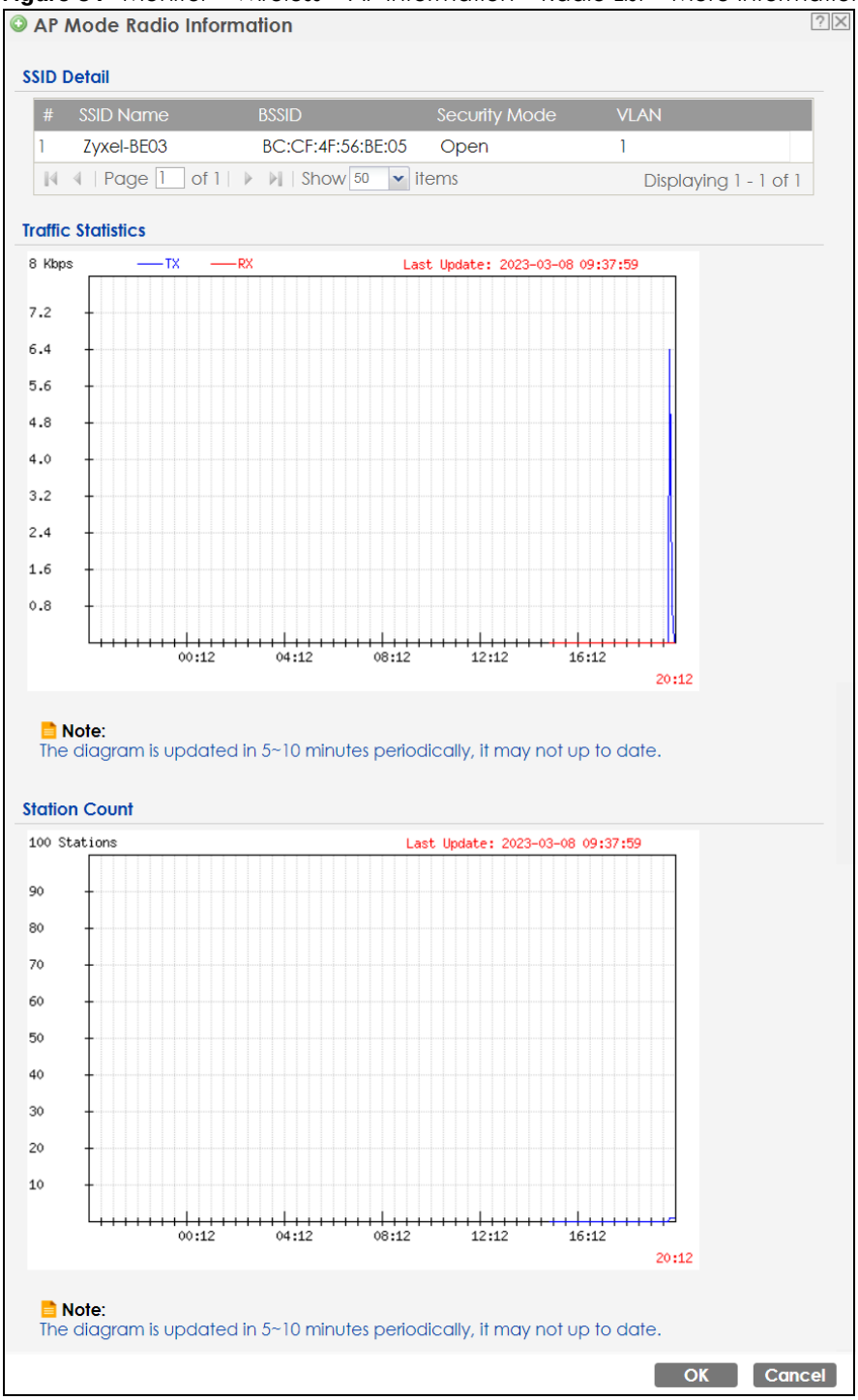
Table 30 Monitor > Wireless > AP Information > Radio List

LABEL	DESCRIPTION
More Information	Click this to view additional information about the selected radio's wireless traffic and station count. Information spans a 24 hour period.
Status	This displays whether or not the radio is enabled.
Frequency Band	This indicates the wireless frequency band currently being used by the radio.
Channel	This indicates the radio's channel ID.
Transmit Power	This displays the output power of the radio.
Station	This displays the number of WiFi clients connected to this radio on the Zyxel Device.
Upload	This displays the total number of packets received by the radio.
Download	This displays the total number of packets transmitted by the radio.
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 54 Monitor > Wireless > AP Information > Radio List > More Information



The following table describes the labels in this screen.

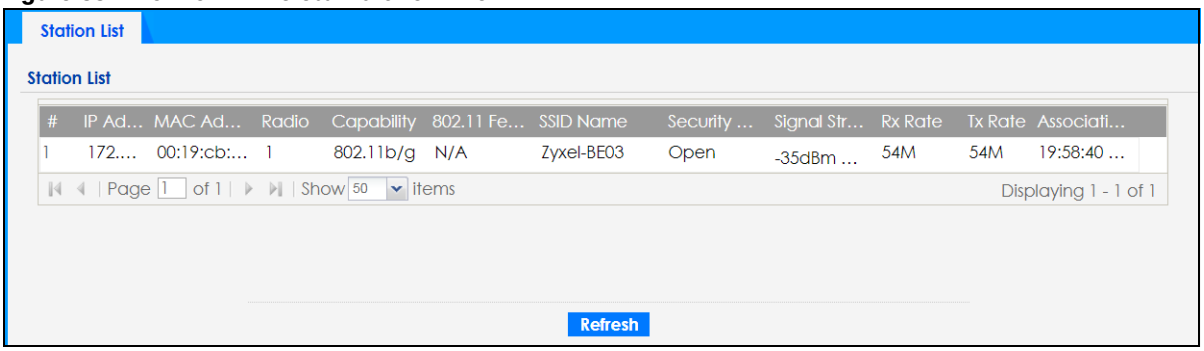
Table 31 Monitor > Wireless > AP Information > Radio List > More Information

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.
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 55 Monitor > Wireless > Station Info



The following table describes the labels in this screen.

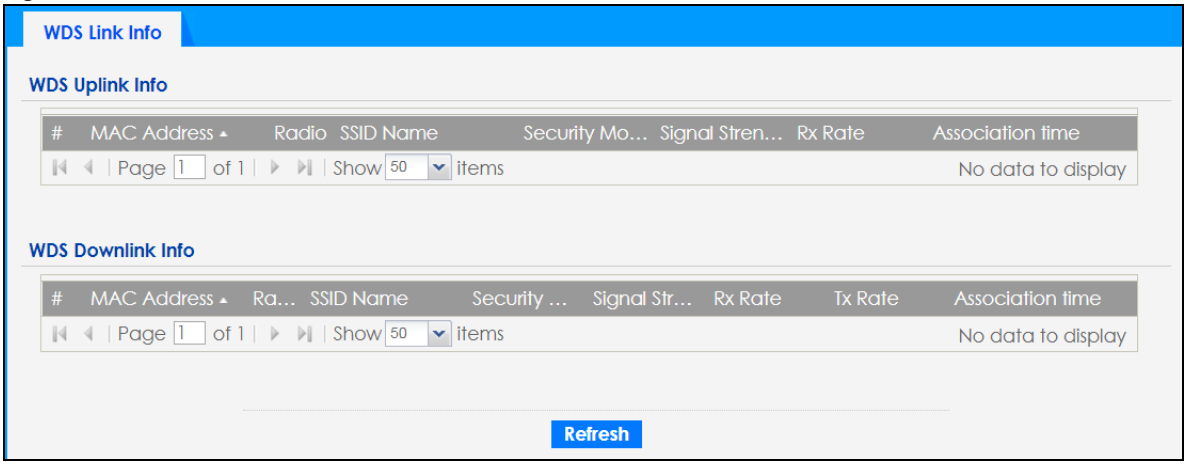
Table 32 Monitor > Wireless > Station Info

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.
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 13 to know more about WDS. Click **Monitor > Wireless > WDS Link Info** to access this screen.

Figure 56 Monitor > Wireless > WDS Link Info



The following table describes the labels in this screen.

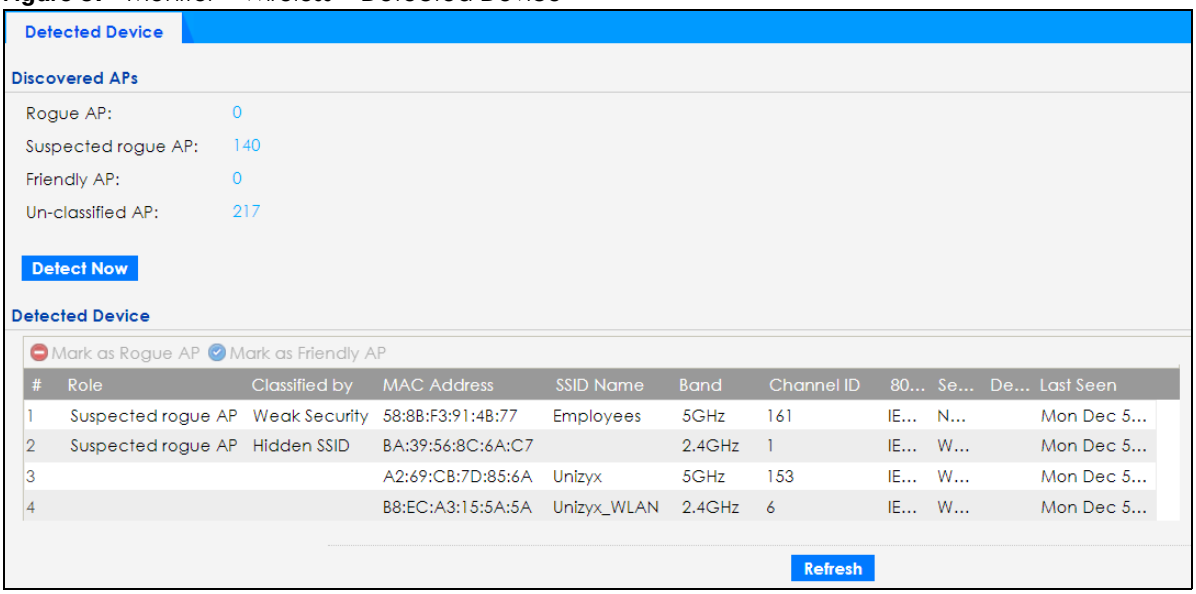
Table 33 Monitor > Wireless > WDS Link Info

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 119.

Figure 57 Monitor > Wireless > Detected Device



The following table describes the labels in this screen.

Table 34 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 119.
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 119).
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 119).
#	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 119).

Table 34 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.

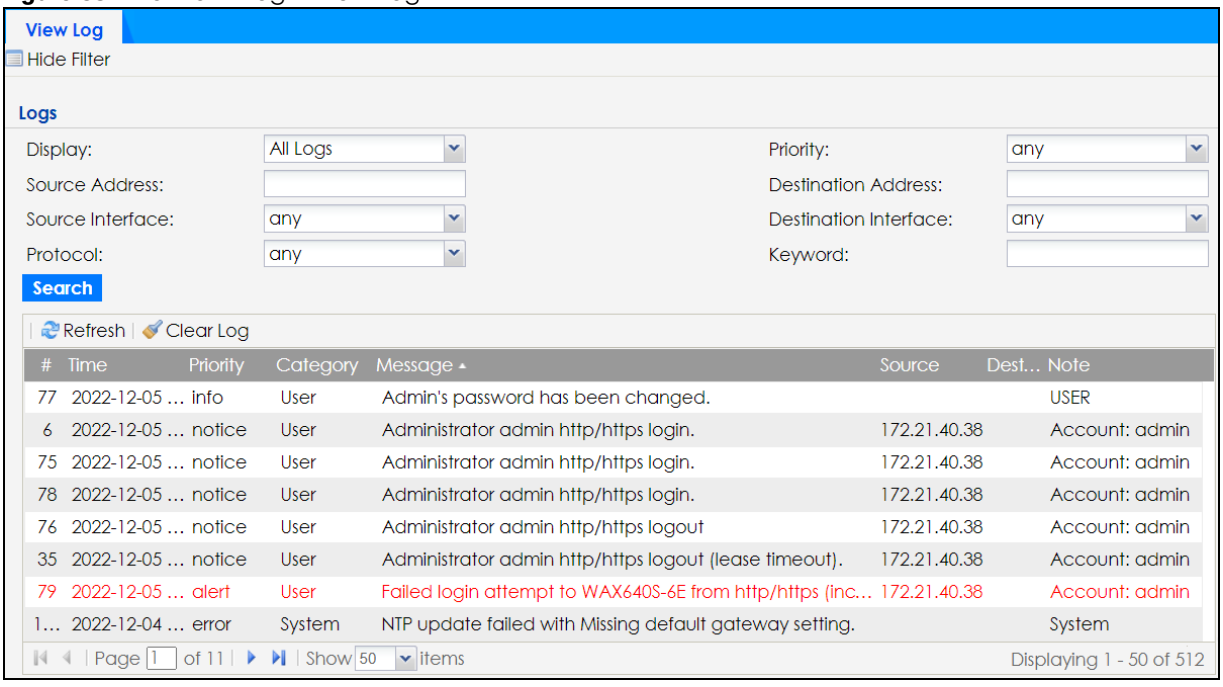
To access this screen, click **Monitor > Log**. The log is displayed in the following screen.

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 58 Monitor > Log > View Log



The following table describes the labels in this screen.

Table 35 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.
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.

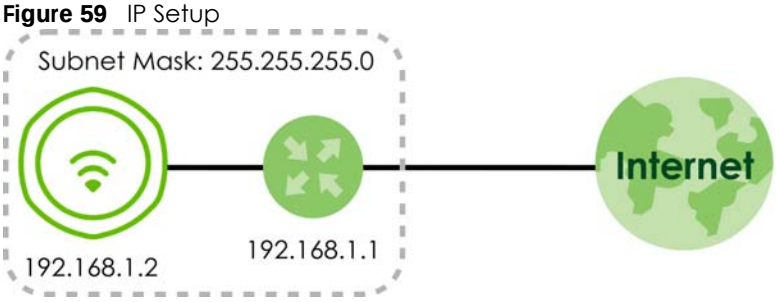
CHAPTER 10
Network

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 59 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.

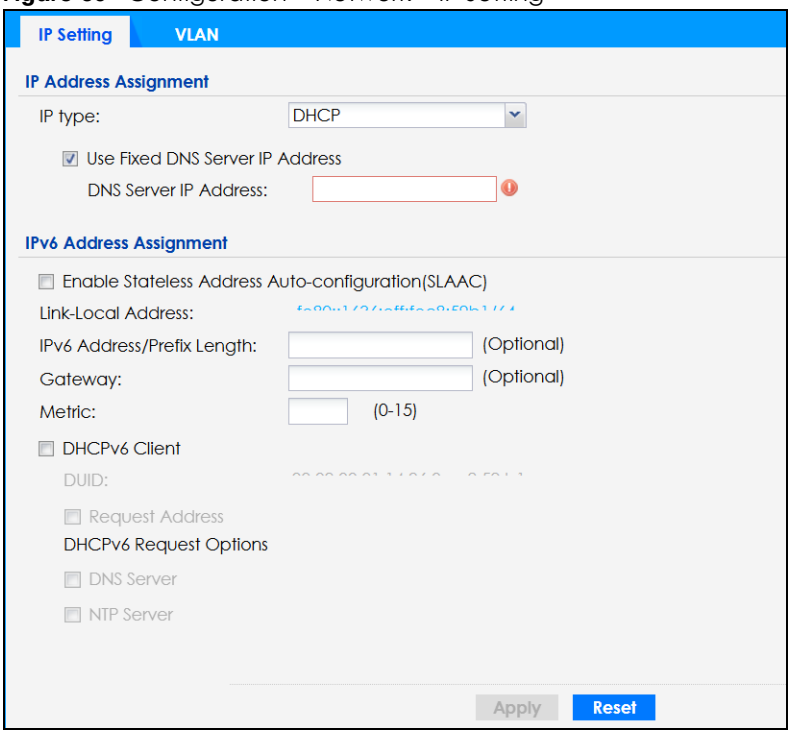
10.1.1 What You Can Do in this Chapter

- The **IP Setting** screen (Section 10.2 on page 106) configures the Zyxel Device's LAN IP address.
- The **VLAN** screen (Section 10.3 on page 108) configures the Zyxel Device's VLAN 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 60 Configuration > Network > IP Setting



Each field is described in the following table.

Table 36 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.
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.

Table 36 Configuration > Network > IP Setting (continued)

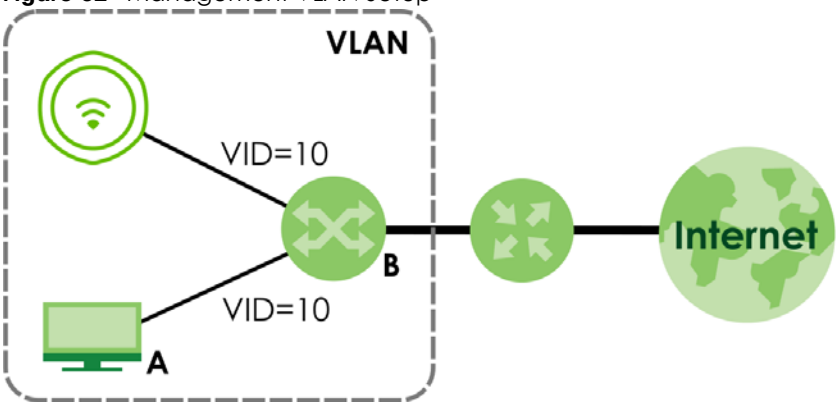
LABEL	DESCRIPTION
IPv6 Address/Prefix Length	Enter the IPv6 address and the prefix length for the LAN interface if you want to use a static IP address. This field is optional. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Gateway	Enter the IPv6 address of the default outgoing gateway using colon (:) hexadecimal notation.
Metric	Enter the priority of the gateway (if any) on the LAN interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first. Enter zero to set the metric to 1024 for IPv6.
DHCPv6 Client	Select this option to set the Zyxel Device to act as a DHCPv6 client.
DUID	This field displays the DHCP Unique IDentifier (DUID) of the Zyxel Device, which is unique and used for identification purposes when the Zyxel Device is exchanging DHCPv6 messages with others. See Appendix B on page 273 for more information.
Request Address	Select this option to get an IPv6 address from the DHCPv6 server.
DHCPv6 Request Options	Select 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 61 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.

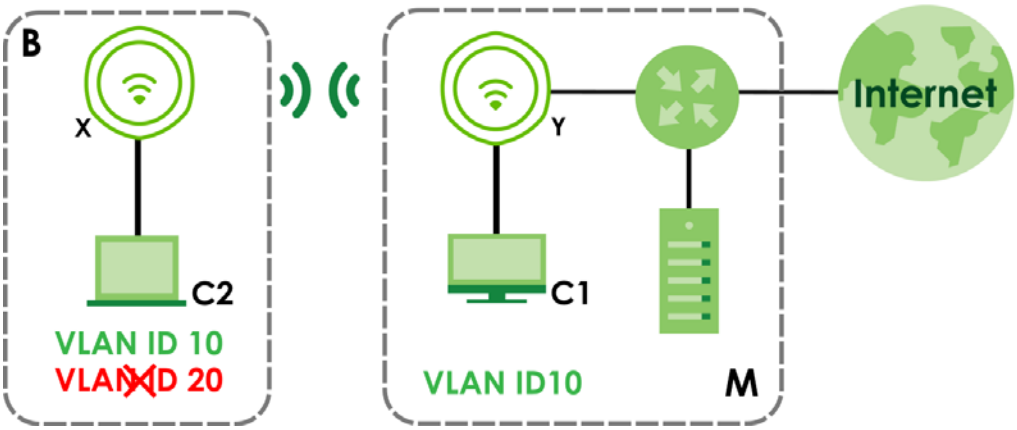
VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

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 13 for more information on the wireless bridge.

In the figure below, a client (**C2**) in the branch office (**B**) wants to connect to the main office (**M**). 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 62 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**.

Note: Not all Zyxel Devices support the wireless bridge VLAN settings; see Section 1.2 on page 11 for more information.

Figure 63 Configuration > Network > VLAN

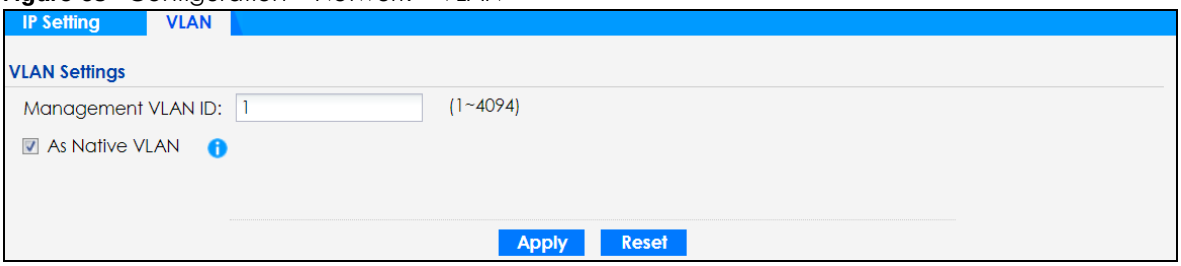
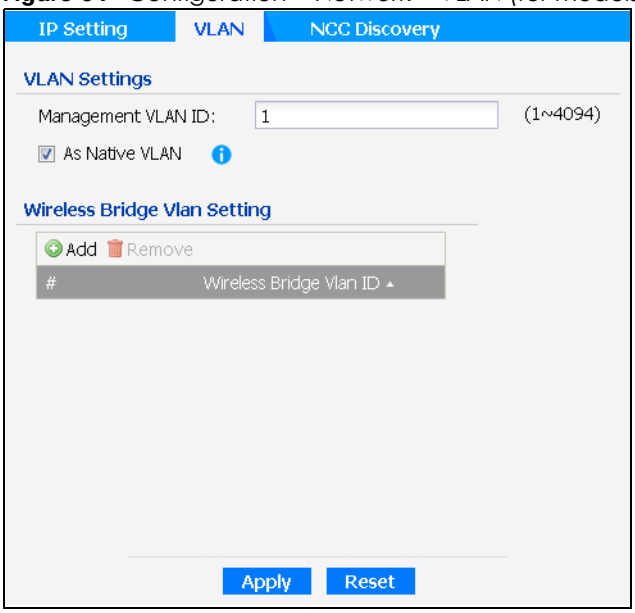


Figure 64 Configuration > Network > VLAN (for models that support Wireless Bridge)



Each field is described in the following table.

Table 37 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.
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.
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.

Table 37 Configuration > Network > VLAN (continued)

LABEL	DESCRIPTION
Wireless Bridge Vlan ID (1-4094)	Enter a VLAN ID for the wireless bridge. Duplicate VLAN IDs are not allowed. The VLAN IDs you set on your root AP should be the same as the VLAN IDs you set here. See Section 1.3 on page 13 for more information on wireless bridge.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

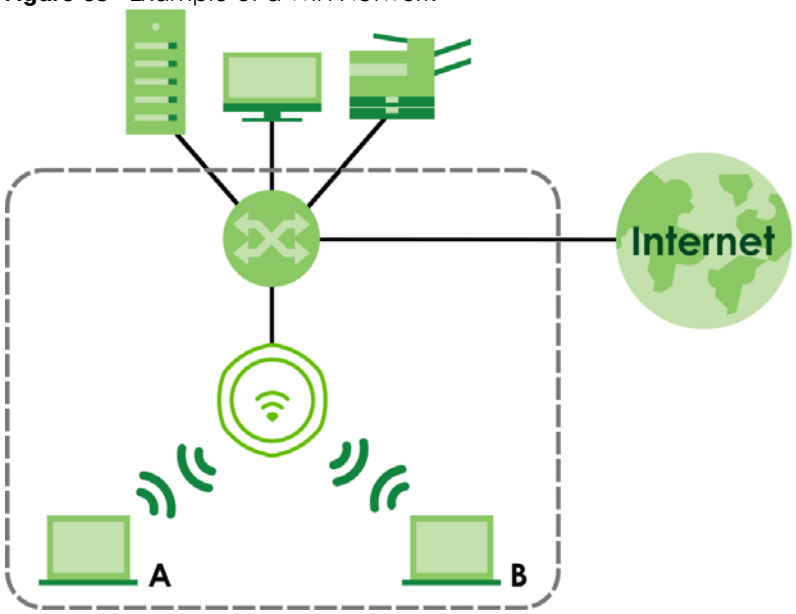
CHAPTER 11
Wireless

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 65 Example of a WiFi Network



The WiFi network is the area within the dotted line. In this WiFi network, devices **A** and **B** are called WiFi clients. The WiFi clients use the Zyxel Device to interact with other devices (such as the printer) or with the Internet.

11.1.1 What You Can Do in this Chapter

- The **AP Management** screen (Section 11.2 on page 113) allows you to manage the Zyxel Device's general WiFi settings.
- The **Rogue AP** screen (Section 11.3 on page 119) allows you to assign APs either to the rogue AP list or the friendly AP list.
- The **DCS** screen (Section 11.4 on page 123) 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 11.5 on page 123.

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.

Note: Not all Zyxel Devices support the wireless bridge VLAN settings; see Section 1.2 on page 11 for more information.

Figure 66 Configuration > Wireless > AP Management – AP Mode

Figure 67 Configuration > Wireless > AP Management – Repeater Mode

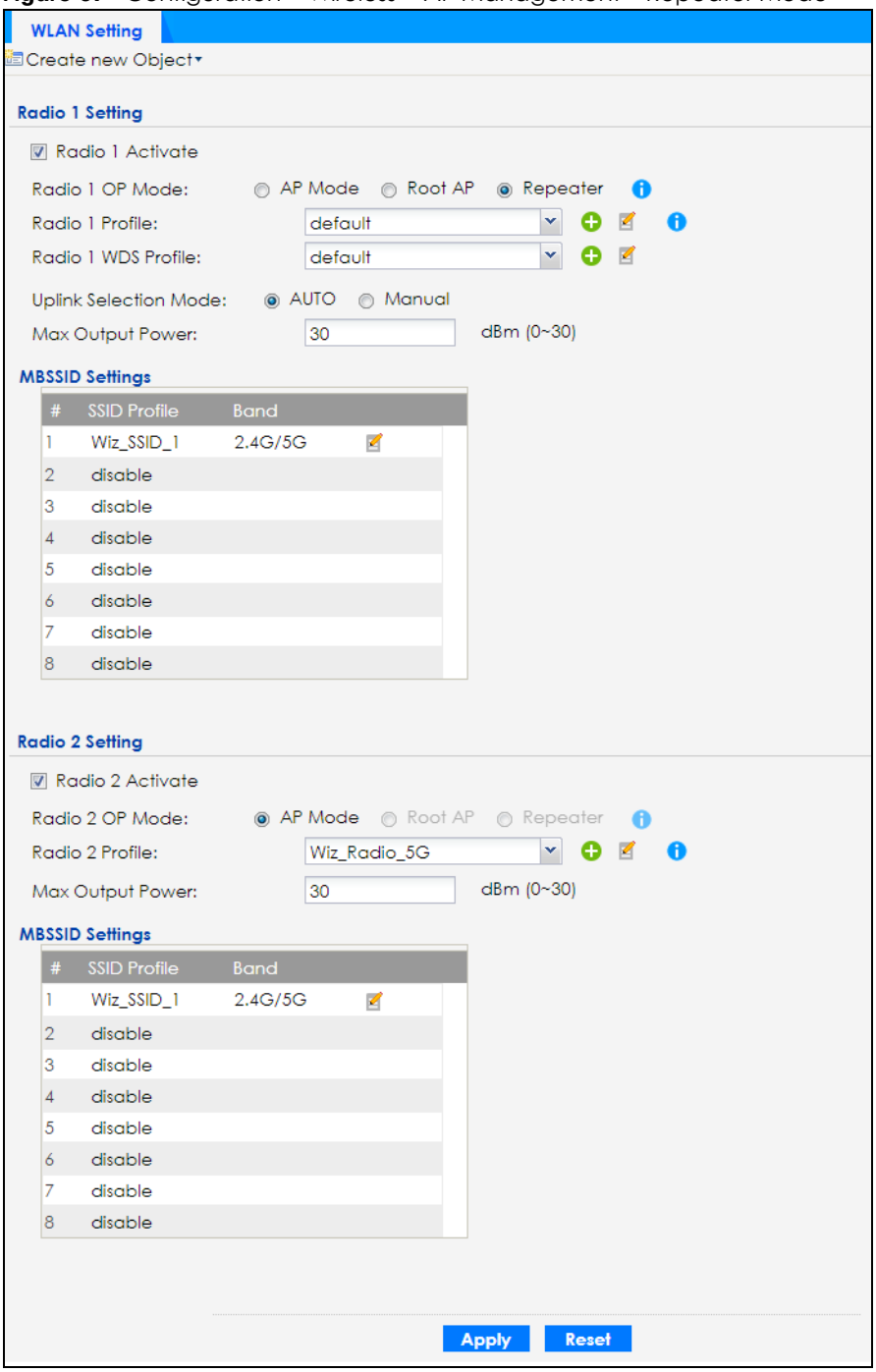
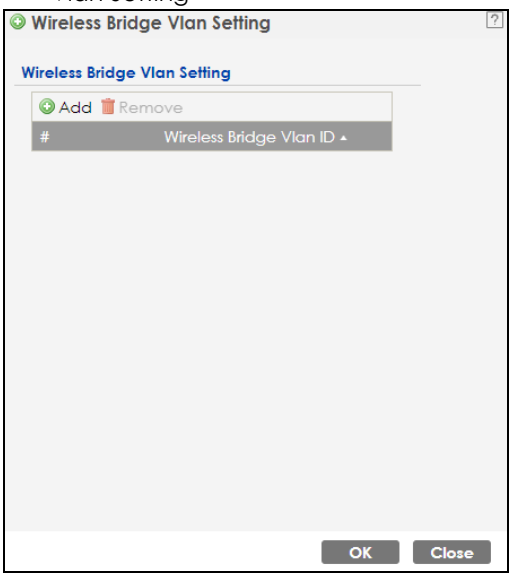


Figure 68 Configuration > Wireless > AP Management > Setup Wireless Bridge Vlan ID: Wireless Bridge Vlan Setting



Each field is described in the following table.

Table 38 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 38 Configuration > Wireless > AP Management (continued)

LABEL	DESCRIPTION
Enable WDS Wireless Bridging	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. See Section 1.3 on page 13 for more information on Wireless Distribution System (WDS).
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 13 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).
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.

Table 38 Configuration > Wireless > AP Management (continued)

LABEL	DESCRIPTION
Radio 2 Setting	
Radio 2 Activate	This displays if the Zyxel Device has a second radio. Select the checkbox to enable the Zyxel Device's second radio.
Radio 2 OP Mode	This displays if the Zyxel Device has a second radio. Select the operating mode for radio 2. **AP Mode** means the radio can receive connections from 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 Profile	This displays if the Zyxel Device has a second radio. Select the radio profile the radio uses.
Radio 2 WDS Profile	This field is available only when the radio is in **Root AP** or **Repeater** mode. Select the WDS profile the radio uses to connect to a root AP or repeater.
Enable WDS Wireless Bridging	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. See Section 1.3 on page 13 for more information on Wireless Distribution System (WDS).
Uplink Selection Mode	This field is available only when the radio is in **Repeater** mode. Select **AUTO** to have the Zyxel Device automatically use the settings in the applied WDS profile to connect to a root AP or repeater. Select **Manual** to have the Zyxel Device connect to the root AP or repeater with the MAC address specified in the **Radio 1 Uplink MAC Address** field.
Setup Wireless Bridge Vlan ID	Click this to show the **Wireless Bridge Vlan Setting** pop-up window. This link is available only when the radio is in **Root AP** or **Repeater** mode.
Wireless Bridge Vlan Setting	
Add	Click this to add an entry in the table.
Remove	Select an entry and click this to remove the selected entry.
#	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 13 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	

Table 38 Configuration > Wireless > AP Management (continued)

LABEL	DESCRIPTION
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

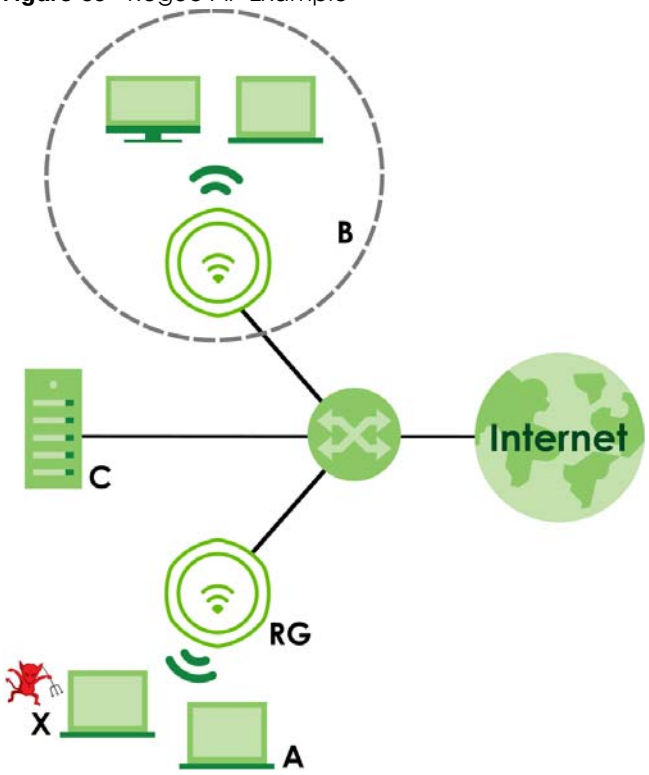
Use this screen to enable **Rogue AP Detection** and import/export a rogue or friendly AP list in a txt file. Click **Configuration > Wireless > Rogue AP** to access this screen.

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 69 Rogue AP Example



Friendly APs

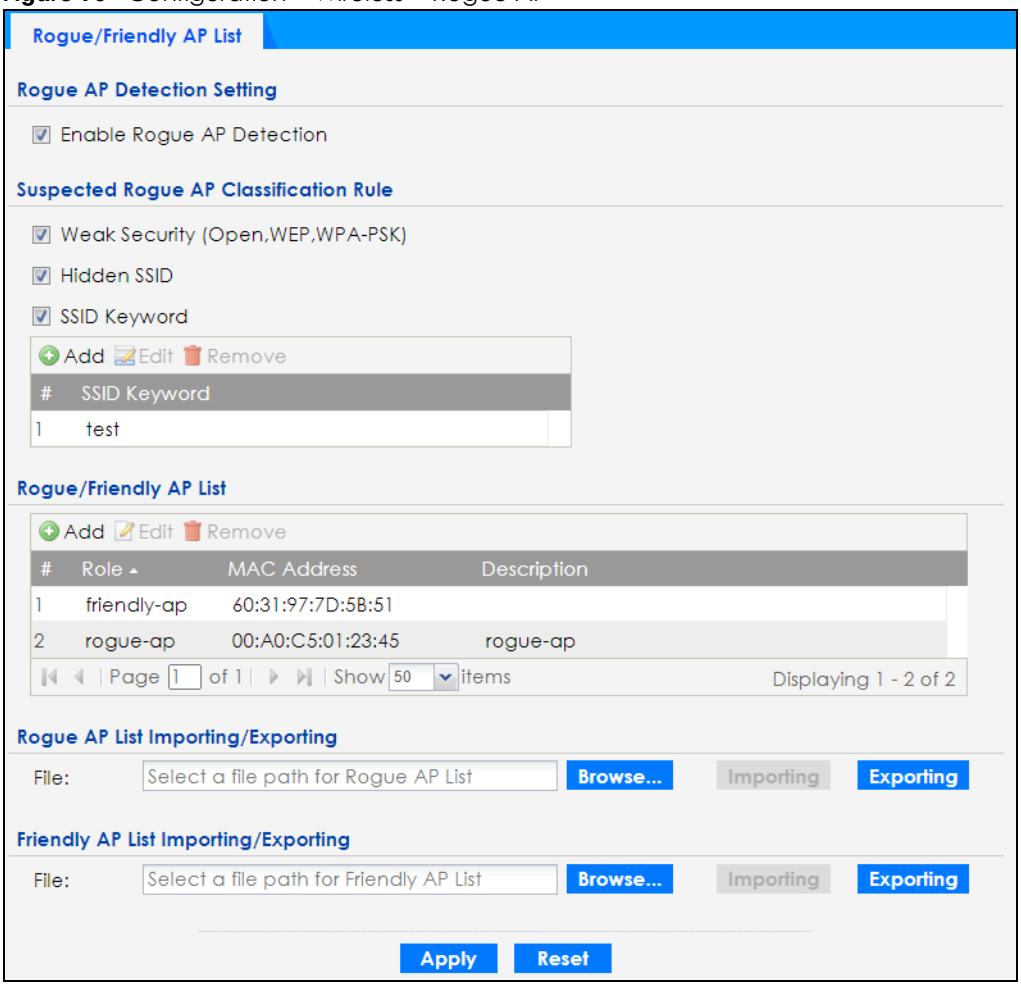
If you have more than one AP in your WiFi network, you should also configure a list of "friendly" APs. Friendly APs are wireless access points that you know are not a threat. It is recommended that you export (save) your list of friendly APs often, especially if you have a network with a large number 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 17). 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 11 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 70 Configuration > Wireless > Rogue AP



Each field is described in the following table.

Table 39 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.

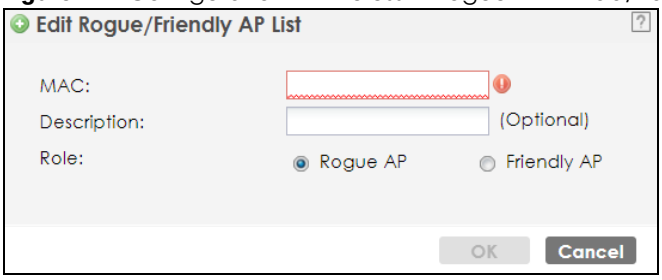
Table 39 Configuration > Wireless > Rogue AP (continued)

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 71 Configuration > Wireless > Rogue AP > Add/Edit Rogue/Friendly AP List



Each field is described in the following table.

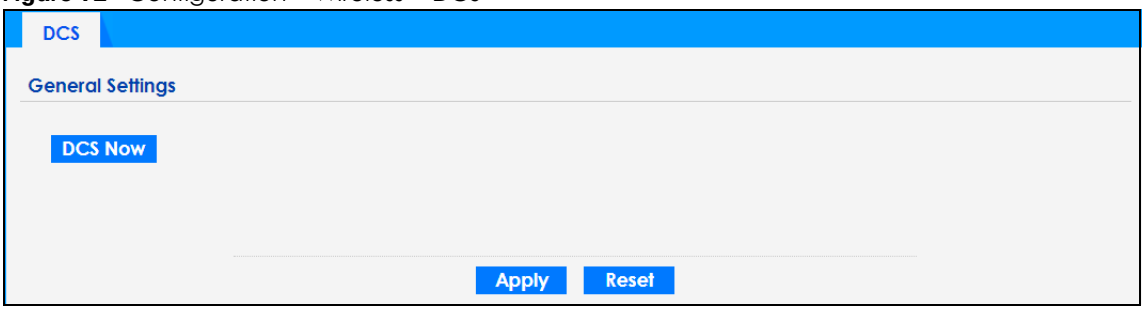
Table 40 Configuration > Wireless > Rogue AP > Add/Edit Rogue/Friendly AP List

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 DCS

Use this screen to configure dynamic radio channel selection (see Dynamic Channel Selection (DCS) on page 113).Click **Configuration > Wireless > DCS** to access this screen.

Figure 72 Configuration > Wireless > DCS



Each field is described in the following table.

Table 41 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.

11.5 Technical Reference

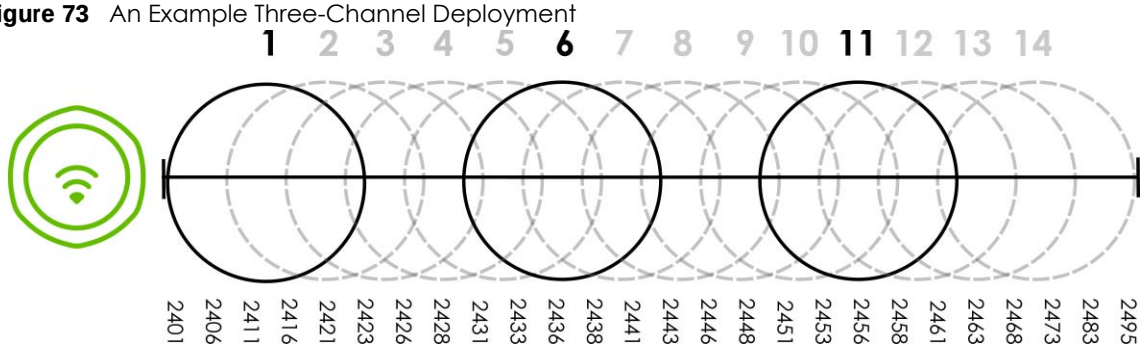
The following section contains additional technical information about the features described in this chapter.

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.

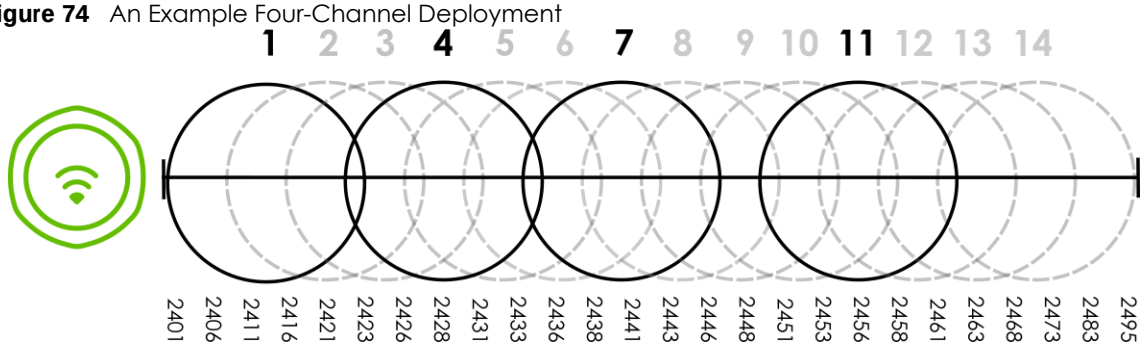
In the 2.4 GHz spectrum, each channel from 1 to 13 is broken up into discrete 22 MHz segments that are spaced 5 MHz apart. Channel 1 is centered on 2.412 GHz while channel 13 is centered on 2.472 GHz.

Figure 73 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.

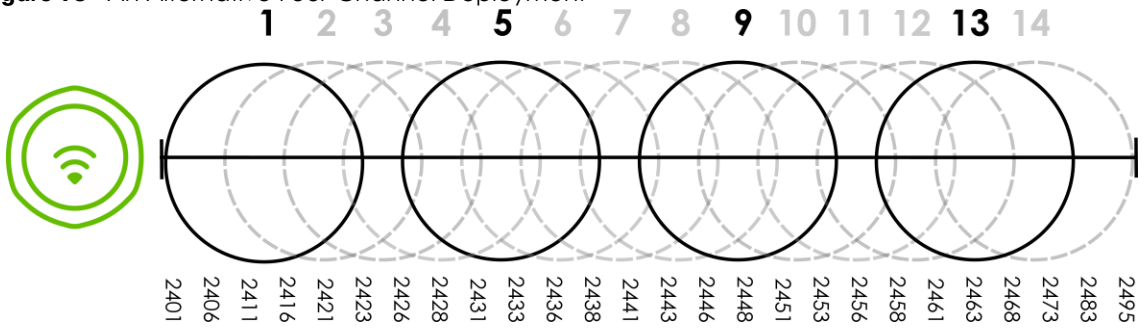
Figure 74 An Example Four-Channel Deployment



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 75 An Alternative Four-Channel Deployment



CHAPTER 12
User

12.1 Overview

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

12.1.1 What You Can Do in this Chapter

- The **User** screen (see Section 12.2 on page 126) provides a summary of all user accounts.
- The **Setting** screen (see Section 12.3 on page 128) controls default settings, login settings, lockout settings, and other user settings for the Zyxel Device.

12.1.2 What You Need To Know

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

User Account

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

User Types

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

Table 42 Types of User Accounts

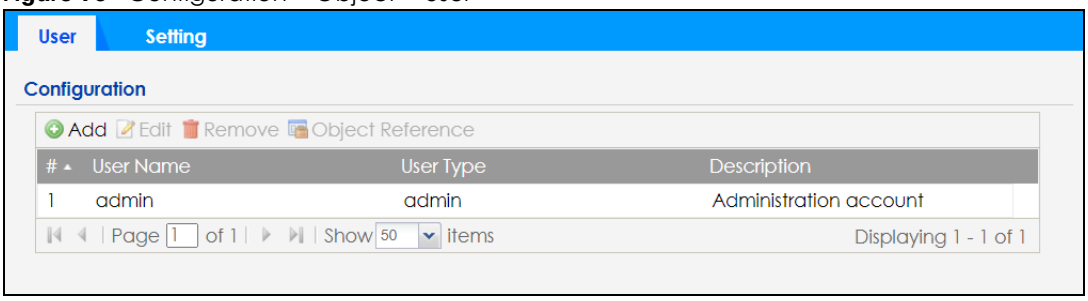
TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
admin	Change Zyxel Device configuration (web, CLI)	WWW, SSH, FTP
limited-admin	Look at Zyxel Device configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, SSH
Access Users		
user	Used for the embedded RADIUS server user access Browse user-mode commands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

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

12.2 User Summary

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

Figure 76 Configuration > Object > User



The following table describes the labels in this screen.

Table 43 Configuration > Object > User

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

12.2.1 Add/Edit User

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

12.2.1.1 Rules for User Names

Enter a user name from 1 to 31 characters.

The user name can only contain the following characters:

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

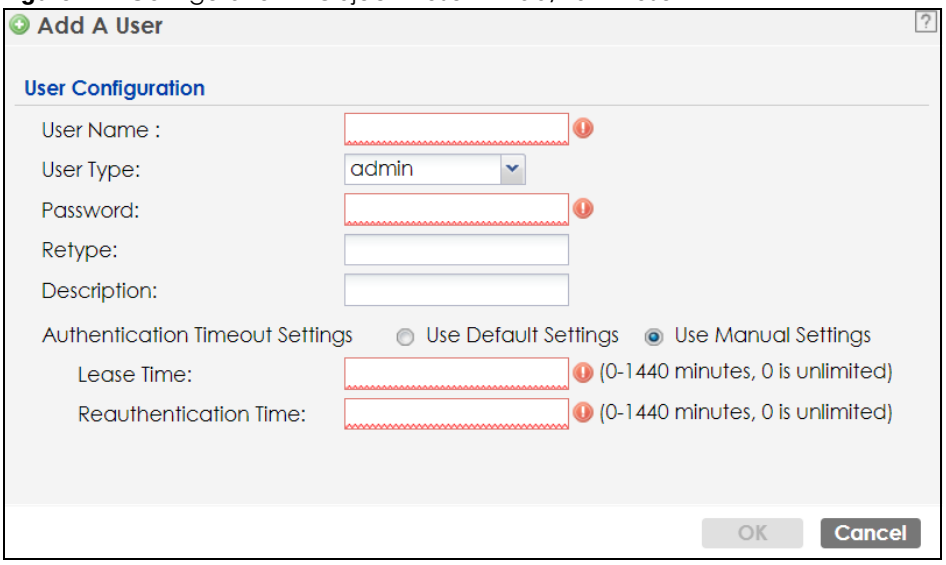
The first character must be alphabetical (A-Z a-z), an underscore (_), or a dash (-). Other limitations on user names are:

- User names are case-sensitive. If you enter a user 'bob' but use 'BOB' when connecting 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 77 Configuration > Object > User > Add/Edit A User



The following table describes the labels in this screen.

Table 44 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 user access
Password	Enter the password of this user account. It can consist of 4 to 63 printable characters. Spaces are not allowed.
Retype	Re-enter the password to make sure you have entered it correctly.

Table 44 Configuration > User > User > Add/Edit a User (continued)

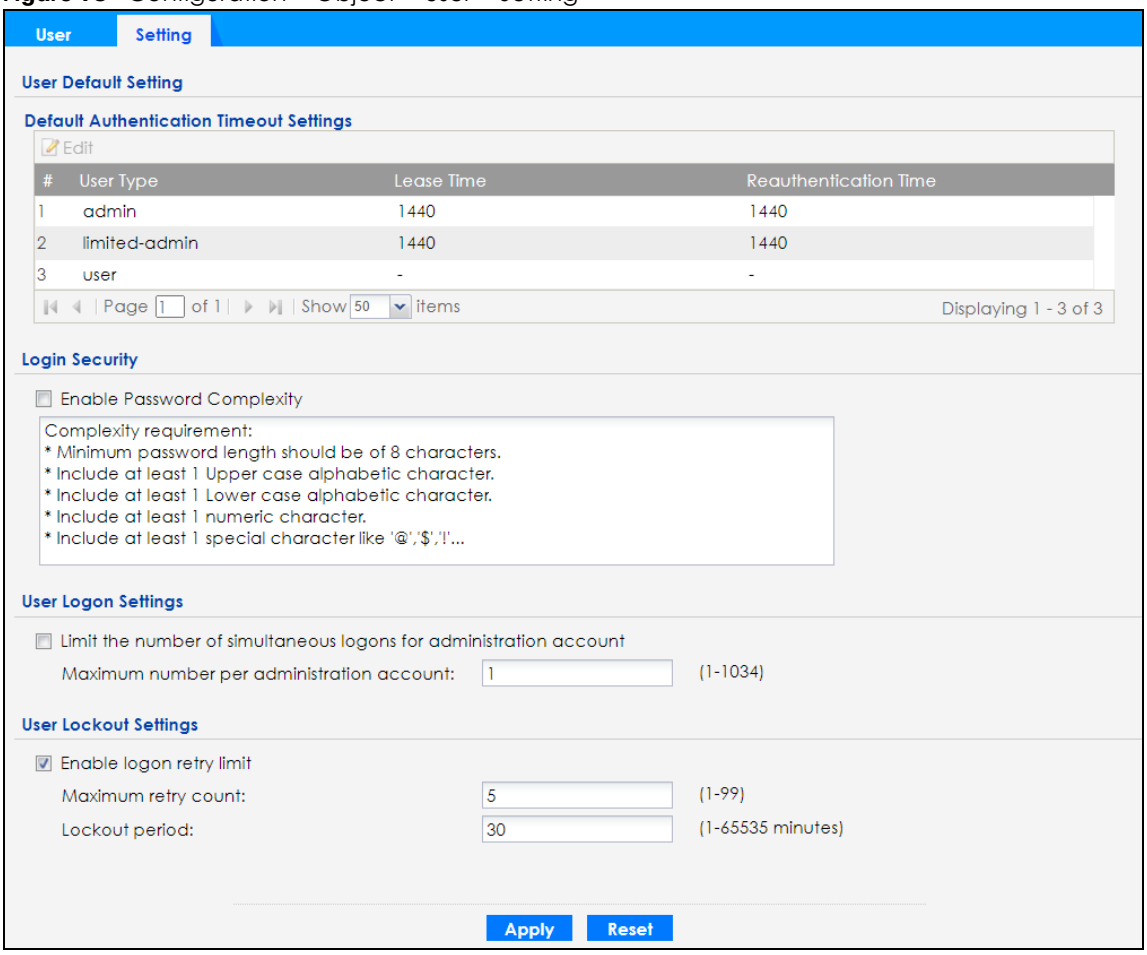
LABEL	DESCRIPTION
Description	Enter the description of each user, if any. You can use up to 60 printable ASCII characters. Default descriptions are provided.
Authentication Timeout Settings	This field is not available if the user type is **user**. If you want to set authentication timeout to a value 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.

12.3 Setting

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

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

Figure 78 Configuration > Object > User > Setting



The following table describes the labels in this screen.

Table 45 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 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 45 Configuration > Object > User > Setting (continued)

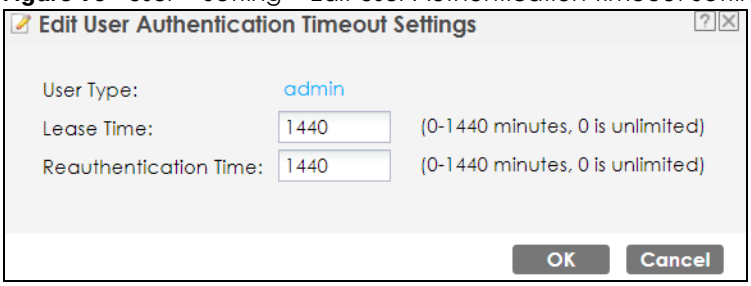
LABEL	DESCRIPTION
Reauthentication Time	This is the default reauthentication time in minutes for each type of user account. It defines the number of minutes the user can be logged into the Zyxel Device in one session before having to log in again. Unlike **Lease Time**, the user has no opportunity to 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.

12.3.1 Edit User Authentication Timeout Settings

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

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

Figure 79 User > Setting > Edit User Authentication Timeout Settings



The following table describes the labels in this screen.

Table 46 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 13
AP Profile

13.1 Overview

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

13.1.1 What You Can Do in this Chapter

- The **Radio** screen (Section 13.2 on page 135) creates radio configurations that can be used by the APs.
- The **SSID** screen (Section 13.3 on page 142) configures three different types of profiles for your networked APs.

13.1.2 What You Need To Know

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

Wireless Profiles

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

- **Radio** - This profile type defines the properties of an AP's radio transmitter. You can have a maximum of 64 radio profiles on the Zyxel Device.
- **SSID** - This profile type defines the properties of a single 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

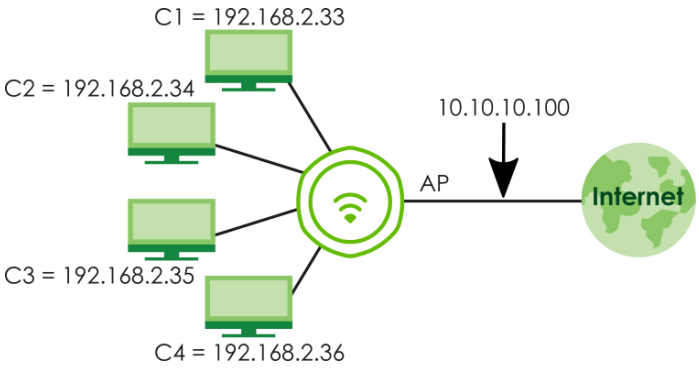
The SSID (Service Set IDentifier) is the name that identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. In other words, it is the name of the WiFi network that clients use to connect to it.

Init SSID

Init (initial) SSID (Service Set IDentifier) is the default WiFi network name of the Zyxel Device. The name consists of **Zyxel-xxxx**, where xxxx are the last four characters of the MAC address. You can find the MAC address on the Zyxel Device label.

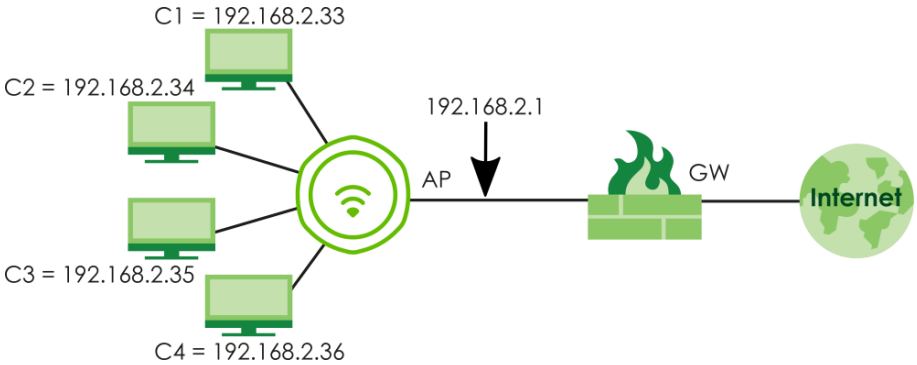
SSID Forwarding Mode - NAT

NAT (Network Address Translation) mode is the default **Forwarding mode** of the Zyxel Device. This allows the SSID to be visible to your WiFi-enabled computer (**C**) and connect to the Zyxel Device (**AP**). Use this mode to log into the Web Configurator to configure secure SSID on the Zyxel Device (**AP**). Use this mode if you do not have a DHCP server router in your network (for example, router or gateway).



SSID Forwarding Mode - Local Bridge

You can set **Local bridge** as the **Forwarding mode** of the Zyxel Device (**Configuration** > **Object** > **AP Profile** > **SSID** > **SSID List** > **Add/Edit SSID Profile**). This allows the connected WiFi client devices (**C1** - **C4**) on the Zyxel Device (**AP**) to get individual IP address from the Gateway (**GW**) directly. Use this mode if you already have a gateway in your network.



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

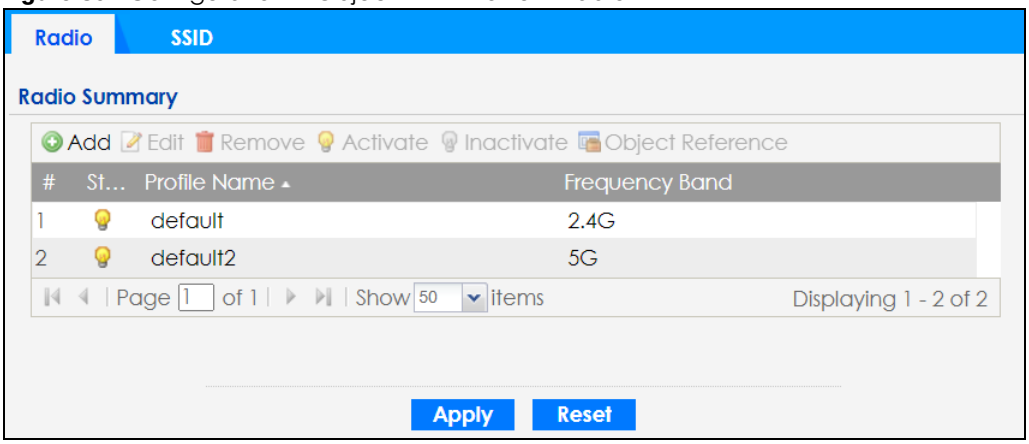
TWT (Target Wake Time) – The AP negotiates with client devices so client devices only wake up and communicate with the AP in specific periods. This conserves the battery life of client devices.

13.2 Radio

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

Note: You can have a maximum of 64 radio profiles on the Zyxel Device.

Figure 80 Configuration > Object > AP Profile > Radio



The following table describes the labels in this screen.

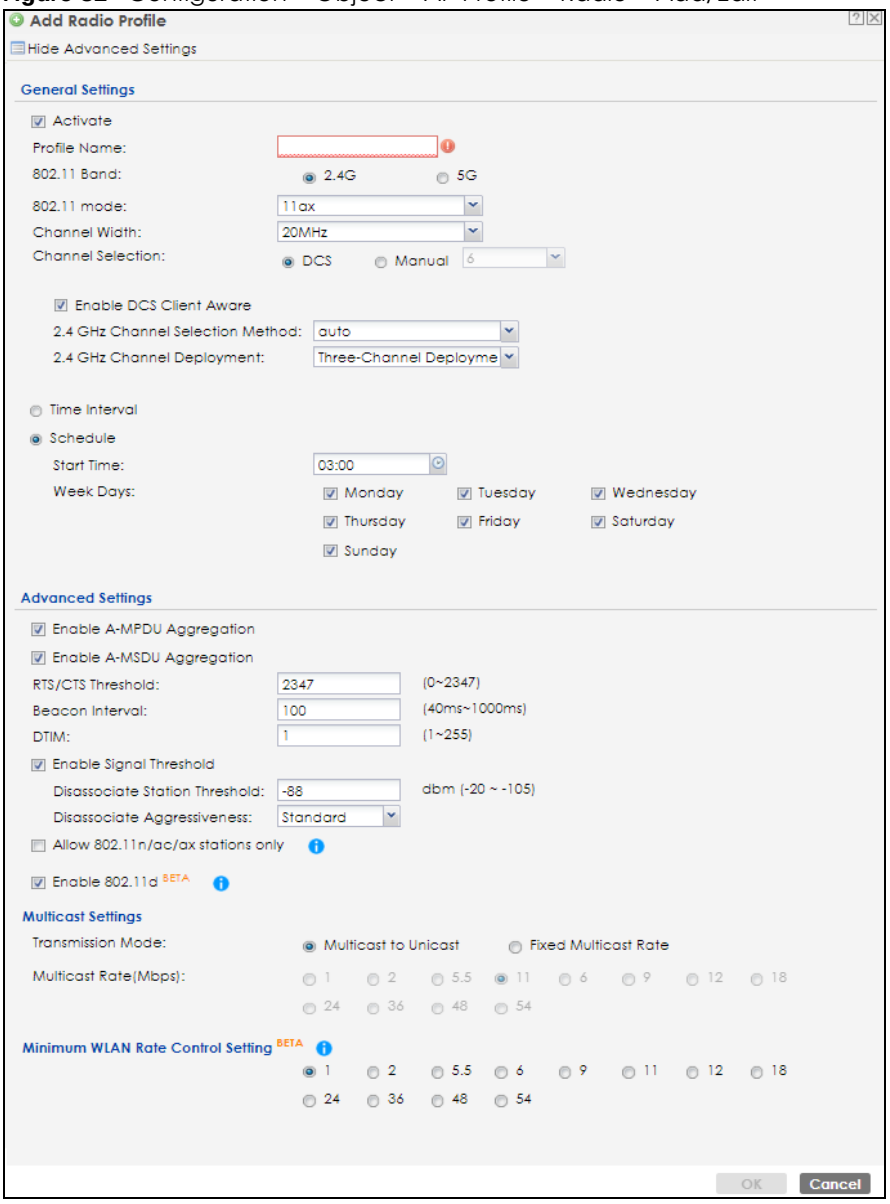
Table 47 Configuration > Object > AP Profile > Radio

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.

13.2.1 Add/Edit Radio Profile

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

Figure 81 Configuration > Object > AP Profile > Radio > Add/Edit



The following table describes the labels in this screen.

Table 48 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 would use the 2.4 GHz or 5 GHz band.

Table 48 Configuration > Object > AP Profile > Radio > Add/Edit (continued)

LABEL	DESCRIPTION
802.11 Mode	Select how to let wireless clients connect to the AP. If **802.11 Band** is set to **2.4G**: • **11b/g**: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the Zyxel Device. The Zyxel Device adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices. • **11n**: allows IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the Zyxel Device. • **11ax**: allows IEEE802.11b, IEEE802.11g, IEEE802.11n, and IEEE802.11ax compliant WLAN devices to associate with the Zyxel Device. If the WLAN device isn't compatible with 802.11ax, the Zyxel Device will communicate with the WLAN device using 802.11n, and so on. If **802.11 Band** is set to **5G**: • **11a**: allows only IEEE 802.11a compliant WLAN devices to associate with the Zyxel Device. • **11n**: allows both IEEE802.11n and IEEE802.11a compliant WLAN devices to associate with the Zyxel Device. • **11ac**: allows IEEE802.11n, IEEE802.11a, and IEEE802.11ac compliant WLAN devices to associate with the Zyxel Device. If the WLAN device isn't compatible with 802.11ac, the Zyxel Device will communicate with the WLAN device using 802.11n, and so on. • **11ax**: allows IEEE802.11n, IEEE802.11a, IEEE802.11ac, and IEEE802.11ax compliant WLAN devices to associate with the Zyxel Device. If the WLAN device isn't compatible with 802.11ax, the Zyxel Device will communicate with the WLAN device using 802.11ac, and so on.
Channel Width	Select the channel bandwidth you want to use for your wireless network. Select **20 MHz** if you want to lessen radio interference with other wireless devices in your neighborhood. Select **40 MHz** to allow the Zyxel Device to choose the channel bandwidth (20 or 40 MHz) that has least interference. Select **80 MHz** to allow the Zyxel Device to choose the channel bandwidth (20 or 40 or 80) that has least interference. This option is available only when you set **802.11 Band** to **5G**, and select **11ac** or **11ax** in the **802.11 Mode** field. Select **160 MHz** to allow the Zyxel Device to choose the channel bandwidth (20 or 40 or 80 or 160) that has least interference. This option is available only when you set **802.11 Band** to **5G**, and select **11ax** in the **802.11 Mode** field. Note: If the environment has poor signal-to-noise ratio (SNR), the Zyxel Device will switch to a lower bandwidth.
Channel Selection	This is the radio channel which the signal will use for broadcasting by this radio profile. • **DCS**: Choose Dynamic Channel Selection to have the Zyxel Device choose a radio channel that has least interference. • **Manual**: Choose from the available radio channels in the list. If your Zyxel Device is outdoor type, be sure to choose non-indoors channels.
Enable DCS Client Aware	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.

Table 48 Configuration > Object > AP Profile > Radio > Add/Edit (continued)

LABEL	DESCRIPTION
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.
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.
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 48 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 48 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	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 48 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, in Mbps. At the time of write, allowed values are: 1, 2, 5. 5, 6, 9, 11, 12, 18, 24, 36, 48, 54. Sets the minimum data rate that 5 GHz WiFi clients can connect at, in Mbps. At the time of write, allowed values are: 6, 9, 12, 18, 24, 36, 48, 54. 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.

13.3 SSID

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

13.3.1 SSID List

This screen allows you to create and manage SSID configurations that can be used by the APs. An SSID, or Service Set IDentifier, is basically the name of the 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 82 Configuration > Object > AP Profile > SSID > SSID List (Default)

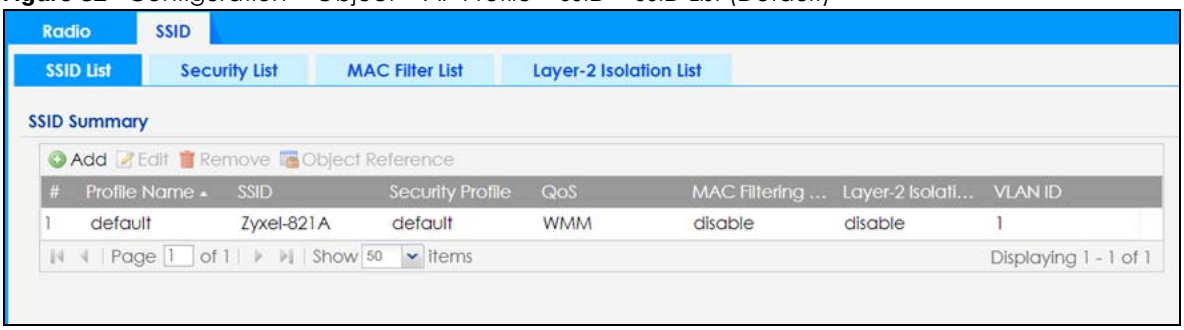
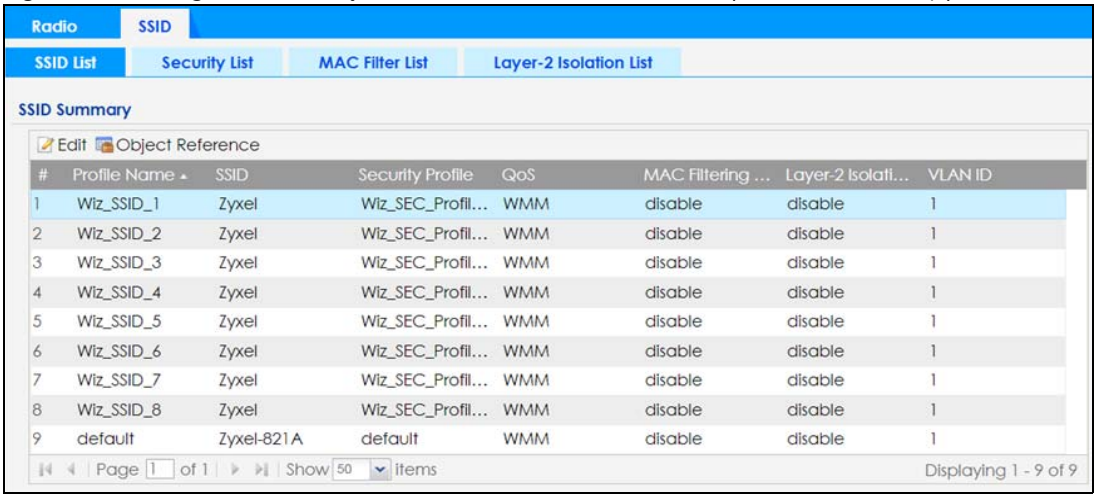


Figure 83 Configuration > Object > AP Profile > SSID > SSID List (After wizard setup)



The following table describes the labels in this screen.

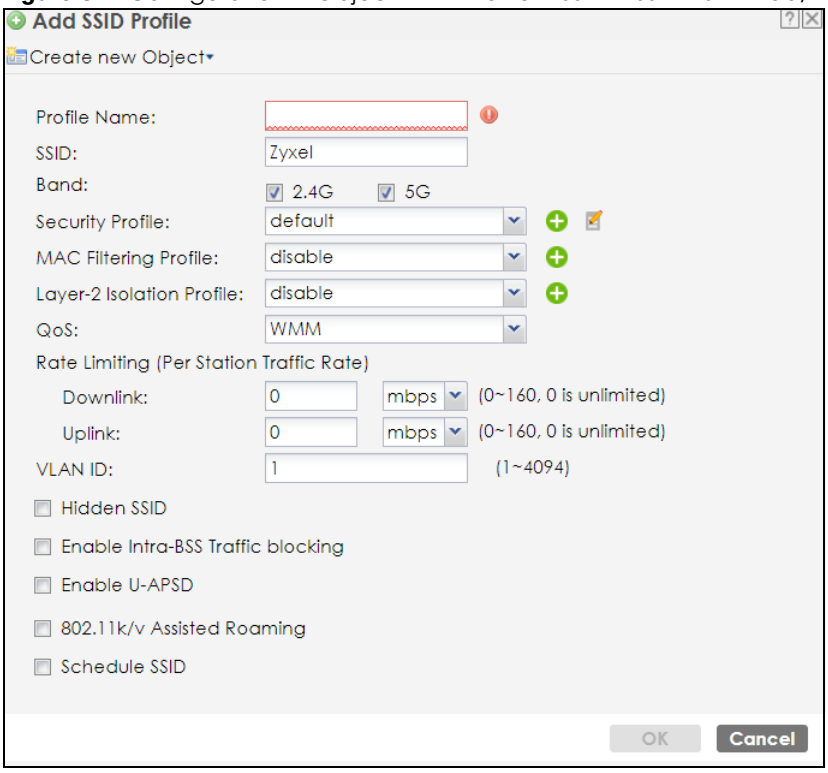
Table 49 Configuration > Object > AP Profile > SSID > SSID List

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.

13.3.2 Add/Edit SSID Profile

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

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



The following table describes the labels in this screen.

Table 50 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.
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.
Forwarding Mode	Select **Local bridge** if you only want to access the Internet. Network traffic from clients connected to the Zyxel Device is sent directly to the network through the local gateway. Select **NAT mode** to have the Zyxel Device create a DHCP subnet with its own NAT for the SSID. This simplifies WiFi network management, as you do not need to configure a separate DHCP server.

Table 50 Configuration > Object > AP Profile > SSID > SSID List > Add/Edit SSID Profile (continued)

LABEL	DESCRIPTION
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. This field does not display when you select **NAT** in **Forwarding Mode** field.
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.
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).

Table 50 Configuration > Object > AP Profile > SSID > SSID List > Add/Edit SSID Profile (continued)

LABEL	DESCRIPTION
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.
802.11k/v Assisted Roaming	Select this option to enable IEEE 802.11k/v assisted roaming on the Zyxel Device. When the connected clients request 802.11k neighbor lists, the Zyxel Device will response with a list of neighbor APs that can be candidates for roaming.
Schedule SSID	Select this option and set whether the SSID is enabled or disabled on each day of the week. You also need to select the hour and minute (in 24-hour format) to specify the time period of each day during which the SSID is enabled/enabled.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

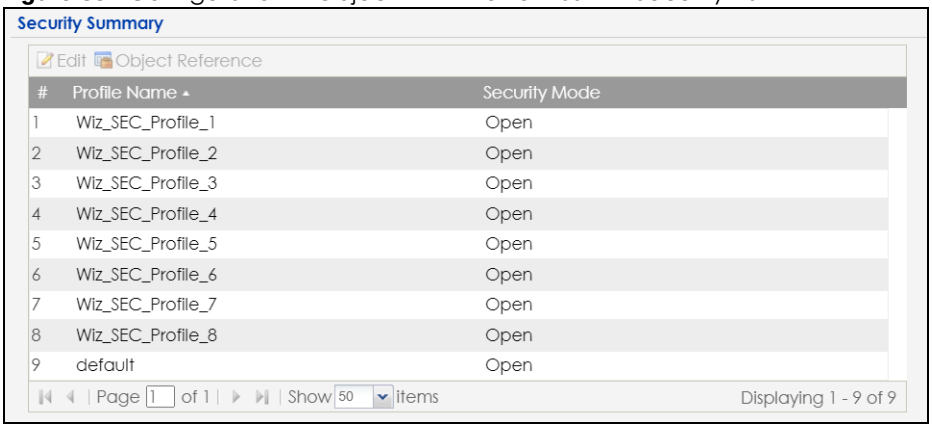
13.4 Security List

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

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

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

Figure 85 Configuration > Object > AP Profile > SSID > Security List



The following table describes the labels in this screen.

Table 51 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.

Table 51 Configuration > Object > AP Profile > SSID > Security List (continued)

LABEL	DESCRIPTION
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).

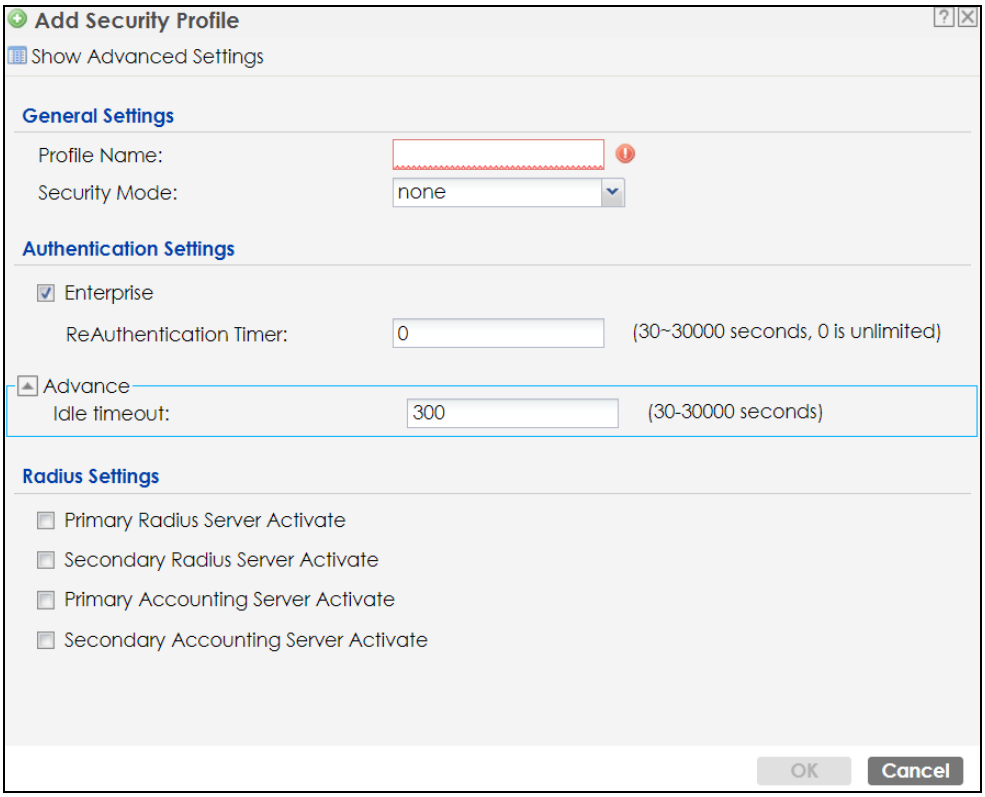
13.4.1 Add/Edit Security Profile

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

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

Note: Not all Zyxel Devices support the enterprise authentication settings and radius settings; see Section 1.2 on page 11 for more information.

Figure 86 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: none



The following table describes the labels in this screen.

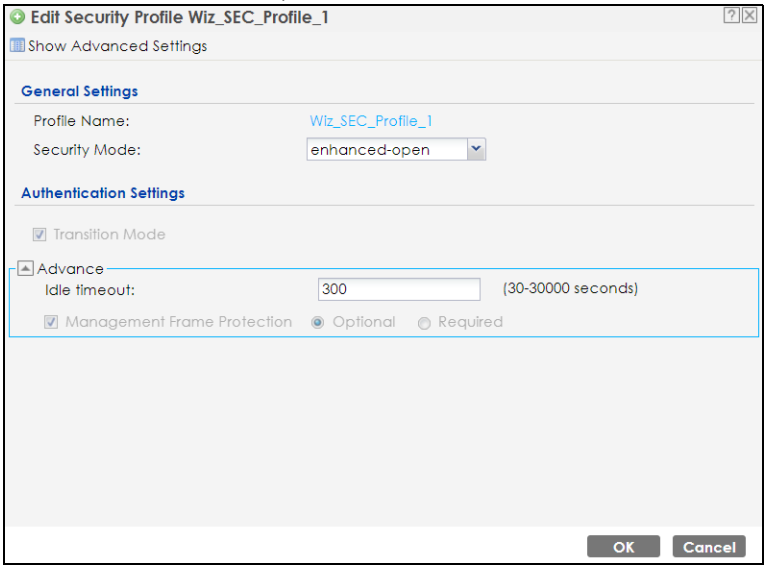
Table 52 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile > Security Mode: none

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.
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	

Table 52 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile > Security Mode: none (continued)

LABEL	DESCRIPTION
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 87 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile > Security Mode: enhanced-open



The following table describes the labels in this screen.

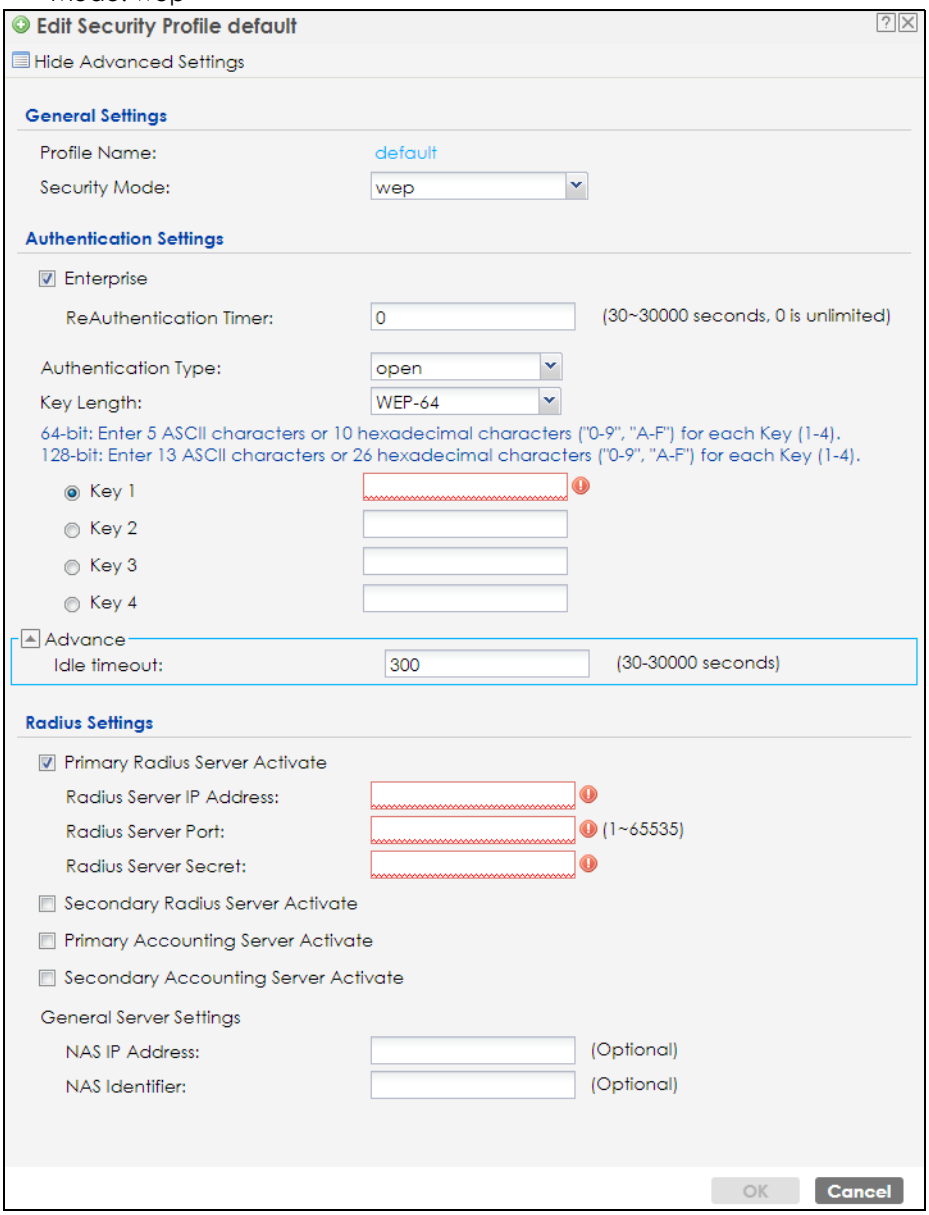
Table 53 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: enhanced-open

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.

Table 53 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: enhanced-open (continued)

LABEL	DESCRIPTION
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.
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 88 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wep



The following table describes the labels in this screen.

Table 54 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.

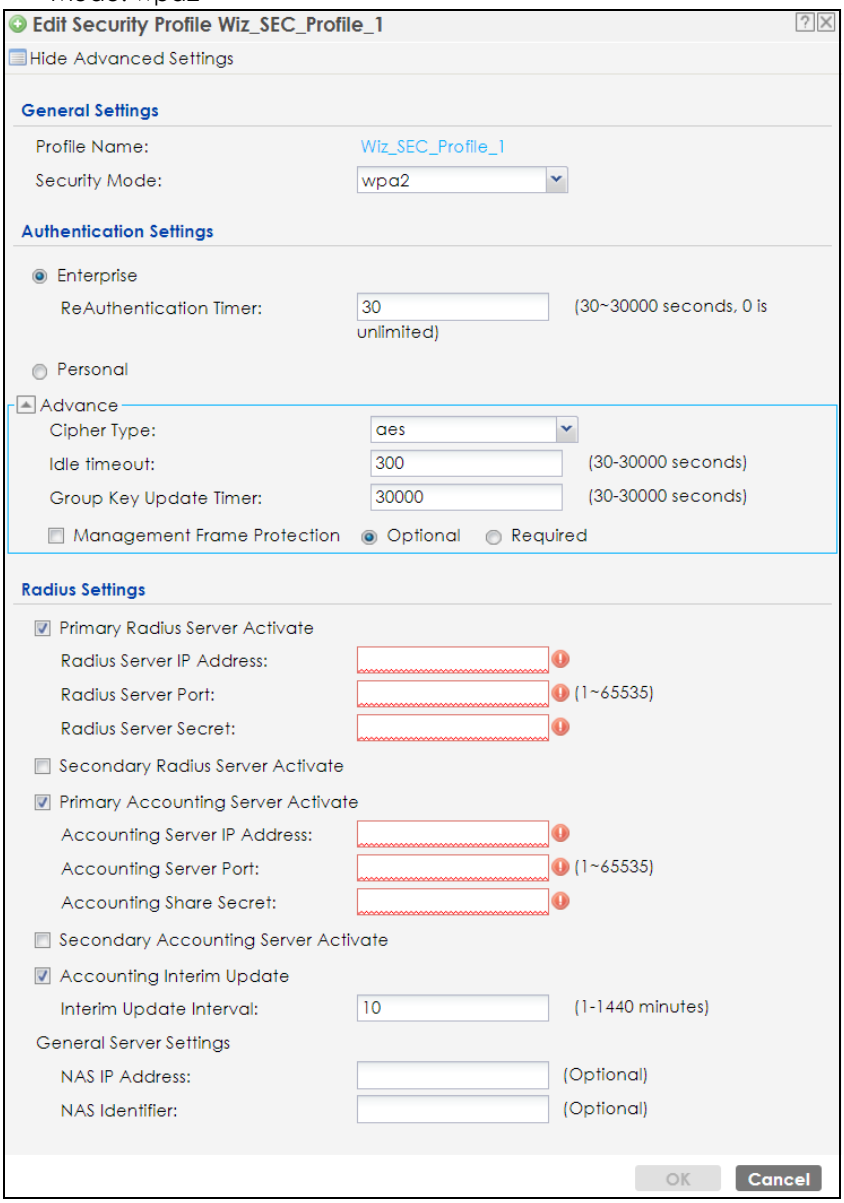
Table 54 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wep (continued)

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 54 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.

Figure 89 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wpa2



The following table describes the labels in this screen.

Table 55 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wpa2

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.

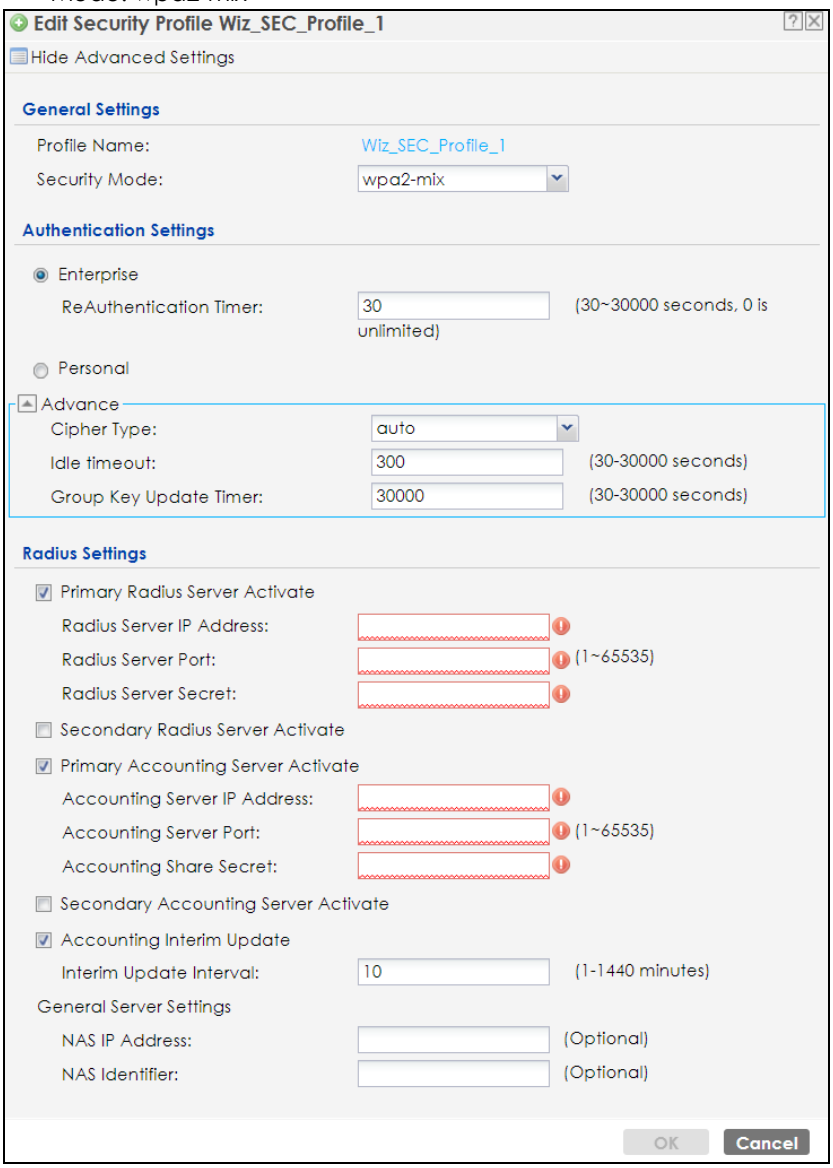
Table 55 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wpa2 (continued)

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.
Personal	This field is available when you select the **wpa2**, **wpa2-mix** or **wpa3** security mode. Select this option to use a Pre-Shared Key (PSK) with WPA2 encryption or Simultaneous Authentication of Equals (SAE) with WPA3 encryption.
Pre-Shared Key	Enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
Advance Note: Click on the **Show Advanced Settings** button to show the fields describe below.	
Cipher Type	Select an encryption cipher type from the list. • **auto** - This automatically chooses the best available cipher based on the cipher in use by the WiFi client that is attempting to make a connection. • **aes** - This is the Advanced Encryption Standard encryption method. It is a more recent development over TKIP and considerably more robust. Not all WiFi clients may support this.
Idle timeout	Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued.
Group Key Update Timer	Enter the interval (in seconds) at which the AP updates the group WPA2 encryption key.
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.
Radius Settings The **Radius Settings** fields are only available when you set **Authentication Settings** to **Enterprise**.	

Table 55 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wpa2 (continued)

LABEL	DESCRIPTION
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 90 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wpa2-mix



The following table describes the labels in this screen.

Table 56 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wpa2-mix

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.

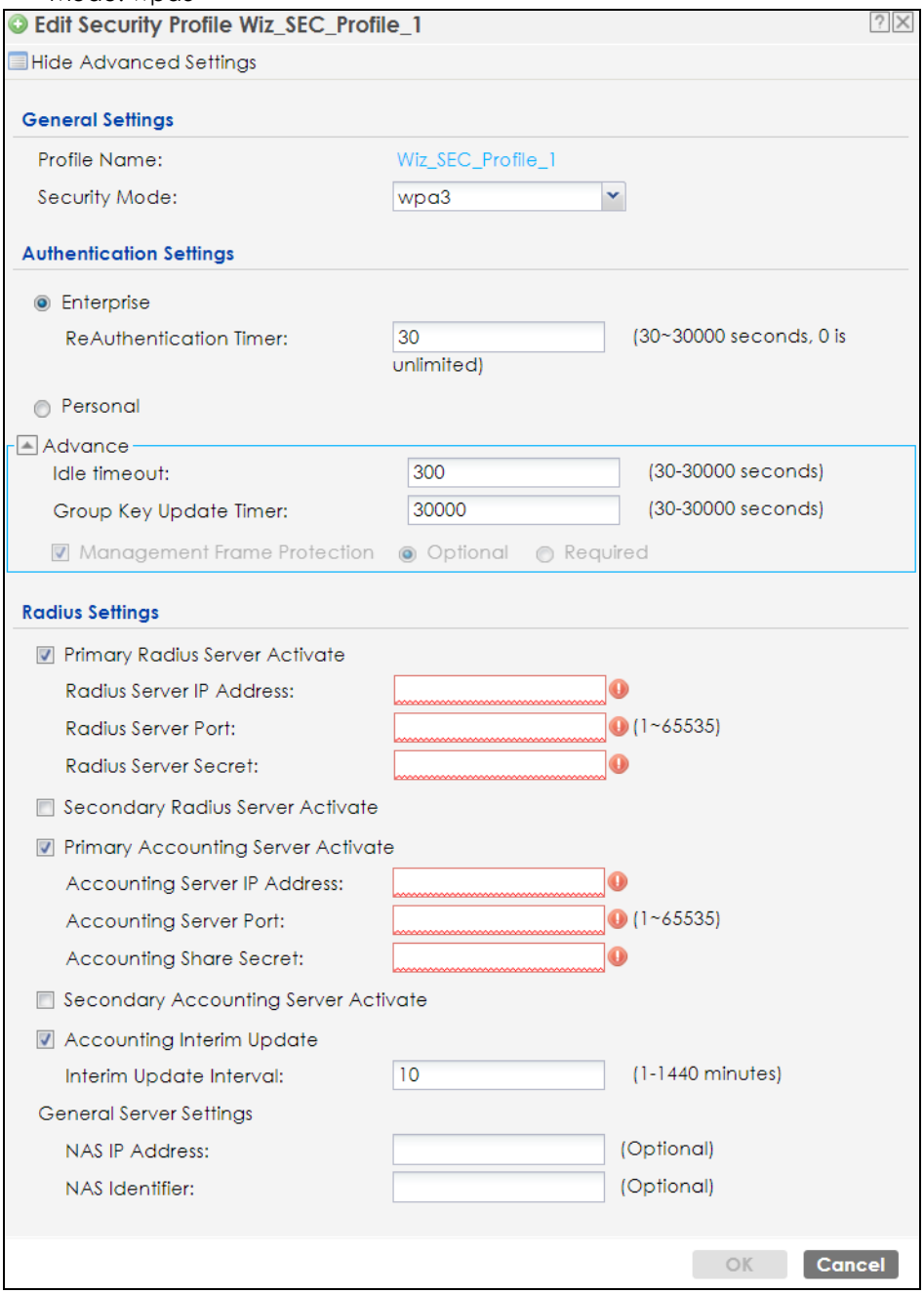
Table 56 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wpa2-mix (continued)

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.
Personal	This field is available when you select the **wpa2**, **wpa2-mix** or **wpa3** security mode. Select this option to use a Pre-Shared Key (PSK) with WPA2 encryption or Simultaneous Authentication of Equals (SAE) with WPA3 encryption.
Pre-Shared Key	Enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
Advance Note: Click on the **Show Advanced Settings** button to show the fields describe below.	
Cipher Type	Select an encryption cipher type from the list. • **auto** - This automatically chooses the best available cipher based on the cipher in use by the WiFi client that is attempting to make a connection. • **aes** - This is the Advanced Encryption Standard encryption method. It is a more recent development over TKIP and considerably more robust. Not all WiFi clients may support this.
Idle timeout	Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued.
Group Key Update Timer	Enter the interval (in seconds) at which the AP updates the group WPA2 encryption key.
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.

Table 56 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wpa2-mix (continued)

LABEL	DESCRIPTION
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 91 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wpa3



The following table describes the labels in this screen.

Table 57 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wpa3

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 57 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wpa3 (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.
Personal	This field is available when you select the **wpa2**, **wpa2-mix** or **wpa3** security mode. Select this option to use a Pre-Shared Key (PSK) with WPA2 encryption or Simultaneous Authentication of Equals (SAE) with WPA3 encryption.
Pre-Shared Key	Enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
Transition Mode	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. If you want to set the security mode to WPA3-only, use the CLI to disable **Transition Mode**. See the CLI Reference Guide for more information.
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.
Group Key Update Timer	Enter the interval (in seconds) at which the AP updates the group WPA2 encryption key.
Management Frame Protection	This field is 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.
Radius Settings The **Radius Settings** fields are only available when you set **Authentication Settings** to **Enterprise**.	

Table 57 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile> Security Mode: wpa3 (continued)

LABEL	DESCRIPTION
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.

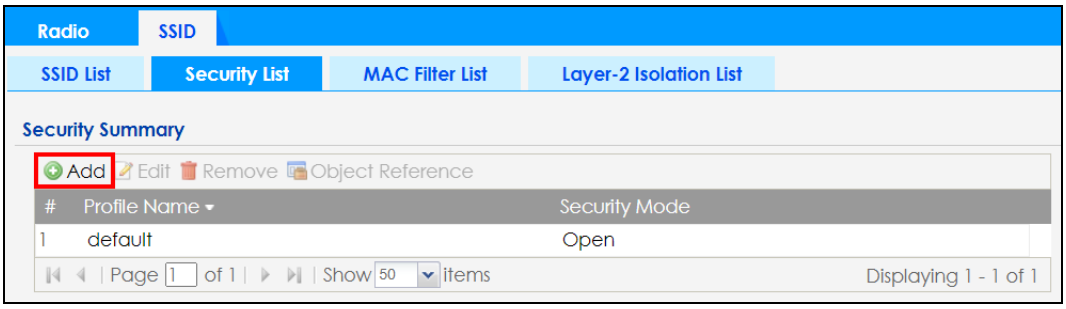
13.4.2 Creating a Security Profile

The following example shows you how to create a security profile using the parameters given in the below table.

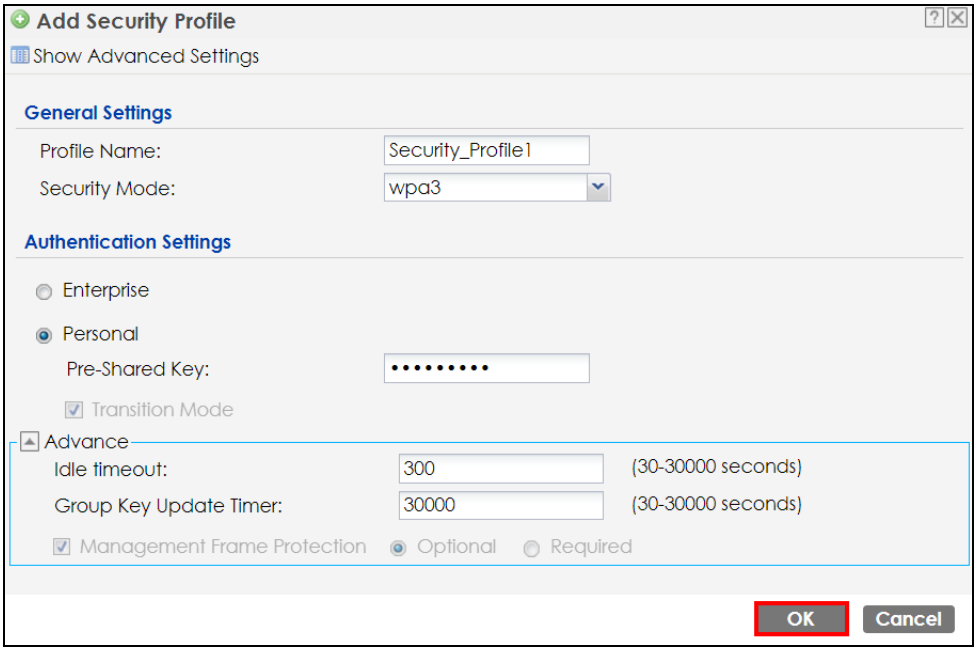
Table 58 Security Profile Settings

	SECURITY PROFILE
Profile Name	Security_Profile1
Security Mode	WPA3
Authentication	Personal
Pre-Shared Key	zyxel1234

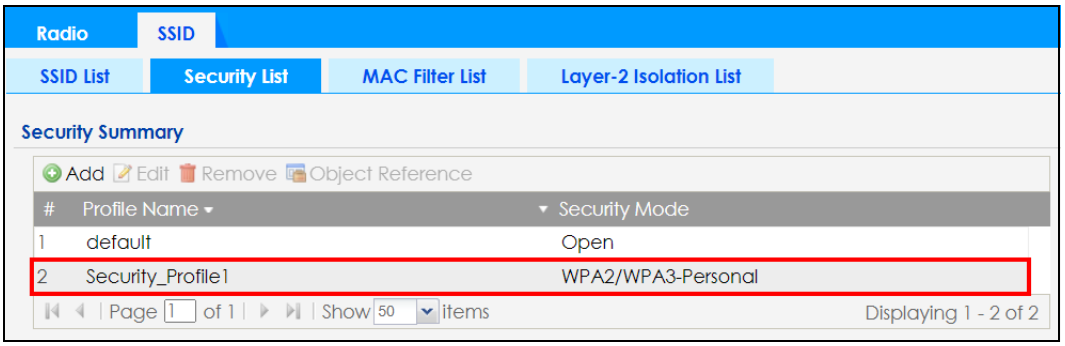
1 Go to **Configuration > Object > AP Profile > SSID > Security List**. Click **Add** to create a new security profile on the Zyxel Device.



2 Use the parameters given above and keep other configurations at their default values. Click **OK**.



3 You will then see the **Security_Profile1** entry in the summary table.

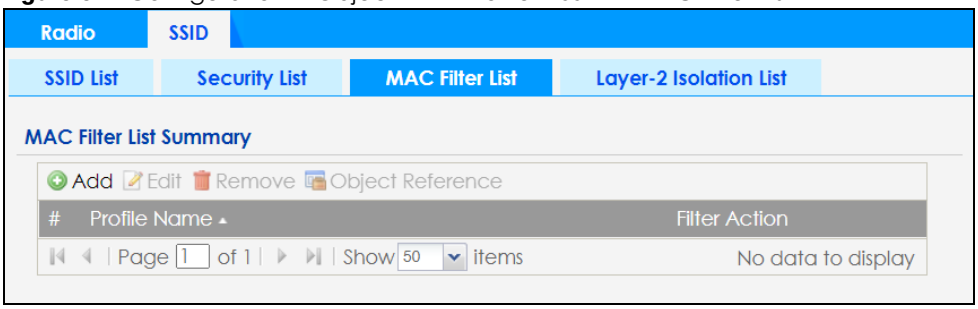


13.5 MAC Filter List

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

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

Figure 92 Configuration > Object > AP Profile > SSID > MAC Filter List



The following table describes the labels in this screen.

Table 59 Configuration > Object > AP Profile > SSID > MAC Filter List

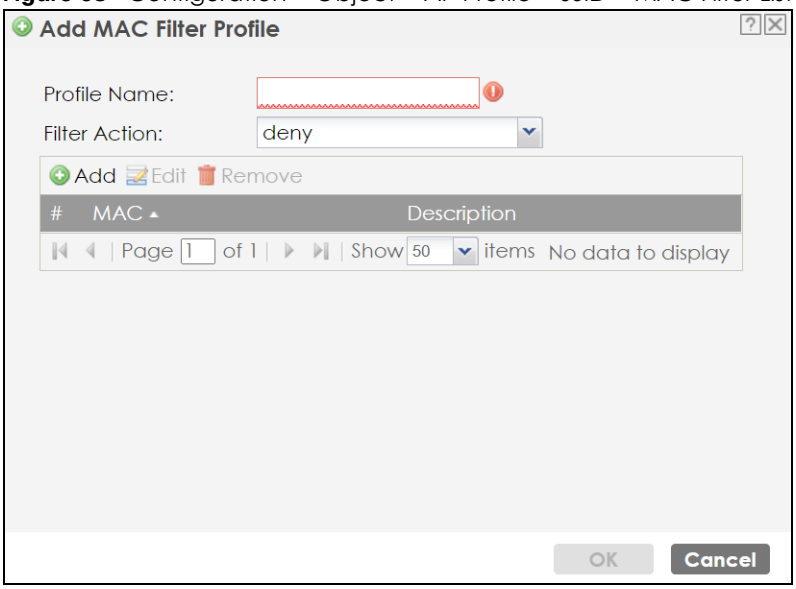
LABEL	DESCRIPTION
Add	Click this to add a new MAC filtering profile.
Edit	Click this to edit the selected MAC filtering profile.
Remove	Click this to remove the selected MAC filtering profile.
Object Reference	Click this to view which other objects are linked to the selected MAC filtering profile (for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

13.5.1 Add/Edit MAC Filter Profile

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

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

Figure 93 Configuration > Object > AP Profile > SSID > MAC Filter List > Add/Edit MAC Filter Profile



The following table describes the labels in this screen.

Table 60 Configuration > Object > AP Profile > SSID > MAC Filter List > Add/Edit MAC Filter Profile

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

13.6 Layer-2 Isolation List

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

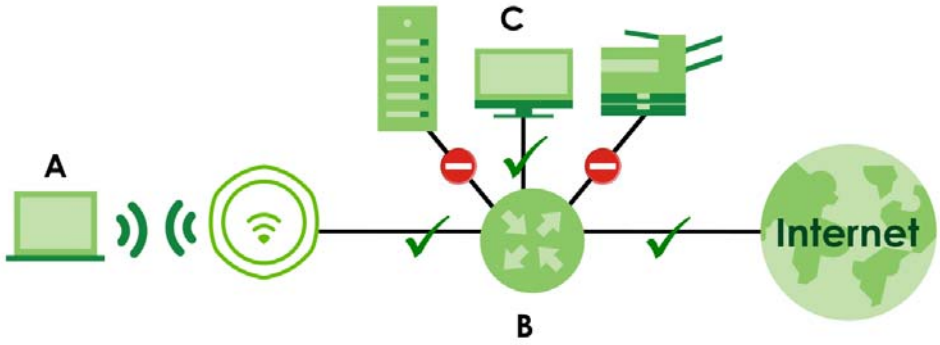
In the following example, layer-2 isolation is enabled on the Zyxel Device to allow a guest WiFi client (**A**) to access the main network router (**B**). The router provides access to the Internet and the network printer

(**C**) while preventing the client from accessing other computers and servers on the network. The client can communicate with other WiFi clients only if Intra-BSS Traffic blocking is disabled.

Note: Not all models support the layer-2 isolation feature. See the feature comparison table in Section 1.2 on page 11.

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

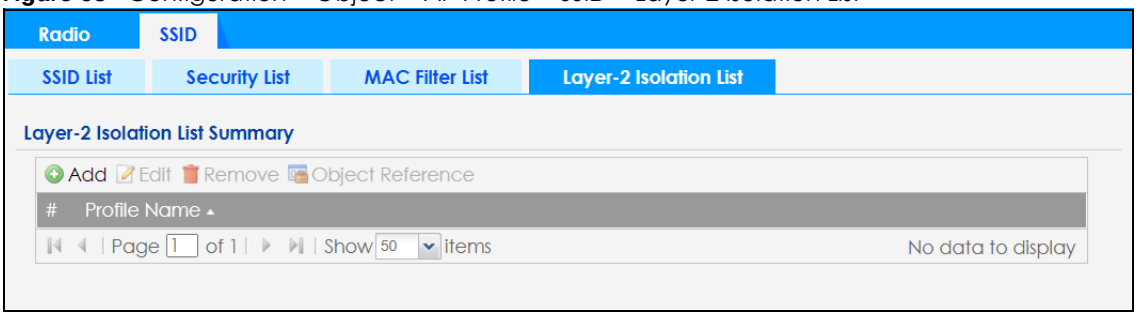
Figure 94 Layer-2 Isolation Application



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

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

Figure 95 Configuration > Object > AP Profile > SSID > Layer-2 Isolation List



The following table describes the labels in this screen.

Table 61 Configuration > Object > AP Profile > SSID > Layer-2 Isolation List

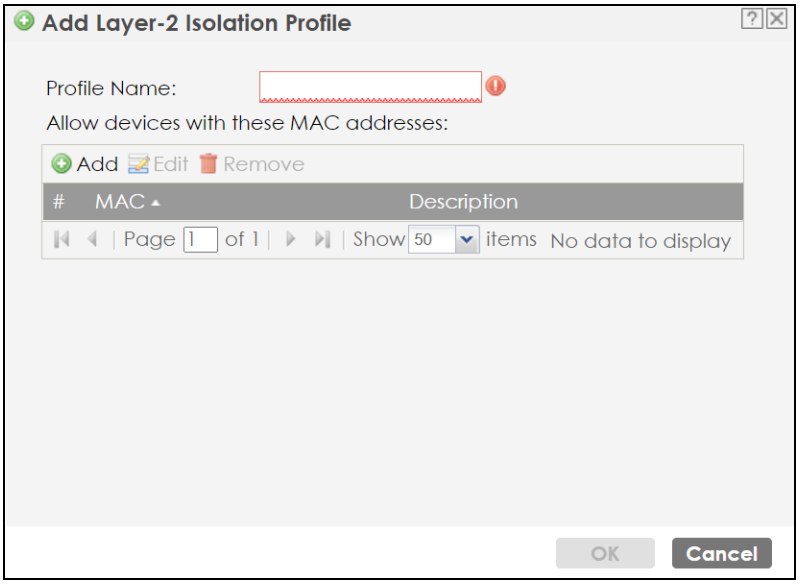
LABEL	DESCRIPTION
Add	Click this to add a new layer-2 isolation profile.
Edit	Click this to edit the selected layer-2 isolation profile.
Remove	Click this to remove the selected layer-2 isolation profile.
Object Reference	Click this to view which other objects are linked to the selected layer-2 isolation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

13.6.1 Add/Edit Layer-2 Isolation Profile

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

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

Figure 96 Configuration > Object > AP Profile > SSID > Layer-2 Isolation List > Add/Edit Layer-2 Isolation Profile



The following table describes the labels in this screen.

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

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

CHAPTER 14
WDS Profile

14.1 Overview

This chapter shows you how to configure WDS (Wireless Distribution System) profiles for the Zyxel Device to form a WDS with other APs.

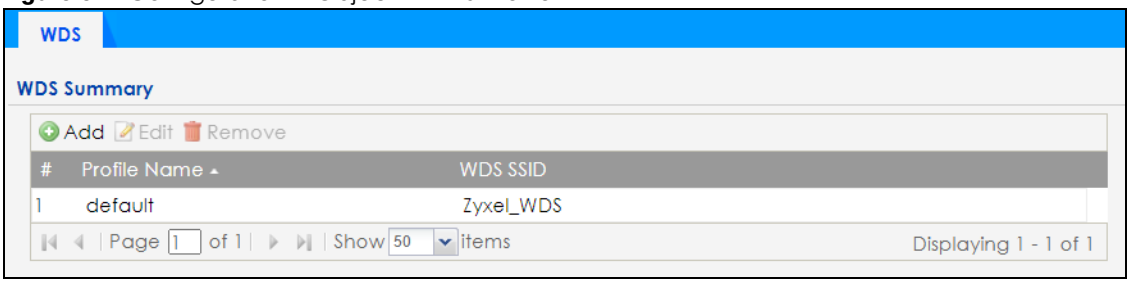
14.1.1 What You Can Do in this Chapter

The **WDS Profile** screen (Section 14.2 on page 168) creates preset WDS configurations that can be used by the Zyxel Device.

14.2 WDS Profile

This screen allows you to manage and create WDS profiles that can be used by the APs. To access this screen, click **Configuration > Object > WDS Profile**.

Figure 97 Configuration > Object > WDS Profile



The following table describes the labels in this screen.

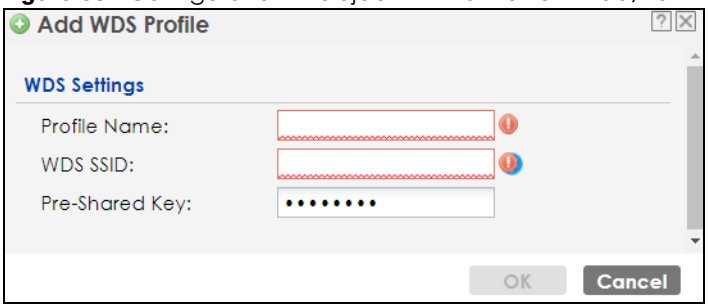
Table 63 Configuration > Object > WDS Profile

LABEL	DESCRIPTION
Add	Click this to add a new profile.
Edit	Click this to edit the selected profile.
Remove	Click this to remove the selected profile.
#	This field is a sequential value, and it is not associated with a specific profile.
Profile Name	This field indicates the name assigned to the profile.
WDS SSID	This field shows the SSID specified in this WDS profile.

14.2.1 Add/Edit WDS Profile

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

Figure 98 Configuration > Object > WDS Profile > Add/Edit WDS Profile



The following table describes the labels in this screen.

Table 64 Configuration > Object > WDS Profile > Add/Edit WDS Profile

LABEL	DESCRIPTION
Profile Name	Enter up to 31 alphanumeric characters for the profile name.
WDS SSID	Enter the SSID with which you want the Zyxel Device to connect to a root AP or repeater to form a WDS.
Pre-Shared Key	Enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters. The key is used to encrypt the traffic between the APs.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

CHAPTER 15
Certificates

15.1 Overview

The Zyxel Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

15.1.1 What You Can Do in this Chapter

- The **My Certificates** screens (Section 15.2 on page 173) generate and export self-signed certificates or certification requests and import the Zyxel Device's CA-signed certificates.
- The **Trusted Certificates** screens (Section 15.3 on page 180) save CA certificates and trusted remote host certificates to the Zyxel Device. The Zyxel Device trusts any valid certificate that you have imported as a trusted certificate. It also trusts any valid certificate signed by any of the certificates that you have imported as a trusted certificate.

15.1.2 What You Need to Know

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

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available. The other key is private and must be kept secure.

These keys work like a handwritten signature (in fact, certificates are often referred to as "digital signatures"). Only you can write your signature exactly as it should look. When people know what your signature looks like, they can verify whether something was signed by you, or by someone else. In the same way, your private key "writes" your digital signature and your public key allows people to verify whether data was signed by you, or by someone else.

This process works as follows:

1. Tim wants to send a message to Jenny. He needs her to be sure that it comes from him, and that the message content has not been altered by anyone else along the way. Tim generates a public key pair (one public key and one private key).
2. Tim keeps the private key and makes the public key openly available. This means that anyone who receives a message seeming to come from Tim can read it and verify whether it is really from him or not.
3. Tim uses his private key to sign the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to verify it. Jenny knows that the message is from Tim, and that although other people may have been able to read the message, no-one can have altered it (because they cannot re-sign the message with Tim's private key).

5 Additionally, Jenny uses her own private key to sign a message and Tim uses Jenny's public key to verify the message.

The Zyxel Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The Zyxel Device does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The Zyxel Device can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

Advantages of Certificates

Certificates offer the following benefits.

- The Zyxel Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

Self-signed Certificates

You can have the Zyxel Device act as a certification authority and sign its own certificates.

Factory Default Certificate

The Zyxel Device generates its own unique self-signed certificate when you first turn it on. This certificate is referred to in the GUI as the factory default certificate.

Certificate File Formats

Any certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The Zyxel Device currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.

- Binary PKCS#12: This is a format for transferring public key and private key certificates.The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the Zyxel Device.

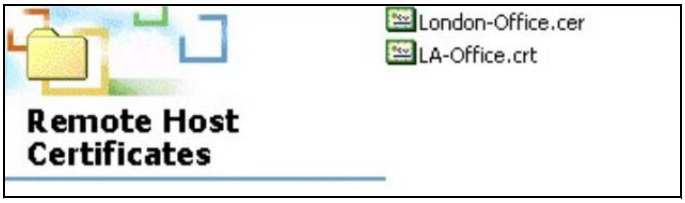
Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

15.1.3 Verifying a Certificate

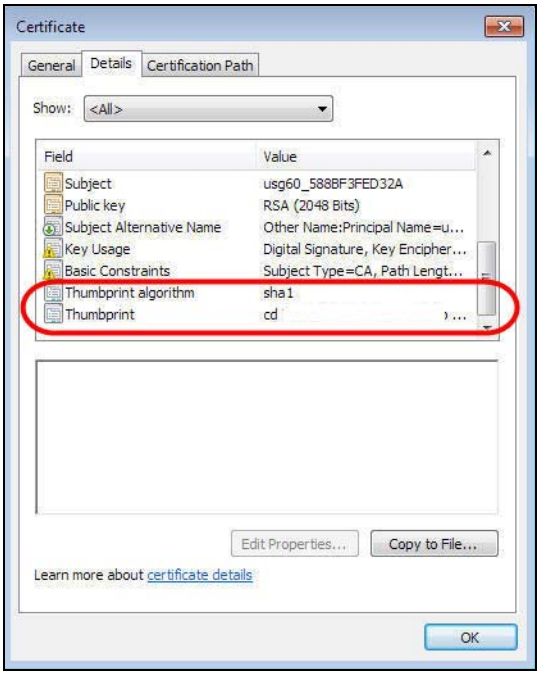
Before you import a trusted certificate into the Zyxel Device, you should verify that you have the correct certificate. You can do this using the certificate's fingerprint. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithm. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

1 Browse to where you have the certificate saved on your computer.

2 Make sure that the certificate has a ".cer" or ".crt" file name extension.



3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

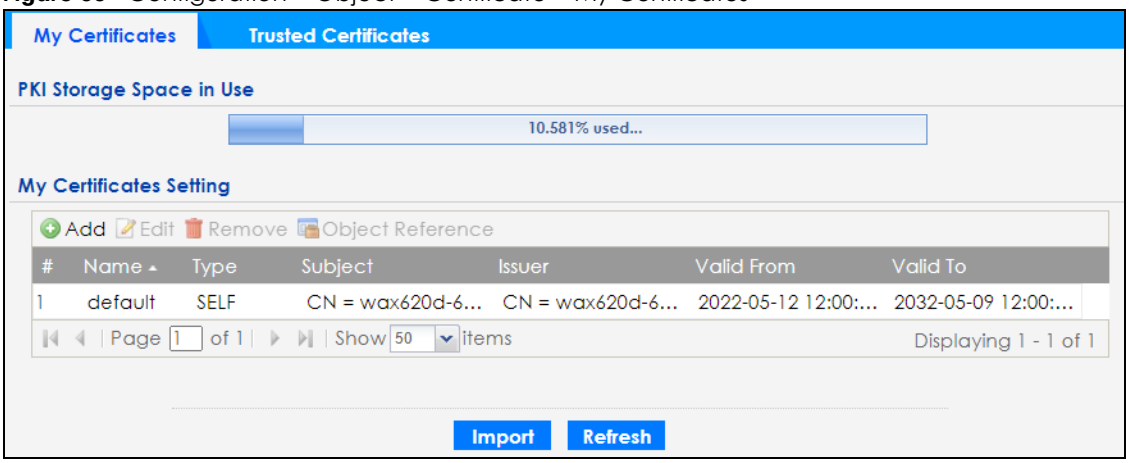


4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may vary based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

15.2 My Certificates

Click **Configuration > Object > Certificate > My Certificates** to open this screen. This is the Zyxel Device's summary list of certificates and certification requests.

Figure 99 Configuration > Object > Certificate > My Certificates



The following table describes the labels in this screen.

Table 65 Configuration > Object > Certificate > My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the Zyxel Device's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
My Certificates Settings	
Add	Click this to go to the screen where you can have the Zyxel Device generate a certificate or a certification request.
Edit	Double-click an entry or select it and click **Edit** to open a screen with an in-depth list of information about the certificate.
Remove	The Zyxel Device keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Subsequent certificates move up by one when you take this action.
Object Reference	You cannot delete certificates that any of the Zyxel Device's features are configured to use. Select an entry and click **Object Reference** to open a screen that shows which settings use the entry.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Type	This field displays what kind of certificate this is. **REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate Import** screen to import the certificate and replace the request. **SELF** represents a self-signed certificate. **CERT** represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.

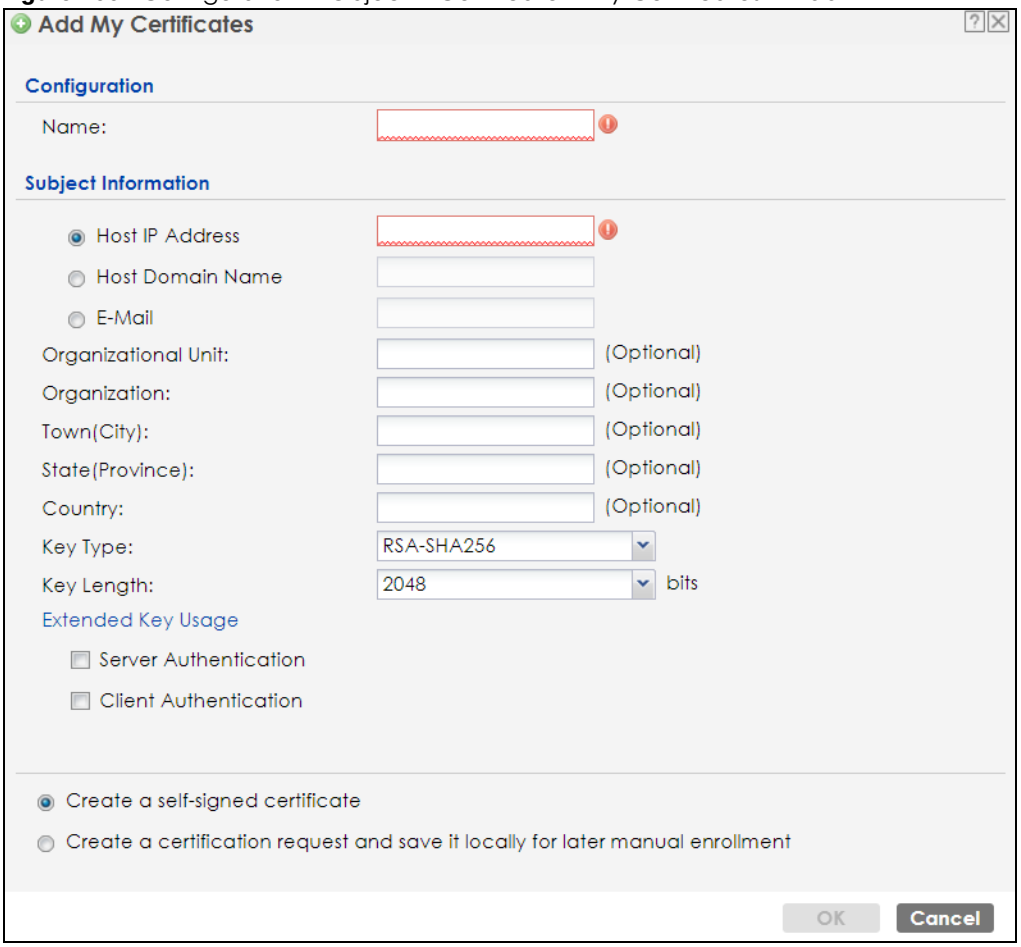
Table 65 Configuration > Object > Certificate > My Certificates (continued)

LABEL	DESCRIPTION
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Import	Click **Import** to open a screen where you can save a certificate to the Zyxel Device.
Refresh	Click **Refresh** to display the current validity status of the certificates.

15.2.1 Add My Certificates

Click **Configuration > Object > Certificate > My Certificates** and then the **Add** icon to open the **Add My Certificates** screen. Use this screen to have the Zyxel Device create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request.

Figure 100 Configuration > Object > Certificate > My Certificates > Add



The following table describes the labels in this screen.

Table 66 Configuration > Object > Certificate > My Certificates > Add

LABEL	DESCRIPTION
Name	Type a name to identify this certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although you must specify a **Host IP Address**, **Host Domain Name**, or **E-Mail**. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information. Select a radio button to identify the certificate's owner by IP address, domain name or email address. Type the IP address (in dotted decimal notation), domain name or email address in the field provided. The domain name or email address is for identification purposes only and can be any string. A domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods. An email address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore.
Organizational Unit	Identify the organizational unit or department to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Organization	Identify the company or group to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Town (City)	Identify the town or city where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
State (Province)	Identify the state or province where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Country	Identify the nation where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Key Type	The Zyxel Device uses the RSA (Rivest, Shamir and Adleman) public-key encryption algorithm. SHA1 (Secure Hash Algorithm) and SHA2 are hash algorithms used to authenticate packet data. SHA2-256 or SHA2-512 are part of the SHA2 set of cryptographic functions and they are considered even more secure than SHA1. Select a key type from **RSA-SHA256** and **RSA-SHA512**.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (1024 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Extended Key Usage	Select **Server Authentication** to allow a web server to send clients the certificate to authenticate itself. Select **Client Authentication** to use the certificate's key to authenticate clients to the secure gateway.
Use the below radio buttons to set how and when the certificate is to be generated.	
Create a self-signed certificate	Select this to have the Zyxel Device generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select this to have the Zyxel Device generate and store a request for a certificate. Use the **My Certificate Edit** screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the **My Certificate Edit** screen and then send it to the certification authority.

Table 66 Configuration > Object > Certificate > My Certificates > Add (continued)

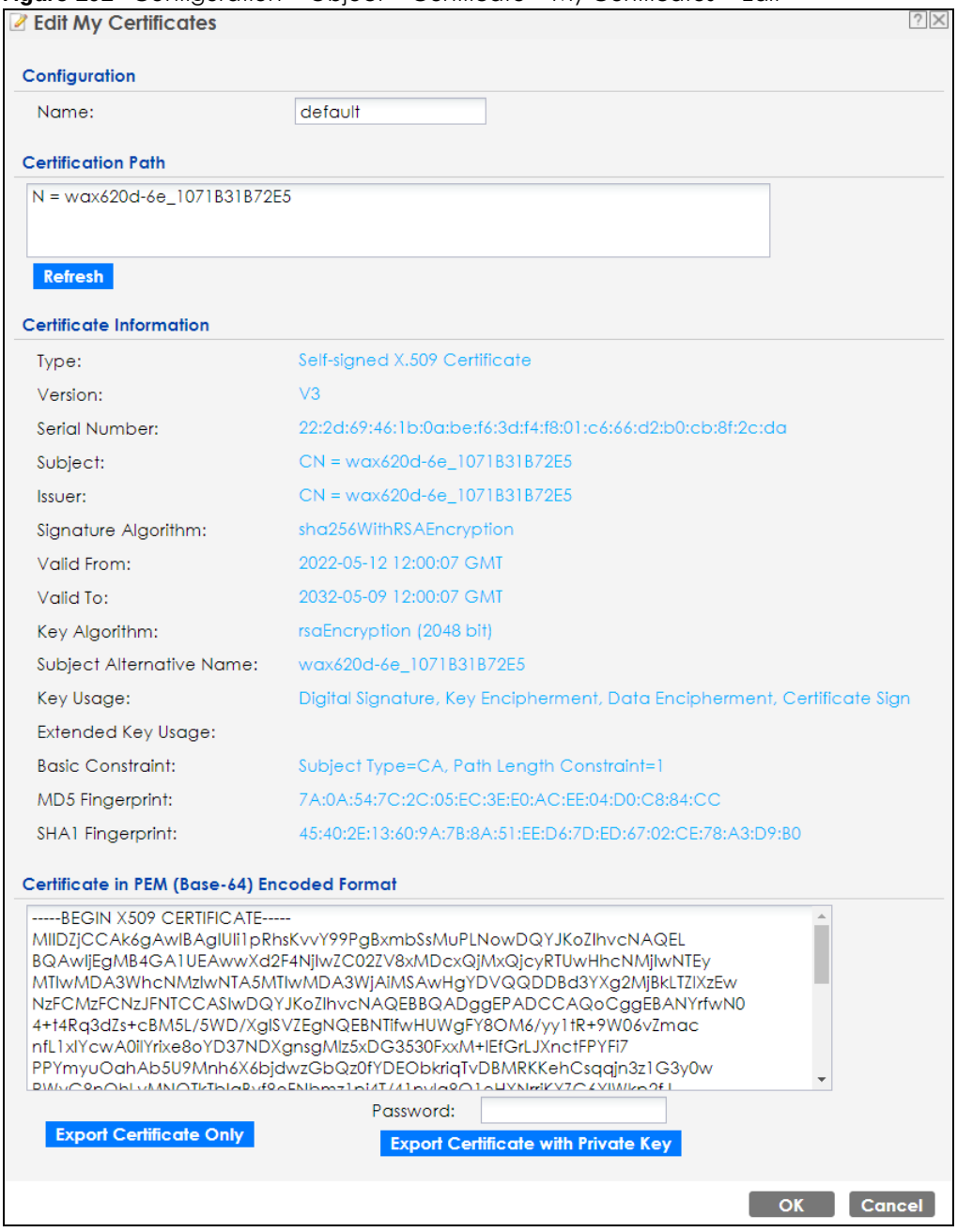
LABEL	DESCRIPTION
OK	Click **OK** to begin certificate or certification request generation.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

If you configured the **Add My Certificates** screen to have the Zyxel Device enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **Add My Certificates** screen. Click **Return** and check your information in the **Add My Certificates** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the Zyxel Device to enroll a certificate online.

15.2.2 Edit My Certificates

Click **Configuration > Object > Certificate > My Certificates** and then the **Edit** icon to open the **My Certificate Edit** screen. You can use this screen to view in-depth certificate information and change the certificate's name.

Figure 101 Configuration > Object > Certificate > My Certificates > Edit



The following table describes the labels in this screen.

Table 67 Configuration > Object > Certificate > My Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
Certification Path This field displays for a certificate, not a certification request. Click the **Refresh** button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The Zyxel Device does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.	
Refresh	Click **Refresh** to display the certification path.
Certificate Information These read-only fields display detailed information about the certificate.	
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the Zyxel Device.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O), State (ST), and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the **Subject Name** field. "none" displays for a certification request.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate.
Valid From	This field displays the date that the certificate becomes applicable. "none" displays for a certification request.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired. "none" displays for a certification request.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the Zyxel Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or email address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Extended Key Usage	This field displays for what EKU (Extended Key Usage) functions the certificate's key can be used.

Table 67 Configuration > Object > Certificate > My Certificates > Edit

LABEL	DESCRIPTION
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path. This field does not display for a certification request.
MD5 Fingerprint	This is the certificate's message digest that the Zyxel Device calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the Zyxel Device calculated using the SHA1 algorithm.
SHA256 Fingerprint	This is the certificate's message digest that the Zyxel Device calculated using the SHA256 algorithm.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form. You can copy and paste a certification request into a certification authority's web page, an email that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an email to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (through floppy disk for example).
Export Certificate Only	Use this button to save a copy of the certificate without its private key. Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Password	If you want to export the certificate with its private key, create a password and type it here. Make sure you keep this password in a safe place. You will need to use it if you import the certificate to another device.
Export Certificate with Private Key	Use this button to save a copy of the certificate with its private key. Type the certificate's password and click this button. Click **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
OK	Click **OK** to save your changes back to the Zyxel Device. You can only change the name.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

15.2.3 Import Certificates

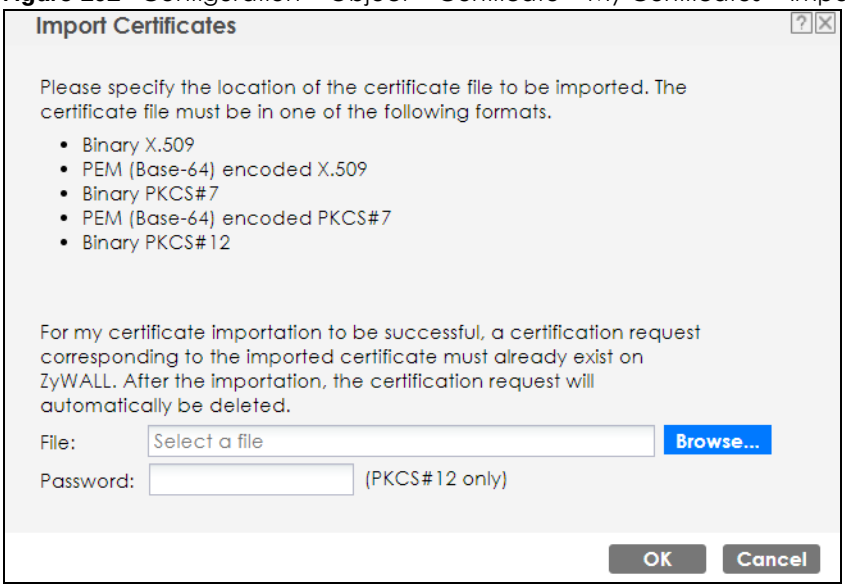
Click **Configuration > Object > Certificate > My Certificates > Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the Zyxel Device.

Note: You can import a certificate that matches a corresponding certification request that was generated by the Zyxel Device. You can also import a certificate in PKCS#12 format, including the certificate's public and private keys.

The certificate you import replaces the corresponding request in the **My Certificates** screen.

You must remove any spaces in the certificate's filename before you can import it.

Figure 102 Configuration > Object > Certificate > My Certificates > Import



The following table describes the labels in this screen.

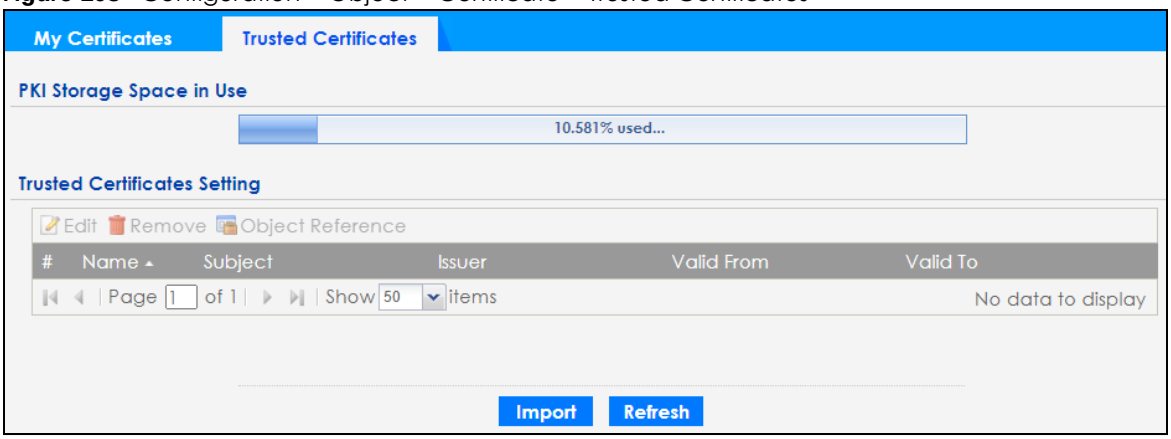
Table 68 Configuration > Object > Certificate > My Certificates > Import

LABEL	DESCRIPTION
File	Type in the location of the file you want to upload in this field or click **Browse** to find it. You cannot import a certificate with the same name as a certificate that is already in the Zyxel Device.
Browse	Click **Browse** to find the certificate file you want to upload.
Password	This field only applies when you import a binary PKCS#12 format file. Type the file's password that was created when the PKCS #12 file was exported.
OK	Click **OK** to save the certificate on the Zyxel Device.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

15.3 Trusted Certificates

Click **Configuration > Object > Certificate > Trusted Certificates** to open the **Trusted Certificates** screen. This screen displays a summary list of certificates that you have set the Zyxel Device to accept as trusted. The Zyxel Device also accepts any valid certificate signed by a certificate on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certificates.

Figure 103 Configuration > Object > Certificate > Trusted Certificates



The following table describes the labels in this screen.

Table 69 Configuration > Object > Certificate > Trusted Certificates

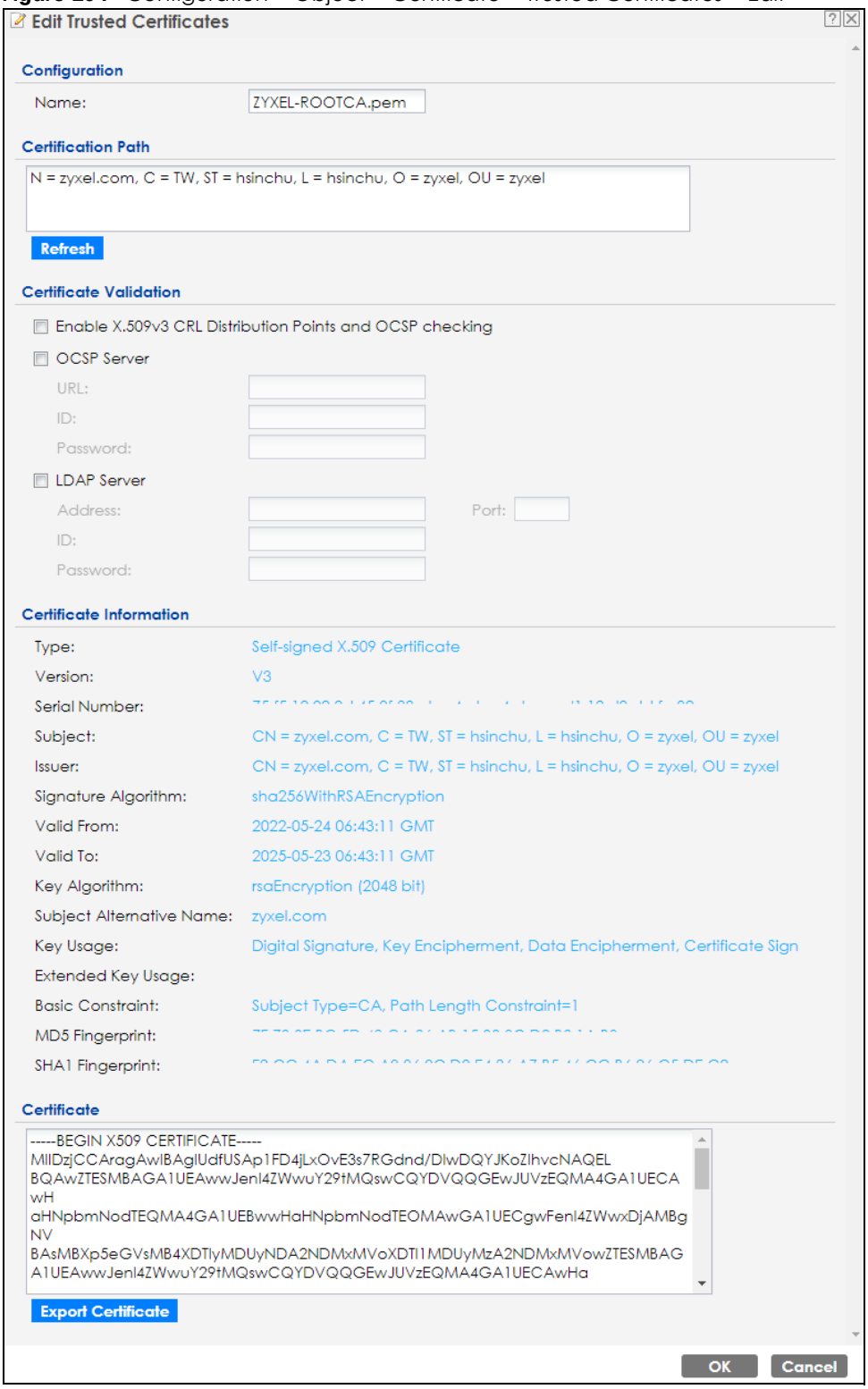
LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the Zyxel Device's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Trusted Certificates Settings	
Edit	Double-click an entry or select it and click **Edit** to open a screen with an in-depth list of information about the certificate.
Remove	The Zyxel Device keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Subsequent certificates move up by one when you take this action.
Object Reference	You cannot delete certificates that any of the Zyxel Device's features are configured to use. Select an entry and click **Object Reference** to open a screen that shows which settings use the entry.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Import	Click **Import** to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the Zyxel Device.
Refresh	Click this button to display the current validity status of the certificates.

15.3.1 Edit Trusted Certificates

Click **Configuration > Object > Certificate > Trusted Certificates** and then a certificate's **Edit** icon to open the **Trusted Certificates Edit** screen. Use this screen to view in-depth information about the certificate, change the certificate's name and set whether or not you want the Zyxel Device to check a

certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Figure 104 Configuration > Object > Certificate > Trusted Certificates > Edit



The following table describes the labels in this screen.

Table 70 Configuration > Object > Certificate > Trusted Certificates > Edit

LABEL	DESCRIPTION
Configuration	
Name	This field displays the identifying name of this certificate. You can change the name. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
Certification Path Click the **Refresh** button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certificate, it may be the only certification authority in the list (along with the end entity's own certificate). The Zyxel Device does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.	
Refresh	Click **Refresh** to display the certification path.
Certificate Validation	
Enable X.509v3 CRL Distribution Points and OCSP checking	Select this checkbox to have the Zyxel Device check incoming certificates that are signed by this certificate against a Certificate Revocation List (CRL) or an OCSP server. You also need to configure the OSCP or LDAP server details.
OCSP Server	Select this checkbox if the directory server uses OCSP (Online Certificate Status Protocol).
URL	Type the protocol, IP address and pathname of the OCSP server.
ID	The Zyxel Device may need to authenticate itself in order to assess the OCSP server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the OCSP server (usually a certification authority).
LDAP Server	Select this checkbox if the directory server uses LDAP (Lightweight Directory Access Protocol). LDAP is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates.
Address	Type the IP address (in dotted decimal notation) of the directory server.
Port	Use this field to specify the LDAP server port number. You must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.
ID	The Zyxel Device may need to authenticate itself in order to assess the CRL directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the CRL directory server (usually a certification authority).
Certificate Information These read-only fields display detailed information about the certificate.	
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the **Subject Name** field.

Table 70 Configuration > Object > Certificate > Trusted Certificates > Edit (continued)

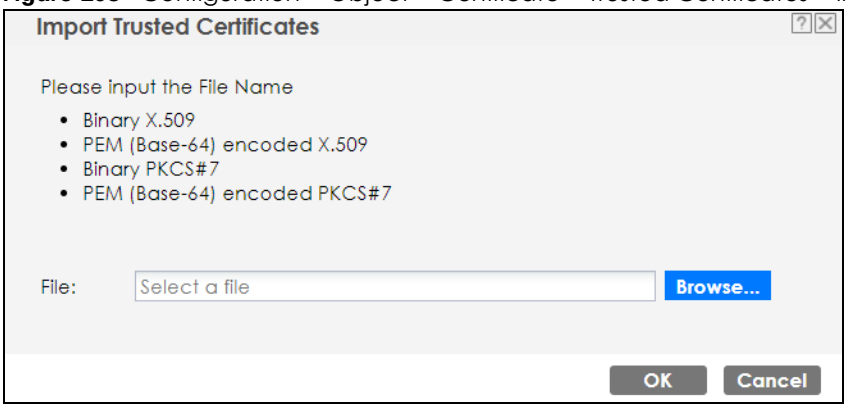
LABEL	DESCRIPTION
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the Zyxel Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or email address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the Zyxel Device calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the Zyxel Device calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form. You can copy and paste the certificate into an email to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (through floppy disk for example).
Export Certificate	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
OK	Click **OK** to save your changes back to the Zyxel Device. You can only change the name.
Cancel	Click **Cancel** to quit and return to the **Trusted Certificates** screen.

15.3.2 Import Trusted Certificates

Click **Configuration > Object > Certificate > Trusted Certificates > Import** to open the **Import Trusted Certificates** screen. Follow the instructions in this screen to save a trusted certificate to the Zyxel Device.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 105 Configuration > Object > Certificate > Trusted Certificates > Import



The following table describes the labels in this screen.

Table 71 Configuration > Object > Certificate > Trusted Certificates > Import

LABEL	DESCRIPTION
File	Type in the location of the file you want to upload in this field or click **Browse** to find it. You cannot import a certificate with the same name as a certificate that is already in the Zyxel Device.
Browse	Click **Browse** to find the certificate file you want to upload.
OK	Click **OK** to save the certificate on the Zyxel Device.
Cancel	Click **Cancel** to quit and return to the previous screen.

15.4 Technical Reference

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

OCSP

OCSP (Online Certificate Status Protocol) allows an application or device to check whether a certificate is valid. With OCSP the Zyxel Device checks the status of individual certificates instead of downloading a Certificate Revocation List (CRL). OCSP has two main advantages over a CRL. The first is real-time status information. The second is a reduction in network traffic since the Zyxel Device only gets information on the certificates that it needs to verify, not a huge list. When the Zyxel Device requests certificate status information, the OCSP server returns a "expired", "current" or "unknown" response.

CHAPTER 16
System

16.1 Overview

Use the system screens to configure general Zyxel Device settings.

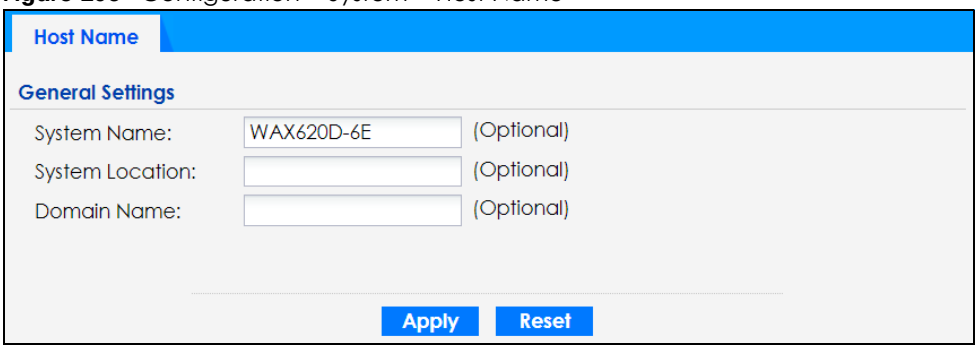
16.1.1 What You Can Do in this Chapter

- The **Host Name** screen (Section 16.2 on page 186) configures a unique name for the Zyxel Device in your network.
- The **Date/Time** screen (Section 16.3 on page 187) configures the date and time for the Zyxel Device.
- The **WWW** screens (Section 16.4 on page 191) configure settings for HTTP or HTTPS access to the Zyxel Device.
- The **SSH** screen (Section 16.5 on page 199) configures SSH (Secure SHell) for securely accessing the Zyxel Device's command line interface.
- The **FTP** screen (Section 16.6 on page 203) specifies FTP server settings. You can upload and download the Zyxel Device's firmware and configuration files using FTP. Please also see Chapter 18 on page 210 for more information about firmware and configuration files.

16.2 Host Name

A host name is the unique name by which a device is known on a network. Click **Configuration > System > Host Name** to open this screen.

Figure 106 Configuration > System > Host Name



The following table describes the labels in this screen.

Table 72 Configuration > System > Host Name

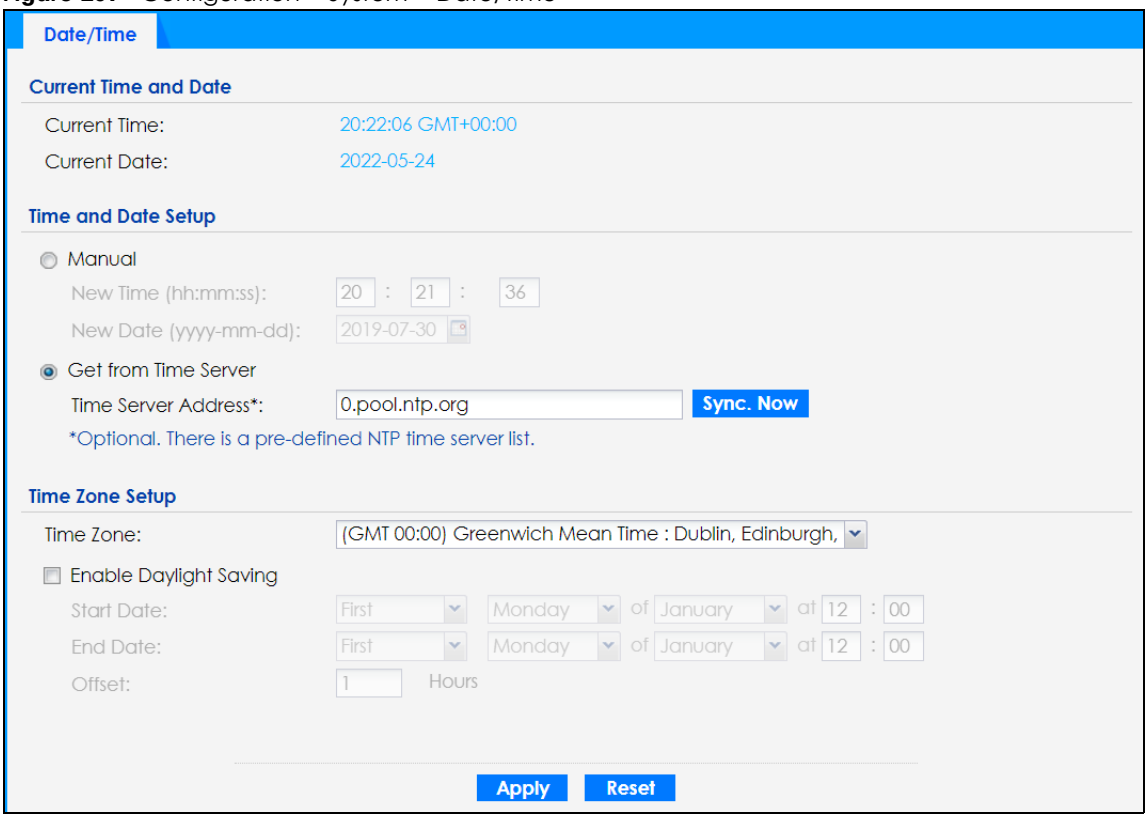
LABEL	DESCRIPTION
General Settings	
System Name	Choose a descriptive name to identify your Zyxel Device device. This name can be up to 64 alphanumeric characters long. Spaces are not allowed, but dashes (-) underscores (_) and periods (.) are accepted.
System Location	Specify the name of the place where the Zyxel Device is located. You can enter up to 60 alphanumeric and '()' ,:;?! +-*/= #$%@ characters. Spaces and underscores are allowed. The name should start with a letter.
Domain Name	Enter the domain name (if you know it) here. This name is propagated to DHCP clients connected to interfaces with the DHCP server enabled. This name can be up to 254 alphanumeric characters long. Spaces are not allowed, but dashes "-" are accepted.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

16.3 Date and Time

For effective scheduling and logging, the Zyxel Device system time must be accurate. The Zyxel Device has a software mechanism to set the time manually or get the current time and date from an external server.

To change your Zyxel Device's time based on your local time zone and date, click **Configuration > System > Date/Time**. The screen displays as shown. You can manually set the Zyxel Device's time and date or have the Zyxel Device get the date and time from a time server.

Figure 107 Configuration > System > Date/Time



The following table describes the labels in this screen.

Table 73 Configuration > System > Date/Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the present time of your Zyxel Device.
Current Date	This field displays the present date of your Zyxel Device.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, time zone and daylight saving at the same time, the time zone and daylight saving will affect the new time and date you entered. When you enter the time settings manually, the Zyxel Device uses the new setting once you click **Apply**.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the Zyxel Device get the time and date from the time server you specify below. The Zyxel Device requests time and date settings from the time server under the following circumstances. • When the Zyxel Device starts up. • When you click **Apply** or **Sync. Now** in this screen. • 24-hour intervals after starting up.

Table 73 Configuration > System > Date/Time (continued)

LABEL	DESCRIPTION
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Sync. Now	Click this button to have the Zyxel Device get the time and date from a time server (see the **Time Server Address** field). This also saves your changes (except the daylight saving settings).
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Enable Daylight Saving	Daylight saving is a period from late spring to fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The **at** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type 2 in the **at** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **at** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **at** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type 2 in the **at** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **at** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Offset	Specify how much the clock changes when daylight saving begins and ends. Enter a number from 1 to 5.5 (by 0.5 increments). For example, if you set this field to 3.5, a log occurred at 6 P.M. in local official time will appear as if it had occurred at 10:30 P.M.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

16.3.1 Pre-defined NTP Time Servers List

When you turn on the Zyxel Device for the first time, the date and time start at 2003-01-01 00:00:00. The Zyxel Device then attempts to synchronize with one of the following pre-defined list of Network Time Protocol (NTP) time servers in order from the first one until it is successful.

Table 74 Default Time Servers

time.windows.com
time.apple.com
time.cloudflare.com

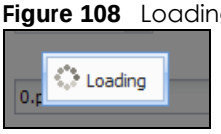
The Zyxel Device continues to use the pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

16.3.2 Time Server Synchronization

Click the **Sync. Now** button to get the time and date from the time server you specified in the **Time Server Address** field.

When the **Loading** message appears, you may have to wait up to one minute.

Figure 108 Loading



The **Current Time** and **Current Date** fields will display the appropriate settings if the synchronization is successful.

If the synchronization was not successful, a log displays in the **View Log** screen. Try re-configuring the **Date/Time** screen.

To manually set the Zyxel Device date and time:

1 Click **System > Date/Time**.

2 Select **Manual** under **Time and Date Setup**.

3 Enter the Zyxel Device's time in the **New Time** field.

4 Enter the Zyxel Device's date in the **New Date** field.

5 Under **Time Zone Setup**, select your **Time Zone** from the list.

6 As an option you can select the **Enable Daylight Saving** checkbox to adjust the Zyxel Device clock for daylight savings.

7 Click **Apply**.

To get the Zyxel Device date and time from a time server:

1 Click **System > Date/Time**.

2 Select **Get from Time Server** under **Time and Date Setup**.

3 Under **Time Zone Setup**, select your **Time Zone** from the list.

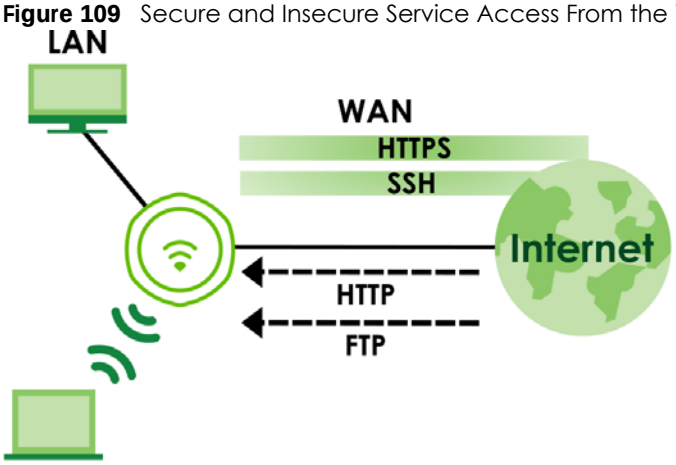
4 Under **Time and Date Setup**, enter a **Time Server Address**.

5 Click **Apply**.

16.4 WWW Overview

The following figure shows secure and insecure management of the Zyxel Device coming in from the WAN. HTTPS and SSH access are secure. HTTP and FTP management access are not secure.

Figure 109 Secure and Insecure Service Access From the WAN



16.4.1 Service Access Limitations

A service cannot be used to access the Zyxel Device when you have disabled that service in the corresponding screen.

16.4.2 System Timeout

There is a lease timeout for administrators. The Zyxel Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

Each user is also forced to log in the Zyxel Device for authentication again when the reauthentication time expires.

You can change the timeout settings in the **User** screens.

16.4.3 HTTPS

You can set the Zyxel Device to use HTTP or HTTPS (HTTPS adds security) for Web Configurator sessions.

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys (see Chapter 15 on page 170 for more information).

HTTPS on the Zyxel Device is used so that you can securely access the Zyxel Device using the Web Configurator. The SSL protocol specifies that the HTTPS server (the Zyxel Device) must always

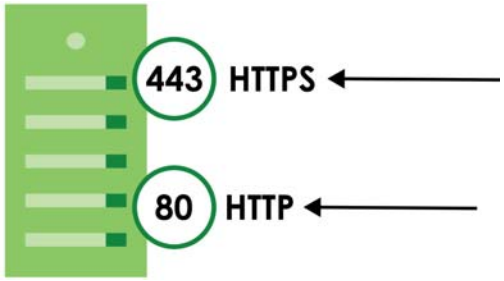
authenticate itself to the HTTPS client (the computer which requests the HTTPS connection with the Zyxel Device), whereas the HTTPS client only should authenticate itself when the HTTPS server requires it to do so (select **Authenticate Client Certificates** in the **WWW** screen). **Authenticate Client Certificates** is optional and if selected means the HTTPS client must send the Zyxel Device a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the Zyxel Device.

Please refer to the following figure.

1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the Zyxel Device's web server.

2 HTTP connection requests from a web browser go to port 80 (by default) on the Zyxel Device's web server.

Figure 110 HTTP/HTTPS Implementation

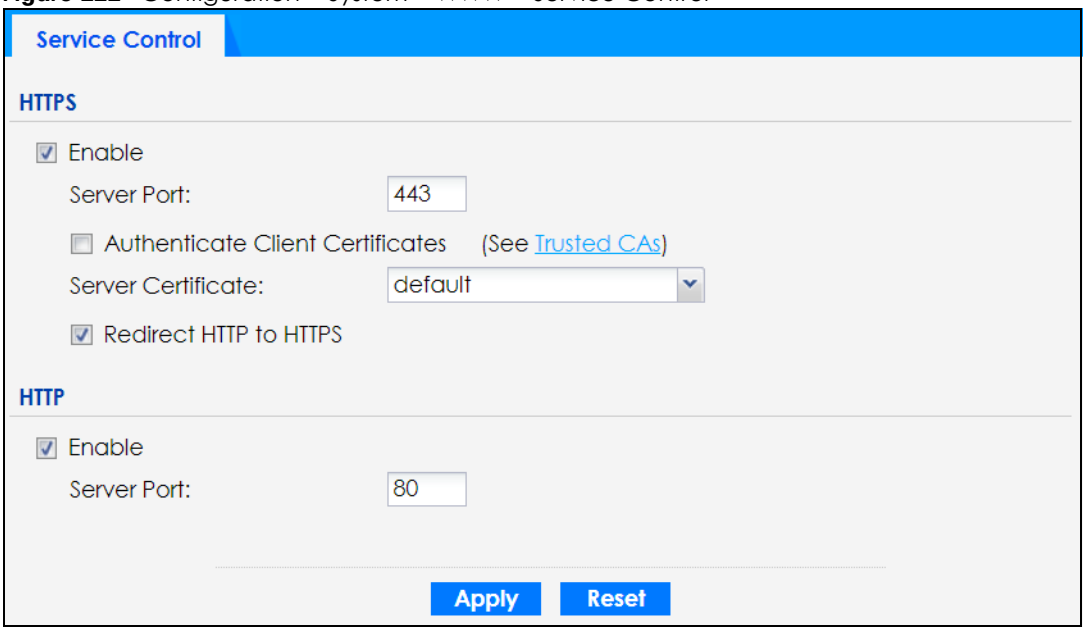


Note: If you disable **HTTP** in the **WWW** screen, then the Zyxel Device blocks all HTTP connection attempts.

16.4.4 Configuring WWW Service Control

Click **Configuration > System > WWW** to open the **WWW** screen. Use this screen to specify HTTP or HTTPS settings.

Figure 111 Configuration > System > WWW > Service Control



The following table describes the labels in this screen.

Table 75 Configuration > System > WWW > Service Control

LABEL	DESCRIPTION
HTTPS	
Enable	Select the checkbox to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the Zyxel Device Web Configurator using secure HTTPs connections.
Server Port	The HTTPS server listens on port 443 by default. If you change the HTTPS server port to a different number on the Zyxel Device, for example 8443, then you must notify people who need to access the Zyxel Device Web Configurator to use "https://Zyxel Device IP Address:**8443**" as the URL.
Authenticate Client Certificates	Select **Authenticate Client Certificates** (optional) to require the SSL client to authenticate itself to the Zyxel Device by sending the Zyxel Device a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the Zyxel Device. Click **Trusted CAs** to go to the **Configuration** > **Object** > **Certificate** > **Trusted Certificates** screen and check for the trusted certificates settings.
Server Certificate	Select a certificate the HTTPS server (the Zyxel Device) uses to authenticate itself to the HTTPS client. You must have certificates already configured in the **My Certificates** screen.
Redirect HTTP to HTTPS	To allow only secure Web Configurator access, select this to redirect all HTTP connection requests to the HTTPS server.
HTTP	
Enable	Select the checkbox to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the Zyxel Device Web Configurator using HTTP connections.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service to access the Zyxel Device.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

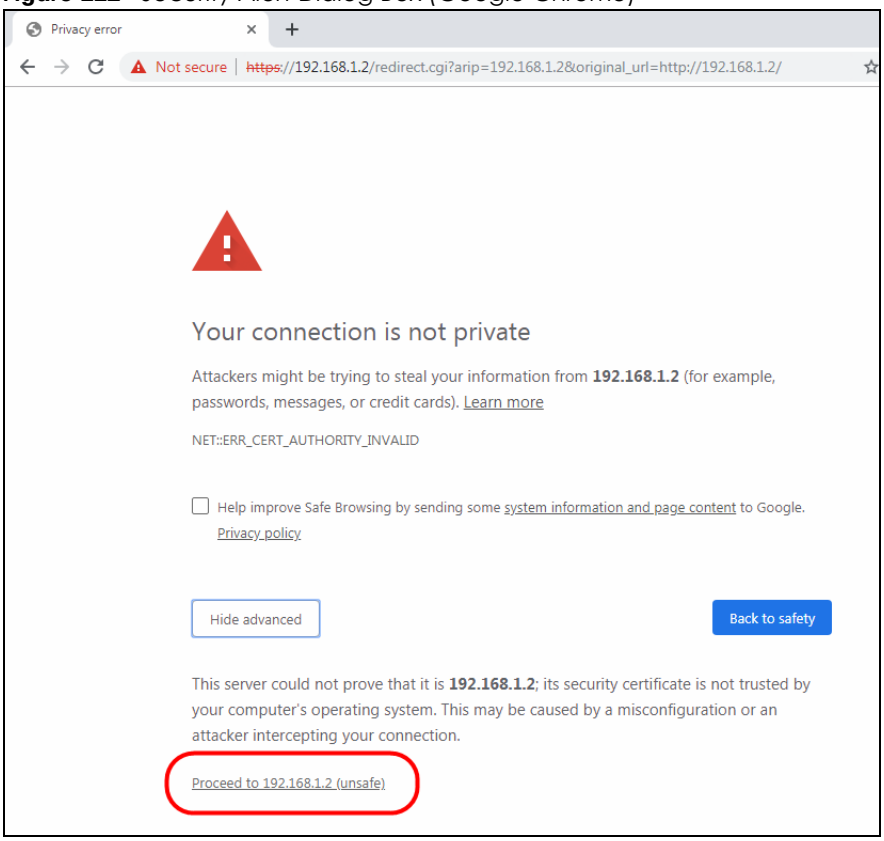
16.4.5 HTTPS Example

If you have not changed the default HTTPS port on the Zyxel Device, then in your browser enter "https://Zyxel Device IP Address/" as the web site address where "Zyxel Device IP Address" is the IP address or domain name of the Zyxel Device you wish to access.

16.4.5.1 Google Chrome Warning Messages

When you attempt to access the Zyxel Device HTTPS server, you will see the error message shown in the following screen.

Figure 112 Security Alert Dialog Box (Google Chrome)



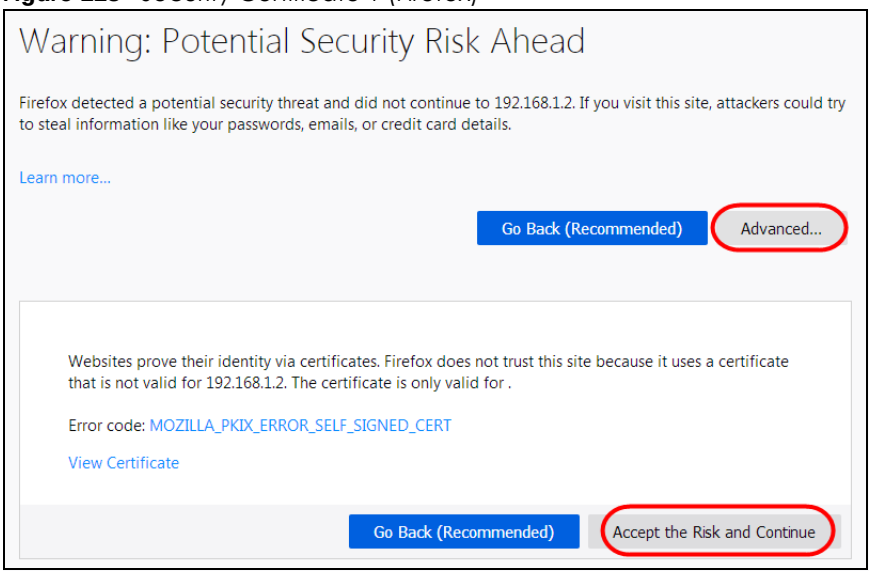
Select **Advanced** > **Proceed to 192.168.1.2 (unsafe)** to proceed to the Web Configurator login screen.

16.4.5.2 Mozilla Firefox Warning Messages

When you attempt to access the Zyxel Device HTTPS server, a Warning screen appears as shown in the following screen. Click **Learn More...** if you want to verify more information about the certificate from the Zyxel Device.

Click **Advanced** > **Accept the Risk and Continue**.

Figure 113 Security Certificate 1 (Firefox)



16.4.5.3 Avoiding Browser Warning Messages

Here are the main reasons your browser displays warnings about the Zyxel Device's HTTPS server certificate and what you can do to avoid seeing the warnings:

- The issuing certificate authority of the Zyxel Device's HTTPS server certificate is not one of the browser's trusted certificate authorities. The issuing certificate authority of the Zyxel Device's factory default certificate is the Zyxel Device itself since the certificate is a self-signed certificate.
- For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.
- To have the browser trust the certificates issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certificate. Refer to Appendix A on page 260 for details.

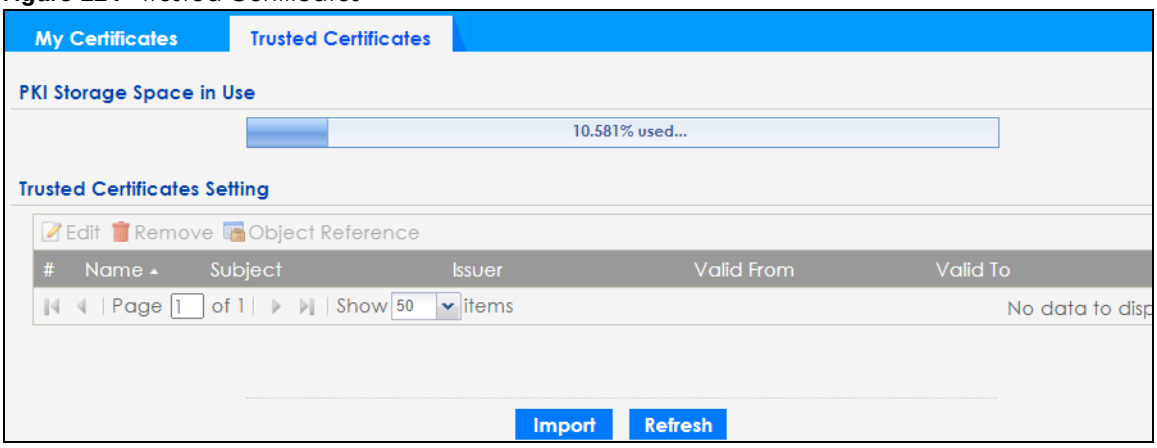
16.4.5.4 Enrolling and Importing SSL Client Certificates

The SSL client needs a certificate if **Authenticate Client Certificates** is selected on the Zyxel Device.

You must have imported at least one trusted CA to the Zyxel Device in order for the **Authenticate Client Certificates** to be active (see the Certificates chapter for details).

Apply for a certificate from a Certification Authority (CA) that is trusted by the Zyxel Device (see the Zyxel Device's **Trusted Certificates** Web Configurator screen).

Figure 114 Trusted Certificates



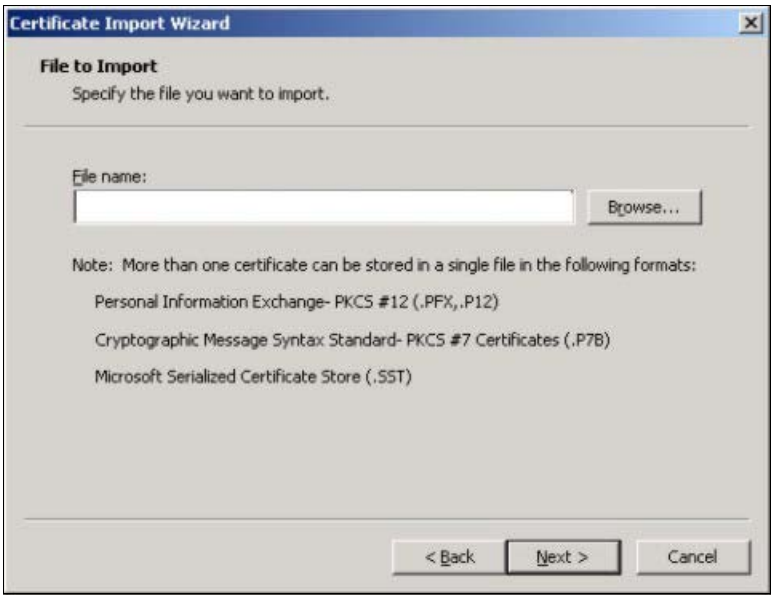
The CA sends you a package containing the CA's trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

16.4.5.5 Installing a Personal Certificate

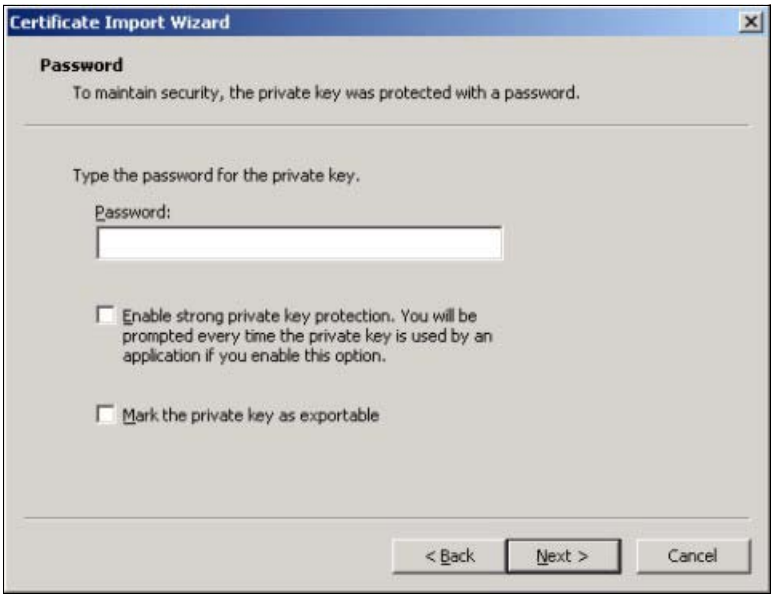
You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next.

1 Click **Next** to begin the wizard.

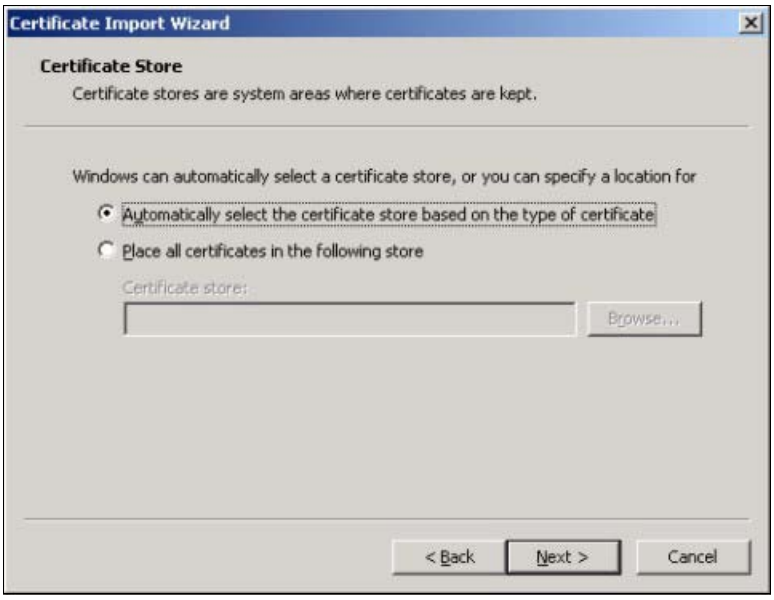
2 The file name and path of the certificate you double-clicked should automatically appear in the **File name** text box. Click **Browse** if you wish to import a different certificate.



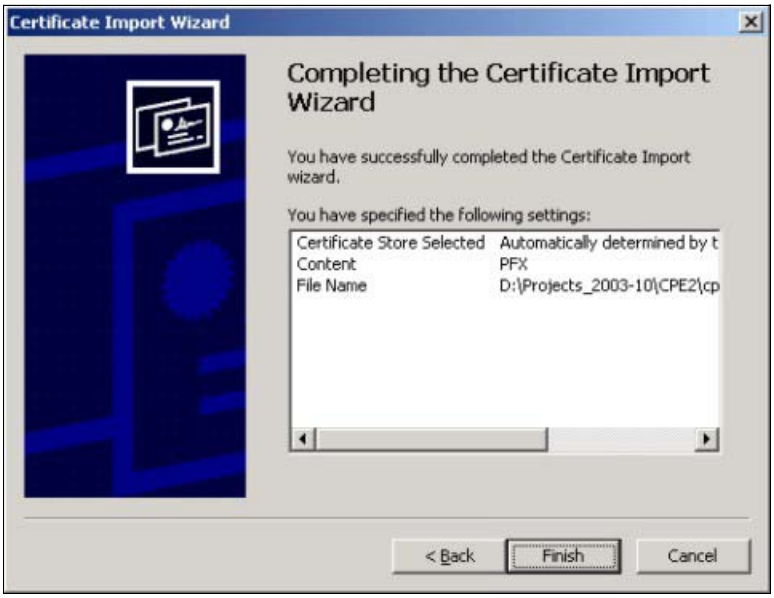
3 Enter the password given to you by the CA.



4 Have the wizard determine where the certificate should be saved on your computer or select **Place all certificates in the following store** and choose a different location.



5 Click **Finish** to complete the wizard and begin the import process.

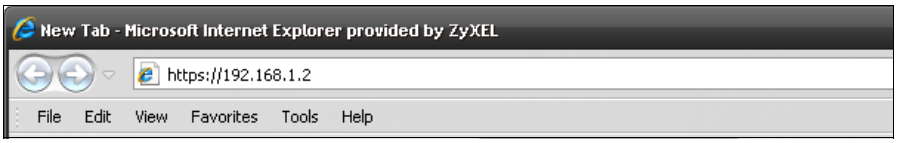


6 You should see the following screen when the certificate is correctly installed on your computer.

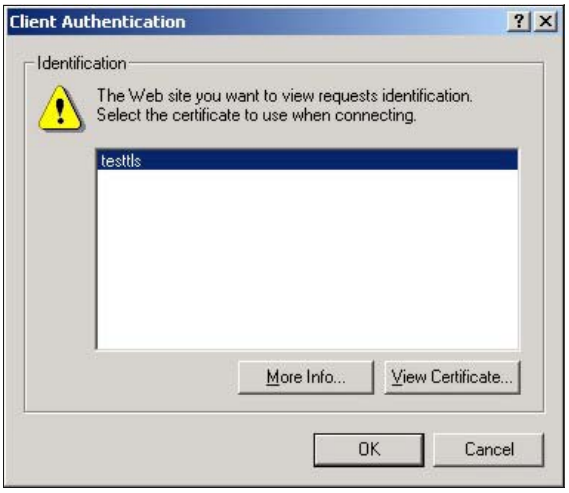
16.4.5.6 Using a Certificate When Accessing the Zyxel Device

To access the Zyxel Device through HTTPS:

1 Enter 'https://Zyxel Device IP Address/' in your browser's web address field.



2 When **Authenticate Client Certificates** is selected on the Zyxel Device, the following screen asks you to select a personal certificate to send to the Zyxel Device. This screen displays even if you only have a single certificate as in the example.



3 You next see the Web Configurator login screen.

16.5 SSH

You can use SSH (Secure SHell) to securely access the Zyxel Device's command line interface.

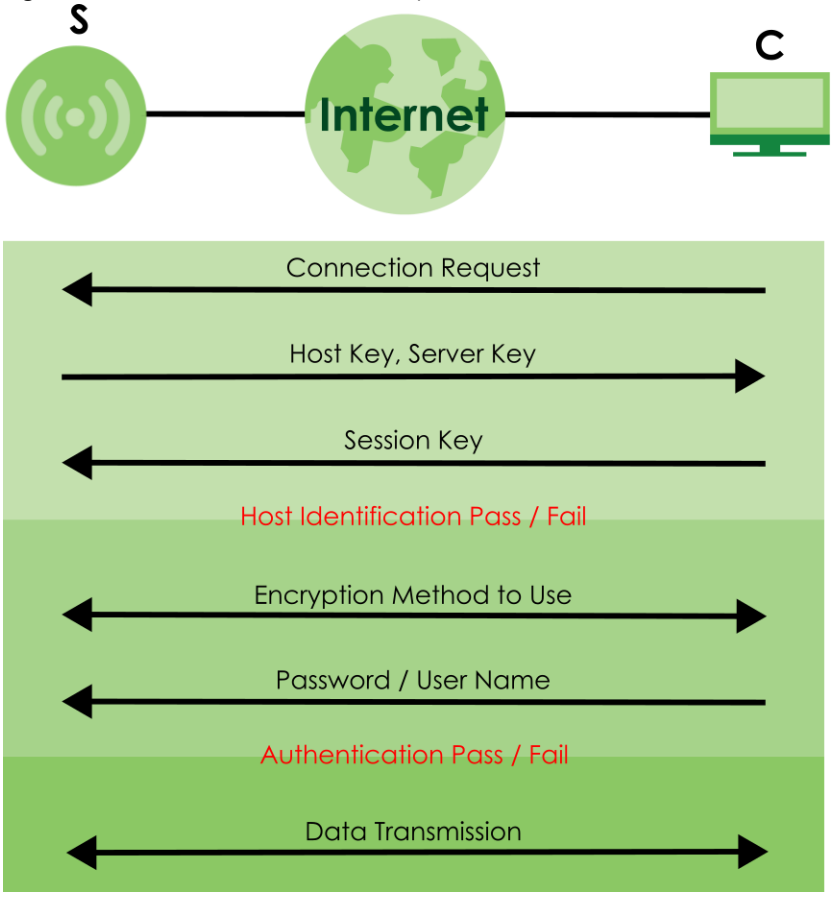
SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. In the following figure, the computer on the Internet uses SSH to securely connect (**SC**) to the Zyxel Device for a management session.

Figure 115 SSH Communication Over the WAN Example

16.5.1 How SSH Works

The following figure is an example of how a secure connection is established between two remote hosts using SSH v1.

Figure 116 How SSH v1 Works Example



1 Host Identification

The SSH client (**C**) sends a connection request to the SSH server (**S**). The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

16.5.2 SSH Implementation on the Zyxel Device

Your Zyxel Device supports SSH versions 1 and 2 using RSA authentication and four encryption methods (AES, 3DES, Archfour, and Blowfish). The SSH server is implemented on the Zyxel Device for management using port 22 (by default).

16.5.3 Requirements for Using SSH

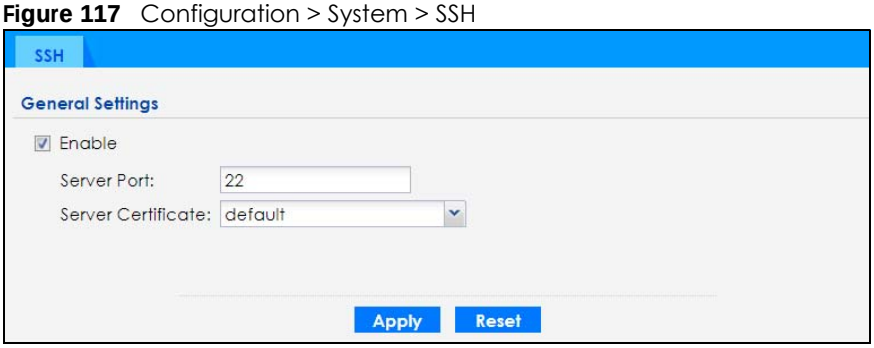
You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the Zyxel Device over SSH.

16.5.4 Configuring SSH

Click **Configuration > System > SSH** to open the following screen. Use this screen to configure your Zyxel Device's Secure Shell settings.

Note: It is recommended that you disable FTP when you configure SSH for secure connections.

Figure 117 Configuration > System > SSH



The following table describes the labels in this screen.

Table 76 Configuration > System > SSH

LABEL	DESCRIPTION
Enable	Select the checkbox to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the Zyxel Device CLI using this service. Note: The Zyxel Device uses only SSH version 2 protocol.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the Zyxel Device for SSH connections. You must have certificates already configured in the **My Certificates** screen.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

16.5.5 Examples of Secure Telnet Using SSH

This section shows two examples using a command interface and a graphical interface SSH client program to remotely access the Zyxel Device. The configuration and connection steps are similar for most SSH client programs. Refer to your SSH client program user's guide.

16.5.5.1 Example 1: Microsoft Windows

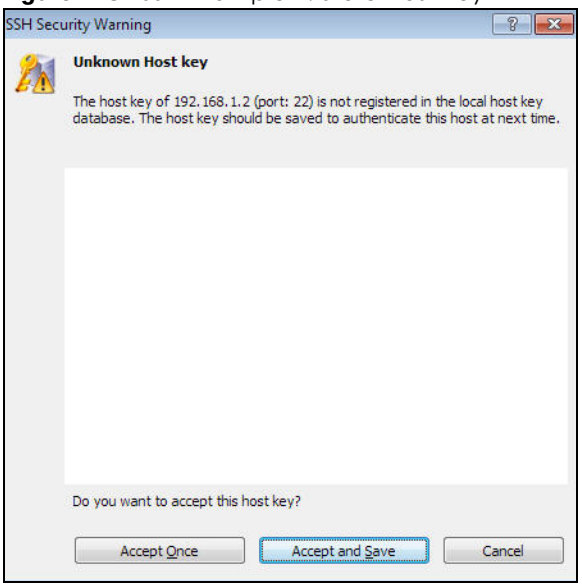
This section describes how to access the Zyxel Device using the Secure Shell Client program.

1 Launch the SSH client and specify the connection information (IP address, port number) for the Zyxel Device.

2 Configure the SSH client to accept connection using SSH version 2.

3 A window displays prompting you to store the host key in you computer. Click **Yes** to continue.

Figure 118 SSH Example 1: Store Host Key



Enter the password to log in to the Zyxel Device. The CLI screen displays next.

16.5.5.2 Example 2: Linux

This section describes how to access the Zyxel Device using the OpenSSH client program that comes with most Linux distributions.

1 Enter "`ssh -2 192.168.1.2`" at a terminal prompt and press [ENTER]. This command forces your computer to connect to the Zyxel Device using SSH version 1. If this is the first time you are connecting to the Zyxel Device using SSH, a message displays prompting you to save the host information of the Zyxel Device. Type "`yes`" and press [ENTER].

Then enter the password to log in to the Zyxel Device.

Figure 119 SSH Example 2: Log in

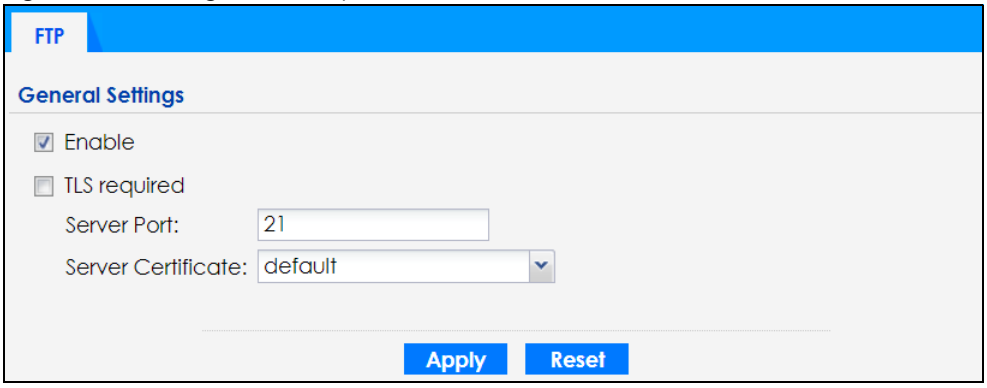
```
$ ssh -2 192.168.1.2
The authenticity of host '192.168.1.2 (192.168.1.2)' can't be established.
RSA1 key fingerprint is 21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.2' (RSA1) to the list of known hosts.
Administrator@192.168.1.2's password:
```

2 The CLI screen displays next.

16.6 FTP

You can upload and download the Zyxel Device's firmware and configuration files using FTP. To use this feature, your computer must have an FTP client. See Chapter 18 on page 210 for more information about firmware and configuration files. To change your Zyxel Device's FTP settings, click **Configuration > System > FTP** tab. The screen appears as shown. Use this screen to specify FTP settings.

Figure 120 Configuration > System > FTP



The following table describes the labels in this screen.

Table 77 Configuration > System > FTP

LABEL	DESCRIPTION
Enable	Select the checkbox to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the Zyxel Device using this service.
TLS required	Select the checkbox to use FTP over TLS (Transport Layer Security) to encrypt communication. This implements TLS as a security mechanism to secure FTP clients and/or servers.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the Zyxel Device for FTP connections. You must have certificates already configured in the **My Certificates** screen.
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 17
Log and Report

17.1 Overview

Use the system screens to configure daily reporting and log settings.

17.1.1 What You Can Do In this Chapter

- The **Log Setting** screens (Section 17.2 on page 204) specify which logs are emailed, where they are emailed, and how often they are emailed.

17.2 Log Setting

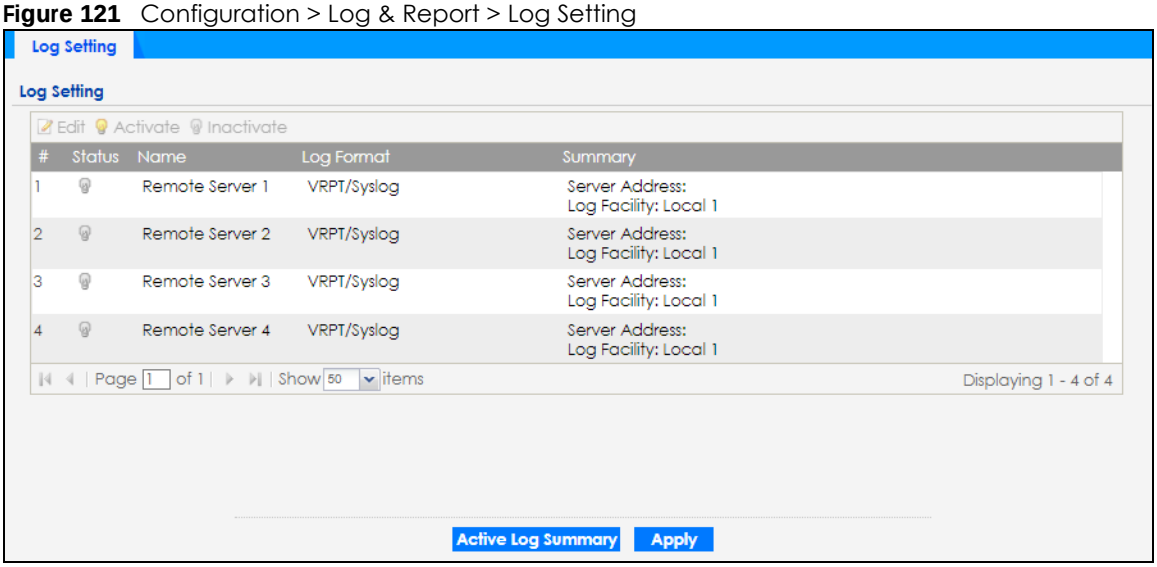
These screens control log messages and alerts. A log message stores the information for viewing (for example, in the **Monitor > View Log** screen). Usually, alerts are used for events that require more serious attention, such as system errors and attacks.

The **Log Setting** screen provides a summary of all the settings. You can use the **Edit Log Setting** screen to maintain the detailed settings (such as log categories, server names, etc.) for any log. Alternatively, if you want to edit what events is included in each log, you can also use the **Active Log Summary** screen to edit this information for all logs at the same time.

17.2.1 Log Setting Screen

To access this screen, click **Configuration > Log & Report > Log Setting**.

Figure 121 Configuration > Log & Report > Log Setting



The following table describes the labels in this screen.

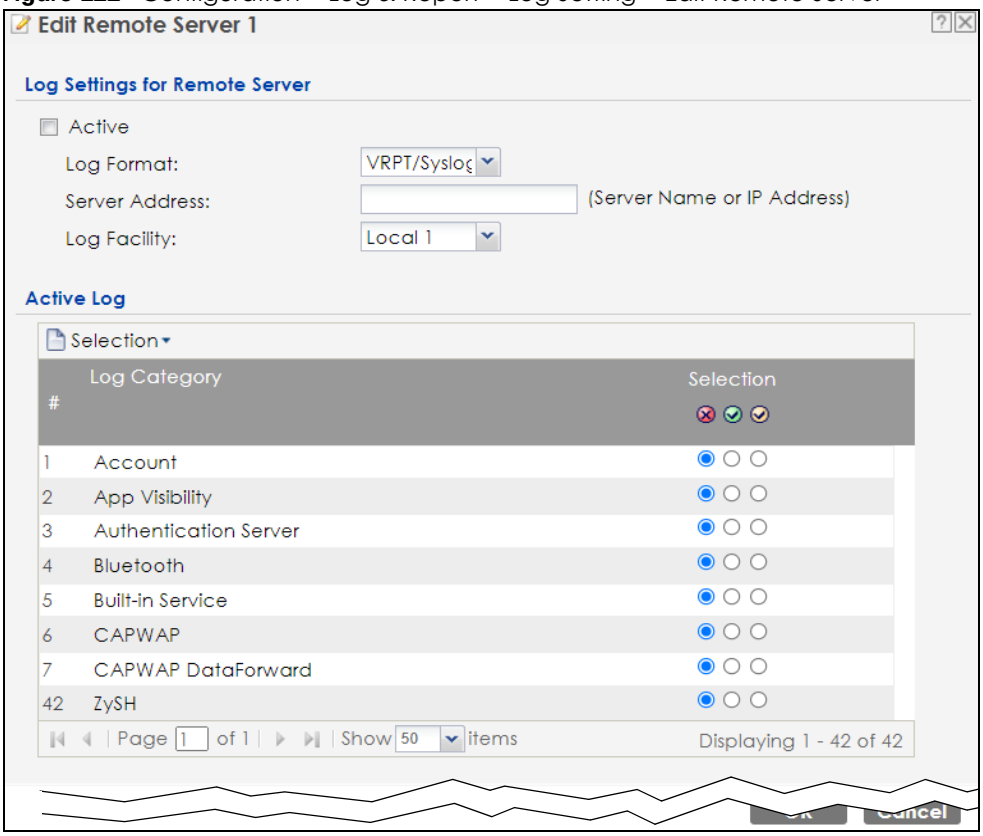
Table 78 Configuration > Log & Report > Log Setting

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
#	This field is a sequential value, and it is not associated with a specific log.
Status	This field shows whether the log is active or not.
Name	This field displays the name of the log (system log or one of the remote servers).
Log Format	This field displays the format of the log. **Internal** - system log; you can view the log on the **View Log** tab. **VRPT/Syslog** - Zyxel's Vantage Report, syslog-compatible format. **CEF/Syslog** - Common Event Format, syslog-compatible format.
Summary	This field is a summary of the settings for each log.
Active Log Summary	Click this button to open the **Active Log Summary** screen.
Apply	Click this button to save your changes (activate and deactivate logs) and make them take effect.

17.2.2 Edit Remote Server

This screen controls the settings for each log in the remote server (syslog). Select a remote server entry in the **Log Setting** screen and click the **Edit** icon.

Figure 122 Configuration > Log & Report > Log Setting > Edit Remote Server



The following table describes the labels in this screen.

Table 79 Configuration > Log & Report > Log Setting > Edit Remote Server

LABEL	DESCRIPTION
Log Settings for Remote Server	
Active	Select this checkbox to send log information according to the information in this section. You specify what kinds of messages are included in log information in the **Active Log** section.
Log Format	This field displays the format of the log information. It is read-only. **VRPT/Syslog** - Zyxel's Vantage Report, syslog-compatible format. **CEF/Syslog** - Common Event Format, syslog-compatible format.
Server Address	Type the server name or the IP address of the syslog server to which to send log information.
Log Facility	Select a log facility. The log facility allows you to log the messages to different files in the syslog server. Please see the documentation for your syslog program for more information.
Active Log	
Selection	Use the **Selection** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not send the remote server logs for any log category. **enable normal logs** (green check mark) - send the remote server log messages and alerts for all log categories. **enable normal logs and debug logs** (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
#	This field is a sequential value, and it is not associated with a specific address.

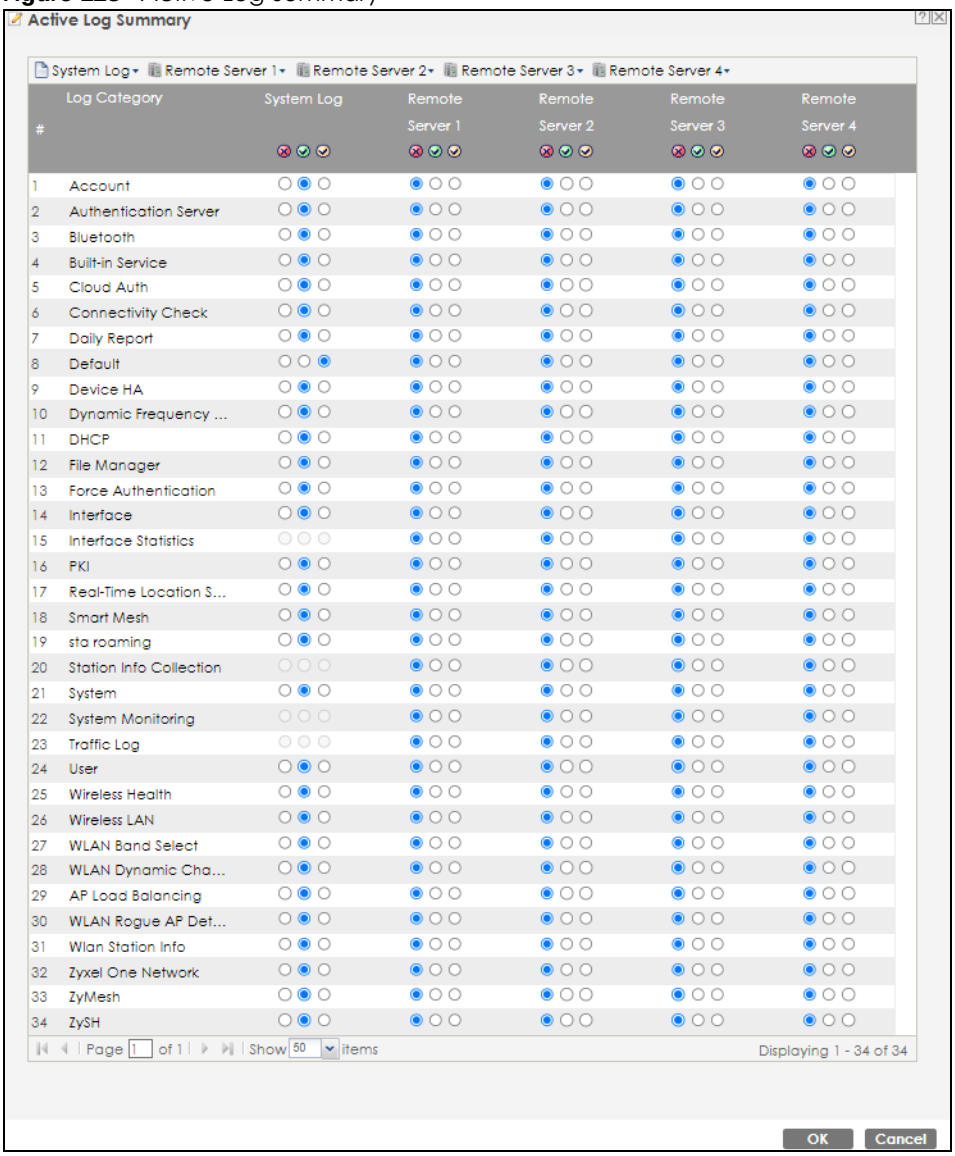
Table 79 Configuration > Log & Report > Log Setting > Edit Remote Server (continued)

LABEL	DESCRIPTION
Log Category	This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.
Selection	Select what information you want to log from each **Log Category** (except **All Logs**; see below). Choices are: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green checkmark) - log regular information and alerts from this category **enable normal logs and debug logs** (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

17.2.3 Active Log Summary

This screen allows you to view and to edit what information is included in the system log and remote servers at the same time. It does not let you change other log settings. To access this screen, go to the **Log Setting** screen, and click the **Active Log Summary** button.

Figure 123 Active Log Summary



This screen provides a different view and a different way of indicating which messages are included in each log and each alert. (The **Default** category includes debugging messages generated by open source software.)

The following table describes the fields in this screen.

Table 80 Configuration > Log & Report > Log Setting > Active Log Summary

LABEL	DESCRIPTION
Active Log Summary	If the Zyxel Device is set to controller mode, the AC section controls logs generated by the controller and the AP section controls logs generated by the managed APs.
System log	Use the **System Log** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not log any information for any category for the system log or email any logs to email server 1 or 2. **enable normal logs** (green check mark) - create log messages and alerts for all categories for the system log. If email server 1 or 2 also has normal logs enabled, the Zyxel Device will email logs to them. **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information for all categories. The Zyxel Device does not email debugging information, even if this setting is selected.
Remote Server 1~4	For each remote server, use the **Selection** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not send the remote server logs for any log category. **enable normal logs** (green check mark) - send the remote server log messages and alerts for all log categories. **enable normal logs and debug logs** (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
#	This field is a sequential value, and it is not associated with a specific address.
Log Category	This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.
System log	Select which events you want to log by **Log Category**. There are three choices: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green checkmark) - create log messages and alerts from this category **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information from this category; the Zyxel Device does not email debugging information, however, even if this setting is selected.
Remote Server 1~4 Syslog	For each remote server, select what information you want to log from each **Log Category** (except **All Logs**; see below). Choices are: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green checkmark) - log regular information and alerts from this category **enable normal logs and debug logs** (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

CHAPTER 18
File Manager

18.1 Overview

Configuration files define the Zyxel Device's settings. Shell scripts are files of commands that you can store on the Zyxel Device and run when you need them. You can apply a configuration file or run a shell script without the Zyxel Device restarting. You can store multiple configuration files and shell script files on the Zyxel Device. You can edit configuration files or shell scripts in a text editor and upload them to the Zyxel Device. Configuration files use a .conf extension and shell scripts use a .zysh extension.

18.1.1 What You Can Do in this Chapter

- The **Configuration File** screen (Section 18.2 on page 213) stores and names configuration files. You can also download and upload configuration files.
- The **Firmware Package** screen (Section 18.3 on page 217) checks your current firmware version and uploads firmware to the Zyxel Device.
- The **Shell Script** screen (Section 18.4 on page 221) stores, names, downloads, uploads and runs shell script files.

18.1.2 What you Need to Know

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

Configuration Files and Shell Scripts

When you apply a configuration file, the Zyxel Device uses the factory default settings for any features that the configuration file does not include. When you run a shell script, the Zyxel Device only applies the commands that it contains. Other settings do not change.

These files have the same syntax, which is also identical to the way you run CLI commands manually. An example is shown below.

Figure 124 Configuration File / Shell Script: Example

```
# enter configuration mode
configure terminal
# change administrator password
username admin password 4321 user-type admin
#configure default radio profile, change 2GHz channel to 11 & Tx output
power # to 50%
wlan-radio-profile default
2g-channel 11
output-power 50%
exit
write
```

While configuration files and shell scripts have the same syntax, the Zyxel Device applies configuration files differently than it runs shell scripts. This is explained below.

Table 81 Configuration Files and Shell Scripts in the Zyxel Device

Configuration Files (.conf)	Shell Scripts (.zysh)
• Resets to default configuration. • Goes into CLI **Configuration** mode. • Runs the commands in the configuration file.	• Goes into CLI **Privilege** mode. • Runs the commands in the shell script.

You have to run the aforementioned example as a shell script because the first command is run in **Privilege** mode. If you remove the first command, you have to run the example as a configuration file because the rest of the commands are executed in **Configuration** mode.

Errors in Configuration Files or Shell Scripts

When you apply a configuration file or run a shell script, the Zyxel Device processes the file line-by-line. The Zyxel Device checks the first line and applies the line if no errors are detected. Then it continues with the next line. If the Zyxel Device finds an error, it stops applying the configuration file or shell script and generates a log.

You can change the way a configuration file or shell script is applied. Include `setenv stop-on-error off` in the configuration file or shell script. The Zyxel Device ignores any errors in the configuration file or shell script and applies all of the valid commands. The Zyxel Device still generates a log for any errors.

Sub commands in Configuration Files or Shell Scripts

In a configuration file or shell script, sub commands are used to further define commands.

In the following example, the commands change the SSID name to "Alice-AP" on the Zyxel Device:

```
configure terminal
wlan-ssid-profile default
ssid Joe-AP
exit
write
```

- Line 1: Enter **Configuration** mode: `configure terminal`
- Line 2: Enter SSID profile (and enter sub command mode): `wlan-ssid-profile default`
- Line 3: Configure the SSID name: `ssid Joe-AP`
- Line 4: Exit sub command mode: `exit`
- Line 5: Save the configuration: `write`

Your configuration files or shell scripts can use "exit" or a command line consisting of a single "!" to have the Zyxel Device exit sub command mode.

Note: "exit" or "!'" must follow sub commands if it is to make the Zyxel Device exit sub command mode.

Sensitive Data Protection

The Zyxel Device by default encrypts local admin and user account passwords for web configurator and CLI.

Enable **Sensitive Data Protection** to have the Zyxel Device use a private key to encrypt local admin and user account passwords for web configurator and CLI.

Note: You can only upload configuration files using FTP that are using the current private key of the Zyxel Device.

The following examples describe the situations you might come across using **Sensitive Data Protection**.

Example 1:

1. Download a configuration file (file1).
2. Enable **Sensitive Data Protection**.
3. Create a private key (key1).
4. When you upload file1 to the Zyxel Device through the Zyxel Device web configurator, you do not need to enter the private key (key1). Configuration file1 is not encrypted by the private key (key1).

Example2:

1. Enable **Sensitive Data Protection**.
2. Create an private key (key1).
3. Download a configuration file (file2).
4. You must use key1 to upload file2 to the Zyxel Device because file2 is encrypted by key1.

Example 3:

1. Change the private key from key1 to key2.
2. Download another configuration file (file3).
3. You must use key2 to upload file3 to the Zyxel Device.

Note: You must still use key1 to upload file2 to the Zyxel Device. Make a note of the key to use when you change the private key and then download a configuration file.

Example 4:

1. Enable **Sensitive Data Protection** on Zyxel Device1 and create a private key.
2. Download a configuration file from Zyxel Device1.
3. You must upload this configuration file using the private key you created on Zyxel Device1 to Zyxel Device2 even if **Sensitive Data Protection** is not enabled on Zyxel Device2.

18.2 Configuration File

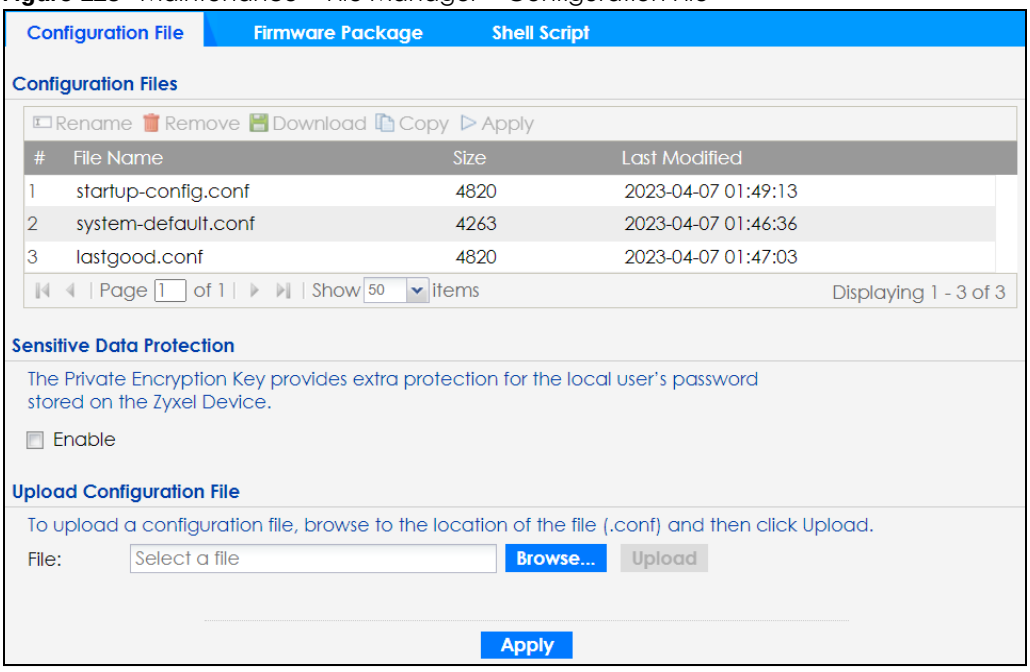
Click **Maintenance > File Manager > Configuration File** to open this screen. Use the **Configuration File** screen to store, run, and name configuration files. You can also download configuration files from the Zyxel Device to your computer and upload configuration files from your computer to the Zyxel Device.

Once your Zyxel Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making further configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Configuration File Flow at Restart

- If there is not a **startup-config.conf** when you restart the Zyxel Device (whether through a management interface or by physically turning the power off and back on), the Zyxel Device uses the **system-default.conf** configuration file with the Zyxel Device's default settings.
- If there is a **startup-config.conf**, the Zyxel Device checks it for errors and applies it. If there are no errors, the Zyxel Device uses it and copies it to the **lastgood.conf** configuration file as a back up file. If there is an error, the Zyxel Device generates a log and copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file. If there isn't a **lastgood.conf** configuration file or it also has an error, the Zyxel Device applies the **system-default.conf** configuration file.
- You can change the way the **startup-config.conf** file is applied. Include the `setenv-startup stop-on-error off` command. The Zyxel Device ignores any errors in the **startup-config.conf** file and applies all of the valid commands. The Zyxel Device still generates a log for any errors.

Figure 125 Maintenance > File Manager > Configuration File



Do not turn off the Zyxel Device while configuration file upload is in progress.

The following table describes the labels in this screen.

Table 82 Maintenance > File Manager > Configuration File

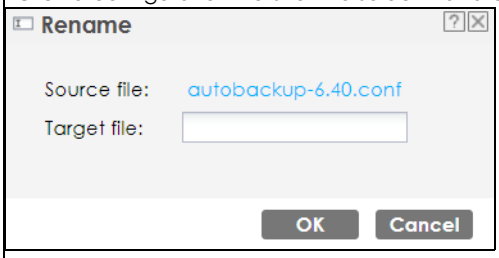
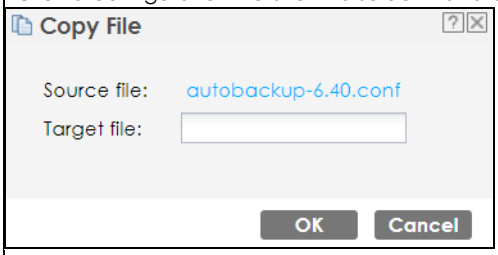
LABEL	DESCRIPTION
Configuration Files	
Rename	Use this button to change the label of a configuration file on the Zyxel Device. You can only rename manually saved configuration files. You cannot rename the **lastgood.conf**, **system-default.conf** and **startup-config.conf** files. You cannot rename a configuration file to the name of another configuration file in the Zyxel Device. Click a configuration file's row to select it and click **Rename** to open the **Rename File** screen.  Specify the new name for the configuration file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Remove	Click a configuration file's row to select it and click **Remove** to delete it from the Zyxel Device. You can only delete manually saved configuration files. You cannot delete the **system-default.conf**, **startup-config.conf** and **lastgood.conf** files. A pop-up window asks you to confirm that you want to delete the configuration file. Click **OK** to delete the configuration file or click **Cancel** to close the screen without deleting the configuration file.
Download	Click a configuration file's row to select it and click **Download** to save the configuration to your computer.
Copy	Use this button to save a duplicate of a configuration file on the Zyxel Device. Click a configuration file's row to select it and click **Copy** to open the **Copy File** screen.  Specify a name for the duplicate configuration file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.

Table 82 Maintenance > File Manager > Configuration File (continued)

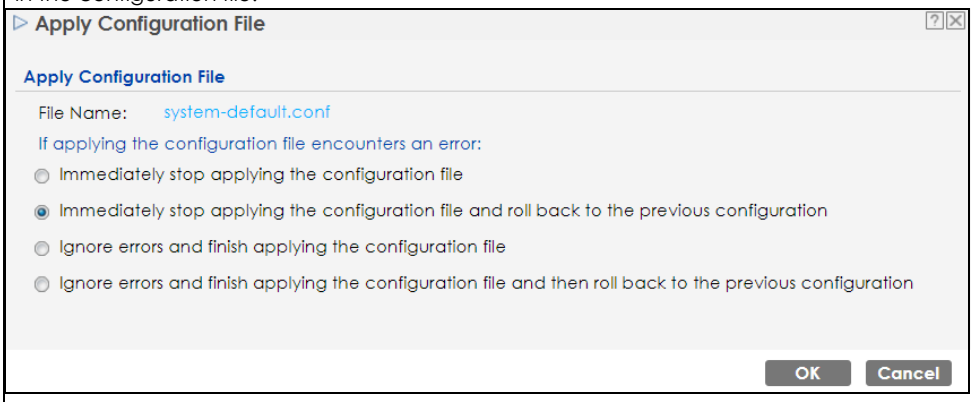
LABEL	DESCRIPTION
Apply	Use this button to have the Zyxel Device use a specific configuration file. Click a configuration file's row to select it and click **Apply** to have the Zyxel Device use that configuration file. The Zyxel Device does not have to restart in order to use a different configuration file, although you will need to wait for a few minutes while the system reconfigures. The following screen gives you options for what the Zyxel Device is to do if it encounters an error in the configuration file.  **Immediately stop applying the configuration file** - this is not recommended because it would leave the rest of the configuration blank. If the interfaces were not configured before the first error, the console port may be the only way to access the Zyxel Device. **Immediately stop applying the configuration file and roll back to the previous configuration** - this gets the Zyxel Device started with a fully valid configuration file as quickly as possible. **Ignore errors and finish applying the configuration file** - this applies the valid parts of the configuration file and generates error logs for all of the configuration file's errors. This lets the Zyxel Device apply most of your configuration and you can refer to the logs for what to fix. **Ignore errors and finish applying the configuration file and then roll back to the previous configuration** - this applies the valid parts of the configuration file, generates error logs for all of the configuration file's errors, and starts the Zyxel Device with a fully valid configuration file. Click **OK** to have the Zyxel Device start applying the configuration file or click **Cancel** to close the screen.
#	This column displays the number for each configuration file entry. This field is a sequential value, and it is not associated with a specific address. The total number of configuration files that you can save depends on the sizes of the configuration files and the available flash storage space.
File Name	This column displays the label that identifies a configuration file. You cannot delete the following configuration files or change their file names. The **system-default.conf** file contains the Zyxel Device's default settings. Select this file and click **Apply** to reset all of the Zyxel Device settings to the factory defaults. This configuration file is included when you upload a firmware package. The **startup-config.conf** file is the configuration file that the Zyxel Device is currently using. If you make and save changes during your management session, the changes are applied to this configuration file. The Zyxel Device applies configuration changes made in the Web Configurator to the configuration file when you click **Apply** or **OK**. It applies configuration changes made through CLI commands when you use the `write` command. The **lastgood.conf** is the most recently used (valid) configuration file that was saved when the Zyxel Device last restarted. If you upload and apply a configuration file with an error, you can apply **lastgood.conf** to return to a valid configuration.
Size	This column displays the size (in KB) of a configuration file.

Table 82 Maintenance > File Manager > Configuration File (continued)

LABEL	DESCRIPTION
Last Modified	This column displays the date and time that the individual configuration files were last changed or saved.
Sensitive Data Protection	
Enable	Select this to enable Sensitive Data Protection; see Section 18.1 on page 210 for more information. You need this key to upload configuration files. Write down the key you set and keep it in a safe place. **Figure 126** Upload Configuration File 
Enter Private Encryption Key	Enter the encryption key in this field. The encryption key should be 4-8 single byte printable characters, including 0-9a-zA-Z`~!@#$%^&*()_-+={}|\\;:'<,>./]|.
Re-enter Private Encryption Key	Enter the encryption key again in this field.
Upload Configuration File The bottom part of the screen allows you to upload a new or previously saved configuration file from your computer to your Zyxel Device. You cannot upload a configuration file named **system-default.conf** or **lastgood.conf**. If you upload **startup-config.conf**, it will replace the current configuration and immediately apply the new settings.	
File	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the .conf file you want to upload. The configuration file must use a ".conf" filename extension. You will receive an error message if you try to upload a fie of a different format. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

18.2.1 Example of Configuration File Download Using FTP

The following example gets a configuration file named startup-config.conf from the Zyxel Device and saves it on the computer.

1 Connect your computer to the Zyxel Device.

2 The FTP server IP address of the Zyxel Device in standalone mode is 192.168.1.2, so set your computer to use a static IP address from 192.168.1.3 ~192.168.1.254.

3 Use an FTP client on your computer to connect to the Zyxel Device. For example, in the Windows command prompt, type `ftp 192.168.1.2`. Keep the console session connected in order to see when the firmware recovery finishes.

4 Enter your user name when prompted.

5 Enter your password as requested.

6 Use "cd" to change to the directory that contains the files you want to download.

7 Use "dir" or "ls" if you need to display a list of the files in the directory.

8 Use "get" to download files. Transfer the configuration file on the Zyxel Device to your computer. Type `get` followed by the name of the configuration file. This examples uses `get startup-config.conf`.

```
C:\>ftp 192.168.1.2
Connected to 192.168.1.2.
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 5 allowed.
220-Local time is now 21:28. Server port: 21.
220-This is a private system - No anonymous login
220 You will be disconnected after 600 minutes of inactivity.
User (192.168.1.2:(none)): admin
331 User admin OK. Password required
Password:
230 OK. Current restricted directory is /
ftp> cd conf
250 OK. Current directory is /conf
ftp> ls
200 PORT command successful
150 Connecting to port 5001
lastgood.conf
startup-config.conf
system-default.conf
226 3 matches total
ftp: 57 bytes received in 0.33Seconds 0.17Kbytes/sec.
ftp> get startup-config.conf
200 PORT command successful
150 Connecting to port 5002
226-File successfully transferred
226 0.002 seconds (measured here), 1.66 Mbytes per second
ftp: 2928 bytes received in 0.02Seconds 183.00Kbytes/sec.
ftp>
```

9 Wait for the file transfer to complete.

10 Enter "quit" to exit the ftp prompt.

18.3 Firmware Package

Click **Maintenance > File Manager > Firmware Package** to open this screen. Use the **Firmware Package** screen to check your current firmware version and upload firmware to the Zyxel Device.

Note: The Web Configurator is the recommended method for uploading firmware. You only need to use the command line interface if you need to recover the firmware. See the CLI Reference Guide for how to determine if you need to recover the firmware and how to recover it.

You can manually download the new firmware from the Zyxel website, or you can click **Check Now** to automatically find the latest firmware for your Zyxel Device (recommended).

The firmware update can take up to five minutes. Do not turn off or reset the Zyxel Device while the firmware update is in progress!

Figure 127 Maintenance > File Manager > Firmware Package

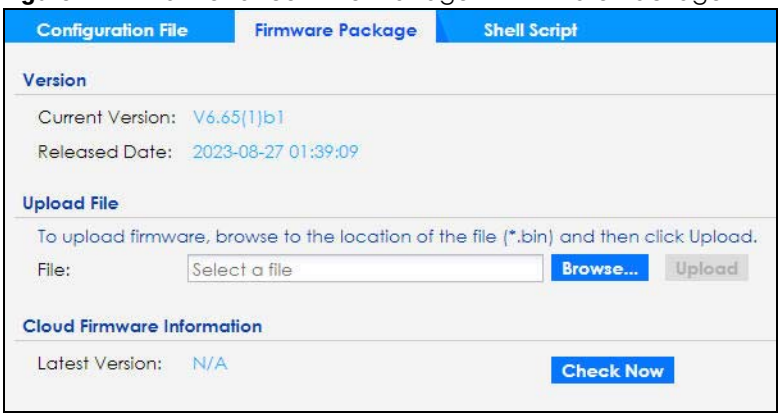


Figure 128 Maintenance > File Manager > Firmware Package > Check now

The following table describes the labels in this screen.

Table 83 Maintenance > File Manager > Firmware Package

LABEL	DESCRIPTION
Current Version	This is the firmware version and the date created.
Released Date	This is the date that the version of the firmware was created.
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.
Check now	Click **Check now** to view the firmware information. The following message appears when there is a new firmware version available for your Zyxel Device.

Table 83 Maintenance > File Manager > Firmware Package (continued)

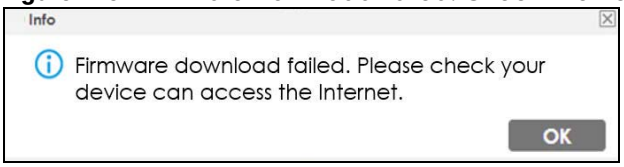
LABEL	DESCRIPTION
New firmware version	This is the new firmware version available for your Zyxel Device. V6.60 is the firmware trunk version and the number in brackets is the release number. 0 is the first release of this version firmware. 1 is the next update release of this version firmware.
Your device current version	This is the current firmware version of your Zyxel Device.
Firmware enhancements	Click **Release Notes** to view the firmware release information of the new firmware, including new features, enhancements and bug fix.
Don't remind for 7 days	Select this to stop receiving this notification for the next 7 days.
upgrade now	Click this to start upgrading your Zyxel Device to the new firmware version.
close	Click this to exit this screen without upgrading your Zyxel Device to the new firmware version.
	The following message appears when the Zyxel Device is checking the latest firmware version available on the cloud server. If it is later than your current firmware version on the Zyxel Device, you will be prompted to download it. 

Firmware Download Failed

The following pop-up messages display the causes and solutions for firmware download failure.

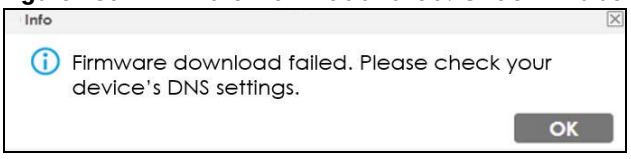
Firmware download failed due to an Internet error. Refer to Section 25.4 on page 255 for more information.

Figure 129 Firmware Download Failed. Check Internet Access.



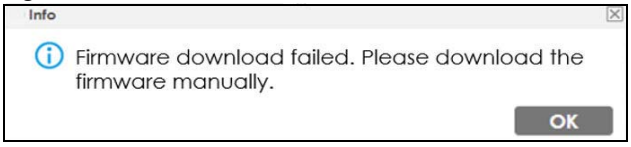
Firmware download failed due to a DNS problem. Please check your device's DNS settings.

Figure 130 Firmware Download failed. Check DNS Settings.



Firmware download failed. Download the new firmware manually from the Zyxel website. Then, go to the **Maintenance** > **File Manager** > **Firmware Package** screen to upload the new firmware.

Figure 131 Firmware Download Failed. Download Manually.

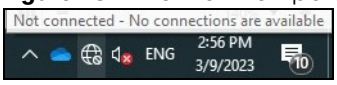


After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the Zyxel Device again.

Note: The Zyxel Device automatically reboots after a successful upload.

The Zyxel Device automatically restarts causing a temporary network disconnect to devices connected to its network. In some operating systems, you may see the following icon on your desktop.

Figure 132 Network Temporarily Disconnected



After five minutes, log in again and check your new firmware version in the **Dashboard** screen.

18.3.1 Example of Firmware Upload Using FTP

This procedure requires the Zyxel Device's firmware. Download the firmware package from www.zyxel.com and unzip it. The firmware file uses a .bin extension, for example, "600ABFH0C0.bin". Do the following after you have obtained the firmware file.

1. Connect your computer to the Zyxel Device.
2. The FTP server IP address of the Zyxel Device in standalone mode is 192.168.1.2, so set your computer to use a static IP address from 192.168.1.3 - 192.168.1.254.
3. Use an FTP client on your computer to connect to the Zyxel Device. For example, in the Windows command prompt, type `ftp 192.168.1.2`. Keep the console session connected in order to see when the firmware recovery finishes.
4. Enter your user name when prompted.
5. Enter your password as requested.
6. Enter "hash" for FTP to print a `#' character for every 1024 bytes of data you upload so that you can watch the file transfer progress.
7. Enter "bin" to set the transfer mode to binary.
8. Transfer the firmware file from your computer to the Zyxel Device. Type `put` followed by the path and name of the firmware file. This examples uses `put C:\ftproot\Zyxel Device_FW\600ABFH0C0.bin`.

```
C:\>ftp 192.168.1.2
Connected to 192.168.1.2.
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 5 allowed.
220-Local time is now 21:28. Server port: 21.
220-This is a private system - No anonymous login
220 You will be disconnected after 600 minutes of inactivity.
User (192.168.1.2:(none)): admin
331 User admin OK. Password required
Password:
230 OK. Current restricted directory is /
ftp> hash
Hash mark printing On  ftp: (2048 bytes/hash mark) .
ftp> bin
200 TYPE is now 8-bit binary
ftp> put C:\ftproot\Zyxel Device_FW\600ABFH0C0.bin
```

Note: The Zyxel Device will not upgrade the firmware if the firmware file you upload is incompatible with the Zyxel Device.

9 Wait for the file transfer to complete.

10 Enter "quit" to exit the ftp prompt.

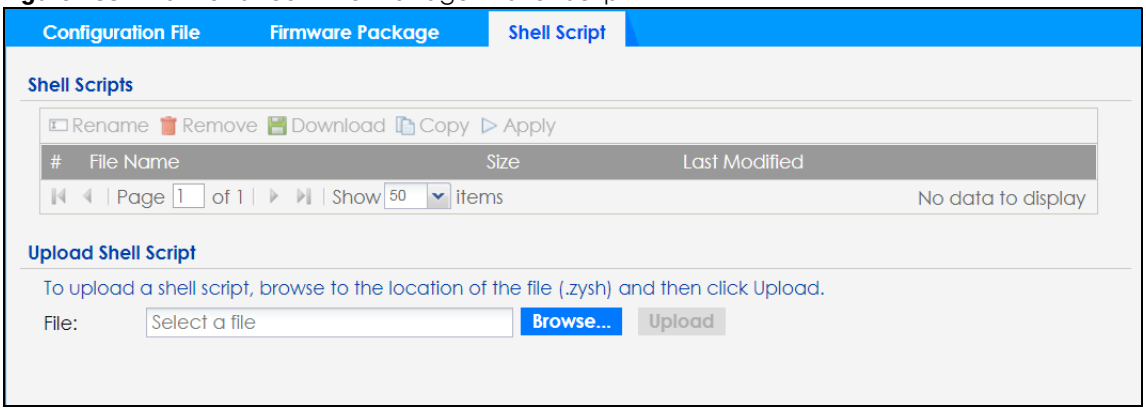
18.4 Shell Script

Use shell script files to have the Zyxel Device use commands that you specify. Use a text editor to create the shell script files. They must use a ".zysh" filename extension.

Click **Maintenance > File Manager > Shell Script** to open this screen. Use the **Shell Script** screen to store, name, download, upload and run shell script files. You can store multiple shell script files on the Zyxel Device at the same time.

Note: You should include `write` commands in your scripts. If you do not use the `write` command, the changes will be lost when the Zyxel Device restarts. You could use multiple `write` commands in a long script.

Figure 133 Maintenance > File Manager > Shell Script



Each field is described in the following table.

Table 84 Maintenance > File Manager > Shell Script

LABEL	DESCRIPTION
Shell Scripts	
Rename	Use this button to change the label of a shell script file on the Zyxel Device. You cannot rename a shell script to the name of another shell script in the Zyxel Device. Click a shell script's row to select it and click **Rename** to open the **Rename File** screen. Specify the new name for the shell script file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.

Table 84 Maintenance > File Manager > Shell Script (continued)

LABEL	DESCRIPTION
Remove	Click a shell script file's row to select it and click **Delete** to delete the shell script file from the Zyxel Device. A pop-up window asks you to confirm that you want to delete the shell script file. Click **OK** to delete the shell script file or click **Cancel** to close the screen without deleting the shell script file.
Download	Click a shell script file's row to select it and click **Download** to save the configuration to your computer.
Copy	Use this button to save a duplicate of a shell script file on the Zyxel Device. Click a shell script file's row to select it and click **Copy** to open the **Copy File** screen. Specify a name for the duplicate file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Apply	Use this button to have the Zyxel Device use a specific shell script file. Click a shell script file's row to select it and click **Apply** to have the Zyxel Device use that shell script file. You may need to wait awhile for the Zyxel Device to finish applying the commands.
#	This column displays the number for each shell script file entry.
File Name	This column displays the label that identifies a shell script file.
Size	This column displays the size (in KB) of a shell script file.
Last Modified	This column displays the date and time that the individual shell script files were last changed or saved.
Upload Shell Script The bottom part of the screen allows you to upload a new or previously saved shell script file from your computer to your Zyxel Device.	
File	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the .zysh file you want to upload.
Upload	Click **Upload** to begin the upload process. This process may take up to several minutes.

CHAPTER 19
Diagnostics

19.1 Overview

Use the diagnostics screen for troubleshooting.

19.1.1 What You Can Do in this Chapter

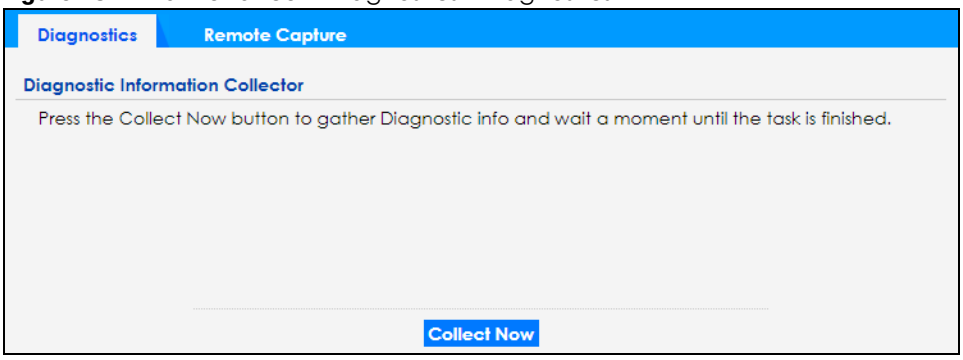
- The **Diagnostics** screen (Section 19.2 on page 223) generates a file containing the Zyxel Device's configuration and diagnostic information if you need to provide it to customer support during troubleshooting.
- The **Remote Capture** screen (Section 19.3 on page 224) enables remote packet captures on wired or wireless interfaces through an external packet analyzer.

19.2 Diagnostics

This screen provides an easy way for you to generate a file containing the Zyxel Device's configuration and diagnostic information. You may need to generate this file and send it to customer support during troubleshooting. All categories of settings and shell script files stored on the Zyxel Device will be included in the diagnostic file.

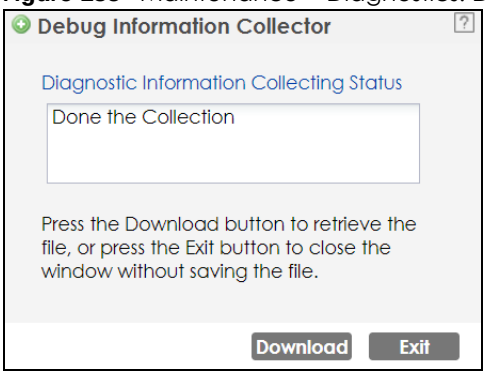
Click **Maintenance > Diagnostics> Diagnostics** to open the **Diagnostics** screen. Click **Collect Now** to have the Zyxel Device create a new diagnostic file.

Figure 134 Maintenance > Diagnostics> Diagnostics



The **Debug Information Collector** screen then displays showing whether the collection is in progress, was successful, or has failed. When the data collection is done, click **Download** to save the most recent diagnostic file to a computer.

Figure 135 Maintenance > Diagnostics: Debug Information Collector

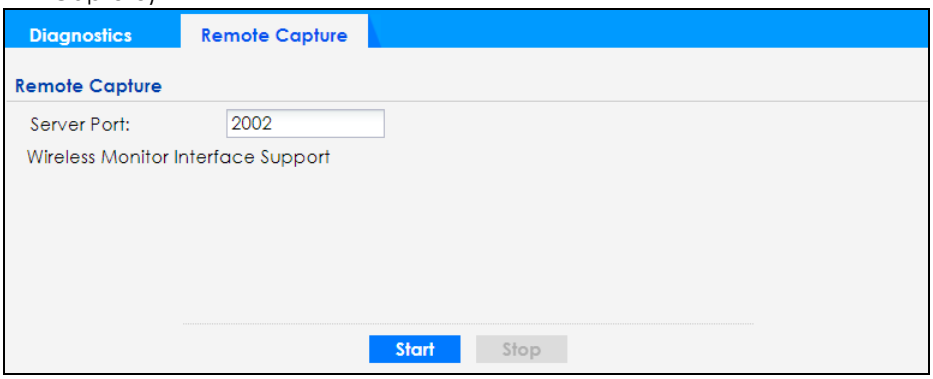


19.3 Remote Capture

Use this screen to capture network traffic going through the Zyxel Device and output the captured packets to a packet analyzer (also known as network or protocol analyzer) such as Wireshark. If the Zyxel Device is connected to the Zyxel gateway or ZyWALL, you might need to configure the Zyxel gateway or ZyWALL to allow remote capture on the Zyxel Device.

Click **Maintenance > Diagnostics > Remote Capture** to open the **Remote Capture** screen.

Figure 136 Maintenance > Diagnostics > Remote Capture (Zyxel Device that supports Wireless Remote Capture)



The following table describes the labels in this screen.

Table 85 Maintenance > Diagnostics > Remote Capture

LABEL	DESCRIPTION
Server Port	Enter the number of the server port you want the packet analyzer to connect to in order to capture traffic going through the Zyxel Device. The default port number is 2002.
Start	Click this button to allow the packet analyzer to start capturing traffic going through the Zyxel Device.
Stop	Click this button to stop the packet analyzer from capturing traffic going through the Zyxel Device.

CHAPTER 20
LEDs

20.1 Overview

The LEDs of your Zyxel Device can be controlled such that they stay lit (ON) or OFF after the Zyxel Device is ready. There are two features that control the LEDs of your Zyxel Device – **Locator** and **Suppression**.

Note: Not all Zyxel Devices have LEDs; see Section 3.2 on page 29 for more information.

20.1.1 What You Can Do in this Chapter

- The **Suppression** screen (Section 20.2 on page 225) allows you to set how you want the LEDs to behave after the Zyxel Device is ready.
- The **Locator** screen (Section 20.3 on page 226) allows users to see the actual location of the Zyxel Device between several devices in the network.

20.2 Suppression Screen

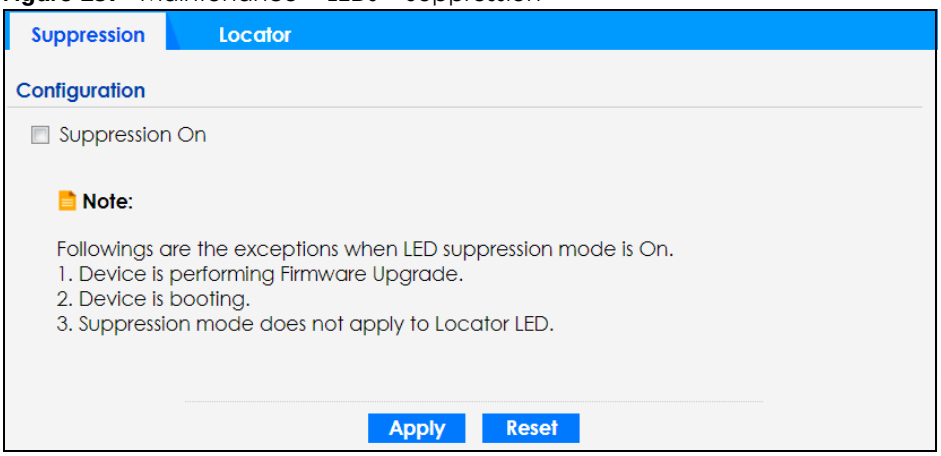
The LED Suppression feature allows you to control how the LEDs of your Zyxel Device behave after it is ready. The default LED suppression setting of your AP is different depending on your Zyxel Device model.

You can go to the **Maintenance** > **LEDs** > **Suppression** screen to see the default LED behavior and change the LED suppression setting. After you make changes in the suppression screen, it will be stored as the default when the Zyxel Device is restarted. See (Section 1.2 on page 11) for information on default values for different models.

Note: When the Zyxel Device is booting or performing firmware upgrade, the LEDs will light up regardless of the setting in LED suppression.

To access this screen, click **Maintenance** > **LEDs** > **Suppression**.

Figure 137 Maintenance > LEDs > Suppression



The following table describes fields in the above screen.

Table 86 Maintenance > LED > Suppression

LABEL	DESCRIPTION
Suppression On	If the **Suppression On** checkbox is checked, the LEDs of your Zyxel Device will turn off after it's ready. If the checkbox is unchecked, the LEDs will stay lit after the Zyxel Device is ready.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

20.3 Locator Screen

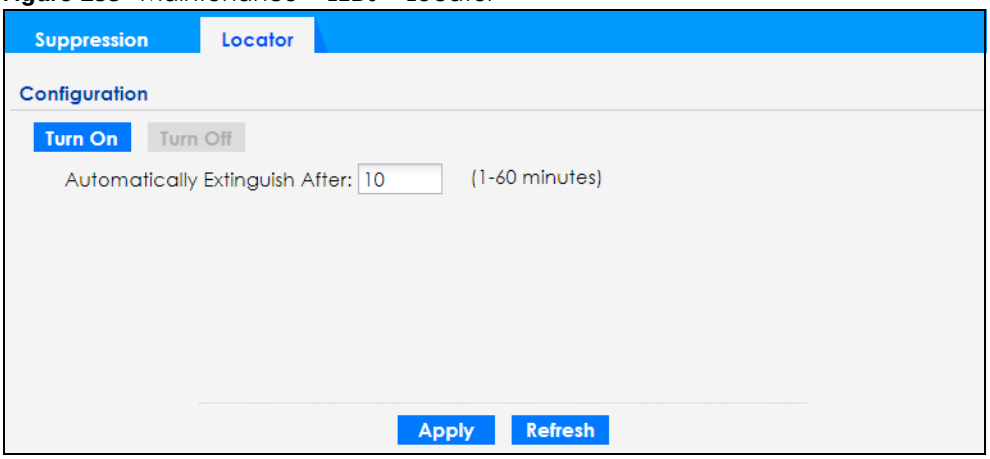
The Locator feature identifies the location of your Zyxel Device among several devices in the network. You can run this feature and set a timer in this screen.

To run the locator feature, enter a number of minutes and click **Turn On** button to have the Zyxel Device find its location. The Locator LED will start to blink for the number of minutes set in the **Locator** screen. The default setting is 10 minutes. While the locator is running, the turn on button will gray out and return after it's finished. If you make changes to the time default setting, it will be stored as the default when the Zyxel Device restarts.

Note: The Locator feature is not affected by the Suppression setting.

To access this screen, click **Maintenance** > **LEDs** > **Locator**.

Figure 138 Maintenance > LEDs > Locator



The following table describes fields in the above screen.

Table 87 Maintenance > LED > Locator

LABEL	DESCRIPTION
Turn On / Turn Off	Click **Turn On** button to activate the locator. The Locator function will show the actual location of the Zyxel Device between several devices in the network. Otherwise, click **Turn Off** to disable the locator feature.
Automatically Extinguish After	Enter a time interval between 1 and 60 minutes to stop the locator LED from blinking. Default is 10 minutes.
Apply	Click **Apply** to save changes in this screen.
Refresh	Click **Refresh** to update the information in this screen.

CHAPTER 21
Reboot

21.1 Overview

Use this screen to restart the Zyxel Device.

21.1.1 What You Need To Know

If you made changes in the Web Configurator, they were saved when you click **Apply**. They do not change when you reboot the Zyxel Device.

If you made changes in the CLI, you have to use the `write` command to save the configuration. They do not change when you reboot the Zyxel Device.

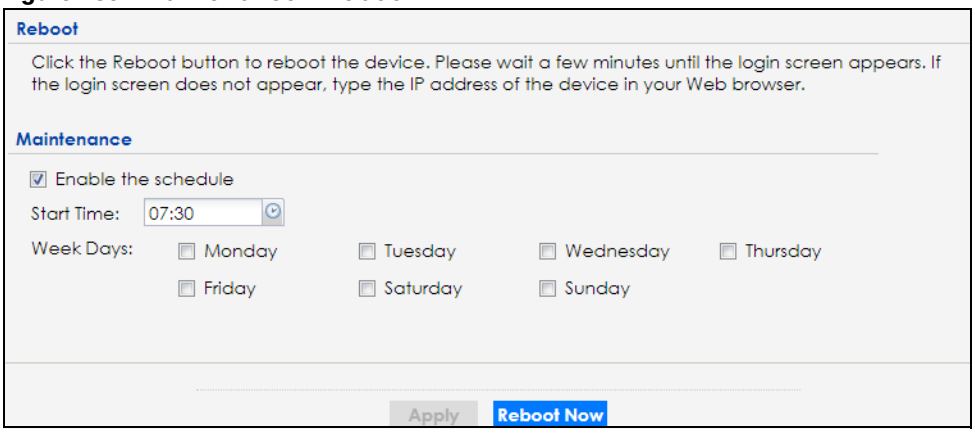
Reboot is different to reset; reset returns the Zyxel Device to its default configuration.

21.2 Reboot

This screen allows remote users to restart the Zyxel Device. To access this screen, click **Maintenance** > **Reboot**.

You can reboot your Zyxel Device when the Internet connection is slow or intermittent.

Figure 139 Maintenance > Reboot



Each field is described in the following table.

Table 88 Maintenance > Reboot

LABEL	DESCRIPTION
Maintenance	
Enable the schedule	Select this checkbox to have your Zyxel Device restart at a specific time on selected days of the week. By scheduling a reboot, you can have the Zyxel Device refresh the network connections at a specified time, allowing automatic reconnection with WiFi clients in case of a connection failure.
Start time	Specify the time of the day (in 24-hour format) to have the Zyxel Device automatically restart. For example, 23:00 is 11:00 PM.
Week Days	Select each day of the week to have the automatically restart.
Apply	Click **Apply** to save your changes to the Zyxel Device.
Reboot Now	Click **Reboot Now** to restart the Zyxel Device immediately.

After the Zyxel Device reboots, wait a few minutes until the login screen appears. If the login screen does not appear, type the IP address of the Zyxel Device in your Web browser.

You can also use the CLI command `reboot` to restart the Zyxel Device.

PART II
Local Troubleshooting - Cloud Managed Mode

CHAPTER 22
Cloud Managed Mode

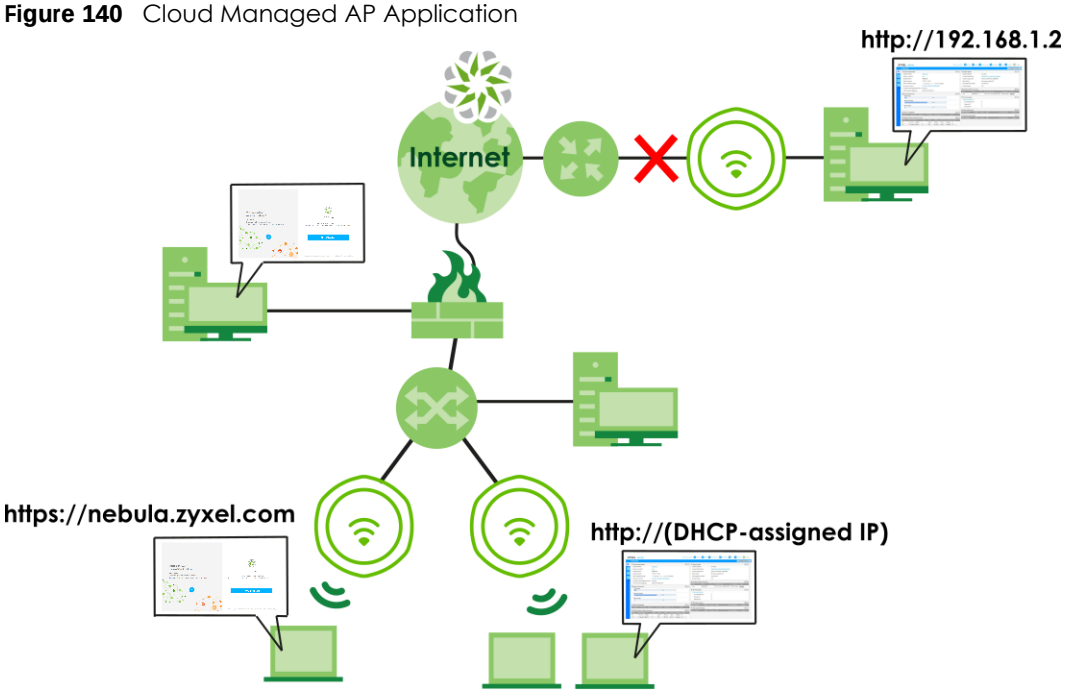
22.1 Overview

The Zyxel Device is managed and provisioned automatically by the *NCC (Nebula Control Center)* when it is connected to the Internet and has been registered with the NCC.

If you cannot access the Zyxel Device from the NCC, you need to access the local GUI screens in cloud managed mode by connecting directly to the LAN port of the Zyxel Device, and check if the Zyxel Device's VLAN setting or IP address has changed. To find the Zyxel Device's current LAN IP address, in NCC, go to **Site-wide** > **Devices** > **Access points** screen or the gateway to which the AP is connected.

Alternatively, disconnect the gateway or disable its DHCP server function and use the Zyxel Device's default static LAN IP address (192.168.1.2).

Figure 140 Cloud Managed AP Application



22.2 Local GUI Screens in Cloud Managed Mode

When your Zyxel Device is managed by NCC, you can access only the following screens through the Web Configurator:

- **Dashboard**
- **Maintenance > File Manager > Firmware Package**

- **Maintenance > File Manager > Shell Script**
- **Maintenance > Legal and Regulatory > Legal and Regulatory**
- **Maintenance > Diagnostics > Diagnostics**
- **Maintenance > Diagnostics > Remote Capture**
- **Maintenance > Log > View Log**
- **Maintenance > Reboot > Reboot**

These screens also have fewer options than those in standalone Zyxel Devices. The rest of the Zyxel Device's features must be configured through NCC.

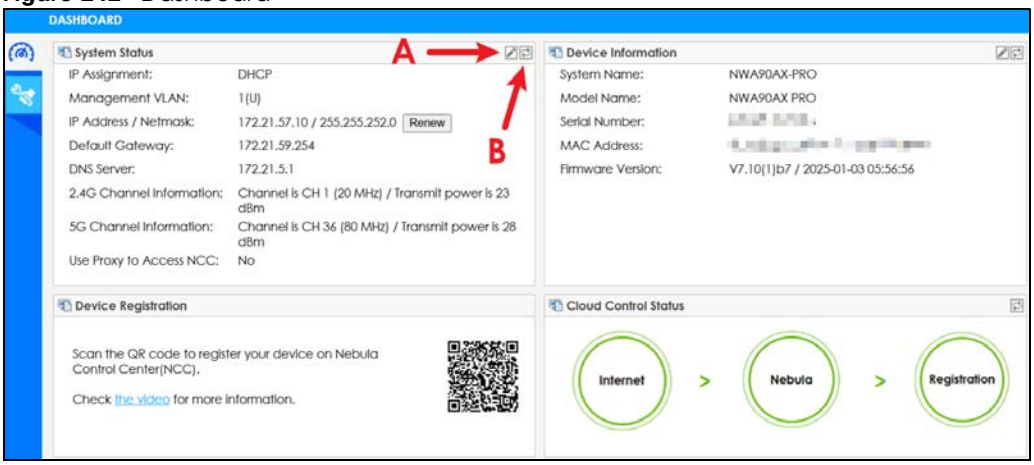
CHAPTER 23
Dashboard

23.1 Overview

This screen displays general AP information, and NCC information in widgets that you can rearrange to suit your needs. You can also edit and refresh individual widgets.

These screens also have fewer options than those in standalone Zyxel Devices. The rest of the Zyxel Device's features must be configured through NCC.

Figure 141 Dashboard



The following table describes the labels in this screen.

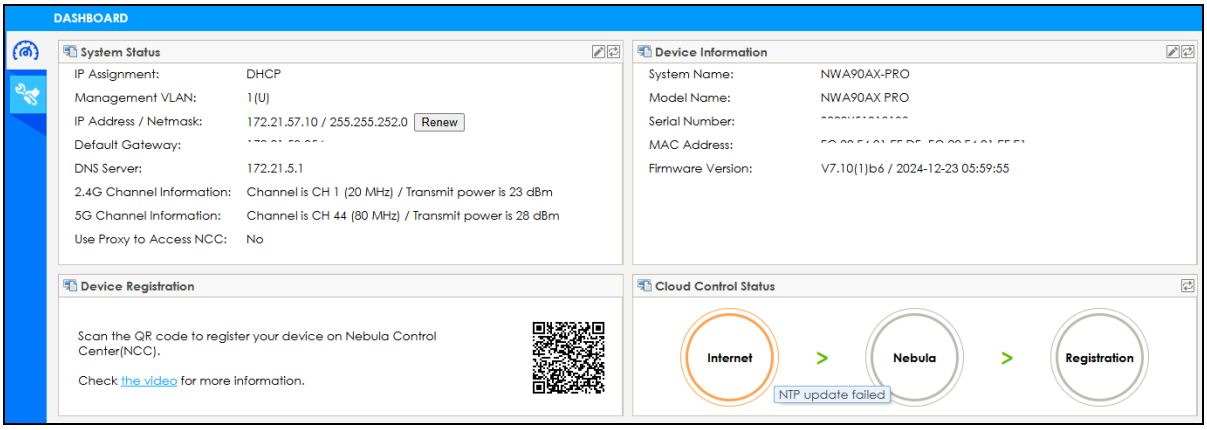
Table 89 Dashboard

LABEL	DESCRIPTION
Edit (A)	Click this to open the setup window to configure settings such as the IP address, VLAN, system name, and other network parameters.
Refresh Now (B)	Click this to update the widget's information immediately.
System Status	
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.
Management VLAN	This field displays the management VLAN ID for the Zyxel Device.
IP Address / 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. If the interface has a dynamic IP address, click **Renew** to update the IP address for the interface.
Default Gateway	This field displays the IP address of the default outgoing gateway.

Table 89 Dashboard (continued)

LABEL	DESCRIPTION
DNS Server	This field display the IP address of the DNS server.
2.4G Channel Information	This field displays the channel number the Zyxel Device is using and its output power in the 2.4 GHz spectrum. This shows **Not activated** if the wireless LAN is disabled.
5G Channel Information	This field displays the channel number the Zyxel Device is using and its output power in the 5 GHz spectrum. This shows **Not activated** if the wireless LAN is disabled.
Use Proxy to Access NCC	This displays whether the Zyxel Device uses a proxy server to access the NCC.
Device Information	
System Name	This field displays the name used to identify the Zyxel Device on any network.
Model Name	This field displays the model name of this Zyxel Device.
Serial Number	This field displays the serial number of the Zyxel Device.
MAC Address	This field displays the MAC address of the Zyxel Device.
Firmware Version	This field displays the firmware version of the Zyxel Device.
Device Registration	This field displays the information on NCC registration.
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. **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.

If the Zyxel Device cannot connect to the Internet or to NCC, move the mouse over the status circle to check the error message. See the NCC (Nebula Control Center) User's Guide for more information.



23.2 Edit System Status

Use this screen to configure the Zyxel Device's network setting and allow a proxy to access NCC.

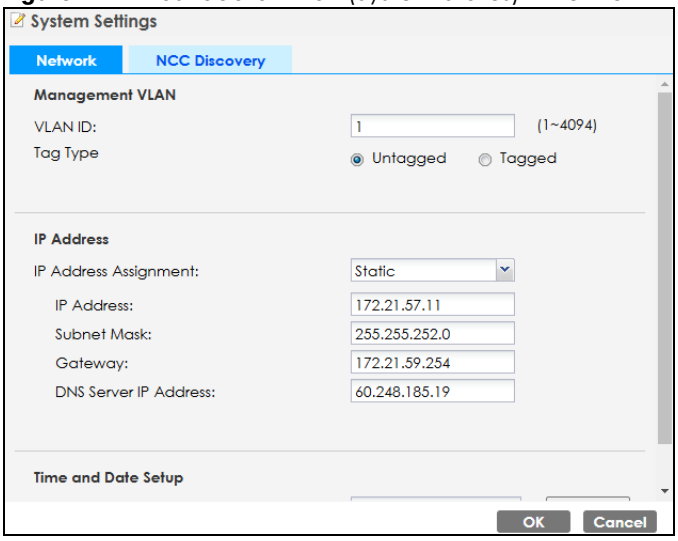
23.2.1 Network

Use this screen to configure the VLAN ID, IP address and time server. To access this screen, click **Dashboard** > **Edit (System Status)** > **Network**.

See Section 10.3 on page 108 for information about VLAN.

See Section 10.1 on page 106 for information about IP addresses.

Figure 142 Dashboard > Edit (System Status) > Network



Each field is described in the following table.

Table 90 Dashboard > Edit (System Status) > Network

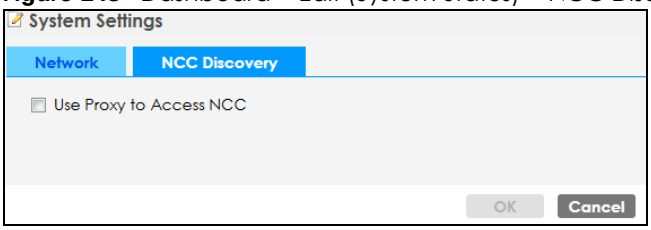
LABEL	DESCRIPTION
Management VLAN	
VLAN ID	Enter a VLAN ID for the Zyxel Device to use to tag traffic originating from this SSID. Make sure your VLAN settings allow the Zyxel Device to connect to the Internet so you could manage it with NCC.
Tag Type	Select **tagged** to make the Zyxel Device adds the Management VLAN ID to outbound traffic transmitted through its Ethernet port. If you select **Untagged**, the outbound traffic transmitted through the Zyxel Device Ethernet port will NOT be tagged with the Management VLAN ID.
IP Address	
IP Address Assignment	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.
DNS Server IP Address	Enter the IP address of a DNS server.
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	Enter the IP address of the gateway. The Zyxel Device sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
DNS Server IP Address	Enter the IP address of the DNS server.
Time and Date Setup	
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Sync. Now	Click this button to have the Zyxel Device get the time and date from the time server (see the **Time Server Address** field). This also saves your changes.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving your changes.

23.2.2 NCC Discovery

Use this screen to allow a proxy to access NCC. To access this screen, click **Dashboard** > **Edit (System Status)** > **NCC Discovery**.

Select the checkbox and click **OK** so that the Zyxel Device can access the NCC through the proxy server.

Figure 143 Dashboard > Edit (System Status) > NCC Discovery



23.3 Edit Device Information

Use this screen to configure the Zyxel Device's system name. To access this screen, click **Dashboard** > **Edit (Device Information)**.

Enter the system name and click **OK** to save the change.

Figure 144 Dashboard > Edit (Device Information)

CHAPTER 24
Maintenance

24.1 Overview

When the Zyxel Device is set to work in cloud managed mode, the **Maintenance** screens allow you to upload firmware, manage shell script files, generate a diagnostic file, view log messages, or reboot the Zyxel Device.

24.1.1 What You Can Do in this Chapter

- The **File Manager > Firmware Package** screen (Section 24.2 on page 238) displays current firmware information and allows you to upload firmware file.
- The **File Manager > Shell Script** screen (Section 24.3 on page 240) allows you to store, name, download, and upload shell script files.
- The **Legal and Regulatory > Legal and Regulatory** screen (Section 24.4 on page 243) allows you to view the legal and regulatory information.
- The **Diagnostics > Diagnostics** screen (Section 24.5 on page 243) allows you to generate a file containing the Zyxel Device's configuration and diagnostic information if you need to provide it to customer support during troubleshooting.
- The **Diagnostics > Remote Capture** screen (Section 24.6 on page 244) allows you to enable remote packet captures on wired or wireless interfaces through an external packet analyzer.
- The **Log > View Log** screen (Section 24.7 on page 245) displays the Zyxel Device's current log messages when it is disconnected from the NCC.
- The **Reboot > Reboot** screen (Section 24.8 on page 246) allows you to reboot the Zyxel Device.

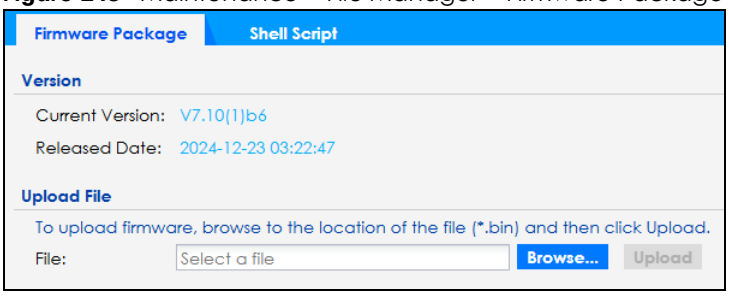
24.2 Firmware Package

Click **Maintenance > File Manager > Firmware Package** to open this screen. Use the **Firmware Package** screen to check your current firmware information and upload firmware to the Zyxel Device. You can manually download the new firmware from the Zyxel website.

Note: The Web Configurator is the recommended method for uploading firmware. You only need to use the command line interface if you need to recover the firmware. See the CLI Reference Guide for how to determine if you need to recover the firmware and how to recover it.

The firmware update can take up to five minutes. Do not turn off or reset the Zyxel Device while the firmware update is in progress!

Figure 145 Maintenance > File Manager > Firmware Package



The following table describes the labels in this screen.

Table 91 Maintenance > File Manager > Firmware Package

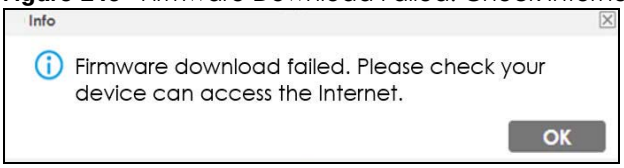
LABEL	DESCRIPTION
Version	
Current Version	This is the firmware version.
Released Date	This is the date that the version of the firmware was created.
Upload File	
File Path	Enter the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

Firmware Download Failed

The following pop-up messages display the causes and solutions for firmware download failure.

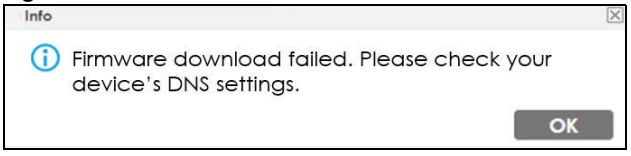
Firmware download failed due to an Internet error. Refer to Section 25.4 on page 255 for more information.

Figure 146 Firmware Download Failed. Check Internet Access.



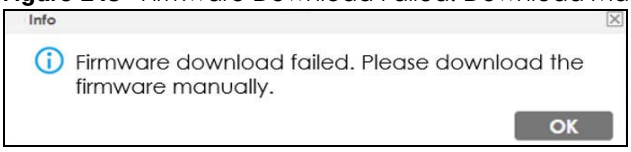
Firmware download failed due to a DNS problem. Please check your device's DNS settings.

Figure 147 Firmware Download failed. Check DNS Settings.



Firmware download failed. Download the new firmware manually from the Zyxel website. Then, go to the **Maintenance** > **File Manager** > **Firmware Package** screen to upload the new firmware.

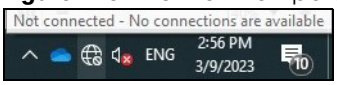
Figure 148 Firmware Download Failed. Download Manually.



Note: The Zyxel Device automatically reboots after a successful upload.

The Zyxel Device automatically restarts causing a temporary network disconnect to devices connected to its network. In some operating systems, you may see the following icon on your desktop.

Figure 149 Network Temporarily Disconnected



After five minutes, log in again and check your new firmware version in the **Dashboard** screen.

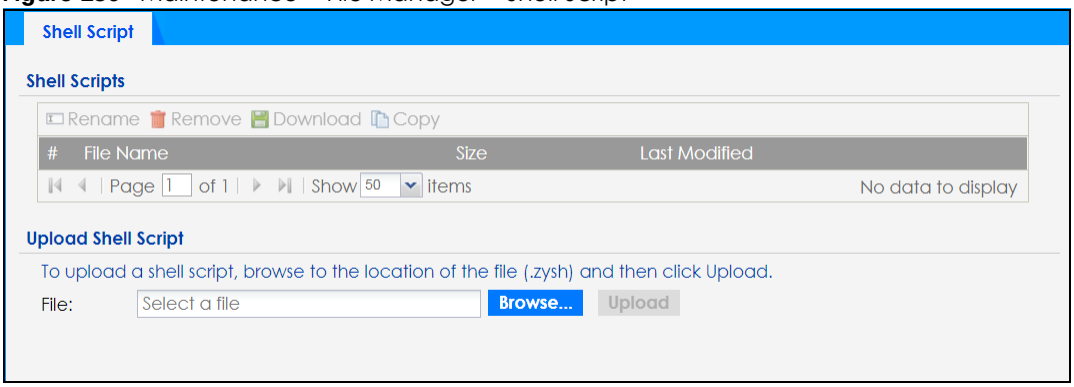
24.3 Shell Script

A shell script is a list of commands to manage the Zyxel Device. Use a text editor to create the shell script files. They must use a ".zysh" filename extension. For example, test.zysh.

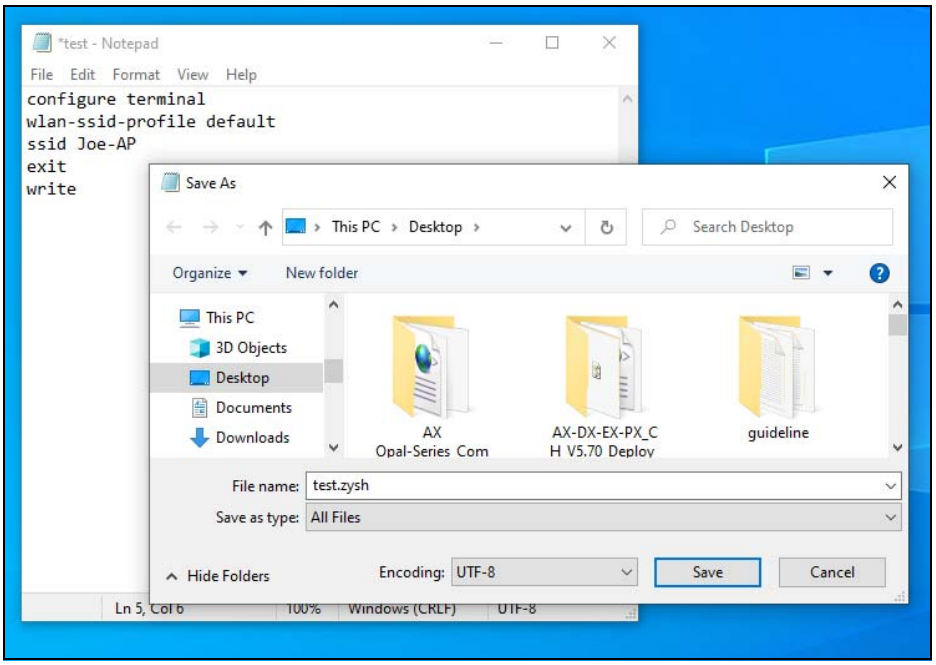
Click **Maintenance > File Manager > Shell Script** to open this screen. Use the **Shell Script** screen to store, name, download, and upload shell script files. You can store multiple shell script files on the Zyxel Device at the same time.

See Chapter 18 on page 210 for information about shell scripts.

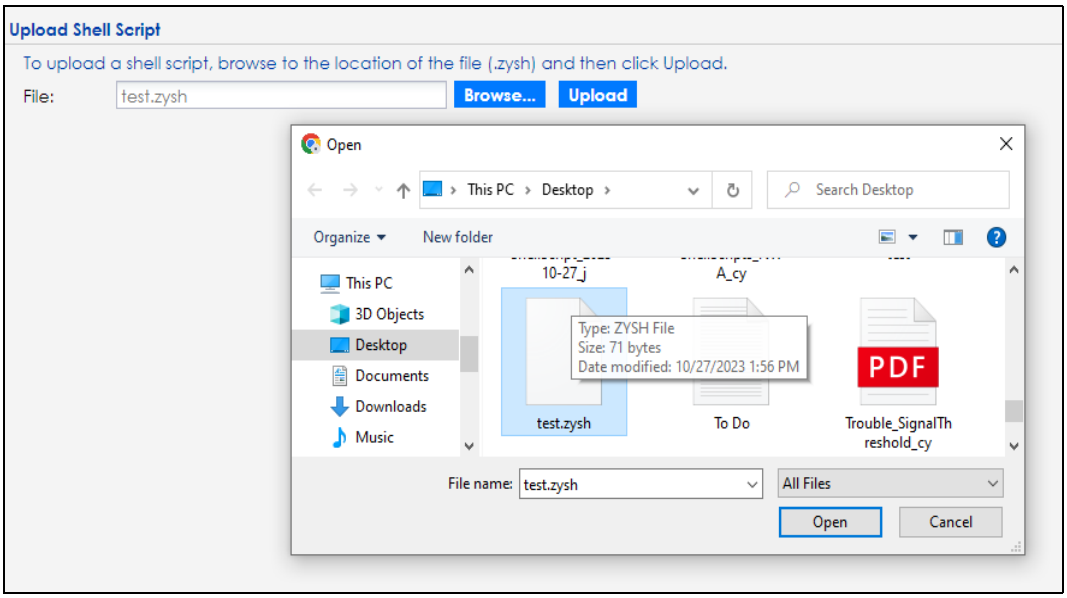
Figure 150 Maintenance > File Manager > Shell Script



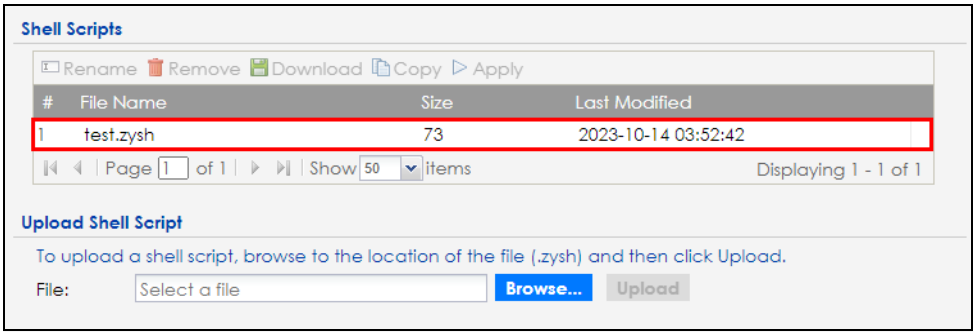
1 In the text editor, save the shell script with a .zysh filename extension. Select **All Files** as the file type.



2 Go to the **Maintenance > File Manager > Shell Script** screen. Click **Browse...** to upload the .zysh file.



3 Click **Upload**. The uploaded shell script will be shown in the **Shell Scripts** field.



Each field is described in the following table.

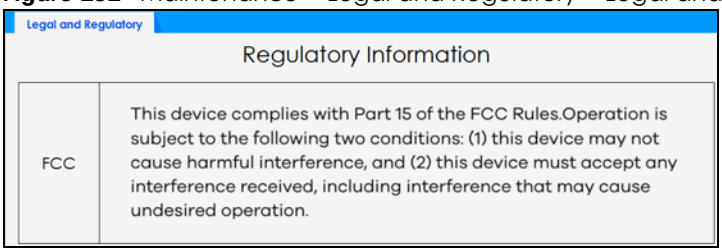
Table 92 Maintenance > File Manager > Shell Script

LABEL	DESCRIPTION
Shell Scripts	
Rename	Use this button to change the label of a shell script file on the Zyxel Device. You cannot rename a shell script to the name of another shell script in the Zyxel Device. Click a shell script's row to select it and click **Rename** to open the **Rename File** screen. Specify the new name for the shell script file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the renamed file or click **Cancel** to close the screen without saving a renamed file.
Remove	Click a shell script file's row to select it and click **Delete** to delete the shell script file from the Zyxel Device. A pop-up window asks you to confirm that you want to delete the shell script file. Click **OK** to delete the shell script file or click **Cancel** to close the screen without deleting the shell script file.
Download	Click a shell script file's row to select it and click **Download** to save the configuration to your computer.
Copy	Use this button to save a duplicate of a shell script file on the Zyxel Device. Click a shell script file's row to select it and click **Copy** to open the **Copy File** screen. Specify a name for the duplicate file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Apply	Use this button to have the Zyxel Device use a specific shell script file. Click a shell script file's row to select it and click **Apply** to have the Zyxel Device use that shell script file. You may need to wait awhile for the Zyxel Device to finish applying the commands.
#	This column displays the number for each shell script file entry.
File Name	This column displays the label that identifies a shell script file.
Size	This column displays the size (in KB) of a shell script file.
Last Modified	This column displays the date and time that the individual shell script files were last changed or saved.
Upload Shell Script	
File	Enter the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the .zysh file you want to upload.
Upload	Click **Upload** to begin the upload process. This process may take up to several minutes.

24.4 Legal and Regulatory

Use this screen to view the information on legal and regulatory. This screen may not display depending on the Zyxel Device model you are using.

Figure 151 Maintenance > Legal and Regulatory > Legal and Regulatory

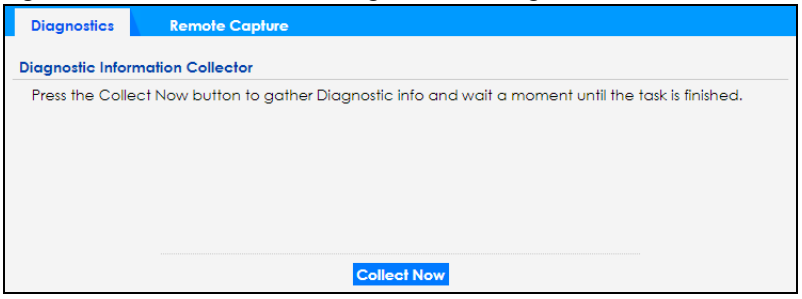


24.5 Diagnostics

This screen provides an easy way for you to generate a file containing the Zyxel Device's configuration and diagnostic information. You may need to generate this file and send it to customer support during troubleshooting. All categories of settings and shell script files stored on the Zyxel Device will be included in the diagnostic file.

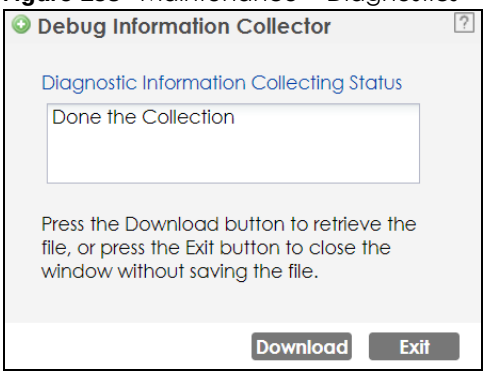
Click **Maintenance > Diagnostics > Diagnostics** to open the **Diagnostics** screen. Click **Collect Now** to have the Zyxel Device create a new diagnostic file.

Figure 152 Maintenance > Diagnostics > Diagnostics



The **Debug Information Collector** screen then displays showing whether the collection is in progress, was successful, or has failed. When the data collection is done, click **Download** to save the most recent diagnostic file to a computer.

Figure 153 Maintenance > Diagnostics > Diagnostics: Debug Information Collector

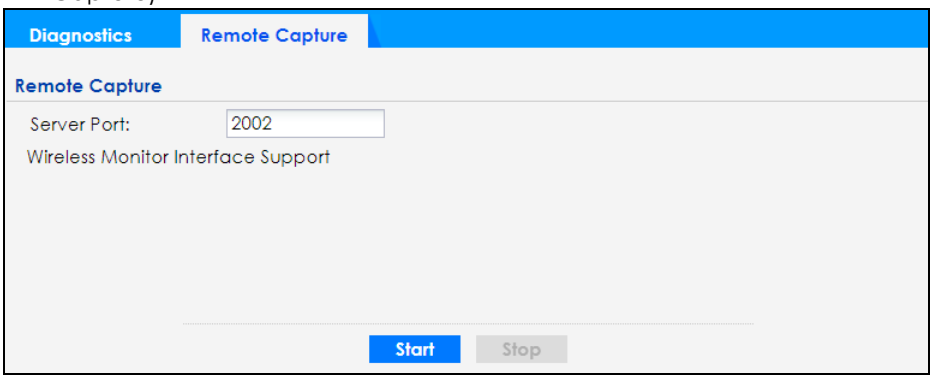


24.6 Remote Capture

Use this screen to capture network traffic going through the Zyxel Device and output the captured packets to a packet analyzer (also known as network or protocol analyzer) such as Wireshark. If the Zyxel Device is connected to the Zyxel gateway or ZyWALL, you might need to configure the Zyxel gateway or ZyWALL to allow remote capture on the Zyxel Device.

Click **Maintenance > Diagnostics > Remote Capture** to open the **Remote Capture** screen.

Figure 154 Maintenance > Diagnostics > Remote Capture (Zyxel Device that supports Wireless Remote Capture)



The following table describes the labels in this screen.

Table 93 Maintenance > Diagnostics > Remote Capture

LABEL	DESCRIPTION
Server Port	Enter the number of the server port you want the packet analyzer to connect to in order to capture traffic going through the Zyxel Device. The default port number is 2002.
Start	Click this button to allow the packet analyzer to start capturing traffic going through the Zyxel Device.
Stop	Click this button to stop the packet analyzer from capturing traffic going through the Zyxel Device.

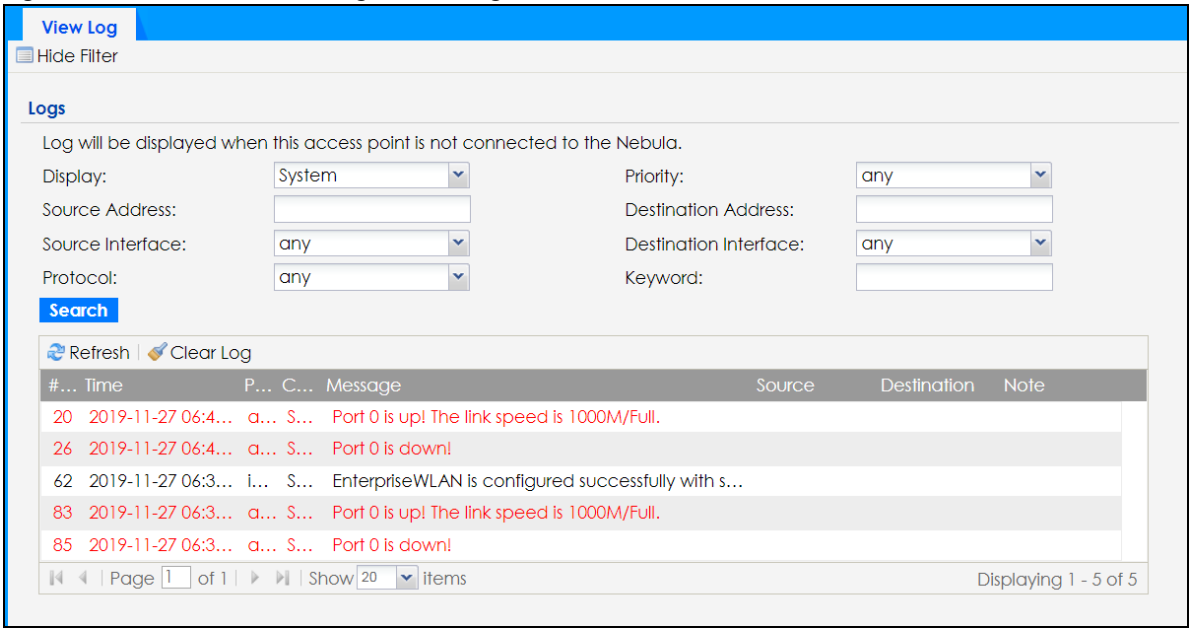
24.7 View Log

The NCC periodically gathers log files from the devices being managed by it. Before the NCC pulls logs from the Zyxel Device or when the Zyxel Device is disconnected from the NCC, you can use this screen to view its current log messages. To access this screen, click **Maintenance > Log > View Log**.

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.

Figure 155 Maintenance > Log > View Log



The following table describes the labels in this screen.

Table 94 Maintenance > Log > View Log

LABEL	DESCRIPTION
Show Filter / Hide Filter	Click this button to show or hide the filter settings. If the filter settings are hidden, the **Display** field is available. If the filter settings are shown, the **Display**, **Priority**, **Source Address**, **Destination Address**, **Source Interface**, **Destination Interface**, **Protocol**, **Keyword**, and **Search** fields are available.
Display	Select the category of log message(s) you want to view. You can also view **All Logs** at one time, or you can view the **Debug Log**.
Priority	This displays when you show the filter. Select the priority of log messages to display. The log displays the log messages with this priority or higher. Choices are: **any**, **emerg**, **alert**, **crit**, **error**, **warn**, **notice**, and **info**, from highest priority to lowest priority. This field is read-only if the **Display** is **Debug Log**.
Source Address	This displays when you show the filter. Enter the source IP address of the incoming packet that generated the log message. Do not include the port in this filter.

Table 94 Maintenance > Log > View Log (continued)

LABEL	DESCRIPTION
Destination Address	This displays when you show the filter. Enter the IP address of the destination of the incoming packet when the log message was generated. Do not include the port in this filter.
Source Interface	This displays when you show the filter. 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. Enter a keyword to look for in the **Message**, **Source**, **Destination** and **Note** fields. If a match is found in any field, the log message is displayed. You can use up to 63 alphanumeric characters and the underscore, as well as punctuation marks ()' ,:;?! +-*/= #$% @ ; the period, double quotes, and brackets are not allowed.
Search	This displays when you show the filter. Click this button to update the log using the current filter settings.
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.

24.8 Reboot

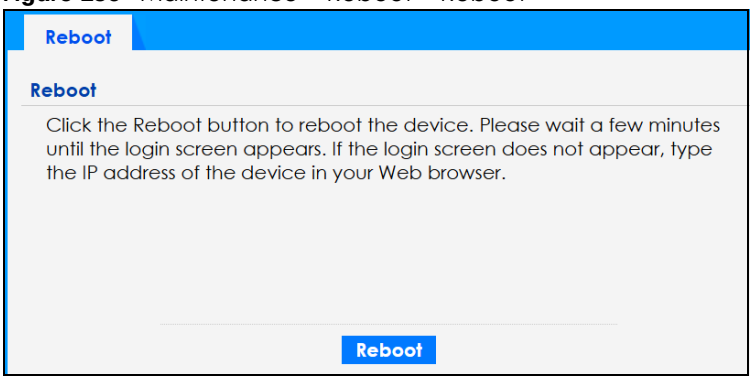
This screen allows users to restart the Zyxel Device. To access this screen, click **Maintenance** > **Reboot** > **Reboot**.

If you made changes in the CLI, you have to use the `write` command to save the configuration. They do not change when you reboot the Zyxel Device.

Reboot is different to reset; reset returns the Zyxel Device to its default configuration.

You can reboot your Zyxel Device when the Internet connection is slow or intermittent.

Figure 156 Maintenance > Reboot > Reboot



The following table describes the labels in this screen.

Table 95 Maintenance > Reboot > Reboot

LABEL	DESCRIPTION
Reboot	Click **Reboot** then click **Yes** to restart the Zyxel Device immediately.

After the Zyxel Device reboots, wait a few minutes until the login screen appears. If the login screen does not appear, type the IP address of the Zyxel Device in your Web browser.

You can also use the CLI command `reboot` to restart the Zyxel Device.

PART III
Appendices and Troubleshooting

CHAPTER 25
Troubleshooting

25.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- Zyxel Device Management, Access, and Login
- Internet Access
- WiFi Network
- Resetting the Zyxel Device

25.2 Power, Hardware Connections, and LEDs

The Zyxel Device does not turn on. Non of the LEDs turn on.

If you are using a power adapter to power the Zyxel Device:

1. Make sure you are using a compatible power adapter.
2. Make sure the power adapter is securely connected to the Zyxel Device and plugged into an appropriate power source.
3. Make sure the power adapter is functional.
4. If the problem persists, contact Zyxel technical support.

If you are using a PSE or PoE injector to power the Zyxel Device:

1. Make sure you are using the correct PoE port on the PSE or PoE injector.
2. Make sure the PSE or PoE injector is functional.
   - Check whether the PSE or PoE injector is malfunctioning. See your PSE or PoE injector user's guide for more information.
   - If the connected PSE or PoE injector does not fully comply with the Zyxel Device's supported PoE standard, replace it with compliant PSE or PoE injector. See Section 1.2 on page 11 for the Zyxel Device's supported PoE standards. Certain PSEs can adjust the power delivered to each PD based on the PoE standard supported by the PD. For detailed instructions, refer to your PSE User's Guide.

3 Make sure the Ethernet cable connected to the PSE or PoE injector is functional.
   - Check whether the Ethernet cable is malfunctioning.
   - Use the correct type of Ethernet cable for the PoE standard supported by the Zyxel Device. See Section 1.2 on page 11 for the Zyxel Device's supported PoE standards and see Table 9 on page 36 for the compliant Ethernet cables.

4 If the problem persists, contact Zyxel technical support.

The LED does not behave as expected.

1 Make sure you understand the normal behavior of the LED. See Section 3.2 on page 29.

2 Check the hardware connections. See the Quick Start Guide.

3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Disconnect and re-connect the power adapter or PoE power injector to the Zyxel Device.

5 If the problem continues, contact the vendor.

25.3 Zyxel Device Management, Access, and Login

I forgot the IP address for the Zyxel Device.

1 The default in-band IP address in standalone mode is **https://DHCP-assigned IP** (when connecting to a DHCP server) or **192.168.1.2**.

2 If you changed the IP address and have forgotten it, you have to reset the Zyxel Device to its factory defaults. See Section 25.6 on page 258.

3 If your Zyxel Device is a DHCP client, you can find your IP address from the DHCP server. This information is only available from the DHCP server which allocates IP addresses on your network. Find this information directly from the DHCP server or contact your system administrator for more information.

4 If the NCC has managed the Zyxel Device, you can also check the NCC's **Site-wide > Devices > Access points** screen for the Zyxel Device's current LAN IP address.

I cannot see or access the **Login** screen in the Web Configurator.

1 Make sure you are using the correct IP address.
   - The default IP address (in standalone mode) is 192.168.1.2.

- If you changed the IP address, use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the Zyxel Device.

2 Check the hardware connections, and make sure the LED is behaving as expected. See the Quick Start Guide and Section 3.2 on page 29.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.

4 Make sure your computer is in the same subnet as the Zyxel Device. (If you know that there are routers between your computer and the Zyxel Device, skip this step.)

- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. Check the DHCP IP address assigned to your Zyxel Device on the connected router.
- If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the Zyxel Device.

5 Reset the Zyxel Device to its factory defaults, and try to access the Zyxel Device with the default IP address. See Section 25.6 on page 258.

6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the Zyxel Device using another service, such as SSH. If you can access the Zyxel Device, check the remote management settings to find out why the Zyxel Device does not respond to HTTP.
- If your computer is connected wirelessly, use a computer that is connected to a **LAN**/**ETHERNET** port.

I forgot the Web Configurator password.

1 The default password is unique to each Zyxel Device and shown on the label. If your Zyxel Device does not have a password on the label, use "**1234**". If the Zyxel Device is connected to the NCC and registered, check the NCC for the password.

2 If this does not work, you have to reset the Zyxel Device to its factory defaults. See Section 25.6 on page 258.

I can see the **Login** screen, but I cannot log into the Zyxel Device.

1 Clear your browser's cache.

2 Check the Zyxel Device's management mode.

- The default password is unique to each Zyxel Device and shown on the label. If your Zyxel Device does not have a password on the label, use "**1234**". If you have changed the username and password, use the ones you configured to log in.

- If the Zyxel Device is in cloud managed mode, use the Nebula **Local credentials Password** to log into the cloud managed mode local GUI. The **Local credentials Password** can be found in **Site-wide > Configure > Site settings > Device configuration: Local credentials: Password** in the NCC portal.

3 Depending on your Zyxel Device's management mode, make sure you have entered the correct user name and password. These fields are case-sensitive, so check if [Caps Lock] is on or off.

Note: Steps 1 and 2 are applicable if you get an "Invalid password" error message when using some functions in the ZON utility. See Section 2.3 on page 23 for more information.

4 Disconnect and re-connect the power adapter or PoE power injector to restart the Zyxel Device.

5 If this does not work, you have to reset the Zyxel Device to its factory defaults. See Section 25.6 on page 258.

I cannot use FTP to upload or download the configuration file.

Ensure you have enabled FTP in the **Configuration** > **System** > **FTP** screen.

I cannot upload the firmware uploaded using FTP.

The Web Configurator is the recommended method for uploading firmware in standalone mode. For managed Zyxel Devices, using the NCC is recommended. You only need to use FTP if you need to recover the firmware. See the CLI Reference Guide for how to determine if you need to recover the firmware and how to recover it.

NCC is managing the Zyxel Device, but the NCC cannot access the Zyxel Device.

Connect to the Zyxel Device directly and log into the Web Configurator with the credentials configured in NCC.

I cannot register the Zyxel Device in NCC because it's already registered by the previous owner.

- If the previous owner has registered the Zyxel Device in NCC and has enabled the NCC **Override device ownership** feature in the **Organization-wide** > **Organization-wide manage** > **Organization settings** screen, use the Nebula Mobile app to scan the NCC QR code on the back label of the Zyxel Device to register with NCC.
- If the previous owner has registered it in NCC and has locked the Zyxel Device with the NCC **Override device ownership** feature in the **Organization-wide** > **Organization-wide manage** > **Organization settings** screen, inform the previous owner to unregister the Zyxel Device or contact Zyxel technical support.

The Zyxel Device is already registered with NCC, but it is still in standalone mode; it cannot connect to the NCC.

1. Check the Zyxel Device LED and make sure the Zyxel Device is on and ready for use.
2. Check your network's firewall/security settings. Make sure the following ports are allowed:
   - TCP: 443, 4335, and 6667
   - UDP: 123 is allowed.
3. Make sure your Zyxel Device has obtained an IP address and can access the Internet. Check the **Cloud Control Status** on the **Dashboard** screen for your Internet connection.
4. Check your network's VLAN settings (see Section 10.3 on page 108). You may have to change the Management VLAN settings of the Zyxel Device to allow it to connect to the Internet and access the NCC.

   Note: Changing the management VLAN and IP address settings on the Zyxel Device also pushes these changes to the NCC. Do this only if your device cannot otherwise connect to the NCC.
5. Make sure your Zyxel Device does not have to go through network authentication such as a captive portal. If your network uses a captive portal, the network administrator may have to create a new VLAN without this requirement. Change your Zyxel Device's management VLAN settings as necessary.
6. Make sure your DNS server can resolve d.nebula.zyxel.com. Open the **Command Prompt** on your computer, enter *nslookup d.nebula.zyxel.com*, see if the DNS server can return the resolved IP address. If not, you can try set your gateway to use the Google Public DNS server 8.8.8.8. Or, set the DNS server address in the Zyxel Device Web Configurator. Go to **Configuration > Network > IP Setting**, select **Use Fixed IP Address**. Set the **DNS Server IP Address:** to 8.8.8.8. Click **Apply**.

Some features I set using the NCC do not work as expected.

1. Make sure your Zyxel Device can access the Internet.
2. Make sure the NCC can access the Zyxel Device. Check your network's firewall/security settings. Make sure the following ports are allowed:
   - TCP: 443, 4335, and 6667
   - UDP: 123
3. After changing your Zyxel Device settings using the NCC, wait 1-2 minutes for the changes to take effect.

I can only see newer logs. Older logs are missing.

When a log reaches the maximum number of log messages (see Section 1.2 on page 11), new log messages automatically overwrite the oldest log messages.

The commands in my configuration file or shell script are not working properly.

- In a configuration file or shell script, use "#" or "!" as the first character of a command line to have the Zyxel Device treat the line as a comment.
- Your configuration files or shell scripts can use "exit" or a command line consisting of a single "!" to have the Zyxel Device exit sub command mode.
- Include `write` commands in your scripts. Otherwise the changes will be lost when the Zyxel Device restarts. You could use multiple `write` commands in a long script.

Note: "exit" or "!'" must follow sub commands if it is to make the Zyxel Device exit sub command mode.

My Zyxel Device's CPU usage is too high.

The Zyxel Device may receive too many HTTPS connection requests. Do the following to reduce the number of HTTPS connection requests:

Go to **Configuration** > **Object** > **User** > **Setting** and select **Limit the number of simultaneous logons for administration account.** Set a number in **Maximum number per administration account** to limit the number of simultaneous logins for each admin.

How do I set up multiple Access Points (APs)?

Avoid positioning APs in direct line of sight of each other, as this can cause interference and reduce the overall performance of your WiFi network.

In case, it may be necessary to position APs in direct line of sight of each other, you can:

- Adjust the transmit power of each AP in the **Configuration** > **Wireless** > **AP Management** screen, so that they are not using too much power and overlapping too much with each other.
- Configure the APs to operate on non-overlapping channels, such as channels 1, 6, and 11 in the 2.4 GHz band, 5 GHz band or 6 GHz band's channels or enabling DCS to let APs scan the best channel to use. This can help to minimize co-channel interference between the APs.

I only want certain users to access specific parts of my network.

See Section 8.4.6 on page 79 for more information on how to allow certain users to access only specific parts of your network.

I only want admins to use HTTPS or SSH to access the Zyxel Device.

See Section 8.8 on page 92 for more information on how to configure access to the Zyxel Device.

25.4 Internet Access

Clients cannot access the Internet through the Zyxel Device.

1. Check the Zyxel Device's hardware connections, and make sure the LEDs are behaving as expected (refer to Section 3.2 on page 29). See the Quick Start Guide and Section 25.1 on page 249.
2. Make sure the Zyxel Device is connected to a broadband modem or router with Internet access and your computer is set to obtain an dynamic IP address.
3. If clients are trying to access the Internet wirelessly, make sure the WiFi settings on the WiFi clients are the same as the settings on the Zyxel Device.
4. Make sure the Zyxel Device has the same VLAN settings configured as the gateway connected to the Zyxel Device. Traffic tagged with a specific VLAN ID tag can only go to the WiFi clients of the WiFi network that uses the same VLAN ID. If you select **Tagged** (**As Native VLAN**) in the **Configuration > Network > VLAN** screen, traffic going out from the Zyxel Device Ethernet port will be tagged with the **Management VLAN ID** you set. Devices connected to the Zyxel Device need to have the same VLAN ID configured to receive traffic from the Zyxel Device .
5. Disconnect all the cables from your Zyxel Device, and follow the directions in the Quick Start Guide again.
6. Reboot the client and reconnect to the Zyxel Device.
7. If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1. There might be a lot of traffic on the network. Look at the LEDs, and check Section 3.2 on page 29. If the Zyxel Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2. Check the signal strength using the NCC or the Zyxel Device Web Configurator, or the client device itself. If the signal is weak, try moving the client closer to the Zyxel Device (if possible), and look around to see if there are any devices that might be interfering with the wireless network (microwaves, other wireless networks, and so on).
3. Reboot the Zyxel Device using the Web Configurator/CLI or the NCC.

4 Check the settings for QoS. If it is disabled, activate it. When enabled, raise or lower the priority for some applications.

5 If the problem continues, contact the network administrator or vendor.

25.5 WiFi Network

I cannot connect to the Zyxel Device WiFi network.

1 Check the Zyxel Device LED status to make sure the Zyxel Device WiFi is on.

2 Make sure your WiFi client is within transmission range of the Zyxel Device.

3 Make sure you enter the correct SSID, password (**Pre-Shared Key**). They are case-sensitive. See the Zyxel Device back label for the default SSID and password.

4 Make sure your WiFi client is using the same WiFi security type (none, Enhanced-open, WEP, WPA, WPA2, WPA3) as the Zyxel Device. If you have previously changed the security settings, remove the SSID profile on the client device. Reconnect again using the correct SSID, password and security type.

5 Make sure the DHCP server is working properly. For example, the client may receive a private IPv4 address such as 192.168.1.x where x is a number for 2 to 254. If the client gets an address like 169.x.x.x, it means the client didn't get a valid IP address from the DHCP server.

6 Make sure the DNS server is working properly. If you can ping an IP address, but cannot ping its related URL, then it means there is a DNS server connection issue. For example, if you can ping 8.8.8.8 successfully but fail to ping google.com, there may be a DNS resolution issue.

7 Make sure the WiFi adapter on your WiFi client is working properly.

8 Make sure the wireless adapter on your WiFi client is IEEE 802.11 compatible and supports the same WiFi standard as the Zyxel Device's active radio. For example, 6 GHz WiFi networks are only available for WiFi clients that support WiFi 6E or higher standards.

The WiFi connection is slow or intermittent.

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your WiFi connection, you can:

- Move your WiFi device closer to the Zyxel Device if the signal strength is low.

- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- To ensure the connected WiFi clients receive strong WiFi signal, adjust the minimum signal strength between the Zyxel Device and its WiFi clients by going to the **Configuration** > **Object** > **AP Profile** > **Radio** screen and selecting **Enable Signal Threshold**. To apply the settings to your Zyxel Device, go to the **Configuration** > **AP Management** > **AP Group** screenand select the **Profile Name** you just created.
- Place the Zyxel Device where there are minimum obstacles (such as walls and ceilings) between the Zyxel Device and the wireless client. Avoid placing the Zyxel Device inside any type of box that might block WiFi signals.

Bandwidth restriction controls the amount of network traffic that WiFi clients can consume. This prevents the WiFi clients from downloading too many movies and slowing down other devices on the network. See Section 8.3 on page 71 for more information on how to restrict network bandwidth for each WiFi client.

Unauthorized users have accessed my wireless LAN.

- WEP is extremely insecure. It is recommended that you use the strongest security mechanism that all the WiFi devices in your network support. WPA2, WPA2-Mix or WPA3 are recommended. See Section 8.3 on page 71 for how to change security settings for a WiFi network.
- Rogue AP is an unauthorized access point in the network that poses a security threat. See Section 8.4.3 on page 75 for how to set up rogue AP detection.
- A MAC filter list blocks or allows a list of clients based on their MAC addresses, ensuring only authorized clients can access the network. See Section 8.4.5 on page 79 for more information about MAC filter.

The wireless security is not following the re-authentication timer setting I specified.

If a RADIUS server authenticates wireless stations, the re-authentication timer on the RADIUS server has priority over the setting in the Zyxel Device. Change the RADIUS server's configuration if you need to use a different re-authentication timer setting.

I forgot the WiFi password.

- If the Zyxel Device is connected to the NCC and registered, the WiFi password can be found in **Configure** > **Access points** > **SSID advanced settings** > **Choose the SSID** in the NCC portal.
- If the Zyxel device is in standalone mode, you can change the WiFi password by going to **Configuration** > **Edit SSID Profile** > **Edit Security Profile** in the Web Configurator, selecting **Personal**, and entering the new password in the **Pre-Shared Key** field.

I cannot import a certificate into the Zyxel Device.

1 For **My Certificates**, you can import a certificate that matches a corresponding certification request that was generated by the Zyxel Device. You can also import a certificate in PKCS#12 format, including the certificate's public and private keys.

2 You must remove any spaces from the certificate's filename before you can import the certificate.

3 Any certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The Zyxel Device currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.
- Binary PKCS#12: This is a format for transferring public key and private key certificates.The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the Zyxel Device.

Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

25.6 Resetting the Zyxel Device

If you cannot access the Zyxel Device by any method, try restarting it by turning the power off and then on again. If you still cannot access the Zyxel Device by any method or you forget the administrator password(s), you can reset the Zyxel Device to its factory-default settings. Any configuration files or shell scripts that you saved on the Zyxel Device should still be available afterwards.

Use the following procedure to reset the Zyxel Device to its factory-default settings. This overwrites the settings in the startup-config.conf file with the settings in the system-default.conf file.

Note: This procedure removes the current configuration.

1 Make sure the Power LED is on and not blinking.

2 Press the **RESET** button and hold it until the Power LED begins to blink. (This usually takes about ten seconds.)

3 Release the **RESET** button, and wait for the Zyxel Device to restart.

You should be able to access the Zyxel Device in standalone mode using the default settings.

25.7 Getting More Troubleshooting Help

Search for support information for your model at *www.zyxel.com* for more troubleshooting suggestions.

APPENDIX A
Importing a Certificate

When you connect to the Zyxel Device web configurator using HTTPS, a warning page "Your connection is not private" may show up. If you see this warning page, it indicates that your browser has failed to verify the Secure Sockets Layer (SSL) certificate, which opens an encrypted connection. You can ignore this message and proceed to the website.

This appendix shows you how to import a public key certificate into your web browser including Google Chrome, Microsoft Edge, and Mozilla Firefox.

Public key certificates are used by web browsers to ensure that a secure web site is legitimate. When a certificate authority such as VeriSign, Comodo, or Network Solutions, to name a few, receives a certificate request from a website operator, they confirm that the web domain and contact information in the request match those on public record with a domain name registrar. If they match, then the certificate is issued to the website operator, who then places it on the site to be issued to all visiting web browsers to let them know that the site is legitimate.

Many Zyxel products, such as the Zyxel Device, issue their own public key certificates. These can be used by web browsers on a LAN or WAN to verify that they are in fact connecting to the legitimate device and not one masquerading as it. However, because the certificates were not issued by one of the several organizations officially recognized by the most common web browsers, you will need to import the Zyxel-created certificate into your web browser and flag that certificate as a trusted authority.

Note: You can see if you are browsing on a secure website if the URL in your web browser's address bar begins with `https://` or there is a sealed padlock icon () somewhere in the main browser window (not all browsers show the padlock in the same location).

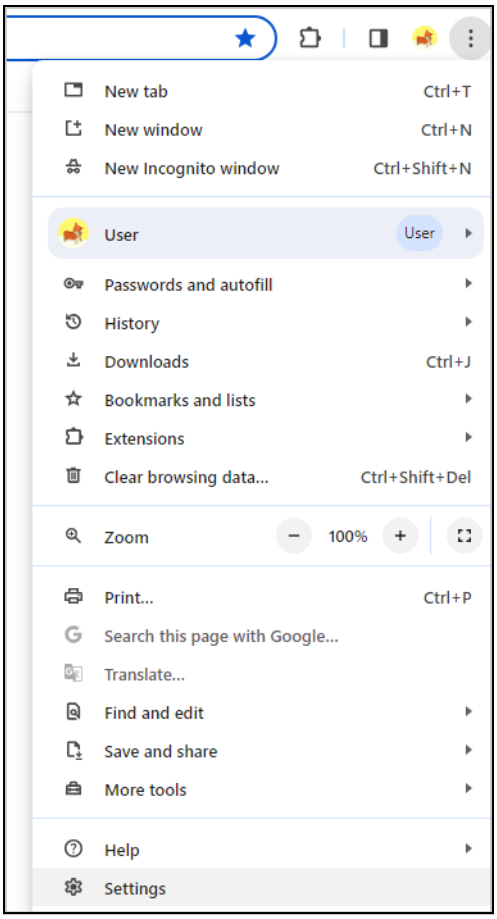
Note: You need a certificate from a trusted Certification Authority (CA) for this Zyxel Device.

Importing a Certificate to Google Chrome and Microsoft Edge

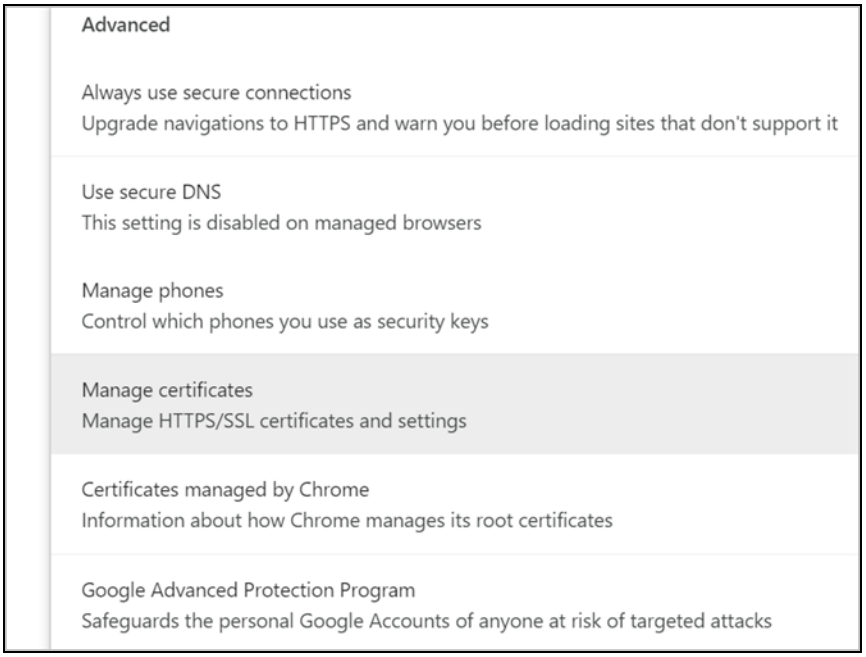
The following example uses Google Chrome on Windows 10 Pro. You first have to store the certificate in your computer and then install it as a Trusted Root CA, as shown in the following tutorials.

The Importing process is quite similar between Google Chrome and Microsoft Edge. The following procedures in Google Chrome can apply the same way in Microsoft Edge.

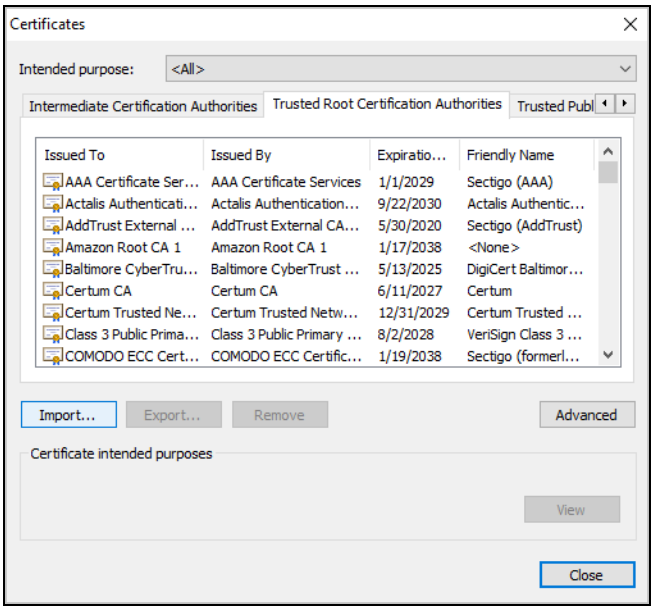
1 Open Google Chrome browser. Click the three dots on the upper right corner. Choose **Settings**.



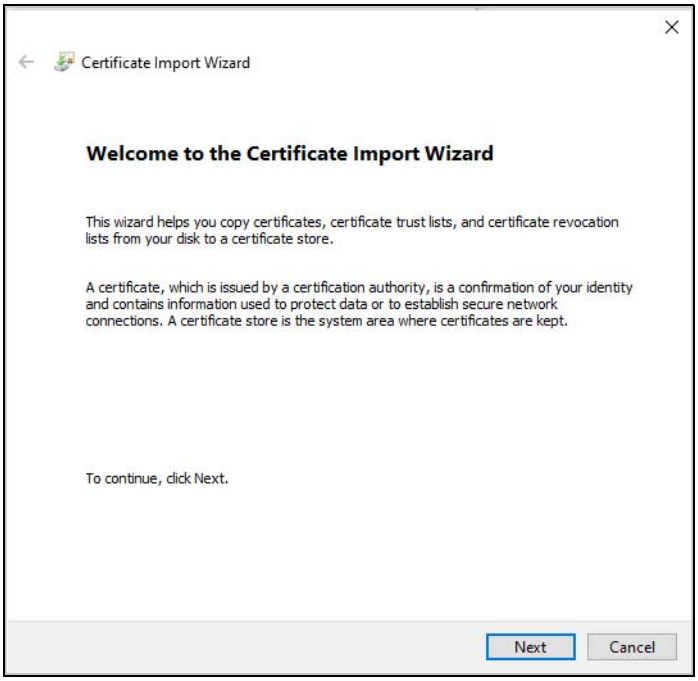
2 In Google Chrome, click **Privacy and security > Security > Manage certificates**. In Microsoft Edge, click **Privacy, search, and services > Manage certificates**.



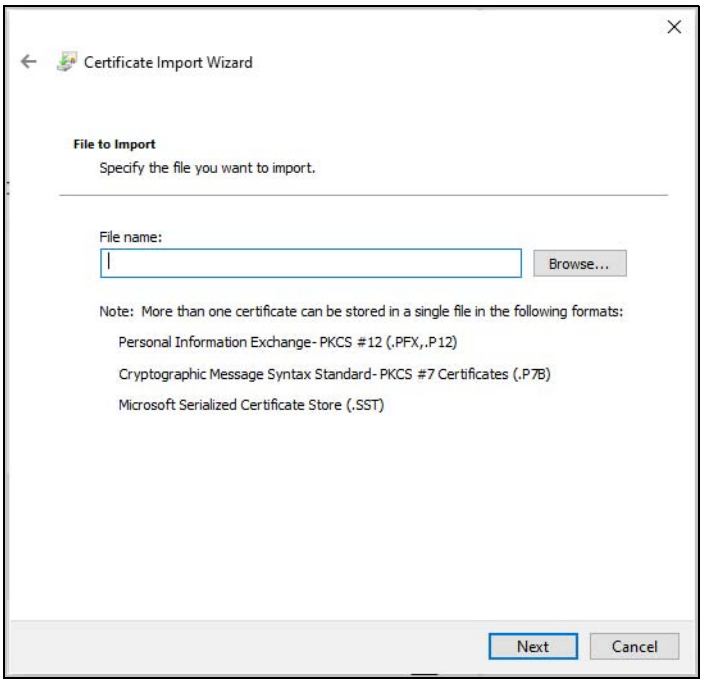
3 Select the **Trusted Root Certification Authorities** tab and click **Import**.



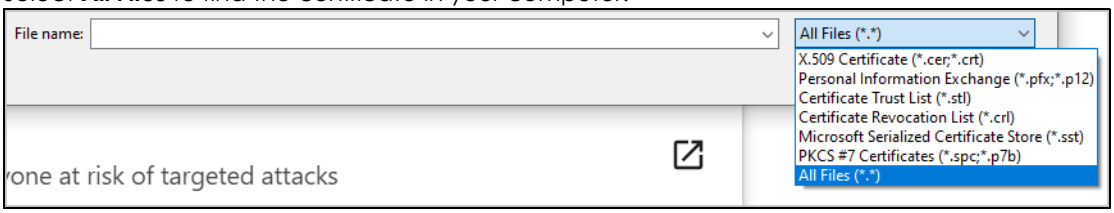
4 Click **Next** to proceed to the **Certificate Import Wizard**.



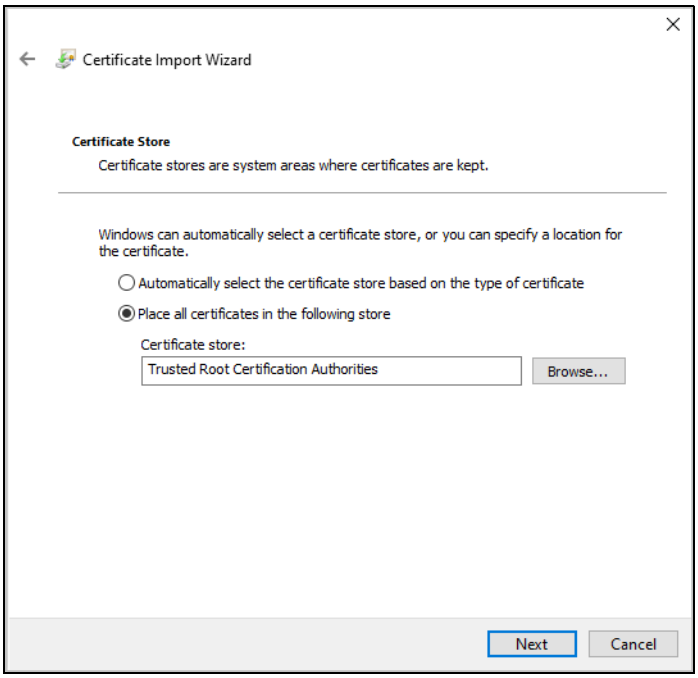
5 Click **Browse** to select a certificate already saved in your computer and click **Next** to continue.



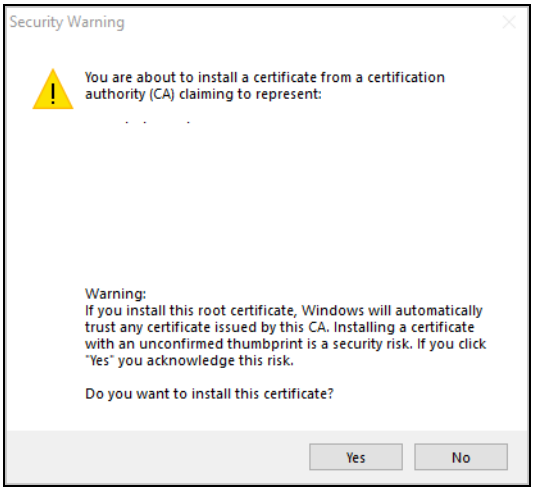
Select **All Files** to find the certificate in your computer.



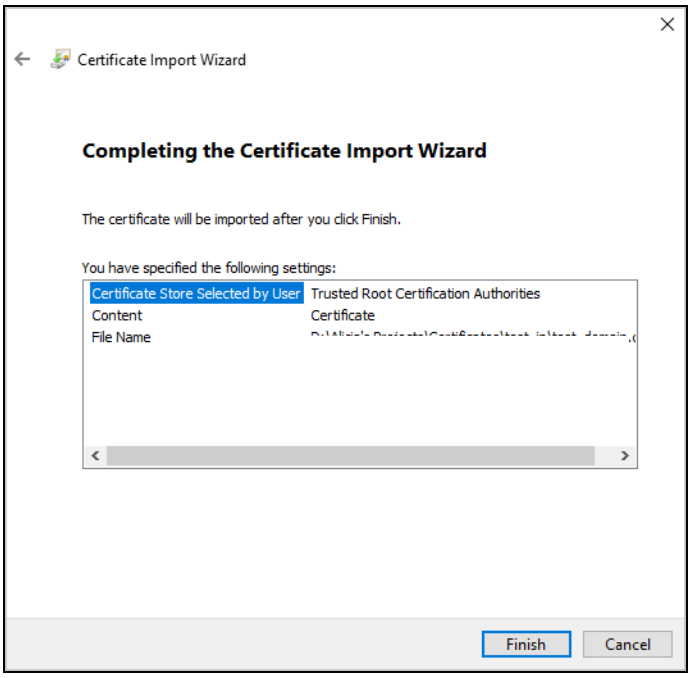
6 Two options are available for certificate stores. One is **Automatically select the certificate store based on the type of certificate**. This means the certificate import wizard can identify from the certificate whether it is a CA certificate or a personal certificate, and install it into the appropriate certificate store. The other option is **Place all certificates in the following store.** With this option, you can choose the desired folder for the certificate store. After selection, click **Next**.



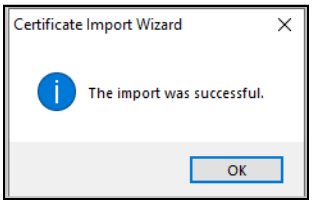
7 The security warning message shows up and click **Yes**.



8 Click **Finish**.



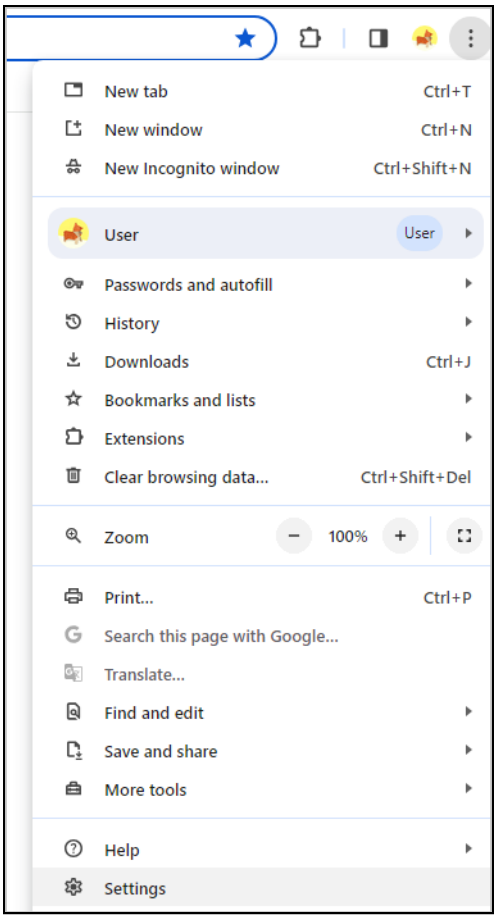
When you click **Finish,** a pop-up screen informs you about import completion.



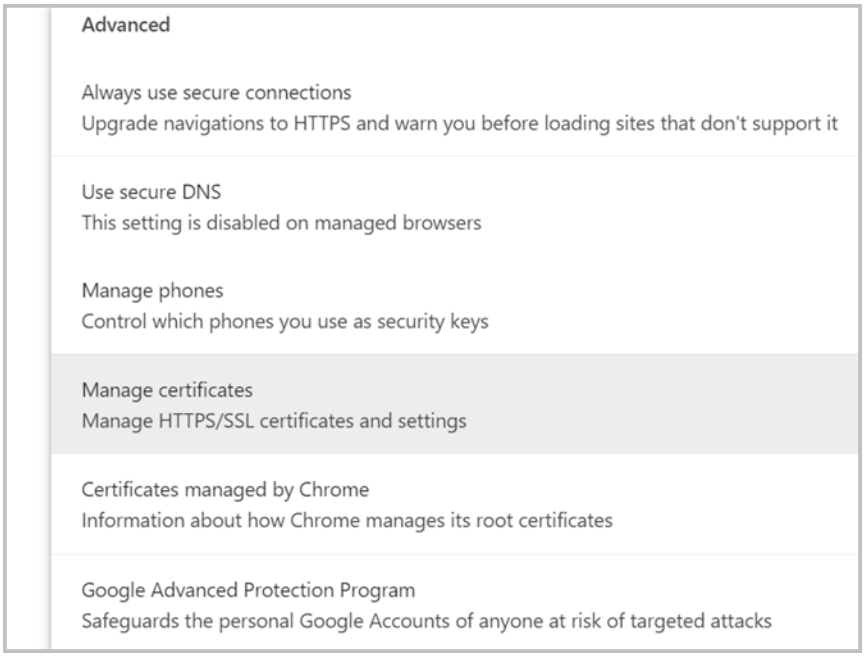
Remove a Certificate in Google Chrome and Microsoft Edge

This section shows you how to remove a public key certificate in Google Chrome and Microsoft Edge on Windows 10 Pro.

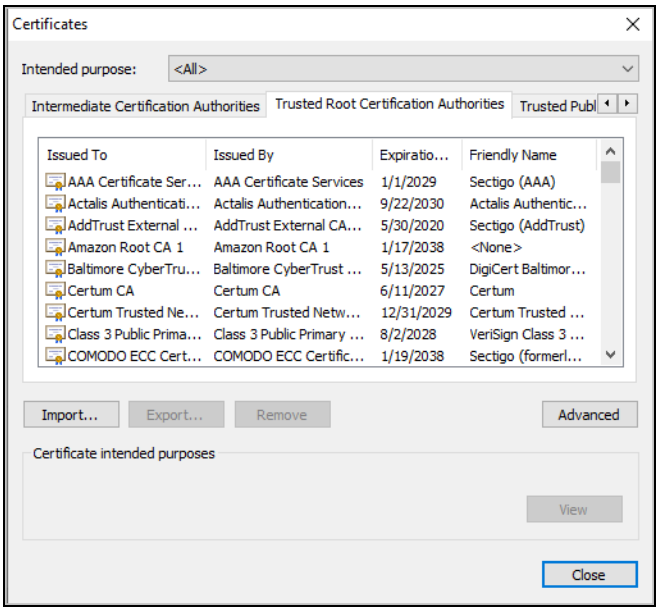
1 Open your web browser, click the menu icon, and click **Settings**.



2 In Google Chrome, click **Privacy and security > Security > Manage certificates**. In Microsoft Edge, click **Privacy, search, and services > Manage certificates**.

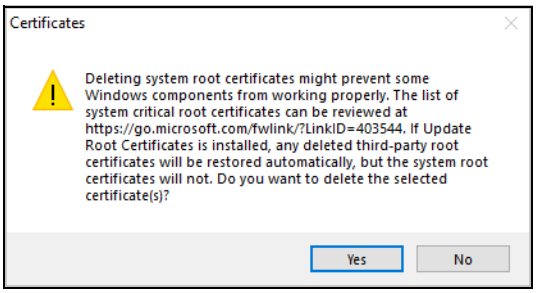


3 In the **Certificates** pop-up screen, select the **Trusted Root Certification Authorities** tab.

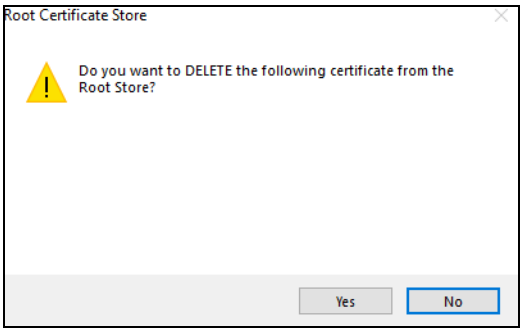


4 Select the certificate you want to remove and click **Remove**.

5 Click **Yes** when you see the following warning message.



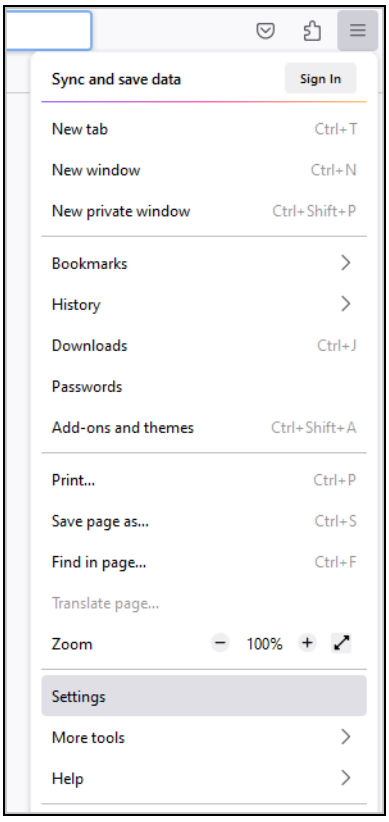
6 Confirm the details displayed in the warning message and click **Yes**.



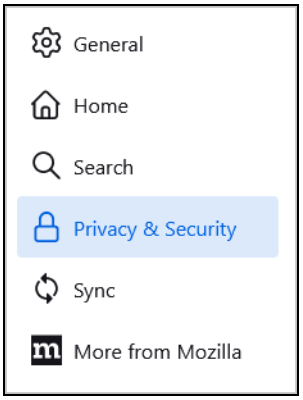
Import a Certificate to Mozilla Firefox

The following example uses Mozilla Firefox on Windows 10 Pro. You first have to store the certificate in your computer and then install it as a Trusted Root CA. To import a certificate to the Firefox browser, please follow the steps below.

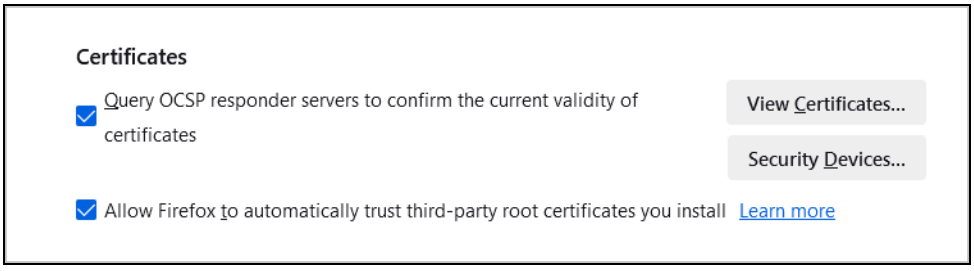
1 Open Firefox browser and click **Option** bar with three horizontal lines on the upper right corner. Click **Settings**.



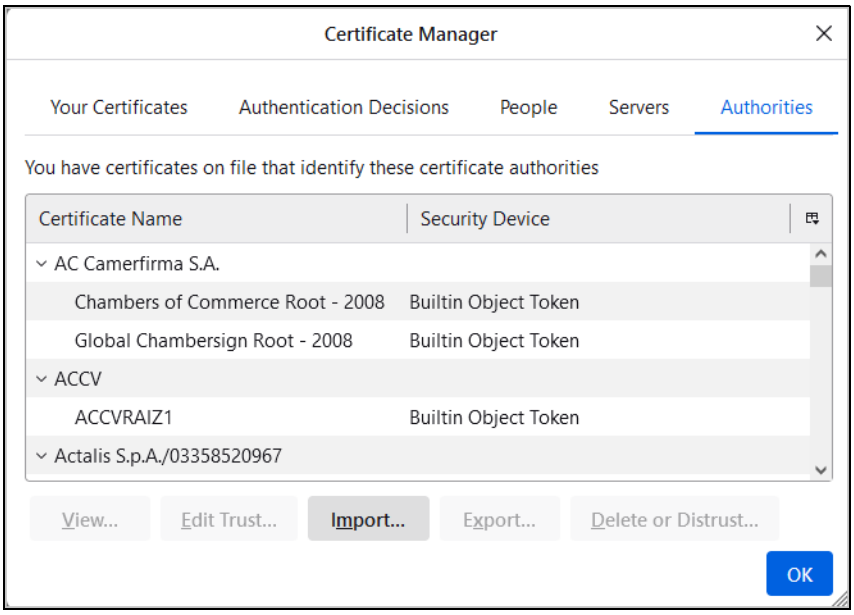
2 Click **Privacy & Security**.



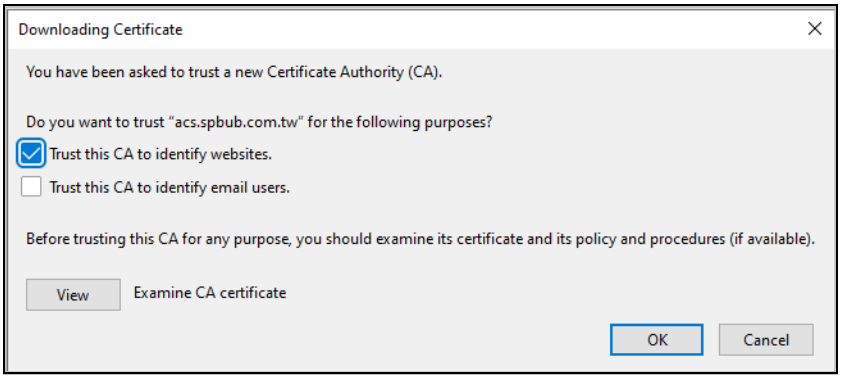
3 On the screen of **Privacy & Security**, scroll down to find **Certificates** and click **View Certificates**.



4 After the **Certificate Manager** displays, select the **Authorities** tab and click **Import**.



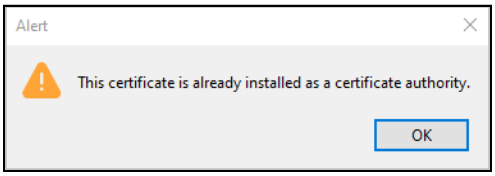
5 Open the certificate file in your computer and the **Downloading Certificate** screen shows up. Click **Trust this CA to identify websites**. Click **View** to examine the imported CA certificate.



6 After clicking **View**, the certificate details appear. Examine the content, ensuring the correct organization name. Verify that the validity period has the accurate start and end dates. The common name can be either an IP or domain name. Confirm that the client's used IP or domain name aligns with the Common Name on the certificate. If all the information on the certificate is correct, close the certificate screen and click **OK**.

The certificate file is installed in Firefox now.

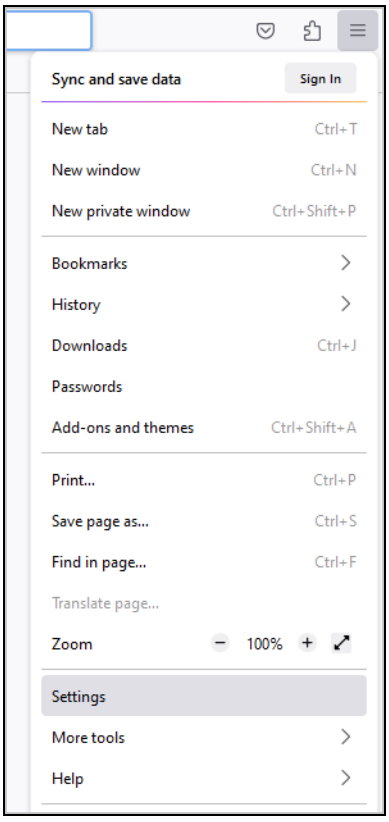
To check if the import is successful, click **Import** to select the same certificate again to see if the alert "**This certificate is already installed as a certificate authority**" pops out.



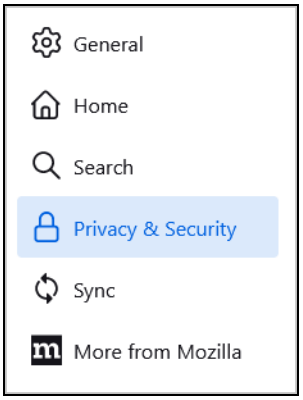
Removing a Certificate in Firefox

This section shows you how to remove a public key certificate in Firefox.

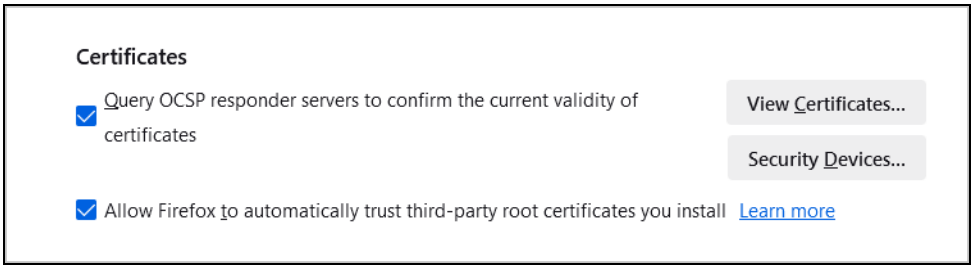
1 Open Firefox browser and click **Option** bar with three horizontal lines on the upper right corner. Click **Settings**.



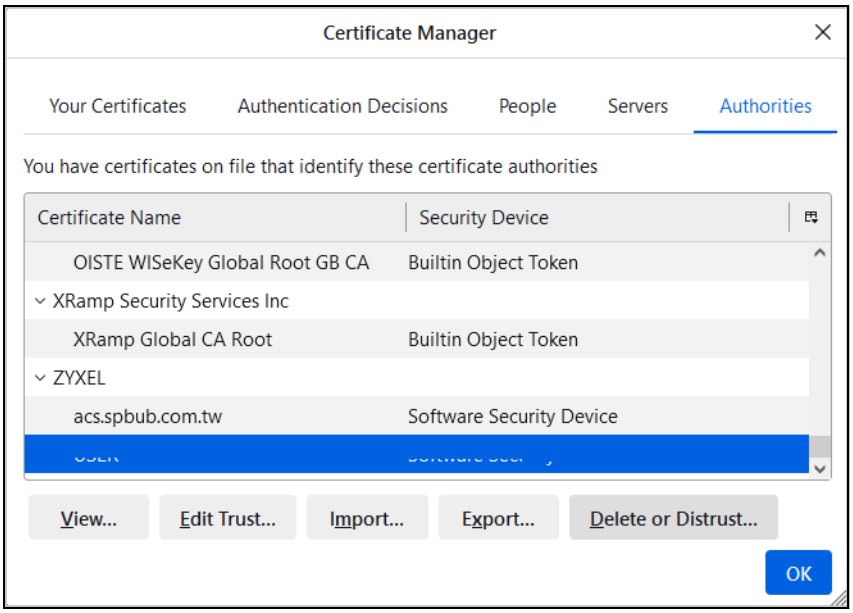
2 Click **Privacy & Security**.



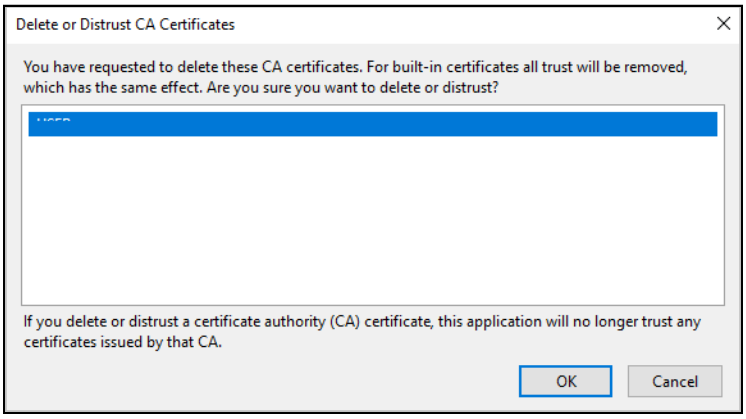
3 On the screen of **Privacy & Security**, scroll down to find **Certificates** and click **View Certificates**.



4 In the **Certificate Manager**, click **Authorities** and select the certificate you want to remove. Click **Delete or Distrust**.



5 In the following dialog box, click **OK**.



6 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

APPENDIX B
IPv6

Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10^{38} IP addresses.

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows.

Table 96 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

Global Address

A global address uniquely identifies a device on the Internet. It is similar to a "public IP address" in IPv4. A global unicast address starts with a 2 or 3.

Unspecified Address

An unspecified address (0:0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to "0.0.0.0" in IPv4.

Loopback Address

A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to "127.0.0.1" in IPv4.

Multicast Address

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined multicast addresses.

Table 97 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP severs on a local site.

The following table describes the multicast addresses which are reserved and can not be assigned to a multicast group.

Table 98 Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

Table 99

MAC	00	:	13	:	49	: 12	:	34	:	56	

Table 100

EUI-64	02	:	13	:	49	:	FF	:	FE	: 12	:	34	:	56

Stateless Autoconfiguration

With stateless autoconfiguration in IPv6, addresses can be uniquely and automatically generated. Unlike DHCPv6 (Dynamic Host Configuration Protocol version six) which is used in IPv6 stateful autoconfiguration, the owner and status of addresses don't need to be maintained by a DHCP server. Every IPv6 device is able to generate its own and unique IP address automatically when IPv6 is initiated on its interface. It combines the prefix and the interface ID (generated from its own Ethernet MAC address, see Interface ID and EUI-64) to form a complete IPv6 address.

When IPv6 is enabled on a device, its interface automatically generates a link-local address (beginning with fe80).

When the interface is connected to a network with a router and the Zyxel Device is set to automatically obtain an IPv6 network prefix from the router for the interface, it generates [1]another address which combines its interface ID and global and subnet information advertised from the router. This is a routable global IP address.

DHCPv6

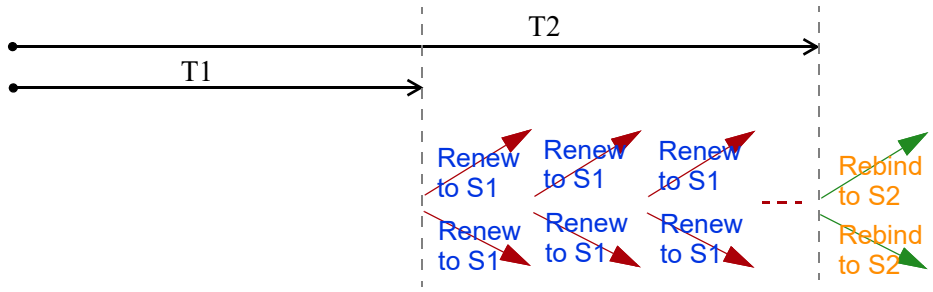
The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

1. In IPv6, all network interfaces can be associated with several addresses.

Each DHCP client and server has a unique DHCP Unique IDentifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not change over time even after you reboot the device.

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.
The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Zyxel Device uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the Zyxel Device passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor's reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Zyxel Device maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Zyxel Device configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Zyxel Device also sends out a neighbor solicitation message. When the Zyxel Device receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Zyxel Device uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The Zyxel Device creates an entry in the default router list cache if the router can be used as a default router.

When the Zyxel Device needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the Zyxel Device uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is onlink, the address is considered as the next hop. Otherwise, the Zyxel Device determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Zyxel Device looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Zyxel Device cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive

multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Example - Enabling IPv6 on Windows XP/2003/Vista

By default, Windows XP and Windows 2003 support IPv6. This example shows you how to use the `ipv6 install` command on Windows XP/2003 to enable IPv6. This also displays how to use the `ipconfig` command to see auto-generated IP addresses.

```
C:\>ipv6 install
Installing...
Succeeded.

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.1.1.46
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : fe80::2d0:59ff:feb8:103c%4
        Default Gateway . . . . . . . . . : 10.1.1.254
```

IPv6 is installed and enabled by default in Windows Vista. Use the `ipconfig` command to check your automatic configured IPv6 address as well. You should see at least one IPv6 address available for the interface on your computer.

Example - Enabling DHCPv6 on Windows XP

Windows XP does not support DHCPv6. If your network uses DHCPv6 for IP address assignment, you have to additionally install a DHCPv6 client software on your Windows XP. (Note: If you use static IP addresses or Router Advertisement for IPv6 address assignment in your network, ignore this section.)

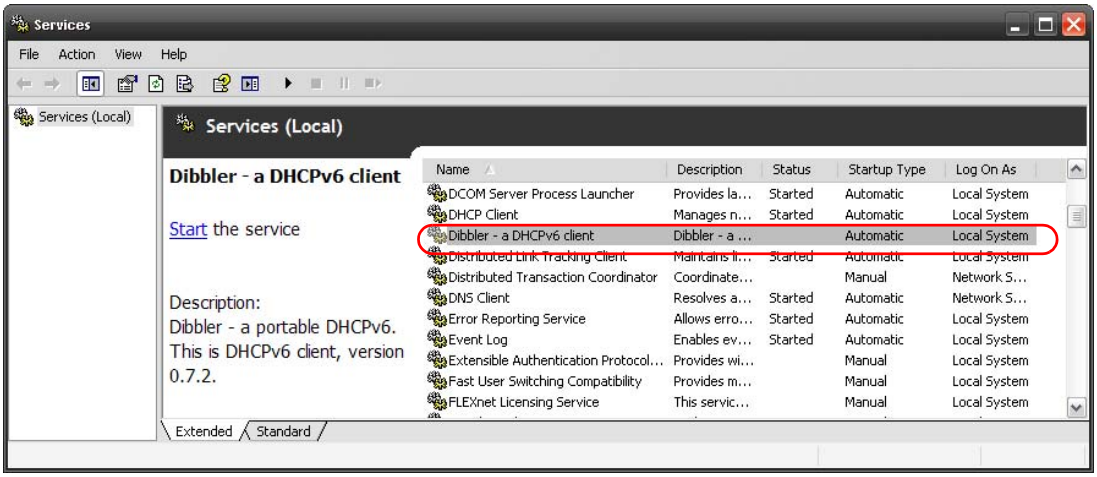
This example uses Dibbler as the DHCPv6 client. To enable DHCPv6 client on your computer:

1 Install Dibbler and select the DHCPv6 client option on your computer.

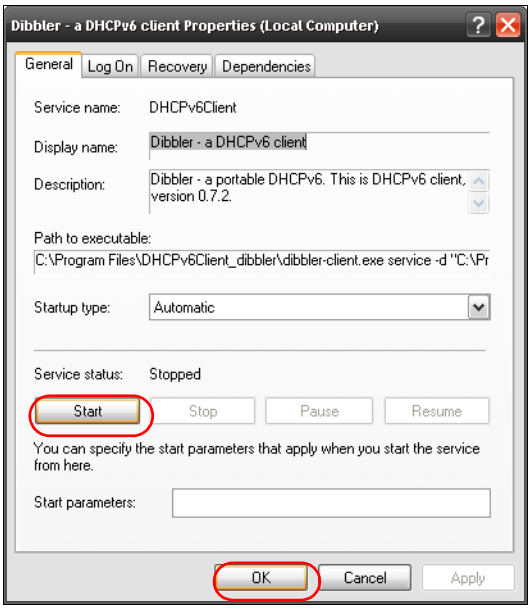
2 After the installation is complete, select **Start** > **All Programs** > **Dibbler-DHCPv6** > **Client Install as service**.

3 Select **Start** > **Control Panel** > **Administrative Tools** > **Services**.

4 Double click **Dibbler - a DHCPv6 client**.



5 Click **Start** and then **OK**.



6 Now your computer can obtain an IPv6 address from a DHCPv6 server.

Example - Enabling IPv6 on Windows 7

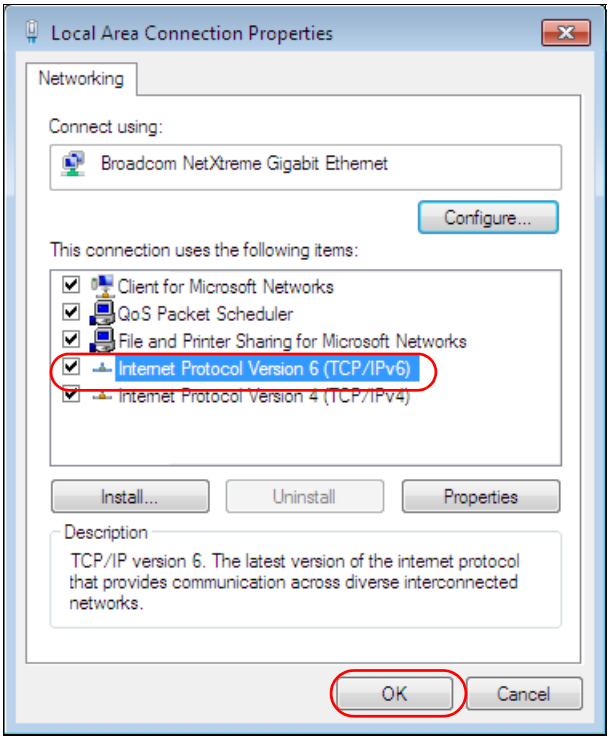
Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

1 Select **Control Panel** > **Network and Sharing Center** > **Local Area Connection**.

2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.

3 Click **OK** to save the change.



4 Click **Close** to exit the **Local Area Connection Status** screen.

5 Select **Start** > **All Programs** > **Accessories** > **Command Prompt**.

6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b021:2d::1000
   Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
   IPv4 Address. . . . . . . . . . . : 172.16.100.61
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::213:49ff:feaa:7125%11
                                       172.16.100.254
```

APPENDIX C
Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

For Zyxel Communication offices, see *https://service-provider.zyxel.com/global/en/contact-us* for the latest information.

For Zyxel Network offices, see *https://www.zyxel.com/index.shtml* for the latest information.

Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- Zyxel Communications (Taiwan) Co., Ltd.
- *https://www.zyxel.com*

Asia

China

- Zyxel Communications Corporation–China Office
- *https://www.zyxel.com/cn/sc*

India

- Zyxel Communications Corporation–India Office
- *https://www.zyxel.com/in/en-in*

Kazakhstan

- Zyxel Kazakhstan
- *https://www.zyxel.com/ru/ru*

Korea

- Zyxel Korea Co., Ltd.
- *http://www.zyxel.kr/*

Malaysia

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Philippines

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Singapore

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Taiwan

- Zyxel Communications (Taiwan) Co., Ltd.
- *https://www.zyxel.com/tw/zh*

Thailand

- Zyxel Thailand Co., Ltd.
- *https://www.zyxel.com/th/th*

Vietnam

- Zyxel Communications Corporation–Vietnam Office
- *https://www.zyxel.com/vn/vi*

Europe

Belarus

- Zyxel Communications Corp.
- *https://www.zyxel.com/ru/ru*

Belgium (Netherlands)

- Zyxel Benelux
- *https://www.zyxel.com/nl/nl*
- *https://www.zyxel.com/fr/fr*

Bulgaria

- Zyxel Bulgaria

- https://www.zyxel.com/bg/bg

Czech Republic

- Zyxel Communications Czech s.r.o.
- https://www.zyxel.com/cz/cs

Denmark

- Zyxel Communications A/S
- https://www.zyxel.com/dk/da

Finland

- Zyxel Communications
- https://www.zyxel.com/fi/fi

France

- Zyxel France
- https://www.zyxel.com/fr/fr

Germany

- Zyxel Deutschland GmbH.
- https://www.zyxel.com/de/de

Hungary

- Zyxel Hungary & SEE
- https://www.zyxel.com/hu/hu

Italy

- Zyxel Communications Italy S.r.l.
- https://www.zyxel.com/it/it

Norway

- Zyxel Communications A/S
- https://www.zyxel.com/no/no

Poland

- Zyxel Communications Poland
- https://www.zyxel.com/pl/pl

Romania

- Zyxel Romania
- https://www.zyxel.com/ro/ro

Russian Federation

- Zyxel Communications Corp.
- https://www.zyxel.com/ru/ru

Slovakia

- Zyxel Slovakia
- https://www.zyxel.com/sk/sk

Spain

- Zyxel Iberia
- https://www.zyxel.com/es/es

Sweden

- Zyxel Communications A/S
- https://www.zyxel.com/se/sv

Switzerland

- Studerus AG
- https://www.zyxel.com/ch/de-ch
- https://www.zyxel.com/fr/fr

Turkey

- Zyxel Turkey A.S.
- https://www.zyxel.com/tr/tr

UK

- Zyxel Communications UK Ltd.
- https://www.zyxel.com/uk/en-gb

Ukraine

- Zyxel Ukraine
- https://www.zyxel.com/ua/uk-ua

South America

Argentina

- Zyxel Communications Corp.
- https://www.zyxel.com/co/es-co

Brazil

- Zyxel Communications Brasil Ltda.

- *https://www.zyxel.com/br/pt*

Colombia

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

Ecuador

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

South America

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

Middle East

Israel

- Zyxel Communications Corp.
- *https://il.zyxel.com*

North America

USA

- Zyxel Communications, Inc. – North America Headquarters
- *https://www.zyxel.com/us/en-us*

APPENDIX D
Legal Information

Copyright

Copyright © 2025 by Zyxel and/or its affiliates

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel and/or its affiliates.

Published by Zyxel and/or its affiliates. All rights reserved.

Disclaimers

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Your use of the Zyxel Device is subject to the terms and conditions of any related service providers.

Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Regulatory Notice and Statement

United States of America

The following information applies if you use the product within USA area.

FCC Statement

- This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
  (1) This device may not cause harmful interference, and
  (2) this device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna
  - Increase the separation between the equipment and receiver
  - Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
  - Consult the dealer or an experienced radio/TV technician for assistance

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

FCC Radiation Exposure Statement (for outdoor model - NWA55AXE)

- This device complies with FCC Radio Frequency (RF) radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 21 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Country Code selection feature to be disabled for products marketed to the US/CANADA.

FCC Radiation Exposure Statement (for indoor model - NWA50AX/NWA90AX)

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 21 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Country Code selection feature to be disabled for products marketed to the US/CANADA.
- Operation of this device is restricted to indoor use only.

FCC Radiation Exposure Statement (for indoor model - NWA50AX PRO/ NWA90AX PRO)

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Country Code selection feature to be disabled for products marketed to the US/CANADA.
- Operation of this device is restricted to indoor use only.

Brazil

The following applies if you use the product within Brazil.

Este produto não é apropriado para uso em ambientes domésticos, pois poderá causar interferências eletromagnéticas que obrigam o usuário a tomar medidas necessárias para minimizar estas interferências.

Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados.

Canada

The following information applies if you use the product within Canada area.

Innovation, Science and Economic Development Canada ICES statement

CAN ICES-003 (B)/NMB-003(B)

Innovation, Science and Economic Development Canada RSS-GEN & RSS-247 statement (for indoor model - NWA50AX/NWA90AX/NWA50AX PRO/NWA90AX PRO)

- This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions: (1) This device may not cause interference; and (2) This device must accept any interference, including interference that may cause undesired operation of the device.
- For indoor use only.

If the product with 5G wireless function operating in 5150-5250 MHz and 5725-5850 MHz, the following attention must be paid,

- The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate; and
- Where applicable, antenna type(s), antenna models(s), and the worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2.3 of RSS 247 shall be clearly indicated.

If the produce with 5G wireless function operating in 5250-5350 MHz and 5470-5725 MHz, the following attention must be paid.

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit
- L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage; (2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- Pour une utilisation en intérieur uniquement.

Lorsque la fonction sans fil 5G fonctionnant en 5150-5250 MHz et 5725-5850 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes

- Les dispositifs fonctionnant dans la bande de 5 150 à 5 250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée, selon le cas;
- Lorsqu'il y a lieu, les types d'antennes (s'il y en a plusieurs), les numéros de modèle de l'antenne et les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, énoncée à la section 6.2.2.3 du CNR-247, doivent être clairement indiqués.

Lorsque la fonction sans fil 5G fonctionnant en 5250-5350 MHz et 5470-5725 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes

- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

Industry Canada radiation exposure statement (for indoor model - NWA50AX/NWA90AX)

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of *24 cm* between the radiator and your body.

Déclaration d'exposition aux radiations: (for indoor model - NWA50AX/NWA90AX)

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé.Cet équipement doit être installé et utilisé avec un minimum de *24 cm* de distance entre la source de rayonnement et votre corps.

Industry Canada radiation exposure statement (for indoor model - NWA50AX PRO/NWA90AX PRO)

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of *20 cm* between the radiator and your body.

Déclaration d'exposition aux radiations: (for indoor model - NWA50AX PRO/NWA90AX PRO)

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé.Cet équipement doit être installé et utilisé avec un minimum de *20 cm* de distance entre la source de rayonnement et votre corps.

Innovation, Science and Economic Development Canada RSS-GEN & RSS-247 statement (for outdoor model - NWA55AXE)

- This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions: (1) This device may not cause interference; and (2) This device must accept any interference, including interference that may cause undesired operation of the device.
- This radio transmitter (2468C-11AXAP22AO) has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Antenna Information

Ant.	Port	Brand	Model Name	Antenna Type	Connector	Gain (dBi)
1	1	MAG.LAYERS	EDA-1613-25GR2-A1	Dipole	Reversed-SMA	Note 1
2	2	MAG.LAYERS	EDA-1613-25GR2-A1	Dipole	Reversed-SMA	

Note 1:

Ant.	Port	Gain (dBi)			
		2.4 GHz	5 GHz Band 2	5 GHz Band 3	5 GHz Band 4
1	1	3.74	4.24	4.24	4.58
2	2	3.74	4.24	4.24	4.58

If the product with 5G wireless function operating in 5725-5850 MHz, the following attention must be paid,

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate; and
- Where applicable, antenna type(s), antenna model(s), and the worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2.3 of RSS 247 shall be clearly indicated.

If the produce with 5G wireless function operating in 5250-5350 MHz and 5470-5725 MHz, the following attention must be paid.

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit

- L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage; (2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- Le présent émetteur radio (2468C-11AXAP22AO) a *été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.*

Informations antenne

Ant.	Port	Brand	Model Name	Antenna Type	Connector	Gain (dBi)
1	1	MAG.LAYERS	EDA-1613-25GR2-A1	Dipole	Reversed-SMA	Note 1
2	2	MAG.LAYERS	EDA-1613-25GR2-A1	Dipole	Reversed-SMA	

Note 1:

Ant.	Port	Gain (dBi)			
		2.4 GHz	5 GHz Band 2	5 GHz Band 3	5 GHz Band 4
1	1	3.74	4.24	4.24	4.58
2	2	3.74	4.24	4.24	4.58

Lorsque la fonction sans fil 5G fonctionnant en 5725-5850 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes

- Les dispositifs fonctionnant dans la bande de 5150 à 5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée, selon le cas;
- Lorsqu'il y a lieu, les types d'antennes (s'il y en a plusieurs), les numéros de modèle de l'antenne et les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, énoncée à la section 6.2.2.3 du CNR-247, doivent être clairement indiqués.

Lorsque la fonction sans fil 5G fonctionnant en 5250-5350 MHz et 5470-5725 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes

- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

Industry Canada radiation exposure statement (for outdoor model - NWA55AXE)

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of *24 cm* between the radiator and your body.

Déclaration d'exposition aux radiations: (for outdoor model - NWA55AXE)

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé.Cet équipement doit être installé et utilisé avec un minimum de *24 cm* de distance entre la source de rayonnement et votre corps.

Europe and the United Kingdom

The following information applies if you use the product within the European Union and United Kingdom.

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED) and UK Radio Equipment Regulations 2017

- Compliance information for wireless products relevant to the EU, United Kingdom and other Countries following the EU Directive 2014/53/EU (RED) and UK regulation 2017 SI 2017-1206. And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) and United Kingdom without any limitation except for the countries mentioned below table:
- In the majority of the EU and other European countries, the 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5GHz wireless LANs.
- If this device operates in the 5150-5350 MHz band, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20 cm between the radio equipment and your body.
- The maximum RF operating power for each band is as follows:

NWA50AX/NWA90AX

- The band 2,400 MHz to 2,483.5 MHz is 98.86 mW,
- The band 5,150 MHz to 5,350 MHz is 199.07 mW,
- The band 5,470 MHz to 5,725 MHz is 979.49 mW.

NWA50AX PRO/NWA90AX PRO

- The band 2,400 MHz to 2,483.5 MHz is 97.27 mW,
- The band 5,150 MHz to 5,350 MHz is 192.31 mW,
- The band 5,470 MHz to 5,725 MHz is 744.73 mW.

NWA55AXE

- The band 2,400 MHz to 2,483.5 MHz is 98.86 mW,
- The band 5,150 MHz to 5,350 MHz is 198.61 mW,
- The band 5,470 MHz to 5,725 MHz is 988.55 mW.

Belgium (English) België (Flemish) Belgique (French)	**National Restrictions** • The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details. • Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie *http://www.bipt.be* voor meer gegevens. • Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez *http://www.bipt.be* pour de plus amples détails.
Čeština (Czech)	Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.
Dansk (Danish)	Undertegnede Zyxel erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU.
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EU põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Zyxel ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/EU.
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Español (Spanish)	Por medio de la presente Zyxel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/UE.

Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/EU.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/EU.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/EU.
Italiano (Italian)	Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/EU. **National Restrictions** • This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check *https://www.mise.gov.it/it/* for more details. • Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare *https://www.mise.gov.it/it/* per maggiori dettagli.
Latviešu valoda (Latvian)	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/EU būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/EU Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU irányelv egyéb elõírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/EU.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 2014/53/EU.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/EU.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/EU.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 2014/53/EU.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EU.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.
Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС.

Notes:

1. Not all European states that implement EU Directive 2014/53/EU are European Union (EU) members.

2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Sweden	SE
Ireland	IE	Switzerland	CH
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not put the device in a place that is humid, dusty, has extreme temperatures, or that blocks the device ventilation slots. These conditions may harm your device.
- Please refer to the device back label, datasheet, box specifications or catalog information for power rating of the device and operating temperature.
- There is a remote risk of electric shock from lightning: (1) Do not use the device outside, and make sure all the connections are indoors. (2) Do not install or service this device during a thunderstorm.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device. Opening or removing the device covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connected cables carefully so that no one will step on them or stumble over them.
- Disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/adaptors. Connect the power adaptor or cord to the right supply voltage (for example, 120V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove the damaged power adaptor or cord from the device and the power source. Do not try to repair the power adaptor or cord by yourself. Contact your local vendor to order a new one.
- CAUTION: There is a risk of explosion if you replace the device battery with an incorrect one. Dispose of used batteries according to the instructions. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do not leave a battery in an extremely high temperature environment or surroundings since it can result in an explosion or the leakage of flammable liquid or gas.
- Do not subject a battery to extremely low air pressure since it may result in an explosion or the leakage of flammable liquid or gas.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,
  - For a permanently connected device, a readily accessible method to disconnect the device shall be incorporated externally to the device;
  - For a pluggable device, the socket-outlet shall be installed near the device and shall be easily accessible.

Environment statement

ErP (Energy-related Products)

Zyxel products put on the EU and United Kingdom markets comply with the requirement of the European Parliament and the Council published Directive 2009/125/EC and UK regulation establishing a framework for the setting of ecodesign requirements for energy-related products (recast), the so called "ErP Directive (Energy-related Products directive), as well as ecodesign requirements laid down in applicable implementation measures. Power consumption has satisfied the regulation requirements which are:

Network standby power consumption < 8W (watts), and/or

Off mode power consumption < 0.5W (watts), and/or

Standby mode power consumption < 0.5W(watts).

For wireless setting, please refer to the chapter about wireless settings for more detail.

Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.

台灣

以下訊息僅適用於產品銷售至台灣地區

- 取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
- 應避免影響附近雷達系統之操作。
- 高增益指向性天線只得應用於固定式點對點系統。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

- 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

安全警告 - 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸
  – 任何液體 – 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
  – 灰塵及污物 – 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝或維修此設備。有遭受電擊的風險。

- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請使用隨貨提供或指定的連接線 / 電源線 / 電源變壓器，將其連接到合適的供應電壓 (如 : 台灣供應電壓 110 伏特)。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。(僅限於 NWA50AX/NWA90AX/NWA50AX PRO/NWA90AX PRO)
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用 :
  - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
  - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC if the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

Viewing Certifications

Go to http://www.zyxel.com to view this product's documentation and certifications.

Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at *https://www.zyxel.com/global/en/support/warranty-information*.

Registration

Register your product online at *www.zyxel.com* to receive email notices of firmware upgrades and related information.

Open Source Licenses

This product may contain in part some free software distributed under GPL license terms and/or GPL-like licenses.
To request the source code covered under these licenses, please go to: *https://www.zyxel.com/form/gpl_oss_software_notice.shtml*.

Index

Numbers

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z