ZYXEL
COMMUNICATIONS

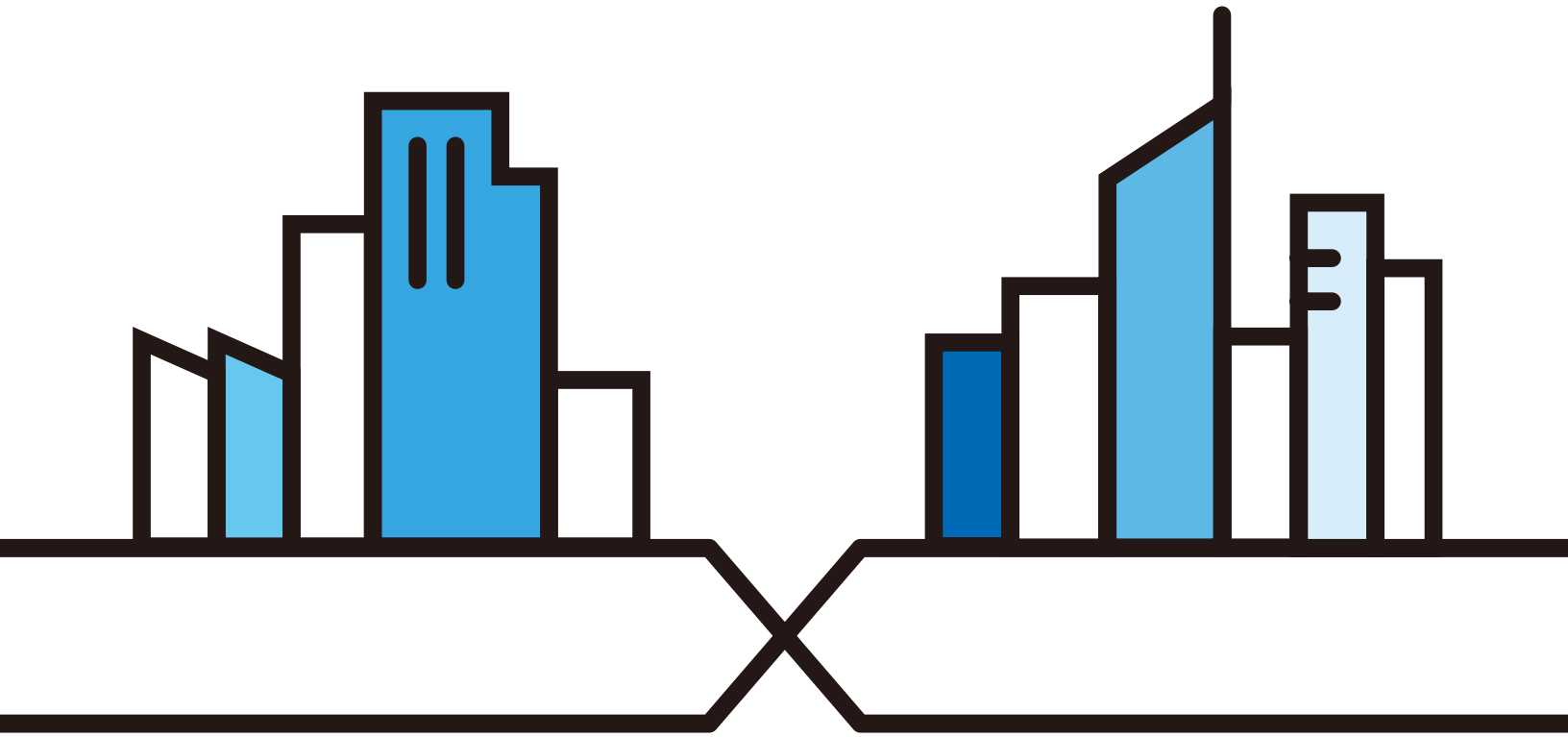
User's Guide

WX Series

Dual-Band Wireless Extender

Default Login Details	
LAN IP Address	http://192.168.1.2
Login	admin
Password	See the device label

Version 5.17-5.70 Ed 4, 5/2024



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from what you see due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the WX Device.

- More Information

  Go to *https://service-provider.zyxel.com/global/en/tech-support* to find other information on the WX Device.

Document Conventions

Warnings and Notes

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

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

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

Syntax Conventions

- The device in this user's guide may be referred to as the "WX Device" in this guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Network Setting** > **Wireless** > **MAC Authentication** means you first click **Network Setting** in the navigation panel, then the **Wireless** sub menu and finally the **MAC Authentication** tab to get to that screen.

Icons Used in Figures

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

WX Device 	Generic Router 	Laptop Computer 
Switch 	Firewall 	Server 
Internet 	User 	Smartphone 

Contents Overview

Table of Contents

PART I
User's Guide

CHAPTER 1
Introduction

1.1 Overview

The WX Device refers to the following models.

- WX3401-B0
- WX3100-T0
- WX5600-T0

Use any of the following methods to manage the WX Device.

- Web Configurator. Use the Web Configurator for management of the WX Device using a supported web browser.
- MPro Mesh App. Download the MPro Mesh app from Google Play or Apple Store to manage the WX Device using a smartphone or tablet.

1.1.1 Introduction

A WX Device is a dual-band WiFi extender that can extend WiFi coverage from a router/modem with Internet access. The WX Device supports MPro Mesh that lets a controller manage your WiFi network.

The following table describes the features of the WX Device by model.

Table 1 WX Device Comparison Table

	WX3401-B0	WX3100-T0	WX5600-T0
2.4 G WiFi	YES	YES	YES
5 G WiFi	YES	YES	YES
MU-MIMO	2.4 GHz: 2x2 5 GHz: 4x4	2.4 GHz: 2x2 5 GHz: 2x2	2.4 GHz: 4x4 5 GHz: 4x4
Antenna	Internal	Internal	Internal
Gigabit Ethernet LAN Port	Two 1GbE	Two 1GbE	Two 2.5 GbE
Mesh	YES	YES	YES
Wall Mount	YES	YES	YES
WPS	YES	YES	YES
Multicast	YES	NO	NO
Mobile APP	MPro Mesh app iOS: v 2.2.2 Android: v 2.2.2	MPro Mesh app iOS: v 2.2.2 Android: v 2.2.2	MPro Mesh app iOS: v 2.2.2 Android: v 2.2.2
LED indicator on/off switch	–	–	YES
Latest Firmware Version	5.17	5.50	5.70

1.1.2 Multi-Gigabit

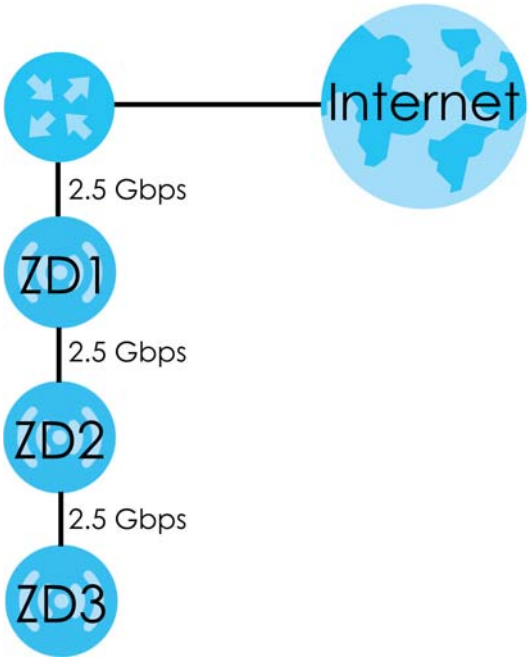
A 2.5 Gigabit port supports speed of 2.5G if the connected device supports 2.5G and a Cat 6a (up to 100 m) or Cat 6 cable (up to 50 m) is used. The speed drops to 1G if these criteria are not met; it drops to 100M if a Cat 5 cable is used (up to 100 m).

If a network device such as an Access Point (AP) only supports 1 Gigabit connectivity, then the maximum speed potential of this device is never reached.

In addition, at the time of writing, most existing cabling is Cat 5e or Cat 6, further limiting maximum speed or distance potential.

Multi-Gigabit (IEEE 802.3bz) solves these problems by additionally supporting 2.5 Gigabit Ethernet connections over Cat 5e and higher Ethernet cables. Multi-Gigabit ports are also backward compatible with 100 Mbps and 1 Gigabit ports.

Figure 1 Multi-Gigabit Application



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

Table 2 Cable Types

CABLE	TRANSMISSION SPEED	MAXIMUM DISTANCE	BANDWIDTH CAPACITY
Category 5	100M	100 m	100 MHz
Category 5e	1G / 2.5G	100 m	100 MHz

1.1.3 Setting Up the WX Device

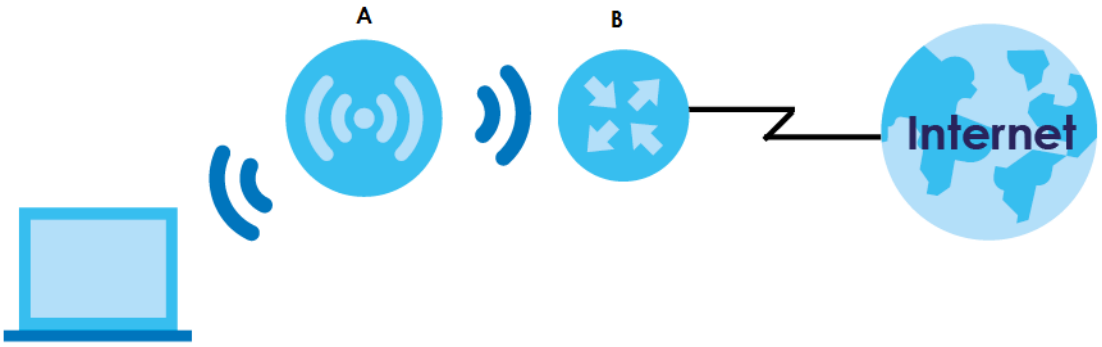
The WX Device can function as a Repeater or an Access Point (AP).

Set your WX Device to **Repeater** (RP) mode, if you want to connect an existing WiFi network through another Access Point and also provide network connection to WiFi clients. In this mode, the WX Device

can be an access point and a WiFi client at the same time. If the WX Device has a WiFi uplink connection, it is in RP mode.

In the following figure, the WX Device (**A**) is in **Repeater** (RP) mode and is letting a WiFi client connect to the network wirelessly through a router (**B**). This helps you expand WiFi coverage when you already have an access point or WiFi router in your network.

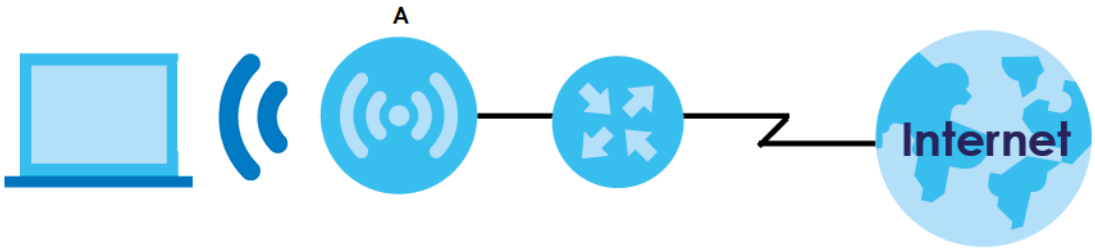
Figure 2 Device Operation Mode Example: Repeater Mode



Set your WX Device to **Access Point** (AP) mode if you already have a router in your network and you want to bridge a wired network (LAN) and another LAN or wireless LAN (WLAN) in the same subnet. If the WX Device has a wired uplink connection, it is in AP mode.

In the following figure, the WX Device (**A**) is in **Access Point** (AP) mode, and is bridging a wired network and a wired LAN in the same subnet.

Figure 3 Device Operation Mode Example: AP Mode



The WX Device can use both 2.4 GHz and 5 GHz networks at the same time. For more information on dual-band WiFi, see Section 1.3 on page 17.

You can add more WX Devices to your network to form a daisy chain. For more information, see Section 1.4 on page 18.

Set up a Mesh network with your WX Device to use band steering, AP steering, auto-configuration and other advanced features for your WiFi network. For more information, see Section 1.2.1 on page 15.

Manage the WX Device and your WiFi network using the MPro Mesh app. You can check your WiFi network status, change passwords or set up a WiFi access with a QR code. For more information, see Chapter 4 on page 38.

1.2 MPro Mesh

The WX Device supports MPro Mesh that lets a controller manage your WiFi network. A controller can automatically configure WiFi settings on extenders in the network as well as optimize bandwidth usage. The controller optimizes bandwidth usage by directing WiFi clients to an extender (AP steering) or 2.4 GHz / 5 GHz band (band steering) that is less busy.

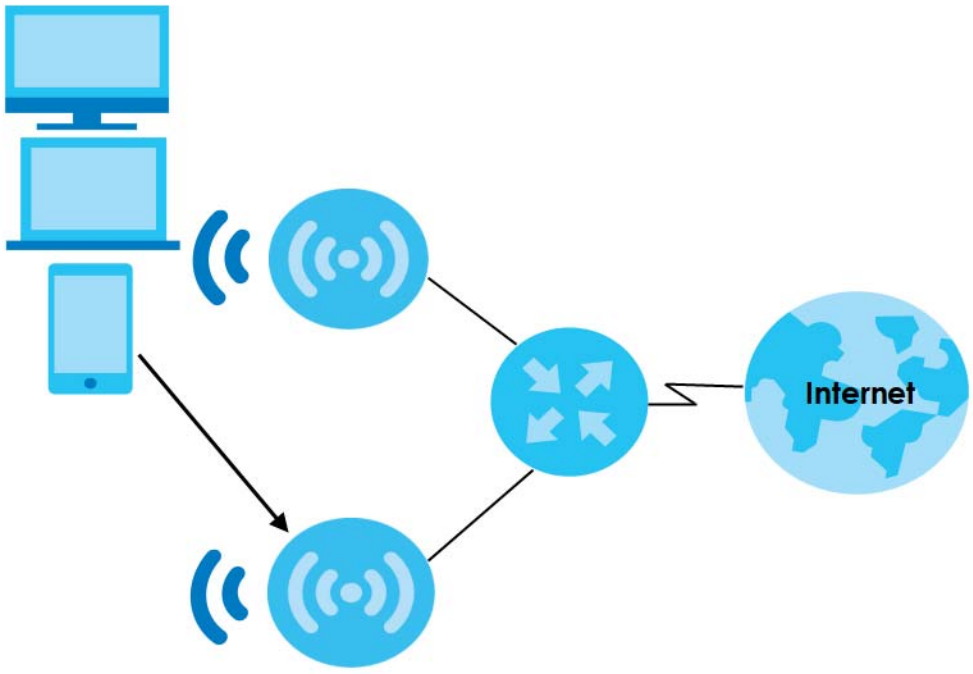
- If the router/modem is an MPro Mesh router/modem, then the router/modem is the controller.
- If the router/modem is not an MPro Mesh router/modem, then the WX Device is the controller.

1.2.1 AP Steering and Band Steering

Zyxel MPro Mesh supports AP steering and Band steering.

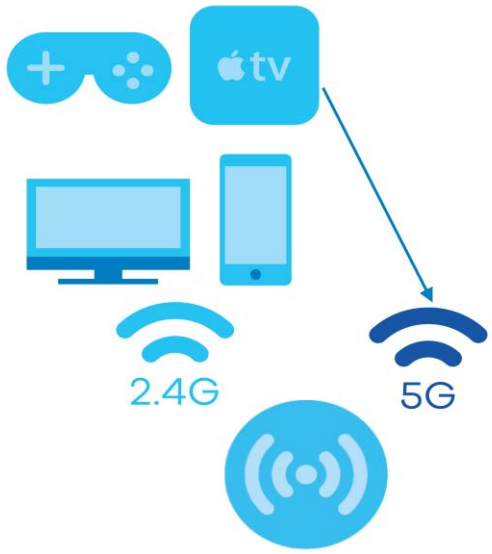
- AP steering allows WiFi clients to roam seamlessly between Mesh supported devices in your Mesh network by using the same SSID and WiFi password. Also, AP steering helps monitor WiFi clients and drop their connections to optimize the WX Device bandwidth when the clients are idle or have a low signal. When a WiFi client is dropped, it has the opportunity to reconnect to a Mesh AP with a strong signal.

Figure 4 AP Steering Application



- Band steering allows 2.4 GHz / 5 GHz dual-band WiFi clients to move from one band to another. For example, if the 2.4 GHz channel is congested, WiFi clients that support 5 GHz can move to the 5 GHz band.

Figure 5 Band Steering Application



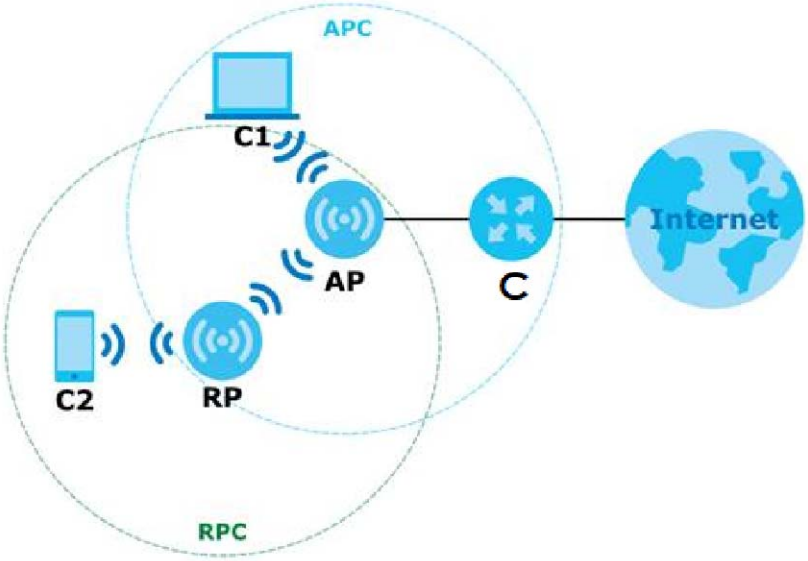
1.2.2 Network Controller

To set up a Mesh network, you need a router or an AP that can function as a controller. A controller manages and coordinates WiFi activity in a network.

A controller also manages the SSIDs and passwords on all APs in a network (auto-configuration). For example, if you change the SSID on the controller, the SSID of each AP in the network will also change.

Note: For AP steering and band steering to work, the controller and all the APs in the network need to have the same SSID and password. Therefore, we recommend using the controller to change the SSID and password.

Figure 6 Mesh Application



The following table describes the icons used in the figure.

Table 3 Icons Used in Mesh Application

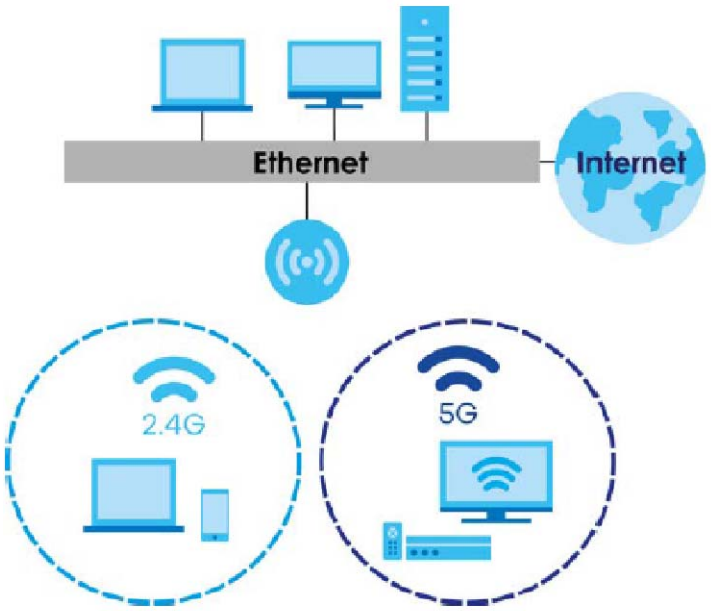
ICON	DESCRIPTION
C	Router Controller (the DX5301-B0 in Scenario 1, see Section 4.3.1 on page 38) or AP controller (the first WX Device in Scenario 2, see Section 4.3.2 on page 43)
AP	Access Point
RP	Repeater
C1	Client1
C2	Client2
APC	Access Point coverage area
RPC	Repeater coverage area

Note: Your router must have an Internet connection whether it supports MPro Mesh or not.

1.3 Dual-Band WiFi

The WX Device is a dual-band device that can use both 2.4 GHz and 5 GHz at the same time. IEEE 802.11a/b/g/n/ac/ax compliant clients can wirelessly connect to the WX Device to access network resources. 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-Band Application



1.4 Daisy Chain

You can add more WX Device to your network to form a daisy chain. Daisy chain refers to the connection from the first WX Device to up to three other WX Devices to extend the WiFi connection from the router to the client. The WX Device uplink connection determines the mode: **Access Point** (AP) or **Repeater** (RP).

- If the WX Device has a wired uplink connection, it is in AP mode.
- If the WX Device has a WiFi uplink connection, it is in RP mode.

Here are some example scenarios for the WX Device's daisy chain connection:

Figure 8 Scenario 1: Three APs

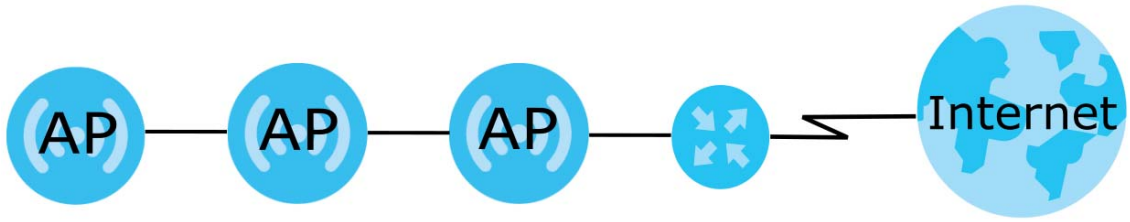


Figure 9 Scenario 2: Two APs and one RP

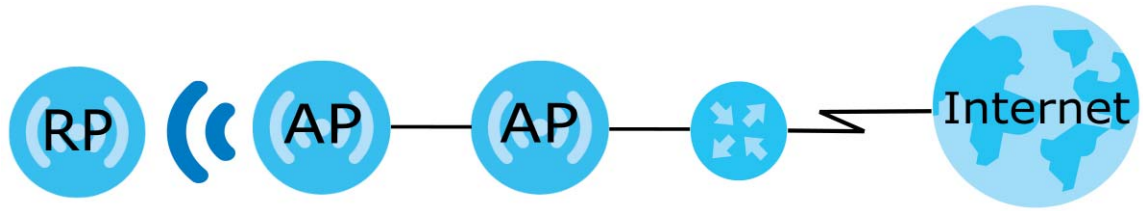


Figure 10 Scenario 3: One AP and two RPs

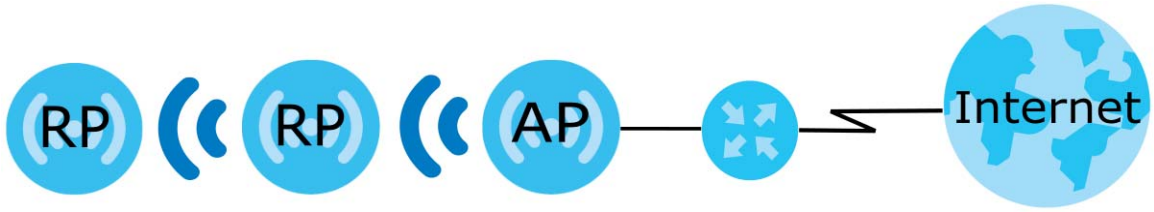
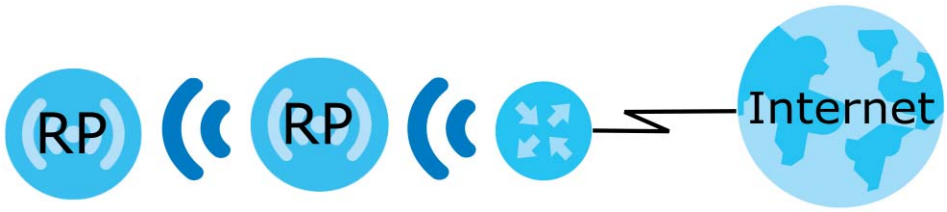


Figure 11 Scenario 4: Two RPs



Note: Set up your network as in Scenarios 1-3 if your router does not support Zyxel MPro Mesh. Scenario 4 is only for routers that support Zyxel MPro Mesh.

Note: We do not recommend connecting more than three WX Devices in your daisy chain network. If you already have two WX Devices in RP mode, we do not recommend adding another WX Device as a repeater.

CHAPTER 2
Hardware

This section describes the front and back panel of the WX Device. Refer to the Quick Start Guides to see how to make the hardware connections.

2.1 Front Panel and LEDs

Use the LEDs to determine if the WX Device is behaving normally or if there are problems on your network.

See Table 5 on page 21 and Table 6 on page 22 for more information on the LEDs.

Figure 12 WX3401-B0 Front Panel

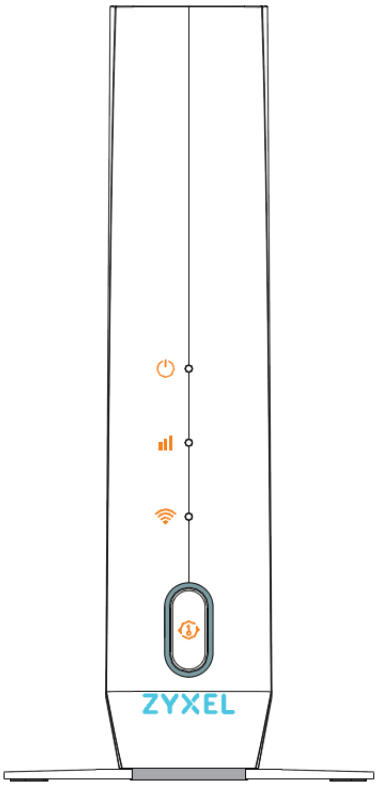


Figure 13 WX5600-T0 / WX3100-T0's Front Panel

2.2 Rear Panel

Figure 14 WX3401-B0 Rear Panel

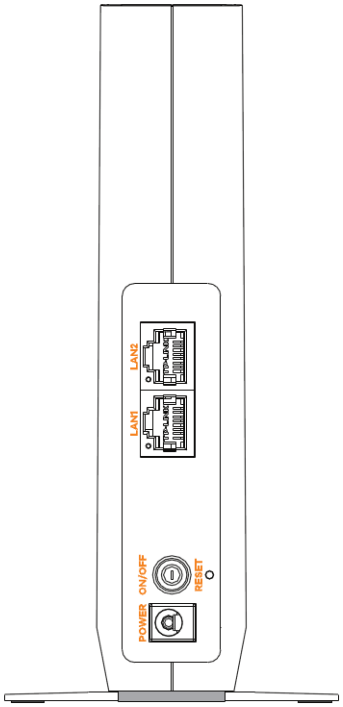


Figure 15 WX5600-T0 / WX3100-T0 Rear Panel

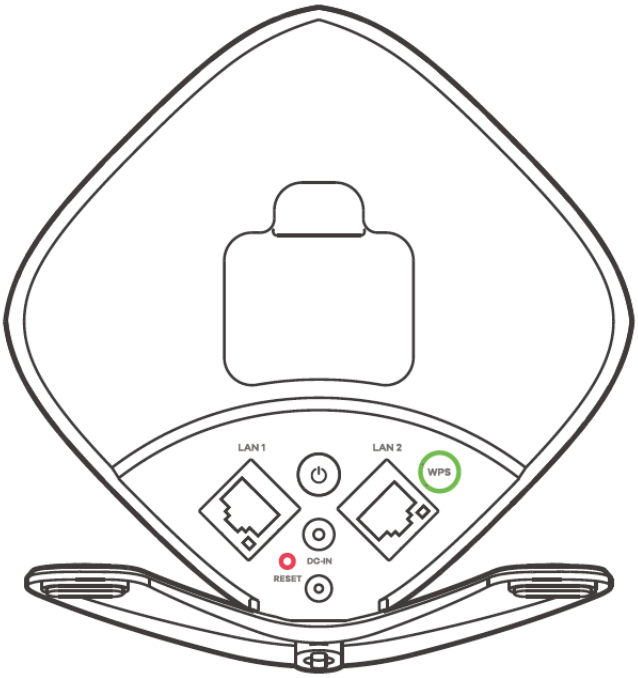


Table 4 Panel Ports and Buttons

LABEL	DESCRIPTION
LAN1/LAN2	Connect computers or other Ethernet devices to Ethernet ports for Internet access.
WPS	Press the **WPS** button once for 1 to 3 seconds to enable the AP/Repeater mode. (See Section 2.5.1 on page 26 for more information)
POWER ON/OFF or DC-IN	Connect the power cable and then press the power button to start the device.
RESET	Press the button to return the WX Device to the factory defaults.

2.3 LEDs (Lights)

None of the LEDs are on if the Zyxel Device is not receiving power.

Table 5 LED Table (for WX Device-1)

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	Power is on or MPro Mesh pairing is done.
		Blinking	The WX Device is starting up or the MPro Mesh pairing is in process.
	Red	On	The WX Device detects a system error.
		Blinking	The WX Device is upgrading firmware or the MPro Mesh pairing has failed.
Link (With a WiFi connection)	Green	On	The WiFi connection to the MPro Mesh router is good.
	Red	On	The signal is too weak. Move the WX Device closer to the MPro Mesh Router.

Table 5 LED Table (for WX Device-1) (continued)

LED	COLOR	STATUS	DESCRIPTION
Link (With a wired connection) 	Green	On	The Ethernet cable is connected to the LAN port on the WX Device.
WiFi 	Green	On	The 2.4G / 5G WiFi is ready.
		Blinking	The WX Device is transmitting/receiving WiFi data.
		Off	The 2.4G / 5G WiFi is disabled.
WPS 	Amber	On	This indicates the WX Device is the controller.
		Blinking	If you press the WPS button, amber blinking within 120 seconds means the WPS is in process.
		Off	The WPS process is done.

Table 6 LED Table (for WX Device-2)

LED	COLOR	STATUS	DESCRIPTION
POWER 	Green	On	Power is on or MPro Mesh pairing is done.
		Blinking	The WX Device-2 is starting up or the MPro Mesh pairing is in process.
	Red	On	The WX Device-2 detects a system error.
		Blinking	The WX Device-2 is upgrading firmware or the MPro Mesh pairing has failed.
Link (with a WiFi connection) 	Green	On	The WiFi connection to the WX Device-1 is good.
	Red	On	The signal is too weak. Move the WX Device-2 closer to the WX Device-1.
Link (with a wired connection) 	Green	On	The Ethernet cable is connected to the LAN port on the WX Device-2.
WiFi 	Green	On	The 2.4 G / 5 G WiFi is ready.
		Blinking	The WX Device-2 is transmitting/receiving WiFi data.
		Off	The 2.4 G / 5 G WiFi is disabled.
WPS 	Amber	Blinking	If you press the WPS button, amber blinking within 120 seconds means the WPS is in process.
		Off	The WPS process is done.

2.4 Wall Mounting

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

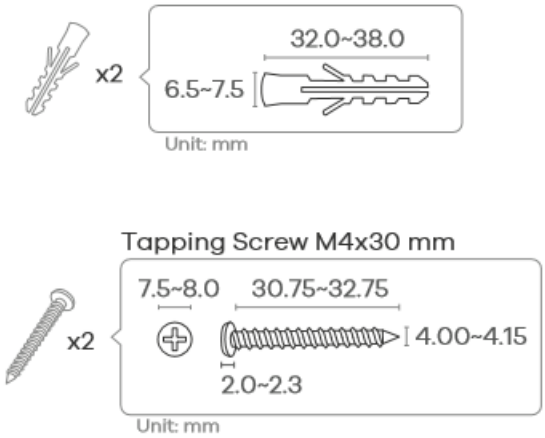
2.4.1 WX3401-B0 Wall-Mounting

You may need screw anchors if mounting on a concrete or brick wall.

Table 7 The WX3401 Wall Mounting Information

Distance between holes	89.00 mm
M4 Screws	Two
Screw anchors (optional)	Two

Figure 16 The WX3401 Screw Specifications

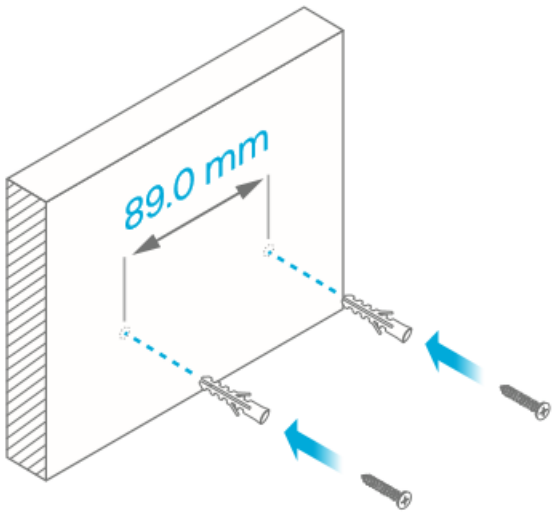


1 Select a position free of obstructions on a wall strong enough to hold the weight of the device.

2 Mark two holes on the wall at the appropriate distance apart for the screws.

Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

Figure 17 WX3401 Wall Mounting Distance



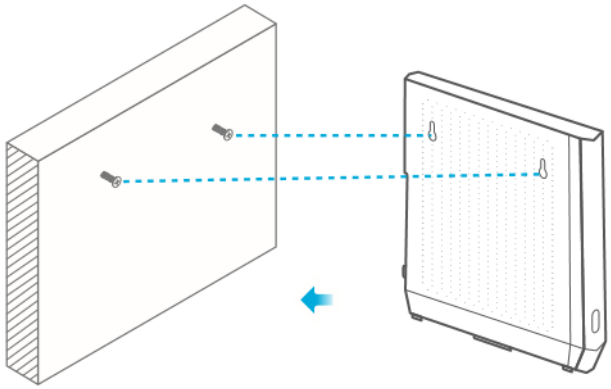
3 If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do not insert the screws all the way in – leave a small gap of about 0.5 cm.

If not using screw anchors, use a screwdriver to insert the screws into the wall. Do not insert the screws all the way in – leave a gap of about 0.5 cm.

4 Make sure the screws are fastened well enough to hold the weight of the WX Device with the connection cables.

5 Align the holes on the back of the WX Device with the screws on the wall. Hang the WX Device on the screws.

Figure 18 WX3401 Wall Mounting Example



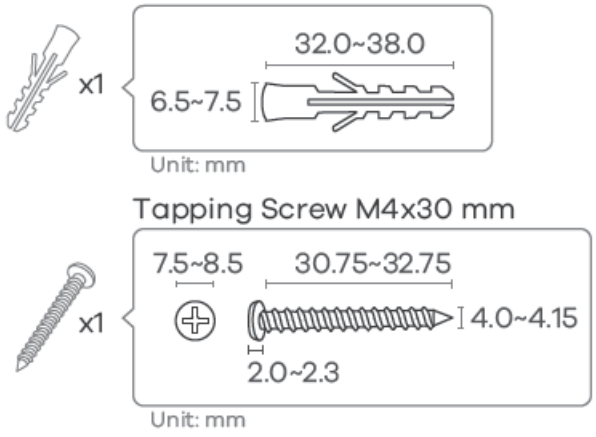
2.4.2 WX5600-T0 / WX3100-T0 Wall-Mounting

You may need screw anchors if mounting on a concrete or brick wall.

Table 8 WX5600-T0 / WX3100 Wall Mounting Information

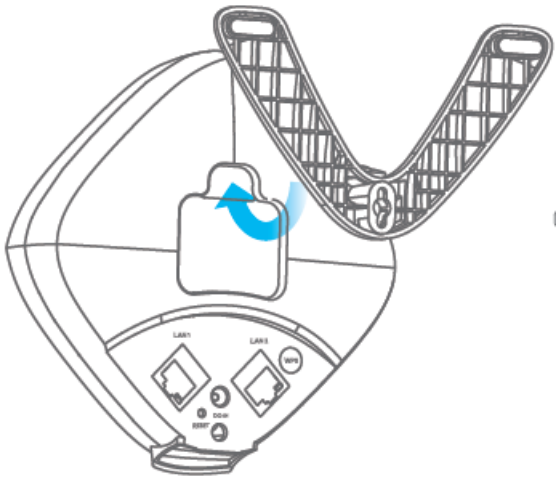
M4 Screws	One
Screw anchors (optional)	One

Figure 19 WX5600-T0 / WX3100 Screw Specifications



1 Attach the bracket to the back of the WX5600-T0 / WX3100-T0 as shown.

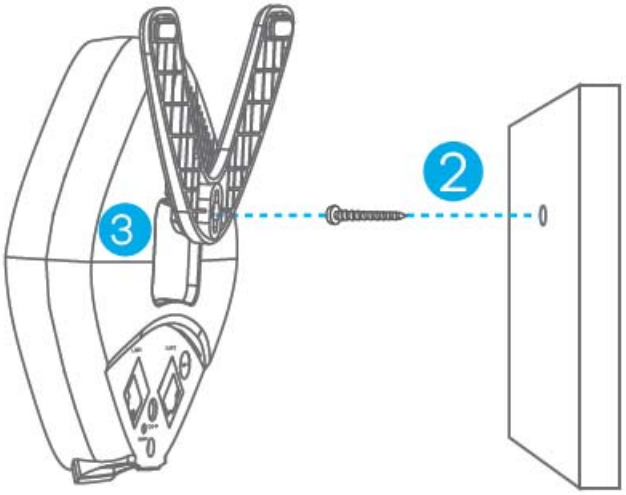
Figure 20 Attach the bracket



2 Drill a hole in the wall. Insert the screw anchor and screw into the hole.

3 Place the WX5600-T0 / WX3100-T0 so the wall mount hole lines up with the screw. Slide the WX5600-T0 / WX3100-T0 down gently to fix it into place.

Figure 21 Wall Mounting



2.5 WPS Button

Your WX Device supports WiFi Protected Setup (WPS), which is an easy way to set up a secure WiFi network. WPS is an industry standard specification, defined by the Wi-Fi Alliance.

WPS allows you to quickly set up a WiFi network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (recommended) on the device

itself, or in its Web Configurator. When WPS is activated on a device, it has 2 minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

The **WPS** button is located at the front panel of the WX Device.

2.5.1 Using the WPS Button

1. Make sure the power LED is on (not blinking).
2. Choose a mode
   - APC mode
     1. Press the WX Device **WPS** button just once for 1 to 3 seconds. The WPS LED should start blinking.
     2. Press the WPS button on the client within 2 minutes.
   - AP Mode (Downlink Daisy Chain For MPro Mesh)
     1. Press the first WX Device **WPS** button just once for 1 to 3 seconds.
     2. Press the **WPS** button once on the downlink WX Device within 2 minutes.
   - Repeater mode (modem/router to the WX Device)
     1. Press the WPS button on the modem/router. Release it when the WPS LED blinks.
     2. Press the WX Device **WPS** button just once for 1 to 3 seconds within 2 minutes to copy the WiFi settings from your modem/router to the WX Device.
     3. The Link LED lights up when the process is finished.
   - Repeater mode (the WX Device to the WiFi client)
     1. Press the WX Device **WPS** button just once for 1 to 3 seconds to copy the WiFi settings from the WX Device to a WiFi client, such as your laptop.
     2. Wait until the WPS LED blinks.
     3. Press the WPS button on the client within 2 minutes.
   - Repeater mode (Downlink Daisy Chain For MPro Mesh)
     1. Press the first WX Device **WPS** button just once for 1 to 3 seconds.
     2. Press the **WPS** button once on the downlink WX Device within 2 minutes.

Note: You must activate WPS in the WX Device and in another WiFi device within 2 minutes of each other. Repeat this procedure separately for each WiFi client.

Note: With WPS, WiFi clients will only connect to the first WiFi network (SSID) in either a 2.4 GHz or 5 GHz WiFi network.

2.6 RESET Button

If you forget your password or you cannot access the Web Configurator, you will need to use the **RESET** button at the back of the WX Device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the password will be reset to the default key on the device label.

2.6.1 Using the RESET Button

1. Make sure the power LED is on (not blinking).
2. Press the **RESET** button for longer than 5 seconds to set the WX Device back to its factory-default configurations.

CHAPTER 3
Web Configurator

3.1 Overview

The Web Configurator is an HTML-based management interface that allows easy system setup and management through an Internet browser. Use a browser that supports HTML5, such as Microsoft Edge, Mozilla Firefox, or Google Chrome. 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).

3.2 Accessing the Web Configurator

3.2.1 When the WX Device is connected to a modem/router

When your WX Device is in the AP mode:

1. Connect your computer to the LAN port of the WX Device using an Ethernet cable.
2. Connect your computer to a LAN port of the router. Log into the router's Web Configurator to check the IP address the router assigned to your WX Device.
3. Open a web browser such as Microsoft Edge and enter “http:// (DHCP-assigned IP)” as the web address in your web browser.
4. Log into the Web Configurator.

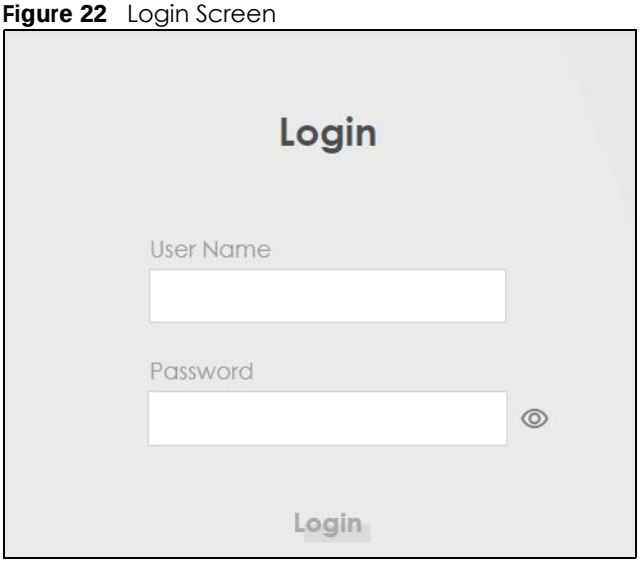
When your WX Device is in the Repeater mode:

1. Connect a modem/router to the first WX Device wirelessly.
2. Connect your computer to a LAN port of the router. Log into the router's Web Configurator to check the IP address the router assigned to your WX Device.
3. Open a web browser such as Microsoft Edge and enter “http:// (DHCP-assigned IP)” as the web address in your web browser.
4. Log into the Web Configurator.

3.2.2 When the WX Device is not connected to a router/modem:

1. Make sure your WX Device hardware is properly connected (refer to the Quick Start Guide).
2. Give your computer a fixed IP address in the range between 192.168.1.3 and 192.168.1.254.
3. After you have set your computer's IP address, open a web browser such as Microsoft Edge and enter "http://192.168.1.2" as the web address in your web browser.
4. Log into the Web Configurator.
5. A login screen displays. Select the language you prefer.
6. To access the administrative Web Configurator and manage the WX Device, enter the default user name **admin** and the randomly assigned default password (see the device label) on the login screen and click **Login**. If you have changed the password, enter your password and click **Login**.

Figure 22 Login Screen



Note: The default allowable times that you can enter the **Password** is 3. If you entered the wrong password for the fourth time, by default the Web Configurator will lock itself for 5 minutes before you can try entering the correct **Password** again. You can change these settings at **Maintenance** > **User Account** > **Add New** / **Edit Account** (see Section 13.2.1 on page 151).

7. The following screen displays when you log into the Web Configurator for the first time. Enter a new password, re-enter it to confirm, and click **Change password**. If you prefer to use the default password, click **Skip**.

Figure 23 Change Password Screen (WX3100-T0 / WX3401-B0)

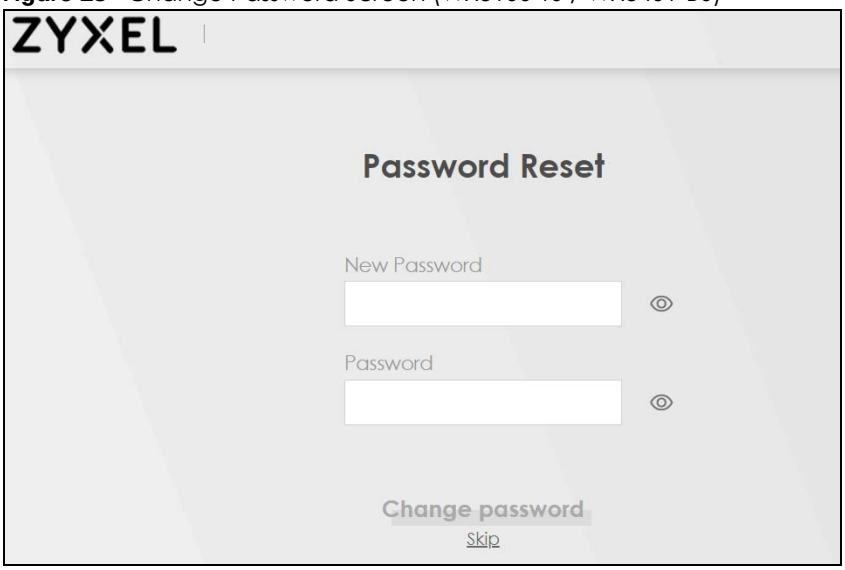
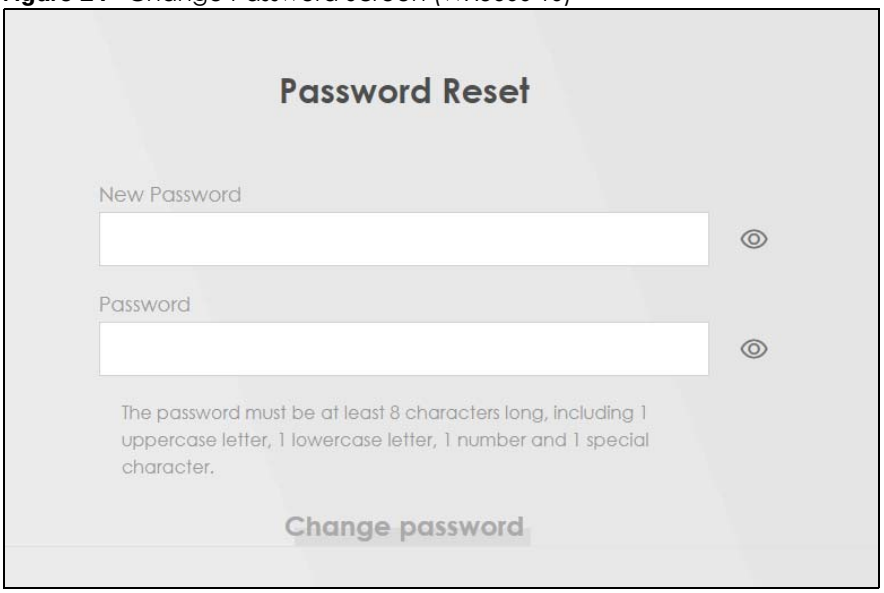
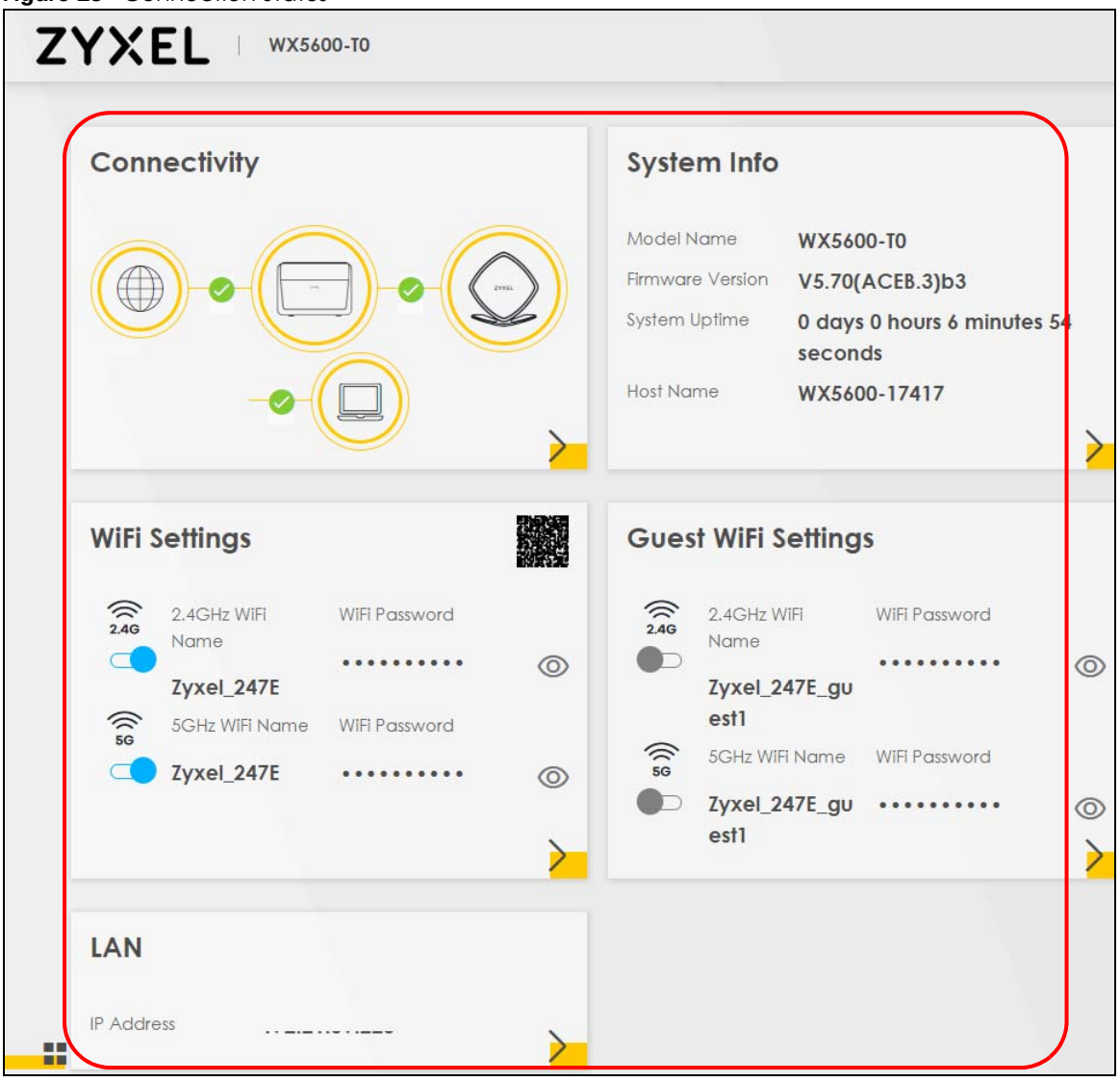


Figure 24 Change Password Screen (WX5600-T0)



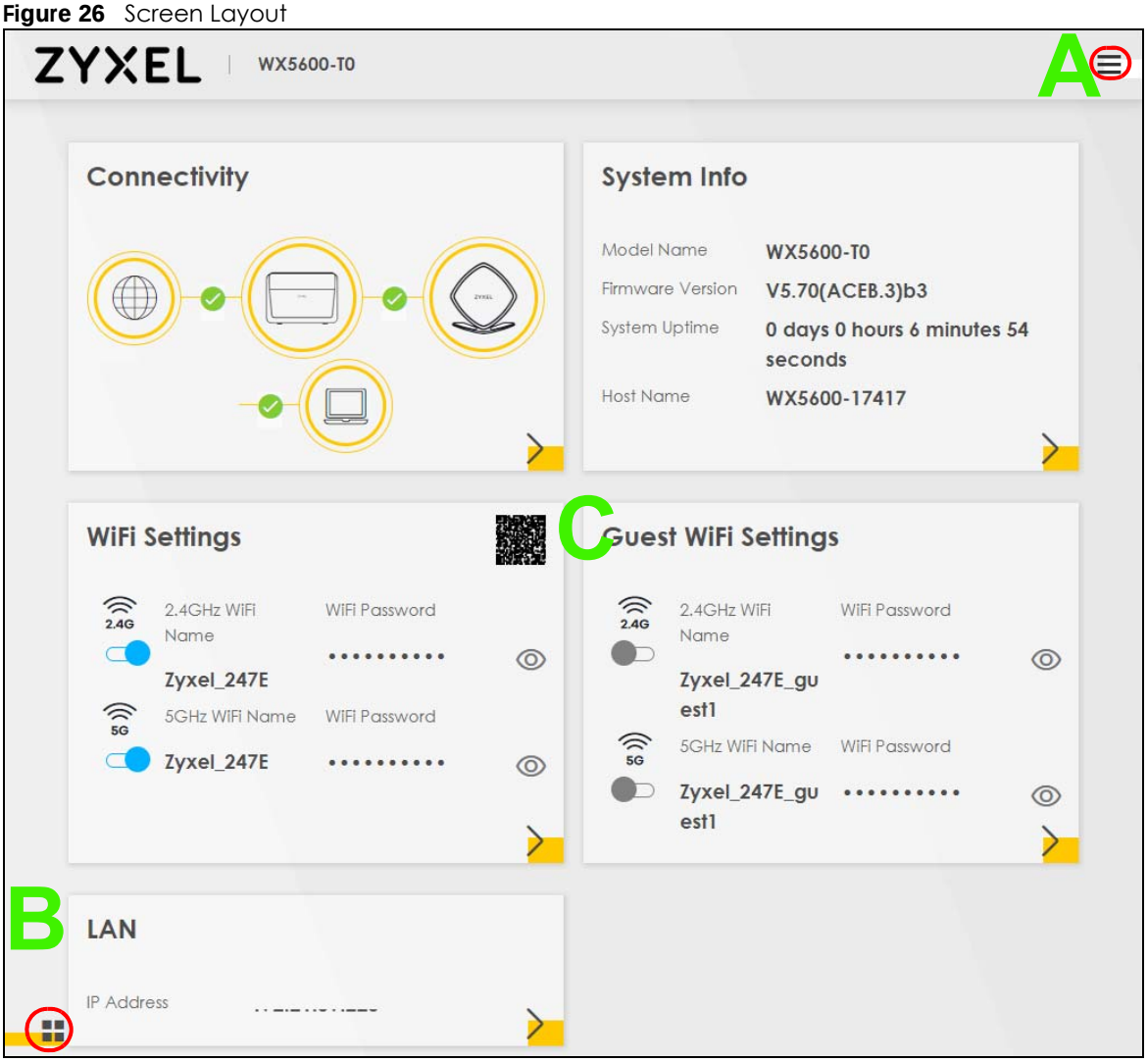
8 The **Connection Status** page appears. Use this screen to configure basic Internet access and WiFi settings (see Section 5.1 on page 72 for details).

Figure 25 Connection Status



3.3 Web Configurator Layout

Figure 26 Screen Layout



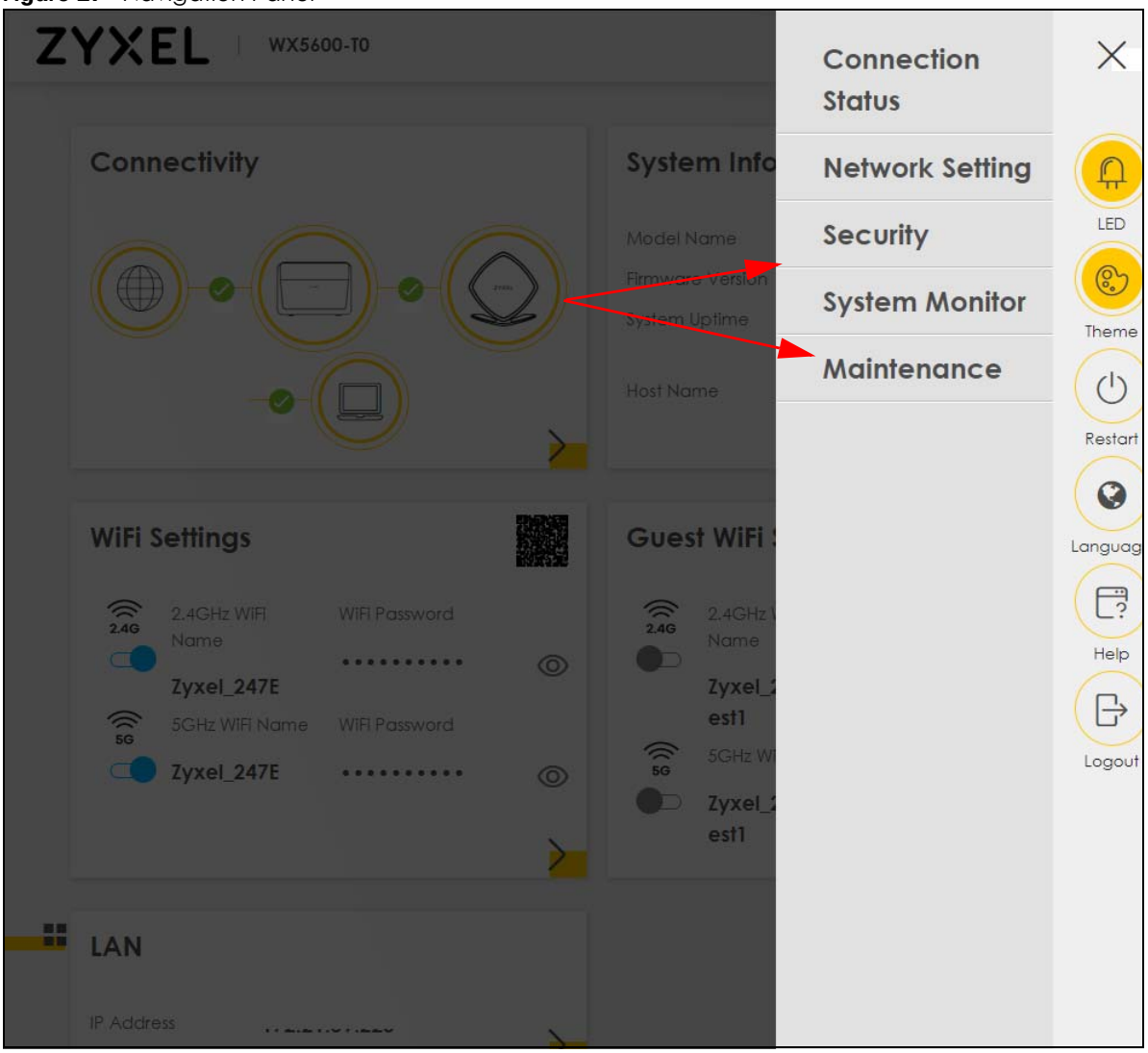
As illustrated above, the main screen is divided into these parts:

- **A** – Navigation Panel
- **B** – Layout Icon
- **C** – Main Window

3.3.1 Navigation Panel

Click the menu icon ( ) to display the navigation panel that contains configuration menus and icons (quick links). Click **X** to close the navigation panel.

Figure 27 Navigation Panel



3.3.1.1 Configuration Menus

Use the menu items on the navigation panel to open screens to configure WX Device features. The following tables describe each menu item.

Table 9 Configuration Menus Summary

LINK	TAB	FUNCTION
Connection Status		Use this screen to configure basic Internet access and WiFi settings. This screen also shows the network status of the WX Device and computers/ devices connected to it.
Network Setting		
Wireless	General	Use this screen to configure the WiFi settings and WiFi authentication/ security settings.
	Guest/More AP	Use this screen to configure multiple BSSs on the WX Device.
	MAC Authentication	Use this screen to block or allow WiFi traffic from WiFi devices of certain SSIDs and MAC addresses to the WX Device.

Table 9 Configuration Menus Summary (continued)

LINK	TAB	FUNCTION
	WPS	Use this screen to configure and view your WPS (WiFi Protected Setup) settings.
	WMM	Use this screen to enable or disable WiFi MultiMedia (WMM).
	Others	Use this screen to configure advanced WiFi settings.
	Channel Status	Use this screen to scan WiFi channel noises and view the results.
Home Networking	Home Networking	Use this screen to configure DHCP/Static IP settings, and other advanced properties.
Security		
Certificates	Local Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CA	Use this screen to view and manage the list of the trusted CAs.
System Monitor		
Log	Log	Use this screen to view the status of events that occurred to the WX Device. You can export or email the logs.
WLAN Station Status	WLAN Station Status	Use this screen to view the WiFi stations that are currently associated with the WX Device.
Maintenance		
System	System	Use this screen to set Device name.
User Account	User Account	Use this screen to change user password on the WX Device.
Remote Management	Remote Management	Use this screen to enable specific traffic directions for network services.
Time	Time	Use this screen to change your WX Device's time and date.
Email Notification	Email Notification	Use this screen to configure up to two mail servers and sender addresses on the WX Device.
Log Setting	Log Setting	Use this screen to change your WX Device's log settings.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your WX Device.
Backup/Restore	Backup/Restore	Use this screen to backup and restore your WX Device's configuration (settings) or reset the factory default settings.
Reboot	Reboot	Use this screen to reboot the WX Device without turning the power off.
Diagnostic	Ping&Traceroute	Use this screen to identify problems with the WX Device. You can use Ping or TraceRoute to help you identify problems.

3.3.1.2 Icons

The navigation panel provides some icons on the right hand side.

Figure 28 Icons of Navigation Panel (WX3401-B0/WX3100-T0)

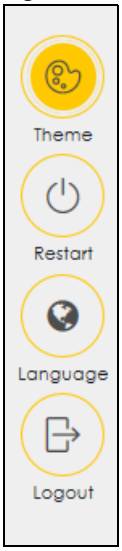
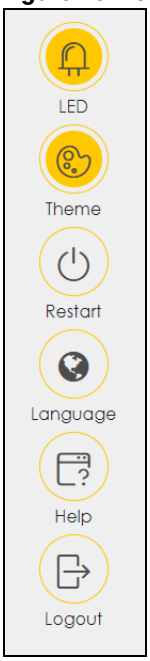
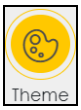
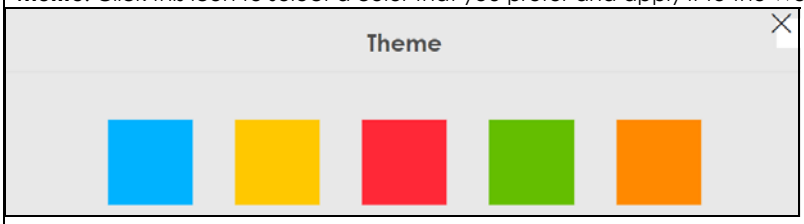
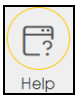


Figure 29 Icons of Navigation Panel (WX5600-T0)



The icons provide the following functions.

Table 10 Web Configurator Icons

ICON	DESCRIPTION
	**LED**: Click this icon to turn off/on the WX Device's panel LEDs.
	**Theme**: Click this icon to select a color that you prefer and apply it to the Web Configurator. 
	**Restart**: Click this icon to reboot the WX Device without turning the power off.
	**Language**: Select the language you prefer.
	**Help**: Click this link to display web help pages. The help pages provide descriptions for all of the configuration screens.
	**Logout**: Click this icon to log out of the Web Configurator.

PART II
Technical Reference

CHAPTER 4
App Tutorials

4.1 Overview

This shows you how to use the MPro Mesh app to manage the WX Device and its Mesh network.

4.2 What You Can Do

- To set up your WX Device with a Zyxel MPro Mesh router using a WiFi connection; see Section 4.3.1 on page 38.
- To set up your WX Device with a non-MPro Mesh router using a wired connection; see Section 4.3.2 on page 43.
- Use the **Home** screen to reboot your WX Device or add WX Devices to your network; see Section 4.4 on page 50.
- Use the **Devices** screen to view the information of WiFi clients connected to the WX Device; see Section 4.5 on page 62.
- Use the **WiFi Settings** screen to configure your main or guest WiFi network; see Section 4.6 on page 64.
- Use the **Account** screen to view your app version or logout; see Section 4.8 on page 70.

4.3 Network Setup

There are several ways to set up your WX Device. You can set it up with a Zyxel MPro Mesh router using a wired or WiFi connection. Alternatively, you can set it up with a non-MPro Mesh router with a wired connection. This section shows you how to connect to a Zyxel MPro Mesh router wirelessly and how to connect to a non-MPro Mesh router with an Ethernet cable. See the following table for more information.

Table 11 Network Setup Scenario

SCENARIO	ZYXEL MPRO MESH ROUTER	NON-ZYXEL MPRO MESH ROUTER
Wired connection from the router to the WX Device	Yes	Yes (see Section 4.3.2 on page 43)
WiFi connection	Yes (see Section 4.3.1 on page 38)	No

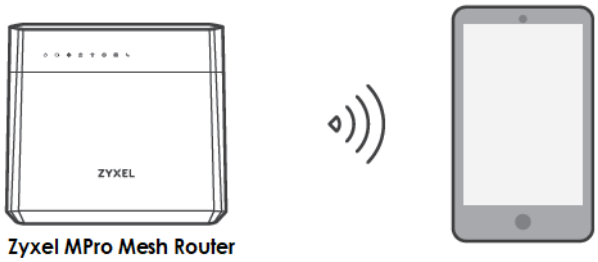
4.3.1 Setting up the WX Device with a Zyxel MPro Mesh Router

Follow the steps below to set up your WX Device with the Zyxel MPro Mesh router. This section uses the WX3401-B0 and DX5301-B0 as an example.

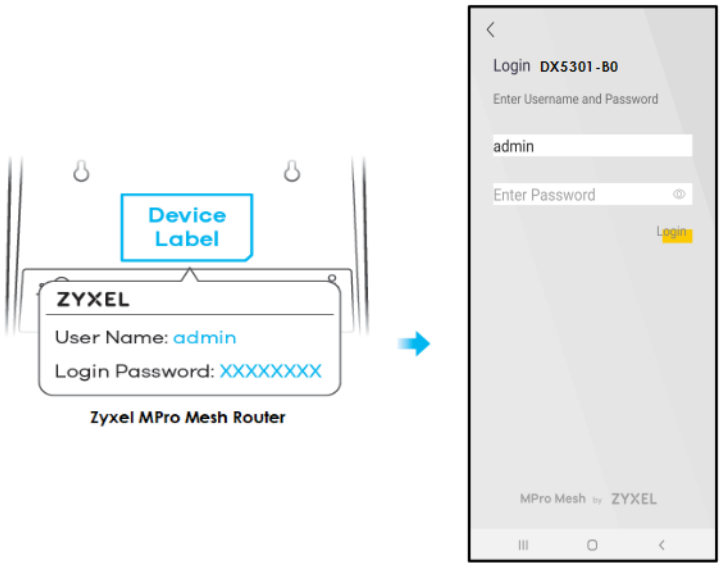
1 Download the MPro Mesh app from Google Play or Apple Store.

2 Connect your mobile device to the WiFi network of the Zyxel MPro Mesh router. Note the SSID and password on the back label of the Zyxel MPro Mesh router. Find this SSID on your mobile device. Enter the key to connect to your router.

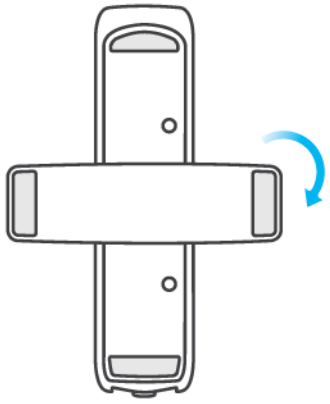
Note: The Zyxel MPro Mesh router is the WiFi controller, so you must connect to it to use the MPro Mesh app to manage WiFi settings.



3 Connect the MPro Mesh app to the Zyxel MPro Mesh router. Open the app, enter the user name and password on the back label of your Zyxel MPro Mesh router to log in the **Home** page of the app.

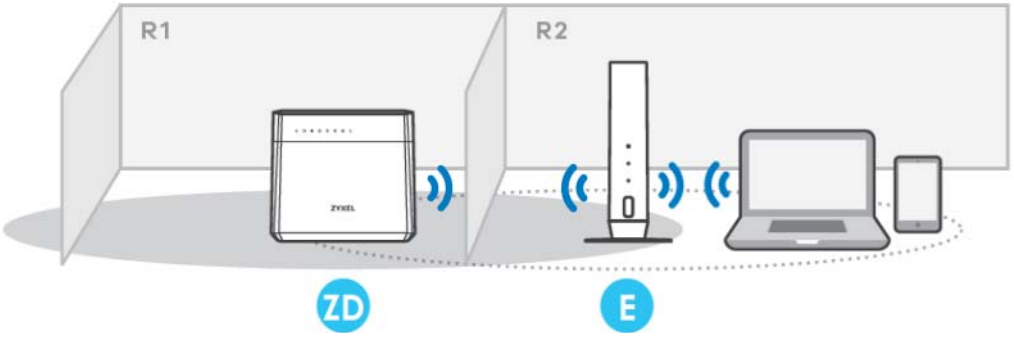


4 Rotate the stand on the bottom of the WX Device 90 degrees.

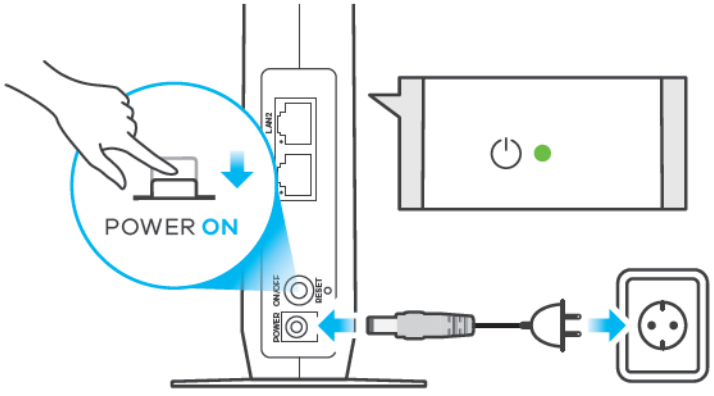


Bottom view

5 Place the WX Device where you want to extend the coverage of your WiFi network.

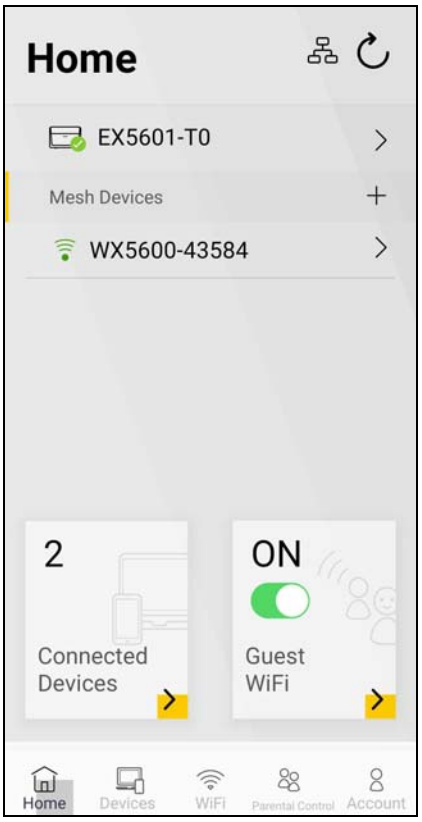


6 Plug in the power cable and switch on the WX Device. Wait until the **POWER** LED turns steady green. This may take up to 2.5 minutes.

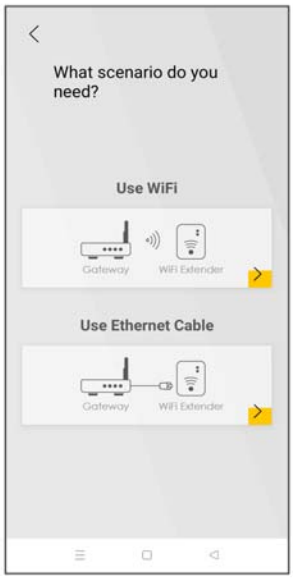


Rear Panel

7 Open the MPro Mesh app. On the **Home** screen, tap the + icon to add a WX Device.

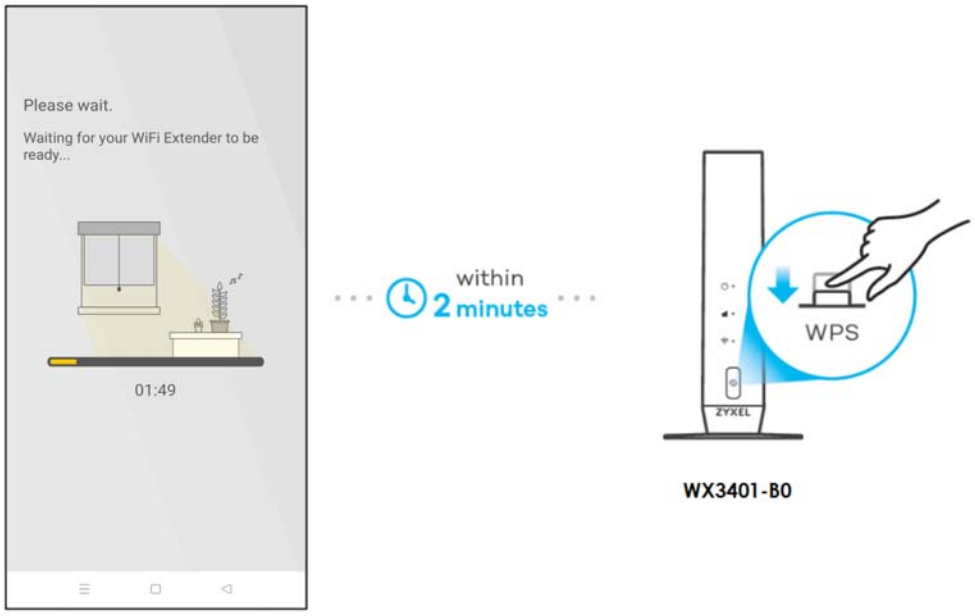


8 Select the **Use WiFi** scenario. Follow the instructions to start pairing the WX Device with a Zyxel MPro Mesh router (with the WX3401-B0 and the DX5301-B0 as an example). Once the pairing starts, a 2-minute countdown timer will begin.



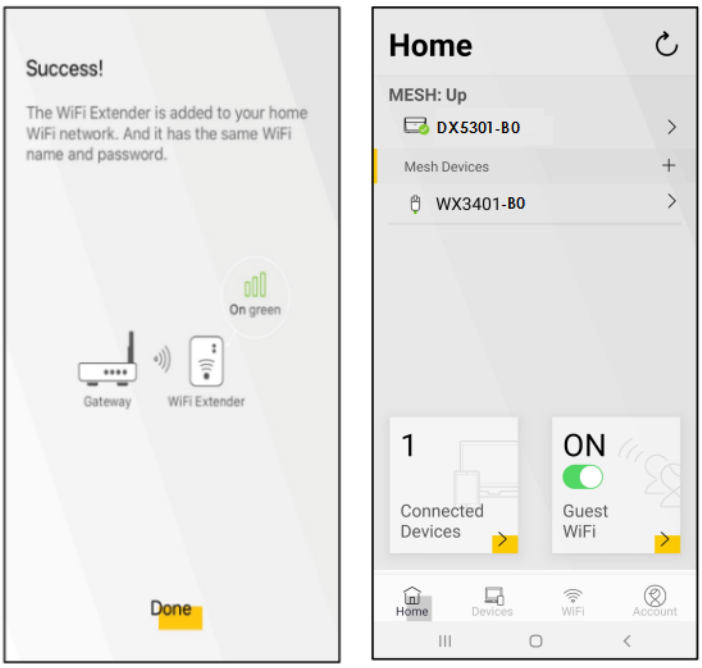
9 Within 2 minutes, press the WPS button once on the WX Device until the WiFi LED starts blinking slowly.

Note: You do not need to press the WPS button on the Zyxel MPro Mesh router.



10 After the WiFi LED turns steady green or fast blinking, wait for up to 2 minutes. The **POWER** LED should start blinking. The **POWER** and **LINK** LED will turn solid green if the pairing process is successful. You can also check the result on the app screen.

11 Click **Done** to finish the pairing process. The MPro Mesh Router (the controller) will undergo an auto-configuration after a Mesh network is established. (See Section 1.2 on page 15 for more information.) Check the status of your MPro Mesh network on the **Home** screen.



12 The **POWER** LED shows if the WX Device is ready to join the WiFi network. The **LINK** LED shows the WiFi link quality. See Section Table 12 on page 43 for more information on LED behaviors.

Table 12 LED Table (for WX Device-1)

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	Power is on or the MPro Mesh configuration process is done.
		Blinking	The WX Device is starting up or under the MPro Mesh configuration process.
	Red	On	The WX Device detects a system error.
		Blinking	The WX Device is upgrading firmware.
Link (With a WiFi connection)	Green	On	The WiFi connection to the MPro Mesh router is good.
	Red	On	The signal is too weak. Move the WX Device closer to the MPro Mesh router.

4.3.2 Setting up the WX Device with a Non-MPro Mesh Router

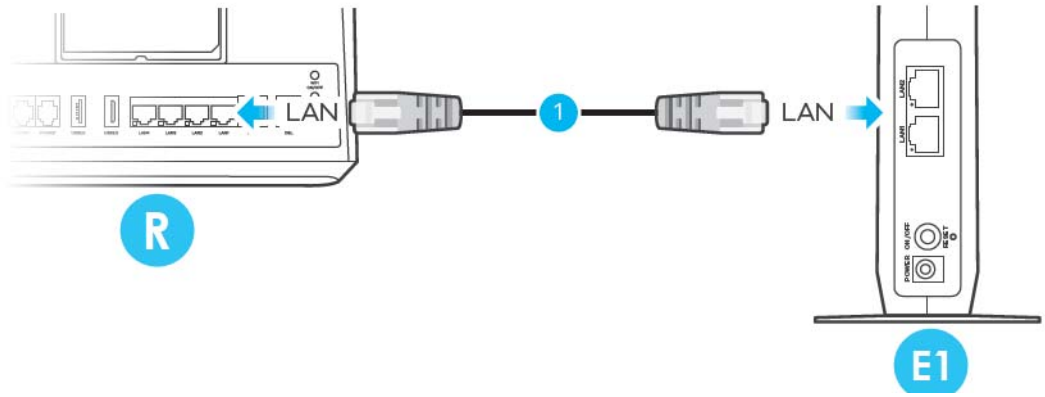
This scenario describes the process to create a Mesh network with a wired connection from the non-MPro Mesh router to the first WX Device (WX Device-1). This section uses a non-MPro Mesh router, the WX3401-1, and WX3401-2 as an example.

Make sure the non-MPro Mesh router is connected to the Internet. The first WX Device (WX Device-1) must be connected to your router using an Ethernet cable. Then, connect the second WX Device (WX Device-2) wirelessly to the first WX Device (WX Device-1).

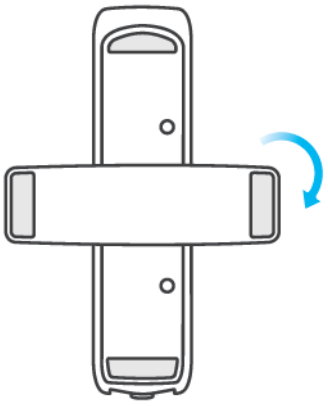
Follow the steps below to set up the WX Device-1 with a non-MPro Mesh router.

Connect the WX Device-1 to the Non-MPro Mesh Router

1 Use an Ethernet cable to connect the WX Device-1 to your non-MPro Mesh router.

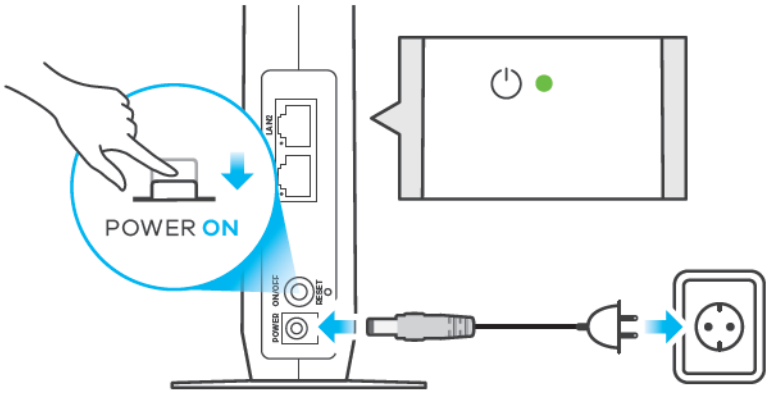


2 Rotate the stand on the bottom of the WX Device-1 90 degrees.



Bottom view

3 Plug in the power cable and switch on the WX Device-1. Wait until the **POWER** LED turns steady green. This may take up to 2.5 minutes.

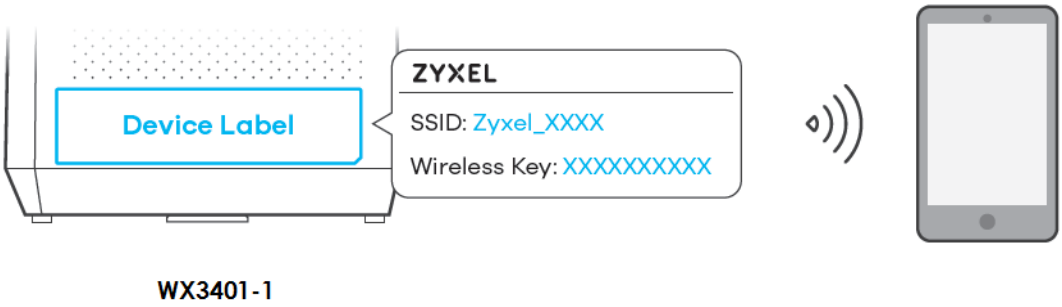


Rear Panel

4 On your mobile device, go to the WiFi settings. Long press your existing WiFi connection. Tap **Forget network** to remove your existing WiFi connection.

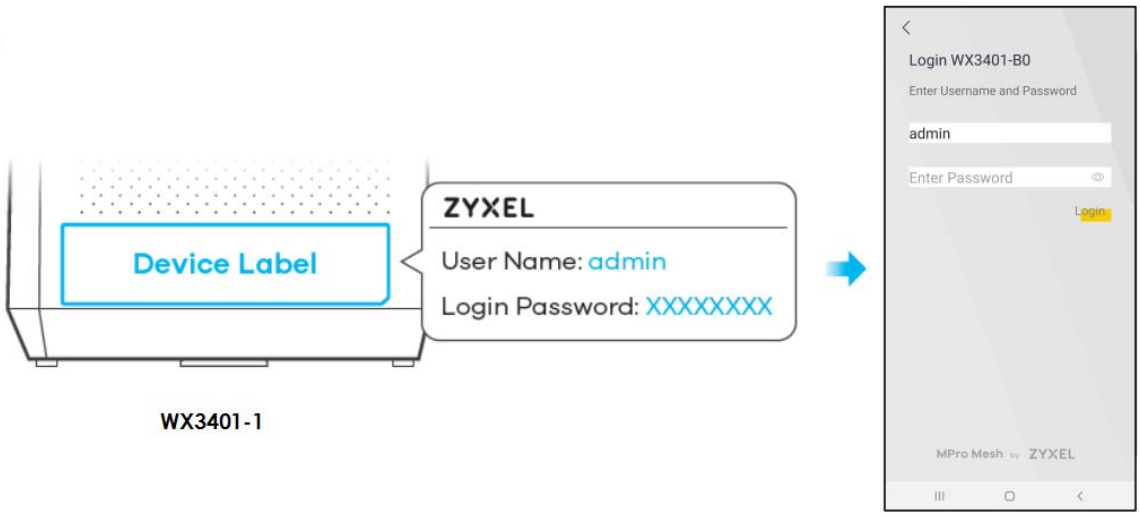
5 Connect your mobile device to the WiFi network of the WX Device-1. Note the SSID and key on the side label of the WX Device-1. Find this SSID on your mobile device. Enter the key to connect to your WX Device-1.

Note: In this scenario, WX Device-1 is the WiFi controller, so you must connect to it to use the MPro Mesh app to manage the WiFi network.



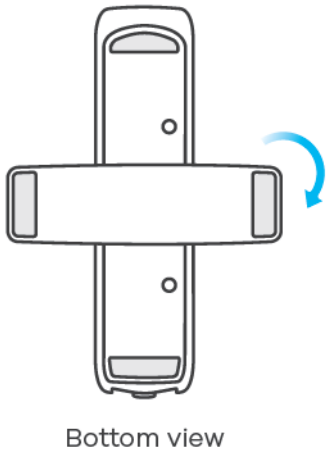
6 Download the MPro Mesh app from Google Play or Apple Store.

7 Connect the MPro Mesh app to the WX Device-1. Open the app, enter the user name and password on the side label of the WX Device-1 when prompted.

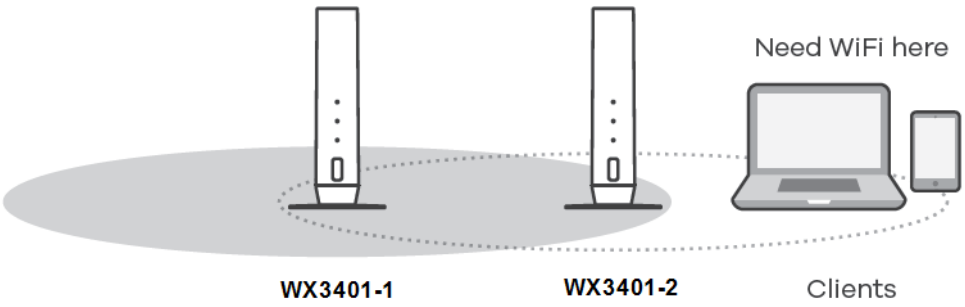


Connect the WX Device-2 to the WX Device-1

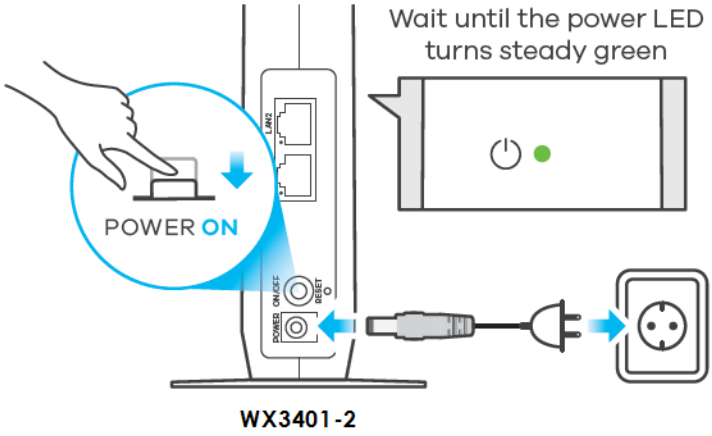
1 Rotate the stand on the bottom of the WX Device-2 90 degrees.



2 Place the WX Device-2 where you want to extend the coverage of your network.

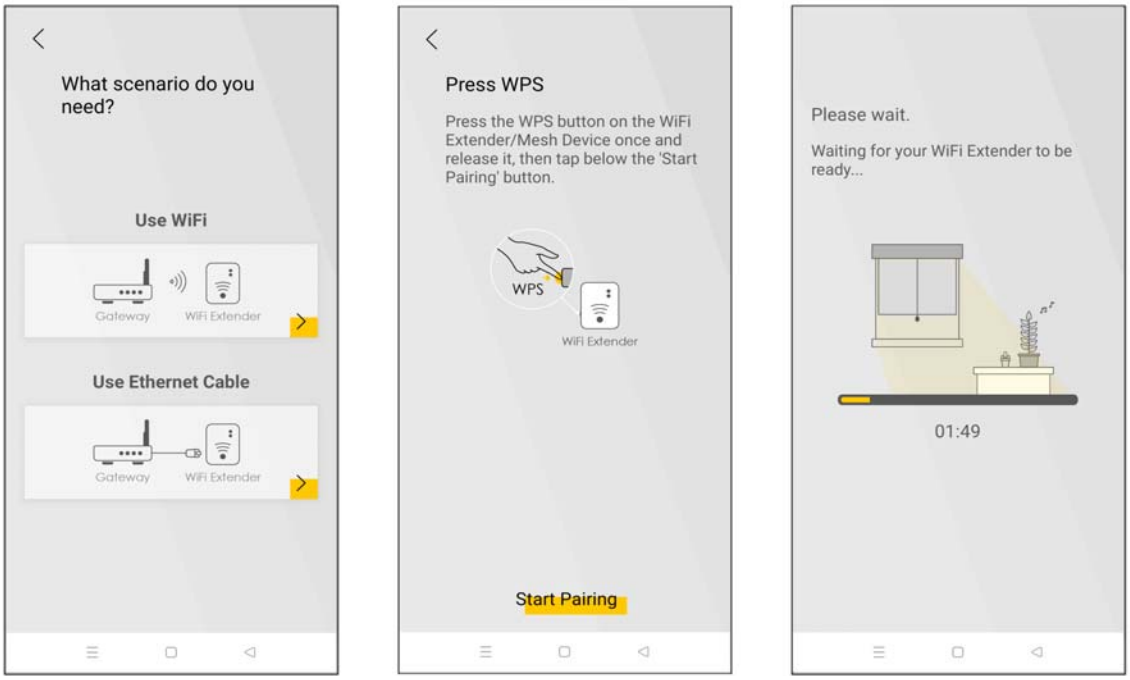


3 Plug in the power cable and switch on the WX Device-2. Wait until the **POWER** LED turns steady green. This may take up to 2.5 minutes.



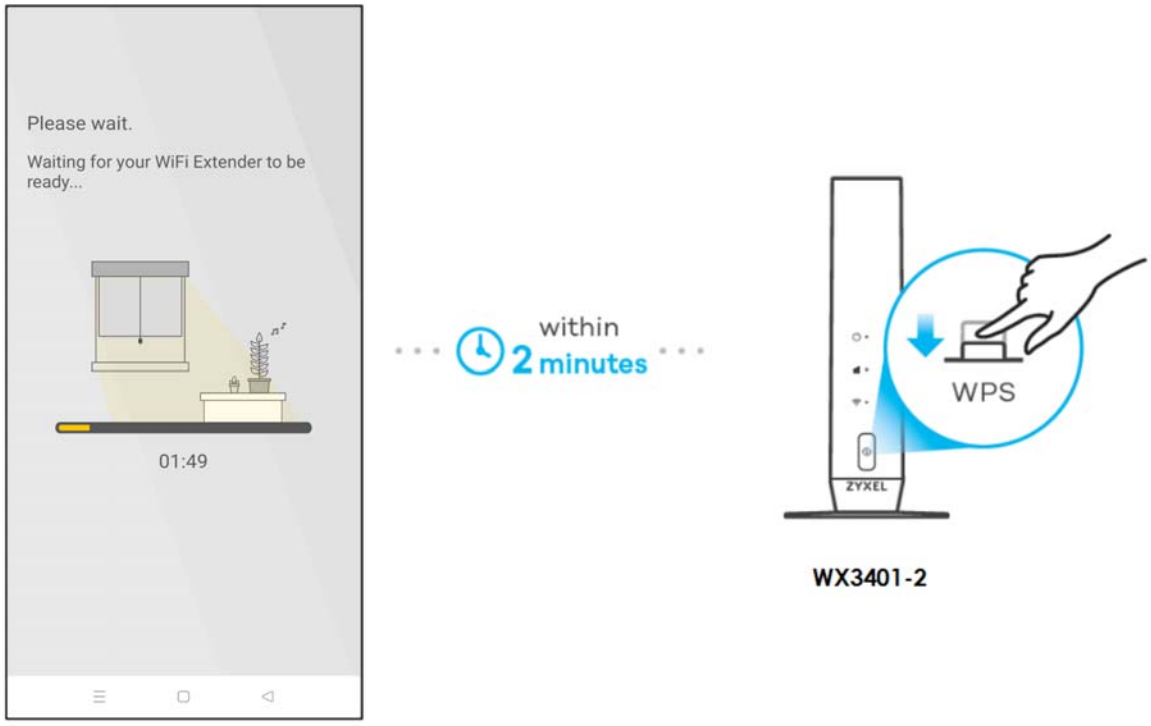
4 When the **POWER** LED on the WX Device-2 is steady green, open the MPro Mesh app. On the **Home** screen, tap the + icon to add the WX Device-2.

5 Select the **Use WiFi** scenario. Follow the instructions to start pairing the WX Device-2 with the WX Device-1. Once the pairing starts, a 2-minute countdown timer will begin.



6 Within 2 minutes, press the WPS button once on the WX Device-2 for less than 3 seconds.

Note: You do not need to press the WPS button on the WX Device-1.



7 The **POWER** and **Link** LED on the WX Device-2 turns steady green if the pairing process is successful. You can also check the result on the app screen.

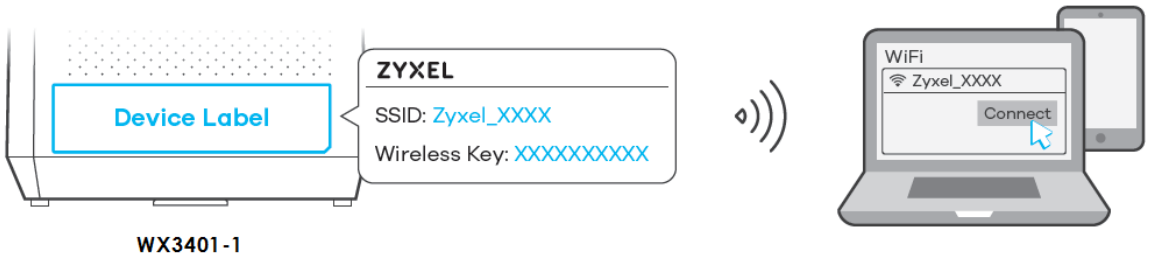
8 Click **Done** to finish the pairing process. The WX Device-1 (the controller) will undergo an automatic configuration after a Mesh network is established. (See Section 1.2 on page 15 for more information). Check the status of your WiFi Mesh network on the **Home** screen.

9 The **POWER** LED shows if the WX Device-2 is ready to join the WiFi network. The **LINK** LED shows the WiFi link quality. See Section Table 13 on page 49 for more information on LED behaviors.

Table 13 LED Table (for WX Device-2)

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	Power is on or the MPro Mesh configuration process is done.
		Blinking	The WX Device-2 is starting up or under the MPro Mesh configuration process.
	Red	On	The WX Device-2 detects a system error.
		Blinking	The WX Device-2 is upgrading firmware
Link (with a WiFi connection)	Green	On	The WiFi connection to the WX Device-1 is good.
	Red	On	The signal is too weak. Move the WX Device-2 closer to the WX Device-1.

10 Now you can connect your WiFi clients to your WiFi Mesh network. To do this, note the SSID and WiFi key printed on the side label of the WX Device-1 using this SSID.



4.4 Network Management with the MPro Mesh App

You can manage your controller (the WX Device-1 or a Zyxel MPro Mesh router) and their WiFi settings through the MPro Mesh app.

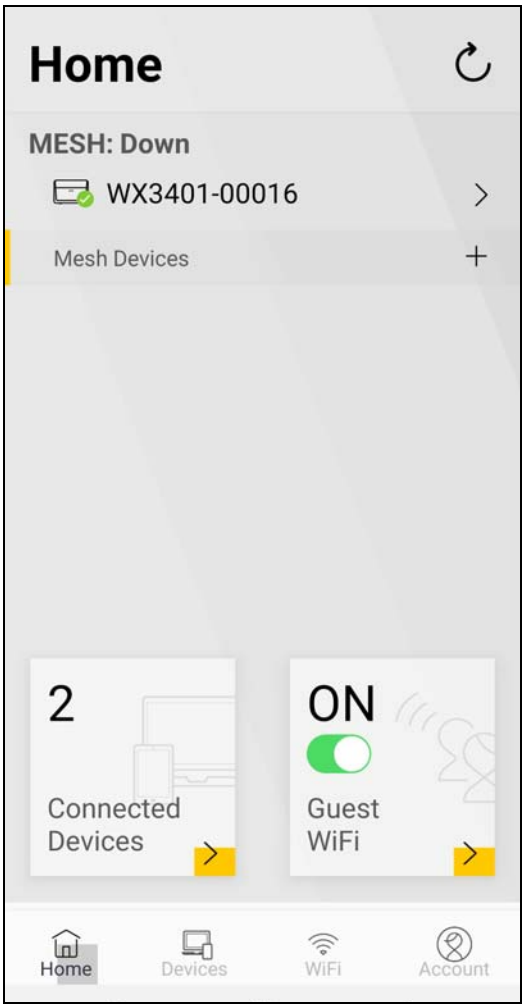
Please note that if you are using a WiFi connection with a Zyxel MPro Mesh router (see Section 4.3.1 on page 38), you must connect your smartphone to the Zyxel MPro Mesh router to manage the Mesh network through the app. This is because the Zyxel MPro Mesh router is the WiFi controller.

If you are using a wired connection with a non-MPro Mesh router (see Section 4.3.2 on page 43), you must connect your smartphone to the WX Device-1 to manage the Mesh network through the app. This is because the WX Device-1 is the WiFi controller.

4.4.1 Managing the Controller

Use this screen to view the navigation panel and the status of your WX Device.

Tap **Home** in the navigation panel to open the following screen.



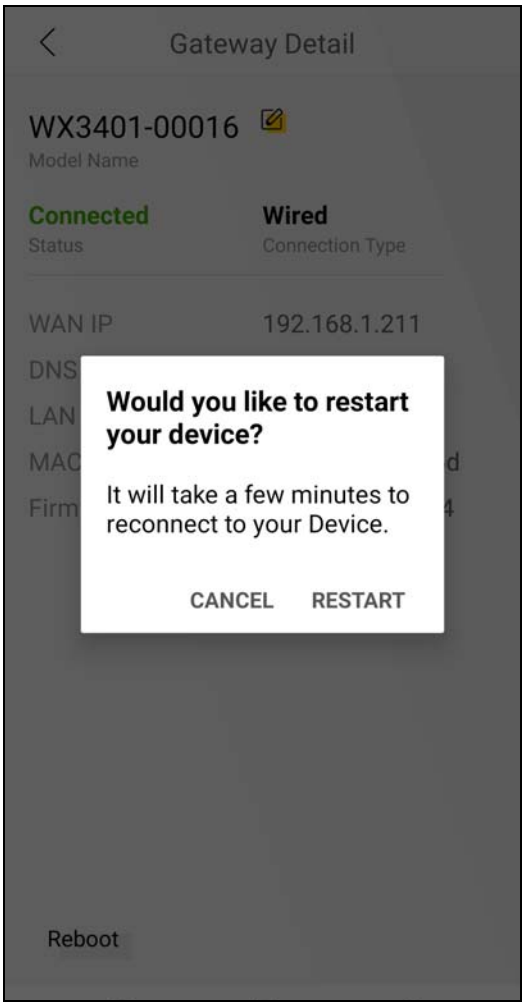
4.4.2 Viewing the Controller Information

Use this screen to view basic information of your controller (the Zyxel MPro Mesh router or WX Device-1).

Tap the > icon next to the model name **WX3401-00016** to open the following screen.

Tap the icon to change the model name shown on the app.

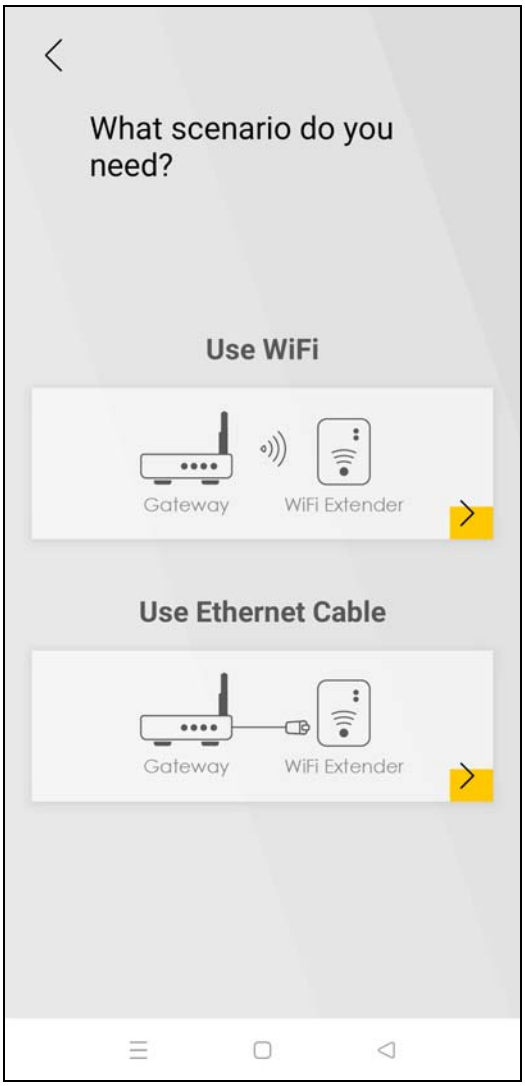
Tap the icon to save the changes made. Tap **Reboot** at the bottom left to restart your device.



4.4.3 Adding Devices to Your Mesh Network with WiFi

Use this screen to add extenders to your network to form a daisy chain (for more information on daisy chain, see Section 1.4 on page 18).

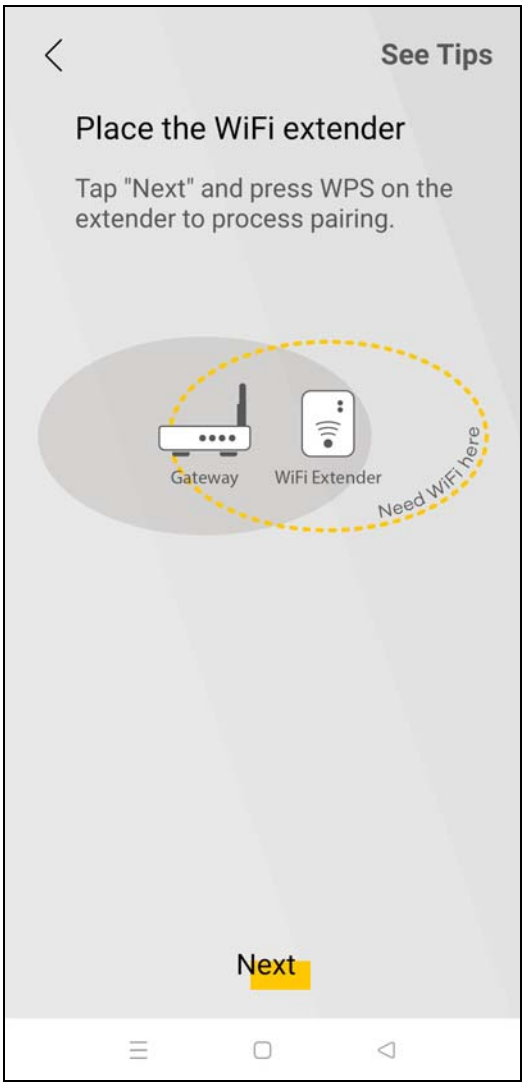
On the **Home** screen, tap the + icon to open the following screen.



To add a WX Device to your network wirelessly:

1 Tap the icon under **Use WiFi**.

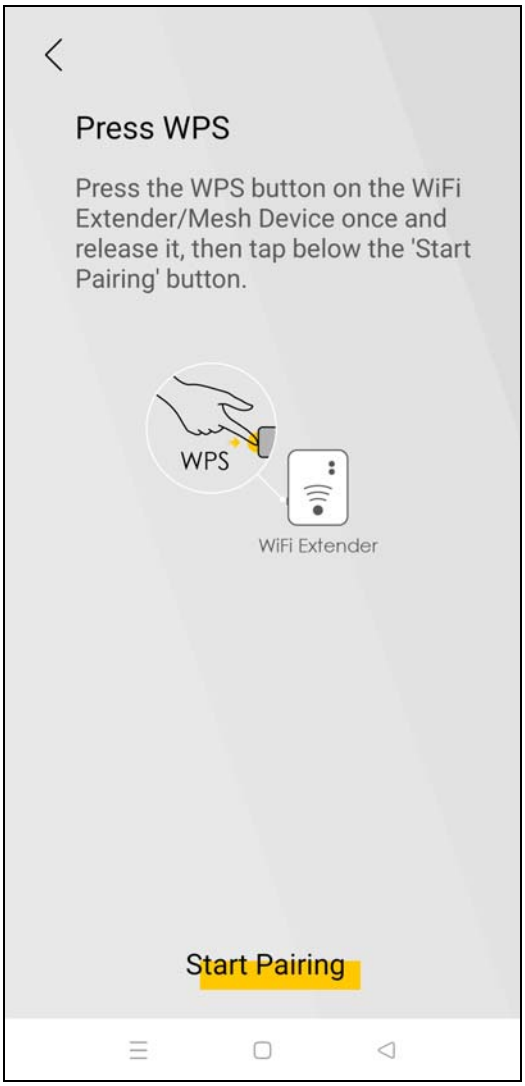
2 The following screen appears. Follow the instruction to set your device to the Repeater mode. Then click **Next** to go to the next step.



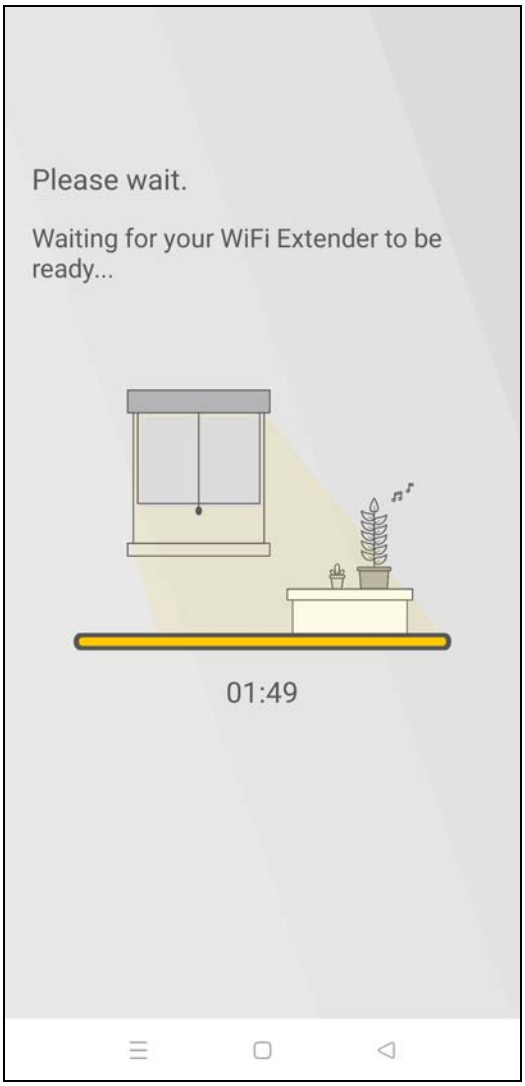
Note: You can tap **See Tips** on the top right to see instruction for finding ideal places to set up your devices.

Note: Your device may not have a mode switch. The method for setting modes for your device may vary depending on the device you use. For WX Device, its mode depends on its uplink connection, see Section 1.1 on page 12 for more information.

3 The following screen appears. Follow the instruction and click **Start Pairing** to connect your devices through the WPS button.



4 The following screen appears. Wait for the WX Device to connect to the MPro Mesh router through the WPS method.

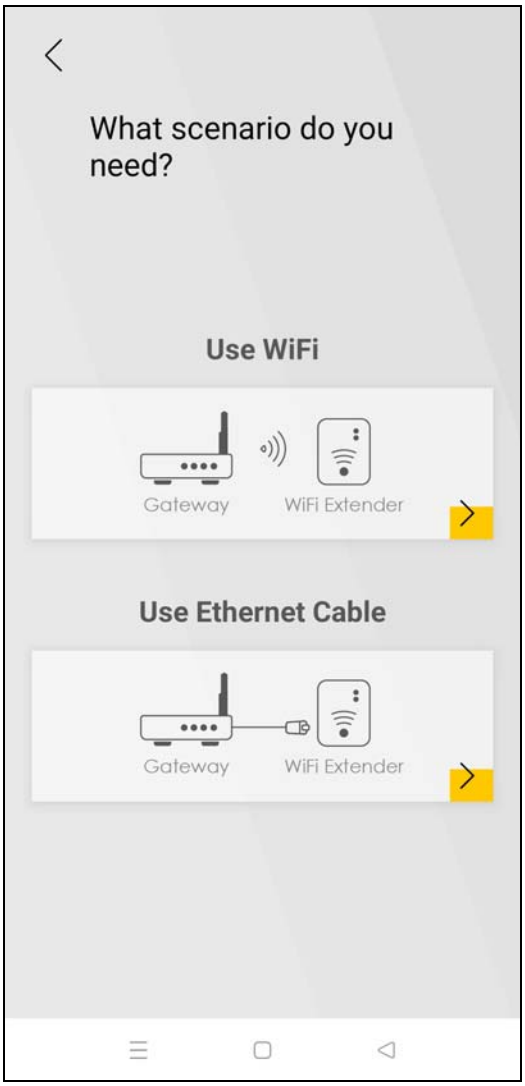


5 The following screen appears if the connection fails. Tap **Need help** to see possible reasons for the connection failure or tap **Try Again** to try connecting your devices through WPS button once more.

6 The following screen appears if the WX Device is connected to the MPro Mesh router successfully. Tap **Done** to go back to the **Home** screen.

4.4.4 Adding Devices to Your Mesh Network with Ethernet Cable

Use this screen to add extenders or APs to your network to form a daisy chain. On the **Home** screen, tap the + icon to open the following screen.



To add a WX Device to your network with an Ethernet cable:

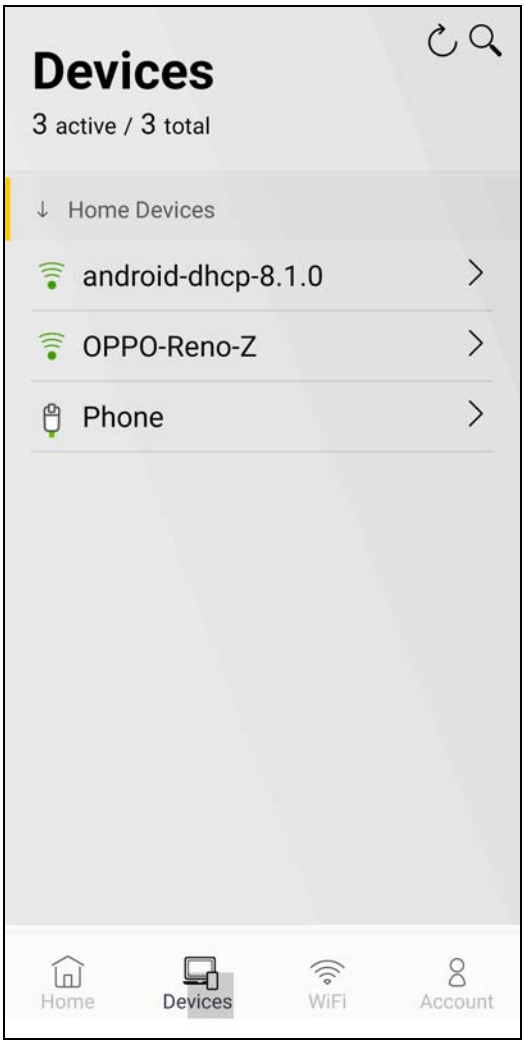
1 Tap the icon under **Use Ethernet Cable**.

2 The following screen shows. Follow the instruction to set your device to the AP mode. Then click **Done** to go back to the **Home** page.

4.5 Devices Screen

Use this screen to view clients that are connected to the WX Device and their link quality. You can tap the search icon to search for a certain client.

Tap **Devices** in the navigation panel to open the following screen.



4.5.1 Viewing Device Information

Use this screen to view basic information of the client connected to the WX Device and block Internet access to it.

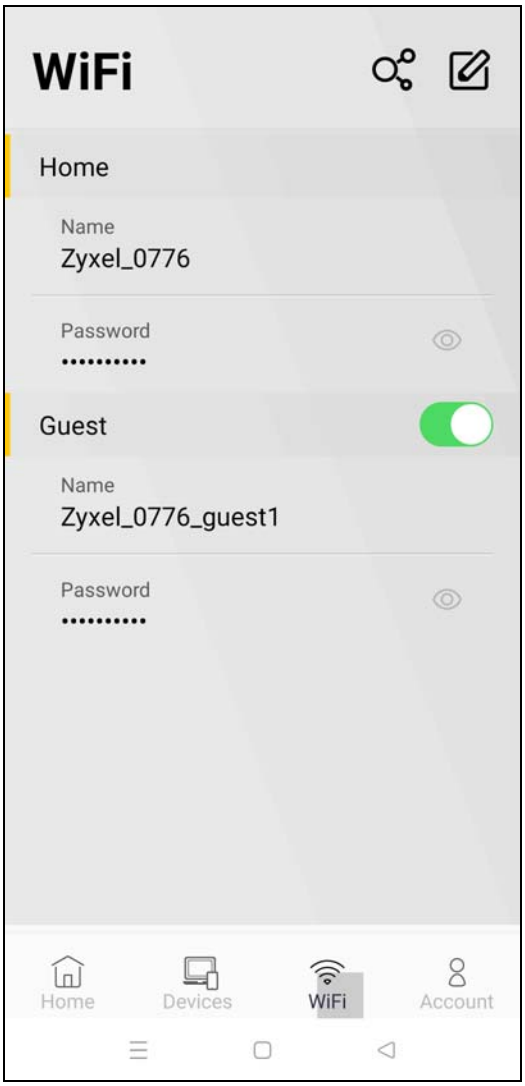
Tap the > icon to open the following screen.

Tap the icon to change the name of your device shown on the app.

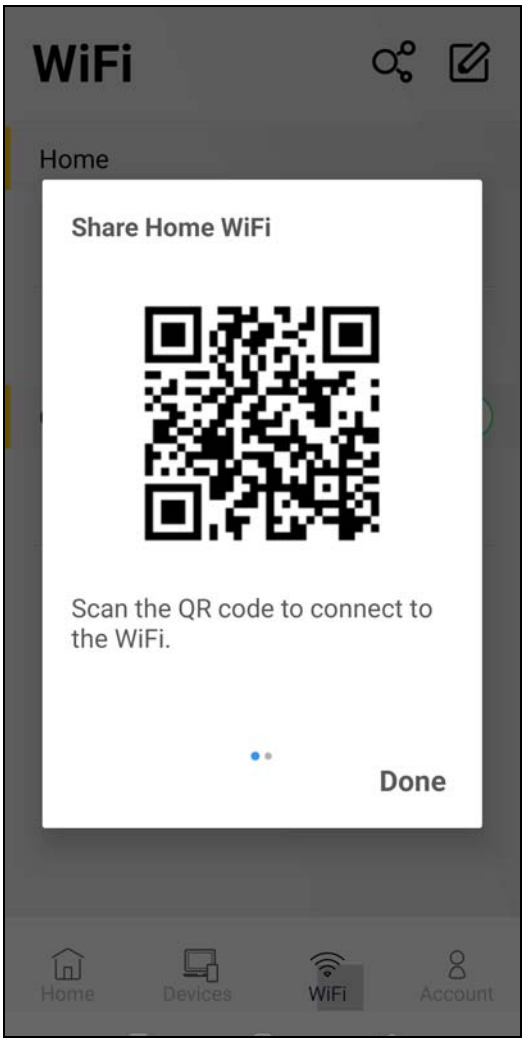
4.6 WiFi Settings Screen

Use this screen to configure settings for your WiFi network. For more information on Guest WiFi, see Section 4.7 on page 67.

Tap **WiFi** in the navigation panel to open the following screen.



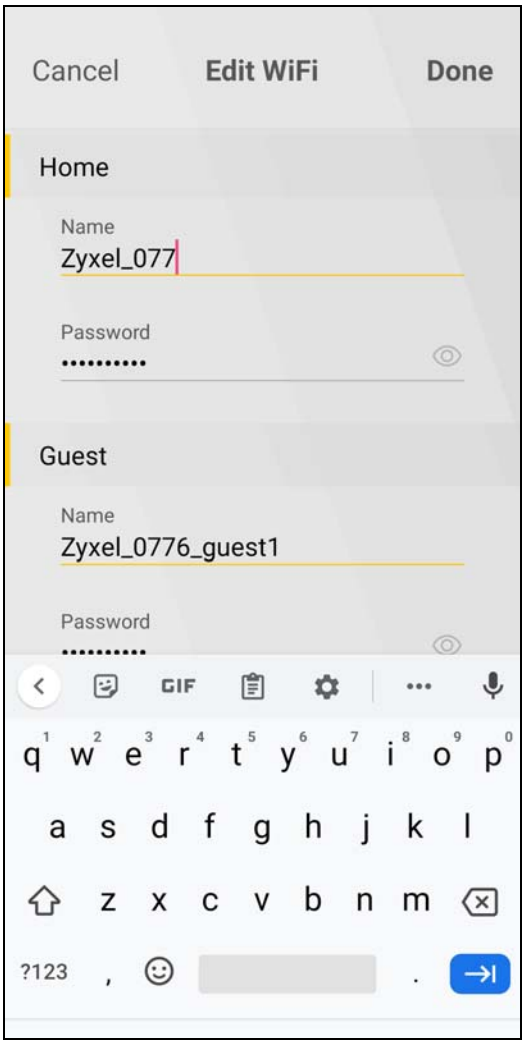
Tap the icon to show the QR code for connecting a WiFi client to the WX Device.



4.6.1 Edit WiFi Settings

Use this screen to edit the SSID (WiFi name) and password for your WiFi network.

Tap the icon to open the following screen.

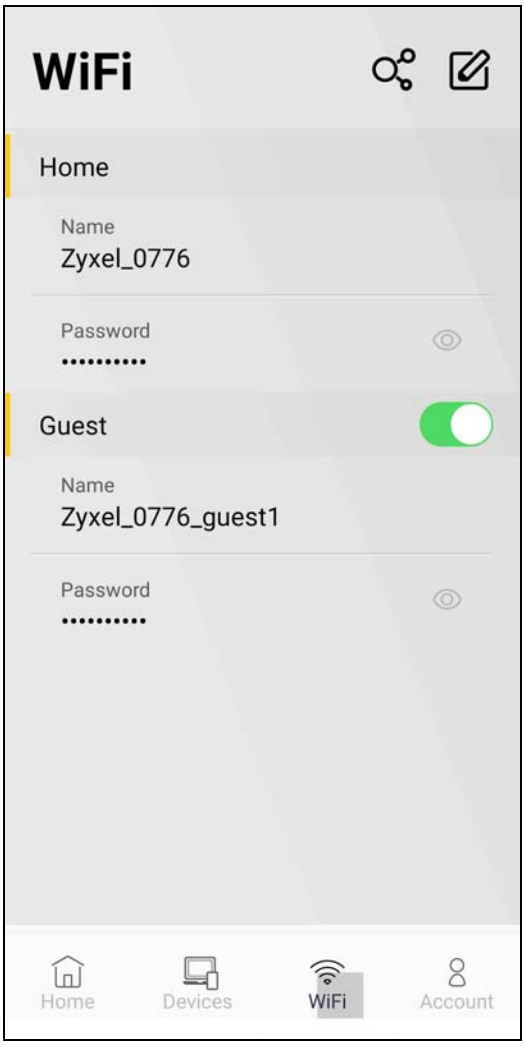


Tap **Done** to save your changes, or tap **Cancel** to go back to the previous screen.

4.7 Guest WiFi Settings Screen

Use this screen to configure Guest WiFi settings. Slide the **Guest WiFi** switch to the right to enable Guest WiFi.

Tap the icon and the following screen appears.



Tap the icon to show the QR code for connecting a WiFi client to the WX Device. Swipe to the left to show the QR code for connecting a guest WiFi client to the WX Device.

4.7.1 Editing Guest WiFi Settings

Use this screen to edit the SSID (WiFi Guest name) and password for your WiFi network.

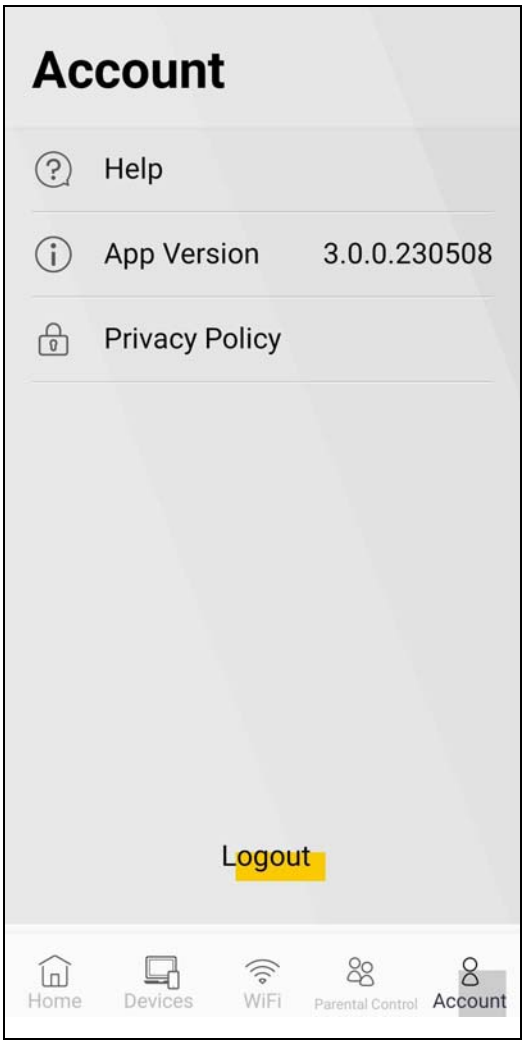
Tap the icon to open the following screen.

Note: If you disable Guest WiFi, you must reconnect to the controller.

Tap **Save** to save your changes, or tap **Cancel** to go back to the previous screen.

4.8 Account Screen

Use this screen to logout or view the app version and privacy policy.

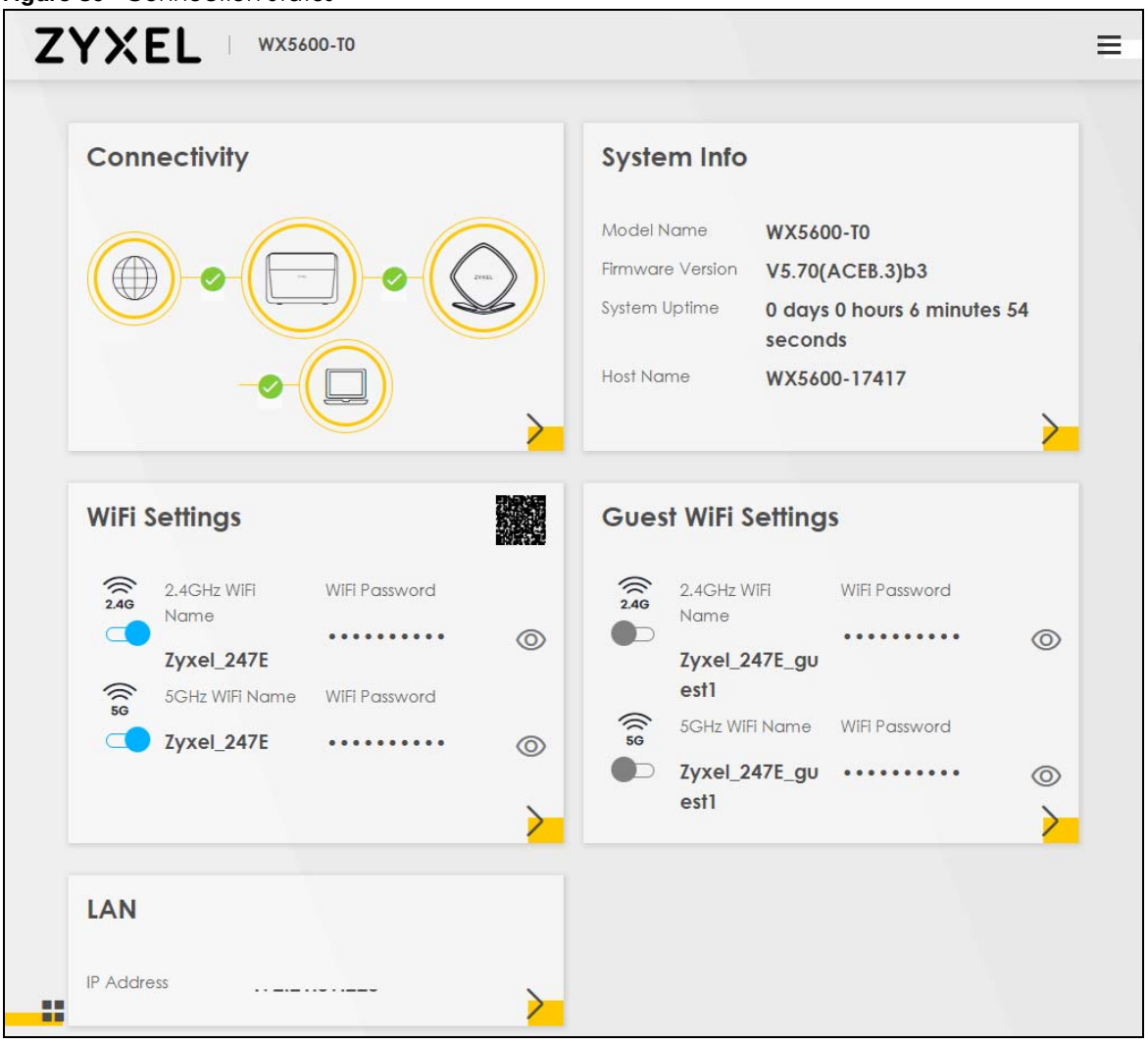

Account
Help
App Version
3.0.0.230508
Privacy Policy
Logout
Home
Devices
WiFi
Parental Control
Account

CHAPTER 5
Connection Status

5.1 Overview

After you log into the Web Configurator, the **Connection Status** screen appears. You can configure basic Internet access and WiFi settings in this screen. It also shows the network status of the WX Device and computers/devices connected to it.

Figure 30 Connection Status



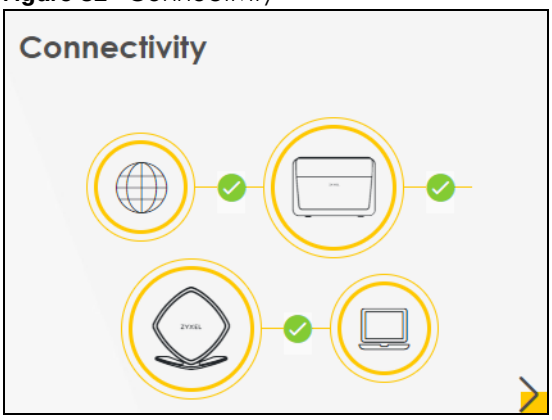
5.1.1 Layout Icon

Click this icon ( ) to arrange the screen order. Select a block and hold it to move around. Click the Check icon ( ) in the lower left corner to save the changes.

5.1.2 Connectivity

Use this screen to view the network connection status of the WX Device and its clients.

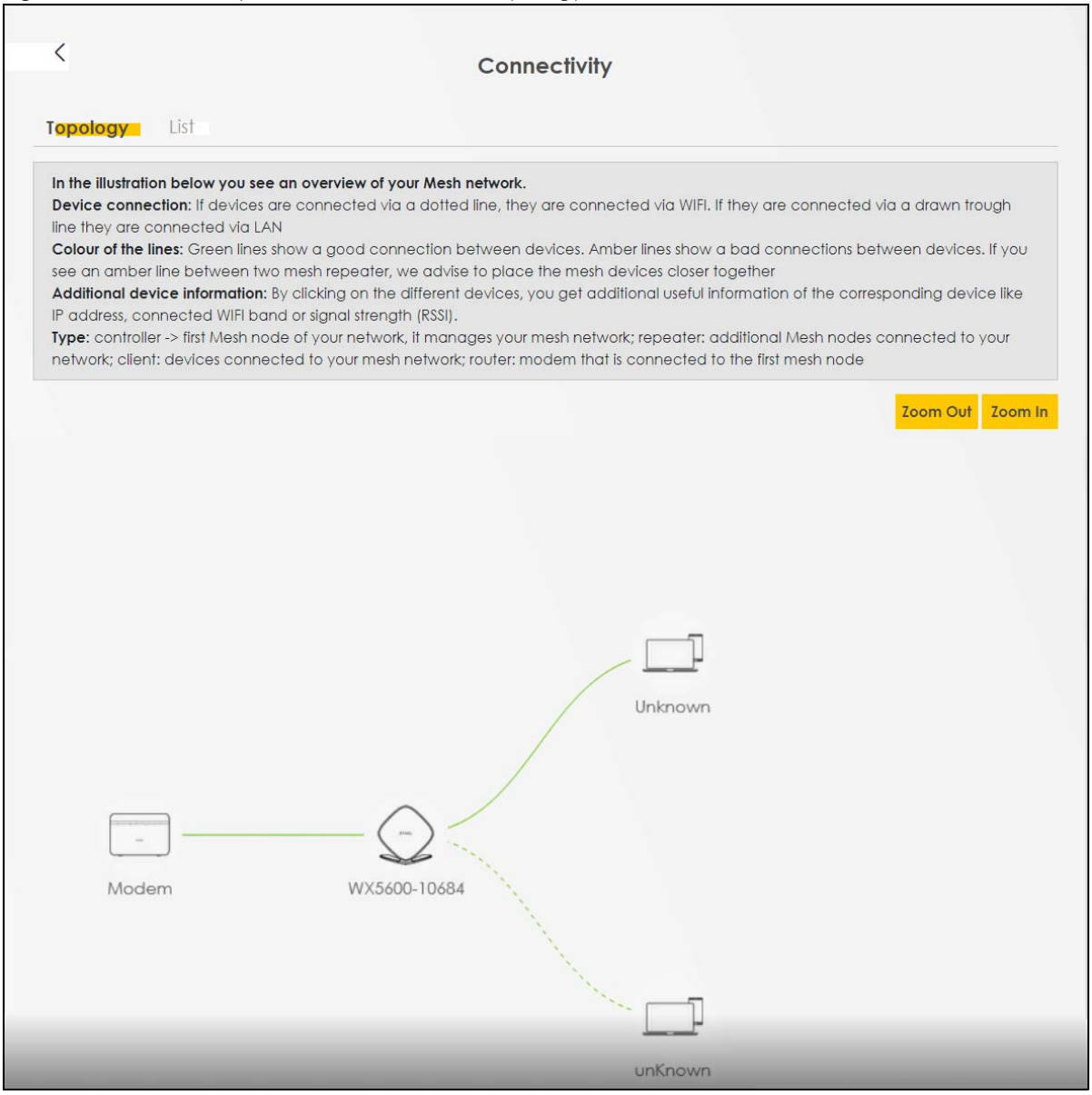
Figure 31 Connectivity



Click the Arrow icon ( ) to open the following screen.

Use the **Topology** view screen to display an overview of your Mesh network.

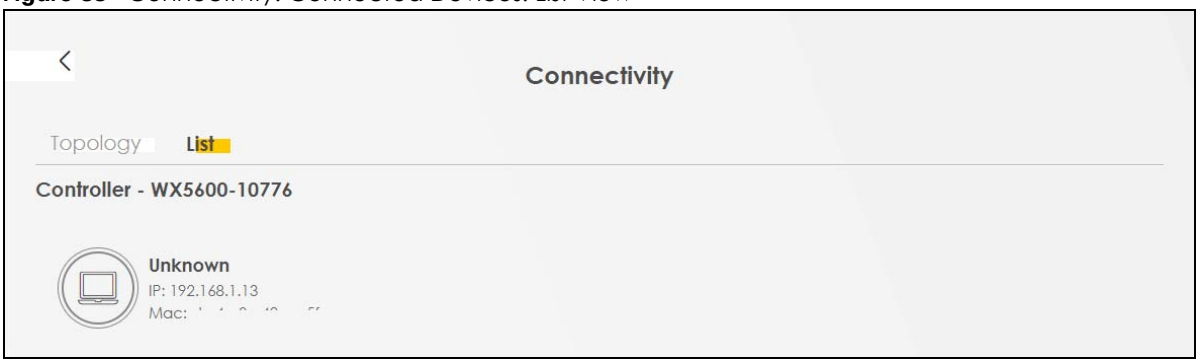
Figure 32 Connectivity: Connected Devices: Topology View



Use the **List** view screen to view IP addresses and MAC addresses of the WiFi and wired devices connected to the WX Device.

Place your mouse within the device block, and an Edit icon ( ) will appear. Click the Edit icon to change the icon and name of a connected device.

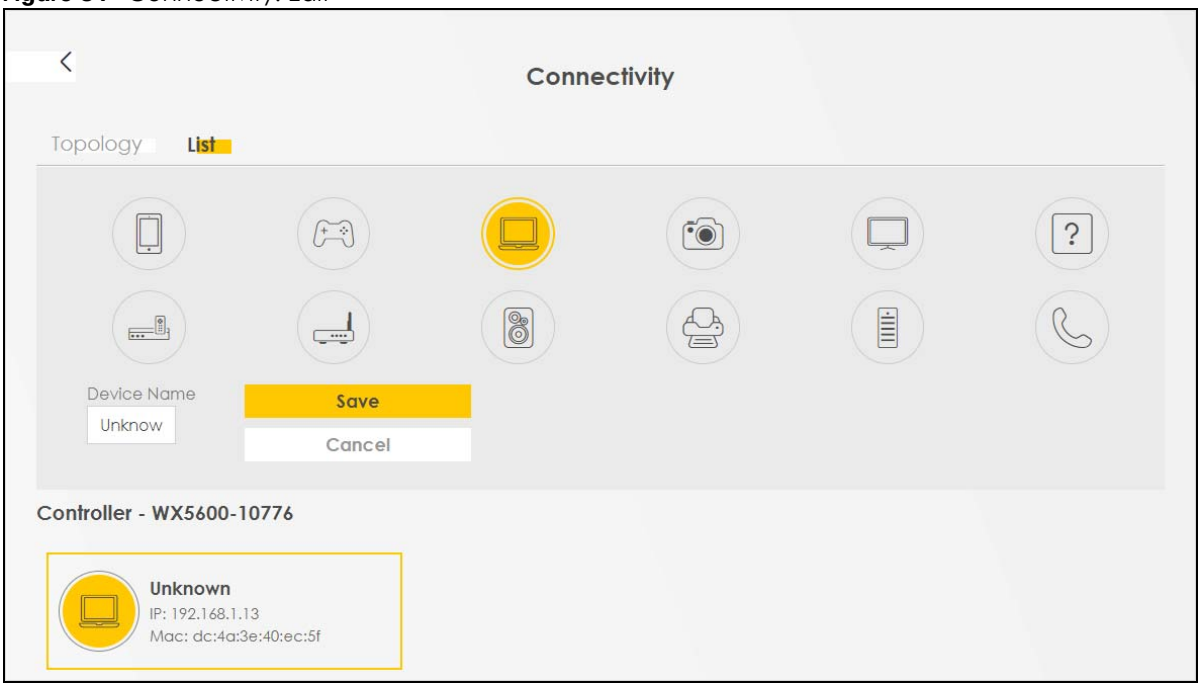
Figure 33 Connectivity: Connected Devices: List View



Icon and Device Name

You can change the icon and name of a connected device by clicking the device's Edit icon. Select an icon and/or enter a name in the **Device Name** field for a connected device. Click **Save** to save your changes.

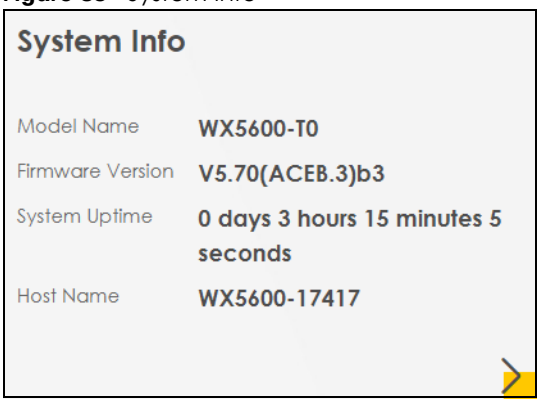
Figure 34 Connectivity: Edit



5.1.3 System Info

Use this screen to view the basic system information of the WX Device.

Figure 35 System Info



Click the Arrow icon ( ) to open the following screen. Use this screen to view more information on the status of your firewall and interfaces (LAN and WiFi).

Figure 36 System Info: Detailed Information

Each field is described in the following table.

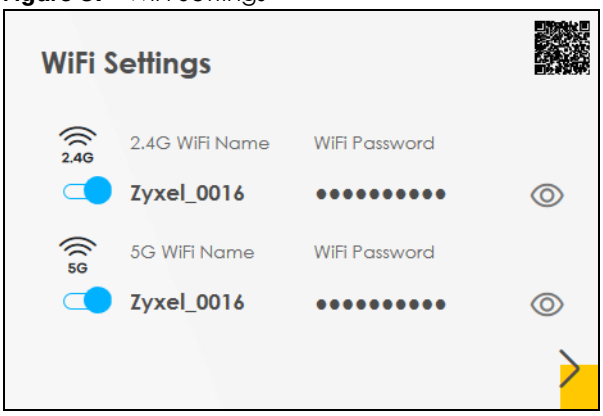
Table 14 System Info: Detailed Information

LABEL	DESCRIPTION
Host Name	This field displays the WX Device system name. It is used for identification.
Model Name	This shows the model number of your WX Device.
Serial Number	This field displays the serial number of the WX Device.
Firmware Version	This is the current version of the firmware on the WX Device.
System Uptime	This field displays how long the WX Device has been running since it last started up. The WX Device starts up when you plug it in, when you restart it (**Maintenance** > **Reboot**), or when you reset it.
CPU Usage	This displays the current CPU usage percentage.
Memory Usage	This displays the current RAM usage percentage.
Interface Status Virtual ports are shown here. You can see whether the ports are in use and their transmission rate.	
LAN Information (These fields display information about the LAN ports.)	
IP Address	This is the current IPv4 address of the WX Device in the LAN.
Subnet Mask	This is the current subnet mask in the LAN.
IPv6 Address	This is the current IPv6 address of the WX Device in the LAN.
IPv6 Link Local Address	This field displays the current link-local address of the WX Device for the LAN interface.
MAC Address	This field displays the LAN Ethernet adapter MAC (Media Access Control) address of your WX Device.
WLAN Information 2.4GHz / 5GHz	
MAC Address	This shows the WiFi adapter MAC (Media Access Control) address of the WiFi interface.
Status	This displays whether WiFi is activated.
SSID	This is the descriptive name used to identify the WX Device in a WiFi network.
Channel	This is the channel number used by the WiFi interface now.
Security	This displays the type of security mode the WiFi interface is using in the WiFi network.
802.11 Mode	This displays the type of 802.11 mode the WiFi interface is using in the WiFi network.
WPS	This displays whether WPS is activated on the WiFi interface.

5.2 WiFi Settings

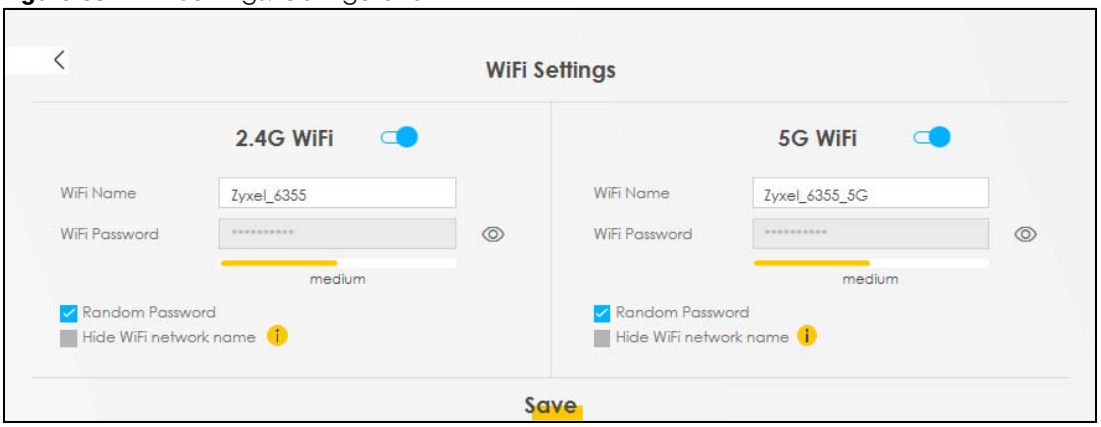
Use this screen to configure the main 2.4G and/or 5G WiFi network settings. When the switch goes to the right ( ), the function is enabled. Otherwise, it is not. You can use this screen or the QR code on the upper right to check the SSIDs (WiFi network name) and passwords of the main WiFi networks. If you want to show or hide your WiFi passwords, click the Eye icon ( ).

Figure 37 WiFi Settings



Click the Arrow icon ( ) to open the following screen. Use this screen to configure the SSIDs and/or passwords for your main WiFi networks. When the switch goes to the right ( ), the function is enabled. Otherwise, it is not.

Figure 38 WiFi Settings: Configuration



Each field is described in the following table.

Table 15 WiFi Settings: Configuration

LABEL	DESCRIPTION
Keep 2.4G and 5G the same	This switch cannot be turned off.
2.4G/5G WiFi	Click this switch to enable or disable the 2.4G and/or 5G WiFi networks. When the switch goes to the right , the function is enabled. Otherwise, it is not.
WiFi Name	The SSID (Service Set IDentity) identifies the service set with which a WiFi device is associated. WiFi devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for WiFi.
WiFi Password	If you selected **Random Password**, this field displays a pre-shared key generated by the WX Device. If you did not select **Random Password**, you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters.
	Click the Eye icon to show or hide the password for your WiFi network. When the Eye icon is slashed , you will see the password in plain text. Otherwise, it is hidden.
Random Password	Select this option to have the WX Device automatically generate a password. The **WiFi Password** field will not be configurable when you select this option.

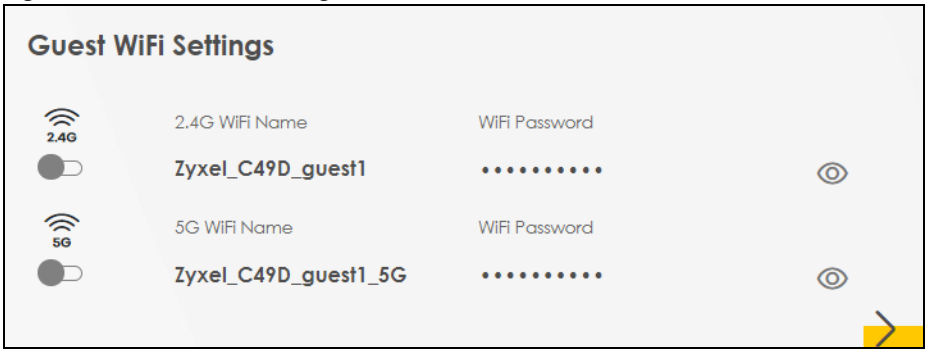
Table 15 WiFi Settings: Configuration (continued)

LABEL	DESCRIPTION
Hide WiFi network name	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. Note: Disable WPS in the **Network Setting** > **Wireless** > **WPS** screen to hide the SSID.
Save	Click **Save** to save your changes.

5.3 Guest WiFi Settings

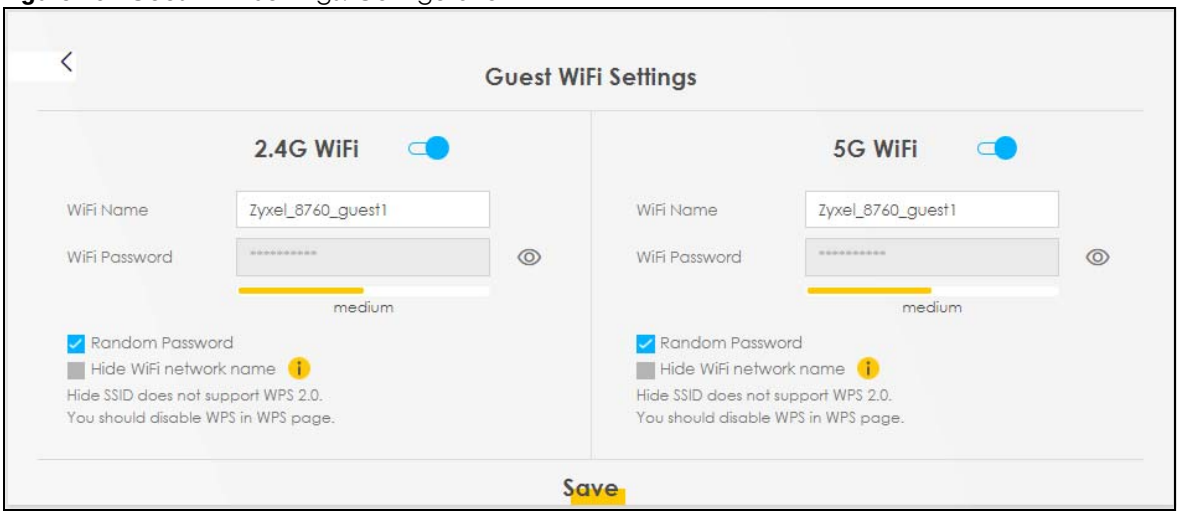
Use this screen to enable or disable the guest 2.4G and/or 5G WiFi networks. When the switch goes to the right ( ), the function is enabled. Otherwise, it is not. You can check their SSIDs (WiFi network name) and passwords from this screen. If you want to show or hide your WiFi passwords, click the Eye icon.

Figure 39 Guest WiFi Settings



Click the Arrow icon ( ) to open the following screen. Use this screen to configure the 2.4G and 5G SSIDs and/or passwords for your guest WiFi networks.

Figure 40 Guest WiFi Settings: Configuration



Each field is described in the following table.

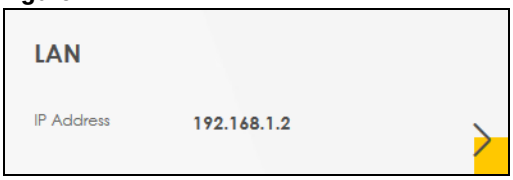
Table 16 WiFi Settings: Configuration

LABEL	DESCRIPTION
WiFi 2.4G/5G WiFi	Click this switch to enable or disable the 2.4G and/or 5G WiFi networks. When the switch goes to the right , the function is enabled. Otherwise, it is not.
WiFi Name	The SSID (Service Set IDentity) identifies the service set with which a WiFi device is associated. WiFi devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for WiFi.
WiFi Password	If you selected **Random Password**, this field displays a pre-shared key generated by the WX Device. If you did not select **Random Password**, you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters.
	Click the Eye icon to show or hide the password of your WiFi network. When the Eye icon is slashed , you will see the password in plain text. Otherwise, it is hidden.
Random Password	Select this option to have the WX Device automatically generate a password. The **WiFi Password** field will not be configurable when you select this option.
Hide WiFi network name	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. Note: Disable WPS in the **Network Setting** > **Wireless** > **WPS** screen to hide the SSID.
Save	Click **Save** to save your changes.

5.4 LAN Settings

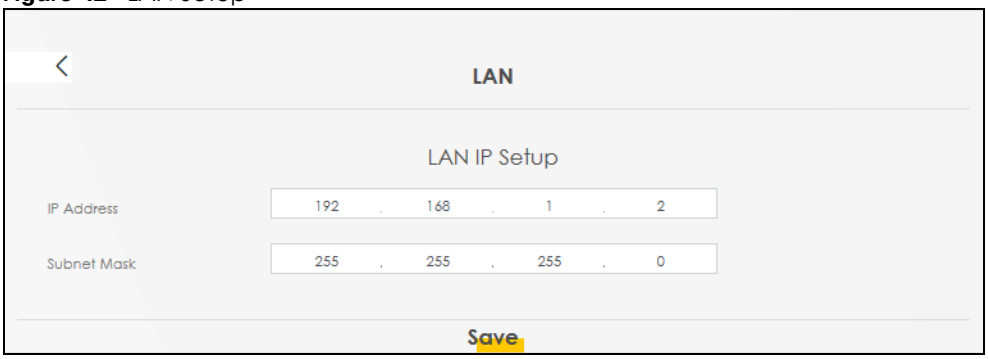
Use this screen to view the LAN IP address and subnet mask of your WX Device.

Figure 41 LAN



Click the Arrow icon ( ) to open the following screen. Use this screen to configure the LAN IP address and subnet mask for your WX Device.

Figure 42 LAN Setup



Each field is described in the following table.

Table 17 Status Screen

LABEL	DESCRIPTION
LAN IP Setup	
IP Address	Enter the LAN IPv4 address you want to assign to your WX Device in dotted decimal notation, for example, 192.168.1.2 (factory default).
Subnet Mask	Enter the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your WX Device automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.
Save	Click **Save** to save your changes.

CHAPTER 6
Web Tutorials

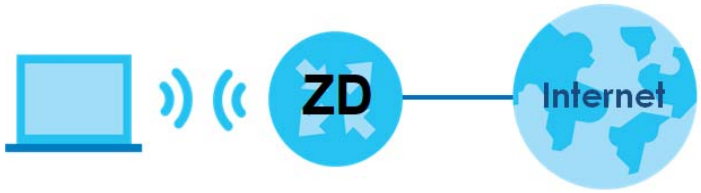
6.1 Overview

This chapter provides Web Configurator tutorials for setting up a secure WiFi network for your WX Device.

- WiFi Network Setup
- Device Maintenance

6.2 WiFi Network Setup

Thomas wants to set up a WiFi network so that he can use his notebook to access the Internet. In this WiFi network, the WX Device serves as an access point (AP), and the notebook is the WiFi client. The WiFi client can access the Internet through the AP.



Thomas has to configure the WiFi network settings on the WX Device. Then he can set up a WiFi network using WPS (Section 6.2.2 on page 86) or manual configuration (Section 6.2.3 on page 88).

6.2.1 Setting Up a WiFi Network

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

SSID	Example
Security Mode	WPA2-PSK
Pre-Shared Key	DoNotStealMyWirelessNetwork
802.11 Mode	802.11b/g/n/ax Mixed

1 Click **Network Setting** > **Wireless** to open the **General** screen. Select **More Secure** as the security level and **WPA2-PSK** as the security mode. Configure the screen using the provided parameters (see Section 6.2.1 on page 83). Click **Apply**.

Figure 43 Network Setting > Wireless(WX3401-B0/WX3100-T0)

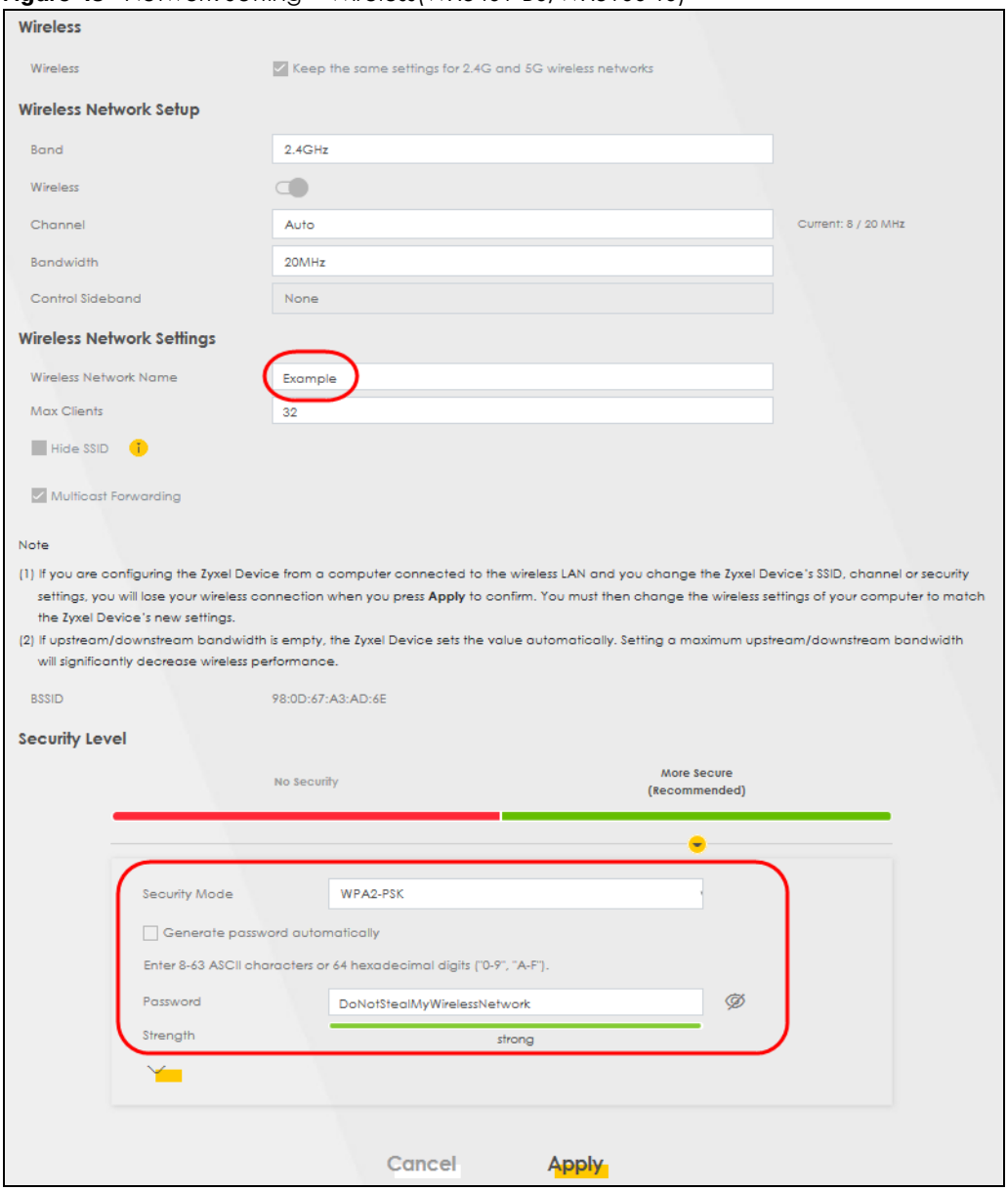
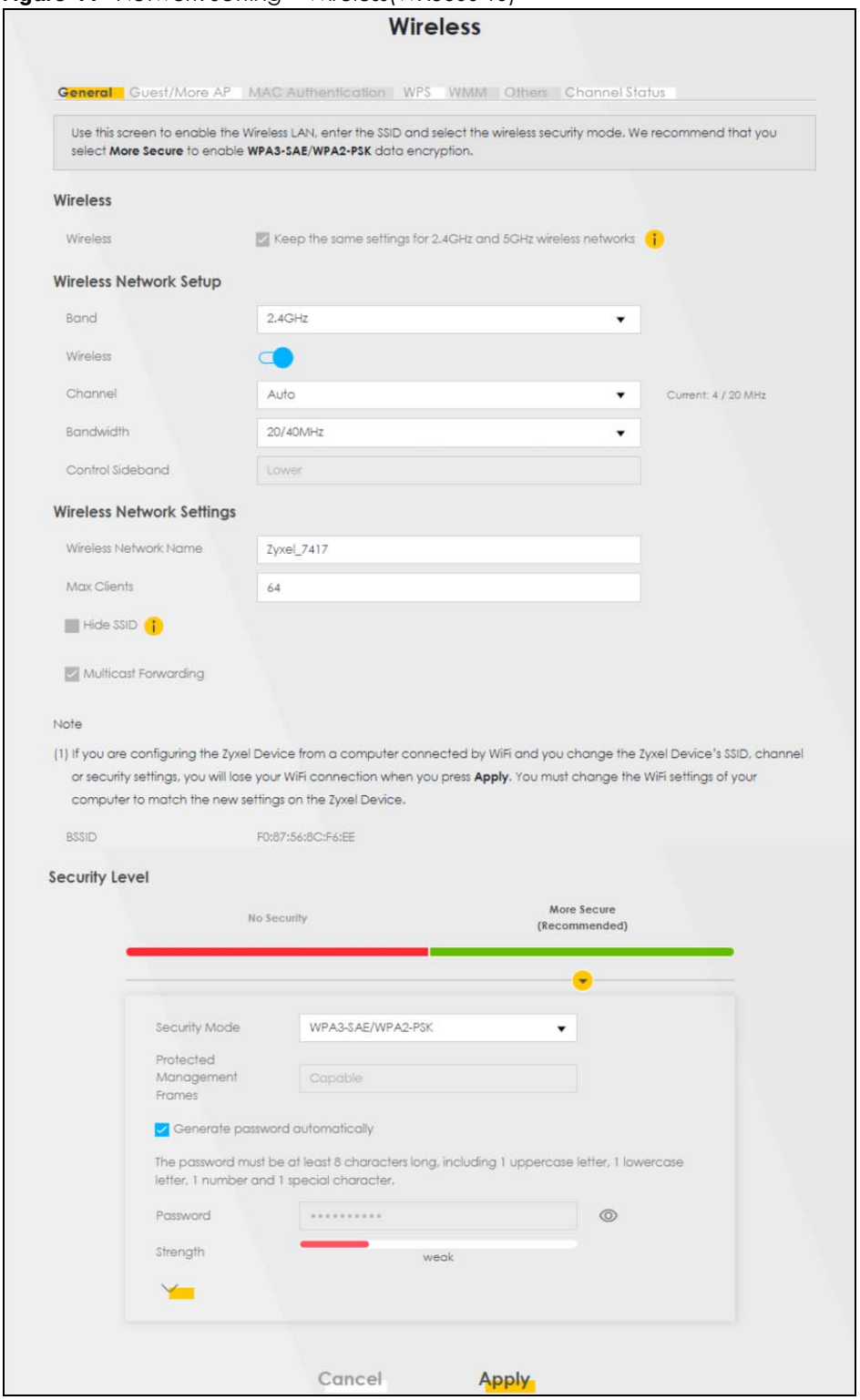
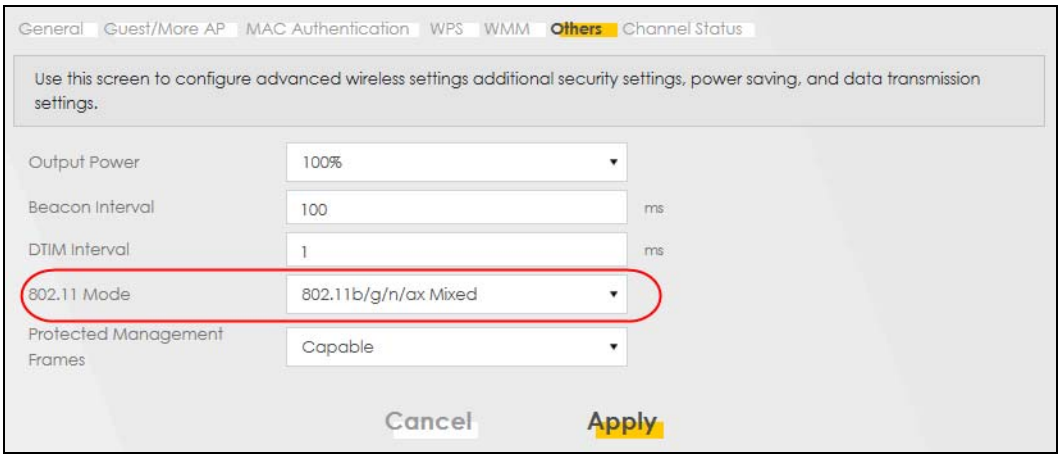


Figure 44 Network Setting > Wireless(WX5600-T0)



2 Go to the **Wireless** > **Others** screen and select **802.11b/g/n/ax Mixed** in the **802.11 Mode** field. Click **Apply**.



3 You can now use the WPS feature to establish a WiFi connection between your notebook and the WX Device (see Section 6.2.2 on page 86). You can also use the notebook's WiFi client to search for the WX Device (see Section 6.2.4 on page 88).

6.2.2 Setting Up a WiFi Network Using WPS

This section gives you an example of how to set up a WiFi network using WPS. This example uses the WX Device as the AP and a WPS-enabled Android smartphone as the WiFi client.

There are two WPS methods for creating a secure connection. This tutorial shows you how to do both.

- **Push Button Configuration (PBC)** – create a secure WiFi network simply by pressing a button. This is the easier method.
- **PIN Configuration** – create a secure WiFi network simply by entering a WiFi client's PIN (Personal Identification Number) in the WX Device's interface. This is the more secure method, since one device can authenticate the other.

Note: When using WPS in the Web Configurator, and depending on your **Band** selection (**2.4 GHz** or **5 GHz**), the secure connection will apply for the selected **Band** only.

Push Button Configuration (PBC)

1 Make sure that your WX Device is turned on and your notebook is within the cover range of the WiFi signal.

2 Push and hold the **WPS** button located on the WX Device's front panel for one second. Alternatively, you may log into the WX Device's Web Configurator and go to the **Network Setting** > **Wireless** > **WPS** screen. Enable the WPS function for method 1 and click **Apply**. Then click the **WPS** button.

Figure 45 Network Setting > Wireless > WPS (WX3401-B0)

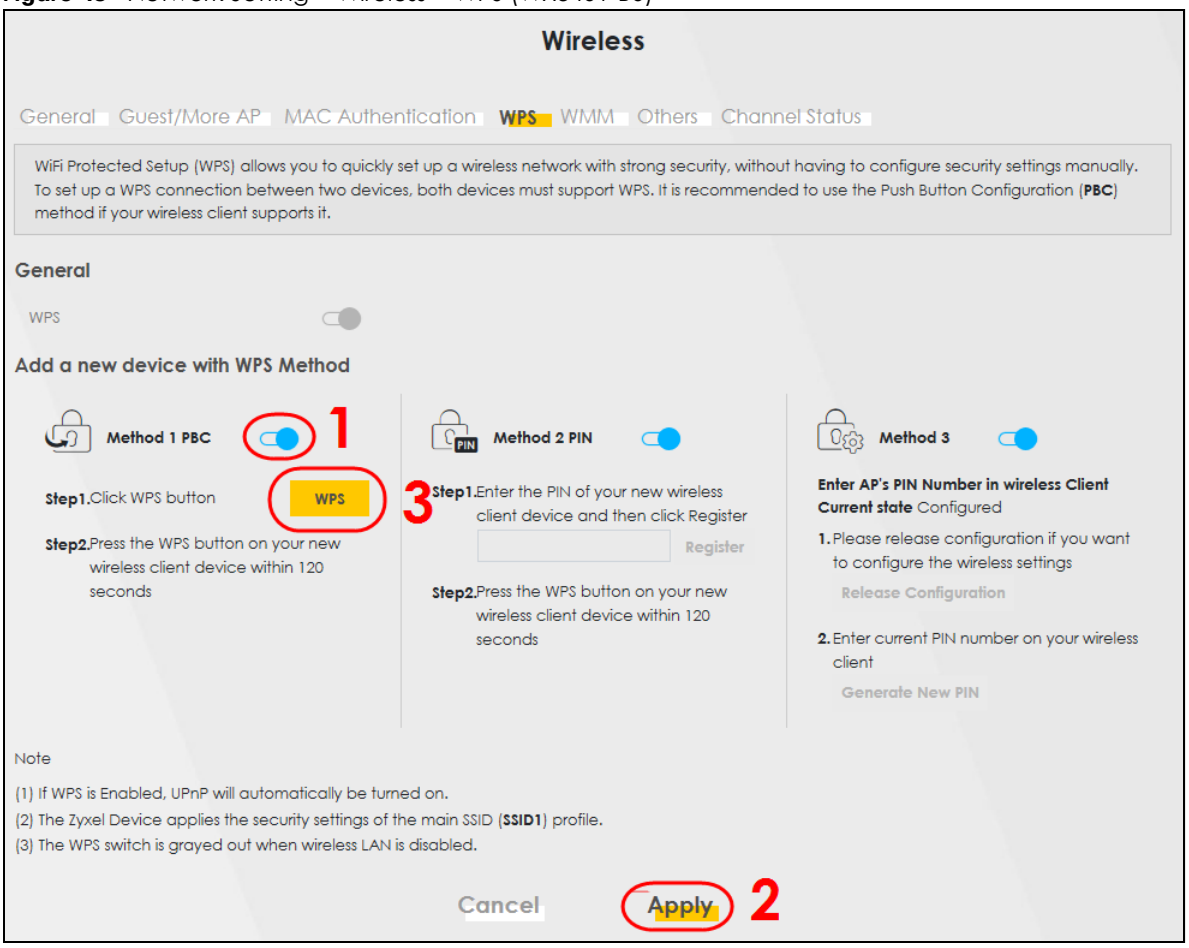
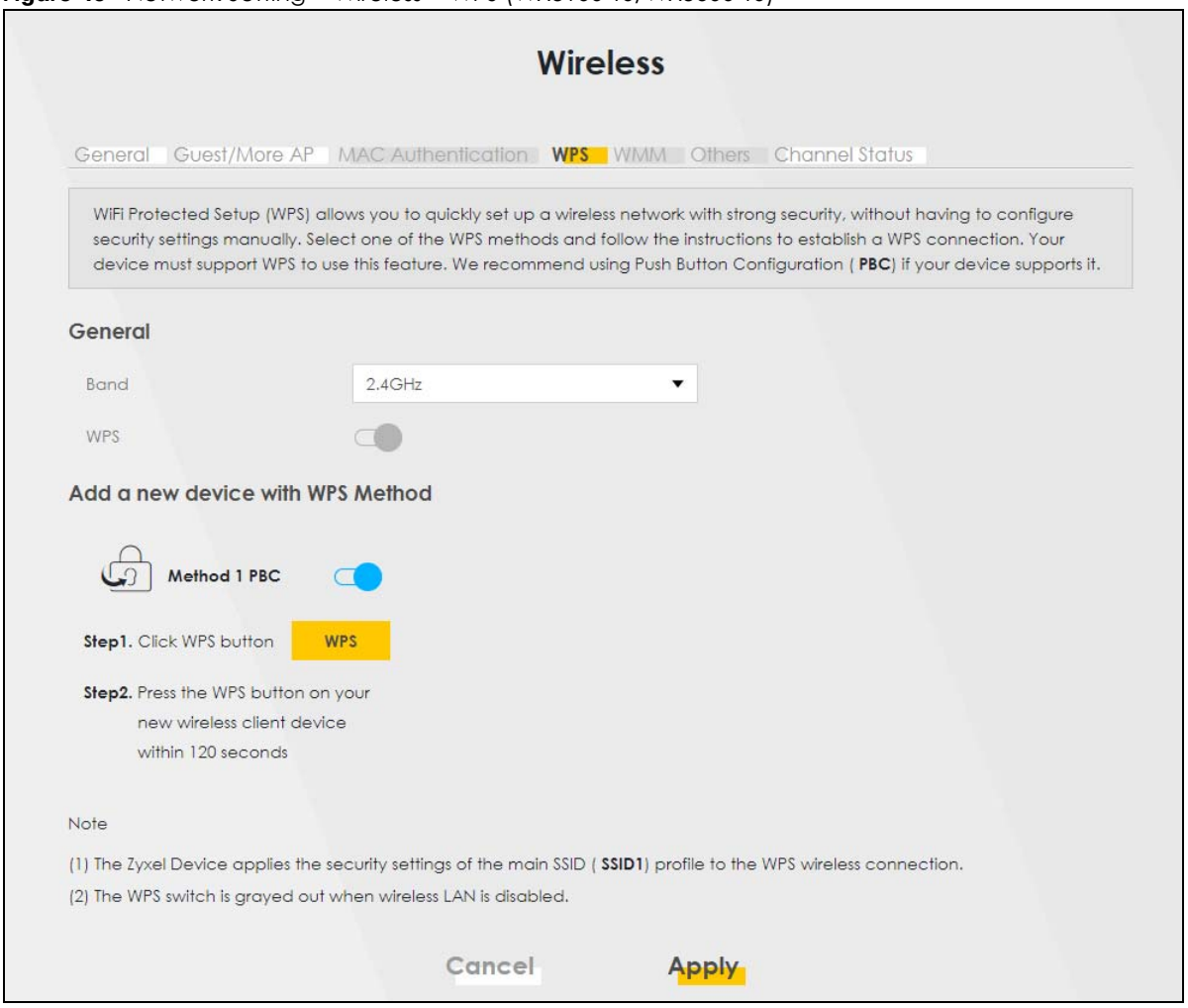


Figure 46 Network Setting > Wireless > WPS (WX3100-T0/WX5600-T0)



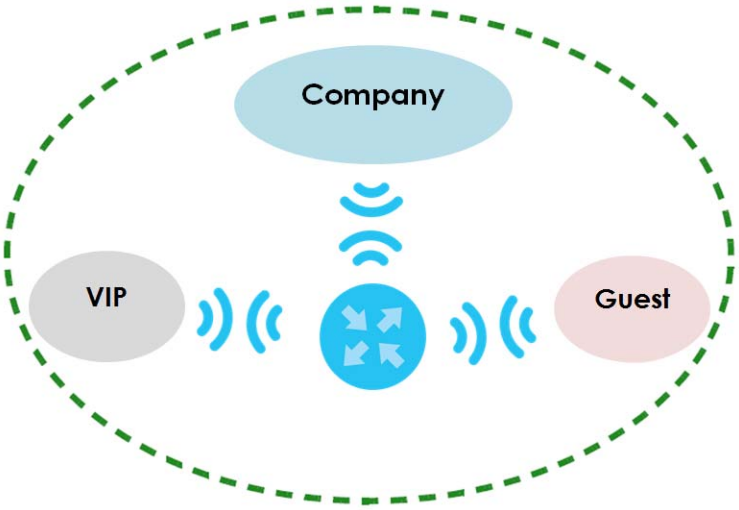
6.2.3 Setting Up a WiFi Network Without WPS

Use the WiFi adapter's utility installed on the notebook to search for the "Example" SSID. Then enter the "DoNotStealMyWirelessNetwork" pre-shared key to establish a WiFi Internet connection.

Note: The WX Device supports IEEE 802.11ac/ax WiFi clients. Make sure that your notebook or computer's WiFi adapter supports one of these standards.

6.2.4 Setting Up WiFi Network Groups

Company A wants to create different WiFi network groups for different types of users as shown in the following figure. Each group has its own SSID and security mode.



- Employees in Company A will use a general **Company** WiFi network group.
- Higher management level and important visitors will use the **VIP** group.
- Visiting guests will use the **Guest** group, which has a different SSID and password.

Company A will use the following parameters to set up the WiFi network groups.

	COMPANY	VIP	GUEST
SSID	Company	VIP	Guest
Security Level	More Secure	More Secure	More Secure
Security Mode	WPA2-PSK	WPA2-PSK	WPA2-PSK
Pre-Shared Key	ForCompanyOnly	123456789	guest123

1 Click **Network Setting** > **Wireless** to open the **General** screen. Use this screen to set up the company's general WiFi network group. Configure the screen using the provided parameters and click **OK**.

Figure 47 Network Setting > Wireless (WX3401-B0/WX3100-T0)

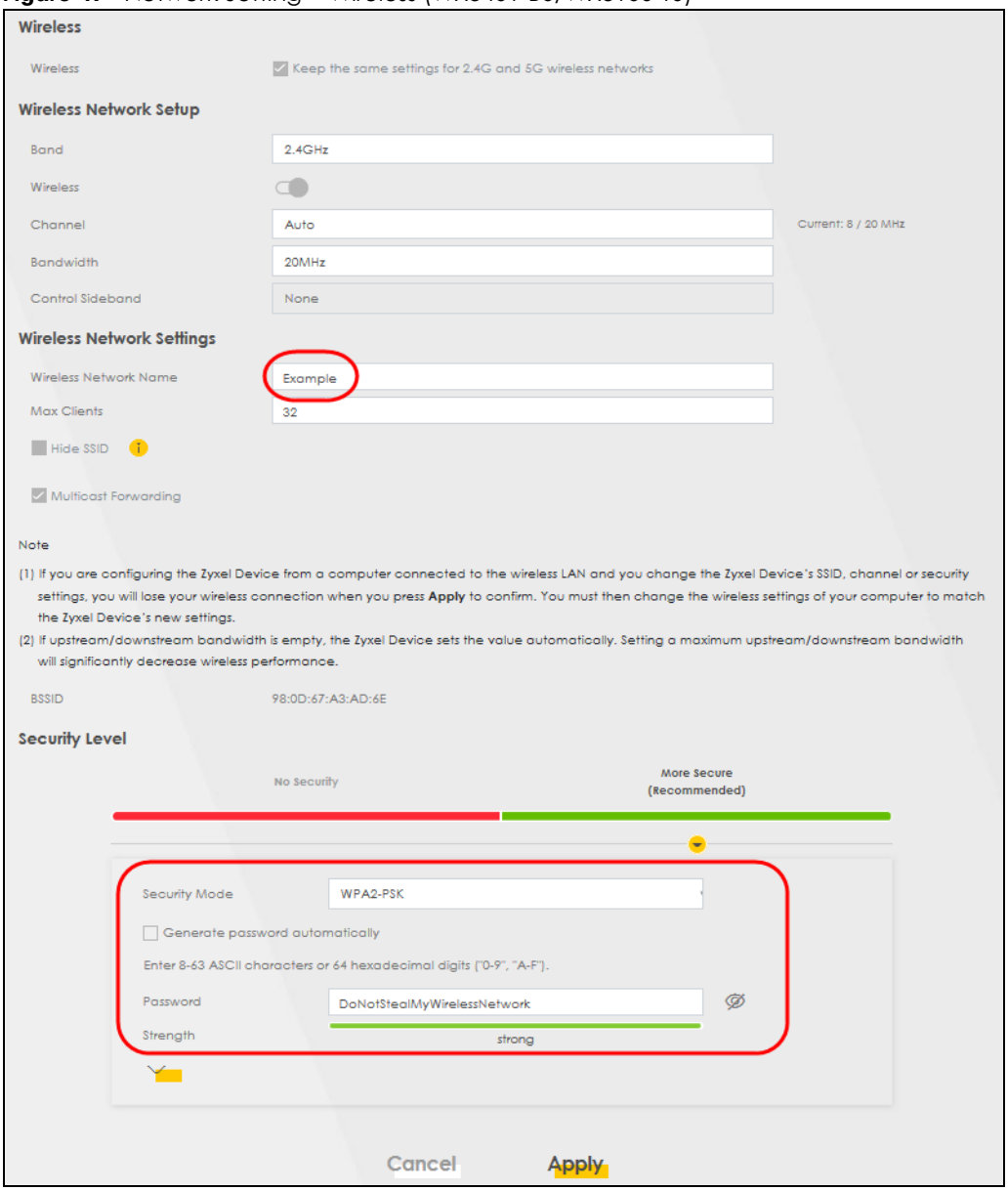
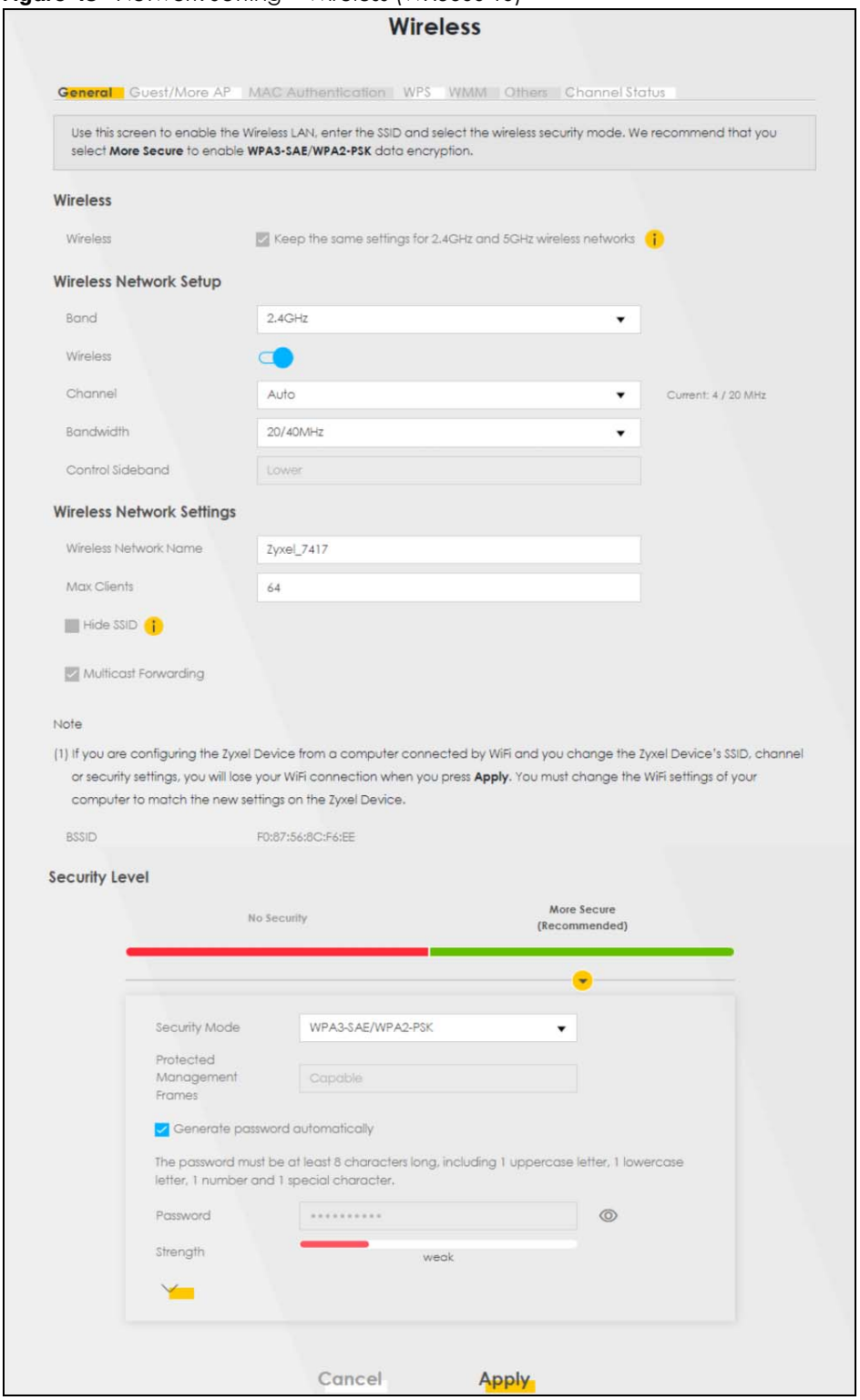


Figure 48 Network Setting > Wireless (WX5600-T0)



2 Click **Network Setting** > **Wireless** > **Guest/More AP** to open the following screen. Click the **Modify** icon to configure the second WiFi network group.

3 Configure the screen using the provided parameters and click **OK**.

Figure 49 More AP Edit (WX3401-B0/WX3100-T0)

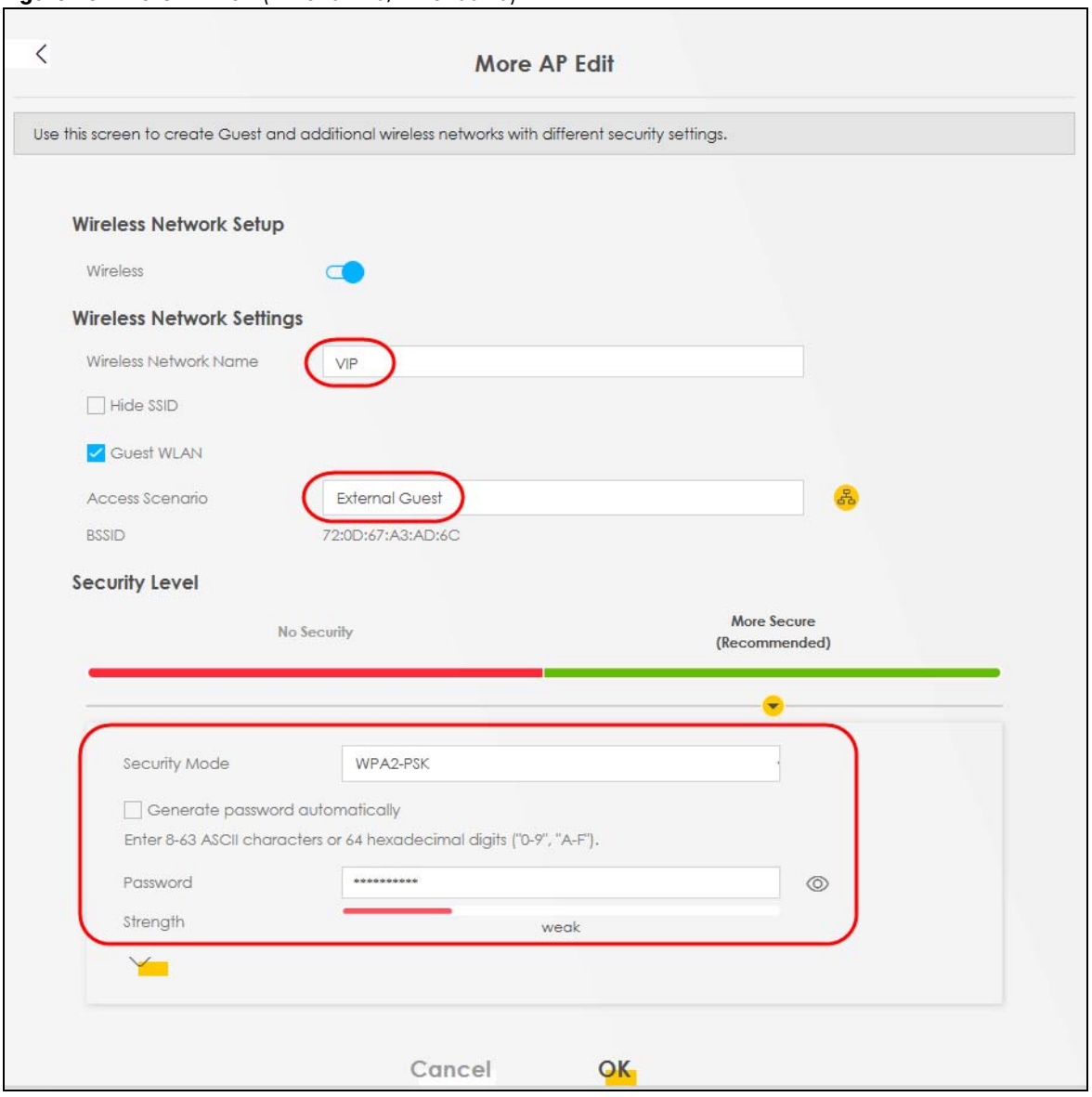
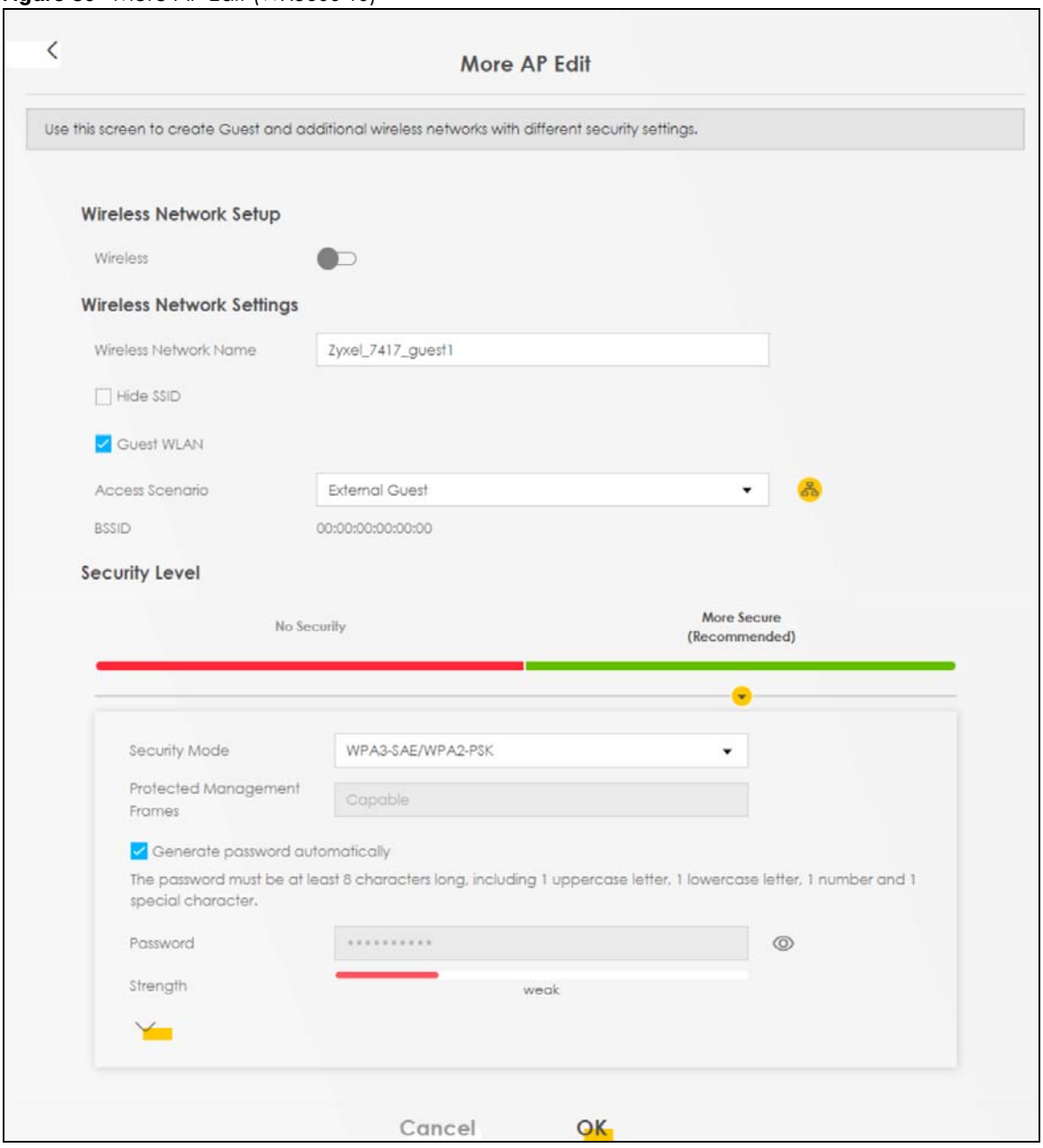


Figure 50 More AP Edit (WX5600-T0)



The Guest SSID (**Wireless Network Name**) depends on the state of the Main SSID. For example, when the 2.4 GHz Main SSID is enabled, then the 2.4 GHz Guest SSID can be enabled. But when the 2.4 GHz Main SSID is disabled, then the 2.4 GHz Guest SSID is automatically disabled (cannot be enabled by the user).

4 In the **Guest/More AP** screen, click the **Modify** icon to configure the third WiFi network group. Configure the screen using the provided parameters and click **OK**.

Figure 51 More AP Edit (WX3401-B0/WX3100-T0)

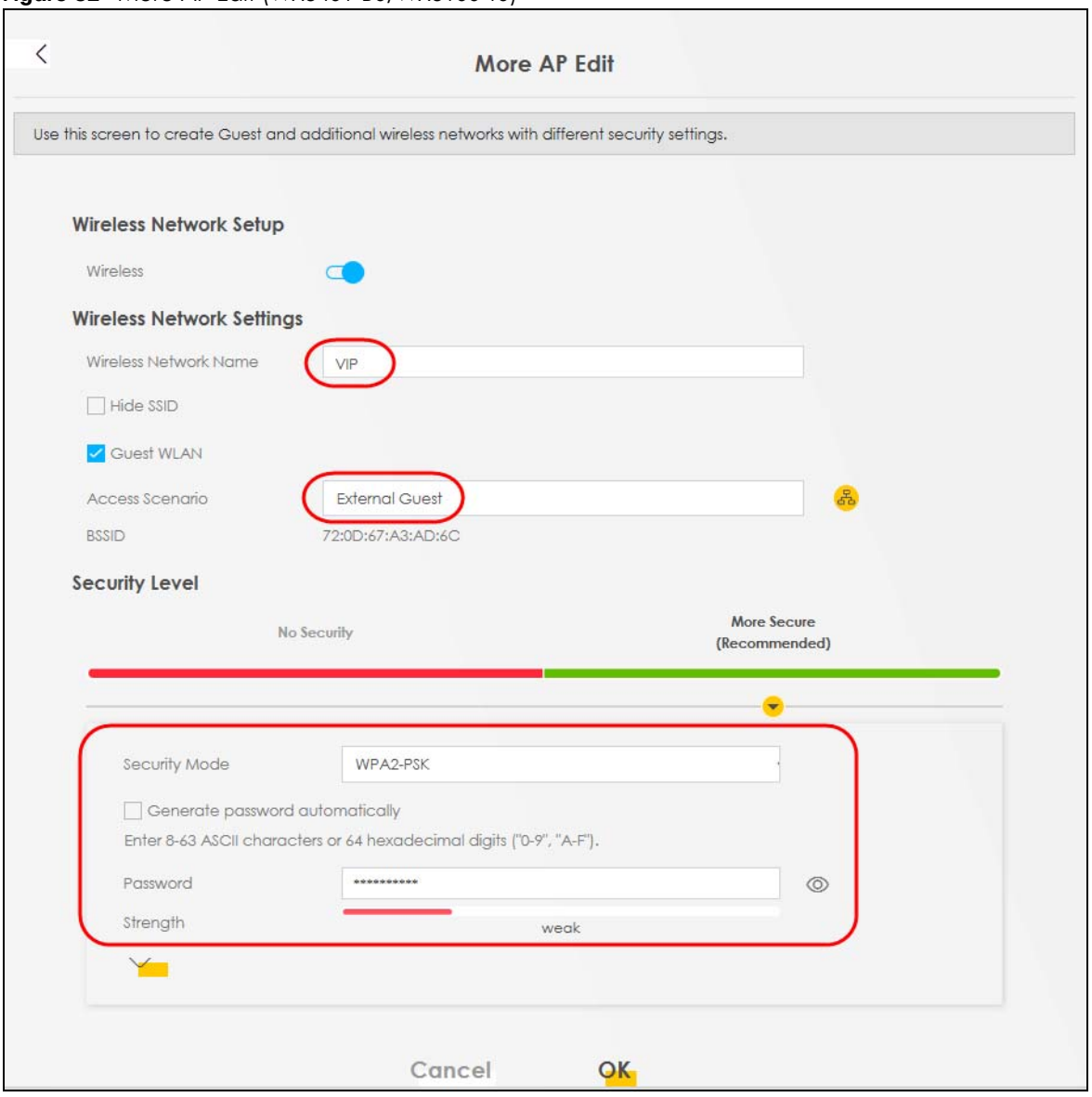
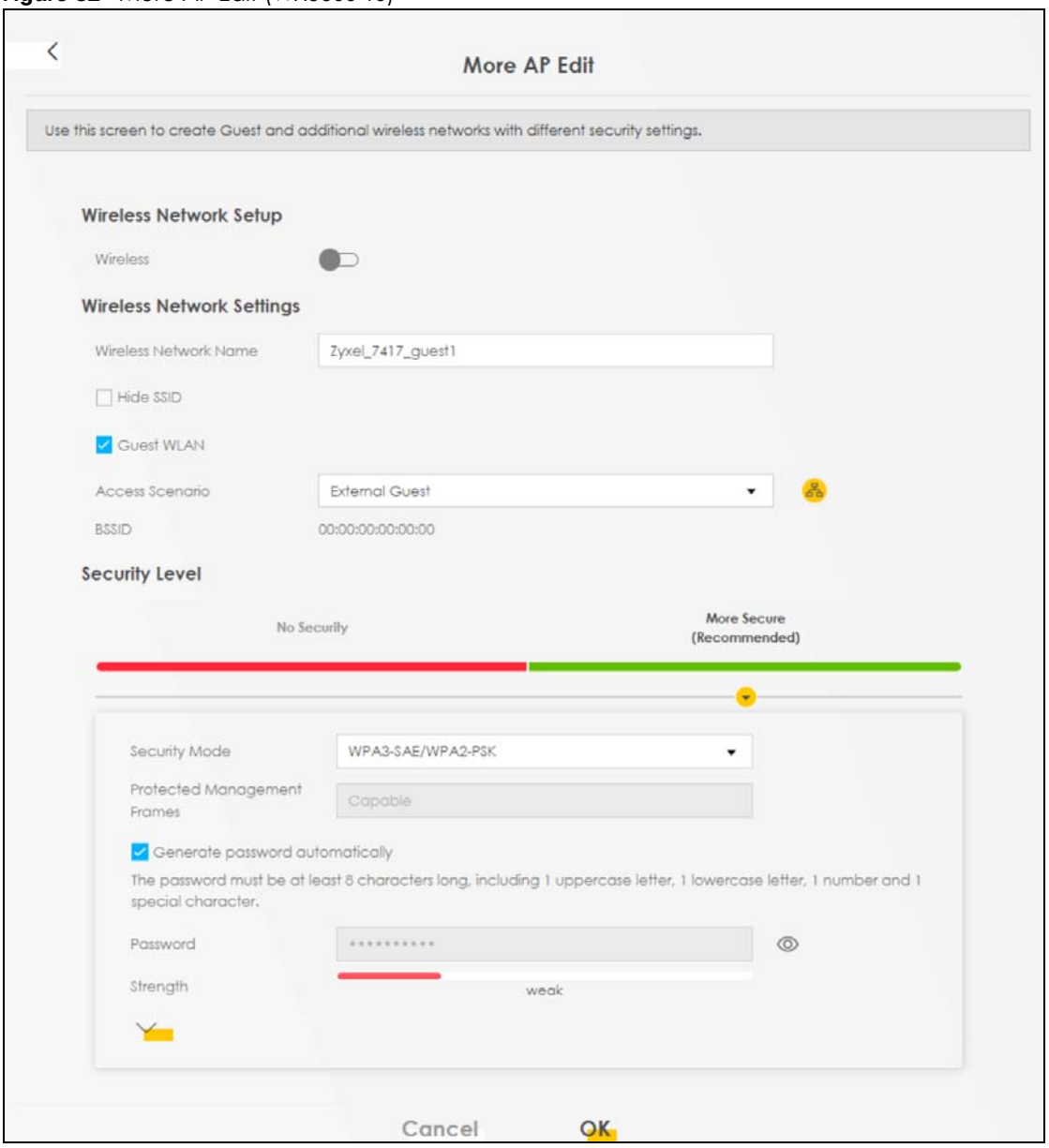


Figure 52 More AP Edit (WX5600-T0)



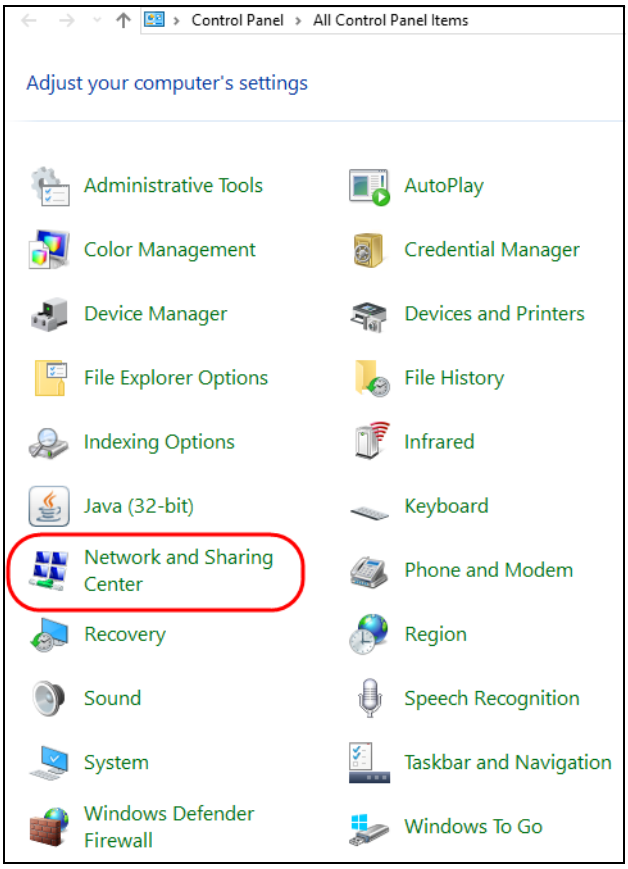
5 Check the status of **VIP** and **Guest** in the **Guest/More AP** screen. The yellow bulbs signify that the SSIDs are active and ready for WiFi access.

6.2.5 Connecting to the WX Device's WiFi Network (Windows 10)

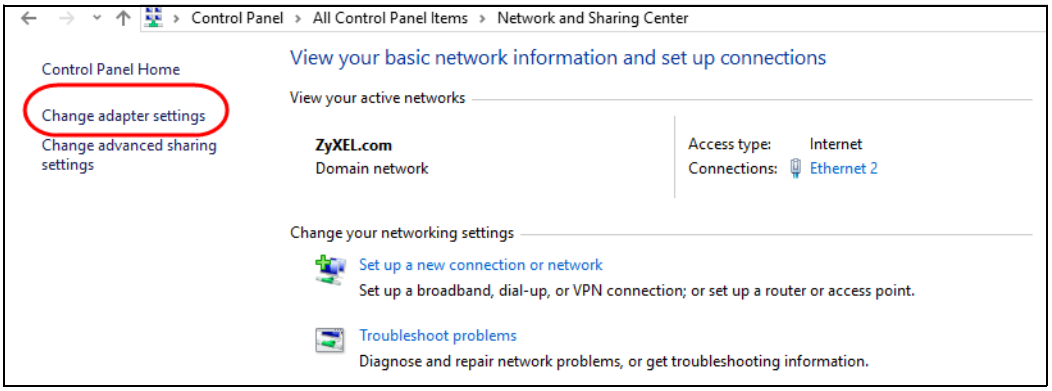
This section shows how to set the IP address of a computer using Windows 10 to be in the same subnet as a WX Device.

1 In Windows 10, open the **Control Panel**.

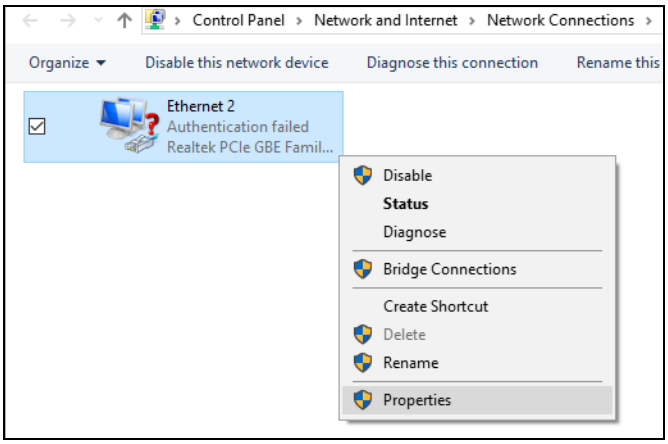
2 Click **Network and Internet** (this field may be missing in your version) > **Network and Sharing Center**.



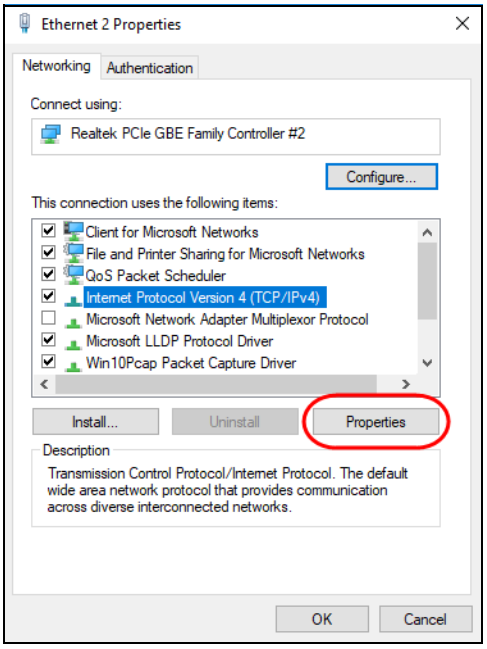
3 Click **Change adapter settings**.



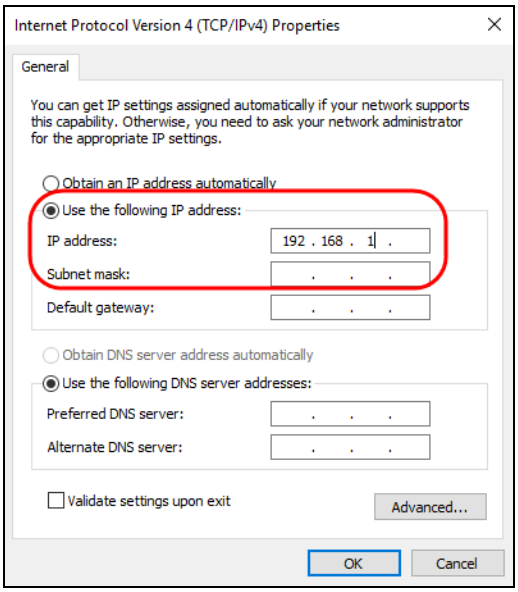
4 Right-click the **Ethernet** icon, and then select **Properties**.



5 Click **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties**.



6 Select **Use the following IP address** and enter an **IP address** from **192.168.1.3** to **192.168.1.254**. The **Subnet mask** will be entered automatically.



7 Click **OK** when you are done and close all windows.

6.3 Device Maintenance

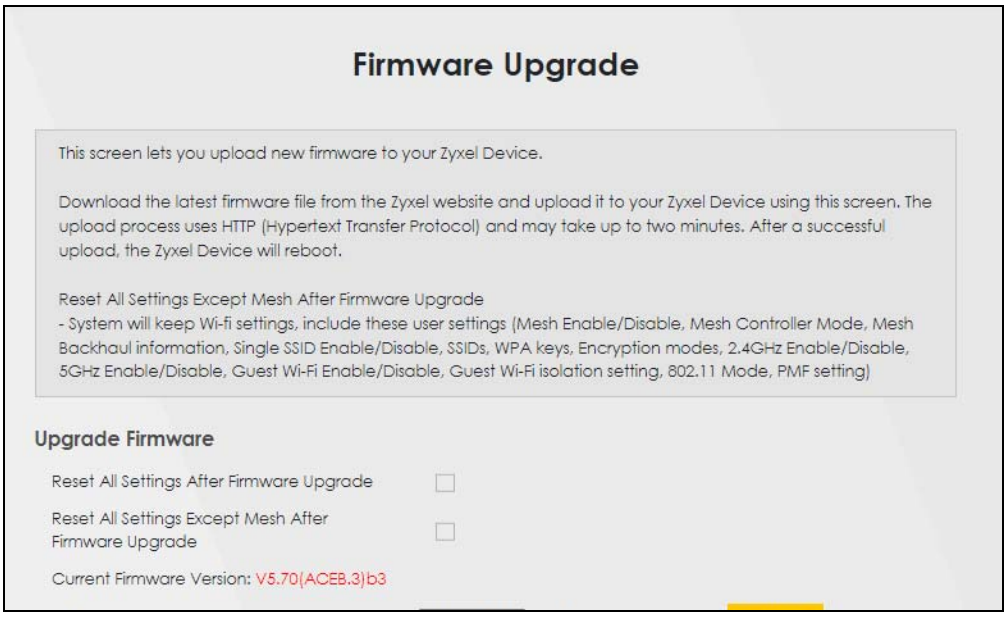
6.3.1 Upgrading the Firmware

Upload the firmware to the WX Device for feature enhancements.

1 Download the firmware file at *www.zyxel.com* in a compressed file. Decompress the file.

2 Go to the **Maintenance** > **Firmware Upgrade** screen.

3 Click **Browse** and select a .bin file to upload. Click **Upload**.



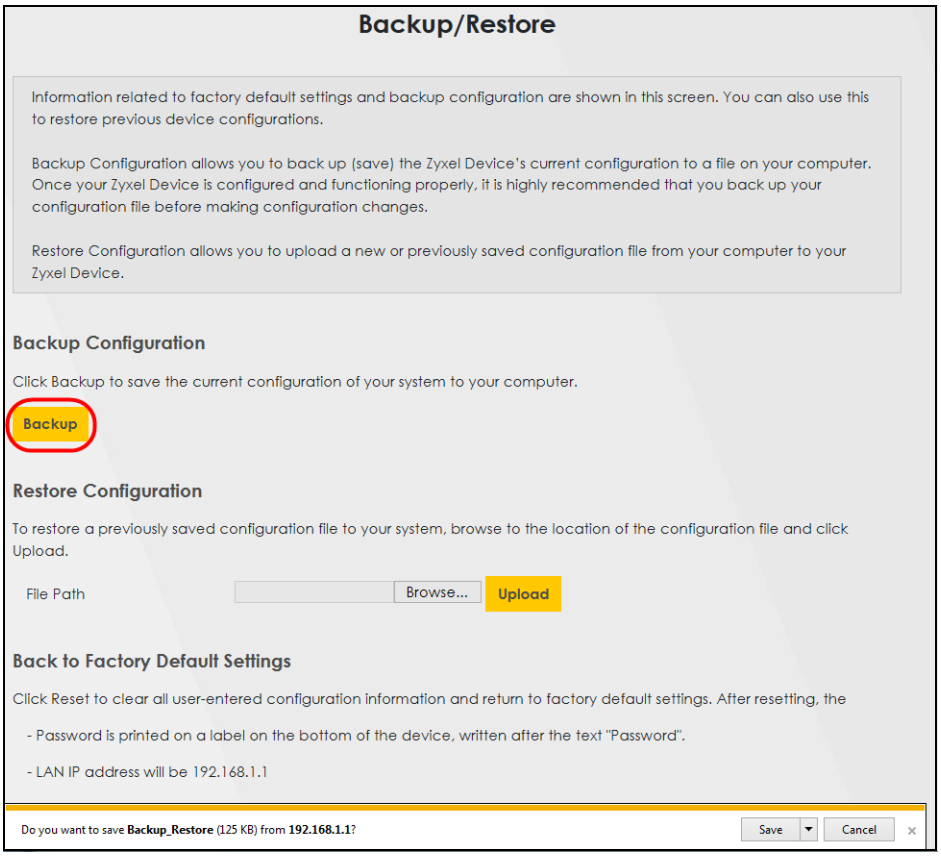
4 This process may take up to 2 minutes to finish. After 2 minutes, log in again and check your new firmware version in the **Status** screen.

6.3.2 Backing up the Device Configuration

Back up a configuration file in case you want to return to your previous settings.

1 Go to the **Maintenance** > **Backup/Restore** screen.

2 Click **Backup** in the **Backup Configuration** section, and a configuration file will be saved to your computer.

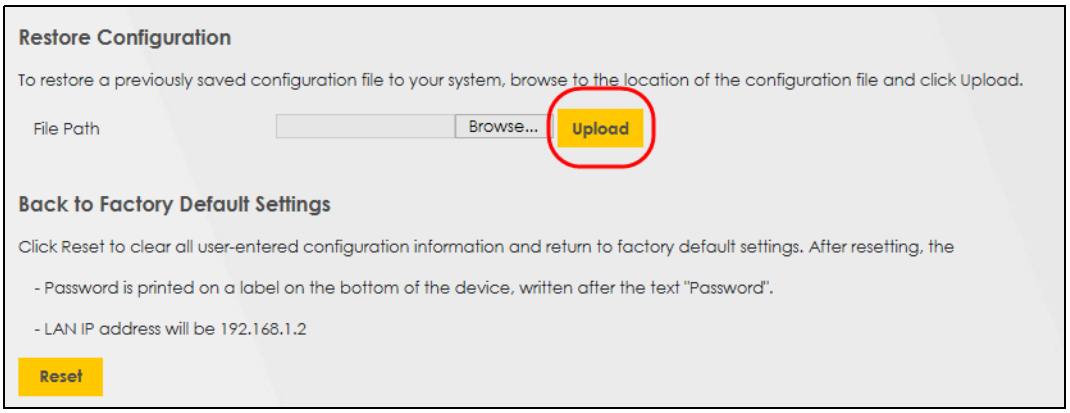


6.3.3 Restoring the Device Configuration

You can upload a previously saved configuration file from your computer to your WX Device to restore that previous configuration.

1 Go to the **Maintenance** > **Backup/Restore** screen.

2 Click **Browse** in **Restore Configuration** section, and select the configuration file that you want to upload. Click **Upload**.



3 The WX Device will restart automatically after the configuration file is successfully uploaded. Wait for one minute before logging into the WX Device again.

CHAPTER 7
Wireless

7.1 Wireless Overview

This chapter describes the WX Device's **Network Setting** > **Wireless** screens. Use these screens to set up your WX Device's WiFi connection and security settings.

7.1.1 What You Can Do in this Chapter

This section describes the WX Device's **Wireless** screens. Use these screens to set up your WX Device's WiFi connection.

- Use the **General** screen to enable WiFi, enter the SSID and select the WiFi security mode (Section 7.2 on page 102).
- Use the **Guest/More AP** screen to set up multiple WiFi networks on your WX Device (Section 7.3 on page 109).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) (Section 7.4 on page 113).
- Use the **WMM** screen to enable WiFi MultiMedia (WMM) to ensure quality of service in WiFi networks for multimedia applications (Section 7.5 on page 116).
- Use the **Others** screen to configure WiFi advanced features, such as the DTIM interval (Section 7.6 on page 117).
- Use the **Channel Status** screen to scan WiFi channel noises and view the results (Section 7.7 on page 119).

7.1.2 What You Need to Know

WiFi Basics

"WiFi" is essentially radio communication. In the same way that walkie-talkie radios send and receive information over the airwaves, WiFi networking devices exchange information with one another. A WiFi networking device is just like a radio that lets your computer exchange information with radios attached to other computers. Like walkie-talkies, most WiFi networking devices operate at radio frequency bands that are open to the public and do not require a license to use. However, WiFi networking is different from that of most traditional radio communications in that there are a number of WiFi networking standards available with different methods of data encryption.

WiFi6 / IEEE 802.11ax

WiFi6 is backwards compatible with IEEE 802.11a/b/g/n/ac and is most suitable in areas with a high concentration of users. WiFi6 devices support Target Wakeup Time (TWT) allowing them to automatically power down when they are inactive.

The following table displays the comparison of the different WiFi standards.

WIFI STANDARD	MAXIMUM LINK RATE *	BAND	SIMULTANEOUS CONNECTIONS
802.11b	11 Mbps	2.4 GHz	1
802.11a/g	54 Mbps	2.4 GHz and 5 GHz	1
802.11n	600 Mbps	2.4 GHz and 5 GHz	1
802.11ac	6.93 Gbps	5 GHz	4
802.11ax	2.4 Gbps	2.4 GHz	128
	9.61 Gbps	5 GHz and 6 GHz	

* The maximum link rate is for reference under ideal conditions only.

7.2 Wireless General Settings

Use this screen to enable WiFi, enter the SSID and select the WiFi security mode. These are basic elements for starting a WiFi service. It is recommended that you select **More Secure** to enable **WPA2-PSK** data encryption.

Note: If you are configuring the WX Device from a computer connected to WiFi and you change the WX Device's SSID, channel or security settings, you will lose your WiFi connection when you press **Apply** to confirm. You must then change the WiFi settings of your computer to match the WX Device's new settings.

Click **Network Setting** > **Wireless** to open the **General** screen.

Figure 53 Network Setting > Wireless > General (WX3401-B0/WX3100-T0)

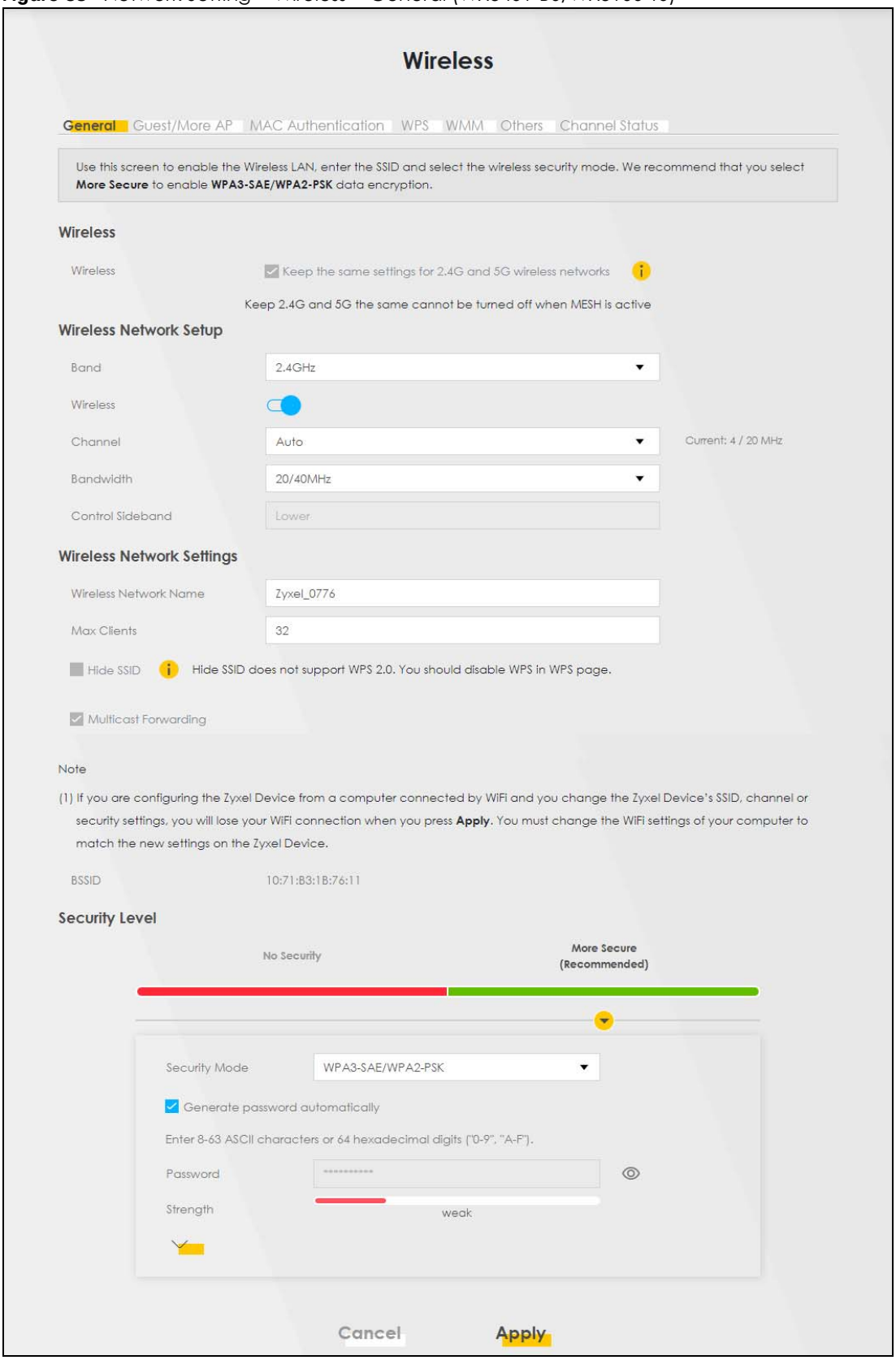
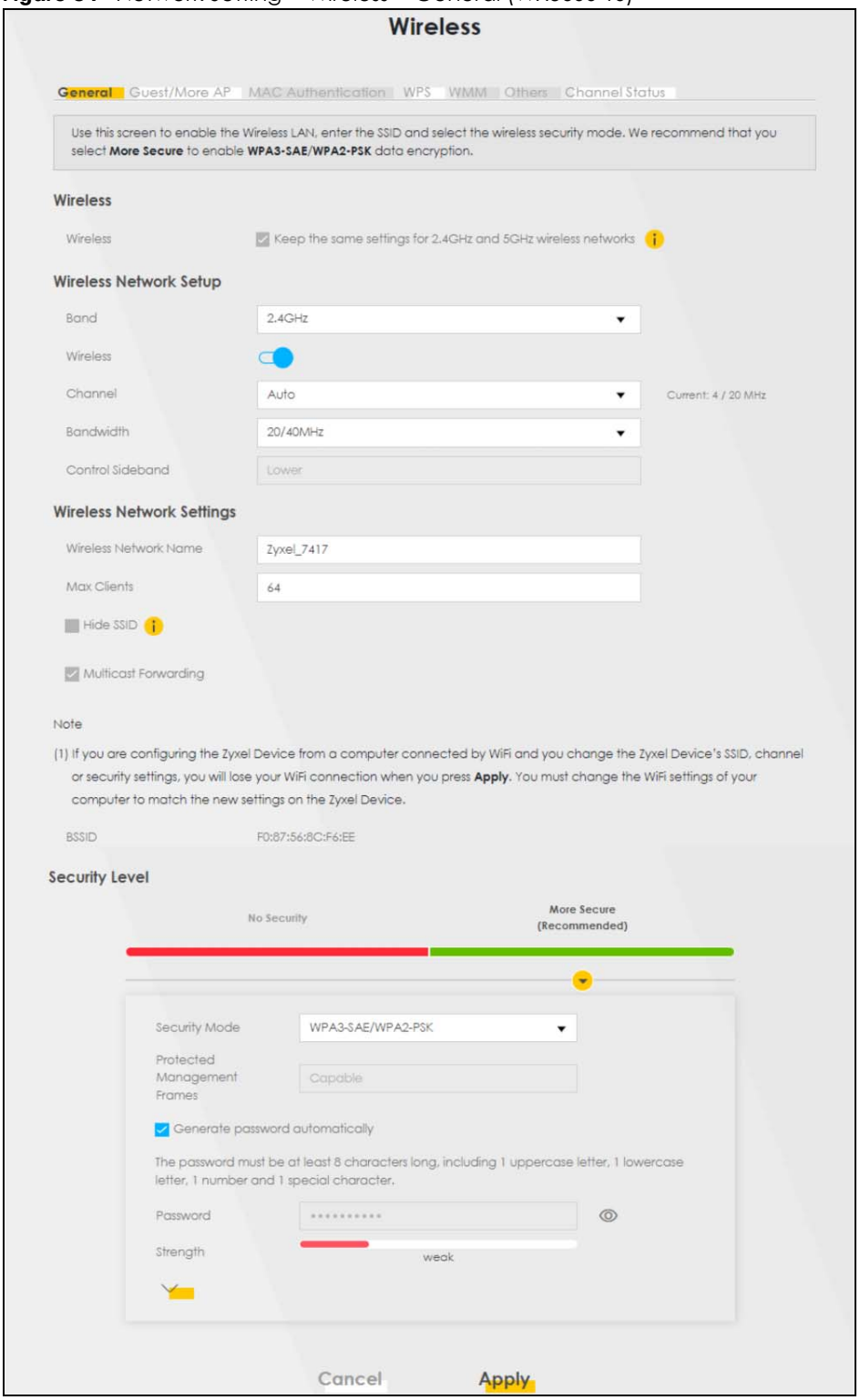


Figure 54 Network Setting > Wireless > General (WX5600-T0)



The following table describes the general WiFi labels in this screen.

Table 18 Network Setting > Wireless > General

LABEL	DESCRIPTION
Wireless	
Wireless	The **Keep the same settings for 2.4G and 5G wireless networks** switch cannot be turned off.
Wireless Network Setup	
Band	This shows the WiFi band which this radio profile is using. **2.4GHz** is the frequency used by IEEE 802.11b/g/n/ax WiFi clients while **5GHz** is used by IEEE 802.11a/n/ac/ax WiFi clients. Note: The **Operating Modes** and **AP List screen** are only available if you select the **5GHz Band**.
Wireless	Click this switch to enable or disable WiFi in this field. When the switch turns blue, the function is enabled. Otherwise, it is not.
Channel	Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. Use **Auto** to have the WX Device automatically determine a channel to use.
Bandwidth	Select whether the WX Device uses a WiFi channel width of **20MHz**, **40MHz, 20/40MHz, 20/40/80MHz**, or **20/40/80/160MHz**. A standard 20 MHz channel offers transfer speeds of up to 150 Mbps whereas a 40 MHz channel uses two standard channels and offers speeds of up to 300 Mbps. 40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. A 80 MHz channel consists of two adjacent 40 MHz channels. The WiFi clients must also support 40 MHz or 80 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the WiFi signal. A standard 20 MHz channel offers transfer speeds of up to 150 Mbps whereas a 40 MHz channel uses two standard channels and offers speeds of up to 300 Mbps. 40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The WiFi clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the WiFi signal. An 80 MHz channel groups adjacent 40 MHz channels into pairs to increase bandwidth even higher. Select **20MHz** if you want to lessen radio interference with other WiFi devices in your neighborhood or the WiFi clients do not support channel bonding. Because not all devices support 40 MHz channels, select **20MHz** or **20/40MHz** to allow the WX Device to adjust the channel bandwidth.
Control Sideband	This is available for some regions when you select a specific channel and set the **Bandwidth** field to **40MHz** or **20/40MHz**. Set whether the control channel (set in the **Channel** field) should be in the **Lower** or **Upper** range of channel bands.
Wireless Network Settings	
Wireless Network Name	The SSID (Service Set IDentity) identifies the service set with which a WiFi device is associated. WiFi devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for WiFi.
Max Clients	Specify the maximum number of clients that can connect to this network at the same time.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. This check box is grayed out if the WPS function is enabled in the **Network Setting** > **Wireless** > **WPS** screen.
Multicast Forwarding	Select this check box to allow the WX Device to convert WiFi multicast traffic into WiFi unicast traffic.
BSSID	This shows the MAC address of the WiFi interface on the WX Device when WiFi is enabled.

Table 18 Network Setting > Wireless > General (continued)

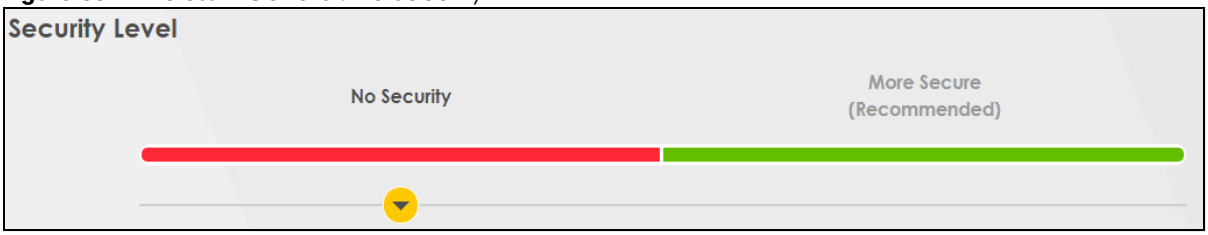
LABEL	DESCRIPTION
Security Level	
Security Mode	Select **More Secure (Recommended)** to add security on this WiFi network. The WiFi clients which want to associate to this network must have same WiFi security settings as the WX Device. When you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See the following sections for more details about this field.
Protected Management Frames	This option is only available when using **WPA2-PSK** as the **Security Mode** and **AES** Encryption in **Network Setting** > **Wireless** > **General**. Management frame protection (MFP) helps prevent WiFi DoS attacks. Select **Disable** if you do not want to use MFP. Select **Capable** to encrypt management frames of WiFi clients that support MFP. Clients that do not support MFP will still be allowed to join the WiFi network, but remain unprotected. Select **Required** to allow only clients that support MFP to join the WiFi network. Note: When Mesh is enabled, the settings of **Protected Management Frames** of 5G will follow 2.4G.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

7.2.1 No Security

Select **No Security** to allow WiFi stations to communicate with the WX Device without any data encryption or authentication.

Note: If you do not enable any WiFi security on your WX Device, your network is accessible to any WiFi networking device that is within range.

Figure 55 Wireless > General: No Security



The following table describes the labels in this screen.

Table 19 Wireless > General: No Security

LABEL	DESCRIPTION
Security Level	Choose **No Security** to allow all WiFi connections without data encryption or authentication.

7.2.2 More Secure (Recommended)

The WPA-PSK security mode provides both improved data encryption and user authentication over WEP. Using a Pre-Shared Key (PSK), both the WX Device and the connecting client share a common

password in order to validate the connection. This type of encryption, while robust, is not as strong as WPA, WPA2 or even WPA2-PSK. The WPA2-PSK security mode is a newer, more robust version of the WPA encryption standard. It offers slightly better security, although the use of PSK makes it less robust than it could be.

Click **Network Setting** > **Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA2-PSK, WPA3-SAE** or **WPA3-SAE/WPA2-PSK** from the **Security Mode** list.

Figure 56 Wireless > General: More Secure: WPA2-PSK (WX3401-B0/WX3100-T0)

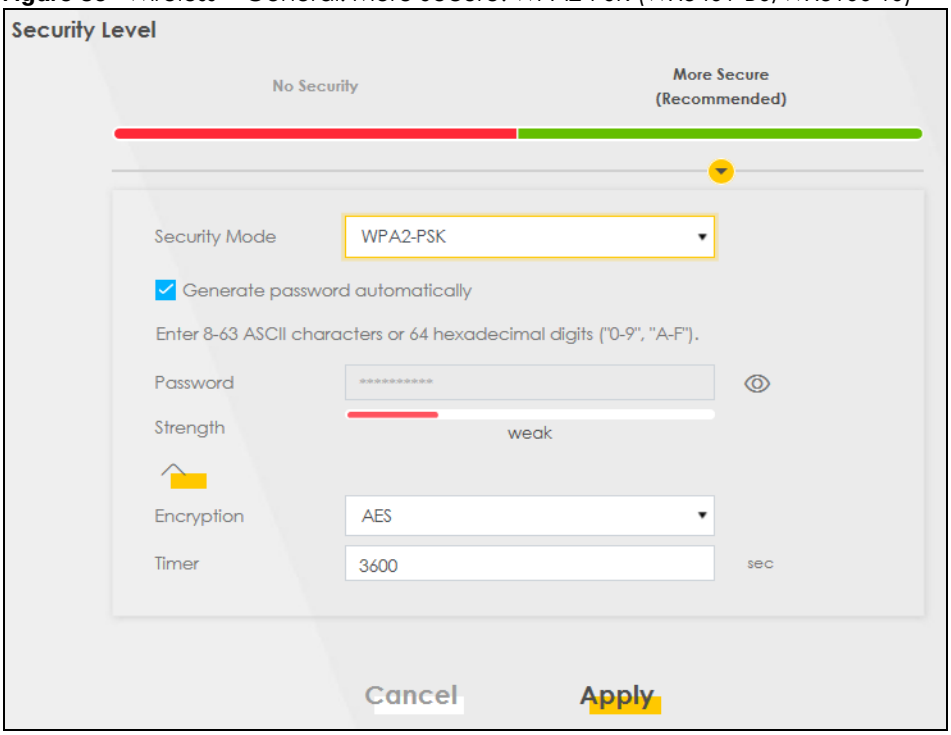
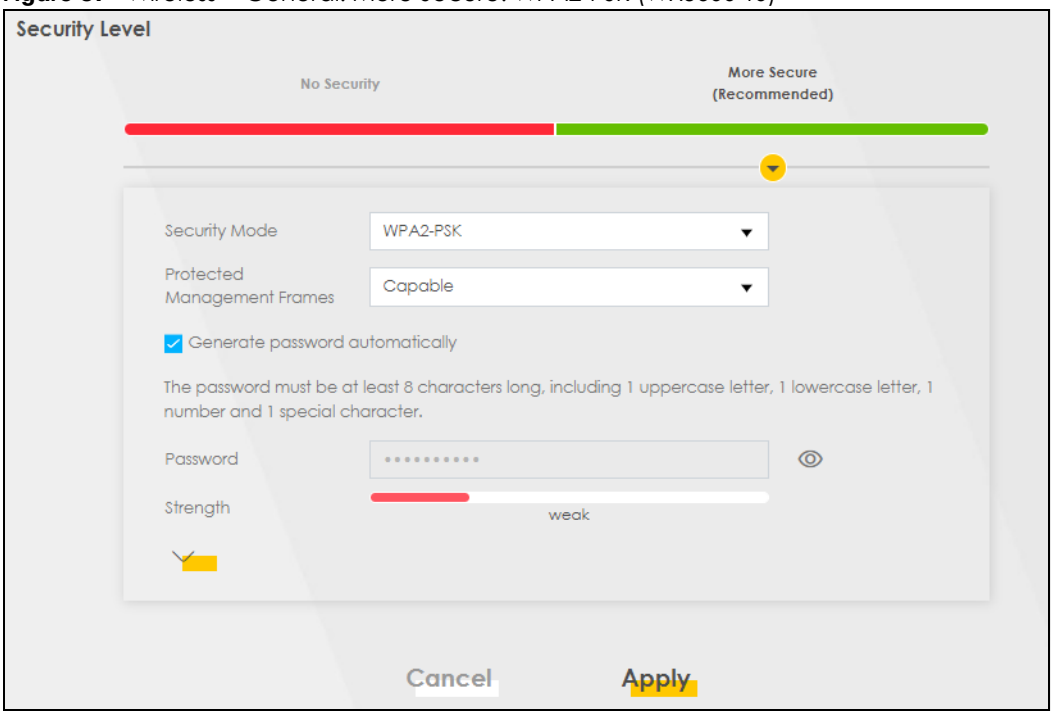


Figure 57 Wireless > General: More Secure: WPA2-PSK (WX5600-T0)



The following table describes the labels in this screen.

Table 20 Wireless > General: More Secure: WPA2-PSK

LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable WPA2-PSK data encryption.
Security Mode	Select the data encryption method the WX Device uses. Select **WPA2-PSK**, **WPA3-SAE** or **WPA3-SAE/WPA2-PSK** to add security on this WiFi network. The WiFi clients which want to associate to this network must have same WiFi security settings as this device. Or you can select **No Security** to allow any client to associate this network without authentication.
Protected Management Frames	This option is only available when using **WPA2-PSK** as the **Security Mode** and **AES** Encryption in **Network Setting** > **Wireless** > **General**. Management frame protection (MFP) helps prevent WiFi DoS attacks. Select **Disable** if you do not want to use MFP. Select **Capable** to encrypt management frames of WiFi clients that support MFP. Clients that do not support MFP will still be allowed to join the WiFi network, but remain unprotected. Select **Required** to allow only clients that support MFP to join the WiFi network. Note: When Mesh is enabled, the settings of **Protected Management Frames** of 5G will follow 2.4G.
Generate password automatically	Select this option to have the WX Device automatically generate a password. The password field will not be configurable when you select this option.

Table 20 Wireless > General: More Secure: WPA2-PSK (continued)

LABEL	DESCRIPTION
Password	Select **Generate password automatically** or enter a **Password**. The password has two uses. 1. Manual. Manually enter the same password on the WX Device and the client. Enter 8 – 63 ASCII characters or exactly 64 hexadecimal ('0 – 9', 'a – f') characters. 2. WPS. When using WPS, the WX Device sends this password to the client. Click the Eye icon to show or hide the password of your WiFi network. When the Eye icon is slashed, you will see the password in plain text. Otherwise, it is hidden.
	Click this to show more fields in this section. Click again to hide them.
Encryption	This field shows the **AES** type of data encryption.
Timer	The **Timer** is the rate at which the RADIUS server sends a new group key out to all clients.

7.3 Guest/More AP

This screen allows you to configure a guest WiFi network that allows access to the Internet only through the WX Device. You can also configure additional WiFi networks, each with different security settings, in this screen.

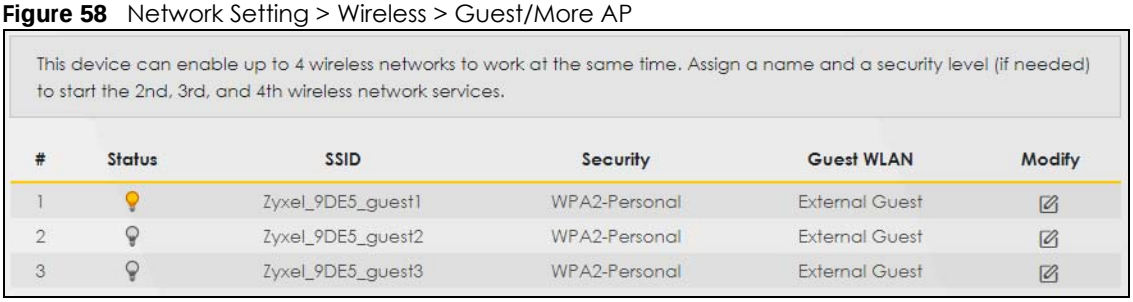
The following table introduces the supported WiFi networks.

Table 21 Supported WiFi Networks

WIFI NETWORKS	WHERE TO CONFIGURE
Main/1	Network Setting > Wireless > General screen
Guest/3	Network Setting > Wireless > Guest/More AP screen

Click **Network Setting** > **Wireless** > **Guest/More AP**. The following screen displays.

Figure 58 Network Setting > Wireless > Guest/More AP



The following table describes the labels in this screen.

Table 22 Network Setting > Wireless > Guest/More AP

LABEL	DESCRIPTION
#	This is the index number of the entry.
Status	This field indicates whether this SSID is active. A yellow bulb signifies that this SSID is active, while a gray bulb signifies that this SSID is not active.

Table 22 Network Setting > Wireless > Guest/More AP (continued)

LABEL	DESCRIPTION
SSID	An SSID profile is the set of parameters relating to one of the WX Device's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a WiFi device is associated. This field displays the name of the WiFi profile on the network. When a WiFi client scans for an AP to associate with, this is the name that is broadcast and seen in the WiFi client utility.
Security	This field indicates the security mode of the SSID profile.
Guest WLAN	This displays if the guest WiFi function has been enabled for this WiFi network. If **Home Guest** displays, clients can connect to each other directly. If **External Guest** displays, clients are blocked from connecting to each other directly. **N/A** displays if the guest WiFi network is disabled.
Modify	Click the **Edit** icon to configure the SSID profile.

7.3.1 Edit Guest/More AP Settings

Use this screen to create Guest and additional WiFi networks with different security settings.

Click the **Edit** icon next to an SSID in the **Guest/More AP** screen. The following screen displays.

Figure 59 Network Setting > Wireless > Guest/More AP > Edit (WX3100-T0 / WX3401-B0)

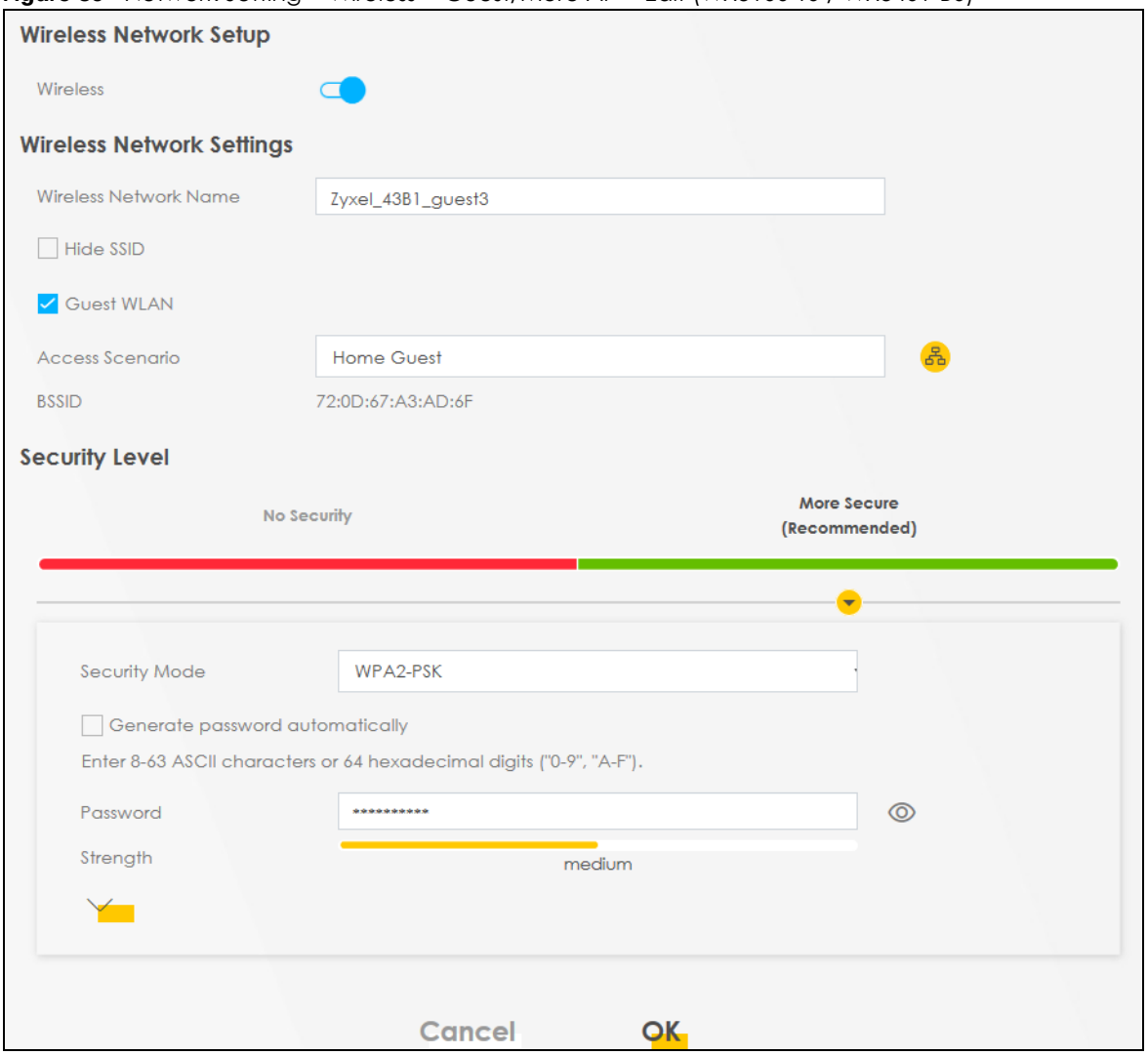
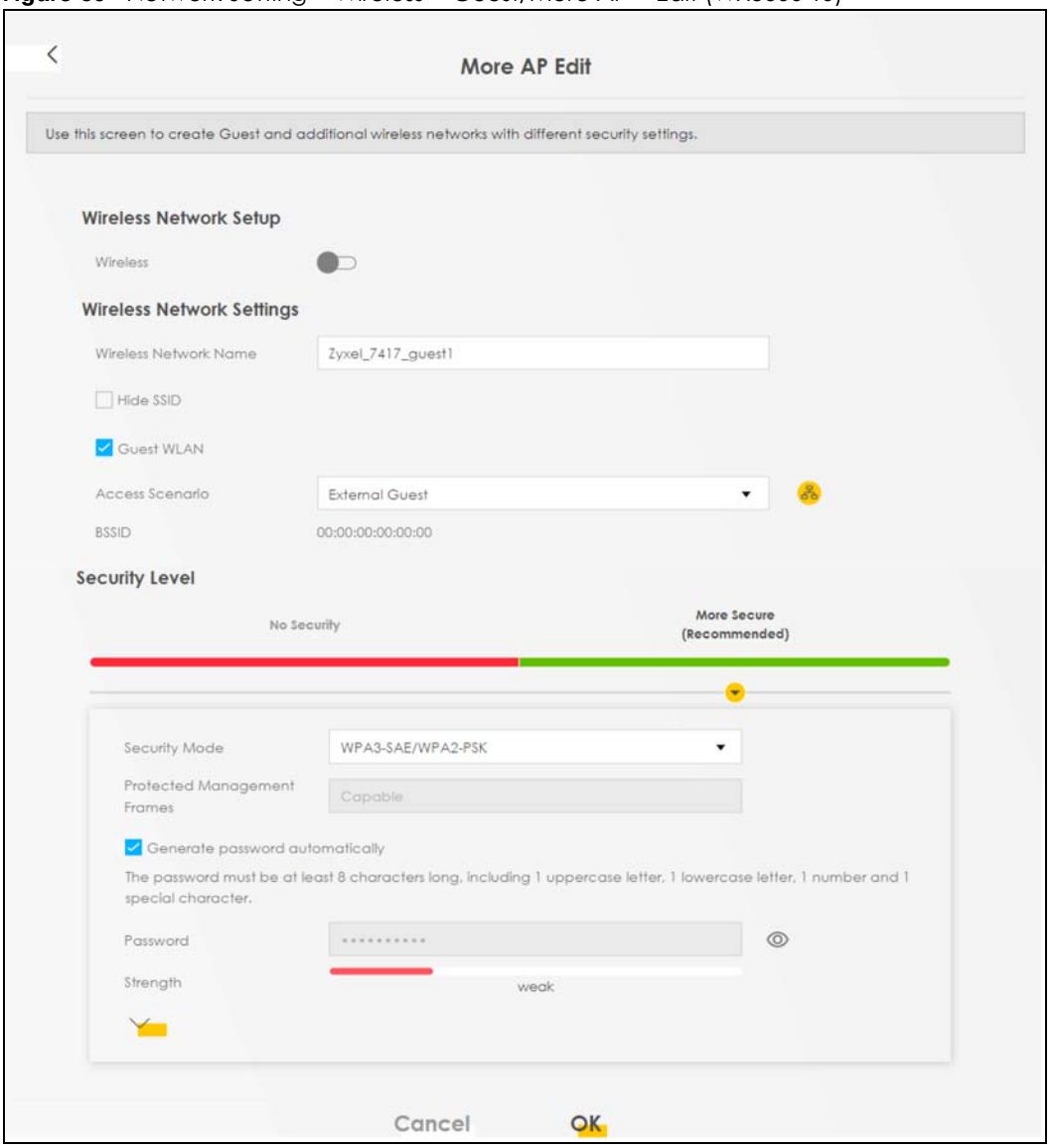


Figure 60 Network Setting > Wireless > Guest/More AP > Edit (WX5600-T0)



The following table describes the fields in this screen.

Table 23 Network Setting > Wireless > Guest/More AP > Edit

LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	Click this switch to enable or disable WiFi in this field. When the switch turns blue, the function is enabled; otherwise, it is not.
Wireless Network Settings	
Wireless Network Name	The SSID (Service Set IDentity) identifies the service set with which a WiFi device is associated. WiFi devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for WiFi.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Guest WLAN	Select this to create Guest WiFis for home and external clients. Select the WiFi type in the **Access Scenario** field.

Table 23 Network Setting > Wireless > Guest/More AP > Edit (continued)

LABEL	DESCRIPTION
Access Scenario	If you select **Home Guest**, clients can connect to each other directly. If you select **External Guest**, clients are blocked from connecting to each other directly.
BSSID	This shows the MAC address of the WiFi interface on the WX Device when WiFi is enabled.
Security Level	Select **More Secure (Recommended)** to add security on this WiFi network. The WiFi clients which want to associate to this network must have the same WiFi security settings as the WX Device. After you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See Section 7.2.1 on page 106 for more details about this field.
Security Mode	Select the security mode the WX Device uses. Select **WPA2-PSK, WPA3-SAE** or **WPA3-SAE/WPA2-PSK** to add security on this WiFi network. The WiFi clients which want to associate to this network must have same WiFi security settings as this device. Or you can select **No Security** to allow any client to associate this network without authentication.
Protected Management Frames	This option is only available when using **WPA2-PSK** as the **Security Mode** and **AES** Encryption in **Network Setting** > **Wireless** > **General**. Management frame protection (MFP) helps prevent WiFi DoS attacks. Select **Disable** if you do not want to use MFP. Select **Capable** to encrypt management frames of WiFi clients that support MFP. Clients that do not support MFP will still be allowed to join the WiFi network, but remain unprotected. Select **Required** to allow only clients that support MFP to join the WiFi network. Note: When Mesh is enabled, the settings of **Protected Management Frames** of 5G will follow 2.4G.
Generate password automatically	Select this option to have the WX Device automatically generate a password. The password field will not be configurable when you select this option.
Password	WPA2-PSK uses a simple common password, instead of user-specific credentials. If you did not select **Generate password automatically**, you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters. Click the Eye icon to show or hide the password of your WiFi network. When the Eye icon is slashed, you will see the password in plain text. Otherwise, it is hidden.
	Click this to show more fields in this section. Click again to hide them.
Encryption	This field shows the **AES** type of data encryption.
Timer	The **Timer** is the rate at which the RADIUS server sends a new group key out to all clients.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

7.4 WPS Settings

WiFi Protected Setup (WPS) allows you to quickly set up a WiFi network with strong security, without having to configure security settings manually. To set up a WPS connection between two devices, both devices must support WPS. It is recommended to use the Push Button Configuration (**PBC**) method if your WiFi client supports it. See Section 7.8.8.3 on page 127 for more information about WPS.

Note: The WX Device applies the security settings of the main SSID (**SSID1**) profile (see Section 7.2 on page 102).

Note: The WPS switch is grayed out when WiFi is disabled.

Click **Network Setting** > **Wireless** > **WPS**. The following screen displays. Click this switch and makes it turn blue. Click **Apply** to activate the WPS function. Then you can configure the WPS settings in this screen.

Figure 61 Network Setting > Wireless > WPS (WX3401-B0)

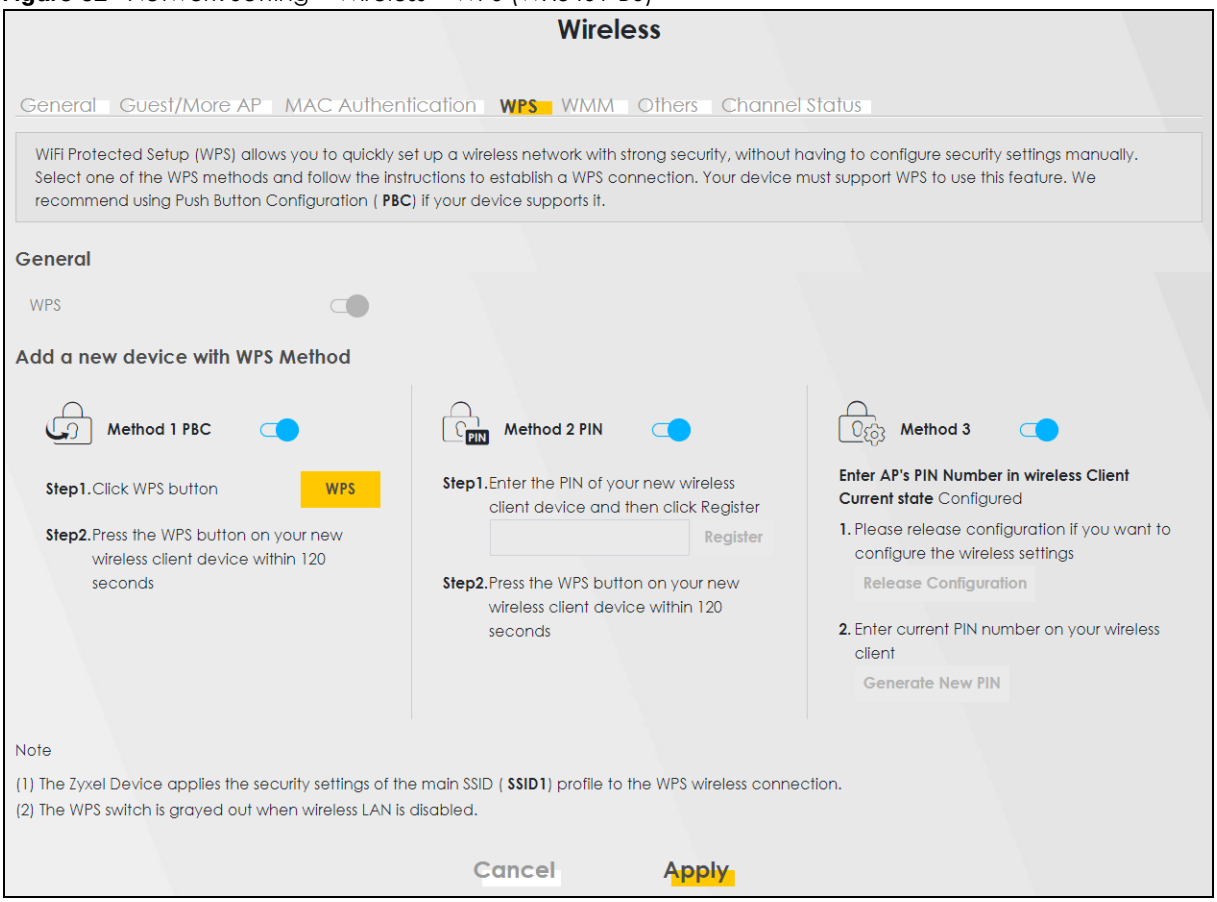
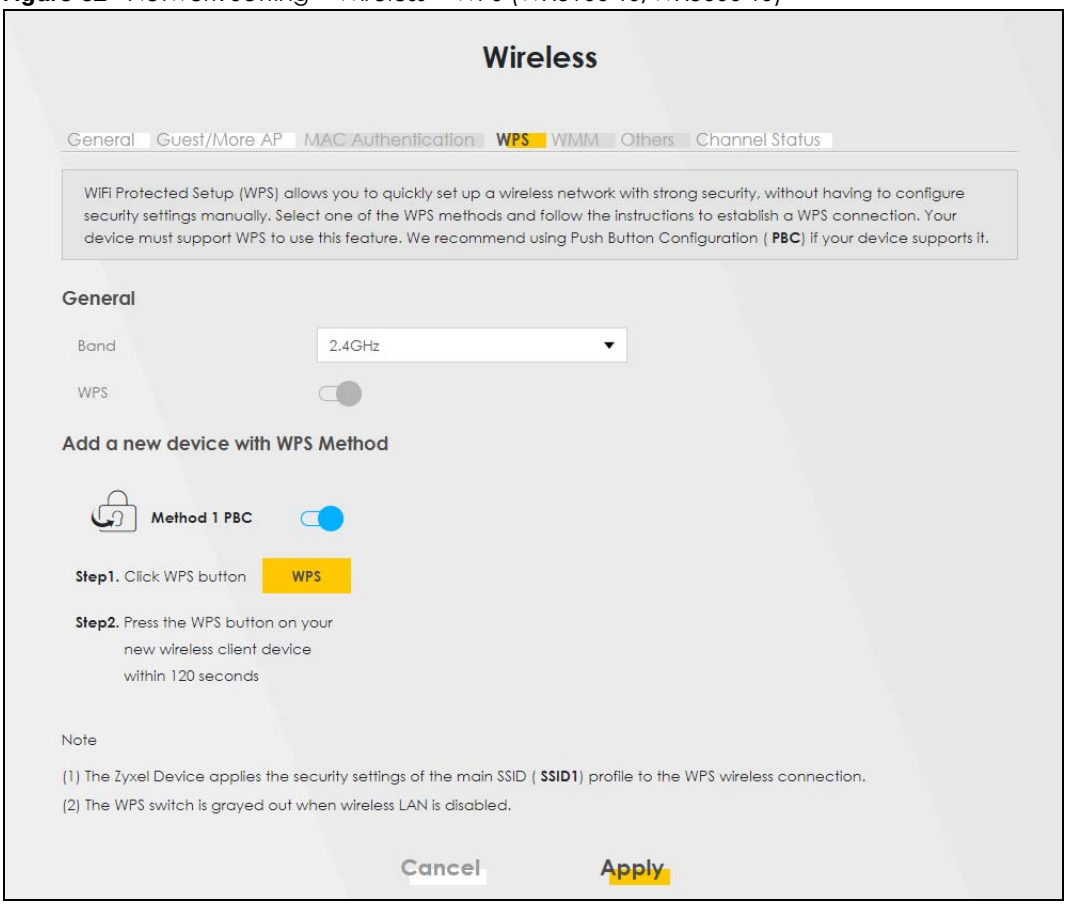


Figure 62 Network Setting > Wireless > WPS (WX3100-T0/WX5600-T0)



The following table describes the labels in this screen.

Table 24 Network Setting > Wireless > WPS

LABEL	DESCRIPTION
General	
WPS	Click this switch to activate or deactivate WPS on this WX Device. When the switch turns blue, the function is enabled. Otherwise, it is not.
Add a new device with WPS Method	
Method 1	Use this section to set up a WPS WiFi network using Push Button Configuration (PBC). Click this switch to make it turn blue. Click **Apply** to activate WPS method 1 on the WX Device.
WPS	Click this button to add another WPS-enabled WiFi device (within WiFi range of the WX Device) to your WiFi network. This button may either be a physical button on the outside of device, or a menu button similar to the **WPS** button on this screen. Note: You must press the other WiFi device's WPS button within 2 minutes of pressing this button.
Method 2	Use this section to set up a WPS WiFi network by entering the PIN of the client into the WX Device. Click this switch and make it turn blue. Click **Apply** to activate WPS method 2 on the WX Device.

Table 24 Network Setting > Wireless > WPS (continued)

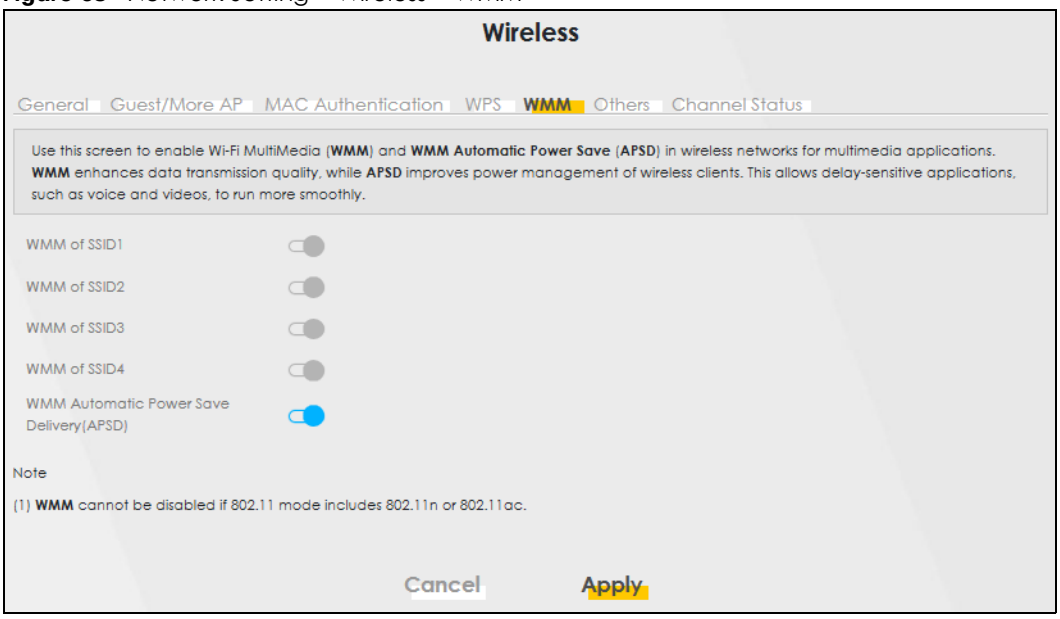
LABEL	DESCRIPTION
Register	Enter the PIN of the device that you are setting up a WPS connection with and click **Register** to authenticate and add the WiFi device to your WiFi network. You can find the PIN either on the outside of the device, or by checking the device's settings. Note: You must also activate WPS on that device within 2 minutes to have it present its PIN to the WX Device.
Method 3	Use this section to set up a WPS WiFi network by entering the PIN of the WX Device into the client. Click this switch and make it turn blue. Click **Apply** to activate WPS method 3 on the WX Device.
Release Configuration	The default WPS status is configured. Click this button to remove all configured WiFi and WiFi security settings for WPS connections on the WX Device.
Generate New PIN	If this method has been enabled, the PIN (Personal Identification Number) of the WX Device is shown here. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use the WPS push-button method. Click the **Generate New PIN** button to have the WX Device create a new PIN.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

7.5 WMM Settings

Use this screen to enable WiFi MultiMedia (**WMM**) and **WMM Automatic Power Save Delivery** (**APSD**) in WiFi networks for multimedia applications. **WMM** enhances data transmission quality, while **APSD** improves power management of WiFi clients. This allows delay-sensitive applications, such as voice and videos, to run more smoothly.

Click **Network Setting** > **Wireless** > **WMM** to display the following screen.

Figure 63 Network Setting > Wireless > WMM



Note: **WMM** cannot be disabled if 802.11 mode includes 802.11n or 802.11ac.

The following table describes the labels in this screen.

Table 25 Network Setting > Wireless > WMM

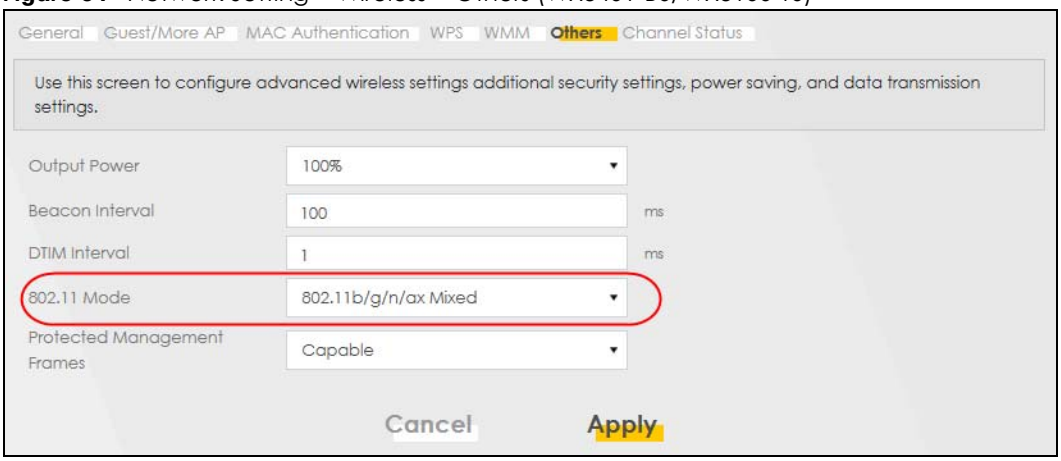
LABEL	DESCRIPTION
WMM of SSID1 – 4	Select **On** to have the WX Device automatically give the WiFi network (SSIDx) a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (WiFi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly. If the **802.11 Mode** in **Network Setting** > **Wireless** > **Others** is set to include 802.11n or 802.11ac, WMM cannot be disabled.
WMM Automatic Power Save Delivery (APSD)	Select this option to extend the battery life of your mobile devices (especially useful for small devices that are running multimedia applications). The WX Device goes to sleep mode to save power when it is not transmitting data. The AP buffers the packets sent to the WX Device until the WX Device "wakes up". The WX Device wakes up periodically to check for incoming data. Note: This works only if the WiFi device to which the WX Device is connected also supports this feature. APSD only affects SSID1. For SSID2~4, APSD is always enabled.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

7.6 Others Settings

Use this screen to configure advanced WiFi settings, such as additional security settings, power saving, and data transmission settings. Click **Network Setting** > **Wireless** > **Others**. The screen appears as shown.

See Section 7.8.2 on page 122 for detailed definitions of the terms listed in this screen.

Figure 64 Network Setting > Wireless > Others (WX3401-B0/WX3100-T0)



The following table describes the labels in this screen.

Table 26 Network Setting > Wireless > Others

LABEL	DESCRIPTION
Output Power	Set the output power of the WX Device. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following: **20%**, **40%**, **60%**, **80%** or **100%**.
Beacon Interval	When a WiFi network device sends a beacon, it includes with it a beacon interval. This specifies the time period before the 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. This value can be set from 50 ms to 1000 ms. A high value helps save current consumption of the access point.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255.

Table 26 Network Setting > Wireless > Others (continued)

LABEL	DESCRIPTION
802.11 Mode	For 2.4 GHz frequency WiFi devices: • Select **802.11b Only** to allow only IEEE 802.11b compliant WiFi devices to associate with the WX Device. • Select **802.11g Only** to allow only IEEE 802.11g compliant WiFi devices to associate with the WX Device. • Select **802.11n Only** to allow only IEEE 802.11n compliant WiFi devices to associate with the WX Device. • Select **802.11b/g Mixed** to allow either IEEE 802.11b or IEEE 802.11g compliant WiFi devices to associate with the WX Device. The transmission rate of your WX Device might be reduced. • Select **802.11b/g/n Mixed** to allow IEEE 802.11b, IEEE 802.11g or IEEE 802.11n compliant WiFi devices to associate with the WX Device. The transmission rate of your WX Device might be reduced. • Select **802.11b/g/n/ax Mixed** to allow IEEE 802.11b, IEEE 802.11g, IEEE 802.11n or IEEE 802.11ax compliant WiFi devices to associate with the WX Device. The transmission rate of your WX Device might be reduced. For 5 GHz frequency WiFi devices: • Select **802.11a Only** to allow only IEEE 802.11a compliant WiFi devices to associate with the WX Device. • Select **802.11n Only** to allow only IEEE 802.11n compliant WiFi devices to associate with the WX Device. • Select **802.11ac Only** to allow only IEEE 802.11ac compliant WiFi devices to associate with the WX Device. • Select **802.11a/n Mixed** to allow either IEEE 802.11a or IEEE 802.11n compliant WiFi devices to associate with the WX Device. The transmission rate of your WX Device might be reduced. • Select **802.11n/ac Mixed** to allow either IEEE 802.11n or IEEE 802.11ac compliant WiFi devices to associate with the WX Device. The transmission rate of your WX Device might be reduced. • Select **802.11a/n/ac Mixed** to allow IEEE 802.11a, IEEE 802.11n or IEEE 802.11ac compliant WiFi devices to associate with the WX Device. The transmission rate of your WX Device might be reduced. • Select **802.11a/n/ac/ax Mixed** to allow IEEE 802.11a, IEEE 802.11n, IEEE 802.11ac or IEEE 802.11ax compliant WiFi devices to associate with the WX Device. The transmission rate of your WX Device might be reduced.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

7.7 Channel Status Settings

Use the **Channel Status** screen to scan WiFi channel noises and view the results. Click **Network Setting** > **Wireless** > **Channel Status**. The screen appears as shown. Click **Scan** to scan the WiFi channels. You can view the results in the **Channel Scan Result** section.

Note: If the current channel is a DFS channel, the warning 'Channel scan process is denied because current channel is a DFS channel (Channel: 52 – 140). If you want to run channel scan, please select a non-DFS channel and try again.' appears.

Figure 65 Network Setting > Wireless > Channel Status

7.8 Technical Reference

This section discusses WiFis in depth. For more information, see Appendix B on page 186.

7.8.1 WiFi Network Overview

WiFi networks consist of WiFi clients, access points and bridges.

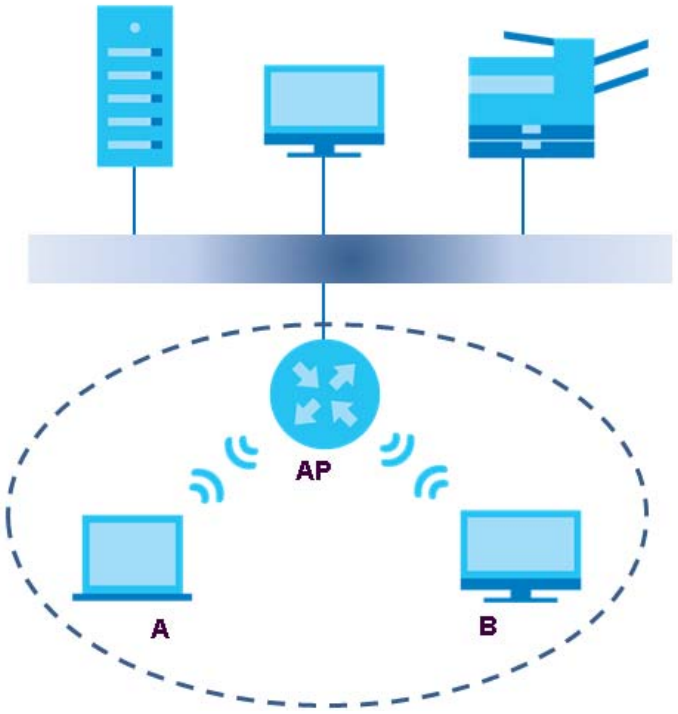
- A WiFi client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous WiFi clients and let them access the network.
- A bridge is a radio that relays communications between access points and WiFi clients, extending a network's range.

Traditionally, a WiFi network operates in one of two ways.

- An "infrastructure" type of network has one or more access points and one or more WiFi clients. The WiFi clients connect to the access points.
- An "ad-hoc" type of network is one in which there is no access point. WiFi clients connect to one another in order to exchange information.

The following figure provides an example of a WiFi network.

Figure 66 Example of a WiFi Network



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

Every WiFi network must follow these basic guidelines.

- Every device in the same WiFi network must use the same SSID.

  The SSID is the name of the WiFi network. It stands for Service Set IDentifier.
- If two WiFi networks overlap, they should use a different channel.

  Like radio stations or television channels, each WiFi network uses a specific channel, or frequency, to send and receive information.
- Every device in the same WiFi network must use security compatible with the AP.

  Security stops unauthorized devices from using the WiFi network. It can also protect the information that is sent in the WiFi network.

Radio Channels

In the radio spectrum, there are certain frequency bands allocated for unlicensed, civilian use. For the purposes of WiFi networking, these bands are divided into numerous channels. This allows a variety of networks to exist in the same place without interfering with one another. When you create a network, you must select a channel to use.

Since the available unlicensed spectrum varies from one country to another, the number of available channels also varies.

7.8.2 Additional WiFi Terms

The following table describes some WiFi network terms and acronyms used in the WX Device's Web Configurator.

Table 27 Additional WiFi Terms

TERM	DESCRIPTION
RTS/CTS Threshold	In a WiFi network which covers a large area, WiFi devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through. By setting this value lower than the default value, the WiFi devices must sometimes get permission to send information to the WX Device. The lower the value, the more often the devices must get permission. If this value is greater than the fragmentation threshold value (see below), then WiFi devices never have to get permission to send information to the WX Device.
Preamble	A preamble affects the timing in your WiFi network. There are two preamble modes: long and short. If a device uses a different preamble mode than the WX Device does, it cannot communicate with the WX Device.
Authentication	The process of verifying whether a WiFi device is allowed to use the WiFi network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

7.8.3 WiFi Security Overview

By their nature, radio communications are simple to intercept. For WiFi data networks, this means that anyone within range of a WiFi network without security can not only read the data passing over the airwaves, but also join the network. Once an unauthorized person has access to the network, he or she can steal information or introduce malware (malicious software) intended to compromise the network. For these reasons, a variety of security systems have been developed to ensure that only authorized people can use a WiFi data network, or understand the data carried on it.

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a user name and password, or a "key" phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only people with the code key can understand the information, and only people who have been authenticated are given the code key.

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Protocol (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is very secure if you use a long key which is difficult for an attacker's software to guess – for example, a twenty-letter long string of apparently random numbers and letters - but it is not very secure if you use a short key which is very easy to guess - for example, a three-letter word from the dictionary.

Because of the damage that can be done by a malicious attacker, it is not just people who have sensitive information on their network who should use security. Everybody who uses any WiFi network should ensure that effective security is in place.

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is Vanishing Point (which you know was made in 1971) you could use "70dodchal71vanpoi" as your security key.

The following sections introduce different types of WiFi security you can set up in the WiFi network.

7.8.3.1 SSID

Normally, the WX Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the WX Device does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized WiFi devices to get the SSID. In addition, unauthorized WiFi devices can still see the information that is sent in the WiFi network.

7.8.3.2 MAC Address Filter

Every device that can use a WiFi network has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the WiFi network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the WX Device which devices are allowed or not allowed to use the WiFi network. If a device is allowed to use the WiFi network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the WiFi network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the WiFi network. Furthermore, there are ways for unauthorized WiFi devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the WiFi network.

7.8.3.3 User Authentication

Authentication is the process of verifying whether a WiFi device is allowed to use the WiFi network. You can make every user log in to the WiFi network before using it. However, every device in the WiFi network has to support IEEE 802.1x to do this.

For WiFi networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized WiFi devices can still see the information that is sent in the WiFi network, even if they cannot use the WiFi network. Furthermore, there are ways for unauthorized WiFi users to get a valid user name and password. Then, they can use that user name and password to use the WiFi network.

1. Some WiFi devices, such as scanners, can detect WiFi networks but cannot use WiFi networks. These kinds of WIFi devices might not have MAC addresses.
2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

7.8.3.4 Encryption

WiFi networks can use encryption to protect the information that is sent in the WiFi network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

Many types of encryption use a key to protect the information in the WiFi network. The longer the key, the stronger the encryption. Every device in the WiFi network must have the same key.

7.8.4 Signal Problems

Because WiFi networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

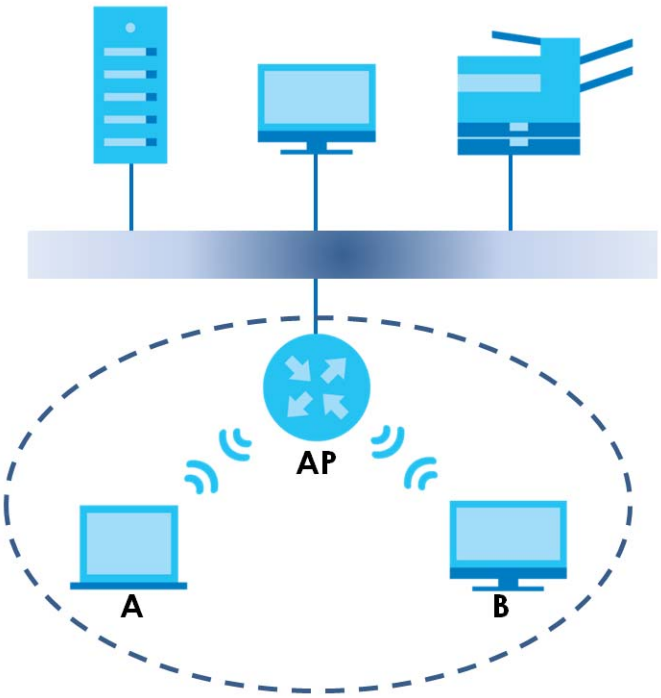
Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

7.8.5 BSS

A Basic Service Set (BSS) exists when all communications between WiFi stations or between a WiFi station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between WiFi stations in the BSS. When Intra-BSS traffic blocking is disabled, WiFi station A and B can access the wired network and communicate with each other. When Intra-BSS traffic blocking is enabled, WiFi station A and B can still access the wired network but cannot communicate with each other.

Figure 67 Basic Service Set



7.8.6 MBSSID

Traditionally, you need to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there is also the possibility of channel interference. The WX Device's MBSSID (Multiple Basic Service Set IDentifier) function allows you to use one access point to provide several BSSs simultaneously. You can then assign varying QoS priorities and/or security modes to different SSIDs.

WiFi devices can use different BSSIDs to associate with the same AP.

7.8.6.1 Notes on Multiple BSSs

- A maximum of eight BSSs are allowed on one AP simultaneously.
- You must use different keys for different BSSs. If two WiFi devices have different BSSIDs (they are in different BSSs), but have the same keys, they may hear each other's communications (but not communicate with each other).
- MBSSID should not replace but rather be used in conjunction with 802.1x security.

7.8.7 Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant WiFi adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other WiFi devices on the network support, and to provide more reliable communications in busy WiFi networks.

Use short preamble if you are sure all WiFi devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all WiFi devices on the network support it, otherwise the WX Device uses long preamble.

Note: The WiFi devices MUST use the same preamble mode in order to communicate.

7.8.8 WiFi Protected Setup (WPS)

Your WX Device supports WiFi Protected Setup (WPS), which is an easy way to set up a secure WiFi network. WPS is an industry standard specification, defined by the Wi-Fi Alliance.

WPS allows you to quickly set up a WiFi network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has 2 minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

7.8.8.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

1. Ensure that the two devices you want to set up are within WiFi range of one another.
2. Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this – for the WX Device, see Section 7.4 on page 113).
3. Press the button on one of the devices (it does not matter which). For the WX Device you must press the WPS button for more than 5 seconds.
4. Within 2 minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through a secure connection to the enrollee.

   If you need to make sure that WPS worked, check the list of associated WiFi clients in the AP's configuration utility. If you see the WiFi client in the list, WPS was successful.

7.8.8.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the WiFi client) into the second device (usually the Access Point or WiFi router). Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

Take the following steps to set up a WPS connection between an access point or WiFi router (referred to here as the AP) and a client device using the PIN method.

1. Ensure WPS is enabled on both devices.
2. Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.
3. Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN – for the WX Device, see Section 7.4 on page 113).
4. Enter the client's PIN in the AP's configuration interface.

5 If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client – it does not matter which.

6 Start WPS on both devices within 2 minutes.

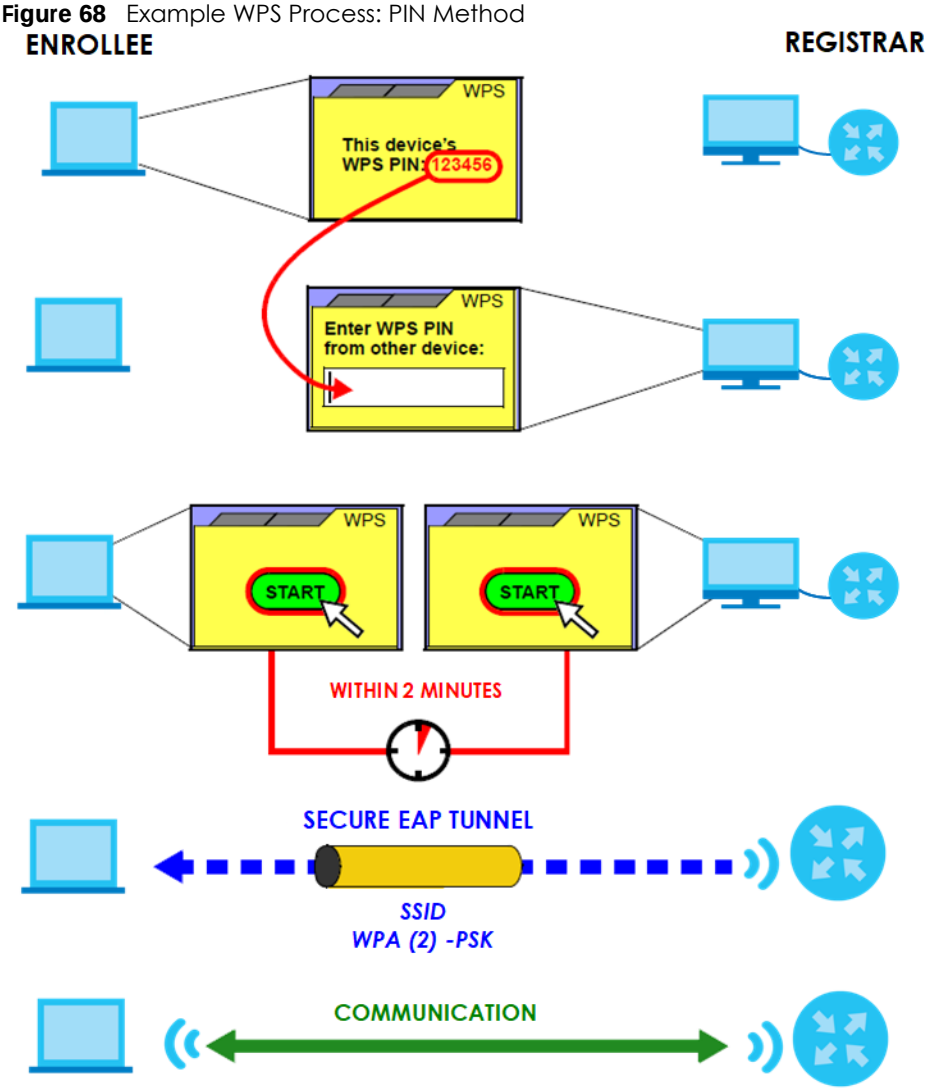
7 Use the configuration utility to activate WPS, not the push-button on the device itself.

8 On a computer connected to the WiFi client, try to connect to the Internet. If you can connect, WPS was successful.

If you cannot connect, check the list of associated WiFi clients in the AP's configuration utility. If you see the WiFi client in the list, WPS was successful.

The following figure shows a WPS-enabled WiFi client (installed in a notebook computer) connecting to the WPS-enabled AP through the PIN method.

Figure 68 Example WPS Process: PIN Method



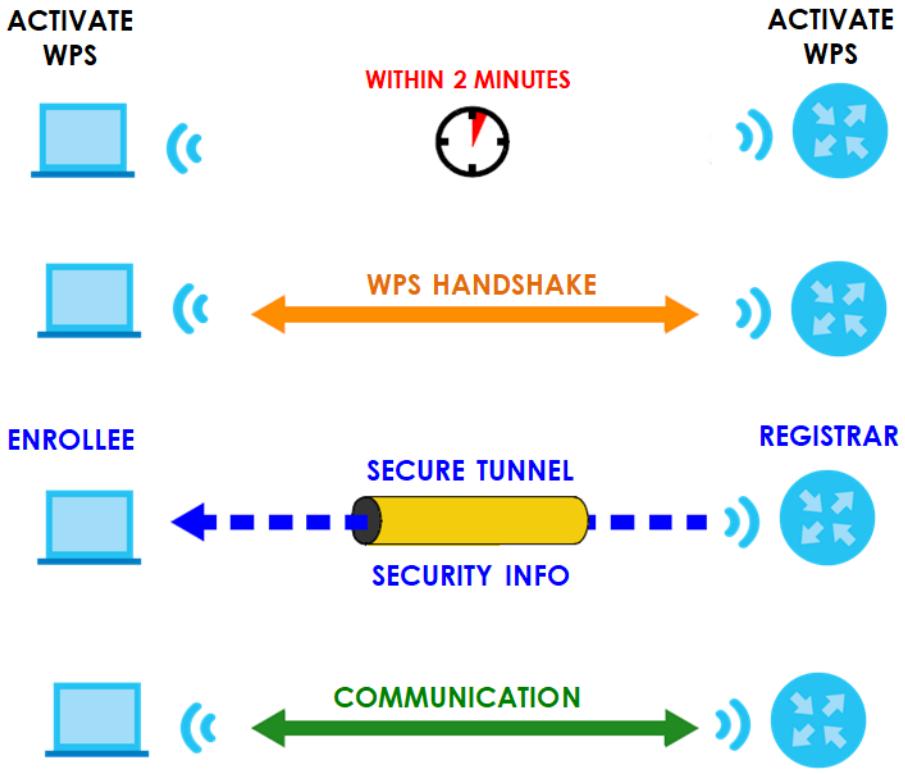
7.8.8.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the

enrollee (the device that receives network and security settings. The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA2-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 69 How WPS Works



The roles of registrar and enrollee last only as long as the WPS setup process is active (2 minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the WiFi client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled WiFi clients.

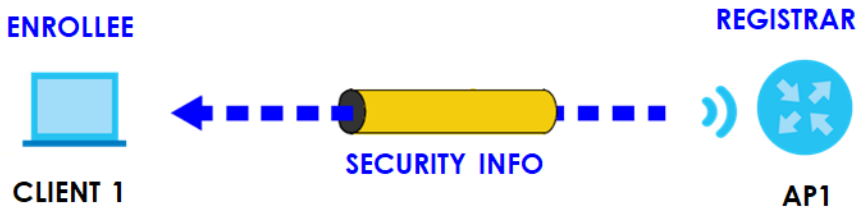
By default, a WPS devices is "unconfigured". This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes "configured". A configured WiFi client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

7.8.8.4 Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

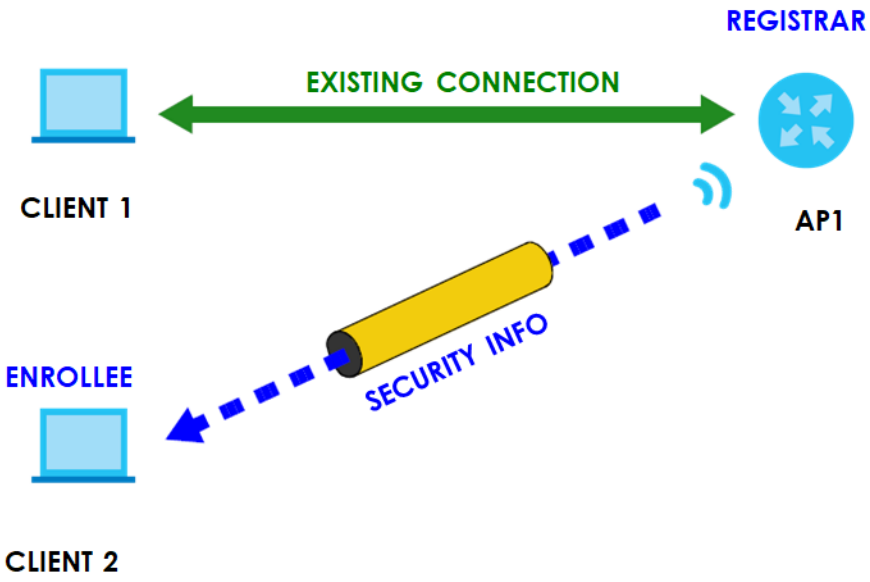
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 70 WPS: Example Network Step 1



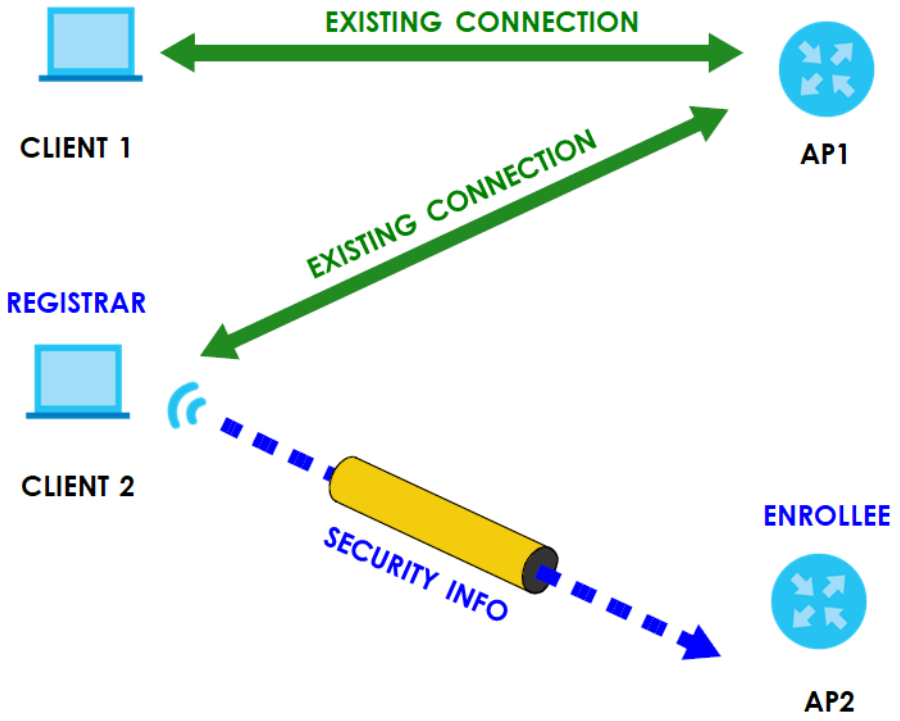
In step **2**, you add another WiFI client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

Figure 71 WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 72 WPS: Example Network Step 3



7.8.8.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a WiFi client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.
- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

  WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).
- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the "correct" enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

  You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point's configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access

point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your WiFi clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

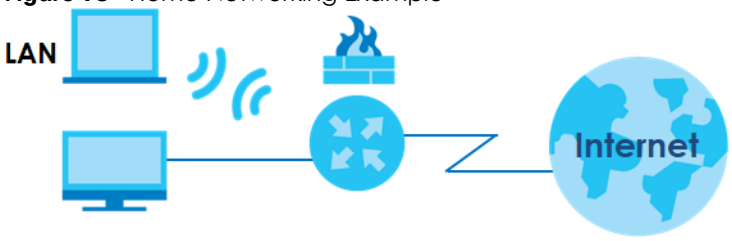
CHAPTER 8
Home Networking

8.1 Home Networking Overview

A Local Area Network (LAN) is a shared communication system to which many networking devices are connected. It is usually located in one immediate area such as a building or floor of a building.

Use the LAN screens to help you configure a LAN DHCP server and manage IP addresses.

Figure 73 Home Networking Example



8.1.1 What You Can Do in this Chapter

Use the **Home Networking** screen to set the LAN IP address, subnet mask, and DHCP settings of your WX Device (Section 8.2 on page 133).

8.1.2 What You Need To Know

8.1.2.1 About LAN

IP Address

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, and so on) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet Mask

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

8.1.3 Before You Begin

Find out the MAC addresses of your network devices if you intend to add them to the DHCP Client List screen.

8.2 Home Networking Screen

Use this screen to set the IP address and subnet mask of your WX Device. Configure DHCP settings to have a DHCP server assign IP addresses to devices. Click **Network Setting** > **Home Networking** to open the **Home Networking** screen.

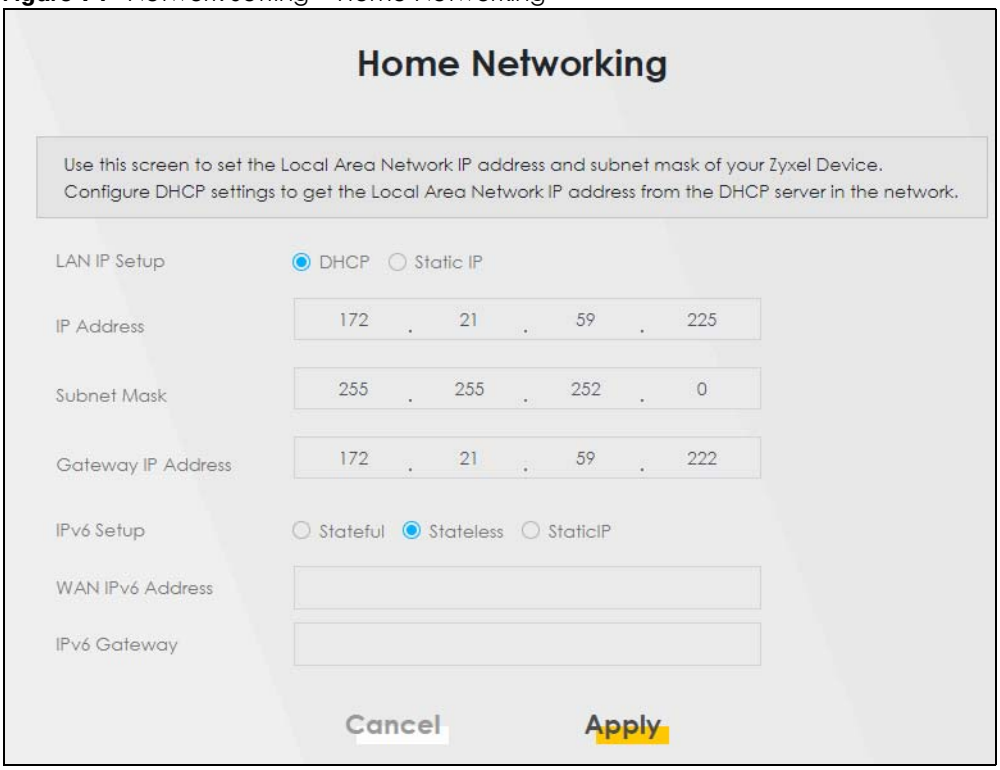
Follow these steps to configure your LAN settings.

1 Enter an IP address into the **IP Address** field. The IP address must be in dotted decimal notation. This will become the IP address of your WX Device.

2 Enter the IP subnet mask into the **IP Subnet Mask** field. Unless instructed otherwise it is best to leave this alone, the configurator will automatically compute a subnet mask based upon the IP address you entered.

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

Figure 74 Network Setting > Home Networking



The following table describes the fields in this screen.

Table 28 Network Setting > Home Networking

LABEL	DESCRIPTION
LAN IP Setup	Select **DHCP** to deploy the WX Device as a DHCP client in the network. When you enable this, the WX Device gets its IP address from the network's DHCP server (for example, your ISP or router). Users connected to the WX Device can now access the network (for example, the Internet if the IP address is given by the ISP or a router with Internet access). When you select this, you cannot enter an IP address for your WX Device in the field below. Select **Static IP** if you want to specify the IP address of your WX Device. Or if your ISP or network administrator gave you a static IP address to access the network or the Internet.
IP Address	Enter the LAN IPv4 IP address you want to assign to your WX Device in dotted decimal notation, for example, 192.168.1.2 (factory default).
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your WX Device automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.
Gateway IP Address	Enter a gateway IPv4 address (if your ISP or network administrator gave you one) in this field.
IPv6 Setup	Select how you want to obtain an IPv6 address: Select **Stateful** to obtain an IPv6 address using IPv6 stateful autoconfiguration. Select **Stateless** to obtain an IPv6 address using IPv6 stateless autoconfiguration. Select **Static** to configure a fixed IPv6 address for the WX Device.
WAN IPv6 Address	Enter an IPv6 IP address that your ISP gave you for the WAN interface.
IPv6 Gateway	Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your WX Device's interfaces. The gateway helps forward packets to their destinations.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

CHAPTER 9
Certificates

9.1 Certificates Overview

The WX 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.

9.1.1 What You Can Do in this Chapter

- Use the **Local Certificates** screen to view and import the WX Device's CA-signed (Certification Authority) certificates (Section 9.3 on page 135).
- Use the **Trusted CA** screen to save the certificates of trusted CAs to the WX Device. You can also export the certificates to a computer (Section 9.4 on page 139).

9.2 What You Need to Know

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

Certification Authority

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates. You can use the WX Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

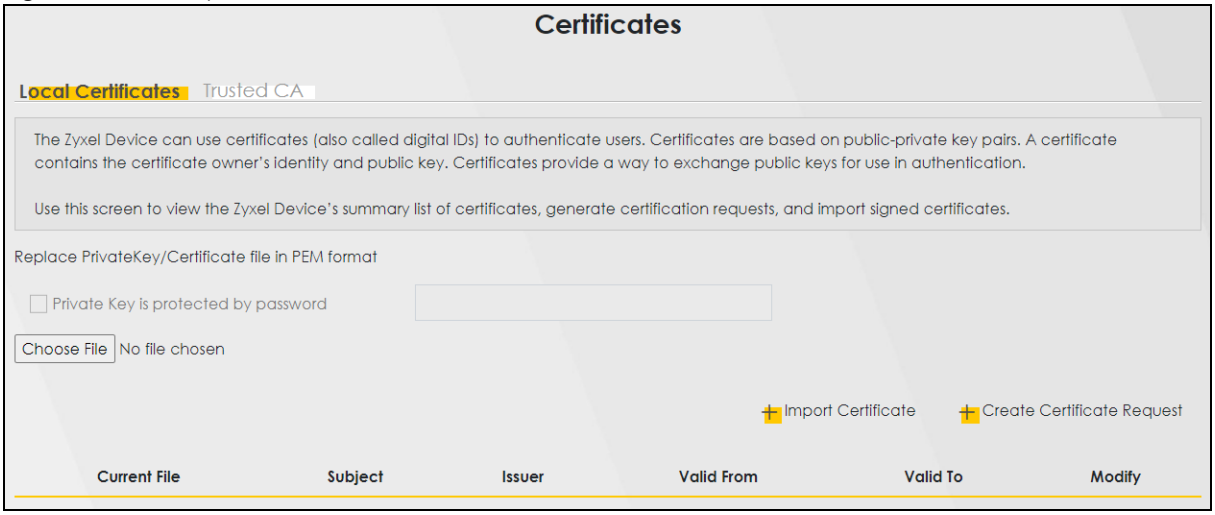
9.3 Local Certificates

Use this screen to view the WX Device's summary list of certificates, generate certification requests, and import signed certificates. You can import the following certificates to your WX Device:

- Web Server – This certificate secures HTTP connections.
- SSH – This certificate secures remote connections.

Click **Security** > **Certificates** to open the **Local Certificates** screen.

Figure 75 Security > Certificates > Local Certificates



The following table describes the labels in this screen.

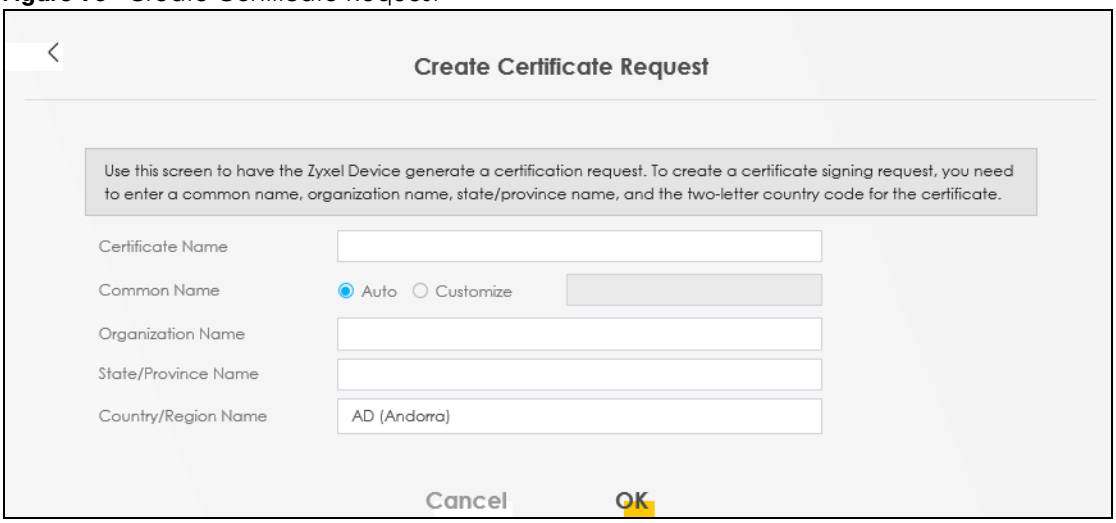
Table 29 Security > Certificates > Local Certificates

LABEL	DESCRIPTION
Replace Private Key/Certificate file in PEM format	
Private Key is protected by password	Select the check box and enter the private key into the text box to store it on the WX Device. The private key should not exceed 63 ASCII characters (not including spaces).
Choose File/ Browse	Click this button to find the certificate file you want to upload.
Import Certificate	Click this button to save the certificate that you have enrolled from a certification authority from your computer to the WX Device.
Create Certificate Request	Click this button to go to the screen where you can have the WX Device generate a certification request.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
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 a 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.
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.
Modify	Click the **View** icon to open a screen with an in-depth list of information about the certificate. For a certification request, click **Load Signed** to import the signed certificate. Click the **Remove** icon to remove the certificate (or certification request). A window displays asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.

9.3.1 Create Certificate Request

Click **Security** > **Certificates** > **Local Certificates** and then **Create Certificate Request** to open the following screen. Use this screen to have the WX Device generate a certification request. To create a certificate signing request, you need to enter a common name, organization name, state or province name, and the default US two-letter country code (The US country code is by default and not changeable when sold in the U.S.) for the certificate.

Figure 76 Create Certificate Request



The following table describes the labels in this screen.

Table 30 Create Certificate Request

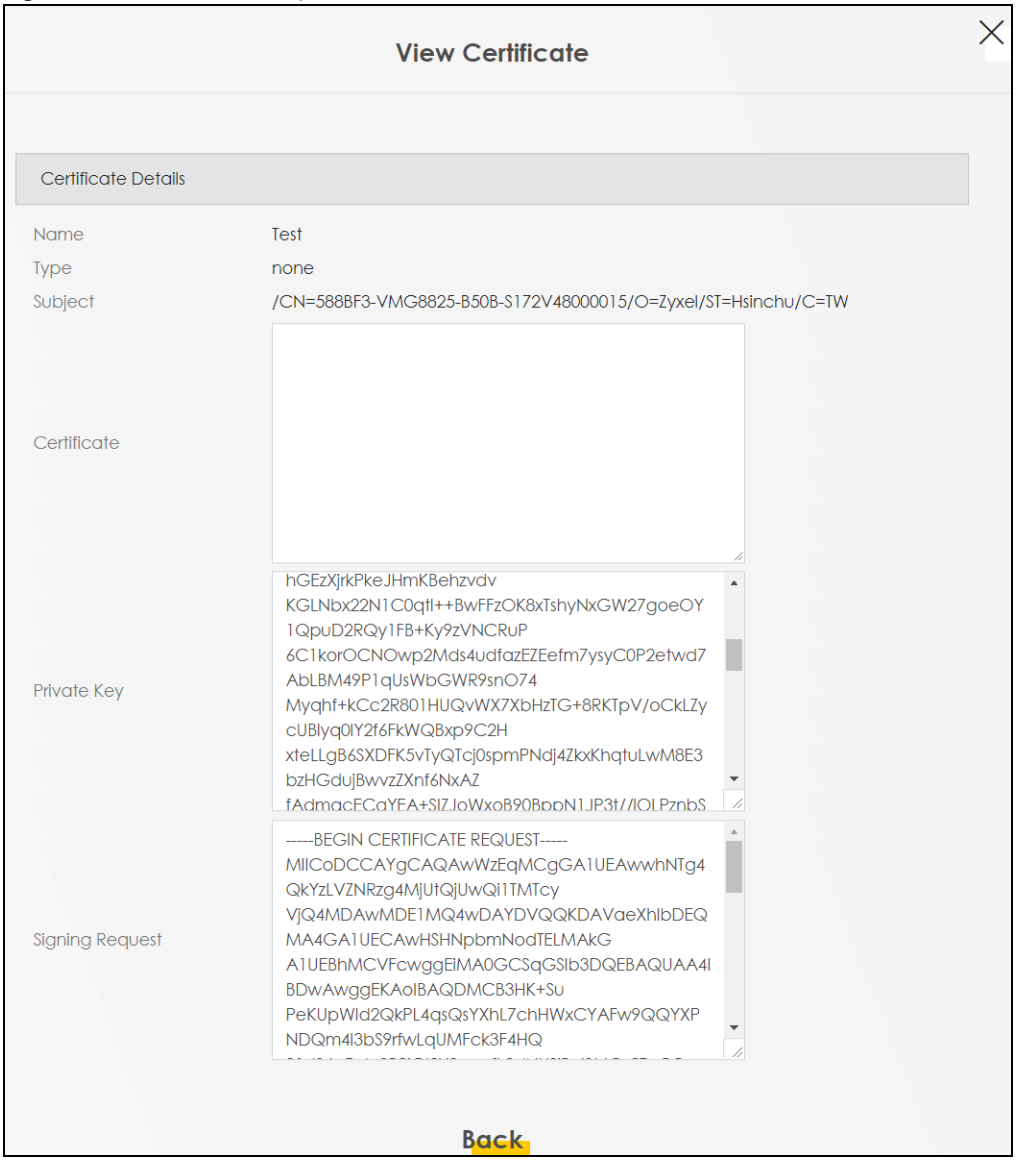
LABEL	DESCRIPTION
Certificate Name	Type up to 63 ASCII characters (not including spaces) to identify this certificate.
Common Name	Select **Auto** to have the WX Device configure this field automatically. Or select **Customize** to enter it manually. Type the IP address (in dotted decimal notation), domain name or email address in the field provided. The domain name or email address can be up to 63 ASCII characters. The domain name or email address is for identification purposes only and can be any string.
Organization Name	Type up to 63 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the WX Device drops trailing spaces.
State/Province Name	Type up to 32 characters to identify the state or province where the certificate owner is located. You may use any character, including spaces, but the WX Device drops trailing spaces.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

9.3.2 View Certificate Request

Use this screen to view in-depth information about the certificate request. The **Certificate** is used to verify the authenticity of the certification authority. The **Private Key** serves as your digital signature for authentication and must be safely stored. The **Signing Request** contains the certificate signing request value that you will copy upon submitting the certificate request to the CA (certificate authority).

Click the **View** icon in the **Local Certificates** screen to open the following screen.

Figure 77 Certificate Request: View



The following table describes the fields in this screen.

Table 31 Certificate Request: View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
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).

Table 31 Certificate Request: View (continued)

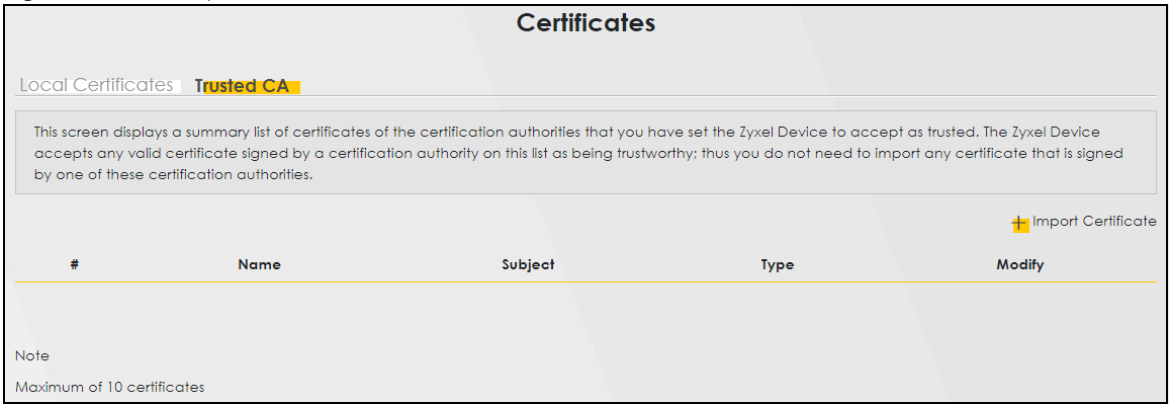
LABEL	DESCRIPTION
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form. You can copy and paste the certificate into an email to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution.
Private Key	This field displays the private key of this certificate.
Signing Request	This field displays the CSR (Certificate Signing Request) information of this certificate. The CSR will be provided to a certificate authority, and it includes information about the public key, organization name, domain name, location, and country of this certificate.
Back	Click **Back** to return to the previous screen.

9.4 Trusted CA

Click **Security** > **Certificates** > **Trusted CA** to open the following screen. This screen displays a summary list of certificates of the certification authorities that you have set the WX Device to accept as trusted. The WX Device accepts any valid certificate signed by a certification authority on this list as being trustworthy, which means you do not need to import any certificate that is signed by one of these certification authorities.

Note: A maximum of ten certificates can be added.

Figure 78 Security > Certificates > Trusted CA



The following table describes the labels in this screen.

Table 32 Security > Certificates > Trusted CA

LABEL	DESCRIPTION
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the WX Device.
#	This is the index number of the entry.
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have a unique subject information.

Table 32 Security > Certificates > Trusted CA (continued)

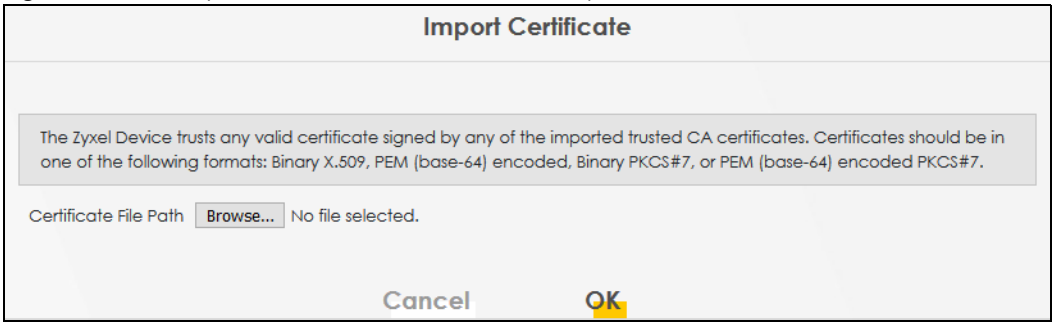
LABEL	DESCRIPTION
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Modify	Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the **Remove** icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

9.5 Import Trusted CA Certificate

Click **Import Certificate** in the **Trusted CA** screen to open the **Import Certificate** screen. The WX Device trusts any valid certificate signed by any of the imported trusted CA certificates. Certificates should be in one of the following formats: Binary X.509, PEM (base-64) encoded, Binary PKCS#7, or PEM (base-64) encoded PKCS#7.

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

Figure 79 Security > Certificates > Trusted CA > Import



The following table describes the labels in this screen.

Table 33 Security > Certificates > Trusted CA > Import

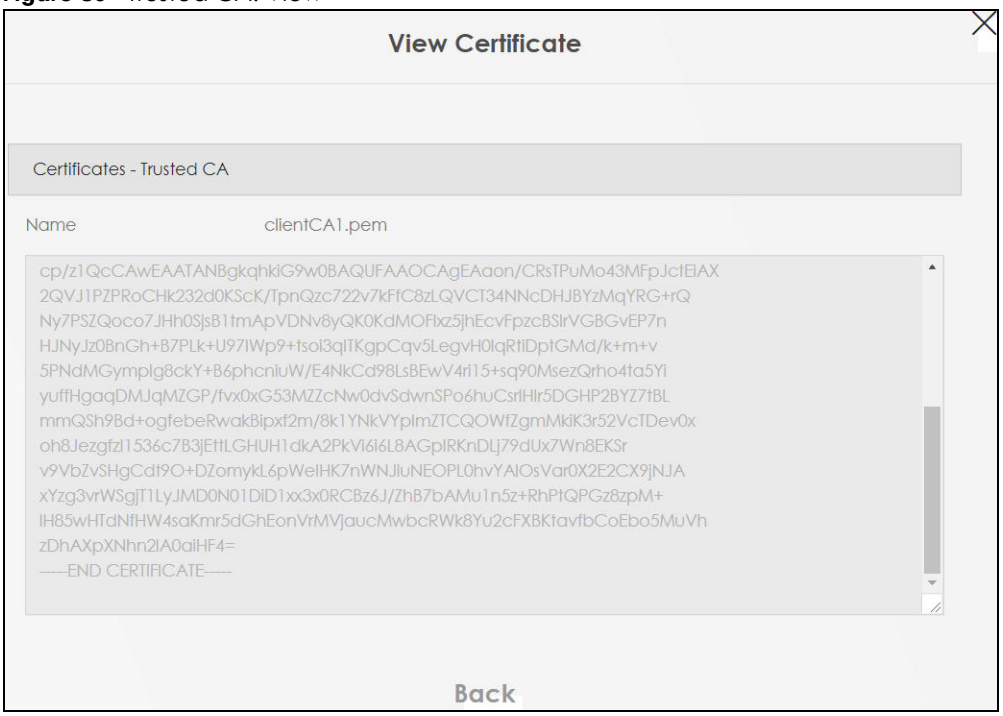
LABEL	DESCRIPTION
Certificate File Path	Type in the location of the file you want to upload in this field or click **Choose File**/**Browse** to find it.
Choose File/ Browse	Click this button to find the certificate file you want to upload.
OK	Click this to save the certificate on the WX Device.
Cancel	Click this to exit this screen without saving.

9.6 View Trusted CA Certificate

Use this screen to view in-depth information about the certification authority's certificate. The certificate text box is read-only and can be distributed to others.

Click **Security** > **Certificates** > **Trusted CA** to open the **Trusted CA** screen. Click the **View** icon to open the **View Certificate** screen.

Figure 80 Trusted CA: View



The following table describes the labels in this screen.

Table 34 Trusted CA: View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the 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 USB thumb drive for example).
Back	Click this to return to the previous screen.

9.7 Certificates Technical Reference

This section provides some technical background information about the topics covered in this chapter.

Certification Authorities

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities.

Public and Private Keys

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. Public-key encryption in general works as follows.

1. Tim wants to send a private message to Jenny. Tim generates a public-private key pair. What is encrypted with one key can only be decrypted using the other.
2. Tim keeps the private key and makes the public key openly available.
3. Tim uses his private key to encrypt the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to decrypt it.
5. Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The WX Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

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

Advantages of Certificates

Certificates offer the following benefits.

- The WX 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.

Certificate File Format

The certification authority certificate that you want to import has to be in PEM (Base-64) encoded X.509 file format. This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.

9.7.1 Verify a Certificate

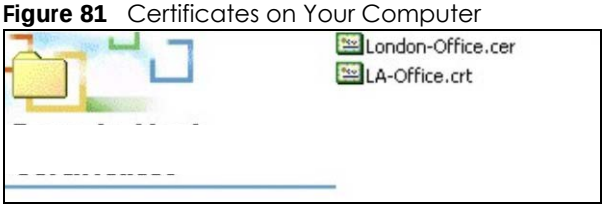
Before you import a trusted CA or trusted remote host certificate into the WX Device, you should verify that you have the actual certificate. This is especially true of trusted CA certificates since the WX Device also trusts any valid certificate signed by any of the imported trusted CA certificates.

You can use a certificate's fingerprint to verify it. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithms. 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.

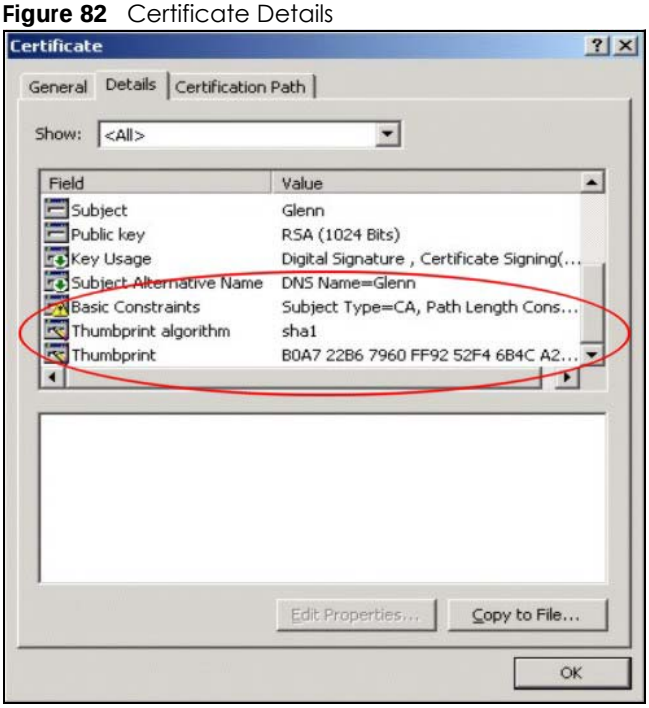
2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 81 Certificates on Your Computer



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

Figure 82 Certificate Details



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.

CHAPTER 10
Log

10.1 Log Overview

These screens allow you to determine the categories of events that the WX Device logs and then display these logs or have the WX Device send them to an administrator (through email) or to a syslog server.

10.1.1 What You Can Do in this Chapter

Use the **System Log** screen to see the system logs (Section 10.2 on page 145).

10.1.2 What You Need To Know

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

Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 35 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.

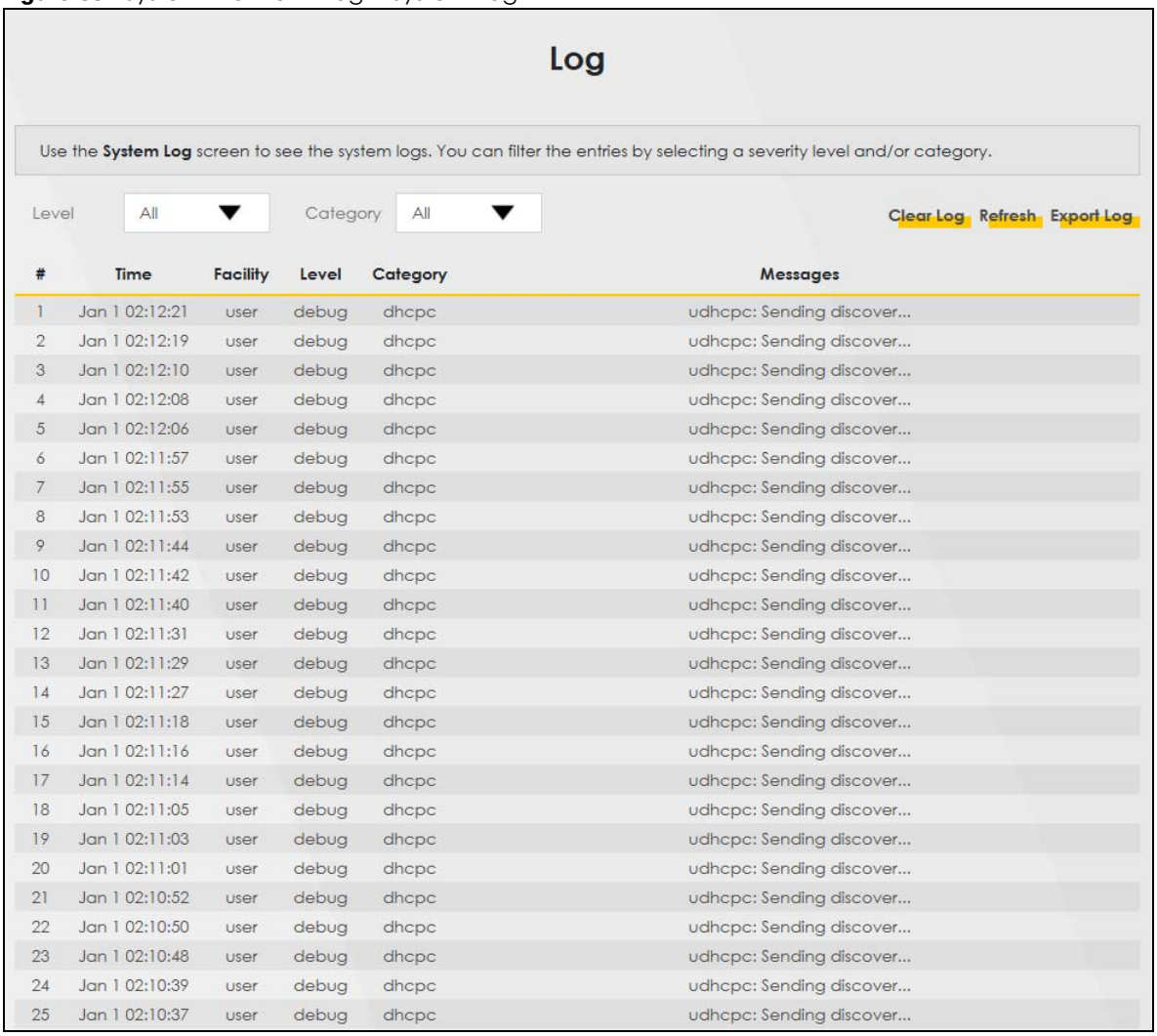
Table 35 Syslog Severity Levels (continued)

CODE	SEVERITY
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

10.2 System Log Settings

Use the **Log** screen to see the system logs. You can filter the entries by selecting a severity level and/or category. Click **System Monitor** > **Log** > **System Log** to open the **System Log** screen.

Figure 83 System Monitor > Log > System Log



The following table describes the fields in this screen.

Table 36 System Monitor > Log > System Log

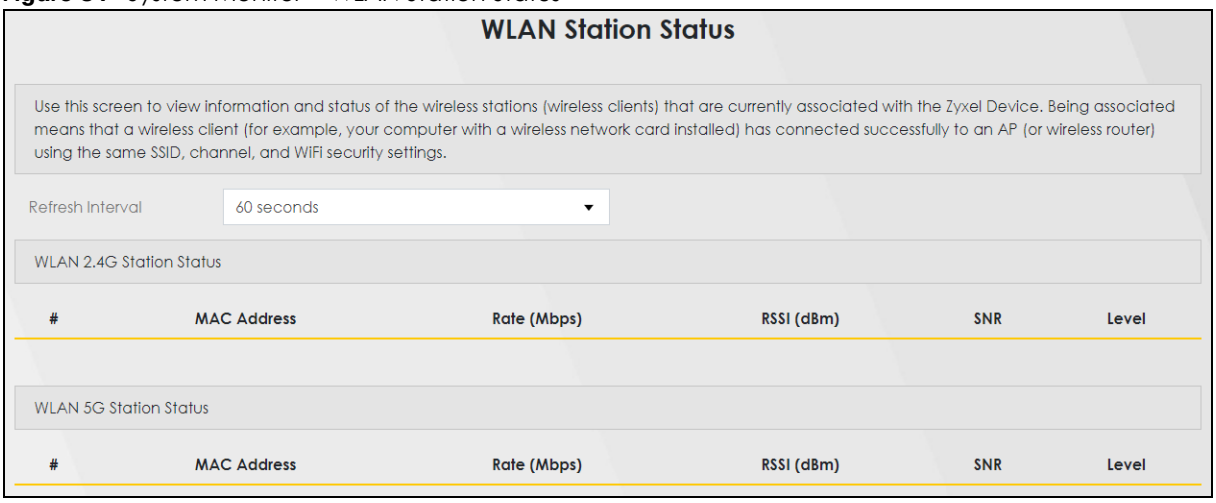
LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the WX Device searches through all logs of that severity or higher.
Category	Select the type of logs to display.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to save the current list of logs to your computer.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the log.
Category	This field displays the type of the log.
Messages	This field states the reason for the log.

CHAPTER 11
WLAN Station Status

11.1 WLAN Station Status Overview

Click **System Monitor** > **WLAN Station Status** to open the following screen. Use this screen to view information and status of the WiFi stations (WiFi clients) that are currently associated with the WX Device. Being associated means that a WiFi client (for example, your computer with a WiFi network card installed) has connected successfully to an AP (or WiFi router) using the same SSID, channel, and WiFi security settings.

Figure 84 System Monitor > WLAN Station Status



The following table describes the labels in this screen.

Table 37 System Monitor > WLAN Station Status

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the WX Device to update this screen.
#	This is the index number of an associated WiFi station.
MAC Address	This field displays the MAC address of an associated WiFi station.
Rate (Mbps)	This field displays the transmission rate of WiFi traffic between an associated WiFi station and the WX Device.
RSSI (dBm)	The RSSI (Received Signal Strength Indicator) field shows the WiFi signal strength of the station's WiFi connection. The normal range is –30 dBm to –79 dBm. If the value drops below –80 dBm, try moving the associated WiFi station closer to the WX Device to get better signal strength.

Table 37 System Monitor > WLAN Station Status (continued)

LABEL	DESCRIPTION
SNR	The Signal-to-Noise Ratio (SNR) is the ratio between the received signal power and the received noise power. The normal range is 15 to 40. If the value drops below 15, try moving the associated WiFi station closer to the WX Device to get better quality WiFi.
Level	This field displays a number which represents the strength of the WiFi signal between an associated WiFi station and the WX Device. The WX Device uses the RSSI and SNR values to determine the strength of the WiFi signal. **5** means the WX Device is receiving an excellent WiFi signal. **4** means the WX Device is receiving a very good WiFi signal. **3** means the WX Device is receiving a weak WiFi signal. **2** means the WX Device is receiving a very weak WiFi signal. **1** means the WX Device is not receiving a WiFi signal.

CHAPTER 12
System

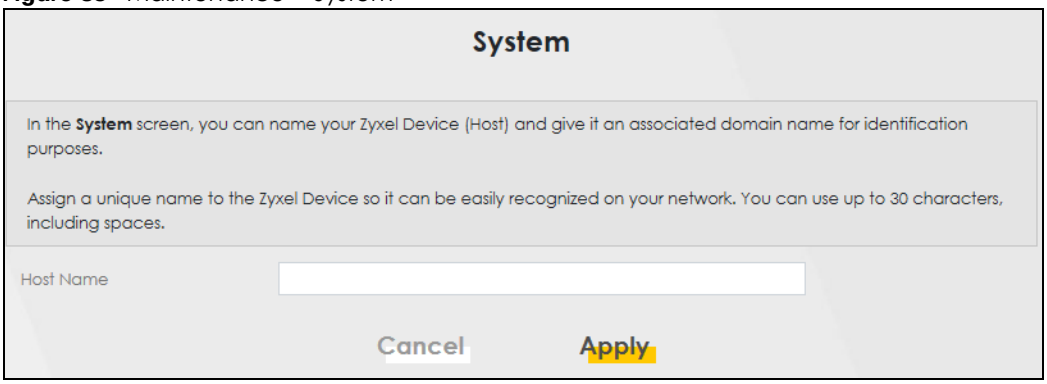
12.1 System Overview

In the **System** screen, you can name your WX Device (Host) and give it an associated domain name. Domain is the name given to a network. It will be required to reach a network from an external point (like the Internet). Knowing the domain name will allow you to reach a particular network, and knowing the host name will allow you to reach a particular device. For this reason, accessing a device from another device within a network may work with just the host name (without the use of the domain name).

12.2 System Settings

Click **Maintenance** > **System** to open the following screen. Assign a unique name to the WX Device so it can be easily recognized on your network. You can use up to 30 characters, including spaces.

Figure 85 Maintenance > System



The following table describes the labels in this screen.

Table 38 Maintenance > System

LABEL	DESCRIPTION
Host Name	Type a host name for your WX Device. Enter a descriptive name of up to 30 alphanumeric characters, not including spaces, underscores, and dashes.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

CHAPTER 13
User Account

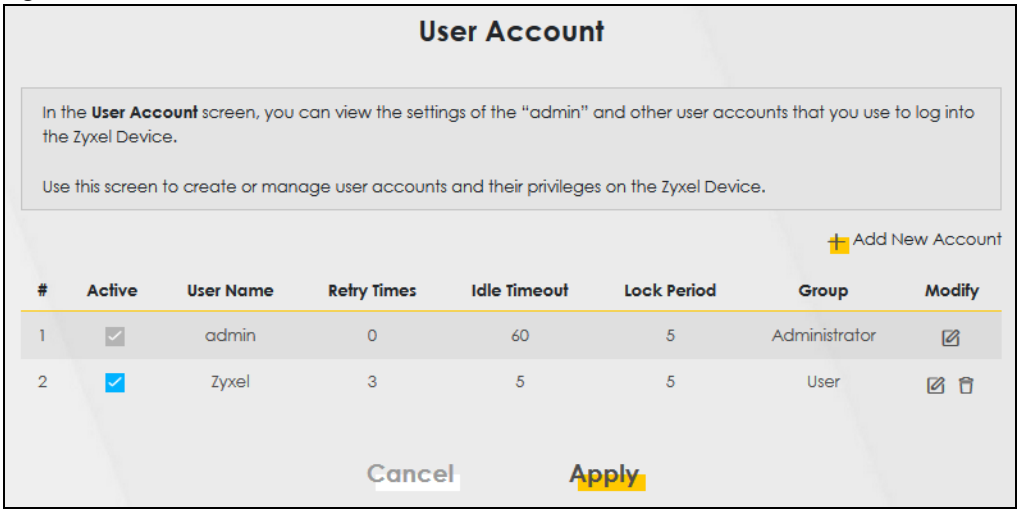
13.1 User Account Overview

In the **User Account** screen, you can view the settings of the 'admin' and other user accounts that you use to log into the WX Device to manage it.

13.2 User Account Settings

Click **Maintenance** > **User Account** to open the following screen. Use this screen to create or manage user accounts and their privileges on the WX Device.

Figure 86 Maintenance > User Account



The following table describes the labels in this screen.

Table 39 Maintenance > User Account

LABEL	DESCRIPTION
Add New Account	Click this button to add a new user account.
#	This is the index number of the user account.
Active	This field indicates whether the user account is active or not. Clear the check box to disable the user account. Select the check box to enable it.
User Name	This field displays the name of the account used to log into the WX Device Web Configurator.
Retry Times	This field displays the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.

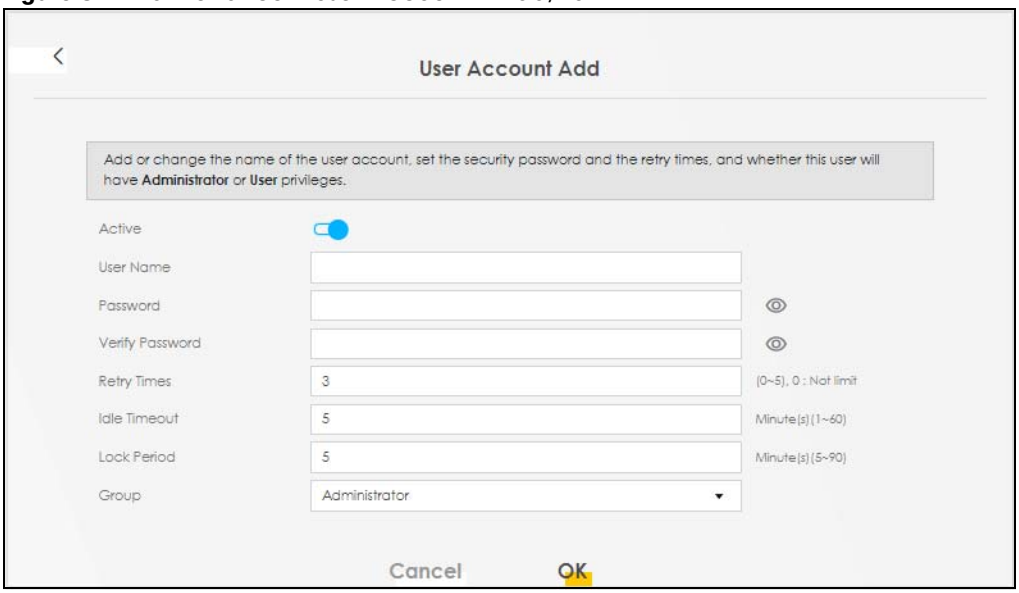
Table 39 Maintenance > User Account (continued)

LABEL	DESCRIPTION
Idle Timeout	This field displays the length of inactive time before the WX Device will automatically log the user out of the Web Configurator.
Lock Period	This field displays the length of time a user must wait before attempting to log in again after a number if consecutive wrong passwords have been entered as defined in **Retry Times**.
Group	This field displays whether this user has **Administrator** or **User** privileges.
Modify	Click the **Edit** icon to configure the entry. Click the **Delete** icon to remove the entry.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

13.2.1 User Account Add/Edit

Click **Add New Account** or the **Edit** icon of an existing account in the **Maintenance** > **User Account** to open the following screen.

Figure 87 Maintenance > User Account > Add/Edit



The following table describes the labels in this screen.

Table 40 Maintenance > User Account > Add/Edit

LABEL	DESCRIPTION
Active	Select **Enable** or **Disable** to activate or deactivate the user account.
User Name	Enter a new name for the account. The **User Name** must contain 1 to 15 characters, including 0 to 9, a to z, and !@#%*()-_+=~,.{}[]\. Spaces are not allowed.
Password	Type your new system password. The **Password** must contain 6 to 64 characters, including 0 to 9 and a to z. Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the WX Device.
Verify Password	Type the new password again for confirmation.
Retry Times	Enter the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.

Table 40 Maintenance > User Account > Add/Edit (continued)

LABEL	DESCRIPTION
Idle Timeout	Enter the length of inactive time before the WX Device will automatically log the user out of the Web Configurator.
Lock Period	Enter the length of time a user must wait before attempting to log in again after a number if consecutive wrong passwords have been entered as defined in **Retry Times**.
Group	Specify whether this user will have **Administrator** or **User** privileges. **Administrator** and **User** privileges are mostly the same, but the following menu items will only display when you log in as an **Administrator**. • **Network Setting** • **Security Settings** • **Maintenance** > **System**
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

CHAPTER 14
Remote Management

14.1 Remote Management Overview

Use remote management to control what services you can use through which interface(s) in order to manage the WX Device.

14.1.1 What You Can Do in this Chapter

Use the **Remote Management** screen to allow various approaches to access the WX Device remotely from a LAN connection (Section 14.2 on page 153).

Note: The WX Device is managed using the Web Configurator.

14.2 Management Services

Use this screen to configure through which interface(s), each service can access the WX Device. You can also specify service port numbers computers must use to connect to the WX Device. Click **Maintenance** > **Remote Management** > **Remote Management** to open the following screen.

Figure 88 Maintenance > Remote Management > Remote Management (WX3401-B0/WX3100-T0)

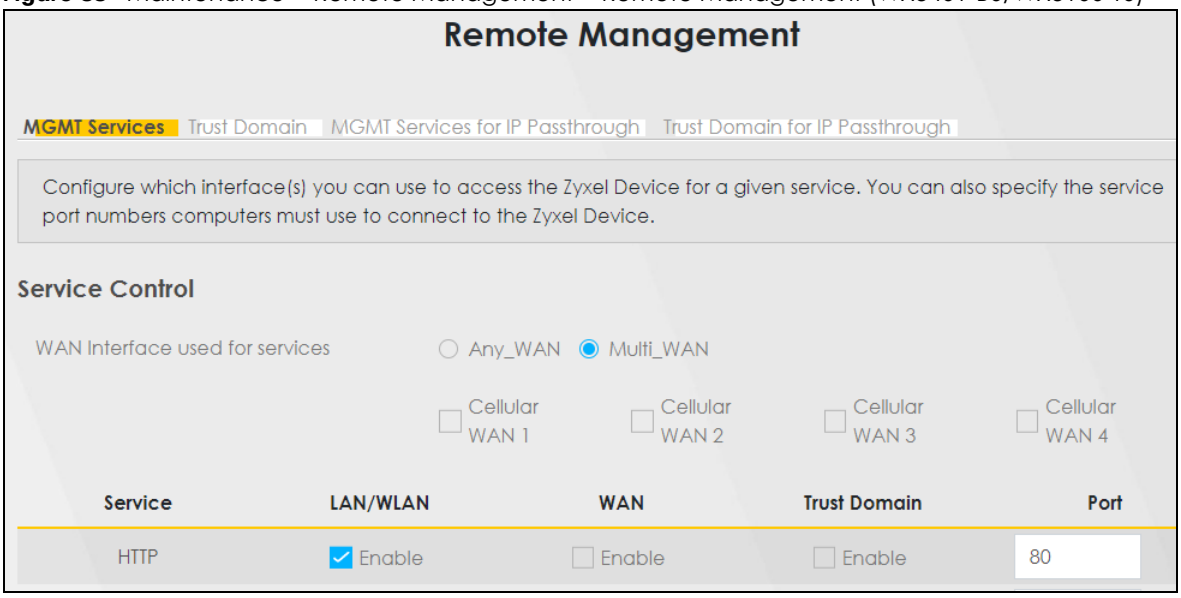
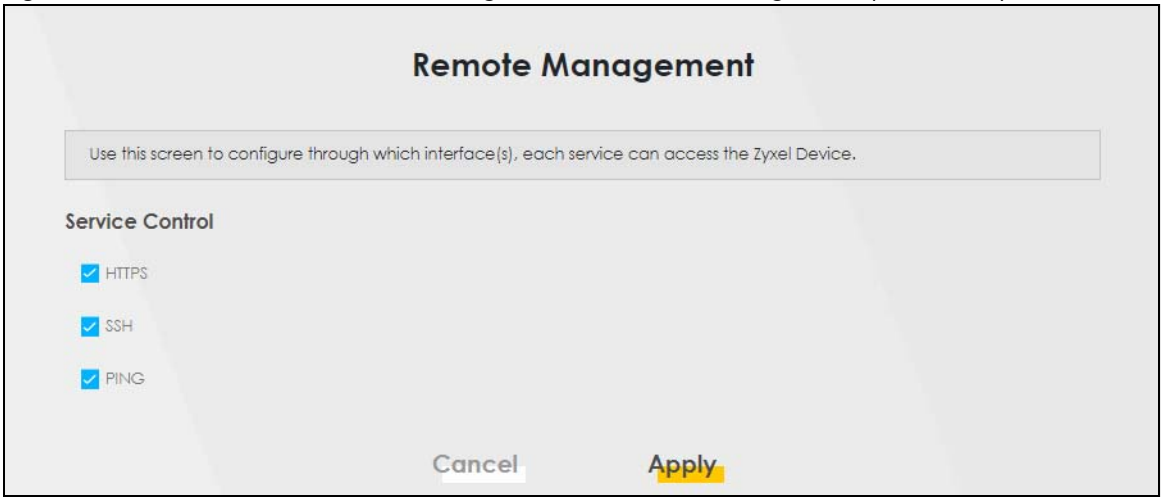


Figure 89 Maintenance > Remote Management > Remote Management (WX5600-T0)



The following table describes the fields in this screen.

Table 41 Maintenance > Remote Management > Remote Management

LABEL	DESCRIPTION
Service Control	This is the service list you may use to access the WX Device. • **HTTP** provides a non secured way. • **HTTPS** is the secured version of HTTP, it makes sure that your data cannot be read during transmission. • **TELNET** provides a way to control your WX Device remotely. • **SSH** prevents leakage of data during remote management. Additionally, it can encrypt all transmitted data. • **PING** is a diagnostic tool that can check if your WX Device is connected to the Internet.
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes back to the WX Device.

CHAPTER 15
Time Settings

15.1 Time Settings Overview

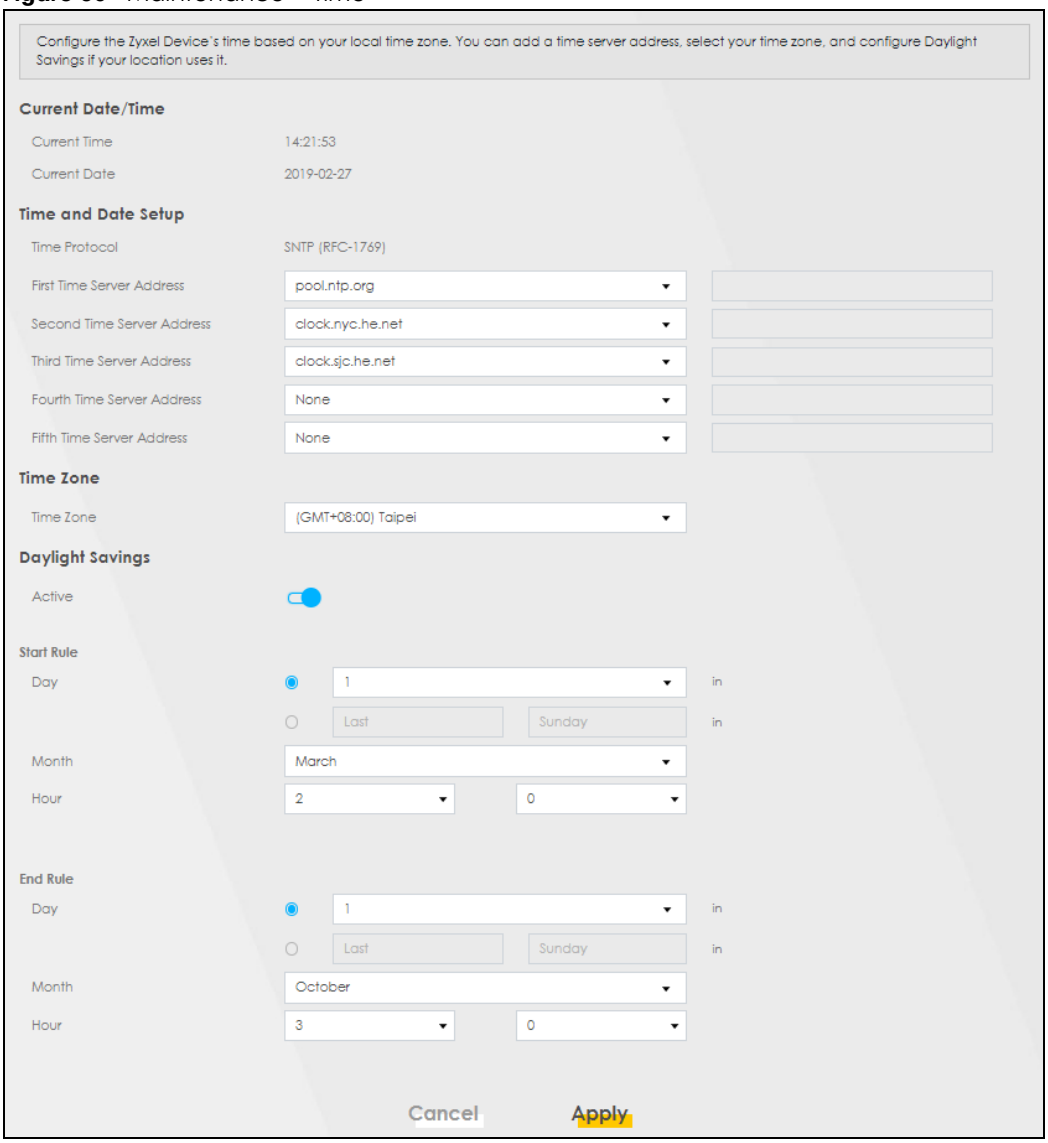
This chapter shows you how to configure the WX Device's system date and time.

15.2 Time

For effective scheduling and logging, the WX Device's system time must be accurate. Use this screen to configure the WX Device's time based on your local time zone. You can enter a time server address, select the time zone where the WX Device is physically located, and configure Daylight Savings settings if needed.

Click **Maintenance** > **Time** to open the following screen.

Figure 90 Maintenance > Time



The following table describes the fields in this screen.

Table 42 Maintenance > Time

LABEL	DESCRIPTION
Current Date/Time	
Current Time	This field displays the time of your WX Device. Each time you reload this page, the WX Device synchronizes the time with the time server.
Current Date	This field displays the date of your WX Device. Each time you reload this page, the WX Device synchronizes the date with the time server.
Time and Date Setup	

Table 42 Maintenance > Time (continued)

LABEL	DESCRIPTION
First – Fifth Time Server Address	Select an NTP time server from the drop-down list box. Otherwise, select **Other** and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server. Select **None** if you do not want to configure the time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Active	Click this switch to enable or disable Daylight Saving Time. When the switch goes to the right  , the function is enabled. Otherwise, it is not.
Start Rule	Configure the day and time when Daylight Saving Time starts if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The **Hour** 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, set the day to **Second**, **Sunday**, the month to **March** and the time to **2** in the **Hour** 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 set the day to **Last**, **Sunday** and the month to **March**. The time you select in the **o'clock** field depends on your time zone. In Germany for instance, you would select **2** in the **Hour** field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Rule	Configure the day and time when Daylight Saving Time ends if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The **Hour** 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 set the day to **First**, **Sunday**, the month to **November** and the time to **2** in the **Hour** 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 set the day to **Last**, **Sunday**, and the month to **October**. The time you select in the **o'clock** field depends on your time zone. In Germany for instance, you would select **2** in the **Hour** field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Cancel	Click **Cancel** to restore the default or previously saved settings.
Apply	Click **Apply** to save your changes.

CHAPTER 16
Email Notification

16.1 Email Notification Overview

A mail server is an application or a computer that can receive, forward and deliver email messages.

To have the WX Device send reports, logs or notifications through email, you must specify an email server and the email addresses of the sender and receiver.

16.2 Email Notification

Use this screen to view, remove and add email account information on the WX Device. This account can be set to send email notifications for logs.

Click **Maintenance** > **E-mail Notification** to open the **E-mail Notification** screen.

Note: The default port number of the mail server is 25.

Figure 91 Maintenance > E-mail Notification

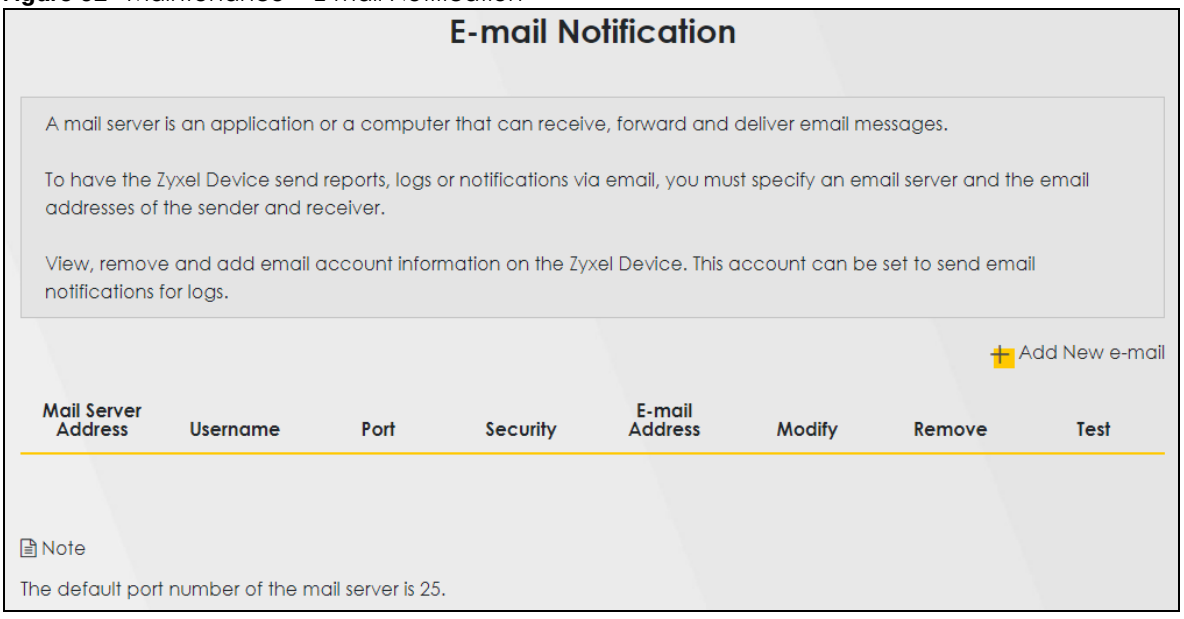
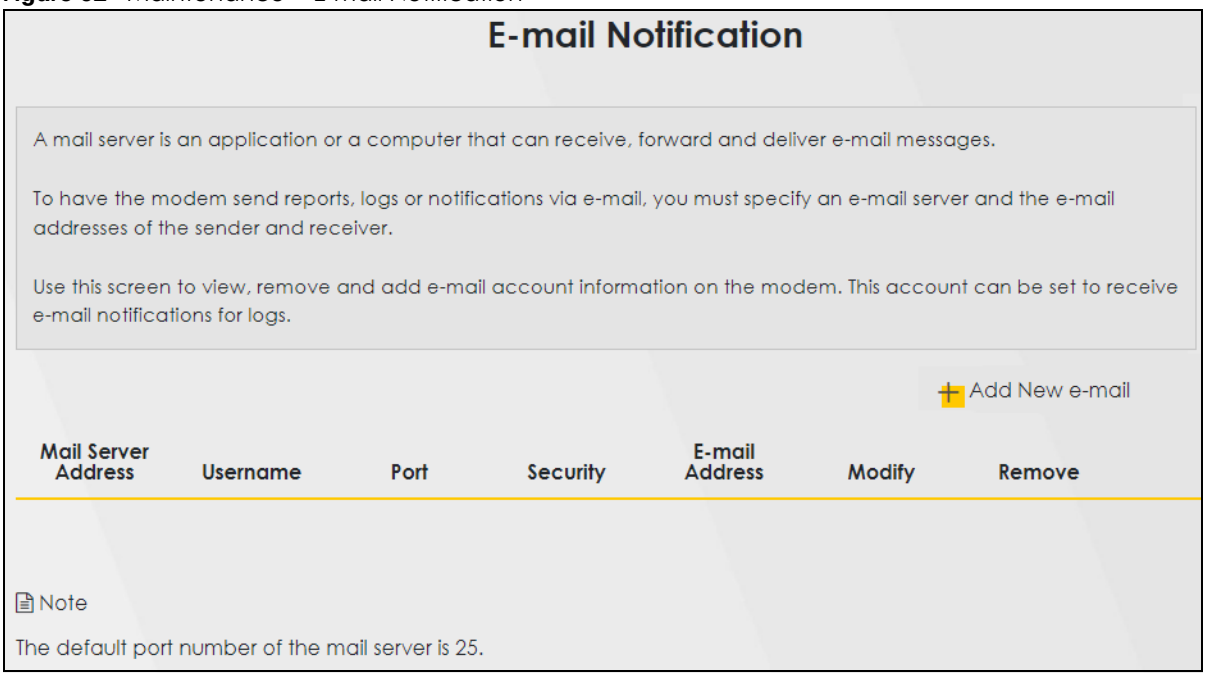


Figure 92 Maintenance > E-mail Notification



The following table describes the labels in this screen.

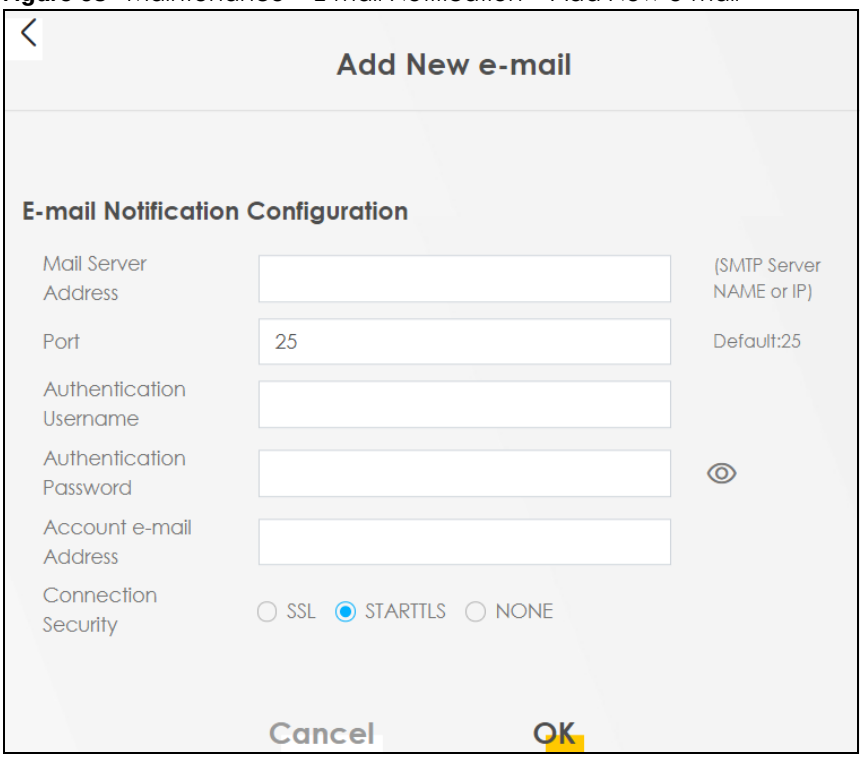
Table 43 Maintenance > E-mail Notification

LABEL	DESCRIPTION
Add New e-mail	Click this button to create a new entry (up to 32 can be created).
Mail Server Address	This displays the server name or the IP address of the mail server.
Username	This displays the user name of the sender's mail account.
Port	This field displays the port number of the mail server.
Security	This field displays the protocol used for encryption.
E-mail Address	This field displays the email address that you want to be in the from or sender line of the email that the WX Device sends.
Modify	Click the **Edit** icon to configure the entry. Click the **Delete** icon to remove the entry.
Remove	Click this button to delete the selected entries.
Test	Click this to send a test email to the configured email address.

16.2.1 Add New e-mail

Click the **Add New e-mail** button in the **E-mail Notification** screen. Use this screen to configure the required information for sending email through a mail server.

Figure 93 Maintenance > E-mail Notification > Add New e-mail



The following table describes the labels in this screen.

Table 44 Maintenance > E-mail Notification > Add New e-mail

LABEL	DESCRIPTION
Mail Server Address	Enter the server name or the IP address of the mail server for the e-mail address specified in the **Account e-mail Address** field. If this field is left blank, reports, logs or notifications will not be sent through e-mail.
Port	Enter the same port number here as is on the mail server for mail traffic.
Authentication Username	Enter the user name. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed. This is usually the user name of a mail account you specified in the **Account e-mail Address** field.
Authentication Password	Enter the password associated with the user name above.
Account e-mail Address	Enter the email address that you want to be in the from or sender line of the email notification that the WX Device sends. If you activate SSL/TLS authentication, the email address must be able to be authenticated by the mail server as well.
Connection Security	Select **SSL** to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) if you want encrypted communications between the mail server and the WX Device. Select **STARTTLS** to upgrade a plain text connection to a secure connection using SSL/TLS. Select **NONE** to disable the connection security.
Cancel	Click this button to begin configuring this screen afresh.
OK	Click this button to save your changes and return to the previous screen.

CHAPTER 17
Log Setting

17.1 Log Setting Overview

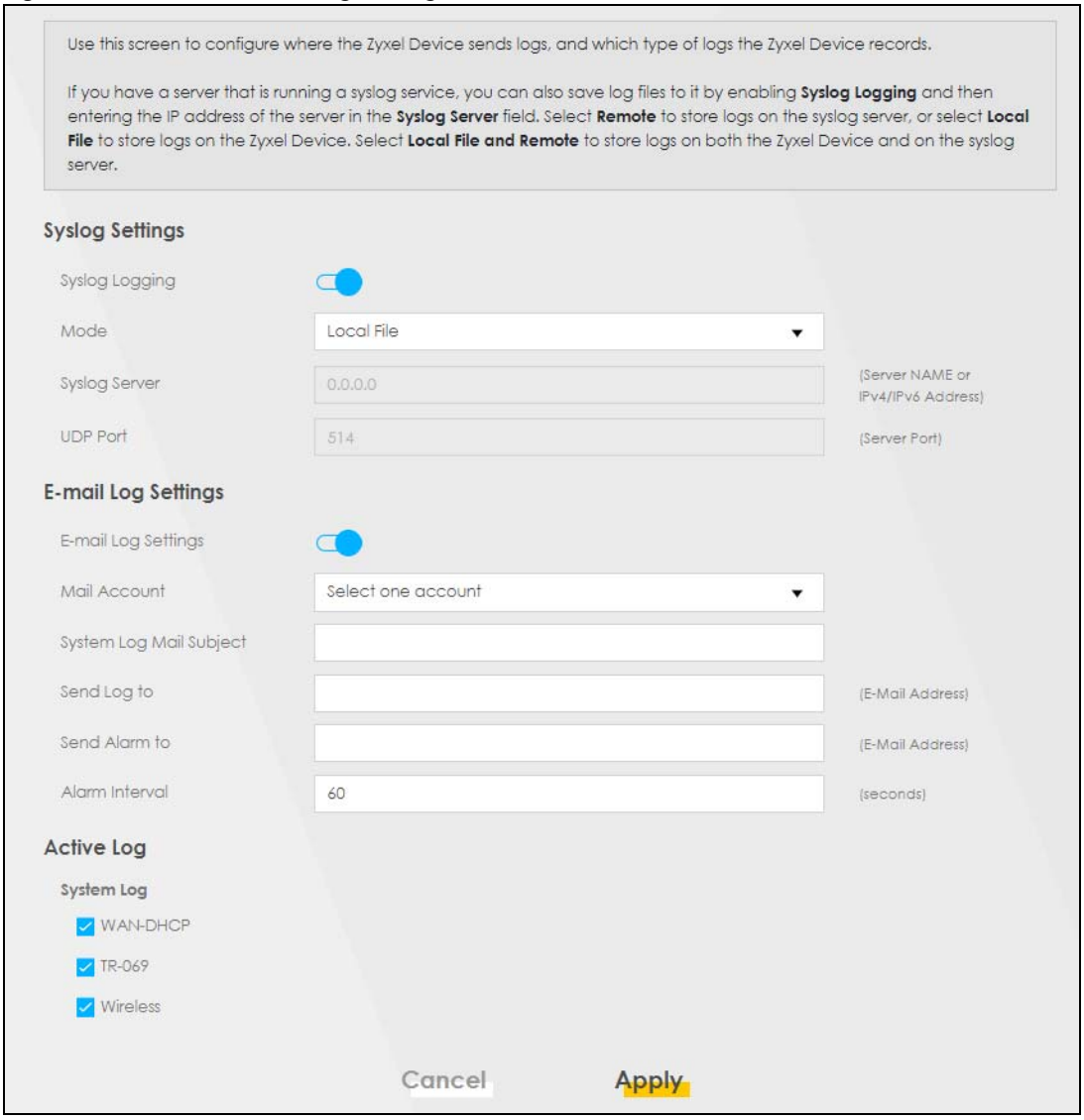
You can configure where the WX Device sends logs and which type of logs the WX Device records in the **Logs Setting** screen.

17.2 Log Setting

Use this screen to configure where the WX Device sends logs, and which type of logs the WX Device records.

If you have a server that is running a syslog service, you can also save log files to it by enabling **Syslog Logging**, and then entering the IP address of the server in the **Syslog Server** field. Select **Remote** to store logs on the syslog server, or select **Local File** to store logs on the WX Device. Select **Local File and Remote** to store logs on both the WX Device and the syslog server. To change your WX Device's log settings, click **Maintenance** > **Log Setting**. The screen appears as shown.

Figure 94 Maintenance > Log Setting



The following table describes the fields in this screen.

Table 45 Maintenance > Log Setting

LABEL	DESCRIPTION
Syslog Settings	
Syslog Logging	Slide the switch to the right to enable syslog logging.
Mode	Select **Remote** to have the WX Device send it to an external syslog server. Select **Local File** to have the WX Device save the log file on the WX Device itself. Select **Local File and Remote** to have the WX Device save the log file on the WX Device itself and send it to an external syslog server. Note: A warning appears upon selecting **Remote** or **Local File and Remote**. Just click **OK** to continue.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.

Table 45 Maintenance > Log Setting (continued)

LABEL	DESCRIPTION
UDP Port	Enter the port number used by the syslog server.
Enable Syslog over TLS	Use **Syslog over TLS** to securely send logs from the WX Device to the syslog server using TLS encryption. On the WX Device, first generate a certificate for syslog authentication of the WX Device. The CN (Certificate Name) must match the IP address of the WX Device's interface to the syslog server. Go to **Certificates** > **Local CA** and import a certificate for syslog authentication. This is required.
Local Certificate Used by Syslog Client	Optionally, the Syslog server may also request a certificate from the WX Device for mutual authentication. Go to **Certificates** > **Local Certificate** and import a WX Device certificate that the syslog server can use to verify the WX Device.
E-mail Log Settings	
E-mail Log Settings	Slide the switch to the right to allow the sending through email the system and security logs to the email address specified in **Send Log to**. Note: Make sure that the **Mail Server Address** field is not left blank in the **Maintenance** > **E-mail Notifications** screen.
Mail Account	Select a server specified in **Maintenance** > **E-mail Notifications** to send the logs to.
System Log Mail Subject	This field allows you to enter a descriptive name for the system log email (for example Zyxel System Log). Up to 127 printable characters are allowed for the **System Log Mail Subject** including special characters inside the square brackets [!#%()*+,–./:=?@[]\{}~].
Security Log Mail Subject	This field allows you to enter a descriptive name for the security log email (for example Zyxel Security Log). Up to 127 printable characters are allowed for the **Security Log Mail Subject** including special characters inside the square brackets [!#%()*+,–./:=?@[]\{}~].
Send Log to	This field allows you to enter the log's designated email recipient. The log's format is plain text file sent as an email attachment.
Send Alarm to	This field allows you to enter the alarm's designated e-mail recipient. The alarm's format is plain text file sent as an email attachment.
Alarm Interval	Select the frequency of showing of the alarm.
Active Log	
Syslog Debug Logging	Slide the switch to the right to enable syslog debug logging.
System Log	Select the categories of **System Log**s that you want to record.
Security Log	Select the categories of **Security Log**s that you want to record.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

17.2.1 Example Email Log

An 'End of Log' message displays for each mail in which a complete log has been sent. The following is an example of a log sent by email.

- You may edit the subject title.
- The date format here is Day-Month-Year.
- The date format here is Month-Day-Year. The time format is Hour-Minute-Second.
- '`End of Log`' message shows that a complete log has been sent.

Figure 95 Email Log Example

```
Subject:
        Firewall Alert From
   Date:
        Fri, 07 Apr 2000 10:05:42
   From:
        user@zyxel.com
     To:
        user@zyxel.com
  1|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |default policy  |forward
   | 09:54:03 |UDP     src port:00520 dest port:00520  |<1,00>          |
  2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |default policy  |forward
   | 09:54:17 |UDP     src port:00520 dest port:00520  |<1,00>          |
  3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10     |match           |forward
   | 09:54:19 |UDP     src port:03516 dest port:00053  |<1,01>          |
……..{snip}……..
……..{snip}……..
126|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:00 |UDP     src port:00520 dest port:00520  |<1,02>          |
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |match           |forward
   | 10:05:17 |UDP     src port:00520 dest port:00520  |<1,02>          |
128|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:30 |UDP     src port:00520 dest port:00520  |<1,02>          |

End of Firewall Log
```

CHAPTER 18
Firmware Upgrade

18.1 Firmware Upgrade Overview

This screen lets you upload new firmware to your WX Device. You can download new firmware releases from your nearest Zyxel FTP site (or www.zyxel.com) to upgrade your device's performance.

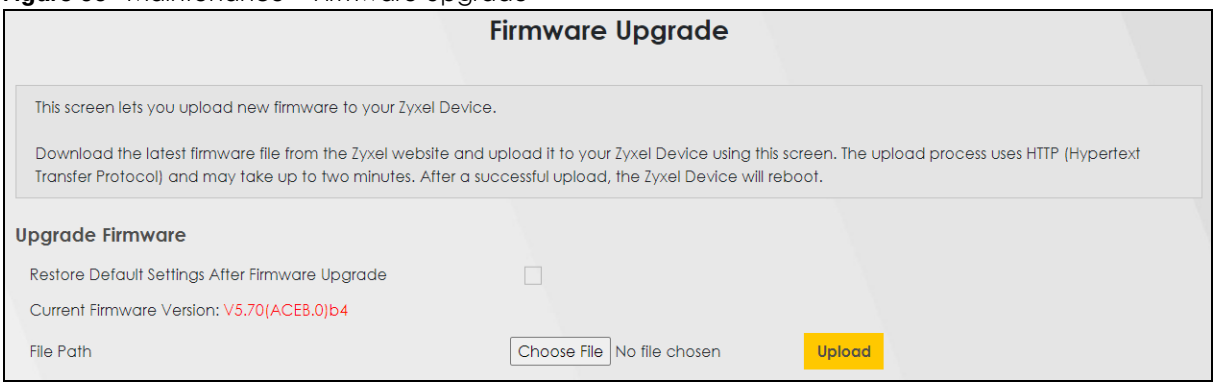
Only use firmware for your device's specific model. Refer to the label on the bottom of your WX Device.

18.2 Firmware Upgrade Settings

Click **Maintenance** > **Firmware Upgrade** to open the following screen. Download the latest firmware file from the Zyxel website and upload it to your WX Device using this screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to 2 minutes. After a successful upload, the WX Device will reboot.

Do NOT turn off the WX Device while firmware upload is in progress!

Figure 96 Maintenance > Firmware Upgrade



The following table describes the labels in this screen. After you see the firmware updating screen, wait two minutes before logging into the WX Device again.

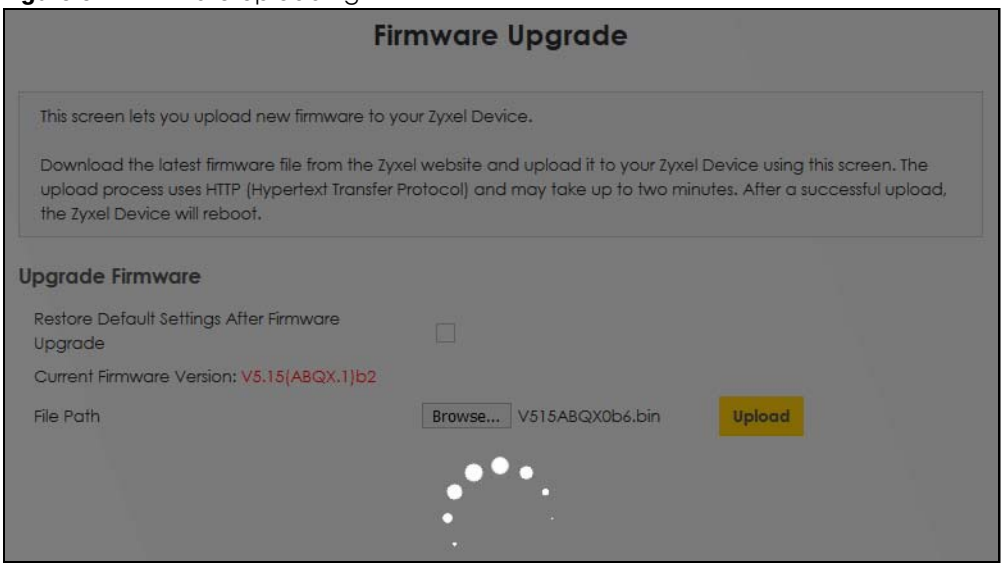
Table 46 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	
Restore Default Settings After Firmware Upgrade	Select the check box to have the WX Device automatically reset itself after the new firmware is uploaded.

Table 46 Maintenance > Firmware Upgrade (continued)

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

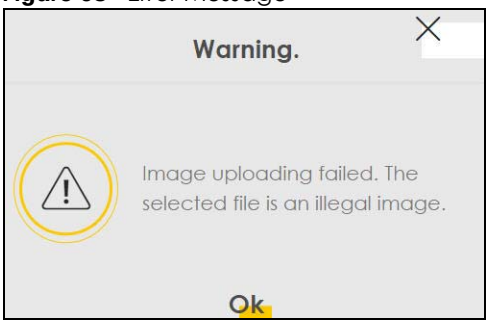
Figure 97 Firmware Uploading



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

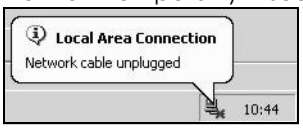
If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Firmware Upgrade** screen.

Figure 98 Error Message



Note that the WX Device automatically restarts during the upload, causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Network Temporarily Disconnected



CHAPTER 19
Backup/Restore

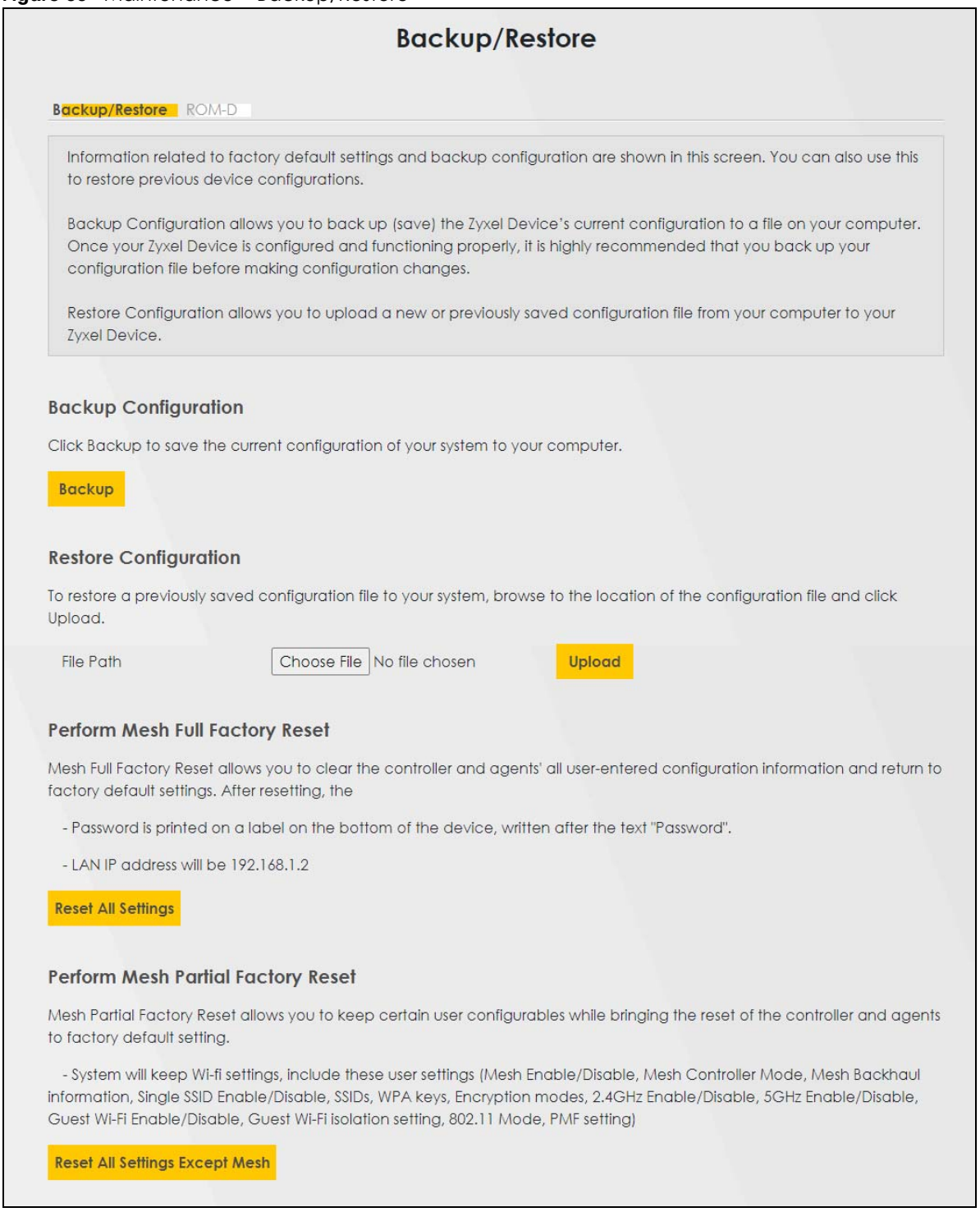
19.1 Backup/Restore Overview

The **Backup/Restore** screen allows you to backup and restore device configurations. You can also reset your device settings back to the factory default.

19.2 Backup/Restore Settings

Click **Maintenance** > **Backup/Restore**. Information related to factory default settings, backup configuration and restoring configuration appears in this screen.

Figure 99 Maintenance > Backup/Restore



Backup Configuration

Backup Configuration allows you to back up (save) the WX Device's current configuration to a file on your computer. Once your WX Device is configured and functioning properly, it is highly recommended

that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the WX Device's current configuration to your computer.

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your WX Device.

Table 47 Maintenance > Backup/Restore: Restore Configuration

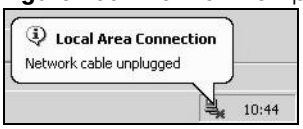
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Choose File** / **Browse** to find it.
Choose File / Browse	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload process.

Do NOT turn off the WX Device while configuration file upload is in progress.

After the WX Device configuration has been restored successfully, the login screen appears. Login again to restart the WX Device.

The WX Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

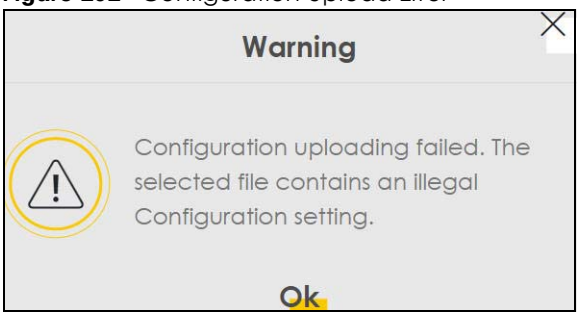
Figure 100 Network Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default WX Device IP address (192.168.1.2).

If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Backup/Restore** screen.

Figure 101 Configuration Upload Error

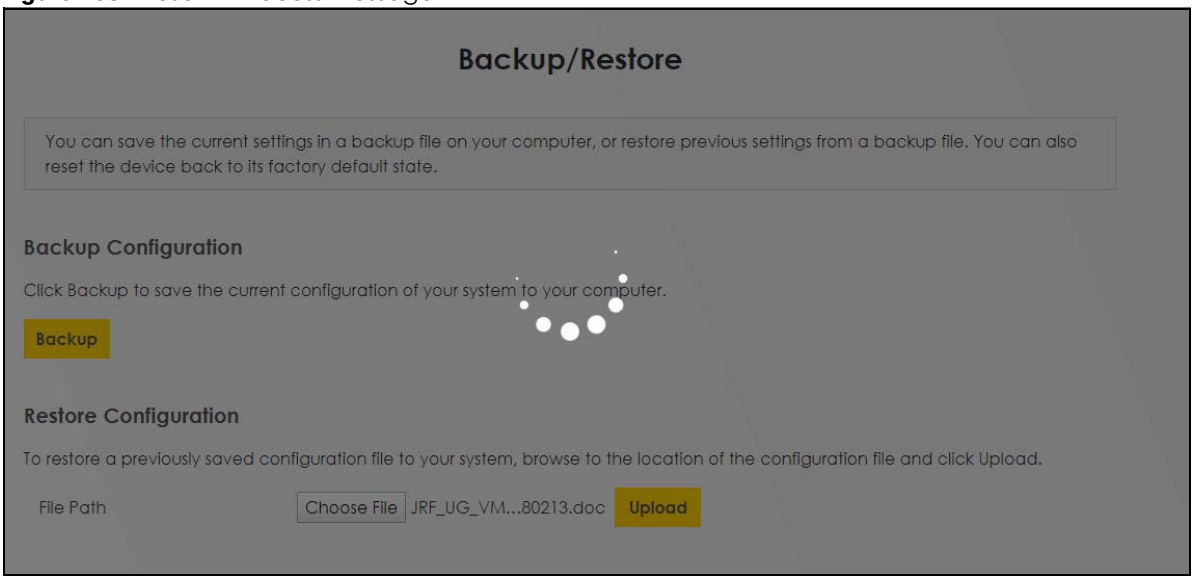


Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the WX Device to its factory defaults. The following warning screen appears.

Figure 102 Reset Warning Message

Figure 103 Reset In Process Message



You can also press the **RESET** button on the rear panel to reset the factory defaults of your WX Device. Refer to Section 2.6 on page 26 for more information on the **RESET** button.

Perform Partial Factory Reset

Click the **Reset All Settings Except Mesh** button to clear all user-entered configuration information and return the WX Device to its factory defaults except for Mesh WiFi settings. The following warning screen appears.

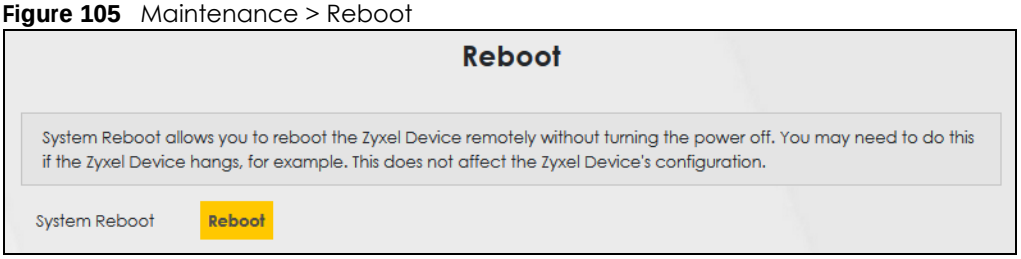
Figure 104 Reset Warning Message

19.3 Reboot

System Reboot allows you to reboot the WX Device remotely without turning the power off. You may need to do this if the WX Device hangs, for example.

Click **Maintenance** > **Reboot**. Click **Reboot** to have the WX Device reboot. This does not affect the WX Device's configuration.

Figure 105 Maintenance > Reboot



Chapter 20
Diagnostic

20.1 Diagnostic Overview

The **Diagnostic** screens display information to help you identify problems with the WX Device.

The route between a Central Office Very-high-bit-rate Digital Subscriber Line (CO VDSL) switch and one of its Customer-Premises Equipment (CPE) may go through switches owned by independent organizations. A connectivity fault point generally takes time to discover and impacts subscriber's network access. In order to eliminate the management and maintenance efforts, IEEE 802.1ag is a Connectivity Fault Management (CFM) specification which allows network administrators to identify and manage connection faults. Through discovery and verification of the path, CFM can detect, analyze and isolate connectivity faults in bridged LANs.

20.1.1 What You Can Do in this Chapter

The **Diagnostic** screen lets you ping an IP address or trace the route packets take to a host (Section 20.3 on page 173).

20.2 What You Need to Know

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

How CFM Works

A Maintenance Association (MA) defines a VLAN and associated Maintenance End Point (MEP) ports on the device under a Maintenance Domain (MD) level. An MEP port has the ability to send Connectivity Check Messages (CCMs) and get other MEP ports information from neighbor devices' CCMs within an MA.

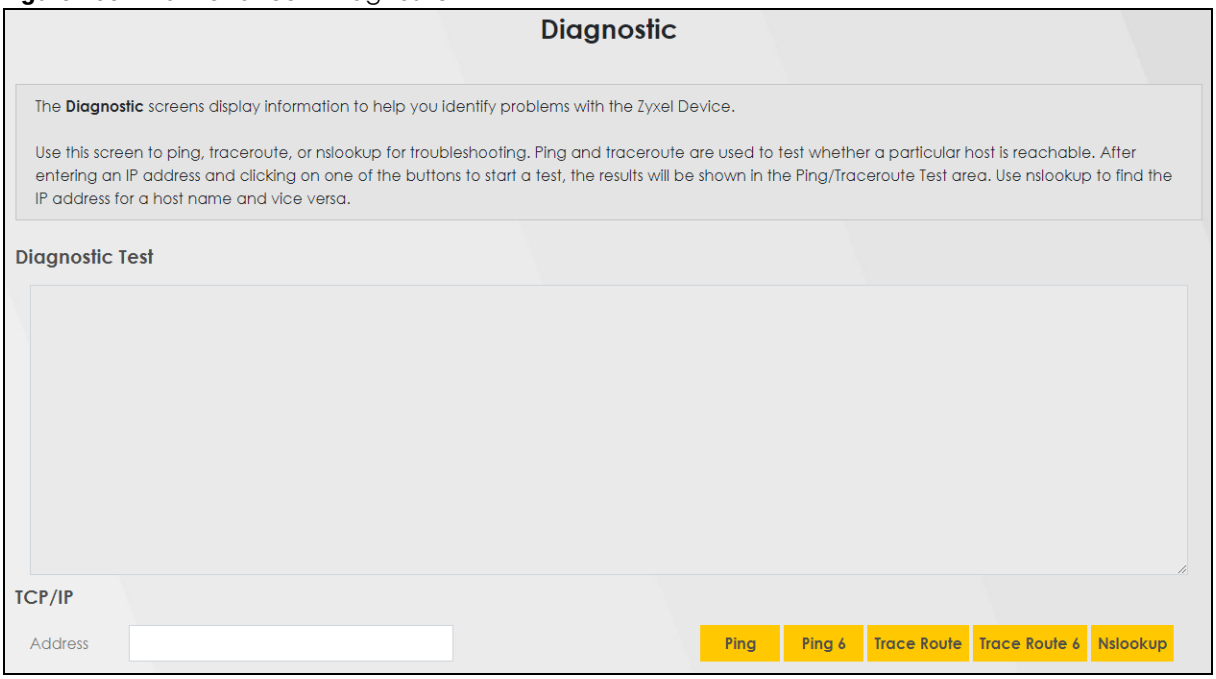
CFM provides two tests to discover connectivity faults.

- Loopback test – checks if the MEP port receives its Loop Back Response (LBR) from its target after it sends the Loop Back Message (LBM). If no response is received, there might be a connectivity fault between them.
- Link trace test – provides additional connectivity fault analysis to get more information on where the fault is. If an MEP port does not respond to the source MEP, this may indicate a fault. Administrators can take further action to check and resume services from the fault according to the line connectivity status report.

20.3 Diagnostic Test

Use this screen use ping, traceroute, or nslookup for troubleshooting. Ping and traceroute are used to test whether a particular host is reachable. After entering an IP address and clicking on one of the buttons to start a test, the results will be shown in the Ping/Traceroute Test area. Use nslookup to find the IP address for a host name and vice versa. Click **Maintenance** > **Diagnostic** to open the screen shown next.

Figure 106 Maintenance > Diagnostic



The following table describes the fields in this screen.

Table 48 Maintenance > Diagnostic

LABEL	DESCRIPTION
Address	Type the IP address of a computer that you want to perform ping, traceroute, or nslookup in order to test a connection.
Ping	Click this to ping the IPv4 address that you entered.
Ping 6	Click this to ping the IPv6 address that you entered.
Trace Route	Click this to display the route path and transmission delays between the WX Device to the IPv4 address that you entered.
Trace Route 6	Click this to display the route path and transmission delays between the WX Device to the IPv6 address that you entered.
Nslookup	Click this button to perform a DNS lookup on the IP address of a computer you enter.

PART III
Troubleshooting and Appendices

Appendices contain general information. Some information may not apply to your WX Device.

CHAPTER 21
Troubleshooting

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

21.1 Power and Hardware Problems

The WX Device does not turn on. None of the LEDs turn on.

1. Make sure the WX Device is turned on.
2. Make sure you are using the power adapter included with the WX Device.
3. Make sure the power adapter is connected to the WX Device and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the WX Device off and on.
5. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Table 12 on page 43.
2. Check the hardware connections.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the WX Device off and on.

5 If the problem continues, contact the vendor.

21.2 Device Access Problems

I do not know the IP address of the WX Device.

1 The default LAN IP address is 192.168.1.2.

2 If your router assigns an IP address to the WX Device, you can find your new IP address on the **Gateway Detail** screen using the MPro Mesh app (See Section 4.5.1 on page 63 for more information) or log into your router's Web Configurator.

3 If this does not work, you have to reset the device to its factory defaults. See Section 21.5 on page 178.

I forgot the admin password.

1 See the cover page for the default login names and associated passwords.

2 If those do not work, you have to reset the device to its factory defaults. See Section 21.5 on page 178.

I cannot access the Web Configurator screen.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.2. See Chapter 3 on page 30 for more details.
- If you changed the IP address (See Section 8.2 on page 133), use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I do not know the IP address of the WX Device.
- Make sure your computer has an IP address in the same subnet as the WX Device. Your computer should have an IP address from192.168.1.3 to 192.168.1.254. See Section 21.5 on page 178.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See Table 12 on page 43.

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

4 If it is possible to log in from another interface, check the service control settings for HTTP and HTTPS (**Maintenance** > **Remote Management**).

5 Reset the device to its factory defaults, and try to access the WX Device with the default IP address. See Section 21.5 on page 178.

6 If the problem continues, contact the network administrator or vendor, or try the advanced suggestion.

Advanced Suggestion

- Make sure you have logged out of any earlier management sessions using the same user account even if they were through a different interface or using a different browser.

I cannot log into the WX Device.

1 Make sure you have entered the password correctly. See the cover page for the default login names and associated passwords. The field is case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the Web Configurator while someone is using Telnet to access the WX Device. Log out of the WX Device in the other session, or ask the person who is logged in to log out.

3 Turn the WX Device off and on.

4 If this does not work, you have to reset the device to its factory defaults. See Section 21.5 on page 178.

21.3 Internet Problems

I cannot access the Internet.

1 Check the hardware connections and follow the instructions at Section 4.3 on page 38 depending on if you choose to use a wired or a WiFi connection. Make sure the LEDs are behaving as expected. See the **Quick Start Guide** and Table 12 on page 43.

2 Make sure you entered your ISP account information correctly in the **Network Setting** > **Home Networking** screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.

3 If you are trying to access the Internet wirelessly, make sure that you enable WiFi on the WX Device (the WX Device's WiFi is enabled by default) and your WiFi client, and that the WiFi settings in the WiFi client are the same as the settings in the WX Device. (see Section 7.3 on page 109 for more information)

4 Disconnect all the cables from your device and reconnect them.

5 If the problem continues, contact your ISP.

I cannot connect to the Internet using an Ethernet cable.

- Make sure you have the Ethernet LAN port connected to a modem or router. (see Section 4.3.2 on page 43 for more information)

21.4 WiFi Problems

The WiFi connection is slow and 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 WiFi devices.

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

- Move your WiFi device closer to the AP if the signal strength is low.
- Reduce WiFi interference that may be caused by other WiFi networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the WiFi client. Avoid placing the WX Device inside any type of box that might block WiFi signals.
- Reduce the number of WiFi clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the WiFi client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

I cannot access the WX Device using WiFi.

- Make sure the WX Device is working in AP or Repeater mode and WiFi is enabled on the WX Device.
- Make sure the WiFi adapter on the WiFi client is working properly.
- Make sure the WiFi adapter installed on your computer is IEEE 802.11 compatible and supports the same WiFi standard as the WX Device.
- Make sure your computer (with a WiFi adapter installed) is within the transmission range of the WX Device.
- Check that both the WX Device and your WiFi station are using the same WiFi and WiFi security settings.

21.5 Resetting the WX Device to Its Factory Defaults

If you reset the WX Device, you lose all of the changes you have made. The WX Device re-loads its default settings, and the password resets to the back-label default key. You have to make all of your changes again.

You will lose all of your changes when you reset the WX Device to its factory defaults.

- You can back up the configuration you made before resetting the WX Device.

To reset the WX Device,

- Make sure the power LED is on.
- Press the **RESET** button for longer than 5 seconds, the Power LED begins to blink, to set the WX Device back to its factory-default configuration.

  OR

  Click **Maintenance** > **Restore** and then click **Reset**.
- If the WX Device restarts automatically, wait for the WX Device to finish restarting, and log in to the Web Configurator. The password is in the device label.

  If the WX Device does not restart automatically, disconnect and reconnect the WX Device. Then, follow the directions above again.
- You can upload a previously saved configuration file from your computer to the WX Device after resetting the device.

21.6 MPro Mesh App Problems

I cannot use the MPro Mesh app to manage my WiFi network.

- Make sure you connect your mobile device to the controller (The Zyxel MPro Mesh router in **Scenario 1** or the WX Device-1 in **Scenario 2**) in order to manage the WiFi network.
- Make sure you use the controller's (The Zyxel MPro Mesh router in **Scenario 1** or the WX Device-1 in **Scenario 2**) SSID and key when logging in with the app.

21.7 Daisy Chain Problems

I cannot add another WX Device to my daisy chain network.

- Check your device mode. The mode of your WX Device will affect how you add another WX Device to your network. For more information on modes, see Section 1.1 on page 12. For more information on how to set your device in AP or Repeater mode, see Section 1.1.3 on page 13.
- If you are using the WPS PBC (Push Button Configuration) method, make sure you press the WPS button in the right way. For more information on adding WX Devices using WPS button, see Section 2.5.1 on page 26.
- If you are using the MPro Mesh app for adding a WX Device to your network, make sure you choose the right scenario.

With an MPro Mesh router, follow the steps in **Scenario1** to add WX Devices to your network (see Section 4.3.1 on page 38 for more information).

With a non-MPro Mesh router, follow the steps in **Scenario 2** to add WX Devices to your network (see Section 4.3.2 on page 43 for more information)

APPENDIX A
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 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 49 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 50 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 cannot be assigned to a multicast group.

Table 51 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

Table 51 Reserved Multicast Address (continued)

MULTICAST ADDRESS
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Subnet Masking

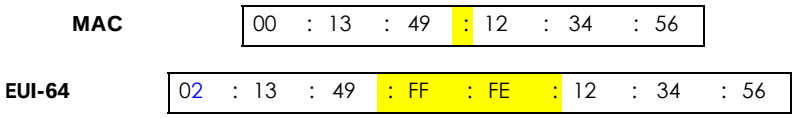
Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 – 10, A – F). Each block's 16 bits are then represented by four hexadecimal characters. For example,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

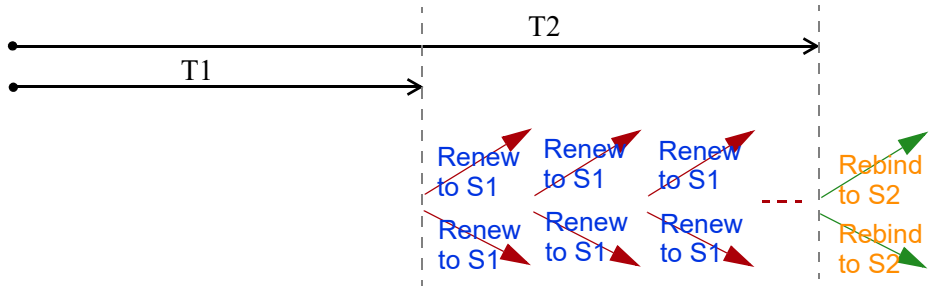
EUI-64

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.



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 WX 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 WX 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 WX Device maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the WX 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 WX Device also sends out a neighbor solicitation message. When the WX Device receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the WX 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 WX Device creates an entry in the default router list cache if the router can be used as a default router.

When the WX 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 WX 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 unlink, the address is considered as the next hop. Otherwise, the WX Device determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the WX Device looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the WX 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 7

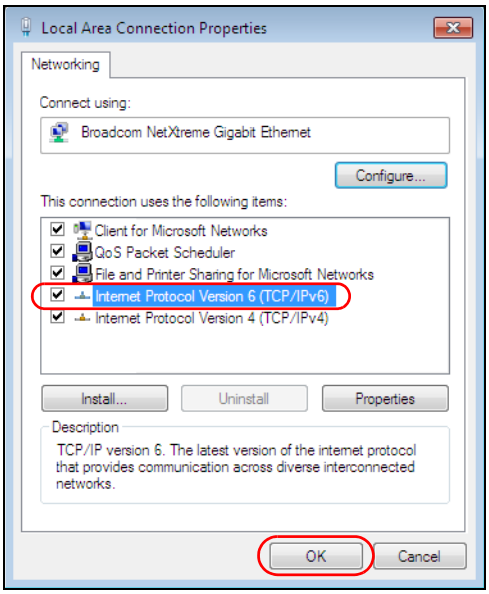
Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

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
Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 52 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for instance *www.zyxel.com*) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Protocol, a program to enable fast transfer of files, including large files that may not be possible by email.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol – a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for email.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.

Table 52 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
NFS	UDP	2049	Network File System – NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one email server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.

Table 52 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
VDOLIVE	TCP UDP	7000 user-defined	A videoconferencing solution. The UDP port number is specified in the application.

APPENDIX D
Legal Information

Copyright

Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement

United States of America

The following information applies if you use the product within USA area.

US Importer: Zyxel Communications, Inc, 1130 North Miller Street Anaheim, CA92806-2001, *https://www.zyxel.com/us/en/*

FCC EMC Statement

- The device complies with Part 15 of 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 product has been tested and complies with the specifications 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 according to 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 device does cause harmful interference to radio or television reception, which is found by turning the device 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 devices
  - Connect the equipment to an outlet other than the receiver's
  - Consult a dealer or an experienced radio/TV technician for assistance

The following information applies if you use the product with RF function within USA area.

FCC Radiation Exposure Statement

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 45 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Operation of this device is restricted to indoor use only, except for relevant user's manual mention that this device can be installed into the external environment.

Europe and the United Kingdom

The following information applies if you use the product within the European Union.

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED)

- Compliance information for wireless products relevant to the EU and other Countries following the EU Directive 2014/53/EU (RED). And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) without any limitation except for the countries mentioned below table:
- In the majority of the EU and other European countries, the 5 GHz 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 5 GHz wireless LANs.
- If this device for operation in the band 5150 – 5350 MHz, 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 power operating for each band as follows:

WX3100-T0:
The band 2.4G is 90.78 mW
The band 5150 to 5350 MHz is 184.93 mW
The band 5470 to 5725 MHz is 926.83 mW

WX3401-B0:
The band 2400 to 2483.5 MHz is 93.54 mW
The band 5150 to 5350 MHz is 189.23 mW
The band 5470 to 5725 MHz is 931.11 mW

WX5600-T0:
The band 2400 to 2483.5 MHz is 87.9 mW
The band 5150 to 5350 MHz is 198.15 mW
The band 5470 to 5725 MHz is 914.11 mW

United Kingdom (WX5600-T0)

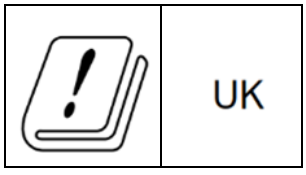
UK Declaration of Conformity

Zyxel hereby declares that the device is in compliance with the essential requirements and other relevant provisions of the Radio Equipment Regulations 2017.

The original UK Declaration of Conformity may be found at *https://service-provider.zyxel.com/global/en/tech-support*.

National Restrictions

Attention: This device may only be used indoors in Great Britain.



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/EL 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/ΕΕ.
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/UE.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/UE.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/UE.
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/UE. **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/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES 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/UE.
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/UE.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/UE.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerințele esențiale şi alte prevederi relevante ale Directivei 2014/53/UE.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EÚ.
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:

- Not all European states that implement EU Directive 2014/53/EU are European Union (EU) members.
- 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	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not put the device in a place that is humid, dusty or has extreme temperatures as these conditions may harm your device.
- Please refer to the device back label, datasheet, box specifications or catalog information for the power rating of the device and operating temperature.
- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- 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 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 connecting cables carefully so that no one will step on them or stumble over them.
- Always 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 it 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 it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,

  – For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;

  – For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

Important Safety Instructions

- Caution! The RJ-45 jacks are not used for telephone line connection.
- Caution! Do not use this product near water, for example a wet basement or near a swimming pool.
- Caution! Avoid using this product (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Caution! Always disconnect all telephone lines from the wall outlet before servicing or disassembling this product.
- Attention: Les prises RJ-45 ne sont pas utilisés pour la connexion de la ligne téléphonique.
- Attention: Ne pas utiliser ce produit près de l'eau, par exemple un sous-sol humide ou près d'une piscine.
- Attention: Évitez d'utiliser ce produit (autre qu'un type sans fil) pendant un orage. Il peut y avoir un risque de choc électrique de la foudre.
- Attention: Toujours débrancher toutes les lignes téléphoniques de la prise murale avant de réparer ou de démonter ce produit.

Environment Statement

ErP (Energy-related Products)

Zyxel products put on the EU market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

- Network standby power consumption < 8W, and/or
- Off mode power consumption < 0.5W, and/or
- Standby mode power consumption < 0.5W.

(Wireless setting, please refer to the chapter about wireless settings for more detail.)

European Union – 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具有無線功能且銷售至台灣地區

- 第十二條 經型式認證合格之低功率射頻電機，非經許可，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。
- 第十四條 低功率射頻電機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。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機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。

- 無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。
- 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中
- 使用無線產品時，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。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用 :
  – 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
  – 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC 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.

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://service-provider.zyxel.com/global/en/gpl-oss-software-notice*.

Index

Numbers

A

B

C

D

E

F

G

H

I

N

O

P

Q

R

S

T

U

V

W

Z