ZYXEL
NETWORKS

User's Guide

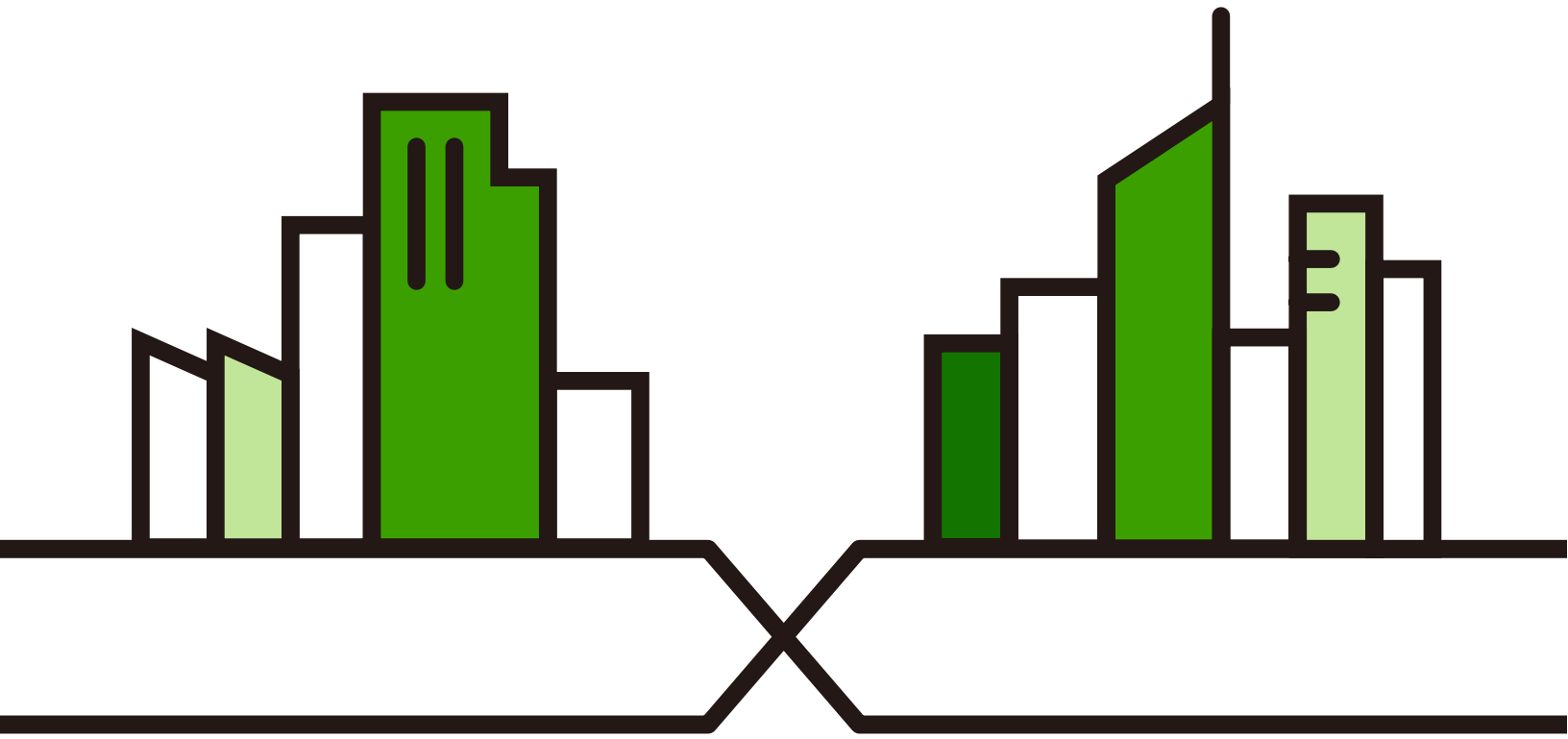
Multy U/Plus/X/Mini/M1

AC/AX WiFi System
Models: WSR30, WSQ60, WSQ50, WSQ20, WSM20

Default Login Details

Zyxel App	Zyxel Multy
myZyxelCloud Account	https://mycloud.zyxel.com

Version 2.4.0 Edition 2, 1/2022



Copyright © 2022 Zyxel and/or its affiliates. All Rights Reserved.

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your app version. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

  The Quick Start Guide contains information on setting up your Multy Device using the Zyxel Multy app.

- Multy App HTML Help

  Go to **https://www.zyxel.com/MultyAppHelp/** to find the Multy App HTML Guide online.

- More Information

  Go to **http://support.zyxel.com** to find other information on the Multy Device.

Table of Contents

Table of Contents **3**

Chapter 1
Get to Know Your Multy WiFi System **8**

1.1 Overview 8
1.2 Applications for the Multy Device 10
1.3 Operating Modes for the Multy Device 12
1.3.1 Standard (Router) Mode 12
1.3.2 Bridge Mode 13
1.4 How to Manage Your Multy Sites 14
1.5 Getting Started 14

Chapter 2
Hardware **15**

2.1 Hardware Connections 15
2.2 Hardware Installation 17
2.2.1 Wall Mounting 17
2.2.2 Leather Strap Hanging 23
2.2.3 Desk Placement 23
2.3 WPS Button 24
2.4 Reset Button 24
2.4.1 Reset the Multy Device Back to Factory Default Settings 25
2.5 LED On/Off Switch 26
2.6 LED Light 27

Chapter 3
Zyxel Multy App Tutorials **30**

3.1 Introduction 30
3.2 Use the Zyxel Multy App 30
3.3 Add and Install Your First Multy Device 34
3.4 Check Your Multy-to-Multy Signal Strength 44
3.5 Remove a Multy Device 46
3.6 Remove a Multy Site 47
3.7 Add a Multy Device to a New Site 49
3.8 Install a Second Multy Site 51
3.9 Test Your Smartphone Connection Speed 55
3.10 Test Your Multy Device Connection Speed 58
3.11 Measure Your WiFi Signal Strength 61
3.12 Enable or Disable Guest WiFi 63

3.13 Share WiFi Name and Password with a QR Code 65
3.14 Set a WiFi Schedule for Clients 67
3.15 Pause Internet Access for an Individual Client 73
3.16 Pause or Resume Internet Access for a Group 76
3.17 Check your Multy Device's Configuration Details 78
3.18 Use Custom DNS Server 80
3.19 Restart Your Multy Device 82
3.20 Change the Name or Picture of a Multy Site 83
3.21 Create or Change Your Web Configurator Password 86
3.22 Enable or Add Port Forwarding Rules 88
3.23 Enable DMZ 92
3.24 Switch to NAT or Bridge Mode 94
3.25 Turn Notifications On or Off 96
3.26 Enable or Disable Daisy Chain Network Topology 99
3.27 Report a Problem With the Zyxel Multy App 101
3.28 Log Out of the myZyxelCloud Account 103
3.29 View Legal and Regulatory Information 104
3.30 Manage Your Multy WiFi System With Amazon Alexa 106

Chapter 4
Multy M1 Wizard 113

4.1 Overview 113
4.2 Accessing the Wizard 113

Chapter 5
Multy M1 Web Configurator 120

5.1 Overview 120
5.2 Accessing the Web Configurator 120
5.3 Navigation Panel 122
5.3.1 Standard Mode Navigation Panel 123
5.3.2 Bridge Mode Navigation Panel 125

Chapter 6
Multy M1 Modes 126

6.1 Overview 126
6.2 Modes 126
6.3 Standard Mode Overview 127
6.4 What You Can Do 127
6.5 Standard Mode Status Screen 127
6.6 Bridge Mode Overview 129
6.7 What You Can Do 129
6.8 Setting your Multy M1 to Bridge Mode 129
6.8.1 Accessing the Web Configurator in Bridge Mode 130

6.9 Bridge Mode Status Screen 131

Chapter 7
Multy M1 Web Configurator Tutorials 132

7.1 Overview 132
7.2 Run a Speed Test 132
7.3 Configure the Multy Devices in a Mesh Network 134
7.4 Configure Main WiFi Networks 136
7.5 Configure Guest WiFi Networks 138
7.6 Configure Parental Control Schedule 139
7.6.1 Create a Parental Control Profile 139
7.7 Configure a Firewall Rule 142
7.7.1 Enable Respond to Ping and Firewall 142
7.7.2 Enable Access Control 143
7.8 Configure the Multy M1 as an OpenVPN Server 145
7.9 Configure the Multy M1 as an OpenVPN Client 147
7.10 Change the Web Configurator Local Password 149
7.11 Change the Operating Mode 150
7.12 Configure a Port Forwarding Rule 151

Chapter 8
Multy Plus Tutorials 154

8.1 Introduction 154
8.2 Use the Web Configurator 154
8.2.1 Login with Local Password 156
8.3 Add and Install Your First Multy Plus 159
8.4 Run a Speed Test 164
8.5 Configure the Multy Plus's WiFi Networks 165
8.6 Enable or Disable a WiFi Network 168
8.7 Add Clients to a Profile 170
8.8 Set a Profile's WiFi Schedule 172
8.9 Pause or Resume Internet Access on a Profile 175
8.10 Turn on or off the Multy Plus's LED (Light) 177
8.11 Remove a Multy Plus 179
8.12 Install a Second Multy Plus WiFi System 180
8.13 Change Your Multy Plus Operating Mode 181
8.14 Configure a Port Forwarding Rule 183
8.15 Enable or Disable Daisy Chain Network Topology 185
8.16 Local Login Password Change 188

Chapter 9
Troubleshooting 191

9.1 Overview 191

9.2 Power, Hardware Connections, and LEDs 191
9.3 Multy Device Access and Login 192
9.4 Internet Access 193
9.5 Resetting the Multy Device to Its Factory Defaults 194
9.6 WiFi Connections 194
9.7 OpenVPN Problems 195
9.8 USB File Sharing Problems 196

Appendix A Customer Support 197

Appendix B Legal Information 202

Index 208

PART I
The Multy Series User's Guide

CHAPTER 1
Get to Know Your Multy WiFi System

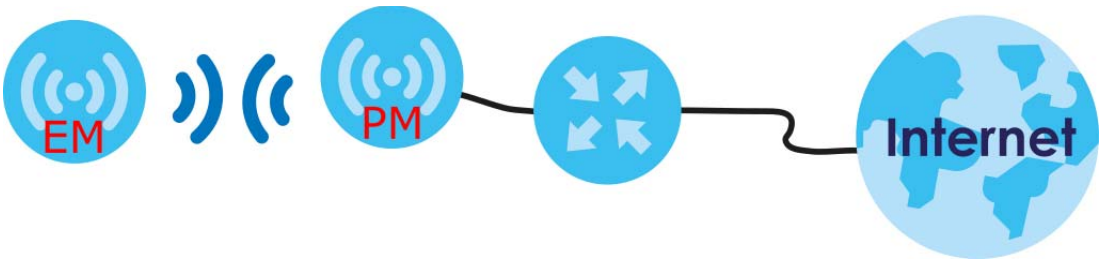
1.1 Overview

Zyxel Multy WiFi System allows you to quickly set up and monitor your WiFi network using the Zyxel Multy app. You can install two or more Multy Devices in a Multy WiFi System, also called a Multy Site, to extend the range of your existing wired network without additional wiring.

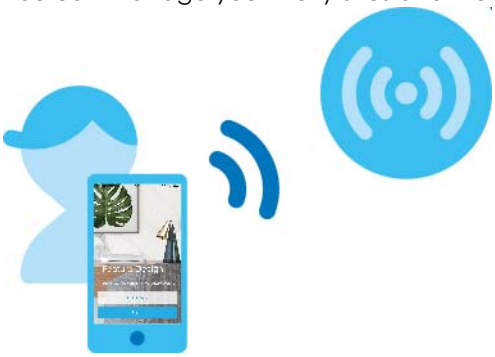
Note: At the time of writing, a maximum of four Multy Devices (one primary Multy and up to three extender Multys) can be used in a Multy Site.

Multy Devices can act either as a primary Multy or an extender Multy. As shown in the next figure, a primary Multy (**PM**) is connected to a modem or router. An extender Multy (**EM**) connects wirelessly to the primary Multy to expand its range. See Table 2 on page 10 to know which Multy devices can be used as a primary Multy or extender Multy.

Note: The primary Multy (**PM**) serves as the controller of a mesh network, while the extender Multy (**EM**) serves as an extender.

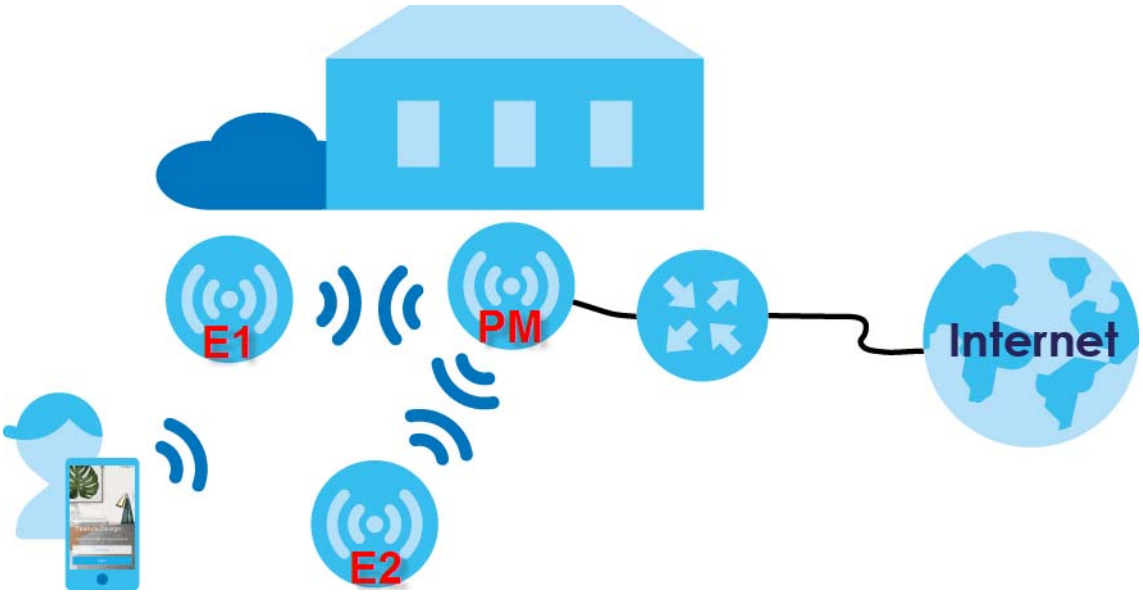


You can manage your Multy Sites and Multy Devices using the Zyxel Multy app, as shown below.



In the following example, the first Multy Device connects to the router to act as the primary Multy (**PM**), while the other Multy Devices are extender Multys (**E1** or **E2**) to expand wireless coverage. The extender

Multys help relay communications from wireless clients to the primary Multy and router.



Multy devices include the following:

- Multy Plus (WSQ60)
- Multy X (WSQ50)
- Multy Mini (WSQ20)
- Multy U (WSR30)
- Multy M1 (WSM20)

Table 1 Differences between Multy devices

FEATURE	MULTY PLUS (WSQ60)	MULTY X (WSQ50)	MULTY MINI (WSQ20)	MULTY U (WSR30)	MULTY M1 (WSM20)
Max. Bandwidth	3000 (Tri-Band)	3000 (Tri-Band)	1750 (Dual-Band)	2100 (Tri-Band)	1800 (Dual Band)
Use as primary Multy	YES	YES	NO	YES	YES
Daisy Chain Topology	YES	YES	NO	NO	NO
Bluetooth	YES	YES	YES	YES	NO
USB Port	YES	YES	YES (Quick Charge 3.0)	NO	NO
Quick Charge	NO	NO	YES	NO	NO
LED On/Off Switch (Side Panel)	NO	NO	NO	NO	YES
LED On/Off Switch (App)	YES	YES	YES	NO	NO
WPS Button	NO	NO	NO	NO	YES
Pairing Method	Bluetooth	Bluetooth	Bluetooth	Bluetooth	WiFi
APP Management	YES	YES	YES	YES	YES
GUI Management	YES	NO	NO	NO	YES
Number of LAN Ports	3	3	1	1	4

Table 1 Differences between Multy devices (continued)

FEATURE	MULTY PLUS (WSQ60)	MULTY X (WSQ50)	MULTY MINI (WSQ20)	MULTY U (WSR30)	MULTY M1 (WSM20)
Number of internal antennas					
5G	6	6	3	4	2
2.4G	2	2	3	2	2
BLE (Bluetooth Low Energy)	1	1	1	1	0
E-label	NO	NO	YES	YES	YES
Amazon Alexa	YES	YES	YES	YES	YES

The Quick Charge function is a fast charging technology that allows you to charge your device through a USB port within a short period of time.

A Tri-Band WiFi System emits one 2.4G wireless signal and two 5G wireless signals. Dual-Band WiFi Systems emit one 2.4G signal and one 5G signal. "Max. Bandwidth" refers to the sum of the bandwidths of all wireless signals (2.4G and 5G) emitted by the Multy Device.

The next table shows which Multy Devices you can use as extender Multys for a given primary Multy.

Table 2 Allowed Extender Multys for a Given Primary Multy

		EXTENDER MULTY				
		MULTY PLUS (WSQ60)	MULTY X (WSQ50)	MULTY MINI (WSQ20)	MULTY U (WSR30)	MULTY M1 (WSM20)
PRIMARY MULTY	Multy Plus (WSQ60)	YES	NO	NO	NO	NO
	Multy X (WSQ50)	NO	YES	YES	NO	NO
	Multy U (WSR30)	NO	NO	NO	YES	NO
	Multy M1 (WSM20)	NO	NO	NO	NO	YES

The following table shows the role of router and extender of the Multy Device in a mesh network.

Table 3 The Assigned Role in a Mesh Network

	MULTY PLUS (WSQ60)	MULTY X (WSQ50)	MULTY MINI (WSQ20)	MULTY U (WSR30)	MULTY M1 (WSM20)
Router Name in the app	Primary Multy	Primary Multy	Primary Multy	Primary Multy	Multy Router
Extender Name in the app	Extender Multy	Extender Multy	Extender Multy	Extender Multy	Satellite

1.2 Applications for the Multy Device

The Multy Device supports the following applications.

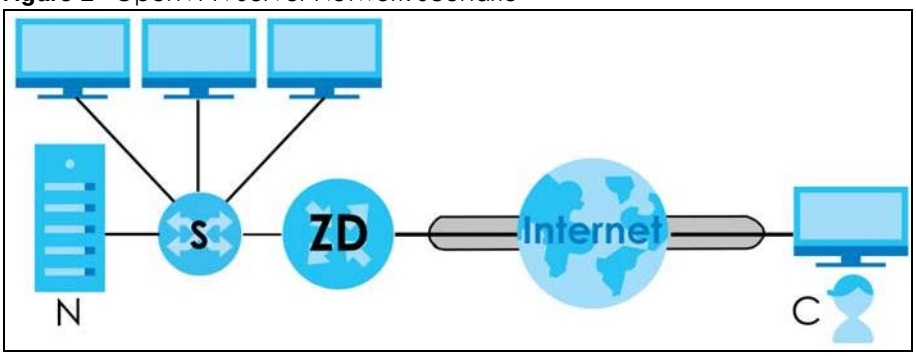
Guest WiFi

The Multy Device allows you to set up a guest WiFi network where users can access the Internet through Multy Device, but not to other networks connected to it.

OpenVPN Server/Client

OpenVPN is a VPN protocol which is open source and free of charge. It can be used to create a virtual private network or to connect local networks.

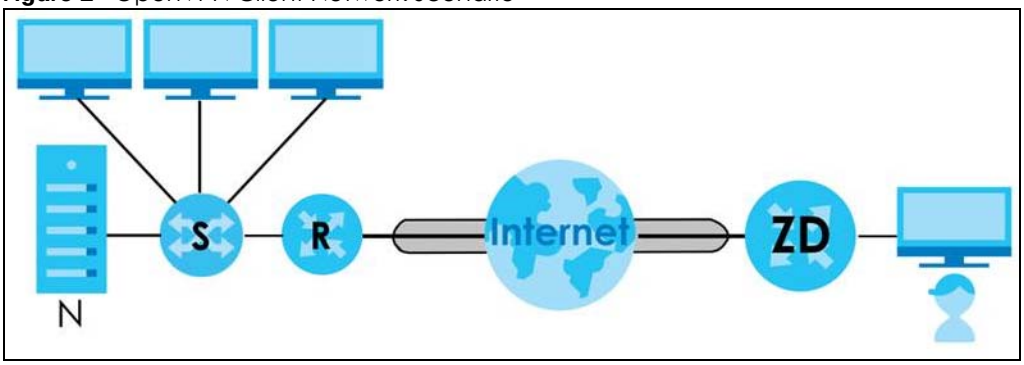
Figure 1 OpenVPN Server Network Scenario



The labels used in the graphic are explained below:

- **C**- A client device connected to the OpenVPN server. Make sure to install OpenVPN client software on the client device first.
- **ZD**- A Multy Device that serves as the OpenVPN server.
- **S**- A switch that connects the Multy Device and the local network.
- **N**- A local network behind the OpenVPN sever.

Figure 2 OpenVPN Client Network Scenario



The labels used in the graphic are explained below:

- **ZD**- A Multy Device that serves as the OpenVPN client.
- **R**- A router that serves as the OpenVPN server.
- **S**- A switch that connects the OpenVPN server and the local network.
- **N**- A local network behind the OpenVPN sever.

IPv6 and IPv6 Firewall

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. The Multy Device can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and support IPv6 rapid deployment (6RD).

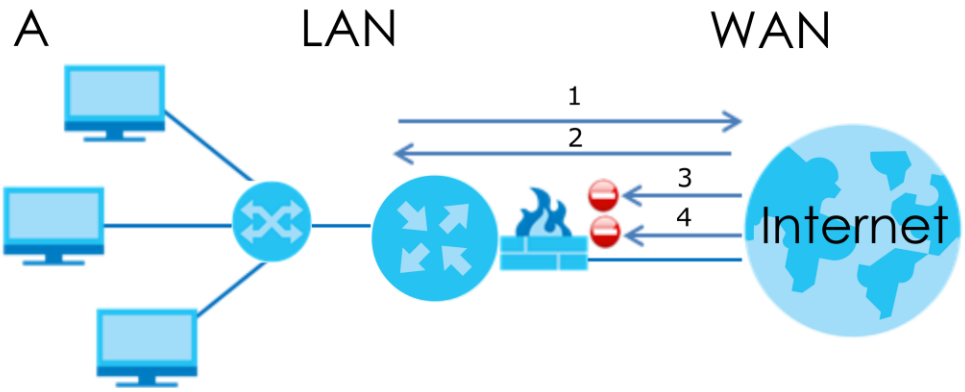
Consequently, you can enable and create IPv6 firewall rules to filter IPv6 traffic.

Firewall protects your Multy Device and network from attacks by hackers on the Internet and control access to it. The firewall:

- allows traffic that originates from your LAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN.

The following figure illustrates the firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (**1**). Return traffic for this session is also allowed (**2**). However other traffic initiated from the WAN is blocked (**3** and **4**).

Figure 3 Default Firewall Action



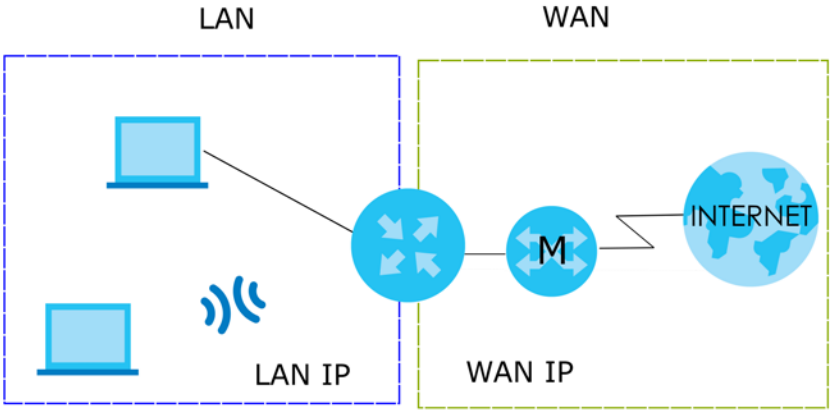
1.3 Operating Modes for the Multy Device

The Multy Device is available in both Standard (router) mode and bridge mode.

1.3.1 Standard (Router) Mode

The Multy Device is set to standard (router) mode by default. The Multy Device is used to connect the local network to another network (for example, the Internet). In standard mode Multy Device has two IP addresses, a LAN IP address and a WAN IP address. It also has more routing features. In the example scenario below, Multy Device connects the local network to the Internet through a modem (**M**).

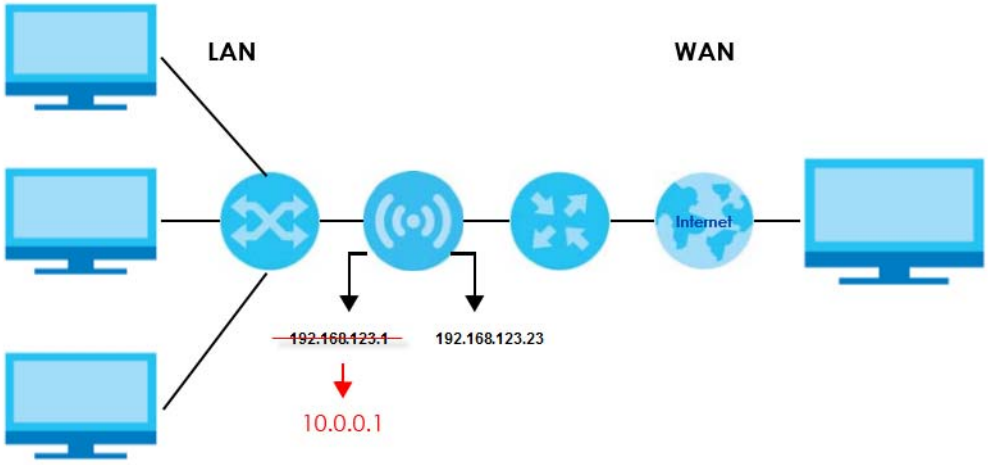
Figure 4 Standard Mode Example



Auto-IP Change

When the Multy Device (**A**) gets a WAN IP address or a DNS server IP address which is in the same subnet as the LAN IP address 192.168.123.1, Auto-IP Change allows the Multy Device to change its LAN IP address to 10.0.0.1 automatically. If the Multy Device's original LAN IP address is 10.0.0.1 and the WAN IP address is in the same subnet, such as 10.0.0.3, the Multy Device switches to use 192.168.123.1 as its LAN IP address.

Figure 5 Auto-IP Change Example



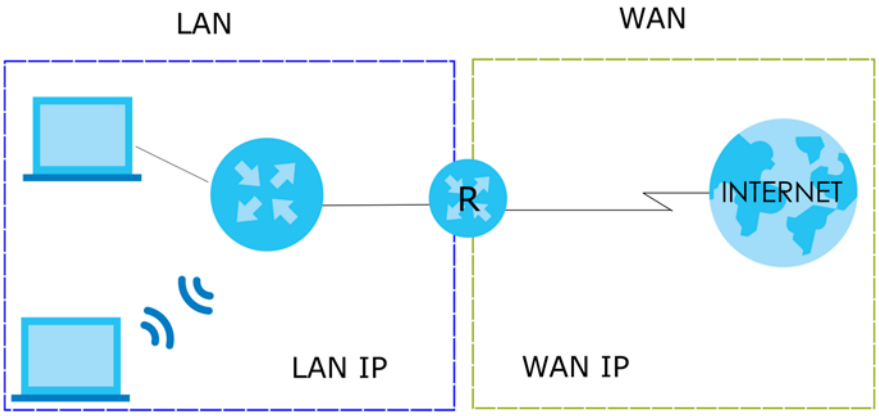
Auto-IP Change only works under the following conditions:

- The Multy Device must be in standard (router) mode for Auto-IP Change to become active.
- The Multy Device is set to receive a dynamic WAN IP address.

1.3.2 Bridge Mode

Use your Multy Device as a bridge if you already have a router or gateway on your network. In this mode your Multy Device bridges a wired network (LAN) and WiFi in the same subnet. In bridge mode, Multy Device has one IP address and Multy Device interfaces are bridged together in the same network. In the example scenario below, Multy Device connects the local network to the Internet through a router (**R**).

Figure 6 Bridge Mode Example



1.4 How to Manage Your Multy Sites

You can use the following way to manage your Multy WiFi System.

• Web Configurator. This is recommended for everyday management of Multy Devices using a (supported) web browser. Please refer to Table 1 on page 9 to for more information.

• Multy. This is the app you can use to manage Multy Devices on your smartphone. This User's Guide provides information about key uses of the Zyxel Multy app. To install the app, scan the QR code on the QSG.

1.5 Getting Started

To set up a Multy Site, you need to:

1. Have a broadband modem or router that is connected to the Internet.
2. Get at least one Multy Device. If you have multiple Multy Devices, the first one you install should be connected to the modem or router. Other Multy Devices can be placed in different rooms to extend WiFi range by wirelessly connecting to the first Multy Device.
3. Install the Zyxel Multy app and turn on Bluetooth or WiFi on your smartphone to pair with your Multy Device. Make sure your smartphone also has Internet access. Pairing method used by your model. See Table 1 on page 9 for more information.
4. Set up your first Multy Device.
5. Use the Zyxel Multy app to set up the Multy Device and manage your Multy Site (see Chapter 3 on page 30).

CHAPTER 2
Hardware

2.1 Hardware Connections

1 Use the included power cable to connect the Multy Device's power port to a power outlet.

2 If you are installing the first Multy Device, connect the Internet port of the Multy Device to a broadband modem or router that is connected to the Internet.

3 You may use Ethernet cables to connect other devices to your Multy Device.

Figure 7 WSQ60/WSQ50 Rear Panel

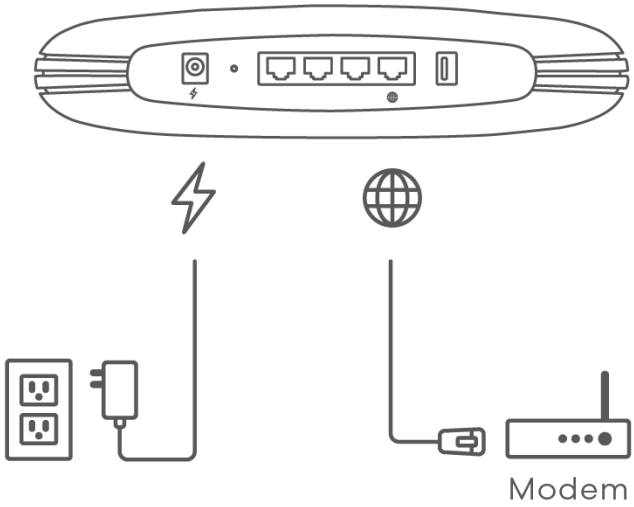


Figure 8 WSQ20 Rear Panel

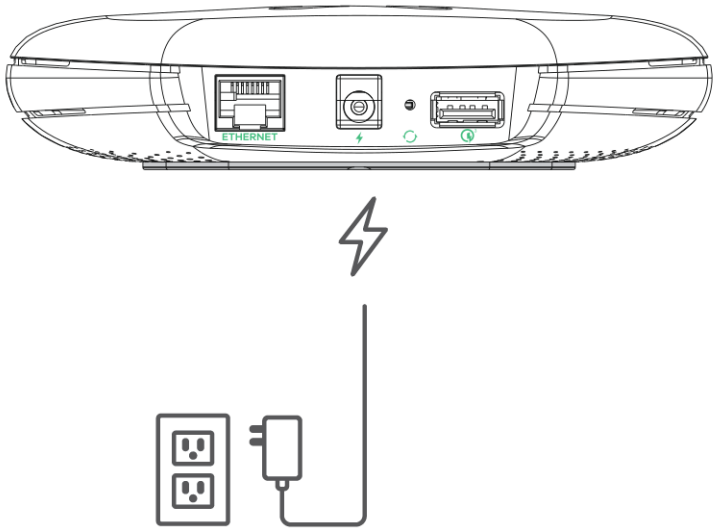


Figure 9 WSR30 Rear Panel

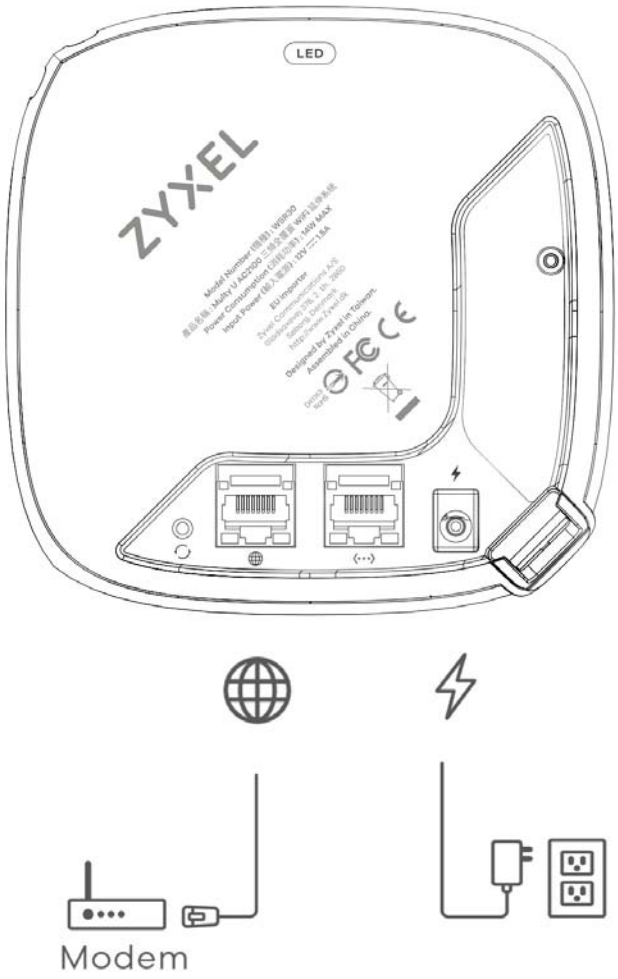
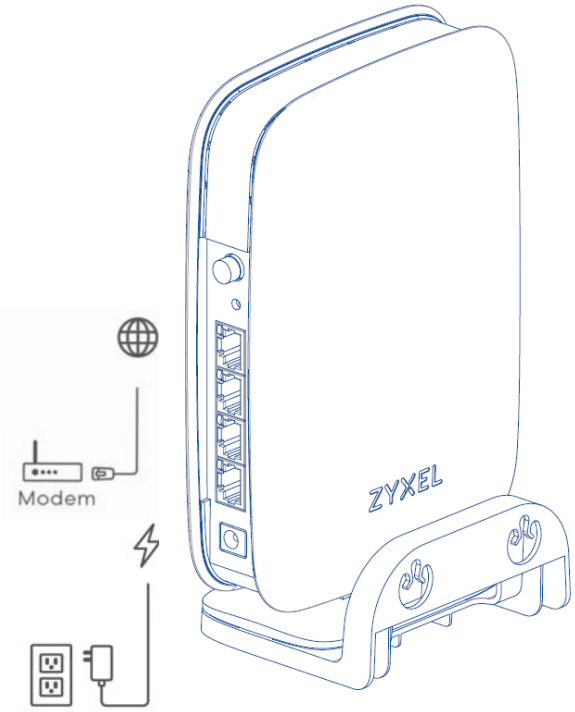


Figure 10 WSM20 Rear Panel



2.2 Hardware Installation

This section describes how the hardware device can be installed.

Table 4 Multy Device Hardware Installation

MULTY DEVICE	WALL MOUNTING	CEILING MOUNTING	DESK PLACEMENT	LEATHER STRAP HANGING
MULTY PLUS (WSQ60)	YES	YES	YES	NO
MULTY X (WSQ50)	YES	YES	YES	NO
MULTY MINI (WSQ20)	YES	YES	YES	NO
MULTY U (WSR30)	NO	NO	YES	YES
MULTY M1 (WSM20)	YES	NO	YES	NO

2.2.1 Wall Mounting

Use the wall mounting method to install your Multy Device. See Table 4 on page 17 for more information.

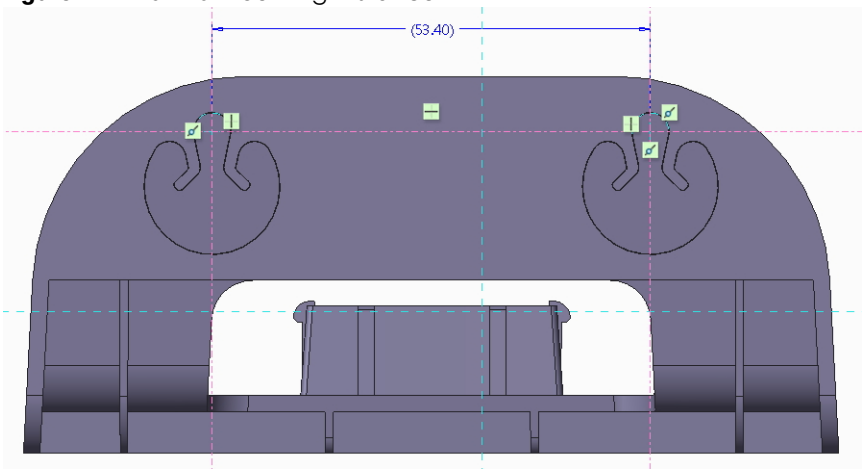
2.2.1.1 WSM20 Wall Mounting

You can use the mounting base to attach the WSM20 to a wall.

Follow these steps for the WSM20 wall mounting:

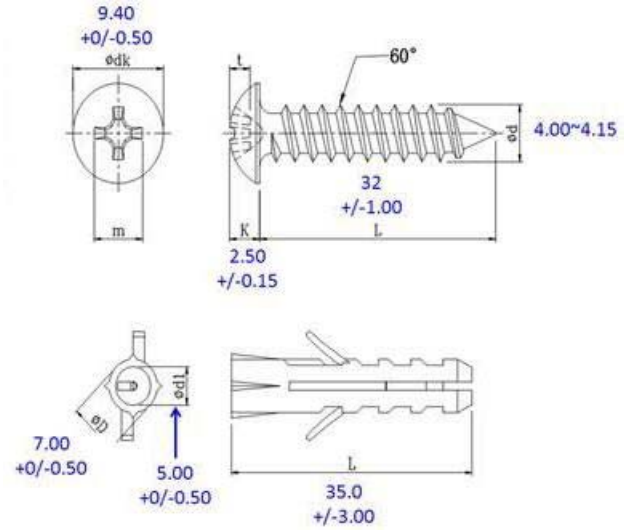
1 Use the mounting base to mark two holes on the wall. Drill two holes at the distance of 53.40 mm.

Figure 11 WSM20 Mounting Distance



2 Insert the anchors and then screw the mounting base into the wall using the screws of the required specs as shown below.

Figure 12 WSM20 M4 Screw/Anchor Spec



3 Slide the WSM20 down gently until it is secured to the mounting base.

Figure 13 Slide the WSM20 Down

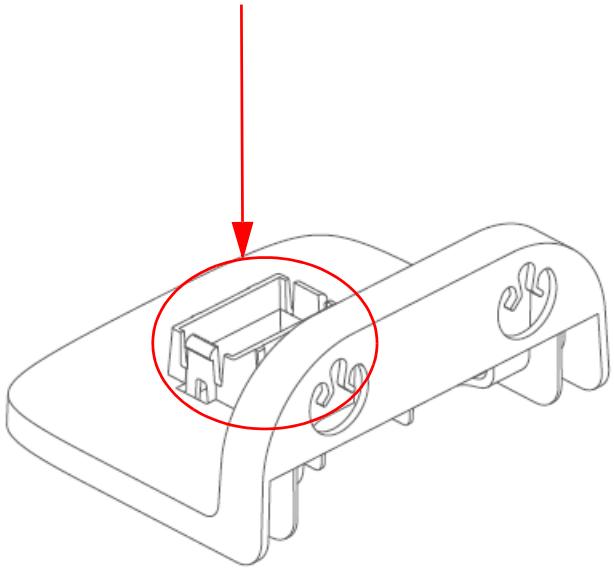
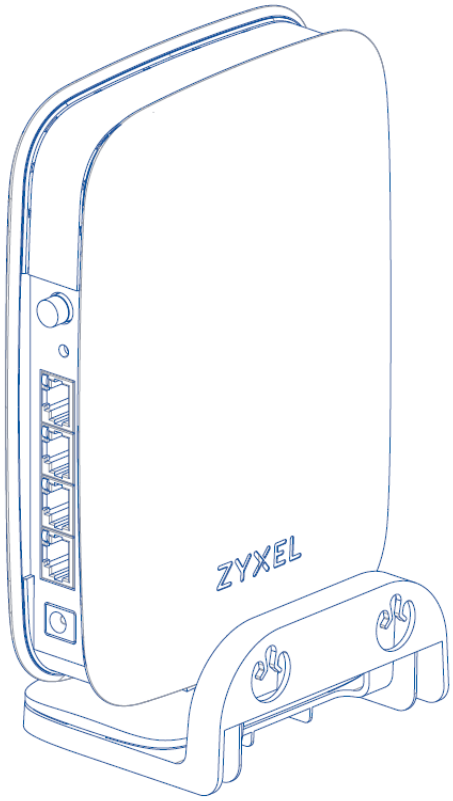


Figure 14 Secure the WSM20 to the Mounting Base



2.2.1.2 WSM20 Removal

There are two hooks on the WSM20. Use a thin object to press the hooks down on the front and rear panel of the WSM20 to release the WSM20 from the mounting base.

Figure 15 The hook on the front panel

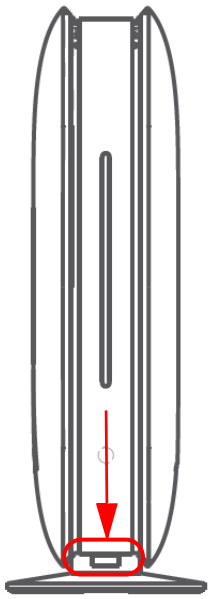
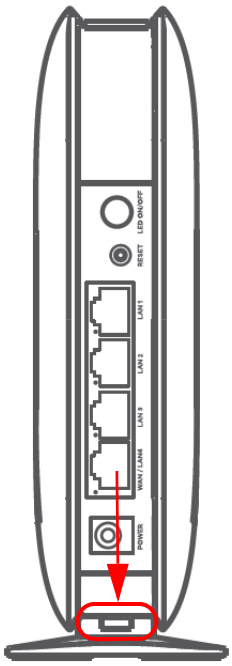


Figure 16 The hook on the back panel



2.2.1.3 WSQ60 / WSQ50 / WSQ20 Wall/Ceiling Mounting

If your Multy Device comes with mounting holes at the bottom, you can use mounting brackets to attach it to a wall or ceiling.

Figure 17 WSQ50/WSQ60 Mounting Holes

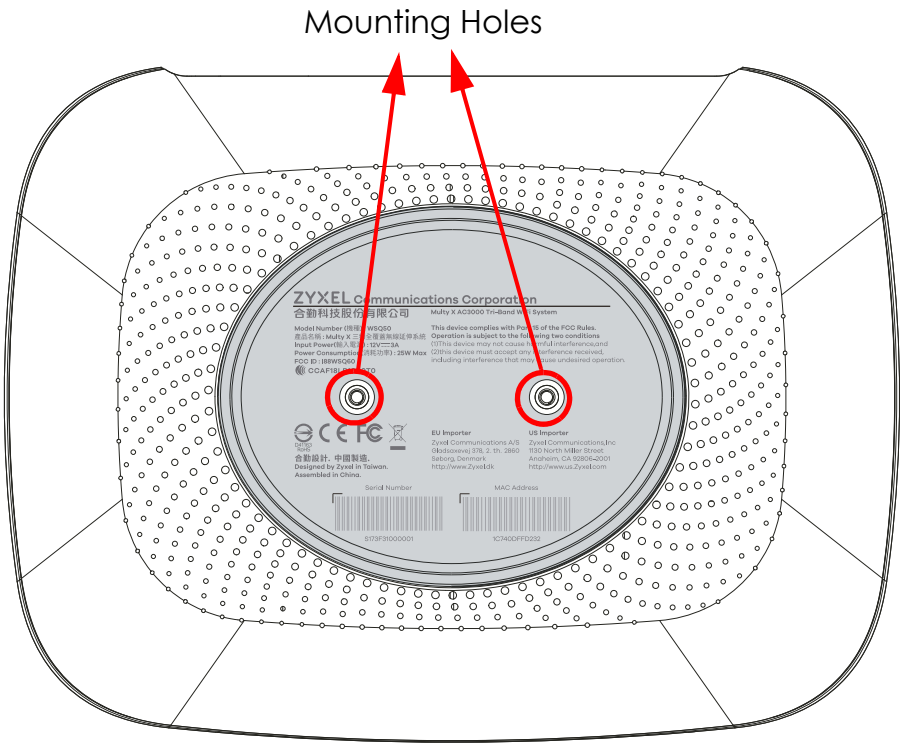
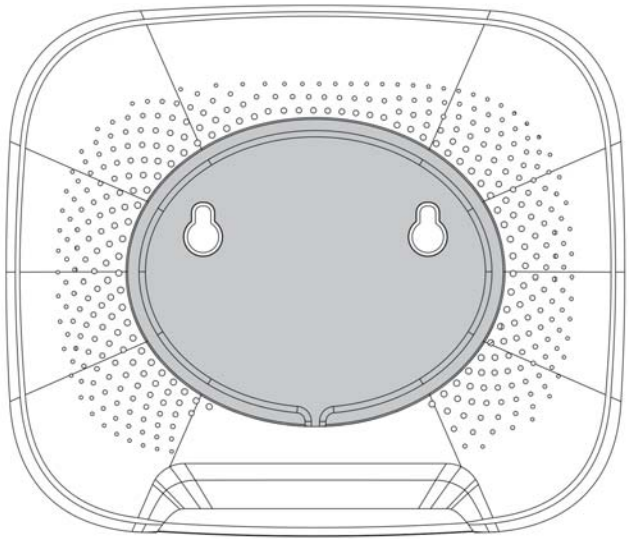
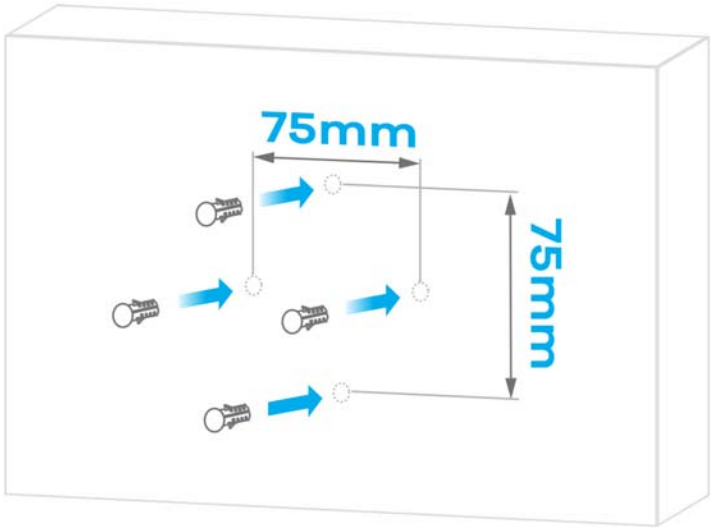


Figure 18 WSQ20 Mounting Holes



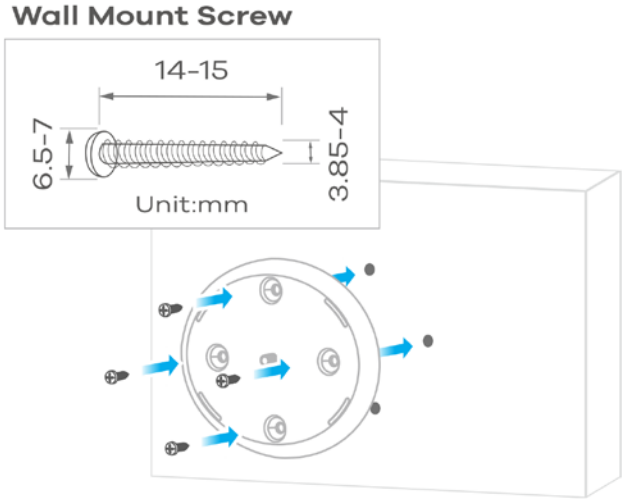
Follow these steps for WSQ60 / WSQ50 / WSQ20 wall or ceiling mounting:

1 Use the mounting base to mark four holes in the wall or ceiling. Drill the holes and insert the anchors.

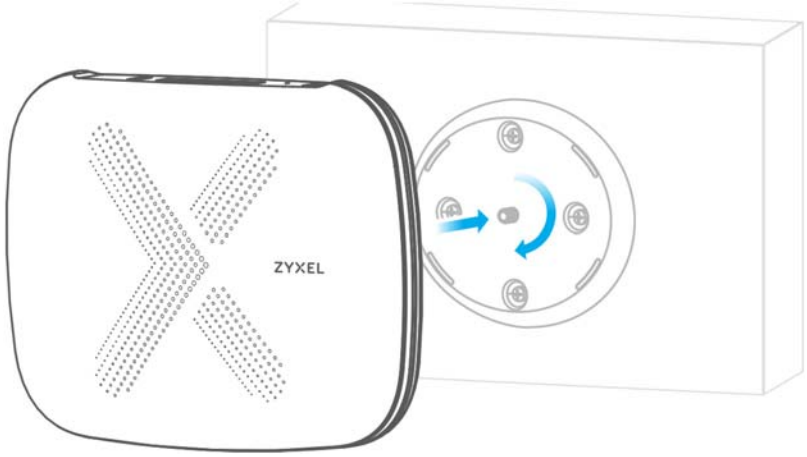


2 Screw the mounting base into the wall or ceiling.

Figure 19 WSQ20/50/60 screw specifications



3 Line up the Multy's base hole with the mounting base screw. Gently turn the Multy clockwise until it is secured to the mounting base.



2.2.2 Leather Strap Hanging

Use the leather strap hanging method to install your Multy Device. See Table 4 on page 17 for more information.

- You can attach the leather strap to the hole at the top of your Multy Device to hang it to a wall or ceiling, as shown in Figure 20 on page 23.

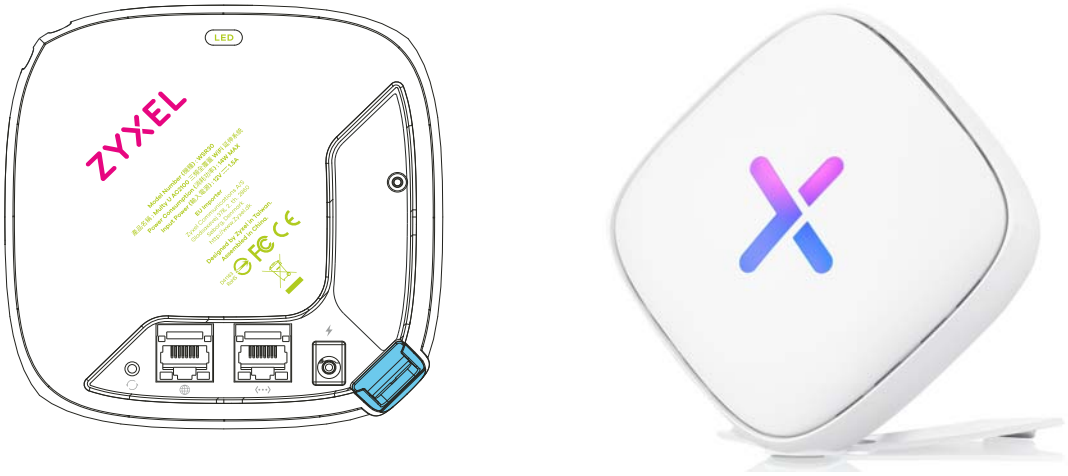
Figure 20 WSR30 Leather Strap

2.2.3 Desk Placement

You may place your Multy Device on a desk, table, shelf, and so on. See Table 4 on page 17 for more information.

- You can use the back port cover as a stand by attaching it to the bottom of the Multy Device (shown blue in Figure 21 on page 23).

Figure 21 WSR30 Stand



2.3 WPS Button

You can use the WPS button to quickly set up a secure WiFi connection between the Multy Device and a WPS-compatible client device by adding one device at a time. See Table 1 on page 9 for more information.

To activate WPS:

1 Make sure the LED lights turns steady blue and not blinking.

2 Press the WPS button until the LED light blink pink and release it.

3 Press the WPS button on another WPS-enabled client device within range of the Multy Device within 120 seconds. The LED blinks pink while the Multy Device sets up a WPS connection with the other WiFi client device.

4 Once the connection is successfully made, the LED turns steady lake green

2.4 Reset Button

If you need to return the Multy Device to its default settings, use the reset button on the rear panel.

Figure 22 WSQ60/WSQ50 Reset Button

Figure 23 WSQ20 Reset Button

Figure 24 WSR30 Reset Button

Figure 25 WSM20 Reset Button

2.4.1 Reset the Multy Device Back to Factory Default Settings

Follow the steps below for a factory reset.

WSQ60 / **WSQ50** / **WSQ20**:

1 Make sure the LED light on the top panel is not blinking white.

2 Press the reset button for at least 5 seconds or until the LED starts to blink red.

WSR30:

Press the reset button for at least 5 seconds or until the LED starts to blink amber.

WSM20:

Press the reset button for at least 5 seconds or until the LED starts to blink yellow.

2.5 LED On/Off Switch

WSM20:

Press the LED On/Off switch to turn on or off LED lights.

Figure 26 WSM20 LED On/Off Switch

2.6 LED Light

Look at the LED behavior to determine the status of the Multy Device. See Table 5 on page 28, Table 6 on page 29, and Table 7 on page 29 for more information.

Figure 27 WSQ50 / WSQ60 LED

Figure 28 WSQ20 LED

Figure 29 WSR30 LED

Figure 30 WSM20 LED

The following are the LED descriptions for your Multy Device.

Table 5 WSQ60 / WSQ50 / WSQ20 LED Descriptions

COLOR	STATUS	DESCRIPTION
	Off	The Multy Device is not receiving power.
White	Blinking	The Multy Device is booting up, undergoing firmware upgrade, or being configured.
	On	The Multy Device is on and connected to the Internet.
Blue	Blinking	Bluetooth is enabled on the Multy Device.
	On	The Multy Device in extender mode is connecting to the primary Multy.

Table 5 WSQ60 / WSQ50 / WSQ20 LED Descriptions (continued)

COLOR	STATUS	DESCRIPTION
Red	On	The Multy Device in primary Multy mode failed to connect to the Internet, the Multy Device in extender mode cannot connect to the primary Multy, Bluetooth is not working on the Multy Device, or the Multy Device encountered a system error.
	Slow Blinking	An error occurred during firmware update.
	Fast Blinking	The Multy Device is in the process of restoring to default.

Table 6 WSR30 LED Descriptions

COLOR	STATUS	DESCRIPTION
	Off	The Multy Device is not receiving power.
White	Blinking	The Multy Device is booting up.
	On	The Multy Device power is on.
Blue	Blinking	The Multy Device Bluetooth is being configured.
	On	The Multy Device Bluetooth is ready.
Pink or Blue	Rotate	The Multy Device is ready for use. Rotate here means the pink light will move around the LED indicator while the blue light is stationary.
Amber	Blinking	The Multy Device is undergoing firmware upgrade.
	Fast Blinking	The Multy Device is being reset.
Red	On	The Multy Device in primary Multy mode failed to connect to the Internet or the Multy Device in extender mode cannot connect to the primary Multy.

Table 7 WSM20 LED Descriptions

COLOR	STATUS	DESCRIPTION
Lake Green	On	The Multy Device is receiving power and ready for use.
	Blinking	The Multy Device is booting up.
	Off	The Multy Device is not receiving power.
Green	On	The Multy Device is ready for use.
	Blinking	The Multy Device setup process is in progress. The Multy Device WAN/ Wireless Web Configuration setup process is in progress.
Yellow	On	The Multy Device is updating firmware.
	Blinking	The Multy Device is being reset.
Red	On	TheMulty Device in Multy Router mode failed to connect to the Internet. OR The Multy Device in extender mode cannot connect to the Multy Router.
Pink	Blinking	The Multy Device is setting up a WPS connection with another Multy Device.

CHAPTER 3
Zyxel Multy App Tutorials

3.1 Introduction

The Zyxel Multy app helps you install Multy Devices and manage your Multy Sites directly with your Android or iOS device.

Note: Your smartphone needs to have Internet access to configure the following settings.

Compatibility

- Android 8.0 or later
- iOS 12.0 or later

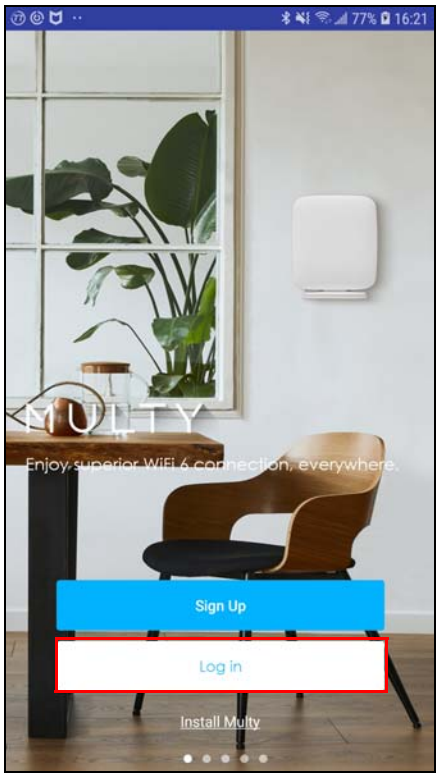
3.2 Use the Zyxel Multy App

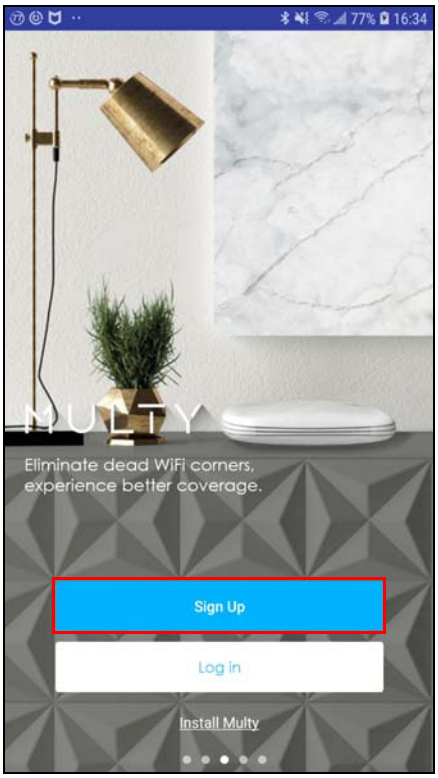
You can log in and use the Zyxel Multy app with or without a myZyxelCloud account.

With a myZyxelCloud account, all your configurations will be stored in the myZyxelCloud server. You then can log in and use the app on any smartphone to manage your Multy Sites once they have been set up. Moreover, Multy Devices can work with Amazon Alexa after the myZyxelCloud account is linked to Alexa (Section 3.30 on page 106).

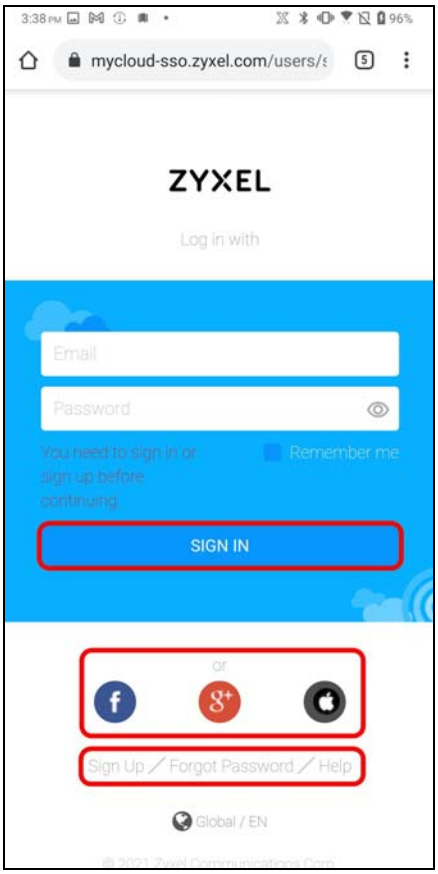
1 Install the Zyxel Multy app from Google Play or the Apple App store. Tap the Multy icon to open it.

2 The **Multy** screen displays. Tap **Log in** to enter your credentials if you already have a myZyxelCloud account. Tap **Sign Up** to create a new myZyxelCloud account.


77% 16:21
MULTY
Enjoy superior WiFi 6 connection, everywhere.
Sign Up
Log in
Install Multy

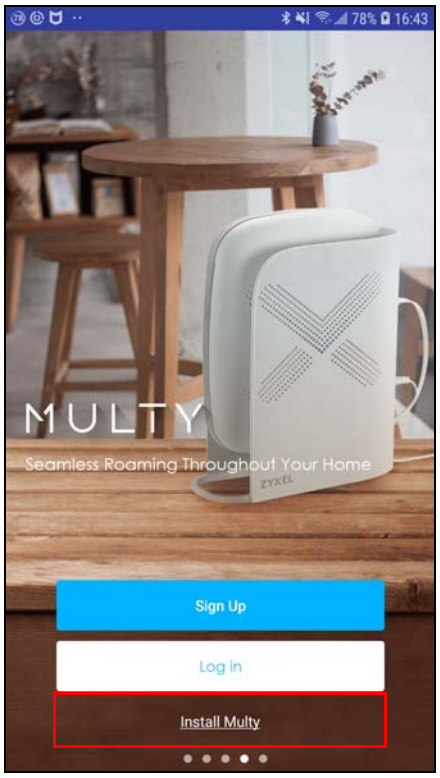

77% 16:34
MULTY
Eliminate dead WiFi corners,
experience better coverage.
Sign Up
Log in
Install Multy

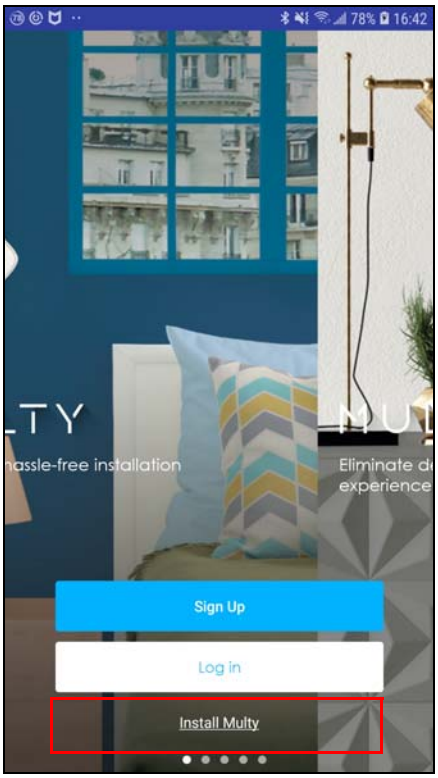
3 The following screen displays. Enter your existing Google/Facebook/Apple account information and tap **SIGN IN** to log in. Tap **Sign Up** if you want to create a myZyxelCloud account.



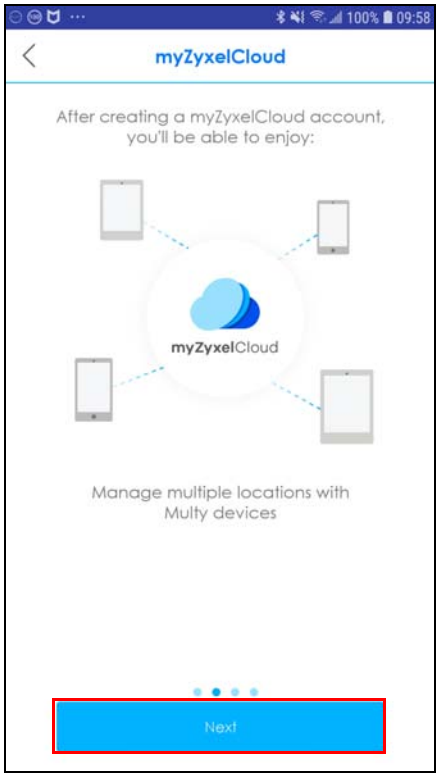
4 If you do not have a myZyxelCloud account or do not want to log in with a myZyxelCloud account, tap **Install Multy** in the **Multy** screen.

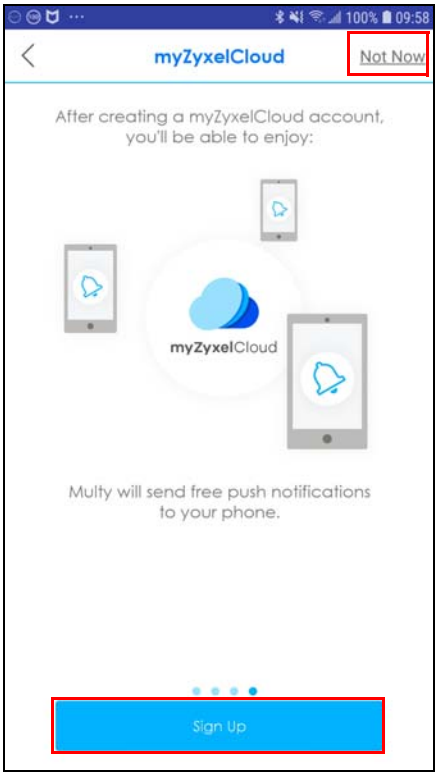
Note: You must create a local password through the Multy app for the Web Configurator If you do not sign in with myZyxelCloud. See Section 3.21 on page 86 for more information.





5 The following **myZyxelCloud** screens display after you tap **Install Multy**. Tap **Next** to continue. Tap **Not Now** to install your Multy Device directly and skip the sign in process.
If you decide to log in with a myZyxelCloud account, Tap **Sign Up**. You will be then redirected to the screen in step 3. See step 3 for more information.





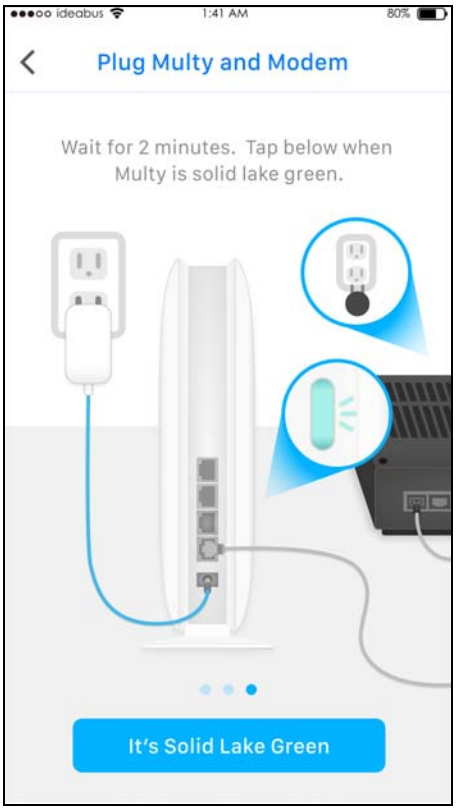
3.3 Add and Install Your First Multy Device

You need to install at least one Multy Device before you can manage a Multy Site. See Section 1.1 on page 8 to prepare for installation and to know which Multy Devices can be used as primary and extender Multys.

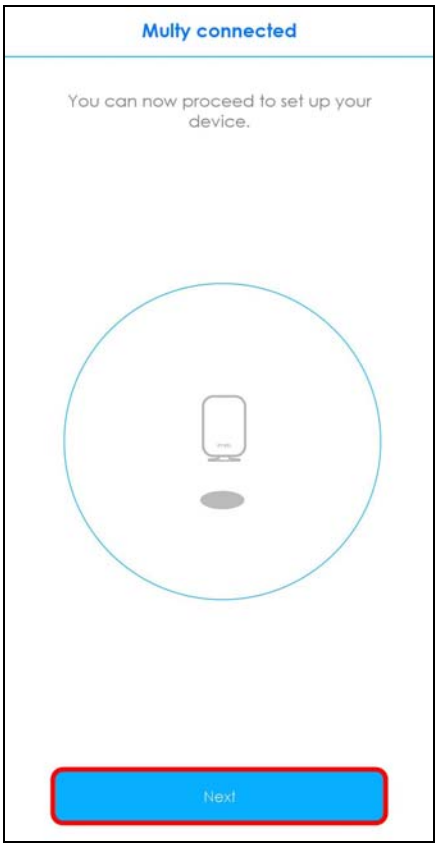
1 The **Get Ready** screen appears after you tap **Not Now**. Choose the product model of your device and tap **Start**.

2 Tap **Start** to install and add a Multy Device to your Multy Site. Follow the next steps that appear on your screen. Unplug and then plug your modem as instructed in the app to prevent errors.

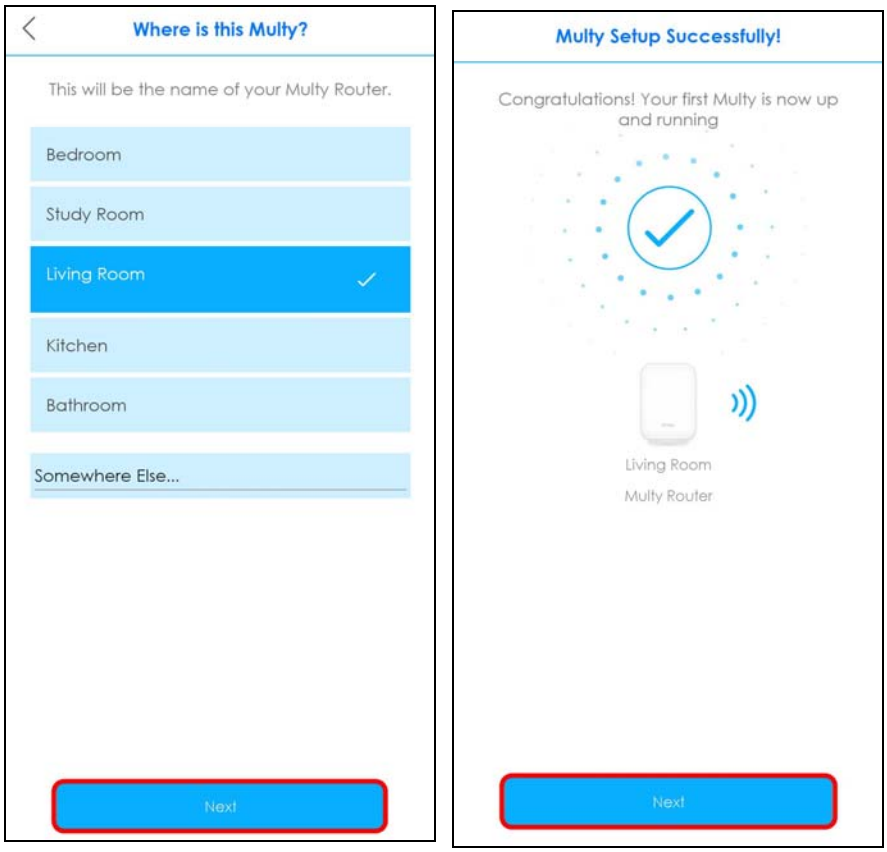
3 After unplugging and plugging your modem as instructed, check the LED light and then then tap **It's Solid Lake Green** or **It's Blinking Blue** according to the Multy Device you use.



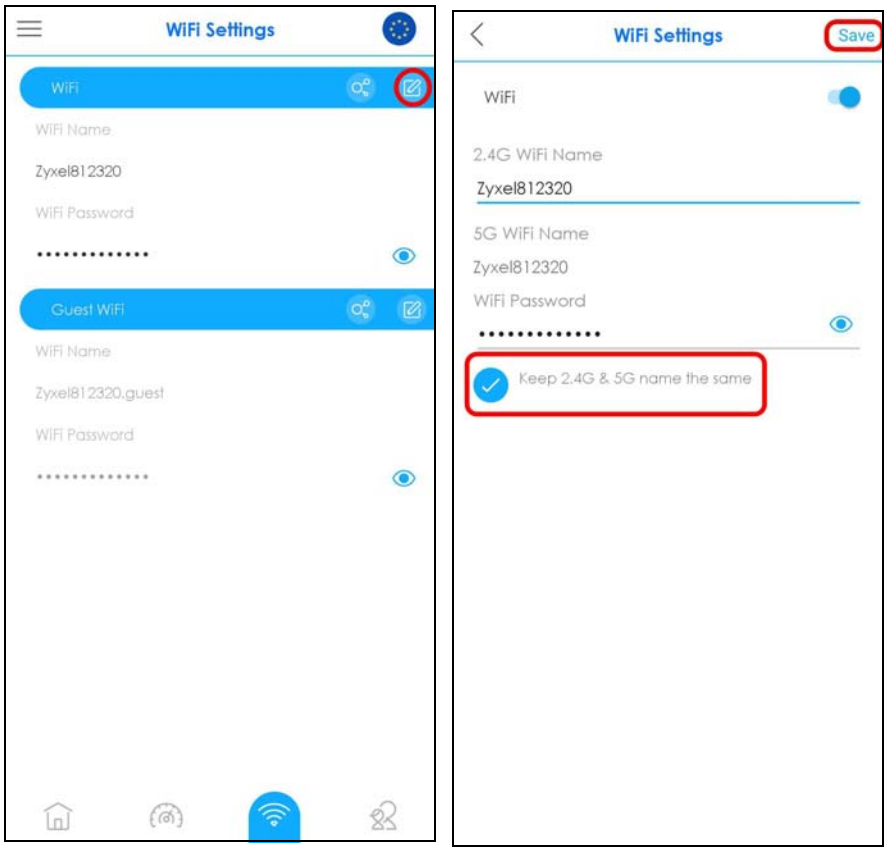
4 Use your smartphone to scan the QR code to connect your smartphone to the WiFi network of the Multy Device. Click **Next** on the **Multy connected** screen to continue.


Multy connected
You can now proceed to set up your device.
Next

5 Select the location where you want to place your Multy Device, and then tap **Next**. The **Multy Setup Successfully!** screen appears.

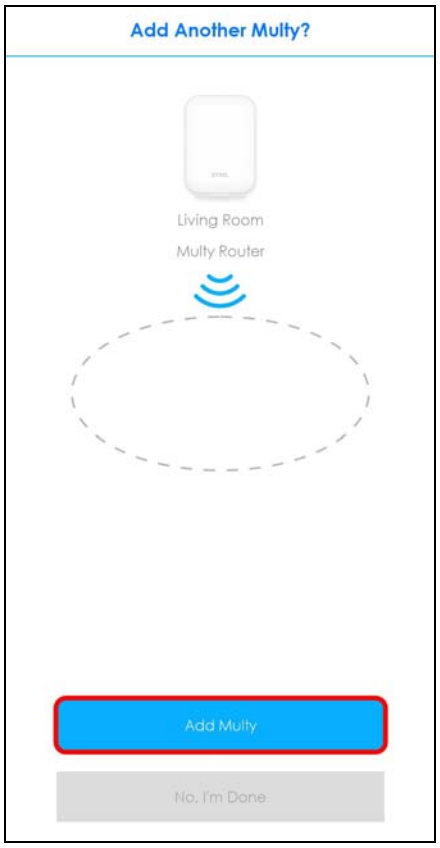


6 Click the edit( ) icon on the WiFi Settings screen and then enable **Keep 2.4G & 5G name the same**. Click **Save** to save the changes. Keeping 2.4G and 5G names the same allows you to seamlessly steer between the two wireless networks.

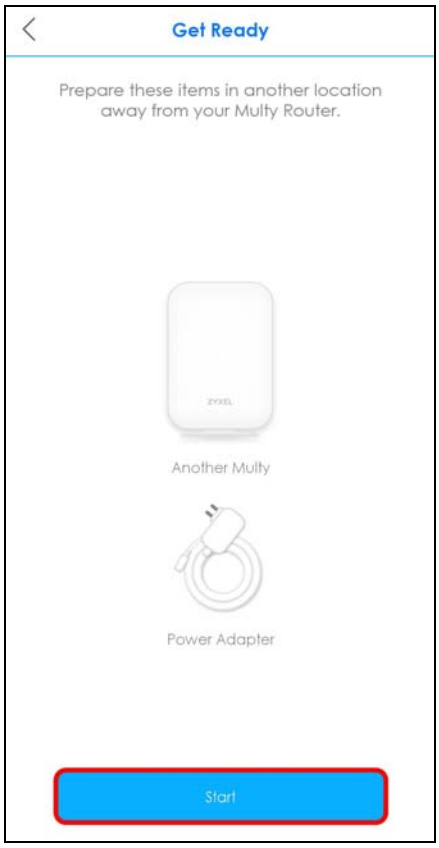


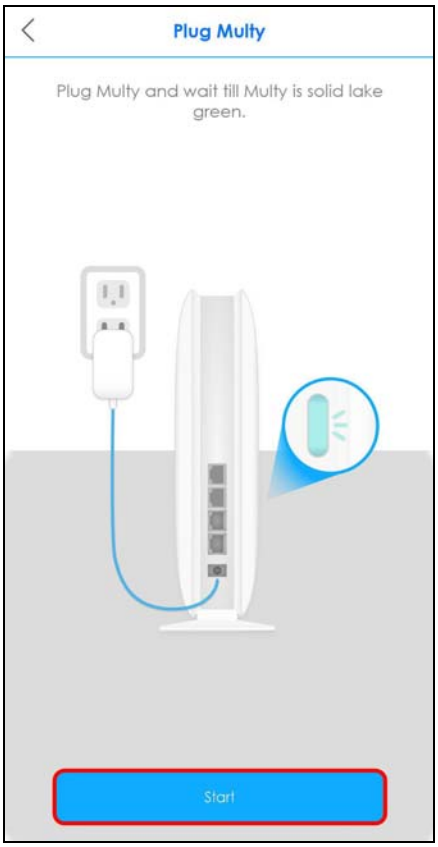
7 After the first Multy Device is installed, click **No, I'm Done** to finish the installation. Otherwise, tap **Add Multy** to add a second Multy device.

Note: You can skip this step and add another Multy Device later. See Section 3.7 on page 49 for more information.


Add Another Multy?
Living Room
Multy Router
Add Multy
No, I'm Done

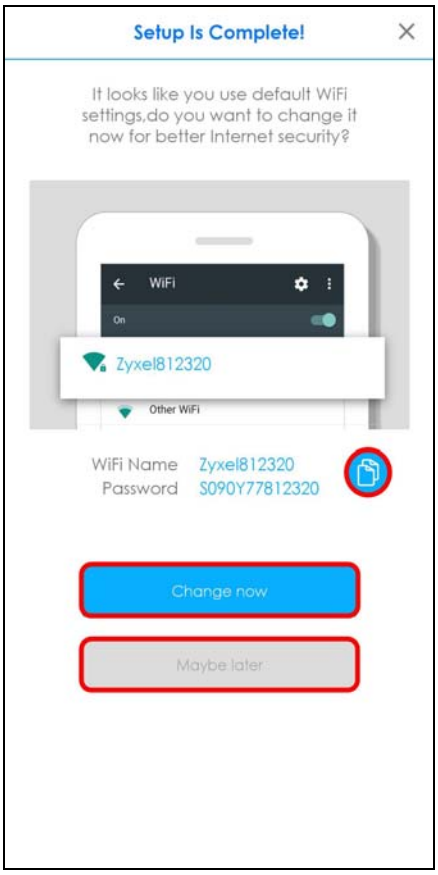
8 The following **Get Ready** screen appears, after you click **Add Multy**. Click **Start** and then click the **WPS** button on the extender to start pairing.





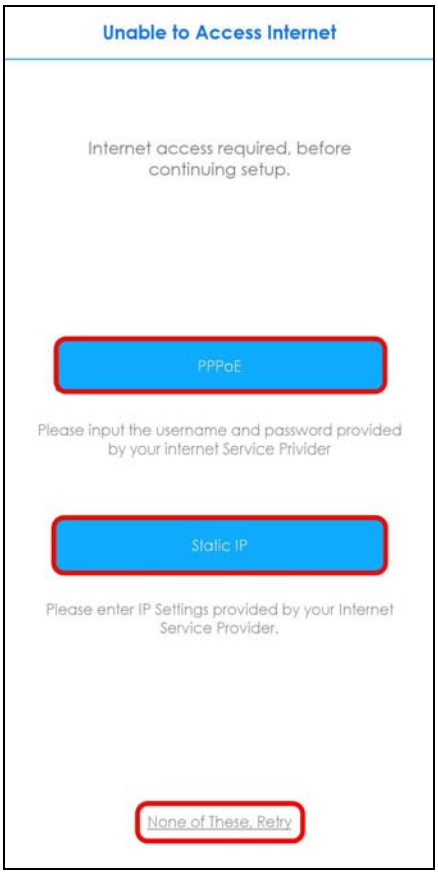
9 When the WiFi setup is completed for all your Multy Devices, you can copy the password by pressing the Copy icon ( ) and use it with the WiFi name to connect your smartphone to the Multy Site.

Multy app detects you are using the default **WiFi name** and **Password**. Click **Change now** to change your WiFi name and password. Otherwise, click **Maybe later** to change your WiFi name and password later.


Setup Is Complete!
It looks like you use default WiFi settings,do you want to change it now for better Internet security?
WiFi
On
Zyxel812320
Other WiFi
WiFi Name Zyxel812320
Password S090Y77812320
Change now
Maybe later

10 A **Multy Site** is a collection of Multy Devices with exactly one Multy Device acting as the primary Multy and the rest acting as extender Multys. After completing the setup, the **Multy Site** screen will be displayed, allowing you to monitor your Multy Devices and Multy WiFi System. It shows whether the Multy Devices in this Multy Site are on. It also shows the number of wireless clients currently connected to the Multy Devices.

Note: If your Multy Device is connected to a modem or router but is unable to access the Internet during the installation process, you will see the following screen. Make sure your smartphone is connected to your broadband router's WiFi network and then tap **None of These, Retry**. If applicable, configure **PPPoE** or **Static IP** settings provided by your ISP.

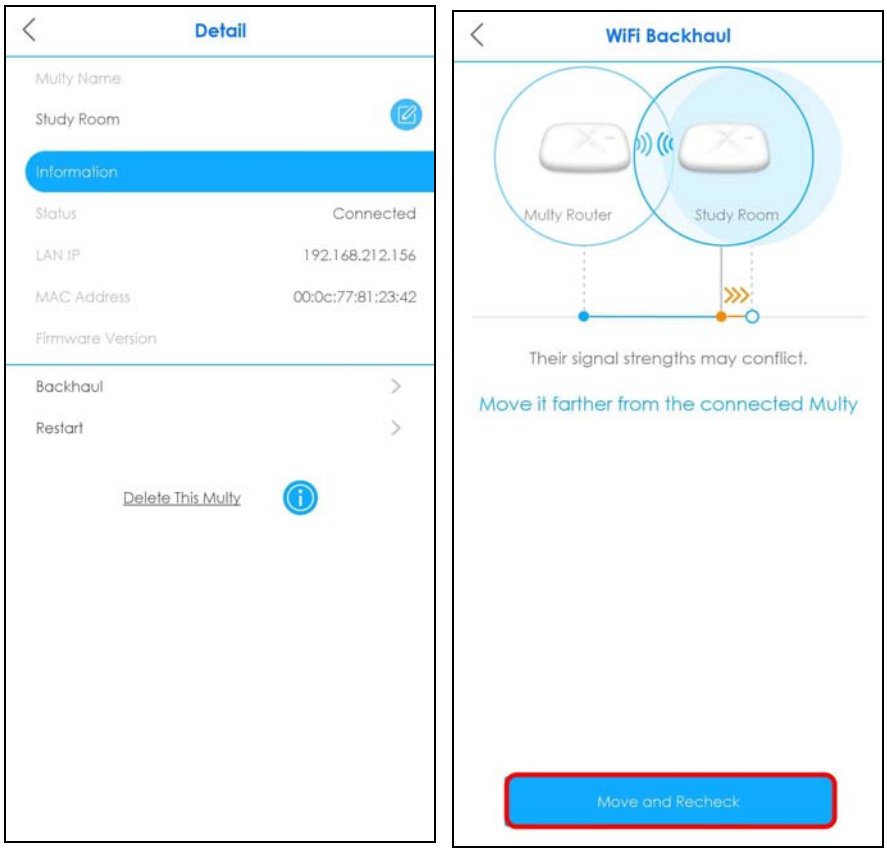


3.4 Check Your Multy-to-Multy Signal Strength

You can always check the signal strength between your extender and primary Multy to see if they need to be moved closer or farther apart.

1 From the **Multy Site** screen, tap the extender Multy you want to check.

2 The **Detail** screen will be displayed. Tap **Backhaul**. The signal strength test will then be carried out. You may move the extender and then tap **Move and Recheck** to recheck the signal strength.



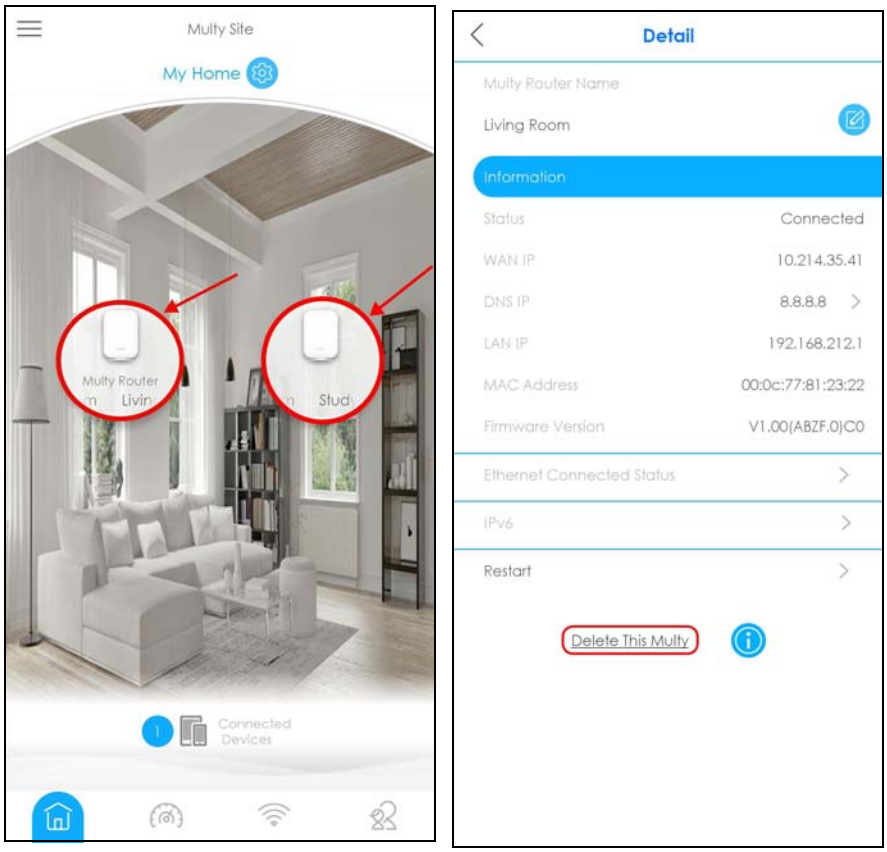
3.5 Remove a Multy Device

If a Multy Device is no longer in use, you can remove it from the Multy Site.

On the Multy Site screen, tap the Multy Device you want to remove. The **Detail** screen will be displayed. Tap **Delete This Multy** to remove the device.

Note: Before pressing the **Reset** button, click **Delete The Multy** on the **Detail** screen.

Note: If the primary Multy is removed on the **Detail** screen, the assigned roles of the mesh network, including the extenders, will be reset to the default settings.

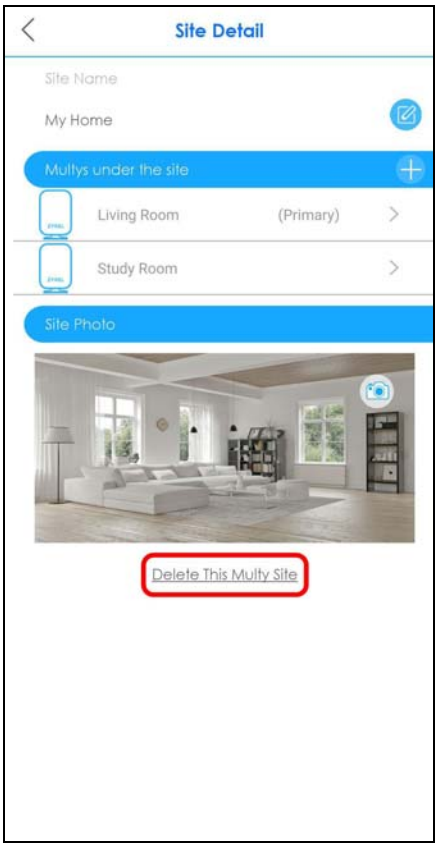


3.6 Remove a Multy Site

All Multy Devices in the Multy Site will be reset after you delete the Multy Site.

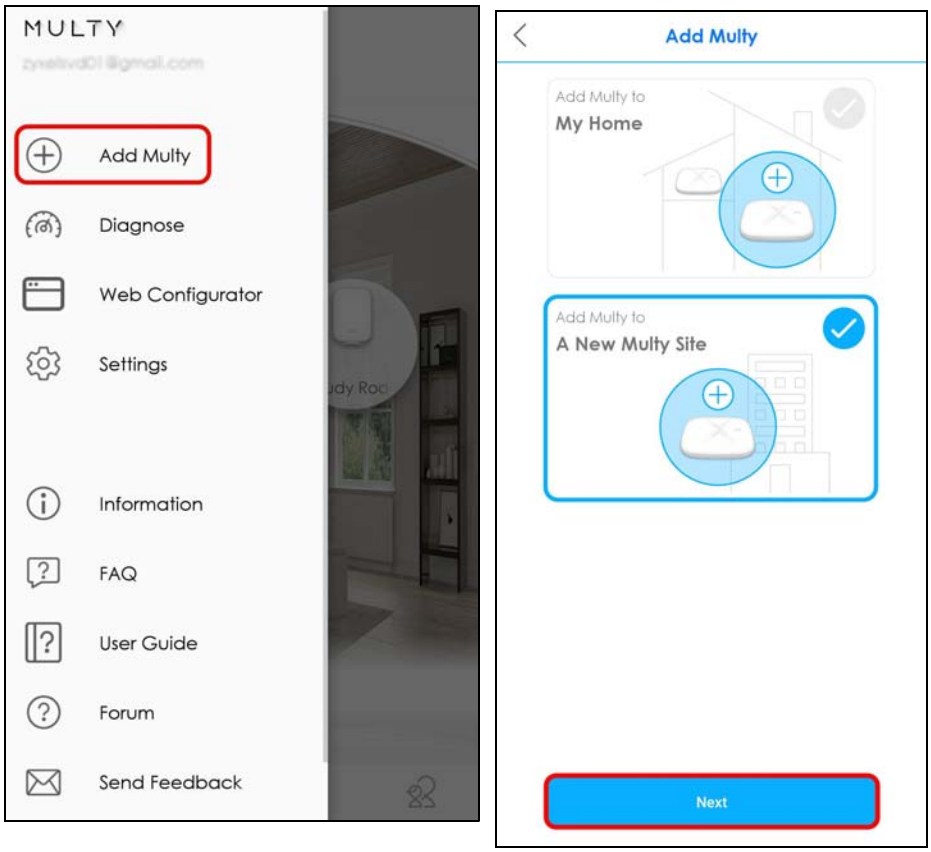
1 From the **Multy Site** screen, tap the Settings icon ( ) to open the **Site Detail** screen.

2 Tap **Delete This Multy Site** to remove the Multy WiFi System.

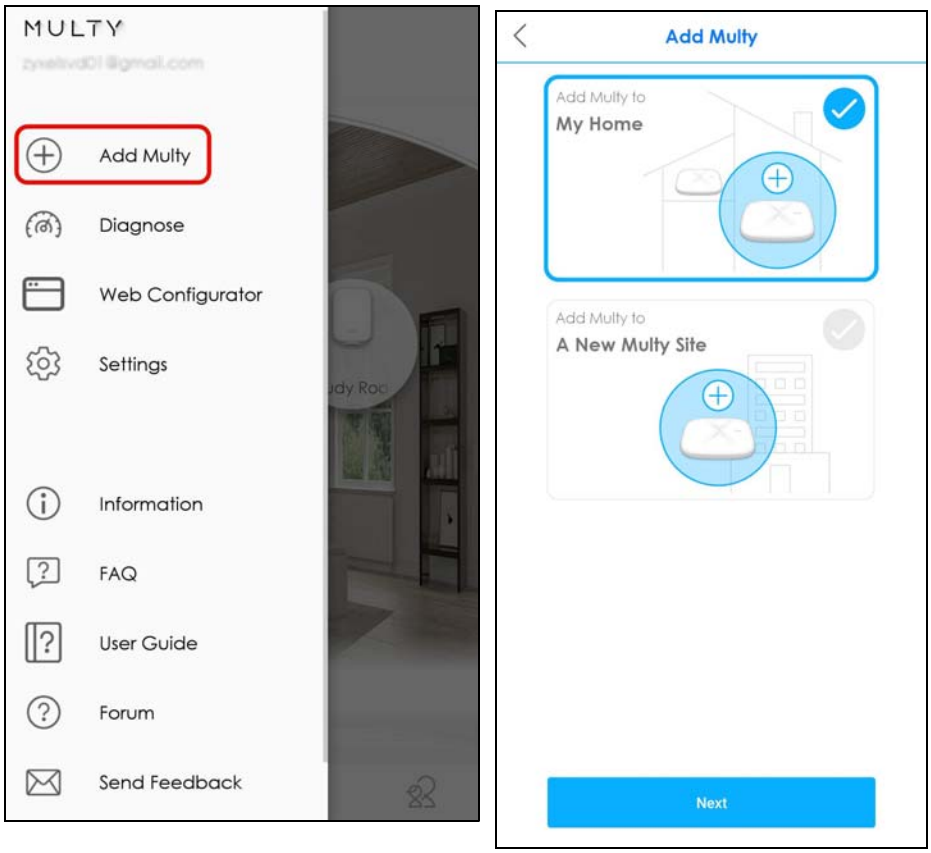


3.7 Add a Multy Device to a New Site

1 To add a Multy Device to a new site, go to the **Menu** screen and then click **Add Multy**. The **Add Multy** screen appears. Select **Add Multy to a New Multy Site** and then click **Next** to continue. The **Get Ready** screen appears. Please refer to Section 3.3 on page 34 for more information about adding a Multy device.



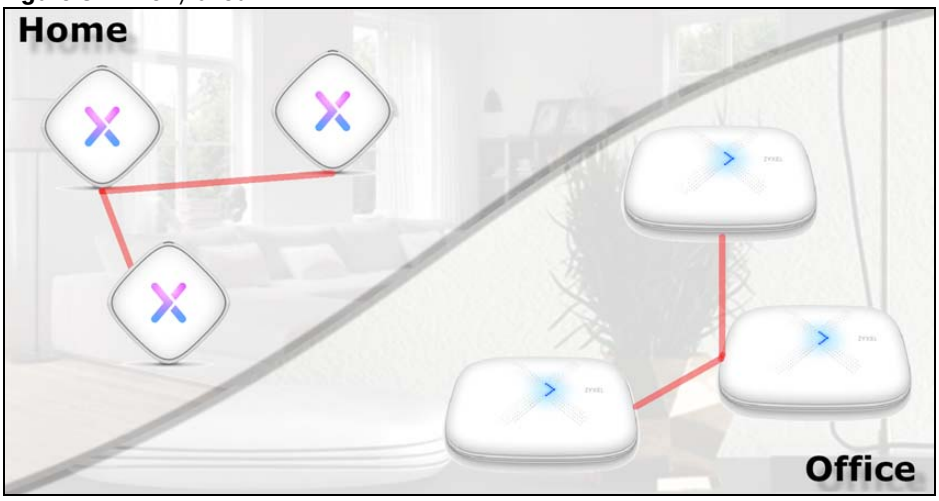
2 To install a second Multy device to this site. Click **Add Multy to My Home**. Click **Next**. Follow the prompts and finish the installation.



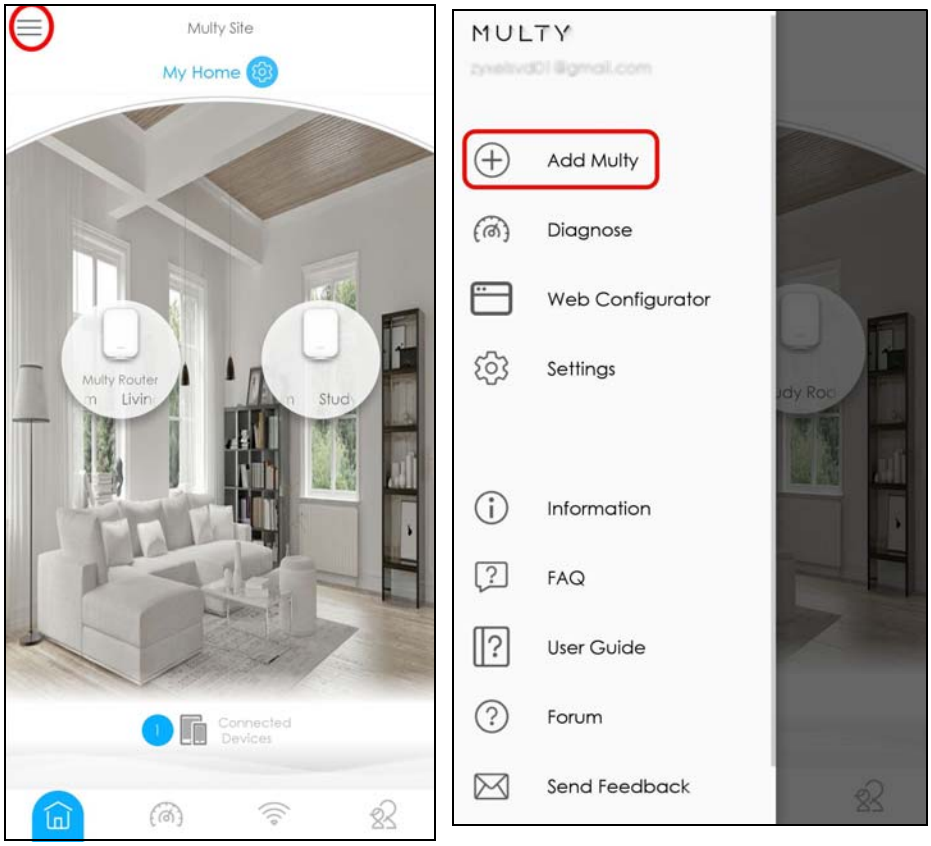
3.8 Install a Second Multy Site

You can manage multiple Multy Sites using the Zyxel Multy app. In the figure below, the app manages two separate Multy Sites with one being installed at home and another in the office.

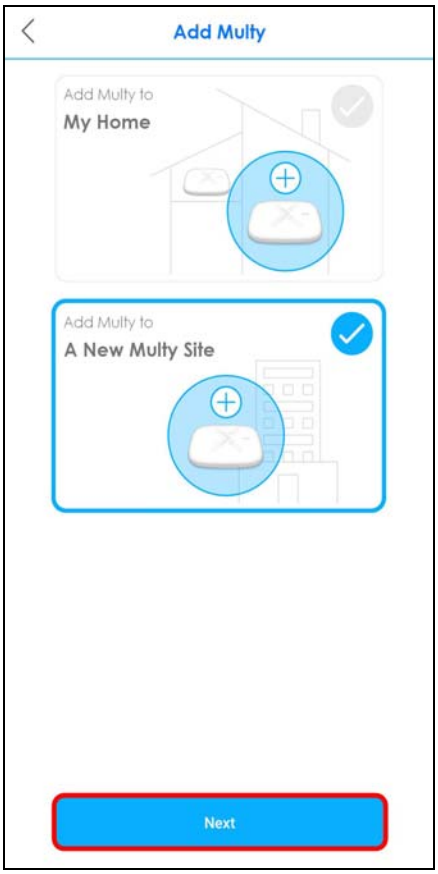
Figure 31 Multy Sites



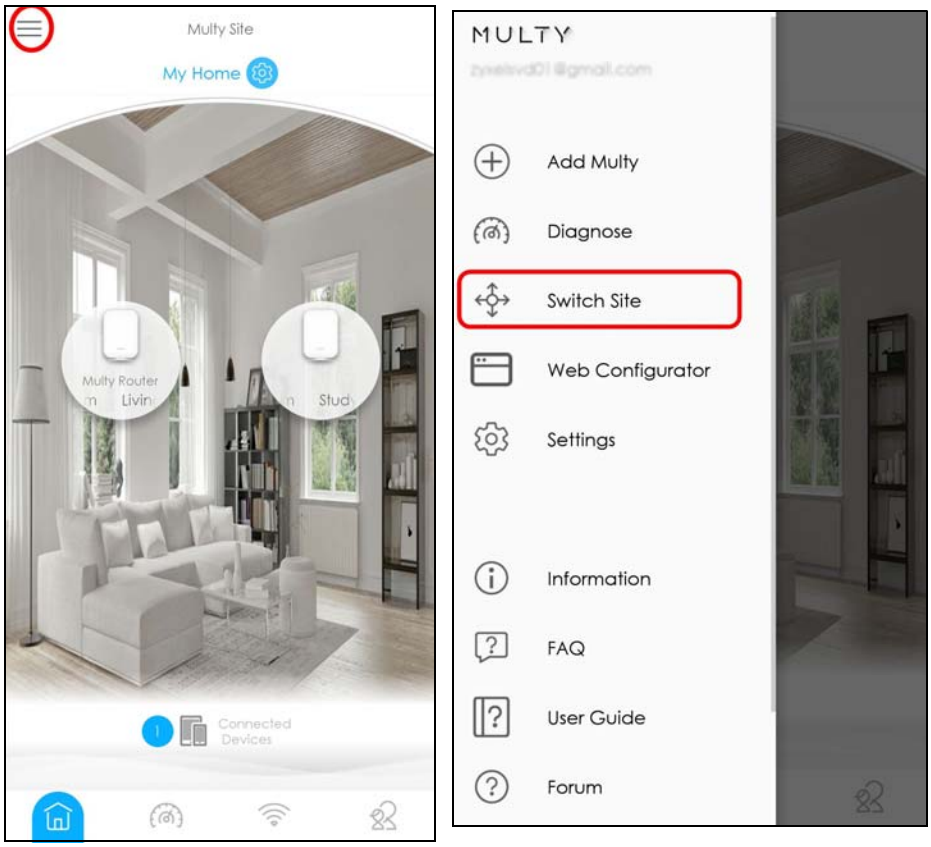
1 Tap the Menu icon in the upper-left to open the navigation panel. Tap **Add Multy**.



2 Tap **A New Multy Site** and **Next** to set up another Multy WiFi System. Follow the instructions in Section 3.3 on page 34 to complete the setup.

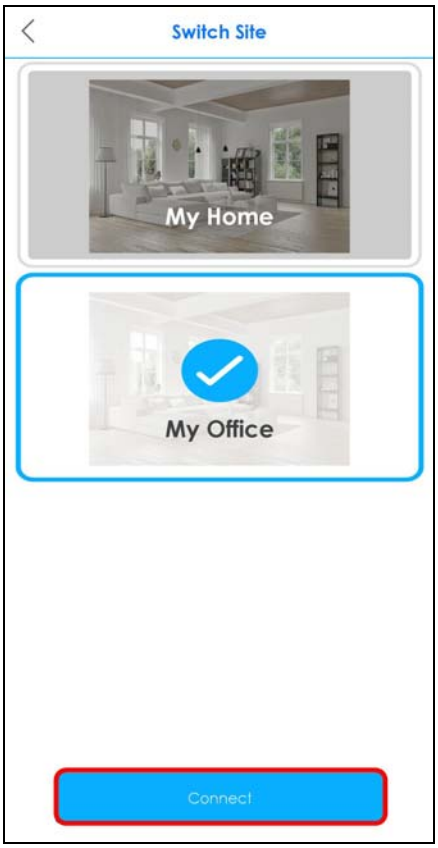


3 To manage a different Multy Site, first tap **Switch Site** from the navigation panel.



4 Select the Multy Site you want to manage and then tap **Connect**.

Note: The **Switch Site** option is available only when you have more than one Multy Site.

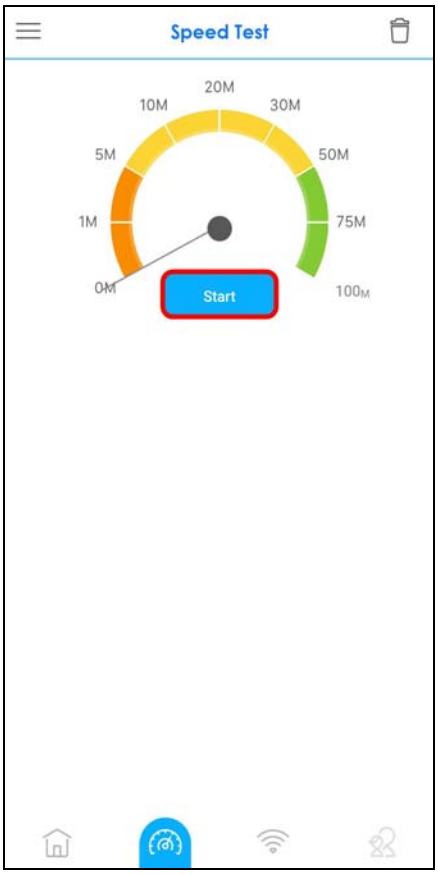


3.9 Test Your Smartphone Connection Speed

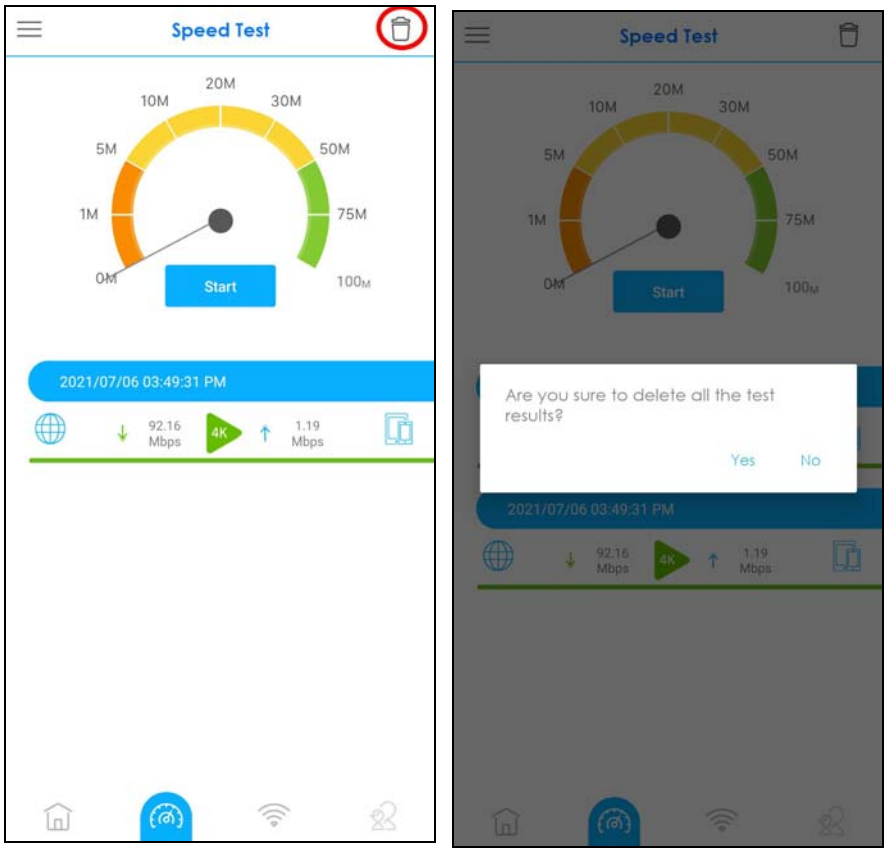
You can run a speed test to check the Internet connection speed at which you send and receive data from your smartphone via the Multy Device.

1 Tap the Speed Test icon ( ) of the Multy Site.

2 Tap **Start** to perform the test. The meter will show data rates for both upstream and downstream traffic.



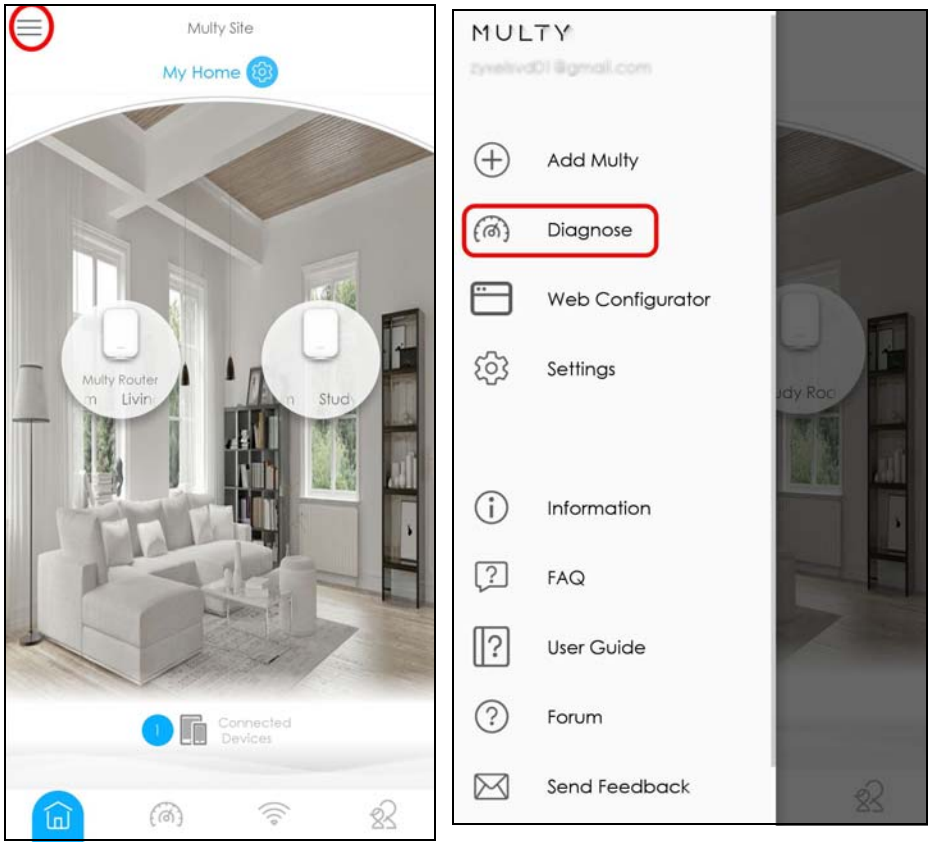
3 The following screens show the results. You can tap the Remove icon ( ) to delete all records.



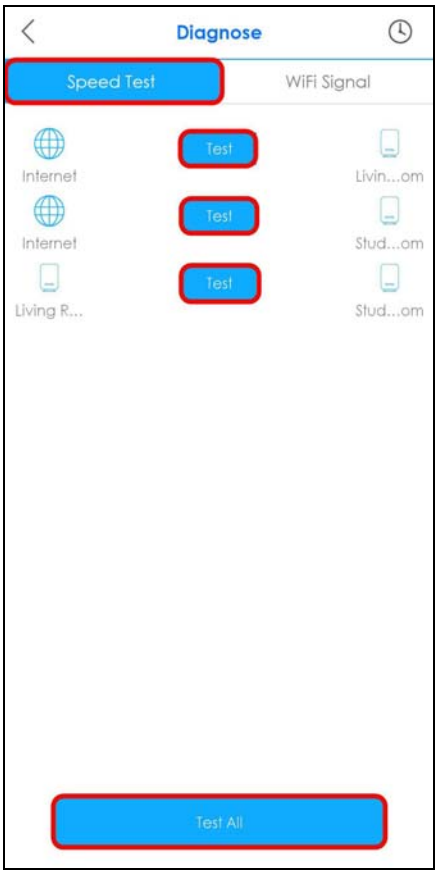
3.10 Test Your Multy Device Connection Speed

With the Zyxel Multy app, you can check the speed of the connection between your Multy Device and your broadband modem or router. You can also check the connection speed between two Multy Devices.

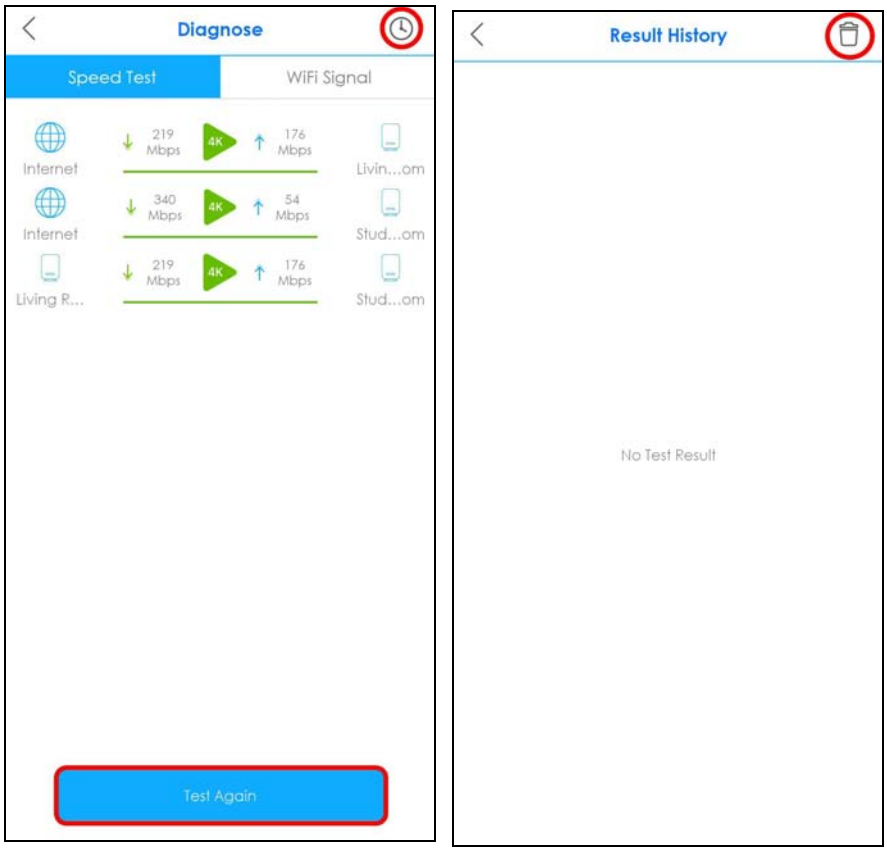
1 Tap the Menu icon in the upper-left to open the navigation panel. Tap **Diagnose**.



2 Tap **Speed Test** and the **Test** or **Test All** button to perform a test. The results will show data rates for both upstream and downstream traffic.



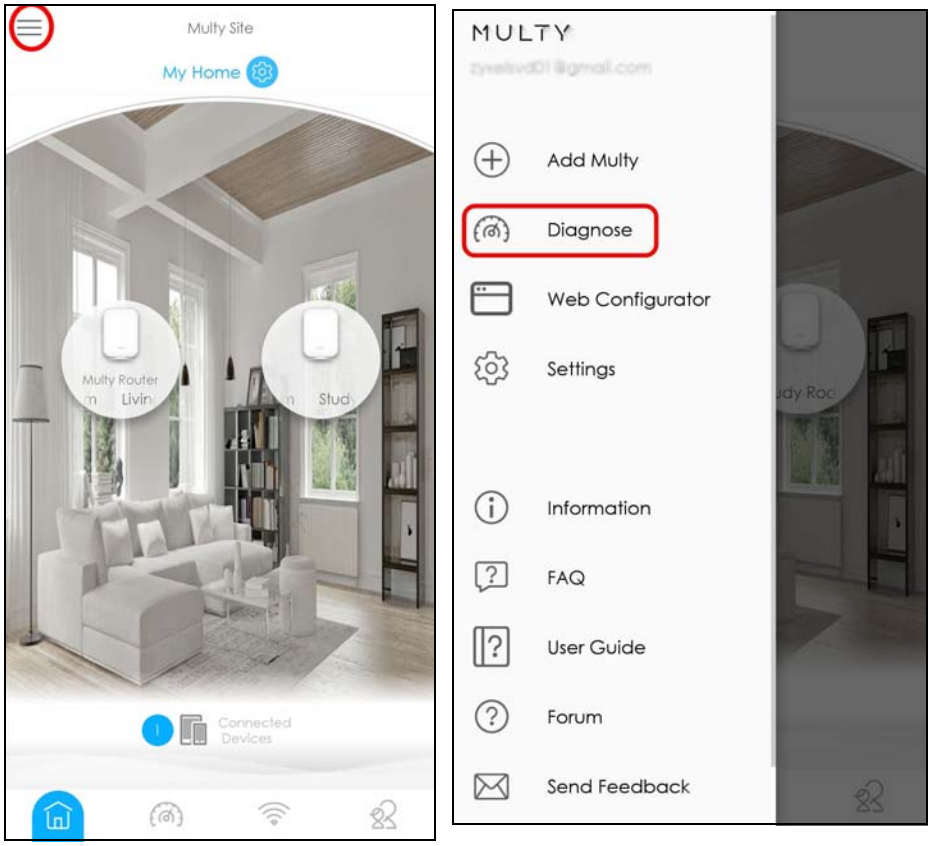
3 Tap **Test Again** to show the **Test** buttons. To view the previous test results, tap the History icon ( ). You can tap the Remove icon ( ) to delete all records.



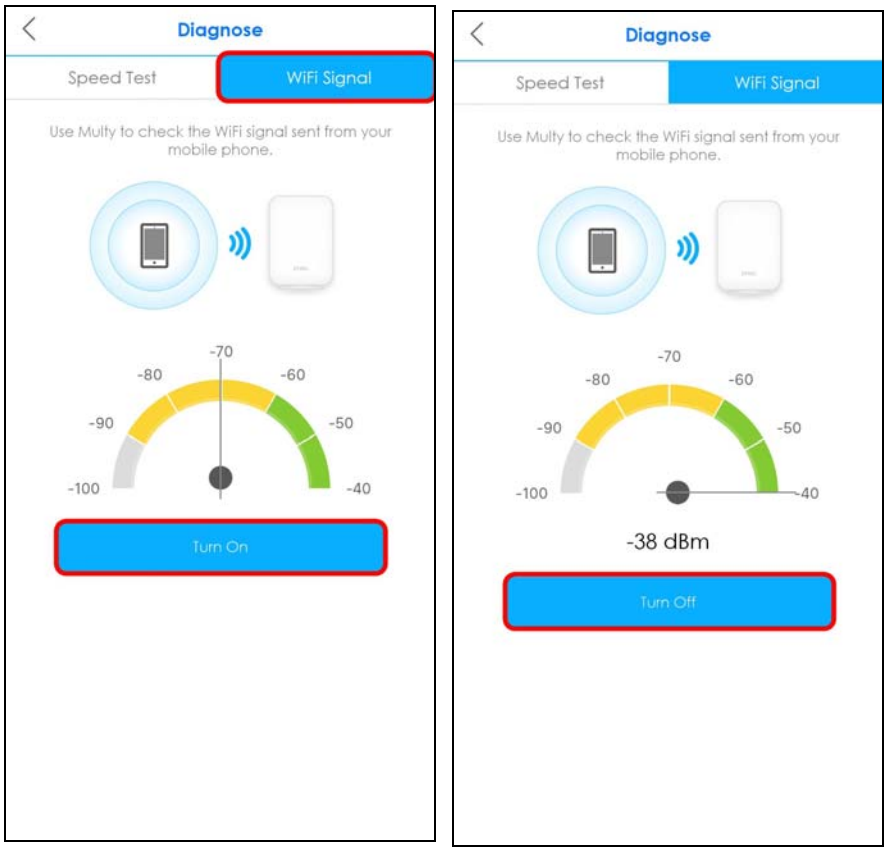
3.11 Measure Your WiFi Signal Strength

When you need to install a new Multy Device, you can perform a signal check to decide where to place it. To use your smartphone to measure your WiFi signal strength, wirelessly connect the smartphone to the Multy Site first. Generally, signal strength is better when you are closer to the WiFi source.

1 Tap the Menu icon in the upper-left to open the navigation panel. Tap **Diagnose**.



2 Tap **WiFi Signal** and then tap the **Turn On** button to perform a check. Tap **Turn Off** to stop the process. A decent WiFi signal would not go below –70 dBm (–70 dBm to –100 dBm).

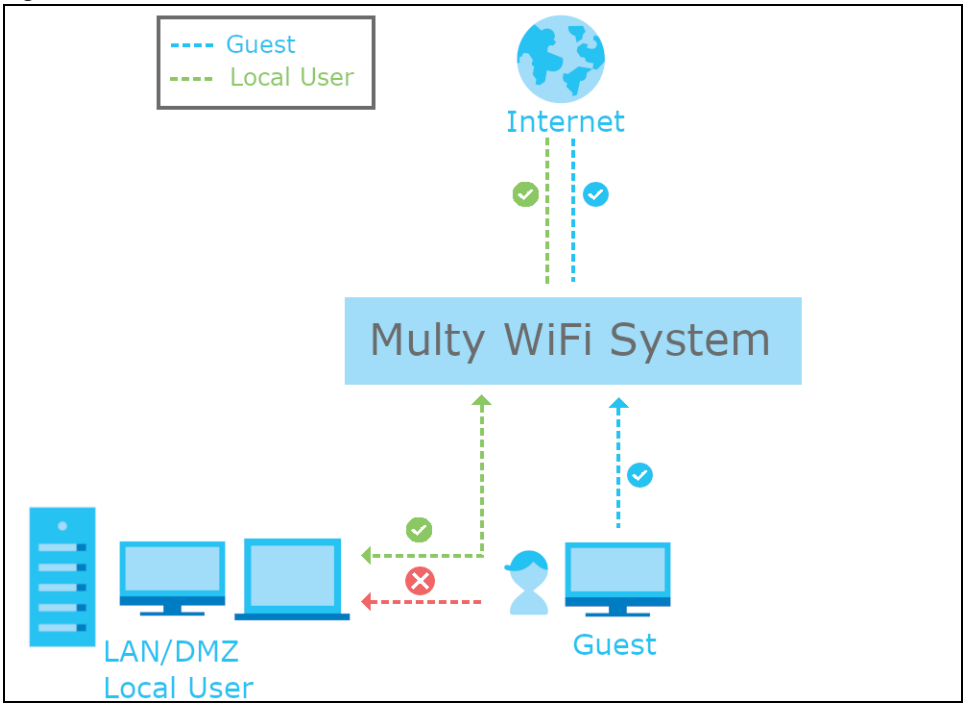


3.12 Enable or Disable Guest WiFi

After the Multy Site is set up, you can create a separate WiFi network for your guests. These guest WiFi settings will be applied to all Multy Devices in the same Multy Site.

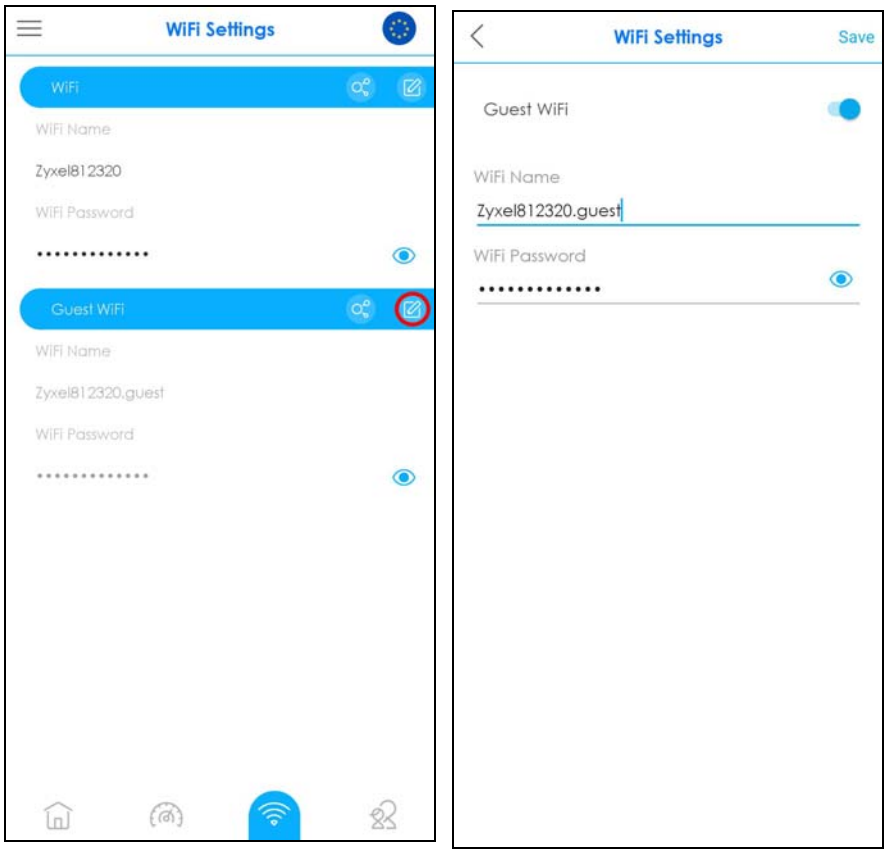
Devices connected to the guest WiFi can access the Internet but they cannot access other devices connected to the Multy Site, as shown in the figure below.

Figure 32 Guest WiFi



1 Tap the WiFi Settings icon ( ) of the Multy Site.

2 Tap the Edit icon ( ) of the **Guest WiFi** settings. Enable **Guest WiFi** and enter the guest **WiFi Name** (SSID) and **WiFi Password**. Tap **Save**. Then tap **Confirm**.



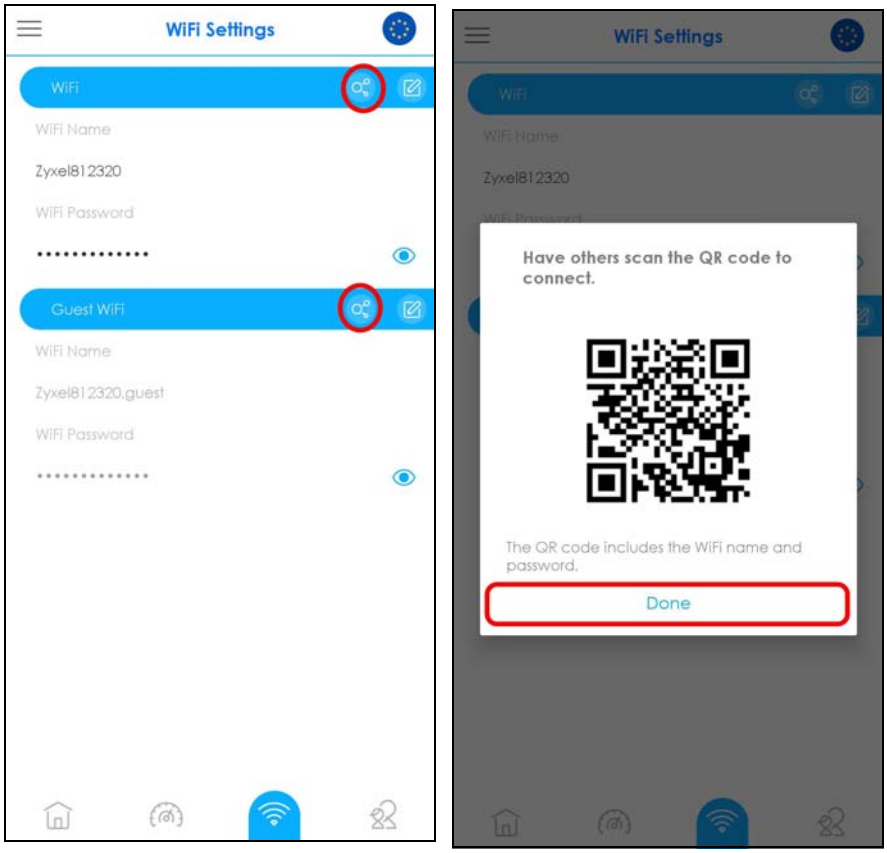
3.13 Share WiFi Name and Password with a QR Code

You can use the app to create a QR code with your WiFi network name and password. By printing and placing the QR code somewhere accessible, you can let your friends or guests scan the QR code and join the WiFi network directly without revealing your actual WiFi password.

1 Tap the WiFi Settings icon ( ) of the Multy Site.

2 Tap the Share icon ( ) of a WiFi network to create a QR code of the WiFi network name and password which you can share with others. Take a screenshot of the QR code if you want to save and print it. Tap **Done** once you are finished.

Note: The Share icon ( ) is available after you enable **WiFi** or **Guest WiFi** and set a WiFi name and password for this WiFi network.



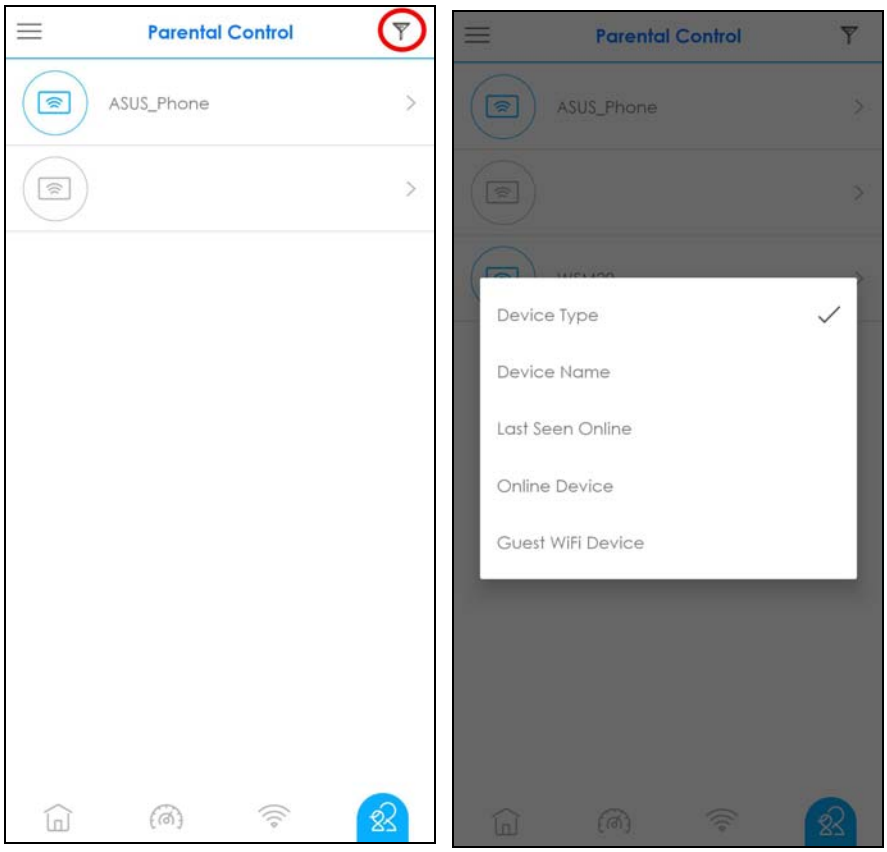
3.14 Set a WiFi Schedule for Clients

By creating a schedule profile, you can schedule the Multy Site to automatically disable the WiFi access of selected clients for preset periods of time.

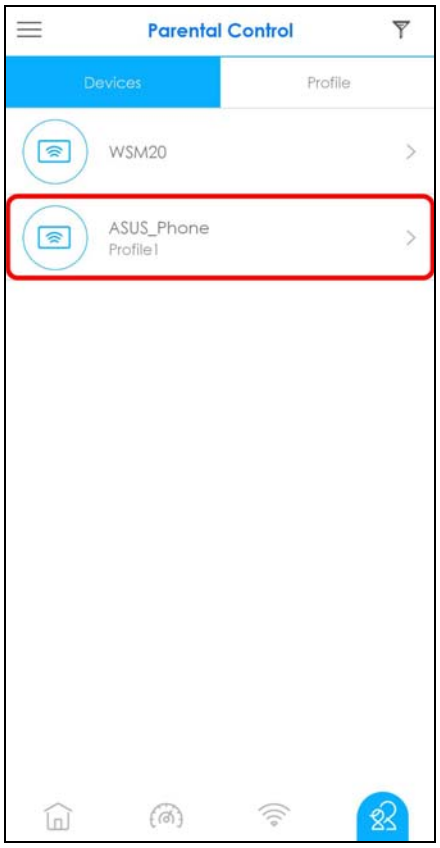
Note: You can group clients by applying the same schedule profile to them. This allows you to block or allow access or set a schedule for all client devices in the same group.

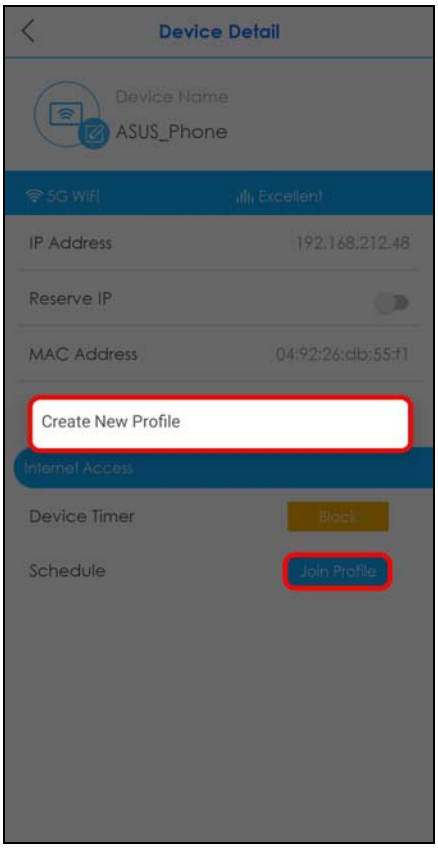
1 Tap the Parental Control icon ( ) of the Multy Site.

2 Tap the Filter icon and select how you want to sort the devices in the list.

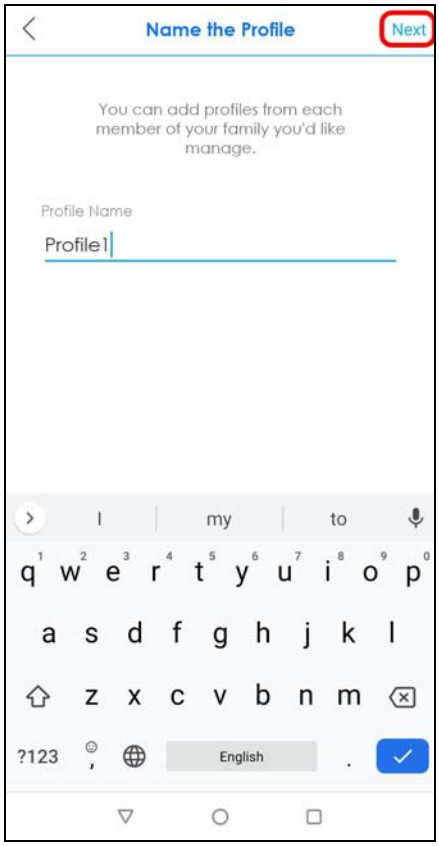


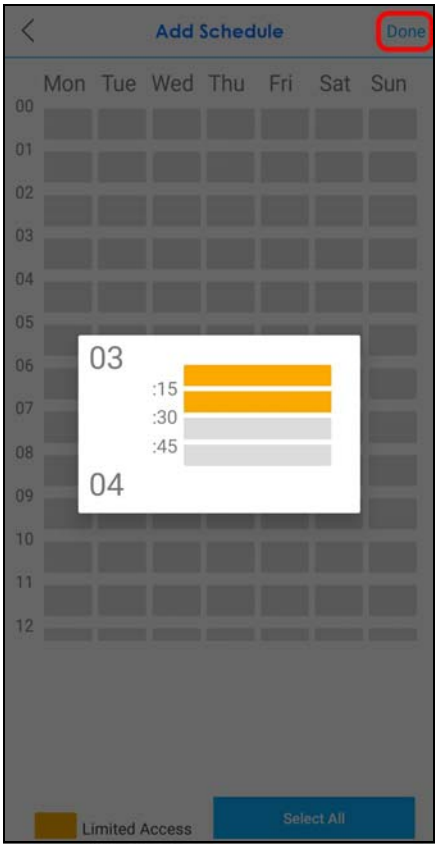
3 Tap a client from the device list to view the client device information. Tap **Join Profile** and then select **Create New Profile** to create a new profile or select a profile to apply a pre-configured schedule profile to the client.


Parental Control
Devices
Profile
WSM20
ASUS_Phone
Profile1


Device Detail
Device Name
ASUS_Phone
5G WiFi
Excellent
IP Address
192.168.212.48
Reserve IP
MAC Address
04:92:26:db:55:f1
Create New Profile
Internet Access
Device Timer
Block
Schedule
Join Profile

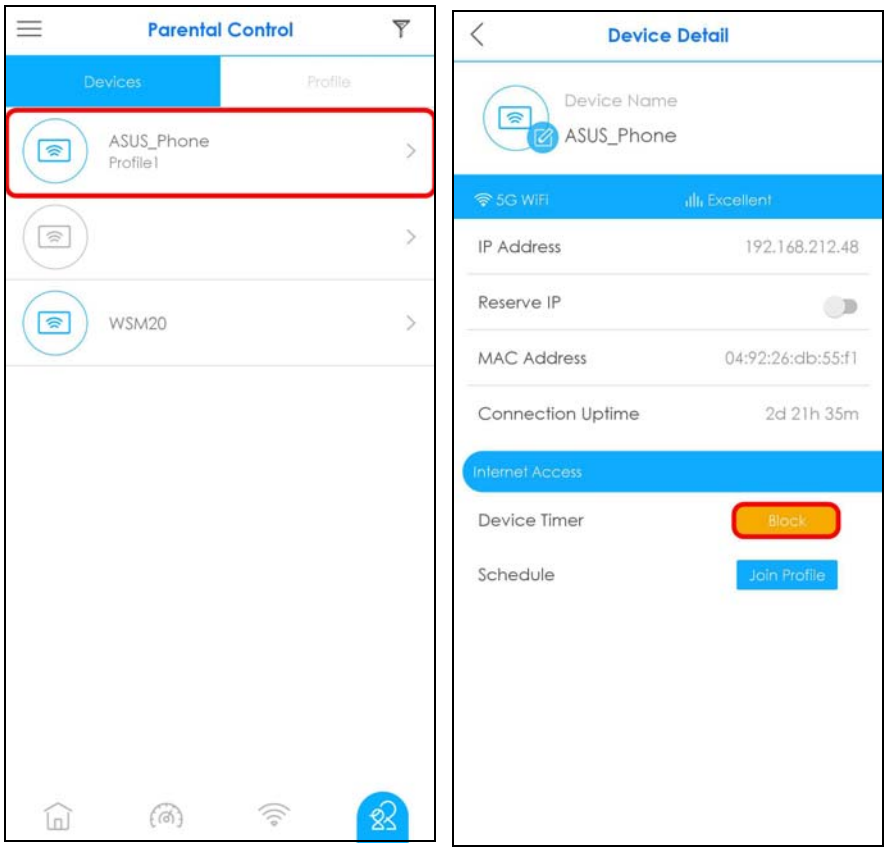
4 If you want to create a new schedule, tap **Create New Profile** shown in the previous step. After you create a profile, name the profile, and then tap **Next**. Tap the gray blocks to specify the time periods during which the client will be blocked from accessing the Internet. If you want to plan a schedule in 15-minute intervals, tap a time slot and hold for 2 or 3 seconds until a small window pops up. To select an entire row or column, tap the row or column label. Tap **Done** to save your settings.



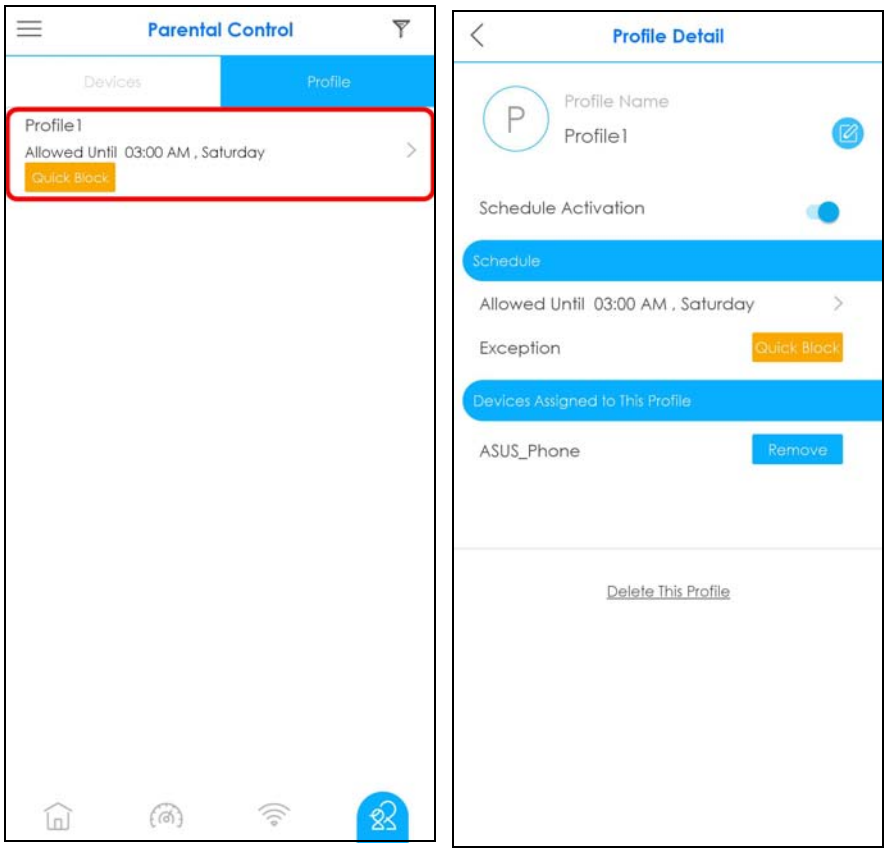


5 The applied profile name will then display on the **Parental Control** > **Devices** screen.

Note: The Device Timer **Block** button is only available if the clients are not in any schedule profile.



6 The **Parental Control** > **Profile** > **Profile Detail** screen becomes available after a schedule profile is created.



3.15 Pause Internet Access for an Individual Client

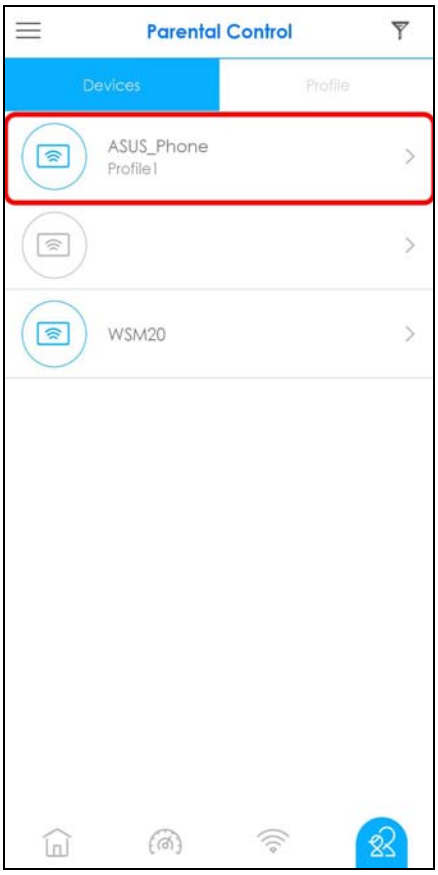
You can set a timer to block a specific client from accessing the Internet without having to create a schedule. The timer is effective only once.

Note: You can only set a timer to block Internet access on the clients that do NOT belong to any schedule group.

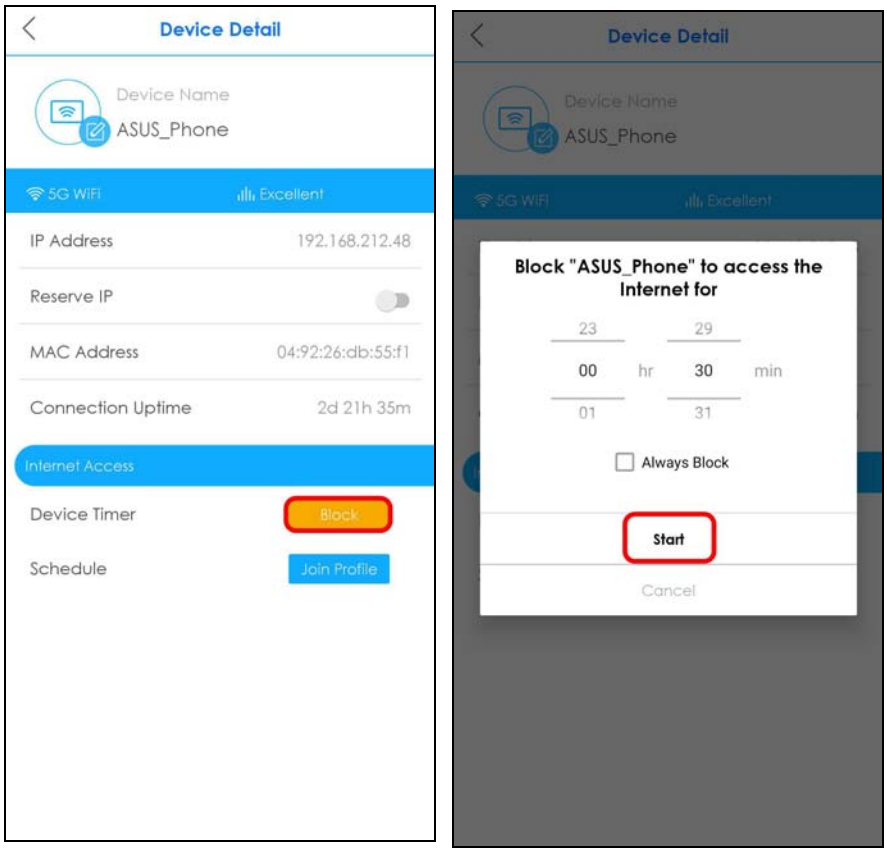
1 Tap the Parental Control icon ( ) of the Multy Site.

Multy Site
My Home
Multy Router
Livin
Stud
Connected
Devices

2 Tap a client from the **Devices** list to view the client device information.



3 To block the selected client device, tap **Block** and specify a time period in hours and minutes. Tap **Start** to start the timer and block the client immediately.



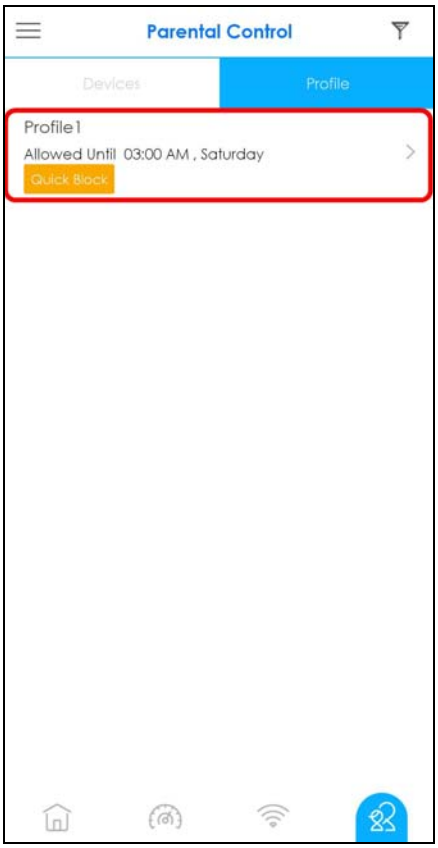
3.16 Pause or Resume Internet Access for a Group

You may want to manually block a group of client devices from accessing the Internet immediately and resume it later.

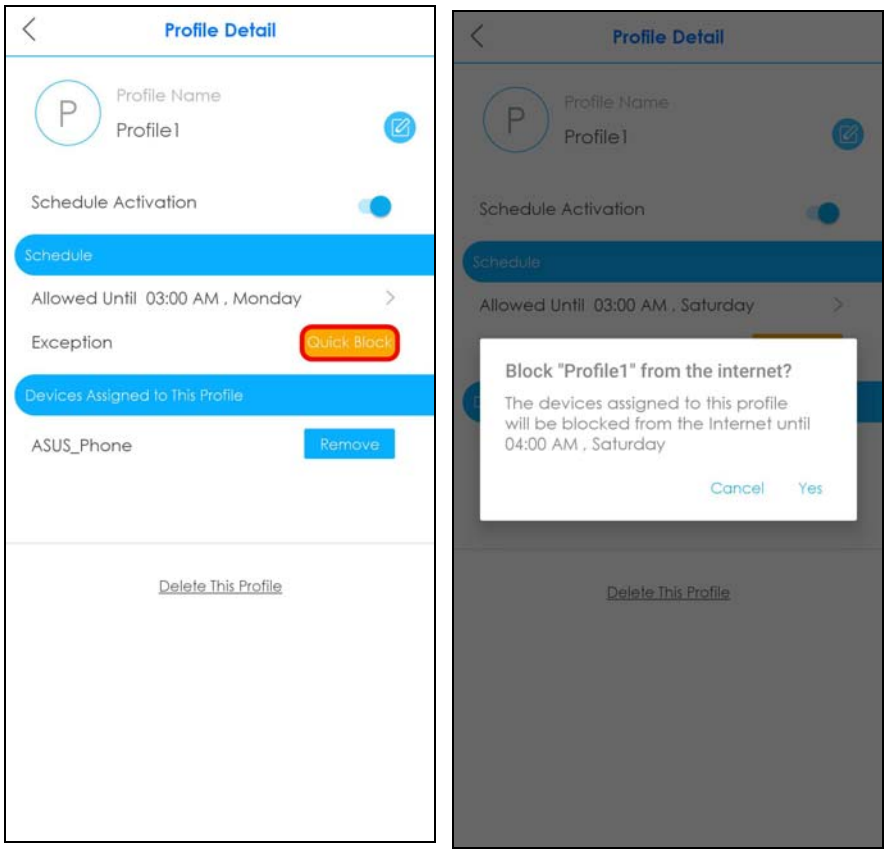
Note: You should already have created a schedule profile and applied the profile to client devices to group them.

1 Tap the Parental Control icon ( ) of the Multy Site. Tap **Profile** to view the schedule profiles previously created in the Multy Site. On the **Parental Control > Profile** screen, tap a profile's **Quick Block** button to block or resume network access at once.

Multy Site
My Home
Multy Router
Connected
Devices


Parental Control
Devices
Profile
Profile1
Allowed Until 03:00 AM , Saturday
Quick Block

2 Otherwise, select a profile from the profile list and then tap the **Quick Block** button on the **Profile Detail** screen to pause Internet access for that specific group.

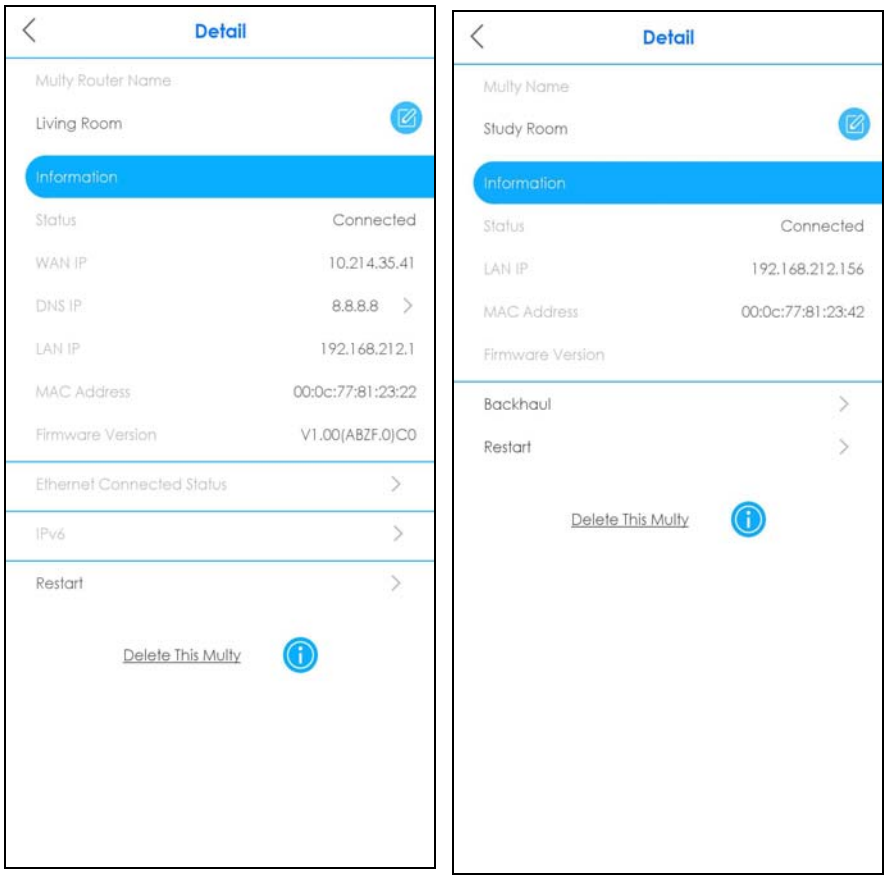


3.17 Check your Multy Device's Configuration Details

After configuring your Multy Device, you can view your Multy Device settings on the **Detail** screen.

1 Tap a Multy Device on the **Multy Site** screen to open its **Detail** screen.

2 The figure on the left appears if you tap on the Multy Device acting as the primary Multy. The figure on the right appears if you tap on an extender Multy. You can configure the DNS IP address, the IPv6 address, and the Ethernet connection status on a primary Multy screen.

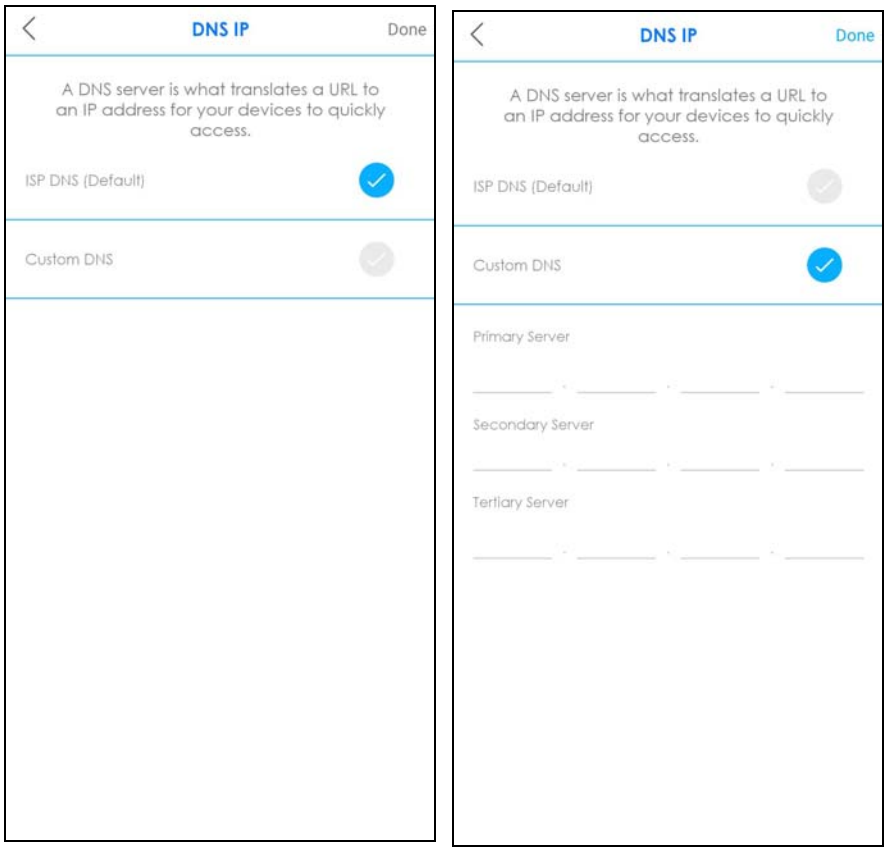


3.18 Use Custom DNS Server

A DNS server is a database that allows you to translates a domain name into an IP address to access the Internet. You can choose to specify a DNS server for your Multy Site.

1 Tap the primary Multy on the **Multy Site** screen to open the **Detail** screen and then tap **DNS IP**.

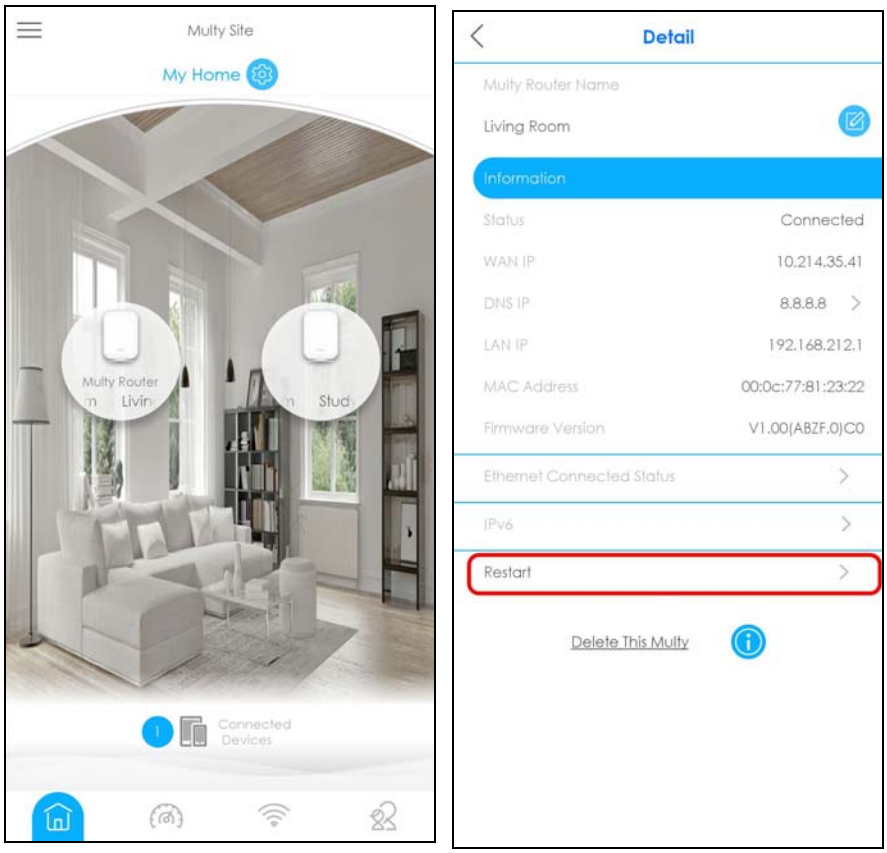
2 Tap **ISP DNS (Default)** to use the default DNS server. Otherwise, tap **Custom DNS** and enter a primary, secondary, and tertiary DNS server. Tap **Done** to apply the changes.



3.19 Restart Your Multy Device

If you need to restart your Multy Device, you can do it remotely using the **Detail** screen.

On the **Multy Site** screen, tap the Multy Device you want to restart. The **Detail** screen will be displayed. Tap **Restart** to restart this device.

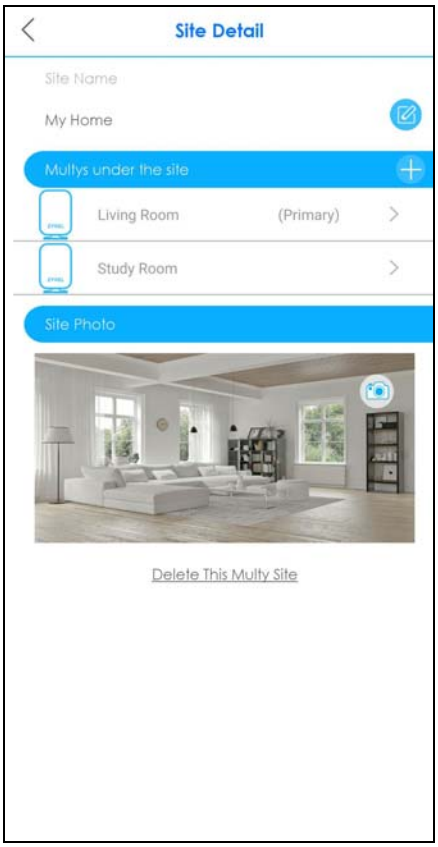


3.20 Change the Name or Picture of a Multy Site

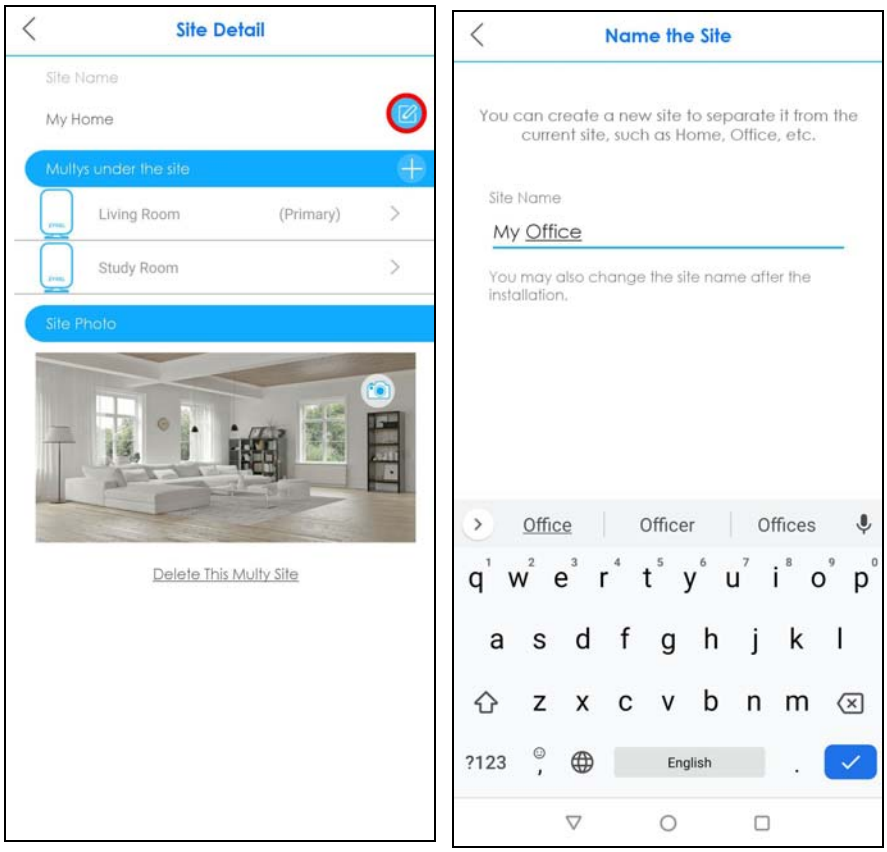
You can rename a Multy Site or change the background picture that is displayed on the Multy Site main screen by following these steps.

Note: To restore back to the default background picture of a Multy site, you need to remove the current Multy site and then recreate a new site. Please refer to Section 3.6 on page 47 for more information.

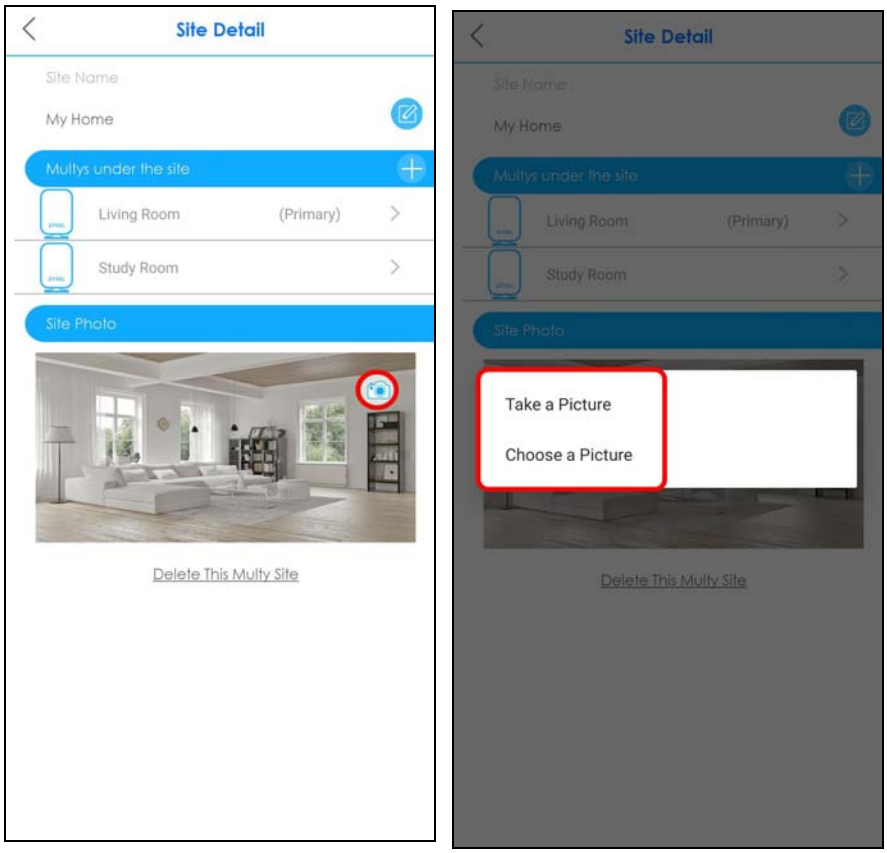
1 From the **Multy Site** screen, tap the Settings icon ( ) to open the **Site Detail** screen.



2 Tap the Edit icon ( ) of **Site Name** to give the Multy Site a new name.



3 Tap the Camera icon ( ) to change the background picture of your Multy Site. Tap **Choose a Picture** to choose an existing picture on your phone. Otherwise. tap **Take a Picture** to use your phone camera to take a picture for your Multy Site. Crop the picture to a proper size and select the check mark to save the changes. Your background picture is now replaced with the new one.

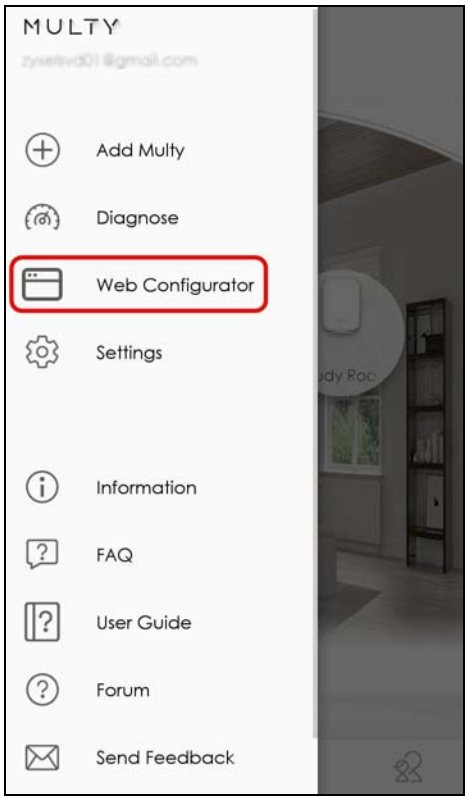


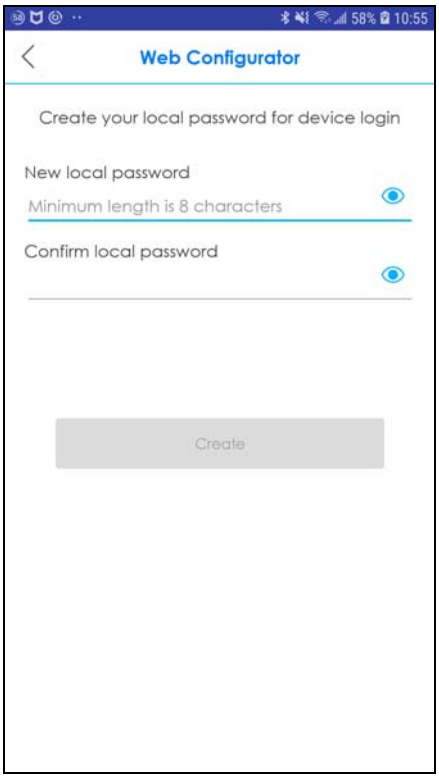
3.21 Create or Change Your Web Configurator Password

This section allows you to create or change your web configurator password through the Multy app. SeeTable 1 on page 9 for more information about the Web Configurator.

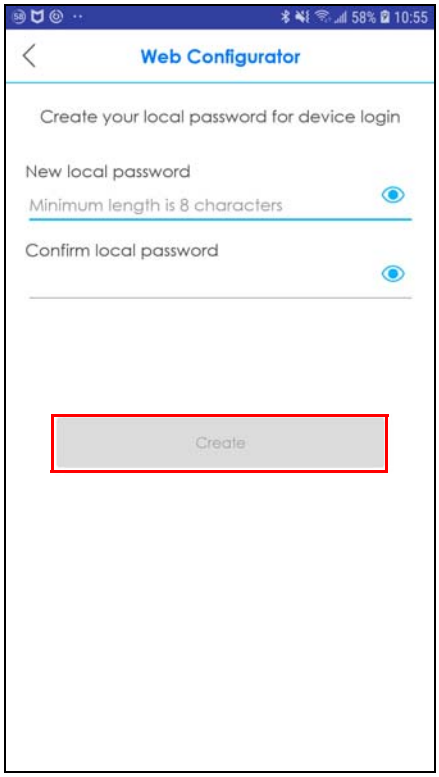
1 From the Multy Site screen, tap the Web Configurator icon ( ). The **Web Configurator** screen displays. Enter your new local password and re-enter it to confirm. The password should contain at least eight alphanumeric characters.

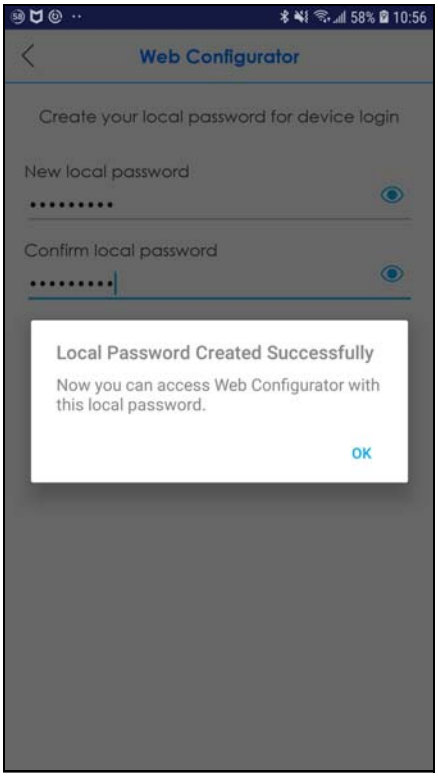
Note: Enter a new password of 8-32 alphanumeric characters. The following special characters listed in the square brackets [\"'`<>^$&] and emojis are not allowed.



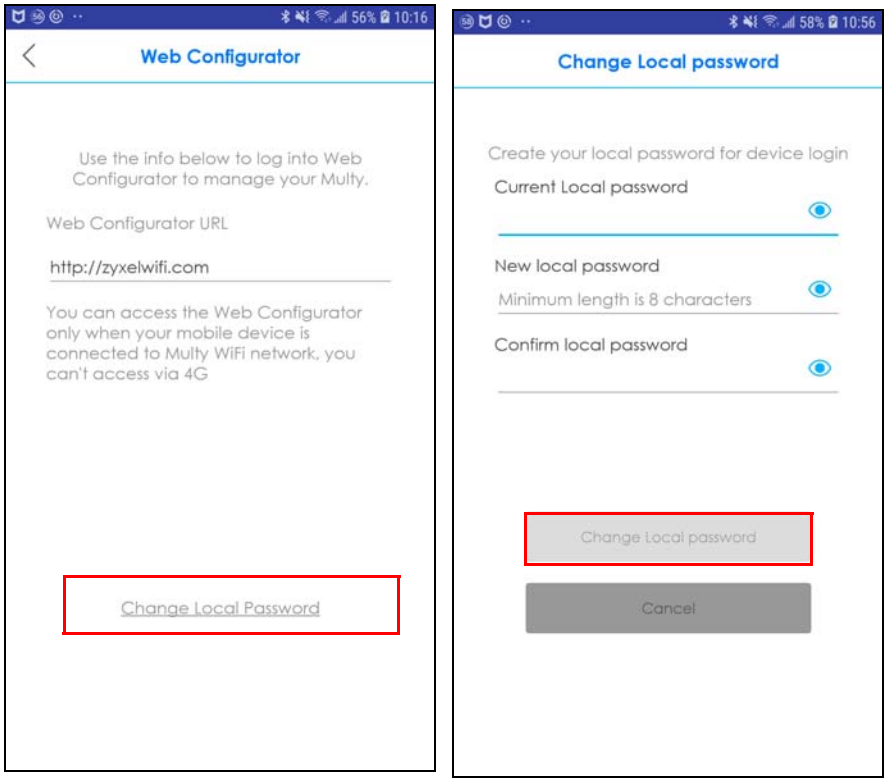


2 Tap **Create** to save the changes. Tap the Visibility icon ( )to see your password. Tap **OK** to close this screen.





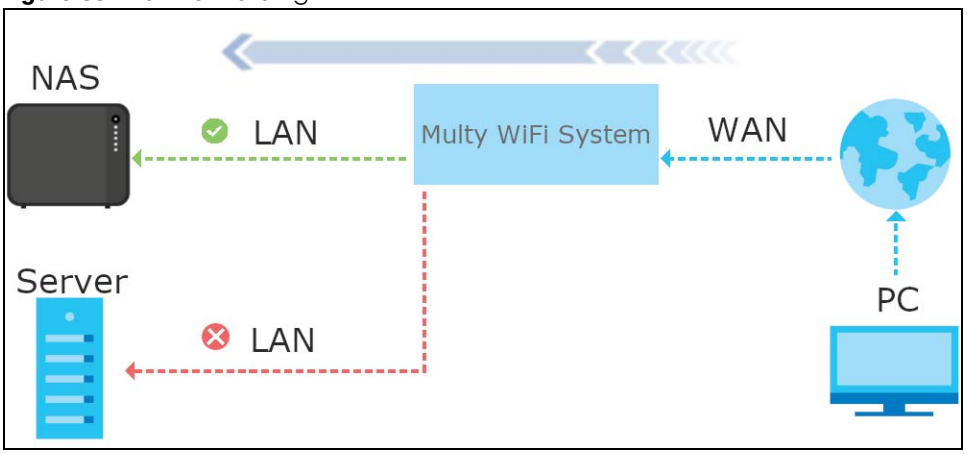
3 The **Web Configurator** screen displays after the set up is completed. Tap **Change Local Password** if you want to change your local password.
The **Change Local Password** screen displays. Enter your **Current Local Password**, and then enter your **New local password** and **Confirm local password** to change your local password. Tap **Change Local password** to apply the changes.



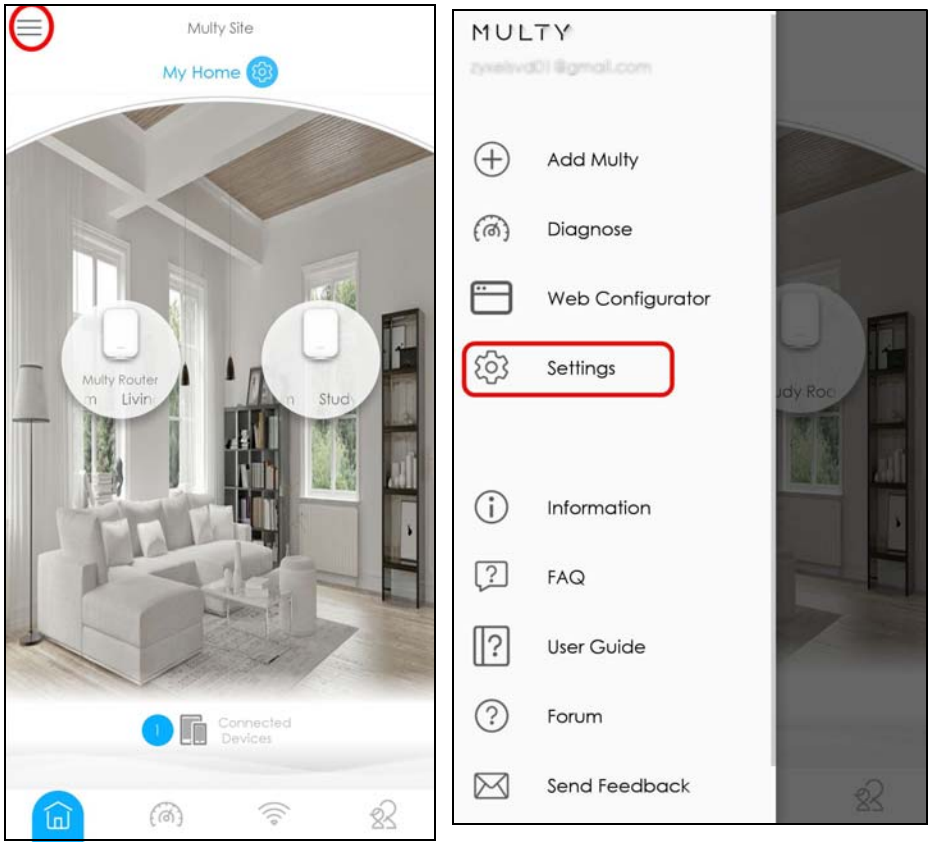
3.22 Enable or Add Port Forwarding Rules

If you want to forward incoming packets to a specific IP address in the private network using ports, set a port forwarding rule. This makes the specified LAN client accessible from the Internet, as shown in the next figure.

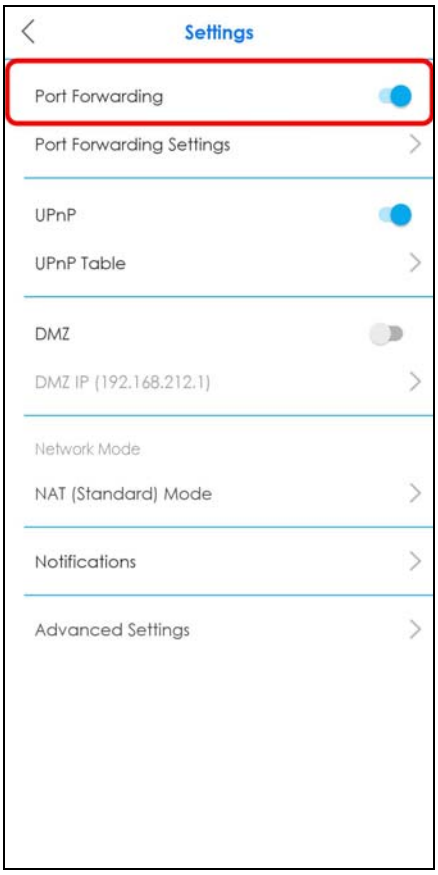
Figure 33 Port Forwarding



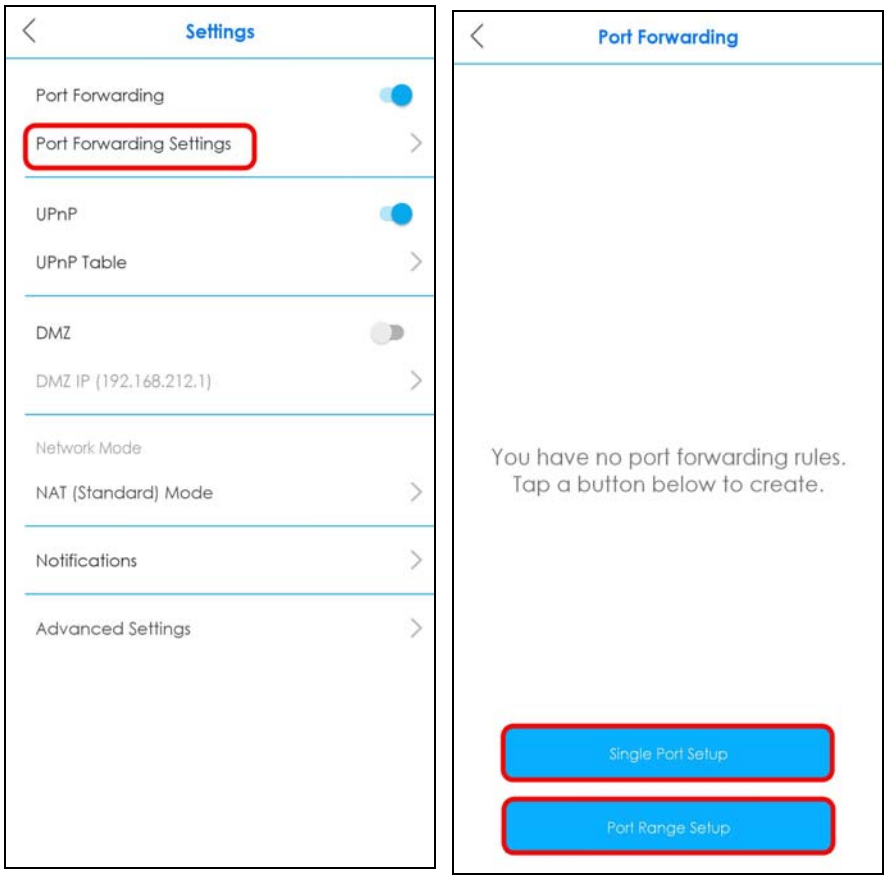
1 Tap the Menu icon in the upper-left to open the navigation panel, and then tap **Settings**.



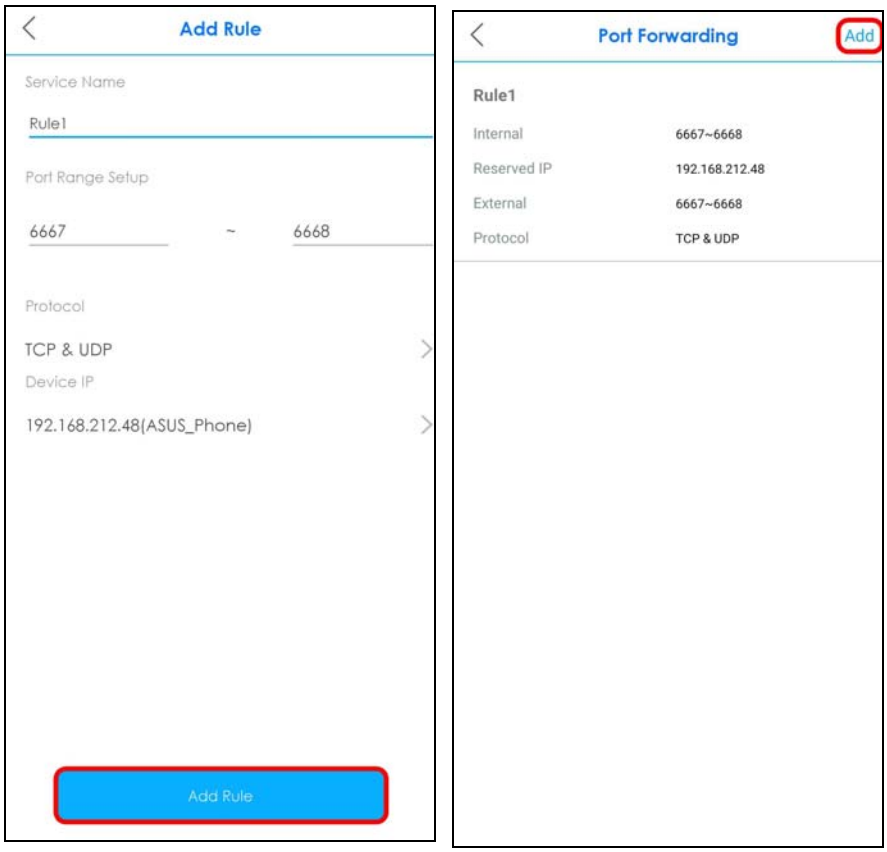
2 Tap **Port Forwarding** on the **Settings** screen to enable port forwarding.



3 Tap **Port Forwarding Settings** to create or update rules. On the **Port Forwarding** screen, tap **Single Port Setup** or **Port Range Setup** to add a rule.



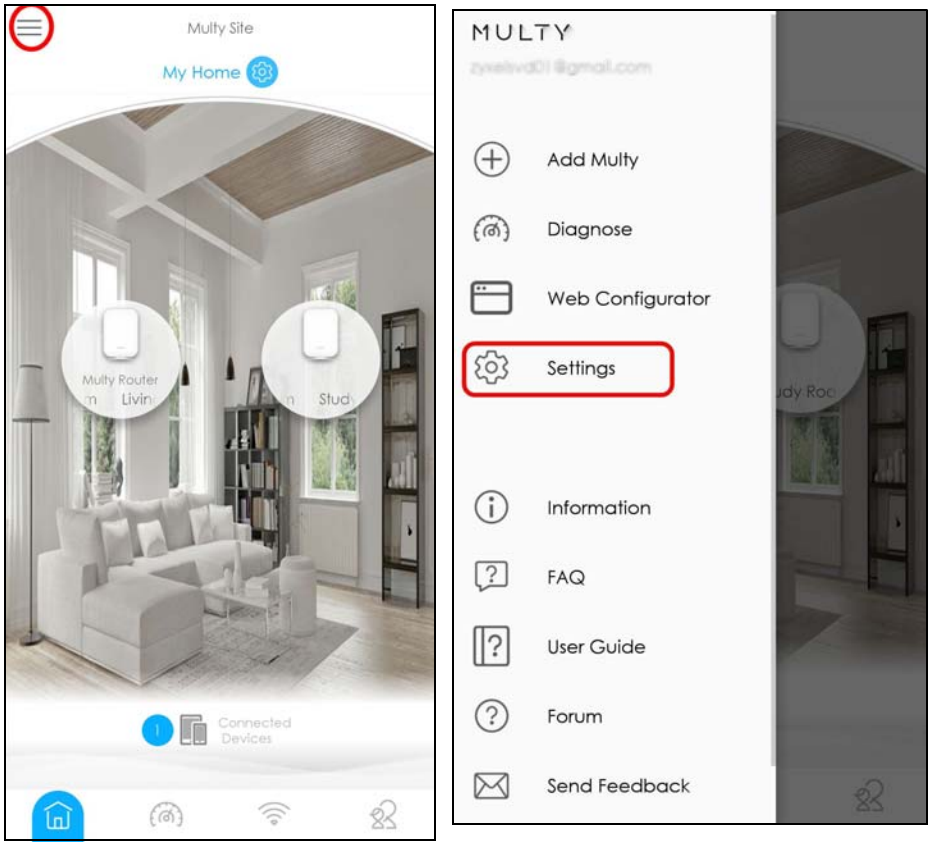
4 Enter a service name and a port number or a range of ports to define the service to be forwarded. Specify the transport layer protocol used for the service. Select a device on your local network that will receive the packets from the ports. Tap **Add Rule** once you are finished. A summary of the rules will be displayed. Tap **Add** if you want to create another rule.



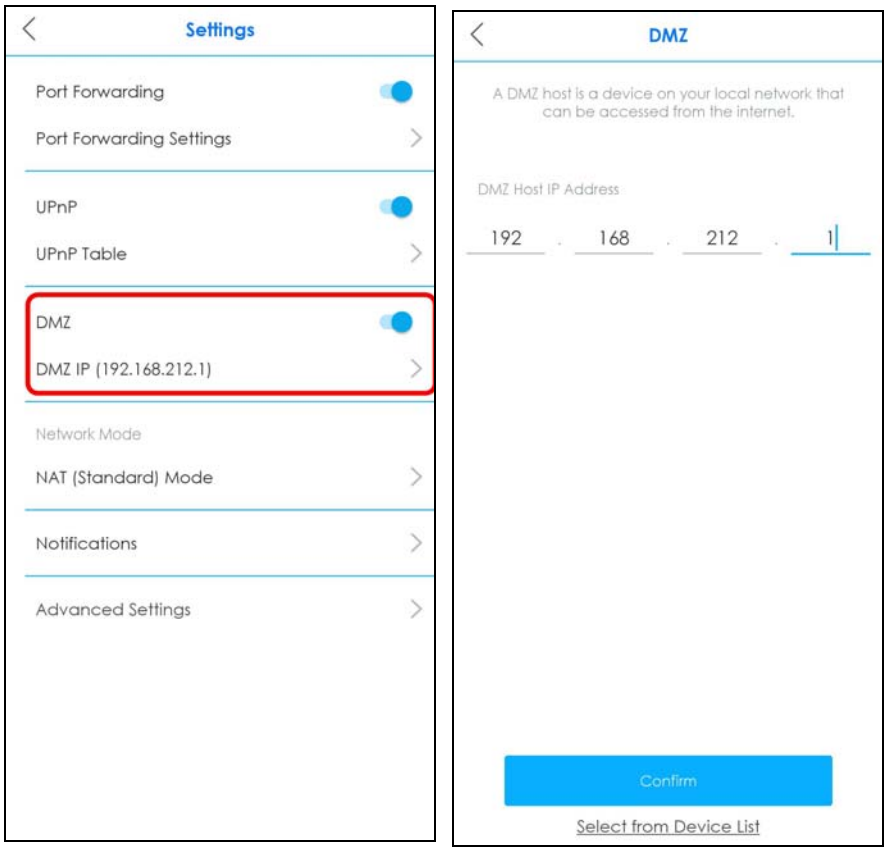
3.23 Enable DMZ

DMZ allows other devices over the Internet to access a DMZ host device within your local network. DMZ, which stands for "DeMilitarized Zone", is a network between the WAN and the LAN that is open to the WAN but still has firewall protection. Devices on the WAN can initiate connections to devices on the DMZ but not to those on the LAN. You could put servers such as mail servers, HTTP or HTTPS web servers and FTP servers on the DMZ to provide services to hosts on the WAN as well as hosts on the LAN. You first need to assign a DMZ host to use DMZ.

1 Tap the Menu icon in the upper-left to open the navigation panel, and then tap **Settings**.



2 Tap **DMZ IP** on the **Settings** screen to configure your DMZ host. Enter a device IP Address or tap **Select from Device List** and choose a device connected to the Multy WiFi network. Make sure **DMZ** is enabled on the **Settings** screen to use this feature.



3.24 Switch to NAT or Bridge Mode

In **NAT** mode, the Multy Device routes traffic between a local network and another network such as the Internet. Choose **NAT** mode if you want the Multy Device to assign local IP addresses to devices connected to it (DHCP) and use routing features.

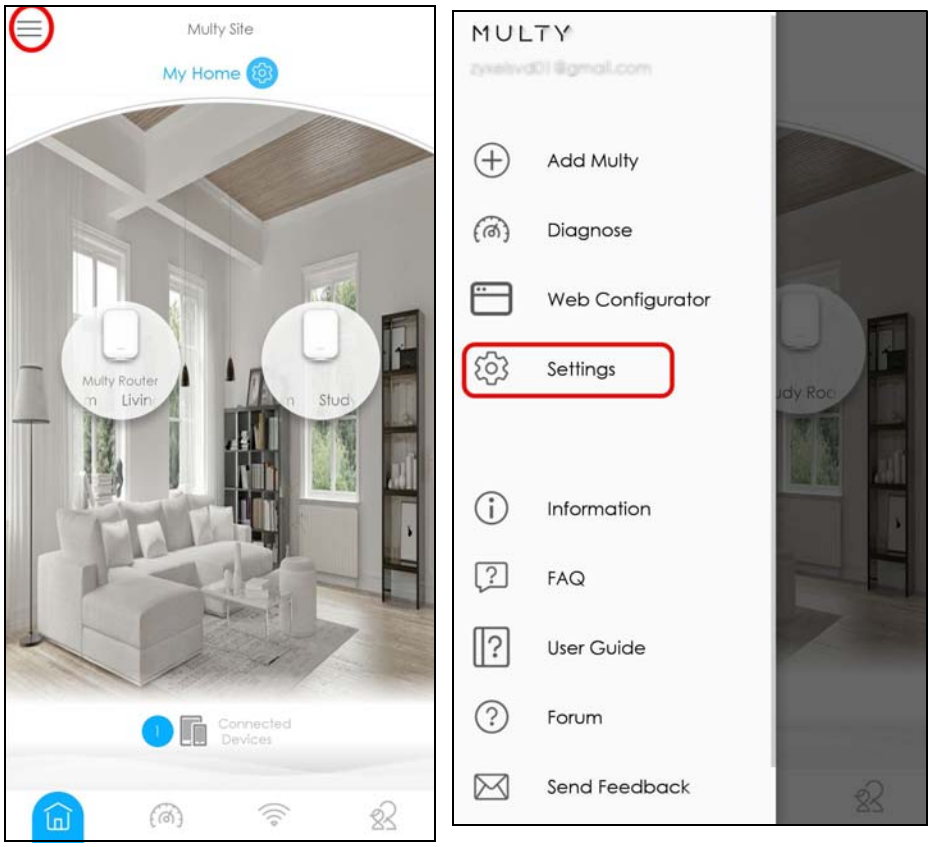
In **Bridge** mode, the Multy Device broadcasts traffic to the local network from the Internet. Choose **Bridge** mode if you have an existing router in your network and you do not want to reconfigure routing settings.

The following (routing) features are enabled in **NAT** mode:

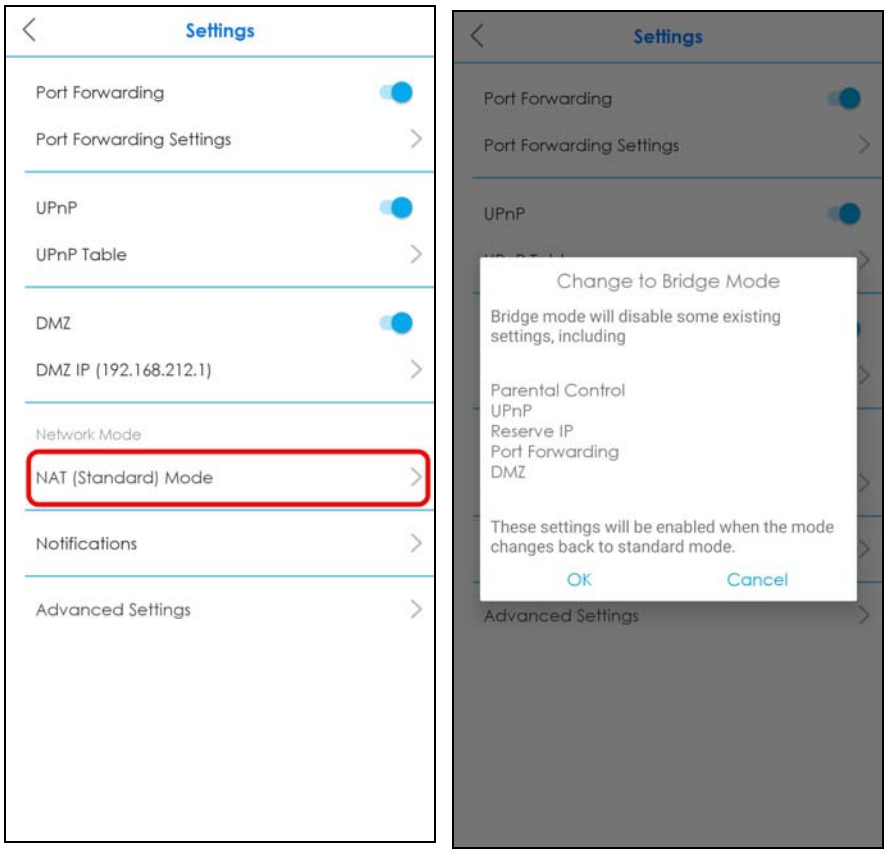
- Parental Control
- UPnP
- Reserve IP
- Port Forwarding
- DMZ
- SIP
- Guest WLAN

Note: These settings apply to the entire Multy Site. By default, your Multy Site is in **NAT** mode.

1 To change your network mode, tap the Menu icon in the upper-left to open the navigation panel, and then tap **Settings**.



2 Tap **NAT (Standard) Mode** if you want to switch between NAT and Bridge mode. Tap **OK** to apply the changes.

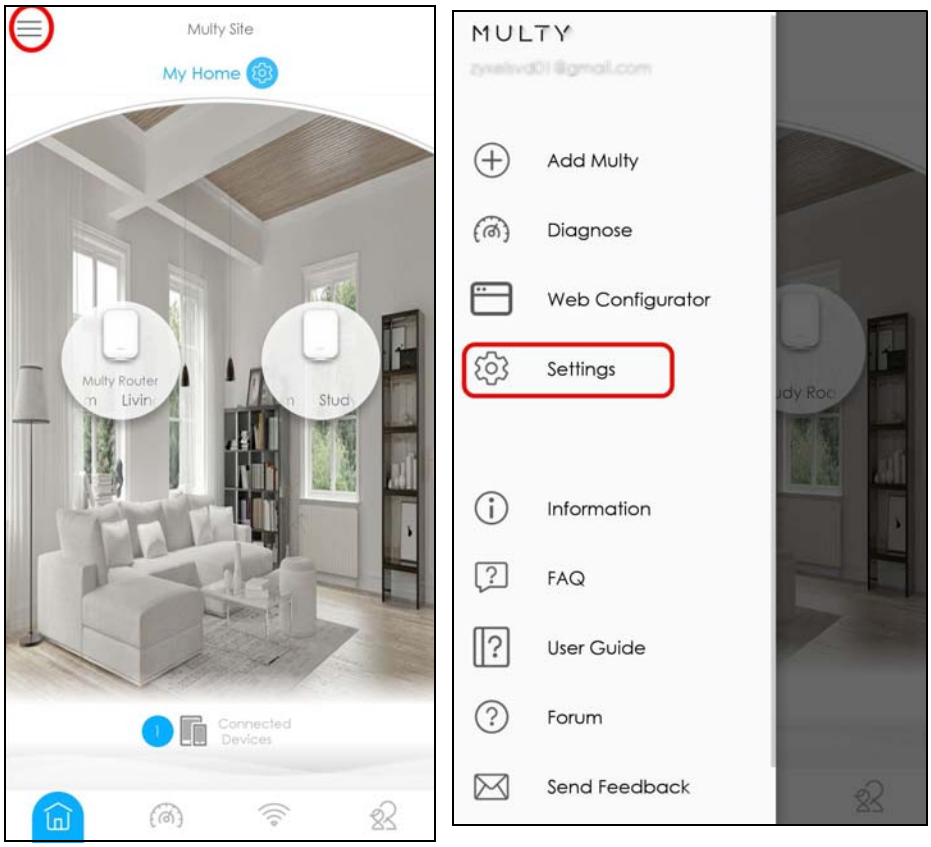


3.25 Turn Notifications On or Off

You can decide whether or not to get updates when new WiFi clients connect to the system, when there are new speed test results, and when firmware updates are available. These updates will show as push notifications on your smartphone.

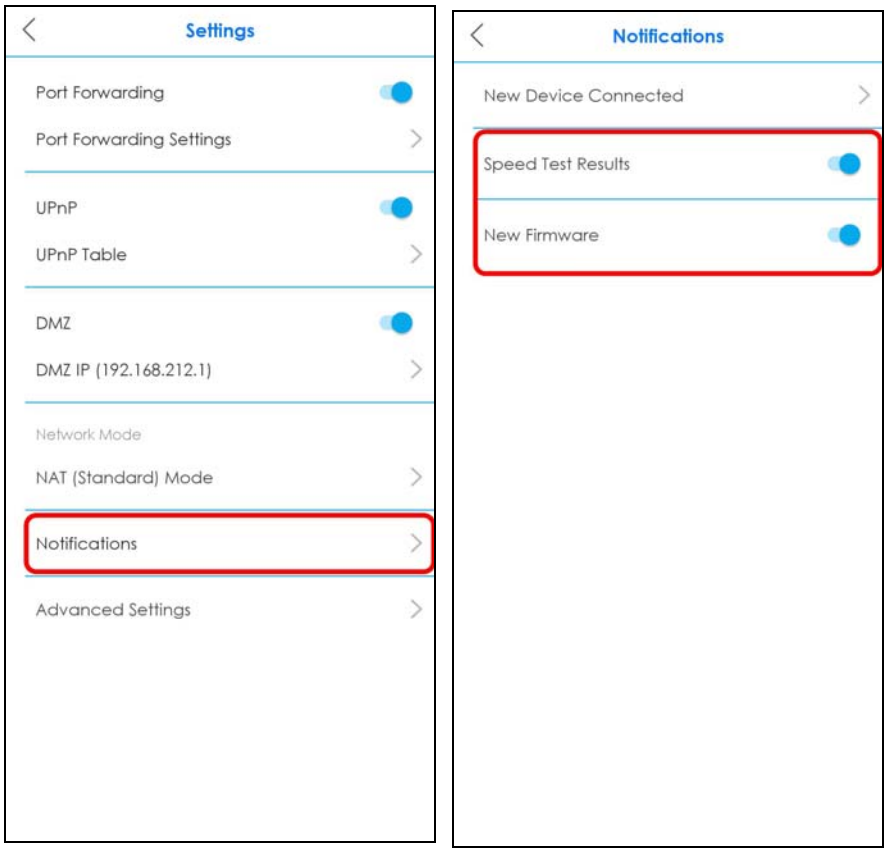
Note: You need to have a myZyxelCloud account to use this feature.

1 Tap the Menu icon in the upper-left to open the navigation panel, and then tap **Settings**.

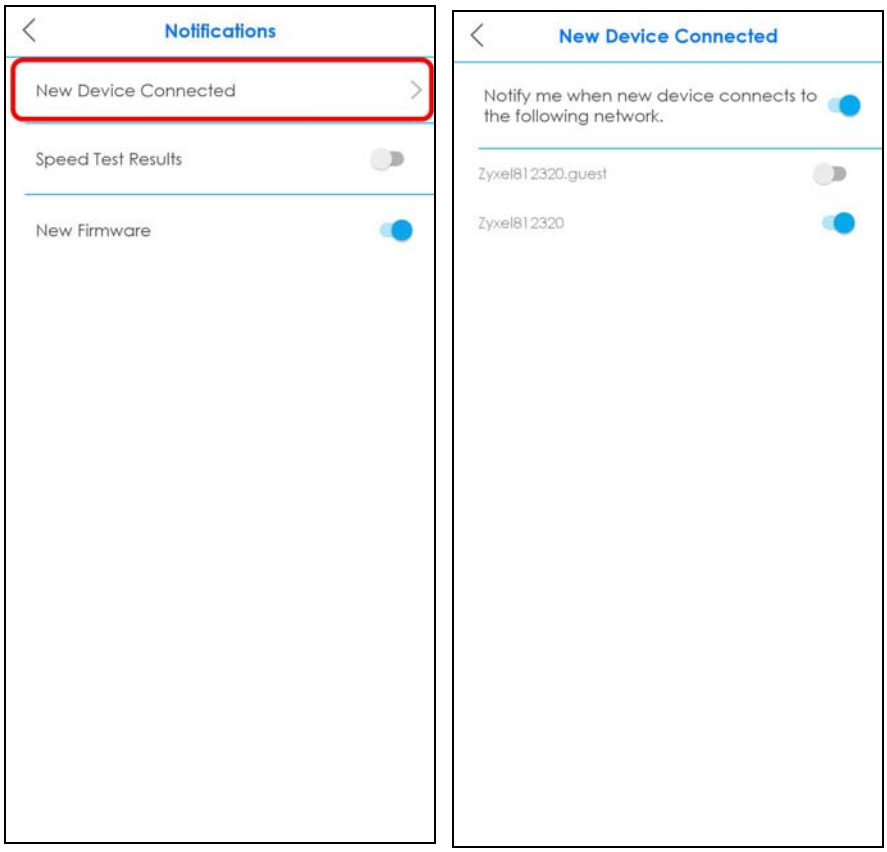


2 Tap **Notifications** on the **Settings** screen. Tap **Speed Test Results** or **New Firmware** to enable and allow the app to send you notifications when there is a new speed test result or new firmware update.

Note: After you turn on notifications for speed test results, you need to use the Alexa voice command "Alexa, ask Zyxel Multy to test Internet speed" to run a speed test to receive the notification. See Section 3.30 on page 106 for more information about how to use the Alexa voice service. This speed test corresponds to **Menu** > **Diagnose** > **Speed Test**, checking the connection between the primary Multy and Internet (see Section 3.10 on page 58).



3 If you want to get notifications when there are new client devices connecting to your WiFi networks, tap **New Device Connected** and enable notifications for the WiFi networks.



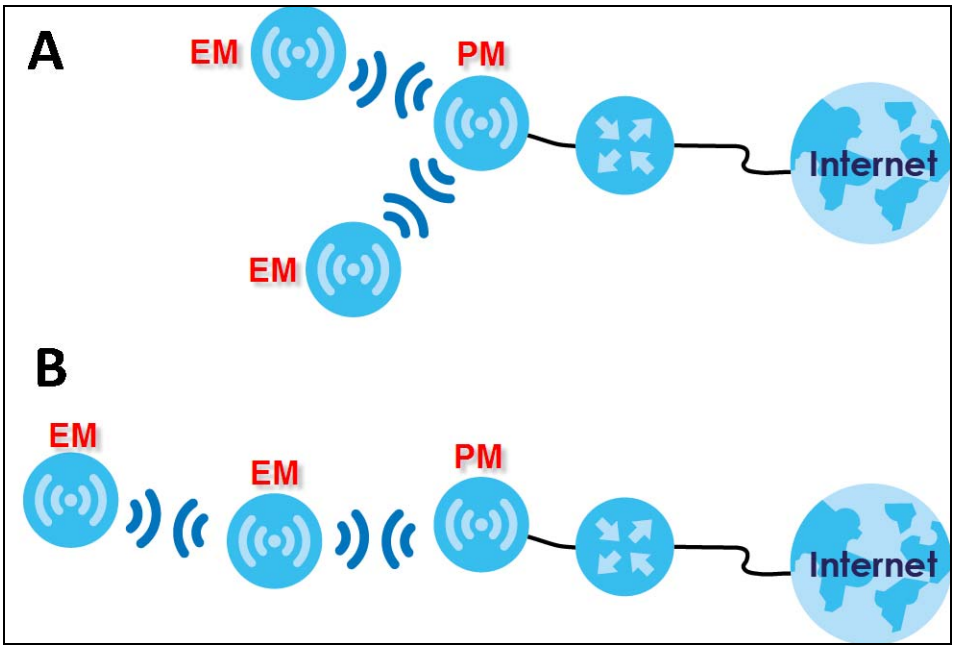
3.26 Enable or Disable Daisy Chain Network Topology

You can "daisy chain" multiple Multy Devices together to create expansive WiFi coverage for your home.

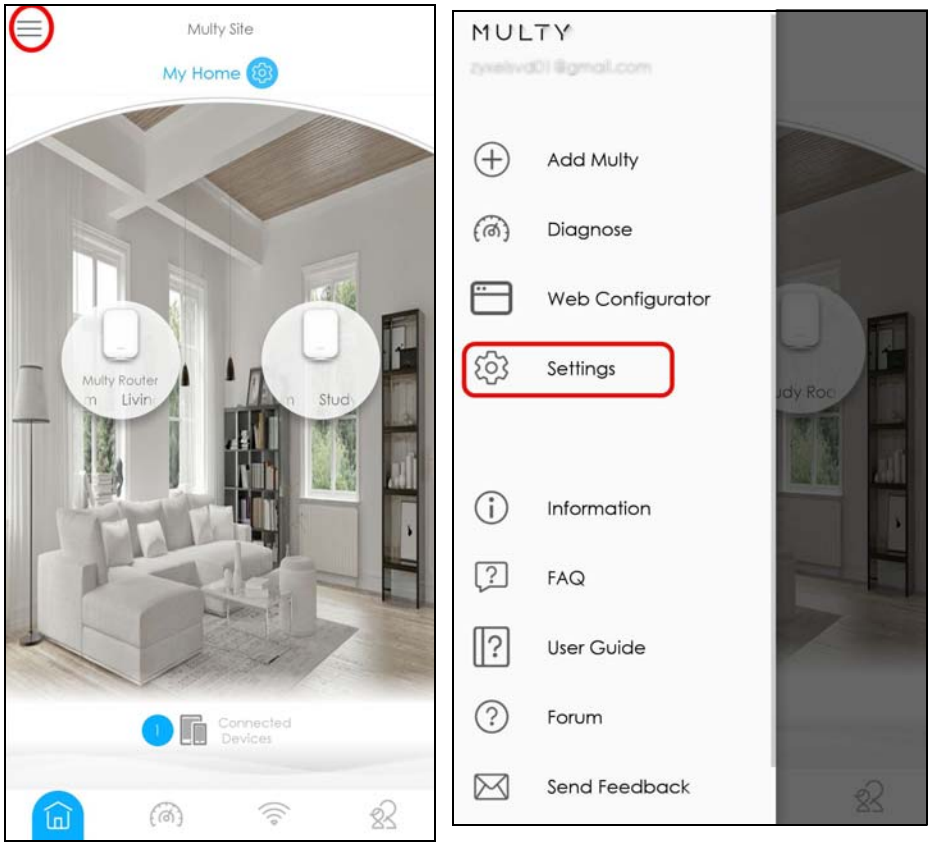
The daisy chain topology is illustrated in the figure below. Figure **A** shows the illustration of **Daisy Chain Disabled**. Figure **B** shows the illustration of **Daisy Chain Enabled**. When daisy chaining is enabled, each extender Multy (**EM**) can go through another extender Multy with a strong WiFi signal to connect to the primary Multy (**PM**).

When Multy Devices are daisy-chained, they do not all need to be placed near the primary Multy, which means you can extend your coverage.

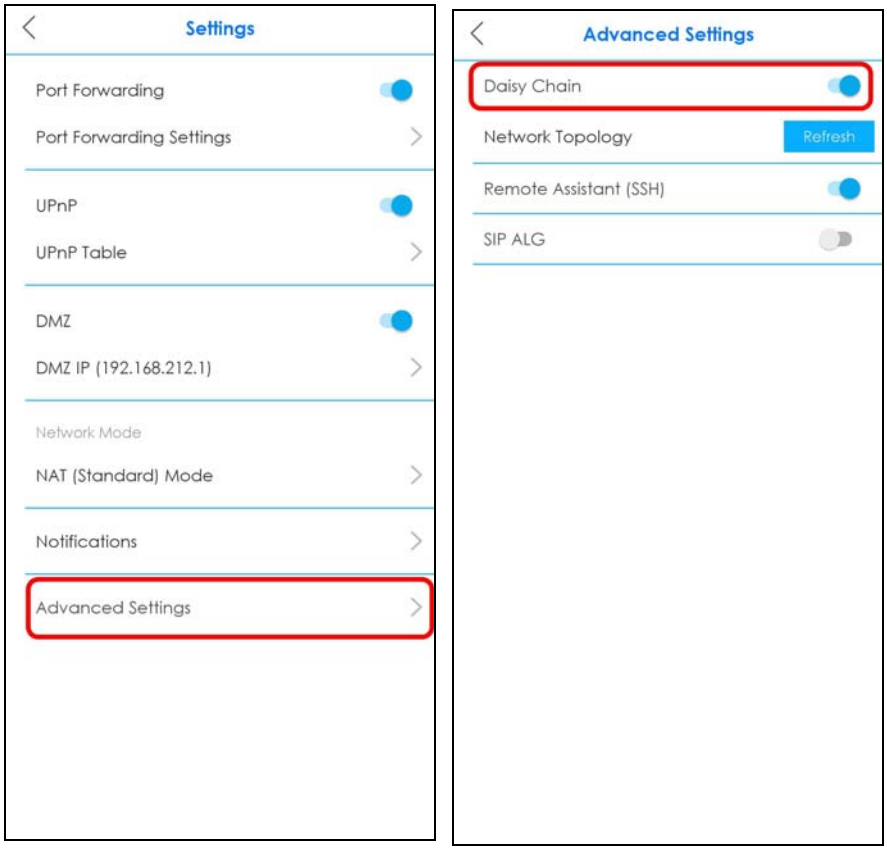
Note: This feature is not available on all Multy Devices. The **Daisy Chain** and **Network Topology** menus appear only when using a Multy Device that supports Daisy Chain. See Table 1 on page 9 to see which devices support this feature.



1 Tap the Menu icon in the upper-left to open the navigation panel, and then tap **Settings**.



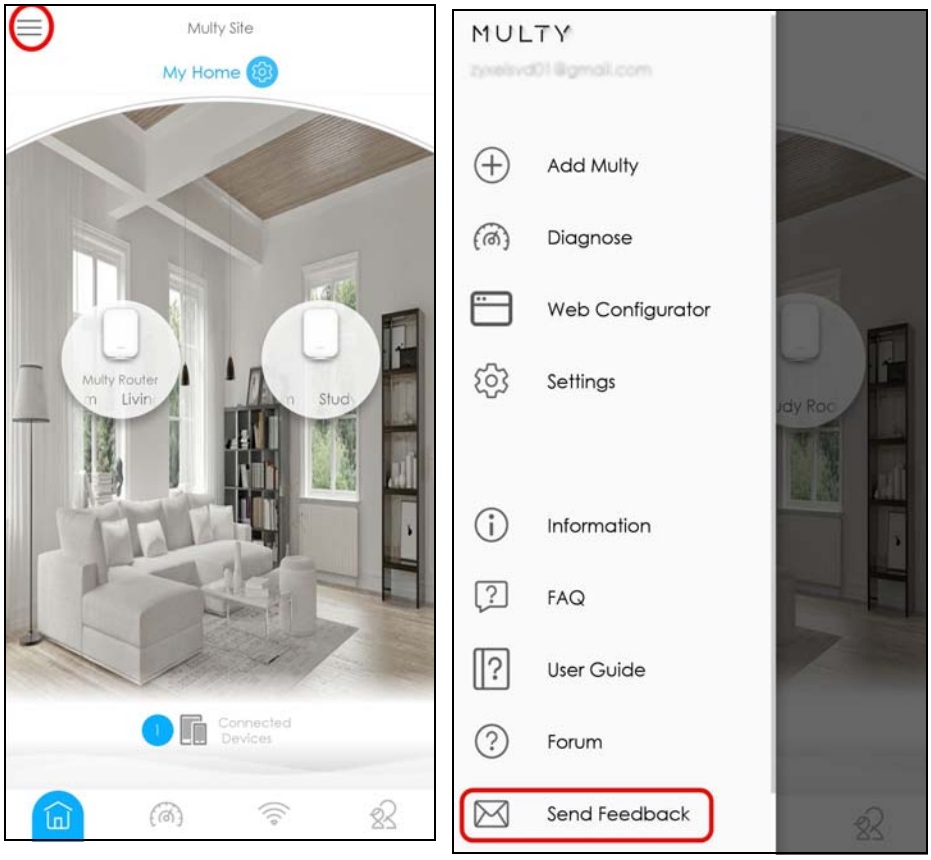
2 Tap **Advanced Settings** on the **Settings** screen. Tap **Daisy Chain** to enable or disable daisy chaining.



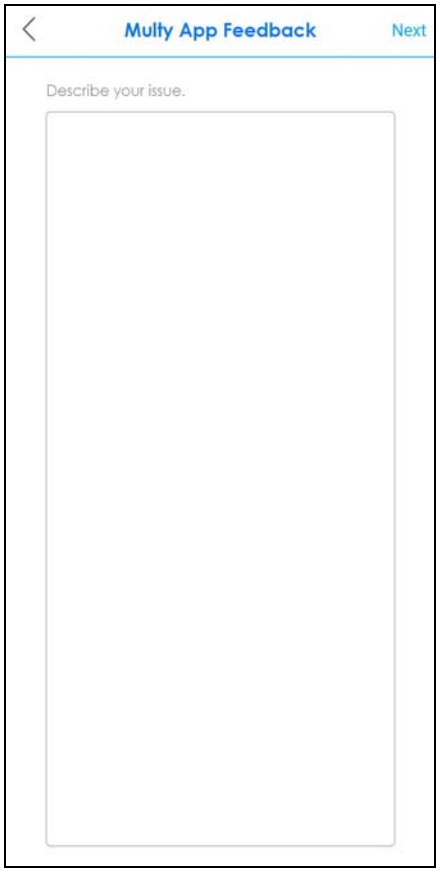
3.27 Report a Problem With the Zyxel Multy App

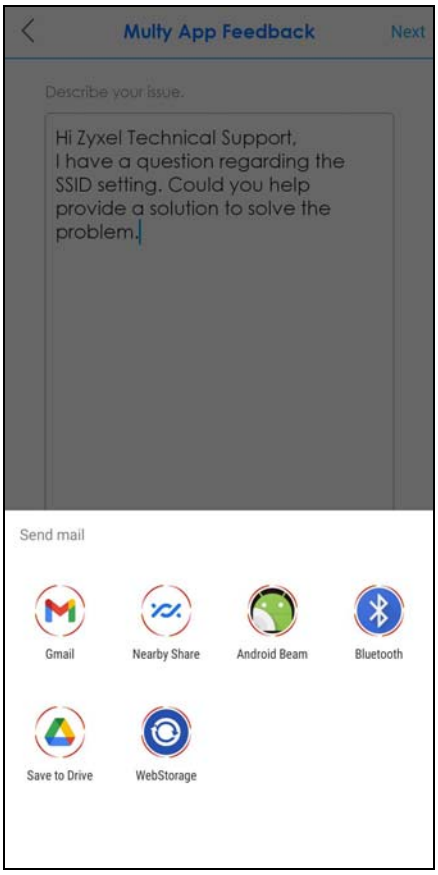
If you encounter problems while using the Zyxel Multy app or want to send us your feedback, you can send an email to customer service.

1 Tap the Menu icon in the upper-left to open the navigation panel. Tap **Send Feedback**.



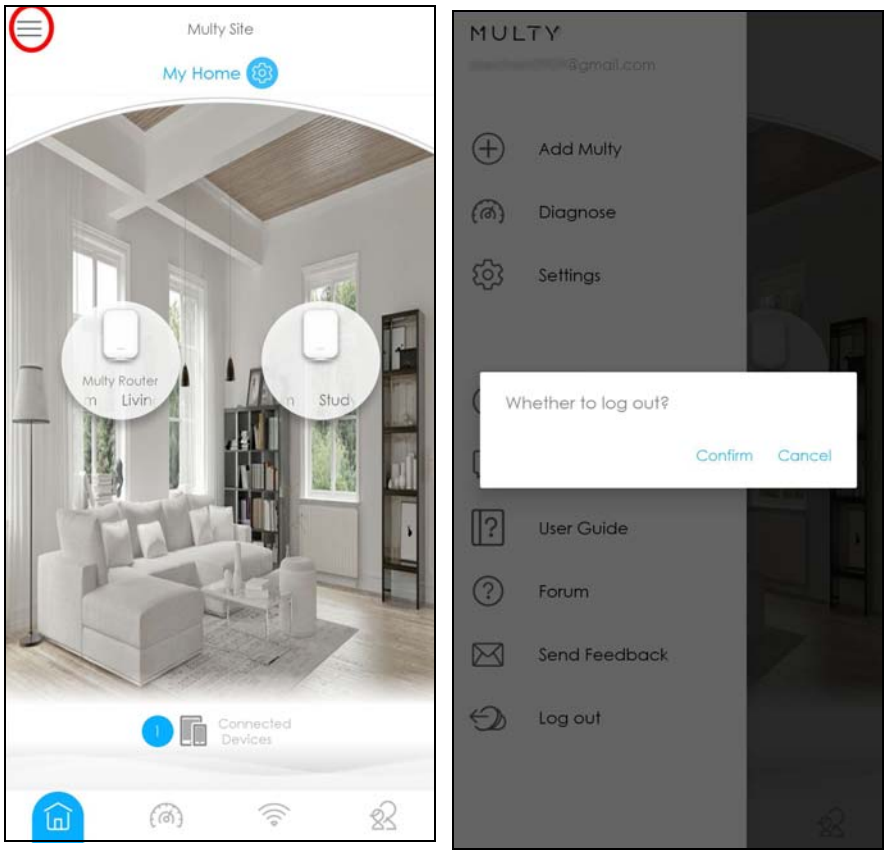
2 Edit the mail and then tap **Next** to send it through the Internet.





3.28 Log Out of the myZyxelCloud Account

Tap the Menu icon in the upper-left to open the navigation panel. Tap **Log Out**.



3.29 View Legal and Regulatory Information

Check the e-label if you want to see legal and regulatory information related to your Multy Device. Note: Not all Multy Devices have an e-label which contains legal and regulatory information in the app (see Table 1 on page 9). For Multy Devices without an e-label, you may check the label printed on the device. See Table 1 on page 9 for more information.

1 From the **Multy Site** screen, tap the Multy Device you want to check. The **Detail** screen will be displayed.

2 Tap the Information icon ( ) to view legal and regulatory information.

3.30 Manage Your Multy WiFi System With Amazon Alexa

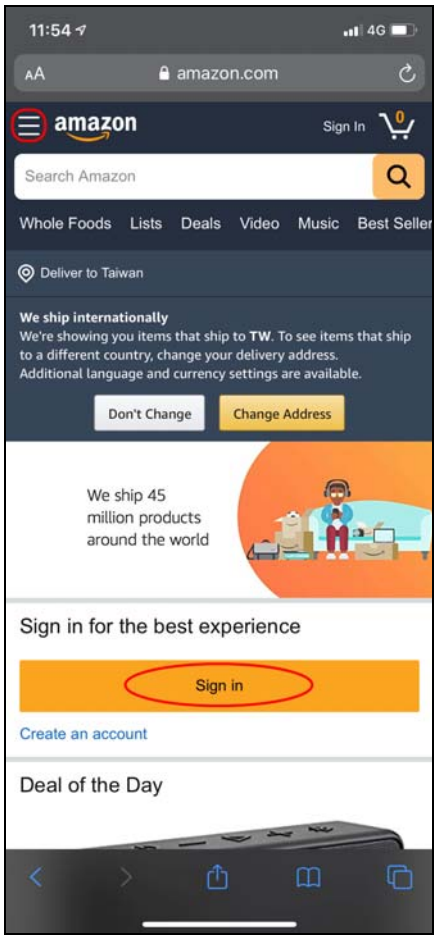
If you have an Alexa-enabled device (Amazon Echo for example), you can use your voice to control the Multy Devices in your Multy Sites. At the time of writing, the available Alexa skill voice commands for Multy Sites are:

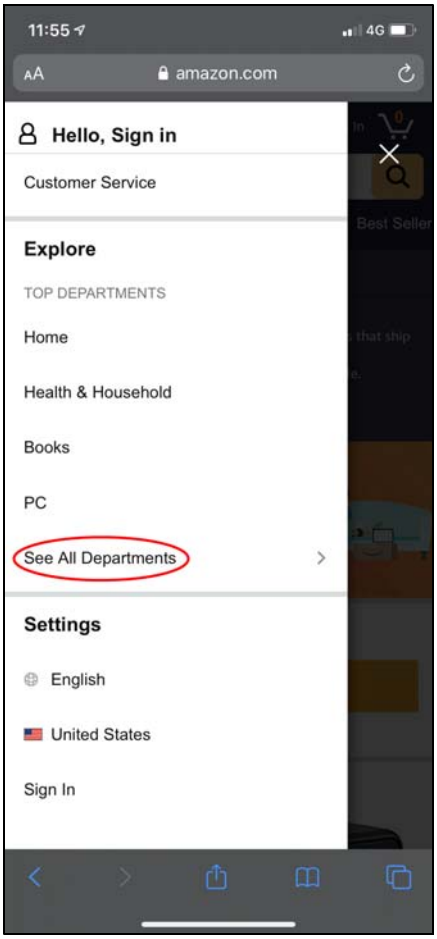
- Alexa, ask Zyxel Multy to turn off guest WiFi
- Alexa, ask Zyxel Multy to test Internet speed
- Alexa, ask Zyxel Multy to turn on WiFi light
- Alexa, ask Zyxel Multy to turn off WiFi light
- Alexa, ask Zyxel Multy to pause the Internet

You need to enable the Multy-Alexa skills to enhance the functionality of your Alexa device and allow Alexa to perform the supported tasks. See Table 1 on page 9 for more information.

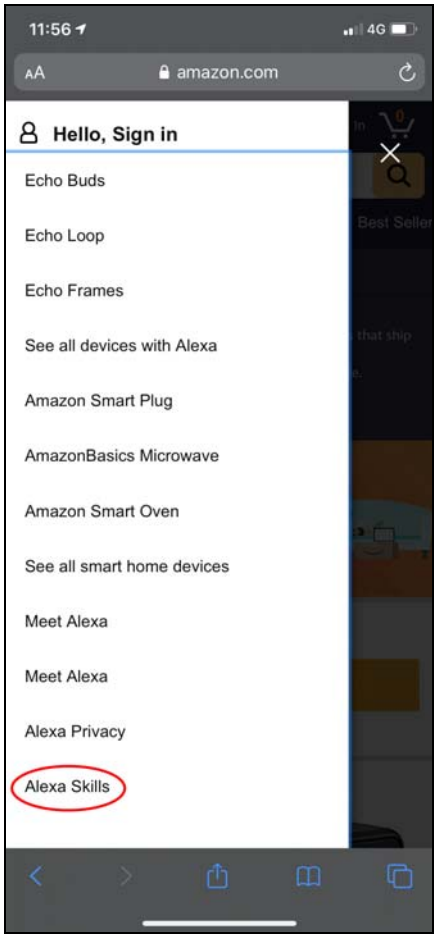
Note: To use the Alexa voice service, you must have logged into the Zyxel Multy app with a myZyxelCloud account and set up the Multy Devices.
Both the Multy Devices and Alexa device should be connected to the same WiFi network.

1 Go to Amazon's website (*https://www.amazon.com*) and sign in with your Amazon account. Tap the Menu icon in the upper-left and tap **See All Departments**.

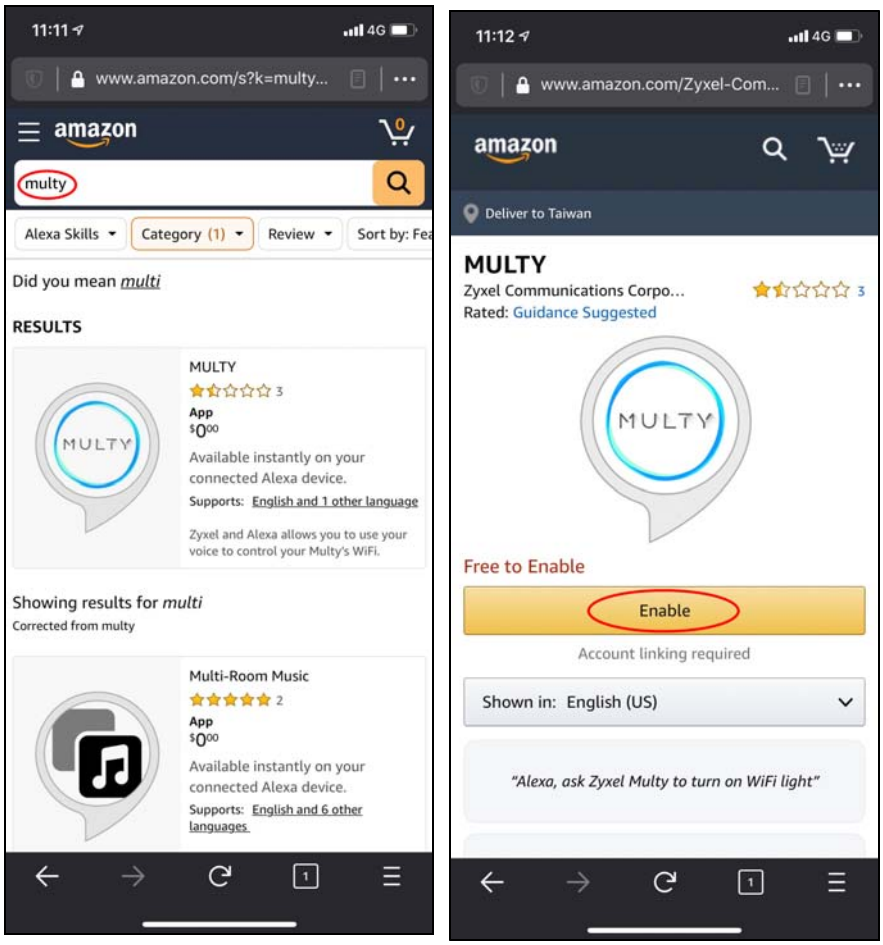

11:54
4G
AA
amazon.com
amazon
Sign In
Search Amazon
Whole Foods
Lists
Deals
Video
Music
Best Seller
Deliver to Taiwan
We ship internationally
We're showing you items that ship to TW. To see items that ship to a different country, change your delivery address.
Additional language and currency settings are available.
Don't Change
Change Address
We ship 45 million products around the world
Sign in for the best experience
Sign in
Create an account
Deal of the Day


11:55
4G
AA
amazon.com
Hello, Sign in
Customer Service
Explore
TOP DEPARTMENTS
Home
Health & Household
Books
PC
See All Departments
Settings
English
United States
Sign In

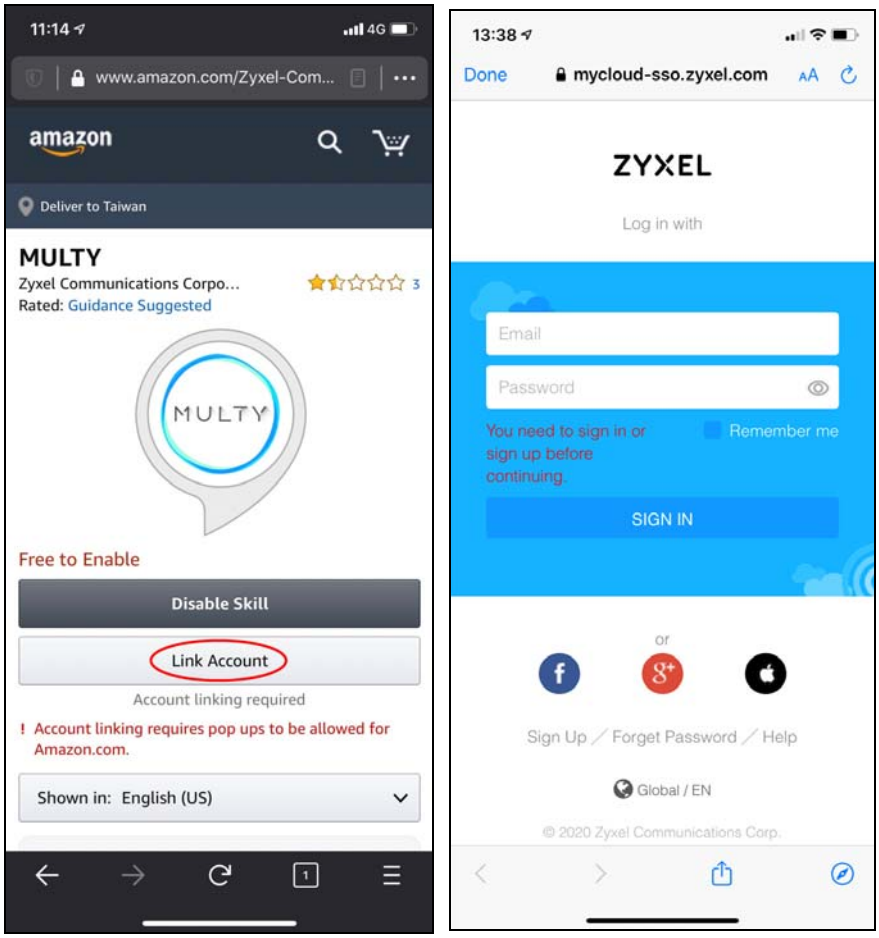
2 Select **Alexa Skills**.



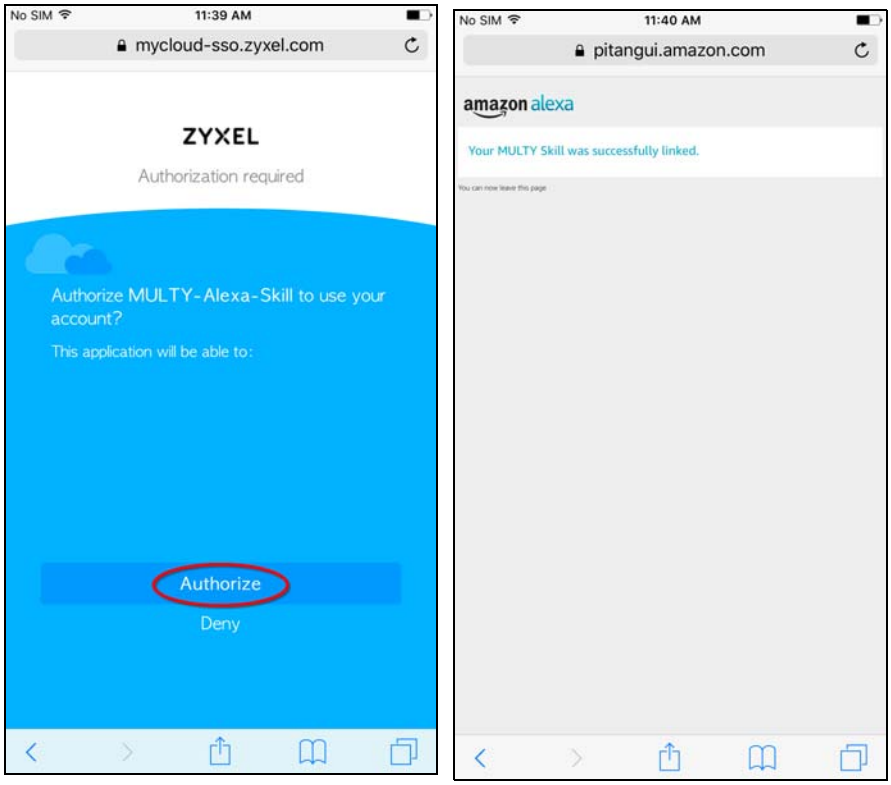
3 Enter the keyword "Zyxel Multy" in the search bar and select "Zyxel Multy" from the list of results. Tap **Enable** to connect the Multy Site to Alexa.



4 Tap **Link Account** and enter your myZyxel account information to associate the skill with your account.



5 Tap **Authorize**. A screen appears showing that the skill for Multy Sites has been successfully linked.



Use either the Alexa app or the voice command "Discover Devices" to have Alexa discover the Multy Devices on the specified myZyxel account. You then can use your voice to control the Multy Device.

PART II
Multy M1

CHAPTER 4
Multy M1 Wizard

4.1 Overview

In this chapter, you will learn how to:

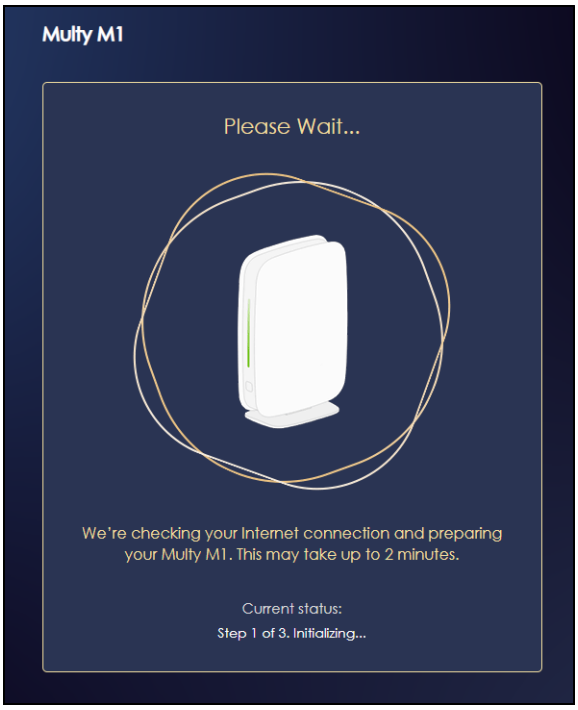
- Go through Multy M1 (WSM20) wizard steps
- Create a myZyxelCloud account.
- Configure basic settings for your WiFi

4.2 Accessing the Wizard

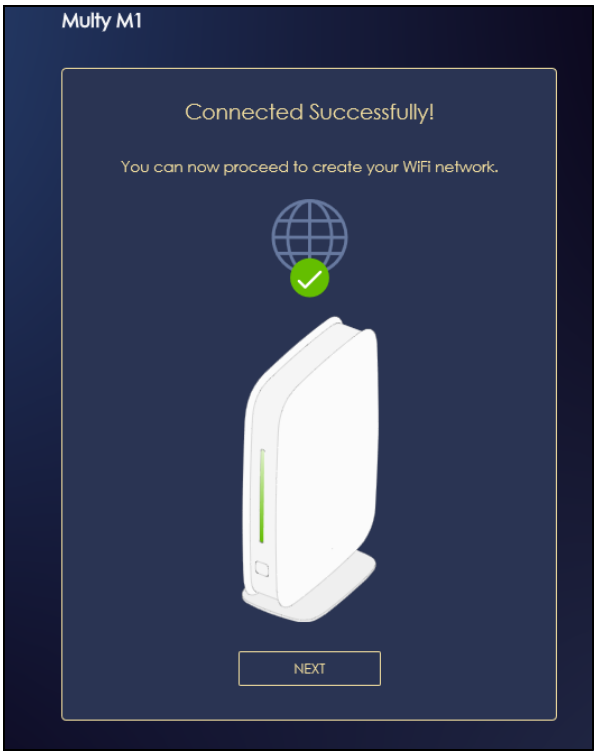
Launch your web browser and enter "http://zyxelwifi.com" or "http://zyxelwifi.net" or "http://192.168.212.1 as the website address.

Note: The wizard appears automatically when the Multy M1 is accessed for the first time or when you reset the Multy M1 to its default factory settings.

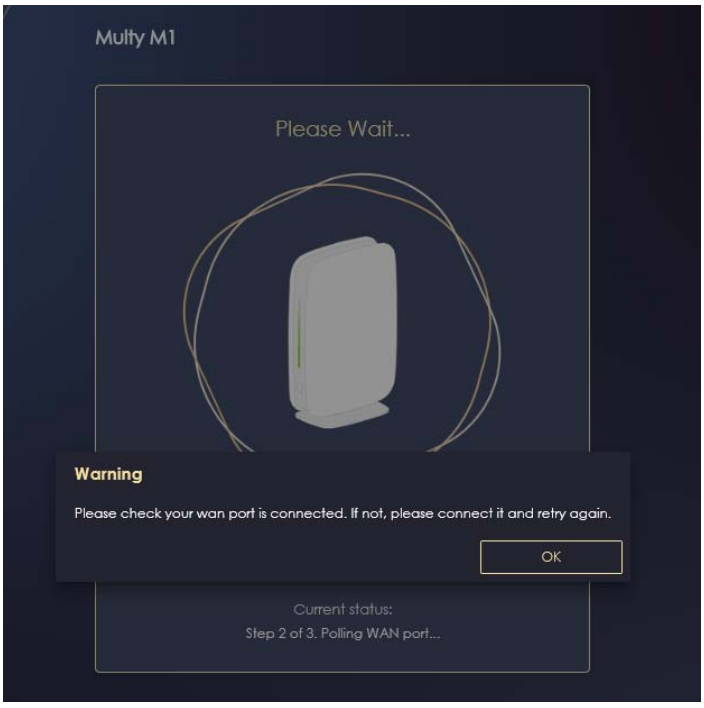
1 Make sure the WAN port of the Multy M1 is connected to a modem or router with Internet access. Your Multy M1 will check the status of your Internet connection the first time you log in.



2 The following screen shows if you are connected to the Internet. Click **Next** to go to the next step in the wizard.



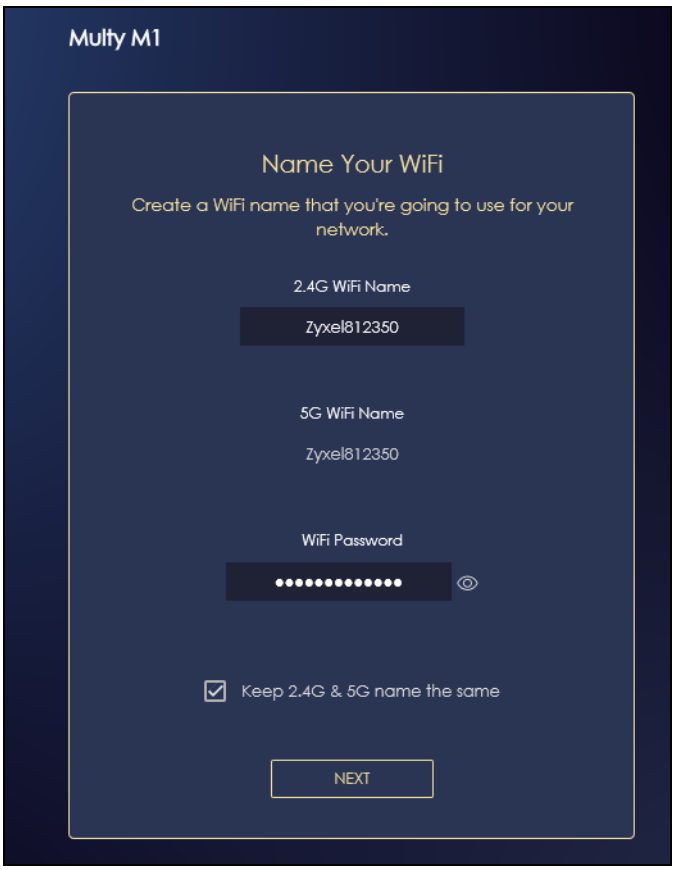
The following screen shows if you are not connected to the Internet.



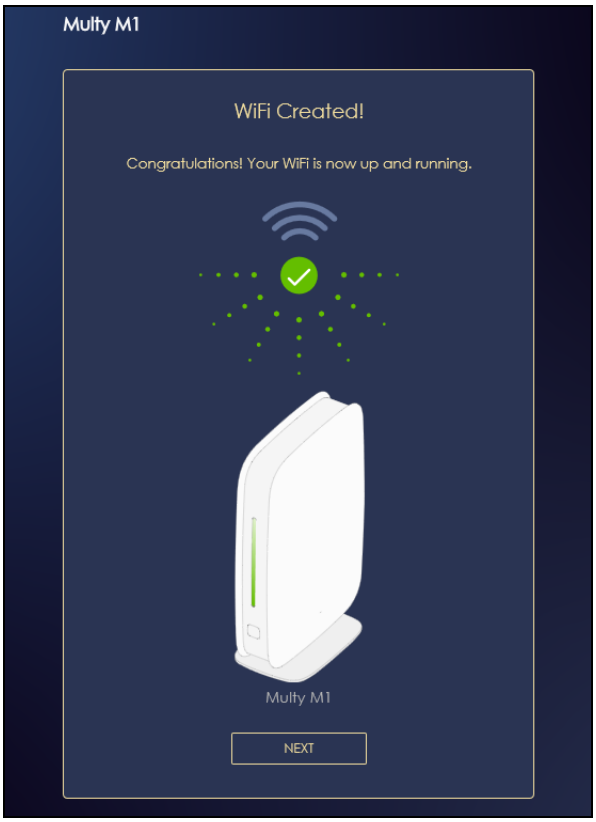
Note: You may need to turn off your network firewall if access to the Internet from the Multy M1 is blocked. Turn on your network firewall after the configuration is completed.

You need to connect to the Internet to access your Multy M1. See Section 4.2 on page 113 if you cannot connect to the Internet.

3 Enter 1-128 single-byte printablecharacters but not ""'<>^$& as your **2.4G/5G WiFi Name** and **WiFi Password**. Select the check box **Keep 2.4G & 5G name the same** if you want to use the same name for your 2.4G and 5G WiFi.



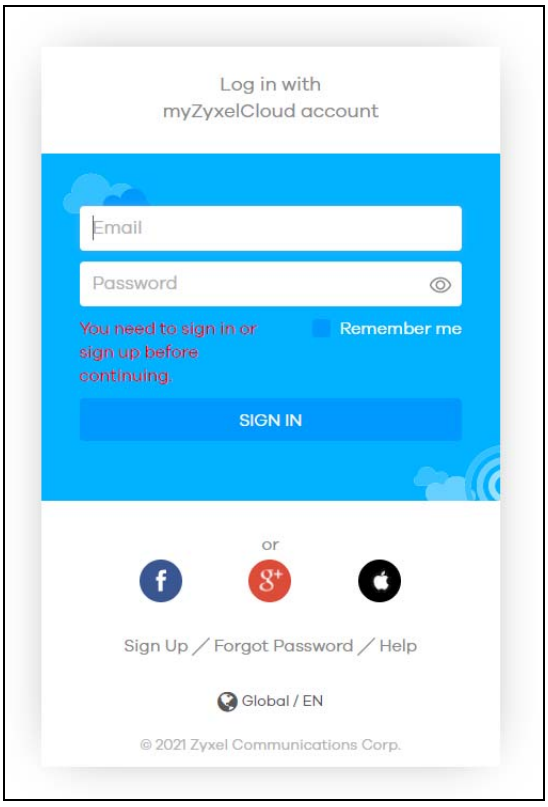
4 The following screen shows if you have set up your WiFi name and password successfully. Click **Next** to go to the next step in the wizard.



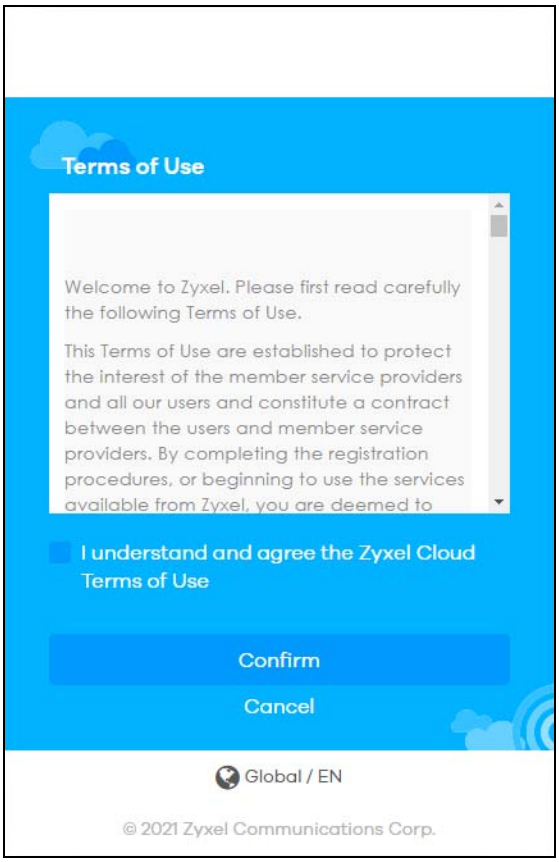
5 You need to create a myZyxelCloud account to log into the Multy M1. Click **Next** to go to the next step in the wizard.

6 A pop up message shows. Click **OK** to be redirected to the registration website of myZyxelCloud.

7 Enter your **Email** and **Password** and click **SIGN IN**, if you already have a myZyxelCloud account. If not, you can create one by clicking **Sign Up**. You can also click the Facbook or Google icon to create an account with your Facebook or Google account.



8 The legal page shows after you log in. Select the check box **I understand and agree the Zyxel Cloud Terms of Use** and then click **Confirm**.

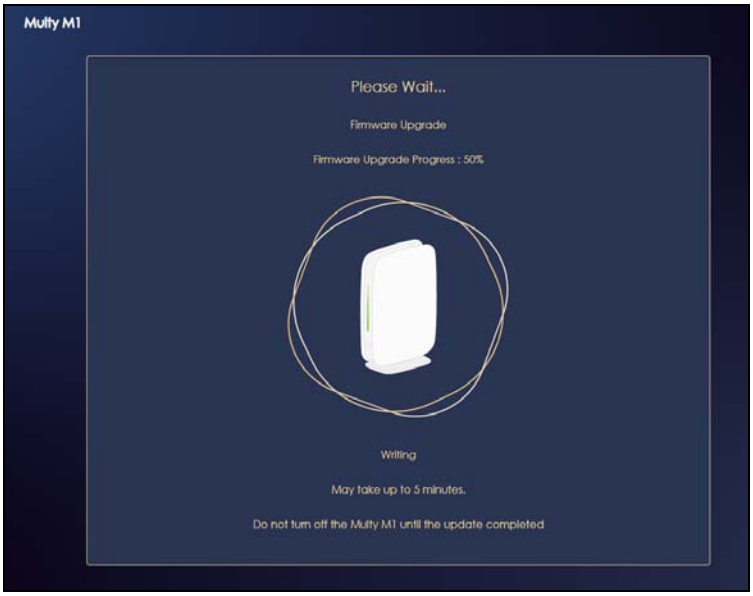


9 Wait a moment for your Multy M1 to link to your myZyxelCloud account.

10 Create a web configurator password to access the Multy M1 directly. You may choose to log in with your myZyxelCloud account or your local password the next time you log in.

Note: You can change your local password in **System** > **General Settings**. See Section 7.9 on page 147 for more information.

11 Wait for a moment to check if your Multy M1 is updated with the latest firmware. If not, your Multy M1 will automatically update the firmware.



CHAPTER 5
Multy M1 Web Configurator

5.1 Overview

This chapter describes how to access the Multy M1 Web Configurator and provides an overview of its screens.

The Web Configurator is an HTML-based management interface that allows easy system setup and management via Internet browser. Use a browser that supports HTML5, such 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).

5.2 Accessing the Web Configurator

1 Make sure your Multy M1 hardware is properly connected (refer to the Quick Start Guide).

2 Launch your web browser.

3 If the Multy M1 is in **Standard Mode** (the default mode), enter "http://zyxelwifi.com or 192.168.212.1" in the browser's address bar.

If the Multy M1 is in **Bridge Mode**, enter "http:// (DHCP-assigned IP)" in the browser's address bar.

4 On the displayed login screen, log in using your myZyxelCloud username and password or the local password.

Note: If this is the first time you are accessing the web configurator or if the device has been reset, you must complete the setup wizard, see Chapter 4 on page 113.

Note: For setting and changing the local password, see Section 7.9 on page 147.

Figure 34 Login

5 The Multy M1 **Overview** screen displays allowing you to monitor your Multy M1. It shows if the Multy M1 is online, and how many wireless clients are currently connected to your device, You can also view WiFi network settings, CPU usage, Memory usage and the LAN/WAN port status on the screen.

Figure 35 Overview (Standard Mode)

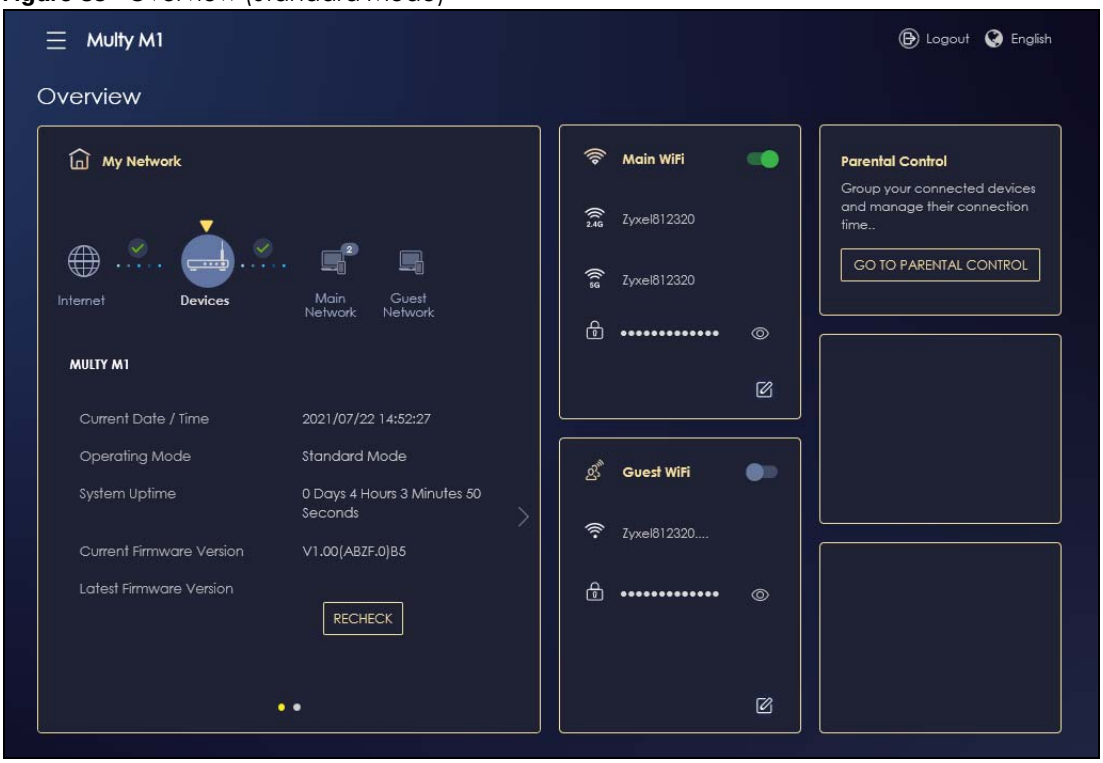
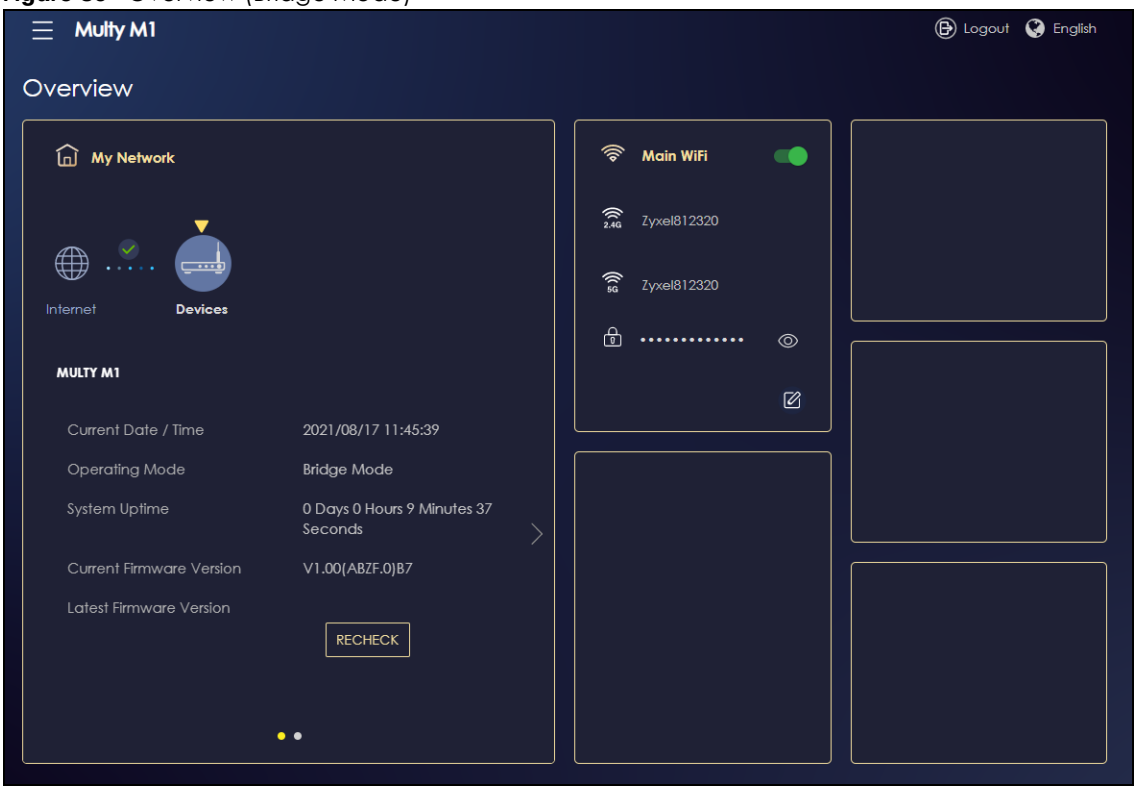


Figure 36 Overview (Bridge Mode)



5.3 Navigation Panel

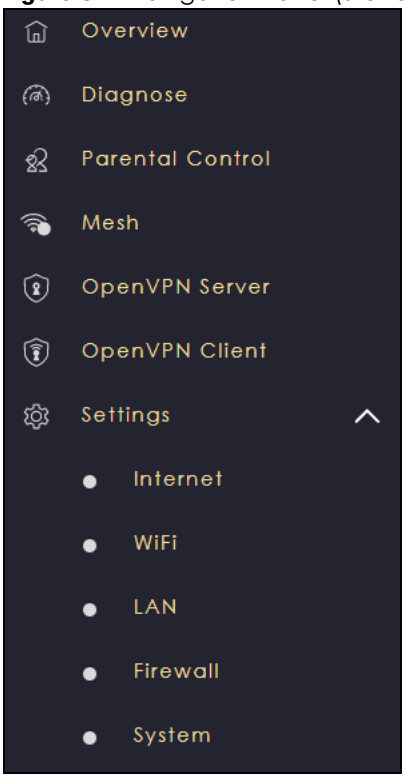
Use the submenus on the navigation panel to configure Multy M1 features. Your navigation panel varies depending on the mode of your Multy M1.

See Section 6.3 on page 127 for more information on Standard Mode.

See Section 6.6 on page 129 for more information on Bridge Mode.

5.3.1 Standard Mode Navigation Panel

Figure 37 Navigation Panel (Standard Mode)



The following table describes the submenus.

Table 8 Settings > System > Status (Standard Mode)

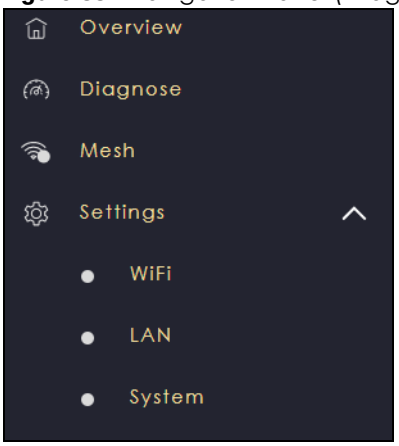
LINK	TAB	FUNCTION
Overview		Use this screen to: • View read-only information about your Multy M1 • Configure WiFi settings •
Diagnose	Advanced Speed Test	Use this screen to check the speed of the connection between your Multy M1 and the broadband modem/router.
	Speed Test History	Use this screen to view a summary of previously run speed tests.
Parental Control	Device	Use this screen to: • View devices information • Add and configure parental control rules or schedules
	Profile	Use this screen to enable or configure existing parental control rules.
Mesh	My Mesh	Use this screen to view Mesh network information.
OpenVPN Server	OpenVPN Server	Use this screen to create and configure an OpenVPN server account.
	OpenVPN Account	Use this screen to: • View basic information about Multy M1 OpenVPN server • View basic information about clients that are connected to the Multy M1 OpenVPN server

Table 8 Settings > System > Status (Standard Mode) (continued)

LINK	TAB	FUNCTION
OpenVPN Client		Use this screen to: • View basic information about OpenVPN Server accounts that you are connected to • Add an OpenVPN Server Account you want your Multy M1 to connect to when the Multy M1 functions as an OpenVPN client.
Settings		
Internet	Internet Connection	This screen allows you to configure ISP parameters, WAN IP address assignment, DNS servers and the WAN MAC address.
	NAT & Port Forwarding	Use this screen to enable NAT. Use this screen to configure servers behind the Multy M1 and forward incoming service requests to the servers on your local network.
	Passthrough	Use this screen to change your Multy M1's port triggering settings.
	Dynamic DNS	Use this screen to configure dynamic DNS.
	UPnP	Use this screen to enable UPnP on the Multy M1.
WiFi	Main WiFi	Use this screen to enable the wireless LAN and configure wireless LAN and wireless security settings.
	Guest WiFi	Use this screen to configure multiple BSSs on the Multy M1.
	WPS	Use this screen to configure WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
LAN	LAN IP	Use this screen to configure the Multy M1's LAN IP address and subnet mask. Use this screen to configure the IPv6 address for the Multy M1 on the LAN. Use this screen to configure your DNS server. Use this screen to enable the Multy M1's DHCP server.
	IPv6 LAN	Use this screen to configure the IPv6 address for your Multy M1 on the LAN.
Firewall	IPv4 Firewall	Use this screen to configure IPv4 firewall rules.
	IPv6 Firewall	Use this screen to configure IPv6 firewall rules.
System	Status	Use this screen to view the basic information of the Multy M1.
	General Setting	Use this screen to change password or to set the timeout period of the management session.
	Remote Access	Use this screen to configure the interface/s from which the Multy M1 can be managed remotely and specify a secure client that can manage the Multy M1.
	Maintenance	Use this screen to upgrade firmware, restartthe Multy M1 without turning the power off or reset the Multy M1 to factory default settings.
	Operating Mode	Use this screen to select whether your device acts as a router, or a bridge.
	Logs	Use this screen to enable log settings or view the list of activities recorded by your Multy M1.

5.3.2 Bridge Mode Navigation Panel

Figure 38 Navigation Panel (Bridge Mode)



The following table describes the submenus.

Table 9 Settings > System > Status (Bridge Mode)

LINK	TAB	FUNCTION
Overview		Use this screen to: • View read-only information about your Multy M1 • Configure WiFi settings •
Diagnose	Advanced Speed Test	Use this screen to check the speed of the connection between your Multy M1 and the broadband modem/router.
	Speed Test History	Use this screen to view a summary of previously run speed tests.
Mesh	My Mesh	Use this screen to view Mesh network information.
Settings		
WiFi	Main WiFi	Use this screen to enable the wireless LAN and configure wireless LAN and wireless security settings.
	WPS	Use this screen to configure WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
LAN	LAN IP	Use this screen to configure the Multy M1's LAN IP address and subnet mask. Use this screen to configure the Multy M1's DNS server.
System	Status	Use this screen to view the basic information of the Multy M1
	General Setting	Use this screen to change password or to set the timeout period of the management session.
	Remote Access	Use this screen to configure remote assistant.
	Maintenance	Use this screen to upgrade firmware, restart the Multy M1 without turning the power off or reset the Multy M1 to factory default settings.
	Operating Mode	Use this screen to select whether your device acts as a router, or a bridge.
	Logs	Use this screen to view the list of activities recorded by your Multy M1.

CHAPTER 6
Multy M1 Modes

6.1 Overview

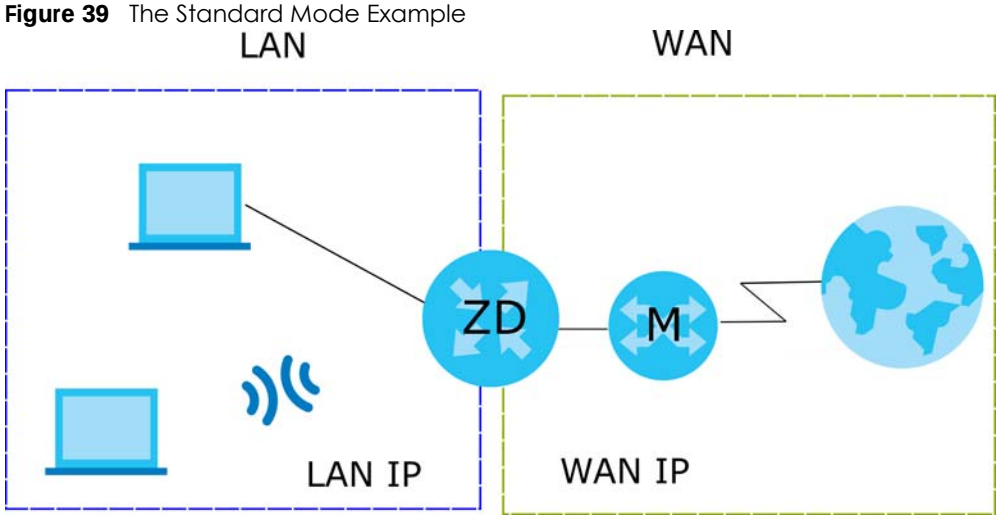
This chapter introduces the different operating modes available on your Multy M1. Or simply how the Multy M1 is being used in the network.

6.2 Modes

This refers to the operating mode of the Multy M1, which can act in:

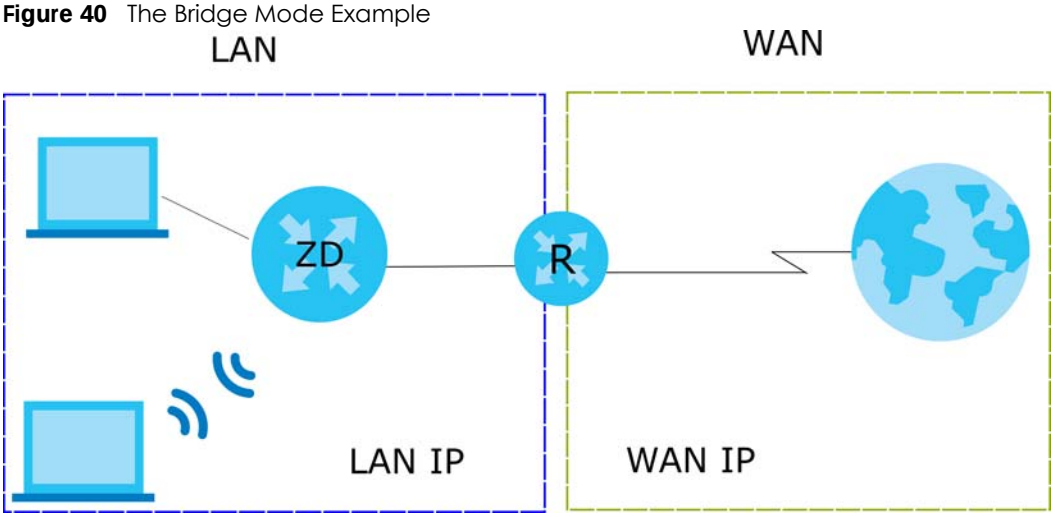
- **Standard Mode**: In standard mode Multy M1 has two IP addresses, a LAN IP address and a WAN IP address. It also has more routing features. To see the standard mode features, go toTable 8 on page 123. In the example scenario below, Multy M1 connects the local network to the Internet through a modem (**M**).

Figure 39 The Standard Mode Example



- **Bridge Mode**: In bridge mode, Multy M1 has one IP address and Multy M1 interfaces are bridged together in the same network. To see the bridge mode features, go to Table 9 on page 125. In the example scenario below, Multy M1 connects the local network to the Internet through a router (**R**).

Figure 40 The Bridge Mode Example



For more information on changing the mode of your Multy M1, refer to Section 7.11 on page 150.

Note: Choose your device mode carefully to avoid having to change it later.

When changing to another mode, the IP address of the Multy M1 changes. The running applications and services of the network devices connected to the Multy M1 may be interrupted.

6.3 Standard Mode Overview

The Multy M1 is set to standard (router) mode by default. Routers are used to connect the local network to another network (for example, the Internet). In the figure below, the Multy M1 connects the local network (**LAN1** ~ **LAN4**) to the Internet.

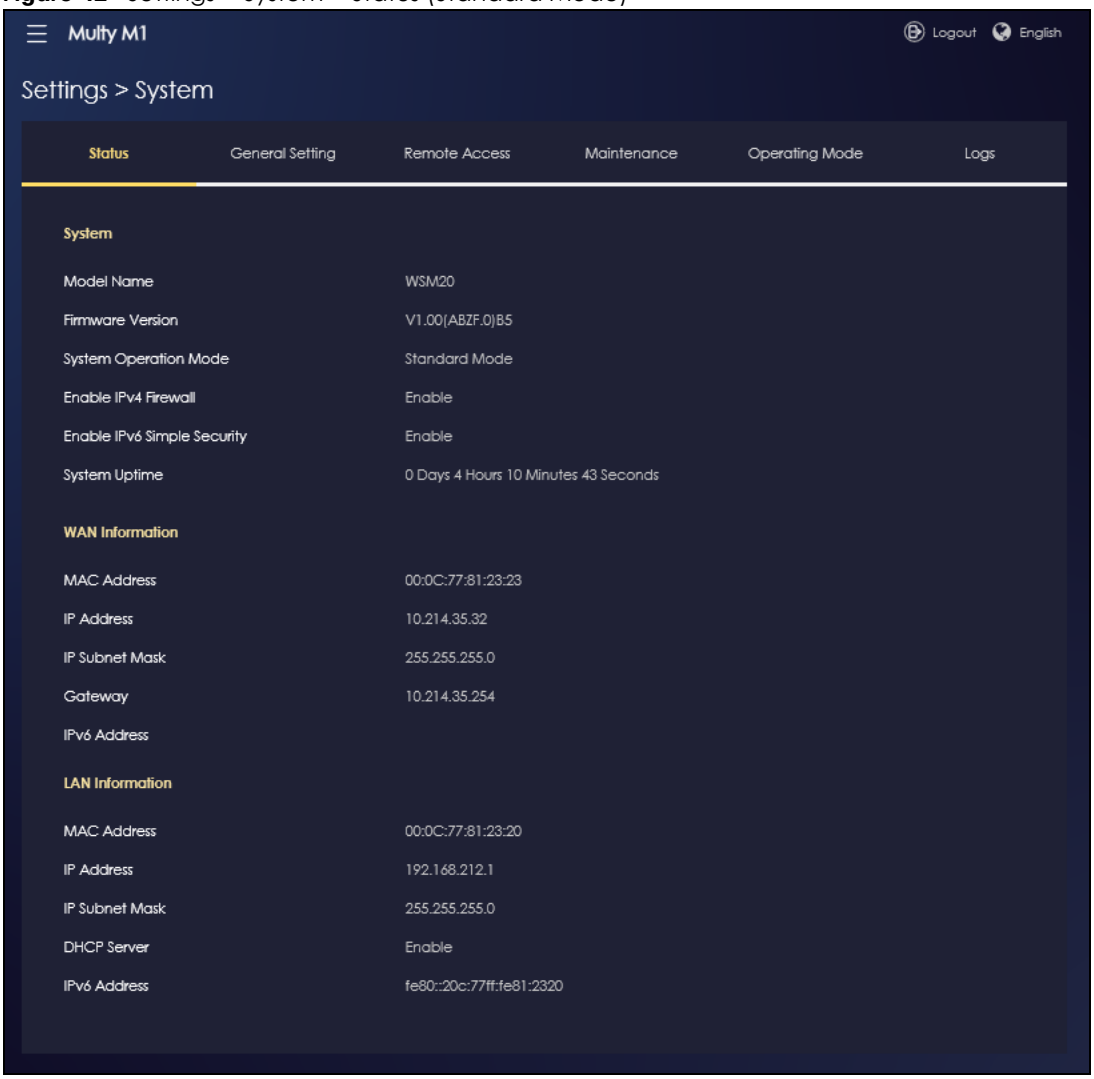
6.4 What You Can Do

- Use the **Status** screen to view read-only information about your Multy M1 (Section 6.5 on page 127).

6.5 Standard Mode Status Screen

Click **Settings** > **System** > **Status** to open the status screen.

Figure 41 Settings > System > Status (Standard Mode)



The following table describes the labels shown on the **Status** screen.

Table 10 Settings > System > Status (Standard Mode)

LABEL	DESCRIPTION
System	
Model Name	This is the model name of your device.
Firmware Version	This is the firmware version.
System Operation Mode	This is the device mode to which the Multy M1 is set, see Section 7.11 on page 150 for more information.
Enable IPv4 Firewall	This shows if the IPv4 firewall is enabled on the Multy M1.
Enable IPv6 Simple Security	This shows if the IPv6 firewall is enabled on the Multy M1.
System Uptime	This is the total time the Multy M1 has been on.
WAN Information	
MAC Address	This shows the WAN Ethernet adapter MAC Address of your device.
IP Address	This shows the WAN port's IP address.

Table 10 Settings > System > Status (Standard Mode) (continued)

LABEL	DESCRIPTION
IP Subnet Mask	This shows the WAN port's subnet mask.
Gateway	This shows the WAN port's gateway IP address.
IPv6 Address	This shows the current IPv6 address of the Multy M1.
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
DHCP Server	This shows the LAN port's DHCP role - **Enable** or **Disable**.
IPv6 Address	This shows the current IPv6 address of the Multy M1 in the LAN.

6.6 Bridge Mode Overview

Use your Multy M1 as a bridge if you already have a router or gateway on your network. In this mode your Multy M1 bridges a wired network (LAN) and wireless LAN (WLAN) in the same subnet. See the figure below for an example.

Many screens that are available in **Standard Mode** are not available in **Bridge Mode**, such as port forwarding and firewall. See Section 5.3 on page 122 for more information.

6.7 What You Can Do

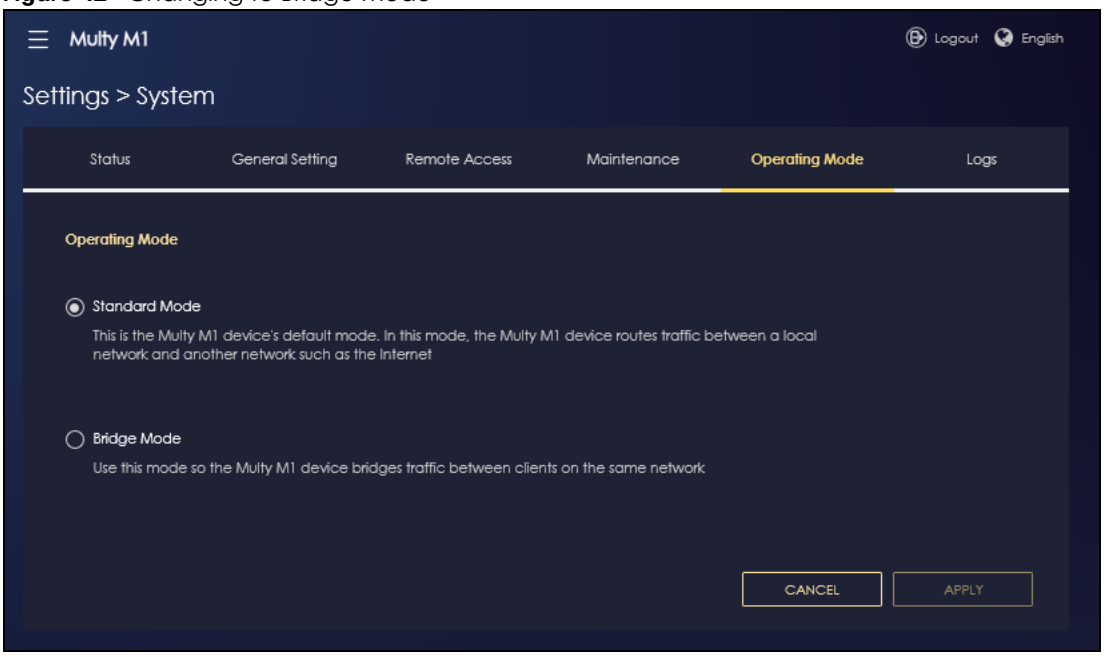
- Set up a network with the Multy M1 as a bridge (Section 6.8 on page 129).
- Use the **Status** screen to view read-only information about your Multy M1 (Section 6.9 on page 131).

6.8 Setting your Multy M1 to Bridge Mode

1. Log into the Web Configurator if you haven't already. See the Quick start Guide for instructions on how to do this.
2. To use your Multy M1 as a bridge, go to **Settings > System > Operating Mode** and select **Bridge Mode**.

Note: You can only set the Multy M1 to Bridge Mode when using the Internet Protocol over Ethernet (IPoE) WAN service.

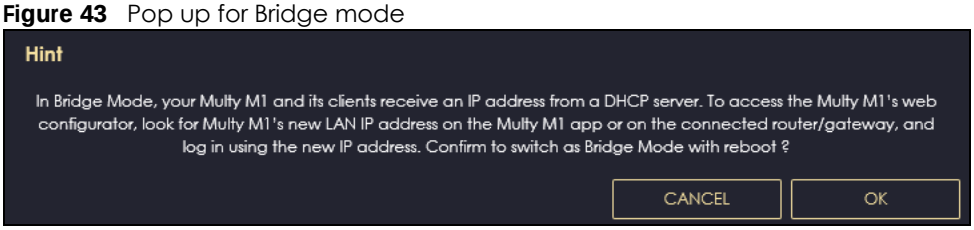
Figure 42 Changing to Bridge mode



Note: You have to log in to the Web Configurator again when you change modes. As soon as you do, your Multy M1 is already in Bridge mode.

3 When you select **Bridge Mode**, the following pop-up message window appears.

Figure 43 Pop up for Bridge mode



Click **OK**. Then click **Apply**. The Web Configurator refreshes once the change to Bridge mode is successful.

6.8.1 Accessing the Web Configurator in Bridge Mode

Log in to the Web Configurator in Bridge mode, do the following:

1 Log into the Web Configurator. See the Quick Start Guide for instructions on how to do this.

2 Connect your computer to one of the LAN port of the Multy M1using an Ethernet cable.

3 Connect a modem/router to the WAN port of the Multy M1 using another Ethernet cable.

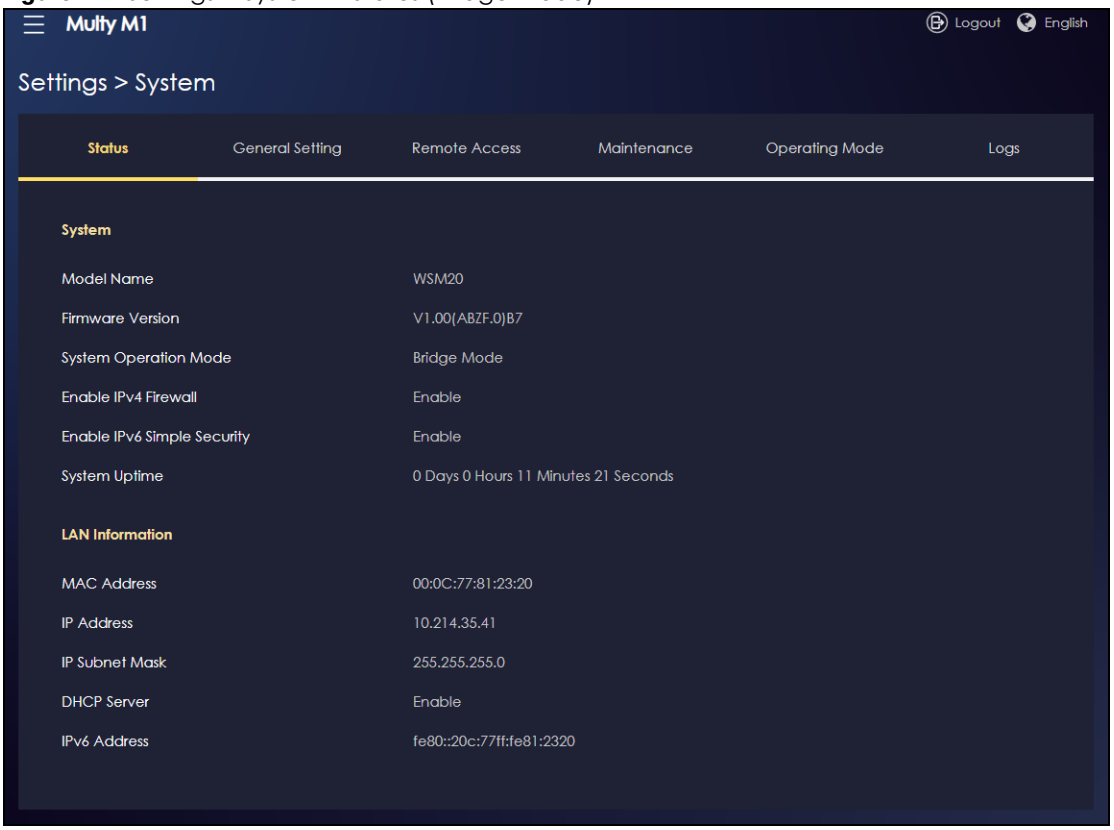
4 If the Multy M1 is not connected to a router or DHCP server, the Multy M1 cannot assign your computer an IP address.

5 After you've set your computer's IP address, open a web browser such as Internet Explorer and enter "http://(DHCP-assigned IP) as the web address in your web browser.

6.9 Bridge Mode Status Screen

Click **Settings** > **System** > **Status** to open the status screen.

Figure 44 Settings > System > Status (Bridge Mode)



The following table describes the labels shown on the **Status** screen.

Table 11 Settings > System > Status (Bridge Mode)

LABEL	DESCRIPTION
System	
Model Name	This is the model name of your device.
Firmware Version	This is the firmware version.
System Operation Mode	This is the device mode to which the Multy M1 is set, see Section 7.11 on page 150 for more information.
Enable IPv4 Firewall	This shows if the IPv4 firewall is enabled on the Multy M1.
Enable IPv6 Simple Security	This shows if the IPv6 firewall is enabled on the Multy M1.
System Uptime	This is the total time the Multy M1 has been on.
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
DHCP Server	This shows the LAN port's DHCP role - **Enable** or **Disable**.
IPv6 Address	This shows the current IPv6 address of the Multy M1 in the LAN.

CHAPTER 7
Multy M1 Web Configurator Tutorials

7.1 Overview

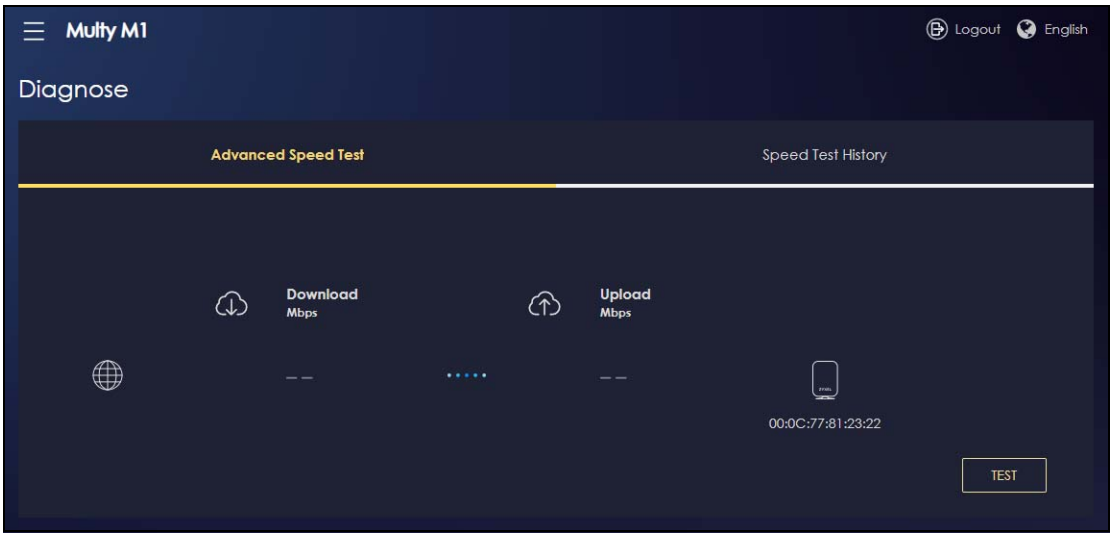
This chapter provides tutorials for setting up your Multy M1.

- Run a Speed Test
- Configure the Multy Devices in a Mesh Network
- Configure Main WiFi Networks
- Configure Guest WiFi Networks
- Configure Parental Control Schedule
- Configure a Firewall Rule
- Configure the Multy M1 as an OpenVPN Server
- Configure the Multy M1 as an OpenVPN Client
- Change the Web Configurator Local Password
- Change the Operating Mode
- Configure a Port Forwarding Rule

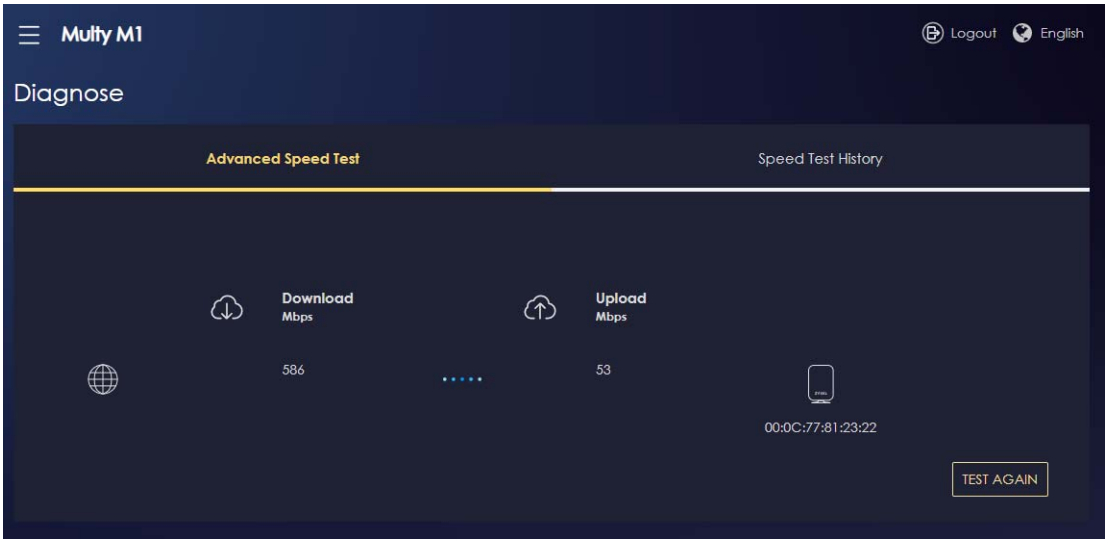
7.2 Run a Speed Test

With the Multy M1 Web Configurator, you can check the speed of the connection between your Multy M1 and the broadband modem/router.

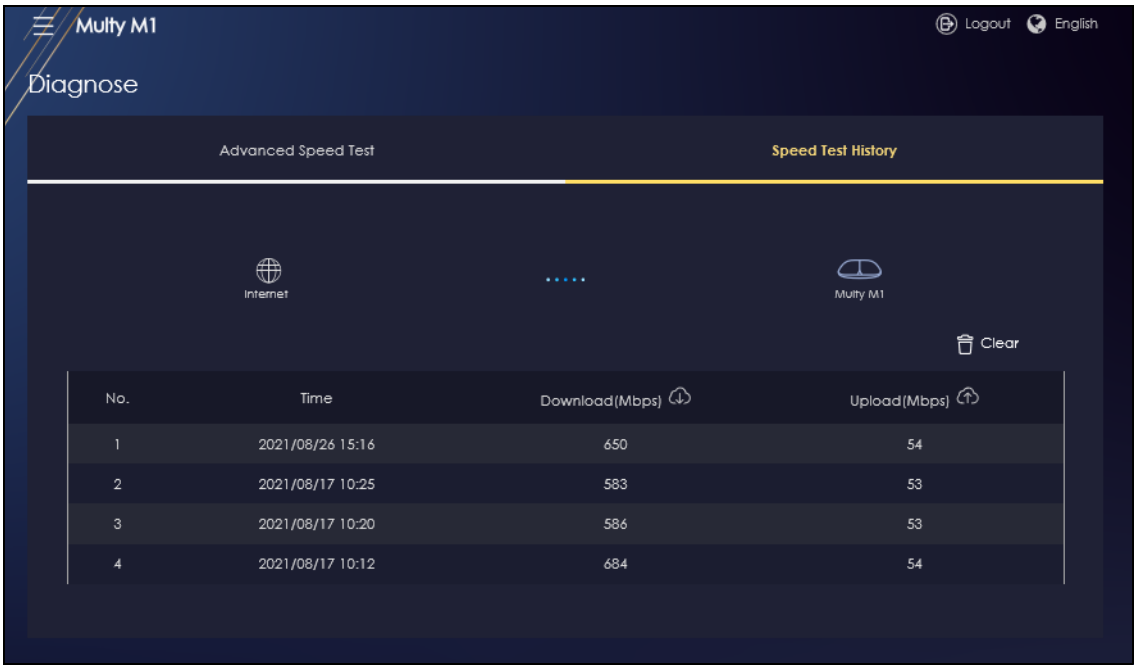
1 Click the **Navigation Panel** icon on the top-left corner ( ), and click **Diagnose** to open the **Advanced Speed Test** screen. Use this screen to view all the available connections in your Multy M1 System.



2 Click **TEST** to perform a speed test. This shows data rates for both upstream and downstream traffic. Click **TEST AGAIN** to update the information.

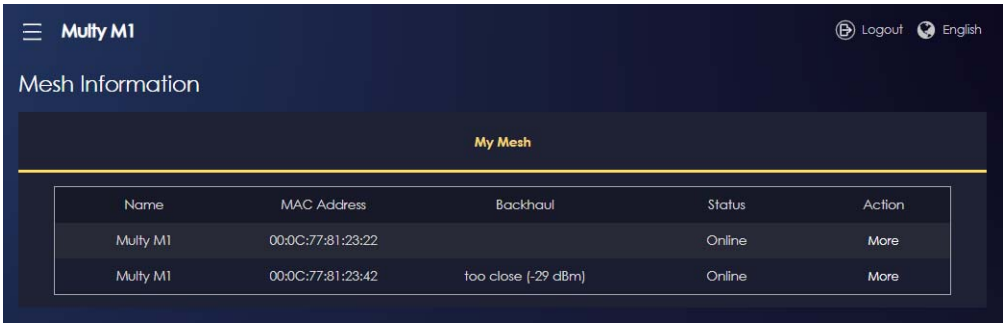


3 Click the **Speed Test History** tab to view a summary of the tests made. Click **Clear** to delete all records.

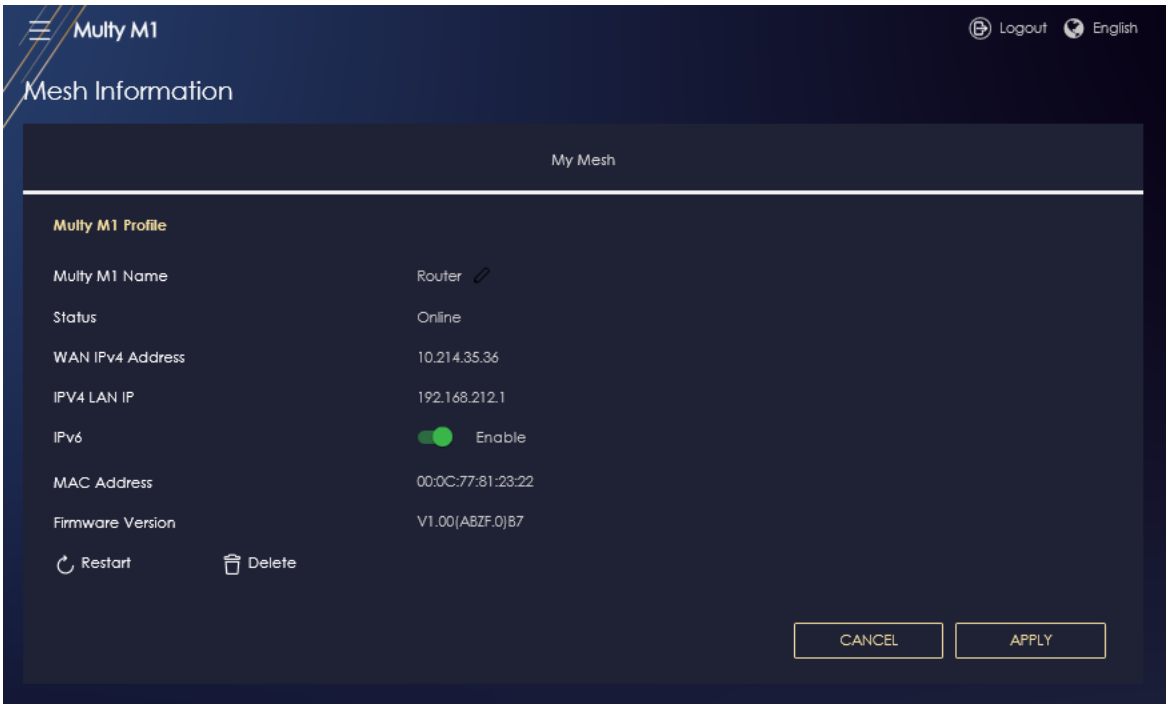


7.3 Configure the Multy Devices in a Mesh Network

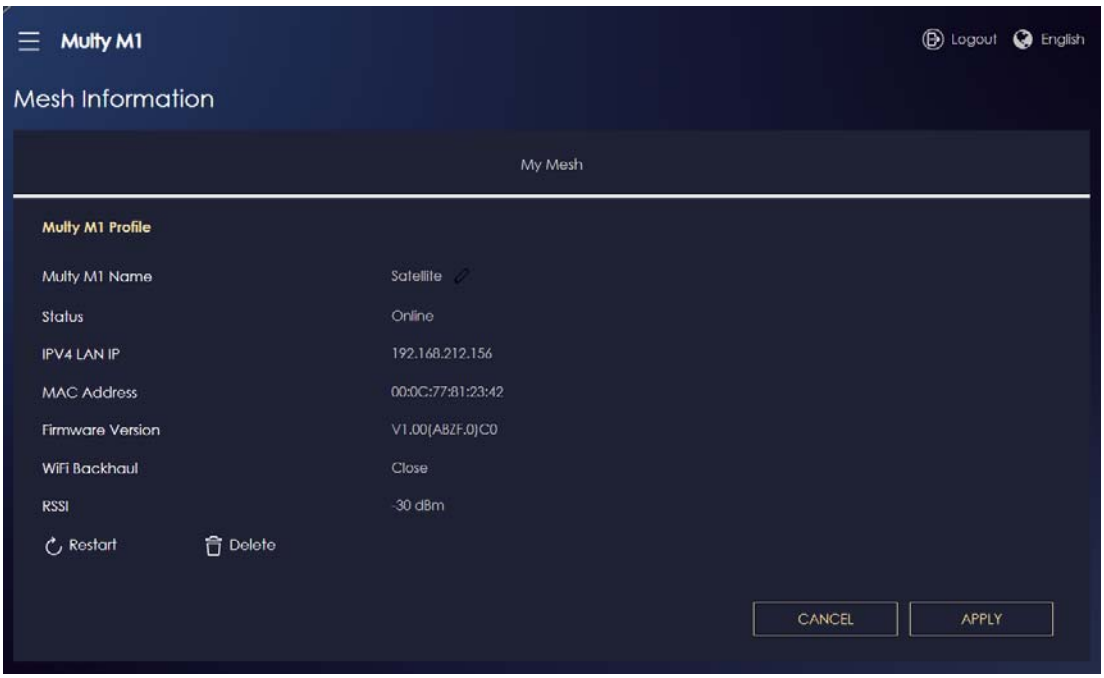
1 Click the **Navigation Panel** icon on the top-left corner ( ), and click **Mesh** to open the **Mesh Information** screen. Click **More** to modify the assigned roles of Multy M1's mesh networks.



2 Click **More** of the Multy M1 router, the following screen appears. Click the **Edit**( ) icon on the Multy Router page to modify the name of the Multy M1 router. Click the **Restart** ( ) icon to reboot the Multy M1 router. Click the **Delete** ( ) icon to remove the assigned roles of the controller and extender of the mesh network, reseting all of the devices of the Mesh network to factory default settings. Click **APPLY** to save the changes.



3 Click **More** of the Multy M1 extender, the following screen appears. Click the **Edit**( ) icon on the satellite page to modify the name of the Multy M1 extender. Click the **Restart** ( ) icon to reboot the Multy M1 extender. Click the **Delete** ( ) icon on the satellite page to remove the assigned role of the extender, reseting the Multy M1 extender to factory default settings. Click **APPLY** to save the changes.



7.4 Configure Main WiFi Networks

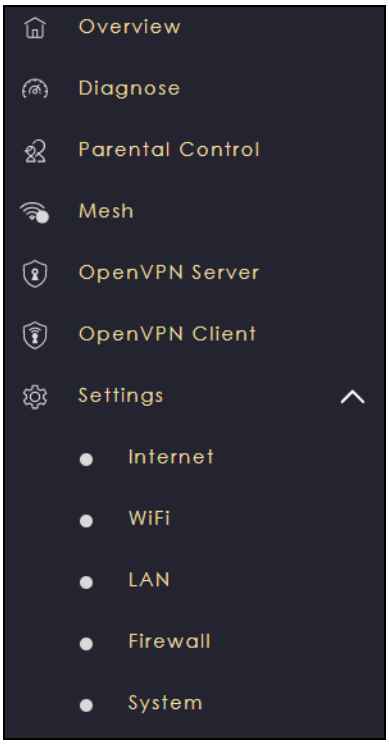
In the Multy M1 you can configure independent wireless networks with different privileges. Clients can associate only with the network for which they have security settings (SSID and password). The following table describes the different Multy M1's profile networks and their privileges.

Table 12 WiFi Network Privileges

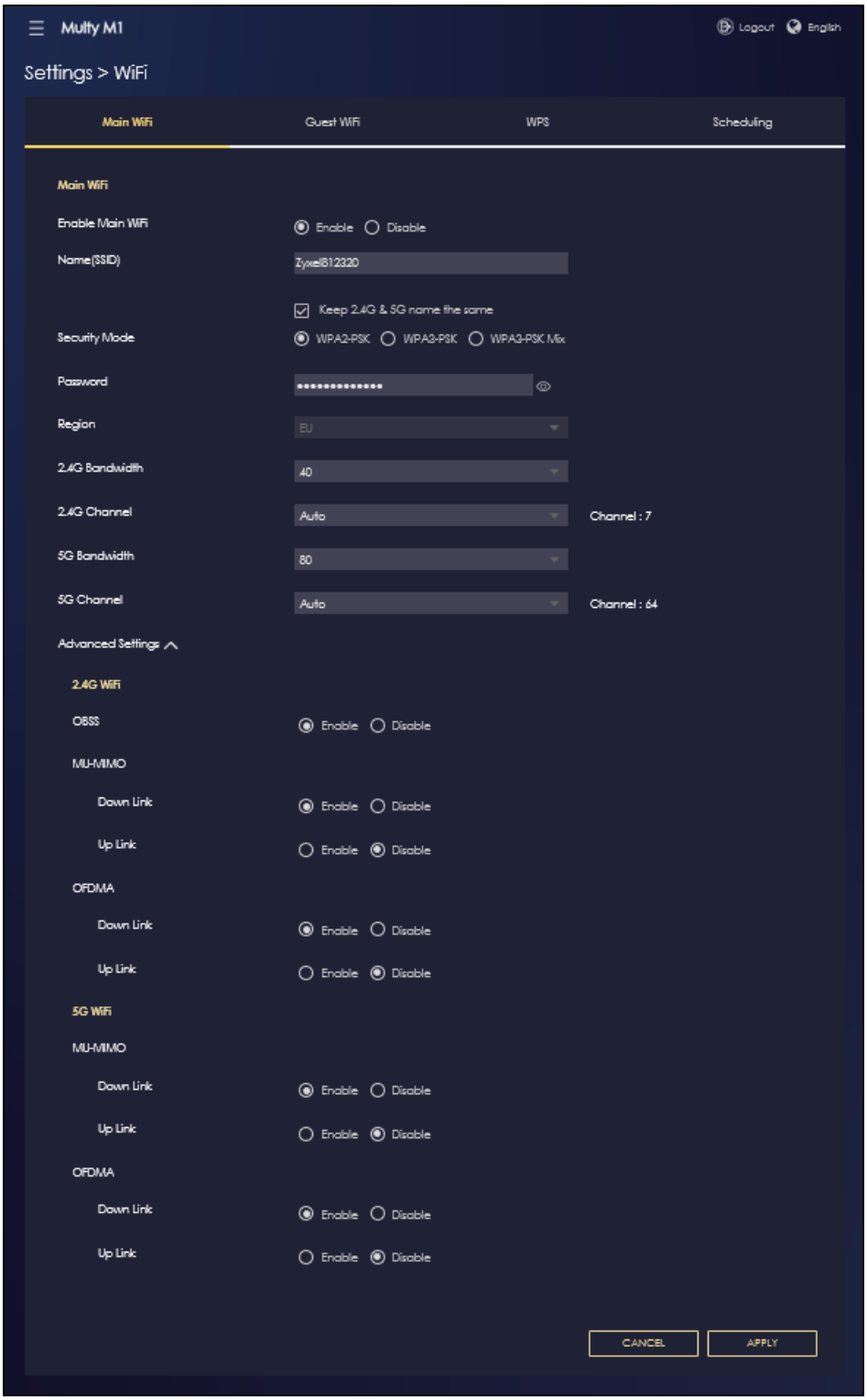
WIFI NETWORK	INTERNET ACCESS	2.4G / 5G WIFI NETWORK	ACCESS TO WEB CONFIGURATOR	ACCESS TO WIRED LAN
Main WiFi	Yes	2.4G and 5G	Yes	Yes
Guest WiFi	Yes	2.4G and 5G	No	No

Note: A user can only configure the WiFi networks' security settings if they are connected to the **Main WiFi** network.

1 Click the **Navigation Panel** icon on the top-left corner ( ), and click **Settings** to open the **WiFi** screen. Use each tab in the **WiFi** menu to configure each of the WiFi networks' security settings.



2 Select **Enable Main WiFi** to activate a WiFi Network. Enter the **2.4G/5G Name** and **Password** clients use to connect to the WiFi network. You can configure two different WiFi Names for the **Main WiFi** 2.4G and 5G networks. Select **Keep 2.4G & 5G name the same,** so they both use the same WiFi Name. Click **Apply** to save your changes.

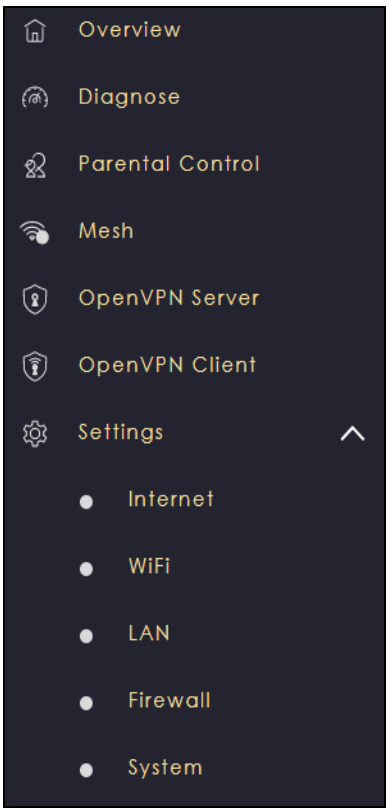

Multy M1
Logout
English
Settings > WiFi
Main WiFi
Guest WiFi
WPS
Scheduling
Main WiFi
Enable Main WiFi
Enable
Disable
Name(SSID)
Zyxel812320
Keep 2.4G & 5G name the same
Security Mode
WPA2-PSK
WPA3-PSK
WPA3-PSK Mix
Password
Region
EU
2.4G Bandwidth
40
2.4G Channel
Auto
Channel : 7
5G Bandwidth
80
5G Channel
Auto
Channel : 64
Advanced Settings
2.4G WiFi
OBSS
Enable
Disable
MU-MIMO
Down Link
Enable
Disable
Up Link
Enable
Disable
OFDMA
Down Link
Enable
Disable
Up Link
Enable
Disable
5G WiFi
MU-MIMO
Down Link
Enable
Disable
Up Link
Enable
Disable
OFDMA
Down Link
Enable
Disable
Up Link
Enable
Disable
CANCEL
APPLY

7.5 Configure Guest WiFi Networks

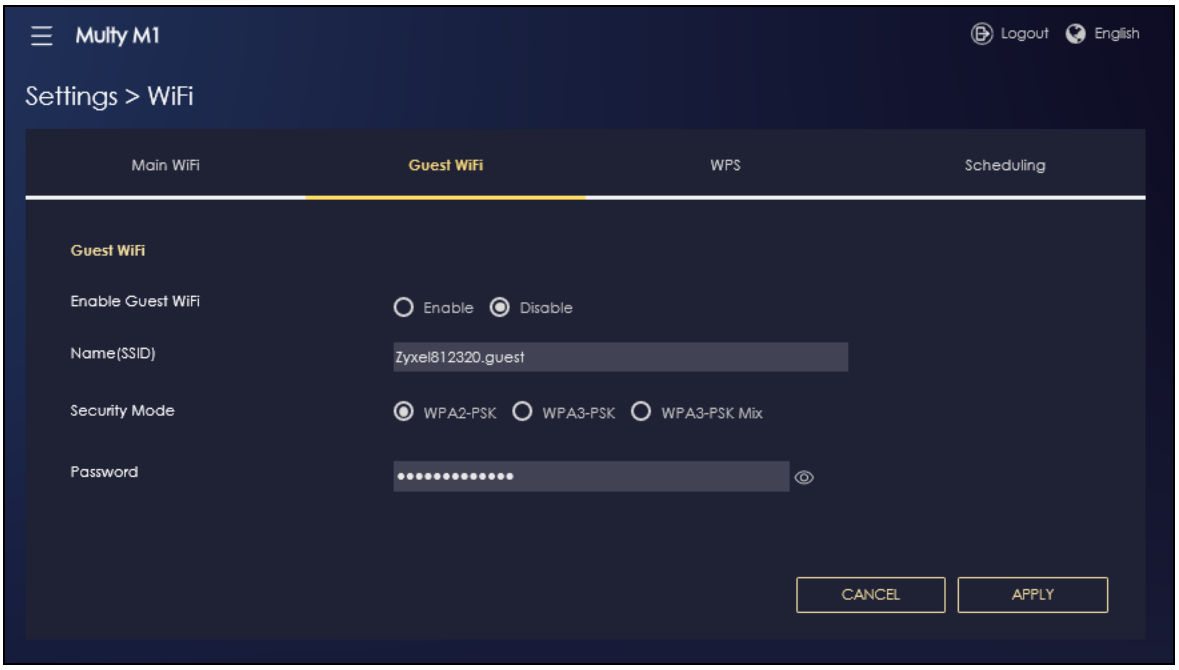
After the Multy M1 is set up, you can use separate WiFi networks for your clients. The WiFi settings will be applied to all clients in the same network.

Note: This is not available if you are using bridge mode.

1 Click the **Navigation Panel** icon on the top-left corner ( ), and click **Settings > WiFi > Guest WiFi** to open the **Guest WiFi** screen.



2 Select **Enable Guest WiFi** and enter the **WiFi Name (SSID)** and **WiFi Password**. Click **Apply** to save your changes.



7.6 Configure Parental Control Schedule

This section shows you how to configure times for accessing the Internet using parental control.

7.6.1 Create a Parental Control Profile

Parental Control Profile allows you to set up a rule to schedule Internet usage. Use this feature to limit the days and times a WiFi client can access the Internet through the Multy M1.

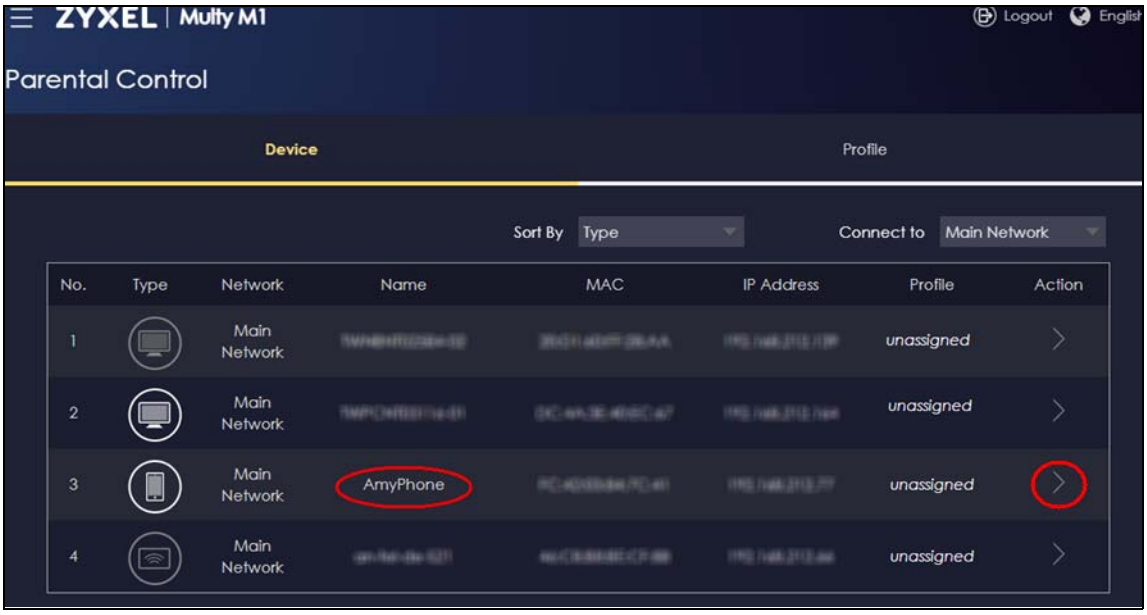
This example shows you how to block a client from accessing the Internet during time for studying. The following example uses the parameters below to configure a **Study** schedule rule.

Table 13 Parental Control Example Parameters

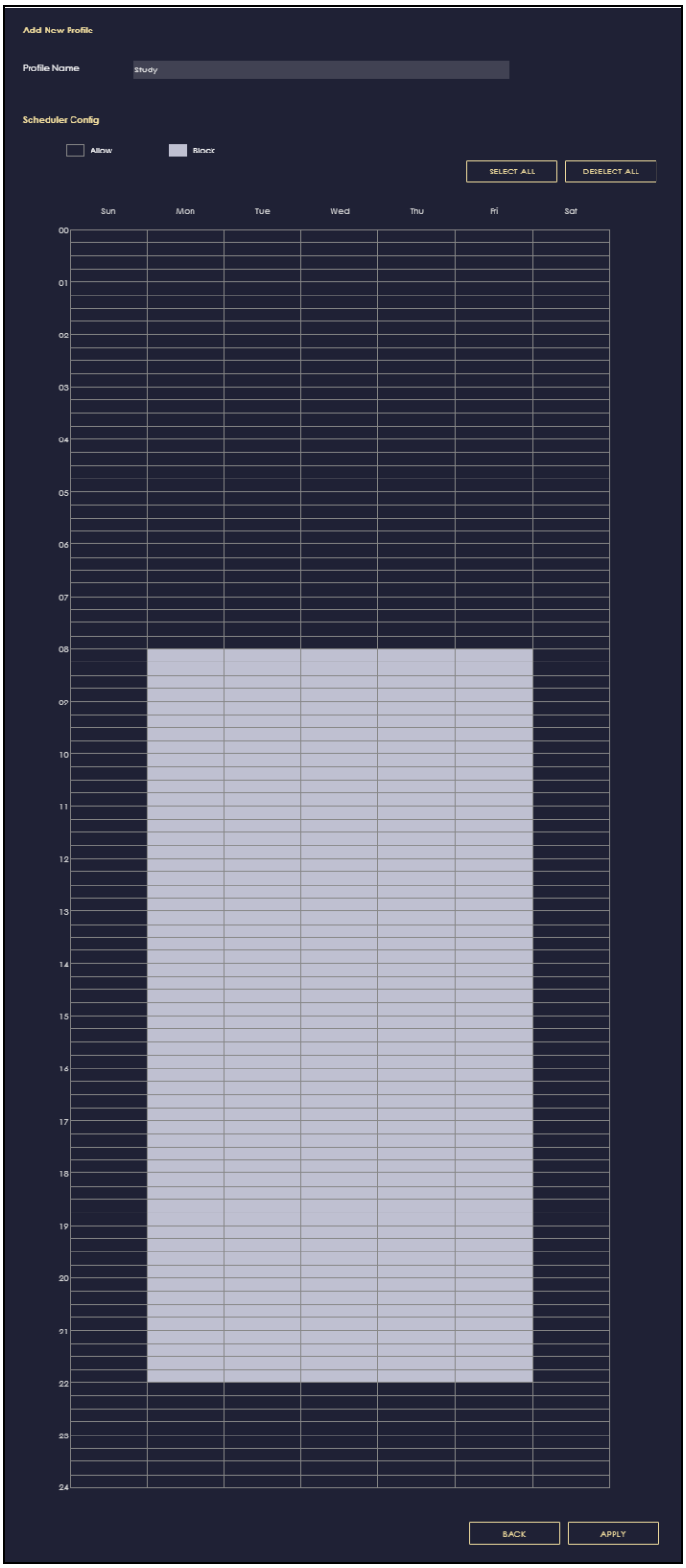
BLOCKED CLIENT	PROFILE NAME	START BLOCKING	END BLOCKING	ENABLED ON
AmyPhone	Study	8:00 am	10:00 pm	from Monday to Friday

Note: **Parental Control** is not available if you are using bridge mode.

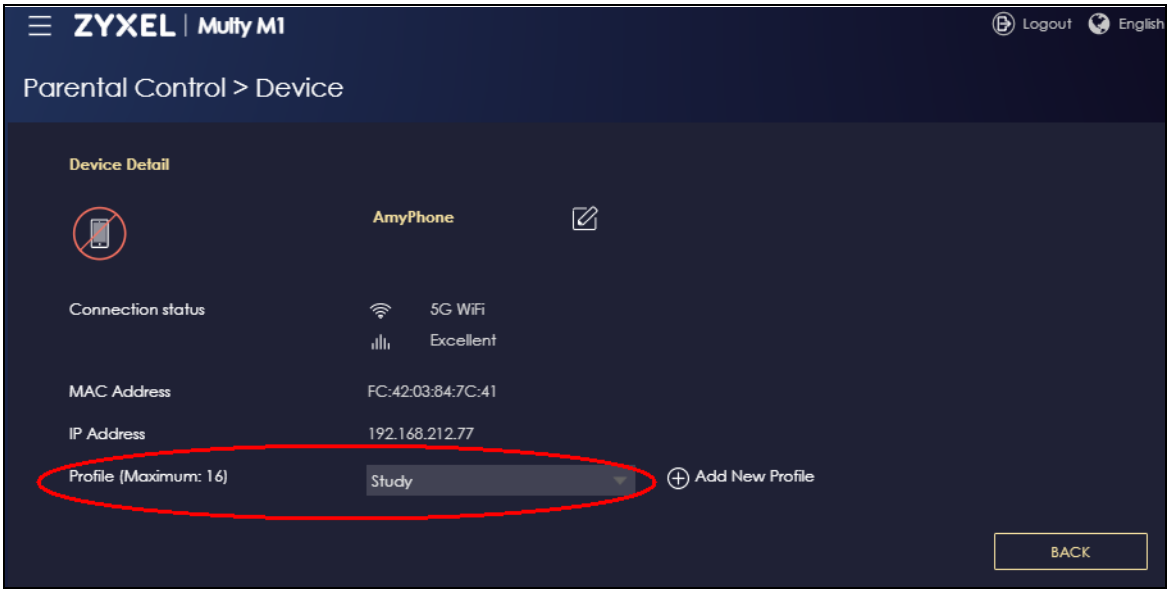
1 Go to **Parental Control** > **Device** to view the clients connected to your Multy M1. Find the client you want to block then click the action icon ( ).



2 Click **Add New Profile** in the **Device Detail** screen to configure the parental control profile schedule. Use the parameters given above to configure the time settings. Click **Apply** to save your settings.


Add New Profile
Profile Name
Study
Scheduler Config
Allow
Block
SELECT ALL
DESELECT ALL
Sun
Mon
Tue
Wed
Thu
Fri
Sat
00
01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
BACK
APPLY

3 After you click **Apply**, the Multy M1 web configurator will go to the **Parental Control** > **Device** > **Device Detail** screen. Make sure the parental control profile you created has been applied to the specific client.



Disable a Parental Control Profile

You can disable the parental control profiles to stop the Multy M1 from blocking the connected clients during the time you set.

Suppose you no longer need to block a specific client from accessing the Internet during the time for studying. Go to **Parental Control** > **Profile** and find the **Study** profile. Slide the switch to the left ( ) to disable the profile.

7.7 Configure a Firewall Rule

This section shows you how to enable the firewall to protect your network from malicious attacks from the Internet.

7.7.1 Enable Respond to Ping and Firewall

Enable **Respond to Ping** to activate Internet Control Message Protocol (ICMP) on the Multy M1. Enable **Firewall** to protect the Multy M1 from DoS attacks.

ICMP

Internet Control Message Protocol (ICMP) is a message control and error-reporting protocol between a host server and a gateway to the Internet. Enable this to have the Multy M1 respond only to incoming Ping requests from the specified interface. Attackers can ping the devices to find their locations through their responds then attack them. If you set the Multy M1 to not respond to Ping requests from the WAN,

the attackers will not be able to find the Multy M1 since they can't receive responds from it. This will prevent the Multy M1 from been attacked.

DoS

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. It can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable.

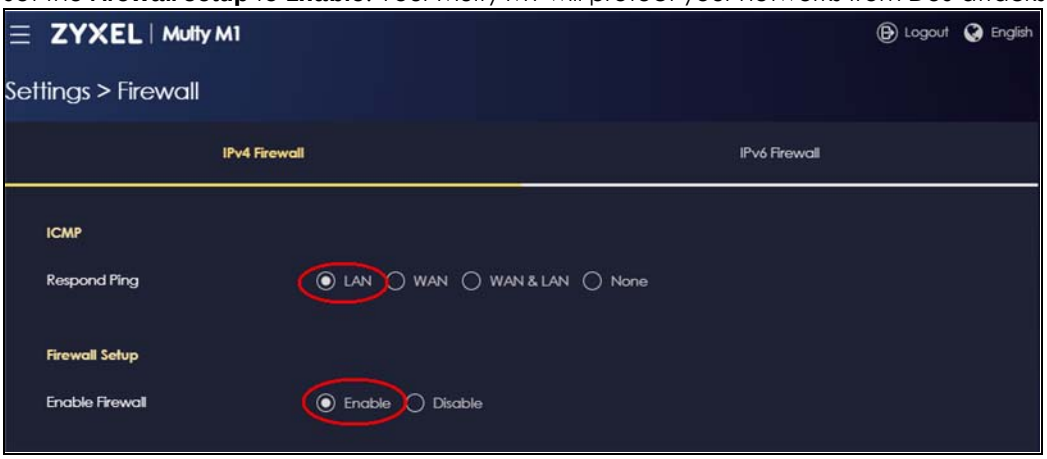
The following example uses the parameters below to configure an example Multy M1 firewall rule to enable ICMP and firewall.

Table 14 Firewall Rule Example Parameters

RESPOND PING	FIREWALL SETUP
LAN	Enable

Go to **Settings** > **Firewall**. Set the **Respond Ping** to **LAN**. Your Multy M1 will now only respond to ping requests from the LAN.

Set the **Firewall Setup** to **Enable**. Your Multy M1 will protect your networks from DoS attacks.



7.7.2 Enable Access Control

An access control rule is a manually-defined rule that can drop or accept incoming or outgoing packets from your network.

Block Access to a Specified IP Address

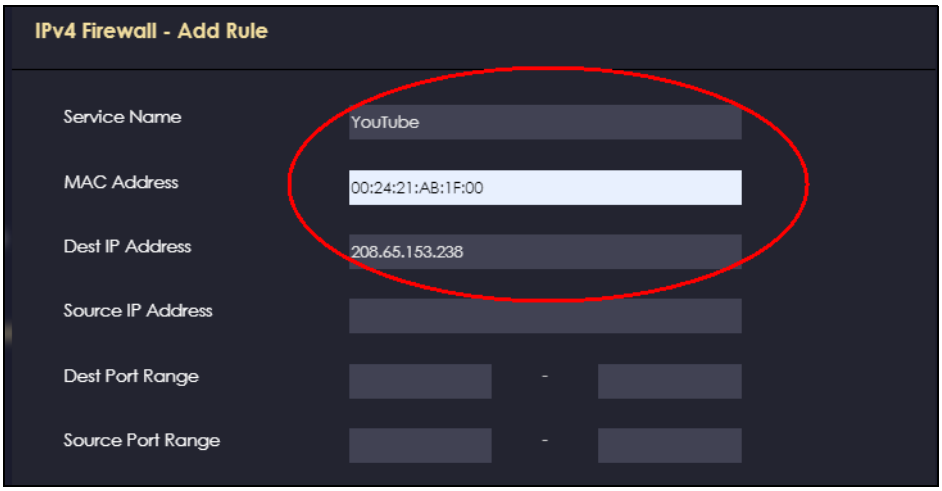
The example below shows you how to block your son's computer MAC address from accessing YouTube without blocking other clients. The following example uses the parameters below to configure the access control rule.

Table 15 Access Control Rule Example Parameters

SERVICE NAME	DESTINATION IP ADDRESS	MAC ADDRESS	ACTIONS
YouTube	208.65.153.238	00:24:21:AB:1F:00	Drop

1 Set **Rule Status** to **Enable** and **Actions** to **Drop**.

2 Click **Add Rule** and enter the service name, destination IP address and MAC address as given above.



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

Block Packets from a Specified IP Address

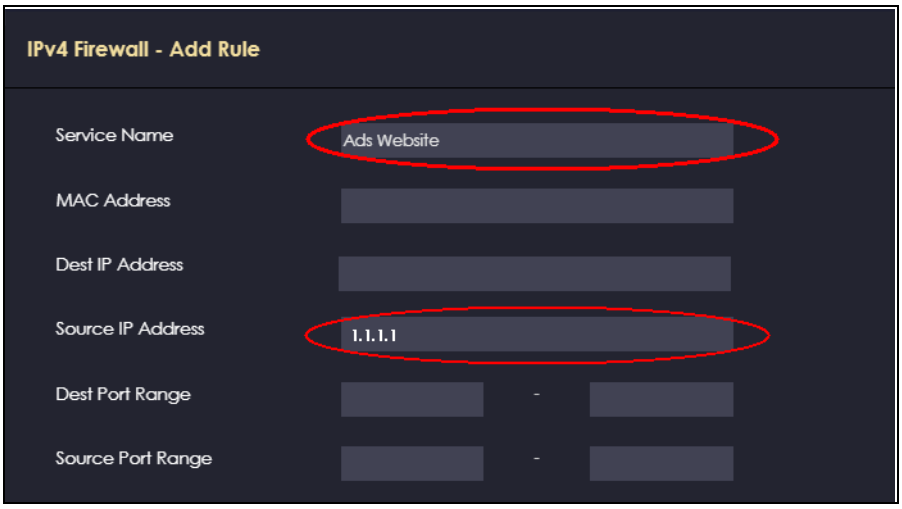
The example below shows you how to block an advertisement website from sending packets to all clients connected to the Multy M1. The following example uses the parameters below to configure the access control rule.

Table 16 Access Control Rule Example Parameters

SERVICE NAME	SOURCE IP ADDRESS	ACTIONS
Ads Website	1.1.1.1	Drop

1 Set **Rule Status** to **Enable** and **Actions** to **Drop**.

2 Click **Add Rule** and enter the service name and source IP address as given above.

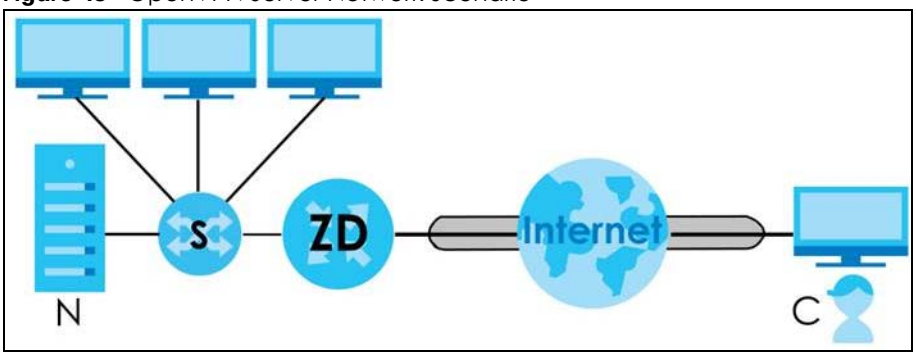


3 Click **Apply** to save your changes.

7.8 Configure the Multy M1 as an OpenVPN Server

OpenVPN is a VPN protocol which is open source and free of charge. It can be used to create a virtual private network or to connect local networks.

Figure 45 OpenVPN Server Network Scenario



The labels used in the graphic are explained below:

- **C**- A client device connected to the OpenVPN server. Make sure to install OpenVPN client software on the client device first.
- **ZD**- A Multy M1 that serves as the OpenVPN server.
- **S**- A switch that connects the Multy M1 and the local network.
- **N**- A local network behind the OpenVPN sever.

The example below shows you how to set up your Multy M1 as an OpenVPN server for employees that are working from home to access the company's local network. You can create separate OpenVPN server accounts for employees in different departments.

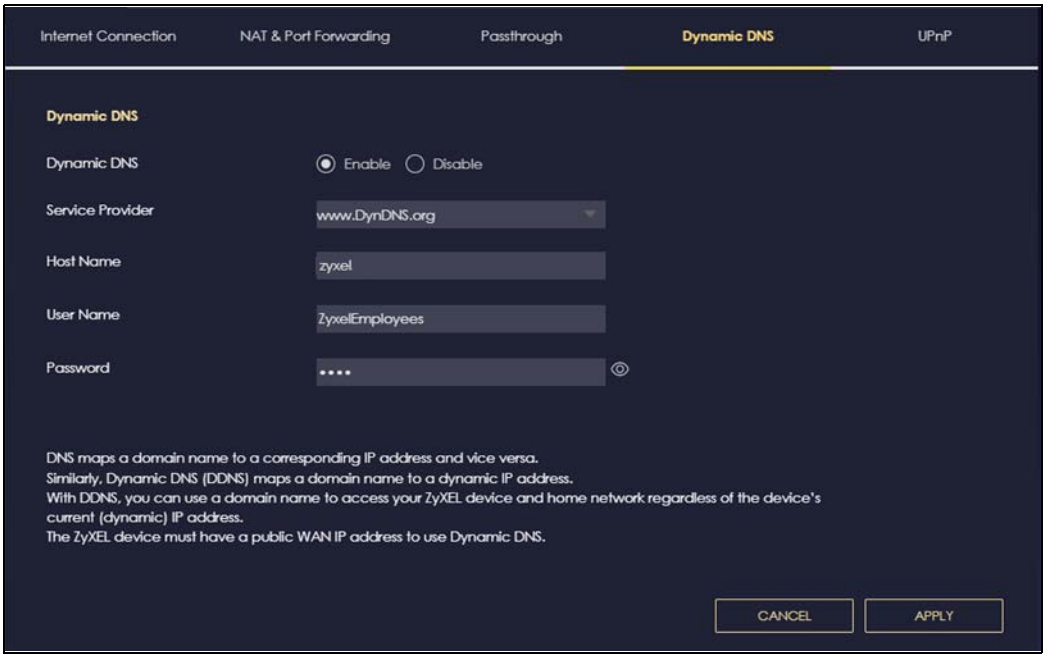
Note: **OpenVPN Server** is not available if you are using bridge mode.

The following example uses parameters below to configure the **OpenVPN Server** settings.

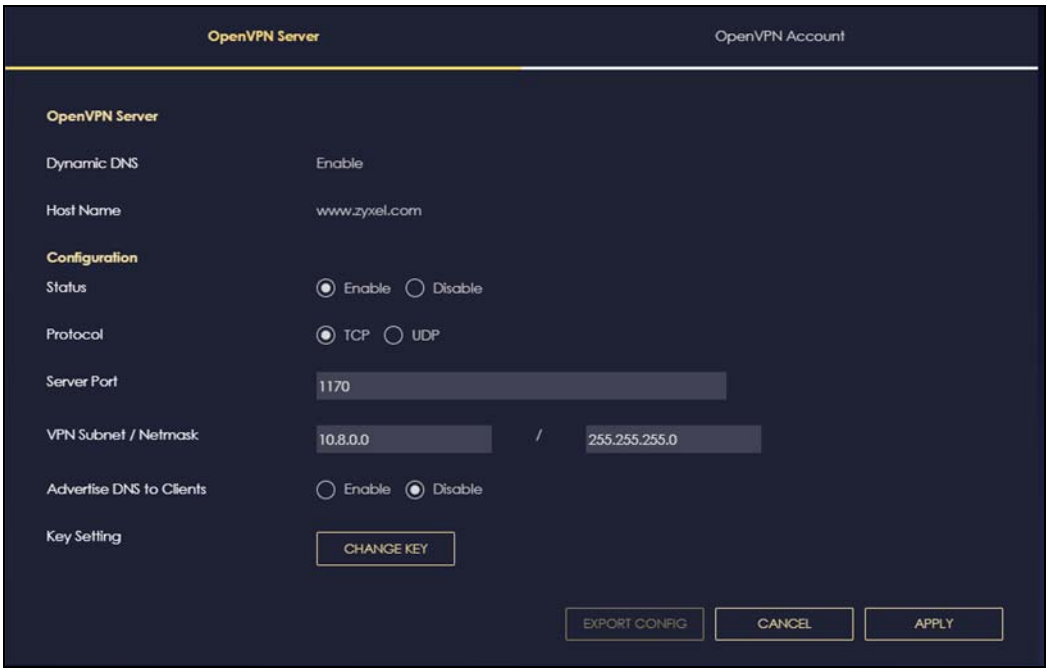
Table 17 OpenVPN Server Example Parameters

DDNS	OPENVPN SERVER	OPENVPN SERVER ACCOUNT
Service Provider: www.DynDNS.org Host Name: zyxel User Name: ZyxelEmployees Password: 1234	Protocol: TCP Server Port: 1170 VPN Subnet: 10.8.0.0 Advertise DNS to Clients: Disable	Account Username: PM Account Password: PM1234 Client Access Allowed: WAN Account Username: RD Account Password: RD1234 Client Access Allowed: WAN

1 Go to **Internet** > **Dynamic DNS** and select **Enable**.



2 Go to the **OpenVPN Server** screen.



3 Go to the **OpenVPN Account** screen. You can view the connection status of each account in this screen.

7.9 Configure the Multy M1 as an OpenVPN Client

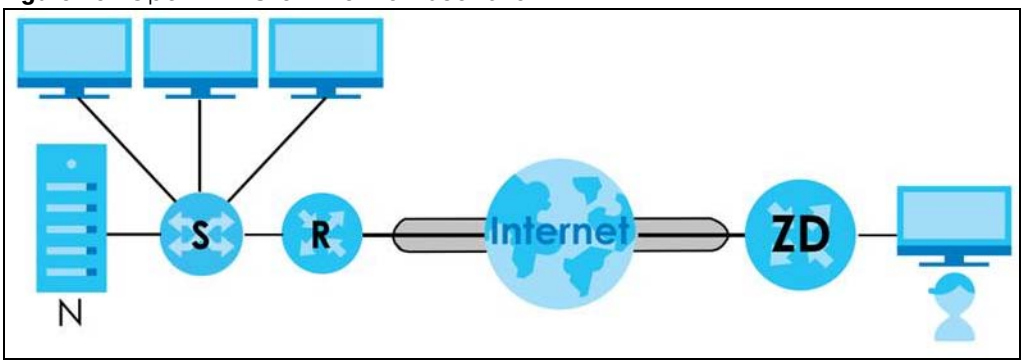
You're running a gaming company branch office in Taiwan. The gaming server is set up in Japan. The example below shows you how to set up your Multy M1 as an OpenVPN client for Taiwan players to

access the gaming server in Japan. Players will not have to set up VPN clients on their own computers individually.

Note: Do not activate OpenVPN Server and OpenVPN Client at the same time on the same Multy M1. The Multy M1 can only connect to one server at a time.

Note: **OpenVPN Client** is not available if you are using bridge mode.

Figure 46 OpenVPN Client Network Scenario



The labels used in the graphic are explained below:

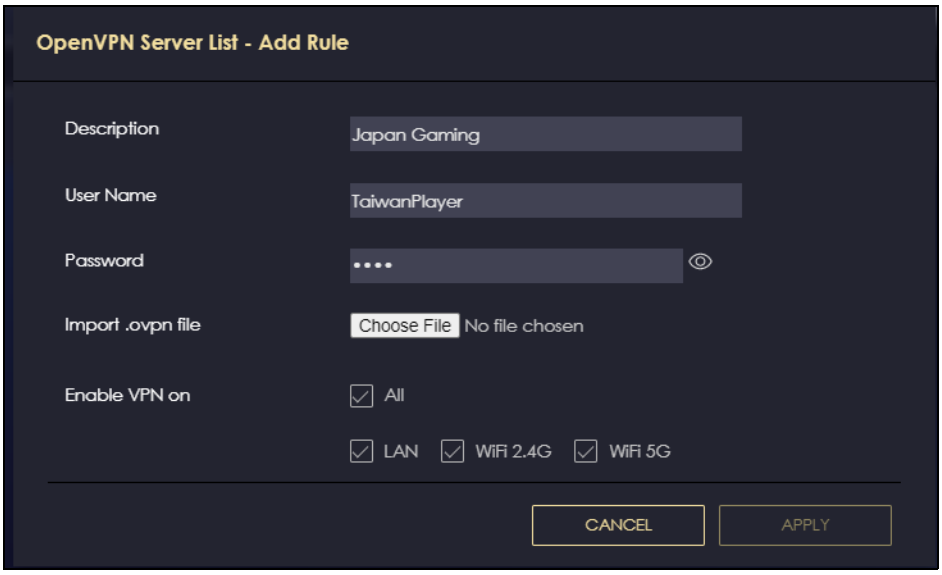
- **ZD**- A Multy M1 that serves as the OpenVPN client.
- **R**- A router that serves as the OpenVPN server.
- **S**- A switch that connects the OpenVPN server and the local network.
- **N**- A local network behind the OpenVPN sever.

The following example uses the parameters below to configure the **OpenVPN Client** settings.

Table 18 OpenVPN Client Example Parameters

DESCRIPTION	USER NAME	PASSWORD
Japan Gaming	TaiwanPlayer	1234

1 Go to the **OpenVPN Client** screen.



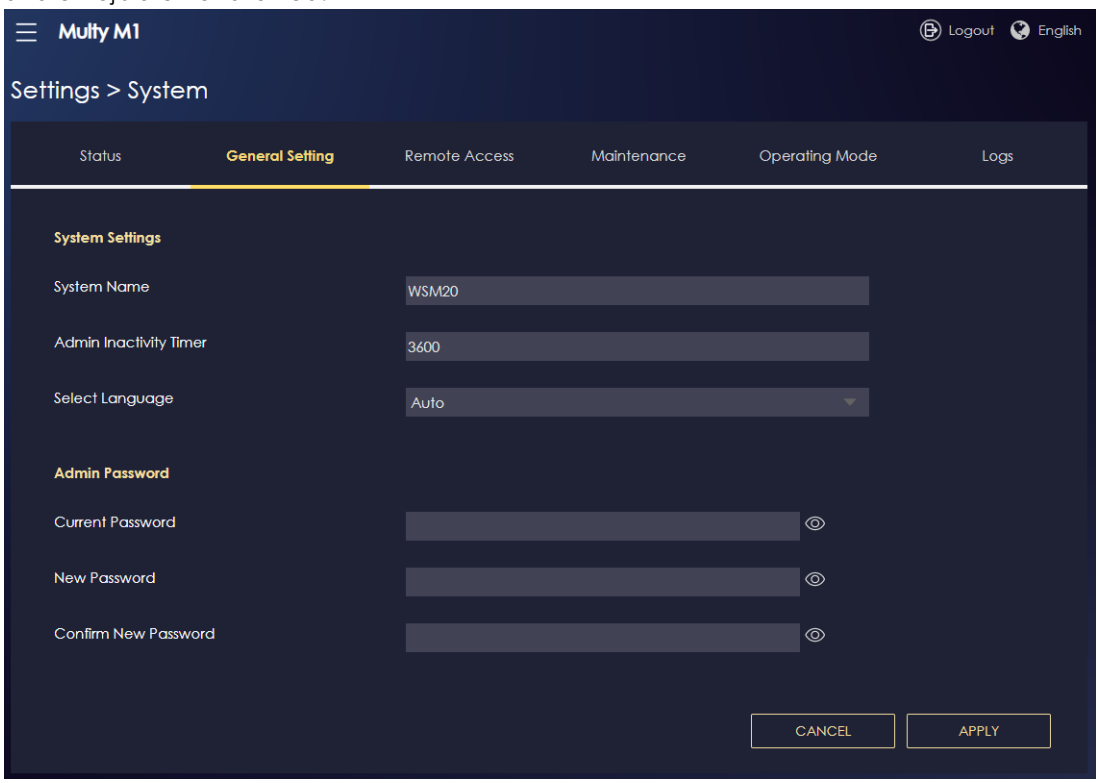
2 Request for an .ovpn file from the OpenVPN server your Multy M1 will connect to and import it. The file should include the OpenVPN server settings.

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

7.10 Change the Web Configurator Local Password

Go to **Settings > System > General Setting** screen to change your web configurator local password. Enter the **Current Password** and **New Password** and enter the new password again to confirm. You can tap the Visibility( ) icon to see the hidden passwords. Click **Apply** to save the changes.

The password should be 8 to 32 single-byte or double-byte characters. Spaces are allowed. \"'‘<>^$& and emojis are not allowed.



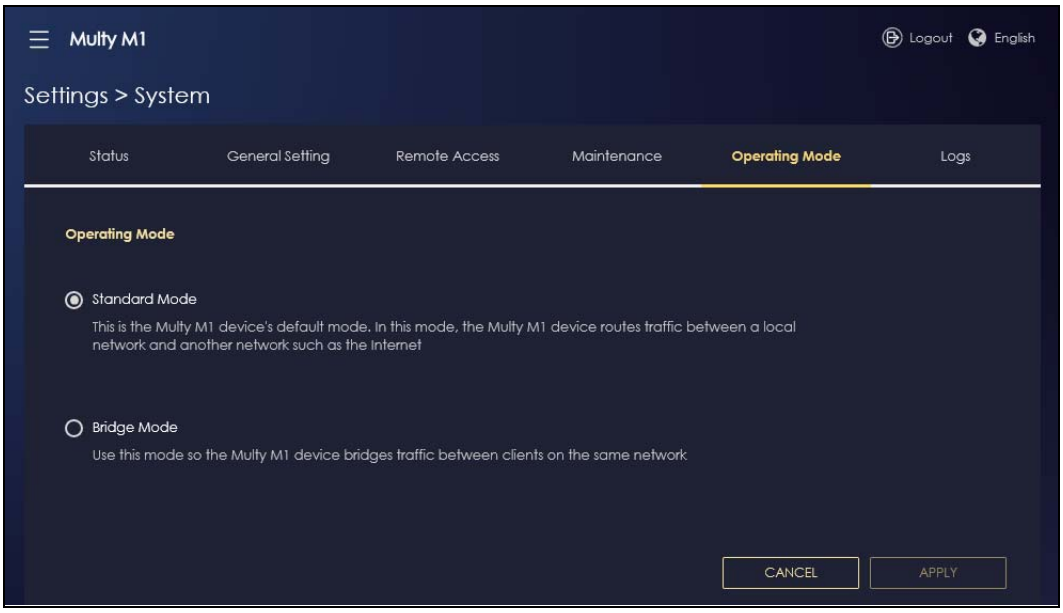
7.11 Change the Operating Mode

The operating mode refers to how the Multy M1 is being used in the network. The Multy M1 has two operating modes:

- **Standard:** This is the Multy M1's default mode. In this mode, the Multy M1 routes traffic between a local network and another network such as the Internet.
- **Bridge:** Use this mode so the Multy M1 bridges traffic between clients on the same network.

Note: The Parental Control, UPnP, Port Forwarding functions are not available in Bridge mode.

1 Click the **Navigation Panel** icon on the top-left corner ( ).From the **Settings** drop-down list, click **System**, then click the **Operating Mode** tab. Select the operating mode you want to use and select **APPLY** to save the changes. Changing the Multy M1's operating mode may take up to two minutes.

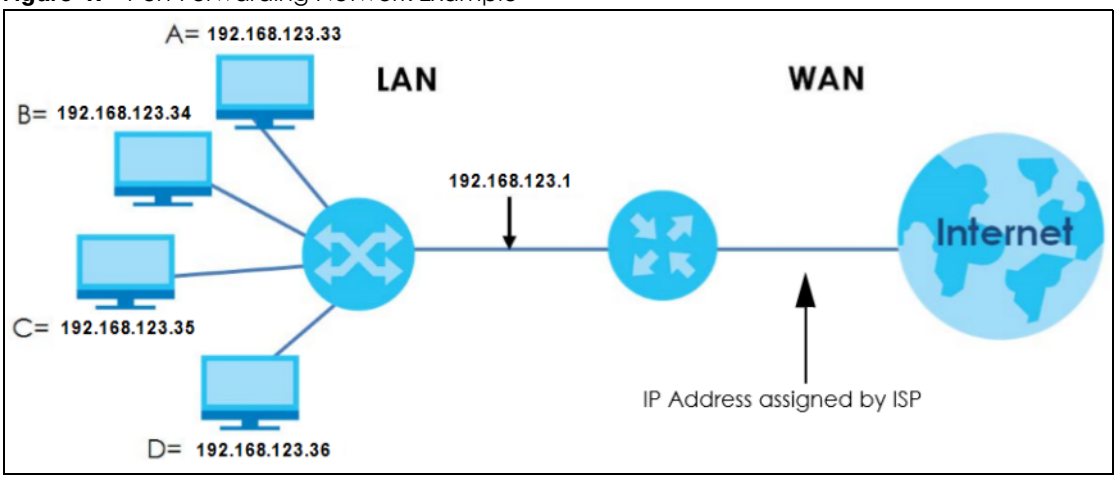


7.12 Configure a Port Forwarding Rule

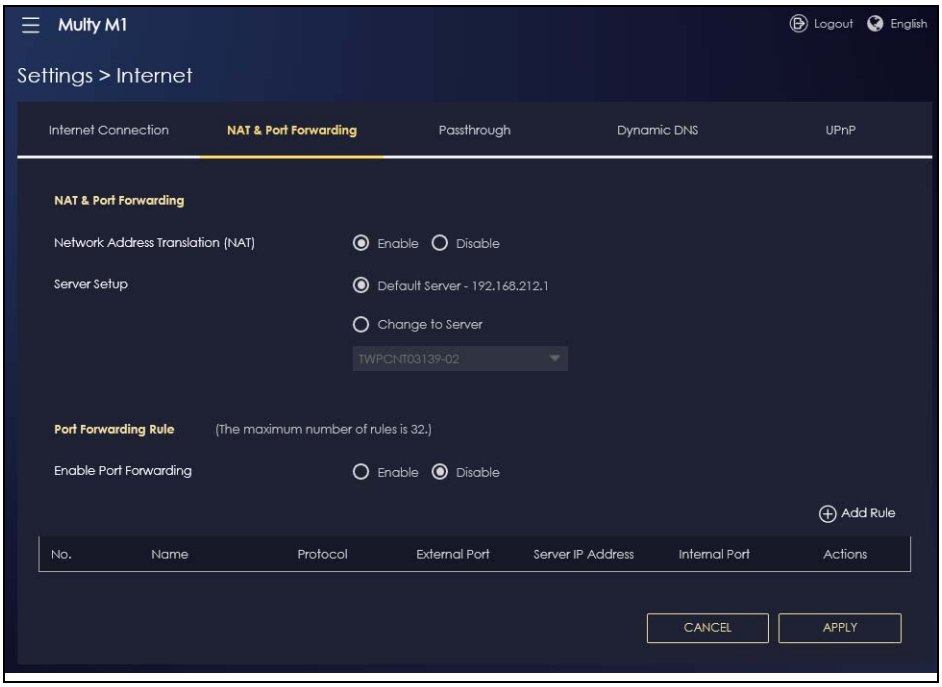
If you want to forward incoming packets to a specific IP address in the private network using ports, set a port forwarding rule.

Note: This is not available if you are using bridge mode.

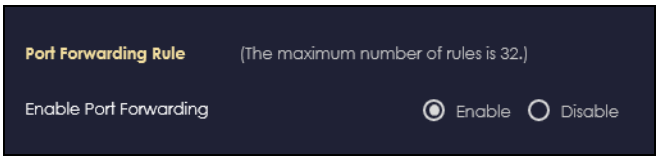
Figure 47 Port Forwarding Network Example



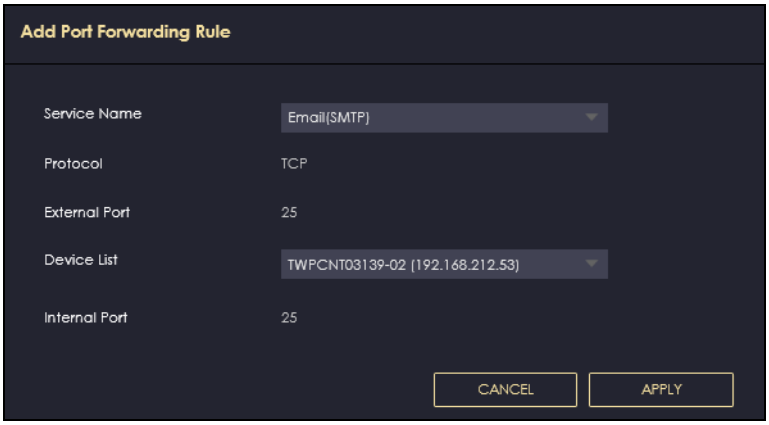
1 Click the **Navigation Panel** icon on the top-left corner ( ). From the **Settings** drop-down list, select **Internet**, and click the **NAT & Port Forwarding** tab.



2 Select **Enable** in the **Enable Port Forwarding** field.



3 Click **Add Rule** to create a port forwarding rule. Add a service name, a port number or a range of ports to define the service to be forwarded, specify the transport layer protocol used for the service, and the IP address of a device on your local network that will receive the packets from the port(s).



PART III
Multy Plus

CHAPTER 8
Multy Plus Tutorials

8.1 Introduction

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Zyxel Multy Plus web configurator helps you install Multy Pluss and manage the Multy Plus WiFi System directly.

Compatibility

- Internet Explorer, versions 8.0 and later.
- Google Chrome, versions 2.0 and later.
- Mozilla Firefox, versions 3.0 and later.
- Safari, versions 2.0 and later.

This section provides tutorials for setting up your Multy Plus.

- Use the Web Configurator
- Add and Install Your First Multy Plus
- Run a Speed Test
- Configure the Multy Plus's WiFi Networks
- Enable or Disable a WiFi Network
- Add Clients to a Profile
- Set a Profile's WiFi Schedule
- Pause or Resume Internet Access on a Profile
- Turn on or off the Multy Plus's LED (Light)
- Remove a Multy Plus
- Install a Second Multy Plus WiFi System
- Change Your Multy Plus Operating Mode
- Configure a Port Forwarding Rule
- Enable or Disable Daisy Chain Network Topology
- Local Login Password Change

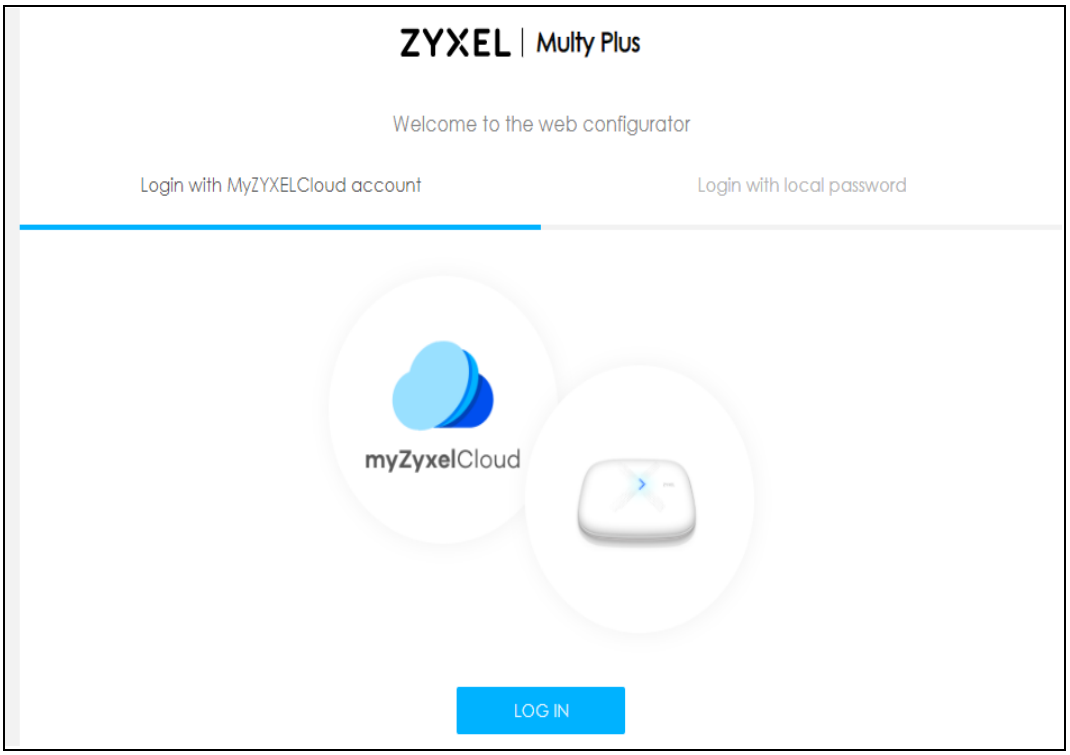
8.2 Use the Web Configurator

With a myZyxelCloud account, all your configurations will be stored in the myZyxelCloud server. You then can log in and use web configurator to manage your Multy Plus WiFi System. Moreover, the Multy Pluss can work with Amazon Alexa after the myZyxelCloud account is linked to Alexa (Section 3.30 on page 106).

1 Make sure your Multy Plus hardware is properly connected (refer to the Quick Start Guide).

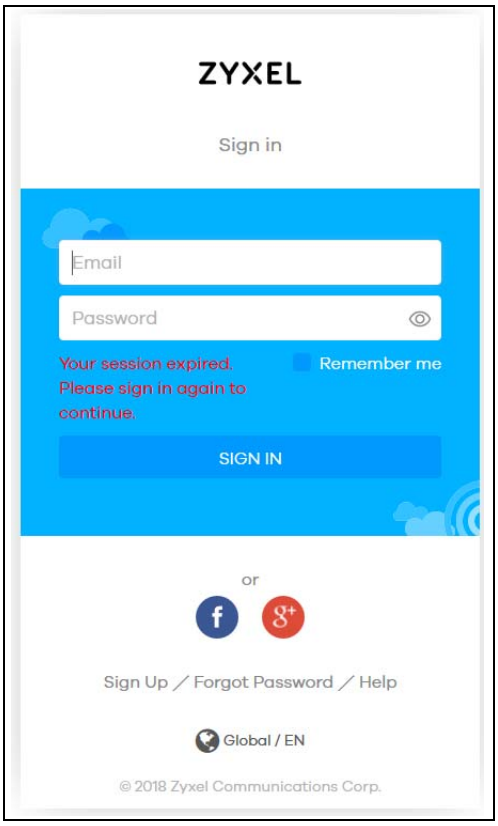
2 Launch your web browser and go to http://Zyxelwifi.com or http://Zyxelwifi.net.

The login screen displays. To access the web configurator and manage the Multy Plus you need to be connected to your myZyxelCloud account. Click **Login with MyZYXELCloud account** and you will be redirected to the myZyxelCloud website to log into your myZyxelCloud account. Or click **Login with local password** if you don't wish to access the myZyxelCloud account. For more information see Section 8.2.1 on page 156.



3 Enter your myZyxelCloud account **Email** and **Password**, and click **SIGN IN**. Alternatively, you can log out If you don't have any Internet Access you will be redirected to the Multy Plus Wizard to add your first Multy. For more information see Section 8.3 on page 159.

Note: If you don't have a myZyxelCloud account, click **Sign Up** to create one. You need to register the Multy Plus in your myZyxelCloud account before you can access its web configurator. Likewise, the option **Login with local password** will only appear after you have set up a myZyxelCloud account (mandatory).



You are redirected back to the Multy Plus web configurator.

8.2.1 Login with Local Password

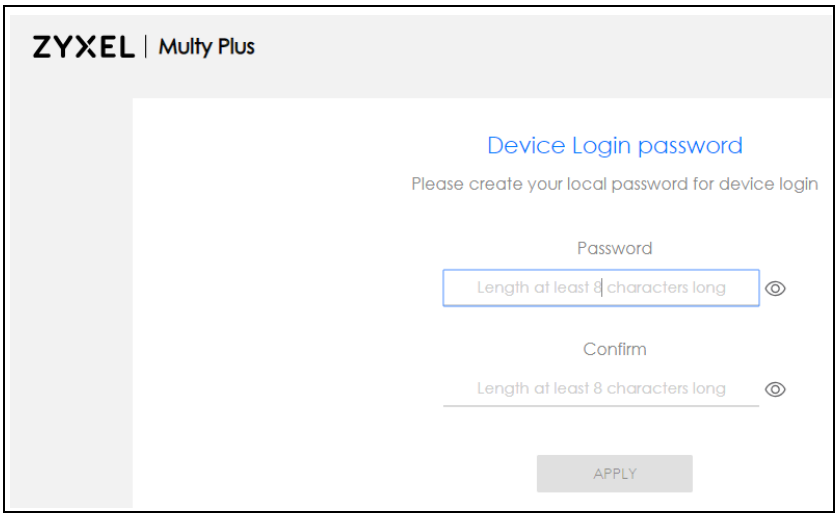
Login with local password is a secondary password and serves as an alternative to logging in with myZyxelCloud.

1 The first time you attempt to login with local password you will be asked to create one. Enter the new password under **Password** (8 - 32 characters). Click the "eyeball" symbol if you wish to view the characters you have entered.

Note: The password may contain a mix of letters, numbers, spaces, and/or special characters; and it is case-sensitive. Backslash, single quote, double quote, accent grave, angle brackets, caret, dollar sign, ampersand (\ ' " ‘ <> ^ $ &), and emoji symbols are not allowed.

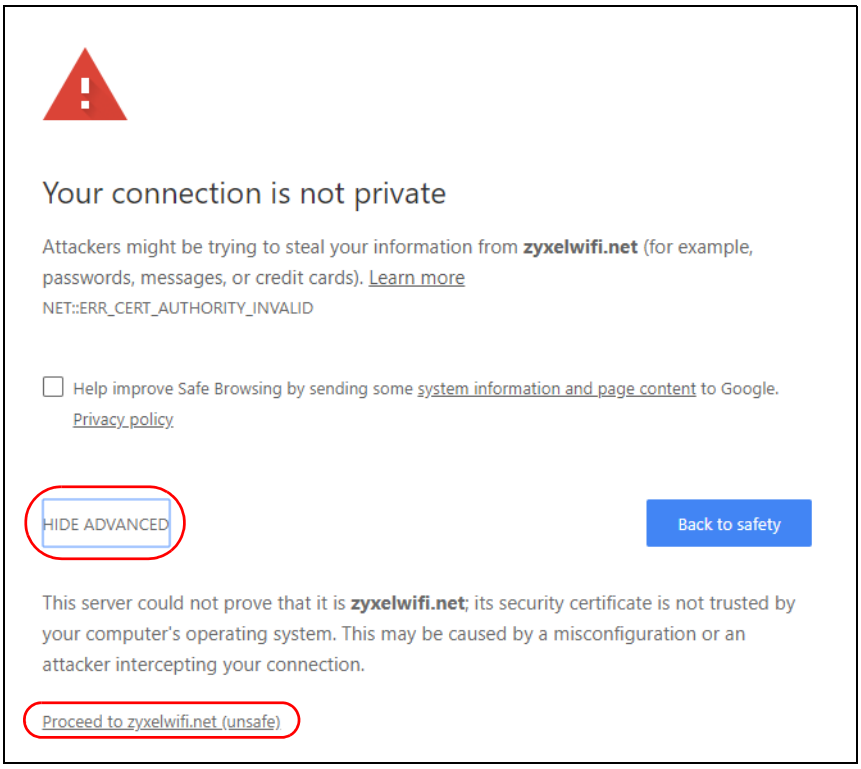
2 Enter the password again under **Confirm** (click the “eyeball” symbol if you wish to view the characters you have entered).

3 Then click **Apply** to accept the changes.

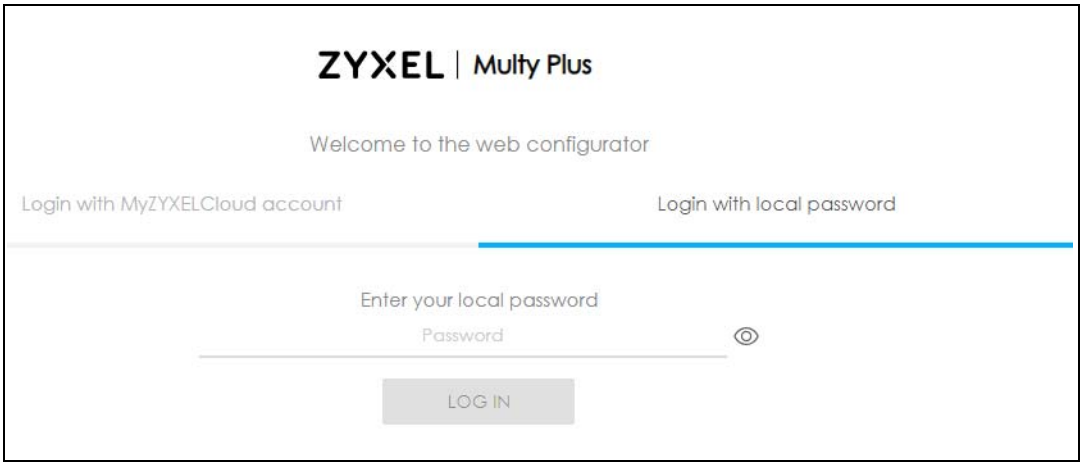


4 Just click **OK** to continue.

5 Click **ADVANCED** (will turn into **HIDE ADVANCED**) and then click **Proceed to zyxelwifi.net (unsafe)**.



6 Upon returning to the login screen, click to select the **Login with local password** tab and **Enter your local password**.



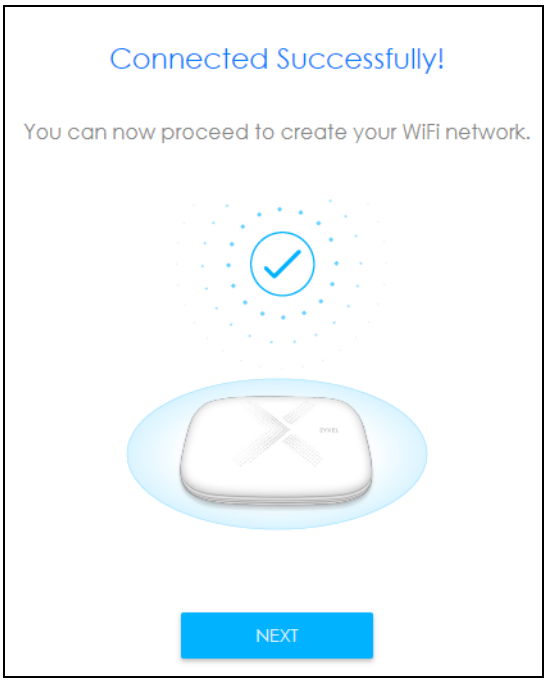
7 Then click **LOG IN**.

8.3 Add and Install Your First Multy Plus

You need to install at least one Multy Plus before you can manage the Multy Plus WiFi System.

1 If your modem or router has DHCP enabled, the Multy Plus attempts to connect automatically to the Internet. If no connection to the Internet is established, select **PPPOE** if you have a username and password from your ISP (Internet Service Provider) to access the Internet. Select **STATIC IP** if you have IP settings assigned by your ISP.

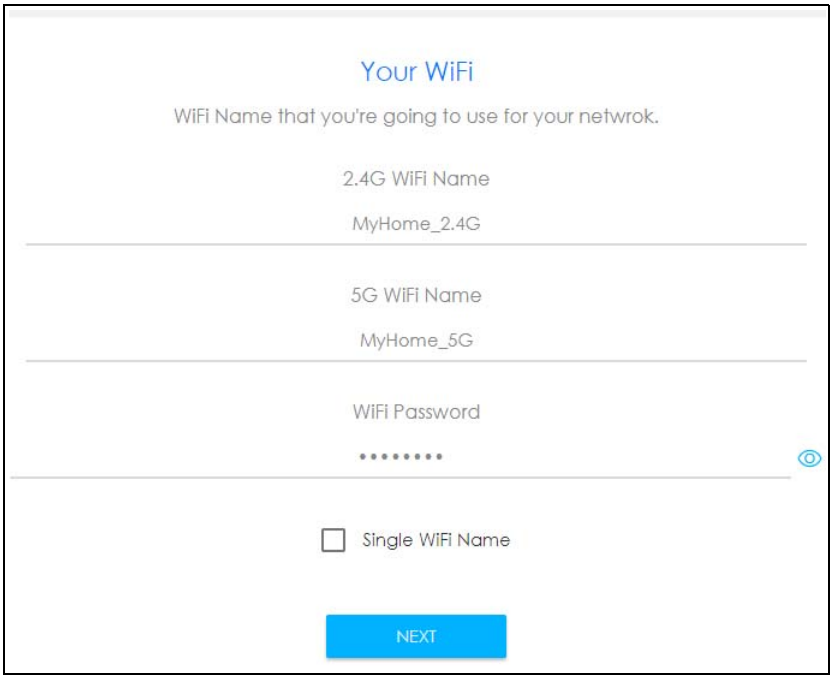
2 Once you have successfully connected to the Internet you can continue creating your Multy Plus WiFi System.



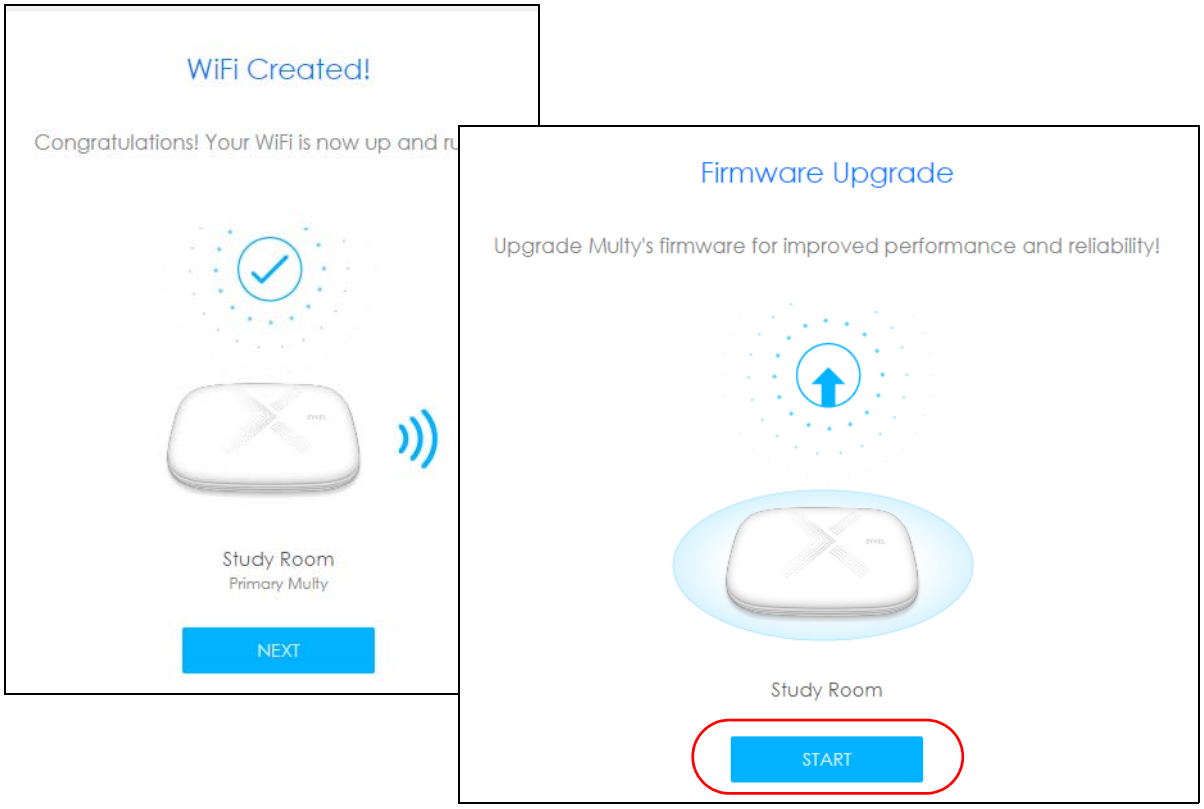
3 Select the location/name where you want to place your Multy Plus, click **Next** and follow the on-screen instructions.

4 Enter the **WiFi Name** and password for your Multy Plus WiFi System WiFi network. Select **Single WiFi Name** for both 2.4G and 5G WiFi networks to have the same WiFi settings. Otherwise, assign different names to both networks, but they will share the same **WiFi Password**.

Note: When the WiFi Name is the same for both 2.4G and 5G WiFi networks the Multy Plus adds **.speed** to the end of the 5G WiFi Name.

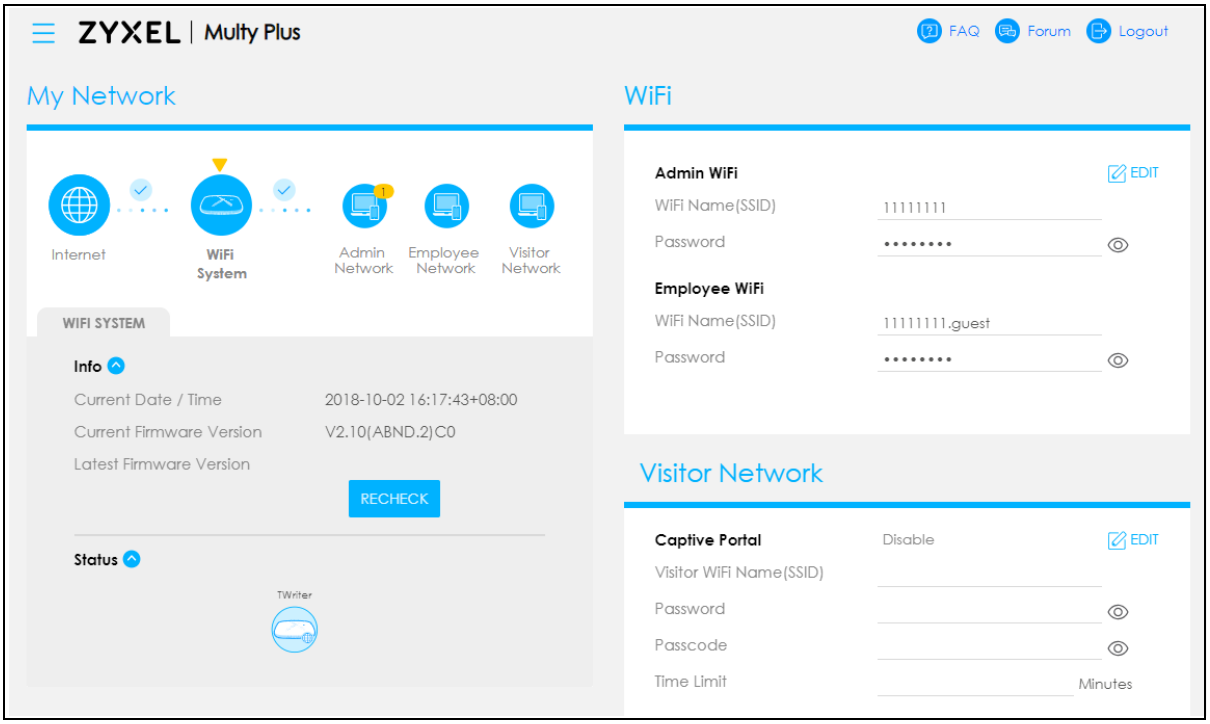


5 Once your WiFi network is created click **Start**. The Multy Plus automatically checks and updates with the latest firmware available.



6 Click **Next** to be redirected to the myZyxelCloud website. Sign up or log in with your myZyxelCloud account, so you can complete the Multy Plus installation, and access its web configurator.

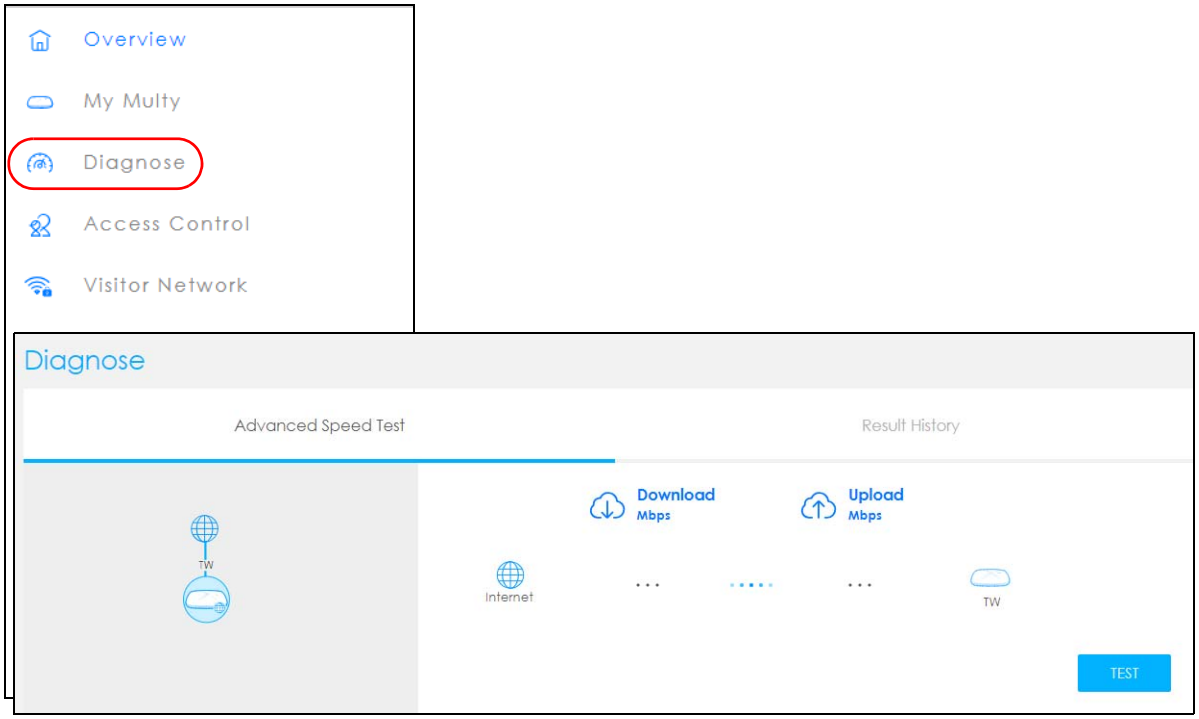
7 The Multy Plus WiFi System **Overview** screen displays allowing you to monitor your Multy Pluss and Multy Plus WiFi System. It shows if the Multy Pluss in this Multy Plus WiFi System are online, and how many wireless clients are currently connected to each Multy Plus, as well as their upstream/downstream data rates. For more information see Table 19 on page 165 for WiFi Network Privileges.



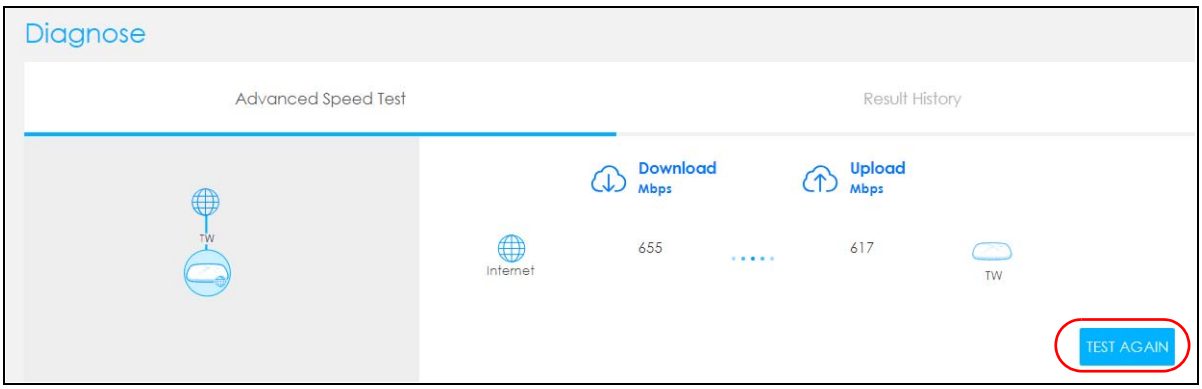
8.4 Run a Speed Test

With the Multy Plus Web Configurator, you can check the speed of the connection between the first Multy Plus and the broadband modem/router or the connection between Multy Pluss.

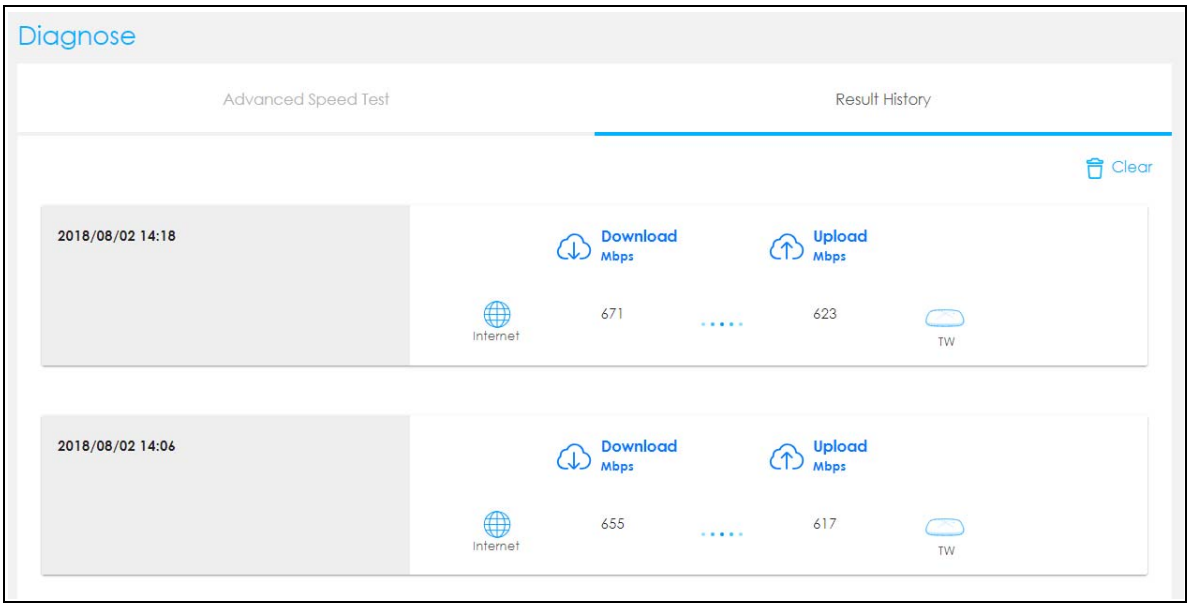
1 Click the Navigation Panel icon on the top-left corner ( ), and click **Diagnose** to open the **Advanced Speed Test** screen. Use this screen to view all the available connections in your Multy Plus WiFi System.



2 Click **TEST ALL** to perform a speed test. This shows data rates for both upstream and downstream traffic. Click **TEST AGAIN** to update the information in this screen.



3 Click the **Result History** tab to view a summary of the tests made. Click **Clear** to delete all records.



8.5 Configure the Multy Plus's WiFi Networks

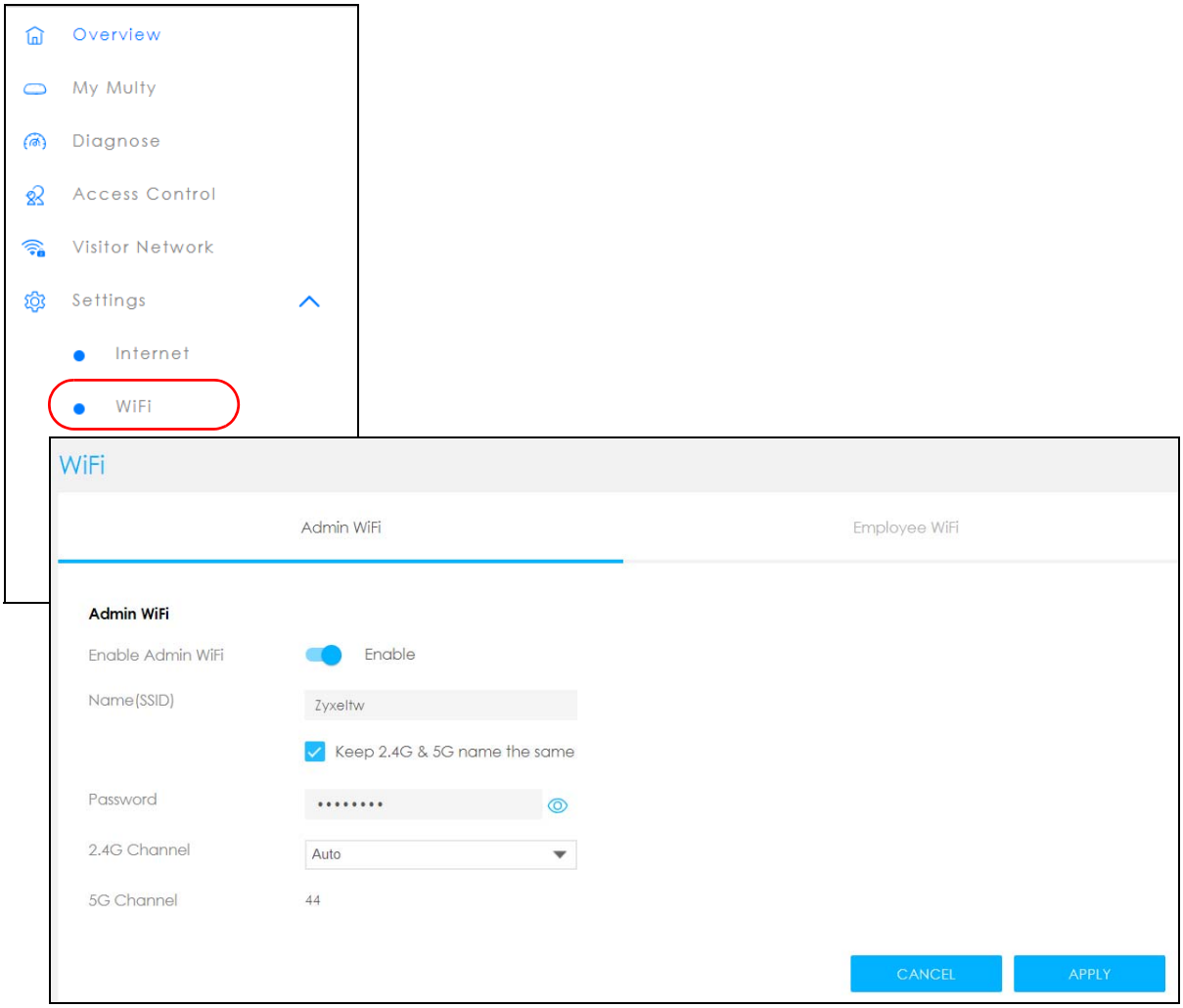
In the The Multy Plus WiFi System you can configure independent wireless networks with different privileges. Clients can associate only with the network for which they have security settings (SSID and password). The following table describes the different Multy Plus's profile networks and their privileges.

Table 19 WiFi Network Privileges

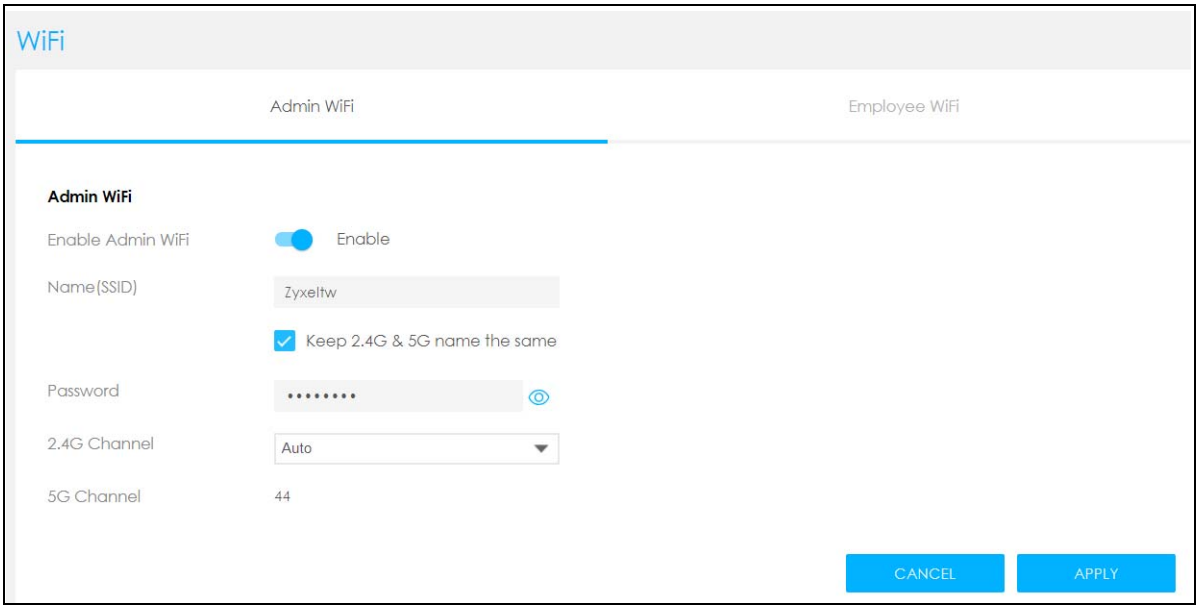
WIFI NETWORK	INTERNET ACCESS	2.4G / 5G WIFI NETWORK	ACCESS TO WEB CONFIGURATOR	ACCESS TO WIRED LAN
Admin WiFi	Yes	2.4G and 5G	Yes	Yes
Employee WiFi	Yes	2.4G and 5G	No	No
Visitor WiFi	Yes, after captive portal log in.	2.4G and 5G	No	No

Note: A user can only configure the WiFi networks' security settings if they are connected to the **Admin WiFi** network.

1 Click the Navigation Panel icon on the top-left corner ( ), click **Settings** to open the **WiFi** screen. Use each tab in the **WiFi** menu to configure each of the WiFi networks' security settings.


Overview
My Multy
Diagnose
Access Control
Visitor Network
Settings
Internet
WiFi
WiFi
Admin WiFi
Employee WiFi
Admin WiFi
Enable Admin WiFi
Enable
Name(SSID)
Zyxeltw
Keep 2.4G & 5G name the same
Password
2.4G Channel
Auto
5G Channel
44
CANCEL
APPLY

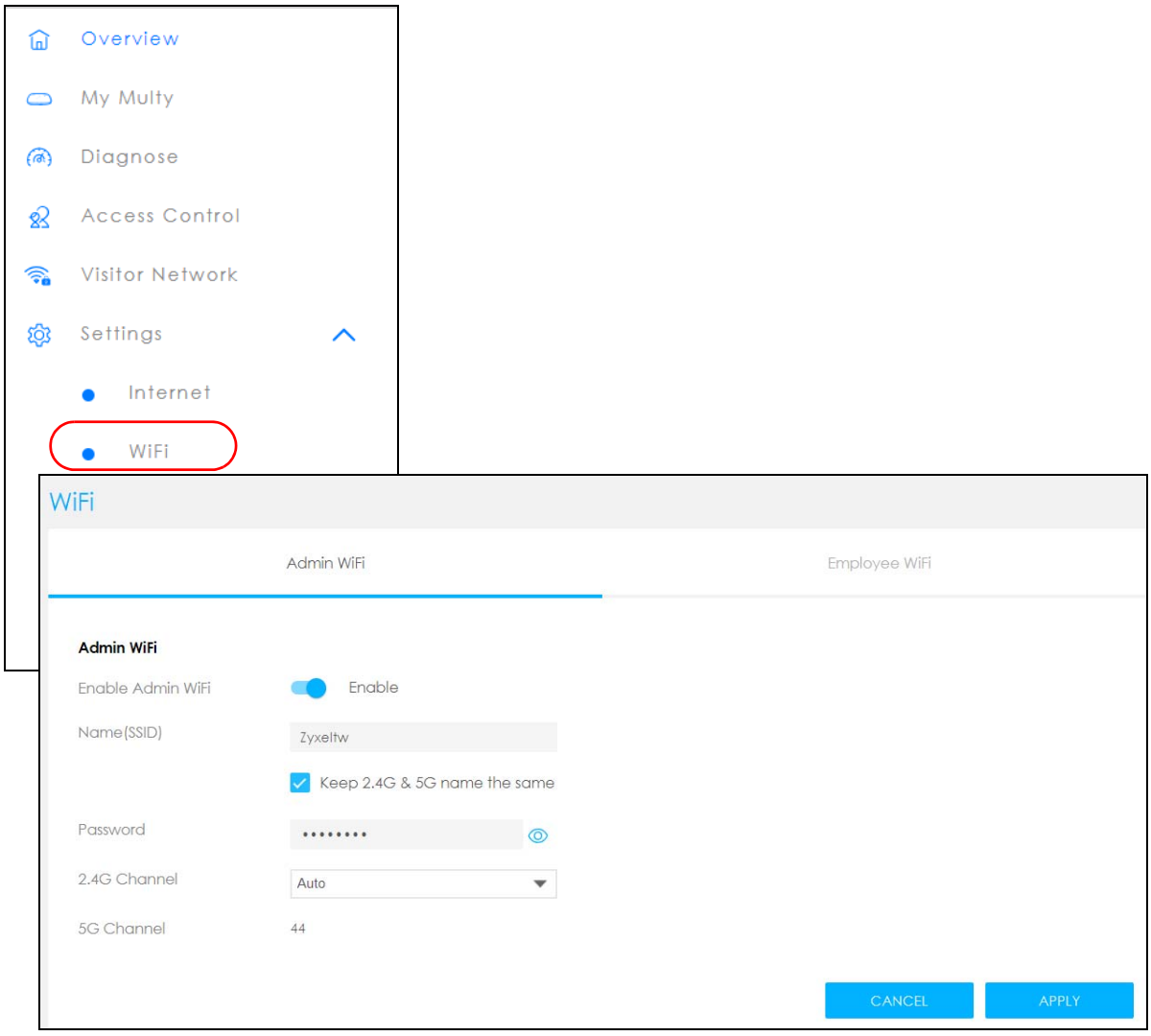
2 Select **Enable** to activate a WiFi Network. Enter the **Name (SSID)** and **Password** clients use to connect to the WiFi network. You can configure two different WiFi Names for the **Admin WiFi** 2.4G and 5G networks. Select **Keep 2.4G & 5G name the same,** so they both use the same WiFi Name (SSID). Click **Apply** to save your changes.



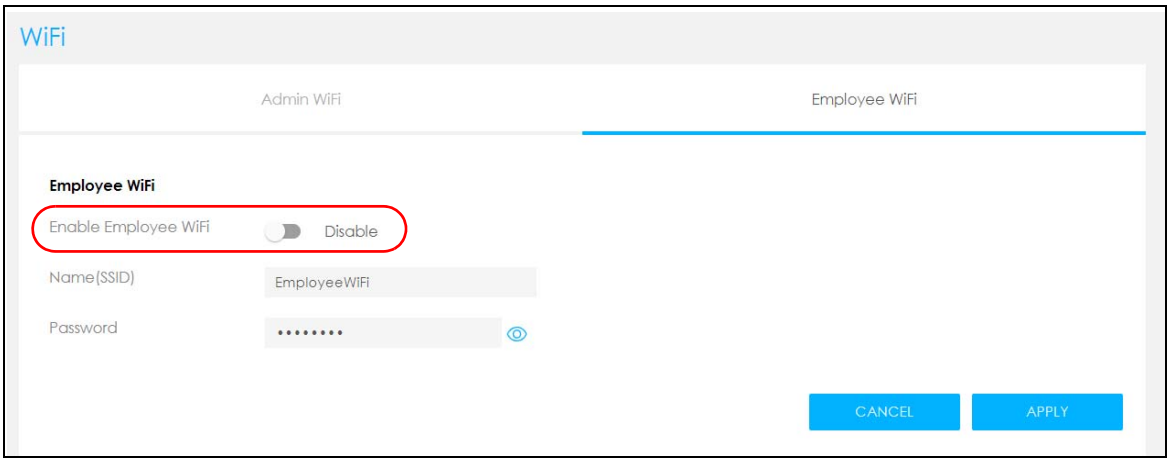
8.6 Enable or Disable a WiFi Network

After the Multy Plus WiFi System is set up, you can use separate WiFi networks for your clients. The WiFi settings will be applied to all Multy Pluss in the same Multy Plus WiFi System.

1 Click the Navigation Panel icon on the top-left corner ( ). From the **Settings** drop-down list click **WiFi** to open the **WiFi** screen.



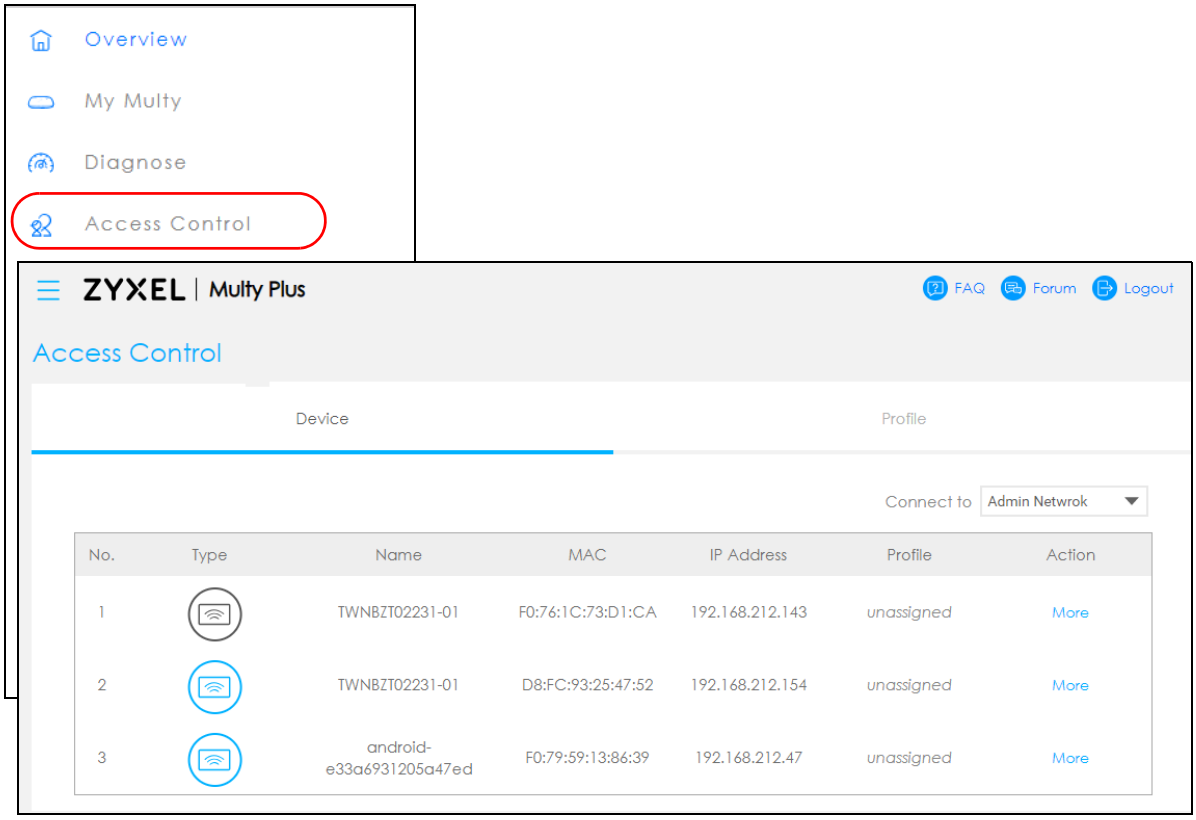
2 **Enable Employee WiFi** and enter the **WiFi Name (SSID)** and **WiFi Password**. Click **APPLY** to save your changes.



8.7 Add Clients to a Profile

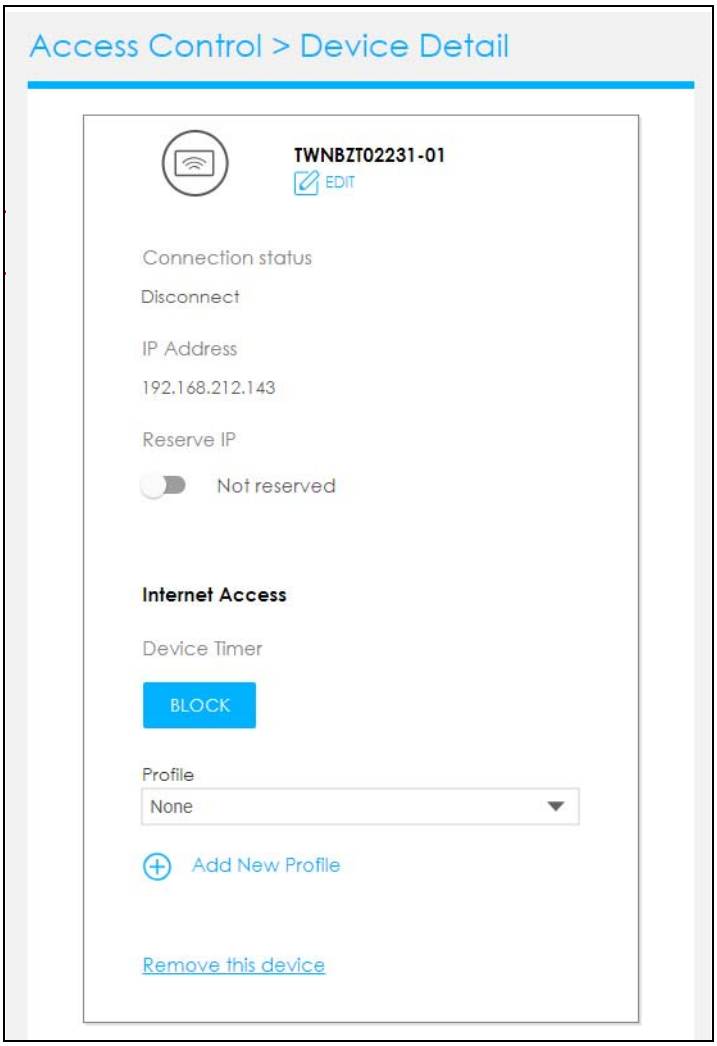
Profiling clients allows you to easily block/allow Internet access or set a schedule for all client devices in the same profile.

1 Click the Navigation Panel icon on the top-left corner ( ), and click **Access Control** to open the **Device** screen. Use the **Device** screen to view all the clients in your Multy Plus WiFi System. Specify which network you want to view in the **Connect to** drop-down list.



2 Click **More** under the **Action** column to view more information about each device. On the **Access Control > Device Detail** screen**,** select a predefined profile and click **APPLY**.

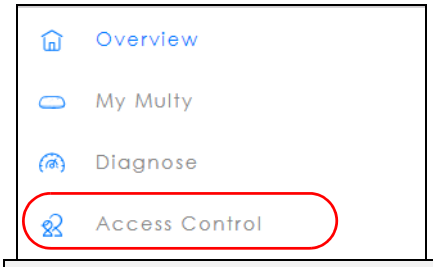
You can also activate **Reserve IP,** so the Multy Plus assigns a specific IP address to a device every time it connects to the Multy Plus WiFi System. For more information on adding/editing new profiles, see Section 8.8 on page 172.

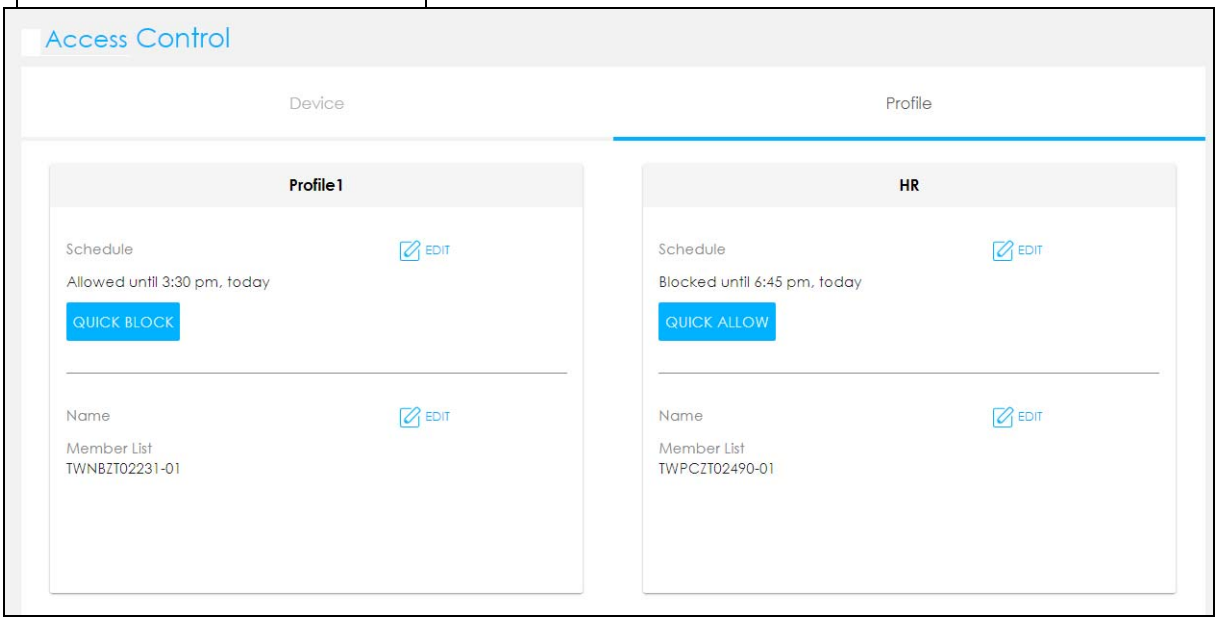


8.8 Set a Profile's WiFi Schedule

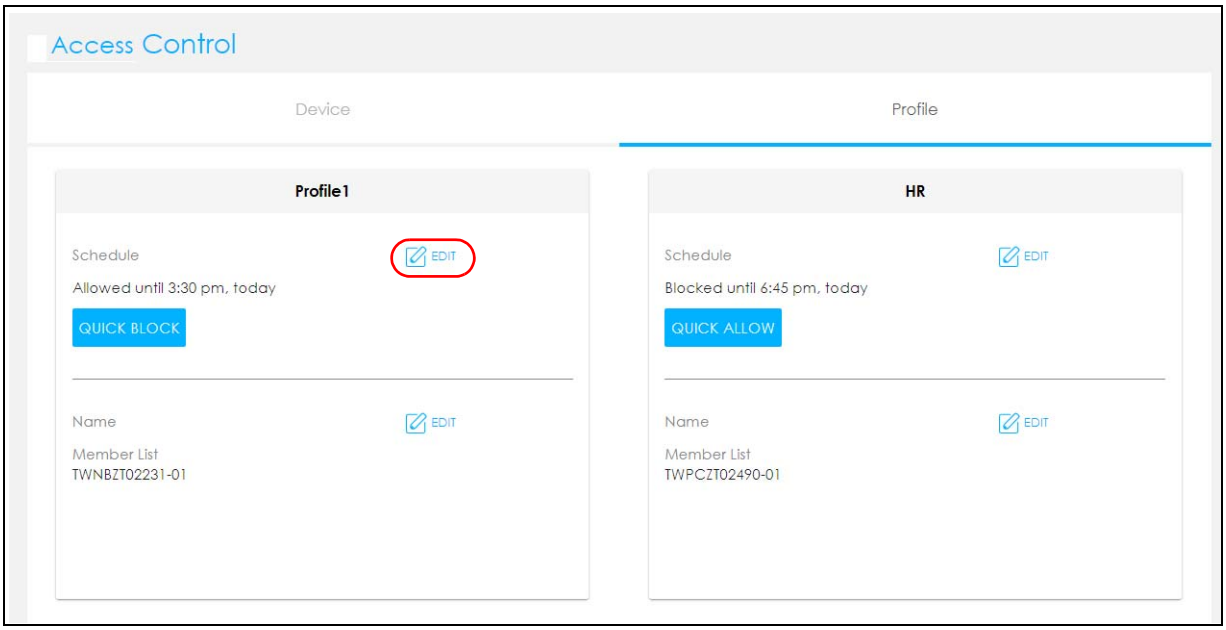
When you create or edit a profile, you can schedule the Multy Plus WiFi System to automatically disable or enable WiFi access during a certain period of time for clients in that profile.

1 Click the Navigation Panel icon on the top-left corner ( ). Select **Access Control**, and click the **Profile** tab. Use the **Profile** screen to display the profiles created in the Multy Plus WiFi System.





2 Click the Edit icon (EDIT)to modify a profile's Internet schedule.

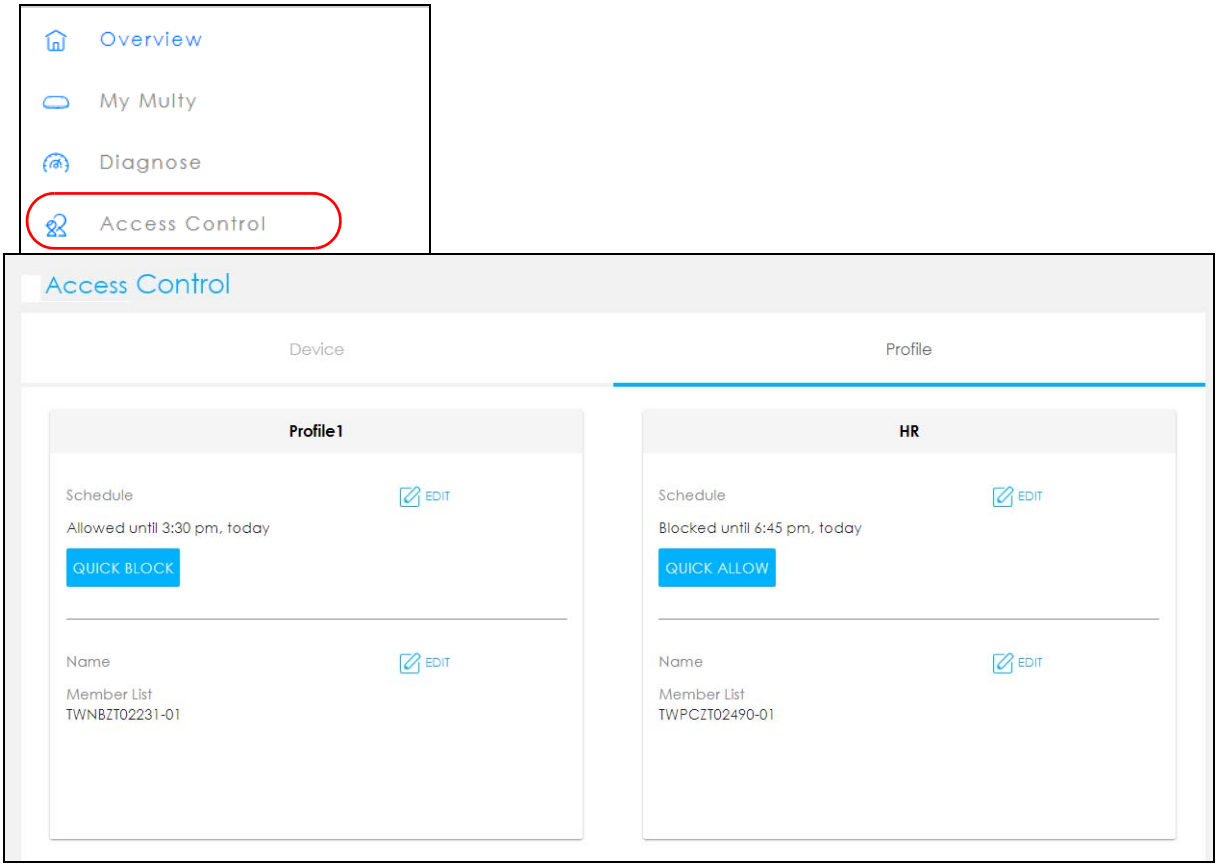


3 Click **Enable** to activate this profile's Internet schedule. Click the start time cell and drag down and/or right to the end time to set up your schedule.

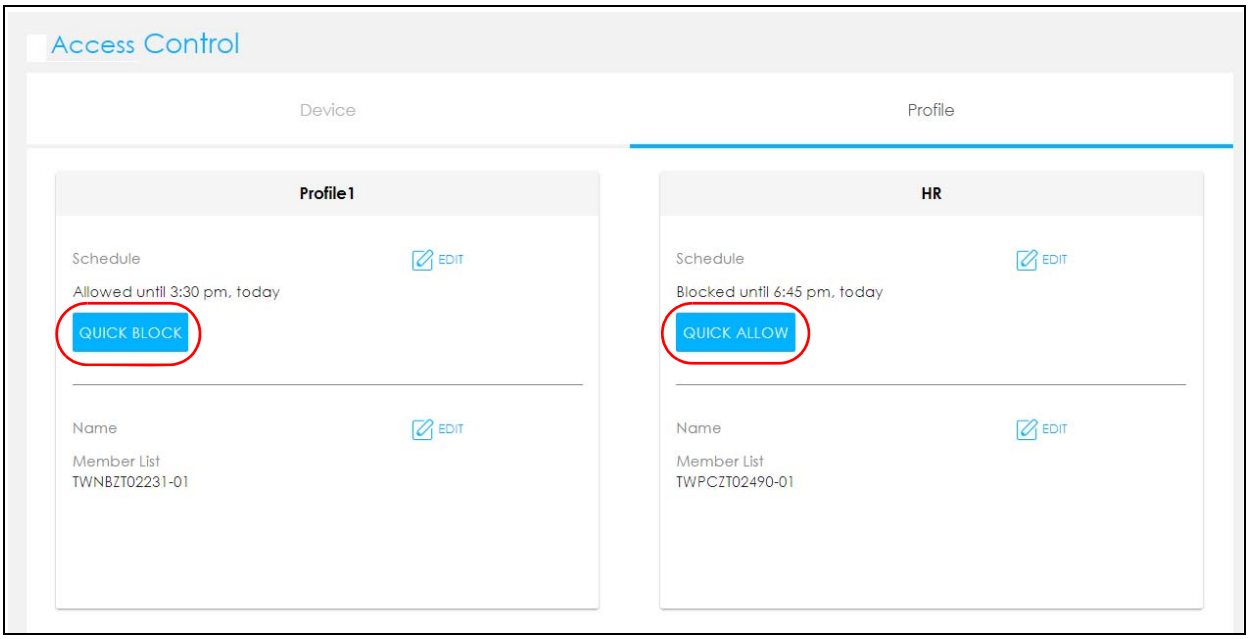
8.9 Pause or Resume Internet Access on a Profile

You may want to manually block a profile of client devices from accessing the Internet immediately and resume it later.

1 Click the Navigation Panel icon on the top-left corner ( ). Select **Access Control**, and click the **Profile** tab. Use the **Profile** screen to display the profiles that are previously created in the Multy Plus WiFi System.

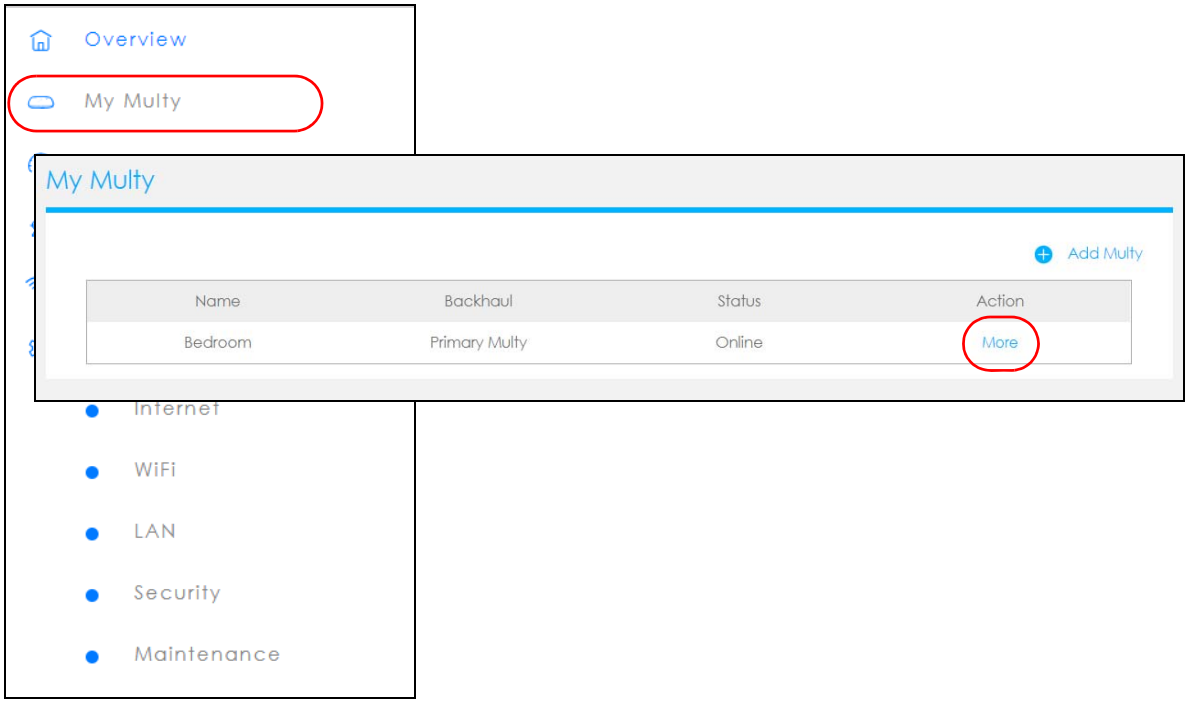


2 Click a profile's **Quick Allow** button to resume network access at once, or click the **Quick Block** button to pause Internet access for that specific profile.

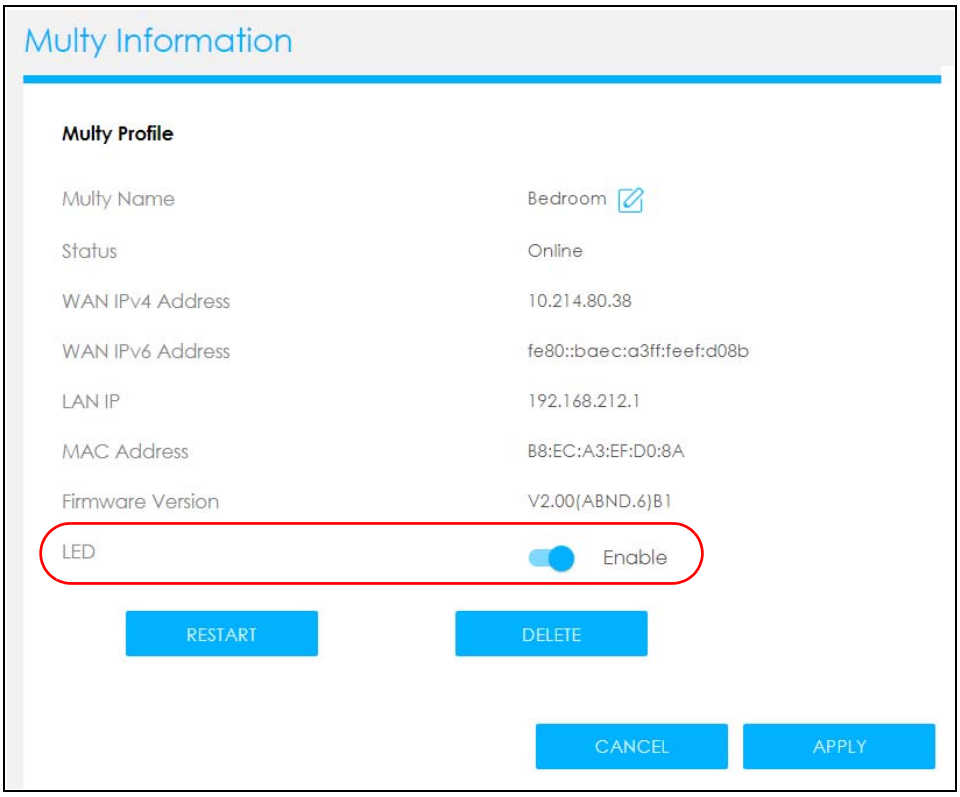


8.10 Turn on or off the Multy Plus's LED (Light)

1 Click the Navigation Panel icon on the top-left corner ( ), and click **My Multy** to view all the Multy Pluss in your Multy Plus WiFi System. Select the device you want to modify and click **More...**



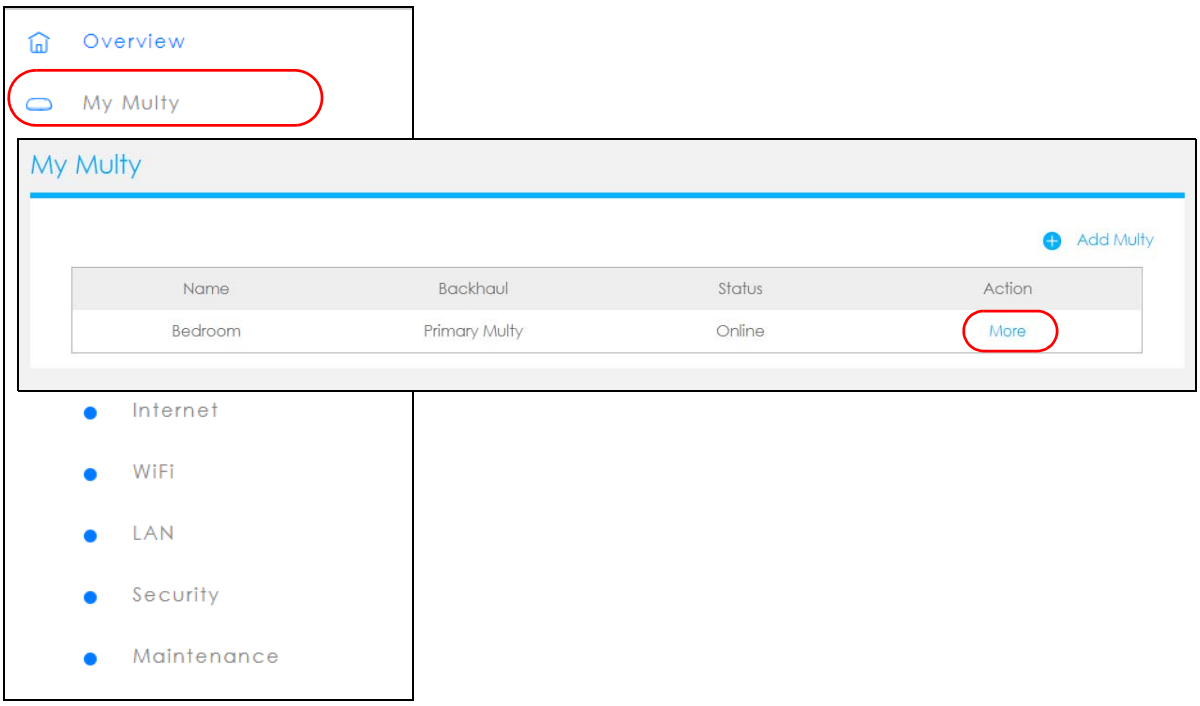
2 The **Multy Information** screen appears. Click the **LED** switch to **Enable** or **Disable** the LED's behavior.



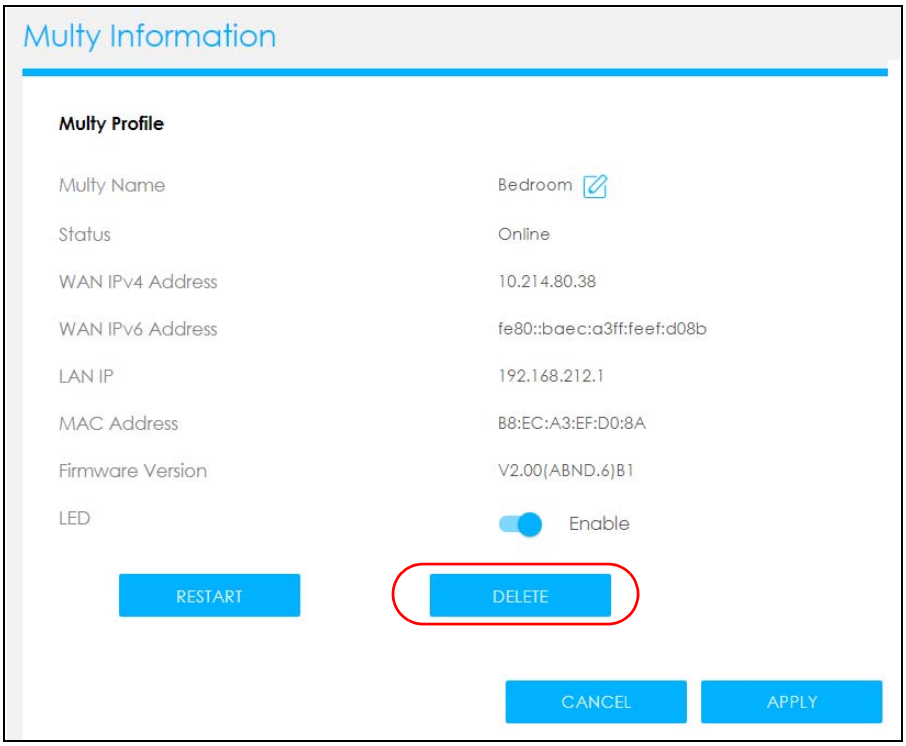
8.11 Remove a Multy Plus

If a Multy Plus is damaged or no longer in use, you can remove it from the Multy Plus WiFi System.

1 Click the Navigation Panel icon on the top-left corner ( ), and click **My Multy** to view all the devices in your Multy Plus WiFi System. Select the device you want to remove and click **More...**



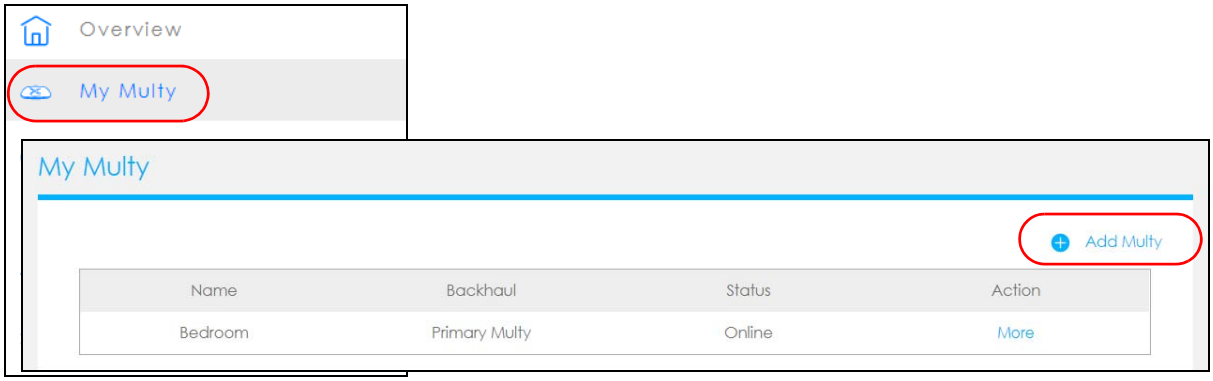
2 The **Multy Information** screen displays. Click **Delete** to remove the device from the Multy Plus WiFi System.



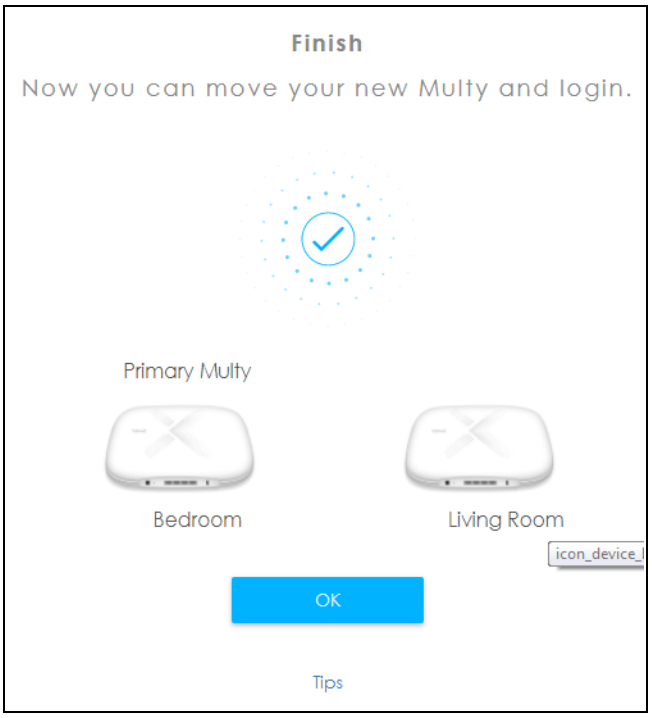
8.12 Install a Second Multy Plus WiFi System

You can manage multiple Multy Pluss using the Multy Plus Web Configurator.

1 Click the Navigation Panel icon on the top-left corner ( ), and click **My Multy** to view all the devices in your Multy Plus WiFi System. Click **Add Multy** to add a Multy Plus to your Multy Plus WiFi System. Follow the on-screen instructions to install the Multy.



2 Once you have successfully finished the Multy installation, you can relocate it to a WiFi dead zone where you need WiFi signal.



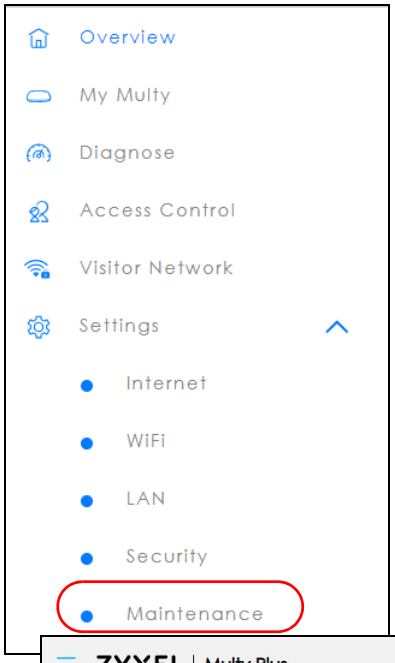
8.13 Change Your Multy Plus Operating Mode

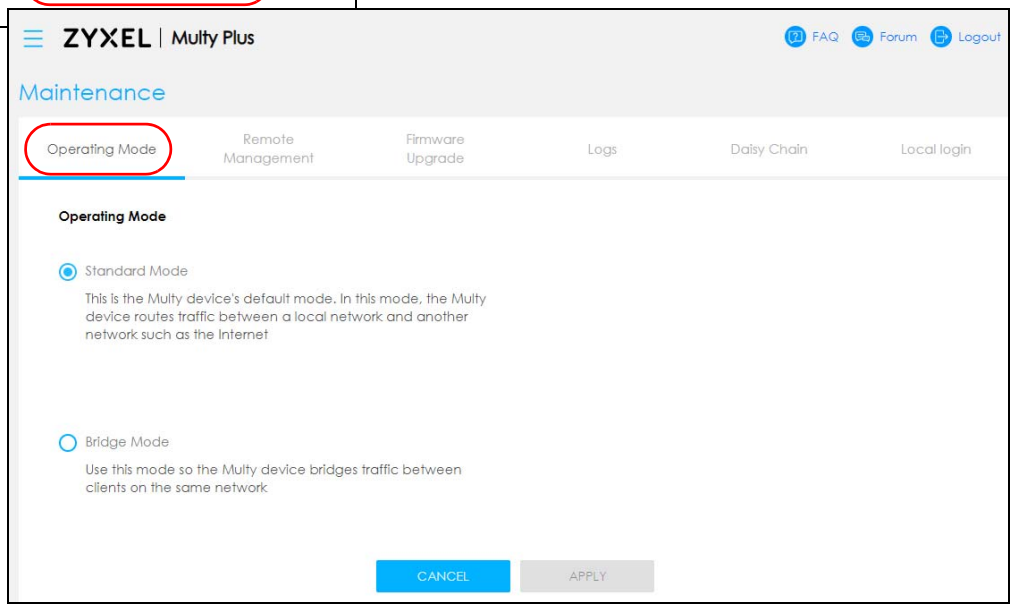
The operating mode refers to how the Multy Plus is being used in the network. The Multy Plus has two operating modes:

- **Standard:** This is the Multy Plus's default mode. In this mode, the Multy Plus routes traffic between a local network and another network such as the Internet. If you wish your Multy Plus to have Access Control, UPnP, Port Forwarding, DMZ function, choose this mode.
- **Bridge:** Use this mode so the Multy Plus bridges traffic between clients on the same network. You can choose this mode if you have an existing router.

Note: AiShield, Access Control, UPnP, Port Forwarding, DMZ are not available in Bridge mode.

1 Click the Navigation Panel icon on the top-left corner ( ). From the **Settings** drop-down list, click **Maintenance**, then click the **Operating Mode** tab. Select the operating mode and select **APPLY** to save your changes. Changing the Multy Plus's operating mode may take up to two minutes.

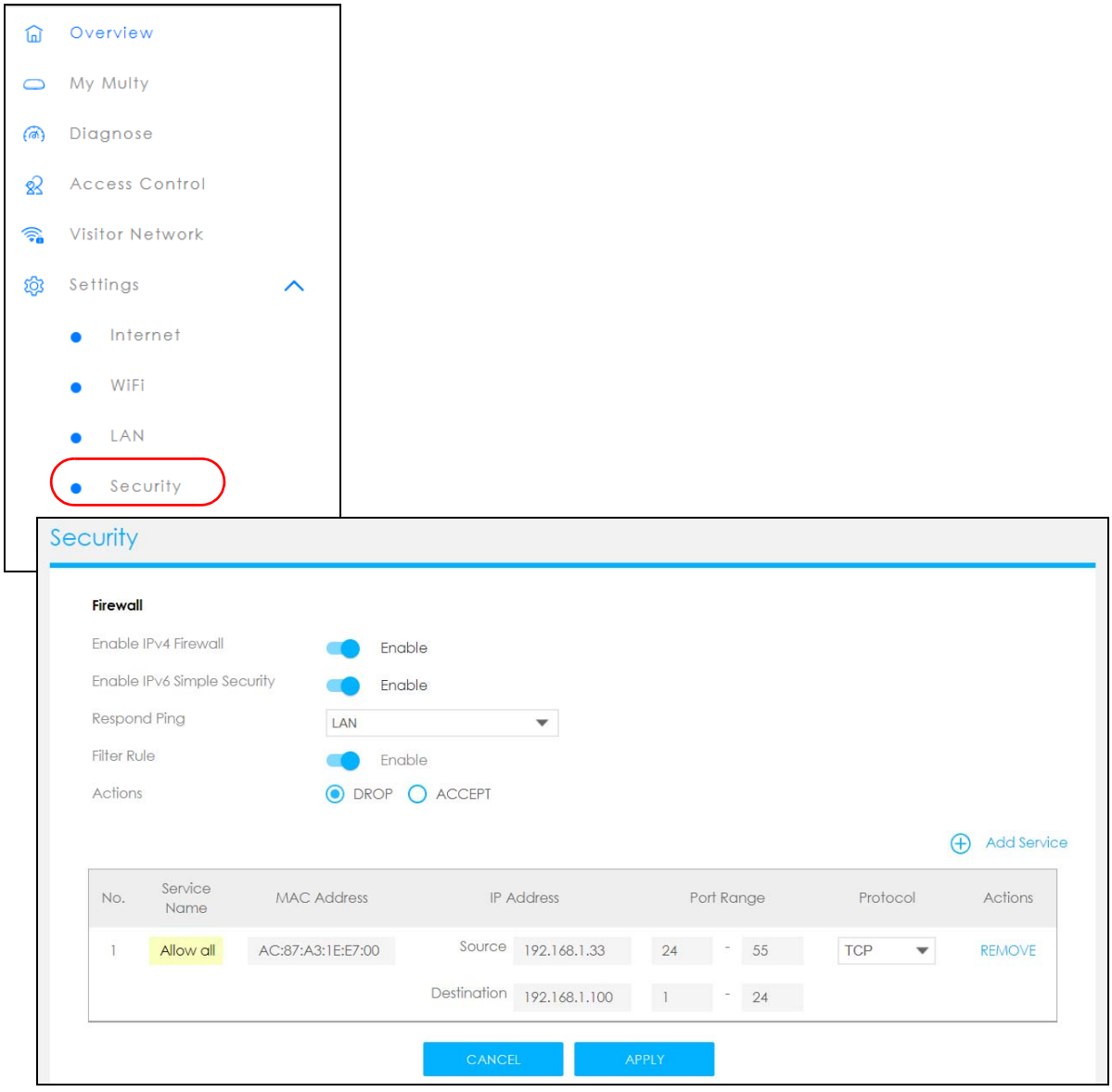




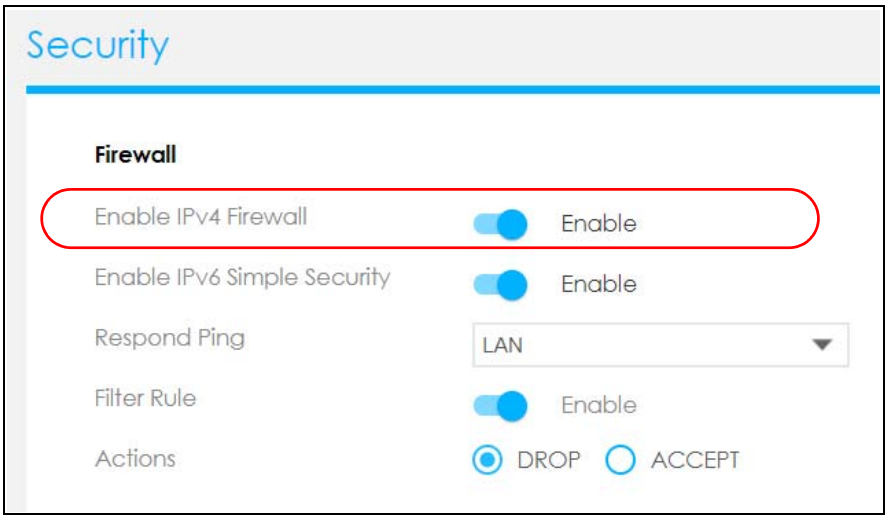
8.14 Configure a Port Forwarding Rule

Port forwarding is commonly used when you want to use Internet activities such as online gaming, P2P file sharing, or even hosting servers on your network. It allows a party from the Internet to contact a specific LAN client on your network correctly. If you want to forward incoming packets to a specific or appropriate IP address in the private network using ports, set a port forwarding rule.

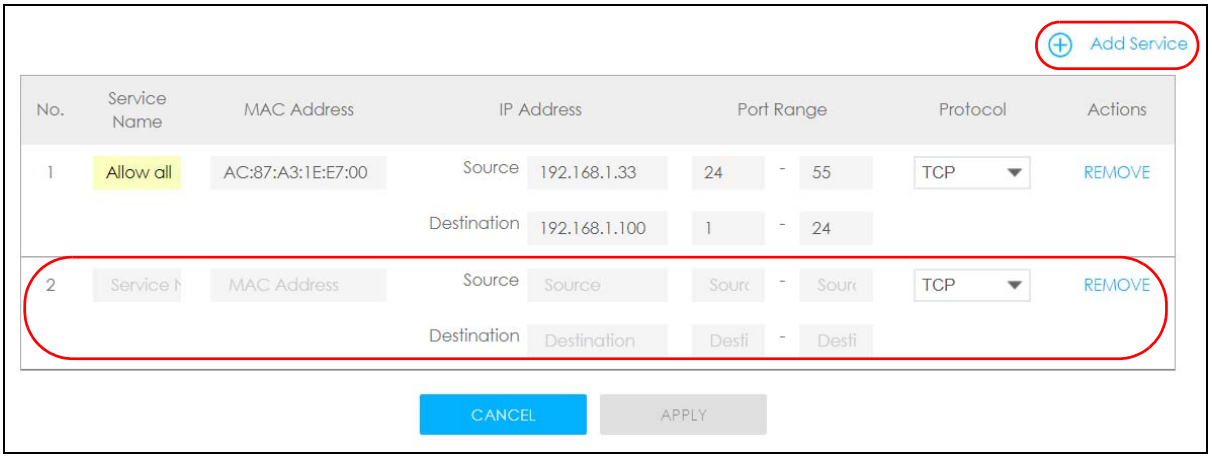
1 Click the Navigation Panel icon on the top-left corner ( ). From the **Settings** drop-down list, click **Security**, the **Firewall** screen appears.



2 Click **Enable IPv4 Firewall** to enable port forwarding.



3 Click **Add service** to create a port forwarding rule. Add a service name, a port number or a range of ports to define the service to be forwarded, specify the transport layer protocol used for the service, and the MAC address of a device on your local network that will receive the packets from the port(s).



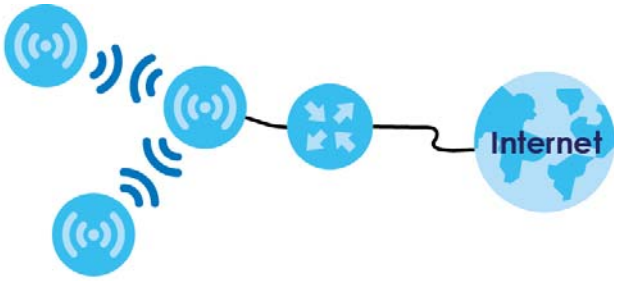
8.15 Enable or Disable Daisy Chain Network Topology

You can “daisy chain” multiple Multy Pluss together to create expansive WiFi coverage for your home.

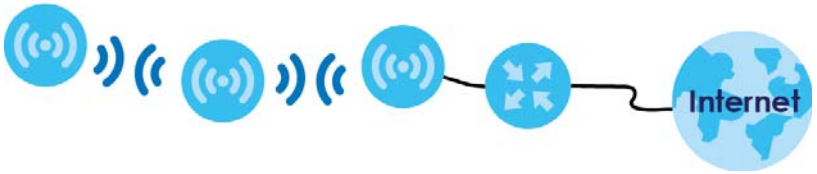
When daisy chaining is enabled, each Multy Plus chooses its own way of connecting to the primary Multy Plus - either by connecting directly, or by going through another Multy Plus with a strong WiFi signal.

When Multy Pluss are daisy-chained, they don’t all need to be placed near the primary Multy Plus, which means you can extend your coverage.

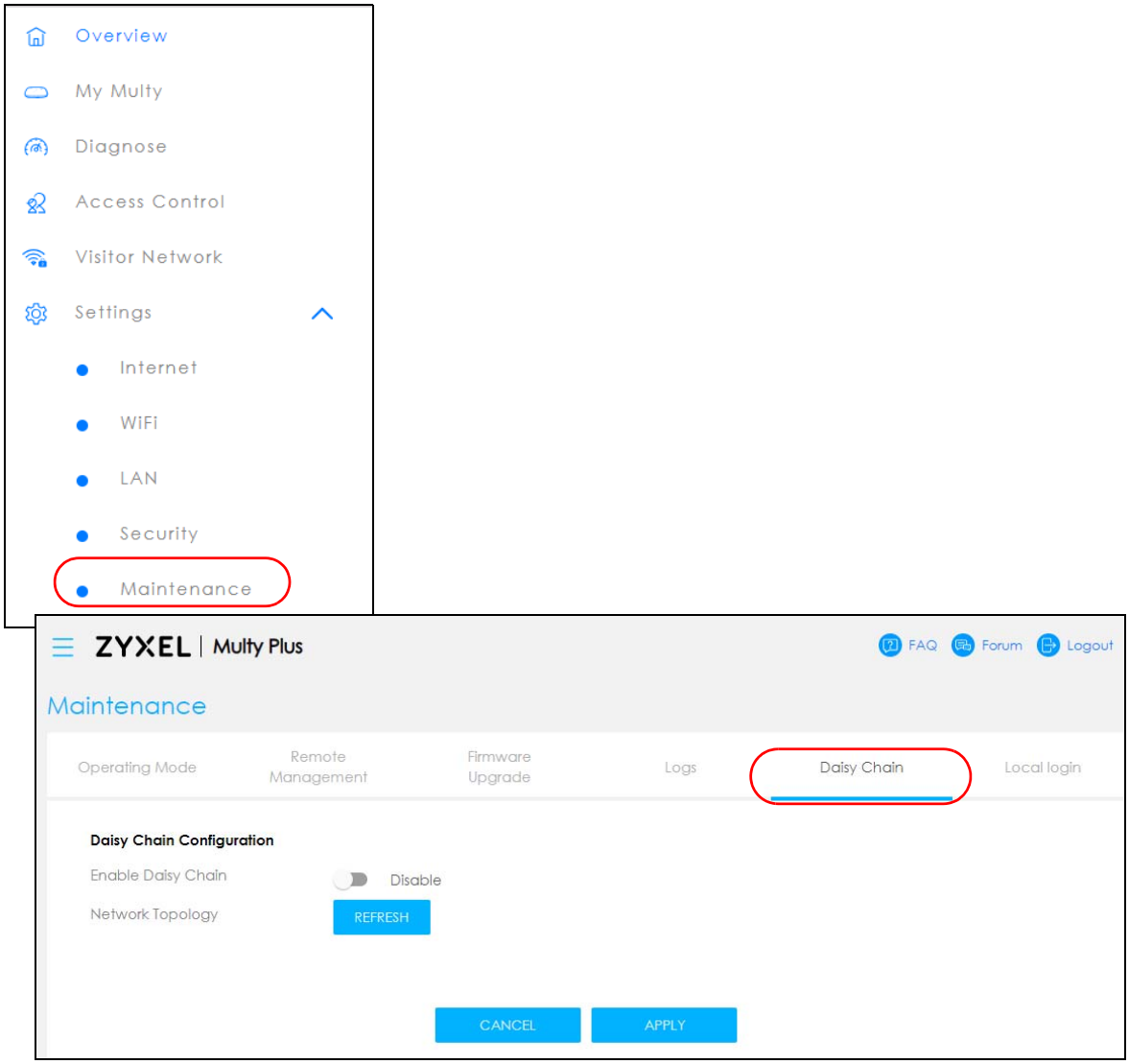
Daisy Chain Disabled



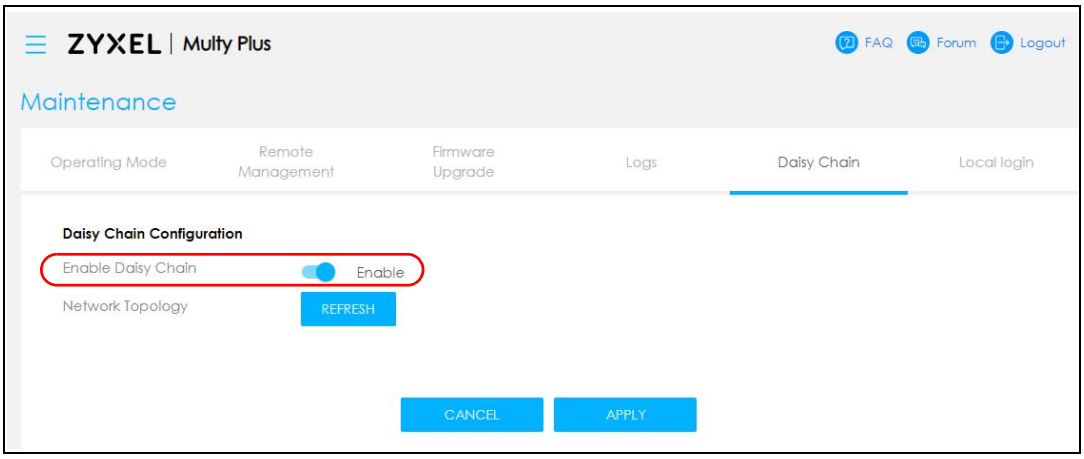
Daisy Chain Enabled



1 Click the Navigation Panel icon on the top-left corner ( ). From the **Settings** drop-down list, click **Maintenance**, then click the **Daisy Chain** tab.



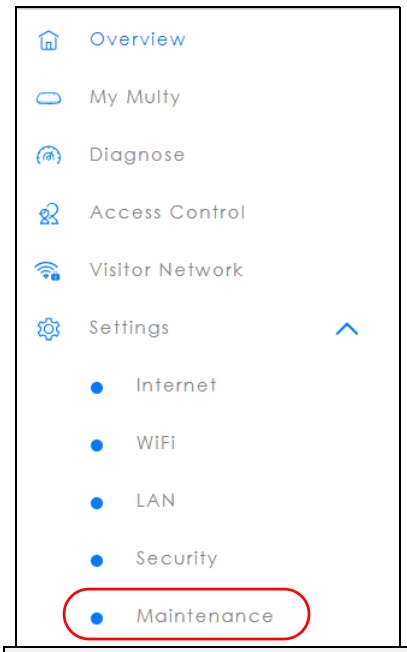
Click the button next to **Enable Daisy Chain** to activate daisy chaining.

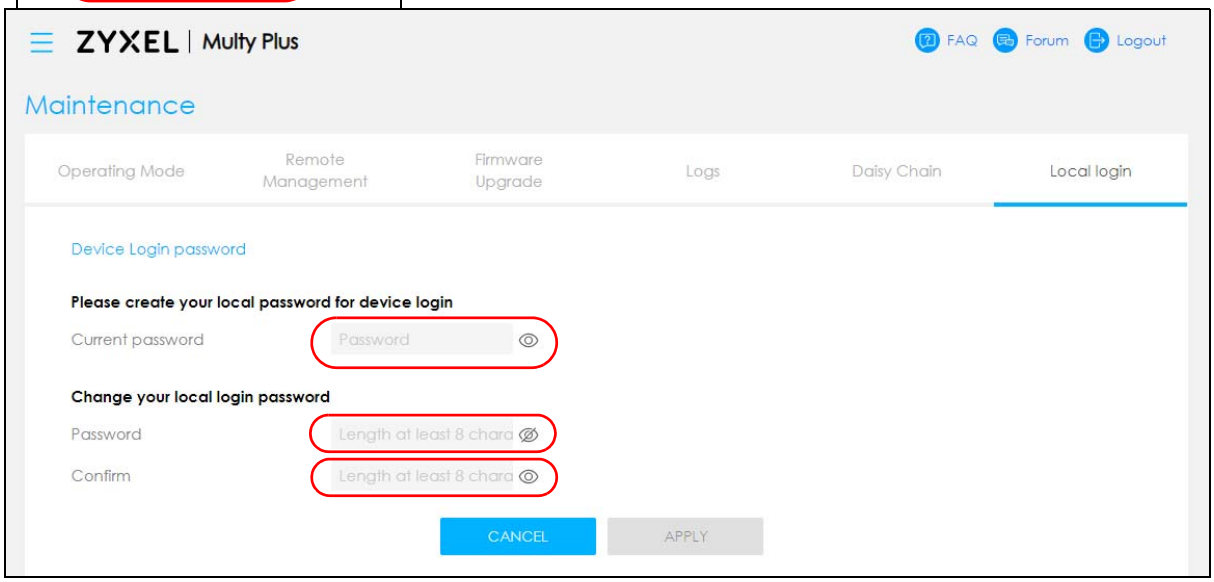


8.16 Local Login Password Change

You can change the Local login password.

1 Click the Navigation Panel icon on the top-left corner ( ). From the **Settings** drop-down list, click **Maintenance**, then click the **Local login** tab.





2 Enter the present password under **Current password** (click the "eyeball" symbol if you wish to view the characters you have entered).

3 Enter the new password under **Password** (8 - 32 characters). Click the "eyeball" symbol if you wish to view the characters you have entered.

Note: The password may contain a mix of letters, numbers, spaces, and/or special characters; and it is case-sensitive. Backslash, single quote, double quote, accent grave, angle brackets, caret, dollar sign, ampersand (\ ' " ‘ <> ^ $ &), and emoji symbols are not allowed.

4 Enter the new password again under **Confirm** (click the “eyeball” symbol if you wish to view the characters you have entered).

5 Then click **Apply** to accept the changes.

PART IV
Troubleshooting and Appendices

CHAPTER 9
Troubleshooting

9.1 Overview

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

- Power, Hardware Connections, and LEDs
- Multy Device Access and Login
- Internet Access
- Resetting the Multy Device to Its Factory Defaults
- WiFi Connections
- OpenVPN Problems
- USB File Sharing Problems

9.2 Power, Hardware Connections, and LEDs

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

- Make sure you are using the power adapter or cord included with the Multy Device.
- Make sure the power adapter or cord is connected to the Multy Device and plugged in to an appropriate power source. Make sure the power source is turned on.
- Disconnect and re-connect the power adapter or cord to the Multy Device.
- If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

- Make sure you understand the normal behavior of the LED.
- Check the hardware connections. See the Quick Start Guide.
- Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- Disconnect and re-connect the power adapter to the Multy Device.
- If the problem continues, contact the vendor.

9.3 Multy Device Access and Login

I do not know the IP address of my Multy Device.

- The default IP address of the Multy Device in **Standard Mode** is **http://Zyxelwifi.com or http://Zyxelwifi.net.**The default IP address of the Multy Device in **Bridge Mode** is **http://(DHCP-assigned IP)**.
- If you changed the IP address and have forgotten it, you might get the IP address of the Multy Device in **Standard Mode** by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start** > **Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the Multy Device (it depends on the network), so enter this IP address in your Internet browser.
- If your Multy Device in **Bridge Mode** is a DHCP client, you can find your IP address from the DHCP server. This information is only available from the DHCP server which allocates IP addresses on your network. Find this information directly from the DHCP server or contact your system administrator for more information.
- Reset your Multy Device to change all settings back to their default. This means your current settings are lost. See Section 9.5 on page 194 in the **Troubleshooting** for information on resetting your Multy Device.

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

- Make sure you are using the correct IP address.
- The default IP address of the Multy Device in **Standard Mode** is **http://Zyxelwifi.com or http://Zyxelwifi.net**.
  The default IP address of the Multy Device in **Bridge Mode** is **http://(DHCP-assigned IP)**.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I do not know the IP address of my Multy Device.
- Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
- Make sure your computer is in the same subnet as the Multy Device. (If you know that there are routers between your computer and the Multy Device, skip this step.)
- Reset the device to its factory defaults, and try to access the Multy Device with the default IP address. See Section 2.4 on page 24.
- If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

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

I can see the **Login** screen, but I cannot log in to the Multy Device.

- This can happen when you fail to log out properly from your last session. Try logging in again after 5 minutes.
- Disconnect and re-connect the power adapter or cord to the Multy Device.
- If this does not work, you have to reset the device to its factory defaults. See Section 9.5 on page 194.

9.4 Internet Access

I cannot access the Internet.

- Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
- Go to **Expert** > **Maintenance** > **Operation Mode**. Check your System Operation Mode setting.

  If the Multy Device is in **Standard Mode**, make sure the WAN port is connected to a broadband modem or router with Internet access. Your computer and the Multy Device should be in the same subnet.

  If the Multy Device is in **Bridge Mode**, make sure the WAN port is connected to a broadband modem or router with Internet access and your computer is set to obtain an dynamic IP address.
- If the Multy Device is in **Standard Mode**, make sure you entered your ISP account information correctly in the wizard or the WAN screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- If you are trying to access the Internet wirelessly, make sure the WiFi settings in the WiFi client are the same as the settings in the AP.
- Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the Multy Device), but my Internet connection is not available anymore.

- Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
- Reboot the Multy Device.
- If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

- There might be a lot of traffic on the network. Look at the LEDs. If the Multy Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- Check the signal strength. If the signal strength is low, try moving the Multy Device closer to the AP if possible, and look around to see if there are any devices that might be interfering with the WiFi network (for example, microwaves, other WiFi networks, and so on).
- Reboot the Multy Device.
- If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

9.5 Resetting the Multy Device to Its Factory Defaults

If you reset the Multy Device, you lose all of the changes you have made. The Multy Device reloads its default settings (for example, default Standard (Router) operation mode and login IP address, WiFi SSID and password). You have to make all of your changes again.

You will lose all of your changes when you push the **Reset** button.

To reset the Multy Device:

- Make sure the power LED is on.
- Press the **Reset** button for 1 to 4 seconds to restart/reboot the Multy Device.
- Press the **Reset** button for longer than 5 seconds to set the Multy Device back to its factory-default configurations.

  If the Multy Device restarts automatically, wait for the Multy Device to finish restarting, and log in to the Web Configurator.

  If the Multy Device does not restart automatically, disconnect and reconnect the Multy Device's power. Then, follow the directions above again.

9.6 WiFi Connections

I cannot access the Multy Device or ping any computer from the WLAN.

- Make sure the WiFi is enabled on the Multy Device.
- Make sure the WiFi adapter on your computer 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 Multy Device.
- Make sure your computer (with a WiFi adapter installed) is within the transmission range of the Multy Device.
- Check that both the Multy Device and the WiFi adapter on your computer are using the same WiFi and WiFi security settings.

- Make sure traffic between WiFi and the LAN is not blocked by the firewall on the Multy Device.
- Make sure you allow the Multy Device to be remotely accessed through the WLAN interface. Check your remote management settings.

The WiFi connection is slow or intermittent.

The following factors may cause interference:

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

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

- Move your WiFi device closer to the Multy Device 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 Multy Device where there are minimum obstacles (such as walls and ceilings) between the Multy Device and the WiFi client. Avoid placing the Multy Device inside any type of box that might block WiFi signals.
- Reduce the number of WiFi clients connecting to the same Multy Device simultaneously, or add additional Multy Devices 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.
- Position the antennas for best reception. If the Multy Device is placed on a table or floor, point the antennas upwards. If the Multy Device is placed at a high position, point the antennas downwards. Try pointing the antennas in different directions and check which provides the strongest signal to the WiFi clients.

9.7 OpenVPN Problems

Client devices cannot connect to the Multy Device server.

- Make sure the Multy Device is in standard (router) mode.
- Make sure DDNS is enabled in the **Settings** > **Internet** > **Dynamic DNS** screen.
- Make sure the OpenVPN Server account is enabled in the **OpenVPN Server** > **OpenVPN Server** screen.
- Make sure **Advertise DNS to Clients** is enabled in **OpenVPN Server** > **OpenVPN Server** screen.
- Make sure the VPN client is using a reliable Internet connection.
- Make sure the VPN client is using the correct protocol (TCP/UDP) to connect to the OpenVPN Server.
- Make sure the client connecting to the OpenVPN Server account is using the same port number (default server port number is 1194) to access the server account.

- Make sure the "key" the VPN clients use to access the OpenVPN Server account is correct. If not, export the new .ovpn configuration file and send it to all OpenVPN clients so that they can use the new key.
- Temporarily disable any Internet security and antivirus software installed on the client device. Some Internet security and antivirus products are known to cause interference with VPN connections and should be disabled.

The Multy Device client cannot connect to an OpenVPN server.

- Do NOT activate OpenVPN Server and OpenVPN Client at the same time on the Multy Device.
- Try to ping the OpenVPN server.
- Make sure connection to an OpenVPN Server account is enabled in the **OpenVPN Server** > **OpenVPN Client** screen.
- Make sure the interface through which the Multy Device connects to an OpenVPN Server account is allowed in the **OpenVPN Server** > **OpenVPN Client** screen's **Enable VPN on** field.
- Make sure you enter the correct user name and password to connect to the OpenVPN Server account.

9.8 USB File Sharing Problems

I cannot access or see a USB device that is connected to the Multy Device.

- Disconnect the problematic USB device, then reconnect it to the Multy Device.
- Ensure that the USB device has power.
- Check your cable connections.
- Restart the Multy Device by disconnecting the power and then reconnecting it.
- If the USB device requires a special driver, install the driver from the installation disc that came with the device. After driver installation, reconnect the USB device to the Multy Device and try to connect to it again with your computer.
- If the problem persists, contact your vendor.

What kind of USB devices do the Multy Device support?

- It is strongly recommended to use version 2.0 or higher USB storage devices (such as NTFS or FAT32 file system, USB hard drives) and/or USB devices. Other USB products are not guaranteed to function properly with the Multy Device.
- The Multy Device do not support 3G/4G USB dongles.

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 Corporation
- https://www.zyxel.com

Asia

China

- Zyxel Communications (Shanghai) Corp.
  Zyxel Communications (Beijing) Corp.
  Zyxel Communications (Tianjin) Corp.
- https://www.zyxel.com/cn/zh/

India

- Zyxel Technology India Pvt Ltd.
- https://www.zyxel.com/in/en/

Kazakhstan

- Zyxel Kazakhstan
- https://www.zyxel.kz

Korea

- Zyxel Korea Corp.
- http://www.zyxel.kr

Malaysia

- Zyxel Malaysia Sdn Bhd.
- http://www.zyxel.com.my

Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

Philippines

- Zyxel Philippines
- http://www.zyxel.com.ph

Singapore

- Zyxel Singapore Pte Ltd.
- http://www.zyxel.com.sg

Taiwan

- Zyxel Communications Corporation
- 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 BY
- https://www.zyxel.by

Bulgaria

- Zyxel България
- 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.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
- https://www.zyxel.com/it/it/

Netherlands

- Zyxel Benelux
- https://www.zyxel.com/nl/nl/

Norway

- Zyxel Communications
- 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

Russia

- Zyxel Russia
- https://www.zyxel.com/ru/ru/

Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- https://www.zyxel.com/sk/sk/

Spain

- Zyxel Communications ES Ltd.
- https://www.zyxel.com/es/es/

Sweden

- Zyxel Communications
- https://www.zyxel.com/se/sv/

Switzerland

- Studerus AG
- https://www.zyxel.ch/de
- https://www.zyxel.ch/fr

Turkey

- Zyxel Turkey A.S.
- https://www.zyxel.com/tr/tr/

UK

- Zyxel Communications UK Ltd.
- https://www.zyxel.com/uk/en/

Ukraine

- Zyxel Ukraine
- http://www.ua.zyxel.com

South America

Argentina

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

Brazil

- Zyxel Communications Brasil Ltda.
- https://www.zyxel.com/br/pt/

Colombia

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

Ecuador

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

South America

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

Middle East

Israel

- Zyxel Communications Corporation
- http://il.zyxel.com/

North America

USA

- Zyxel Communications, Inc. – North America Headquarters
- https://www.zyxel.com/us/en/

APPENDIX B
Legal Information

Copyright

Copyright © 2022 by Zyxel and/or its affiliates

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel and/ or affiliates.

Published by Zyxel and/ or its affiliates. All rights reserved.

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 22 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.

EUROPEAN UNION and UNITED KINGDOM

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

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

- Compliance information forwireless products relevant to the EU, United Kingdom. and other Countries following the EU Directive 2014/53/EU (RED) and UK regulation. And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) and United Kingdom without any limitation except for the countries mentioned below table:
- In the majority of the EU, United Kingdom, and other European countries, the 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5GHz wireless LANs.
- If this device for operation in the band 5150-5350 MHz, it is for indoor use only.
- This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.
  - The maximum RF power operating for each band as follow:
  - The band 2,400-2,483.5 MHz is 99.77 mW.
  - The band 5150-5350 MHz is 198.15 mW.
  - The band 5470-5725 MHz is 995.41 mW.

Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС. **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.ibpt.be pour de plus amples détails.
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..
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. **National Restrictions** • In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage. • I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.
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.
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 http://www.sviluppoeconomico.gov.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 http://www.sviluppoeconomico.gov.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. **National Restrictions** • The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details. • 2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.
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.
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 cerinţele esenţiale 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.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 2014/53/EU.

Notes:

- Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 2014/53/EU has also been implemented in those countries.
- 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 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, use, 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 or unit. 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, 110V 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.
- 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.

Environment Statement

ErP (Energy-related Products)

Zyxel products put on the EU and United Kingdom market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC and UK regulation establishing a framework for the setting of ecodesign requirements for energy-related products (recast), 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 setting for more detail.

Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.

台灣

以下訊息僅適用於產品具有無線功能且銷售至台灣地區

- 取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
- 低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
- 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，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座 (如：北美 / 台灣電壓 110V AC，歐洲是 230V AC)。
- 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. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online at www.zyxel.com to receive email notices of firmware upgrades and related information

Open Source Licenses

This product may contain in part some free software distributed under GPL license terms and/or GPL-like licenses.

To request the source code covered under these licenses, please go to: https://www.zyxel.com/form/gpl_oss_software_notice.shtml

Index

A

Access Control 181
Add Rule 91
Advanced Settings 101
Alexa voice command 98
Amazon account 106
Amazon Alexa 30, 106, 154
Amazon's website 106
Android 30
AP Mode
  menu 131
  status screen 131
Auto-IP Change 13
  conditions 13

B

Backhaul 45
Bluetooth 9, 29
Bridge 94
Bridge Mode 120, 126, 129, 130
Bridge mode 130
bridge mode 13
  default IP address 192
bridge mode example 14
broadband 14, 15, 164

C

certifications 205
  viewing 207
check mark 85
client 75
contact information 197
controller 8, 134
copyright 202
coverage 8
CPU 121
customer service 101
customer support 197

D

Daisy Chain 99, 101
daisy chain 99
data rate 59
DHCP 94
DHCP client 192
DHCP enabled 159
disclaimer 202
DMZ 92, 94, 181
DNS 80, 81, 124, 125
DNS server 80
domain name 80
downstream 56, 59, 164

E

email 101
ESSID 194
Ethernet 80
Ethernet cable 130
extender 8, 44, 45, 80, 134
extender Multy 99

F

feature 99
feedback 101
firmware 97

G

guest WiFi 11

H

HTTP 92
HTTPS 92

I

incoming packet 88
Internet access
problem 193
Internet connection
slow or intermittent 193
Internet connection speed 55
Internet Protocol version 6 12
Internet Service Provider 159
iOS 30
IP address 80
ipconfig 192
IPv4/IPv6 dual stack 12
IPv6 12
IPv6 rapid deployment (6RD) 12
ISP 44

L

LAN client 183
LED 35
LEDs 27
Local login password 188

M

MAC Address 131
Menu 59
mounting base 18, 21, 22
mounting bracket 20
mounting hole 20
Multy Site 34, 35, 46
Multy-Alexa skills 106
myZyxelCloud 30, 32, 96, 103, 106, 117, 118, 119, 120, 154, 162

N

NAT 94, 95
Navigation Panel 164
navigation panel 96

O

OpenVPN Server/Client 11
Operating Mode 150
operating mode 150
ort Forwarding 181
overview 8

P

password 41, 66
ping 194
Port Forwarding 94
port forwarding 88, 152
Port Forwarding Rule 151
Port Forwarding Settings 90
power cable 15
power outlet 15
PPPOE 159
PPPoE 44
primary Multy 99
private network 88

Q

QR code 36, 65, 66

Quick Charge 10

R

reset
NBG7815 194
Reset button 24
reset button 194
Router Mode
status screen 127

S

schedule 71
signal strength 45
smartphone 44, 55, 61
Speed Test 164
speed test 164
standard (router) mode 12
Standard Mode 120, 126, 129
standard mode
default IP address 192
standard mode example 13
Static IP 44
Status 127

T

Telnet
access the NBG7815 192
transmission range
WiFi 194
Tri-Band 10

U

UPnP 94, 124, 181
upstream 56, 59, 164
USB storage device
supported 196

W

warranty 207
note 207
Web Configurator
how to access 120
web configurator 162
WiFi adapter 194
WiFi channel 194
WiFi connection
optimize speed and quality 195
slow or intermittent 195
WiFi coverage 185
WiFi interference
factors 195
WiFi network 65
WiFi password 65
WiFi security 194
WiFi security setting 194
WiFi signal 63
wireless LAN 194
Wireless tutorial 132
WPS 125

Z

Zyxel Multy app 101