

User's Guide

Multy WiFi System

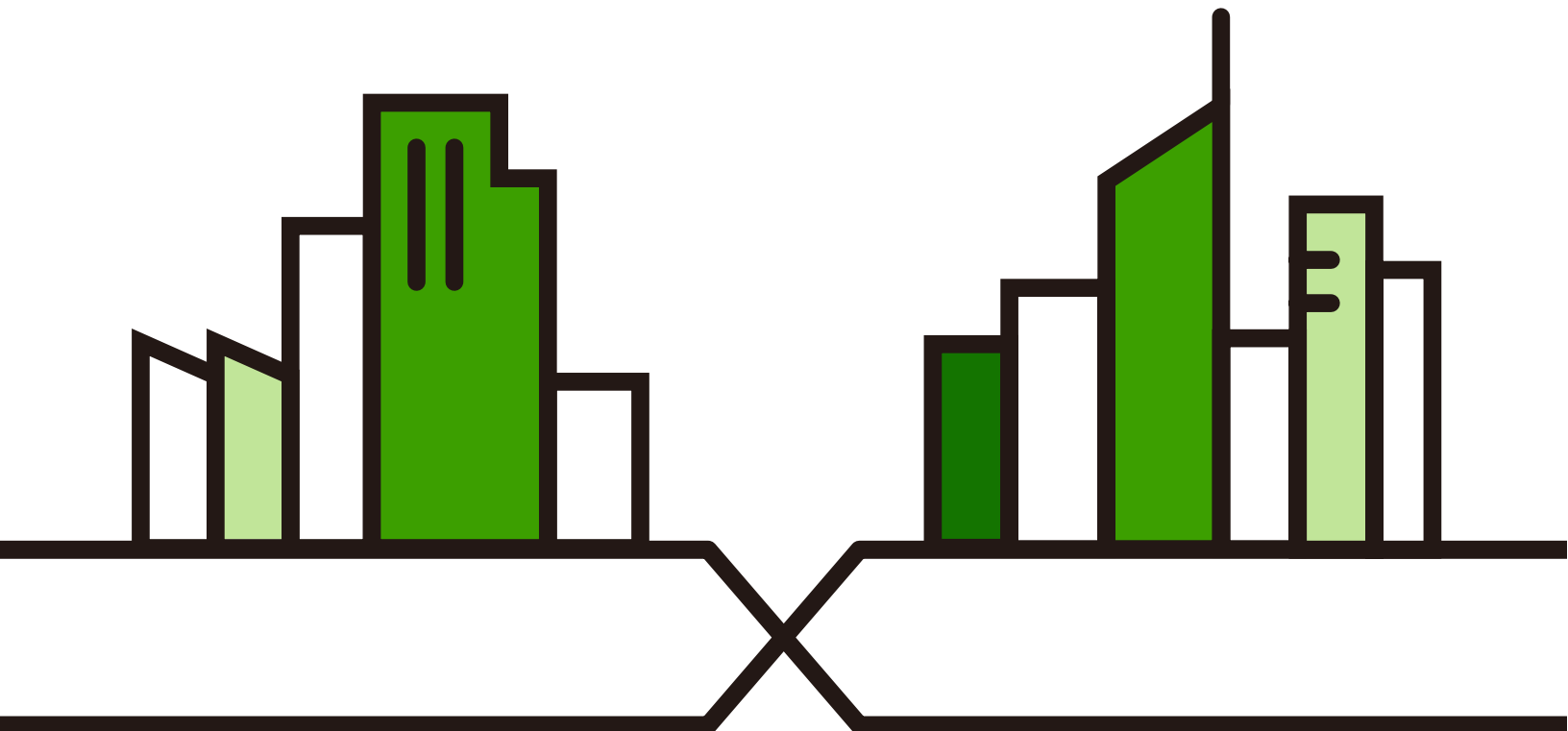
AC/AX WiFi System

Models: WSQ60, WSQ50, WSQ20, WSR30, WSM20, WSQ65, WSQ63,
SCR 50AXE

Default Login Details

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

Version 2.4.0 Edition 1, 12/2022



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 Mesh Network	10
1.2.1 Dual-Band WiFi	12
1.2.2 AP Steering	12
1.2.3 Band Steering	13
1.3 Applications for the Multy Device	13
1.4 Operating Modes for the Multy Device	15
1.4.1 Standard (Router) Mode	15
1.4.2 Bridge Mode	16
1.5 How to Manage Your Multy Sites	17
1.6 Getting Started	17
Chapter 2	
Hardware	18
2.1 Hardware Connections	18
2.2 Hardware Installation	20
2.2.1 Wall Mounting	20
2.2.2 Leather Strap Hanging	27
2.2.3 Desk Placement	28
2.3 WPS Button	30
2.4 Reset Button	30
2.4.1 Reset the Multy Device Back to Factory Default Settings	33
2.5 LED On/Off Switch	33
2.6 LED Light	34
Chapter 3	
App Tutorials – Zyxel Multy	39
3.1 Introduction	39
3.2 Using the Zyxel Multy App	40
3.3 Add and Install Your First Multy Device	44
3.4 Check Your Multy-to-Multy Signal Strength	61
3.5 Remove a Multy Device	63
3.6 Remove a Multy Site	64
3.7 Add a Multy Device to a New Site	66
3.8 Install a Second Multy Site	68

3.9 Test Your Smartphone Connection Speed	72
3.10 Test Your Multy Device Connection Speed	75
3.11 Measure Your WiFi Signal Strength	78
3.12 Enable or Disable Guest WiFi	80
3.13 Share WiFi Name and Password with a QR Code	82
3.14 Set a WiFi Schedule for Clients	84
3.15 Pause Internet Access for an Individual Client	90
3.16 Pause or Resume Internet Access for a Group	93
3.17 Check your Multy Device's Configuration Details	95
3.18 Use Custom DNS Server	97
3.19 Restart Your Multy Device	99
3.20 Change the Name or Picture of a Multy Site	100
3.21 Create or Change Your Web Configurator Password	103
3.22 Enable or Add Port Forwarding Rules	105
3.23 Enable DMZ	109
3.24 Switch to NAT or Bridge Mode	111
3.25 Turn Notifications On or Off	113
3.26 Enable or Disable Daisy Chain Network Topology	116
3.27 Report a Problem With the Zyxel Multy App	118
3.28 Log Out of the myZyxeCloud Account	120
3.29 View Legal and Regulatory Information	121
3.30 Manage Your Multy WiFi System With Amazon Alexa	123

Chapter 4

Wizard – Multy M1 (WSM20)128

4.1 Overview	128
4.2 Accessing the Wizard	128

Chapter 5

Web Configurator – Multy M1 (WSM20)138

5.1 Overview	138
5.2 Accessing the Web Configurator	138
5.3 Navigation Panel	140
5.3.1 Standard Mode Navigation Panel	141
5.3.2 Bridge Mode Navigation Panel	143

Chapter 6

Multy M1 (WSM20) Modes.....144

6.1 Overview	144
6.2 Modes	144
6.3 Standard Mode Overview	145
6.4 What You Can Do	145
6.5 Standard Mode Status Screen	145

6.6 Bridge Mode Overview	147
6.7 What You Can Do	147
6.8 Setting your Multy Device to Bridge Mode	147
6.8.1 Accessing the Web Configurator in Bridge Mode	148
6.9 Bridge Mode Status Screen	149

Chapter 7

Web Interface Tutorials – Multy M1 (WSM20)150

7.1 Overview	150
7.2 Run a Speed Test	150
7.3 Configure the Multy Devices in a Mesh Network	152
7.4 Configure Main WiFi Networks	154
7.5 Configure Guest WiFi Networks	156
7.6 Configure Parental Control Schedule	157
7.6.1 Create a Parental Control Profile	157
7.7 Configure a Firewall Rule	160
7.7.1 Enable Respond to Ping and Firewall	160
7.7.2 Enable Access Control	161
7.8 Configure the Multy Device as an OpenVPN Server	163
7.9 Configure the Multy Device as an OpenVPN Client	165
7.10 Change the Web Configurator Local Password	167
7.11 Change the Operating Mode	167
7.12 Configure a Port Forwarding Rule	168

Chapter 8

Web Interface Tutorials – Multy Plus (WSQ60)171

8.1 Introduction	171
8.2 Using the Web Configurator	171
8.2.1 Login with Local Password	173
8.3 Add and Install Your First Multy Device	175
8.4 Run a Speed Test	179
8.5 Configure the Multy Device's WiFi Networks	180
8.6 Enable or Disable a WiFi Network	182
8.7 Add Clients to a Profile	184
8.8 Set a Profile's WiFi Schedule	185
8.9 Pause or Resume Internet Access on a Profile	187
8.10 Turn On or Off the Multy Device's LED (Light)	189
8.11 Remove a Multy Device	190
8.12 Install a Second Multy WiFi System	192
8.13 Change Your Multy Device Operating Mode	192
8.14 Configure a Port Forwarding Rule	194
8.15 Enable or Disable Daisy Chain Network Topology	195
8.16 Local Login Password Change	198

Chapter 9	
Web Interface Tutorials – Multy M6E (WSQ65).....	201
9.1 Overview	201
9.2 WiFi Network Setup	201
9.2.1 Changing Security on a WiFi Network	201
9.2.2 Connecting to the Multy Device's WiFi Network Using WPS	203
9.2.3 Setting Up a Guest Network	205
9.2.4 Setting Up Two Guest WiFi Networks on Different WiFi Bands	210
9.3 Network Security	215
9.3.1 Configuring a Firewall Rule	215
9.3.2 Parental Control	217
9.3.3 Configuring a MAC Address Filter	219
9.4 Device Maintenance	220
9.4.1 Upgrading the Firmware	220
9.4.2 Backing Up the Device Configuration	221
9.4.3 Restoring the Device Configuration	222
Chapter 10	
Troubleshooting.....	225
10.1 Overview	225
10.2 Power, Hardware Connections, and LEDs	225
10.3 Multy Device Access and Login	226
10.4 Internet Access	227
10.5 Resetting the Multy Device to Its Factory Defaults	228
10.6 WiFi Connections	228
10.7 OpenVPN Problems	229
10.8 USB File Sharing Problems	230
Appendix A Customer Support	231
Appendix B Legal Information	236
Index	242

PART I

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.

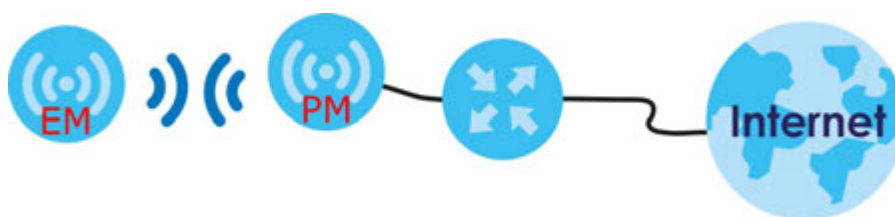
Note: At the time of writing, a maximum of four Multy Devices (one primary Multy and up to three extender Multys) can be used in a Multy Site.

The table below explains the terms used in this User's Guide:

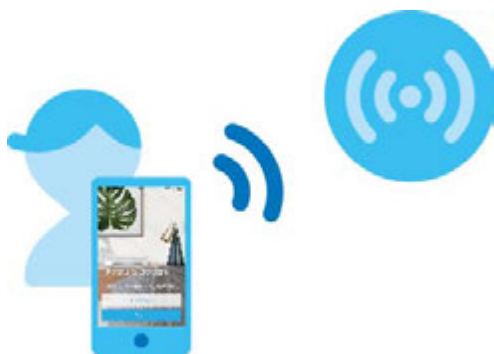
Table 1 Tutorial Terms Definition

TERM	DEFINITION
Primary Multy (PM)	Multy Device that serves as the controller of a mesh network.
Extender Multy (EM)	Multy Device that serves as an extender of a mesh network.

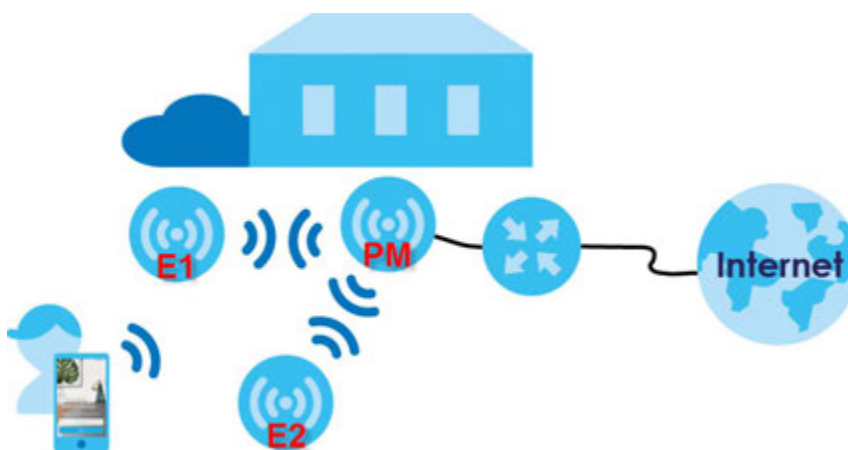
Multy Devices can act either as a primary Multy or an extender Multy. As shown in the next figure, a primary Multy (**PM**) is connected to a modem or router. An extender Multy (**EM**) connects wirelessly to the primary Multy to expand its range. See [Table 3 on page 11](#) to know which Multy devices can be used as a primary Multy or extender Multy.



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 WiFi coverage. The extender Multys help relay communications from WiFi 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)
- Multy M6E (WSQ65)

Table 2 Differences Between Multy Devices

FEATURE	MULTY PLUS (WSQ60)	MULTY X (WSQ50)	MULTY MINI (WSQ20)	MULTY U (WSR30)	MULTY M1 (WSM20)	MULTY M6E (WSQ65)
Maximum Bandwidth	3000 (WiFi6 Tri-Band)	3000 (WiFi6 Tri-Band)	1750 (Dual-Band)	2100 (WiFi6 Tri-Band)	1800 (Dual Band)	5400 (WiFi6E Tri-Band)
Use as primary Multy	YES	YES	NO	YES	YES	YES
Daisy Chain Topology	YES	YES	NO	NO	NO	NO
Bluetooth	YES	YES	YES	YES	NO	NO
USB Port	YES	YES	YES (Quick Charge 3.0)	NO	NO	NO

Table 2 Differences Between Multy Devices (continued)

FEATURE	MULTY PLUS (WSQ60)	MULTY X (WSQ50)	MULTY MINI (WSQ20)	MULTY U (WSR30)	MULTY M1 (WSM20)	MULTY M6E (WSQ65)
Quick Charge	NO	NO	YES	NO	NO	NO
LED On/Off Switch (Side Panel)	NO	NO	NO	NO	YES	NO
LED On/Off Switch (App)	YES	YES	YES	NO	NO	NO
WPS Button	NO	NO	NO	NO	YES	YES
Pairing Method	Bluetooth	Bluetooth	Bluetooth	Bluetooth	WiFi	WiFi
APP Management	YES	YES	YES	YES	YES	YES
GUI Management	YES	NO	NO	NO	YES	YES
Number of LAN Ports	3	3	1	1	4	5
Number of internal antennas						
5G	6	6	3	4	2	4
2.4G	2	2	3	2	2	4
BLE (Bluetooth Low Energy)	1	1	1	1	0	0
E-label	NO	NO	YES	YES	YES	NO
Amazon Alexa	YES	YES	YES	YES	YES	NO

A WiFi 6E Tri-Band WiFi System emits one 2.4 GHz, one 5 GHz and one 6 GHz WiFi signals. A WiFi 6 Tri-Band WiFi System emits one 2.4G WiFi signal and two 5G WiFi signals. Dual-Band WiFi Systems emit one 2.4G signal and one 5G signal.

“Maximum Bandwidth” refers to the sum of the bandwidths of all WiFi signals (2.4G and 5G) emitted by the Multy Device. 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.

1.2 Mesh Network

A Mesh network is composed of three key components.

- (A) The primary Multy works as a controller to manage and optimize the Mesh network.
- (B) One or more extender Multy in the Mesh network function a WiFi extender to extend the WiFi communication range.
- (C) Multiple client devices connect to the Mesh network for Internet connections.

Assigned Roles in a Mesh Network

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

Table 3 The Assigned Roles in a Mesh Network

		EXTENDER MULTY					
		MULTY PLUS (WSQ60)	MULTY X (WSQ50)	MULTY MINI (WSQ20)	MULTY U (WSR30)	MULTY M1 (WSM20)	MULTY M6E (WSQ65)
PRIMARY MULTY	Multy Plus (WSQ60)	YES	NO	NO	NO	NO	NO
	Multy X (WSQ50)	NO	YES	YES	NO	NO	NO
	Multy U (WSR30)	NO	NO	NO	YES	NO	NO
	Multy M1 (WSM20)	NO	NO	NO	NO	YES	NO
	Multy M6E (WSQ65)	NO	NO	NO	NO	NO	YES

Assigned Roles in the Zyxel Multy App

The following table shows the role of router and extender of the Multy Device in the Zyxel Multy app.

Table 4 The Assigned Roles in the Zyxel Multy App

	MULTY PLUS (WSQ60)	MULTY X (WSQ50)	MULTY MINI (WSQ20)	MULTY U (WSR30)	MULTY M1 (WSM20)	MULTY M6E (WSQ65)
Router Name in the app	Primary Multy	Primary Multy	Primary Multy	Primary Multy	Multy Router	Primary Router
Extender Name in the app	Extender Multy	Extender Multy	Extender Multy	Extender Multy	Satellite	Satellite

Primary Multy

The primary Multy functions as a network controller to coordinate and optimize WiFi activity in the Mesh network. The controller collects Channel Availability Check responses and scan reports from the Extender Multy. Then, the controller selects the best channel and the final optimized topology based on the current situation.

The Mesh network uses AP steering and Band steering mechanisms to improve WiFi performance.

AP steering allows WiFi clients to roam seamlessly in a Mesh network. Band steering allows 2.4 GHz / 5 GHz dual-band WiFi clients to move from one band to another less busy band. For AP steering to work, the controller and the devices in the Mesh network must use the same SSID and password. For band steering to work, the SSIDs and passwords of 2.4 GHz and 5 GHz must be identical.

See [Section 1.2.2 on page 12](#) and [Section 1.2.3 on page 13](#) for more information. The controller synchronizes the SSIDs and passwords during auto-configuration.

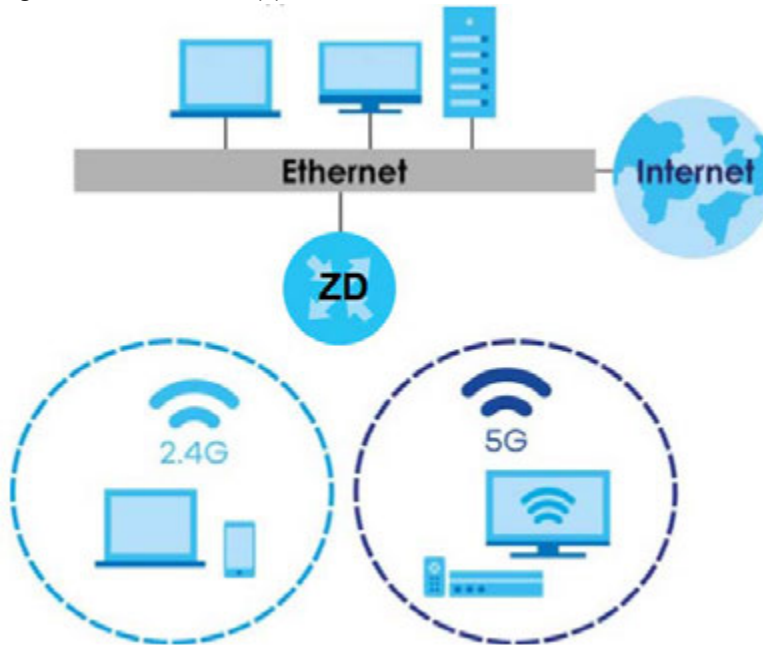
Extender Multy (Satellite)

The Primary Multy connects to a Extender Multy using WiFi. You can place the Extender Multy between the Primary Multy and the WiFi clients who require WiFi but are not in the coverage of the Primary Multy.

1.2.1 Dual-Band WiFi

The Multy Device is a dual-band device that can use both 2.4 GHz and 5 GHz at the same time. IEEE 802.11a/b/g/n/ac/ax compliant clients can wirelessly connect to the Multy Device to access network resources. You could use the 2.4 GHz band for regular Internet surfing and downloading while using the 5 GHz band for time sensitive traffic like high-definition video, music, and gaming.

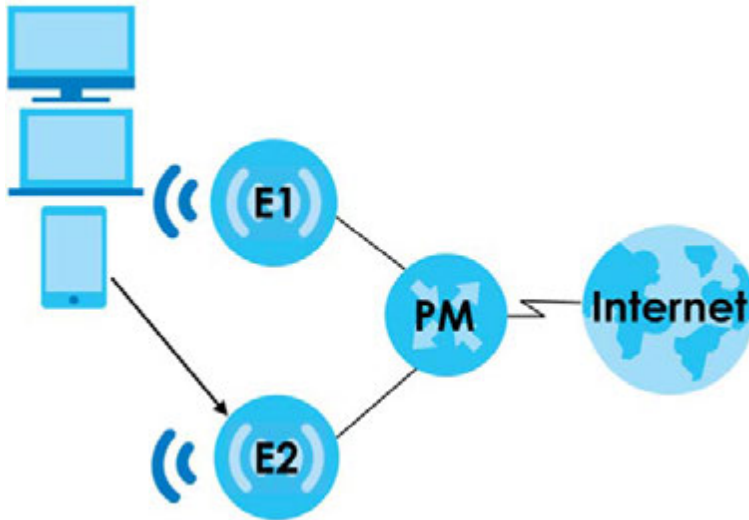
Figure 1 Dual-Band Application



1.2.2 AP Steering

AP steering allows WiFi clients to roam seamlessly in the Mesh network. AP steering helps monitor WiFi clients and drops their connections to optimize the Multy Device bandwidth when the clients are idle or have a low signal. When a WiFi client is dropped, it has the opportunity to reconnect to an AP or WiFi Extender with a stronger signal.

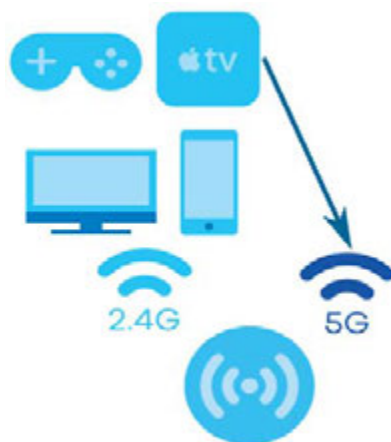
In the following example, the controller (**ZD**) drops the connection between the client device (**C**) and the Extender Multy 1 (**E1**) so that the client device (**C**) can connect to the Extender Multy 2 (**E2**), which has a stronger signal.

Figure 2 AP Steering Application

1.2.3 Band Steering

Band steering allows 2.4 GHz / 5 GHz dual-band WiFi clients to move from one band to another. The controller detects if the client device are dual-band compatible. If a client device supports dual-band WiFi and the 2.4 GHz band is congested, its 2.4 GHz connection is dropped so that it can connect to the less congested 5 GHz band.

In the following example, the Apple TV is a dual-band client device that uses the 5 GHz band.

Figure 3 Band Steering Application

1.3 Applications for the Multy Device

The Multy Device supports the following applications.

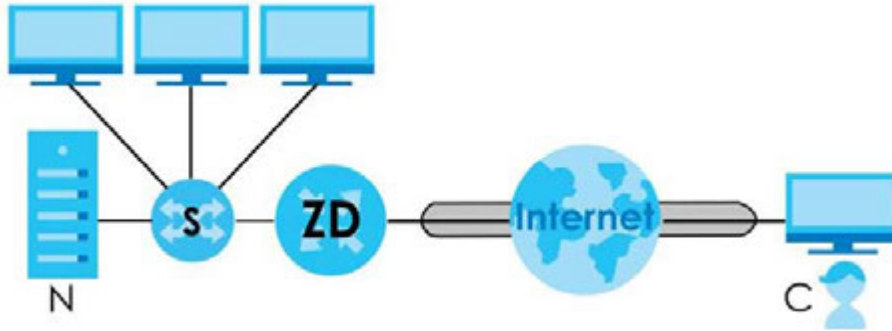
Guest WiFi

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.

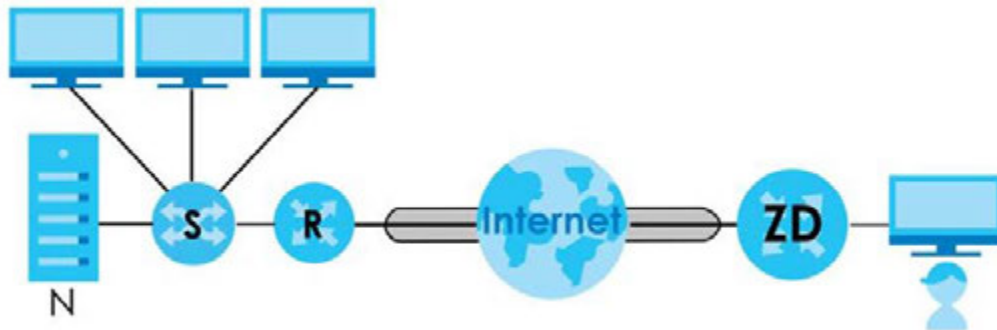
Figure 4 OpenVPN Server Network Scenario



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 5 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 3.4×10^{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).

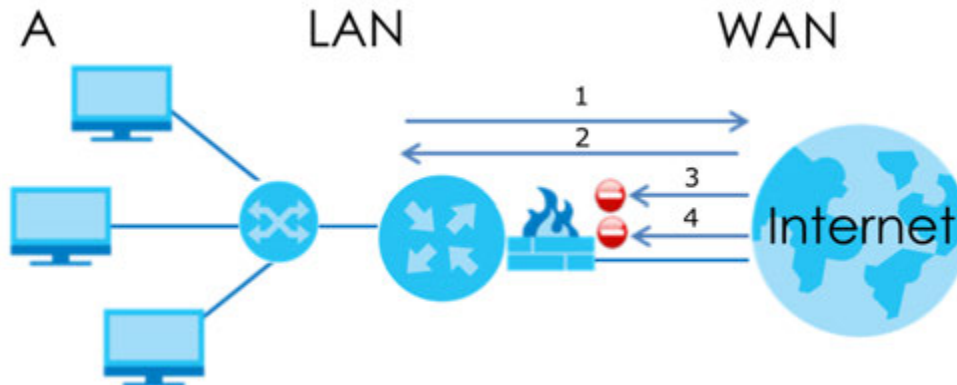
Consequently, you can enable and create IPv6 firewall rules to filter IPv6 traffic.

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 6 Default Firewall Action

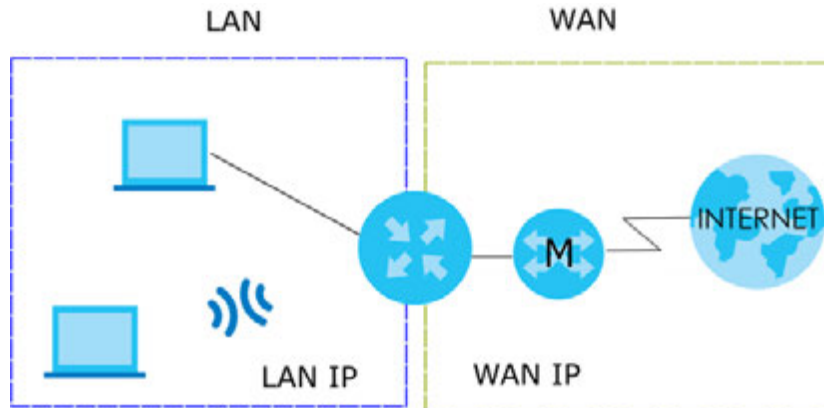


1.4 Operating Modes for the Multy Device

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

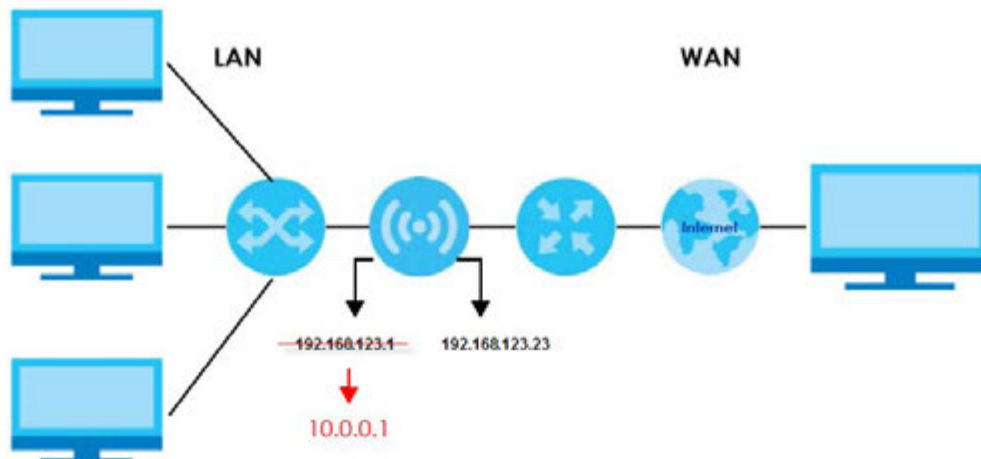
1.4.1 Standard (Router) Mode

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 (router) 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 7 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.

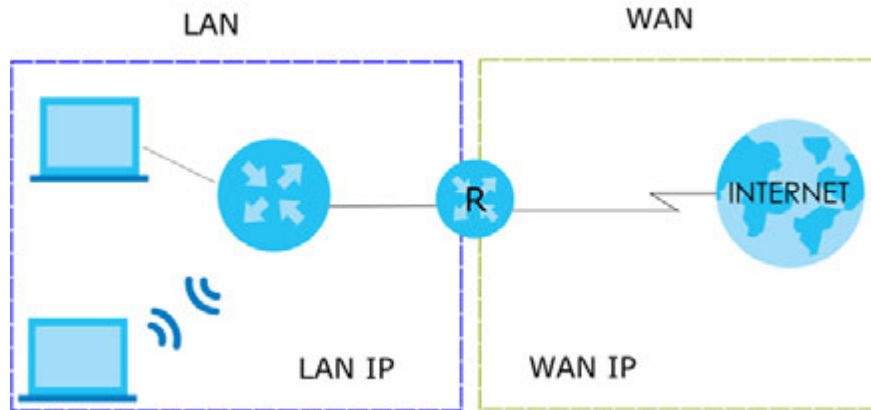
Figure 8 Auto-IP Change Example

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.

1.4.2 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 9 Bridge Mode Example

1.5 How to Manage Your Multy Sites

Use the following methods to manage your Multy WiFi System.

- Web Configurator. This is recommended for everyday management of Multy Devices using a (supported) web browser.
- Multy. Use this app 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.

1.6 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 2 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 39](#)).

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 10 WSQ60 / WSQ50 Rear Panel

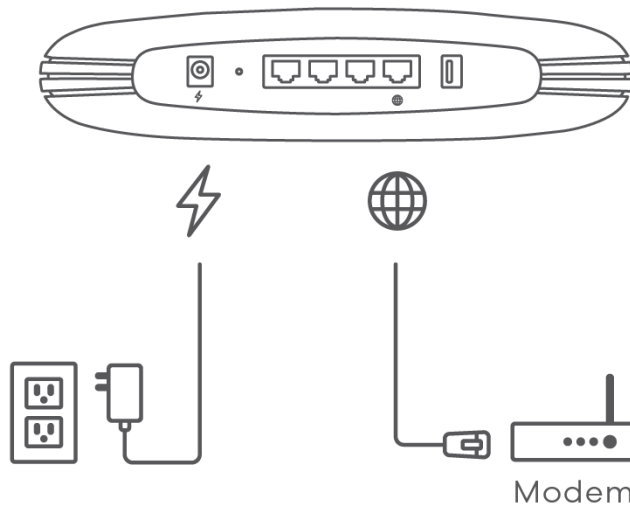


Figure 11 WSQ20 Rear Panel

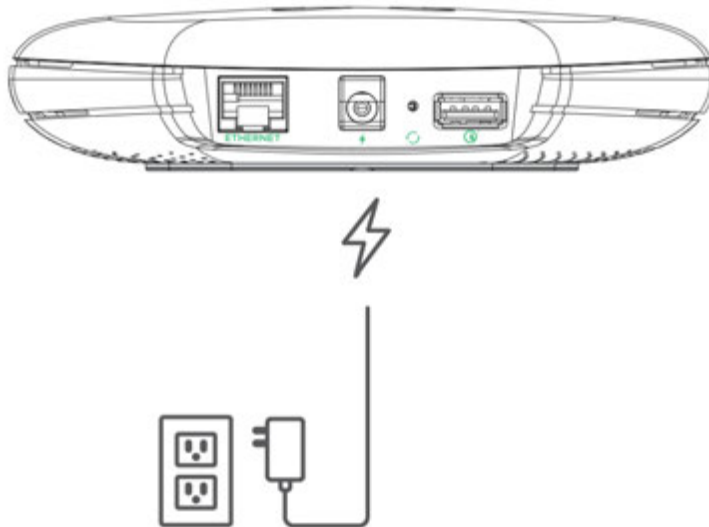


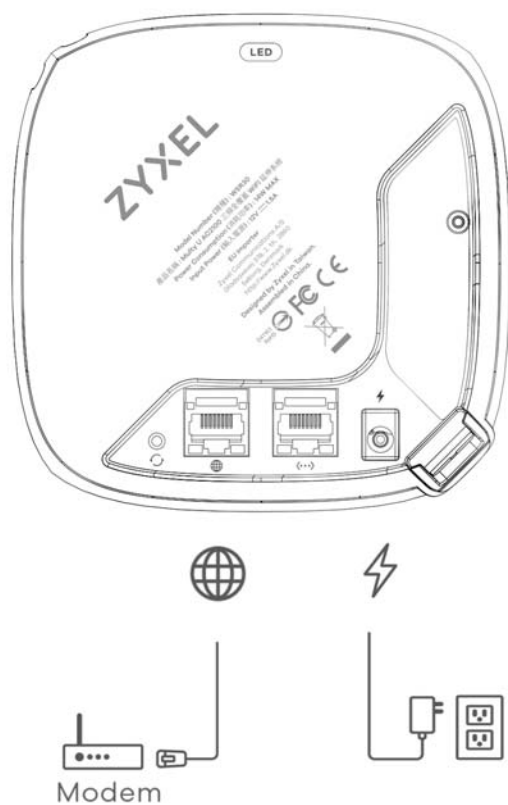
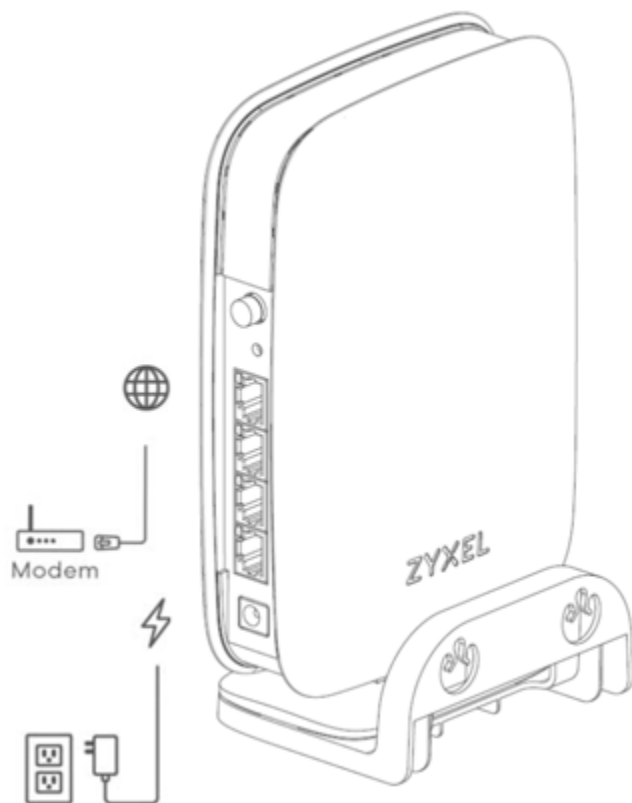
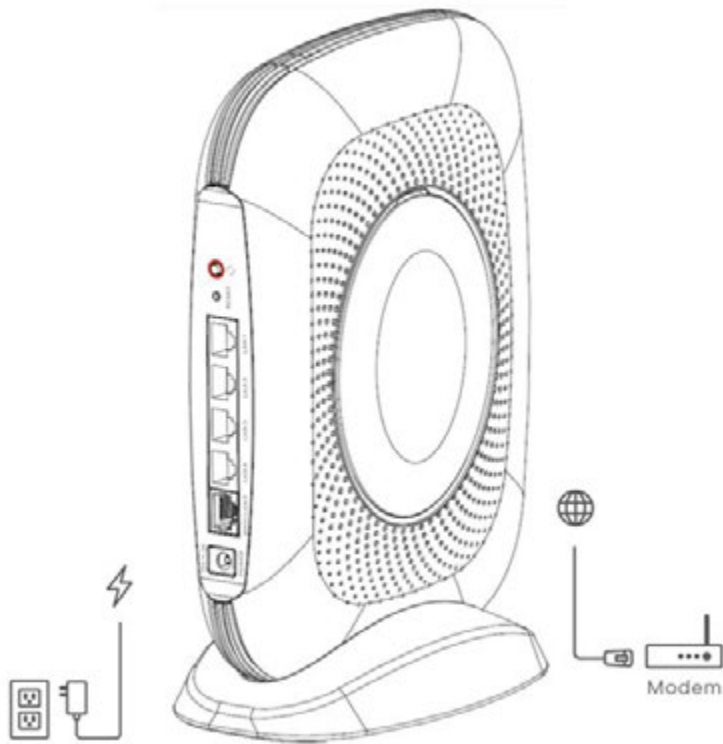
Figure 12 WSR30 Rear Panel**Figure 13** WSM20 Rear Panel

Figure 14 WSQ65 Rear Panel

2.2 Hardware Installation

This section describes how the hardware device can be installed.

Table 5 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
MULTY M6E (WSQ65)	YES	NO	YES	NO

2.2.1 Wall Mounting

Use the wall mounting method to install your Multy Device. See [Table 5 on page 20](#) for more information.

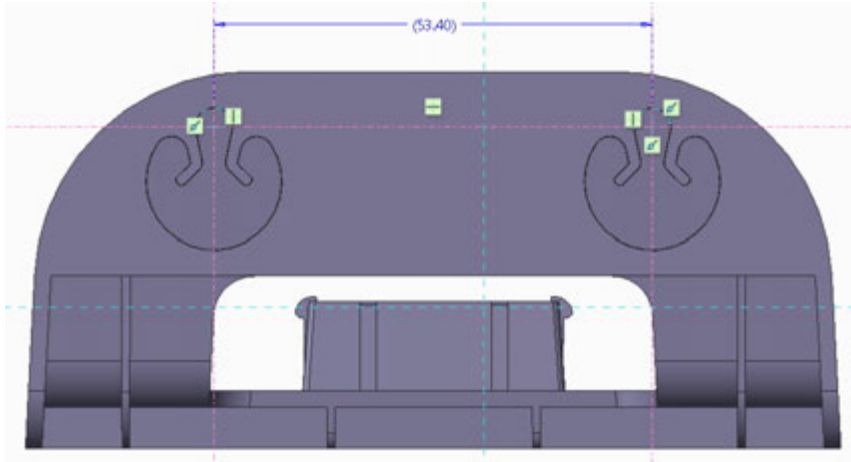
2.2.1.1 WSM20 Wall Mounting

Use the mounting base to attach the WSM20 to a wall.

Follow these steps for the WSM20 wall mounting:

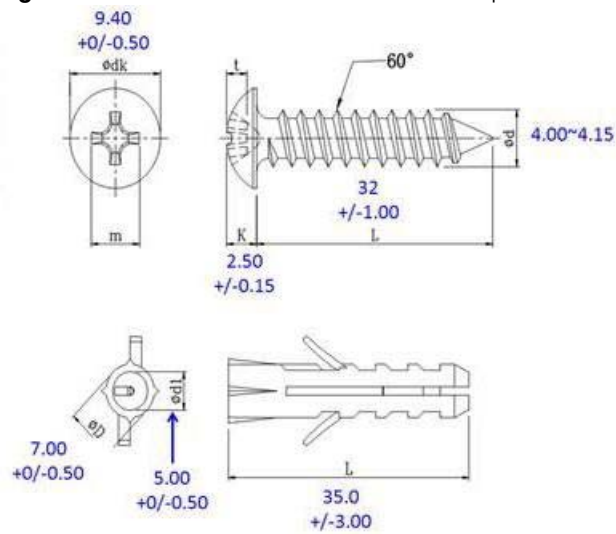
- 1 Use the mounting base to mark two holes on the wall. Drill two holes at the distance of 53.40 mm.

Figure 15 WSM20 Mounting Distance



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

Figure 16 WSM20 M4 Screw and Anchor Specifications



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

Figure 17 Slide the WSM20 Down

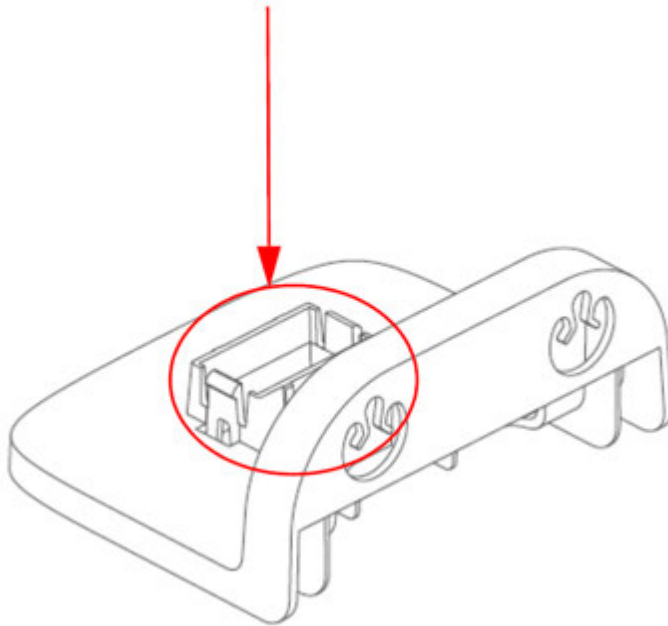
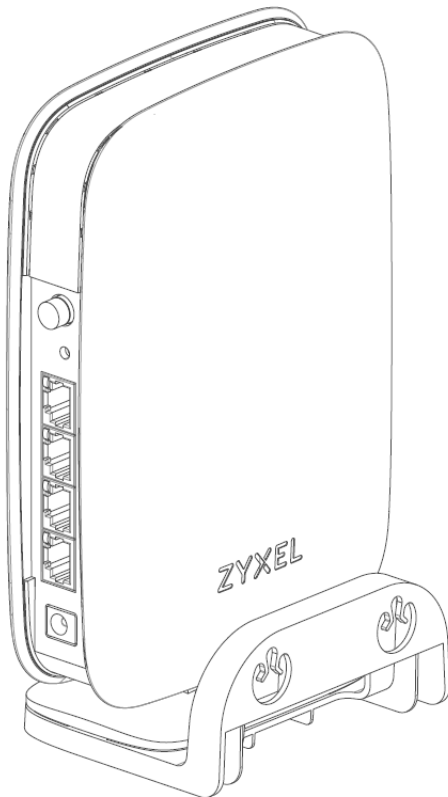


Figure 18 Secure the WSM20 to the Mounting Base



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 19 Hook on the Front Panel

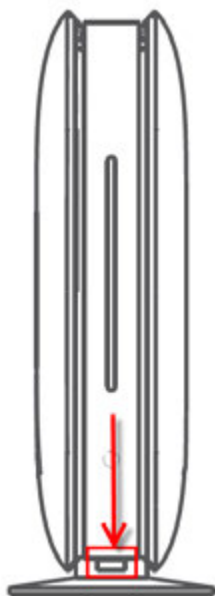
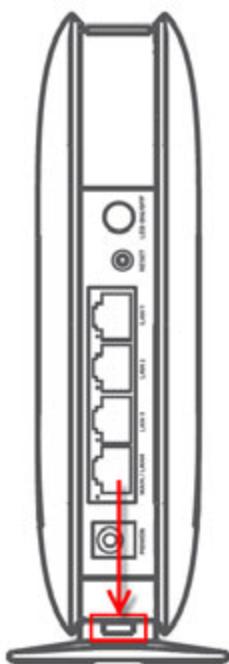
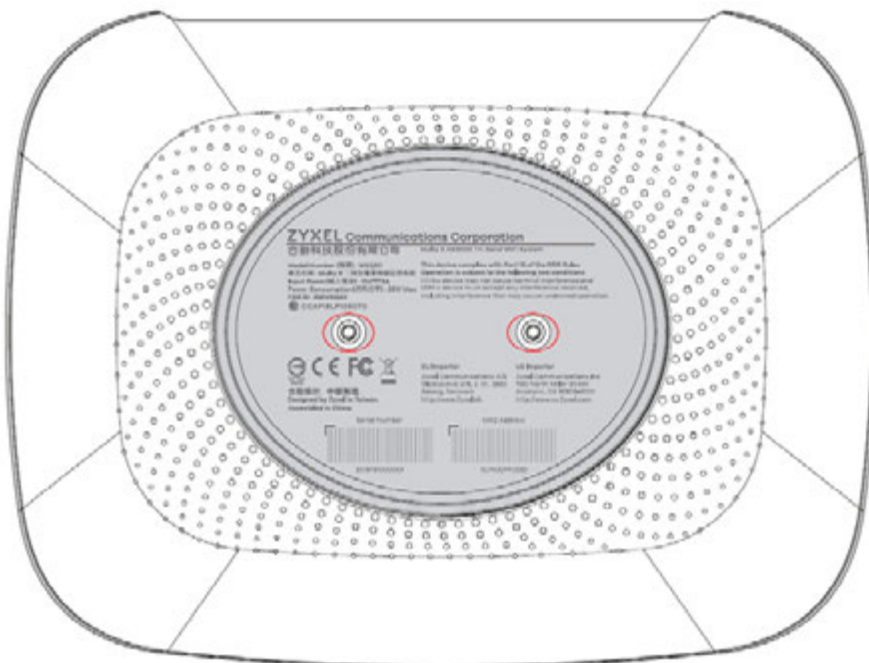
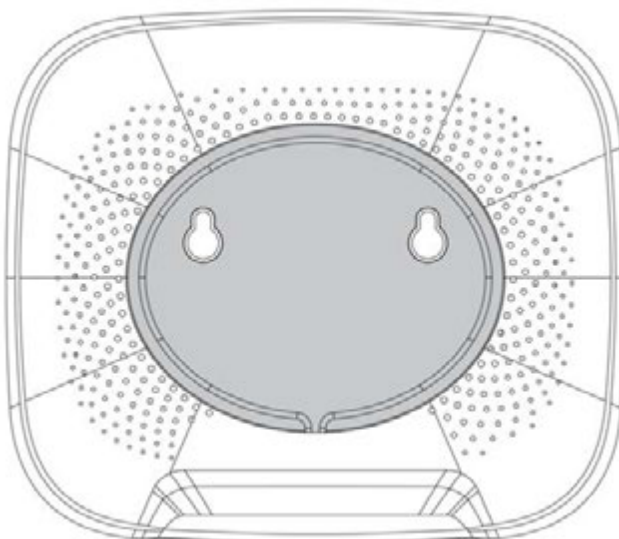


Figure 20 Hook on the Rear Panel



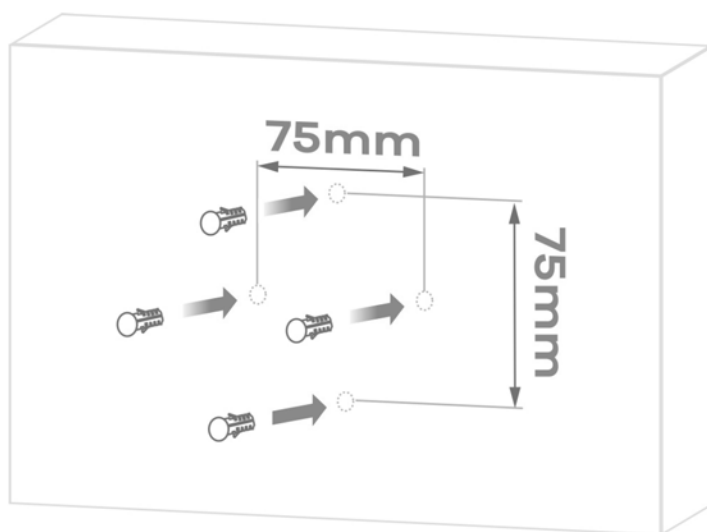
2.2.1.3 WSQ60 / WSQ50 / WSQ20 Wall/Ceiling Mounting

If your Multy Device comes with mounting holes, use mounting brackets to attach it to a wall or ceiling.

Figure 21 WSQ50 / WSQ60 Mounting Holes**Figure 22** WSQ20 Mounting Holes

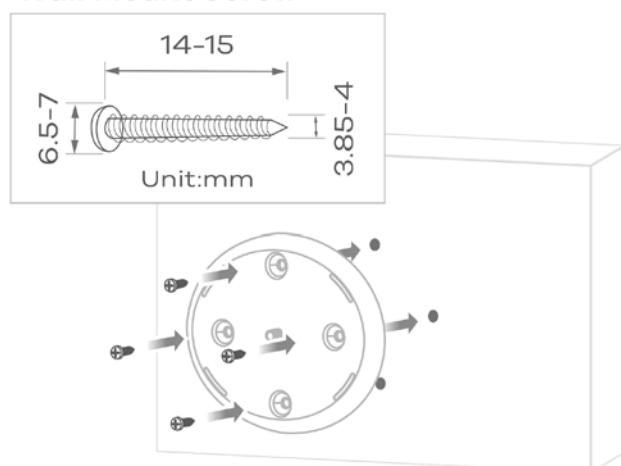
Follow these steps for WSQ60 / WSQ50 / WSQ20 wall or ceiling mounting:

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

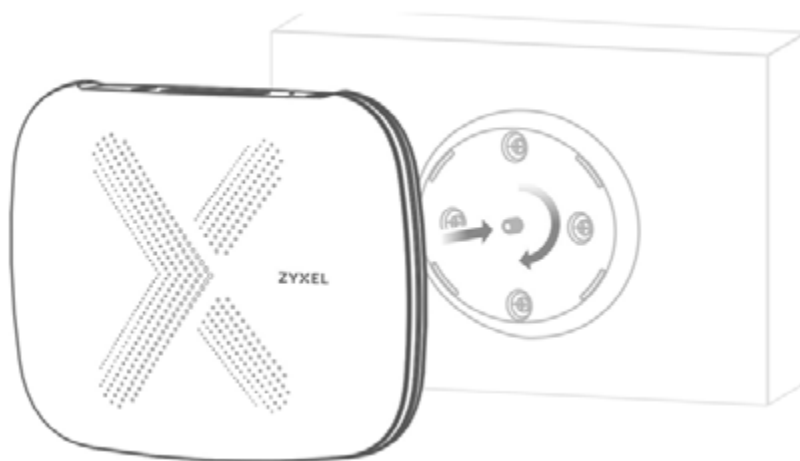


- 2 Screw the mounting base into the wall or ceiling.

Wall Mount Screw



- 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.

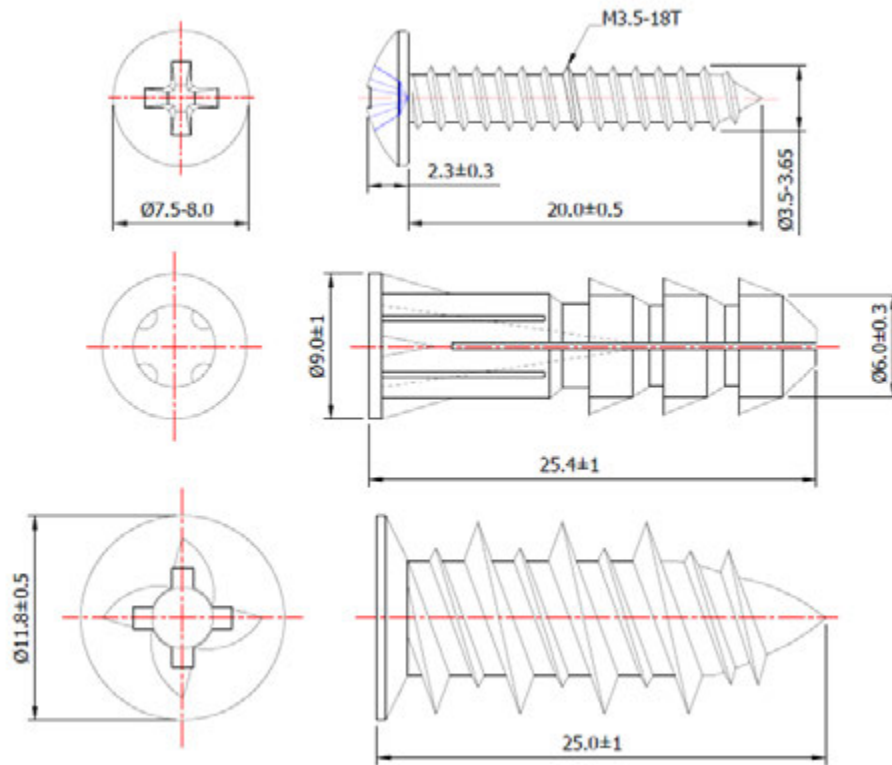


2.2.1.4 WSQ65 Wall Mounting

Mark a hole on the wall at least 2 meter-high from the ground level. Drill the hole and insert the included anchor and wall mount screw into the wall. Align the mounting hole on the Multy Device to the wall mount screw on the wall. Adjust the angle of the Multy Device to make sure it is secure in place.

Figure 23 WSQ65 Mounting Holes



Figure 24 WSQ65 Screw Specifications

2.2.2 Leather Strap Hanging

Use the leather strap hanging method to install your Multy Device. See [Table 5 on page 20](#) 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 25 on page 28](#).

Figure 25 WSR30 Leather Strap



2.2.3 Desk Placement

You may place your Multy Device on a desk, table, shelf, and so on. See [Table 5 on page 20](#) for more information.

2.2.3.1 WSR30

Use the rear port cover as a stand by attaching it to the bottom of the Multy Device (shown in [Figure 26 on page 29](#)).

Figure 26 WSR30 Rear Port Cover**Figure 27** WSR30 Stand

2.2.3.2 WSQ65

Attach the bottom of the Multy Device to the magnetic stand. Then, place the Multy Device on a desk, table, shelf, and so on.

Figure 28 WSQ65 Desk Placement

2.3 WPS Button

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 2 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 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 29 WSQ60 / WSQ50 Reset Button



Figure 30 WSQ20 Reset Button



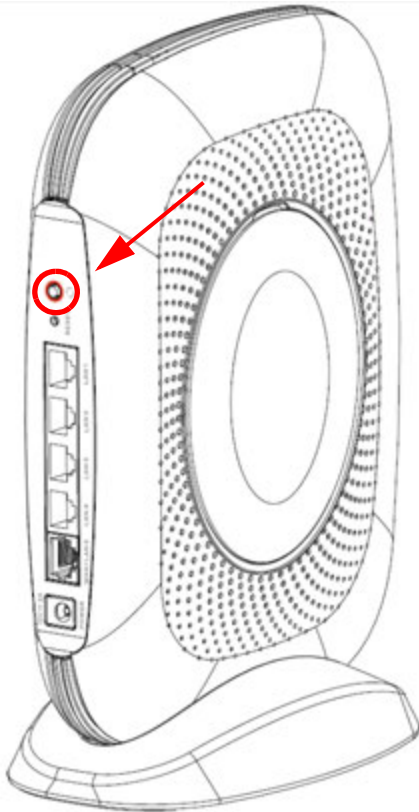
Figure 31 WSR30 Reset Button



Figure 32 WSM20 Reset Button



Figure 33 WSQ65 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.

WSQ65:

Press the reset button for at least 3 seconds or until the LED starts to blink green.

2.5 LED On/Off Switch

WSM20:

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

Figure 34 WSM20 LED On/Off Switch

2.6 LED Light

Look at the LED behavior to determine the status of the Multy Device. See [Table 6 on page 37](#), [Table 7 on page 37](#), and [Table 8 on page 37](#) for more information.

Figure 35 WSQ50 / WSQ60 LED

Figure 36 WSQ20 LED



Figure 37 WSR30 LED



Figure 38 WSM20 LED



Figure 39 WSQ65 LED



The following are the LED descriptions for your Multy Device.

Table 6 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.
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 7 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 8 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	The Multy 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.

Table 9 WSQ65 LED Descriptions

COLOR	STATUS	DESCRIPTION
Blue	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 is setting up a WPS connection with another Multy Device.
Red	On	The Multy Device in AP mode failed to connect to the Internet.
		The Multy Device in extender mode cannot connect to the Primary Multy.
Purple	On	The Multy Device is updating firmware.
	Blinking	The Multy Device is being reset.

CHAPTER 3

App Tutorials – Zyxel Multy

3.1 Introduction

The Zyxel Multy app helps you install Multy Devices and manage your Multy Sites directly with your smartphone.

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

- [Using the Zyxel Multy App](#)
- [Add and Install Your First Multy Device](#)
- [Check Your Multy-to-Multy Signal Strength](#)
- [Remove a Multy Device](#)
- [Remove a Multy Site](#)
- [Add a Multy Device to a New Site](#)
- [Install a Second Multy Site](#)
- [Test Your Smartphone Connection Speed](#)
- [Test Your Multy Device Connection Speed](#)
- [Measure Your WiFi Signal Strength](#)
- [Enable or Disable Guest WiFi](#)
- [Share WiFi Name and Password with a QR Code](#)
- [Set a WiFi Schedule for Clients](#)
- [Pause Internet Access for an Individual Client](#)
- [Pause or Resume Internet Access for a Group](#)
- [Check your Multy Device's Configuration Details](#)
- [Use Custom DNS Server](#)
- [Restart Your Multy Device](#)
- [Change the Name or Picture of a Multy Site](#)
- [Create or Change Your Web Configurator Password](#)
- [Enable or Add Port Forwarding Rules](#)
- [Enable DMZ](#)
- [Switch to NAT or Bridge Mode](#)
- [Turn Notifications On or Off](#)
- [Enable or Disable Daisy Chain Network Topology](#)
- [Report a Problem With the Zyxel Multy App](#)
- [Log Out of the myZykelCloud Account](#)
- [View Legal and Regulatory Information](#)

- [Manage Your Multy WiFi System With Amazon Alexa](#)

Compatibility

- Android 8.0 or later
- iOS 12.0 or later

3.2 Using the Zyxel Multy App

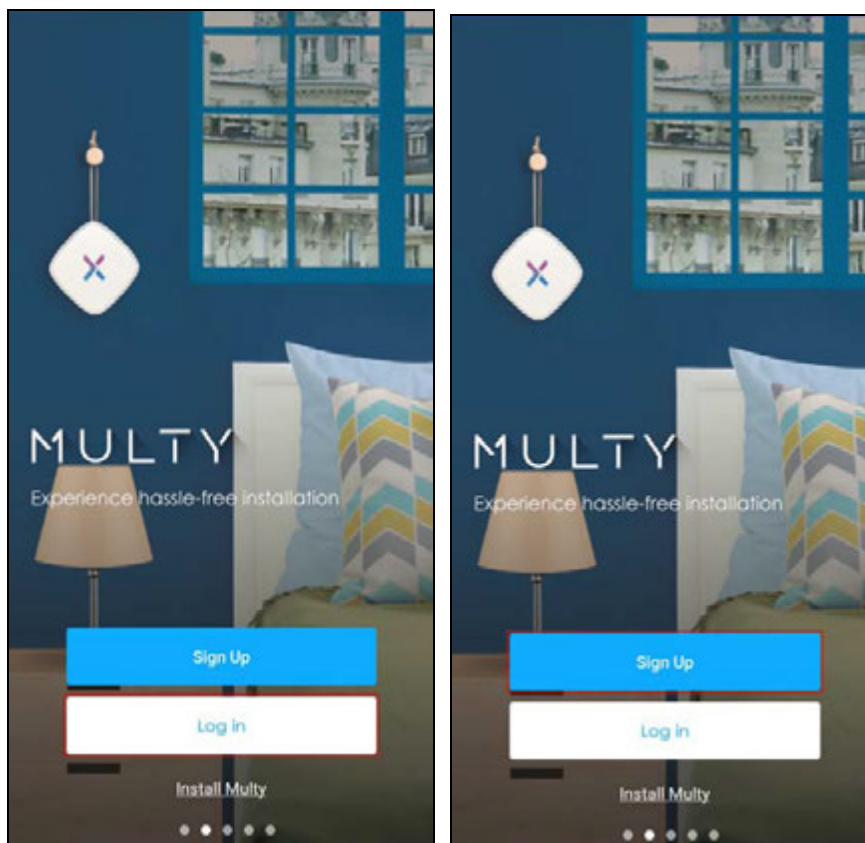
You can log in and use the Zyxel Multy app with or without a myZyxelCloud account.

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 123](#)).

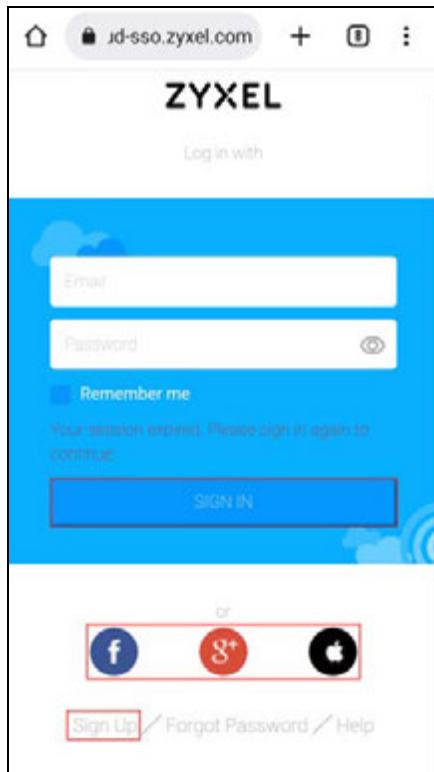
- 1 Install the Zyxel Multy app from Google Play or the Apple App store. Tap the Multy icon to open it.



- 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.

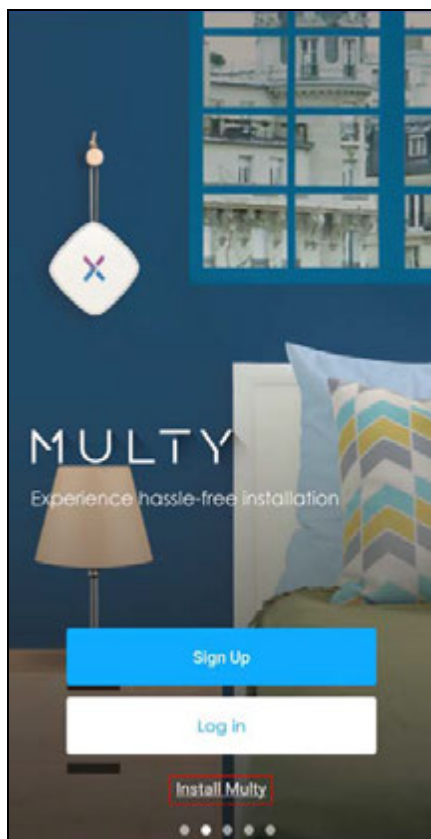


- 3 The following screen displays. Enter your existing Google / Facebook / Apple ID account information and tap **SIGN IN** to log in. Tap **Sign Up** if you want to create a myZyxelCloud account.

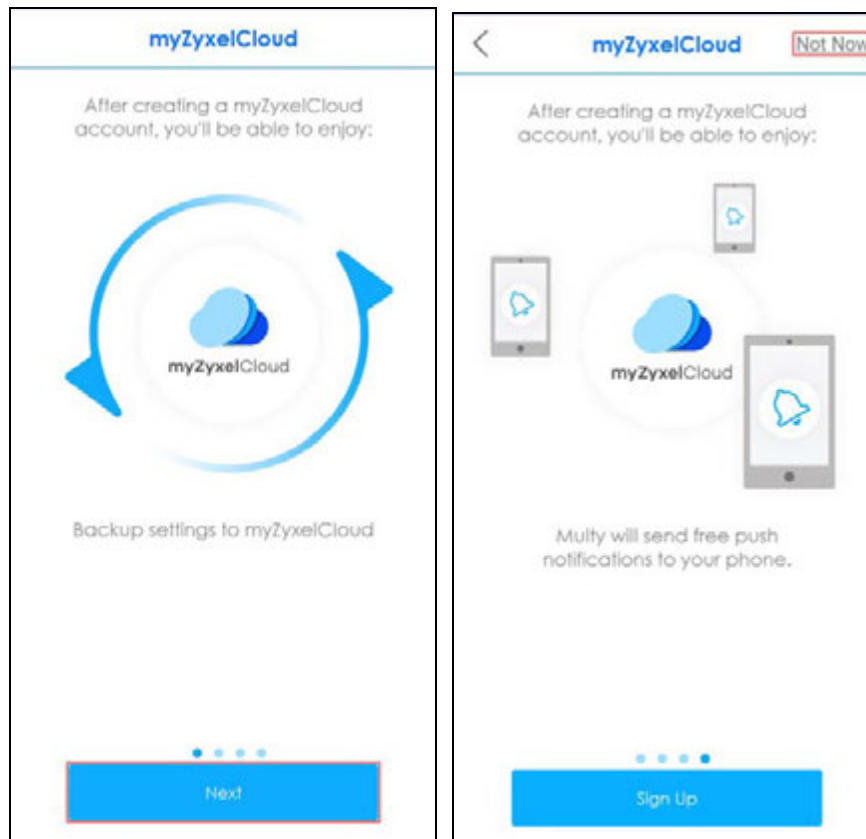


- 4 If you do not have a myZyxelCloud account or do not want to log in with a myZyxelCloud account, tap **Install Multy** in the **Multy** screen.

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 103](#) for more information.



- 5 The following **myZyxeCloud** 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 myZyxeCloud 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.

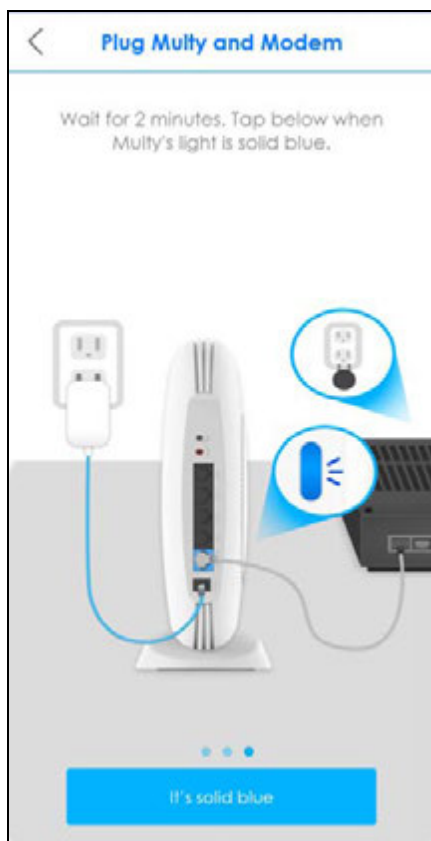
- 1 The **Get Ready** screen appears after you tap the upper right **Not Now**. Choose the product model of your device and tap **Start**.



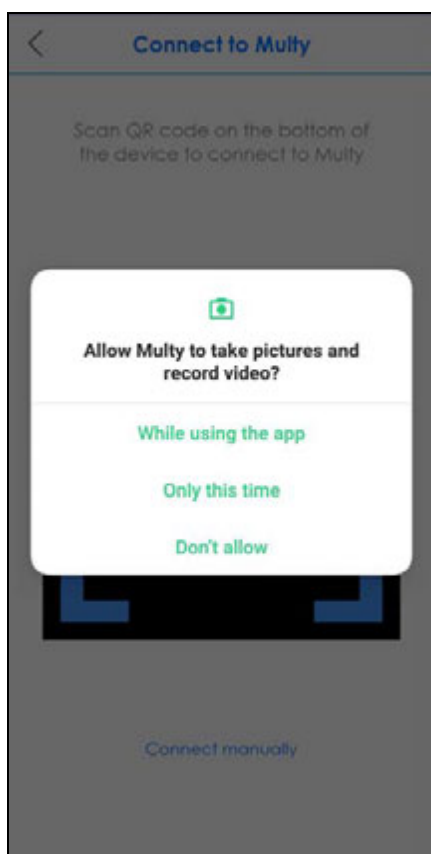
- 2 Tap **Start** to install and add a Multy Device to your Multy Site. Follow the next steps that appear on your screen. Unplug and then plug your modem as instructed in the app to prevent errors.



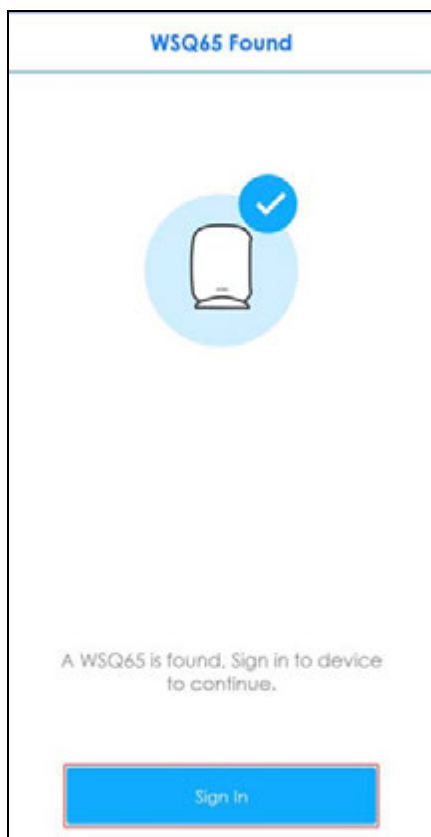
- 3 After unplugging and plugging your modem as instructed, check the LED light and then tap **It's solid lake green** or **It's solid blue** according to the Multy Device you use.



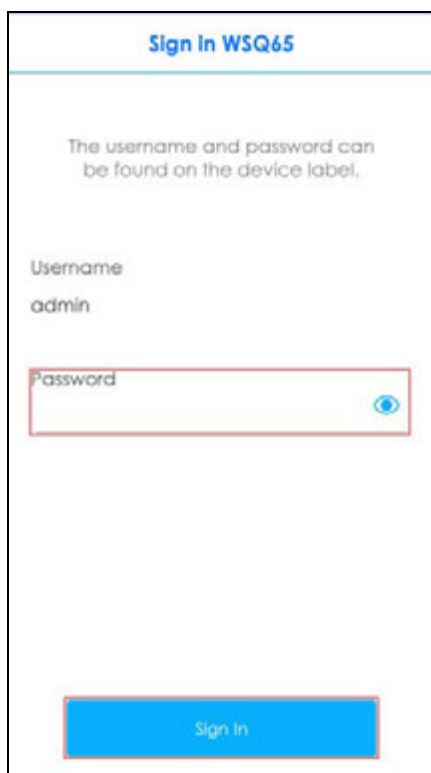
- 4 Allow the Multy app to take pictures. Use your smartphone to scan the QR code to connect your smartphone to the WiFi network of the Multy Device.



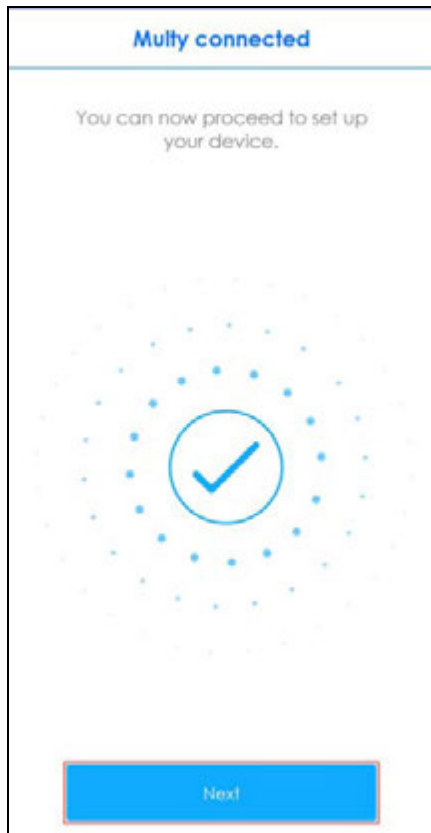
- 5 Your screen displays **Multy Device Found** when your smartphone connects to the WiFi network of the Multy Device. Tap **Sign In** to continue.



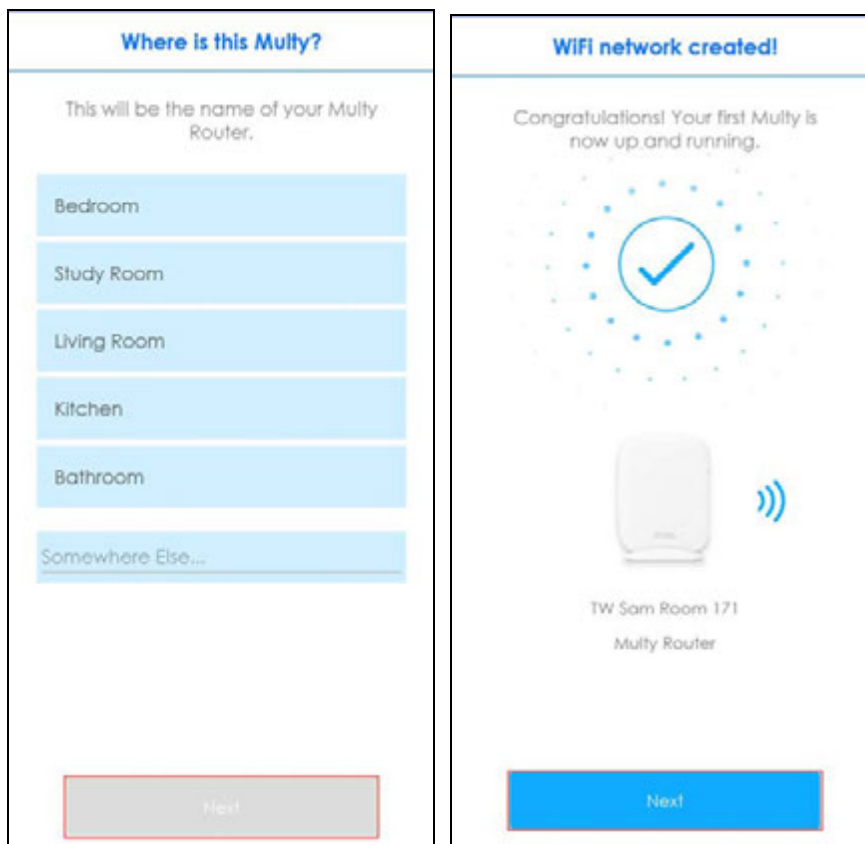
- 6 Enter the **Password** on the Multy Device label. Then tap **Sign In**.



- 7 Wait until the WAN connection has been set up on the Multy Device. Tap **Next** on the **Multy connected** screen to continue.

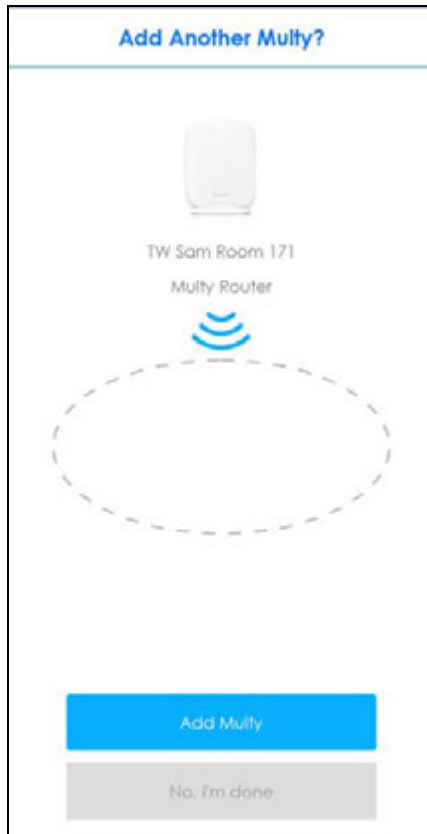


- 8 Select the location where you want to place your Multy Device, and then tap **Next**. The **WiFi network created!** screen appears, and then tap **Next**.



- 9 After the first Multy Device is installed, tap **No, I'm done** to finish the installation. Otherwise, tap **Add Multy** to add another Multy Device (Multy Satellite).

Note: You can skip this step and add another Multy Device later. See [Section 3.7 on page 66](#) for more information.



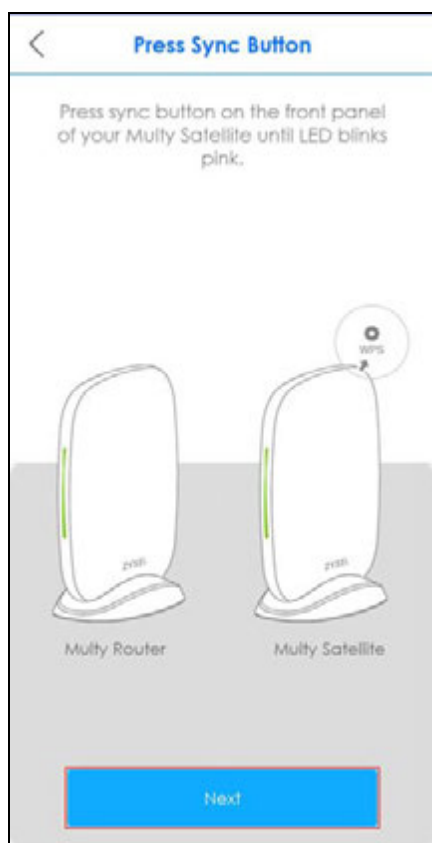
- 10 The following **Get Ready** screen appears after you tap **Add Multy**. Tap **Start** and connect power to your other Multy Device as instructed in the app.



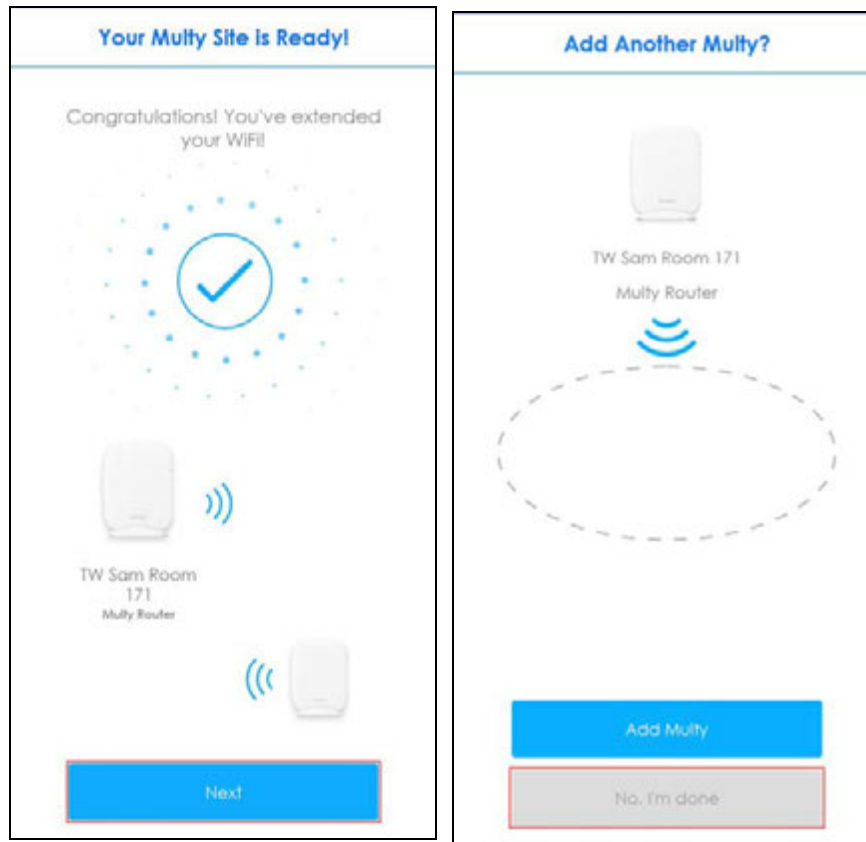
- 11 After connecting power to your other Multy Device, check the LED light and then tap **It's Solid Lake Green** or **It's Solid Blue** according to the Multy Device you use.



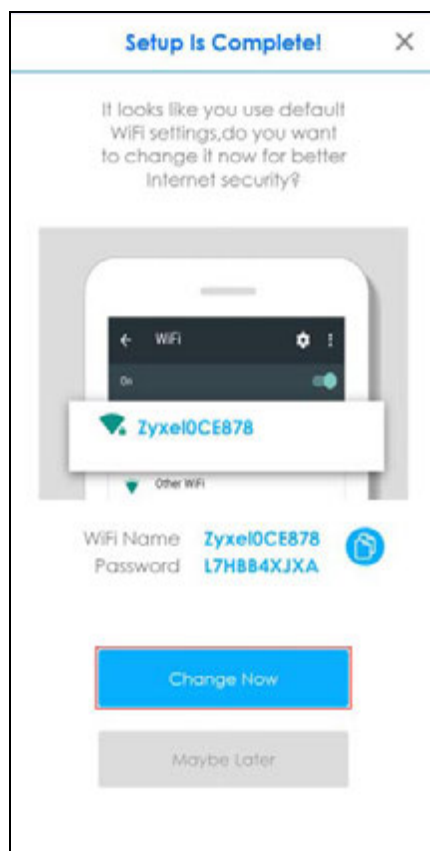
- 12** Press the **WPS** button on your other Multy Device within range of the first Multy Device within 120 seconds. The LED blinks pink on your other Multy Device while it sets up a WPS connection with the first Multy Device. Then tap **Next**.



- 13 The **Your Multy Site is Ready!** screen appears, and then tap **Next**.
Tap **Add Multy** if you wish to add another Multy Device.
Alternatively, tap **No, I'm done**.



- 14 The Multy app detects you are using the default **WiFi name** and **Password**. Tap the copy (📋) icon to copy the WiFi **Password**. Click **Change now** to change your WiFi name and password. Otherwise, click **Maybe Later** to change your WiFi name and password later.



- 15 Tap **Smart Connect with 2.4G/5G/6G name the same** to keep 2.4G, 5G and 6G name the same. Tap **Save** to save the changes. Keeping the 2.4G, 5G and 6G names the same allows you to steer seamlessly between the three WiFi networks.

<

WiFi Settings

Save

WiFi

2.4G WiFi Name

Zyxel0CE878

5G WiFi Name

Zyxel0CE878

6G WiFi Name

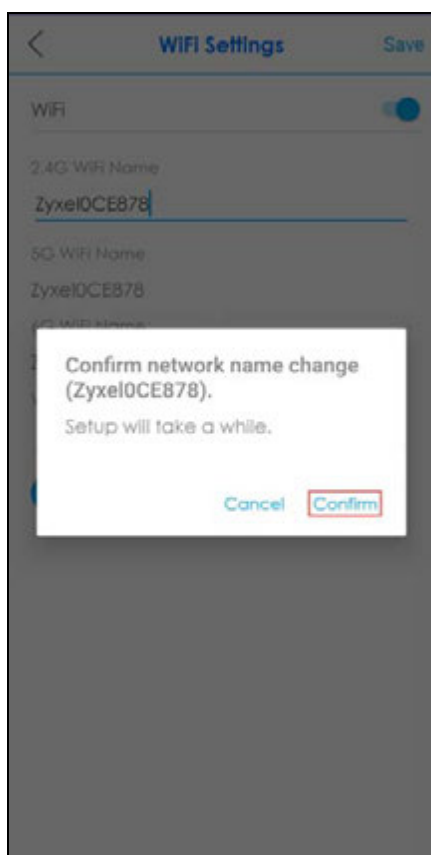
Zyxel0CE878

WiFi Password

••••••••

Smart Connect with 2.4G/5G/6G name the same

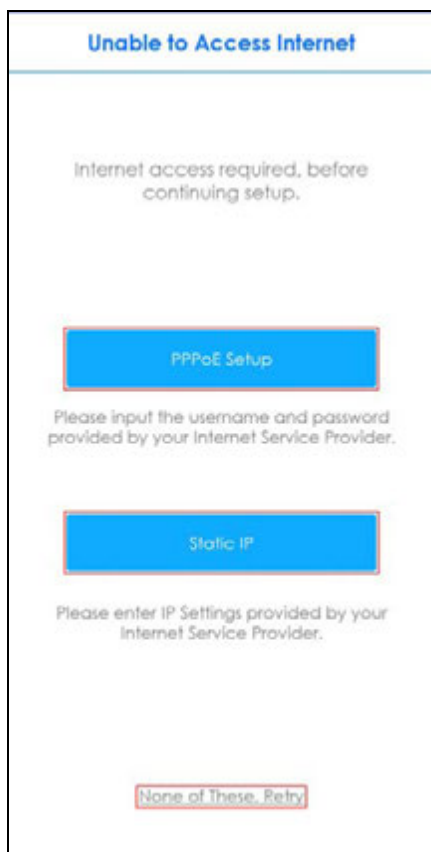
- 16 Tap **Confirm** to continue and update your WiFi settings.



- 17 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 WiFi 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.



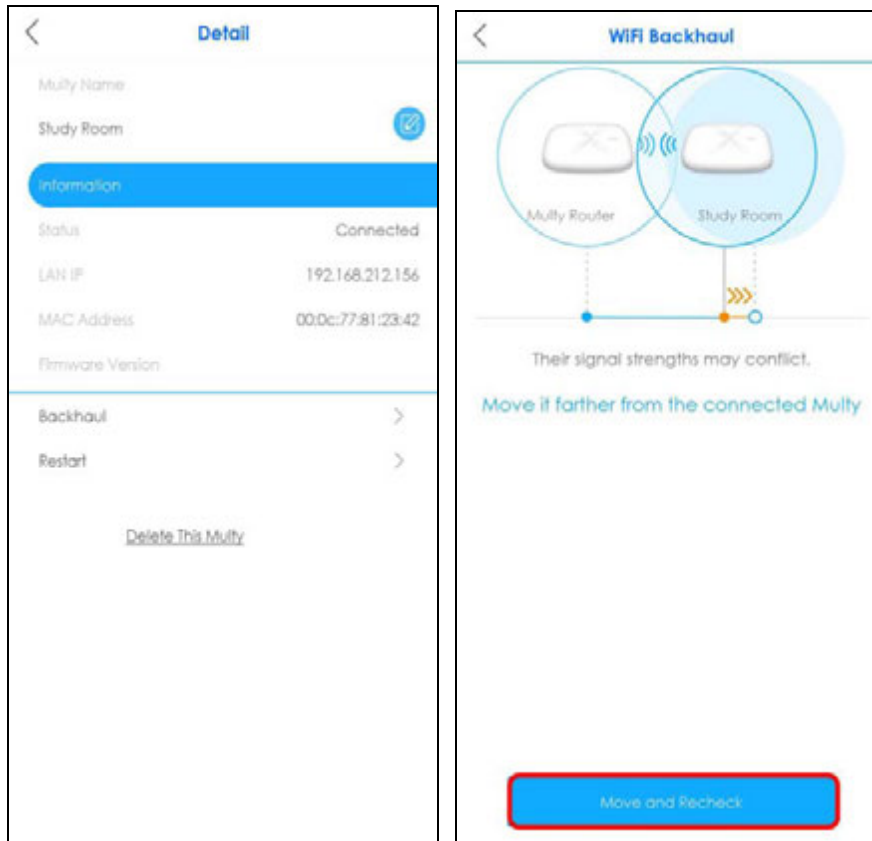
3.4 Check Your Multy-to-Multy Signal Strength

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.



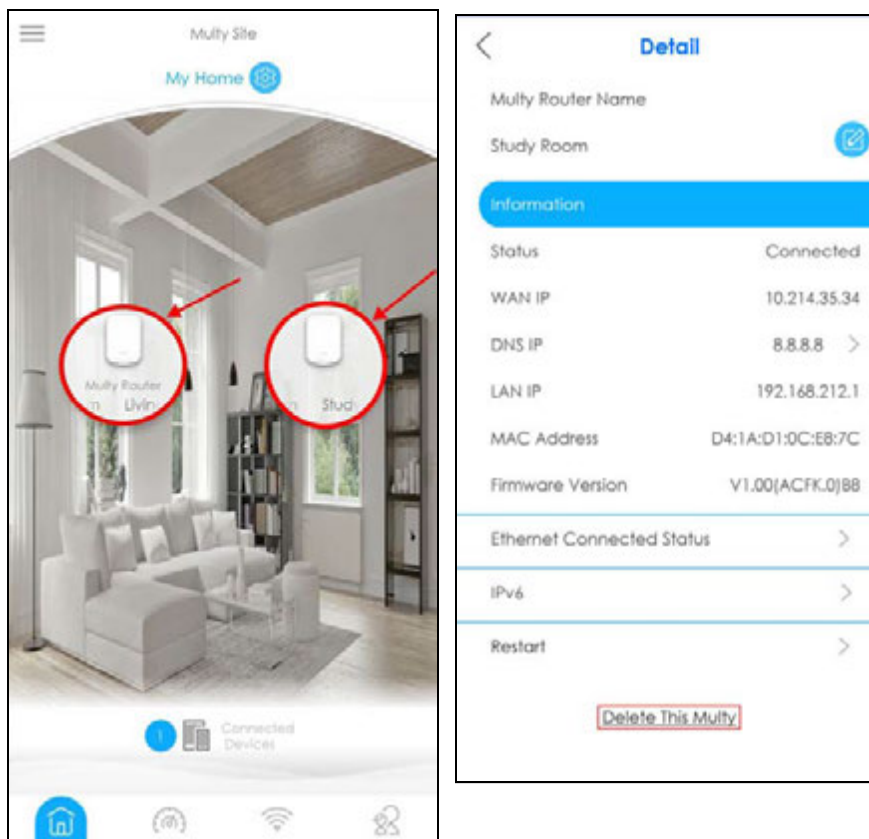
3.5 Remove a Multy Device

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 Multy Device.

Note: Before pressing the **RESET** button on the Multy Device, click **Delete This 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.



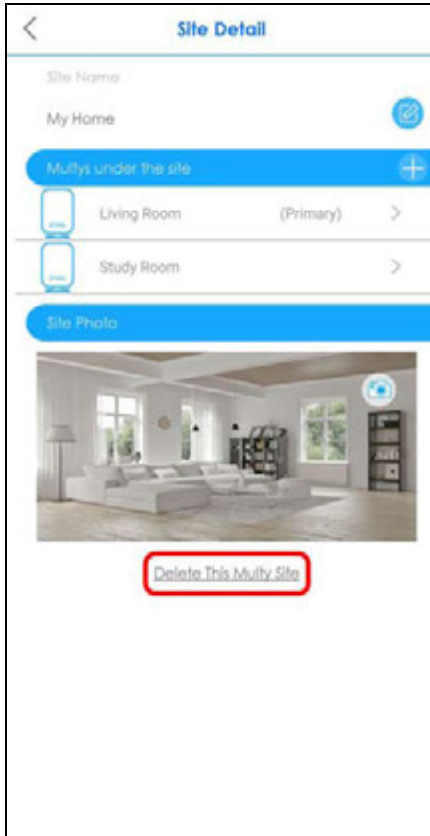
3.6 Remove a Multy Site

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.

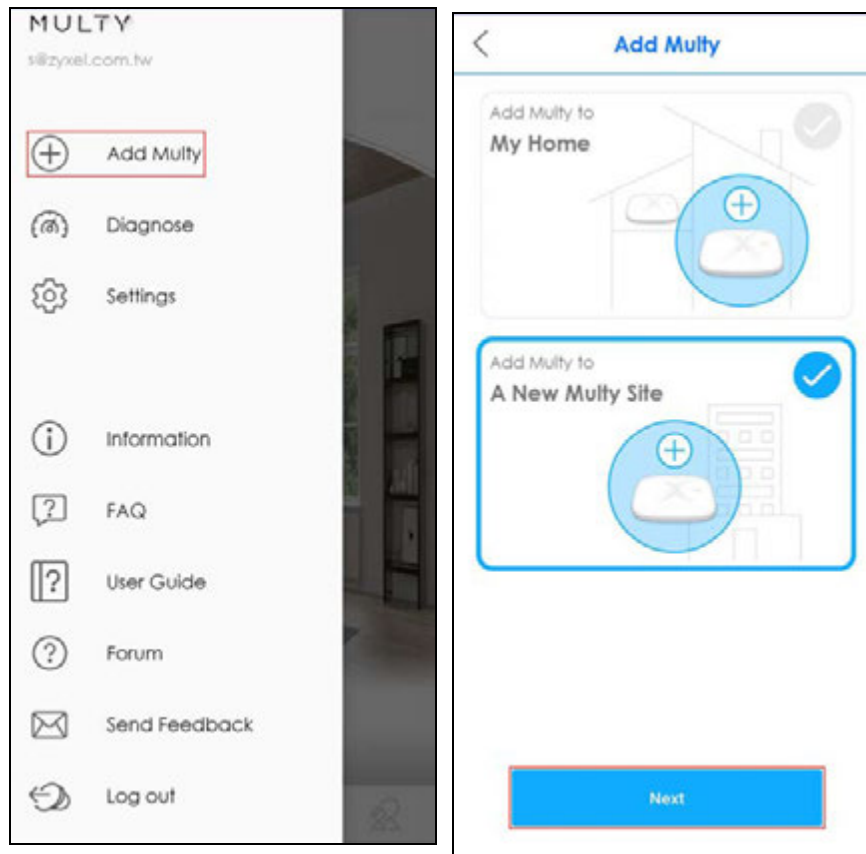


- 2 Tap **Delete This Multy Site** to remove the Multy WiFi System.

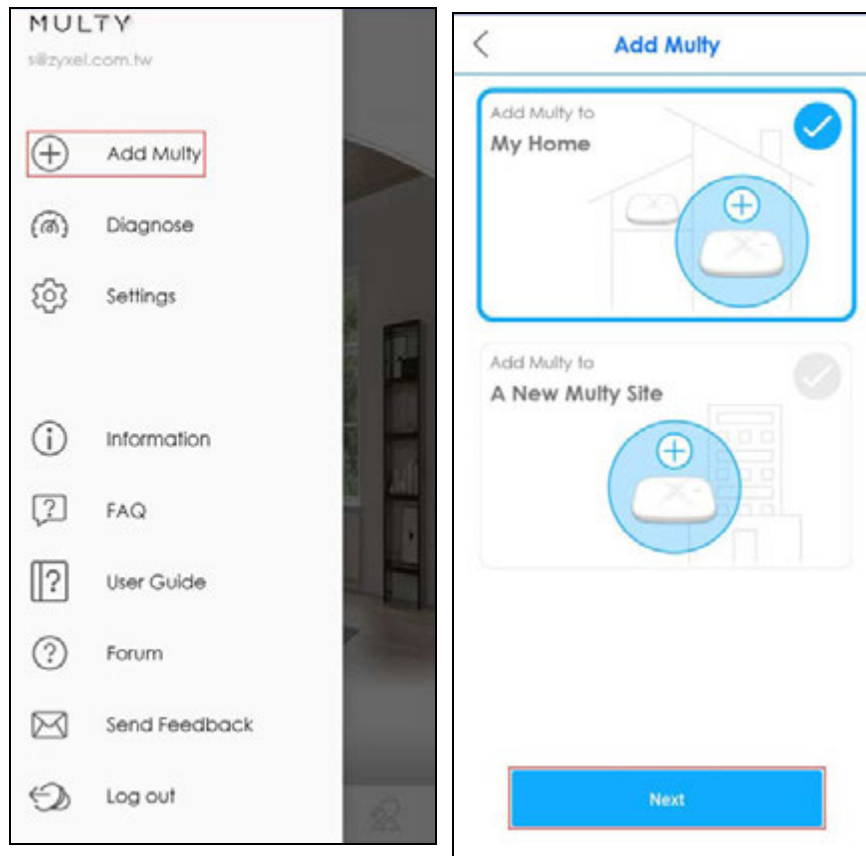


3.7 Add a Multy Device to a New Site

- 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 44](#) 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.



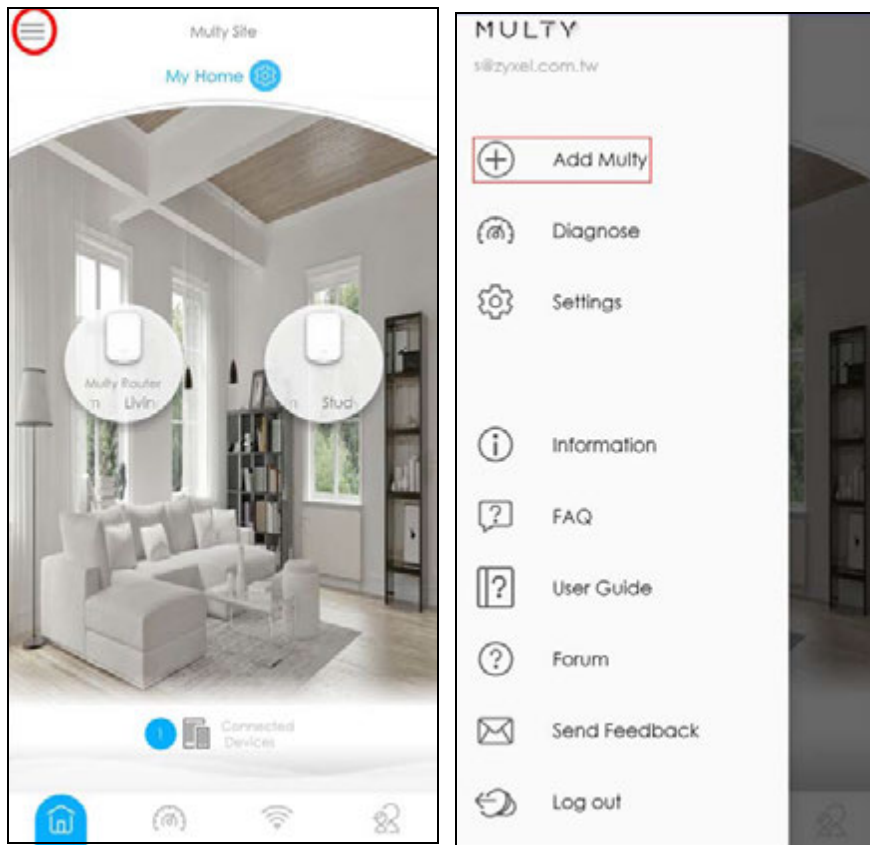
3.8 Install a Second Multy Site

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.

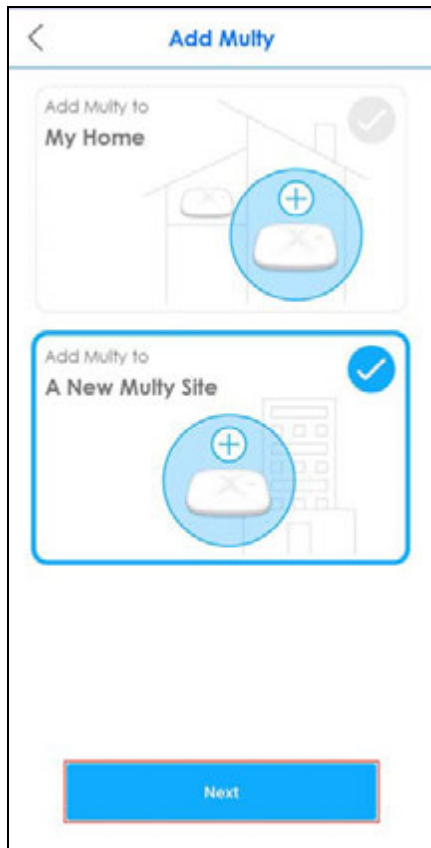
Figure 40 Multy Sites



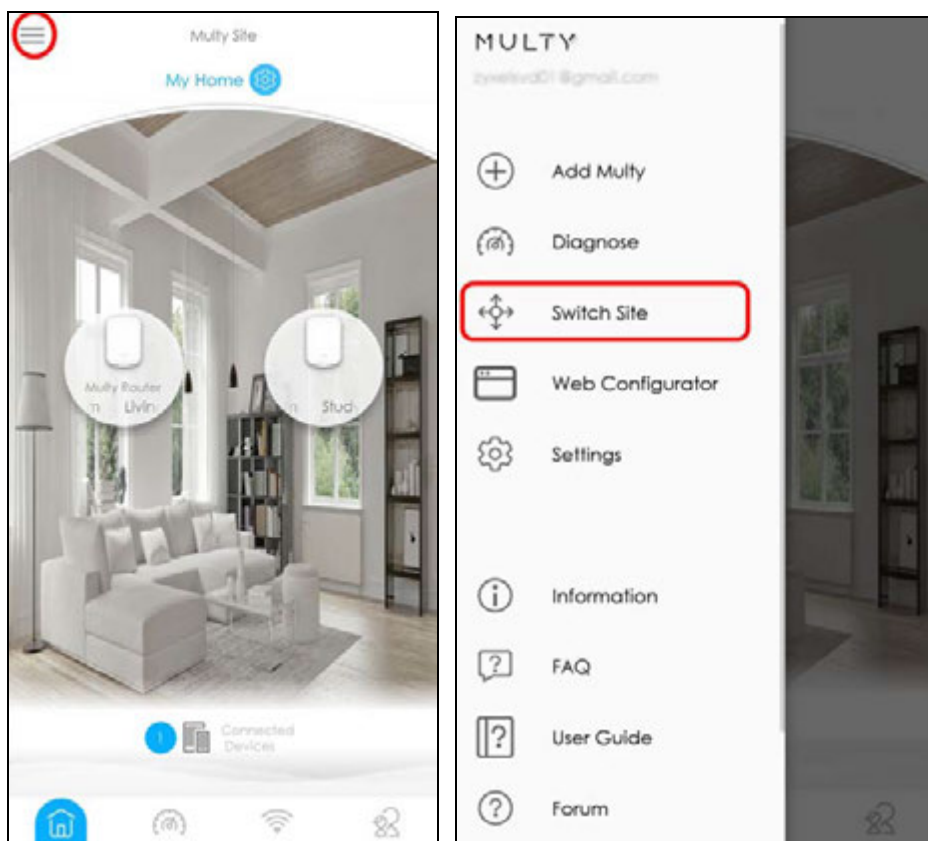
- 1 Tap the Menu icon in the upper-left to open the navigation panel. Tap **Add Multy**.



- 2 Tap **A New Multy Site** and **Next** to set up another Multy WiFi System. Follow the instructions in [Section 3.3 on page 44](#) to complete the setup.

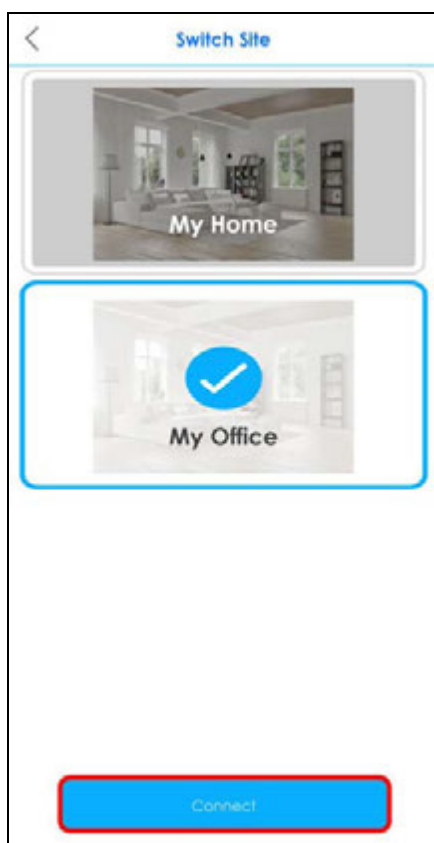


- 3 To manage a different Multy Site, first tap **Switch Site** from the navigation panel.



- 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.



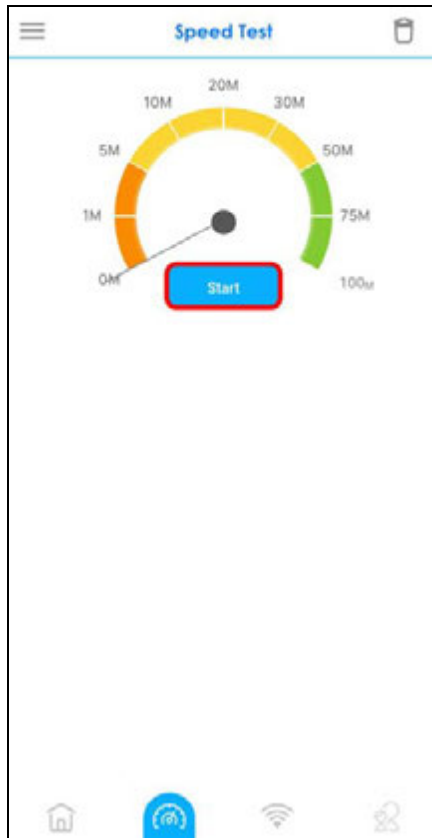
3.9 Test Your Smartphone Connection Speed

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

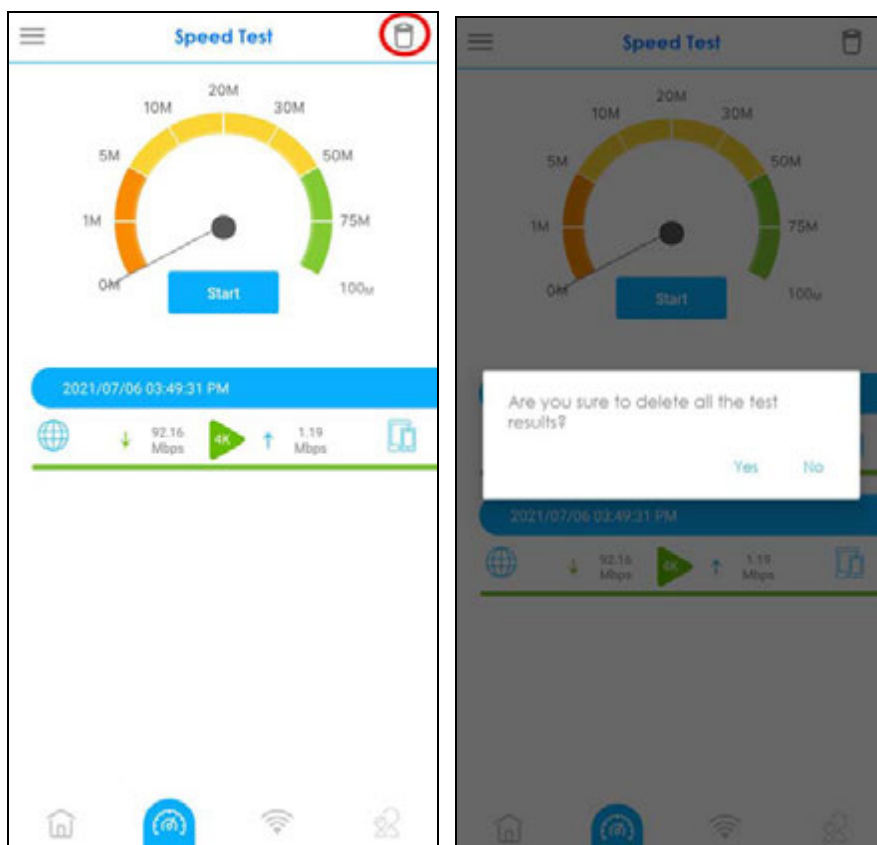
- 1 Tap the Speed Test icon (📶) of the Multy Site.



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



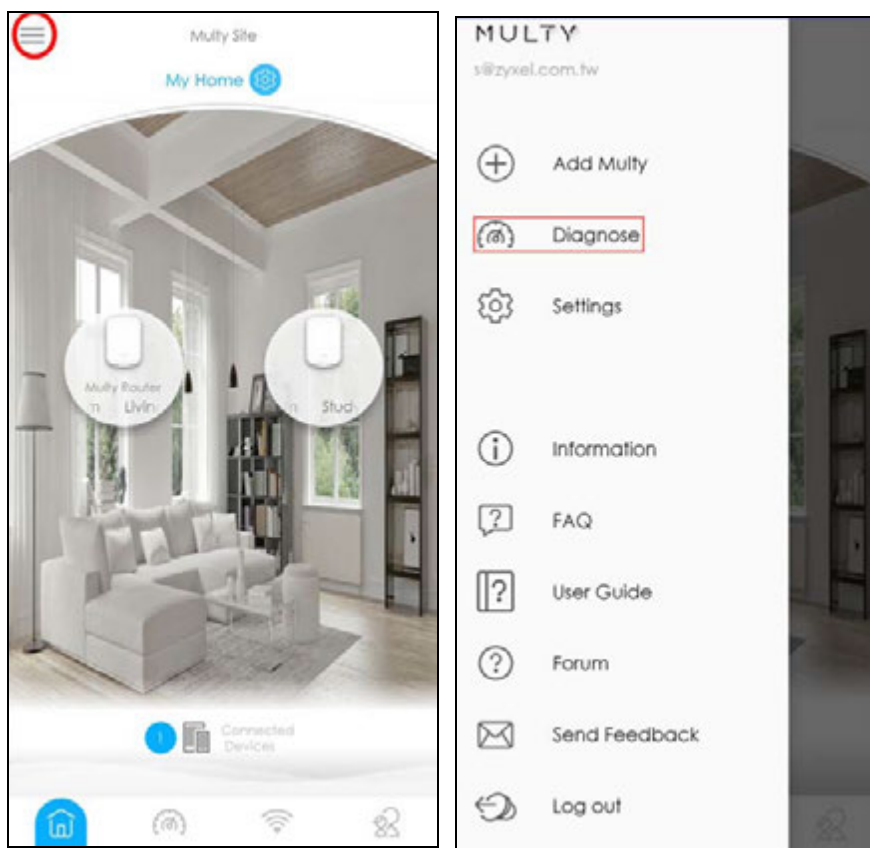
- 3 The following screens show the results. You can tap the Remove icon () to delete all records.



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.

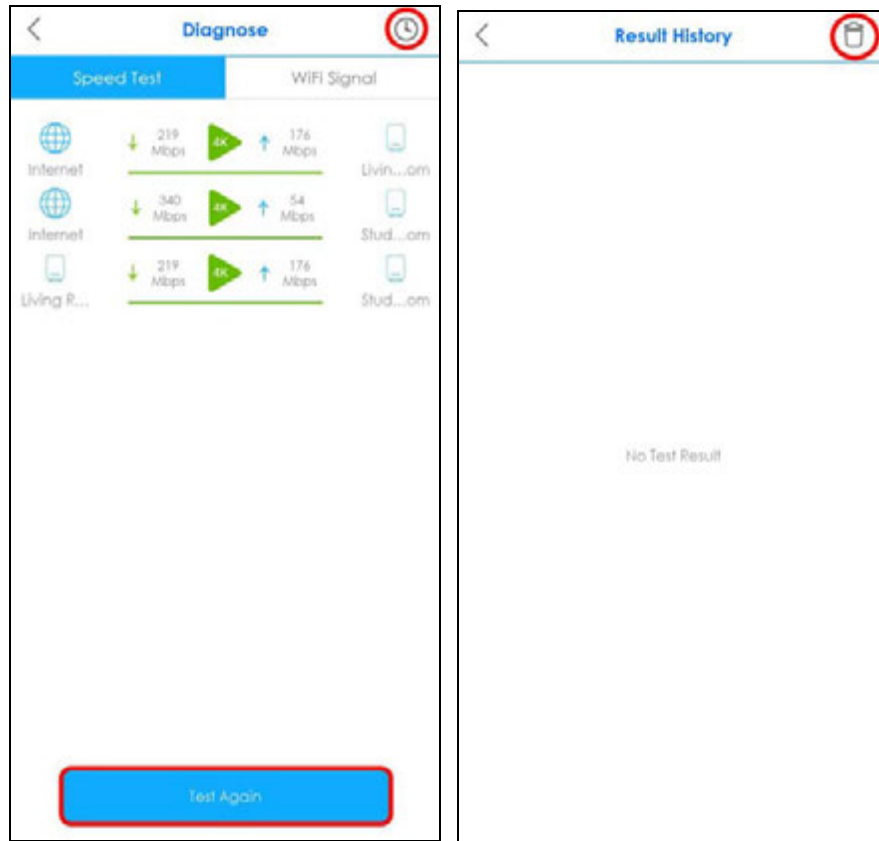
- 1 Tap the Menu icon in the upper-left to open the navigation panel. Tap **Diagnose**.



- 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.



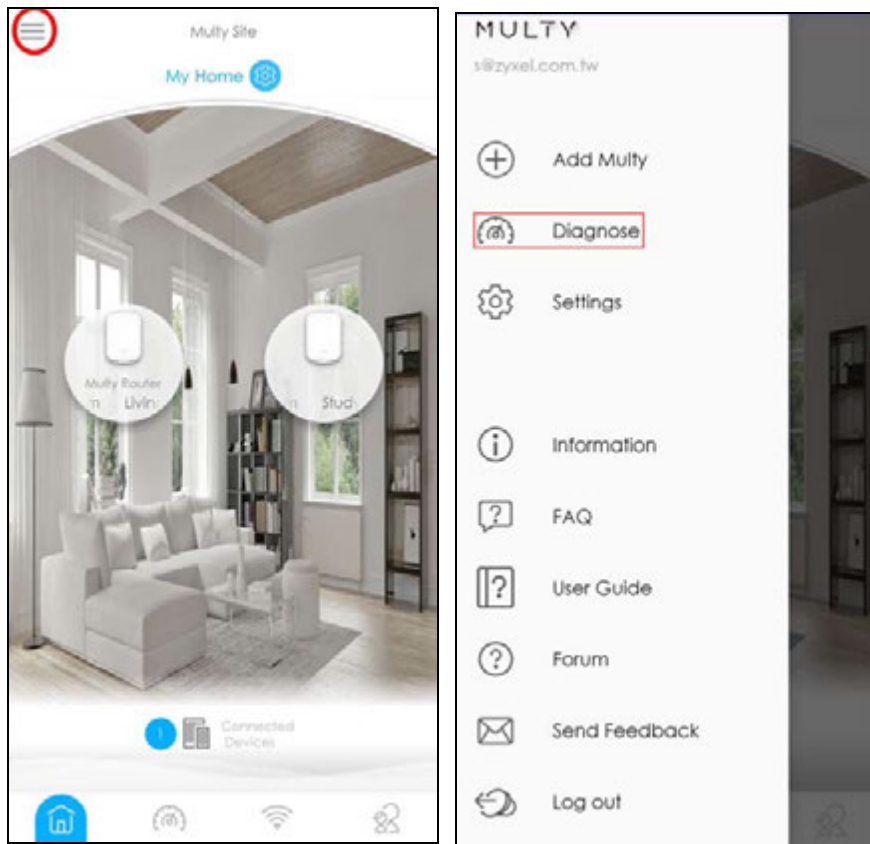
- 3 Tap **Test Again** to show the **Test** buttons. To view the previous test results, tap the History icon (🕒). You can tap the Remove icon (🗑️) to delete all records.



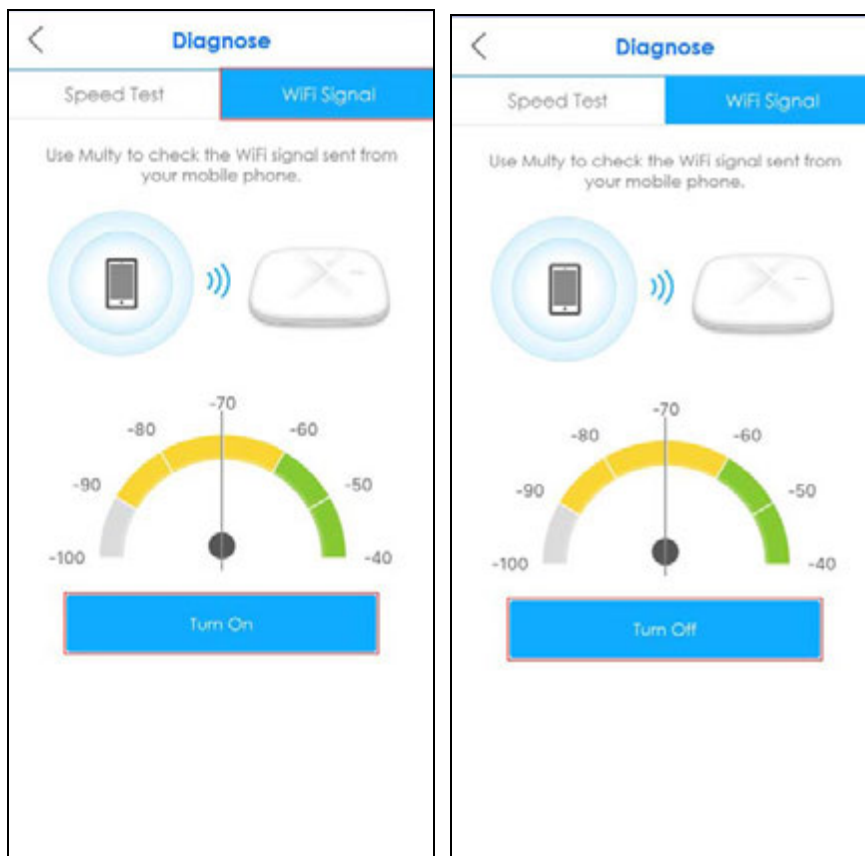
3.11 Measure Your WiFi Signal Strength

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**.



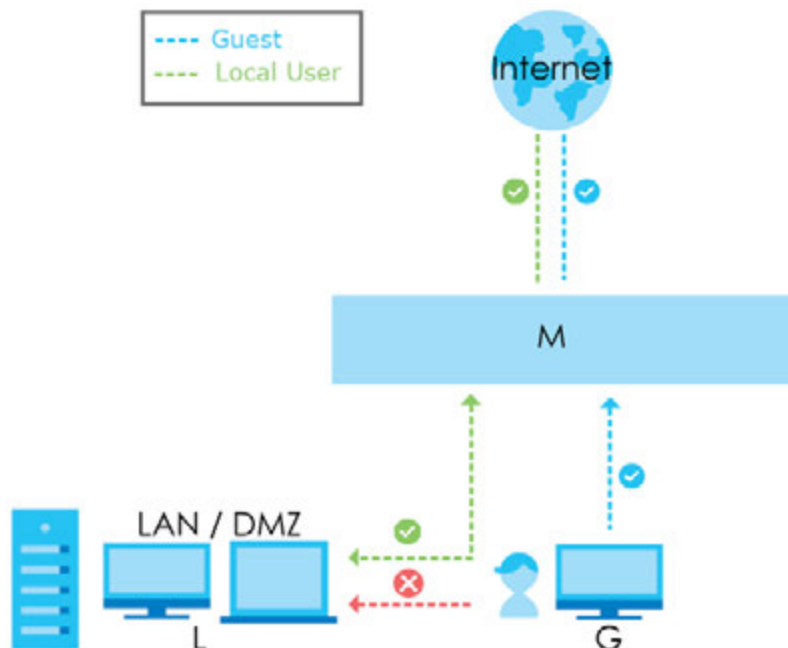
- 2 Tap **WiFi Signal** and then tap the **Turn On** button to perform a check. Tap **Turn Off** to stop the process. A decent WiFi signal would not go below -70 dBm (-70 dBm to -100 dBm).



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.

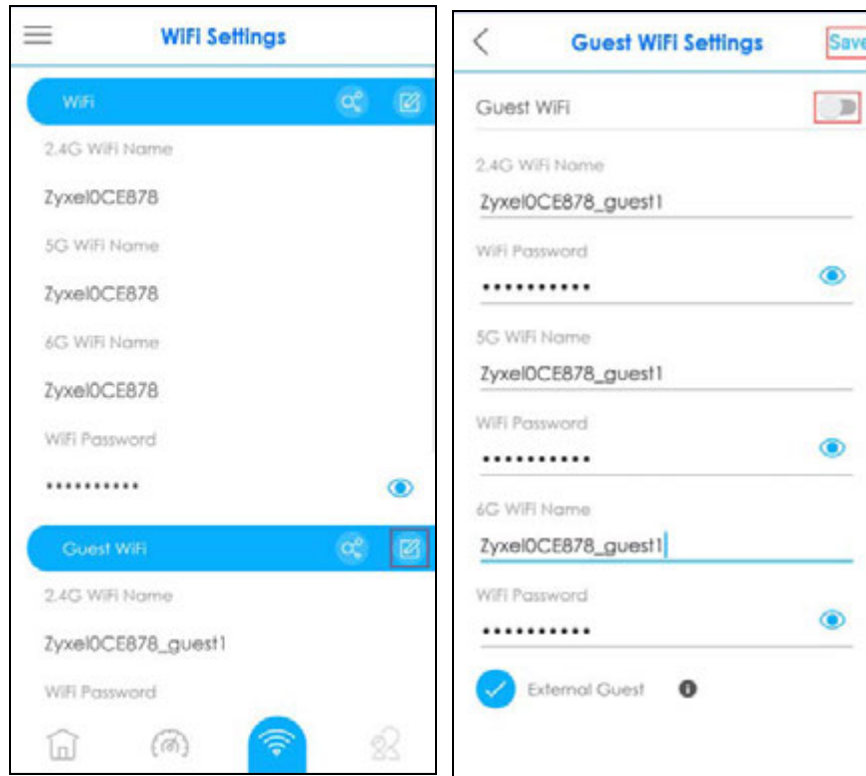
The client device (**G**) connected to the guest WiFi (**Guest**) can access the Internet but they cannot access other client devices (**L**) connected to the Multy Site (**M**), as shown in the next figure.

Figure 41 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

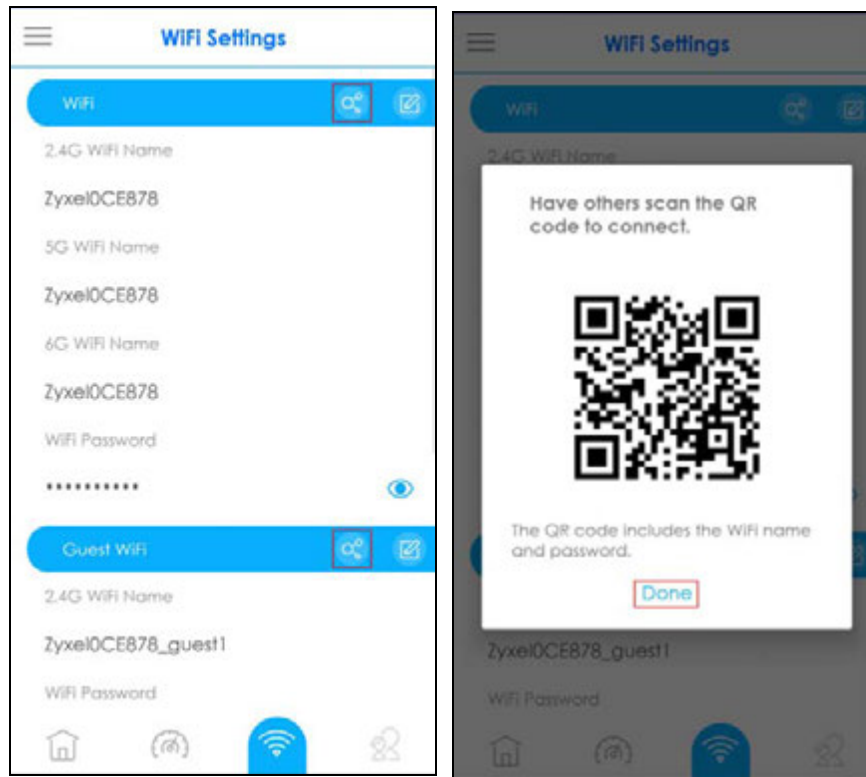
Use the app to create a QR code with your WiFi network name and password. By printing and placing the QR code somewhere accessible, you can let your friends or guests scan the QR code and join the WiFi network directly without revealing your actual WiFi password.

- 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

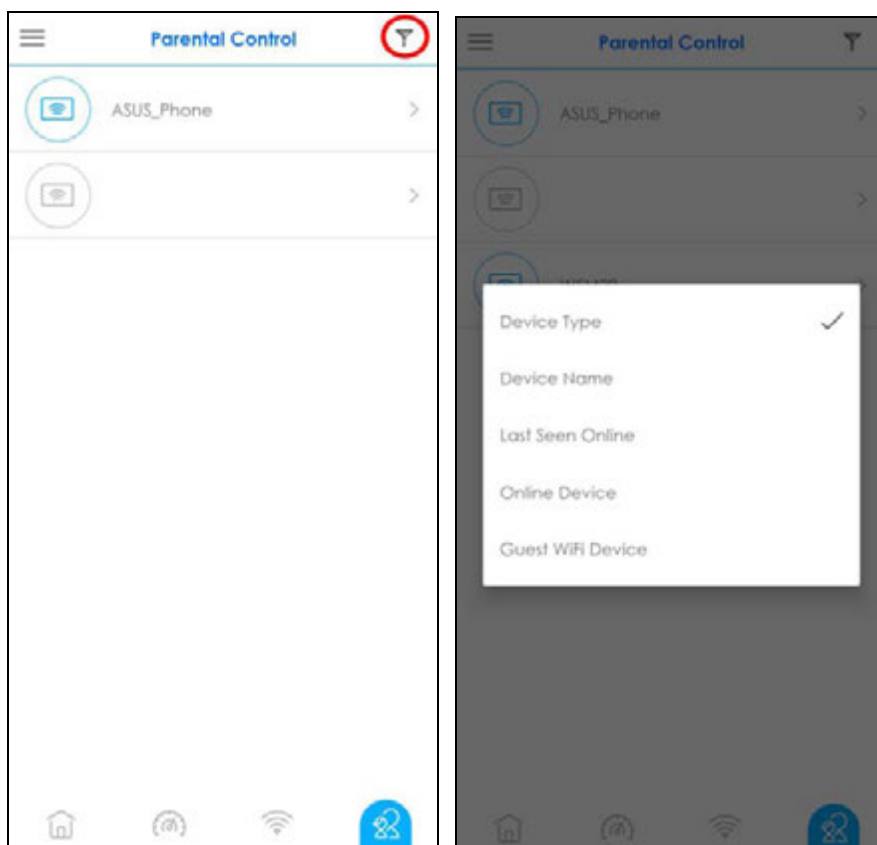
By creating a schedule profile, you can schedule the Multy Site to automatically disable the WiFi access of selected clients for preset periods of time.

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.

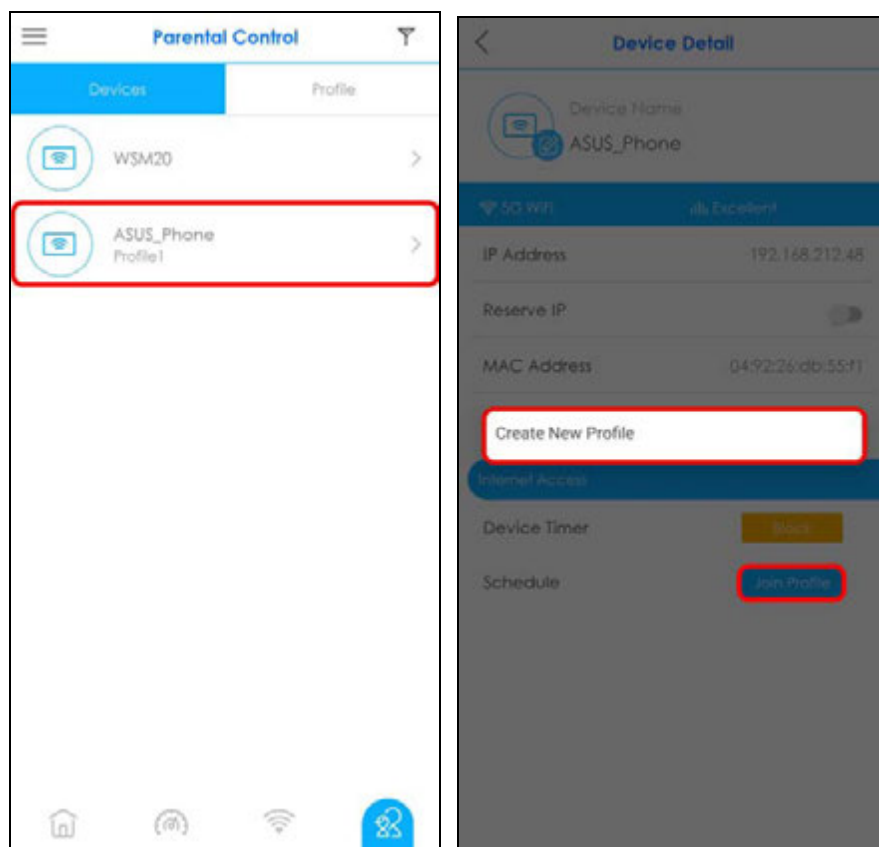
- 1 Tap the Parental Control icon () of the Multy Site.



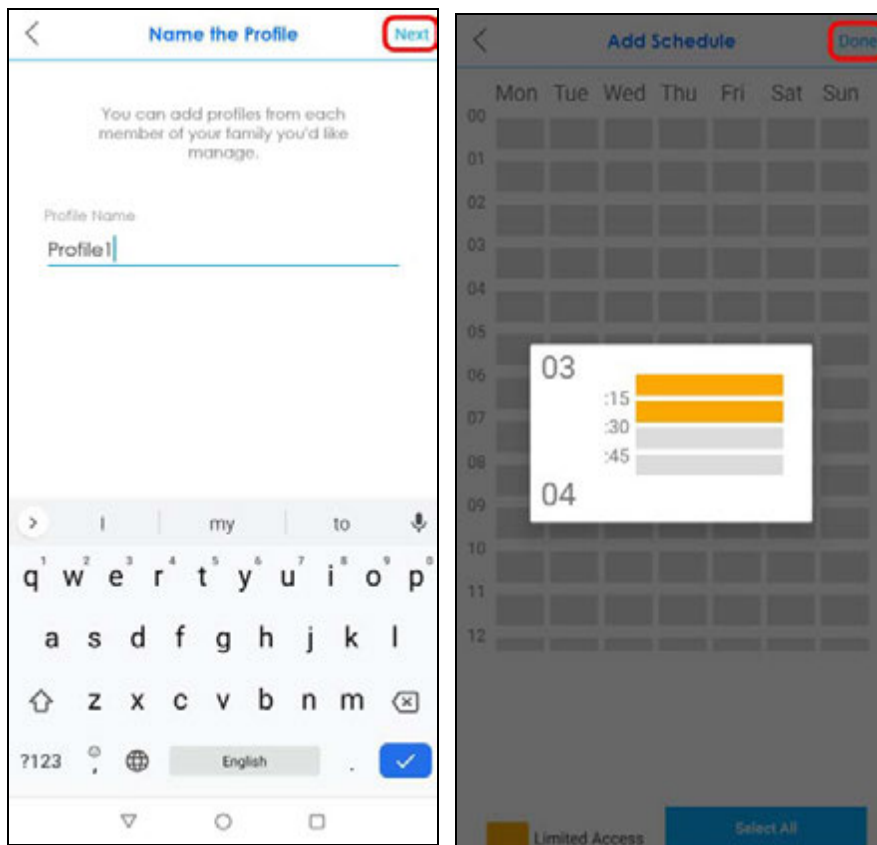
- 2 Tap the Filter icon and select how you want to sort the devices in the list.



- 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.

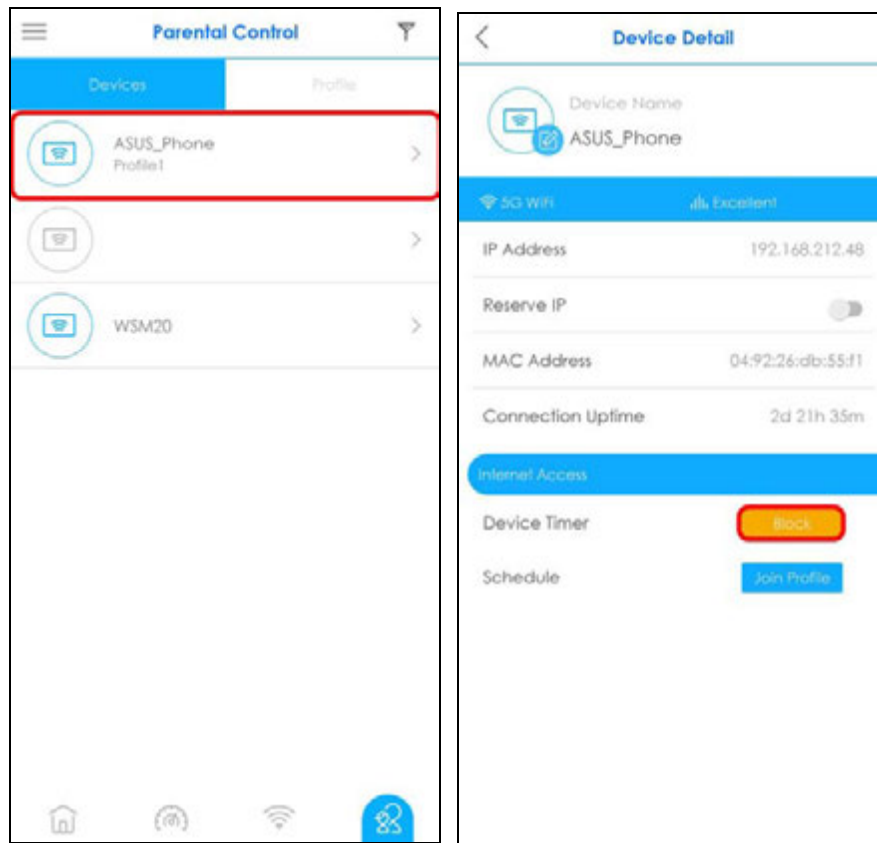


- 4 If you want to create a new schedule, tap **Create New Profile** shown in the previous step. After you create a profile, name the profile, and then tap **Next**. Tap the gray blocks to specify the time periods during which the client will be blocked from accessing the Internet. If you want to plan 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.

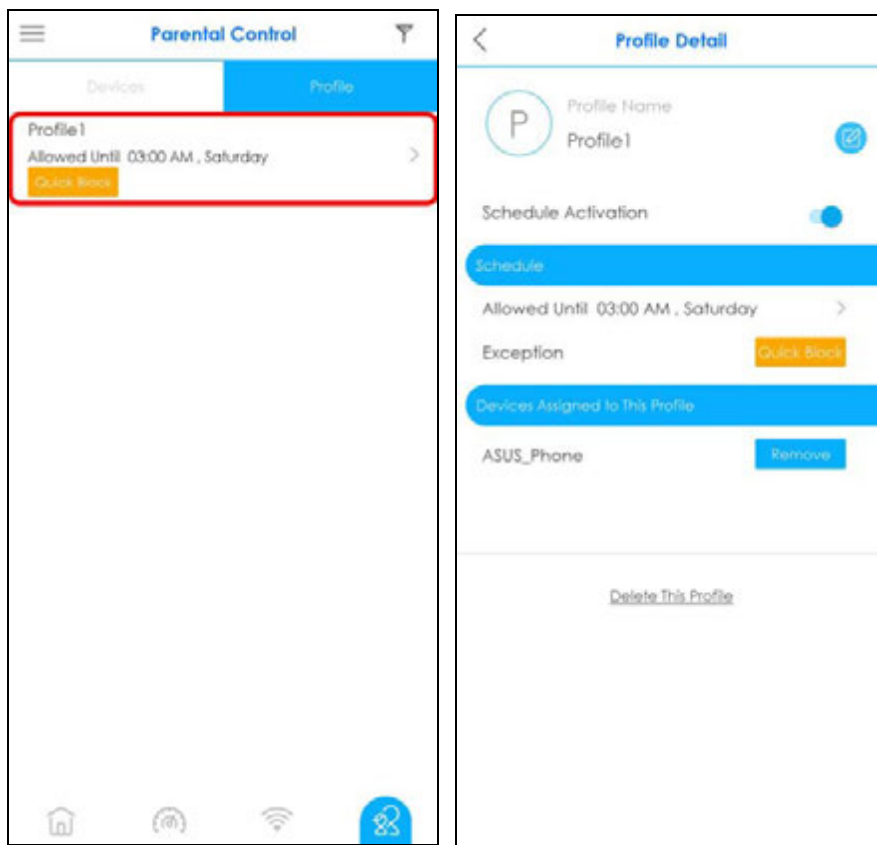


- 5 The applied profile name will then display on the **Parental Control > Devices** screen.

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

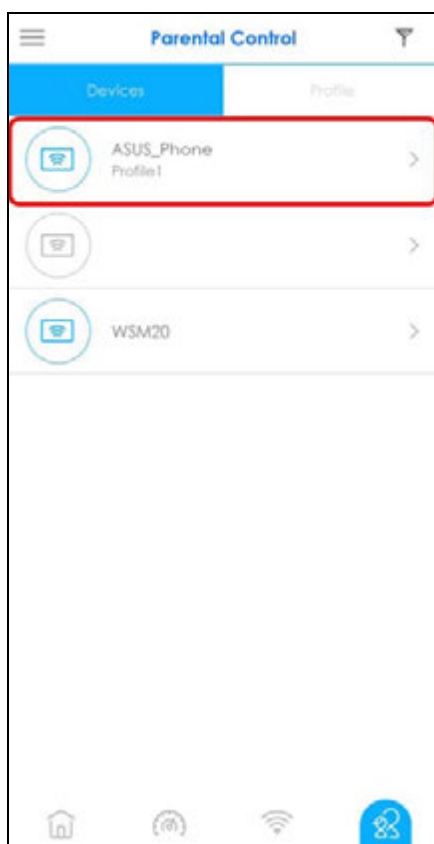
You can set a timer to block a specific client from accessing the Internet without having to create a schedule. The timer is effective only once.

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

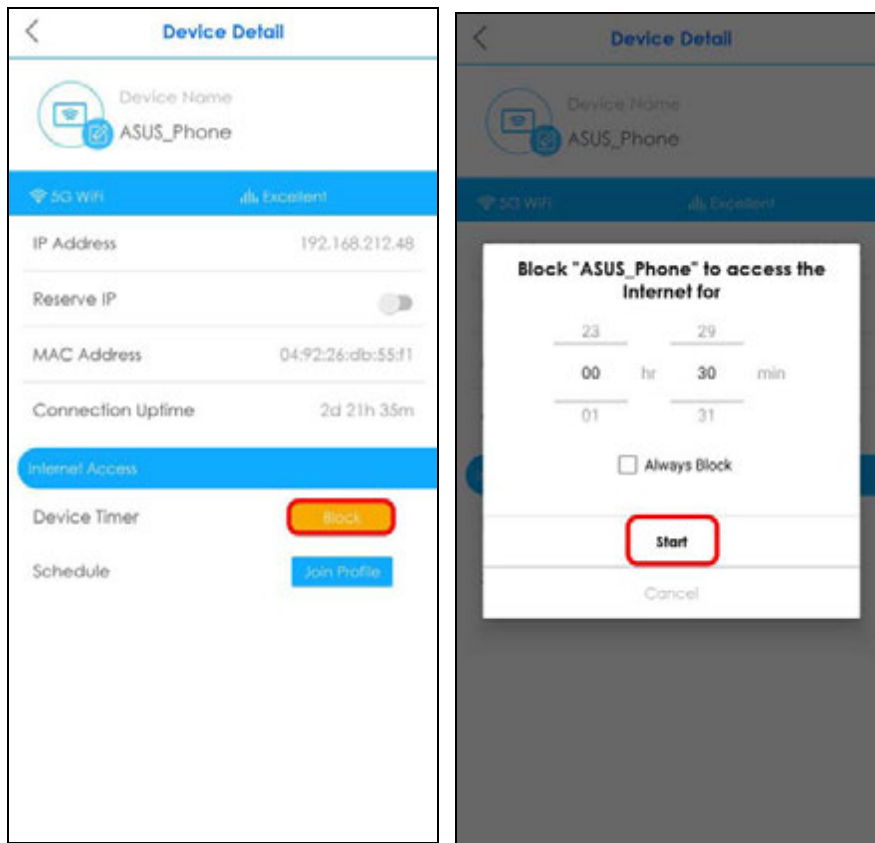
- 1 Tap the Parental Control icon () of the Multy Site.



- 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.

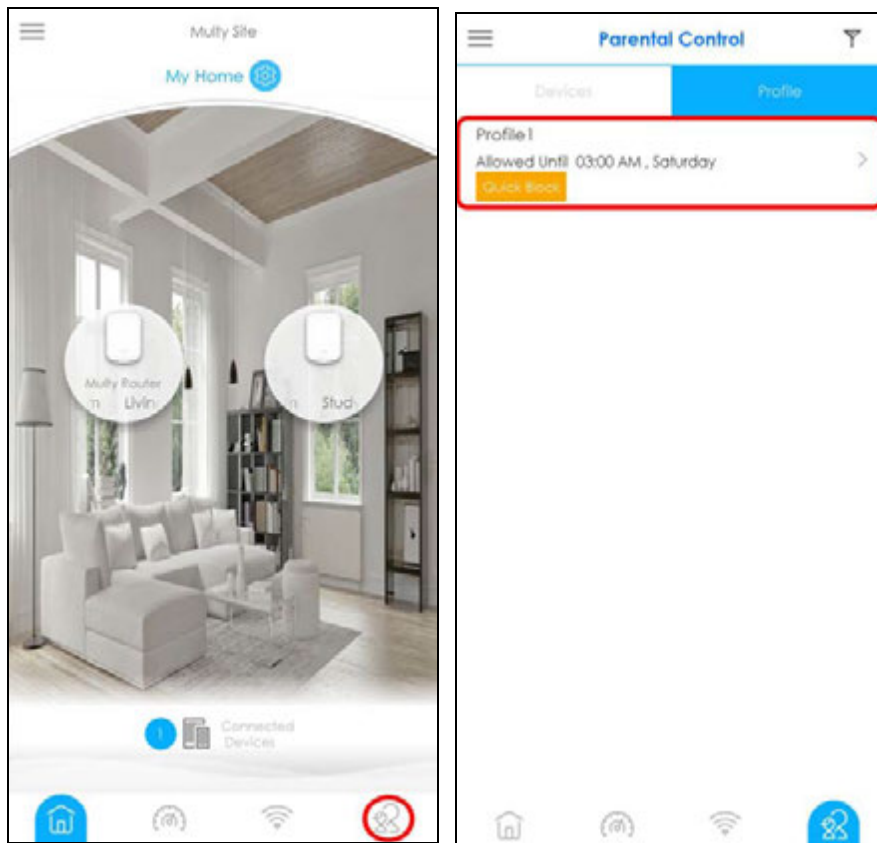


3.16 Pause or Resume Internet Access for a Group

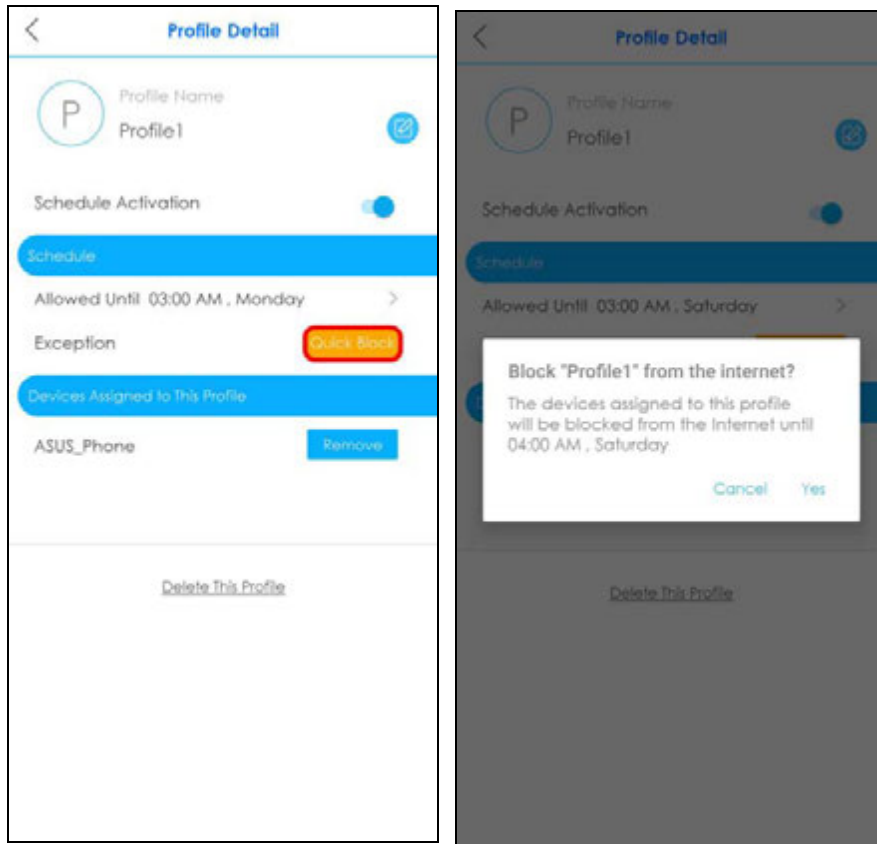
You may want to manually block a group of client devices from accessing the Internet immediately and resume it later.

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 immediately.



- 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.



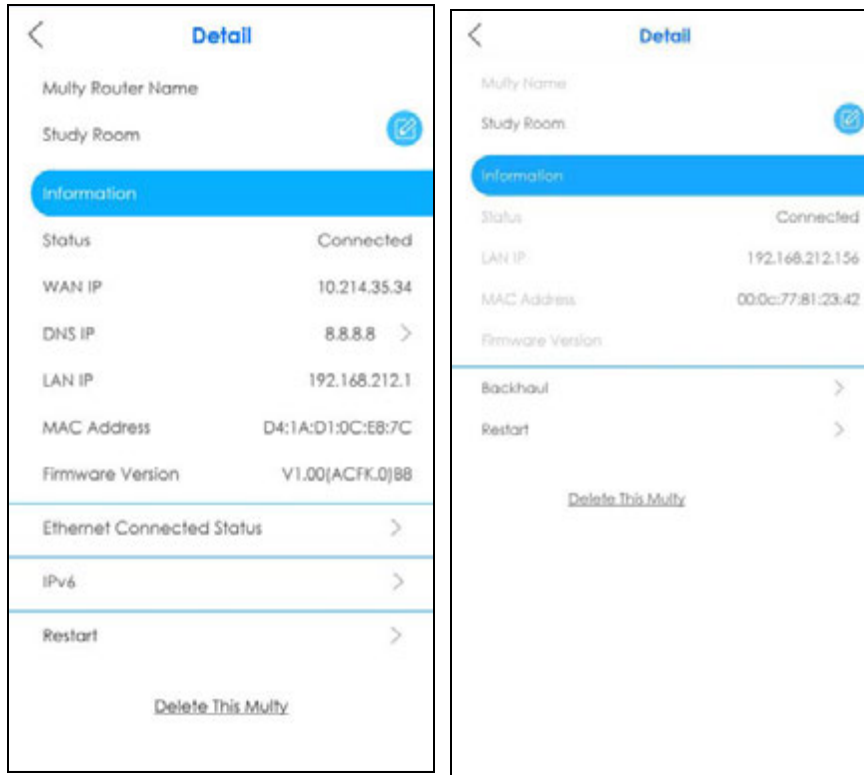
3.17 Check your Multy Device's Configuration Details

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.



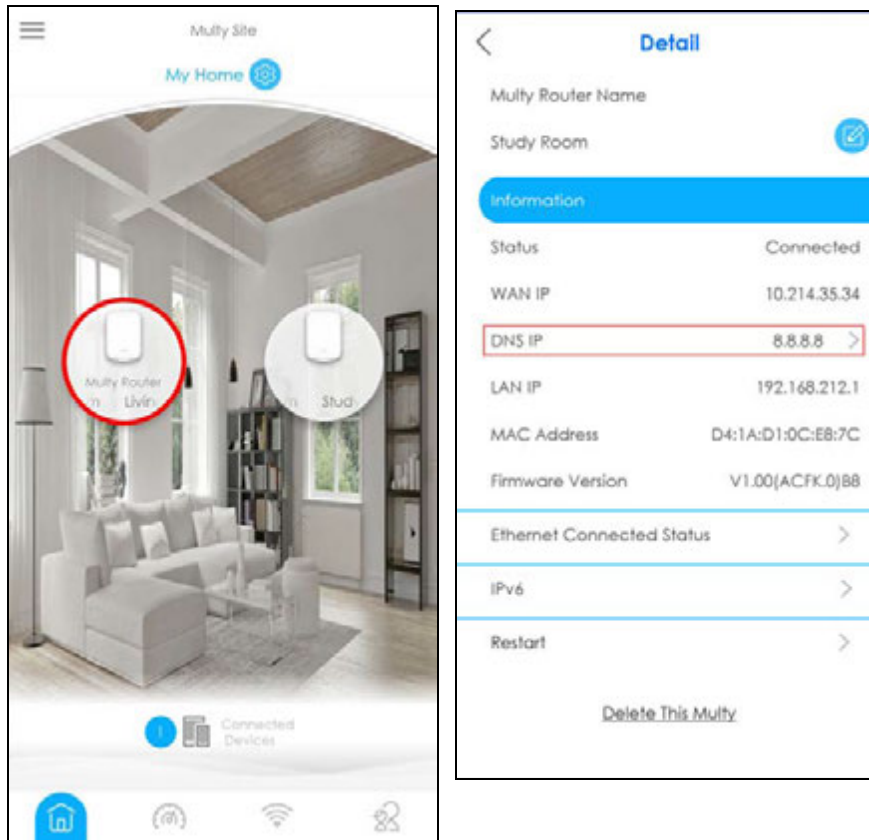
- 2 The figure on the left appears if you tap on the Multy Device acting as the primary Multy. The figure on the right appears if you tap on an extender Multy. You can configure the DNS IP address, the IPv6 address, and the Ethernet connection status on a primary Multy screen.



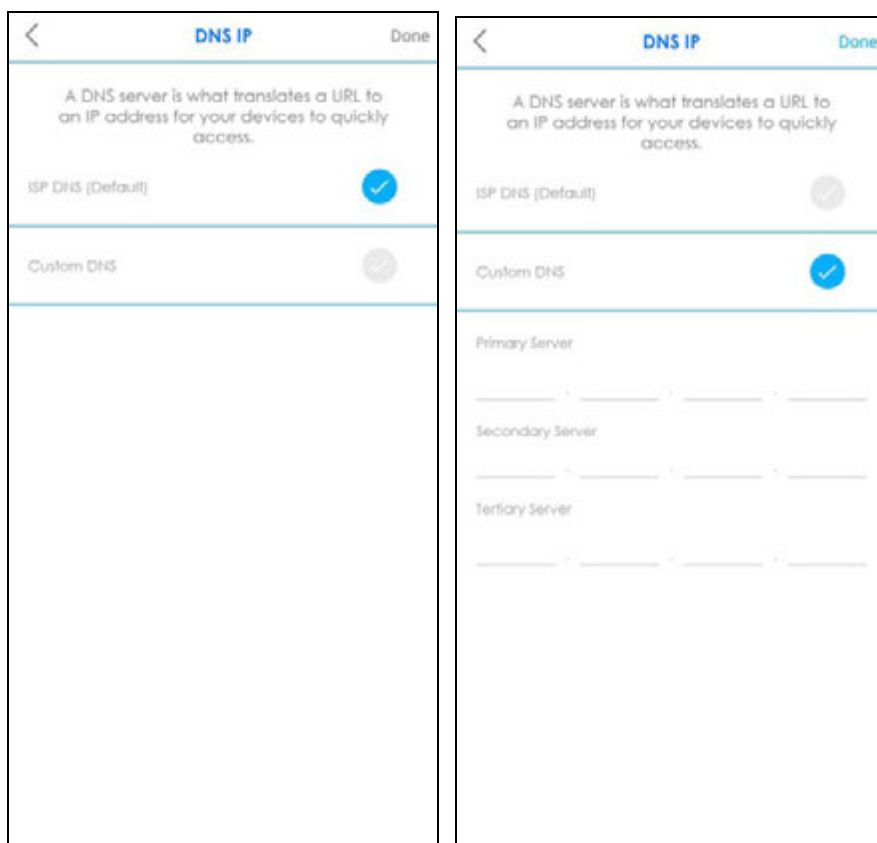
3.18 Use Custom DNS Server

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**.



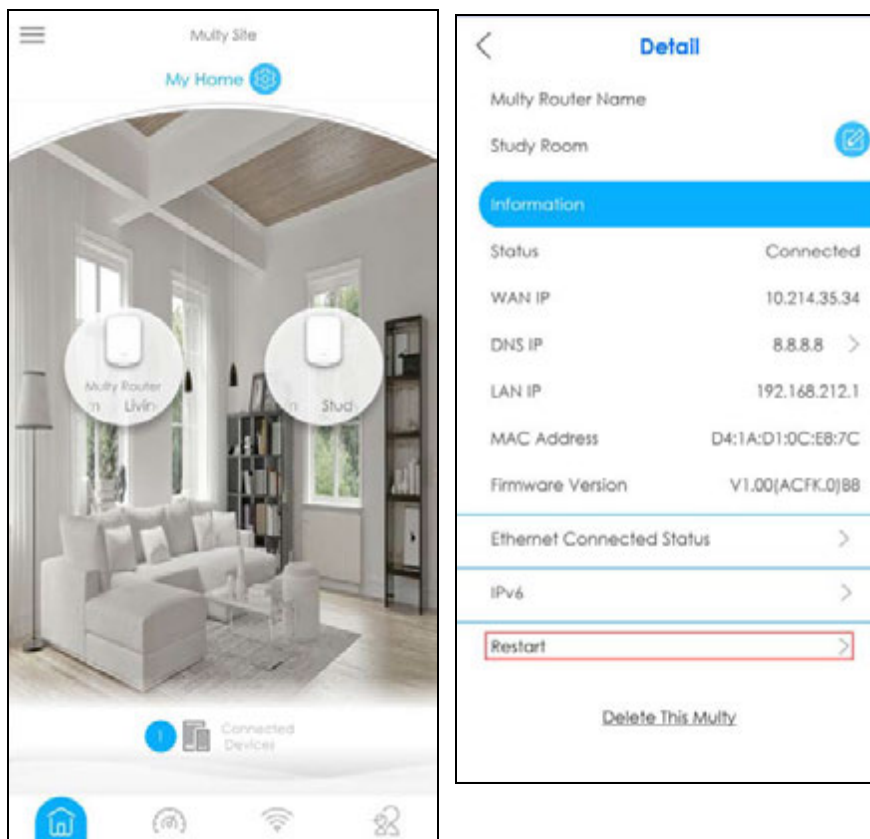
- 2 Tap **ISP DNS (Default)** to use the default DNS server. Otherwise, tap **Custom DNS** and enter a primary, secondary, and tertiary DNS server. Tap **Done** to apply the changes.



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.

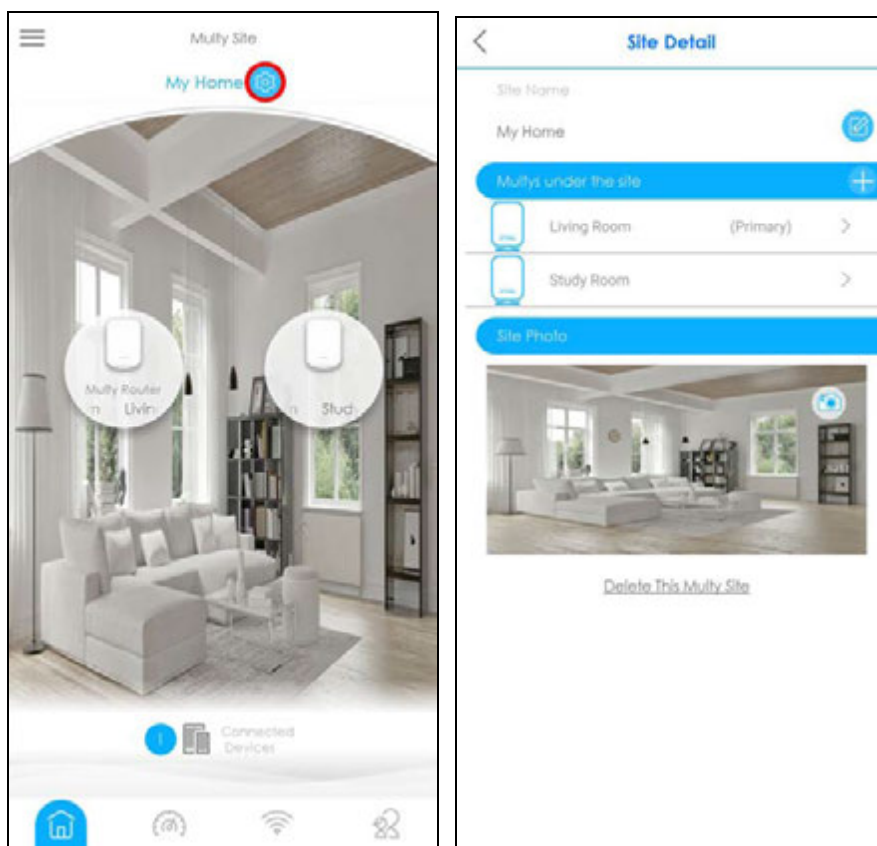


3.20 Change the Name or Picture of a Multy Site

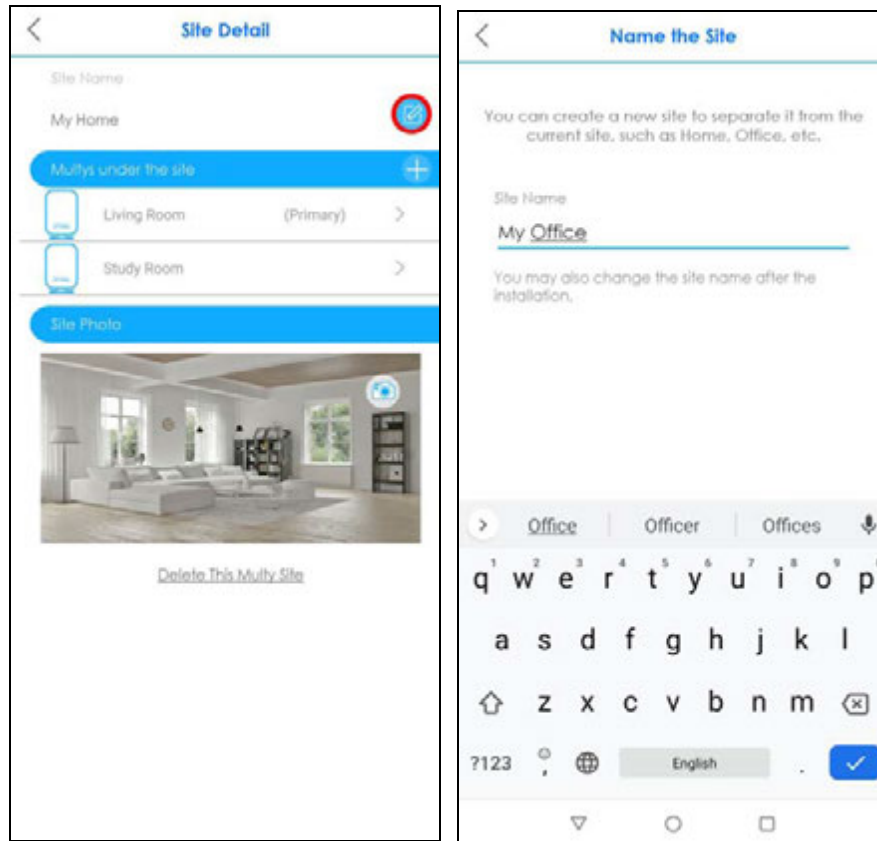
You can rename a Multy Site or change the background picture that is displayed on the Multy Site main screen by following these steps.

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 64](#) for more information.

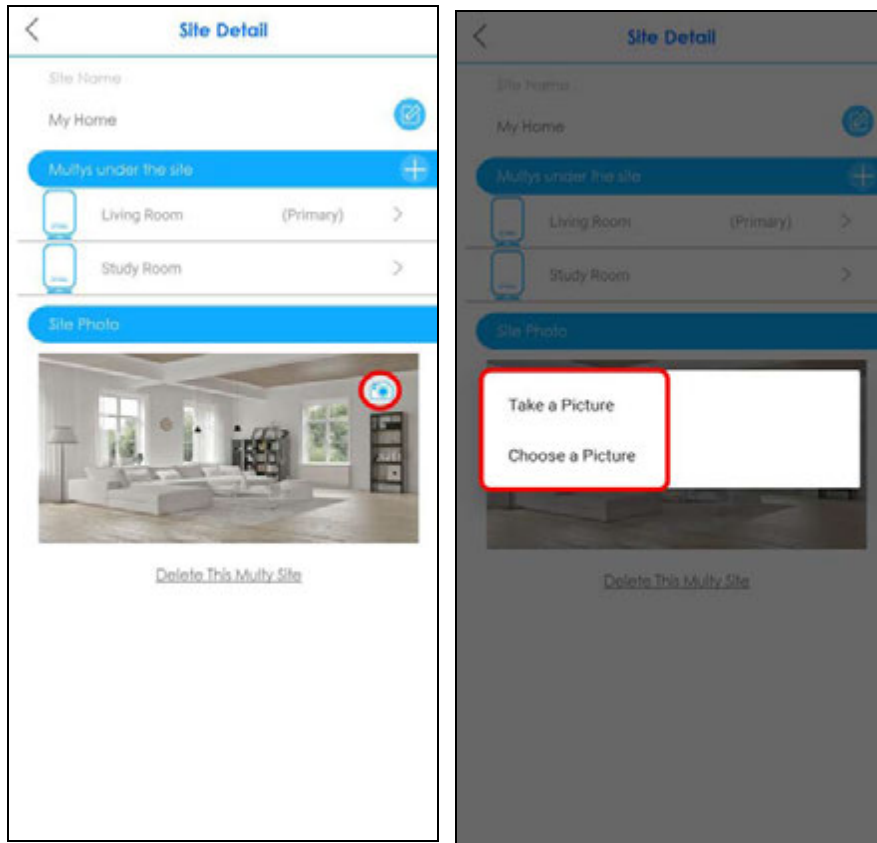
- 1 From the **Multy Site** screen, tap the Settings icon (⚙️) to open the **Site Detail** screen.



- 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 smartphone 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.

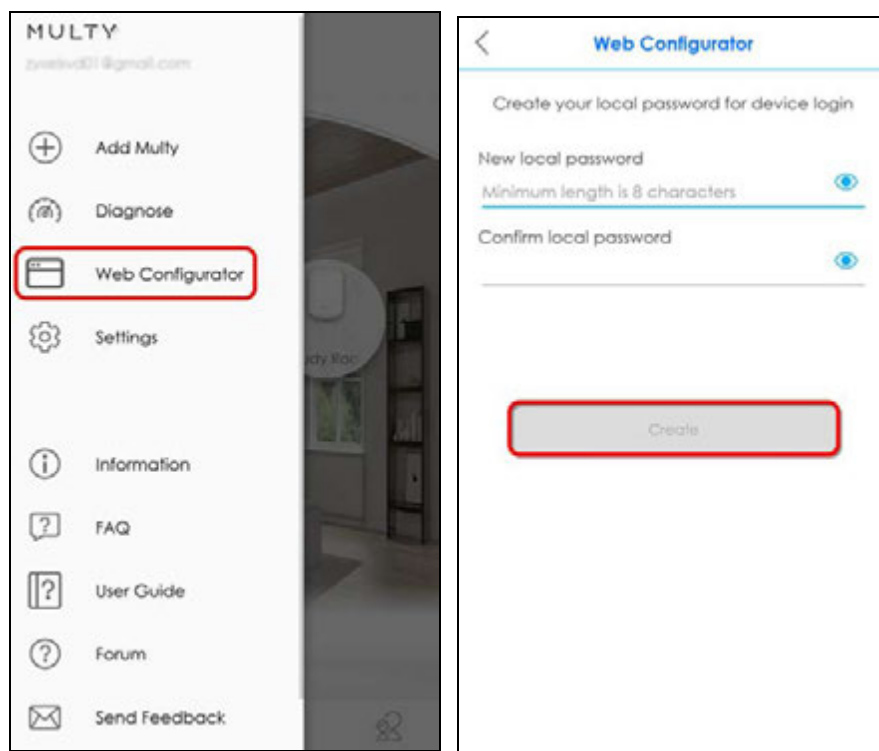


3.21 Create or Change Your Web Configurator Password

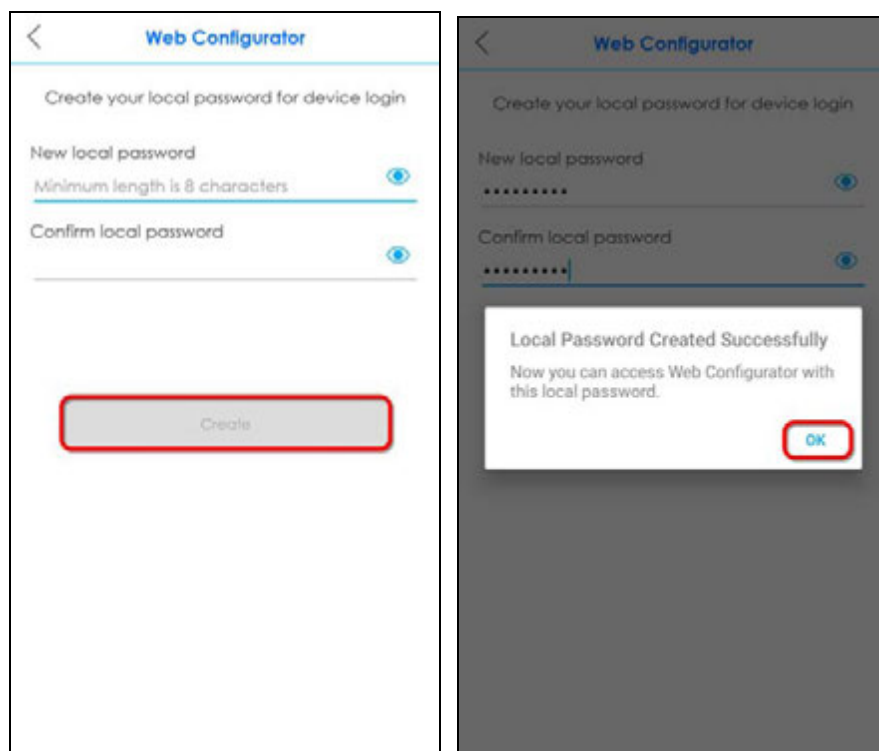
This section allows you to create or change your Web Configurator password through the Multy app.

- 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.

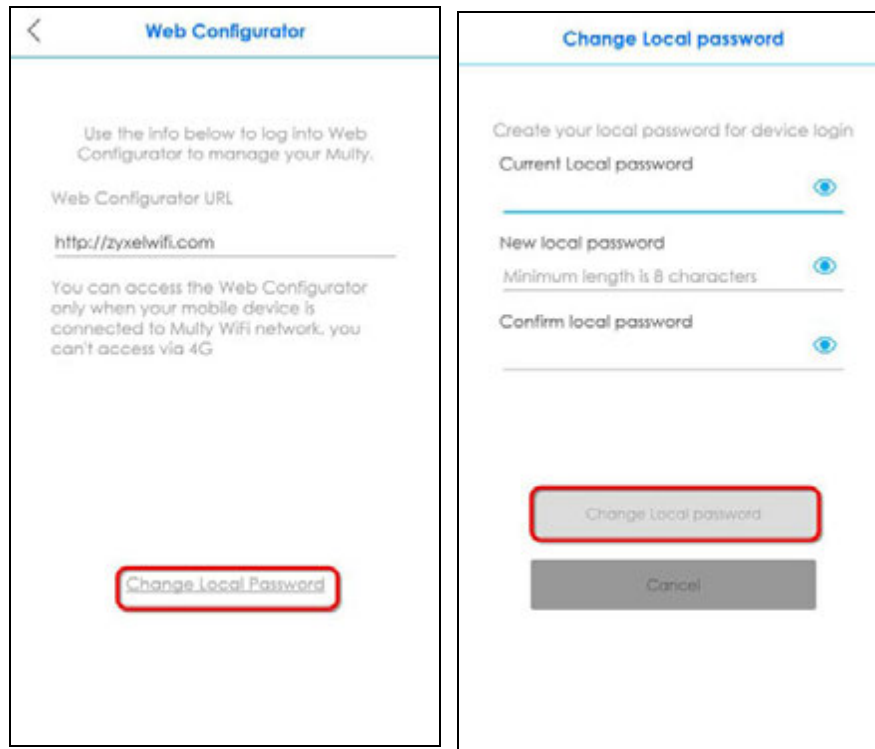
Note: Enter a new password of 8 – 32 alphanumeric characters. The following special characters listed in the square brackets [\ " ' < > ^ \$ &] and emojis are not allowed.



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



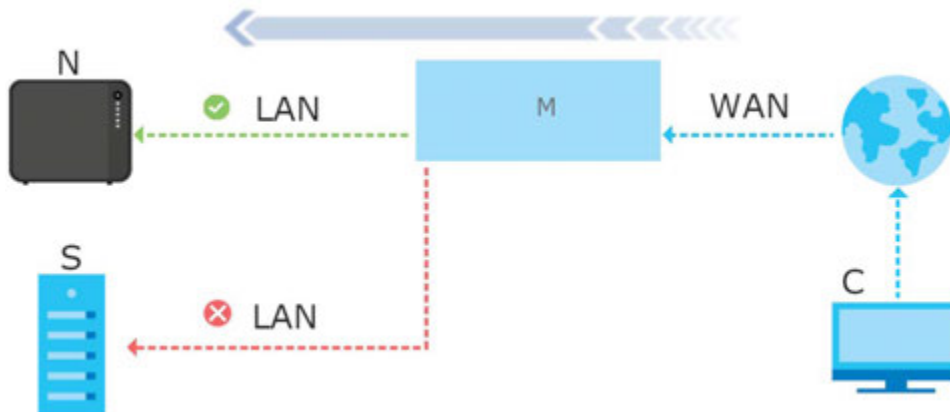
- 3 The **Web Configurator** screen displays after the set up is completed. Tap **Change Local Password** if you want to change your local password.
- The **Change Local Password** screen displays. Enter your **Current Local Password**, and then enter your **New local password** and **Confirm local password**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



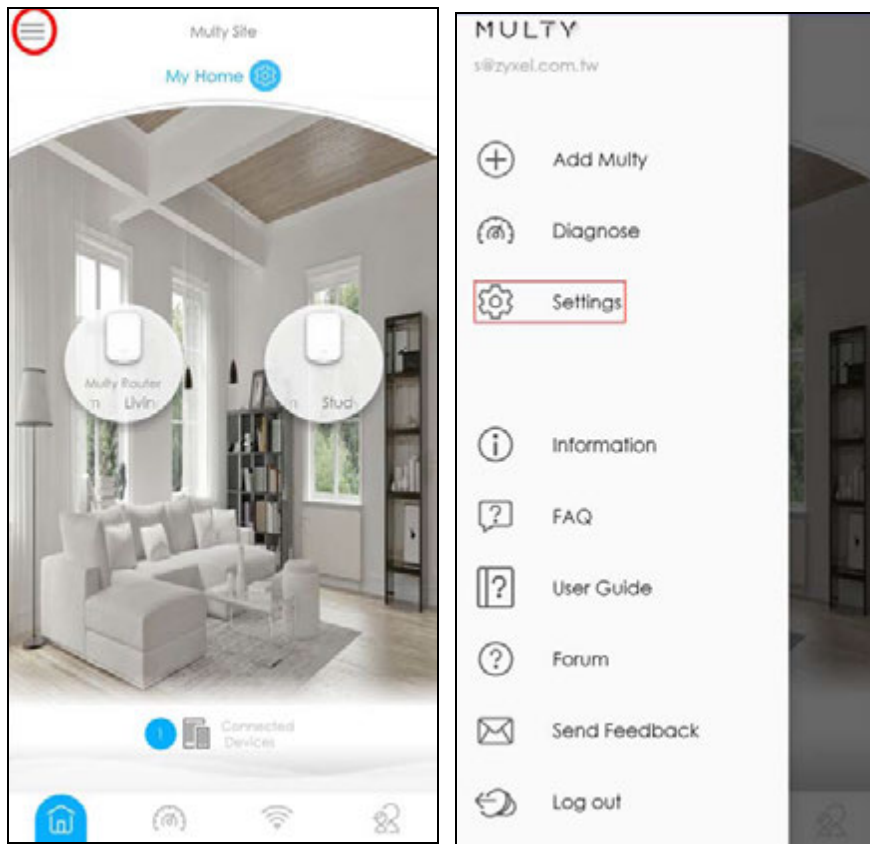
3.22 Enable or Add Port Forwarding Rules

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 (C) accessible from the Internet, as shown in the next figure.

Figure 42 Port Forwarding



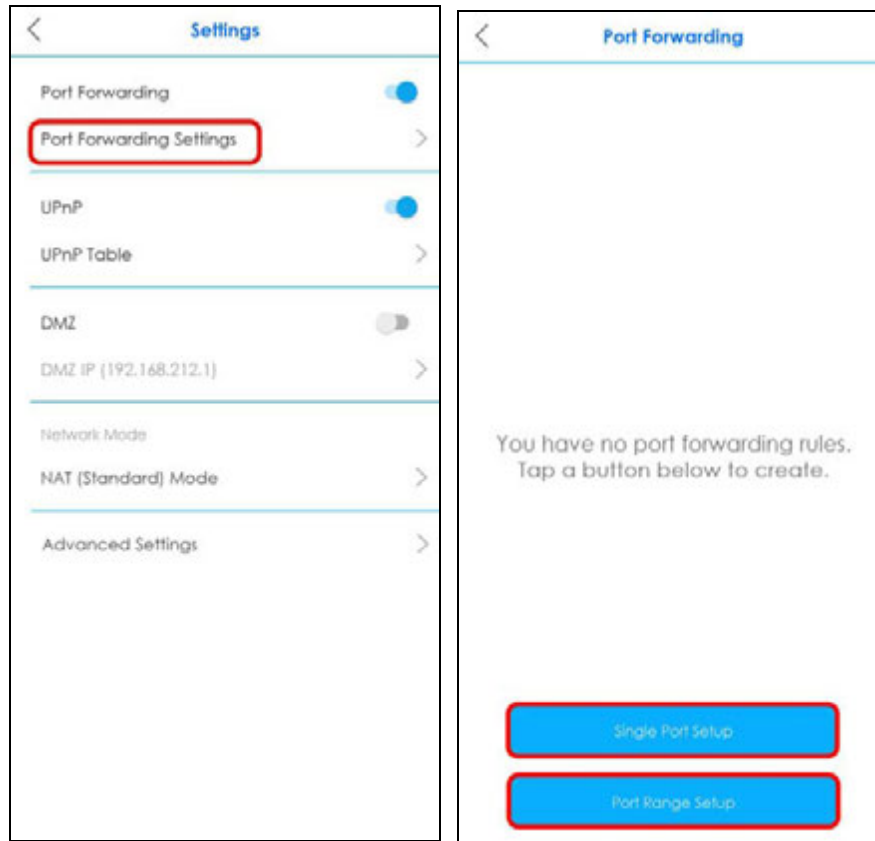
- 1 Tap the Menu icon in the upper-left to open the navigation panel, and then tap **Settings**.



- 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.

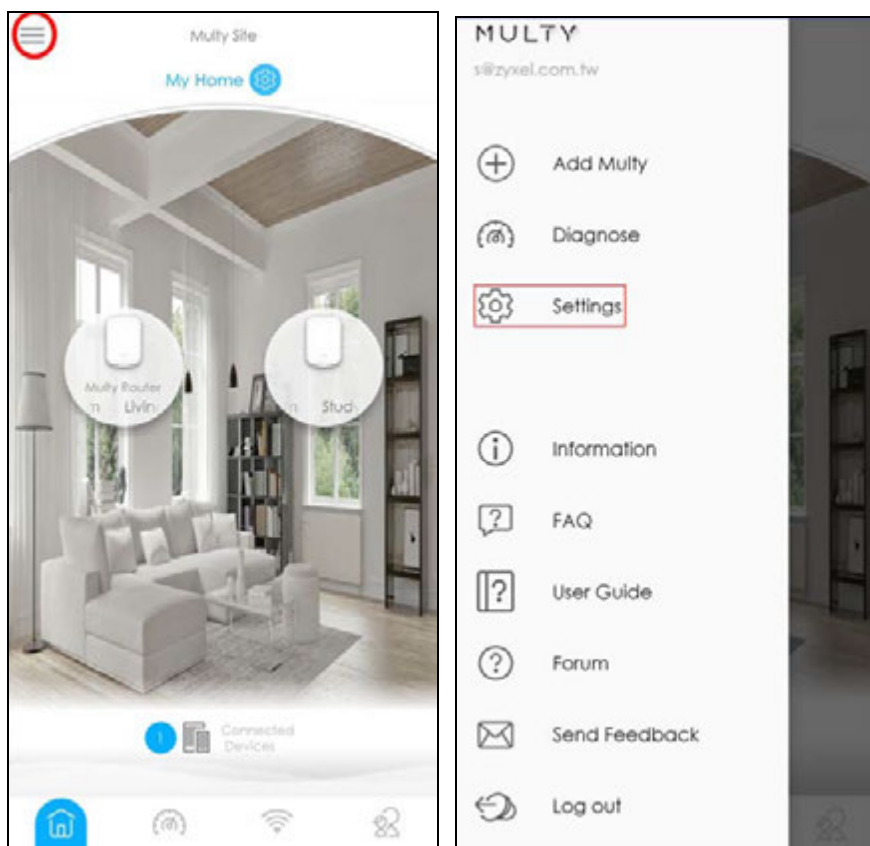
Add Rule	
Service Name	Rule1
Port Range Setup	6667 ~ 6668
Protocol	TCP & UDP
Device IP	192.168.212.48(ASUS_Phone)
Add Rule	

Port Forwarding	
Rule1	
Internal	6667~6668
Reserved IP	192.168.212.48
External	6667~6668
Protocol	TCP & UDP

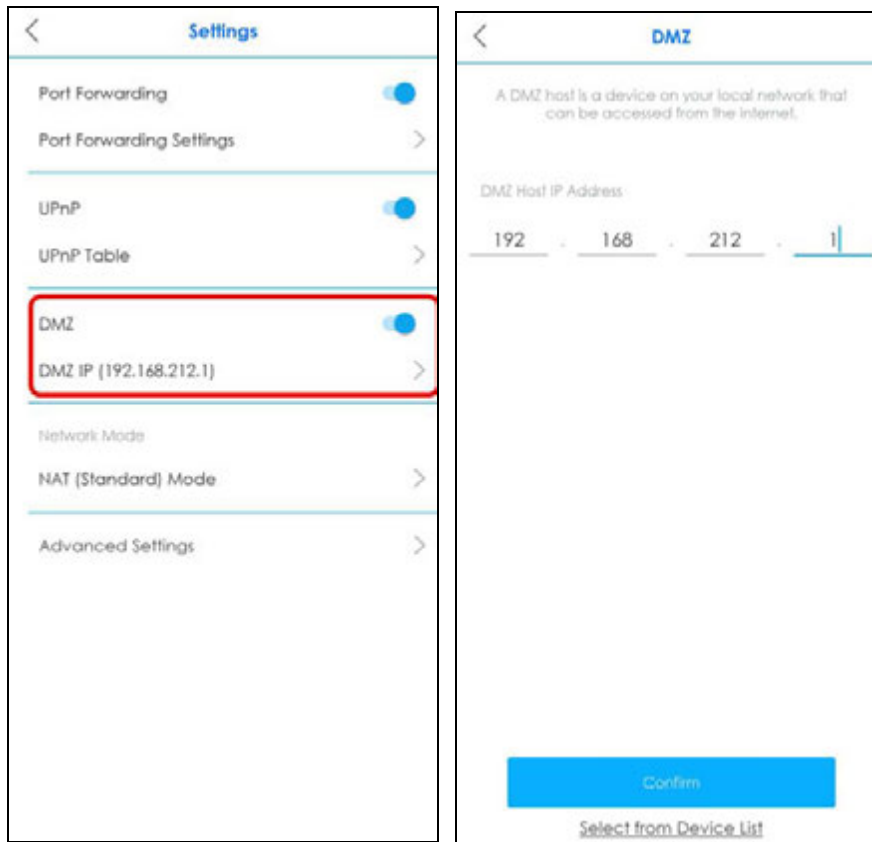
3.23 Enable DMZ

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 System. 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.

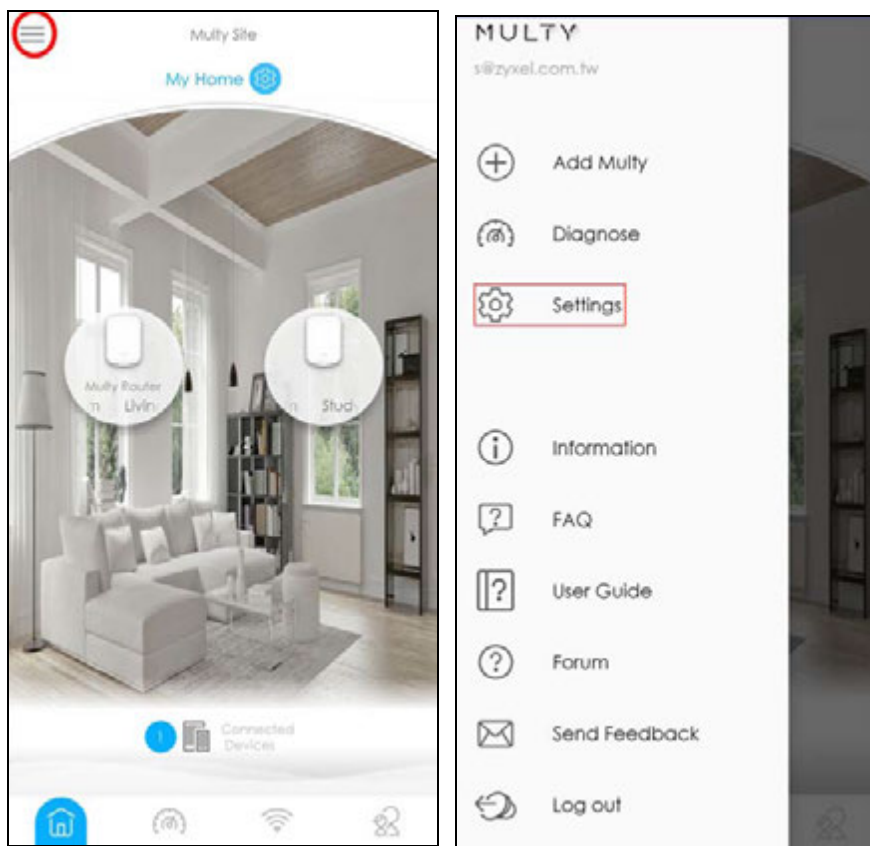
In **Bridge** mode, the Multy Device broadcasts traffic to the local network from the Internet. Choose **Bridge** mode if you have an existing router in your network and you do not want to reconfigure routing settings.

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

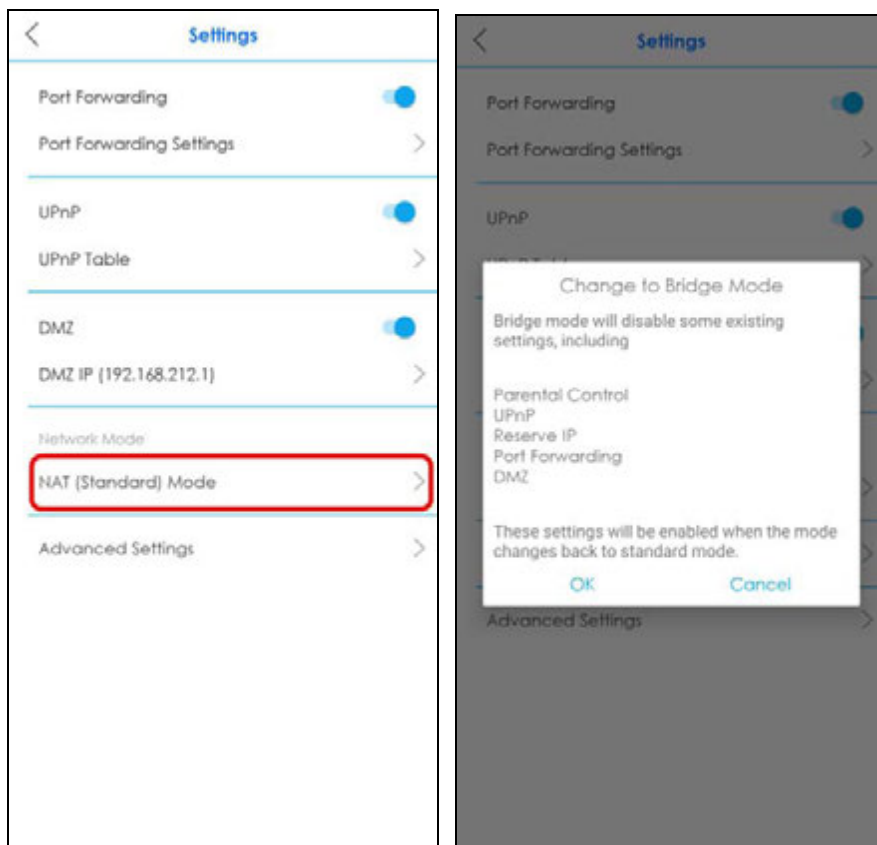
- Parental Control
- UPnP
- Reserve IP
- Port Forwarding
- DMZ
- SIP
- Guest WLAN

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.

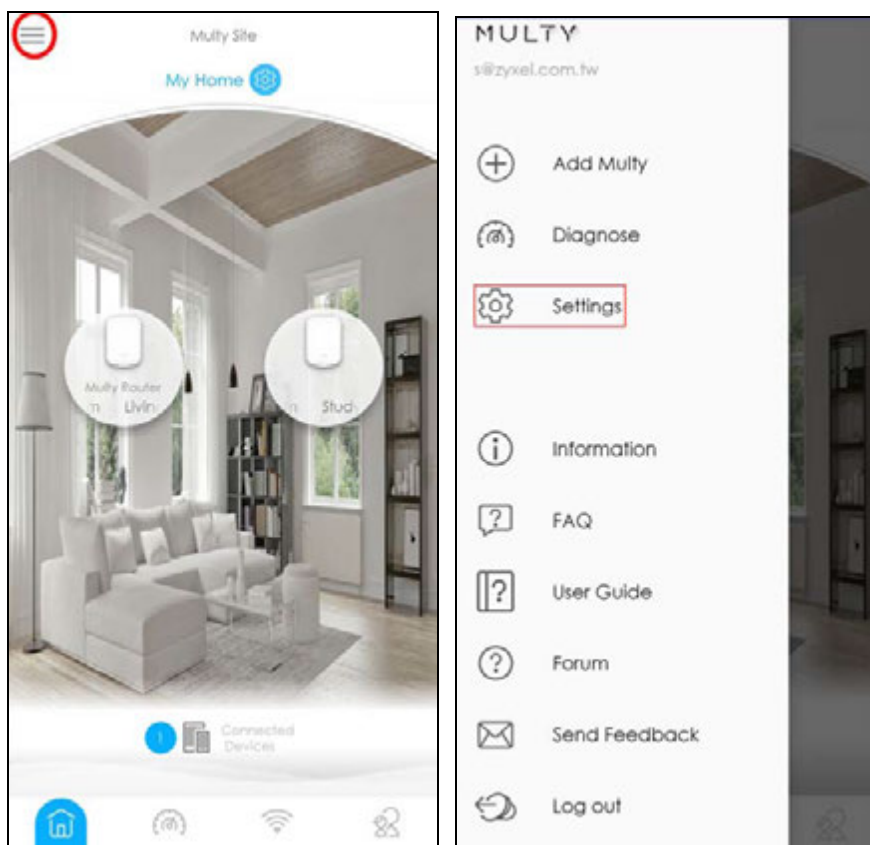


3.25 Turn Notifications On or Off

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.

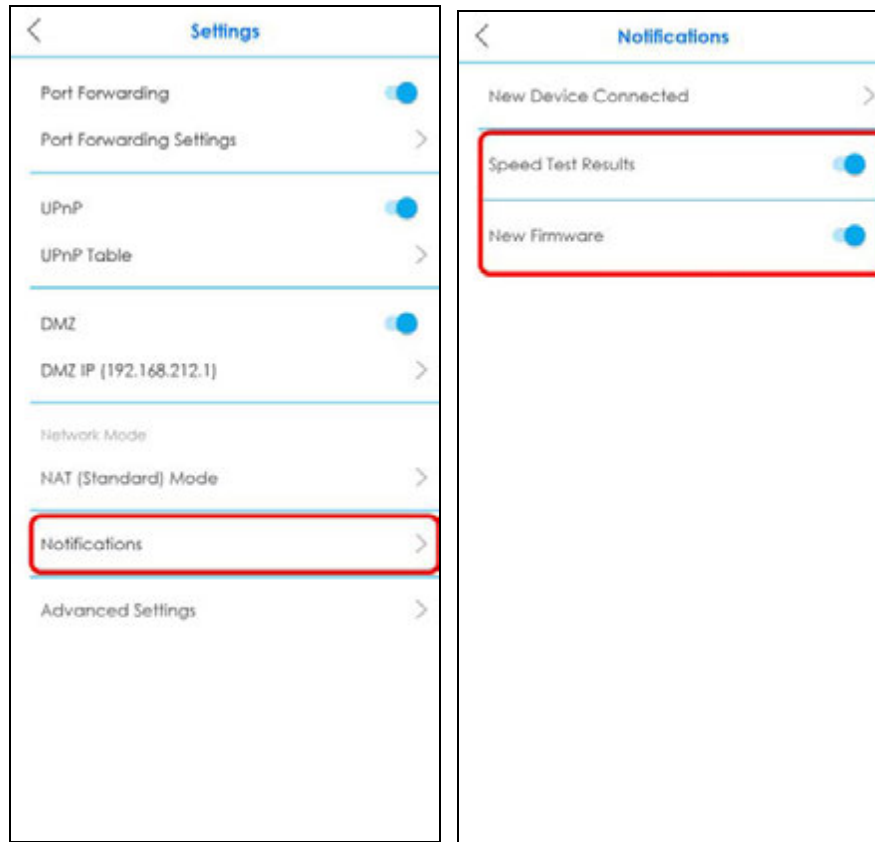
Note: You need to have a myZyxeCloud account to use this feature.

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

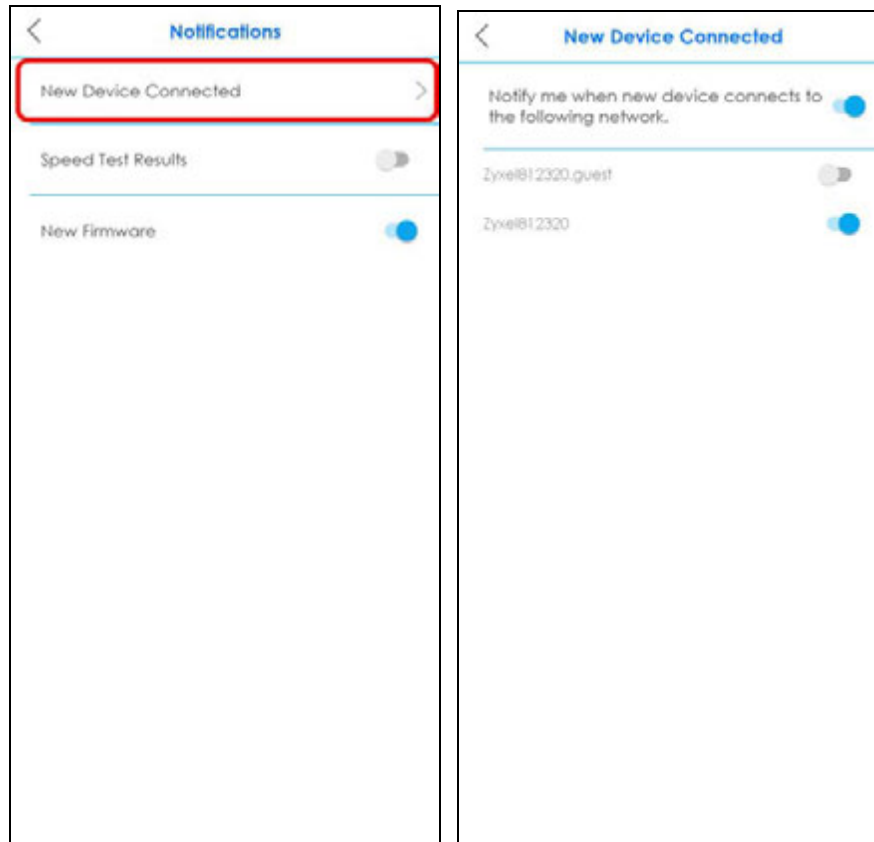


- 2 Tap **Notifications** on the **Settings** screen. Tap **Speed Test Results** or **New Firmware** to enable and allow the app to send you notifications when there is a new speed test result or new firmware update.

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 123](#) 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 75](#)).



- 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.



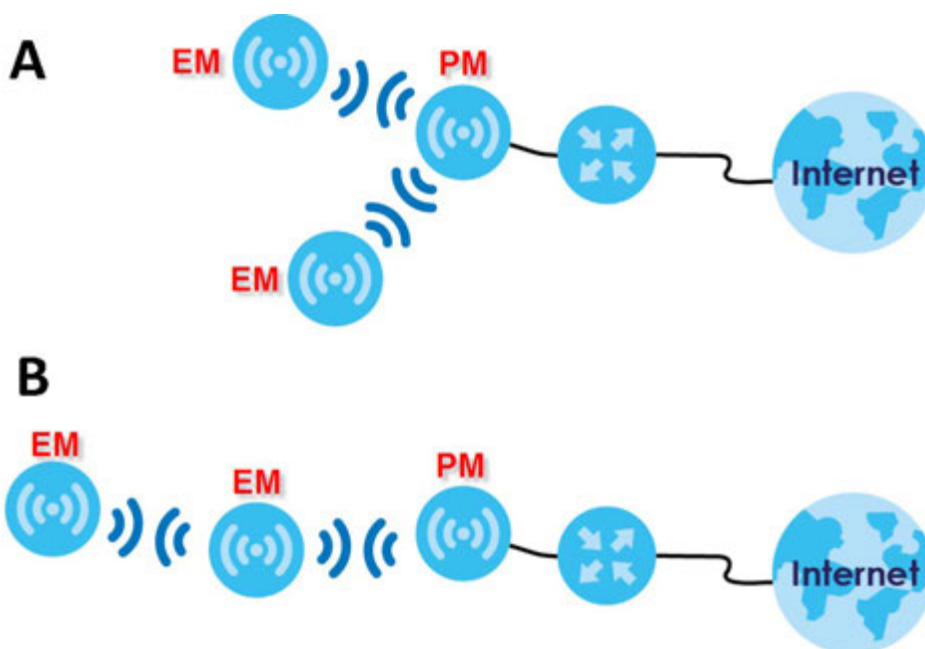
3.26 Enable or Disable Daisy Chain Network Topology

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

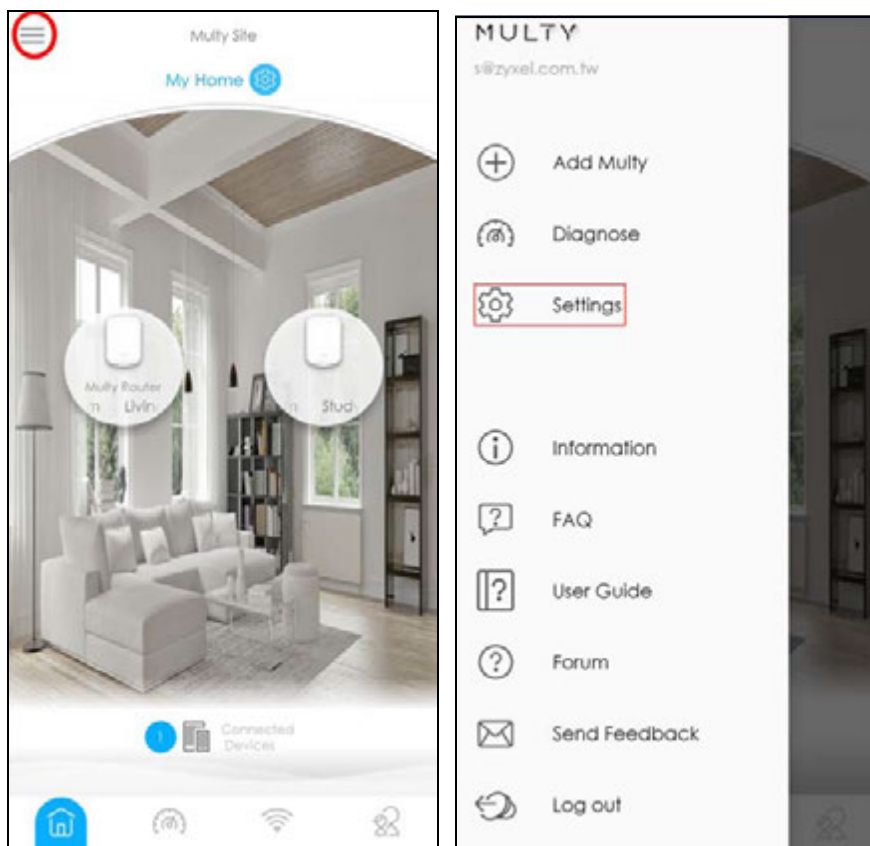
The daisy chain topology is illustrated in the figure below. Figure **A** shows the illustration of **Daisy Chain Disabled**. Figure **B** shows the illustration of **Daisy Chain Enabled**. When daisy chaining is enabled, each extender Multy (**EM**) can go through another extender Multy with a strong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

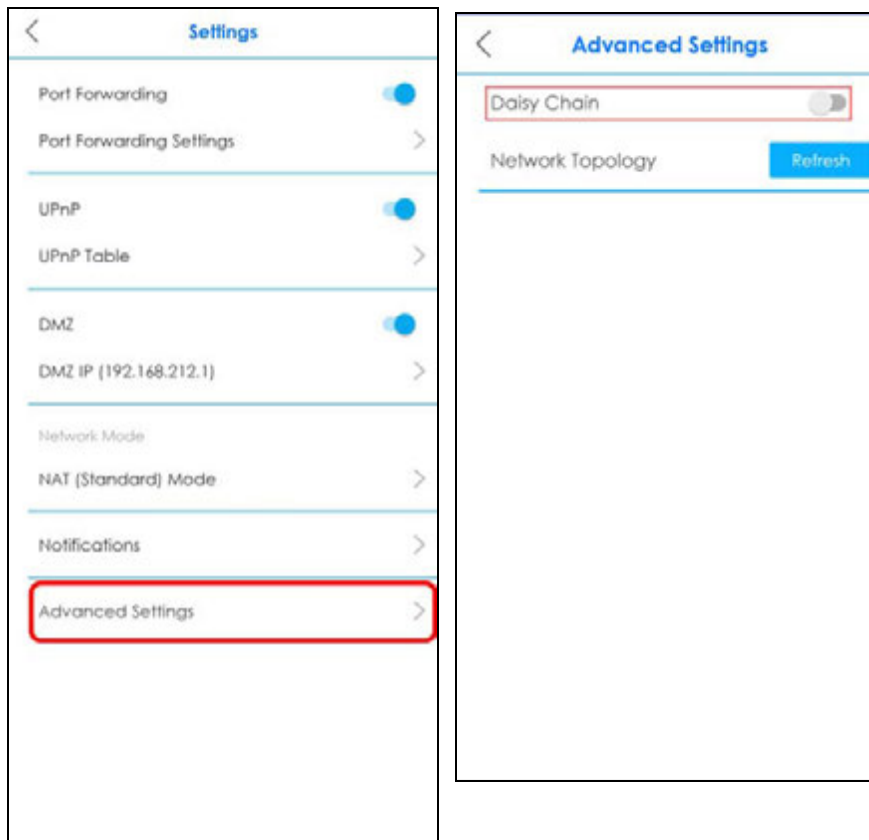
Note: This feature is not available on all Multy Devices. The **Daisy Chain** and **Network Topology** menus appear only when using a Multy Device that supports Daisy Chain. See [Table 2 on page 9](#) to see which devices support this feature.



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



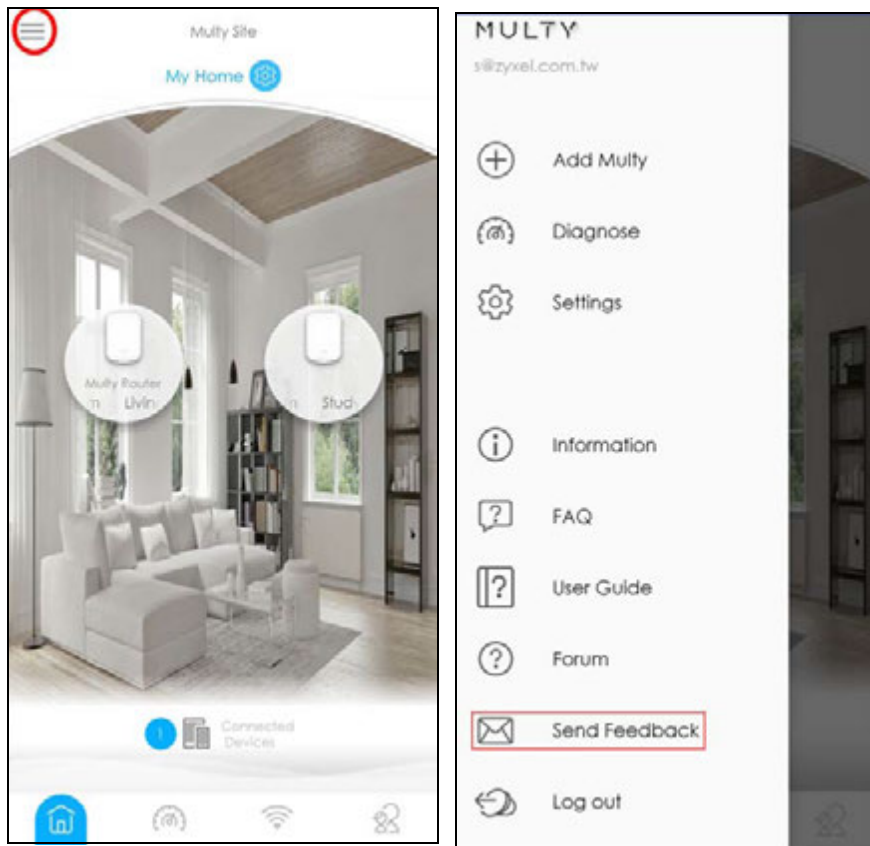
- 2 Tap **Advanced Settings** on the **Settings** screen. Tap **Daisy Chain** to enable or disable daisy chaining.



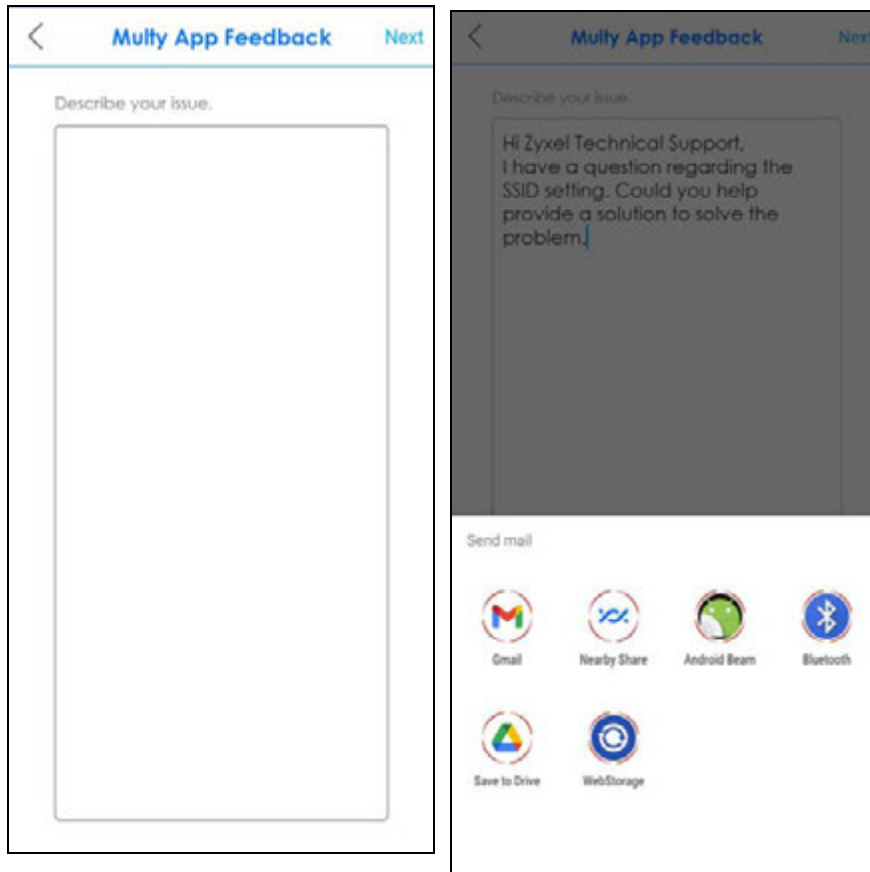
3.27 Report a Problem With the Zyxel Multy App

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**.

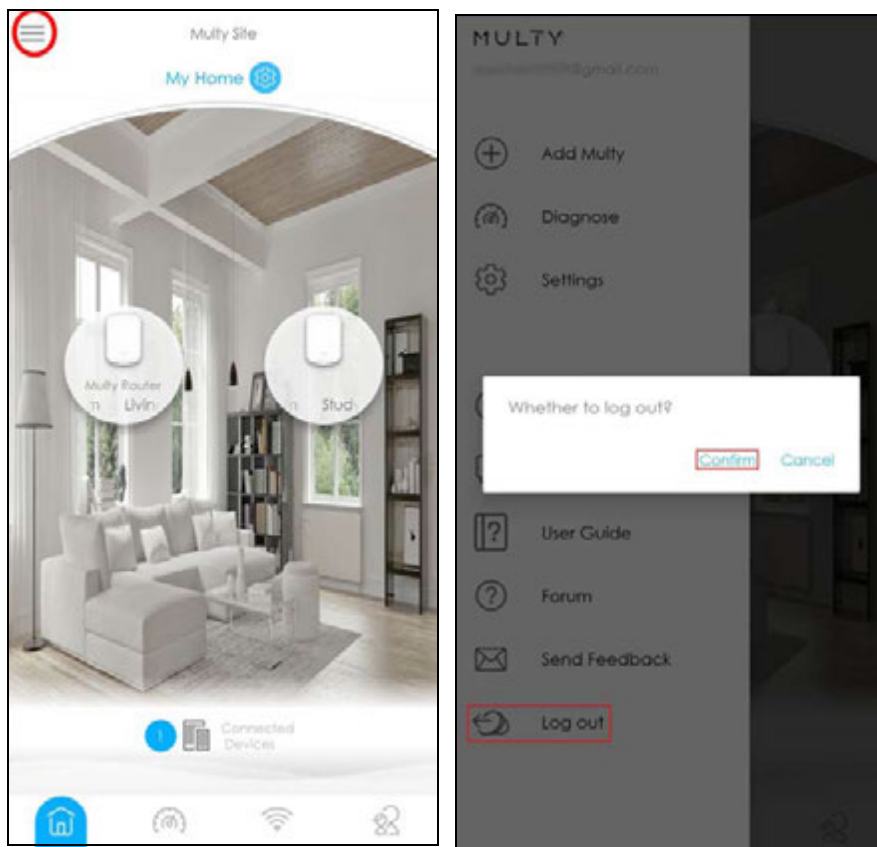


- 2 Edit the mail and then tap **Next** to send it through the Internet.



3.28 Log Out of the myZyxeCloud Account

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



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 2 on page 9](#)). For Multy Devices without an e-label, you may check the label printed on the Multy Device. See [Table 2 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

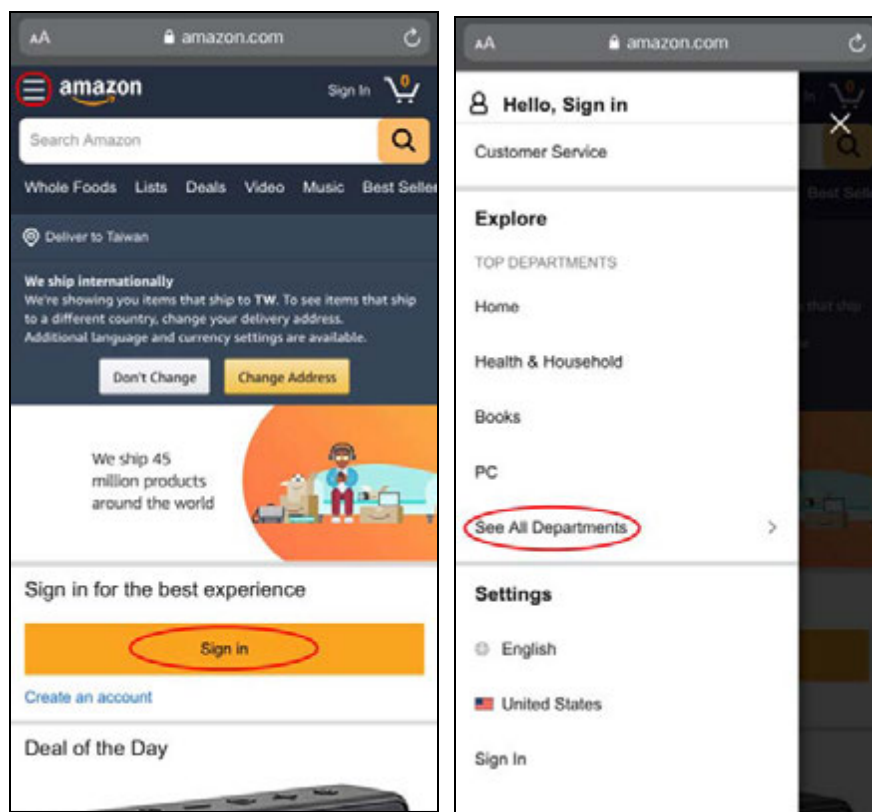
If you have an Alexa-enabled device (Amazon Echo for example), use your voice to control the Multy Devices in your Multy Sites. At the time of writing, the available Alexa skill voice commands for Multy Sites are:

- 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

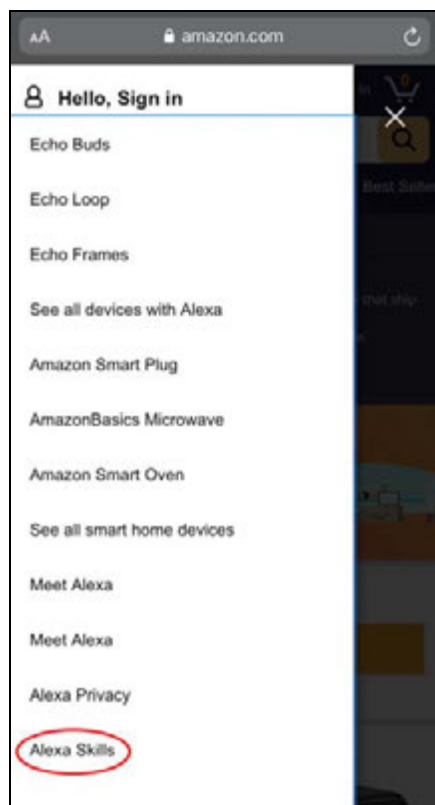
You need to enable the Multy-Alexa skills to enhance the functionality of your Alexa device and allow Alexa to perform the supported tasks. See [Table 2 on page 9](#) for more information.

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

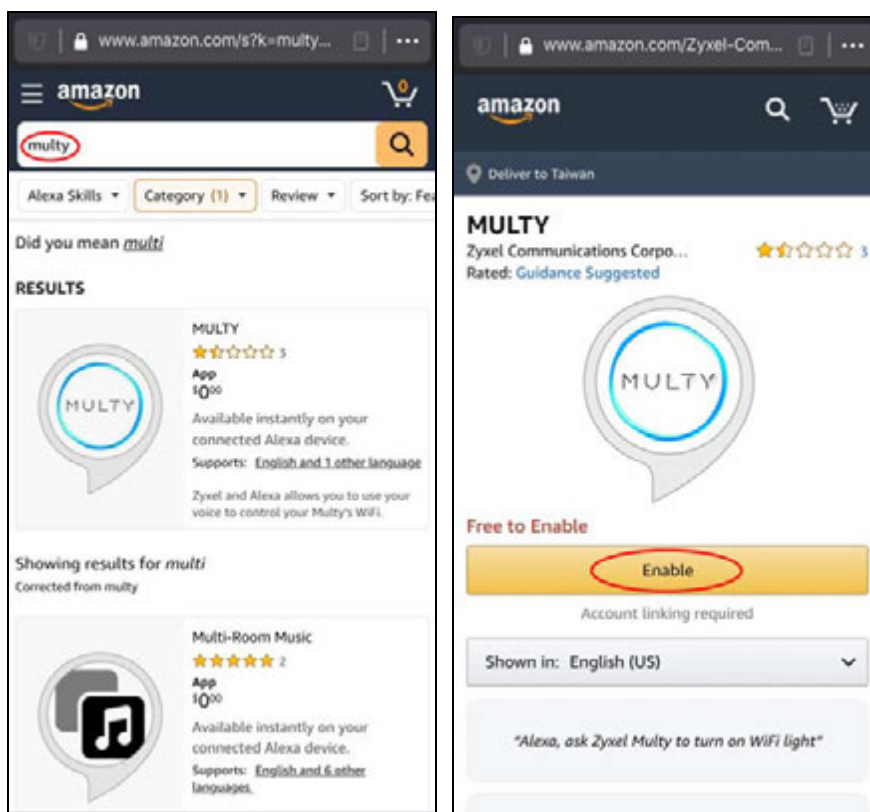
- 1 Go to the Amazon website (<https://www.amazon.com>) and sign in with your Amazon account. Tap the Menu icon in the upper-left and tap **See All Departments**.



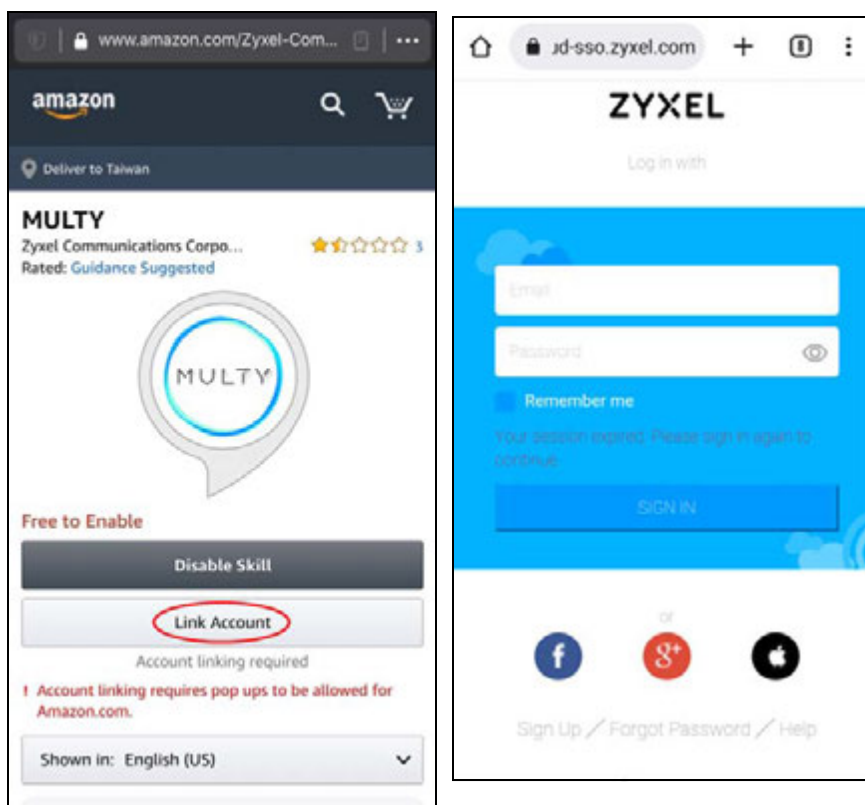
2 Select **Alexa Skills**.



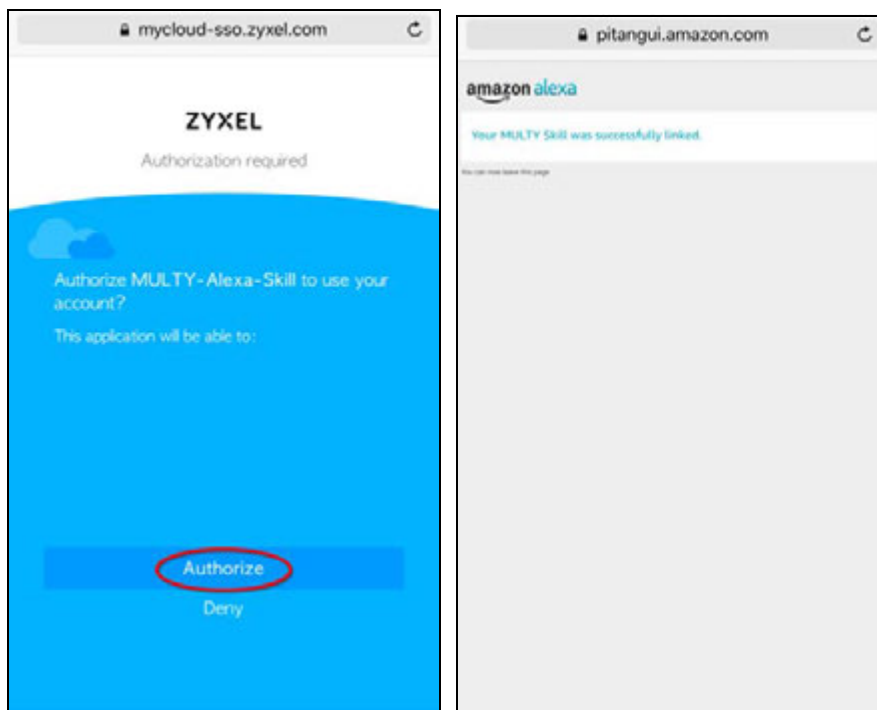
- 3 Enter the keyword "Zyxel Multy" in the search bar and select "Zyxel Multy" from the list of results. Tap **Enable** to connect the Multy Site to Alexa.



- 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

Wizard – Multy M1 (WSM20)

4.1 Overview

In this chapter, you will learn how to:

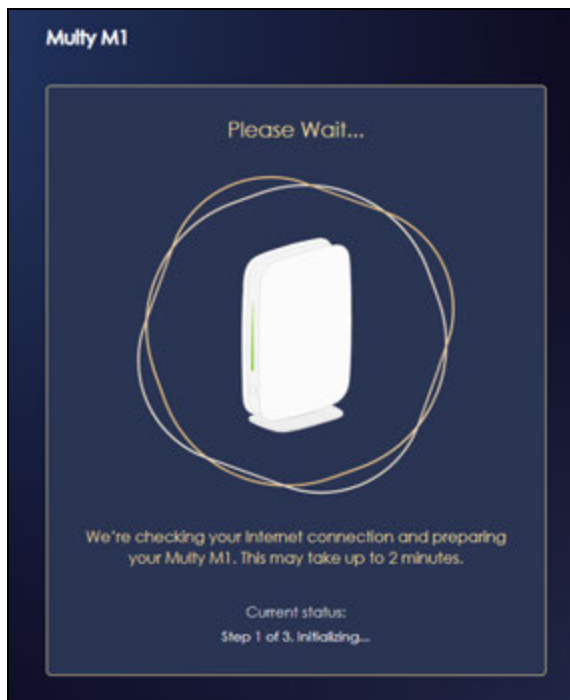
- Go through Multy Device (WSM20) wizard steps
- Create a myZyxeCloud account.
- Configure basic settings for your WiFi

4.2 Accessing the Wizard

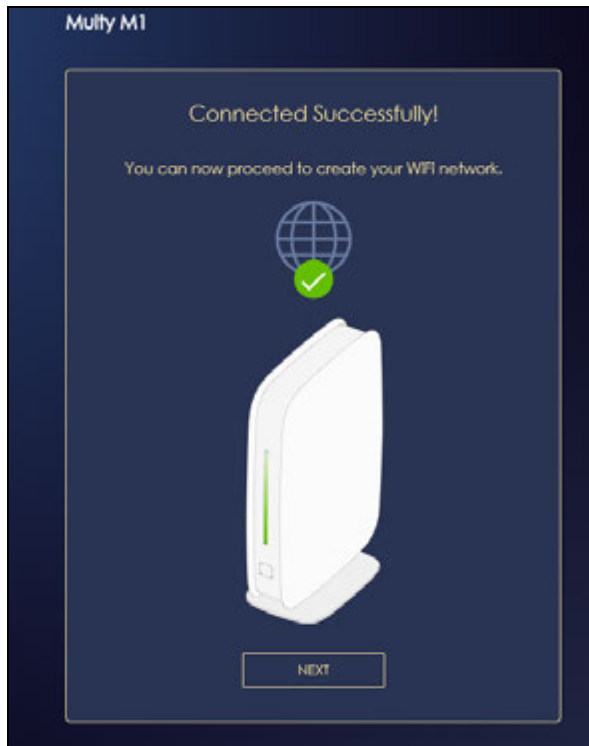
Launch your web browser and enter "<http://zyxelwifi.com>" or "<http://zyxelwifi.net>" or "<http://192.168.212.1>" as the website address.

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

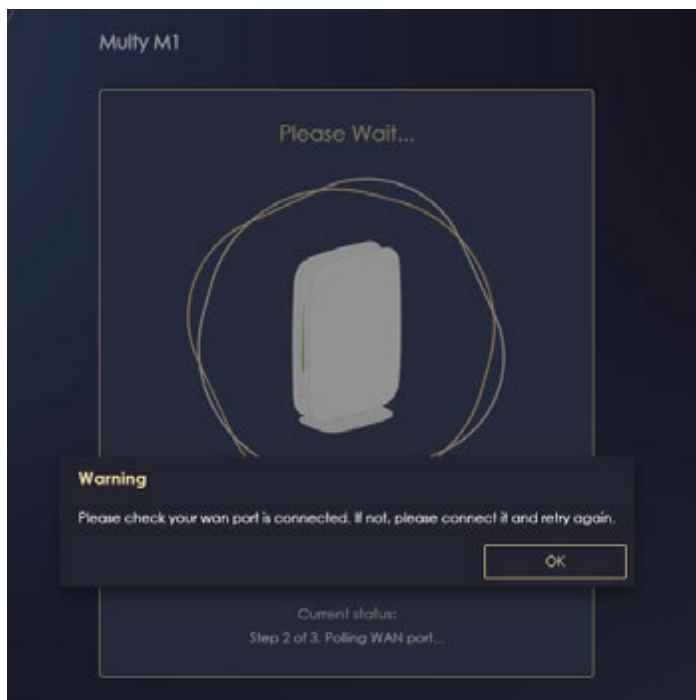
- 1 Make sure the WAN port of the Multy Device is connected to a modem or router with Internet access. Your Multy Device will check the status of your Internet connection the first time you log in.



- 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 Device is blocked. Turn on your network firewall after the configuration is completed.

You need to connect to the Internet to access your Multy Device. See [Section 4.2 on page 128](#) if you cannot connect to the Internet.

- 3 Enter 1 – 128 single-byte printable characters 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.

Multy M1

Name Your WiFi

Create a WiFi name that you're going to use for your network.

2.4G WiFi Name
Zyxel812350

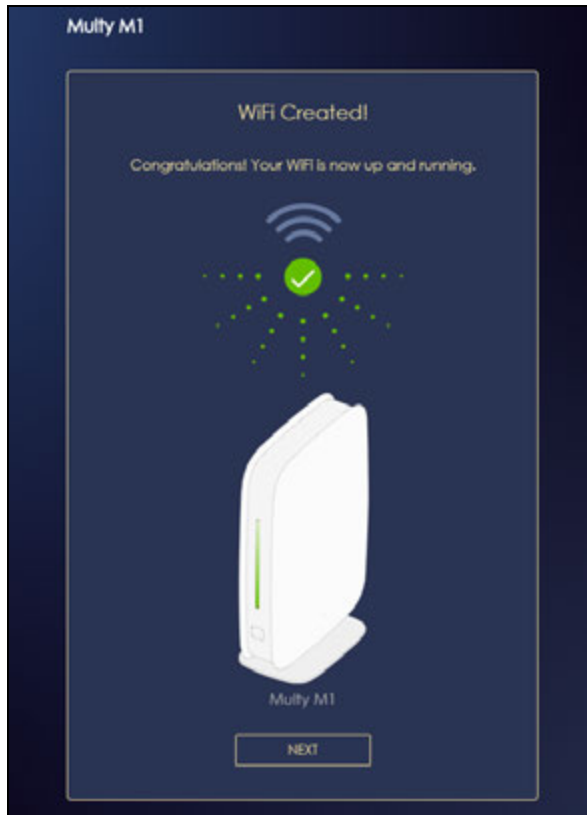
5G WiFi Name
Zyxel812350

WiFi Password
••••••••••

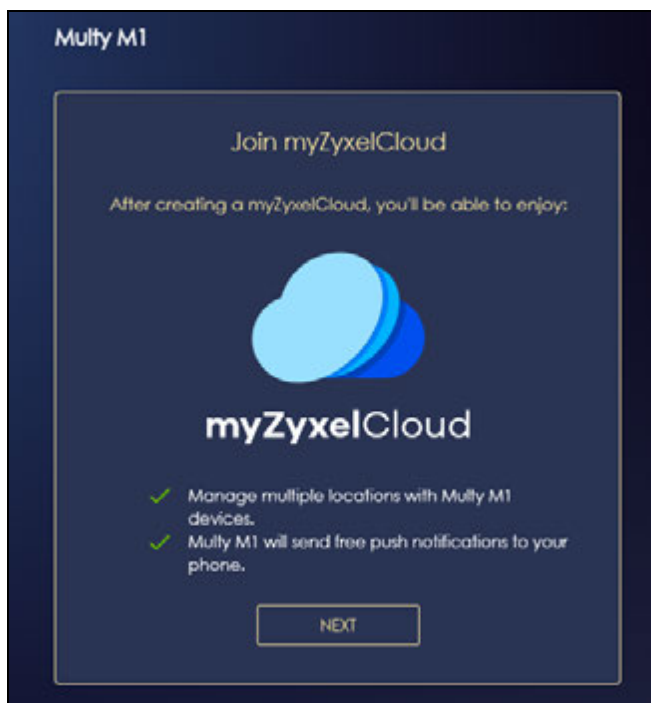
☒ Keep 2.4G & 5G name the same

NEXT

- 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.



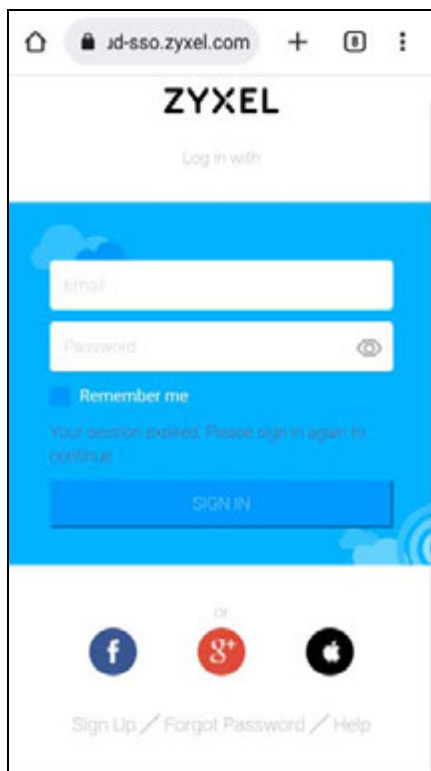
- 5 You need to create a myZyxeCloud account to log into the Multy Device. Click **Next** to go to the next step in the wizard.



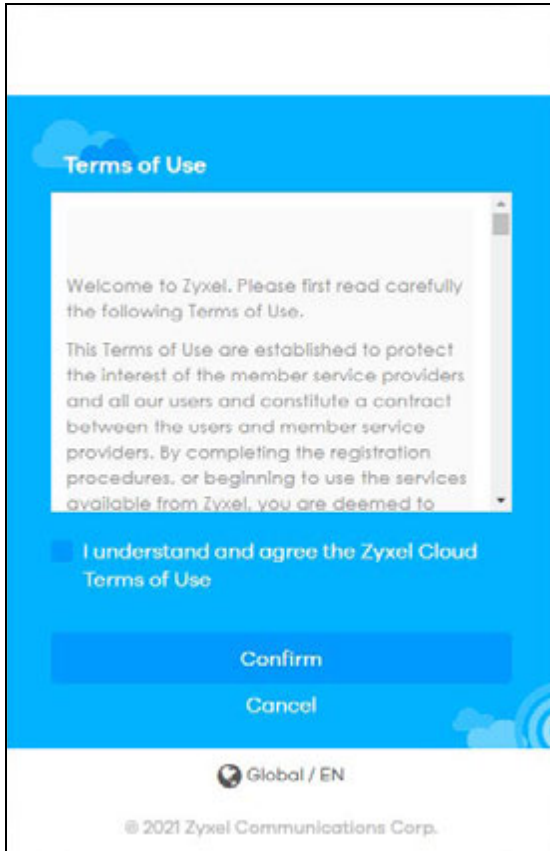
- 6 A pop up message shows. Click **OK** to be redirected to the registration website of myZyxeCloud.



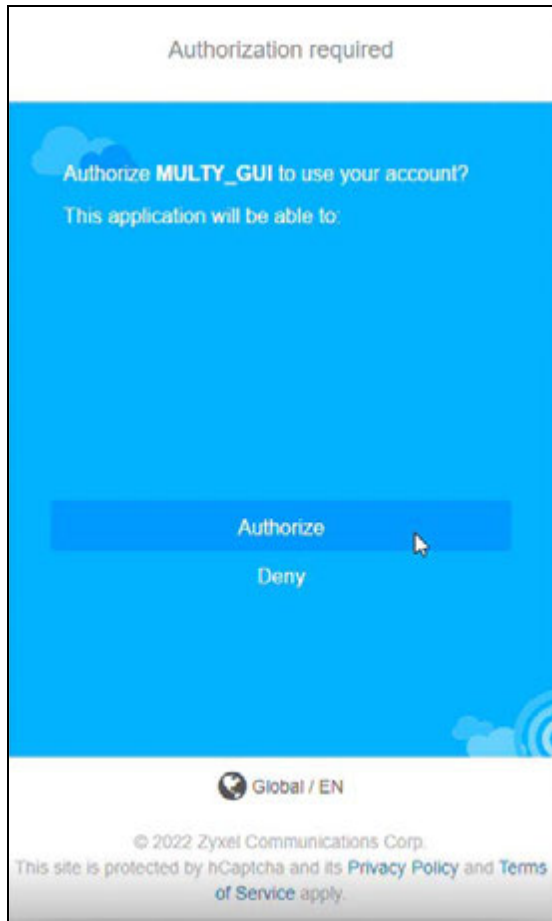
- 7 Enter your **Email** and **Password** and click **SIGN IN**, if you already have a myZyxeCloud account. If not, you can create one by clicking **Sign Up**. You can also click the Facebook or Google icon to create an account with your Facebook or Google account.



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



- 9 Click **Authorize** to allow the Web Configurator to link to your myZyxeCloud account.



- 10** Wait a moment for your Multy Device to link to your myZyxeCloud account. You will be redirected to the Web Configurator. Click **Next** to continue.



- 11 Create a Web Configurator password to access the Multy Device directly. You may choose to log in with your myZyxeCloud account or your local password the next time you log in.

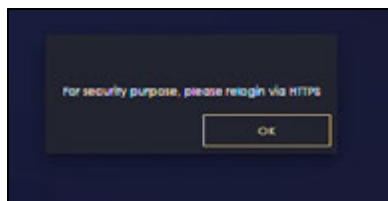
Note: You can change your local password in **System > General Settings**. See [Section 7.9 on page 165](#) for more information.



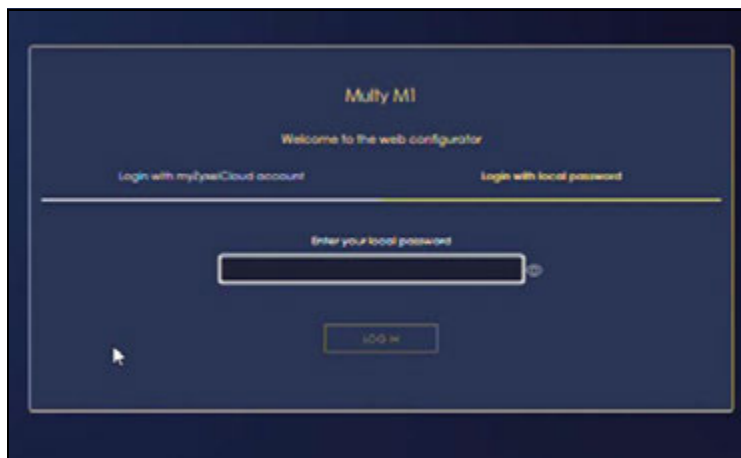
- 12 Wait for a moment to check if your Multy Device is updated with the latest firmware. If not, your Multy Device will automatically update the firmware.



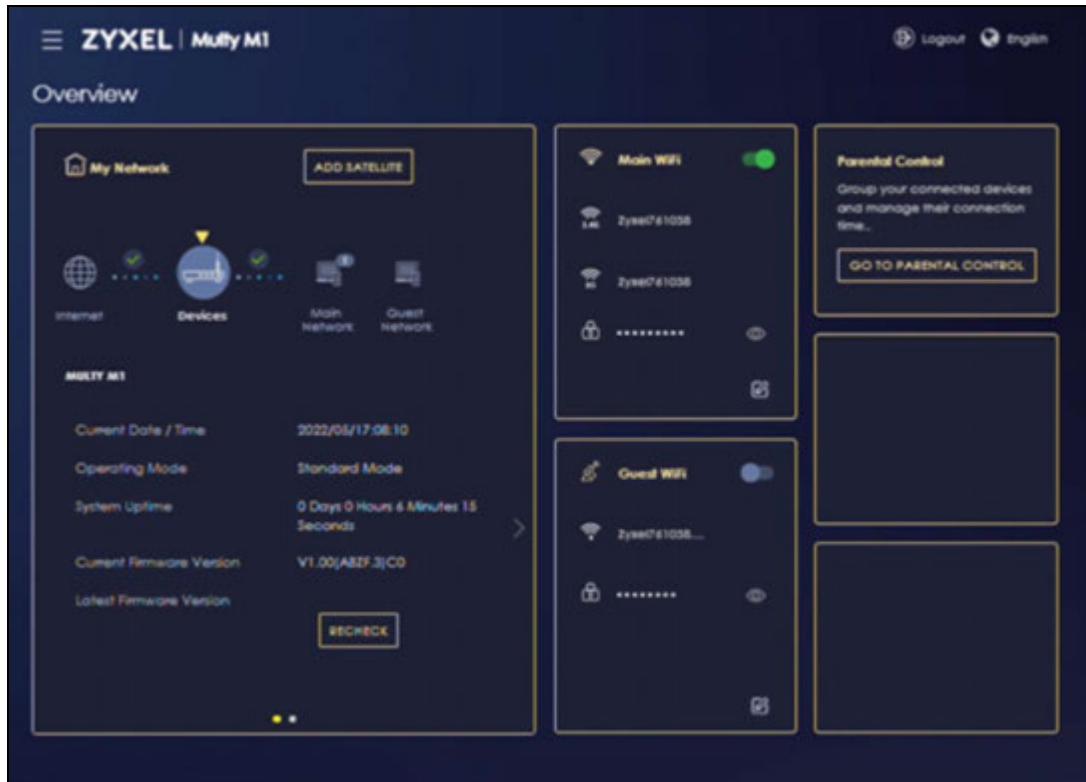
- 13 Click **OK** when the next screen appears.



- 14 On the displayed login screen, log in using your local password.



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



The Multy Device LED will light solid green after completing the installation.

CHAPTER 5

Web Configurator – Multy M1 (WSM20)

5.1 Overview

This chapter describes how to access the Multy Device 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 through Internet browser. Use a browser that supports HTML5, such as 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 Device hardware is properly connected (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 If the Multy Device 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 Device 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 myZyxeCloud 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 128](#).

Note: For setting and changing the local password, see [Section 7.9 on page 165](#).

Figure 43 Login

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

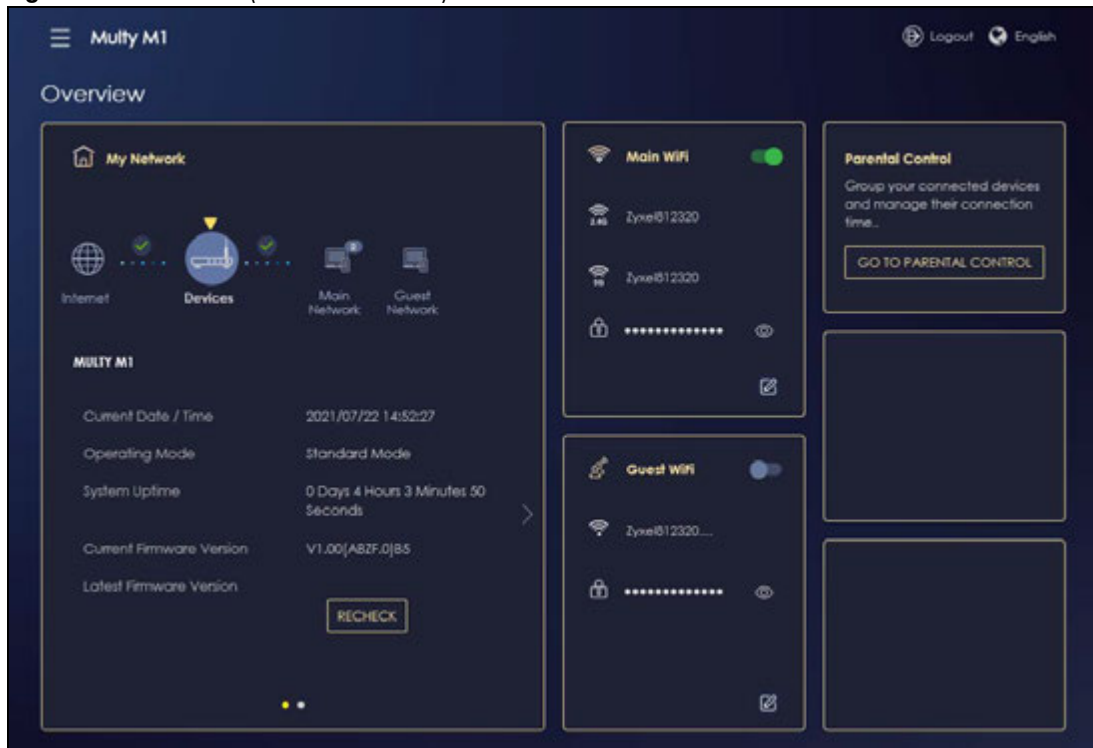
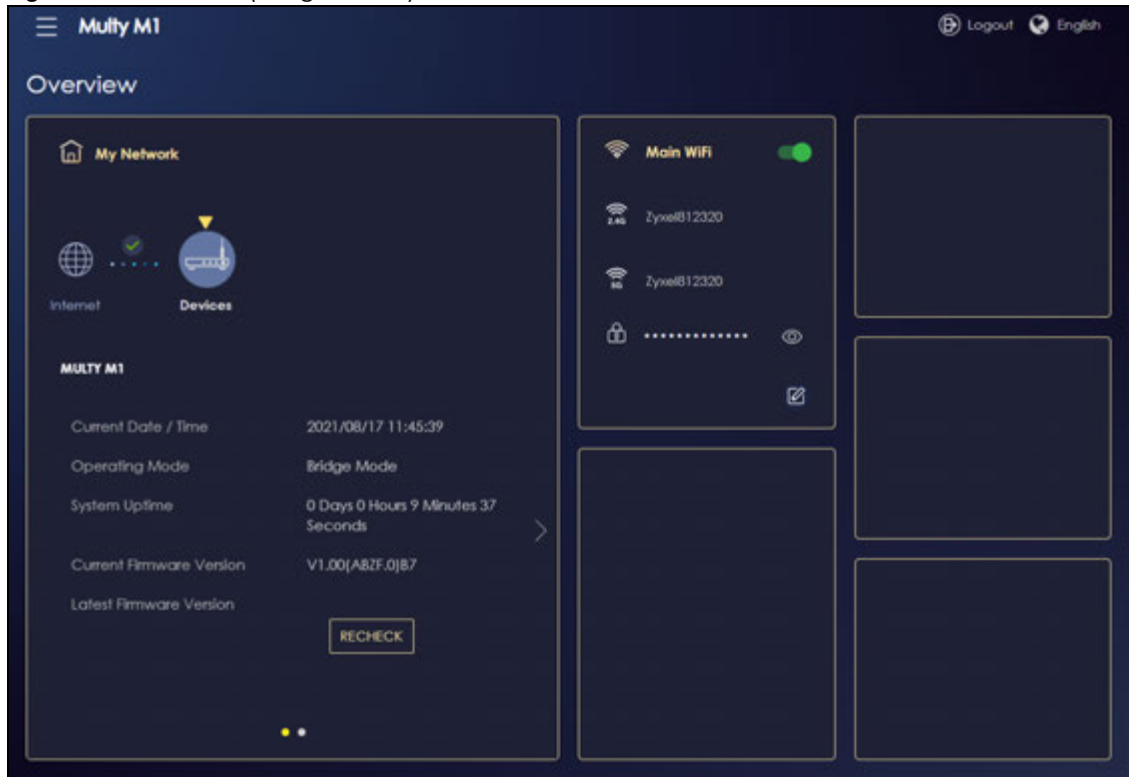
Figure 44 Overview (Standard Mode)

Figure 45 Overview (Bridge Mode)

5.3 Navigation Panel

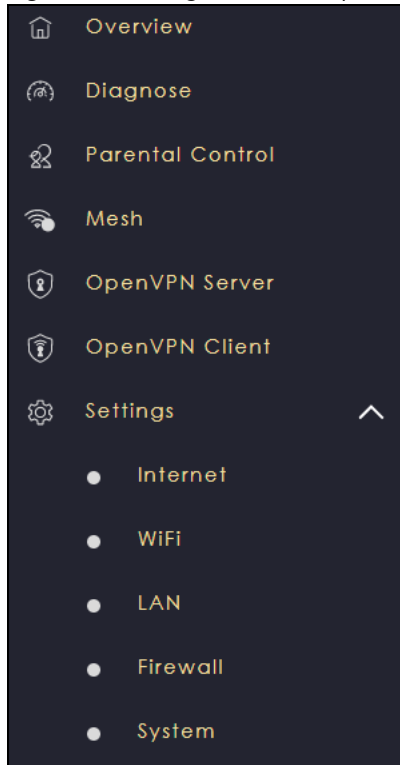
Use the submenus on the navigation panel to configure Multy Device features. Your navigation panel varies depending on the mode of your Multy Device.

See [Section 6.3 on page 145](#) for more information on Standard Mode.

See [Section 6.6 on page 147](#) for more information on Bridge Mode.

5.3.1 Standard Mode Navigation Panel

Figure 46 Navigation Panel (Standard Mode)



The following table describes the submenus.

Table 10 Settings > System > Status (Standard Mode)

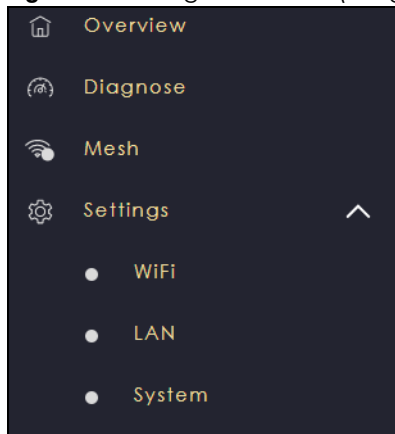
LINK	TAB	FUNCTION
Overview		Use this screen to: - View read-only information about your Multy Device - Configure WiFi settings.
Diagnose	Advanced Speed Test	Use this screen to check the speed of the connection between your Multy Device and the broadband modem/router.
	Speed Test History	Use this screen 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 Device OpenVPN server - View basic information about clients that are connected to the Multy Device OpenVPN server.

Table 10 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 Device to connect to when the Multy Device 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 Device and forward incoming service requests to the servers on your local network.
	Passthrough	Use this screen to change your Multy Device's port triggering settings.
	Dynamic DNS	Use this screen to configure dynamic DNS.
	UPnP	Use this screen to enable UPnP on the Multy Device.
WiFi	Main WiFi	Use this screen to enable WiFi and configure WiFi and WiFi security settings.
	Guest WiFi	Use this screen to configure multiple BSSs on the Multy Device.
	WPS	Use this screen to configure WPS.
	Scheduling	Use this screen to schedule the times WiFi is enabled.
LAN	LAN IP	Use this screen to configure the Multy Device's LAN IP address and subnet mask. Use this screen to configure the IPv6 address for the Multy Device on the LAN. Use this screen to configure your DNS server. Use this screen to enable the Multy Device's DHCP server.
	IPv6 LAN	Use this screen to configure the IPv6 address for your Multy Device 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 Device.
	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 interfaces from which the Multy Device can be managed remotely and specify a secure client that can manage the Multy Device.
	Maintenance	Use this screen to upgrade firmware, restart the Multy Device without turning the power off or reset the Multy Device 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 Device.

5.3.2 Bridge Mode Navigation Panel

Figure 47 Navigation Panel (Bridge Mode)



The following table describes the submenus.

Table 11 Settings > System > Status (Bridge Mode)

LINK	TAB	FUNCTION
Overview		Use this screen to: - View read-only information about your Multy Device - Configure WiFi settings
Diagnose	Advanced Speed Test	Use this screen to check the speed of the connection between your Multy Device 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 WiFi and configure WiFi and WiFi security settings.
	WPS	Use this screen to configure WPS.
	Scheduling	Use this screen to schedule the times WiFi is enabled.
LAN	LAN IP	Use this screen to configure the Multy Device's LAN IP address and subnet mask. Use this screen to configure the Multy Device's DNS server.
System	Status	Use this screen to view the basic information of the Multy Device.
	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 Device without turning the power off or reset the Multy Device 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 Device.

CHAPTER 6

Multy M1 (WSM20) Modes

6.1 Overview

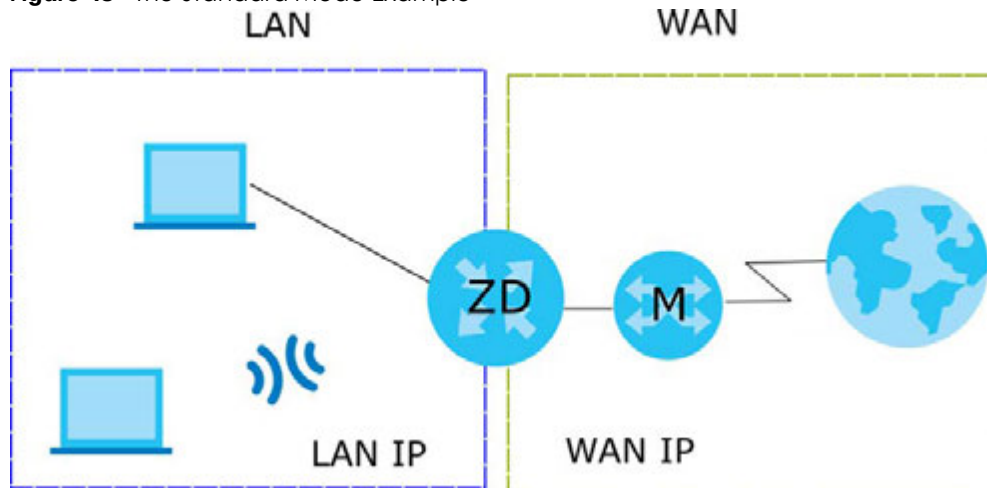
This chapter introduces the different operating modes available on your Multy Device. Or simply how the Multy Device is being used in the network.

6.2 Modes

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

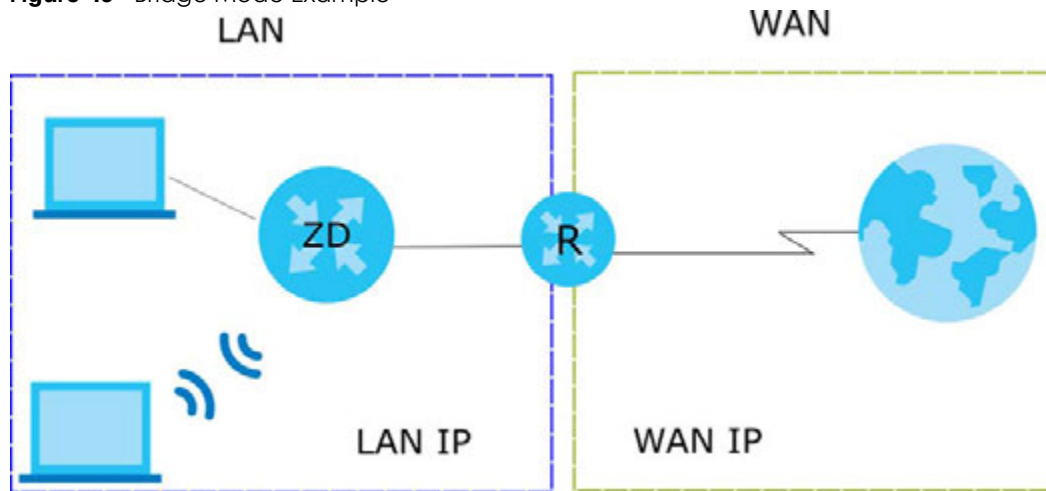
- **Standard Mode:** In standard mode Multy Device has two IP addresses, a LAN IP address and a WAN IP address. It also has more routing features. To see the standard mode features, go to [Table 10 on page 141](#). In the example scenario below, Multy Device connects the local network to the Internet through a modem (**M**).

Figure 48 The Standard Mode Example



- **Bridge Mode:** In bridge mode, Multy Device has one IP address and Multy Device interfaces are bridged together in the same network. To see the bridge mode features, go to [Table 11 on page 143](#). In the example scenario below, Multy Device connects the local network to the Internet through a router (**R**).

Figure 49 Bridge Mode Example



For more information on changing the mode of your Multy Device, refer to [Section 7.11 on page 167](#).

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

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

6.3 Standard Mode Overview

The Multy Device 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 Device 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 Device ([Section 6.5 on page 145](#)).

6.5 Standard Mode Status Screen

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

Figure 50 Settings > System > Status (Standard Mode)

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

Table 12 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 Device is set, see Section 7.11 on page 167 for more information.
Enable IPv4 Firewall	This shows if the IPv4 firewall is enabled on the Multy Device.
Enable IPv6 Simple Security	This shows if the IPv6 firewall is enabled on the Multy Device.
System Uptime	This is the total time the Multy Device 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 12 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 Device.
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 Device in the LAN.

6.6 Bridge Mode Overview

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 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 140](#) for more information.

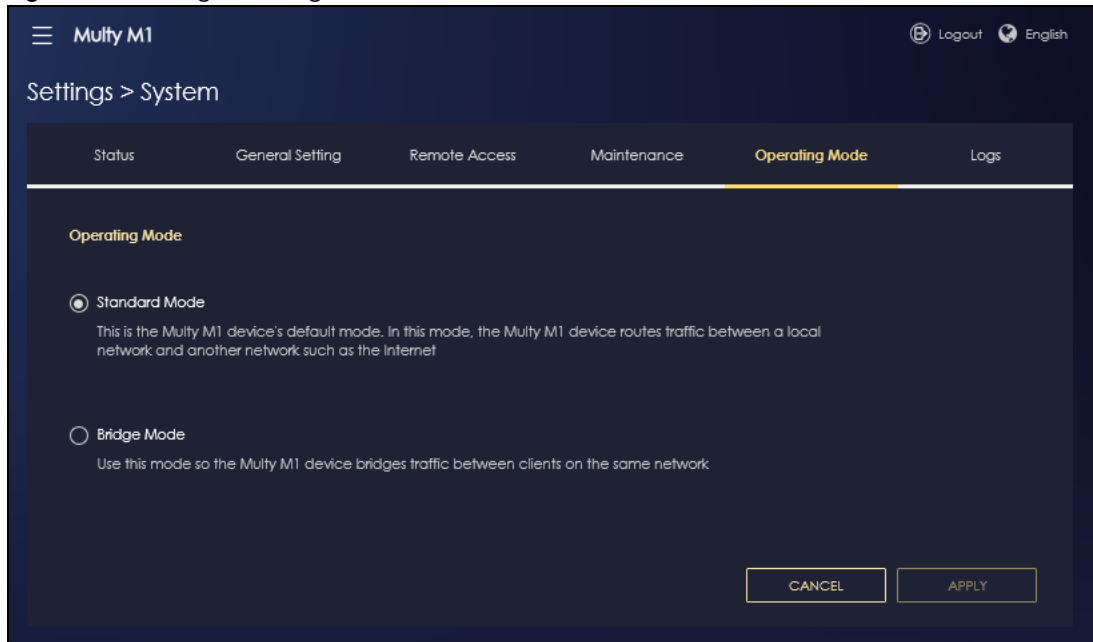
6.7 What You Can Do

- Set up a network with the Multy Device as a bridge ([Section 6.8 on page 147](#)).
- Use the **Status** screen to view read-only information about your Multy Device ([Section 6.9 on page 149](#)).

6.8 Setting your Multy Device to Bridge Mode

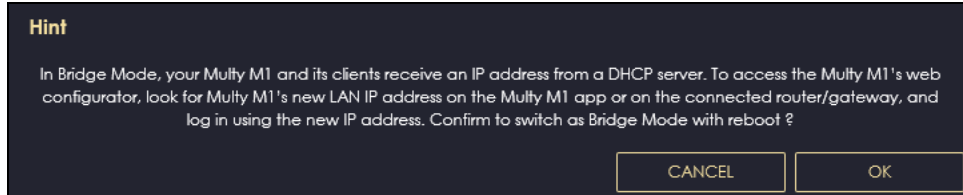
- 1 Log into the Web Configurator if you haven't already. See the Quick start Guide for instructions on how to do this.
- 2 To use your Multy Device as a bridge, go to **Settings > System > Operating Mode** and select **Bridge Mode**.

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

Figure 51 Change 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 Device is already in Bridge mode.

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

Figure 52 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

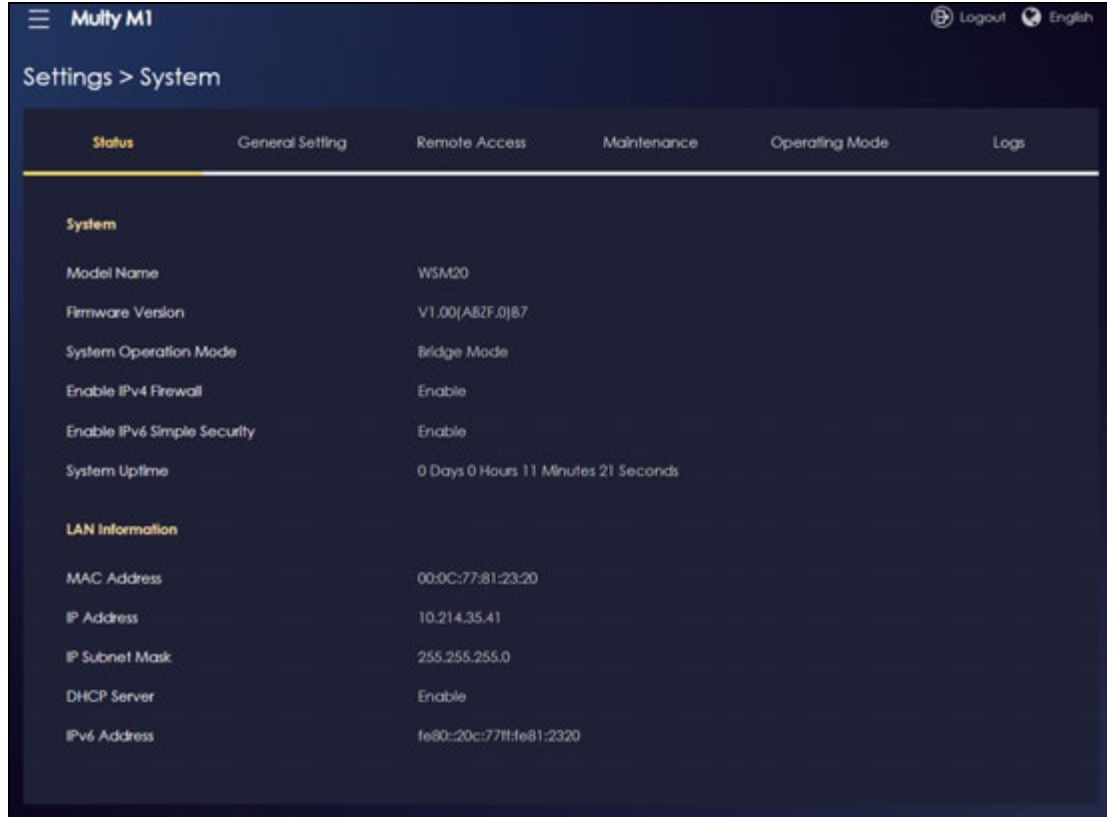
Log in to the Web Configurator in Bridge mode, do the following:

- 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 Device using an Ethernet cable.
- 3 Connect a modem/router to the WAN port of the Multy Device using another Ethernet cable.
- 4 If the Multy Device is not connected to a router or DHCP server, the Multy Device cannot assign your computer an IP address.
- 5 After you have set your computer's IP address, open a web browser such as Microsoft Edge 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 53 Settings > System > Status (Bridge Mode)



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

Table 13 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 Device is set, see Section 7.11 on page 167 for more information.
Enable IPv4 Firewall	This shows if the IPv4 firewall is enabled on the Multy Device.
Enable IPv6 Simple Security	This shows if the IPv6 firewall is enabled on the Multy Device.
System Uptime	This is the total time the Multy Device 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 Device in the LAN.

CHAPTER 7

Web Interface Tutorials – Multy M1 (WSM20)

7.1 Overview

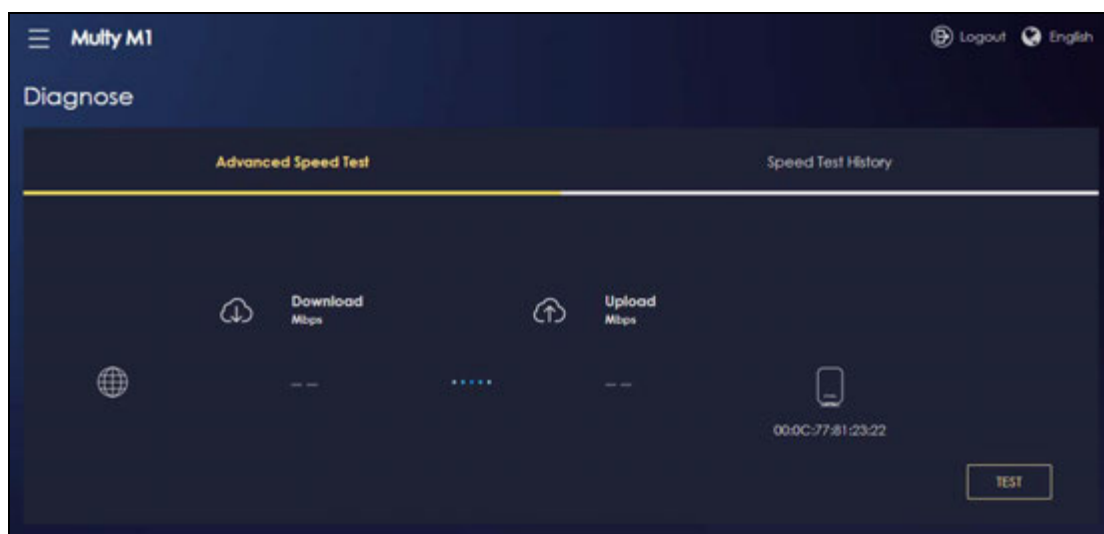
This chapter provides tutorials for setting up your Multy Device.

- [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 Device as an OpenVPN Server](#)
- [Configure the Multy Device as an OpenVPN Client](#)
- [Change the Web Configurator Local Password](#)
- [Change the Operating Mode](#)
- [Configure a Port Forwarding Rule](#)

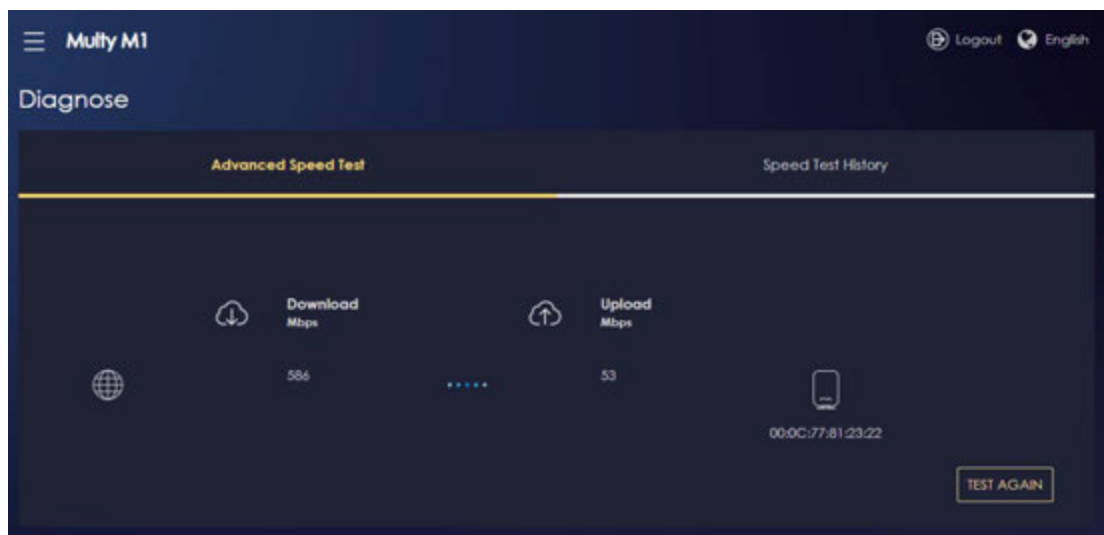
7.2 Run a Speed Test

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

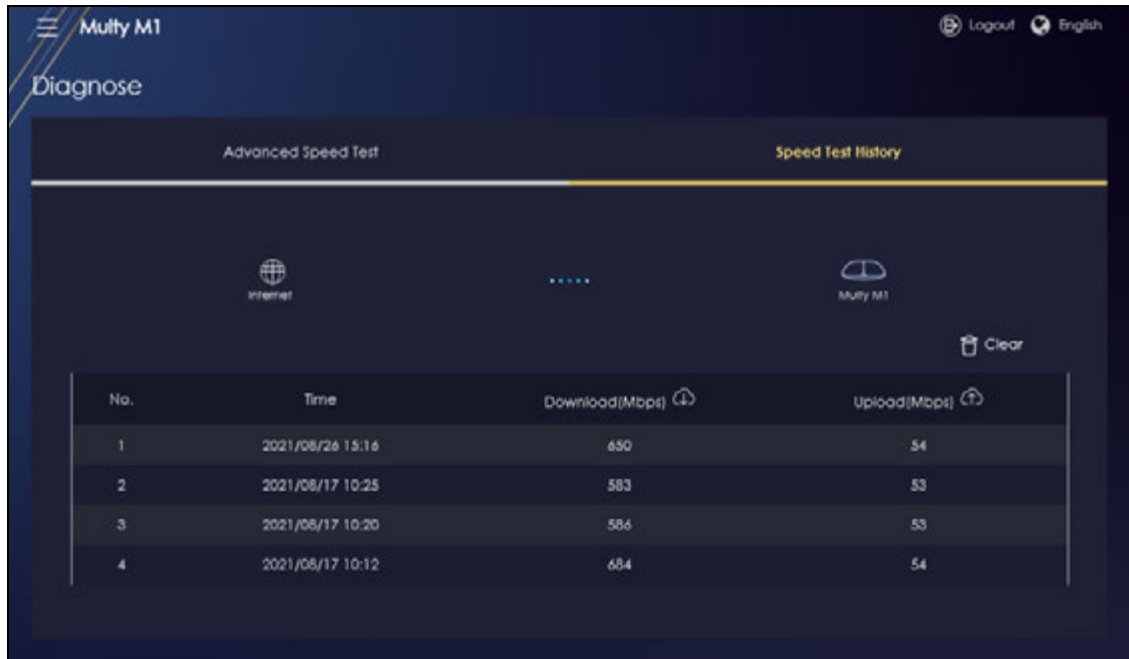
- 1 Click the **Navigation Panel** icon on the top-left corner () and click **Diagnose** to open the **Advanced Speed Test** screen. Use this screen to view all the available connections in your Multy Device System.



- 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.

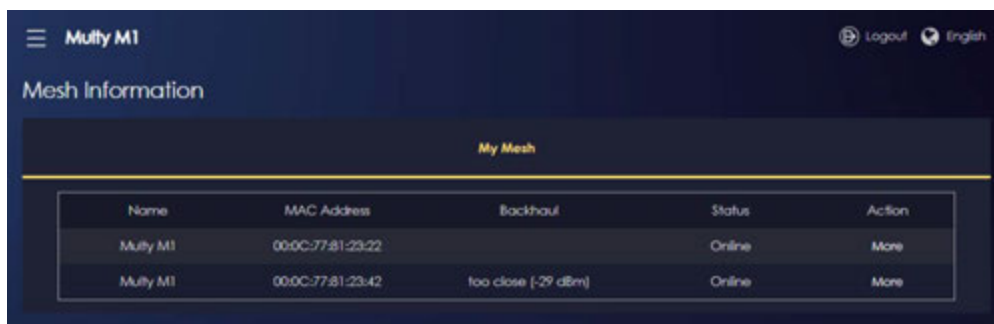


- 3 Click the **Speed Test History** tab to view a summary of the tests made. Click **Clear** to delete all records.

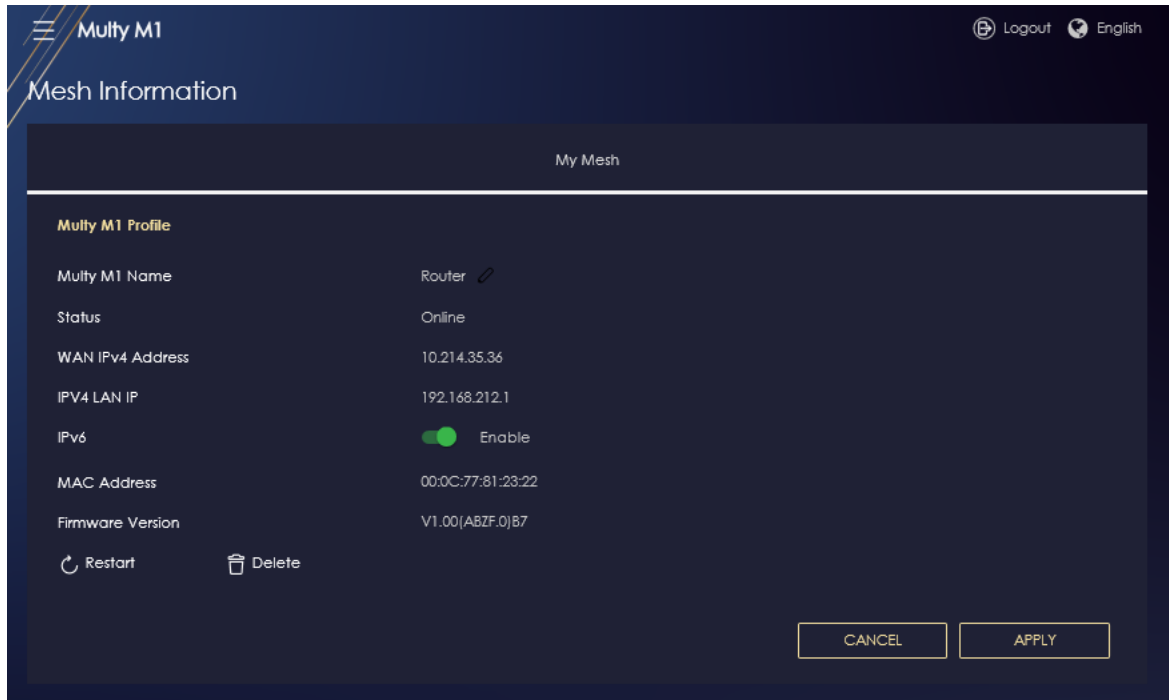


7.3 Configure the Multy Devices in a Mesh Network

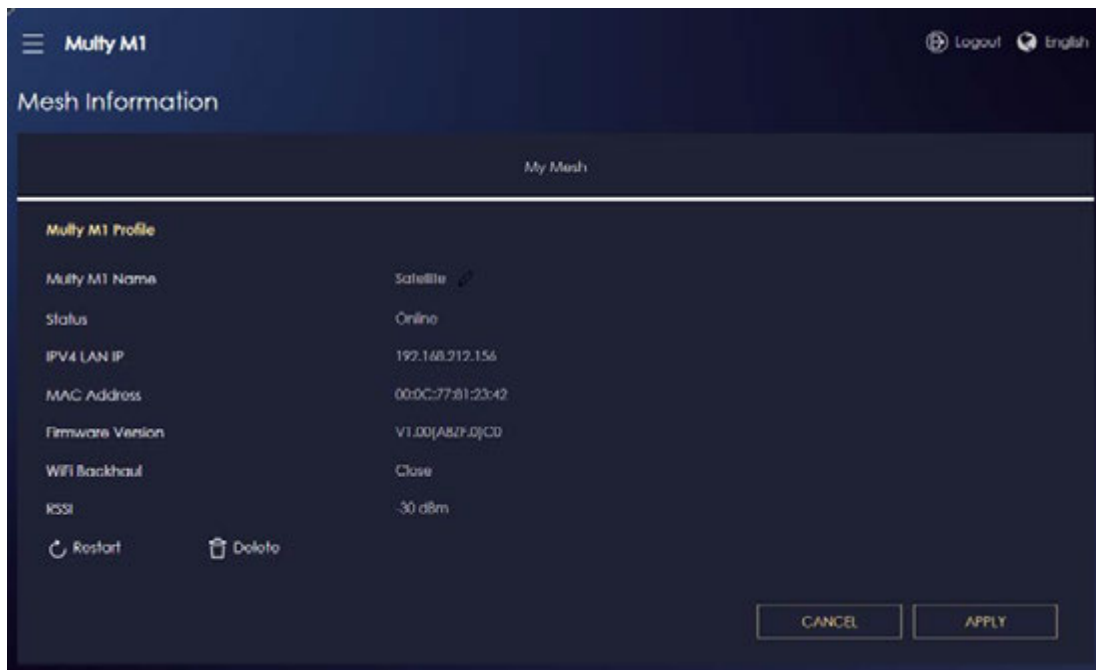
- 1 Click the **Navigation Panel** icon on the top-left corner (☰), and click **Mesh** to open the **Mesh Information** screen. Click **More** to modify the assigned roles of Multy M1's mesh networks.



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



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



7.4 Configure Main WiFi Networks

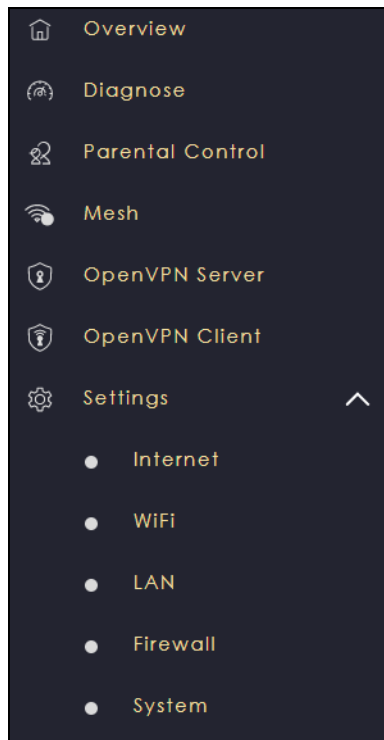
In the Multy Device you can configure independent WiFi networks with different privileges. Clients can associate only with the network for which they have security settings (SSID and password). The following table describes the different Multy Device's profile networks and their privileges.

Table 14 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)

☒ Keep 2.4G & 5G name the same

Security Mode ☒ WPA2-PSK ☐ WPA3-PSK ☐ WPA3-PSK Mix

Password

Region

2.4G Bandwidth

2.4G Channel Channel : 7

5G Bandwidth

5G Channel 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

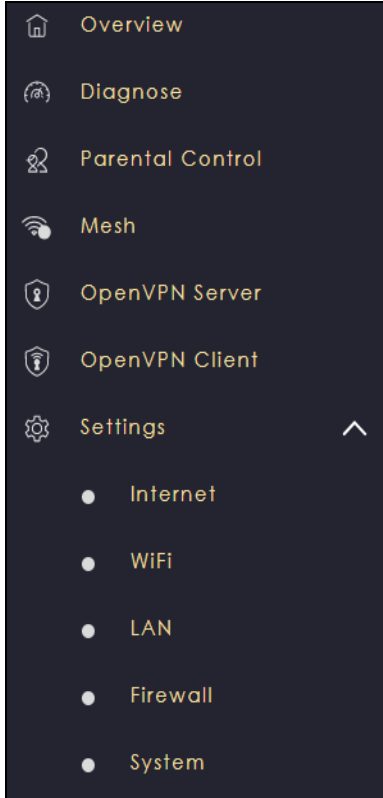
CANCEL
APPLY

7.5 Configure Guest WiFi Networks

After the Multy Device 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 Device.

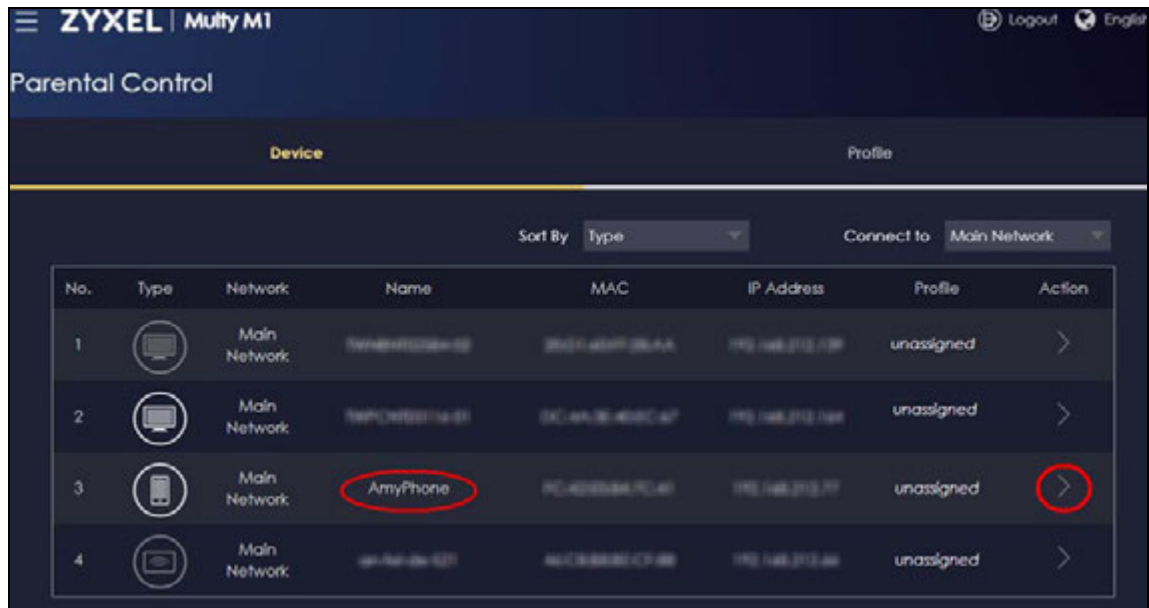
This example shows you how to block a client from accessing the Internet during time for studying. The following example uses the parameters below to configure a **Study** schedule rule.

Table 15 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 Device. Find the client you want to block then click the action icon ().



- 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

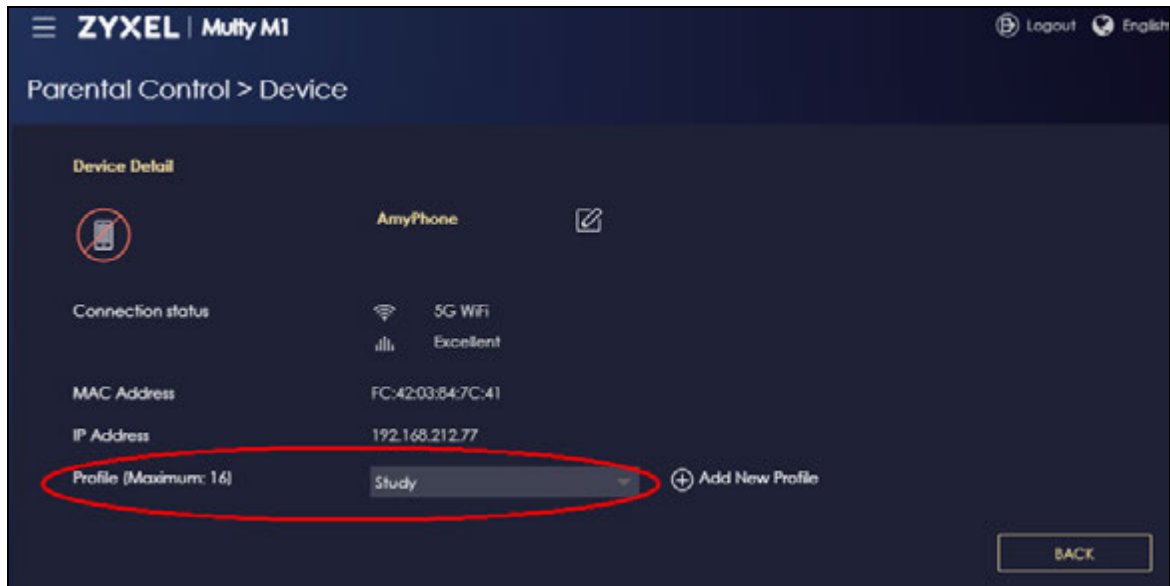
Profile Name

Scheduler Config

☐ Allow ☒ Block

	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							

- After you click **Apply**, the Multy Device 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 Device 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 Device. Enable **Firewall** to protect the Multy Device 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 Device 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 Device to not respond to Ping requests from the WAN, the attackers will not be able to find the Multy Device since they can't receive responds from it. This will prevent the Multy Device 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.

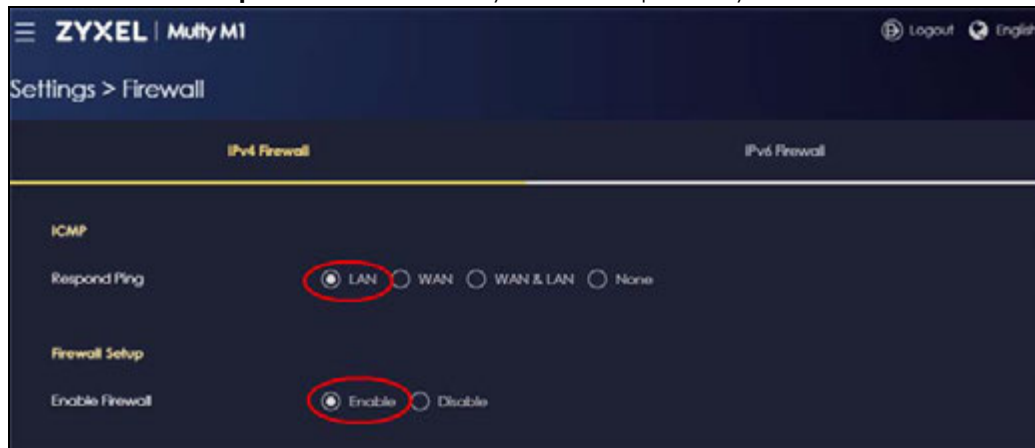
The following example uses the parameters below to configure an example Multy Device firewall rule to enable ICMP and firewall.

Table 16 Firewall Rule Example Parameters

RESPOND PING	FIREWALL SETUP
LAN	Enable

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

Set the **Firewall Setup** to **Enable**. Your Multy Device 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 17 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**.

Enable Firewall Rule

Rule Status ☒ Enable ☐ Disable

Actions ☒ Drop ☐ Accept

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

IPv4 Firewall - Add Rule

Service Name

MAC Address

Dest IP Address

Source IP Address

Dest Port Range -

Source Port Range -

- 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 Device. The following example uses the parameters below to configure the access control rule.

Table 18 Access Control Rule Example Parameters

SERVICE NAME	SOURCE IP ADDRESS	ACTIONS
Ads Website	1.1.1.1	Drop

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

Enable Firewall Rule

Rule Status ☒ Enable ☐ Disable

Actions ☒ Drop ☐ Accept

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

IPv4 Firewall - Add Rule

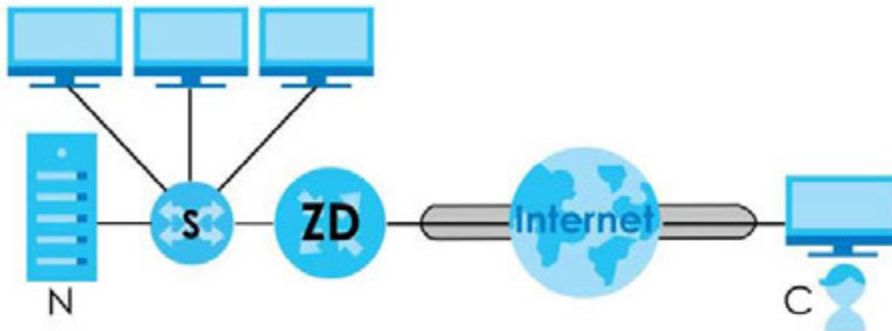
Service Name	Ads Website	
MAC Address		
Dest IP Address		
Source IP Address	1.1.1.1	
Dest Port Range		-
Source Port Range		-

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

7.8 Configure the Multy Device 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 54 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.

The example below shows you how to set up your Multy Device 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 19 OpenVPN Server Example Parameters

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

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

Internet Connection NAT & Port Forwarding Passthrough **Dynamic DNS** UPnP

Dynamic DNS

Dynamic DNS ☒ Enable ☐ Disable

Service Provider

Host Name

User Name

Password ⓘ

DNS maps a domain name to a corresponding IP address and vice versa. Similarly, Dynamic DNS (DDNS) maps a domain name to a dynamic IP address. With DDNS, you can use a domain name to access your ZyXEL device and home network regardless of the device's current (dynamic) IP address. The ZyXEL device must have a public WAN IP address to use Dynamic DNS.

- 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.

No.	Username	Client Access Allowed	Actions
1	PM	WAN	[Icons]
2	RD	WAN	[Icons]

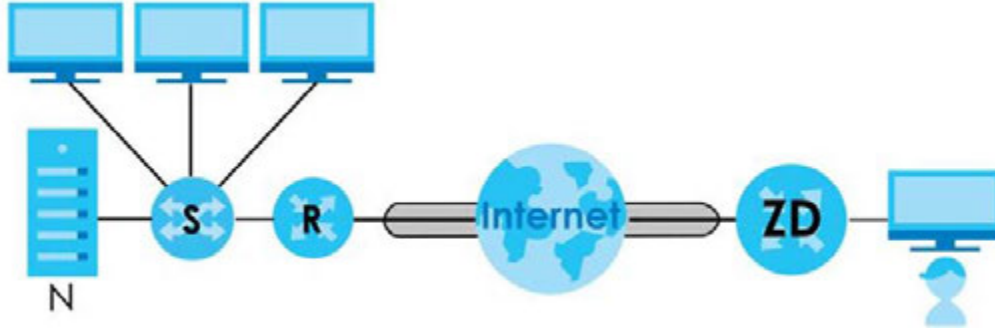
7.9 Configure the Multy Device as an OpenVPN Client

You are 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 Device 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 Device. The Multy Device can only connect to one server at a time.

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

Figure 55 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.

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

Table 20 OpenVPN Client Example Parameters

DESCRIPTION	USER NAME	PASSWORD
Japan Gaming	TaiwanPlayer	1234

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

OpenVPN Server List - Add Rule

Description: Japan Gaming

User Name: TaiwanPlayer

Password:

Import .ovpn file: Choose File No file chosen

Enable VPN on: ☒ All ☒ LAN ☒ WIFI 2.4G ☒ WIFI 5G

CANCEL APPLY

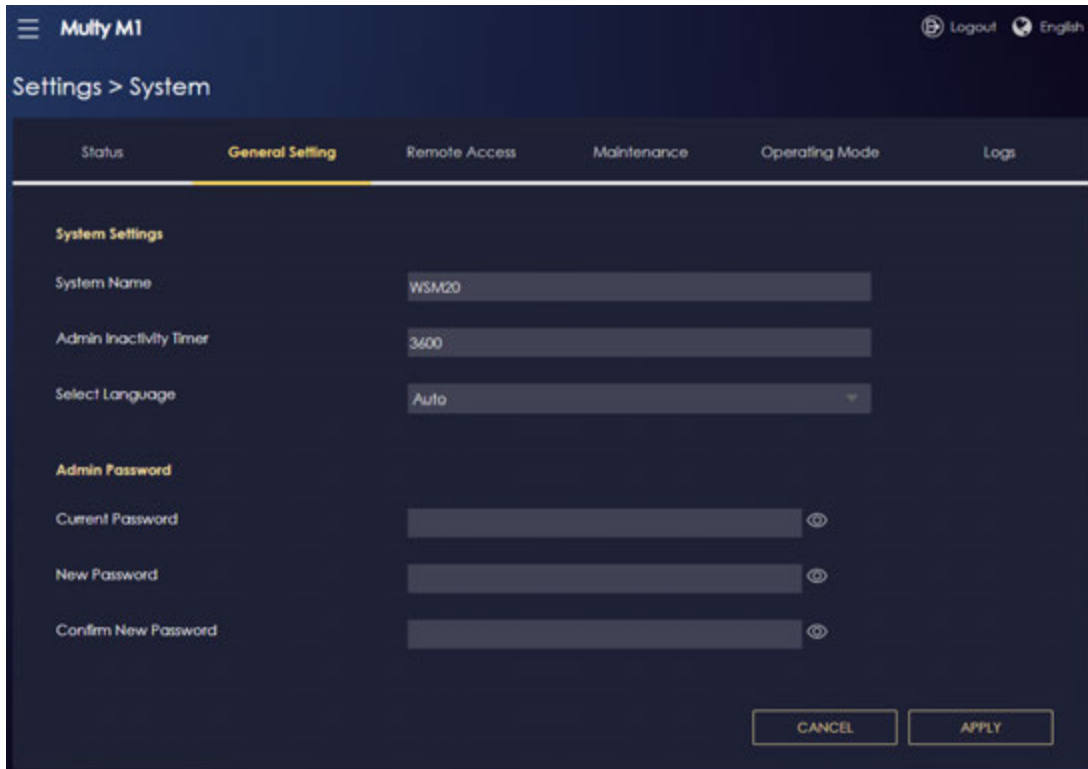
- 2 Request for an .ovpn file from the OpenVPN server your Multy Device will connect to and import it. The file should include the OpenVPN server settings.

- 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.



The screenshot displays the Multy M1 web interface. The top navigation bar includes a menu icon, 'Multy M1', and links for 'Logout' and 'English'. The main heading is 'Settings > System'. Below this is a tabbed interface with 'General Setting' selected. The 'General Setting' tab contains two sections: 'System Settings' and 'Admin Password'. 'System Settings' includes 'System Name' (WSM20), 'Admin Inactivity Timer' (3600), and 'Select Language' (Auto). 'Admin Password' includes three password fields: 'Current Password', 'New Password', and 'Confirm New Password', each with a visibility icon. At the bottom right are 'CANCEL' and 'APPLY' buttons.

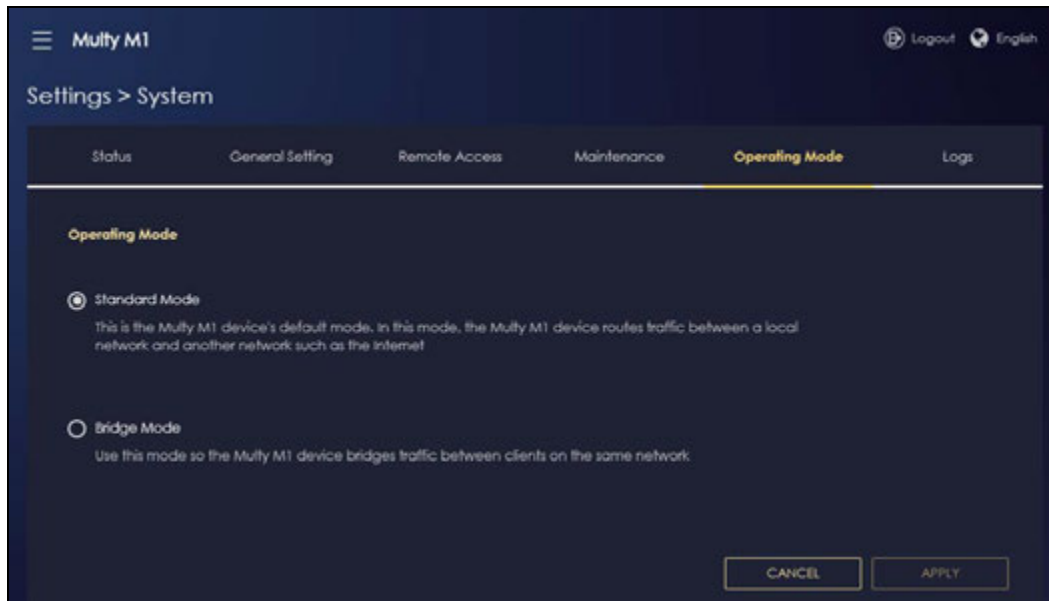
7.11 Change the Operating Mode

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

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

Note: Parental Control, UPnP, and 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 Device's operating mode may take up to 2 minutes.

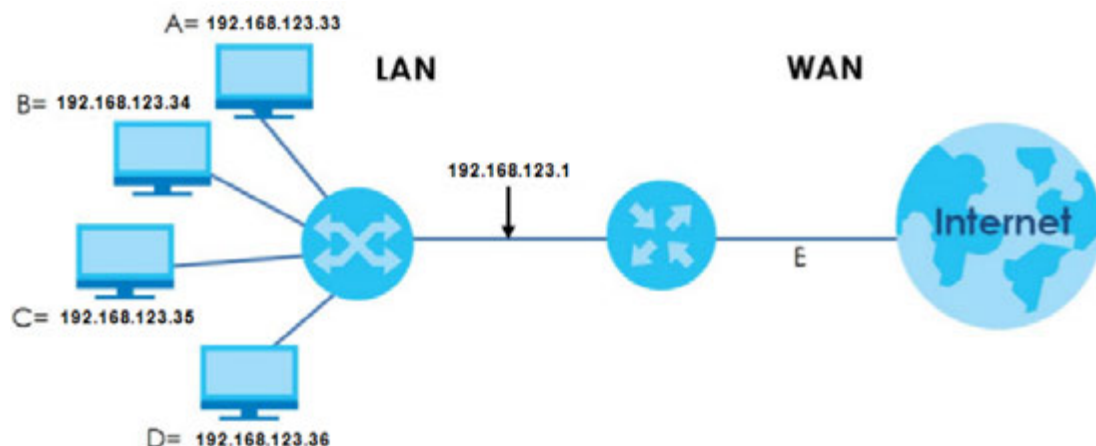


7.12 Configure a Port Forwarding Rule

If you want to forward incoming packets to a specific IP address in the private network using ports, set a port forwarding rule. In the following example figure, the ISP assigns the IP address (E).

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

Figure 56 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.

Multy M1

Settings > Internet

Internet Connection **NAT & Port Forwarding** Passthrough Dynamic DNS UPnP

NAT & Port Forwarding

Network Address Translation (NAT) ☒ Enable ☐ Disable

Server Setup ☒ Default Server - 192.168.212.1 ☐ Change to Server

TWPCNT03139-02

Port Forwarding Rule (The maximum number of rules is 32.)

Enable Port Forwarding ☐ Enable ☒ Disable

+ Add Rule

No.	Name	Protocol	External Port	Server IP Address	Internal Port	Actions
-----	------	----------	---------------	-------------------	---------------	---------

CANCEL APPLY

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

Port Forwarding Rule (The maximum number of rules is 32.)

Enable Port Forwarding ☒ Enable ☐ Disable

- 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 ports.

Add Port Forwarding Rule

Service Name Email(SMTP)

Protocol TCP

External Port 25

Device List TWPCNT03139-02 (192.168.212.53)

Internal Port 25

CANCEL APPLY

PART III

Multy Plus

CHAPTER 8

Web Interface Tutorials – Multy Plus (WSQ60)

8.1 Introduction

This section provides tutorials for setting up your Multy Device.

- [Using the Web Configurator](#)
- [Add and Install Your First Multy Device](#)
- [Run a Speed Test](#)
- [Configure the Multy Device'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 Device's LED \(Light\)](#)
- [Remove a Multy Device](#)
- [Install a Second Multy WiFi System](#)
- [Change Your Multy Device Operating Mode](#)
- [Configure a Port Forwarding Rule](#)
- [Enable or Disable Daisy Chain Network Topology](#)
- [Local Login Password Change](#)

8.2 Using the Web Configurator

The Web Configurator is an HTML-based management interface that allows easy device setup and management through Internet browser. Zyxel Multy Plus Web Configurator helps you install Multy Devices and manage the Multy WiFi System directly.

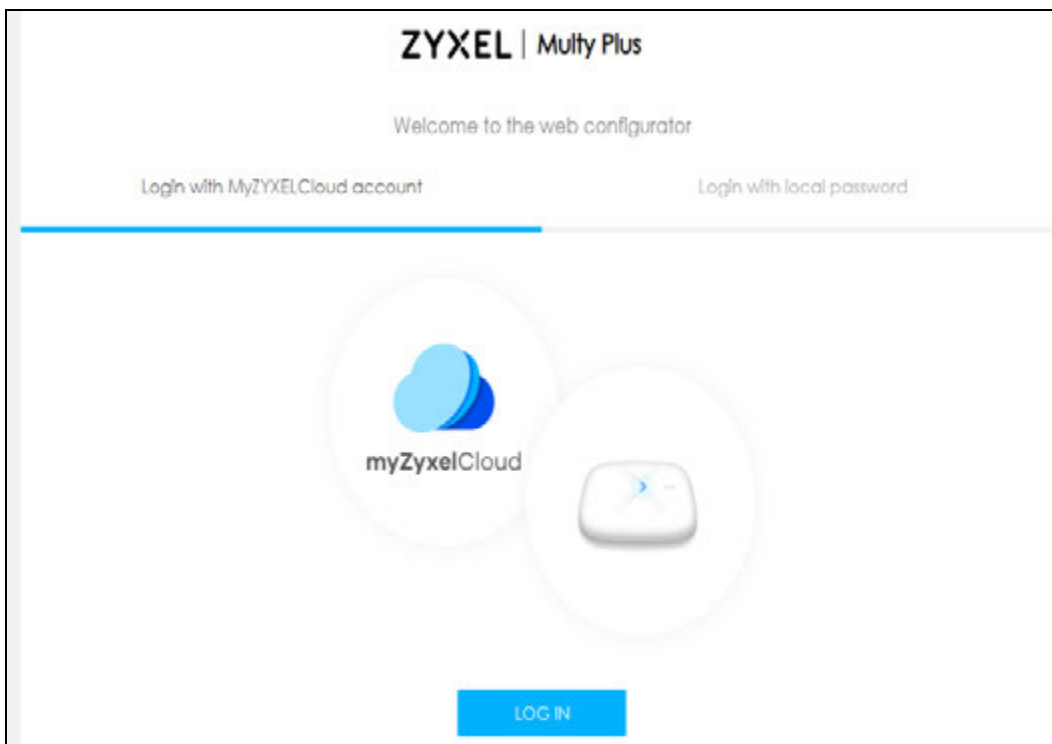
Compatibility

- Microsoft Edge
- Google Chrome, versions 2.0 and later
- Mozilla Firefox, versions 3.0 and later
- Safari, versions 2.0 and later

With a myZyxeCloud account, all your configurations will be stored in the myZyxeCloud server. You then can log in and use Web Configurator to manage your Multy WiFi System. Moreover, the Multy Devices can work with Amazon Alexa after the myZyxeCloud account is linked to Alexa ([Section 3.30 on page 123](#)).

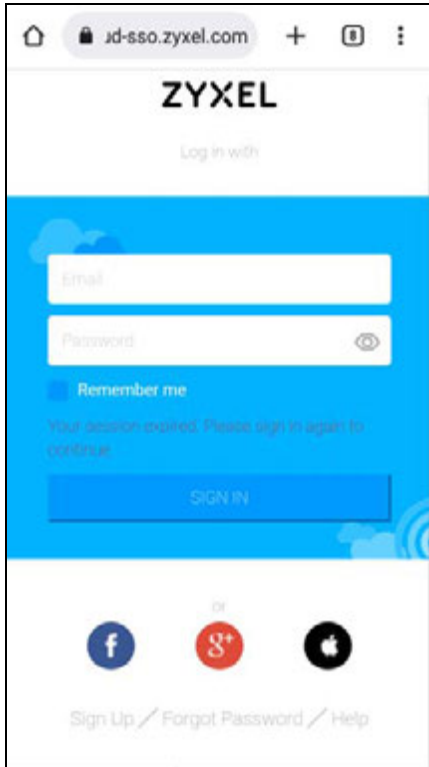
- 1 Make sure your Multy Device hardware is properly connected (refer to the Quick Start Guide).
- 2 Launch your web browser and go to <http://Zyxelwifi.com> or <http://Zyxelwifi.net>.

The login screen displays. To access the Web Configurator and manage the Multy Device you need to be connected to your myZyxeCloud account. Click **Login with MyZYXELCloud account** and you will be redirected to the myZyxeCloud website to log into your myZyxeCloud account. Or click **Login with local password** if you do not wish to access the myZyxeCloud account. For more information see [Section 8.2.1 on page 173](#).



- 3 Enter your myZyxeCloud account **Email** and **Password**, and click **SIGN IN**. Alternatively, you can log out. If you do not have any Internet Access you will be redirected to the Multy Device Wizard to add your first Multy. For more information see [Section 8.3 on page 175](#).

Note: If you do not have a myZyxeCloud account, click **Sign Up** to create one. You need to register the Multy Device in your myZyxeCloud account before you can access its Web Configurator. Likewise, the option **Login with local password** will only appear after you have set up a myZyxeCloud account (mandatory).



You are redirected back to the Multy Device Web Configurator.

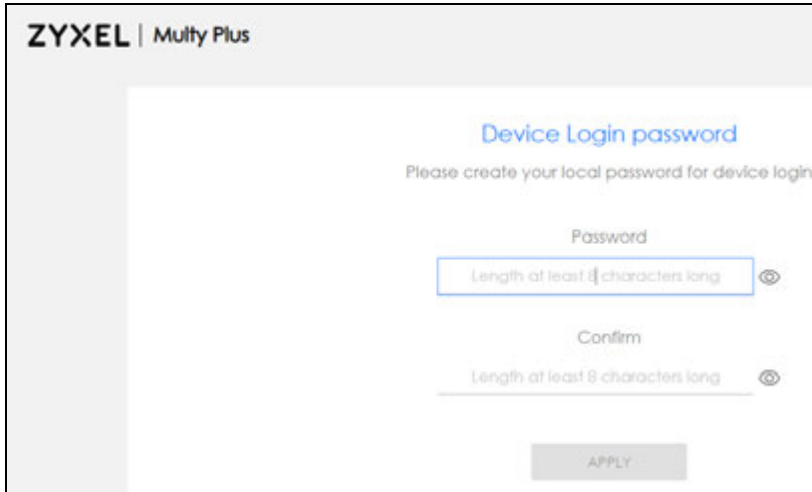
8.2.1 Login with Local Password

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

- 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.



ZYXEL | Multy Plus

Device Login password

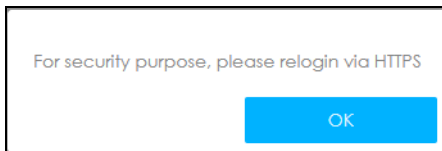
Please create your local password for device login

Password
Length at least 8 characters long

Confirm
Length at least 8 characters long

APPLY

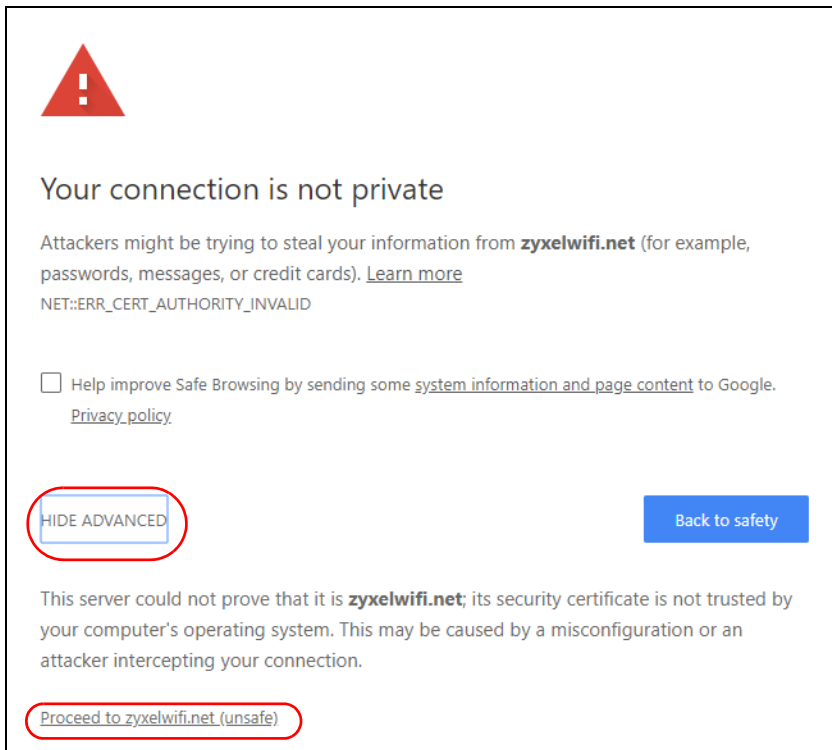
- 4 Just click **OK** to continue.



For security purpose, please relogin via HTTPS

OK

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



! Your connection is not private

Attackers might be trying to steal your information from **zyxelwifi.net** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

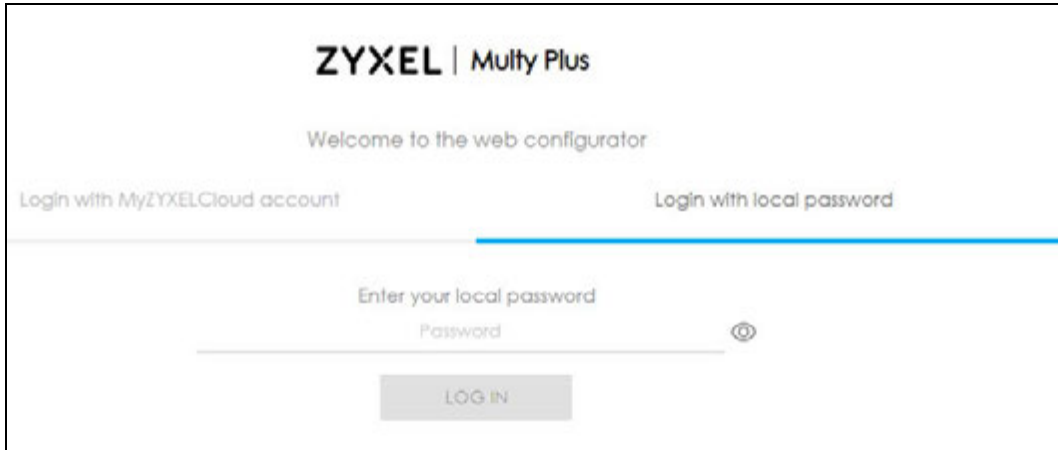
☐ Help improve Safe Browsing by sending some [system information and page content](#) to Google. [Privacy policy](#)

HIDE ADVANCED **Back to safety**

This server could not prove that it is **zyxelwifi.net**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

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**.



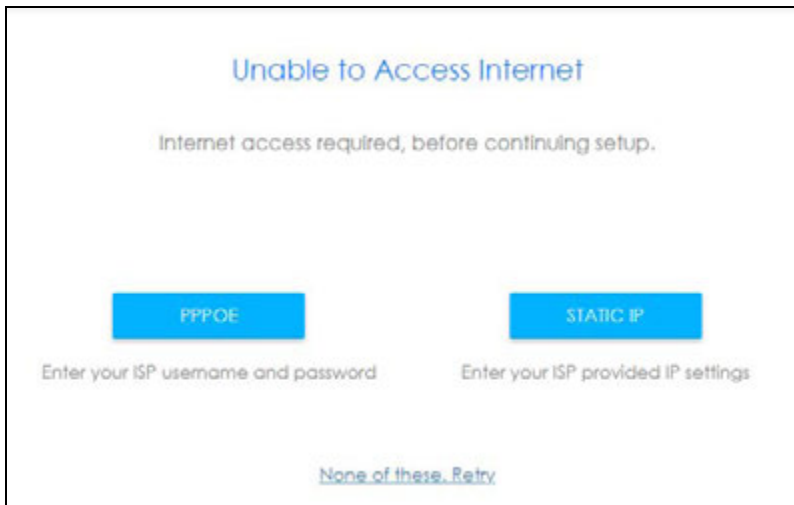
The image shows the ZYXEL Multy Plus login interface. At the top, it says "ZYXEL | Multy Plus". Below that, it says "Welcome to the web configurator". There are two login options: "Login with MyZYXELCloud account" and "Login with local password". The "Login with local password" option is selected, indicated by a blue underline. Below this, there is a text input field labeled "Enter your local password" and "Password". To the right of the input field is a small circular icon with a question mark. Below the input field is a "LOG IN" button.

- 7 Then click **LOG IN**.

8.3 Add and Install Your First Multy Device

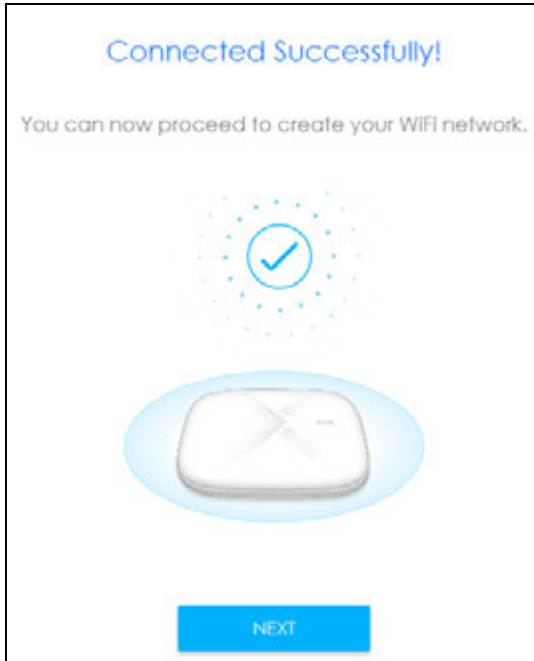
You need to install at least one Multy Device before you can manage the Multy WiFi System.

- 1 If your modem or router has DHCP enabled, the Multy Device 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.



The image shows a screen titled "Unable to Access Internet". Below the title, it says "Internet access required, before continuing setup." There are two blue buttons: "PPPOE" and "STATIC IP". Below the "PPPOE" button, it says "Enter your ISP username and password". Below the "STATIC IP" button, it says "Enter your ISP provided IP settings". At the bottom, there is a link that says "None of these, Retry".

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

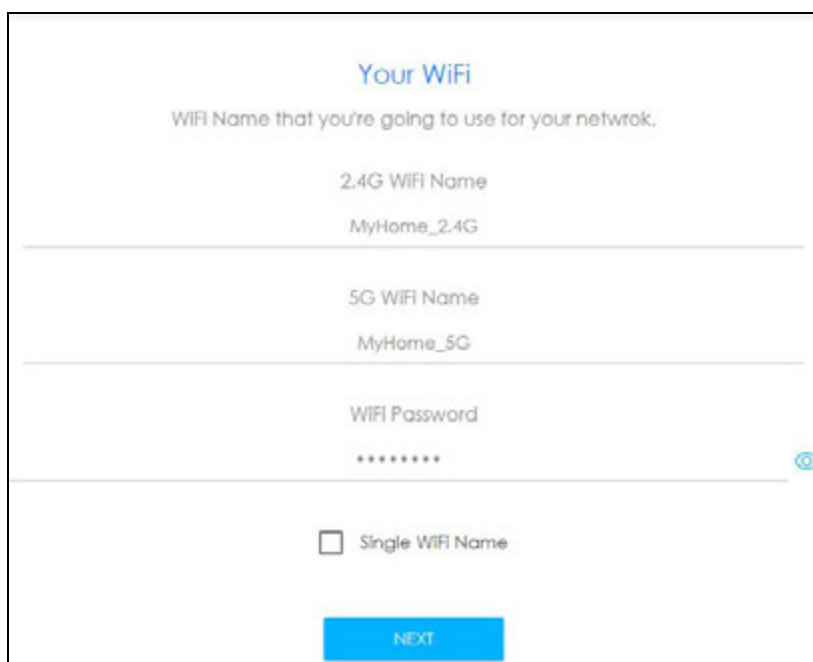


- 3 Select the location/name where you want to place your Multy Device, click **Next** and follow the on-screen instructions.



- 4 Enter the **WiFi Name** and password for your Multy 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 Device adds **.speed** to the end of the 5G WiFi Name.



Your WiFi

WiFi Name that you're going to use for your network.

2.4G WiFi Name
MyHome_2.4G

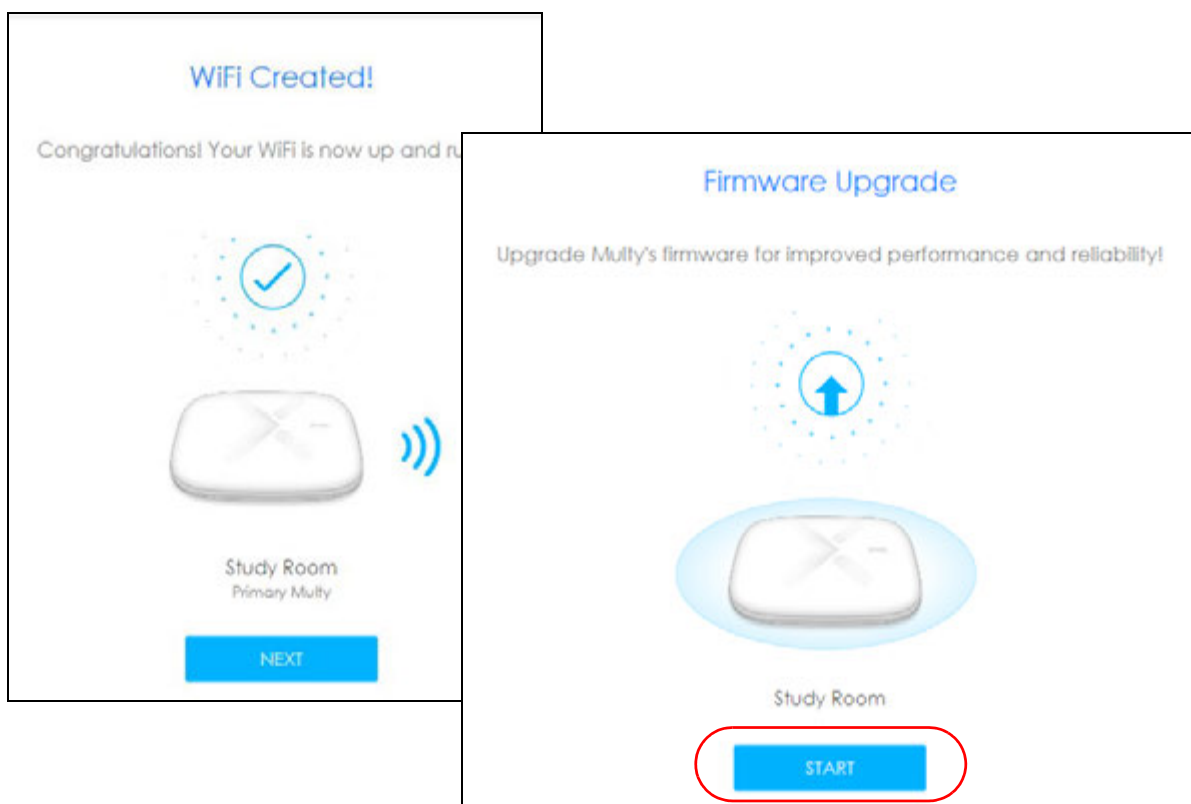
5G WiFi Name
MyHome_5G

WiFi Password

☐ Single WiFi Name

NEXT

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



WiFi Created!

Congratulations! Your WiFi is now up and running.

Study Room
Primary Multy

NEXT

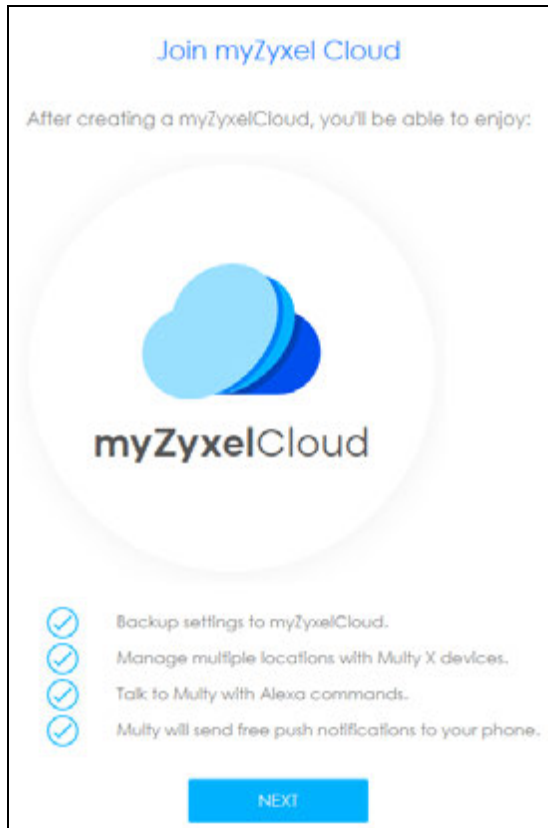
Firmware Upgrade

Upgrade Multy's firmware for improved performance and reliability!

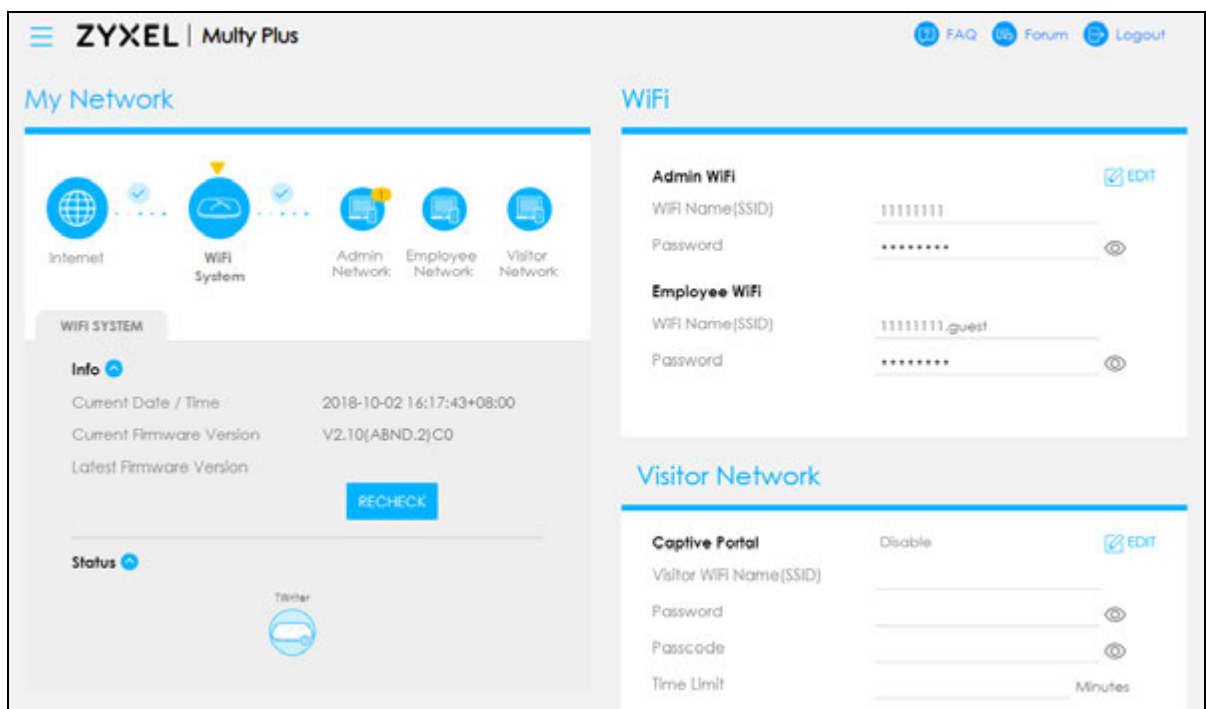
Study Room

START

- 6 Click **Next** to be redirected to the myZyxeCloud website. Sign up or log in with your myZyxeCloud account, so you can complete the Multy Device installation, and access its Web Configurator.



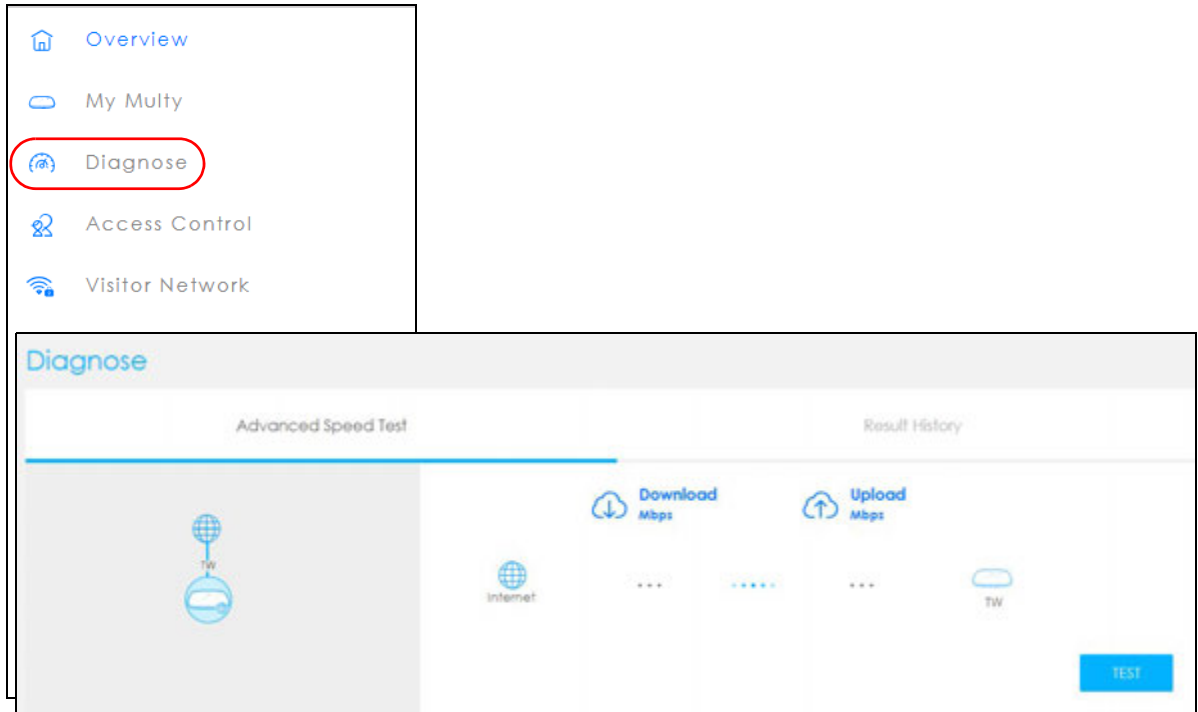
- 7 The Multy WiFi System **Overview** screen displays allowing you to monitor your Multy Devices and Multy WiFi System. It shows if the Multy Devices in this Multy WiFi System are online, and how many WiFi clients are currently connected to each Multy Device, as well as their upstream/downstream data rates. For more information see [Table 21 on page 180](#) for WiFi Network Privileges.



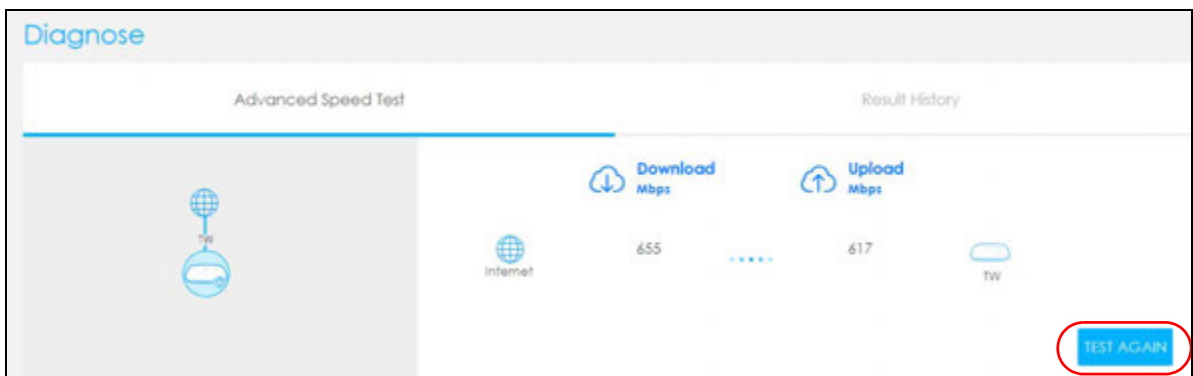
8.4 Run a Speed Test

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

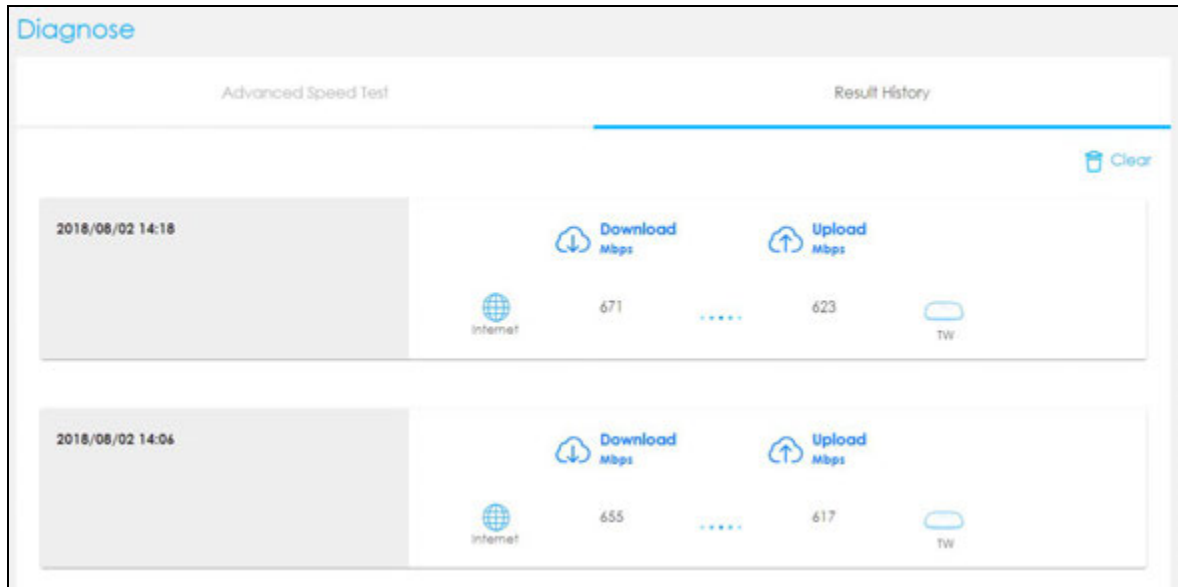
- 1 Click the Navigation Panel icon on the top-left corner (), and click **Diagnose** to open the **Advanced Speed Test** screen. Use this screen to view all the available connections in your Multy WiFi System.



- 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 Device's WiFi Networks

In the The Multy WiFi System you can configure independent WiFi 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 Device's profile networks and their privileges.

Table 21 WiFi Network Privileges

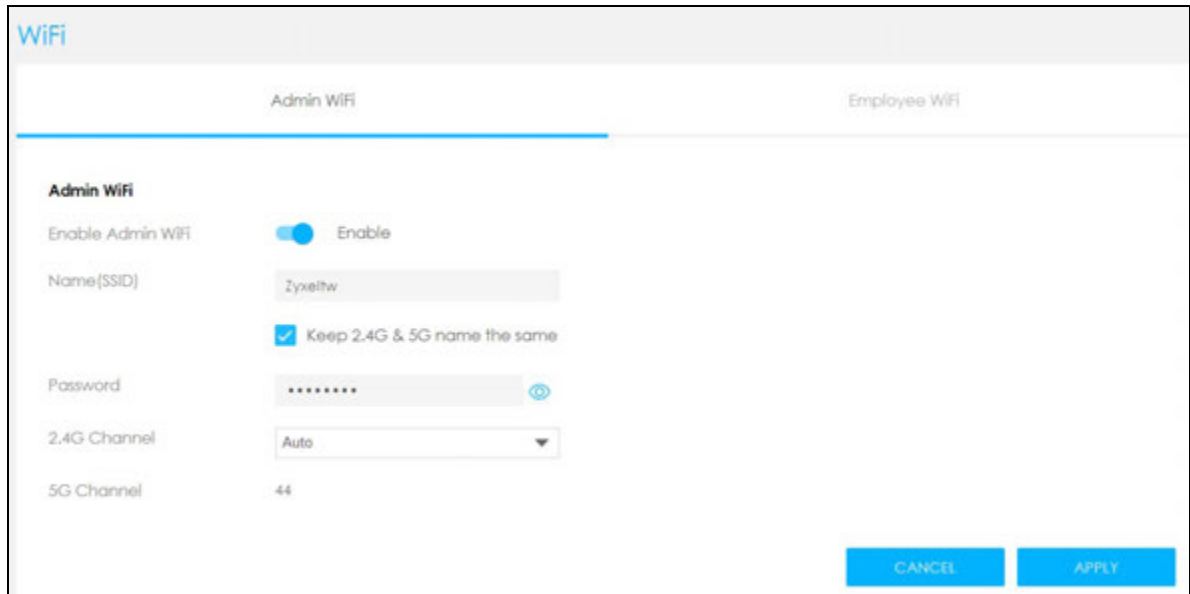
WIFI NETWORK	INTERNET ACCESS	2.4G / 5G WIFI NETWORK	ACCESS TO WEB CONFIGURATOR	ACCESS TO WIRED LAN
Admin WiFi	Yes	2.4G and 5G	Yes	Yes
Employee WiFi	Yes	2.4G and 5G	No	No
Visitor WiFi	Yes, after captive portal log in.	2.4G and 5G	No	No

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.

The screenshot displays the Multy Plus web interface. On the left, a sidebar menu lists various system functions: Overview, My Multy, Diagnose, Access Control, Visitor Network, Settings, Internet, and WiFi. The 'WiFi' option is highlighted with a red circle. The main content area is titled 'WiFi' and features two tabs: 'Admin WiFi' and 'Employee WiFi'. The 'Admin WiFi' tab is currently selected, showing configuration options for the Admin WiFi network. These options include a toggle for 'Enable Admin WiFi' (set to 'Enable'), a text field for 'Name (SSID)' containing 'Zyxelhw', a checked checkbox for 'Keep 2.4G & 5G name the same', a password field with masked characters, a dropdown for '2.4G Channel' set to 'Auto', and a field for '5G Channel' set to '44'. At the bottom right of the configuration area are 'CANCEL' and 'APPLY' buttons.

- 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.



The screenshot displays the 'WiFi' configuration page with two tabs: 'Admin WiFi' (selected) and 'Employee WiFi'. Under the 'Admin WiFi' tab, the 'Enable Admin WiFi' toggle is turned on. The 'Name (SSID)' field contains 'Zyxelhw'. The 'Keep 2.4G & 5G name the same' checkbox is checked. The 'Password' field is masked with dots. The '2.4G Channel' is set to 'Auto' and the '5G Channel' is set to '44'. 'CANCEL' and 'APPLY' buttons are at the bottom right.

8.6 Enable or Disable a WiFi Network

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

The screenshot shows the Multy Plus web interface. On the left, a sidebar menu contains the following items: Overview, My Multy, Diagnose, Access Control, Visitor Network, Settings, Internet, and WiFi. The WiFi item is highlighted with a red circle. The main content area displays the WiFi settings page, which is divided into two tabs: Admin WiFi and Employee WiFi. The Admin WiFi tab is currently selected. The Admin WiFi configuration includes the following fields: Enable Admin WiFi (a toggle switch set to 'Enable'), Name (SSID) (a text field containing 'Zyxelhw'), Keep 2.4G & 5G name the same (a checked checkbox), Password (a masked text field with a strength indicator), 2.4G Channel (a dropdown menu set to 'Auto'), and 5G Channel (a text field containing '44'). At the bottom right of the Admin WiFi section are 'CANCEL' and 'APPLY' buttons.

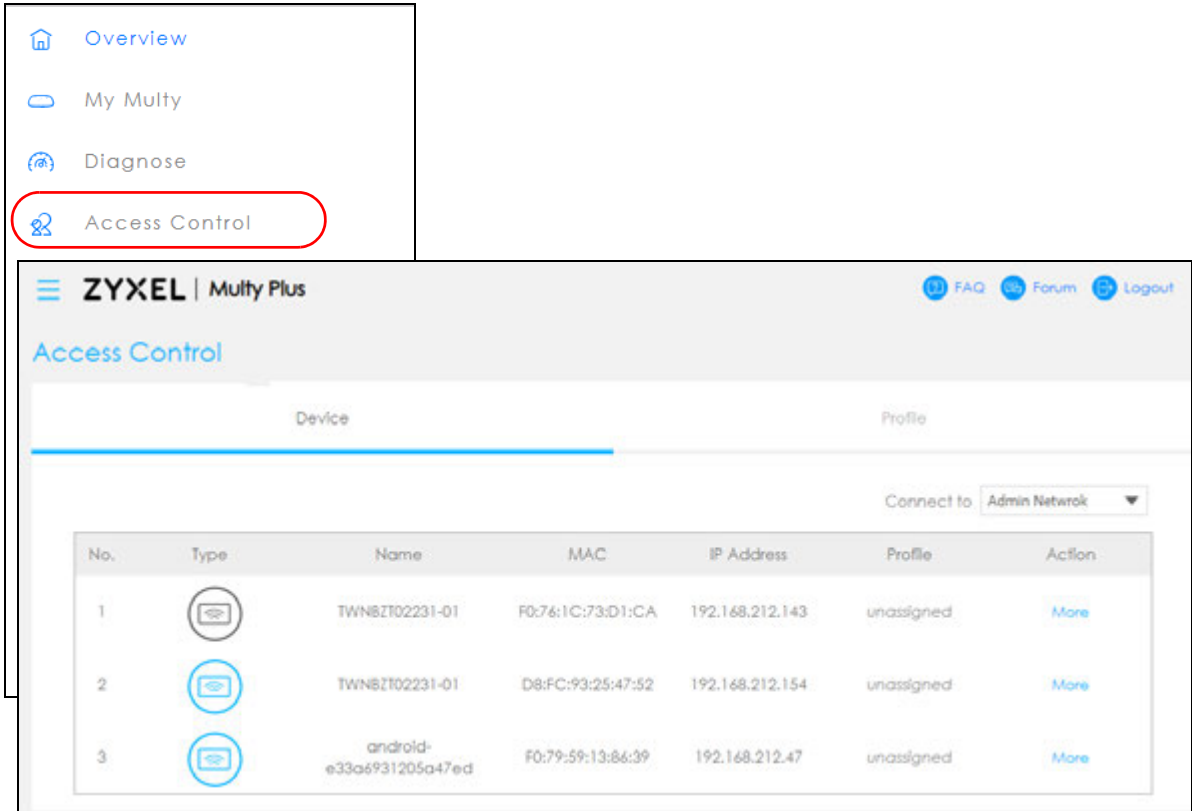
- 2 **Enable Employee WiFi** and enter the **WiFi Name (SSID)** and **WiFi Password**. Click **APPLY** to save your changes.

The screenshot shows the Multy Plus web interface with the Employee WiFi tab selected. The Employee WiFi configuration includes the following fields: Enable Employee WiFi (a toggle switch set to 'Disable', highlighted with a red circle), Name (SSID) (a text field containing 'EmployeeWiFi'), and Password (a masked text field with a strength indicator). At the bottom right of the Employee WiFi section are 'CANCEL' and 'APPLY' buttons.

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 WiFi System. Specify which network you want to view in the **Connect to** drop-down list.

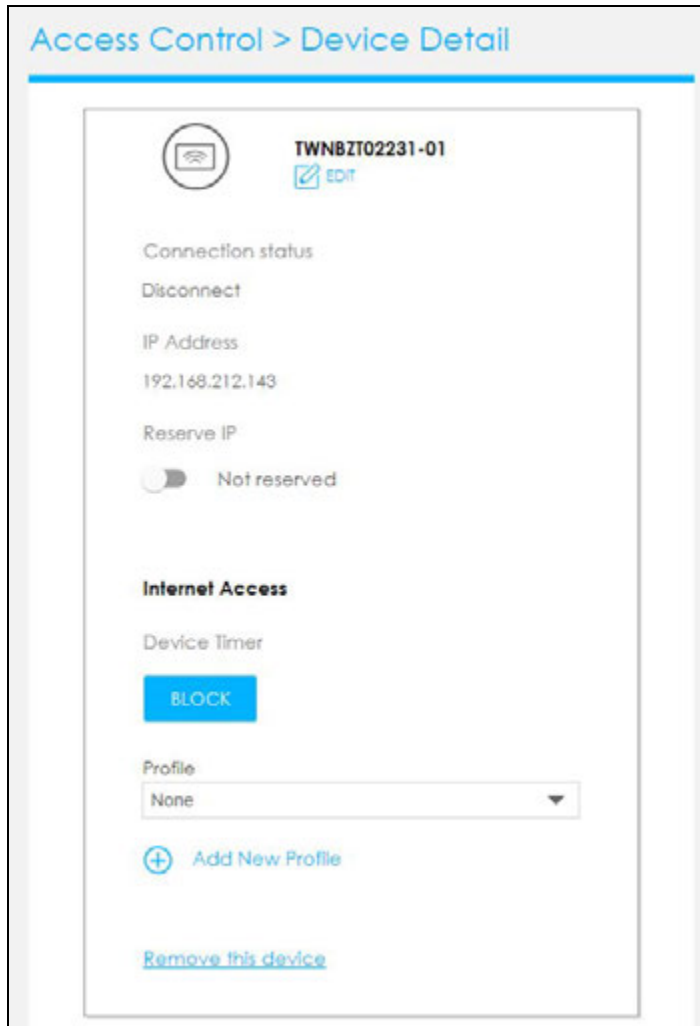


The screenshot shows the ZYXEL Multy Plus web interface. On the left, a navigation panel lists 'Overview', 'My Multy', 'Diagnose', and 'Access Control', with 'Access Control' highlighted by a red circle. The main area is titled 'Access Control' and has tabs for 'Device' (selected) and 'Profile'. A 'Connect to' dropdown menu is set to 'Admin Network'. Below this is a table of connected devices.

No.	Type	Name	MAC	IP Address	Profile	Action
1		TWN8T02231-01	F0:76:1C:73:D1:CA	192.168.212.143	unassigned	More
2		TWN8T02231-01	D8:FC:93:25:47:52	192.168.212.154	unassigned	More
3		android-e33a6931205a47ed	F0:79:59:13:86:39	192.168.212.47	unassigned	More

- 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**.

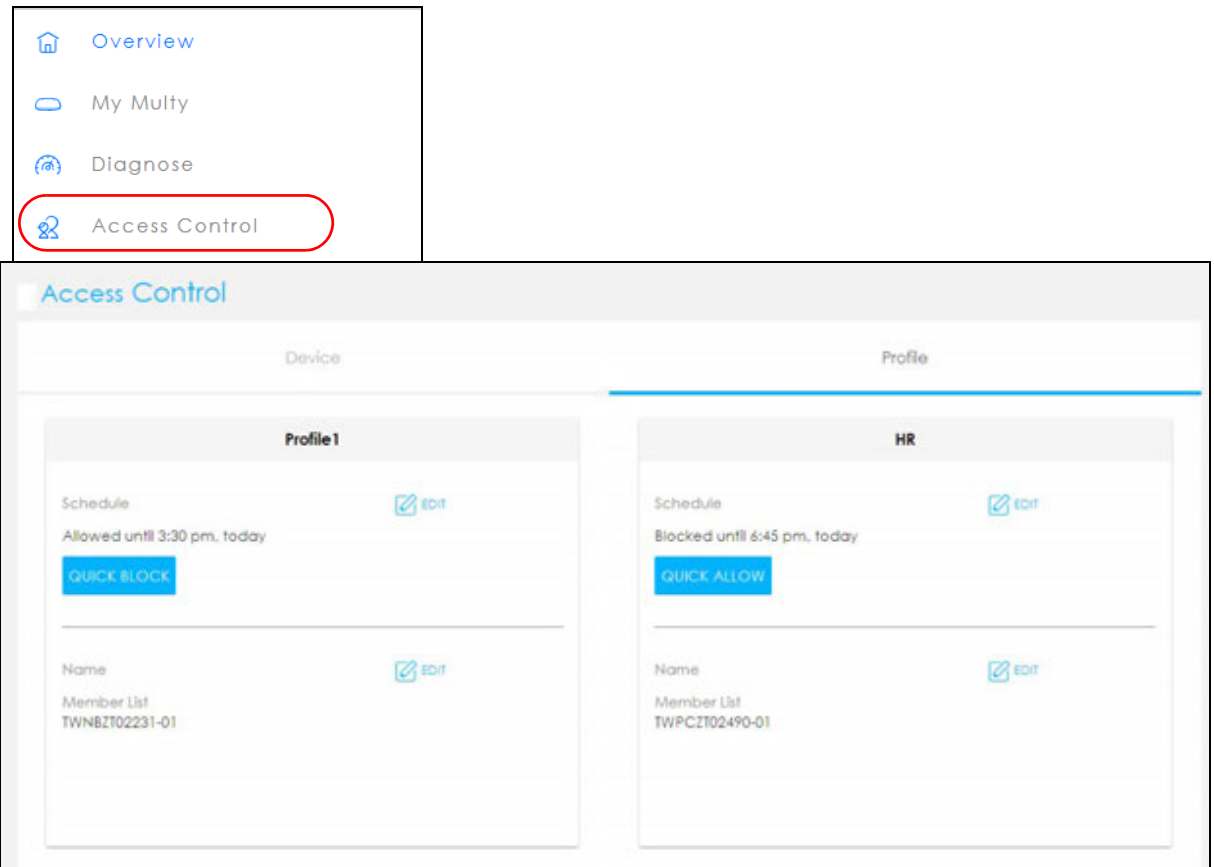
You can also activate **Reserve IP**, so the Multy Device assigns a specific IP address to a device every time it connects to the Multy WiFi System. For more information on adding/editing new profiles, see [Section 8.8 on page 185](#).



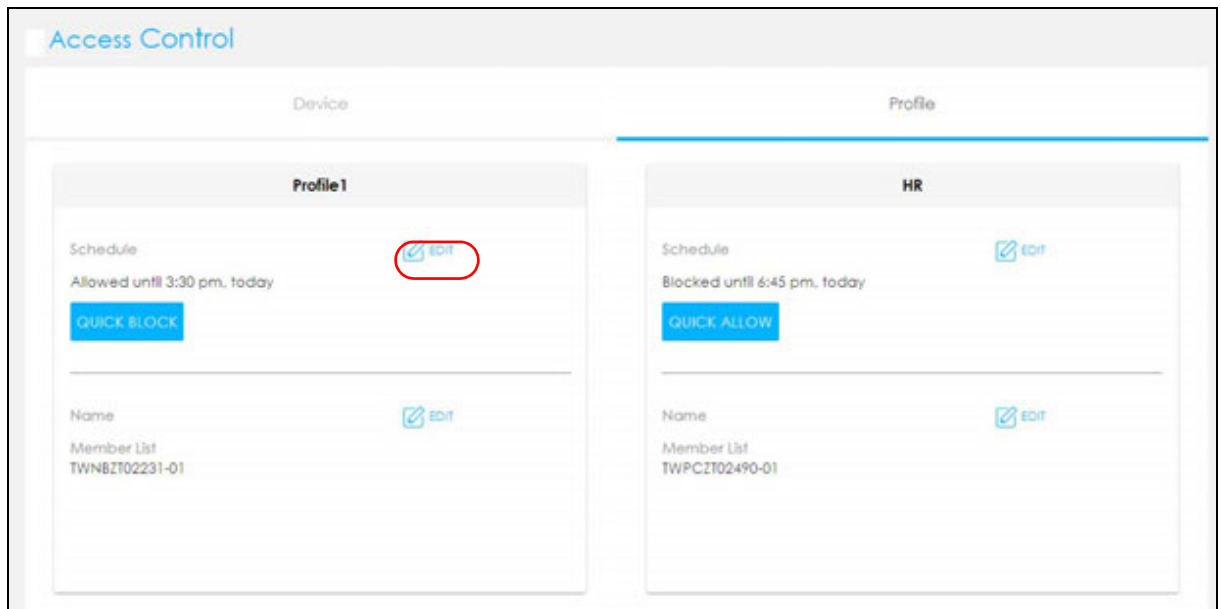
8.8 Set a Profile's WiFi Schedule

When you create or edit a profile, you can schedule the Multy 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 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.

Access Control > Scheduler Config

Enable schedule ☒ Enable

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
00							
01		Block	Block	Block	Block	Block	
02		Block	Block	Block	Block	Block	
03		Block	Block	Block	Block	Block	
04		Block	Block	Block	Block	Block	
05		Block	Block	Block	Block	Block	
06		Block	Block	Block	Block	Block	
07		Block	Block	Block	Block	Block	
08		Block	Block	Block	Block	Block	
09		Block	Block	Block	Block	Block	
10		Block	Block	Block	Block	Block	
11		Block	Block	Block	Block	Block	
12		Block	Block	Block	Block	Block	
13		Block	Block	Block	Block	Block	
14		Block	Block	Block	Block	Block	
15		Block	Block	Block	Block	Block	
16		Block	Block	Block	Block	Block	
17		Block	Block	Block	Block	Block	
18		Block	Block	Block	Block	Block	
19		Block	Block	Block	Block	Block	
20		Block	Block	Block	Block	Block	
21		Block	Block	Block	Block	Block	
22							
23							
24							

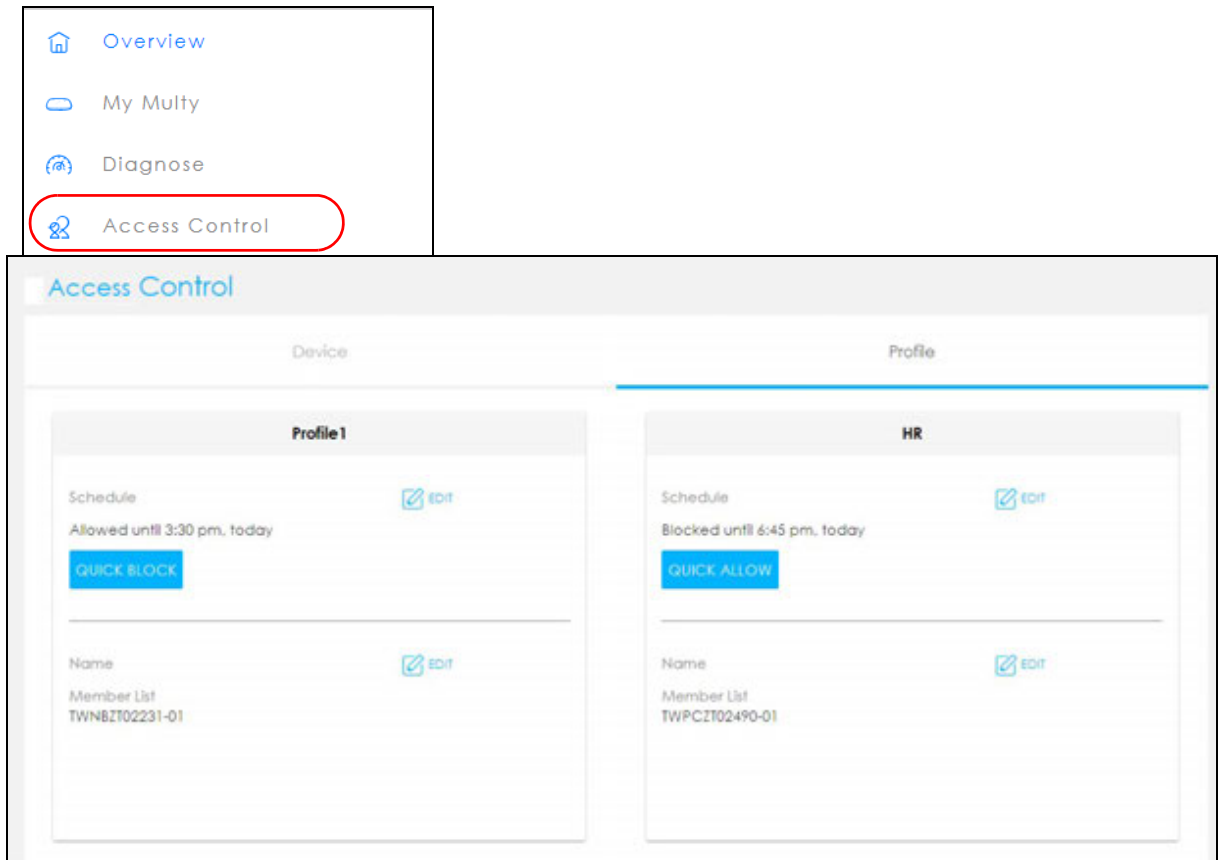
☐ Allow ☒ Block

[Select All](#) [Deselect All](#)

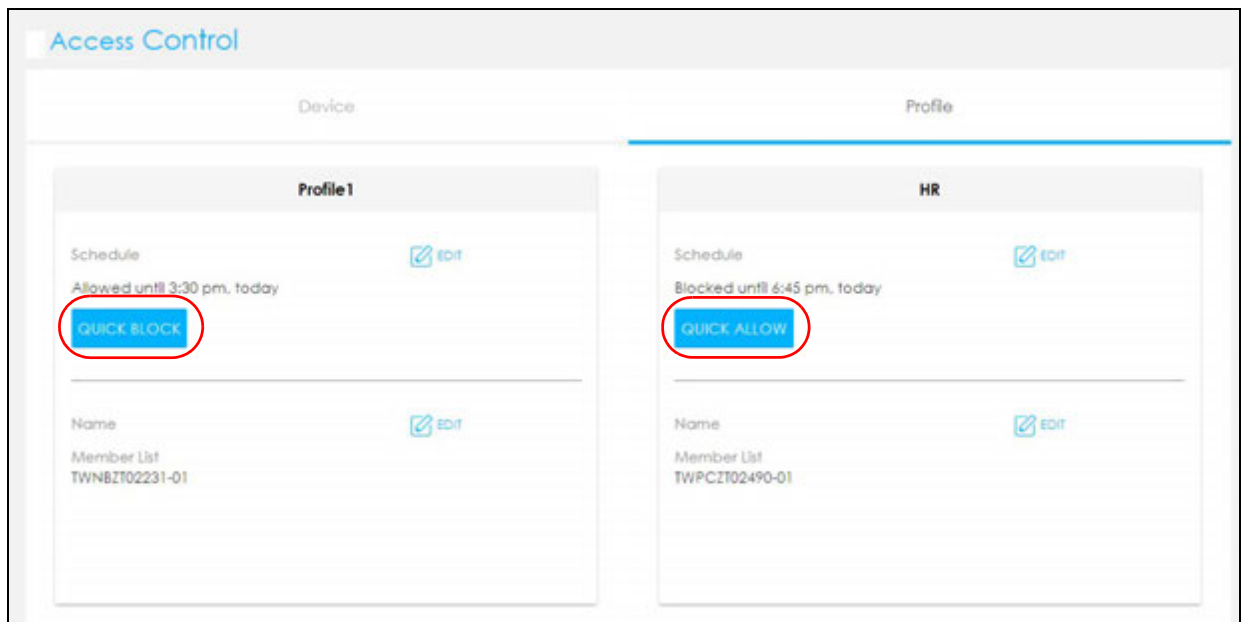
8.9 Pause or Resume Internet Access on a Profile

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 WiFi System.

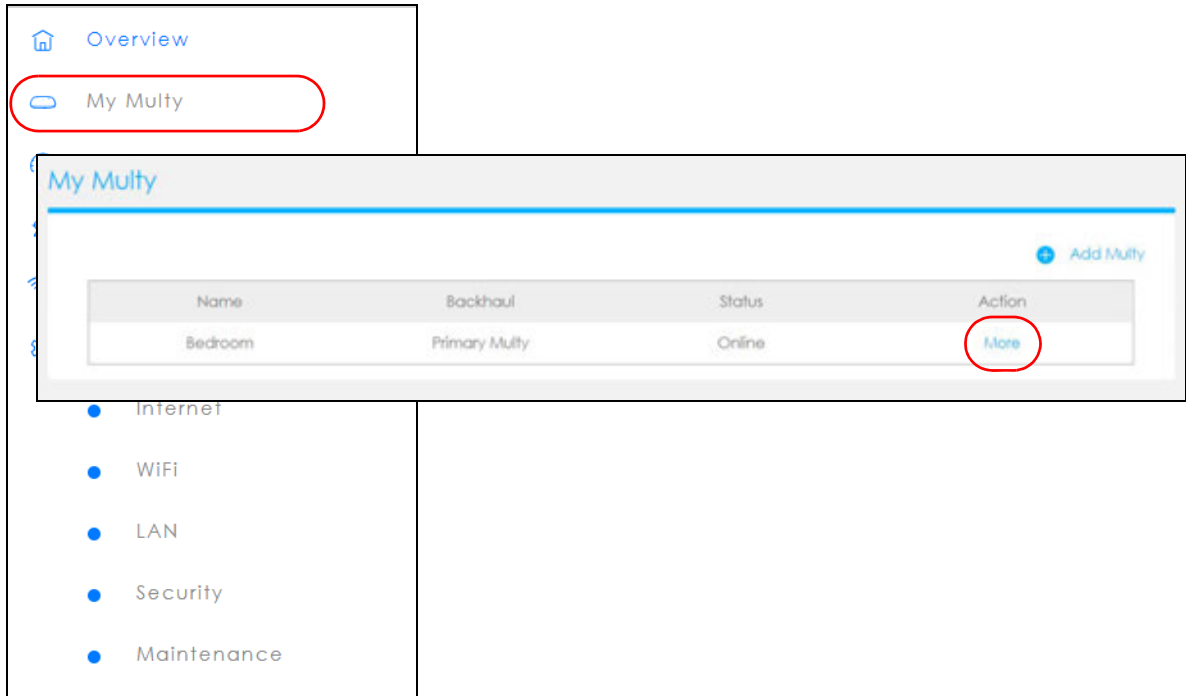


- 2 Click a profile's **Quick Allow** button to resume network access at once, or click the **Quick Block** button to pause Internet access for that specific profile.

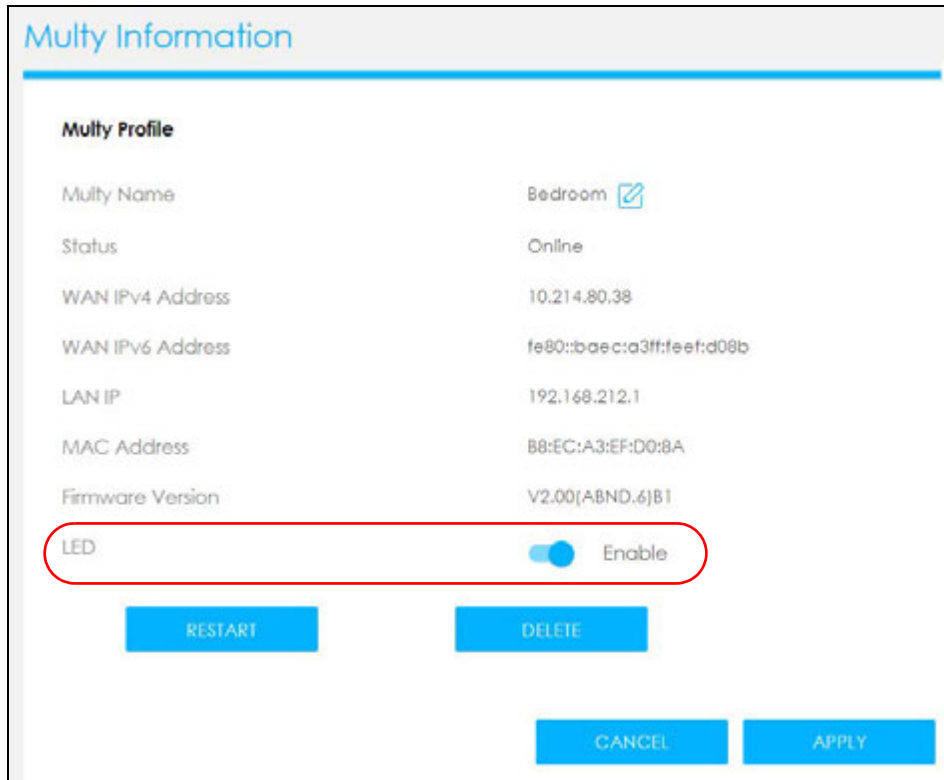


8.10 Turn On or Off the Multy Device's LED (Light)

- 1 Click the Navigation Panel icon on the top-left corner (), and click **My Multy** to view all the Multy Devices in your Multy 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.



The screenshot shows the 'Multy Information' page. It contains a table of device details and a red circle highlighting the 'LED' toggle switch.

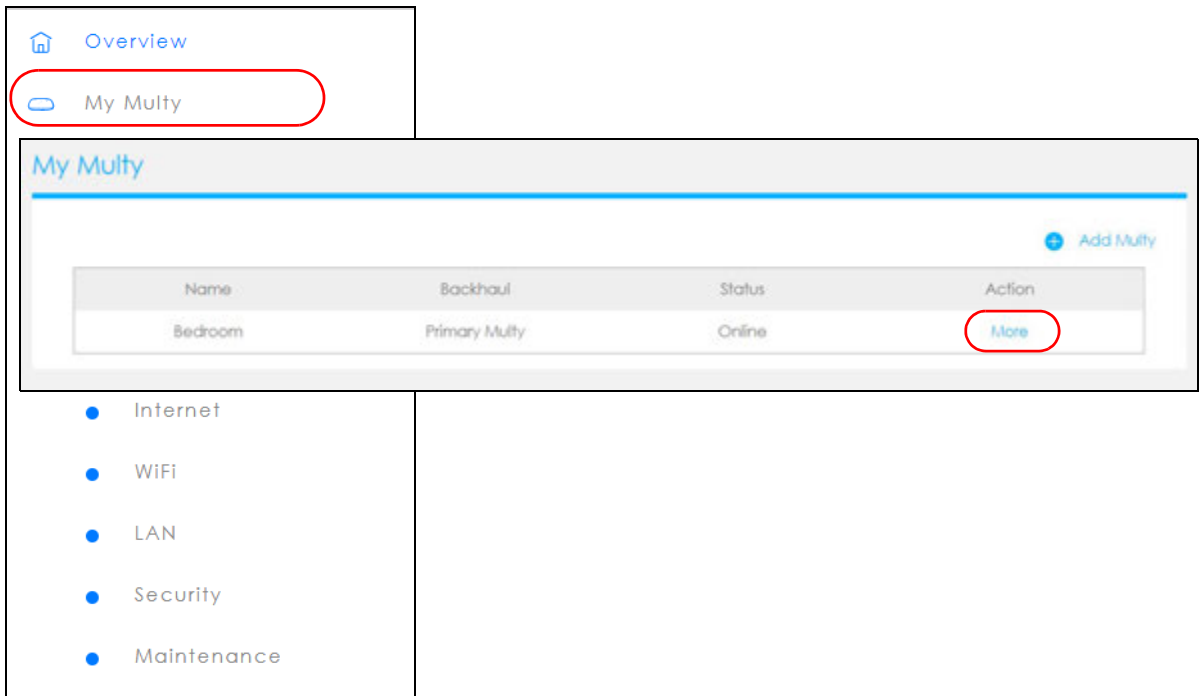
Multy Profile	
Multy Name	Bedroom 
Status	Online
WAN IPv4 Address	10.214.80.38
WAN IPv6 Address	fe80::baec:a3ff:feef:d08b
LAN IP	192.168.212.1
MAC Address	B8:EC:A3:EF:D0:8A
Firmware Version	V2.00[ABND.6]B1
LED	☒ Enable

Buttons: RESTART, DELETE, CANCEL, APPLY

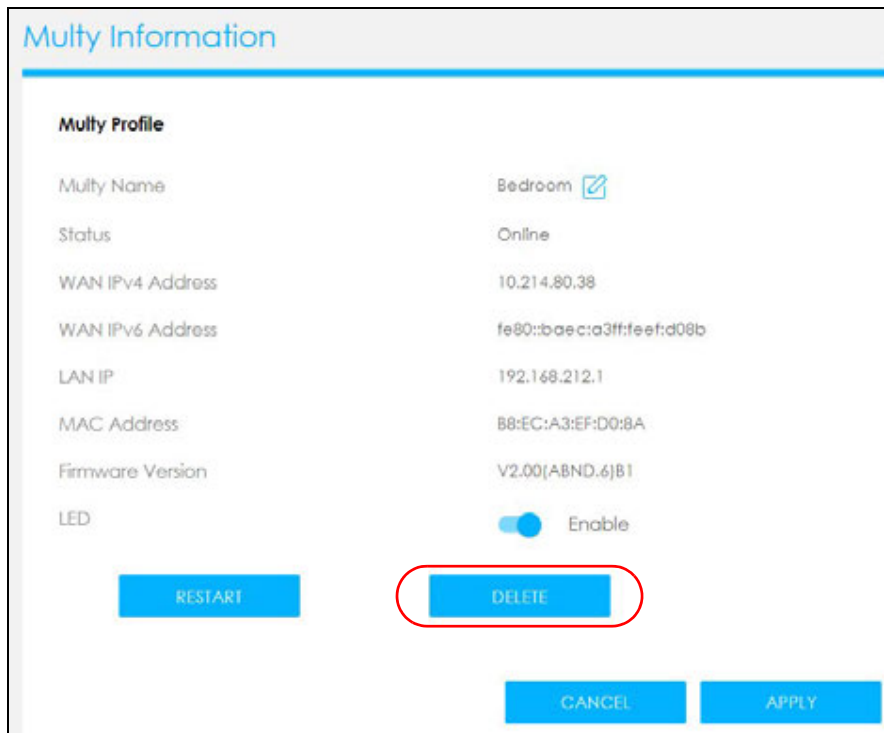
8.11 Remove a Multy Device

If a Multy Device is damaged or no longer in use, you can remove it from the Multy 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 WiFi System. Select the device you want to remove and click **More...**



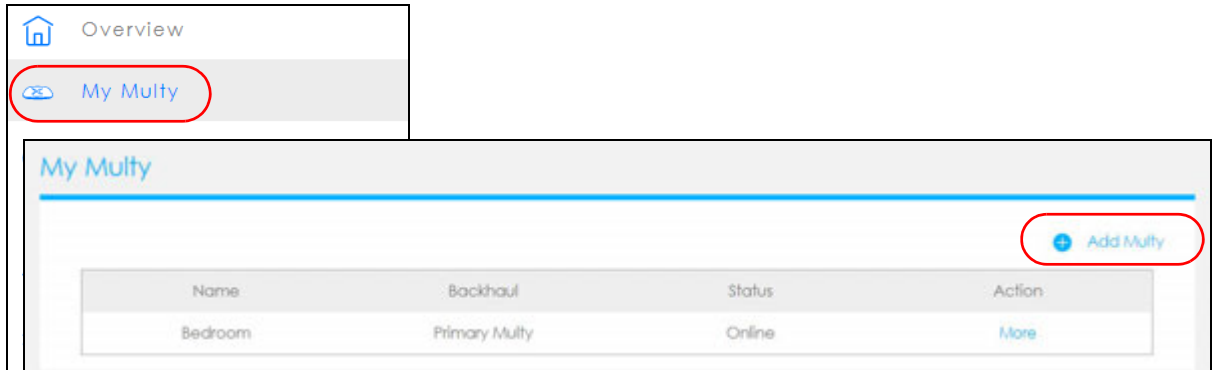
- 2 The **Multy Information** screen displays. Click **Delete** to remove the device from the Multy WiFi System.



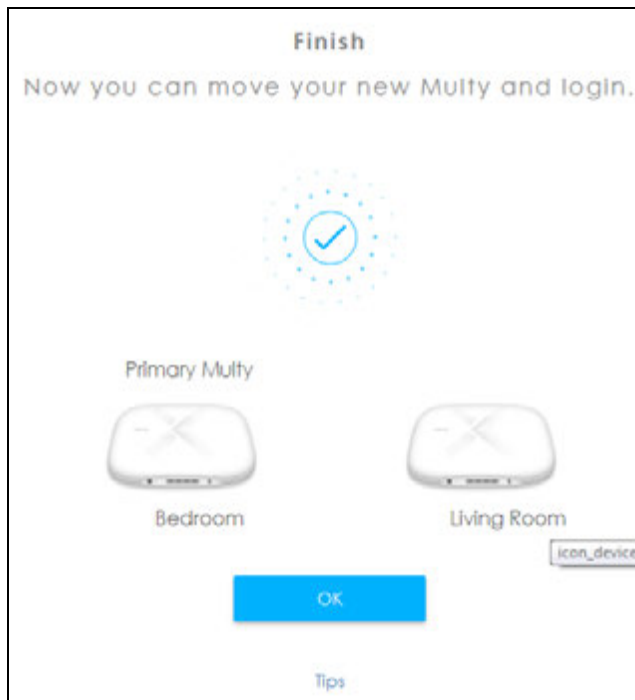
8.12 Install a Second Multy WiFi System

You can manage multiple Multy Devices 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 WiFi System. Click **Add Multy** to add a Multy Device to your Multy 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.



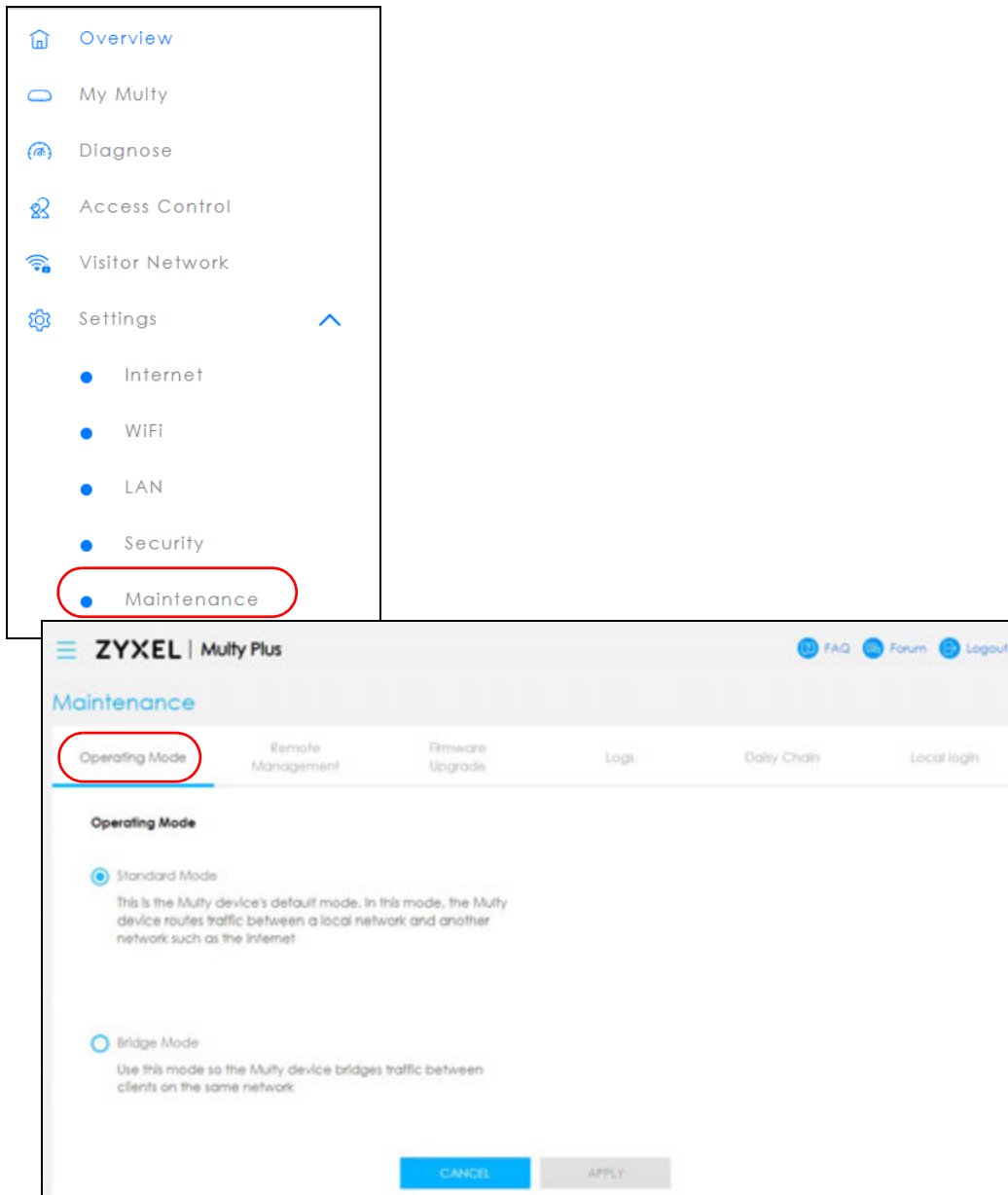
8.13 Change Your Multy Device Operating Mode

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

- **Standard:** This is the Multy Device's default mode. In this mode, the Multy Device routes traffic between a local network and another network such as the Internet. If you wish your Multy Device to have Access Control, UPnP, Port Forwarding, DMZ function, choose this mode.
- **Bridge:** Use this mode so the Multy Device 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.

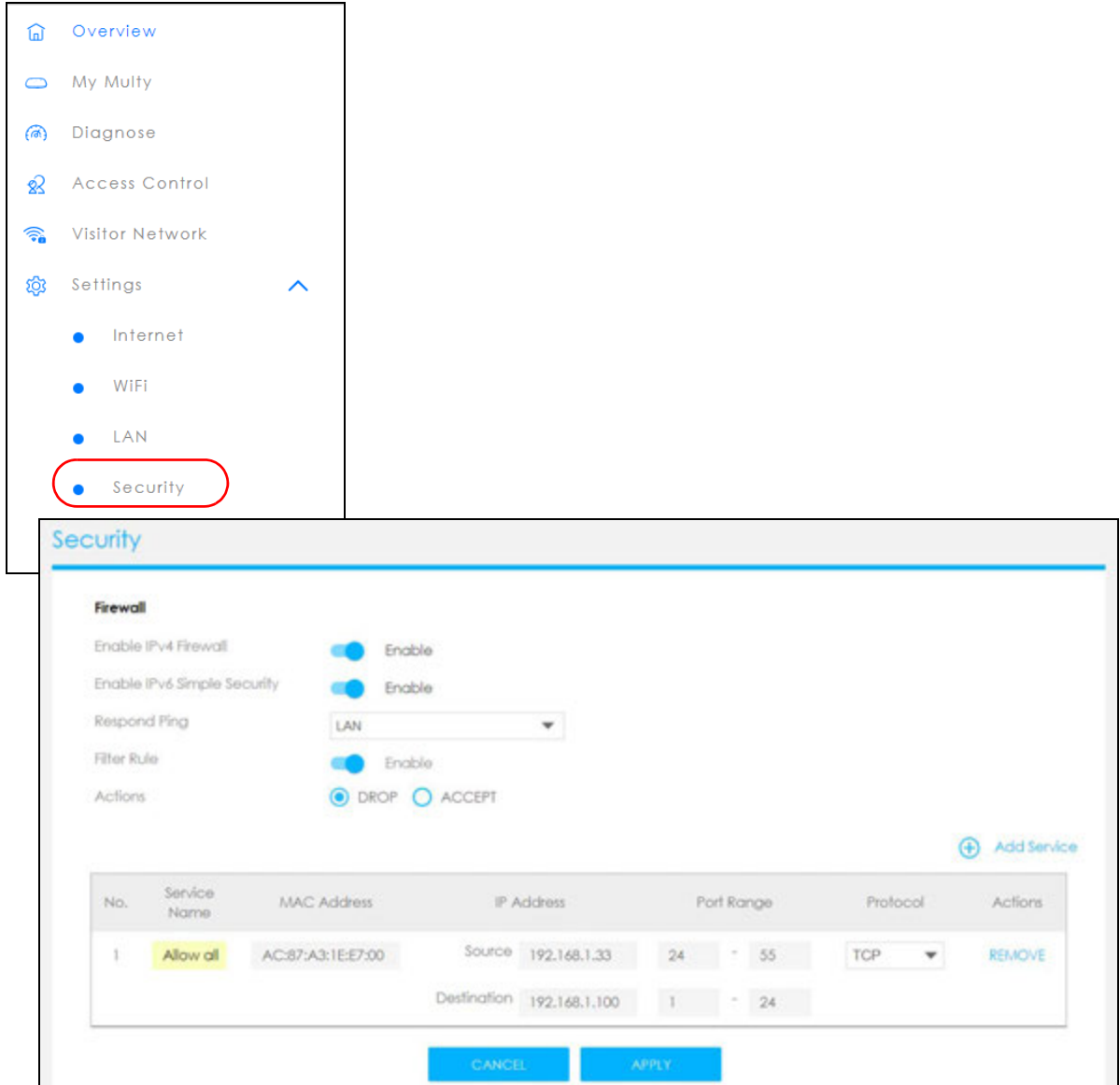
- 1 Click the Navigation Panel icon on the top-left corner (). From the **Settings** drop-down list, click **Maintenance**, then click the **Operating Mode** tab. Select the operating mode and select **APPLY** to save your changes. Changing the Multy Device's operating mode may take up to 2 minutes.



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.

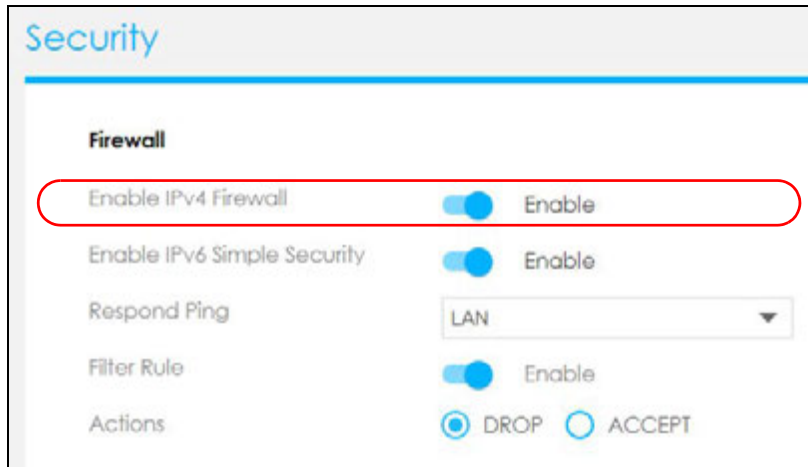


The screenshot shows the Multy Plus web interface. On the left is a navigation panel with the following items: Overview, My Multy, Diagnose, Access Control, Visitor Network, Settings (with a sub-menu arrow), Internet, WiFi, LAN, and Security (highlighted with a red circle). The main content area is titled 'Security' and contains the 'Firewall' settings. The Firewall settings include: 'Enable IPv4 Firewall' (toggle on), 'Enable IPv6 Simple Security' (toggle on), 'Respond Ping' (dropdown set to LAN), 'Filter Rule' (toggle on), and 'Actions' (radio buttons for DROP and ACCEPT, with DROP selected). Below these settings is a table with one rule:

No.	Service Name	MAC Address	IP Address	Port Range	Protocol	Actions
1	Allow all	AC:87:A3:1E:E7:00	Source: 192.168.1.33 Destination: 192.168.1.100	24 ~ 55 1 ~ 24	TCP	REMOVE

At the bottom of the Firewall settings are 'CANCEL' and 'APPLY' buttons. An 'Add Service' button is also visible in the top right of the rule table area.

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



Security

Firewall

Enable IPv4 Firewall ☒ Enable

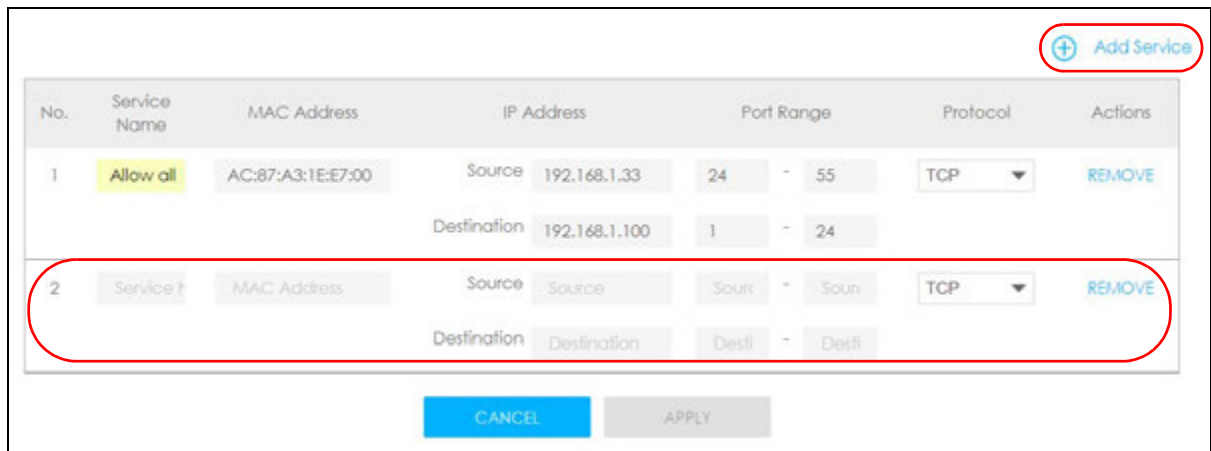
Enable IPv6 Simple Security ☒ Enable

Respond Ping LAN

Filter Rule ☒ Enable

Actions ☒ DROP ☐ ACCEPT

- 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).



+ Add Service

No.	Service Name	MAC Address	IP Address	Port Range	Protocol	Actions
1	Allow all	AC:87:A3:1E:E7:00	Source 192.168.1.33 Destination 192.168.1.100	24 - 55 1 - 24	TCP	REMOVE
2	Service ?	MAC Address	Source Destination	Source - Source Dest - Dest	TCP	REMOVE

CANCEL **APPLY**

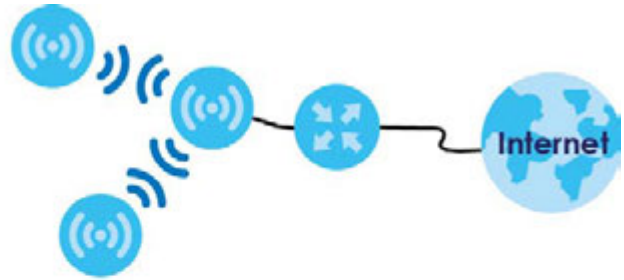
8.15 Enable or Disable Daisy Chain Network Topology

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

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

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

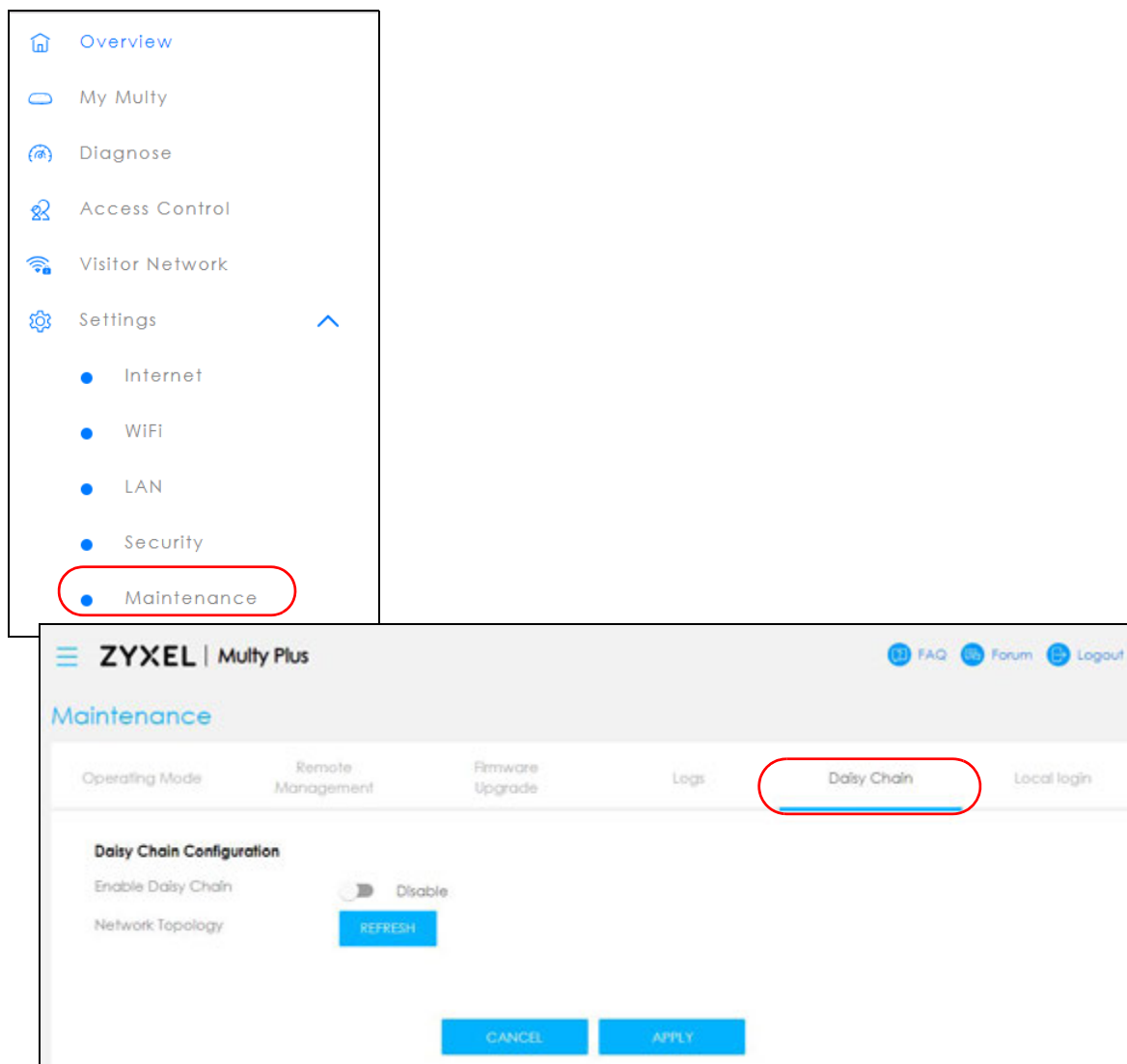
Daisy Chain Disabled



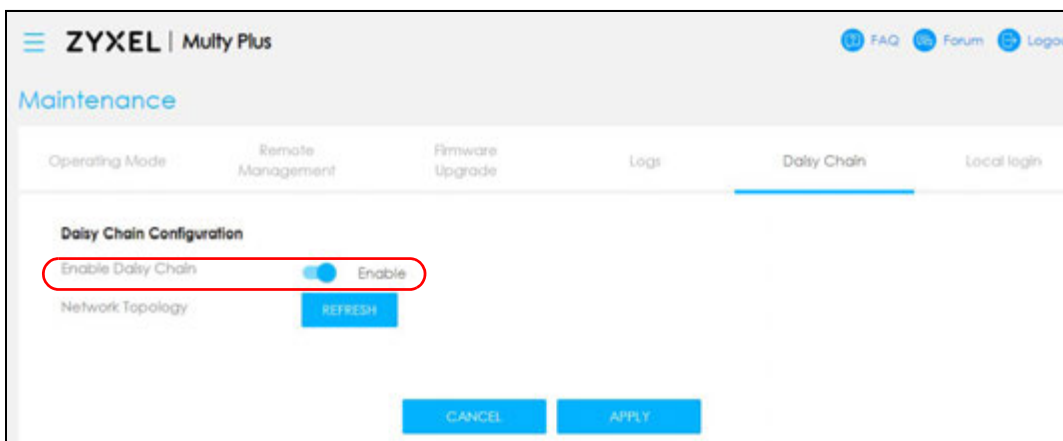
Daisy Chain Enabled



- 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.



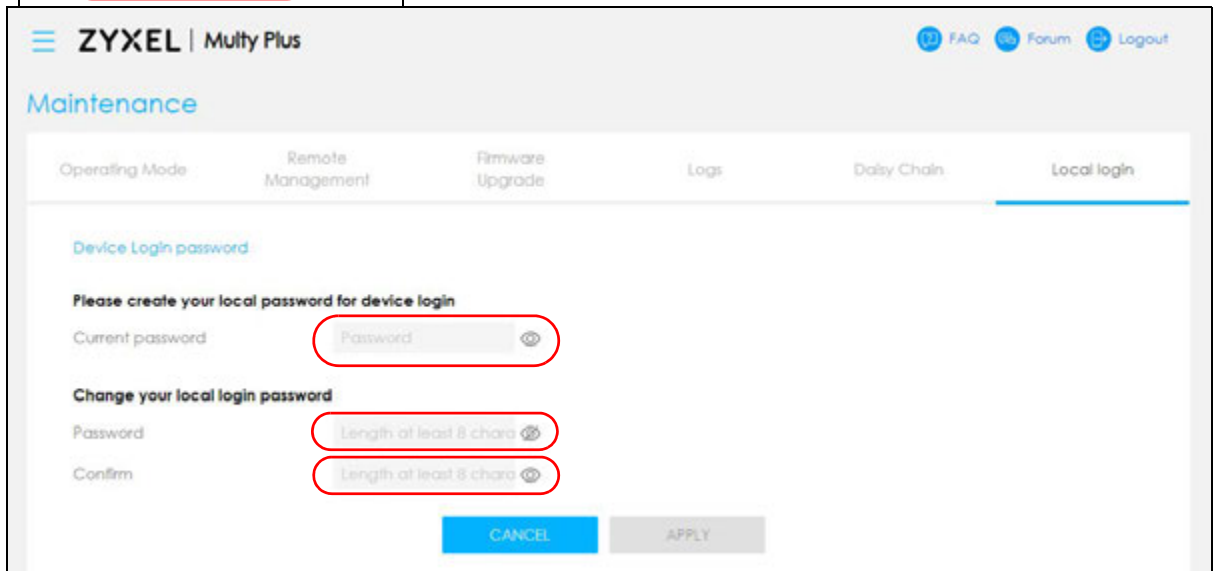
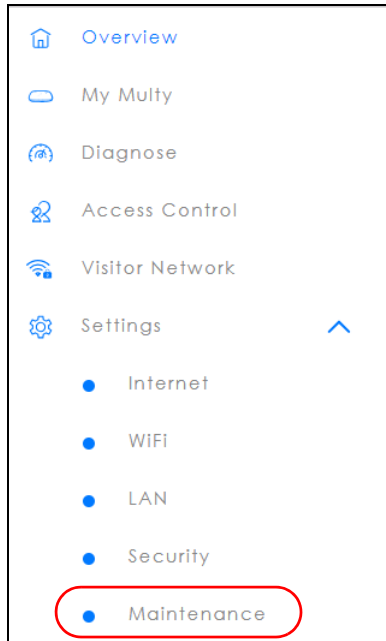
Click the button next to **Enable Daisy Chain** to activate daisy chaining.



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

Multy M6E

CHAPTER 9

Web Interface Tutorials – Multy M6E (WSQ65)

9.1 Overview

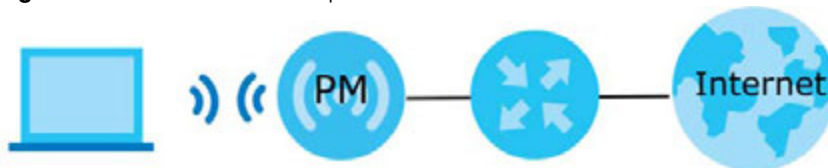
This chapter shows you how to use the Multy Device's various features.

- [WiFi Network Setup](#)
- [Network Security](#)
- [Device Maintenance](#)

9.2 WiFi Network Setup

In this example, you want to set up a WiFi network so that you can use your notebook to access the Internet. In this WiFi network, the Multy Device is an Primary Multy (PM) connected to a router/modem using an Ethernet cable, and the notebook is a WiFi client. The WiFi client can access the Internet through the Primary Multy.

Figure 57 WiFi Network Setup



See the label on the Multy Device for the WiFi network settings and then connect manually to the Multy Device. Alternatively, you can set up a WiFi network using WPS. See [Section 9.2.2.1 on page 203](#).

9.2.1 Changing Security on a WiFi Network

This example changes the default security settings of a WiFi network to the following:

SSID	Example
Security Mode	WPA3-SAE/WPA2-PSK
Pre-Shared Key	DoNotStealMyWirelessNetwork

- 1 Go to the **Network Setting > Wireless > General** screen. Select **More Secure** as the security level and **WPA3-SAE/WPA2-PSK** as the security mode. Configure the screen using the provided parameters. Click **Apply**.

Wireless

General | Guest/More AP | MAC Authentication | WPS | WMM | Channel Status

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode. We recommend that you select **More Secure** to enable WPA3-SAE/WPA2-PSK data encryption.

Wireless

Wireless ☐ Keep the same settings for 2.4G, 5G and 6G wireless networks ⓘ
Keep 2.4G, 5G and 6G the same cannot be turned off when MESH is active

Wireless Network Setup

Band: 2.4GHz
Wireless: ☒
Channel: Auto Current: 1 / 20 MHz
Bandwidth: 20/40MHz
Control Sideband: None

Wireless Network Settings

Wireless Network Name: Example
Max Clients: 64
☐ Hide SSID ⓘ Hide SSID does not support WPS 2.0. You should disable WPS in WPS page.
☒ Multicast Forwarding

Note

- (1) If you are configuring the Zyxel Device from a computer connected by WiFi and you change the Zyxel Device's SSID, channel or security settings, you will lose your WiFi connection when you press **Apply**. You must change the WiFi settings of your computer to match the new settings on the Zyxel Device.
- (2) If upstream/downstream bandwidth is empty, the Zyxel Device sets the value automatically. Setting a maximum upstream/downstream bandwidth will significantly decrease wireless performance.

BSSID: DA:1A:D1:0C:E8:81

Security Level

No Security More Secure (Recommended)

Security Mode: WPA3-SAE/WPA2-PSK

☐ Generate password automatically

Enter 8-63 ASCII characters or 64 hexadecimal digits [0-9, "A-F"].

Password: DoNotStealMyWirelessNetwork ⓘ

Strength: strong

Cancel
Apply

You can now use the WPS feature to establish a WiFi connection between your notebook and the Multy Device (see [Section 9.2.2.1 on page 203](#)). Now use the new security settings to connect to the Internet through the Multy Device using WiFi.

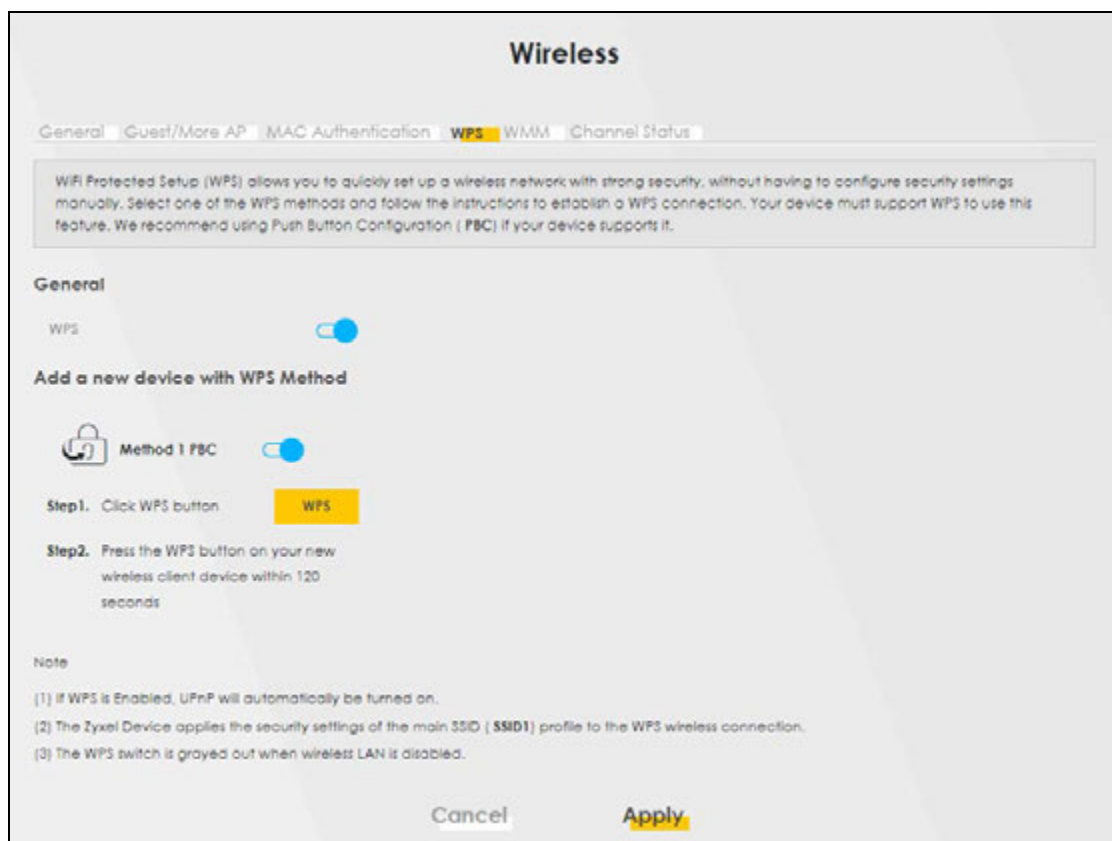
9.2.2 Connecting to the Multy Device's WiFi Network Using WPS

This section shows you how to connect a WiFi device to the Multy Device's WiFi network using WPS. WPS (Wi-Fi Protected Setup) is a security standard that allows devices to connect to a router securely without you having to enter a password.

9.2.2.1 WPS Push Button Configuration (PBC)

This example shows how to connect to the Multy Device's WiFi network from a notebook computer running Windows 10.

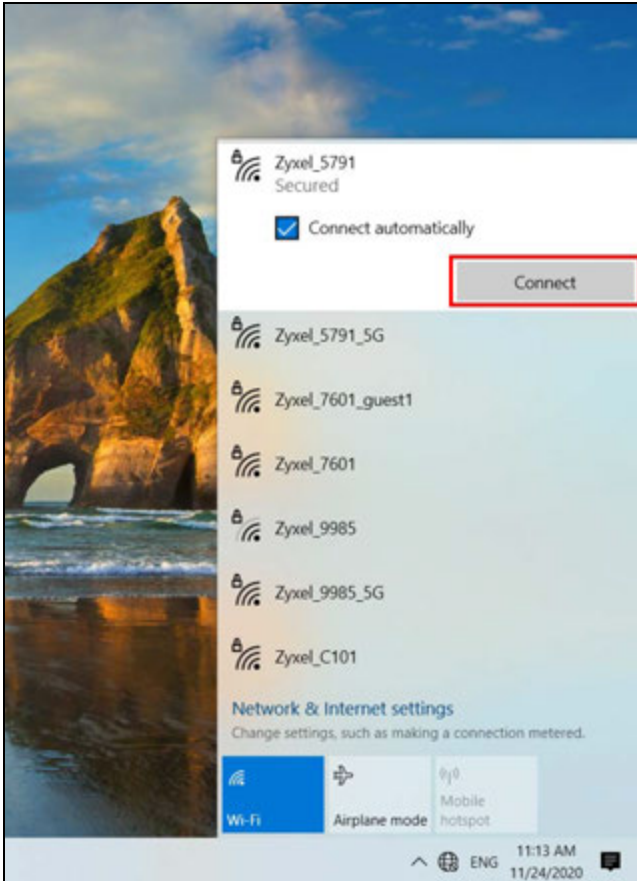
- 1 Make sure that your Multy Device is turned on, and your notebook is within range of the Multy Device's WiFi signal.
- 2 Push and hold the **WPS** button located on the Multy Device until the **WiFi** or **WPS** LED starts blinking slowly. Alternatively, log into the Multy Device's Web Configurator, and then go to the **Network Setting** > **Wireless** > **WPS** screen. Enable **WPS** and **Method 1 PBC**, click **Apply**, and then click the **WPS button**.



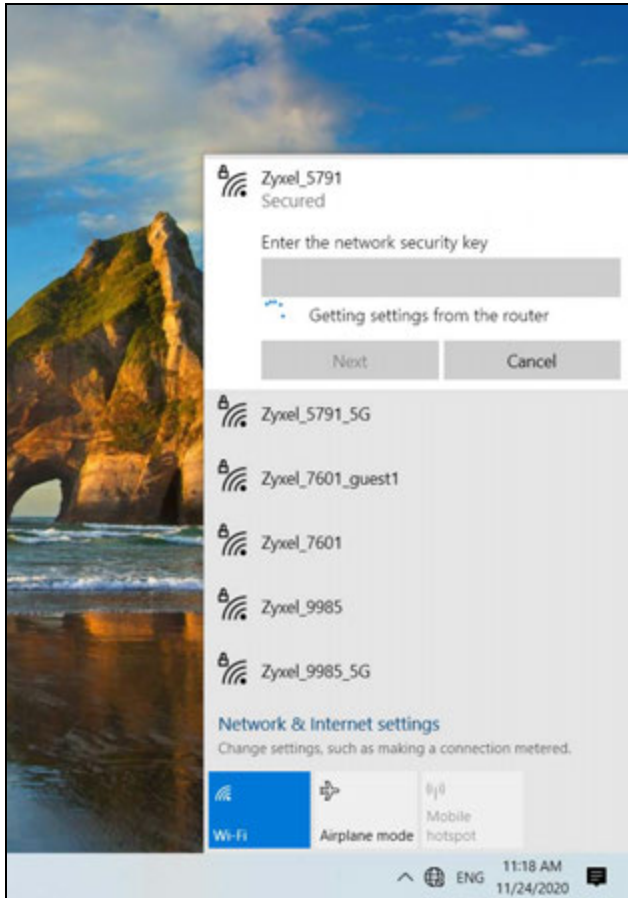
- 3 In Windows 10, click on the Network icon in the system tray to open the list of available WiFi networks.



- 4 Locate the WiFi network of the Multy Device. The default WiFi network name is "Zyxel_XXXX" (2.4G) or "Zyxel_XXXX_5G" (5G). Then click **Connect**.



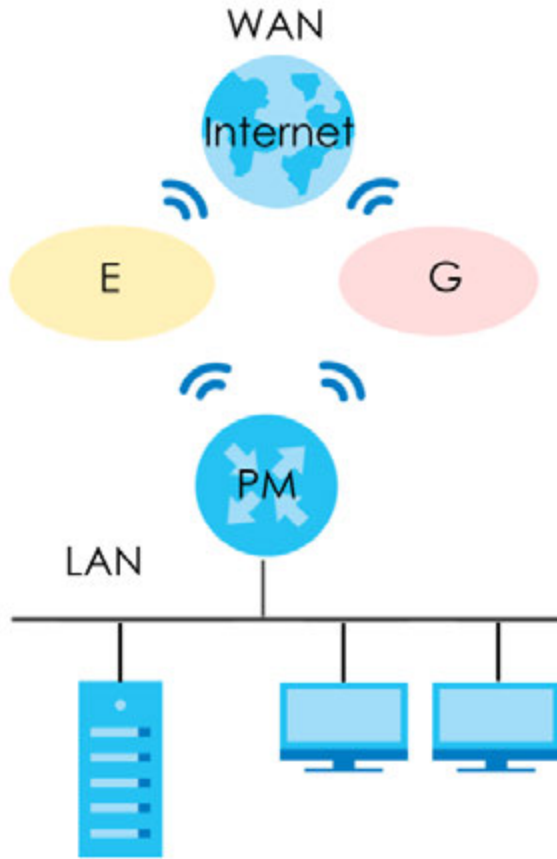
The Multy Device sends the WiFi network settings to Windows using WPS. Windows displays "Getting settings from the router".



The WiFi device is then able to connect to the WiFi network securely.

9.2.3 Setting Up a Guest Network

A company wants to create two WiFi networks for different groups of users as shown in the following figure. Each WiFi network has its own SSID and security mode. Both networks are accessible on both 2.4G and 5G WiFi bands.



- Employees (E) using the **GENERAL** WiFi network group will have access to the local network (LAN) and the Internet.
- Visitors (G) using the **GUEST** WiFi network group with a different SSID and password will have access to the Internet only.

Use the following parameters to set up the WiFi network groups.

	GENERAL	GUEST
2.4/5G SSID	Employee	Guest
Security Level	More Secure	More Secure
Security Mode	WPA3-SAE/WPA2-PSK	WPA3-SAE/WPA2-PSK
Pre-Shared Key	ForCompanyOnly	guest123

- 1 Go to the **Network Setting > Wireless > General** screen. Use this screen to set up the company's general WiFi network group. Configure the screen using the provided parameters and click **Apply**. Note that if you have employees using 2.4G and 5G devices, enable **Keep the same settings for 2.4G and 5G wireless networks** to use the same SSID and password. Clear it if you want to configure different SSIDs and passwords for 2.4G and 5G bands.

Wireless

General Guest/More AP MAC Authentication WPS WMM Channel Status

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode. We recommend that you select **More Secure** to enable **WPA3-SAE/WPA2-PSK** data encryption.

Wireless

Wireless ☒ Keep the same settings for 2.4G, 5G and 6G wireless networks ⓘ
Keep 2.4G, 5G and 6G the same cannot be turned off when MESH is active

Wireless Network Setup

Band

2.4GHz

Wireless ☒

Channel

Auto

Current: 1 / 20 MHz

Bandwidth

20/40MHz

Control Sideband

None

Wireless Network Settings

Wireless Network Name

Employee

Max Clients

64

☐ Hide SSID ⓘ Hide SSID does not support WPS 2.0. You should disable WPS in WPS page.

☒ Multicast Forwarding

Note

(1) If you are configuring the Zyxel Device from a computer connected by WIFI and you change the Zyxel Device's SSID, channel or security settings, you will lose your WIFI connection when you press **Apply**. You must change the WIFI settings of your computer to match the new settings on the Zyxel Device.

(2) If upstream/downstream bandwidth is empty, the Zyxel Device sets the value automatically. Setting a maximum upstream/downstream bandwidth will significantly decrease wireless performance.

BSSID DA:1A:D1:0C:E8:B1

Security Level

No Security

More Secure
(Recommended)

Security Mode

WPA3-SAE/WPA2-PSK

☐ Generate password automatically

Enter 8-63 ASCII characters or 64 hexadecimal digits ("0-9", "A-F").

Password

ForCompanyOnly

 ⓘ

Strength

medium

Cancel

Apply

Multy WiFi System User's Guide

207

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



- 3 On the **Guest/More AP** screen, click the **Modify** icon to configure the other Guest WiFi network group. Configure the screen using the provided parameters and click **OK**.

More AP Edit

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

Wireless Network Setup

Wireless ☒

Wireless Network Settings

Wireless Network Name

☐ Hide SSID

☒ Guest WLAN

Access Scenario

BSSID DE:1A:D1:0C:E8:81

SSID Subnet ☐

Security Level

No Security More Secure (Recommended)

Security Mode

☐ Generate password automatically

Enter 8-63 ASCII characters or 64 hexadecimal digits ("0-9", "A-F").

Password

Strength weak

Cancel OK

- 4 Check the status of **Guest** in the **Guest/More AP** screen. A yellow bulb under **Status** means the SSID is active and ready for WiFi access.

Wireless

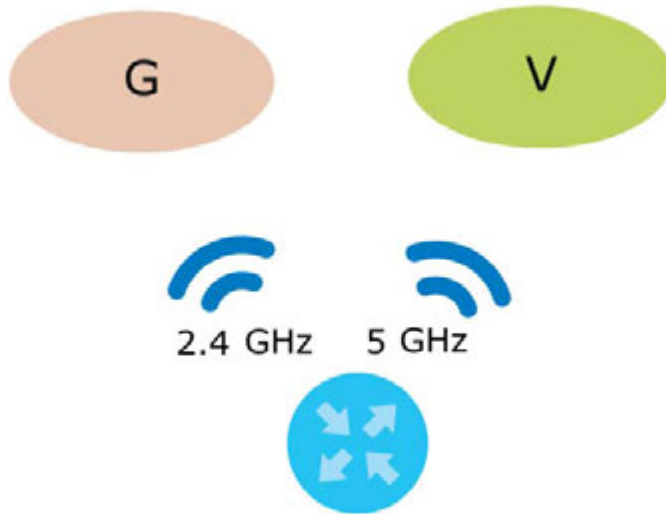
General **Guest/More AP** MAC Authentication WPS WMM Channel Status

This screen allows you to configure a guest wireless network that allows access to the Internet only through the Zyxel Device.

#	Status	SSID	Security	Guest WLAN	Modify
1		Employee	WPA3-SAE/WPA2-PSK	External Guest	
2		Guest	WPA3-SAE/WPA2-PSK	External Guest	
3		ZyxeI0CE878_guest3	WPA3-SAE/WPA2-PSK	External Guest	

9.2.4 Setting Up Two Guest WiFi Networks on Different WiFi Bands

In this example, a company wants to create two Guest WiFi networks: one for the **Guest** (G) group and the other for the **VIP** (V) group as shown in the following figure. Each network will have its SSID and security mode to access the internet.



- The **Guest** (G) group will use the 2.4G band.
- The **VIP** (V) group will use the 5G band.

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

Table 22 WiFi Settings Parameters Example

BAND	2.4G	5G
SSID	Guest	VIP
Security Mode	WPA2-PSK	WPA2-PSK
Pre-Shared Key	guest123	123456789

- 1 Go to the **Wireless > General** screen and set **Band** to **2.4GHz** to configure 2.4G Guest WiFi settings for **Guest**. Click **Apply**.

Note: You will not be able to configure the 2.4G and 5G Guest WiFi settings separately if **Keep the same settings for 2.4G and 5G wireless network** is enabled.

Wireless

General Guest/More AP MAC Authentication WPS WMM Channel Status

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode. We recommend that you select **More Secure** to enable WPA3-SAE/WPA2-PSK data encryption.

Wireless

Wireless ☐ Keep the same settings for 2.4G, 5G and 6G wireless networks ⓘ
Keep 2.4G, 5G and 6G the same cannot be turned off when MESH is active

Wireless Network Setup

Band 2.4GHz ▼

Wireless ☒

Channel Auto ▼ Current: 1 / 20 MHz

Bandwidth 20/40MHz ▼

Control Sideband None

Wireless Network Settings

Wireless Network Name Zyx@DCEB78

Max Clients 64

☐ Hide SSID ⓘ Hide SSID does not support WPS 2.0. You should disable WPS in WPS page.

☒ Multicast Forwarding

- 2 Go to the **Wireless > Guest/More AP** screen and click the **Modify** icon. The following screen appears. Configure the **Security Mode** and **Password** using the provided parameters and click **OK**.

<

More AP Edit

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

Wireless Network Setup

Wireless ☒

Wireless Network Settings

Wireless Network Name

☐ Hide SSID

☒ Guest WLAN

Access Scenario

External Guest

BSSID DE:1A:D1:0C:E8:79

SSID Subnet ☐

Security Level

No Security

More Secure
(Recommended)

Security Mode

WPA2-PSK

☐ Generate password automatically
Enter 8-63 ASCII characters or 64 hexadecimal digits ("0-9", "A-F").

Password

Strength weak

Cancel

OK

The 2.4G **Guest** WiFi network is now configured.

Wireless					
General Guest/More AP MAC Authentication WPS WMM Channel Status					
This screen allows you to configure a guest wireless network that allows access to the Internet only through the Zyxel Device.					
#	Status	SSID	Security	Guest WLAN	Modify
1		Guest	WPA2-PSK	External Guest	

- 3
- Go to the **Wireless > General** screen and set **Band** to **5GHz** to configure the 5G Guest WiFi settings for **VIP**. Click **OK**.

Wireless

General Guest/More AP MAC Authentication WPS WMM Channel Status

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode. We recommend that you select **More Secure** to enable **WPA3-SAE/WPA2-PSK** data encryption.

Wireless

Wireless ☐ Keep the same settings for 2.4G, 5G and 6G wireless networks ⓘ

Wireless Network Setup

Band 5GHz ▼

Wireless ☒

Channel Auto ▼ Current: 104 / 80 MHz

Bandwidth 20/40/80MHz ▼

Control Sideband None

Wireless Network Settings

Wireless Network Name Zyxel0CE878

Max Clients 64

☐ Hide SSID ⓘ Hide SSID does not support WPS 2.0. You should disable WPS in WPS page.

☒ Multicast Forwarding

- 4 Go to the **Wireless > Guest/More AP** screen and click the **Modify** icon. The following screen appears. Configure the **Security Mode** and **Password** using User's Guide and click **OK**.

<

More AP Edit

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

Wireless Network Setup

Wireless ☒

Wireless Network Settings

Wireless Network Name

VIP

☐ Hide SSID

☒ Guest WLAN

Access Scenario

External Guest

BSSID

E2:1A:D1:0C:E8:79

SSID Subnet ☐

Security Level

No Security

More Secure
(Recommended)

Security Mode

WPA2-PSK

☐ Generate password automatically
Enter 8-63 ASCII characters or 64 hexadecimal digits ("0-9", "A-F").

Password

123456789

Strength

weak

Cancel

OK

The 5G **VIP** WiFi network is now configured.

Wireless					
General Guest/More AP MAC Authentication WPS WMM Channel Status					
This screen allows you to configure a guest wireless network that allows access to the Internet only through the Zyxel Device.					
#	Status	SSID	Security	Guest WLAN	Modify
1		Guest	WPA2-PSK	External Guest	
2		VIP	WPA2-PSK	External Guest	

9.3 Network Security

This section shows you how to configure a Firewall rule, Parental Control rule, and MAC Filter rule.

9.3.1 Configuring a Firewall Rule

You can enable the firewall to protect your LAN computers from malicious attacks from the Internet.

- 1 Go to the **Security > Firewall > General** screen.
- 2 Select **IPv4 Firewall/IPv6 Firewall** to enable the firewall, and then click **Apply**.

Firewall

General Protocol Access Control Dos

Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it. Use this screen to set the security level of the firewall on the Zyxel Device. Firewall rules are grouped based on the direction of travel of packets to which they apply. A higher firewall level means more restrictions on the Internet activities you can perform.

IPv4 Firewall ☒

IPv6 Firewall ☒

Low Medium (Recommended) High

☐ ☒ ☐

	Low	Medium (Recommended)	High
LAN to WAN	☒	☒	☐
WAN to LAN	☒	☐	☐

Note

(1) LAN to WAN is your access to all Internet services. WAN to LAN is the access of other computers on the Internet to devices behind the Zyxel Device.

(2) When the security level is set to **High**, Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3, SMTP, and/or IPv6 ICMPv6 (Ping) traffic from the LAN are still allowed.

(3) We do not recommend you to disable the Firewall for your Zyxel device and network.

Cancel **Apply**

- 3 Open the **Access Control** screen to create a rule.

The screenshot shows the 'Add New ACL Rule' configuration page. It features a list of settings on the left and their corresponding input fields on the right. The 'Active' toggle is turned on. The 'Filter Name' field is empty. The 'Order' is set to 1. The 'Select Source IP Address' dropdown is set to 'Specific IP Address'. The 'Source IP Address' field is empty, with a '[prefix length]' label to its right. The 'Select Destination Device' dropdown is set to 'Specific IP Address'. The 'Destination IP Address' field is empty, with a '[prefix length]' label to its right. The 'MAC Address' field contains five asterisks. The 'IP Type' dropdown is set to 'IPv4'. The 'Select Service' dropdown is set to 'Specific Service'. The 'Protocol' dropdown is set to 'ALL'. The 'Custom Source Port' and 'Custom Destination Port' fields each have a 'Range' button and two input boxes, both containing '1'. The 'Policy' dropdown is set to 'ACCEPT'. The 'Direction' dropdown is set to 'WAN to LAN'. The 'Enable Rate Limit' toggle is turned on. The 'Rate Limit' section has an empty input box, a 'packet(s) per' label, a 'Minute' dropdown, and a '[1-512]' label. The 'Scheduler Rules' dropdown is empty. At the bottom, there are 'Cancel' and 'OK' buttons.

- 4 Click **Add New ACL Rule** and use the following fields to configure and apply a new ACL (Access Control List) rule.
 - 4a **Filter Name:** Enter a name to identify the firewall rule.
 - 4b **Order:** Assign the order of your rules as rules are applied in turn.
 - 4c **Select Source IP Address:** If you want the source to come from a particular (single) IP, select Specific IP Address. If not, select from a detected device.
 - 4d **Source IP Address:** Enter the IP address of the computer that initializes traffic for the application or service.
 - 4e **Select Destination Device:** If you want your rule to apply to packets with a particular (single) IP, select Specific IP Address. If not, select a detected device.
 - 4f **Destination IP Address:** Enter the IP address of the computer to which traffic for the application or service is entering.
 - 4g **MAC Address:** Enter the MAC address of the Multy Device.

- 4h IP Type:** Select the type (**IPv4** or **IPv6**) of the Source/Destination IP address.
 - 4i Select Device:** Select the device you want to block or allow from the drop down list box.
 - 4j Protocol:** Select the protocol (**ALL**, **TCP/UDP**, **TCP**, **UDP**, **ICMP** or **ICMPv6**) used to transport the packets.
 - 4k Custom Source Port:** Enter the port number that defines your rule.
 - 4l Custom Destination Port:** Enter the port number that defines your rule.
 - 4m Policy:** Select whether to (**ACCEPT**, **DROP**, or **REJECT**) the packets.
 - 4n Direction:** Select the direction (**WAN to LAN**, **LAN to WAN**, **WAN to ROUTER**, or **LAN to ROUTER**) of the traffic to which this rule applies.
- 5** Select **Enable Rate Limit** to activate the rules you created. Click **OK**.

9.3.2 Parental Control

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

Note: The style and features of your parental control vary depending on the Multy Device you are using.

9.3.2.1 Configuring Parental Control Schedule and Filter

Parental Control Profile (**PCP**) allows you to set up a rule for:

- Internet usage scheduling.
- Websites and URL keyword blocking.

Use this feature to:

- Limit the days and times a user can access the Internet.
- Limit the websites a user can access on the Internet.

This example shows you how to block a user from accessing the Internet during time for studying. It also shows you how to stop a user from accessing specific websites.

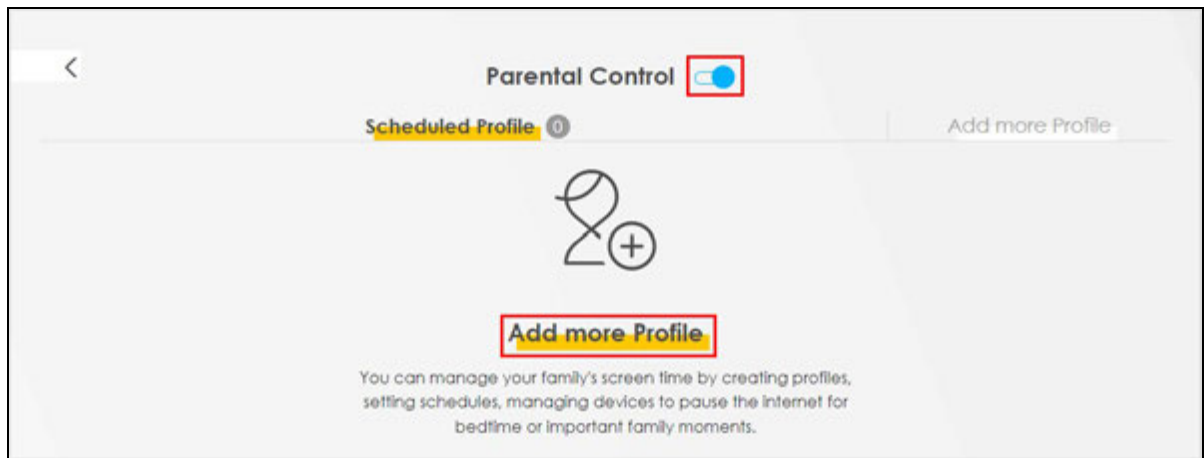
Use the parameter below to configure a schedule rule and a URL keyword blocking rule.

PROFILE NAME	INTERNET ACCESS SCHEDULE	NETWORK SERVICE	SITE / URL KEYWORD
Study	Day: Monday to Friday	Network Service Setting: Block	Block or Allow the Web Site: Block the web URLs
	Time: 8:00 to 11:00 13:00 to 17:00	Service Name: HTTP	Website: gambling

PROFILE NAME	INTERNET ACCESS SCHEDULE	NETWORK SERVICE	SITE / URL KEYWORD
		Protocol: TCP	
		Port: 80	

Parental Control Screen

Go to the **Security > Parental Control** screen. Click the switch to enable parental control.



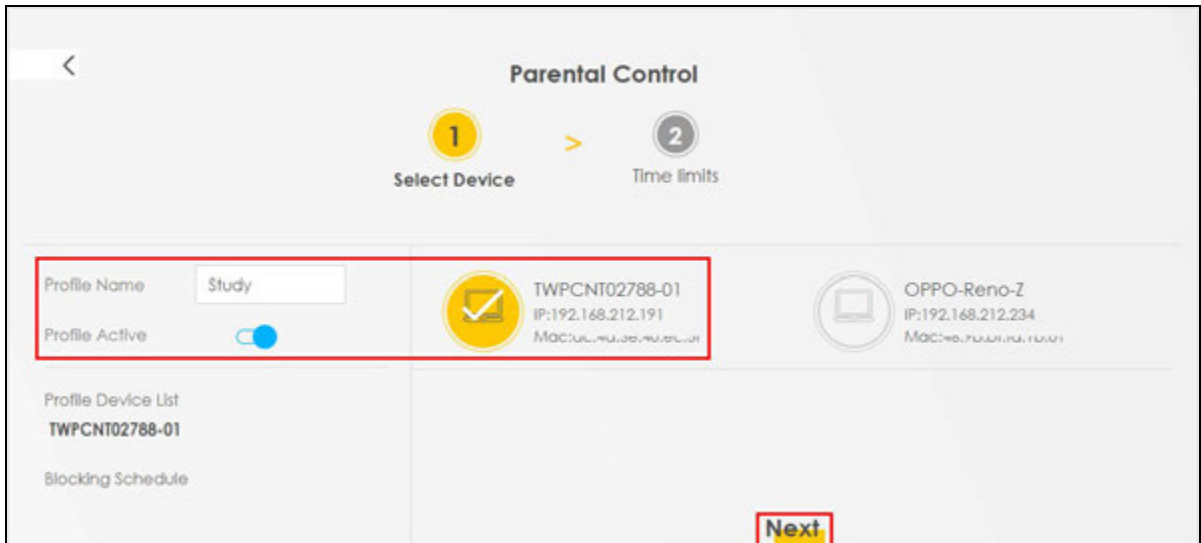
9.3.2.2 Configuring a Parental Control Schedule

Parental Control Profile allows you to set up a schedule rule for Internet usage. Use this feature to limit the days and times a user can access the Internet.

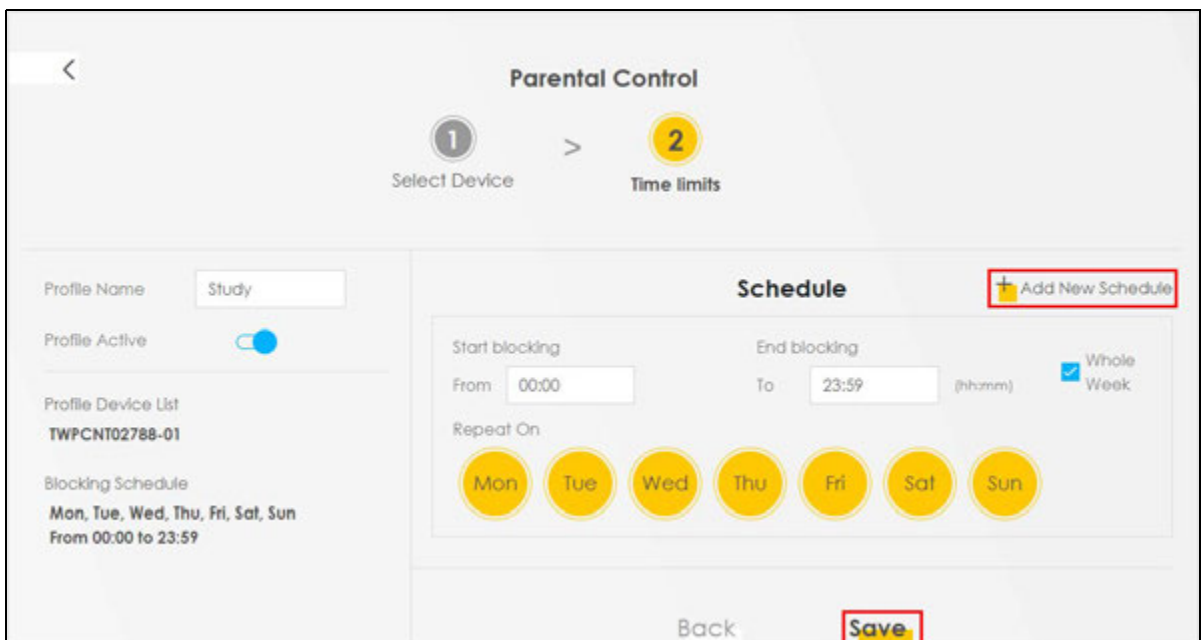
This example shows you how to block an user from accessing the Internet during time for studying. Use the parameter below to configure a schedule rule.

PROFILE NAME	START BLOCKING	END BLOCKING	REPEAT ON
Study	8:00 am	11:00 am	from Monday to Friday
	1:00 pm	5:00 pm	from Monday to Friday

- 1 Click **Add more Profile** to open the **Parental Control** screen.
- 2 Use this screen to add a Parental Control rule.
 - 2a Enter the **Profile Name** given in the above parameter.
 - 2b Click on the switch to enable **Profile Active**.
 - 2c Select a device, and then click **Next** to proceed.



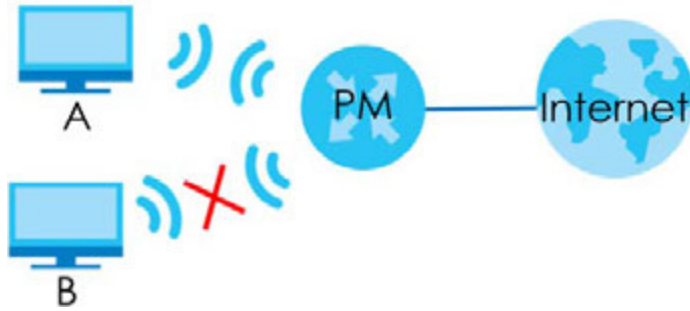
- 3 Use this screen to edit the Parental Control schedule.
 - 3a Click **Add New Schedule** to add a second schedule.
 - 3b Use the parameter given above to configure the time settings of your schedules.
 - 3c Click **Save** to save the settings.



9.3.3 Configuring a MAC Address Filter

Use a MAC address filter to exclusively allow or permanently block someone from connecting to your WiFi based on the MAC address of the device they are using to connect.

This example shows that computer (B) is not allowed access to the WiFi network.



- 1 Go to the **Security > MAC Filter > MAC Filter** screen. Under **MAC Address Filter**, select **Enable**.
- 2 Select **Deny** to block computer (B) from accessing your WiFi network.
- 3 Click **Add** to add a new entry. Select **Active**, and then enter the **Host Name** and **MAC Address** of computer (B). Click **Apply** to save the changes.

MAC Filter

You can configure the Zyxel Device to permit access to clients based on their MAC addresses in the **MAC Filter** screen. This applies to wired connections. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the LAN client to configure this screen.

Enable **MAC Address Filter** and add the host name and MAC address of a LAN client to the table if you wish to allow or deny them access to your network. You can choose to enable or disable the filters per entry; make sure that the check box under **Active** is selected if you want to use a filter.

MAC Address Filter ☒ Enable ☐ Disable (Settings are invalid when disable)

MAC Restrict Mode ☒ Allow ☐ Deny

Add New Rule: TWPCNT02788-01 (dc-4a-3e-40-ec-5f) Add

Set	Active	Host Name	MAC Address	Delete
1	☒	B	04 - 42 - 1a - de - b6 - 18	

Cancel Apply

9.4 Device Maintenance

This section shows you how to upgrade device firmware, back up the device configuration and restore the device to its previous or default settings.

9.4.1 Upgrading the Firmware

Upload the router firmware to the Multy Device for feature enhancements.

- 1 Download the correct firmware file from the download library at the Zyxel website. The model code for the Multy Device in this example is ACFK. Note the model code for your device. Unzip the file.
- 2 Go to the **Maintenance > Firmware Upgrade** screen.

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



The screenshot shows the 'Local Firmware Upgrade' web interface. At the top, it says 'Local Firmware Upgrade'. Below that, a message states: 'This screen lets you upload new firmware to your Zyxel Device.' and 'Download the latest firmware file from the Zyxel website and upload it to your Zyxel Device using this screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the Zyxel Device will reboot.' Under the heading 'Upgrade Firmware', there is a checkbox for 'Restore Default Settings After Firmware Upgrade'. Below this, it shows 'Current Firmware Version: V1.00(ACFK.0)B7'. At the bottom, there is a 'File Path' field with a 'Choose File' button (highlighted with a red box) and an 'Upload' button (highlighted with a yellow box). The file path shown is 'V1.00(ACFK.0)B8.bin'.

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

9.4.2 Backing Up the Device Configuration

Back up a configuration file allows you to return to your previous settings.

- 1 Go to the **Maintenance > Backup/Restore** screen.
- 2 Under **Backup Configuration**, click **Backup**. A configuration file is saved to your computer. In this case, the **Backup/Restore** file is saved.

Backup/Restore

Information related to factory default settings and backup configuration are shown in this screen. You can also use this to restore previous device configurations.

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

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

Backup Configuration

Click Backup to save the current configuration of your system to your computer.

Backup

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path No file chosen

Back to Factory Default Settings

Click Reset to clear all user-entered configuration information and return to factory default settings. After resetting, the

- Password is printed on a label on the bottom of the device, written after the text "Password".
- LAN IP address will be 192.168.212.1
- DHCP will be reset to default setting

Reset

9.4.3 Restoring the Device Configuration

This section shows you how to restore a previously-saved configuration file from your computer to your Multy Device.

- 1 Go to the **Maintenance > Backup/Restore** screen.
- 2 Under **Restore Configuration**, click **Browse/Choose File**, and then select the configuration file that you want to upload. Click **Upload**.

Backup/Restore

Information related to factory default settings and backup configuration are shown in this screen. You can also use this to restore previous device configurations.

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

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

Backup Configuration

Click Backup to save the current configuration of your system to your computer.

Backup

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path **Choose File** **Upload**

Back to Factory Default Settings

Click Reset to clear all user-entered configuration information and return to factory default settings. After resetting, the

- Password is printed on a label on the bottom of the device, written after the text "Password".
- LAN IP address will be 192.168.212.1
- DHCP will be reset to default setting

Reset

- The Multy Device automatically restarts after the configuration file is successfully uploaded. Wait for one minute before logging into the Multy Device again. Go to the **Connection Status** page to check the firmware version after the reboot.

PART V

Troubleshooting and Appendices

CHAPTER 10

Troubleshooting

10.1 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](#)

10.2 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.

10.3 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 10.5 on page 228](#) 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 30](#).
- 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 10.5 on page 228](#).

10.4 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.

10.5 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.

10.6 WiFi Connections

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

- Make sure WiFi is enabled on the Multy Device.
- Make sure the WiFi adapter on your computer is working properly.
- Make sure the WiFi adapter 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 client 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.

10.7 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.

10.8 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 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter. This transmitter must be at least 22 cm (WSM20) from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Country Code selection feature to be disabled for products marketed to the US/CANADA.
- Operation of this device is restricted to indoor use only, except for relevant user's manual mention that this device can be installed into the external environment.
- FCC regulations restrict the operation of this device to indoor use only.
- The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet.
- Operation of transmitters in the 5.925 – 7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

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 for wireless 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 5 GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5 GHz wireless LANs.
- If this device for operation in the band 5150 – 5350 MHz, it is for indoor use only.
- This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.
 - The maximum RF power operating for each band as follow:

WSM20

- The band 2,400 – 2,483.5 MHz is 99.77 mW
- The band 5,150 – 5,350 MHz is 198.15 mW
- The band 5,470 – 5,725 MHz is 995.41 mW.

WSQ20

- The band 2,400 – 2,483.5 MHz is 88.72 mW
- The band 5,150 – 5,350 MHz is 173.78 mW
- The band 5,470 – 5,725 MHz is 868.96 mW.

WSR30

- The band 2,400 – 2,483.5 MHz is 99.54 mW
- The band 5,150 – 5,350 MHz is 198.61 mW
- The band 5,470 – 5,725 MHz is 685.49 mW.

WSQ50

- The band 2,400 – 2,483.5 MHz is 97.95 mW
- The band 5,150 – 5,350 MHz is 182.81 mW
- The band 5,470 – 5,725 MHz is 916.22 mW.

WSQ60

- The band 2,400 – 2,483.5 MHz is 92.26 mW
- The band 5,150 – 5,350 MHz is 171.79 mW
- The band 5,470 – 5,725 MHz is 465.59 mW.

WSQ65, WSQ63, SCR 50AXE

- The band 2,400 – 2,483.5 MHz is 85.31 mW
- The band 5,150 – 5,350 MHz is 161.81 mW
- The band 5,470 – 5,725 MHz is 334.20 mW.
- The band 5,925 MHz to 6,425 MHz is 168.27 mW

Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществения 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 zařízený je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.

Dansk (Danish)	Undertegnede Zyxel erklærer herved, at følgende 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 vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΙΑ 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 frekvenču joslas izmantošanai ārpus telpām nepieciešama atļauja no Elektronisko sakaru direkcijas. Vairāk informācijas: 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 alapvető követelményeknek és az 2014/53/EU irányelv egyéb előírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ftigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Direttiva 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 cerințele esențiale și 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 adaptor 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 < 8 W, and/or
- Off mode power consumption < 0.5 W, and/or
- Standby mode power consumption < 0.5 W.

(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 is 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

Numbers

2.4G and 5G names
the same [57](#)

A

Access Control [193](#)
Add Multy screen [66](#)
Advanced Settings [118](#)
Alexa app [126](#)
Alexa voice command [115](#)
Alexa-enabled device [123](#)
Amazon account [123](#)
Amazon Alexa [10](#), [40](#), [172](#)
manage Multy WiFi System [123](#)
Amazon Echo [123](#)
Amazon website [123](#)
Android version [40](#)
antenna
internal [10](#)
AP Mode
menu [149](#)
status screen [149](#)
AP steering [11](#), [12](#)
APP management
availability [10](#)
Apple App store [40](#)
Apple ID account information [42](#)
Auto-IP Change [16](#)
conditions [16](#)
example [16](#)

B

background picture
change [100](#)

restore default [100](#)
Backhaul [62](#)
Band steering [11](#)
band steering [13](#)
bandwidth
maximum [9](#)
BLE (Bluetooth Low Energy) [10](#)
Block button [88](#)
Bluetooth [9](#), [37](#)
Bridge Mode [16](#), [138](#), [144](#), [147](#), [148](#)
default IP address [226](#)
example [17](#)
Bridge mode [111](#)
broadband [179](#)
broadband modem [17](#), [18](#)
button
Block [88](#)
Quick Block [93](#)
reset [30](#), [63](#)
Test All [76](#)
Turn Off [80](#)
Turn On [80](#)
WPS [30](#), [54](#)

C

Camera icon [102](#)
certifications [239](#)
viewing [241](#)
Channel Availability Check [11](#)
client
block [92](#)
client device information
view [92](#)
client devices group
block [93](#)
compatibility
Multy app [40](#)
contact information [231](#)

- control Multy Device
 - using voice commands [126](#)
- controller [152](#)
 - mesh network [8](#)
- copyright [236](#)
- coverage
 - WiFi [9](#)
- CPU [136, 139](#)
- customer service
 - send email [118](#)
- customer support [231](#)

D

- daisy chain
 - enable/disable [118](#)
 - multiple Multy Devices [116](#)
- daisy chain disabled
 - illustration [116](#)
- daisy chain enabled
 - illustration [116](#)
- daisy chain topology [9, 116](#)
- data rate [76](#)
- default setting [30, 63](#)
- DeMilitarized Zone (DMZ) [109](#)
- desk placement [28](#)
- Detail screen [62, 63, 95, 99](#)
- Devices screen [88](#)
- DHCP [111](#)
- DHCP client [226](#)
- DHCP enabled [175](#)
- disclaimer [236](#)
- distance
 - mounting [21](#)
- DMZ [111, 193](#)
 - overview [109](#)
- DMZ host
 - assign [109](#)
 - configure [111](#)
- DMZ host device [109](#)
- DNS [142, 143](#)
 - custom [98](#)
- DNS IP address [97](#)
- DNS server [97](#)

- default [98](#)
- domain name [97](#)
- downstream [179](#)
- downstream traffic
 - data rate [73, 76](#)
- dual-band application [12](#)
- dual-band compatible [13](#)
- dual-band WiFi [10, 12](#)

E

- Edit icon [81](#)
- E-label
 - availability [10](#)
- e-label
 - check [121](#)
- ESSID [228](#)
- Ethernet cable [18, 148](#)
- Ethernet connection status [97](#)
- extender [152](#)
 - mesh network [8](#)
- extender and primary Multy
 - signal strength [61](#)
- extender Multy [8, 97, 116](#)
- extender Multy (satellite) [12](#)
- extender name
 - in the app [11](#)

F

- Facebook account information [42](#)
- factory reset
 - steps [33](#)
- fast charging technology [10](#)
- feedback
 - send [118](#)
- Filter icon [85](#)
- Firewall [15](#)
- firewall
 - default action [15](#)
- firmware update
 - get update [113](#)

FTP server [109](#)

G

Get Ready screen [66](#)

Google account information [42](#)

Google Play store [40](#)

group

 pause Internet access [95](#)

guest WiFi [14](#)

Guest WiFi setting [81](#)

guest WiFi setting [80](#)

Guest WLAN [111](#)

GUI management

 availability [10](#)

H

hardware connection [18](#)

History icon [77](#)

hook

 front panel [23](#)

 rear panel [23](#)

HTTP web server [109](#)

HTTPS web server [109](#)

I

icon

 Camera [102](#)

 Edit [81](#)

 Filter [85](#)

 History [77](#)

 Information [122](#)

 Menu [68, 76, 79](#)

 Parental Control [85, 90, 93](#)

 Remove [74, 77](#)

 Settings [65](#)

 Share [83, 84](#)

 Speed Test [73](#)

 Visibility [104](#)

 Web Configurator [103](#)

 WiFi Settings [81, 83](#)

IEEE 802.11a/b/g/n/ac/ax [12](#)

IM (Instant Messaging) [15](#)

Information icon [122](#)

Internet access

 problem [227](#)

Internet connection

 slow or intermittent [227](#)

Internet connection speed

 check [72](#)

Internet port [18](#)

Internet Protocol version 6 [15](#)

Internet Service Provider [175](#)

Internet speed

 test [115](#)

iOS version [40](#)

IP address [97](#)

ipconfig [226](#)

IPv4/IPv6 dual stack [15](#)

IPv6 [15](#)

IPv6 address [97](#)

IPv6 firewall rule [15](#)

IPv6 rapid deployment (6RD) [15](#)

IPv6 traffic [15](#)

ISP [61](#)

L

LAN client [105, 194](#)

LAN port [10](#)

leather strap

 hang [27](#)

 WSR30 [28](#)

LED

 check [46, 53](#)

 on/off switch [33](#)

LED behavior [34](#)

LED description [37](#)

Local login password [198](#)

location select

 place the Multy Device [51](#)

M

- MAC address [149](#)
- magnetic stand [29](#)
- maximum bandwidth [10](#)
- Menu icon [68, 76, 79](#)
- Menu screen [66](#)
- Mesh network [10](#)
 - assigned role [63](#)
- mounting base [21, 24](#)
- mounting bracket [23](#)
- mounting hole [23, 24](#)
 - WSQ65 [26](#)
- Multy app [17](#)
 - log in [40](#)
- Multy Device
 - differences between models [9](#)
 - maximum number of [8](#)
- Multy Device label [49](#)
- Multy Satellite [51](#)
- Multy Site [44](#)
 - give new name [101](#)
 - multiple [68](#)
 - remove Multy Device [63](#)
 - switching [70](#)
- Multy-Alexa skills [123](#)
- myZyxeCloud [131, 135, 138, 172, 177](#)
- myZyxeCloud account [40, 113, 123](#)
 - log out [120](#)
 - Multy Device link to [134](#)
 - sign up [40](#)
- myZyxeCloud server [40](#)

N

- name
 - WiFi network [83](#)
- NAT (Standard) Mode [112](#)
- NAT and Bridge mode
 - switching [112](#)
- NAT mode [111](#)
 - Multy Site default [112](#)
 - routing features [111](#)
- navigation panel [179](#)

- network controller [11](#)

O

- OpenVPN client software [14](#)
- OpenVPN server/client [14](#)
- operating mode [167, 168](#)
- overview
 - Multy WiFi System [8](#)

P

- packet
 - forward [105](#)
- pairing method [10, 17](#)
- parental control [111](#)
- Parental Control icon [85, 90, 93](#)
- password
 - change [105](#)
 - create [42](#)
 - WiFi network [83](#)
- ping [228](#)
- port
 - LAN [10](#)
 - USB [9](#)
- Port Forwarding [169, 193](#)
- port forwarding [111](#)
- Port Forwarding Rule [168](#)
- port forwarding rule
 - create/update [107](#)
 - set [105](#)
 - summary display [108](#)
- Port Forwarding screen [107](#)
- Port Forwarding Settings [107](#)
- port number [108](#)
- power cable [18](#)
- power outlet [18](#)
- PPPoE [175](#)
- PPPoE setting
 - configure [61](#)
- primary Multy [8, 116](#)
- private network [105](#)

Profile Detail screen [89, 95](#)
profile name
 applied [88](#)
Profile screen [93](#)
push notification
 on smartphone [113](#)

Q

QR code [47](#)
 create [82, 83](#)
 in QSG [17](#)
 print [82](#)
 scan [82](#)
 take screenshot [83](#)
Quick Block button [93](#)
quick charge
 availability [10](#)
quick charge function [10](#)

R

rear panel
 WSM20 [19](#)
 WSQ20 [18](#)
 WSQ50 [18](#)
 WSQ60 [18](#)
 WSQ65 [20](#)
 WSR30 [19](#)
rear port cover
 as stand [28](#)
relay communication [9](#)
Remove icon [74, 77](#)
rename Multy Site [100](#)
reserve IP [111](#)
Reset button [30, 63, 228](#)
restart device [100](#)
role
 in Mesh network [11](#)
 in Multy app [11](#)
Router Mode
 status screen [145](#)
router name
 in the app [11](#)

routing features
 NAT mode [111](#)

S

schedule
 create [88](#)
schedule group [90](#)
schedule profile
 create [84](#)
screw/anchor specification
 WSM20 [21](#)
service name
 enter [108](#)
Settings icon [65](#)
Share icon [83, 84](#)
sign in process
 myZyxeCloud [43](#)
signal check [78](#)
signal strength [78](#)
signal strength test [62](#)
SIP [111](#)
Site Detail screen [65, 101](#)
smartphone [72, 78](#)
 connect to WiFi network [61](#)
Speed Test [179](#)
speed test
 run [115](#)
Speed Test icon [73](#)
speed test result
 get update [113](#)
stand
 use rear port cover [28](#)
Standard (router) Mode [15](#)
Standard Mode [138, 144, 147](#)
 default IP address [226](#)
Standard Mode example [16](#)
Static IP setting
 configure [61](#)
Status [145](#)

T

Test All button [76](#)
timer
 set [90](#)
transmission range
 WiFi [228](#)
transport layer protocol
 specify [108](#)
Turn Off button [80](#)
Turn On button [80](#)

U

updates
 get when new WiFi client connect [113](#)
UPnP [111](#), [142](#), [193](#)
upstream [179](#)
upstream traffic
 data rate [73](#), [76](#)
USB port [9](#)
USB storage device
 supported [230](#)

V

Visibility icon [104](#)
voice command [126](#)
VPN protocol [14](#)

W

wall mount
 WSQ65 [26](#)
wall mounting
 WSM20 [20](#)
wall mounting method [20](#)
wall/ceiling mount [23](#)
 steps [24](#)
WAN connection
 set up [50](#)

warranty
 note [241](#)
Web Configurator [17](#), [177](#)
 how to access [138](#)
 password change [103](#)
Web Configurator icon [103](#)
Web Configurator screen [103](#)
WiFi [228](#)
WiFi 6 Tri-Band [10](#)
WiFi 6E Tri-Band [10](#)
WiFi access
 disable [84](#)
WiFi adapter [228](#)
WiFi channel [228](#)
WiFi client
 show number of [60](#)
WiFi client device [30](#)
WiFi connection
 optimize speed and quality [229](#)
 slow or intermittent [229](#)
WiFi coverage [9](#), [195](#)
 expand [116](#)
WiFi interference
 factors [229](#)
WiFi name
 change [56](#)
WiFi name (SSID) [81](#)
WiFi network
 for guest [80](#)
 join [82](#)
WiFi networks
 steer between [57](#)
WiFi password [81](#), [82](#)
 change [56](#)
WiFi security [228](#)
WiFi security setting [228](#)
WiFi Settings icon [81](#), [83](#)
WiFi signal
 decent [80](#)
WiFi signal strength [78](#)
WiFi tutorial [150](#), [203](#)
WPS [30](#), [143](#)
 activate [30](#)
WPS button [54](#)
 availability [10](#)

WPS connection [30](#)
 set up [54](#)
WPS-compatible client device [30](#)
WSM20
 LED [36](#)
 LED switch [34](#)
 mounting distance [21](#)
 rear panel [19](#)
 reset button [32](#)
 wall mounting [20](#)
WSM20 removal
 from mounting base [22](#)
WSQ20
 LED [35](#)
 mounting hole [24](#)
 rear panel [18](#)
 reset button [31](#)
 screw specification [25](#)
 wall/ceiling mount [23](#)
WSQ50
 LED [34](#)
 mounting hole [24](#)
 rear panel [18](#)
 reset button [31](#)
 screw specification [25](#)
 wall/ceiling mount [23](#)
WSQ60
 LED [34](#)
 mounting hole [24](#)
 rear panel [18](#)
 reset button [31](#)
 screw specification [25](#)
 wall/ceiling mount [23](#)
WSQ65
 desk placement [30](#)
 LED [36](#)
 mounting hole [26](#)
 rear panel [20](#)
 reset button [32](#)
 screw specification [27](#)
 wall mount [26](#)
WSR30
 LED [35](#)
 rear panel [19](#)
 rear port cover [29](#)
 reset button [31](#)
 stand [29](#)

Z

Zyxel Multy app
 problem with [118](#)