HUMAX
NETWORKS

User Manual

Turbo E-PON Wireless Voice Gateway

HPS11-2GE



HUMAX Networks Inc.
www.humax-networks.com

Contents

Chapter 1. Introducing Your Device 1

1.1 Package Contents 1

1.2 Device Overview 2

Chapter 2. Connecting Your Device 6

2.1 Position 6

2.2 Connection 7

Chapter 3. Logging into Your Device 9

3.1 Access to Web UI through Web/Mobile Browser 10

Chapter 4. Knowing Connection Status 13

4.1 Quick Menu 13

4.2 Home Menu 14

Chapter 5. Setting Wireless Network 15

5.1 Basic Wireless Setting 15

5.2 Primary Wireless Setting 20

5.3 MAC Access Control 26

5.4 Mesh Setting 29

Chapter 6. Setting Local Setting 30

6.1 LAN Setting 30

6.2 Reserved IP Address 32

Chapter 7. Providing Network Service 34

7.1 Packet Filtering 34

7.2 DDNS Setting 36

7.3 Port Forwarding Setting 38

7.4 DMZ Setting 40

7.5 Parental Control Rules 41

Chapter 8 Setting Advanced Options 43
8.1 Advanced Network Setting 43
8.2 Routing Rule Setting 46
8.3 UPnP Setting 49
8.4 Diagnostics 51
8.5 Statistics 54
Chapter 9. Managing the System 55
9.1 Factory Reset/Restart 55
9.2 LED Mode 57
9.3 Change Password 58
9.4 Energy Saving Mode 59
9.5 Operation Mode 60
9.6 Date/Time 60
Chapter 10. Media Share 62
10.1 USB 62
10.2 FTP Server 63
10.3 DLNA 66
10.4 Samba 67
10.5 Printer Server 69
Chapter 11. Troubleshooting 70
Chapter 12. Safety and Regulatory Information 72
Chapter 13. Specification 74

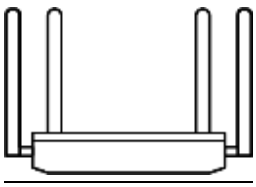
Chapter 1. Introducing Your Device

Please read this user's manual carefully to safely install, use and maintain the device at maximum performance. The information in this user's manual is subject to change without notice. The detailed description may slightly differ depending on each device, and the images are merely for illustrational purposes and thus may differ from the screens you actually see.
Throughout the whole manual, pay special attention to the following marks that indicate hazardous situations.

	**Warning**	Indicates a hazardous situation that could result in serious injury.
	**Note**	Indicates additional information to make the user aware of possible problems and information of any importance to help understand, use, and maintain the installation.
	**Tips**	Indicates information helpful to the user, like showing an easier way to do something.

1.1 Package Contents

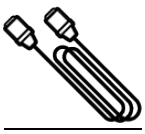
Your package contains the following items.



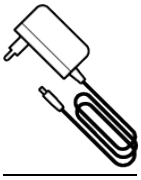
HPS11-2GE
10G EPON Unit



Quick Installation
Guide



RJ-45
Ethernet Cable



Power Adapter

 *Note:*

Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact your distributor.

1.2 Device Overview

1.2.1 Front Panel

The front panel provides 12 LEDs, and the WPS button is located on the right side of the device.



You can use the LEDs to verify status and connections. The following table lists and describes each LED on the front panel of the device.

LED	Operation	
Power	Green On	Power is on.
	Green Blinking	Booting is in progress.
	Red On	Power failure.
	Red Blinking	POST (Power-ON-Self-Test) failure.
	Off	Power is off.
Internet	Green On	Internet is connected.
	Green Blinking	Internet is connecting.
	White Blinking	Mesh pairing is in progress.
	Red Blinking	Unable to use Internet. (Not assigned IP address)
	Blue Blinking	Firmware is being upgraded.
	Off	Internet is not connected.
PON	Green On	Registration and provisioning are done.
	Green Blinking	Registration is done but provisioning is in progress.
	Green Fast Blinking	Registration is in progress.
	Off	PON port is not connected.
LOS	Red On	There is no optical signal.
	Off	There is an optical signal.
LAN 1~4	Green On	The device is connected to the LAN Port.
	Off	The device is not connected to the LAN Port.
WAN/LAN (2.5G)	Green On	The device is connected to the WAN/LAN Port.
	Off	The device is not connected to the WAN/LAN Port.
USB	Green On	USB device is connected.
	Off	USB device is not connected
2.4GHz & 5GHz	Green On	2.4GHz(or 5GHz) radio is on.
	Green Blinking	WPS is operating for 2 minutes. If WPS succeeds within 2 minutes, the blinking stops and the LED turns off.
	Green Fast Blinking	If WPS fails after 2 minutes, it operates as Fast Blinking for 5 seconds, after which the LED turns off.
	Off	2.4GHz(or 5GHz) radio is off.

- **WPS** Button**:** The WPS button makes it easier to connect to devices you want to connect wirelessly. Press the WPS button and check the progress through the 2.4GHz and 5GHz LEDs. For more details, see Connecting your device > Connection.

1.2.2 Back Panel

The back panel provides the connections and button shown in the following figure.



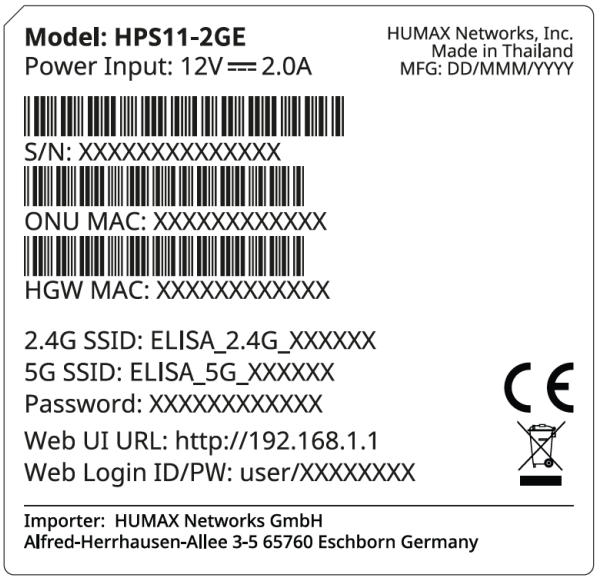
- **Power**: Connect the power adapter provided in the package and plug it into an electrical outlet.
- **PON**: Connect the fiber optic cable.
- **On/Off** button: Turns the device on and off.
- **LAN 1~4**: Provides four 1Gbps LAN ports.
- **WAN/LAN (2.5G)**: Provides one 2.5Gbps LAN port.
- **USB**: Provides one USB 2.0 port.
- **Reset** button: Press and hold the Reset button for 5 seconds to restore factory default settings.

Note: All user settings will be erased and this action cannot be undone.

LED	Operation	
LAN 1~4	Green On	1G link up status
	Orange On	100M/10M link up status
	Off	The LAN is not connected.
WAN/LAN (2.5G)	Green On	2.5G link up status
	Orange On	1G/100M link up status
	Off	The LAN is not connected.

1.2.3 Label

The label is on the side of the device. You can check the wireless and Web UI connection information.



To get help from your internet service provider, you may need to provide the model name, ONU, and MAC address listed on the label.

Chapter 2. Connecting Your Device

2.1 Position

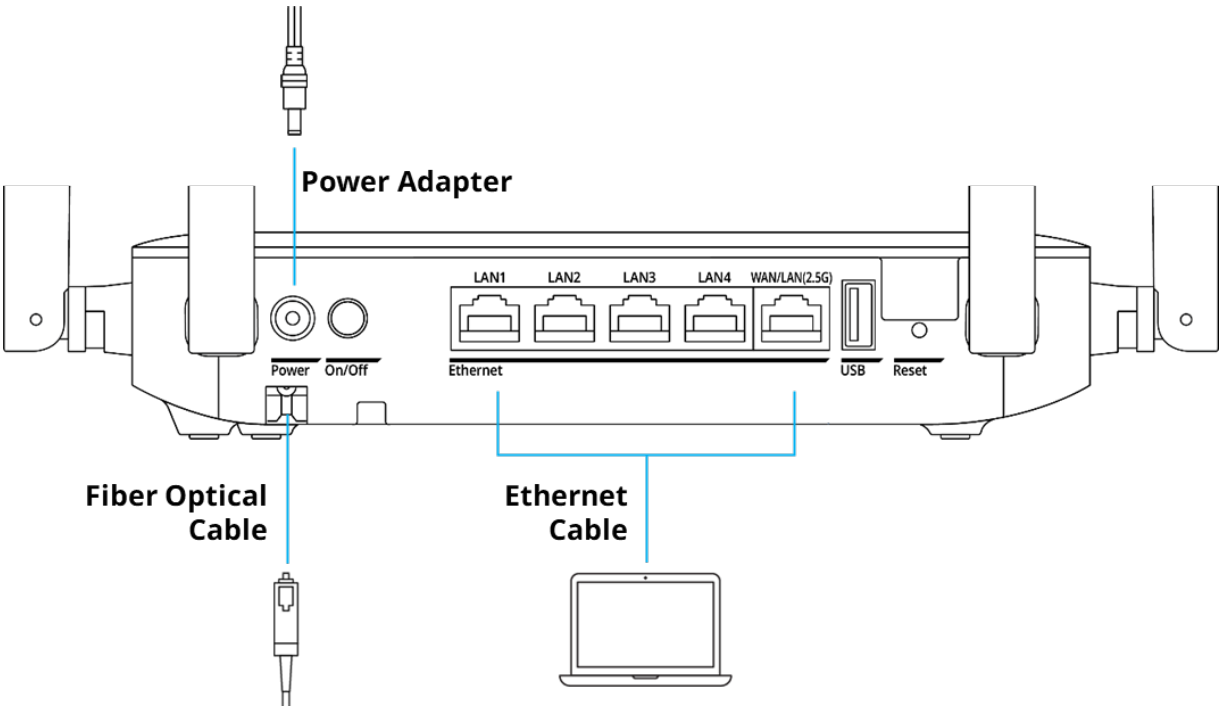
When you install your device, some tips make the Wi-Fi network more stable and robust at home.

- Locate your device near the center of the area where PC and other devices operate. The center will be the best place for optimum connection.
- Please install this device in a place where there are no objects such as PC or wall within 10cm from the front, rear, left, right, and top.
- Place your device in the location where it can be connected to various devices as well as to a power source.
- Safely place the cables and power cord out of the way so they do not create a tripping hazard.
- Place your device in an elevated location, minimizing the number walls and ceilings between the device and your other devices.
- Keep away from the intense electromagnetic radiation and the device of electromagnetic sensitive.
- Stand your device on a flat surface in an upright position not to tilt it.

2.2 Connection

Connect the DC power adaptor from the power connector to the electric outlet. If the power successfully turns on, a Power LED at the front panel turns on.

Note: Be sure to use the power adaptor provided.



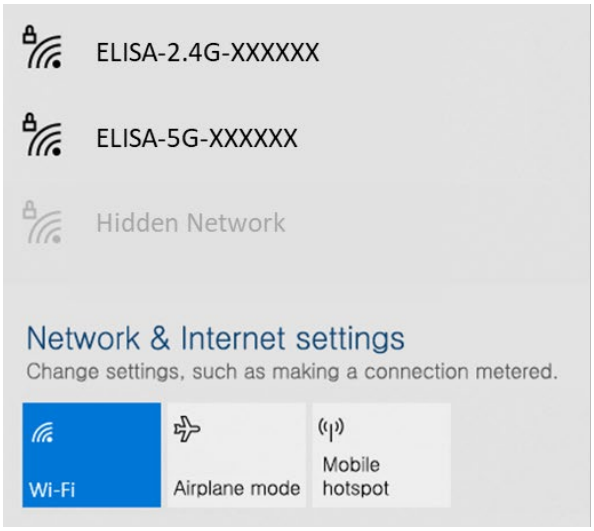
Connect the Devices (PC, etc.)

Over wired Ethernet connection

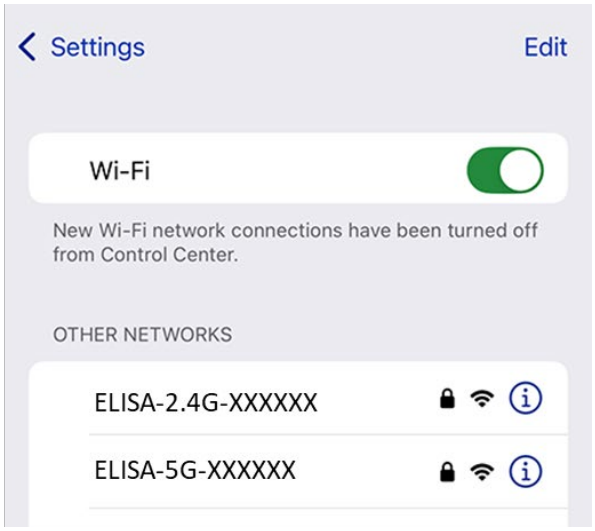
① Connect network devices such as PC, IPTV, OTT or game console using an Ethernet cable.

Wirelessly

① Go to the Wi-Fi setting menu on your network devices.



PC



Mobile

② Select the network name (SSID) of your device from the Wi-Fi list and enter the password. If the network name is not shown, you need to enter it manually. The default network name (SSID) and password are printed on the bottom of the device.

If there is no Network Name (SSID) you are looking for, you can also connect by manually entering the Network Name (SSID).

Using WPS button

If your network device supports WPS, you can connect it to the device by simply pressing the WPS button.

① Press the WPS button on your device within 2 minutes.

Note:

- Place your network device close to the device during WPS configuration.
- If security is set to WPA3-SAE, the WPS function is disabled and does not work.
- If Hide SSID is set to On, connection through the WPS button is not possible.

Chapter 3. Logging into Your Device

This device can be used to check the device status and set various settings using a **Web or mobile browser**.

The screen resolution may vary depending on the device you are accessing.

Mobile Browser

Mobile browsers are suitable for checking device status and basic configuration settings.

Pre-connection Check

Your mobile device must be connected to the device's Wi-Fi network. Connection status can be verified in your mobile device's Wi-Fi settings.

Recommended Environment

- iOS Safari browser
- Android Chrome browser
- Other default mobile browsers

Web Browser

Web browsers are recommended for advanced settings and detailed environment configuration.

Recommended Environment

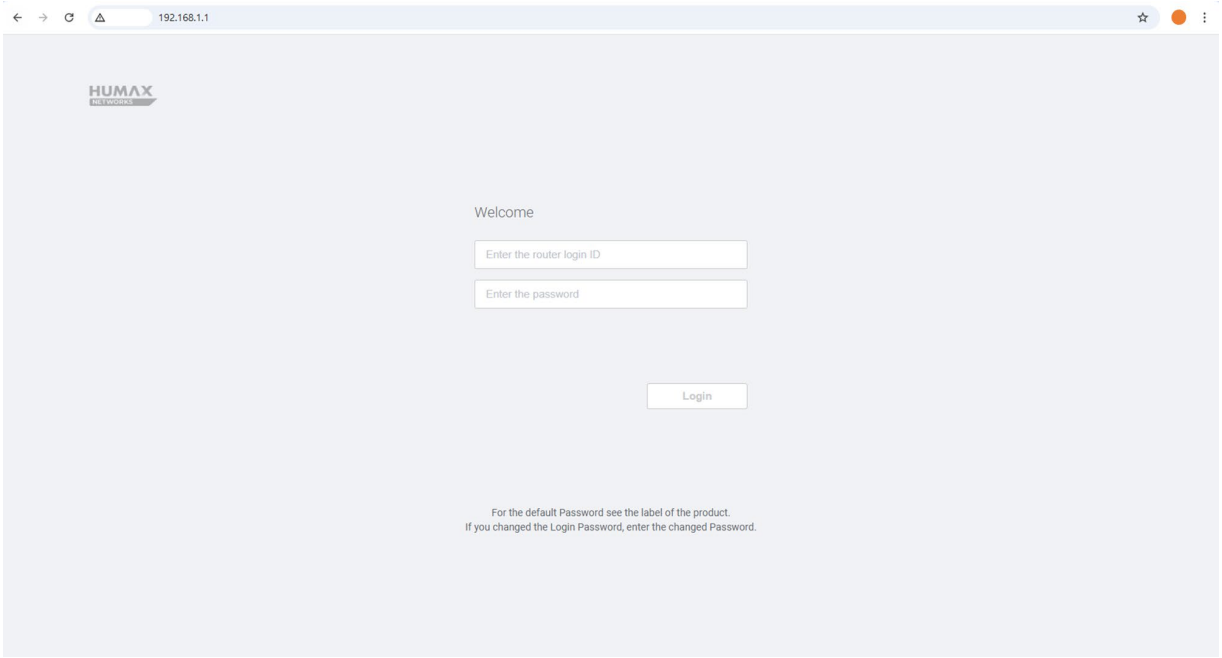
* Microsoft Windows 7 or later - Microsoft Edge 80 or later - Internet Explorer 10 or later - Google Chrome 23 or later - Firefox Mozilla 21 or later - Opera 15 or later	* MAC OS 10.7 or later - Safari 6 or later
* iOS 10.3 or later - Safari 6 or later	* Android 6.0 or later - Google Chrome 23 or later

3.1 Access to Web UI through Web/Mobile Browser

When you access the Web UI, you need to set up the login ID and password.

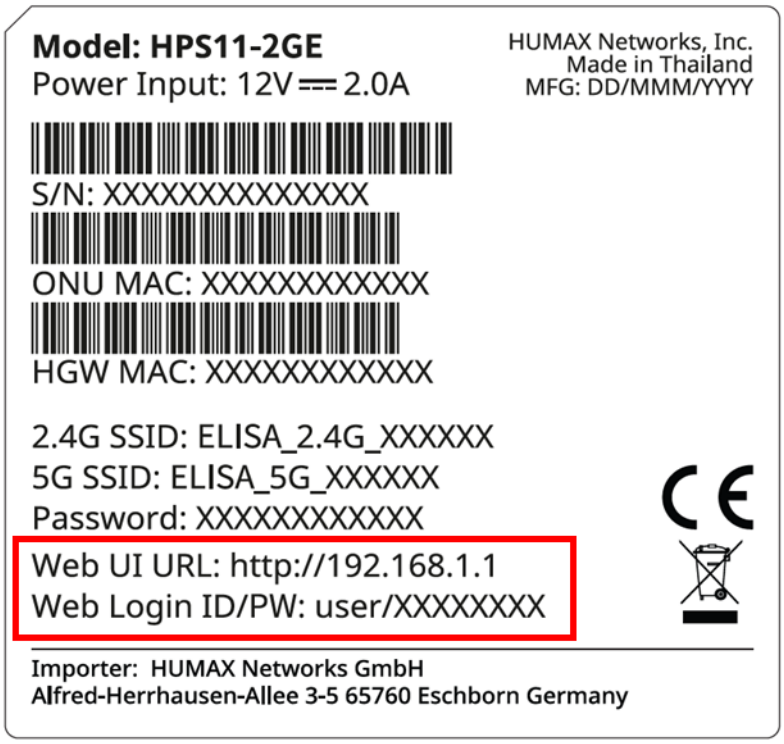
① Open the web/mobile browser.

② Enter **http://192.168.1.1** to the address bar, and then press the **Enter** key.



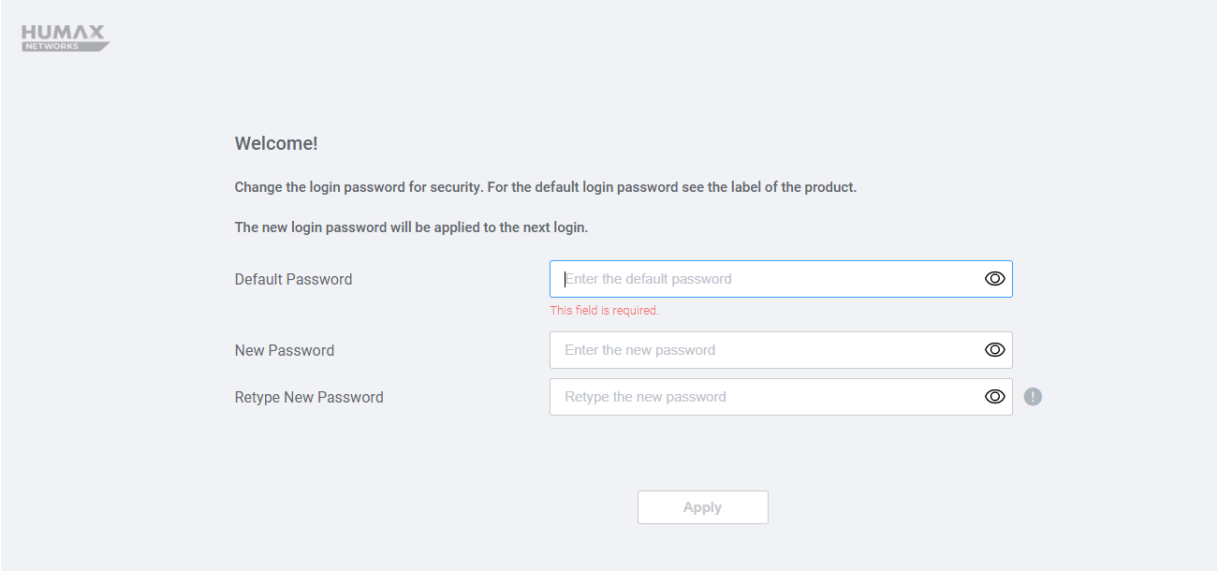
③ Enter the **default ID and password** to login to the user interface.

The default ID and password is printed on the device label.



※ 'XXXXXX' is a combination of 8 letters, numbers, and uppercase and lowercase letters that are different for each device, so you should check the label of the actual device.

④ When you first enter the Web UI, you can change your password.



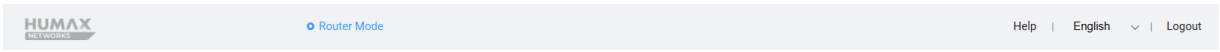
Note:

- The new password can be from 6 to 64 characters A-Z, a-z, 0-9, and all characters. A combination of letters and numbers is recommended.
- If you lose your password, you must perform a factory reset, which will erase all custom settings.

Chapter **4. Knowing Connection Status**

4.1 Quick Menu

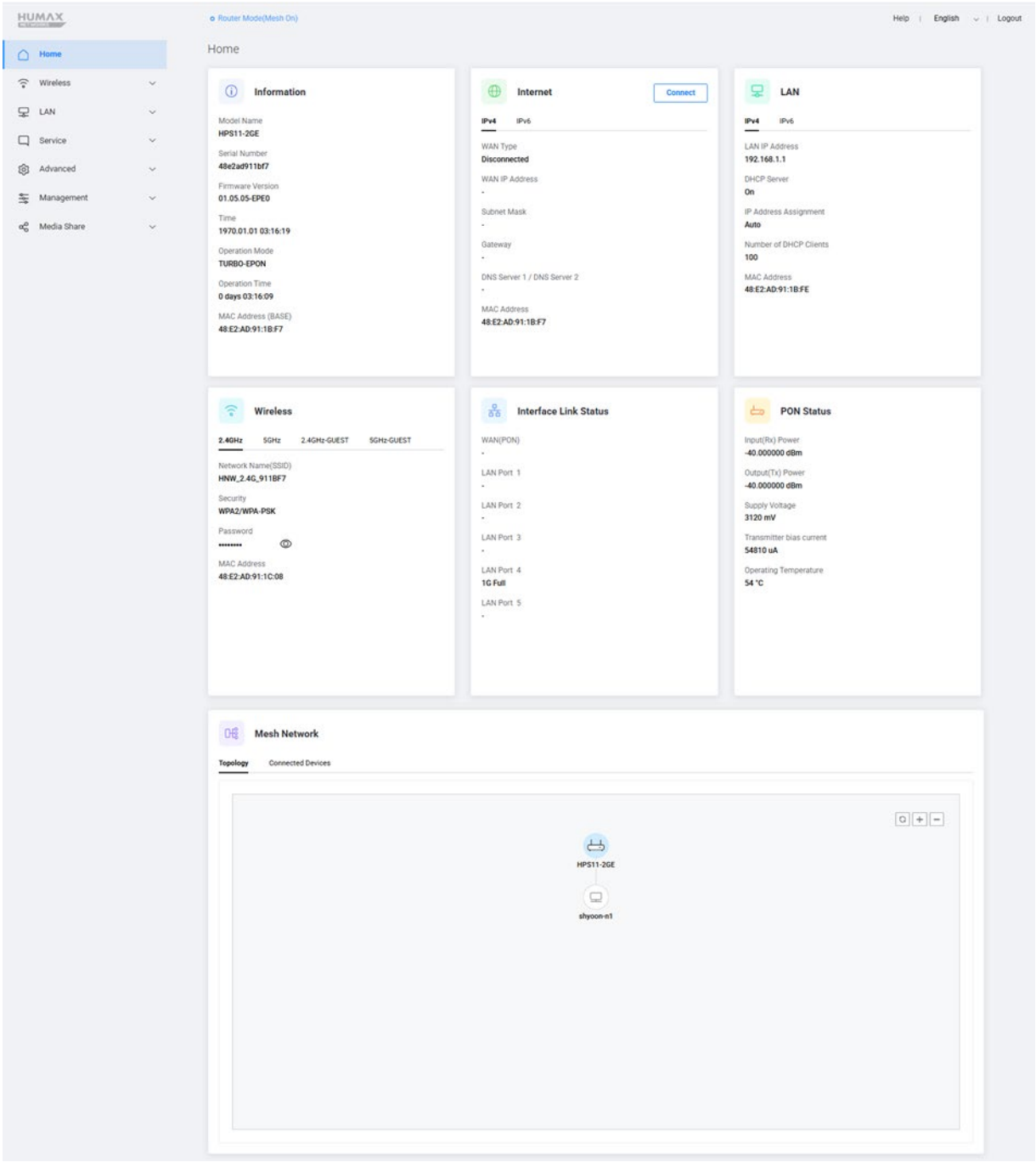
You can see the quick menu at the top right. Using the quick menu, you can check the operation mode and simply change the system environment.



- **HUMAX Networks Logo**
- **Operation Mode:** Means the current operation mode of the device.
- **Help:** If you click this hyperlink, display the help message popup.
- **Language:** Set the language to display the WEB UI.
- **Logout:** Press this button to logout of Web UI.

4.2 Home Menu

You can see the information on the **Information**, **Internet, LAN, Wireless, Interface Link Status, PON Status, Mesh Topology and Connected Devices** in the HOME menu.



Chapter 5. Setting Wireless Network

5.1 Basic Wireless Setting

This page configures each frequency used in your wireless.

This model is a dual-band model, providing a total of two frequencies (2.4GHz, 5GHz).
Each frequency has different characteristics in terms of range, speed, interference, and supported devices. Understanding the differences between these bands can help you optimize wireless network performance for your specific environment and requirements.

Feature	2.4 GHz	5 GHz
Range	Long range	Shorter range than 2.4 GHz
Speed	Up to 600 Mbps (theoretical)	Up to 3.5 Gbps or more
Interference	High interference (crowded)	Less interference
Number of Channels	Fewer channels (3 non-overlapping)	More channels (19 non-overlapping)
Device Compatibility	Supported by most devices	Supported by modern devices
Use Cases	General browsing, IoT, long range	Streaming, gaming Fast data

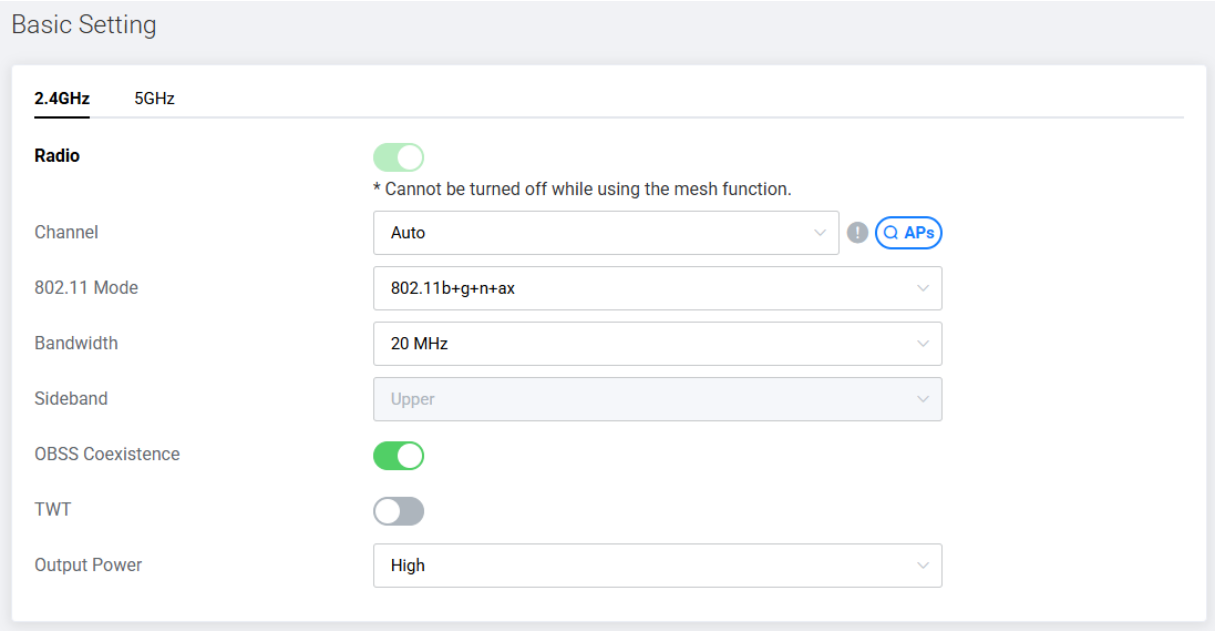
Using the Band Steering function, you can divide the wireless by frequency or use it as one SSID.
Please refer to section '*5.2 Primary Wireless Setting*' for details.

5.1.1 2.4GHz

Settings for the 2.4GHz frequency.
(*Do not change default settings unless it is necessary.)

① Enter the **Wireless > Basic Setting.**

2.4GHz



② Enter the option values:

Display	Description
Radio	Enable or disable the 2.4GHz wireless network. • If you turn it off, all the options below will disappear, and you cannot use 2.4GHz wireless network. The default value is '**On**'. • Radio cannot be turned off if Mesh Setting is set.
Channel	Select an operating channel for the 2.4GHz wireless network. • The default value is '**Auto**' that enables selecting an optimal channel for the current network environment. You can also set it to a manual channel (1-13). • If you press the APs button, you can check the surrounding 2.4GHz frequency usage.
802.11 Mode	Select 802.11 mode according to your wireless client devices to allow 802.11 supported devices on your wireless network. • Available: 802.11b, 802.11b+g, 802.11b+g+n, 802.11 b+g+n+ax • It is recommended to select the highest level of 802.11 mixed mode to ensure compatibility with previous versions. • The default value is '**802.11 b+g+n+ax**'
Bandwidth	Select a bandwidth for the 2.4GHz wireless network. • The default setting is '**20MHz**'.

Display	Description
Sideband	Set the sideband. • When using channels 5-9, you can select either the upper channel or lower channel when the bandwidth is set to 40MHz. • Available: Lower, Upper
OBSS Coexistence	Enable or disable the OBSS Coexistence. • The default setting is '**On'**.
TWT	Enable or disable the TWT((Target Wake Time). • TWT (Target Wake Time) is a Wi-Fi 6 (802.11ax) power-saving feature that extends battery life by scheduling when devices wake up to send or receive data. This feature reduces network congestion and improves efficiency, particularly in environments with multiple IoT devices. • The default setting is '**Off'**.
Output Power	Set the radio signal strength. • You can select one from "High," "Medium," and "Low." > High (Default): Outputs the maximum wireless signal strength. > Medium: 25% reduction in 'High' output. > Low: 50% reduction in 'High' output • If you lower the signal strength, your wireless range may be reduced.

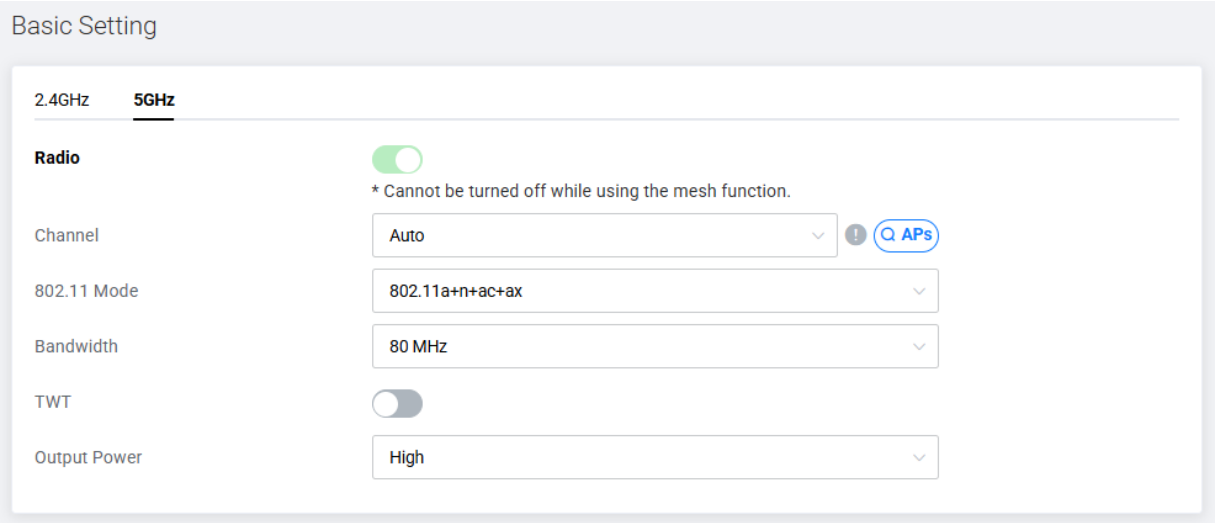
5.1.2 5GHz

Settings for the 5GHz frequency.

(*Do not change default settings unless it is necessary.)

① Click the **5GHz** tab.

5GHz



② Enter the option values:

Display	Description
Radio	Enable or disable the 5GHz wireless network. • If you turn it off, all the options below will disappear, and you cannot use 5GHz wireless network. The default value is On. • Radio cannot be turned off if Mesh Setting is set.
Channel	Select an operating channel for the wireless network. • The default value is '**Auto**' that enables selecting an optimal channel for the current network environment. You can also set it to a manual channel (36~140, 19 Channels). • If you press the APs button, you can check the surrounding 5GHz frequency usage.
802.11 Mode	Select 802.11 mode according to your wireless client devices to allow 802.11 supported devices on your wireless network. • Available: 802.11a, 802.11a+n, 802.11a+n+ac, 802.11a+n+ac+ax • It is recommended to select the highest level of 802.11 mixed mode to ensure compatibility with previous versions. • The default value is '**802.11a+n+ac+ax'**
Bandwidth	The available bandwidth values vary depending on the selected Channel and 802.11 Mode. • The default setting is '**80MHz'**.

Display	Description
TWT	Enable or disable the TWT((Target Wake Time). • TWT (Target Wake Time) is a Wi-Fi 6 (802.11ax) power-saving feature that extends battery life by scheduling when devices wake up to send or receive data. This feature reduces network congestion and improves efficiency, particularly in environments with multiple IoT devices. • The default setting is '**Off**'.
Output Power	Set the radio signal strength. • You can select one from "High," "Medium," and "Low." > High: (Default): Outputs the maximum wireless signal strength. > Medium: 25% reduction in 'High' output. > Low: 50% reduction in 'High' output • If you lower the signal strength, your wireless range may be reduced.

Note:

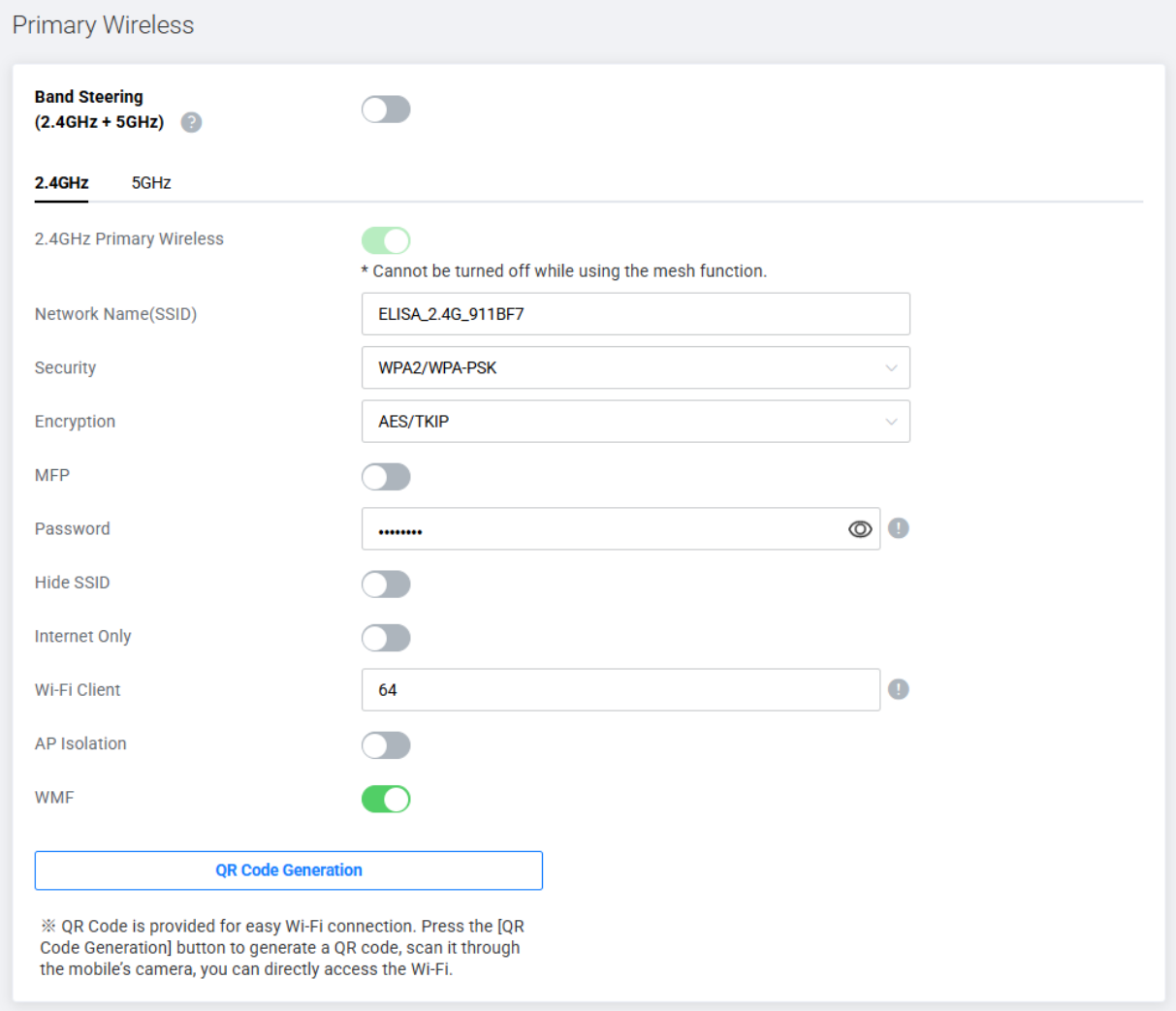
- If a radar signal is detected during communication, the communication may be temporarily interrupted because the DFS function automatically changes the channel.
- Depending on the environment, it may be connected with a lower bandwidth than the actual setting.

5.2 Primary Wireless Setting

Set up the main wireless network.

The configuration on both 2.4GHz and 5GHz network is identical to each other. Therefore, how to configure the 2.4GHz wireless network will be described and the description for the 5GHz wireless network will be omitted.

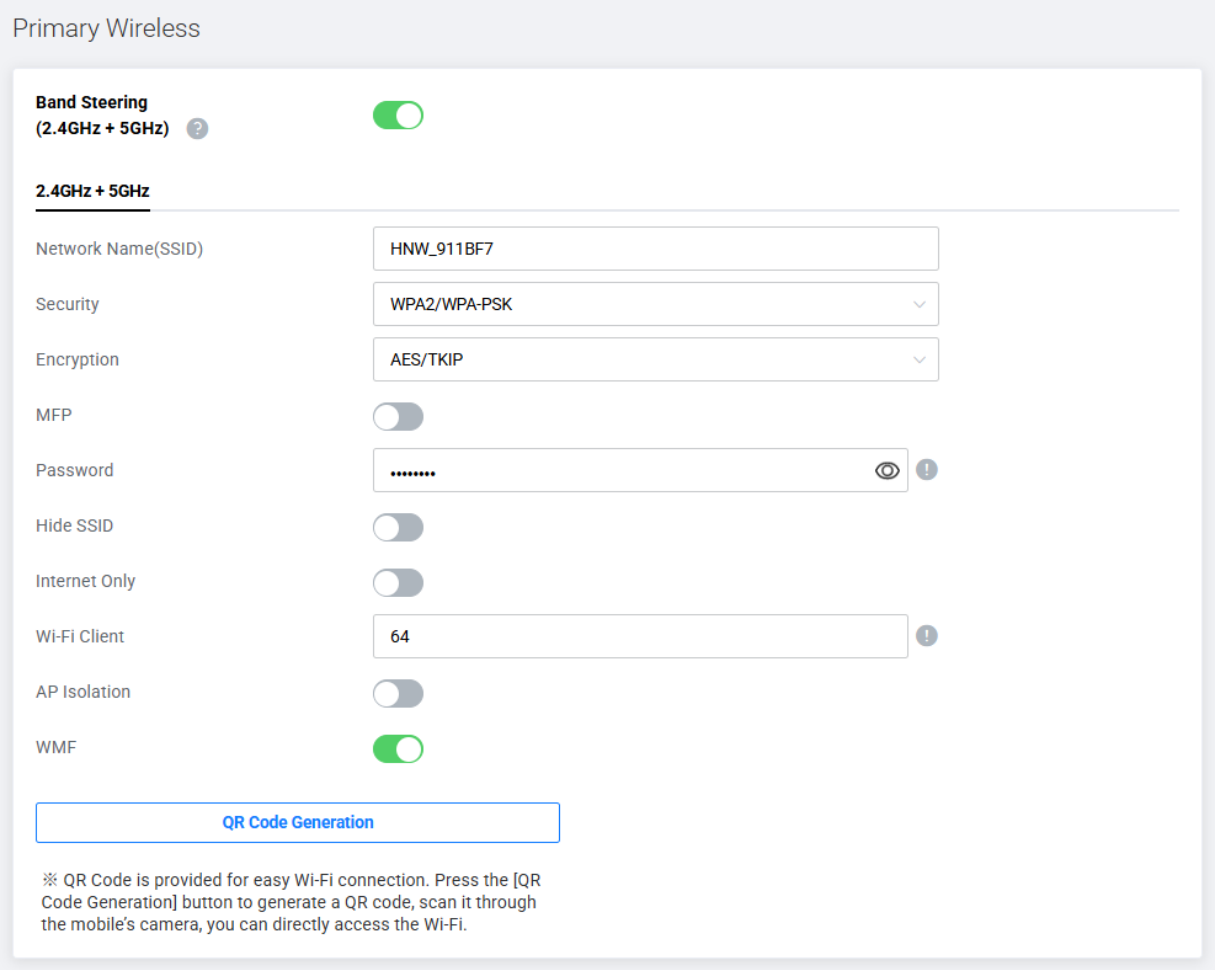
① Enter the **Wireless > Primary Wireless**.



.

5.2.1 2.4GHz+5GHz

When Band Steering is enabled, 2.4GHz and 5GHz bands operate under a single SSID, providing optimal wireless connection and simplified network management across both frequency bands.



Display	Description
Network Name (SSID)	Enter a network name of your device if you want to change it. • You can enter up to 32 characters a-z, A-Z, 0-9, and special characters, and they are case sensitive. • The default Network Name(SSID) is printed on the label of your device.

Display	Description
Security	Select a security type for your device. • Your device provides None, WPA2-PSK, WPA2/WPA-PSK, WPA3-SAE and WPA2-PSK/WPA3-SAE Mixed. > None : No security is applied. This option leaves your network open to the public and is not recommended unless you are creating a guest or test network. > WPA2-PSK : Offers strong security using AES encryption. Recommended for most modern devices. Compatible with Wi-Fi 4, 5, and 6 clients. > WPA2/WPA-PSK : Provides compatibility with both newer (WPA2) and older (WPA) devices. Use this mode only if you have legacy clients that do not support WPA2. > WPA3-SAE : Provides the highest level of security with enhanced protection against brute-force attacks. Only supported by newer devices (Wi-Fi 6 and above). > WPA2-PSK/WPA3-SAE : Mixed mode offering both WPA2 and WPA3 compatibility. Ideal for networks with a mix of legacy and modern devices. • If your Wi-Fi client supports it, you should consider setting the security mode accordingly. We recommend choosing WPA3-SAE/WPA2-PSK or WPA2-PSK.
Encryption	Select an encryption type to protect the data of the users who have connected to the wireless network. > AES provides the most robust encryption. > AES/TKIP offers strong encryption with improved backward compatibility. • The default setting is '**AES/TKIP**'.
MFP	Enable or disable the MFP(Management Frame Protection) • Sets client devices that support the MFP(Management Frame Protection) function to communicate with enhanced security.
Password	Enter the password of the Wi-Fi network. • You can enter the only a~z, A~Z, 0~9, and special characters !) + . _ : ? ~ $ ' " < , / , and they are case-sensitive. • The default password is printed on the label of your device. • This will be required when you connect a mobile device wirelessly to your wireless network.

Display	Description
Hide SSID	Enable or disable the Hide SSID. • You can prevent other users from detecting your network when they scan for the available wireless network.
Internet Only	Enables or disables the feature that allows only Internet access. • Users connected to that Wi-Fi cannot communicate with each other over the internal network and cannot enter the Web UI.
Wi-Fi Client	Set the maximum number of allowed wireless clients. • The value can be set between 1 and 75.
AP Isolation	Enable or disable AP Isolation. • AP Isolation prevents wireless clients connected to the same access point from communicating with each other, enhancing network security.
WMF	Enable or disable the WMF(.(Wireless Multicast Forwarding) • WMF optimizes network traffic by forwarding multicast data only to intended wireless clients, improving overall network performance.

② Click **Apply** to save the changes.

Tips: Scanning the QR Code makes it easier to access Primary Wireless.

If you press [Generate the QR Code], a QR Code with Primary Wireless information on the right is created. Scan the QR Code on your mobile, and you will be connected directly to the Wireless.

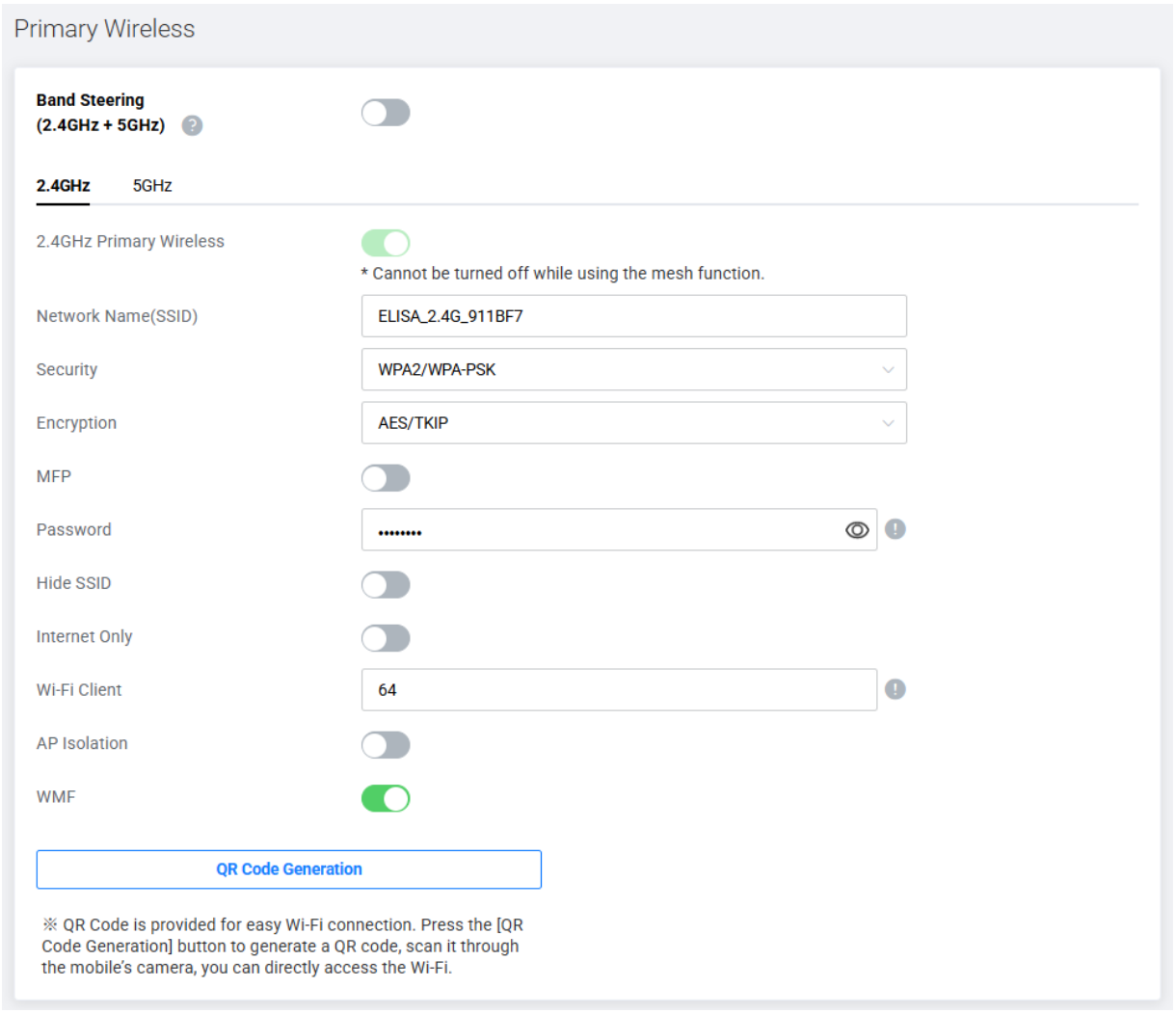
Note:

- The default network name(SSID) and password is printed on the label of your device.
- If the SSID is hidden, some devices may not detect the Wi-Fi network of your device. You need to search the SSID to connect to the Wi-Fi network manually. Connection through the WPS button is not possible.
- The WPS feature is available when the security level has been set to 'None', 'WPA2-PSK', 'WPA2/WPA-PSK', or 'WPA3-SAE/WPA2-PSK'. The WPS feature will not be available when the security level has been set to "WPA3-SAE."
- When the security is set to WPA3-SAE, only clients that support WPA3-SAE can access it.

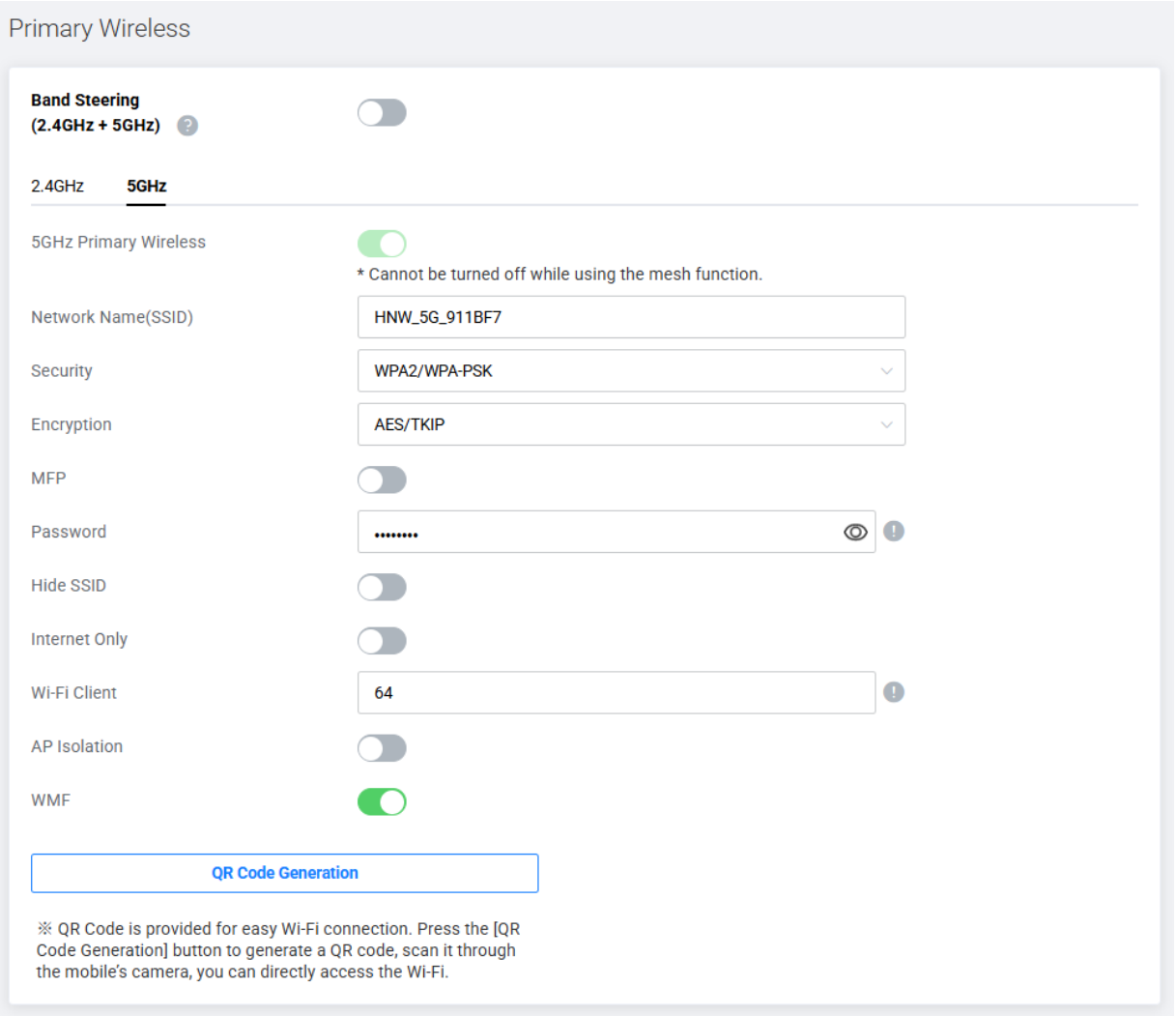
5.2.2 2.4GHz, 5GHz

When Band Steering is disabled, 2.4GHz and 5GHz bands operate independently with separate SSIDs, allowing manual selection of frequency bands.

2.4GHz



5GHz



- The description for each item is the same as '5.2.1 2.4GHz+5GHz', so please refer to that item.

② Click **Apply** to save the changes.

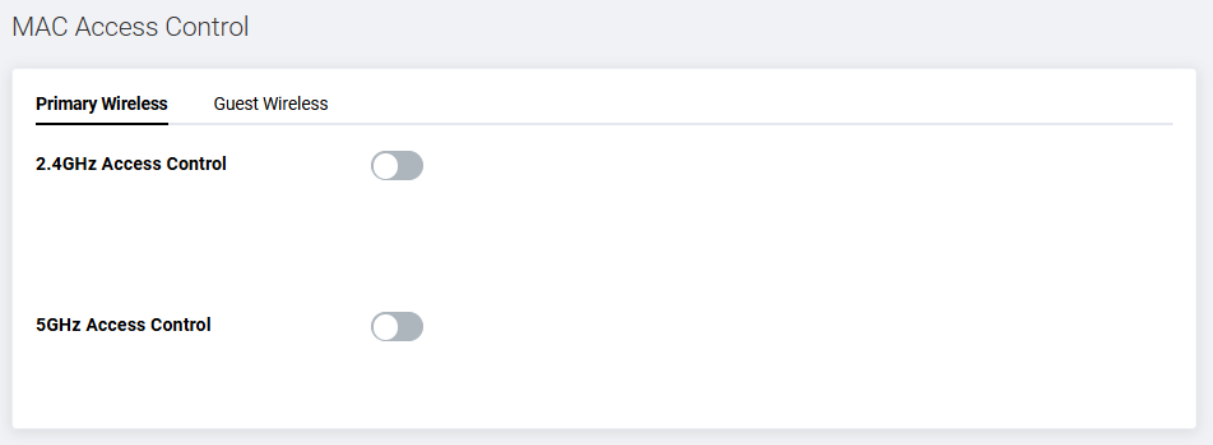
Tips: Scanning the QR Code makes it easier to access Primary Wireless.

If you press [Generate the QR Code], a QR Code with Primary Wireless information on the right is created. Scan the QR Code on your mobile, and you will be connected directly to the Wireless.

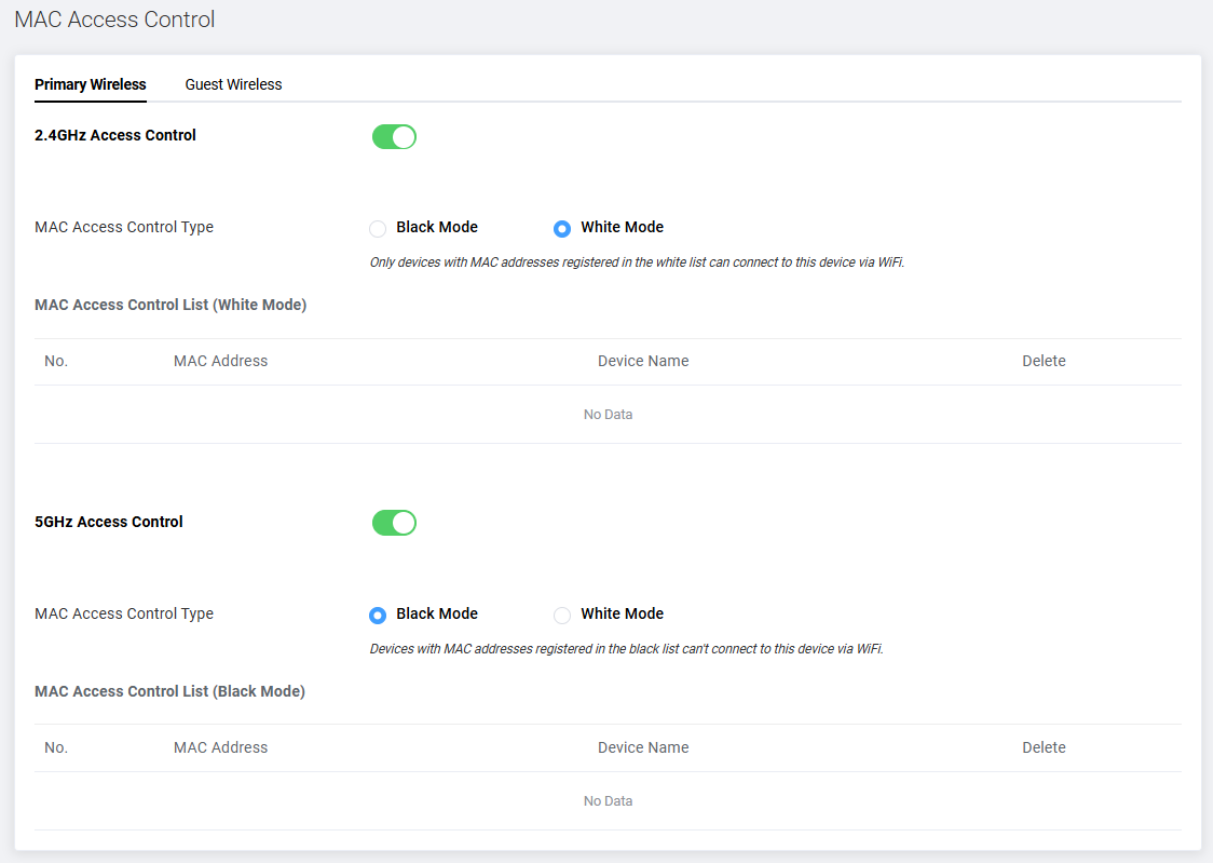
5.3 MAC Access Control

Manage the MAC address you want to allow/reject connections. You can set up Primary Wireless and Secondary Wireless separately, and the setup method is the same.

① Enter the **Wireless > MAC Access Control**.



② Turn **On** the wireless type you wish to allow/reject access to.



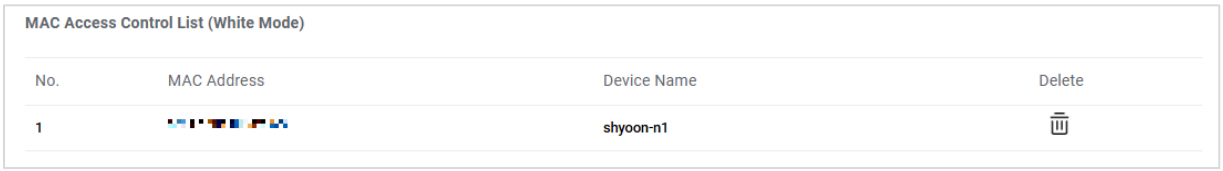
You can set Primary Wireless 2.4GHz and 5GHz to Black Mode or White Mode respectively.

• **Black Mode**: Register/manage MAC addresses that do not allow access.

• **White Mode**: Register/manage MAC addresses that allow access. Unregistered devices cannot connect to the wireless.

Note:

When setting White Mode, if there are no registered devices, no device will be connected wirelessly. If there are no registered devices, all existing devices will be disconnected. In this case, you can connect to another available wireless or wired connection and then connect to the Web UI. Be careful when setting. (* When you select White Mode and press the [OK] button in the pop-up that appears, it will be applied immediately, so be careful.)



MAC Access Control List

It shows the rules set by the user. You can delete them individually by pressing the **Delete** button.

To add an item

To add a new entry, click the **Add** button at the bottom. You can add up to 32 rules.

① Click **Add** to add a rule.



② Select the wireless type (SSID) you want to set up.

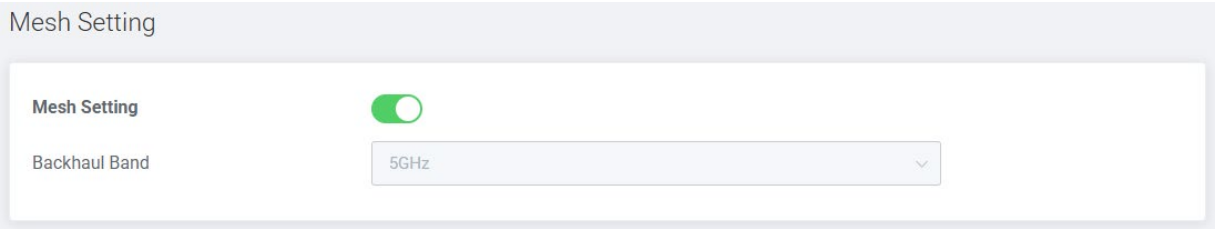
③ Select a device from the list of connected devices. You can enter the MAC address if there is no device name in the list. In this case, you do not need to enter the Device Name.

④ Click **Apply** to save the changes.
You can see the list of registered MAC addresses.

5.4 Mesh Setting

Set whether to use Mesh function.

① Enter the **Wireless > Mesh Setting**.



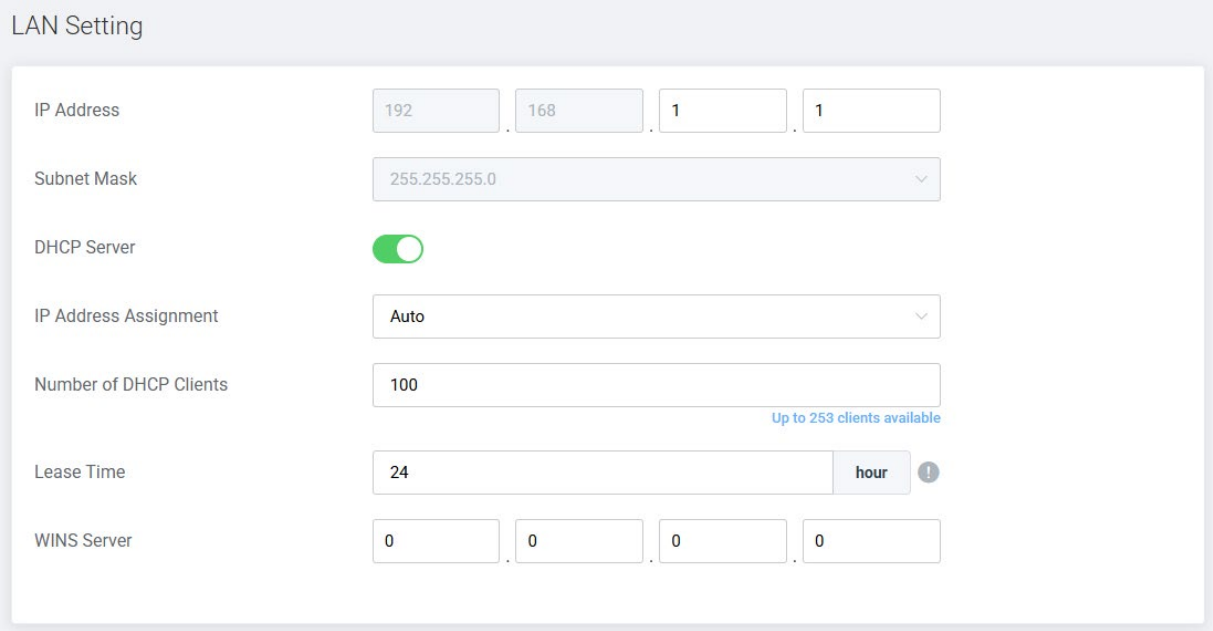
Display	Description
Mesh Setting	Enable or disable the Mesh Setting. • The default setting is '**On**'.
Backhaul Band	Set the frequency to use when connecting to the Mesh Network with Agent. • The default setting is '**5GHz**'.

Chapter 6. Setting Local Setting

6.1 LAN Setting

You can set LAN IP address, subnet mask, and DHCP server and allocate specific IP addresses to MAC address.

① Enter the **LAN > LAN Setting**.



② Enter the options.

Display	Description
IP Address	Enter the IP address of your device. • You can access the web UI page via the IP address. • The default value is '**192.168.1.1'.**
Subnet Mask	Display the subnet mask value.
DHCP Server	Enables or disables the use of a DHCP server to assign IP addresses to devices connected to the local network.

Display	Description
IP Address Assignment	Set the IP address allocation type via the DHCP server. • If set to '**Auto'**, IP addresses will be automatically allocated as many as the number of allocatable IP addresses (Client Account). • If set to '**Manual'**, IP addresses will be allocated within the given range as many as the number of allocatable IP addresses starting from the start IP address.
Start IP Address	Set the starting address for the DHCP server to begin assigning IP addresses.(*Only if IP Address Assignment is set to '**Manual'**)
Number of DHCP Client	Set the maximum number of devices that will be connected. • The maximum number of devices that can be connected is provided below the settings field.
Lease Time	Set the time duration for the connected device to stay connected using the assigned IP. • The default setting is **'24 hours'.**
WINS Server	Enter the address for the WINS server to notify the DHCPv4 client.

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

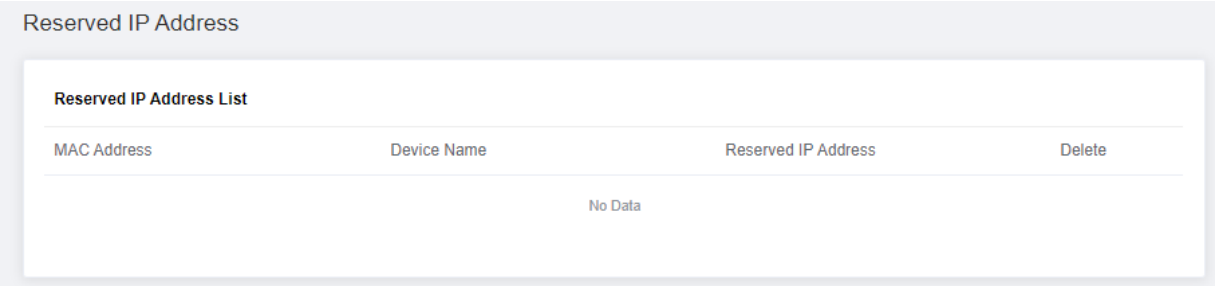
Note:

- If DHCP server is turned off, connected clients cannot automatically obtain addresses within the local network range. In this case, addresses must be manually configured on client devices.
- Incorrect settings can cause connection problems. It is recommended to use the default value.
- If the IP address has changed, you will need to restart the system. The phone cannot be used during reboot, and after reboot, you need to access the web page with the new address.

6.2 Reserved IP Address

You can allocate IP addresses to MAC address. Your device is allocated for the same IP address whenever accessing the DHCP server. Allocating IP address is similar to configuring static IP address.

① Enter the **LAN > Reserved IP Address**.



Reserved IP Address List

It shows the rules set by the user. You can delete them individually by pressing the **Delete** button.

To add an item

Click **Add** to add a rule. You can add up to 32 rules.

② Click **Add** to add a rule.



③ Select a device from the list of connected devices. You can enter the MAC address if there is no device name in the list. In this case, you do not need to enter the Device Name.

④ Enter the last digit of IP address to allocate to the selected device.

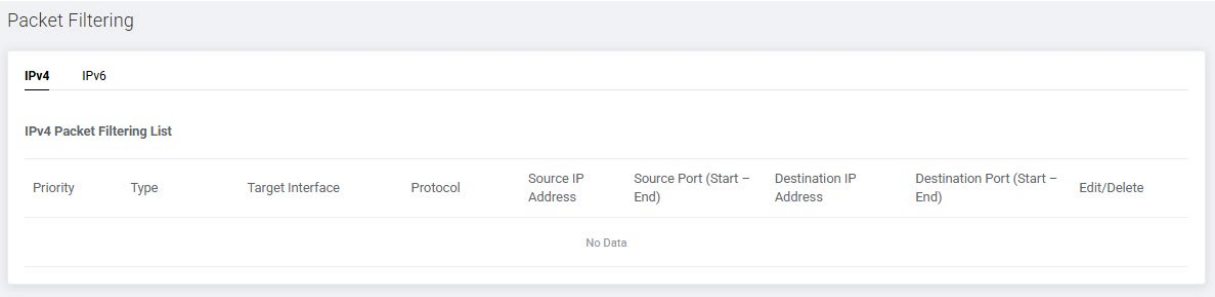
⑤ Click **Apply** to save the changes.

You can see the list of reserved IP address.

Chapter 7. Providing Network Service

7.1 Packet Filtering

① Enter the **Service** > **Packet Filtering**.



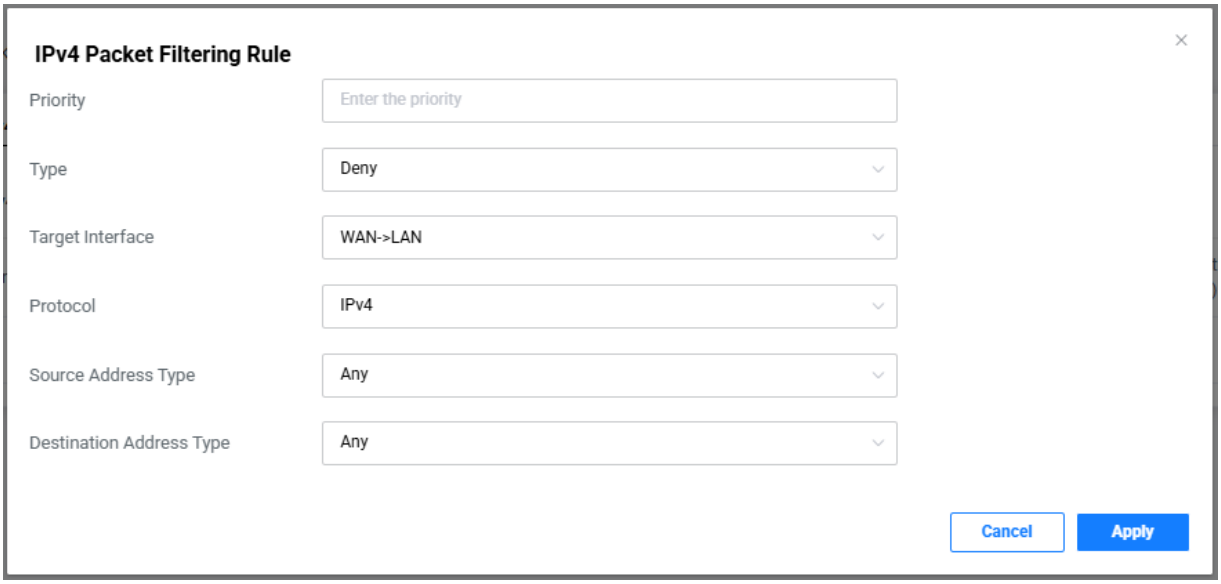
IPv4 Packet Filtering List

Shows the rules set by the user. Each item can be turned **On** or **Off**, and can be individually edited or deleted by pressing the **Edit** or **Delete** button.

To add an item

Click **Add** below to register a new rule. You can add up to 32 rules.

① Click **Add** to add a rule.



② Enter the option values:

Display	Description
Priority	Enter the priority of the IPv4 (or IPv6) filtering conditions. You can enter a value from 1 to 32.
Type	Set Deny/Allow for packets matching the filter condition.
Target Interface	Set the direction in which the set packet is delivered.
Protocol	Select the type of IP protocol to be filtered.
Source Address Type	Set the source IP address type of the packet to be filtered. > Any: If you want to perform filtering on packets originating from all IP addresses. > Localhost: If you want to perform filtering only the packets of this product. > IPv4: If you only want to filter packets coming from specified IP addresses, enter the appropriate IP Address value.
Destination Address Type	Select the type of destination IP address to be filtered. Enter the appropriate IP Address value according to the selected value.

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

You can see the list of packet filtering rule.

Note:

IPv6 is the same, so explanation is omitted.

7.2 DDNS Setting

When DDNS is set, the specified domain name and the changed IP address are linked in real time, so that regardless of whether the IP address is changed or not, the corresponding IP address can be accessed through the domain name.

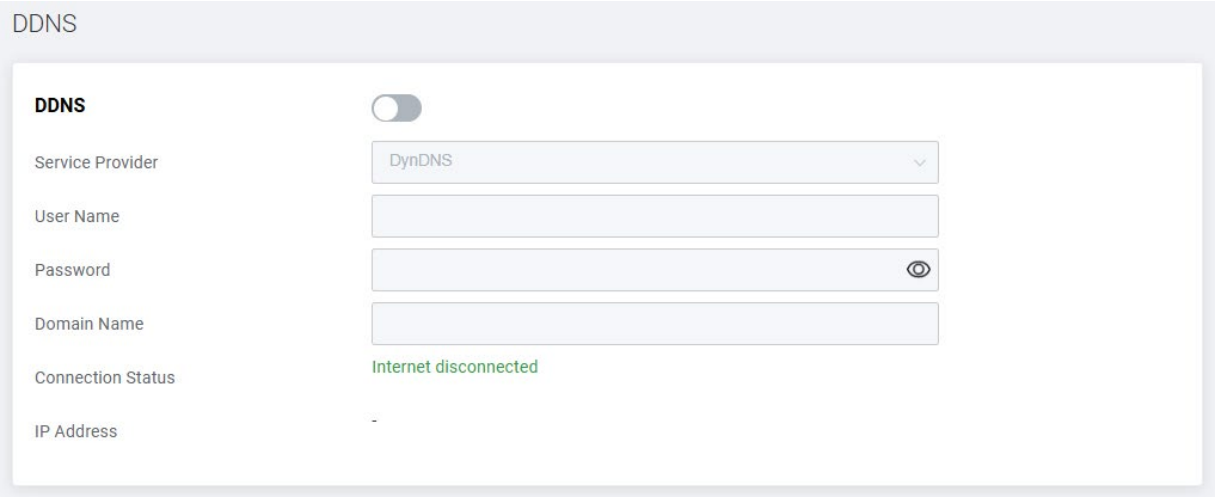
The DNS service supports Noip.com and dyn.com providers, and to the user, you need to subscribe to the service of the site.

Note:

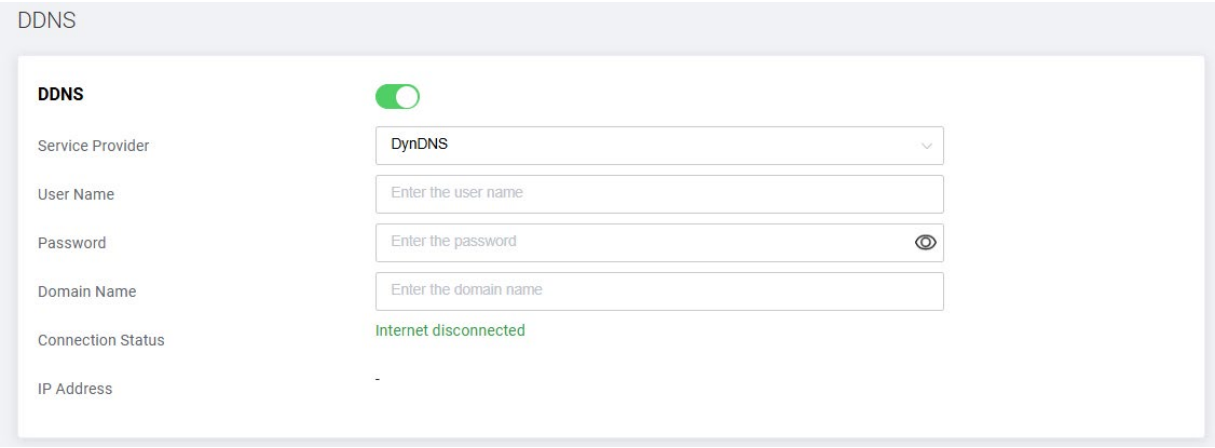
DNS services require prior registration with Noip.com or dyn.com. you must enter the registered username and password.

- DynDNS : account.dyn.com
- NoIP : https://www.noip.com/

① Enter the **Service > DDNS**.



② Toggle **On** to use a DDNS service.



③ Enter the option values:

Display	Description
Service Provider	Select a service provider. • Select either NoIP or DynDNS.
User Name	Enter the user name or account name provided by the selected service.
Password	Enter the password provided by the selected service.
Domain Name	Enter the domain name to be used. • A DDNS address will be generated with the name you have entered.
Connection Status	Displays the connection status to the DDNS server. You can check whether the actual DDNS service is available through the DDNS status message. - DDNS Update Successful: The generated DDNS is available for use. - DDNS Update Failed: The generated DDNS is not available for use. - Duplicated Hostname: The host name is already in use. Enter another host name. - Contact Service Provider: An error related to the service occurred. Contact your service provider for troubleshooting.
IP Address	Display the IP address for the DDNS.

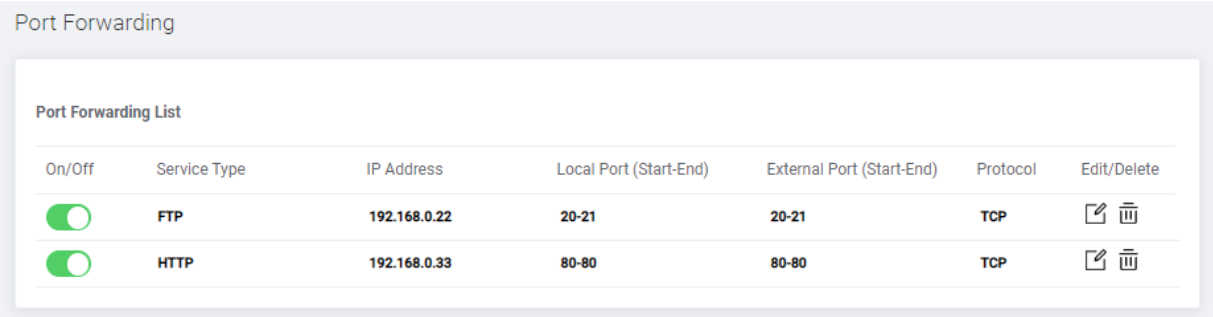
④ Click **Apply** to save the changes.

You can check whether the actual DDNS service is available through the DDNS status message.

7.3 Port Forwarding Setting

Port Forwarding is a Network Address Translation (NAT) application technique that allows direct transmission of data from an external network to a specific device within an internal network. This feature enables access to specific services or applications in the internal network from the outside.

① Enter the **Service > Port Forwarding**.



Port Forwarding List

Shows the rules set by the user. Each item can be turned **On** or **Off**, and can be individually edited or deleted by pressing the **Edit** or **Delete** button.

To add an item

Click **Add** below to register a new rule. You can add up to 32 rules.

① Click **Add** to add a rule.



② Enter the option values:

Display	Description
Service Type	Enter the service type or click the input box to select from predefined services. • When you select a predefined service, the local port, external port, and protocol will be automatically filled with the corresponding values. You can modify these values manually. • For manual entry, you can enter up to 16 characters.
IP Address	Enter the IP address of the internal client device running the application.
Local Port (Start-End)	Enter the service port number for the internal client device. • For a single port, enter the same value in both Start and End fields. • For a port range, enter different Start and End port values • Enter a number between 1 to 65535.
External Port (Start-End)	Enter the service port of the running application.
Protocol	Select the protocol to be used by the service program. • Available options: TCP, UDP, or TCP/UDP

Note:

- Multiple service applications can be run on a single device. In such cases, configure different port numbers for the same IP address. Note that the same port cannot be used on two different PCs.
- Since dynamically assigned IP addresses to vary, we recommend you allocate a static IP address.

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

7.4 DMZ Setting

You can configure the DMZ to make applications free from port restrictions.
When a PC is set to be a DMZ host in the local network, it is totally exposed to the Internet, which can realize the unlimited bidirectional communication between internal hosts and external hosts. The DMZ host becomes a virtual server with all ports opened. When you are not clear about which ports to open in some special applications, such as IP camera and database software, you can set the PC to be a DMZ host. But, in this case, all ports open, and it may cause security vulnerabilities.

① Enter the **Service > DMZ**.



② Toggle **On** to enable DMZ host configuration.

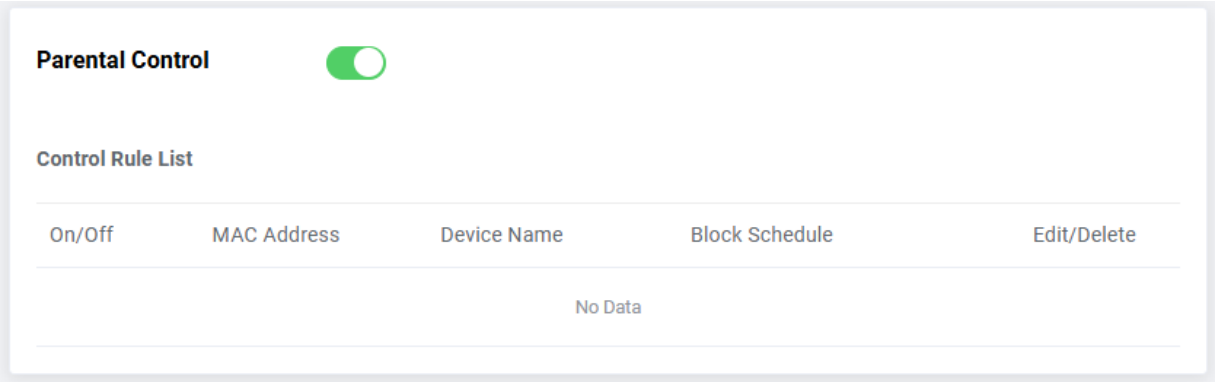


③ Enter the Destination (Host IP Address).

④ Click **Apply** to save the changes.

7.5 Parental Control Rules

① Enter the **Service** > **Parental Control**.



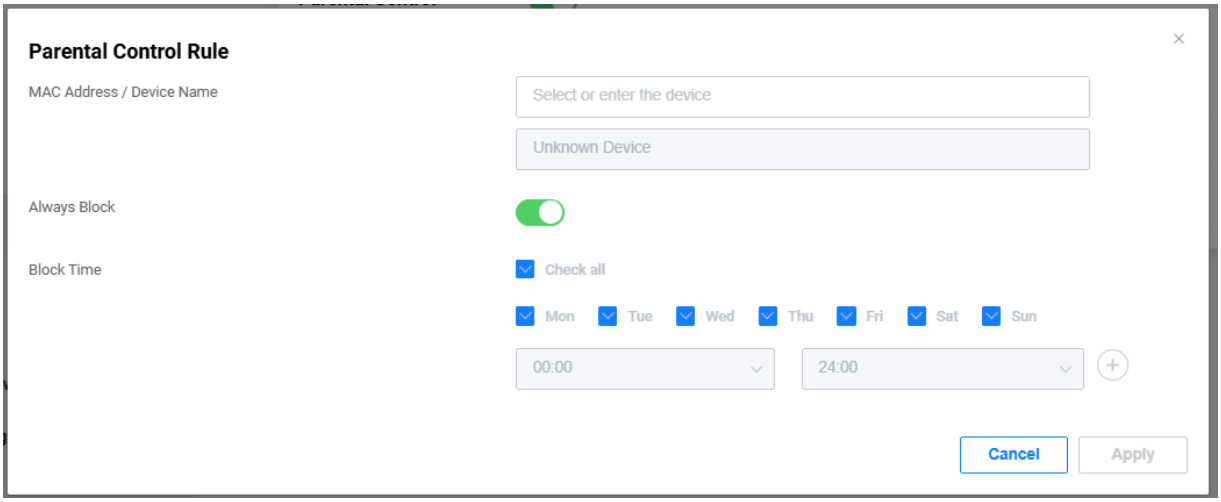
Control Rule List

Shows the rules set by the user. Each item can be turned **On** or **Off**, and can be individually edited or deleted by pressing the **Edit** or **Delete** button.

To add an item

Click **Add** below to register a new rule. You can add up to 6 rules.

① Click **Add** to add a rule.



② Enter the option values:

Display	Description
MAC Address/Device Name	Set the devices to which you want to restrict access. • Select a device from the list of connected devices. • You can enter the MAC address if there is no device name in the list. In this case, you do not need to enter the Device Name.
Always Block	Set whether to Always Block. • Enabling Always Block blocks Internet access for registered MAC addresses at all times.
Block Time	Set the blocking time and days. • Disabling Always Block allows you to configure dates and times for access control.

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

You can see the list of registered MAC addresses.

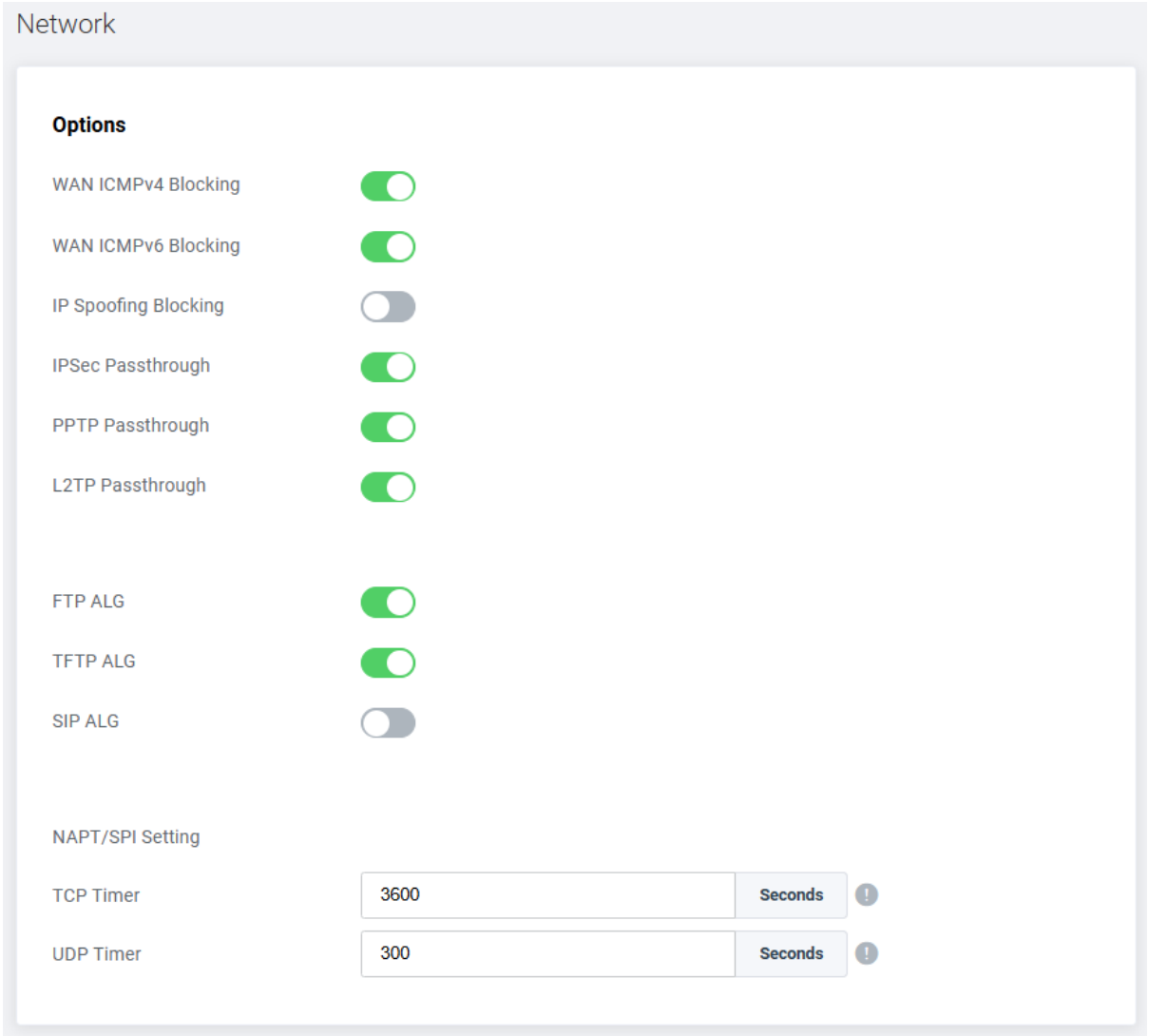
Chapter 8 Setting Advanced Options

You can set the advanced network options. If you are not familiar with network settings, we recommend not to change the settings in the advanced menus. Most users do not need to change these settings.

8.1 Advanced Network Setting

You can block network traffic from any source in several ways.

① Enter the **Advanced > Network**.



② Enter the option values:

Display	Description
WAN ICMPv4 Blocking	Set whether to block WAN ICMPv4. • Enabling WAN ICMPv4 Blocking blocks incoming ICMP packets from external networks, preventing ping requests and similar network diagnostics from outside sources.
WAN ICMPv6 Blocking	Set whether to block WAN ICMPv6. • Enabling WAN ICMPv6 Blocking blocks incoming ICMP packets from external networks, preventing ping requests and similar network diagnostics from outside sources.
IP Spoofing Blocking	Set whether to block IP Spoofing. •Enabling IP Spoofing Blocking prevents unauthorized access by blocking packets with forged (spoofed) source IP addresses.
IPSec Passthrough	Set whether to enable IPSec Passthrough. • Enabling IPSec Passthrough allows IPSec tunneled packets to pass through the device, enabling VPN connections that use IPSec protocol.
PPTP Passthrough	Set whether to enable PPTP Passthrough. • Enabling PPTP Passthrough allows PPTP tunneled packets to pass through the device, enabling VPN connections that use PPTP protocol.
L2TP Passthrough	Set whether to enable L2TP Passthrough. • Enabling L2TP Passthrough allows L2TP tunneled packets to pass through the device, enabling VPN connections that use L2TP protocol.
FTP ALG	Set whether to enable FTP ALG. • Enabling FTP ALG allows the device to recognize FTP traffic and handle port connections automatically for FTP transfers.
TFTP ALG	Set whether to enable TFTP ALG. • Enabling TFTP ALG allows the device to recognize TFTP traffic and handle port connections automatically for TFTP transfers.
SIP ALG	Set whether to enable SIP ALG. • Modern VoIP systems and devices often have built-in mechanisms to handle NAT and routing without the need for SIP ALG. In such cases, it is recommended to disable SIP ALG for professional VoIP setups, as it may conflict with the built-in NAT handling mechanisms.

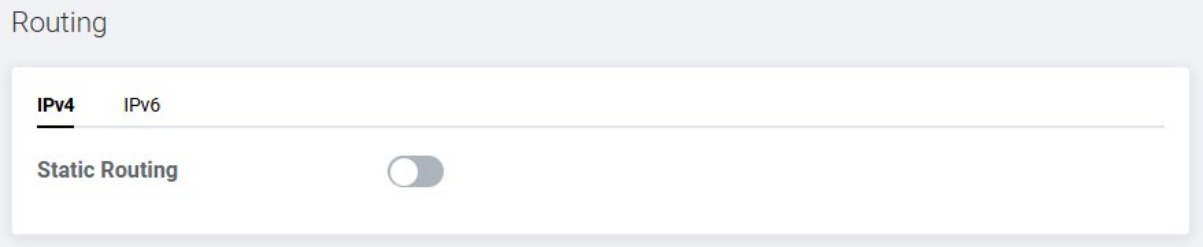
Display	Description
TCP Timer	Set the TCP timer value between 30 and 432000 (seconds). • The default value is '**3600** (seconds)'.
UDP Timer	Set the UDP timer value between 30 and 36000 (seconds). • The default value is '**300**(seconds)'.

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

8.2 Routing Rule Setting

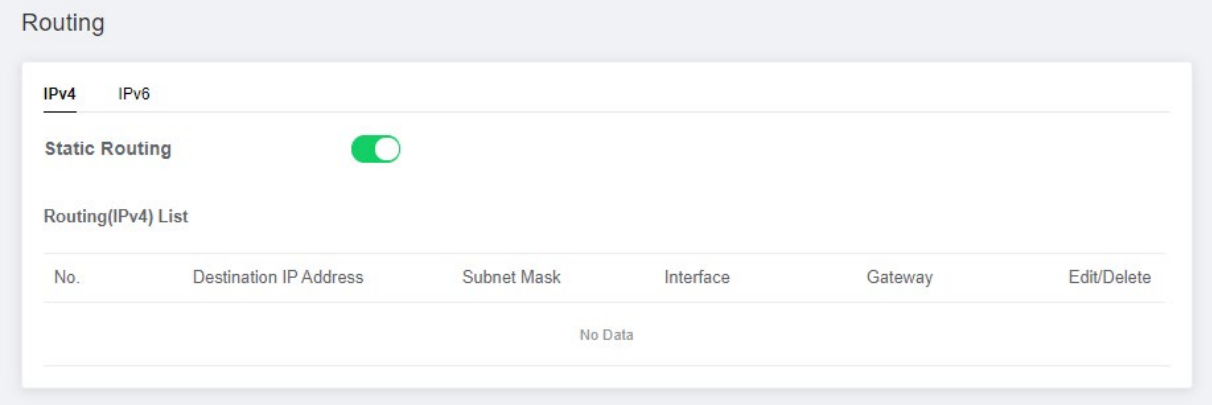
You can manually set the network routing path of packets for data to travel from one network to another with optimal speed and minimal delay.

① Enter the **Advanced** > **Routing**.



IPv4

② Toggle **On** to use a Routing (IPv4).



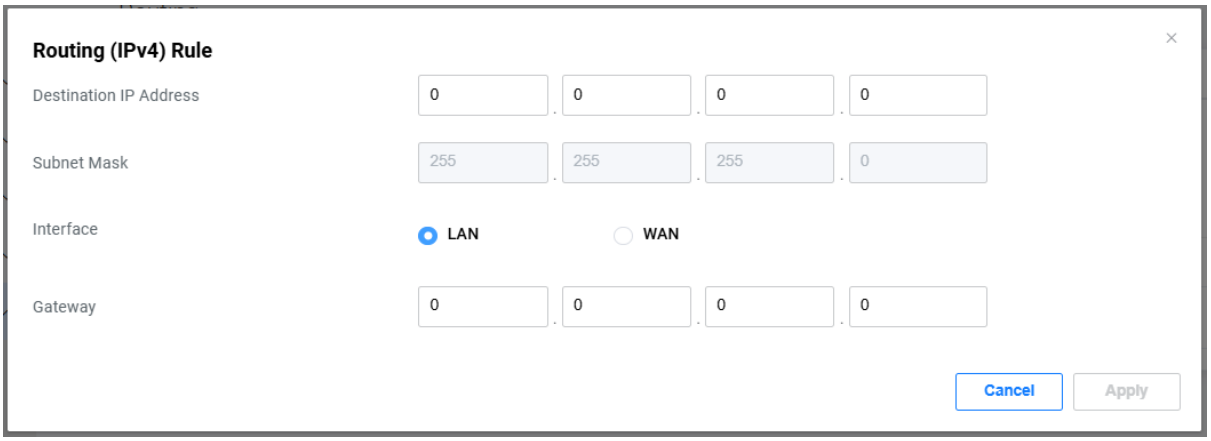
Routing(IPv4) List

Shows the rules set by the user. You can be individually edited or deleted by pressing the **Edit** or **Delete** button.

To add an item

Click **Add** below to register a new rule. You can add up to 32 rules.

① Click **Add** to add a rule.



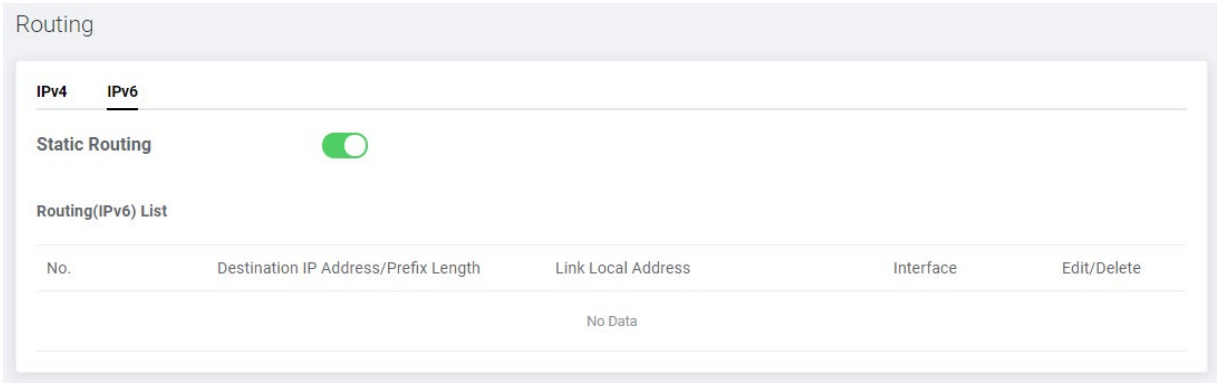
② Enter the option values:

Display	Description
Destination IP Address	Enter a destination IP address.
Subnet Mask	Enter a subnet mask of destination IP address. The value is automatically entered, so you do not need to enter it.
Interface	Select the interface type of destination IP address.
Gateway	Enter a gateway address.

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

IPv6

① Click **IPv6** and toggle **On**.



Routing(IPv6) List

Shows the rules set by the user. You can be individually edited or deleted by pressing the **Edit** or **Delete** button.

To add an item

Click **Add** below to register a new rule. You can add up to 32 rules.

① Click **Add** to add a rule.



② Enter the option values:

Display	Description
Destination IP Address	Enter a destination IPv6 address.
IPv6 Prefix Length	Enter the Prefix Length of IPv6. • The value is automatically entered, so you do not need to enter it.
Link Local Address	Enter the IPv6 link-local address.
Interface	Select the interface type of destination IPv6 address.

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

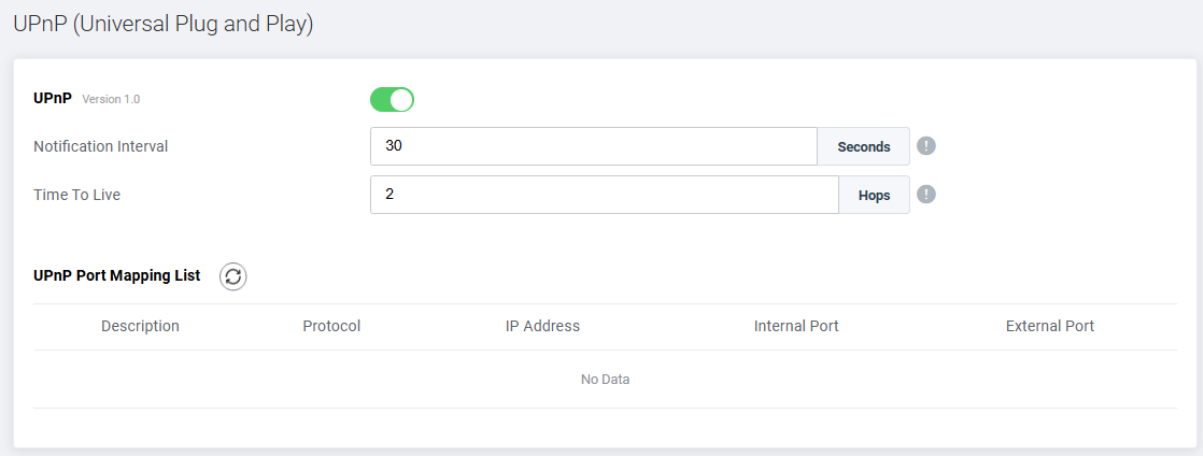
Note:

- In case of IPv6, it is available only if you have subscribed to the service.

8.3 UPnP Setting

UPnP (Universal Plug and Play) is a network protocol that allows devices on a network to discover each other and automatically establish communication without requiring manual configuration. It's commonly used in home networks to enable devices like gaming consoles, smart TVs, IoT devices, and media servers to connect seamlessly with a device or other devices on the same network. UPnP simplifies tasks such as port forwarding, enabling devices to dynamically open and close network ports as needed to communicate with external networks or services.

① Enter the **Advanced > UPnP**.



② Enter the option values:

Display	Description
UPnP	Set whether to support UPnP protocol. • Enabling UPnP allows free communication between the host device and client devices.
Notification Interval	Enter the time interval between 15 and 360 in seconds to be notified. • The default value is 30 (Seconds).
Time To Live	Enter the TTL value. A packet will be discarded if the hot-count exceeds the value. • The default value is 2 (Hops).

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

UPnP Port Mapping List

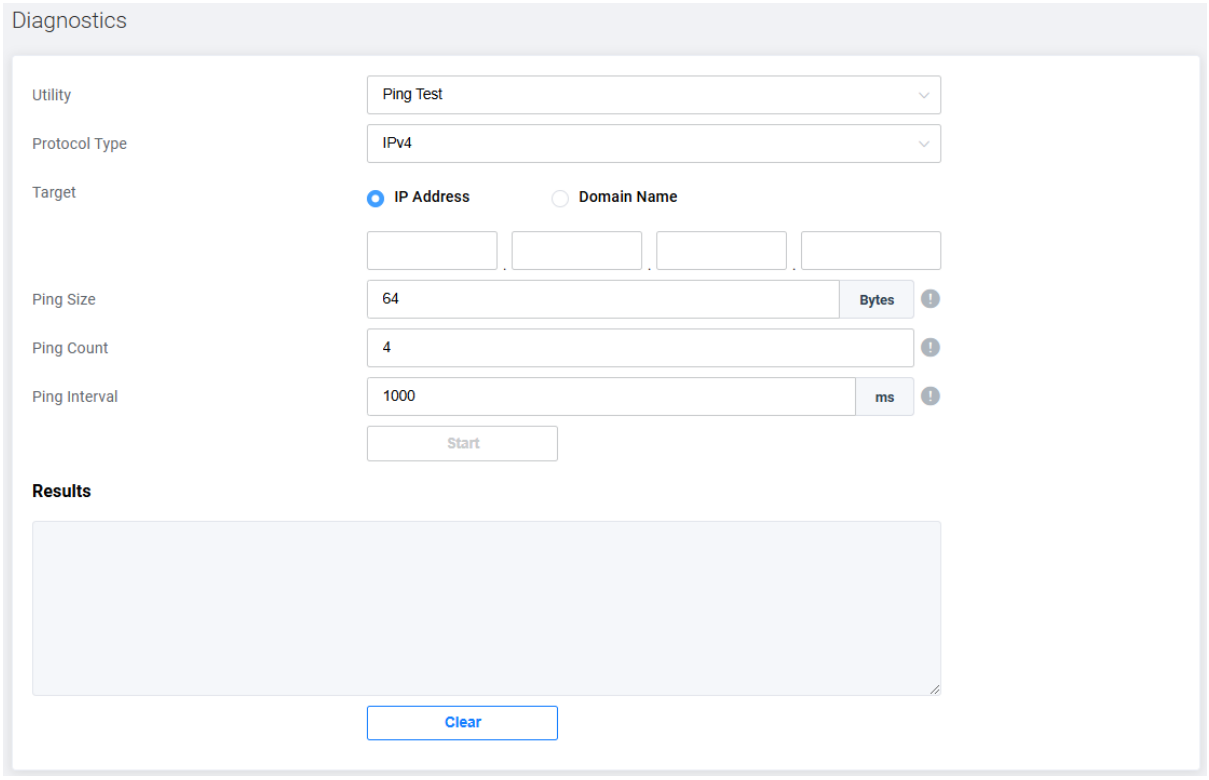
The UPnP table will show the information on each UPnP device that is accessing the device, including what type of port is open and whether that port is still active for each IP address. Click the refresh button to update the UPnP port mapping table.

Note: If you want to use applications such as multiplayer gaming, pear-to-peer connections, real-time communications like an instant messaging or remote assistance (a feature in Windows OS), enable UPnP. Free the improved network connections with UPnP.

8.4 Diagnostics

You can diagnose the network connection problems with the ping test or traceroute.

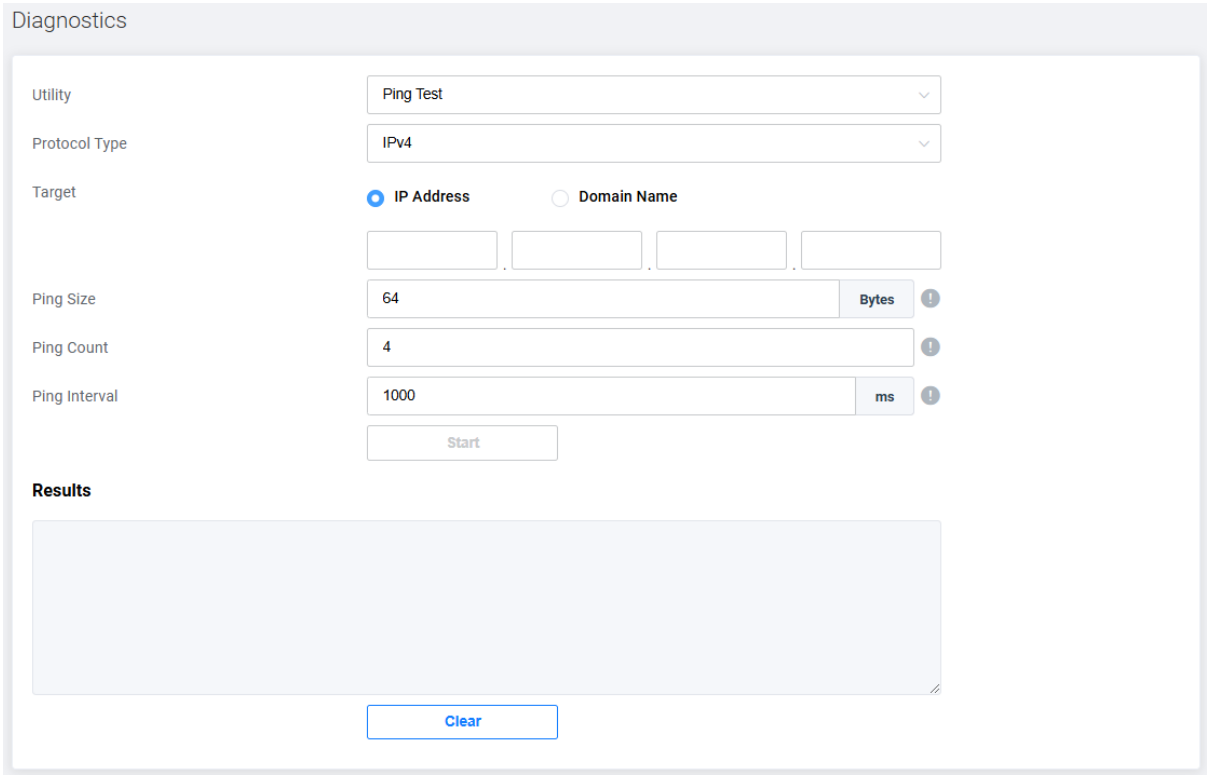
① Enter the **Advanced** > **Diagnostics**.



② Select the **Utility** type either Ping Test or Traceroute. According to the test type, the following options will be changed.

- **Ping Test:** Method for checking if your PC is connected to a network. It also determines the latency or delay between two PCs.
- **Traceroute:** Method for recording the route through the Internet between your PC and a specified destination device. It also calculates and displays the amount of time each hop took.

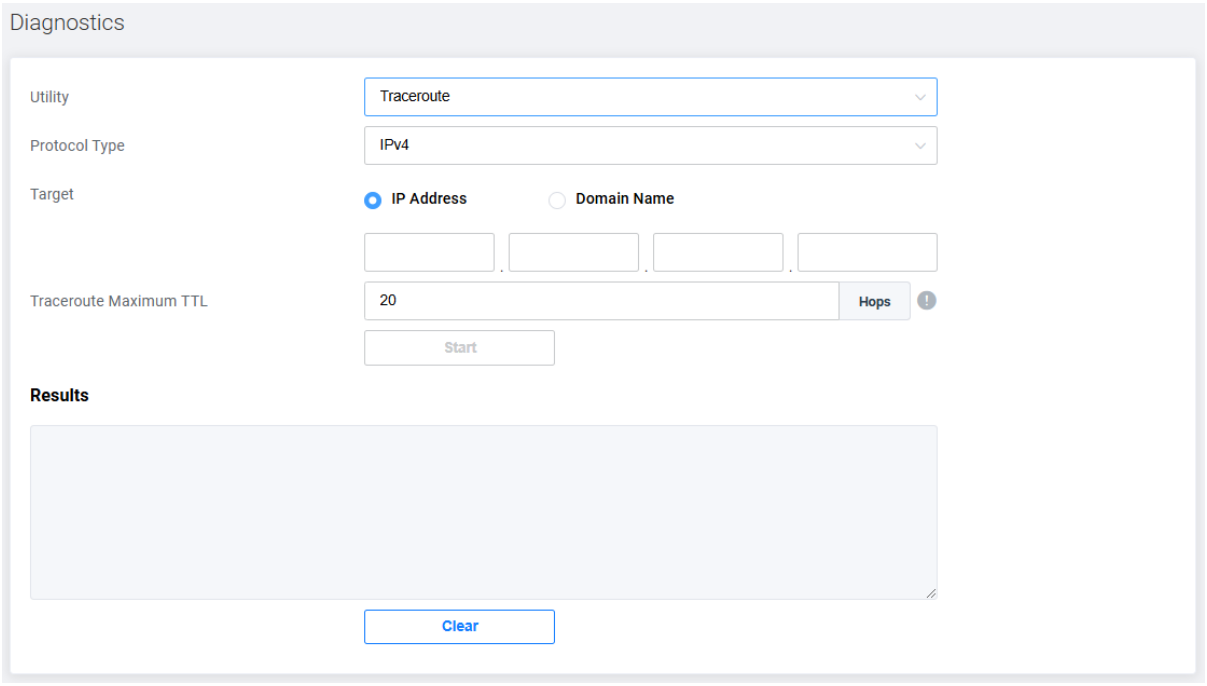
Ping Test



③ Enter the Option Values:

Display	Description
Protocol Type	Select either "IPv4" or "IPv6."
Target IP Address/Domain Name	Enter the IP address or domain name to transmit ping packets.
Ping Size	Enter the size of the ping packet between 64 and 1518. • The default setting is '**64**'.
Ping Count	Enter the number of pings between 1 and 256. • The default setting is '**4**'.
Ping Interval	Enter the interval for transmitting pings between 100 and 3600000. • The default setting is '**1000**'.

Traceroute



③ Enter the Option Values:

Display	Description
Protocol Type	Select either "IPv4" or "IPv6."
Target IP Address/Domain Name	Enter the IP address or domain name to transmit ping packets.
Traceroute Maximum TTL	Set the maximum effective duration for the transmitted packets. • The available setting range is between 1 and 30, and the default setting is 20.

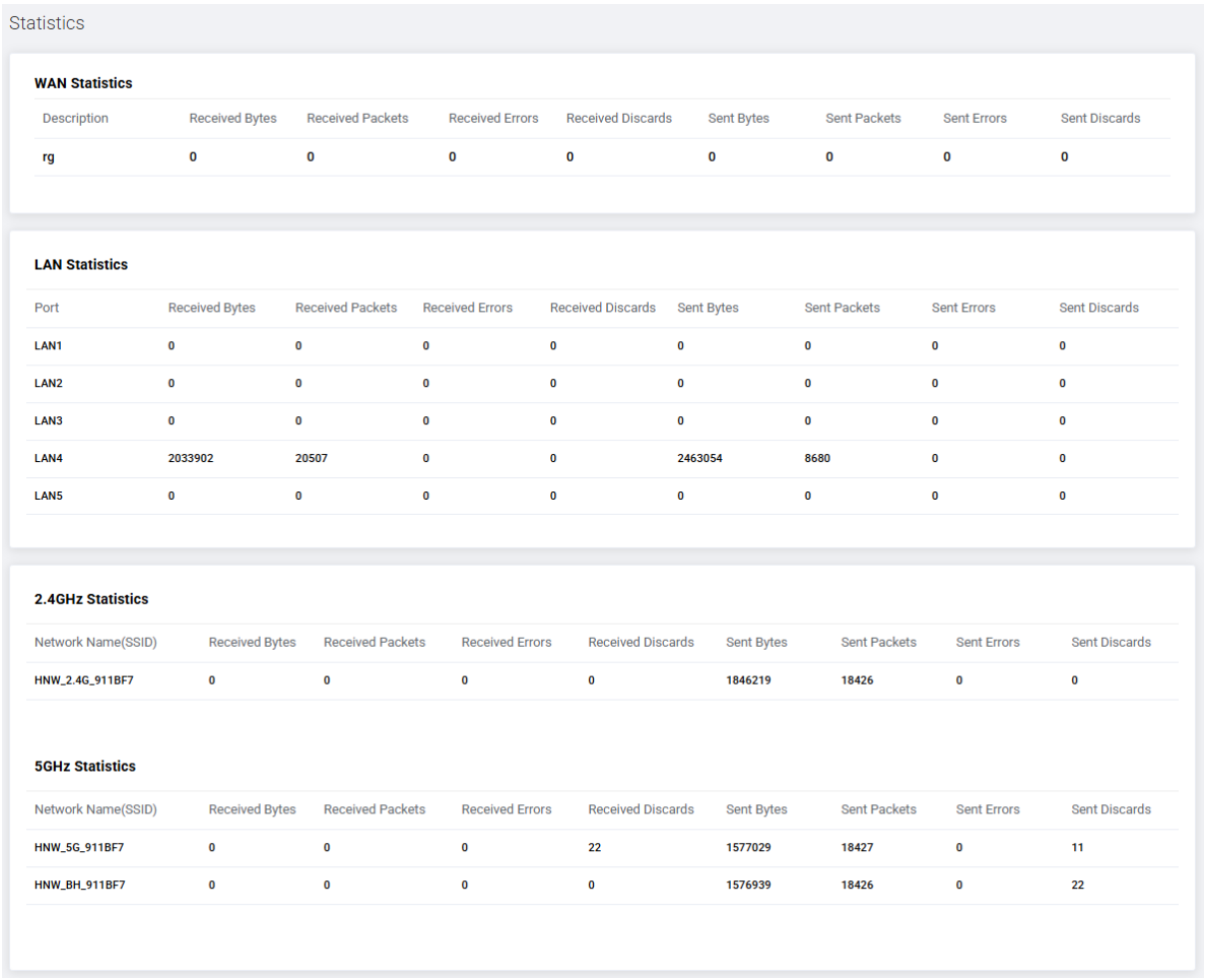
④ Click **Start** to run the test.

Check the test results in the table below.

⑤ You can use the results to rule out a connection issue or identify where in the network the issue is occurring. To clear the results, click **Clear**.

8.5 Statistics

Provides detailed packet information or error information for WAN, LAN, 2.4GHz, and 5GHz.

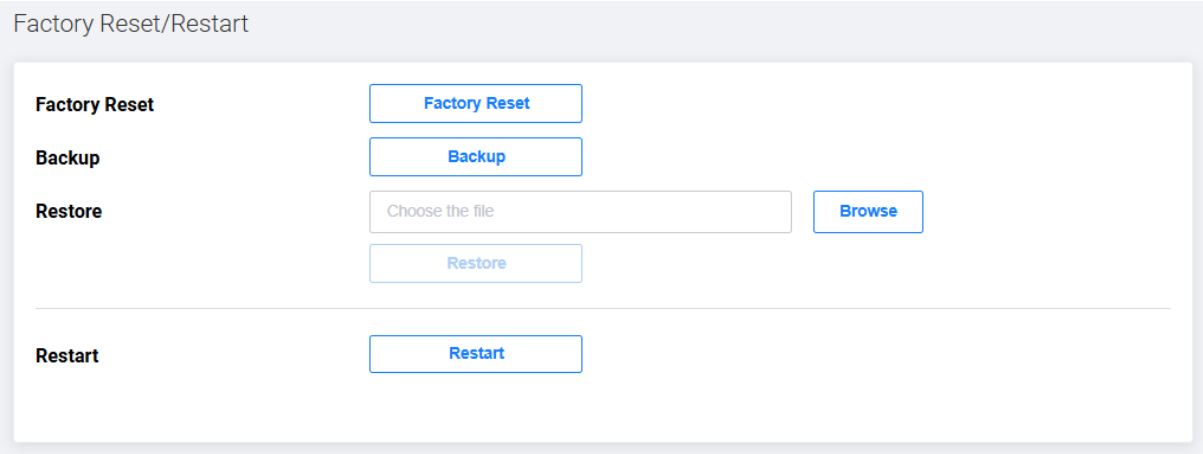


Chapter 9. Managing the System

9.1 Factory Reset/Restart

You can factory reset the device or restart it.

① Enter the **Management** > **Factory Reset/Restart.**



- **Factory Reset** Button: Click **Factory Default** to restore to the factory default settings. Then, the system will restart and it may take a few minutes.

Warning!

If you perform a factory reset, all current settings will be lost. If you want to keep the current settings, use the Backup function to back up the current settings. After a factory reset, you can restore the current settings using the Restore function.

- **Backup** Button: Click **Backup** to save the current configuration. The backup file name is Setting_HPS11-2GE.bin.
- **Restore** Button: To restore a saved backup file, click **Browse** to select the backup file. After selecting, click the **Restore** button to restore. After restoration, the system will restart and may take several minutes.
- **Restart** Button: Click **Restart** to restart the system.

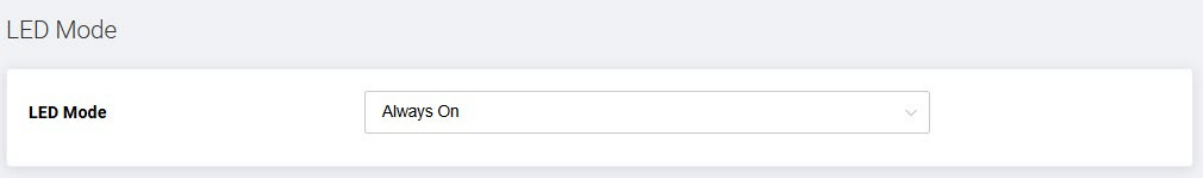
Note:

- In order to complete the Factory Reset/Restore/Restart must be restart. All services cannot be used during the reboot.
- Restore and backup features are only possible on the same device.

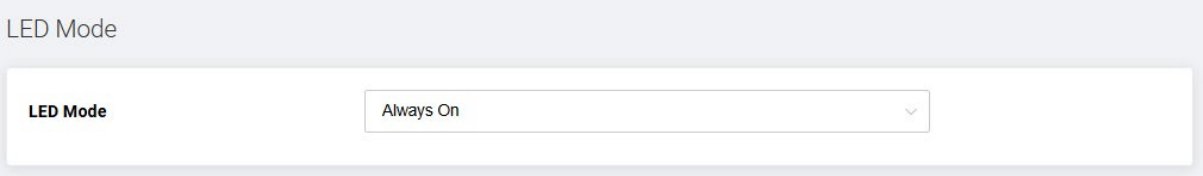
9.2 LED Mode

You can set the LED displayed on the product to always be off, or to turn off only at certain times.

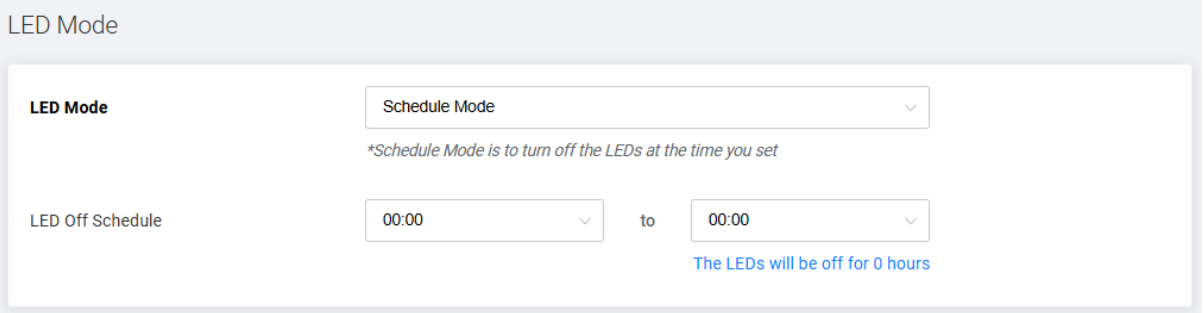
① Enter the **Management > LED Mode.**



② Select the LED Mode Type.



- **Always On:** Always turn on all LEDs.
- **Always Off:** Always turn off all LEDs (except the power LED).



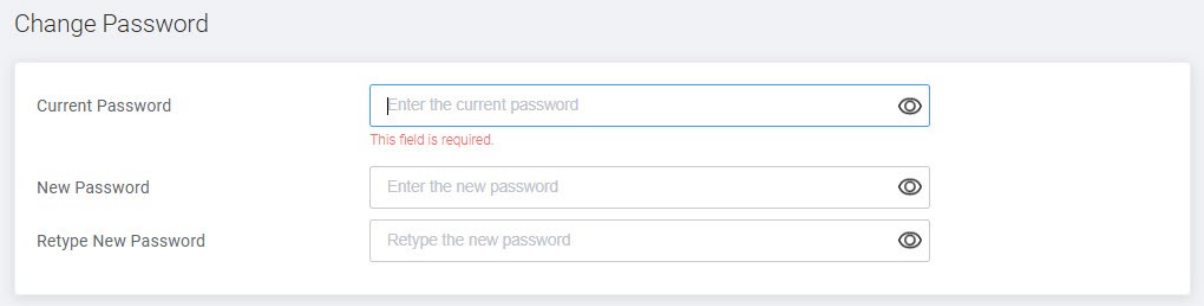
- **Schedule Mode:** Turns off all LEDs only at the set time. Set the time you want to turn off the LEDs in the 'LED Off Schedule' item.

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

9.3 Change Password

You can change the password required when logging in to the Web UI.

① Enter the **Management > Change Password.**



- **Current Password**: Enter the current password. The default password is printed on the device label.
- **New Password**: Enter a new password. The new password can be from 6 to 64 characters A-Z, a-z, 0-9, and all characters. A combination of letters and numbers is recommended.
- **Retype New Password**: Enter the new password again.

② Click **Apply** to save the changes.

Note:

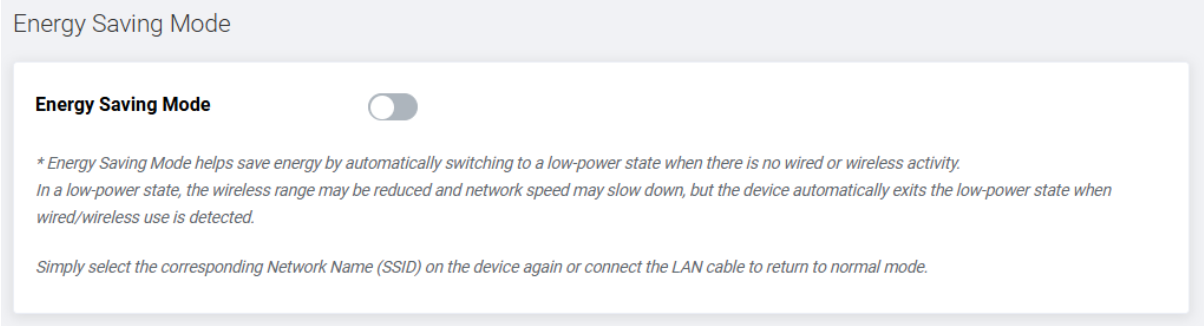
- If you lose your password, you must perform a factory reset, which will erase all custom settings.

9.4 Energy Saving Mode

Energy saving mode automatically switches to low power mode (under 8W) when there is no wired/wireless activity on the device to save energy. When in low power mode, wireless coverage is reduced to maintain only minimal connections, and wired connections may also have reduced network speeds.

When wired/wireless activity is detected (SSID is re-selected, LAN cable is re-plugged in), low power mode is terminated and returns to normal mode.

① Enter the **Management** > **Energy Saving Mode**.

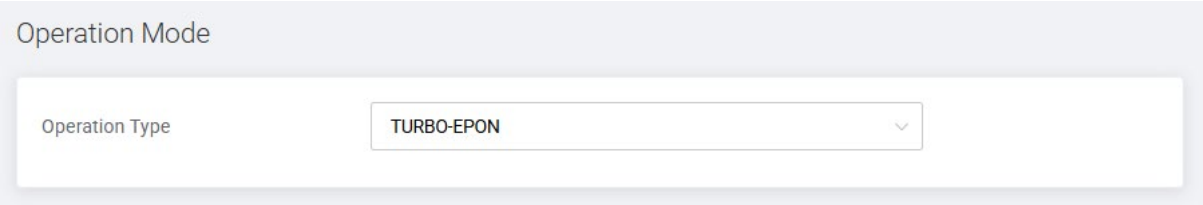


② Toggle **On** to use Energy Saving Mode.

9.5 Operation Mode

① Enter the **Management** > **Operation Mode.**

You can choose TURBO-EPON or Ethernet WAN.



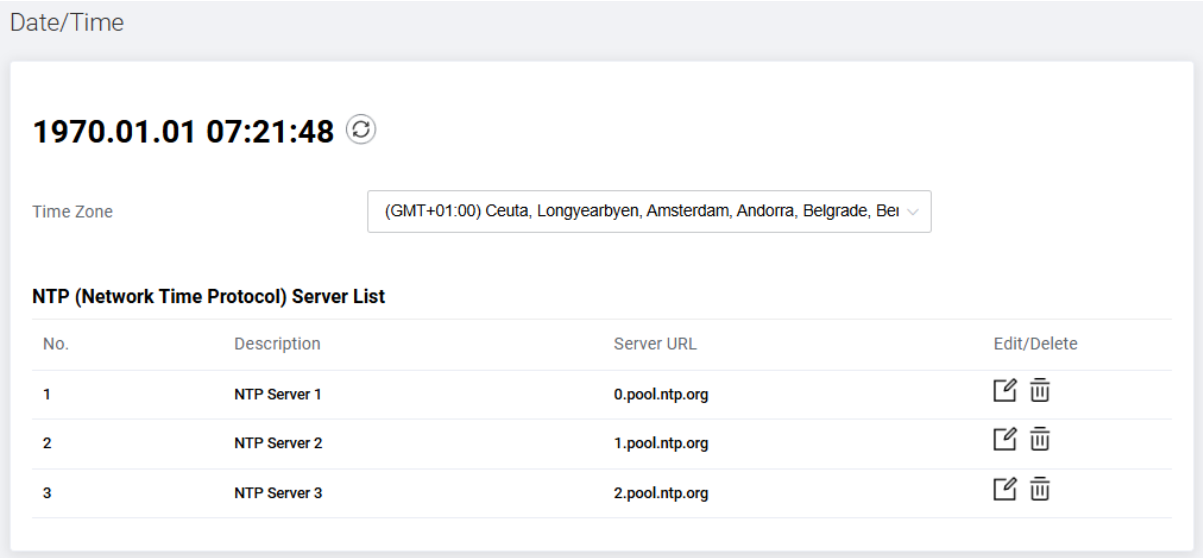
9.6 Date/Time

You can set the date and time of the device.

When connected to the Internet, the current time is automatically set. If correction is required, you can set it manually.

① Enter the **Management** > **Date/Time.**

You can check the currently set time.



- **Time Zone**: Set the Time Zone.

NTP(Network Time Protocol) Server List

It shows the rules set by default. You can edit or delete items by clicking **Edit** or **Delete**. It is recommended to modify it only if necessary.

② Click **Apply** to save the changes.

Chapter 10. Media Share

To use the Media Share feature, a USB is required.

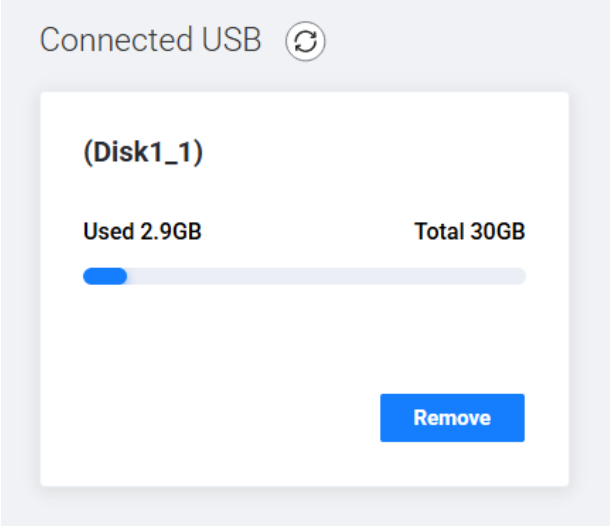
Note:

The supported File Systems for USB are as follows:

FAT, FAT32, exFAT, NTFS, EXT2, EXT3, EXT4

10.1 USB

① Enter the **Media Share** > **USB**.

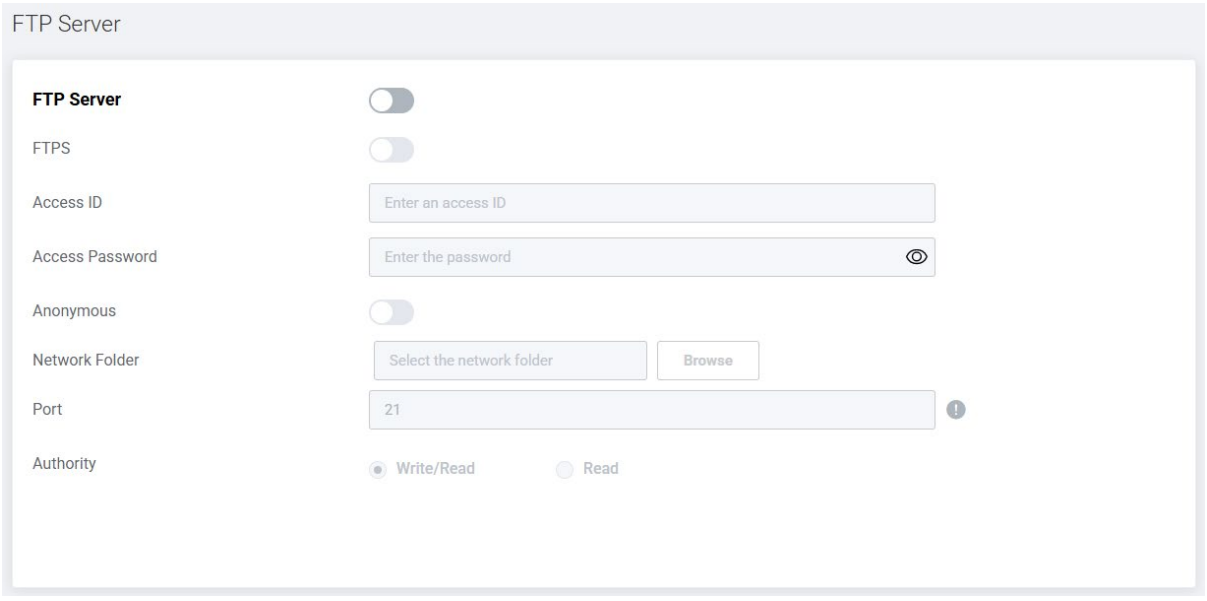


You can check the information and capacity of the currently connected USB.

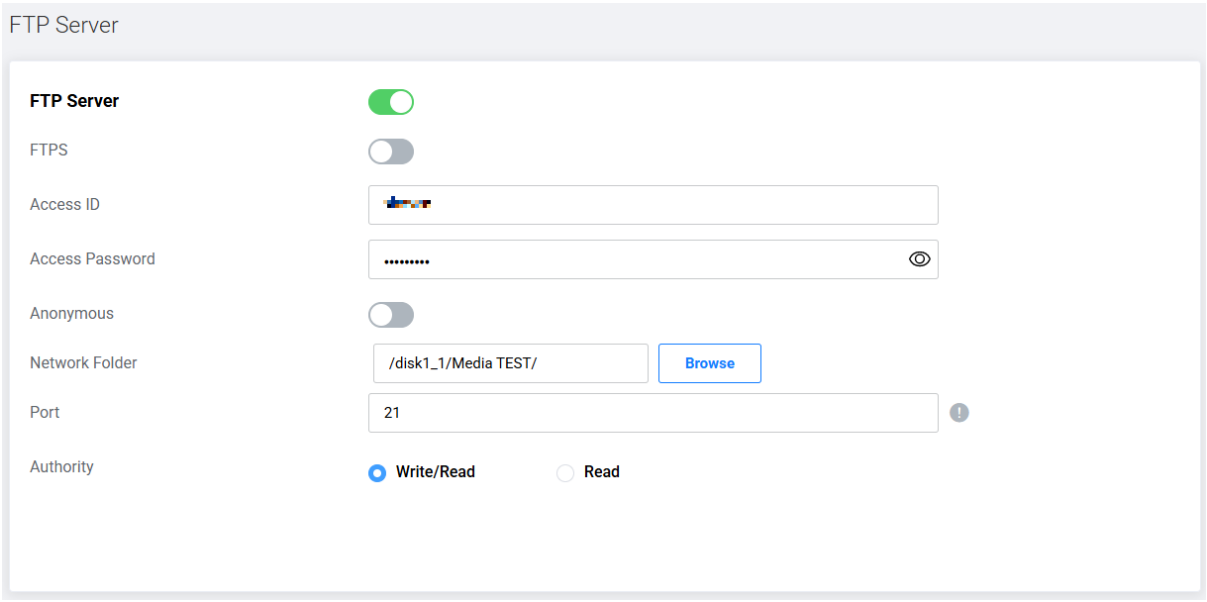
10.2 FTP Server

You can access the connected USB storage device via the FTP server.

① Enter the **Media Share** > **FTP Server**.



② Toggle **On** to use FTP server service.



③ Enter the option values:

Display	Description
FTPS	Set whether to encrypt FTP over SSL for secure data transfer. • Recommended for enhanced security, but requires an FTPS compatible client (e.g. FileZilla).
Access ID	Set the ID to log in to the server.
Access Password	Set the password to log in to the server.
Anonymous	Allows users to connect without an ID or password. • If enabled, anyone can access the shared folder. For security reasons, this option is not recommended.
Network Folder	Set the folder to share within the connected USB. Press the Browser button to select the folder.
Port	Sets the FTP service port. • The default is 21 for FTP/FTPS server. • Custom ports (e.g., 2121) can be used for additional security or to avoid conflicts.
Authority	Set permissions. • Read: Users can view and download files only. • Write/Read: Users can upload, modify, and delete files.

Note:

• To access from outside, you need to set up port forwarding on your router.

• When activating FTPS, some clients may have connection errors due to encryption certificate issues, so client-side settings need to be adjusted.

• Anonymous access is dangerous, so it is safe to turn it off in most cases.

FTP Access Method

You can access the connected USB storage device outside the local area network.

① Open a web browser on your PC.

② Enter the server address ftp://<WAN IP address of your device>.

Note:

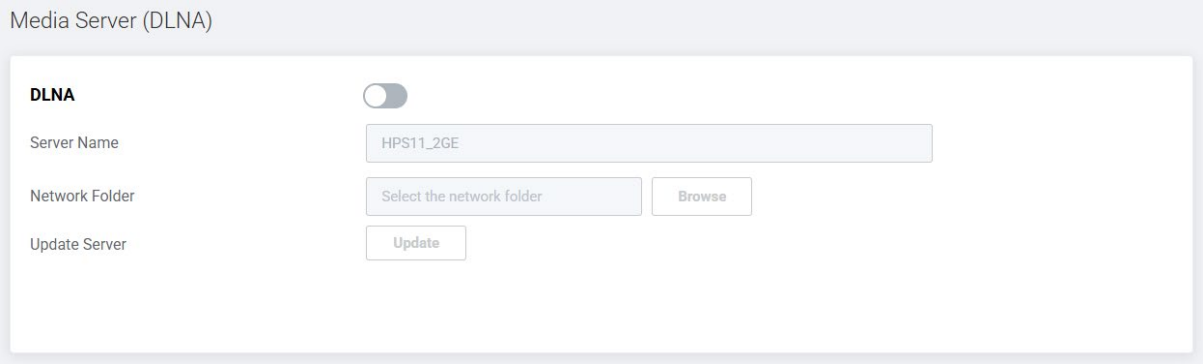
If you set up a domain name for your router, enter the server address ftp://<domain name of your router>. Refer to the DDNS setting page to learn how to set up a domain name for your device.

③ Log in to the server with the ID and password.
Shows call history for both incoming and outgoing calls, arranged by date. Individual call records can be deleted.

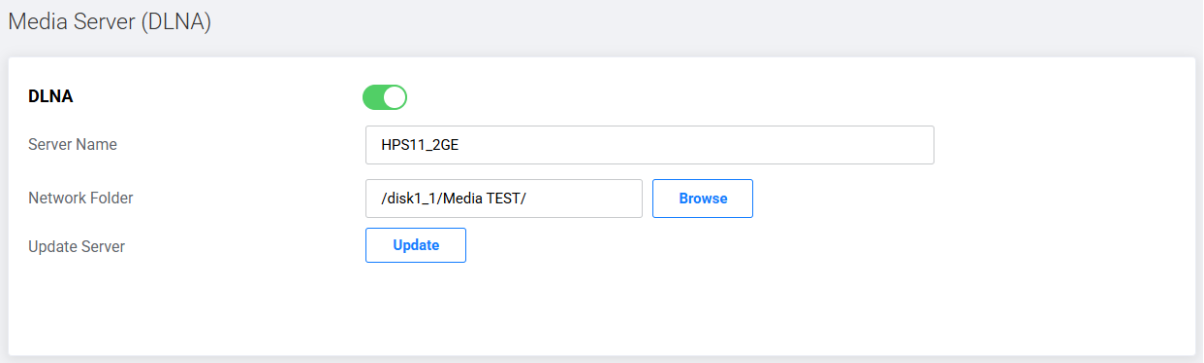
④ Enjoy multimedia contents from the USB storage device even though you are away from your home.

10.3 DLNA

① Enter the **Media Share > DLNA**.



② Toggle **On** to use DLNA service.



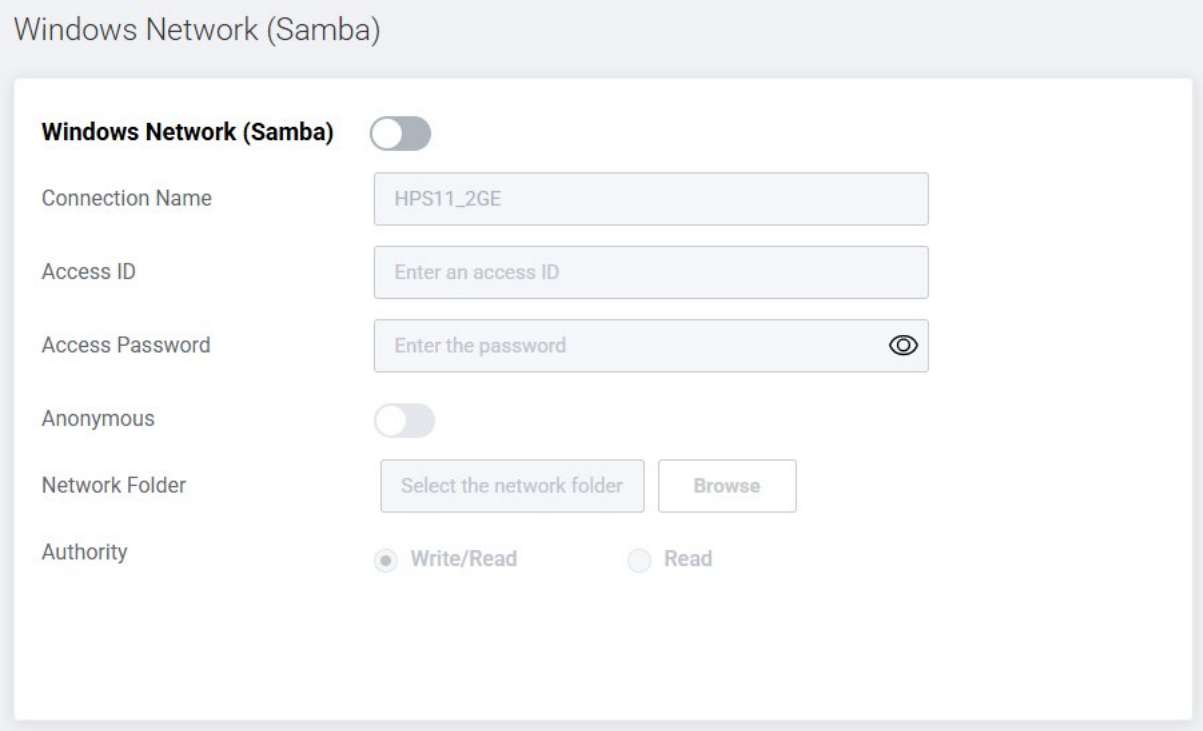
③ Enter the option values:

Display	Description
Server Name	Set the name of the DLNA server that will appear on client devices.
Network Folder	Set the folder to share within the connected USB. • Press the Browser button to select the folder.
Update Server	Buttons for synchronizing folders with DLNA servers.

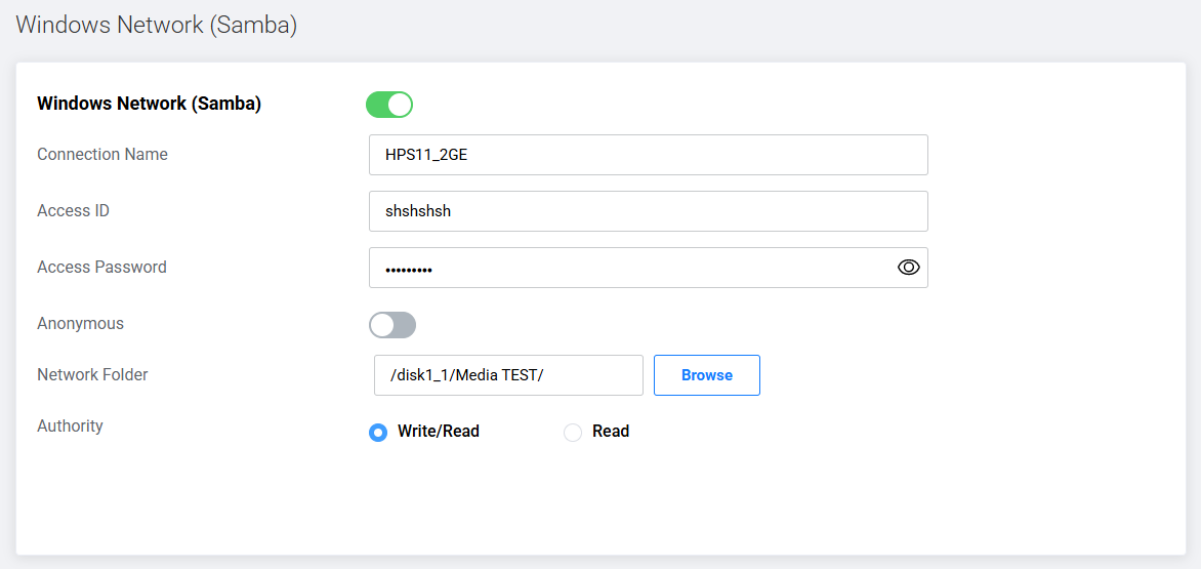
④ Click **Apply** to save the changes.

10.4 Samba

① Enter the **Media Share > Samba**.



② Toggle **On** to use Samba server.



③ Enter the option values:

Display	Description
Connection Name	Set the name of the Samba server that will appear on client devices.
Access ID	Set the ID to log in to the server.
Access Password	Set the password to log in to the server.
Anonymous	Allows users to connect without an ID or password. • If enabled, anyone can access the shared folder. For security reasons, this option is not recommended.
Network Folder	Set the folder to share within the connected USB. • Press the Browser button to select the folder.
Authority	Set permissions. • Write/Read: Users can upload, modify, and delete files. • Read: Users can view and download files only.

④ Click **Apply** to save the changes.

10.5 Printer Server

Your device supports USB Printer Server functionality, allowing you to share a USB printer across your local network. This enables multiple devices (PCs, laptops, etc.) to print using a single printer connected to the device.

Note:

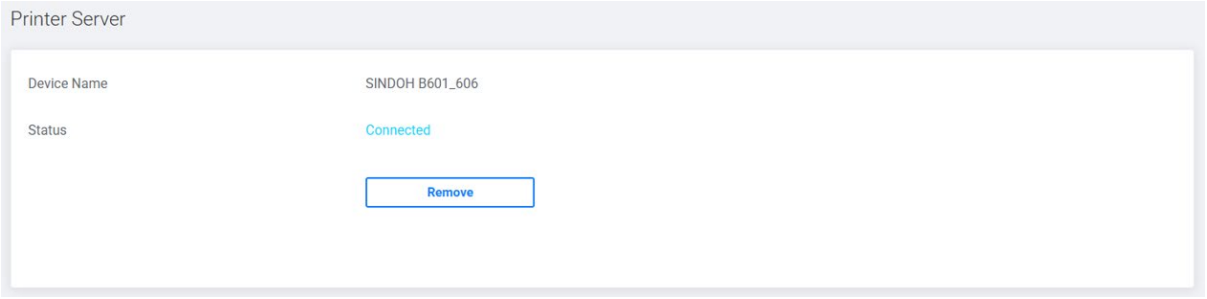
You will need a USB printer. May not be supported depending on model.

① Connect the printer you want to use as the Printer Server via a USB port.

It may take some time for the printer to be recognized.

② Enter the **Media Share > Print Server**.

Check the name and status of the connected printer.



Chapter 11. Troubleshooting

You can find information to diagnose and solve problems you might have with your device. Before contacting the customer service center, make sure to read the tips below carefully. If the problem persists after you complete the following procedure, please contact the customer service for further instructions.

√ The device does not work

- Check the Power LEDs light green.
- Check the power adaptor is plugged into a suitable power outlet.
- Connect the power adaptor to another power outlet.
- Restart the system and wait until the Power LEDs light green.

√ Cannot access the web interface

- Check the Ethernet cable is correctly connected between the device and PC.
- If the PC is connected to the Wi-Fi, check with the SSID the connected device is correct.
- Try to access with IP address 192.168.1.1.
- Power off the device by detaching the power adaptor and then restart the system within a few seconds.

√ Cannot log in to this device

- Check the IP address of your PC is on the same subnet as the device.
- Check your login information is correct. The default password is printed on the label of your device. The password is case-sensitive.

√ Cannot remember the login password

- Reset the device to the factory settings. Press the reset button for 5 seconds. Then, log in to the device with a default password. The password is printed on the label of your device.

√ Cannot search for SSID on the network devices

- Check if the wireless Radio is enabled or not in Wireless > Basic Setting.
- Check if Hide SSID feature is turned on in Wireless > Primary Wireless.

√ Cannot remember the Wi-Fi password

- Go to Home menu and click the eye icon at the password option. You can change the password in Wireless > Primary Wireless.

√ If the device lasts a long time with high temperature,

- If the temperature of the CPU is over 110 degrees Celsius or the wireless interface is maintained over 110 degrees Celsius for more than 300 seconds, the system will be shutdown Wi-Fi interfaces. 2.4GHz and 5GHz LEDs are off and Wi-Fi (wireless) is not available. (Cutoff Stage 1)
- In Cutoff Stage 1, if the cumulative duration lasts more than 600 seconds, the system will be shut down all LAN interfaces. All of the LAN port LEDs on the back are turned off, and LAN (wired) cannot be used. (Cutoff Stage 2)
- In Cutoff Stage 2, when the CPU temperature lasts more than 120 degrees and more than 60 seconds, the system automatically reboots. (Cutoff Stage 3)
- When the temperature of the CPU falls below 90 degrees for more than 60 seconds, all interfaces are restored.

√ Can check the detailed status of the system through log data.

Chapter 12. Safety and Regulatory Information

Please read these instructions carefully before installation/use, and install/use correctly. The precautions given are intended to help you use the device safely and correctly and prevent harm or damage to you or others.

Installation Safety

▪ Conducted only by professional installer who has been accurately trained.

▪ Use only the power adapter provided. Using a different one may cause device damage.

▪ The power supply must be connected to a main outlet with a protective earth connection.

▪ Do not defeat the protective earth connection.

▪ Do not install the device in wet or damp conditions.

▪ Do not install near heat sources such as fire, boilers, or air conditioners.

▪ Do not install in a location where electromagnetic interference (EMI) does not occur.

Laser Safety

Invisible laser radiation may be emitted from disconnected fibers or connectors.
Never stare into beams or look directly to optical connectors.

▪ Invisible radiation might be emitted from the aperture of the port when no fiber cable is connected.

Usage Caution

Please read these instructions before using your device. We do not want you to get hurt or your device to get damaged.

▪ Do not place any object on the device to avoid damaging the device.

▪ Do not open the enclosure without permission and technical support, which voids the provider's warranty.

▪ If need to clean the dust of the equipment, please cut off the power supply first and unplug the relevant connecting cable, then use dry cloth to clean, do not use any liquid.

▪ Power off the device and unplug the cables when the device is not using for a long Time.

Energy Saving Mode

Energy Saving Mode helps save energy by automatically switching to a low-power state when there is no wired or wireless activity.

▪ To use Energy Saving Mode, go to Management > Energy Saving Mode menu in the Web UI and set it to On.

Chapter 13. Specification

12 LEDs	
Power, Internet, PON, LOS, LAN 1~4, WAN/LAN (2.5G), USB, 2.4GHz, 5GHz	
2 Buttons	
WPS (Right side), On/Off, Reset (Back panel)	
Interface	
Fiber Optical Interface	1 x SC/APC Optical Interface Supports EPON (Transmitting: 1310 nm, Receiving: 1490 nm)
LAN Ports	LAN 1~4 : 4 x 1 Gigabit Ethernet (RJ-45) - 1G/100M/10Mbps (Full Duplex) WAN/LAN (2.5G) : 1 x 2.5 Gigabit Ethernet(RJ-45) - 2.5G/1G/100Mbps (Full Duplex)
USB	1 x USB (2.0)
Wireless (2.4GHz)	
Frequency	2,400~2,484MHz : 1~13ch
802.11 Mode	IEEE802.11 b/g/n/ax
Transmission Speed	IEEE802.11ax up to 1147Mbps (HE40)
	IEEE802.11n up to 600Mbps (HT40)
	IEEE802.11g up to 54Mbps
	IEEE802.11b up to 11Mbps
Antenna	4(Tx) x 4(Rx) External Antenna
Wireless (5GHz)	
Frequency	[W52] 5.2GHz (5,150~5,250MHz) : 36/40/44/48ch
	[W53] 5.3GHz (5,250~5,350MHz) : 52/56/60/64ch
	[W56] 5.6GHz (5,470~5,730MHz) : 100/104/108/112/116/120/124/128/132/136/140ch
802.11 Mode	IEEE802.11 a/n/ac/ax
Transmission Speed	IEEE802.11ax up to 4803Mbps (HE160)
	IEEE802.11ac up to 3466Mbps (VHT160)
	IEEE802.11n up to 600Mbps (HT40)
	IEEE802.11a up to 54Mbps
Antenna	4(Tx) x 4(Rx) External Antenna
Environmental	
Input	AC100-240V ~ 50/60Hz

Output	DC12V, 2A (Network Standby under 8W)
Operating Temperature	0° ~ 40°C
Storage Temperature	-20°C ~ 60°C
Operating Humidity	10% ~ 95% (Non-condensing)
Physical Specification	
Dimension	197 (H) x 254 (W) x 166 (D) mm (with foot)

Note:

* Depending on the usage environment and connected devices, it may be connected with a lower bandwidth than the actual setting.

* The maximum speed is the theoretical speed according to the standard, and the actual data transmission speed may vary depending on the usage environment and connected devices.