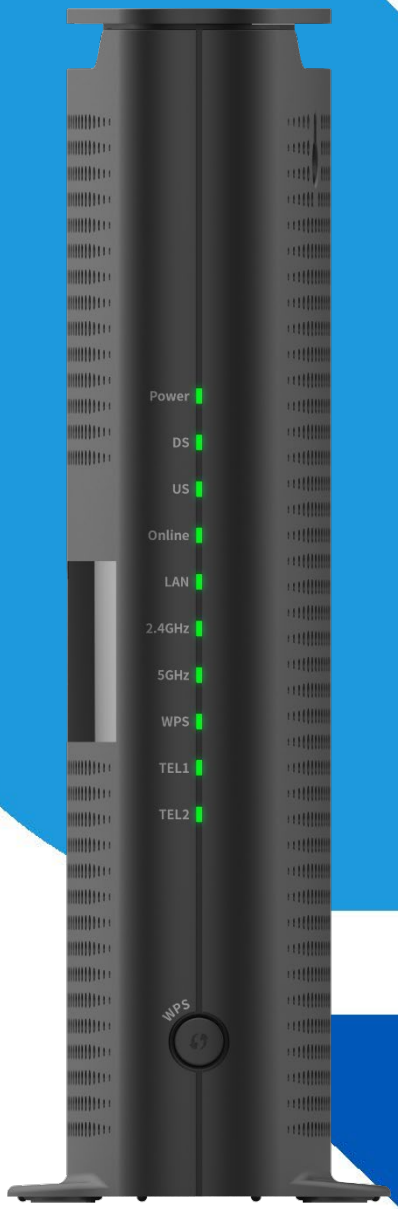


HGF310/EU

User Manual

DOCSIS 3.1 11ax Wireless Voice Gateway

HUMAX Networks, Inc. www.humax-networks.com

Contents

1. Overviews

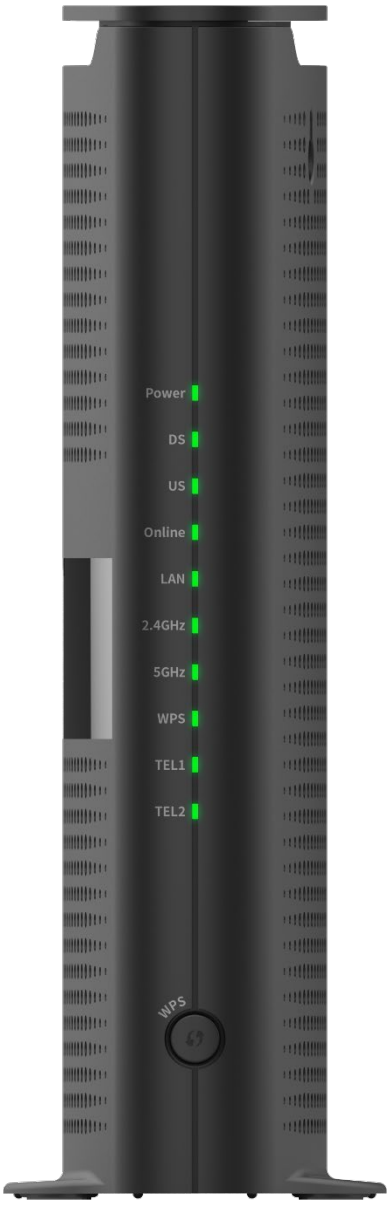
HGF310/EU is a Docsis3.1 product equipped with 802.11ax and Voice Gateway functions.

1.1. Physical Design

Front View

1.2. LED Status

HGF310/EU has 10 LEDs to indicate system status.



LED Status		
Power	Green On	Power is on.
	Off	Power is off.
DS	Green On	Downstream channel is operating normally. (Downstream locked or W/US bonding completed.)
	Green Blinking	Scanning for DS channel.

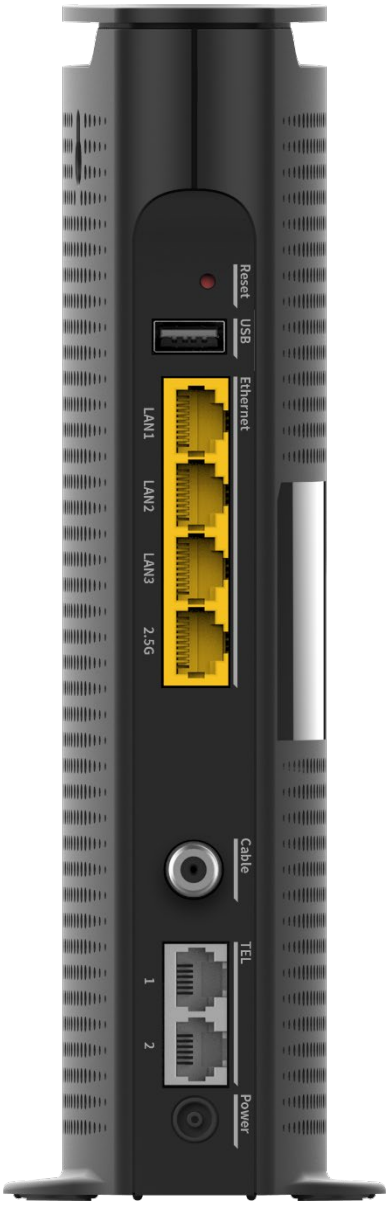
	Green Slow Blinking	Firmware is being upgraded.
	Red On	One Downstream locked.
	Off	Cable interface is idle.
US	Green On	Upstream channel is operating normally. (Upstream locked or W/US bonding completed.)
	Green Blinking	Scanning for US channel.
	Green Slow Blinking	Firmware is being upgraded.
	Red On	One Upstream locked.
	Off	Cable interface is idle.
Online	Green On	Online
	Green Blinking	Provisioning
	Off	Offline
LAN	Green On	LAN 1~3 ports are operating at 1Gbps or When the 2.5GHz port is operating at 2.5Gbps.
	Orange On	LAN 1~3 ports are operating at less than 1Gbps. When the 2.5GHz port is operating at less than 2.5Gbps.
	Off	Ethernet is not connected.
2.4GHz	Green On	2.4GHz radio is on.
	Green Blinking	Data is being transmitted.
	Off	2.4GHz radio is off.
5GHz	Green On	5GHz radio is on.
	Green Blinking	Data is being transmitted
	Off	5GHz radio is off.
WPS	Green Blinking	WPS is operating for 2 minutes. If WPS succeeds within 2 minutes, the blinking stops and the LED turns off.
	Orange Fast Blinking	If WPS fails after 2 minutes, it operates as Fast Blinking for 5 seconds and then the blinking stops.
	Off	WPS is not working.
TEL1	Green On	Telephone 1 is connected and on hook.
	Green Blinking	Telephone 1 is off hook. (Making a call or having a conversation)
	Green Slow Blinking	Provisioning
	Off	Telephone 1 disabled.
TEL2	Green On	Telephone 2 is connected and on hook.

	Green Blinking	Telephone 2 is off hook. (Making a call or having a conversation)
	Green Slow Blinking	Provisioning
	Off	Telephone 2 disabled.

• Slow Blinking blinks at 1000msec and Fast Blinking blinks at 200msec. All other blinking blinks at 500 msec.

1.3. Rear Panel

The rear of HGF310/EU is shown below.



I/O Interface	
Reset Button	Short Press: Rebooting the device Long Press (3 seconds or longer): Factory default reset.
USB Port	USB 2.0 (A-type)
LAN 1-3 Ports	Connect your PC or other devices by wire using the included Ethernet Cable. The data transfer speed supports up to 1Gbps.
2.5G LAN Port	Connect your PC or other devices by wire using the included Ethernet Cable. The data transfer speed supports up to 2.5Gbps.
Cable	Connect the coaxial cable.

TEL 1-2 Ports	Connect the telephone cable to the TEL port.
Power	Connect the DC power adaptor from the power connector to the wall outlet.

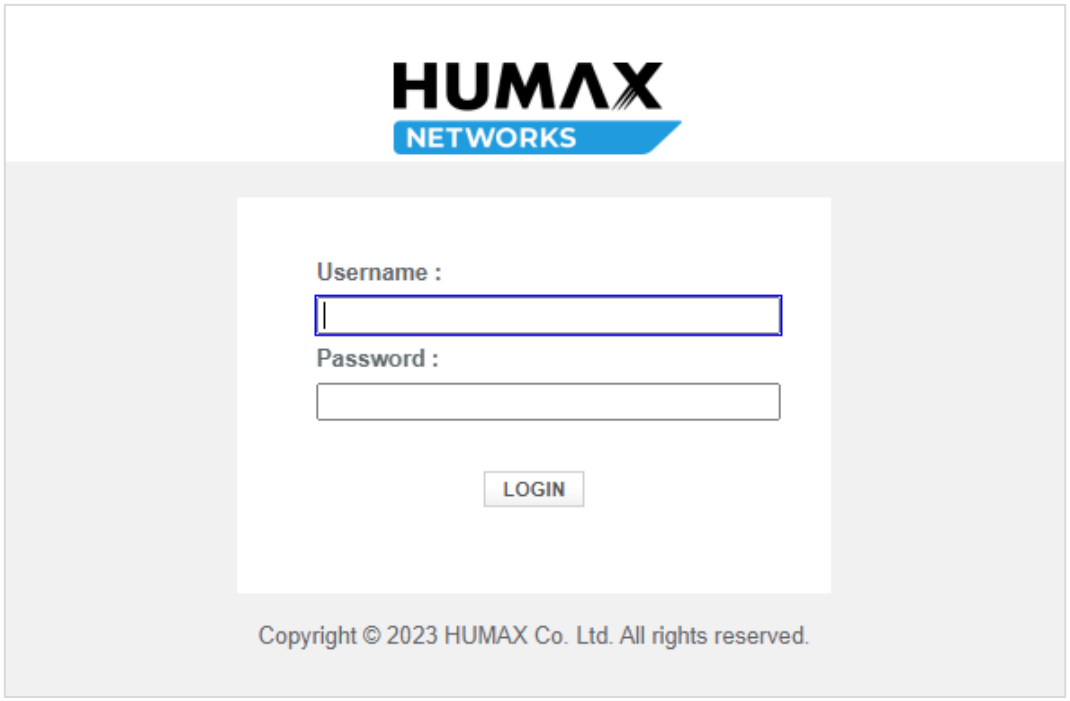
2. Accessing the Web UI

① Connect to the HGF310/EU's network via a wired or Wi-Fi connection.

② **Launch a browser** (Microsoft Edge, Google Chrome, Apple Safari, Mozilla Firefox ect) on a wired or wirelessly connected device.

③ Enter the **http://192.168.20.1** in your browser's address bar and press Enter.

④ If the connection is successful, the **Login** screen will be displayed.



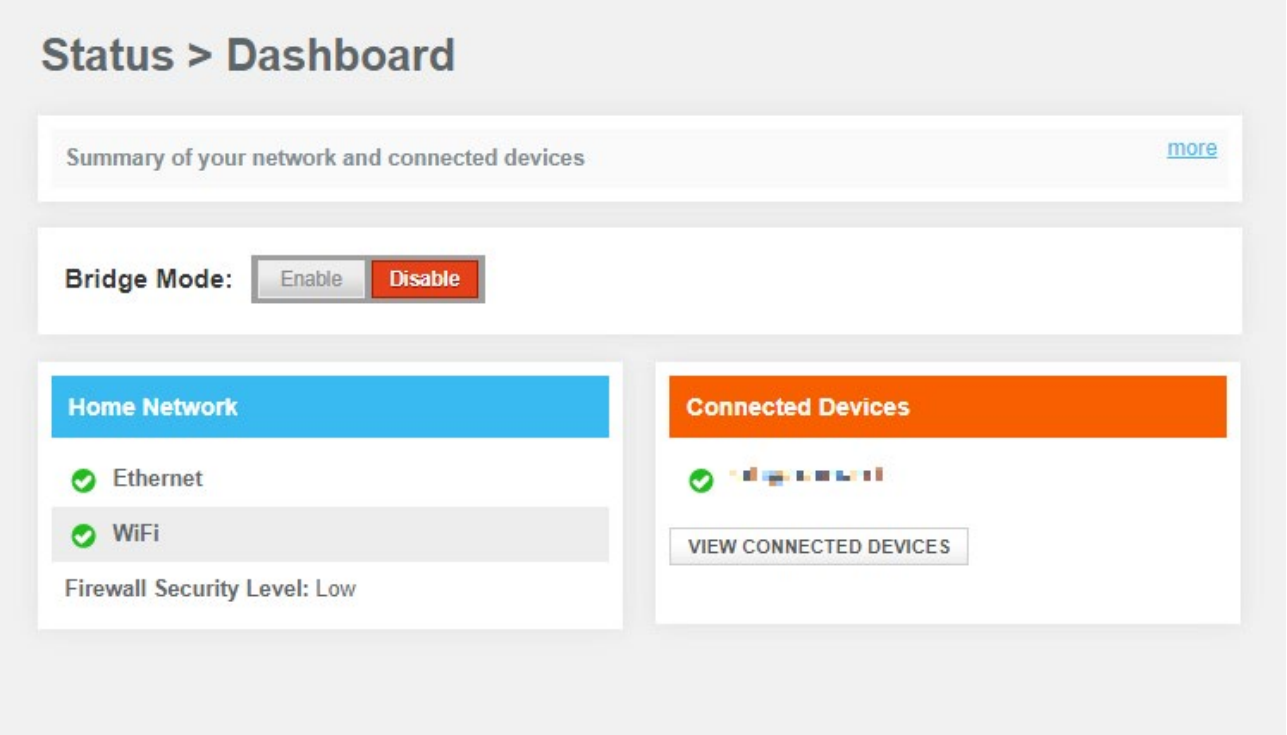
⑤ Enter the **Username and Password** to log in. The default password can be found on the product label.

⑥ If you successfully log in, you will be moved to the **Status** screen.

3. Status

3.1. Dashboard

This page shows the summary of your network and connected devices.



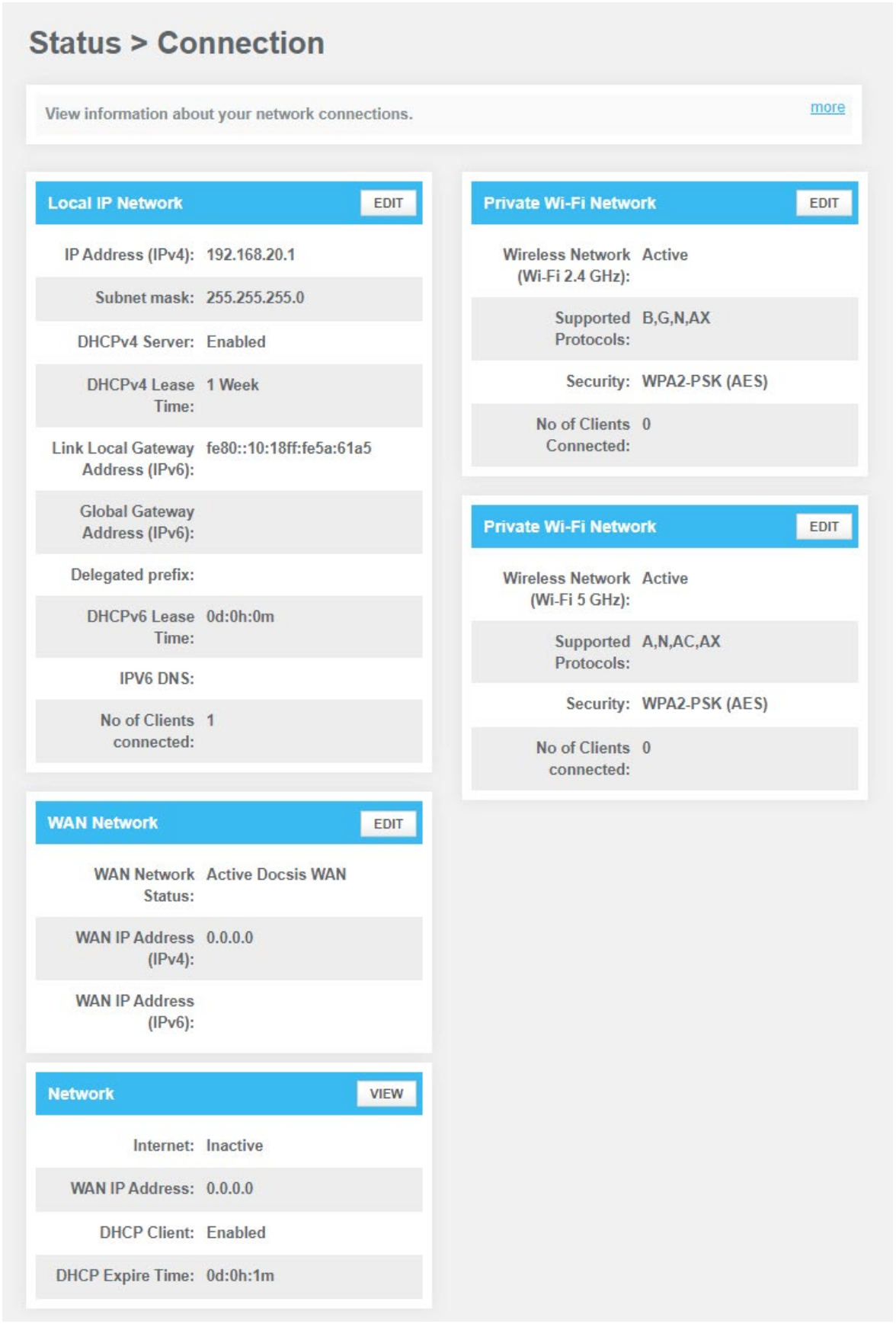
① **Bridge Mode** Enable/Disable: You can set/disable bridge mode.

② **Home Network** : Displays the status of Ethernet (wired) and Wi-Fi (wireless) networks and firewall security level.

③ **Connected Devices** : Displays currently connected computers and devices. Select [VIEW CONNECTED DEVICES] to go to the 'Connected Devices > Devices' screen to manage connected devices. For more details, please refer to page 5. Connected Devices of this document.

3.2. Connection

Shows information about connection status such as local configuration, Wi-Fi, and WAN network.



① **Local IP Network**: Displays all IPv4 and IPv6 information of the local network. If you press the

[EDIT] button, you can go to 'Setup > Local IP Network' and edit it.

② **Private Wi-Fi Network 2.4GHz/5GHz**: Displays information about 2.4GHz/5GHz Private Wireless. If you press the [EDIT] button, you can go to 'Setup > Wi-Fi' and edit it.

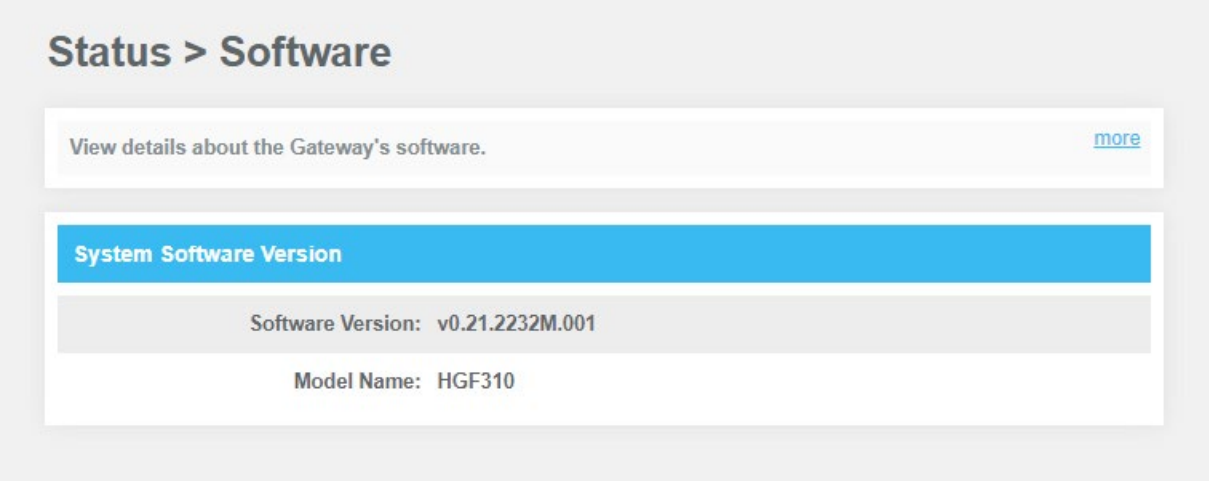
③ **WAN Network**: Displays the status and IP information of WAN Network. If you press the [EDIT] button, you can go to 'Setup > WAN IP Network' and edit it.

④ **Network**: Displays the status of WAN Networks and DHCP settings. When you press the [EDIT] button, go to the 'Status > Networks' screen to see more detailed information.

3.3. Software

Displays detailed information about the HGF310/EU software.

You may need this information for troubleshooting assistance.

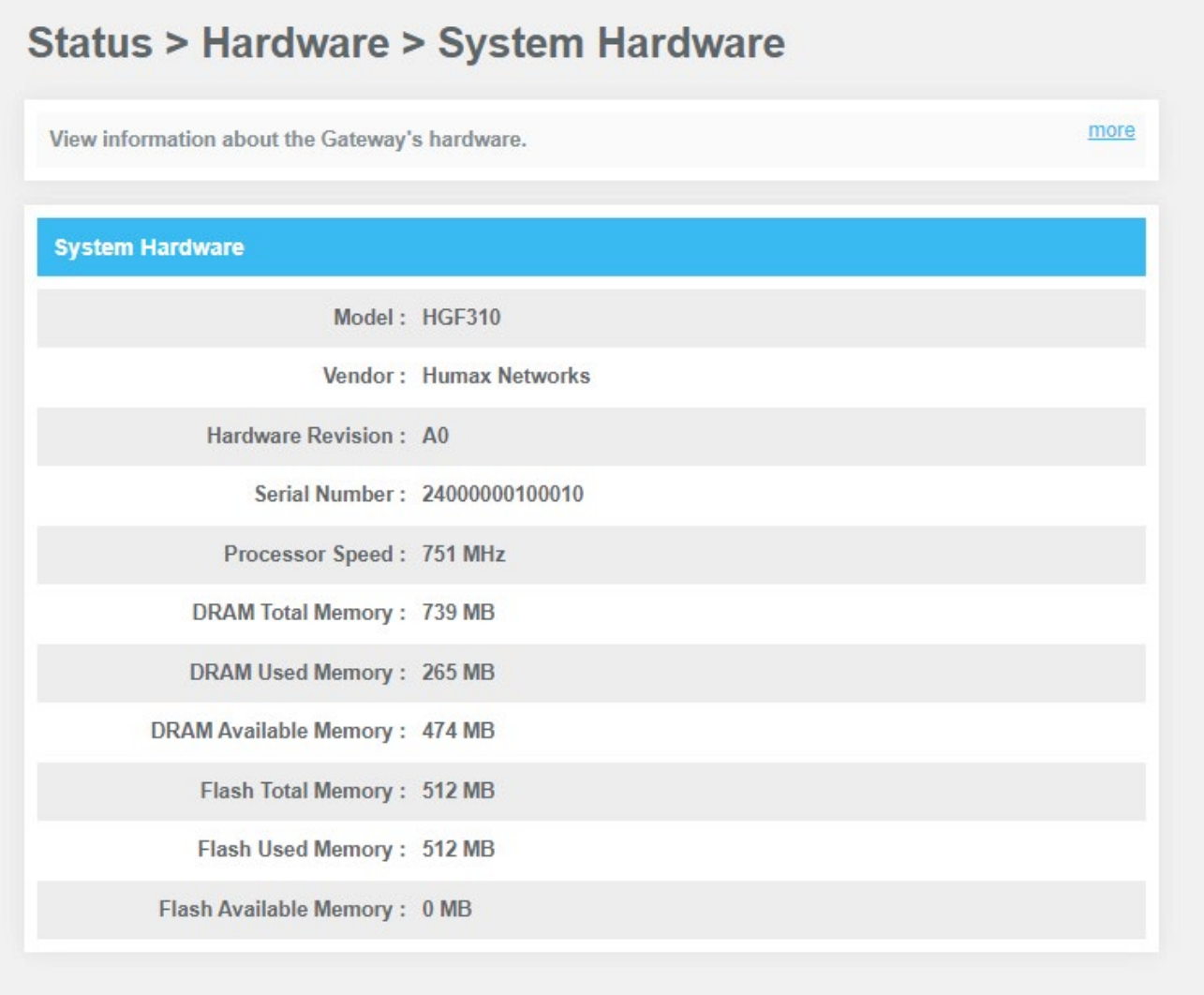


3.4. Hardware

View hardware system information, LAN Ethernet, and Wireless information of HGF310/EU.

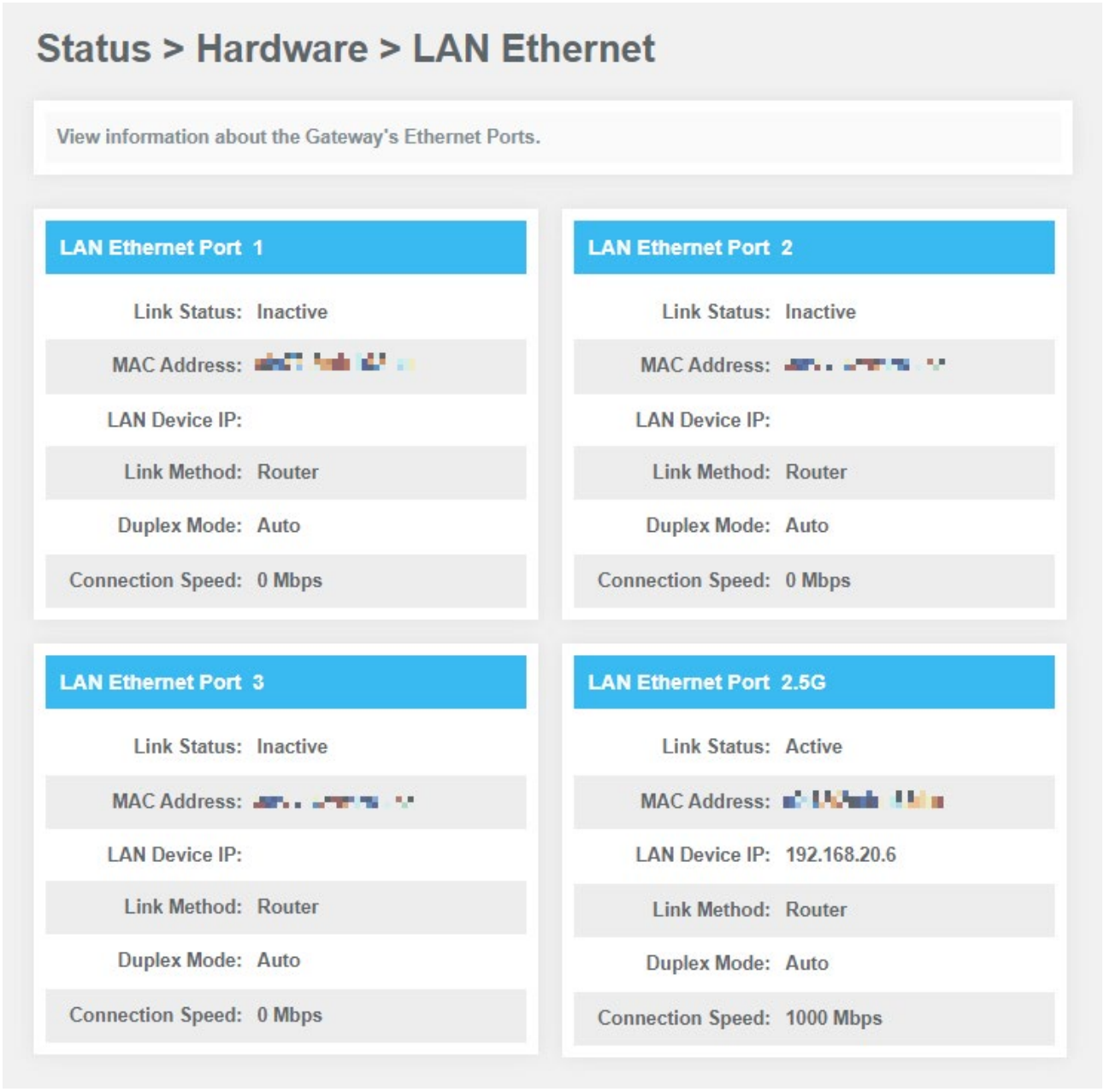
3.4.1. System Hardware

The "Hardware" section provides information about system hardware, LAN Ethernet, and wireless. You may need this information to assist with troubleshooting.



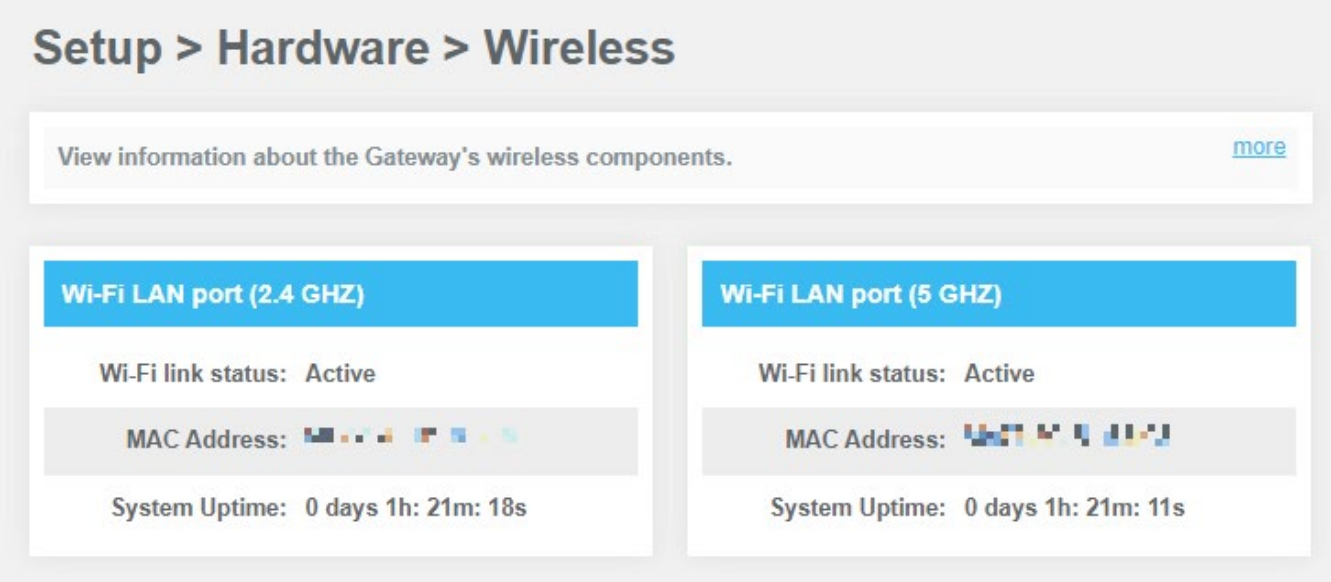
3.4.2 LAN Ethernet

View information about all connected wired computers and devices.



3.4.3. Wireless

View information about all Wi-Fi settings.

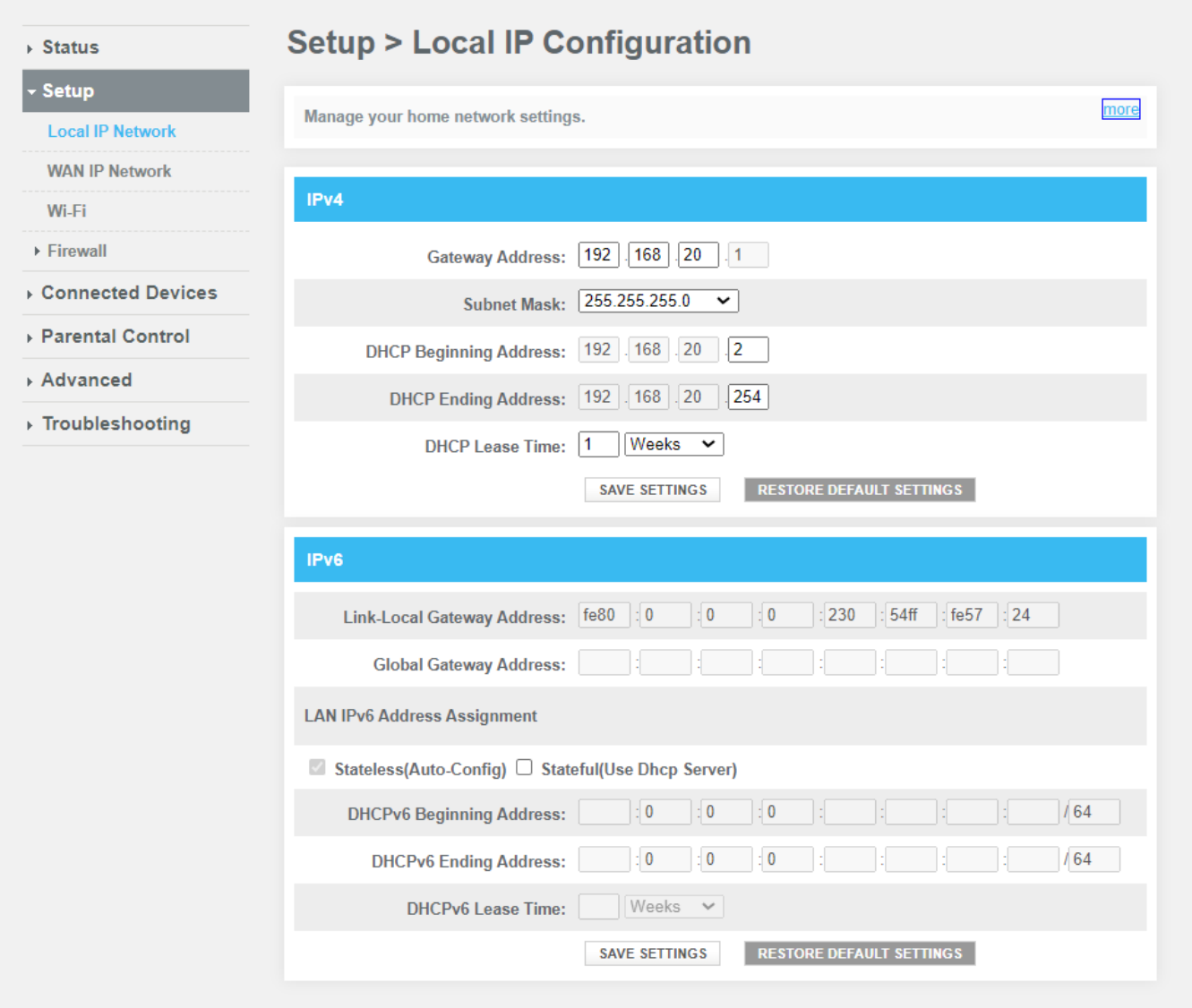


4. Setup

There are four sections under this category, including Local IP Network, WAN IP Network, Wi-Fi, and Firewall.

4.1. Local IP Network

You can view and modify information about your local network.



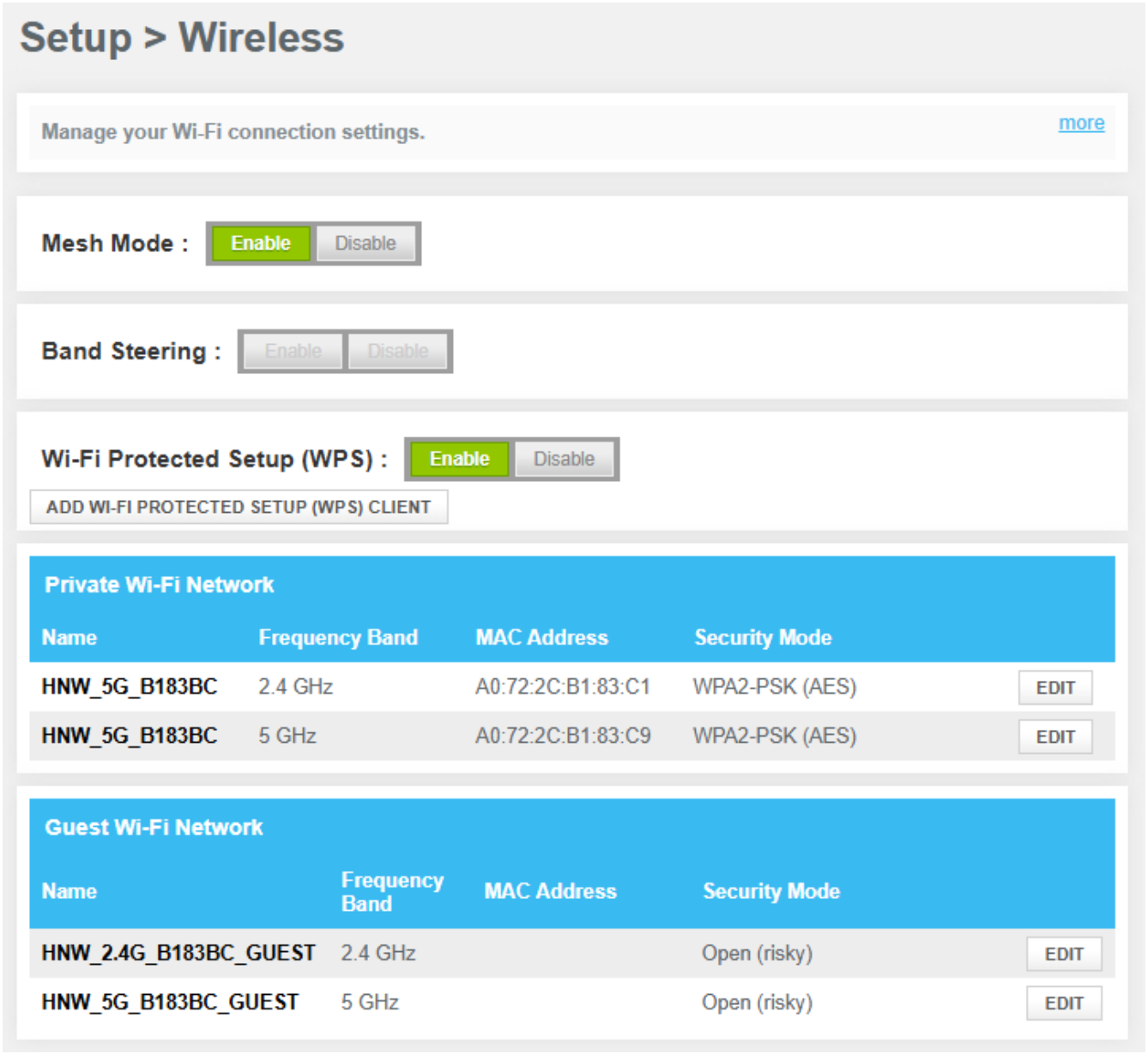
IPv4	
Gateway Address	Enter the IPv4 address of the Gateway.
Subnet Mask	Subnet address for the LAN (3 subnets to choose from)
DHCP Beginning Address	First available Local IPv4 Address in the DHCP pool

DHCP Ending Address	Last available Local IPv4 Address in the DHCP pool
DHCP Lease Time	Set the time duration for the connected device to stay connected using the assigned IPv4.
IPv6	
Link-Local Gateway Address	Enter the link local address for WAN IPv6.
Global Gateway Address	Enter the global address for WAN IPv6.
LAN IPv6 Address Assignment	Set the LAN address allocation method for IPv6. Available: Stateless, Statusful
DHCPv6 Beginning Address	First available Local IPv6 Address in the DHCP pool
DHCPv6 Ending Address	Last available Local IPv6 Address in the DHCP pool
DHCPv6 Lease Time	Set the time duration for the connected device to stay connected using the assigned IPv6.

- Enter all values and save them by pressing the [SAVE SETTINGS] button.
- Click the [RESTORE DEFAULT SETTINGS] button will reset the current page settings.

4.2. Wi-Fi

You can view and modify information about your wireless network.



① **Mesh Mode**: Set whether to use Mesh Mode. Enabling Mesh Mode automatically turns on Band Steering. (Cannot modify)

② **Band Steering**: Set whether to use Band Steering.

Band Steering is a feature that combines 2.4GHz and 5GHz wireless networks into one network name to provide wireless network connectivity through the optimal channel.

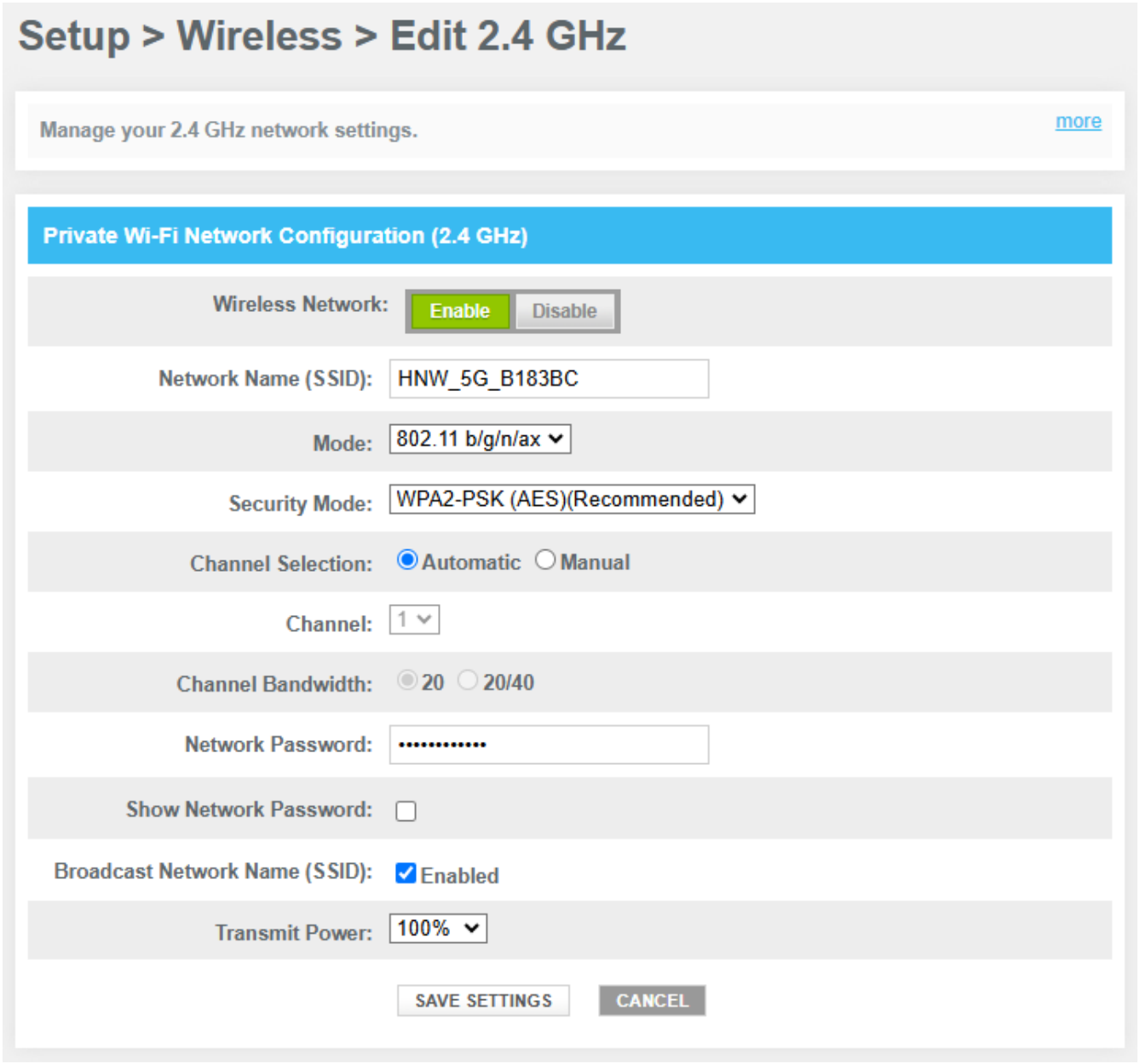
③ **Wi-Fi Protected Setup(WPS)**: Set whether or not the WPS button works.

WPS (Wireless LAN Protected Setup) is for convenient wireless connection between HGF310/EU and client devices. If set to Disable, the WPS button on the product will not work, so caution is required. The WPS LED also turns off.

④ **Private Wi-Fi Network**: Information about Primary Wireless. Click [EDIT] next to the Network Name you'd like to modify its Wi-Fi network settings: Network Name (SSID), Mode, Security Mode, Channel, Network Password (Key), and Broadcasting feature. Please refer to the '4.3.1. Edit 2.4GHz/ 4.3.2. Edit 5GHz' section.

⑤ **Guest Wi-Fi Network**: Information about Guest Wireless. Click [EDIT] next to the Network Name you'd like to modify its Wi-Fi network settings: Network Name (SSID), Mode, Security Mode, Channel, Network Password (Key), and Broadcasting feature.

4.2.1. Edit 2.4GHz

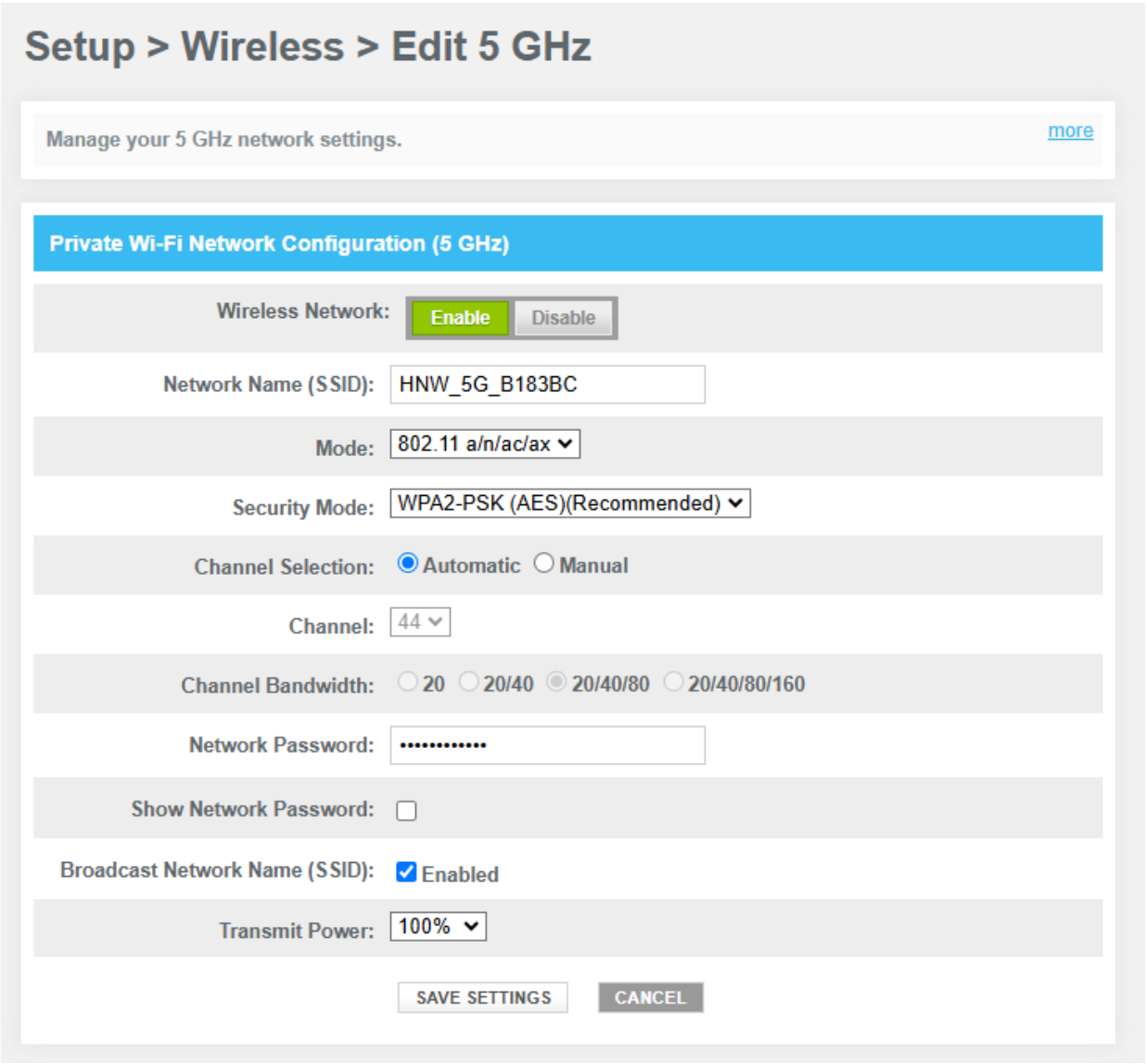


Edit 2.4GHz	
Wireless Network	Set whether to use 2.4GHz Primary Wireless.
Network Name (SSID)	Set the name of the wireless network. The name will appear in the list of devices that will be connected wirelessly.
Mode	Set 802.11 mode.
Security Mode	Set the level of security for the wireless network. The default setting(WPA2-PSK(AES)) is recommended for network security.
Channel Selection	Set the channel for the wireless network. - Set it to "Automatic" to automatically select the optimal channel(recommended).

	- Set “Manual” to manually select a specific channel and channel bandwidth.
Channel	Set the wireless channel you want to use. (*Only for Channel Selection set to "Manual")
Channel Bandwidth	Set the bandwidth. (*Only for Channel Selection set to "Manual")
Network Password	Set the password for the wireless network. Enter 8 – 63 characters for the password. The password setting is not required if the security level has been set to “None.”
Show Network Password	Check “Enable” to see the encrypted password.
Broadcast Network Name (SSID)	Check “Enable” to hide the network name from the list of available wireless networks on other devices. This feature is not recommended unless necessary for security reasons.
Transmit Power	Select the intensity of the wireless signal.

• Enter all values and save them by pressing the [SAVE SETTINGS] button.

4.2.2. Edit 5GHz



Edit 5GHz	
Wireless Network	Set whether to use 2.4GHz Primary Wireless.
Network Name (SSID)	Set the name of the wireless network. The name will appear in the list of devices that will be connected wirelessly.
Mode	Set 802.11 mode.
Security Mode	Set the level of security for the wireless network. The default setting(WPA2-PSK(AES)) is recommended for network security.
Channel Selection	Set the channel for the wireless network. - Set it to "Automatic" to automatically select the optimal channel(recommended). - Set "Manual" to manually select a specific channel and channel bandwidth.

Channel	Set the wireless channel you want to use. (*Only for Channel Selection set to "Manual")
Channel Bandwidth	Set the bandwidth. (*Only for Channel Selection set to "Manual")
Network Password	Set the password for the wireless network. Enter 8 – 63 characters for the password. The password setting is not required if the security level has been set to "None."
Show Network Password	Check "Enable" to see the encrypted password.
Broadcast Network Name (SSID)	Check "Enabled" to hide the network name from the list of available wireless networks on other devices. This feature is not recommended unless necessary for security reasons.
Transmit Power	Select the intensity of the wireless signal.

4.3. Firewall

4.3.1. IPv4

Set the firewall security level for IPv4.

Select a security level for details. If you're unfamiliar with firewall settings, keep the default security level, Minimum Security (Low).


Setup > Firewall > IPv4
Manage your firewall settings.
more
Firewall Security Level
Maximum Security (High)
LAN-to-WAN: Allow as per below.
HTTP and HTTPS (TCP port 80, 443)
DNS (TCP/UDP port 53)
NTP (TCP port 119, 123)
email (TCP port 25, 110, 143, 465, 587, 993, 995)
VPN (GRE, UDP 500, 4500, 62515, TCP 1723)
iTunes (TCP port 3689)
WAN-to-LAN: Block all unrelated traffic and enable IDS.
Typical Security (Medium)
LAN-to-WAN: Allow all.
WAN-to-LAN: Block as per below and enable IDS.
IDENT (port 113)
ICMP request
Peer-to-peer apps:
kazaa - (TCP/UDP port 1214)
bittorrent - (TCP port 6881-6999)
gnutella - (TCP/UDP port 6346)
vuze - (TCP port 49152-65534)
Minimum Security (Low)
LAN-to-WAN: Allow all.
WAN-to-LAN: Block as per below and enable IDS
IDENT (port 113)
Custom Security
LAN-to-WAN : Allow all.
WAN-to-LAN : IDS Enabled and block as per selections below.
Block http (TCP port 80, 443)
Block ICMP
Block Multicast
Block Peer-to-peer applications
Block IDENT (port 113)
Disable entire firewall
SAVE SETTINGS
RESTORE DEFAULT SETTINGS

Firewall Security Level - IPv4	
Maximum Security (High)	Most applications are blocked except for browsing, email, iTunes and VPN.
Typical Security (Medium)	All peer-to-peer apps are blocked.
Minimum Security (Low)	Minimum Security is the default setting. All secure apps are enabled.
Custom Security	Users can set which ports they want to block.

- Enter all values and save them by pressing the [SAVE SETTINGS] button.
- Click the [RESTORE DEFAULT SETTINGS] button will reset the current page settings.

4.3.2. IPv6

Set the firewall security level for IPv6.

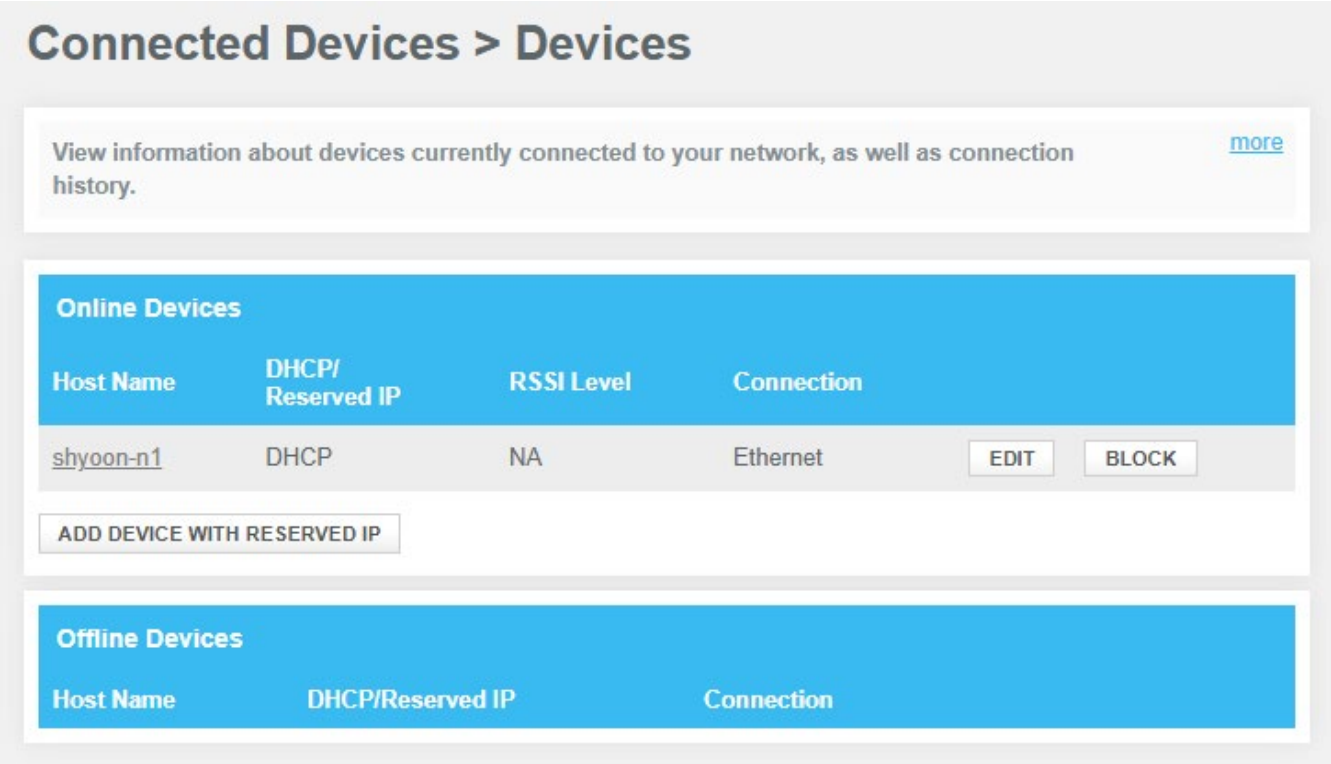
Select a security level for details. If you're unfamiliar with firewall settings, keep the default security level, Typical Security.

Firewall Security Level - IPv6	
Minimum Security (Low)	Minimum Security is the default setting. All secure apps are enabled.
Custom security	Users can set which ports they want to block.

- Enter all values and save them by pressing the [SAVE SETTINGS] button.
- Click the [RESTORE DEFAULT SETTINGS] button will reset the current page settings.

5. Connected Devices

5.1. Devices



① **Online Devices**: View information about the client devices connected to HGF310/EU.

• Click the [EDIT] button to go to the editable page.

• Click the [BLOCK] button to block access the internet.

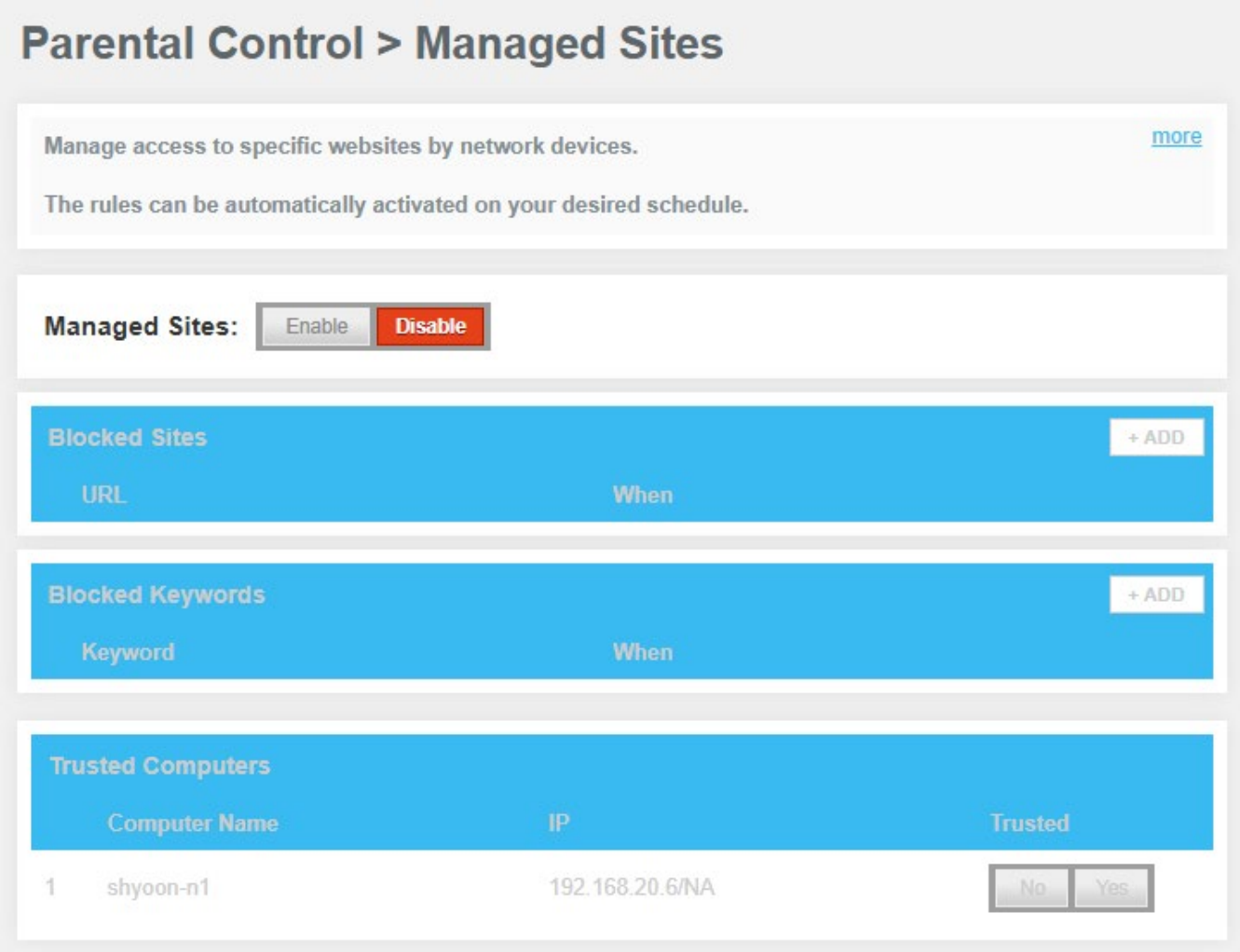
• Click the [ADD DEVICE WITH RESERVED IP] button, you will be taken to a page where you can set a static IP address.

② **Offline Devices**: View information about the client devices that have been connected, but are not currently connected.

6. Parental Control

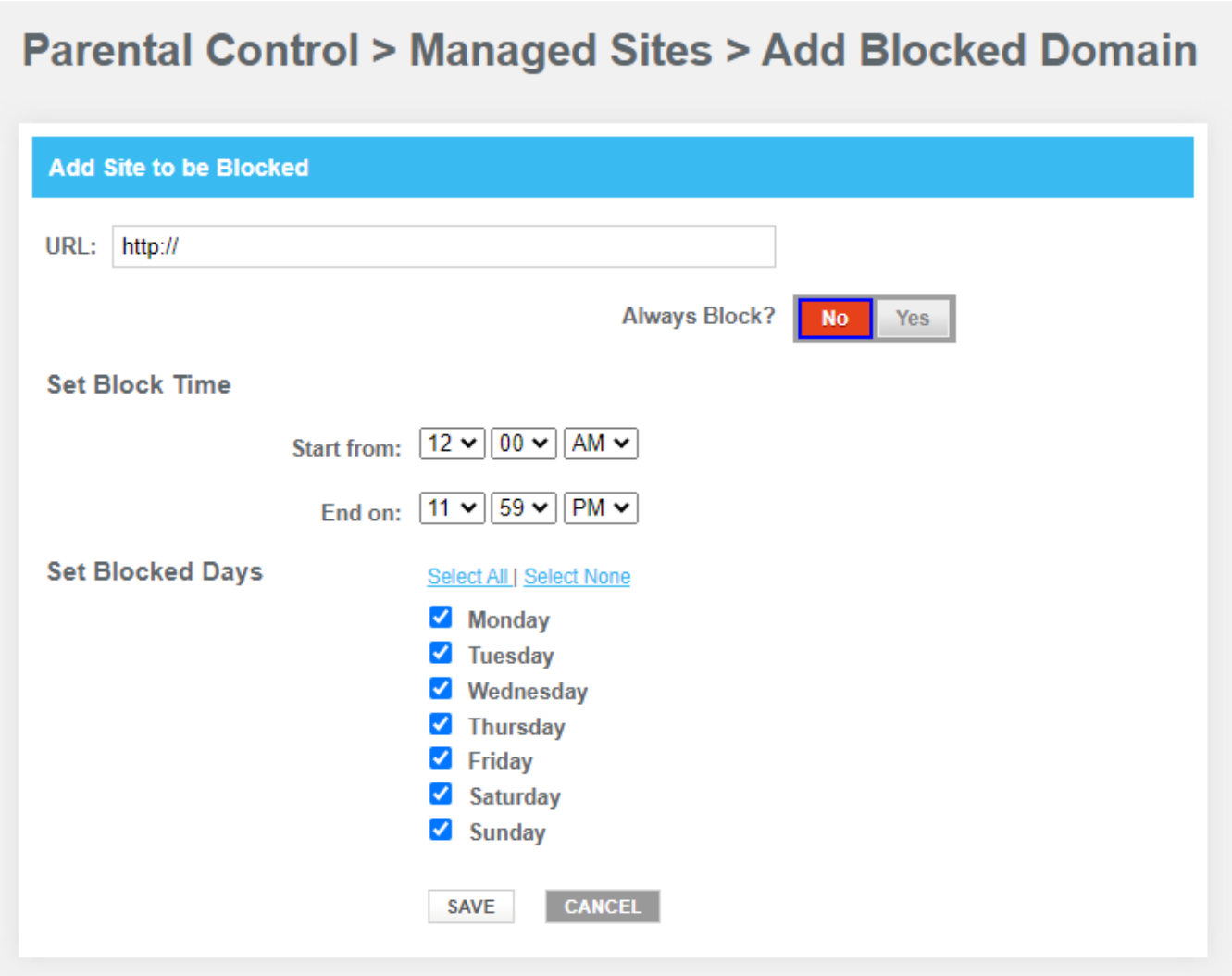
There are five sections under this category, including Managed Sites, Managed IP Address, Managed Services, Managed Devices and Reports.

6.1. Managed Sites



6.1.1. Add Blocked Domain

Register the site you want to block and block access to it. When you press the [+ADD] button, the screen below will be displayed.



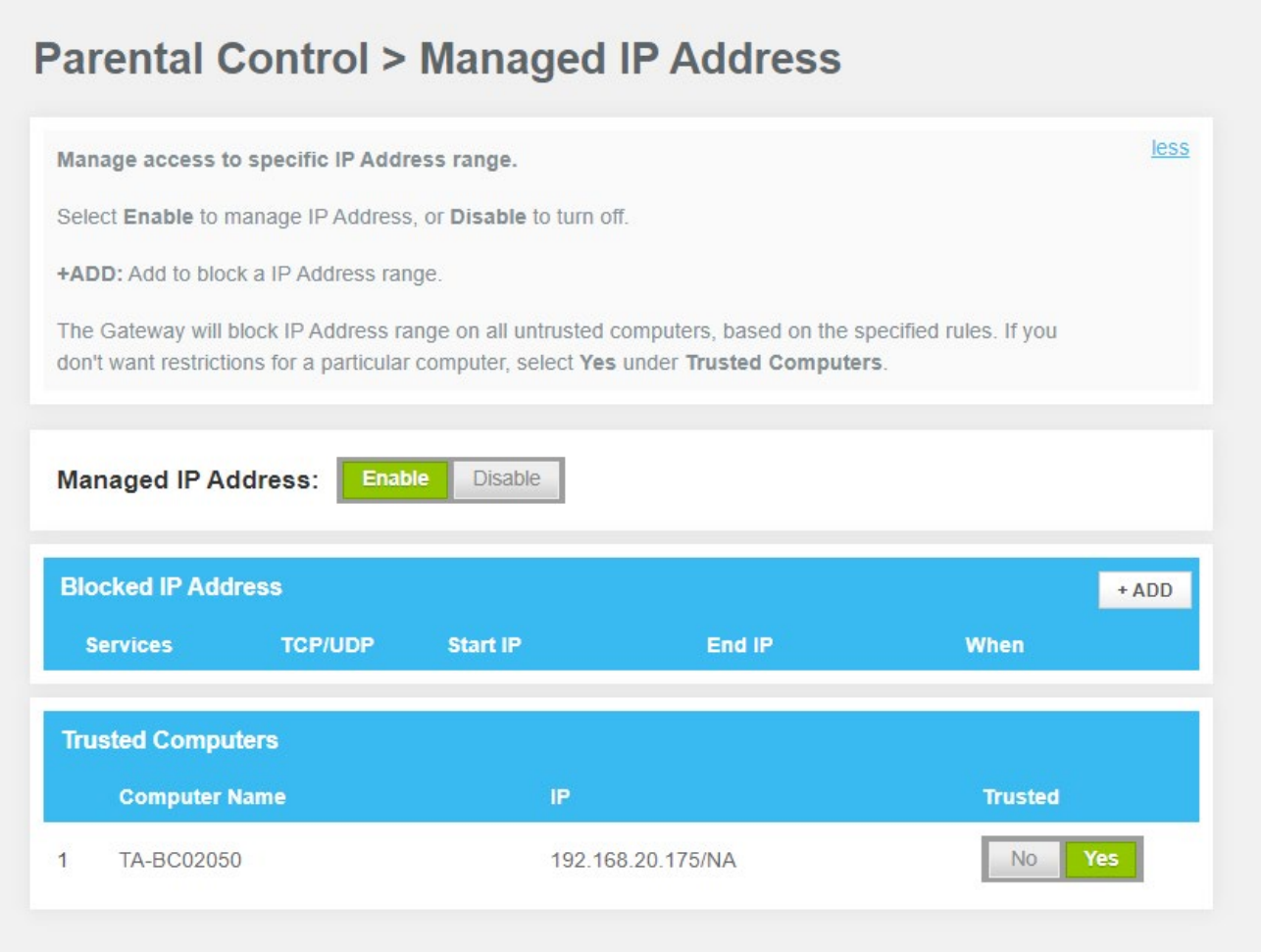
Add Blocked Domain	
URL	Enter the address of the site you want to block.
Always Block	Set whether to always block access or only at certain times to the entered address. If you select No, you can set the days and times you want to block.
Set Block Time	Enter the start and end times you want to block.
Set Blocked Days	Select the day of the week you want to block.

• Enter all values and save them by pressing the [SAVE] button.

• When you press the [CANCEL] button, all entered values will not be saved and you will return to the previous screen.

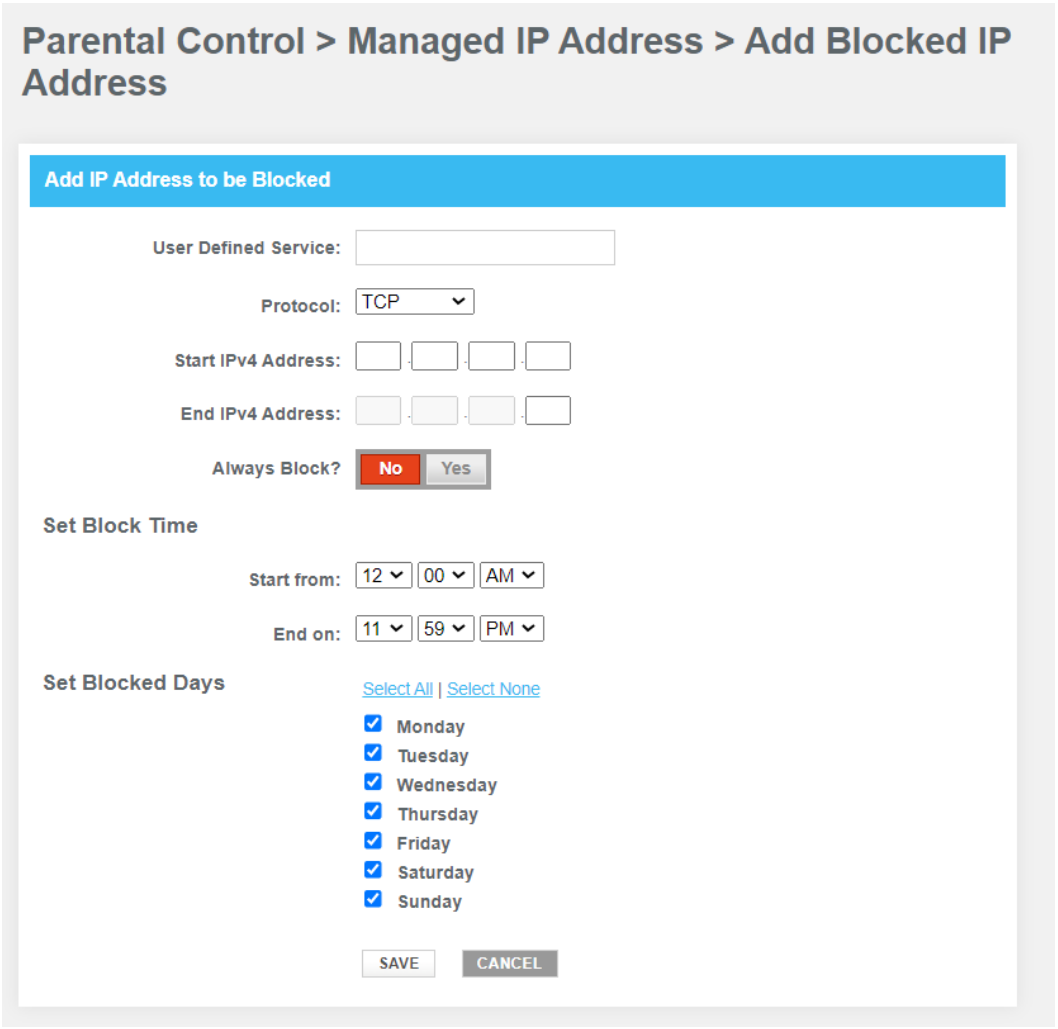
6.2. Managed IP Address

Block access to specific IP address ranges and always set access to trusted devices.



6.2.1. Add Blocked IP Address

Register IP address for the site you want to block to block access. When you press the [+ADD] button, the screen below will be displayed.



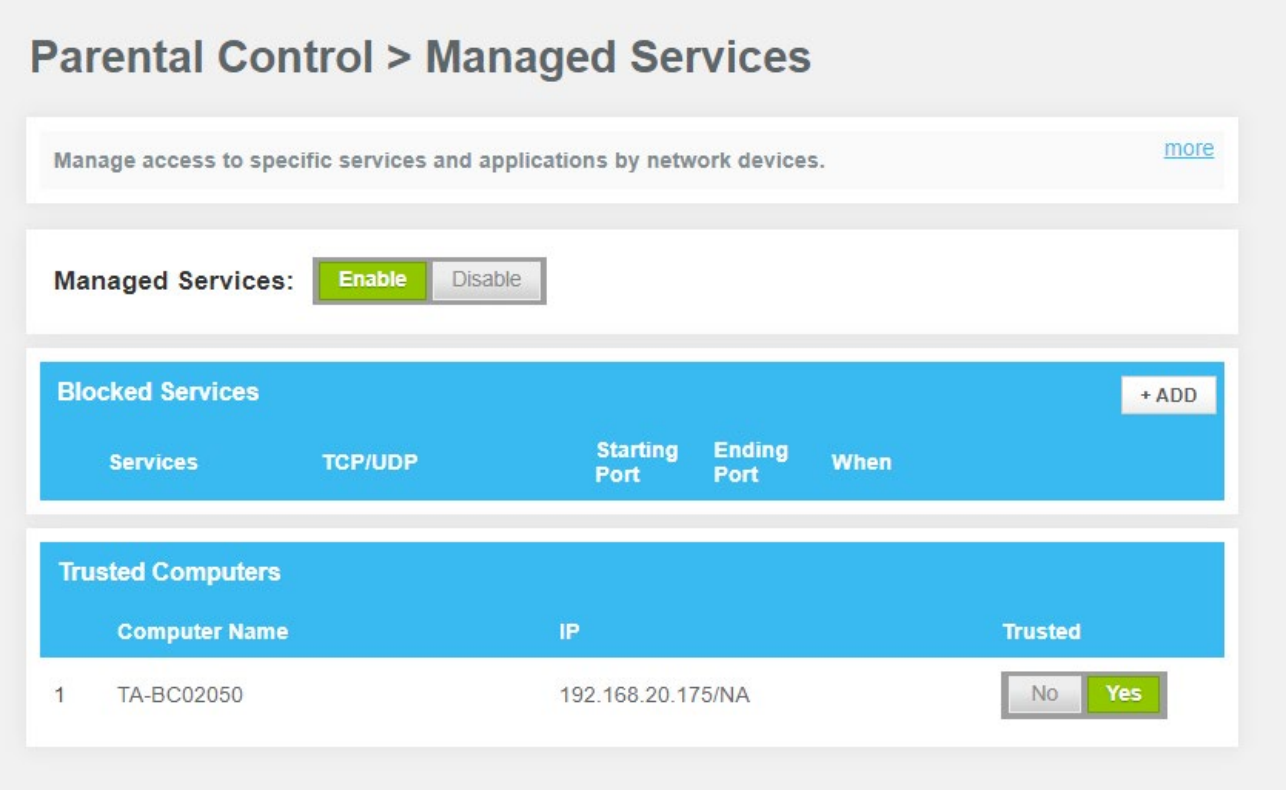
Add Blocked IP Address	
User Defined Service	Enter the IP address you want to block.
Protocol	Select the type of protocol.
Start IPv4 Address	Enter the starting address of the IP address range you want to block.
End IPv4 Address	Enter the end address of the IP address range you want to block.
Always Block	Set whether to always block access or only at certain times to the entered address. If you select No, you can set the days and times you want to block.
Set Block Time	Enter the start and end times you want to block.
Set Blocked Days	Select the day of the week you want to block.

- Enter all values and save them by pressing the [SAVE] button.

• When you press the [CANCEL] button, all entered values will not be saved and you will return to the previous screen.

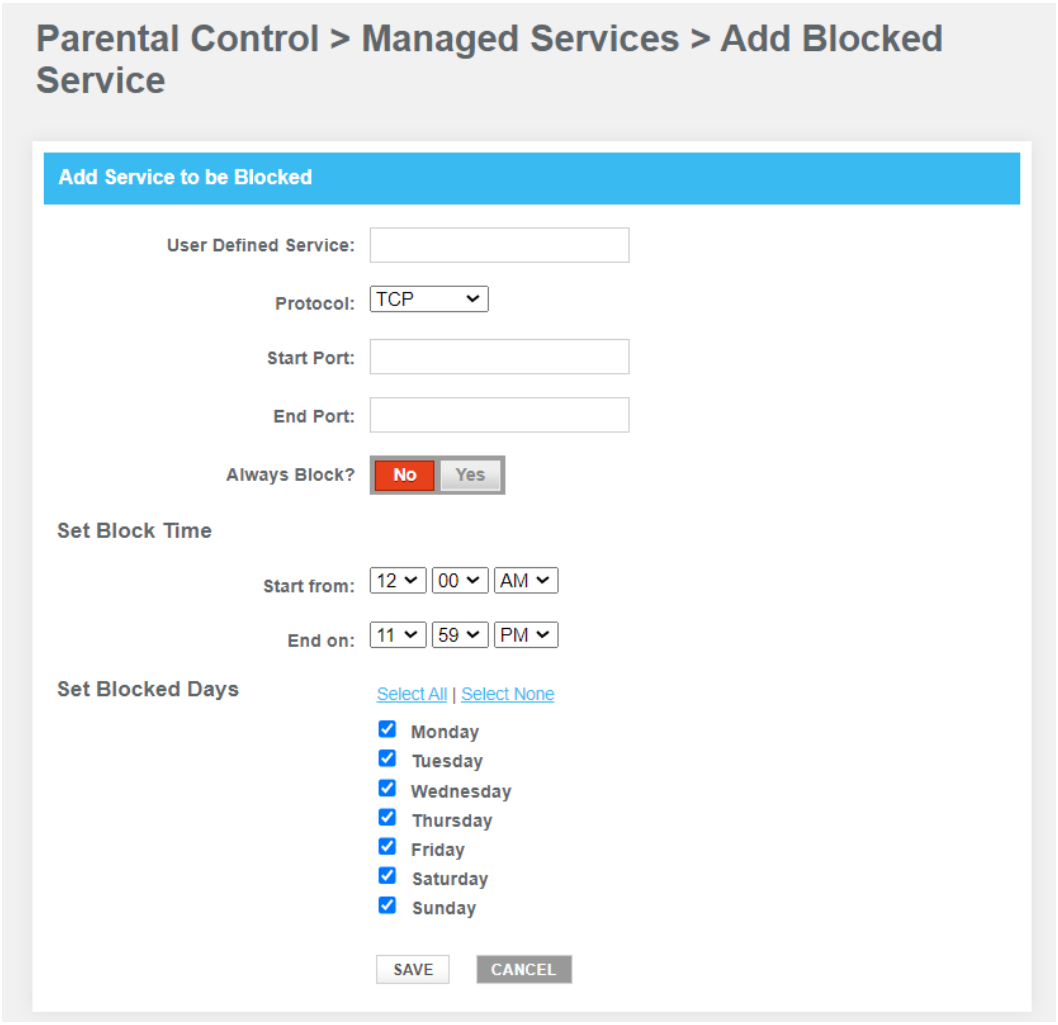
6.3. Managed Services

Manage access to specific services and applications.



6.3.1. Add Blocked Port

Enter the starting port from the port range of the service or application you want to block. When you press the [+ADD] button, the screen below will be displayed.



Add Blocked IP Address	
User Defined Service	Enter the IP address you want to block.
Protocol	Select a protocol(TCP, UDP , or TCP/UDP).
Start Port	Enter the starting port of the Port number range you want to block.
End Port	Enter the end port of the IP address range you want to block.
Always Block	Set whether to always block access or only at certain times to the entered address. If you select No, you can set the days and times you want to block.
Set Block Time	Enter the start and end times you want to block.
Set Blocked Days	Select the day of the week you want to block.

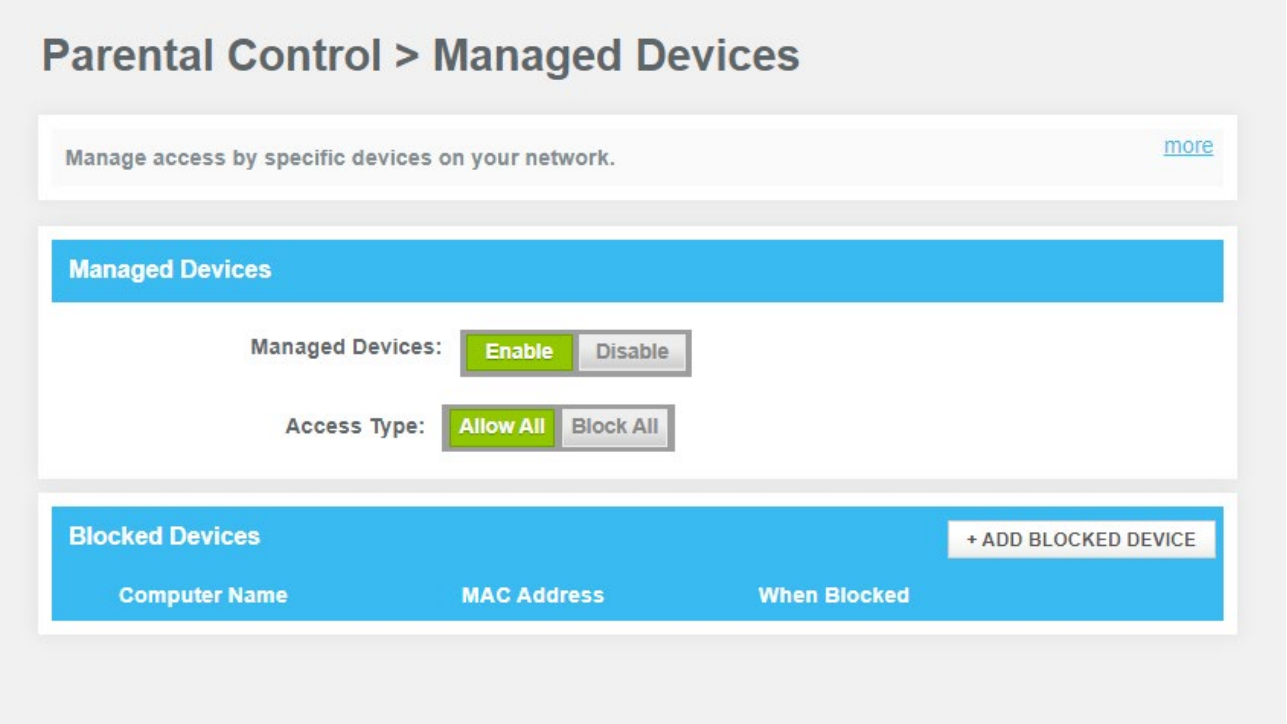
Enter all values and save them by pressing the [SAVE] button.

When you press the [CANCEL] button, all entered values will not be saved and you will return to the previous screen.

6.4. Managed Devices

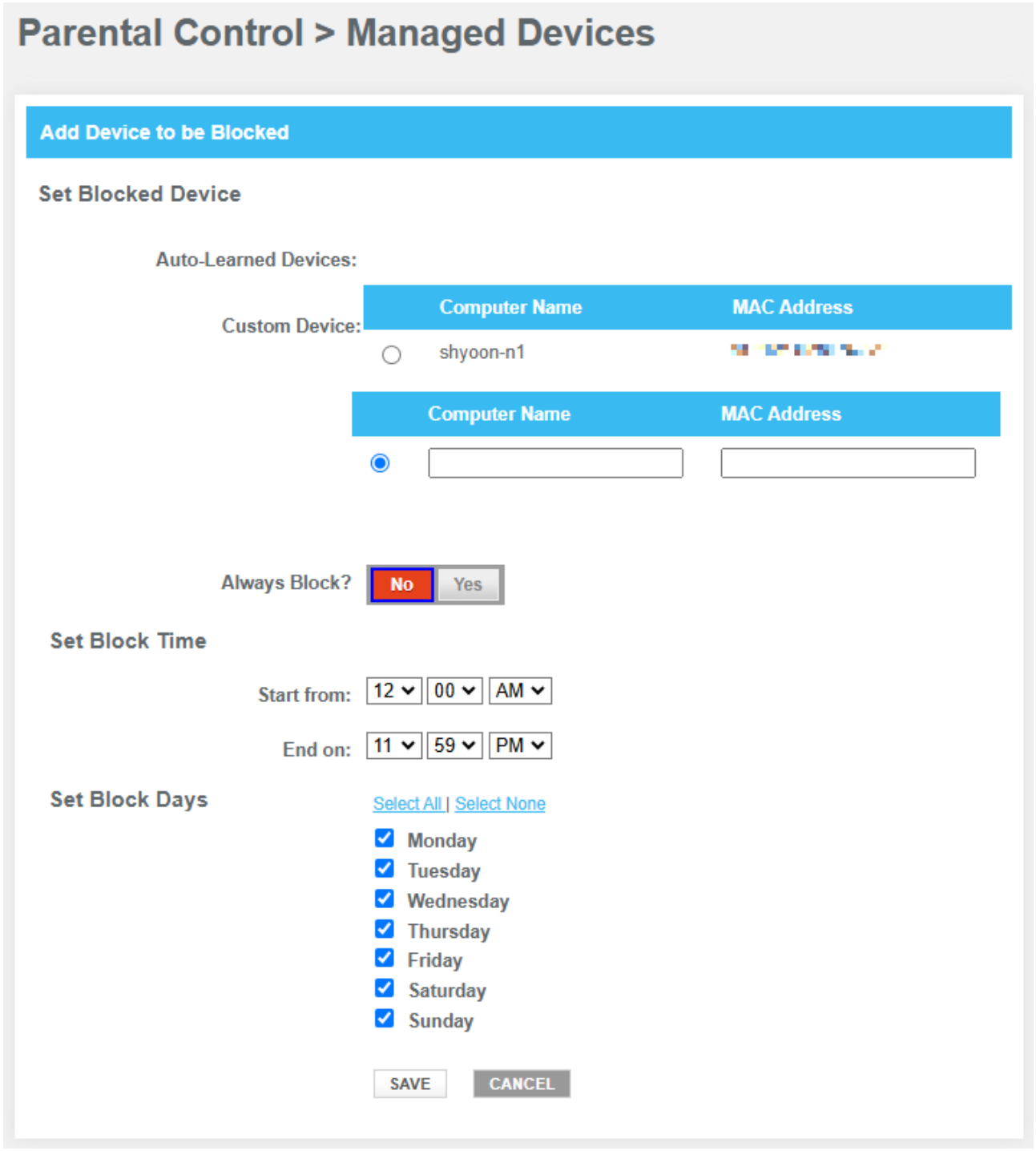
Manage access to specific devices on your network.
Select Enabled to manage network devices, or disabled to turn them off.

If you do not want to restrict devices, select 'Allow All' for Access Type. Then click [+ADD BLOCKED DEVICE] to add only the devices you want to restrict.
To restrict devices, select Block All for Access Type. To add devices that you do not want to restrict, click [+ADD ALLOWED DEVICE].



6.4.1. Add Blocked/Allowed Devices

Enter the port information of the service or application you want to block. When you press the [+ADD BLOCKED DEVICE] button, the screen below appears.

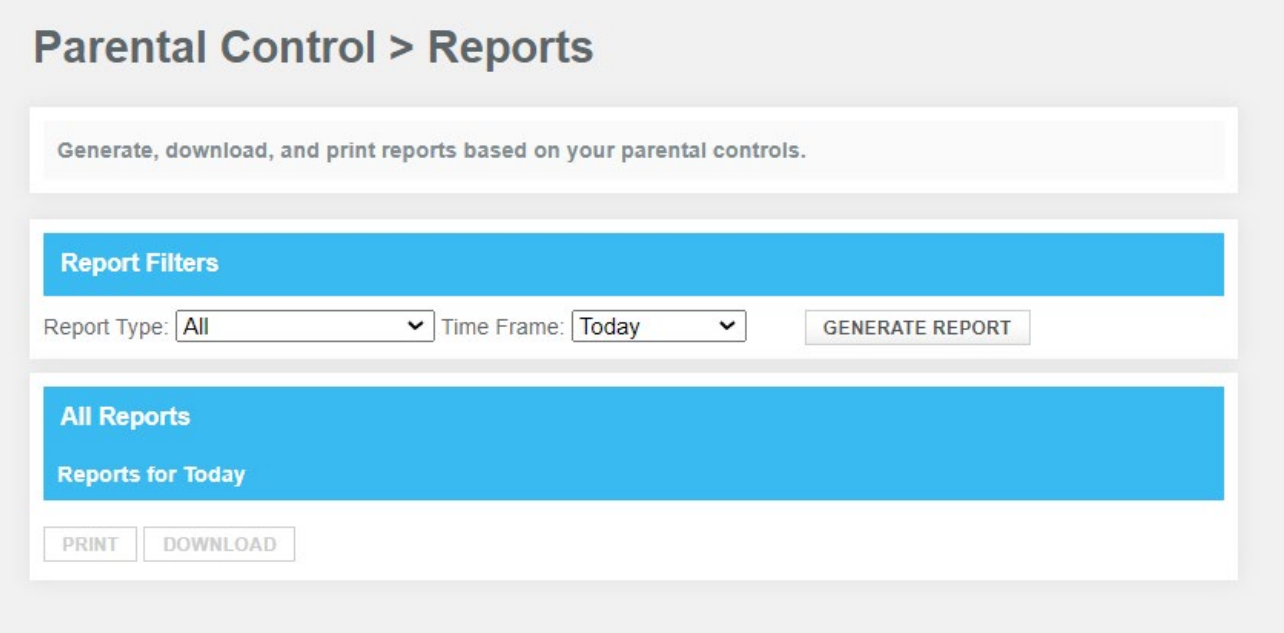


Add Blocked Device	
Set Blocked Device	Set the device you want to block.
Auto-Learned Devices	Select from the list of currently connected devices.
Custom Device	You can directly enter the device name and MAC Address.
Always Block	Set whether to always block access or only at certain times to the

	entered address. If you select No, you can set the days and times you want to block.
Set Block Time	Enter the start and end times you want to block.
Set Blocked Days	Select the day of the week you want to block.

6.5. Reports

You can receive a report on the operation results of the items set for parental control (Managed Site/IP Address/Service/Devices).



Report Filters

① Report Type: Select the management Parental Control type (Managed Site/IP Address/Service/Devices) for which you would like to receive a report.

② Time Frame: Select the period you would like to receive the report. Data is only kept for a maximum of 90 days.

All Reports

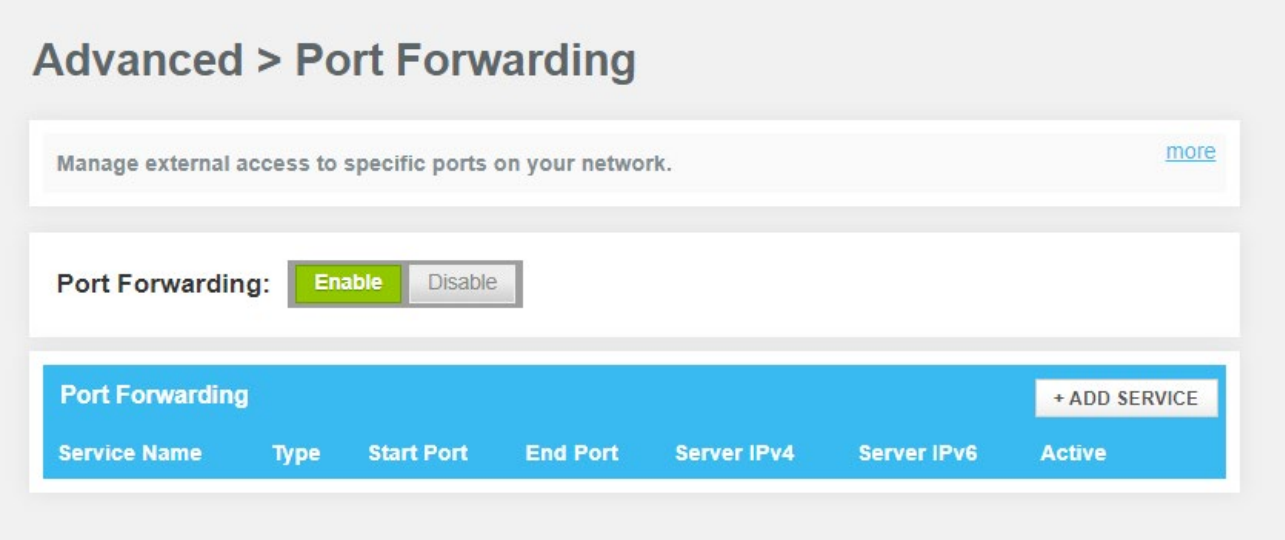
Shows data set in Report Filters. You can print by pressing the [PRINT] button. You can save by pressing the [DOWNLOAD] button.

7. Advanced

7.1. Port Forwarding

Manage external access to specific ports on your network. Port forwarding permits communications from external hosts by forwarding them to a particular port.

Port forwarding settings can affect the device's performance.

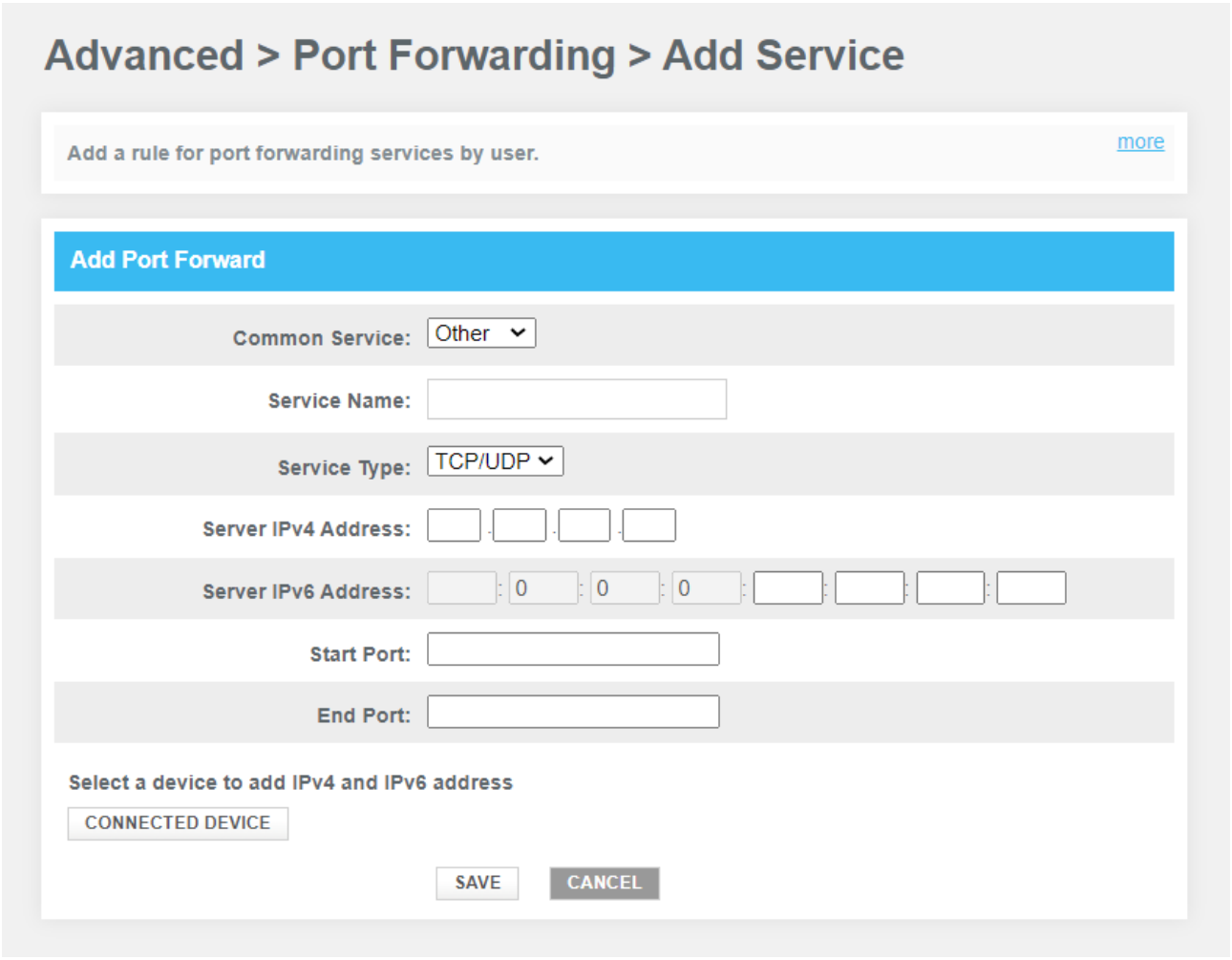


① **Port Forwarding** Enable/Disable: Select Enable to manage external access to specific ports on your network.

Click [+ADD SERVICE] to add new port forwarding rules.

7.1.1. Add Port Forwarding Rule

Add a rule for port forwarding services. When you press the [+ADD SERVICE] button, the screen below appears.



Add Port Forward	
Common Service	Provides a list of applications using the specified port. The port number is automatically populated when you select an application. If the service you want to add is not in the list, select 'Others', then enter the service name and specify the local port and external port.
Service Name	After selecting 'Others', you can directly enter the Service Name.
Select Type	Select a protocol(TCP, UDP, or TCP/UDP).
Server IPv4 Address	Enter the internal IPv4 address of the device for port forwarding.
Server IPv6 Address	Enter the internal IPv6 address of the device for port forwarding.
Start Port	Enter the starting port you want to open on the device for port forwarding.
End Port	Enter the end port you want to open on the device for port forwarding.

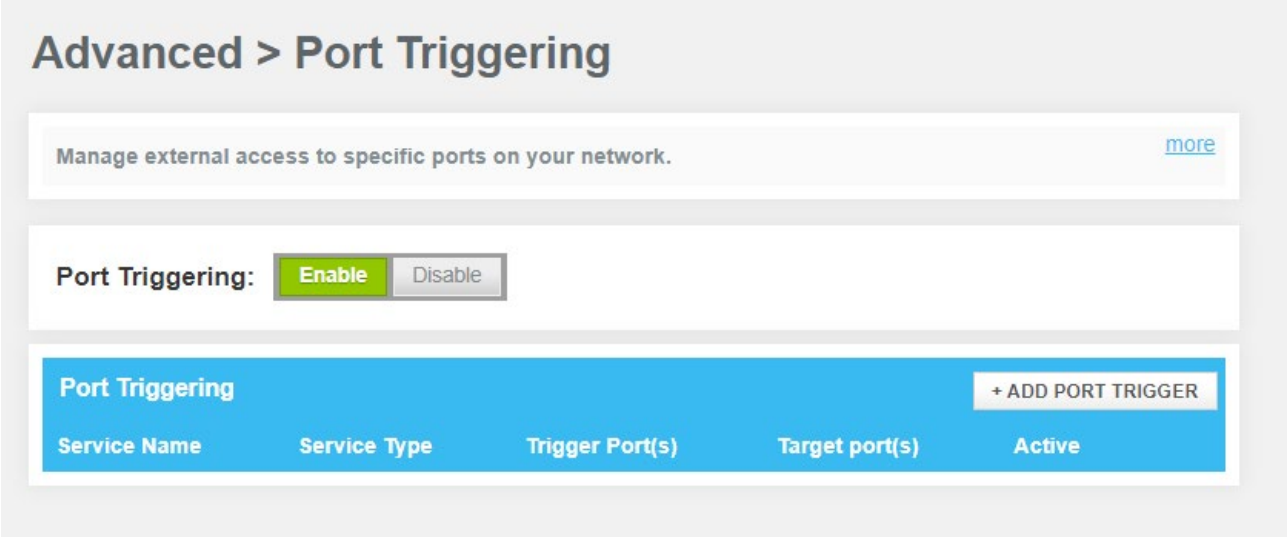
- Enter all values and save them by pressing the [SAVE] button.

7.2. Port Triggering

Set the necessary ports in the network environment to ensure that specific applications function correctly.

Port triggering monitors outbound traffic on your network. When traffic is detected on a particular outbound port, the device remembers that computer's IP address, triggers the inbound port to accept the incoming traffic, and directs the communications to the same computer.

Port triggering settings can affect the device's performance.

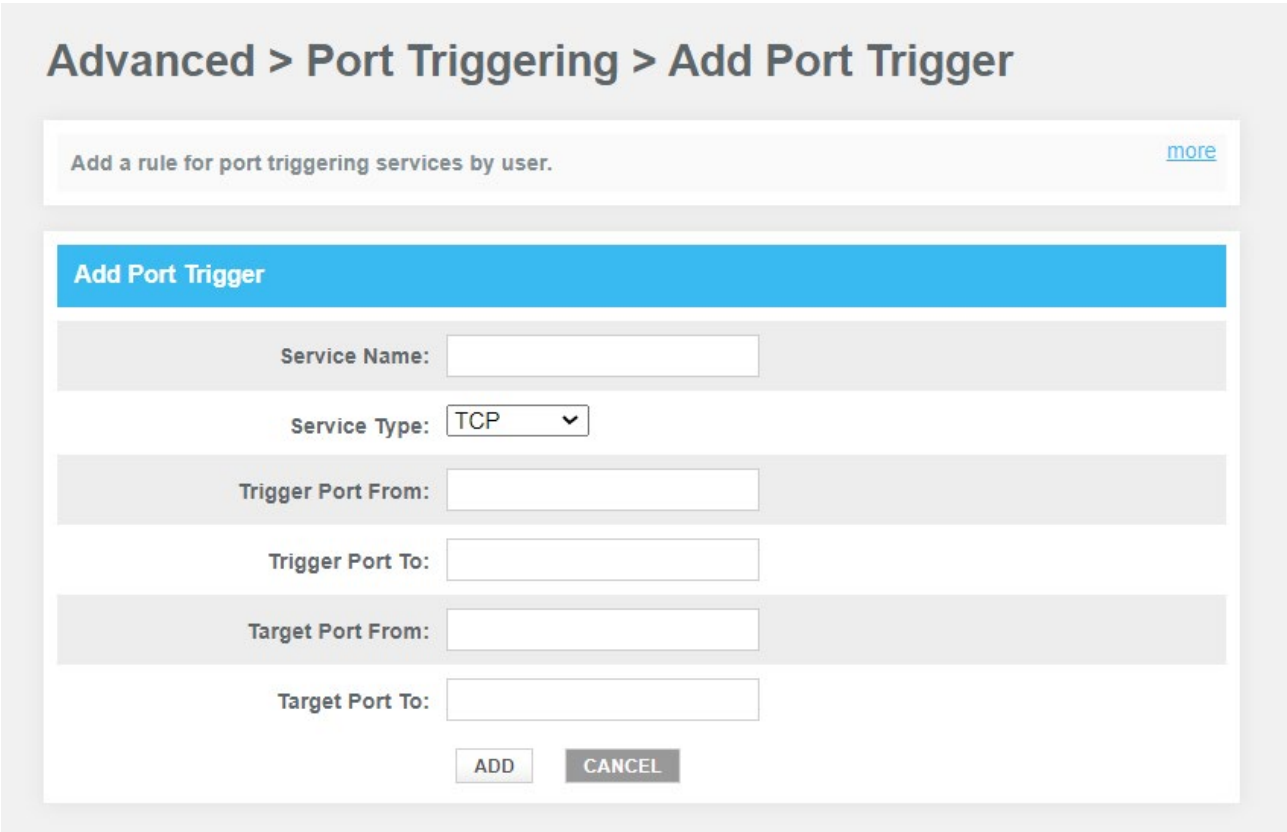


① **Port Triggering** Enable/Disable: Select Enable to manage external access to specific ports on your network.

Click [+ADD SERVICE] to add new port triggering rules.

7.2.1. Add Port Triggering Rule

Add a rule for port triggering services. When you press the [+ADD SERVICE] button, the screen below appears.

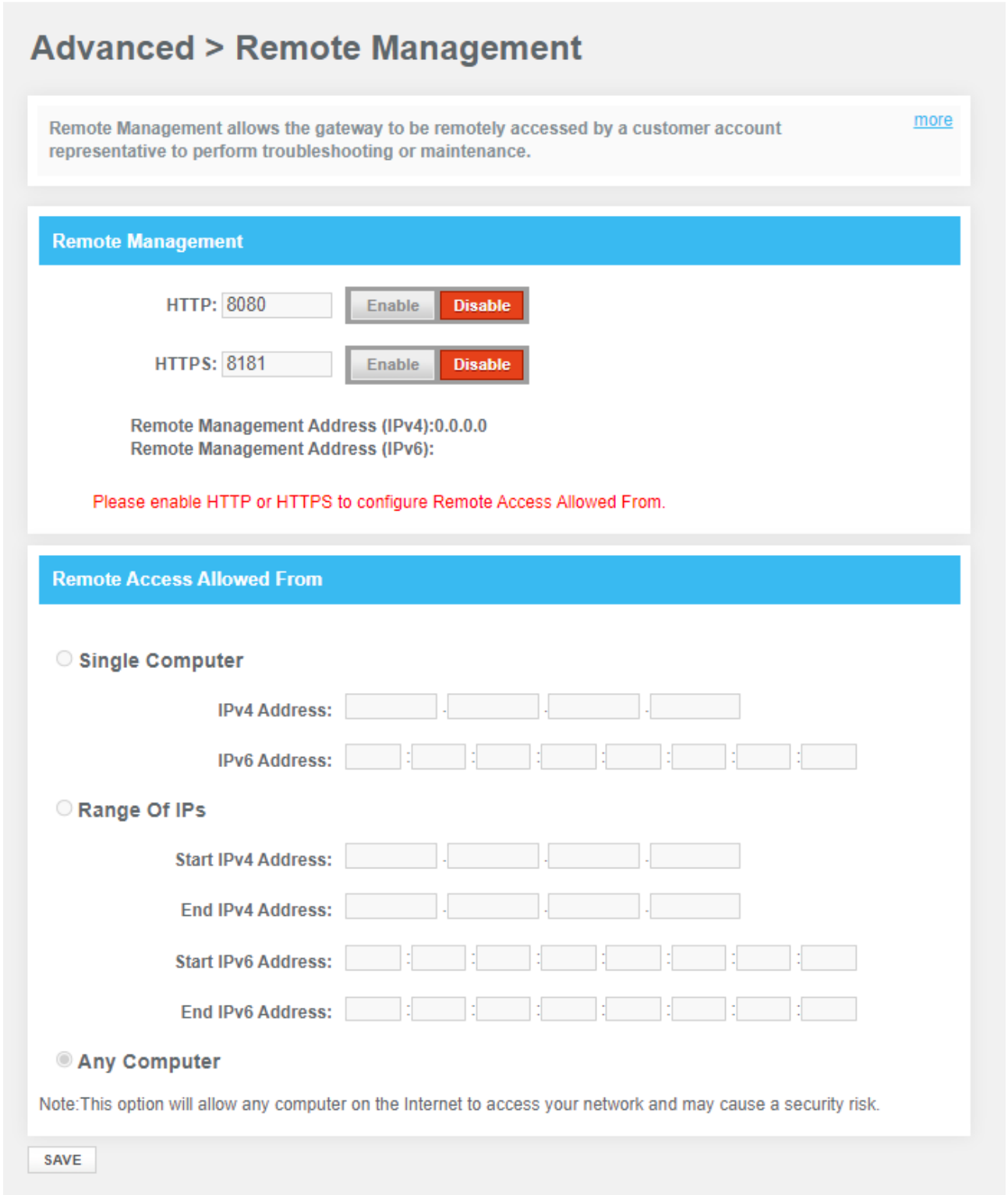


Add Port Trigger	
Service Name	Enter the Service Name.
Select Type	Select a protocol(TCP, UDP, or TCP/UDP).
Trigger Port From	Set the Start port among the port ranges used when the application connects to an external server.
Trigger Port To	Set the End port among the port ranges used when the application connects to an external server.
Target Port From	Enter the starting port you want to open on the device for port forwarding.
Target Port To	Enter the end port you want to open on the device for port forwarding.

- Enter all values and save them by pressing the [SAVE] button.

7.3 Remote Management

Remote Management allows the device to be remotely accessed by a customer account representative to perform troubleshooting or maintenance.



Remote Management

Remote Management can be used via HTTP and HTTPS.

① **HTTP** Enable/Disable: Set whether to use the HTTP protocol. Enable the HTTP option and enter the value for HTTP Port, then you can access your device from HTTP. For example, if the WAN IP address is 11.22.11.22 and the HTTP port number is 8080, then you would use http://11.22.11.22:8080

② **HTTPS** Enable/Disable: Set whether to use the HTTPS protocol. It's the same way to configure HTTPS.

Remote Access Allowed From

Select the remote access range below.

① **Single Computer**: Remote access is only possible through designated IPv4/IPv6.

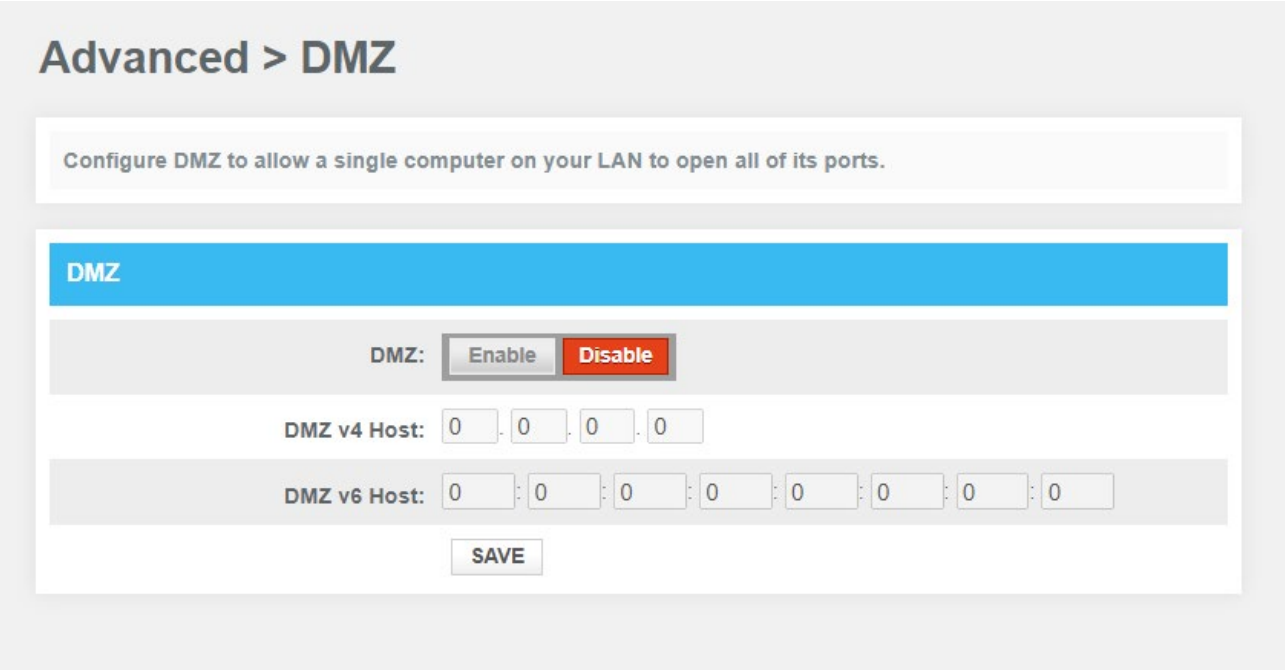
② **Range Of IPs**: Remote access is only possible within the specified IPv4/IPv6 address range.

③ **Any Computer**: All devices in the network can be accessed remotely.

• Enter all values and save them by pressing the [SAVE] button.

7.4. DMZ

DMZ (De-Militarized Zone) is an intermediate network area situated between the public internet and the internal network. Servers or devices located in this zone are accessible from the internet but have restricted access to the internal network. This setup protects the internal network from security threats while providing necessary services to external users.



① **DMZ** Enable/Disable: Set whether to use the DMZ feature.

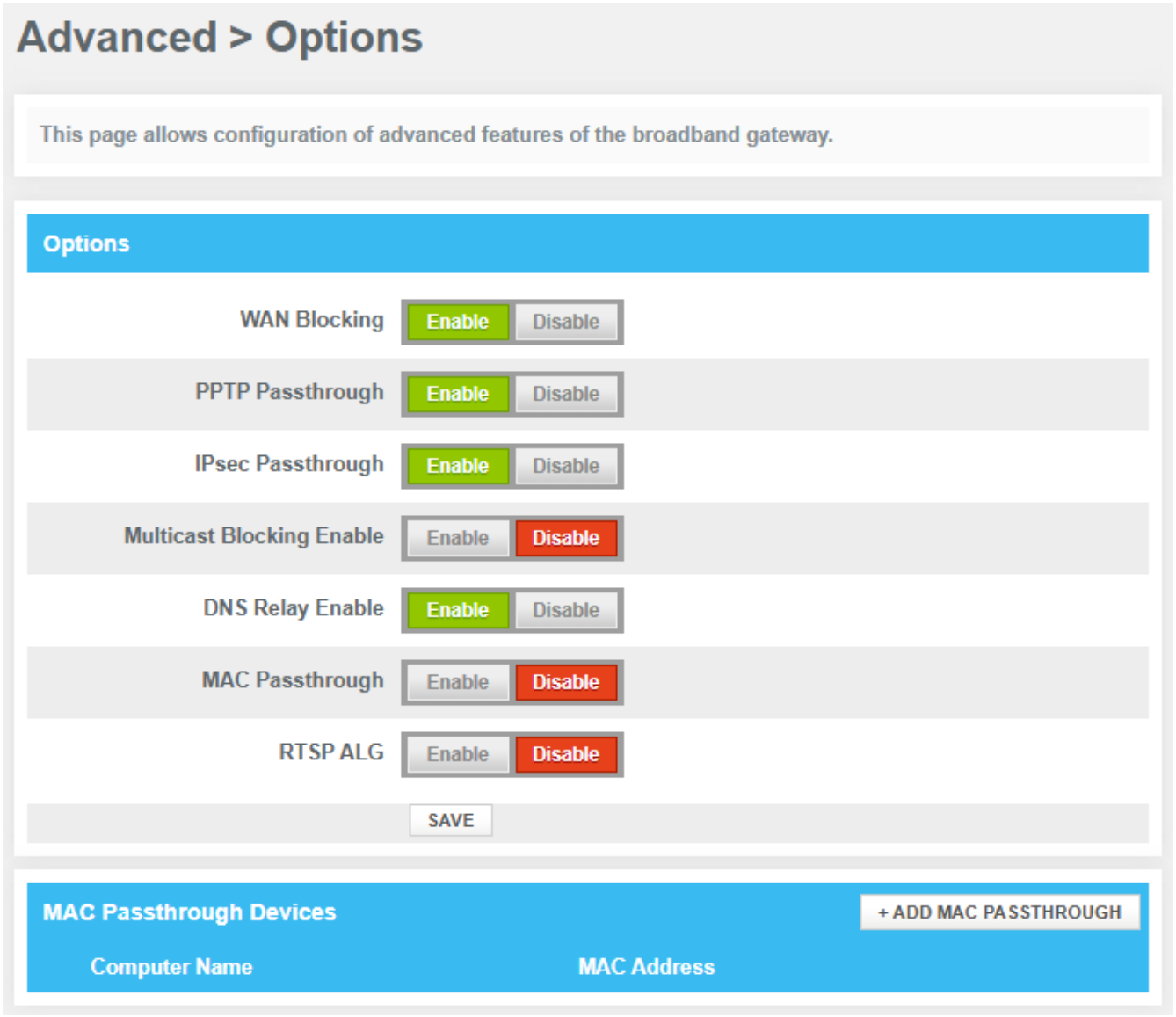
② **DMZ v4 host**: Enter the IPv4 address of the externally accessible DMZ host device.

③ **DMZ v6 host**: Enter the IPv6 address of the externally accessible DMZ host device.

- Enter all values and save them by pressing the [SAVE] button.

7.5. Options

This page allows configuration of advanced features of the broadband device.



Options

① **WAN Blocking** Enable/Disable: To block the WAN IP to response the ping.

② **PPTP Passthrough** Enable/Disable: Allow the PPTP protocol passthrough the NAT.

③ **IPsec Passthrough** Enable/Disable: Allow the IPsec protocol passthrough the NAT.

④ **Multicast Blocking** Enable/Disable: Not Allow Multicast forwarding to other LAN or WLAN.

⑤ **DNS Relay** Enable/Disable: DNS Relay is a feature that forwards DNS queries to DNS servers. When enabled, it processes DNS requests from local network devices, caching responses to improve resolution speed and reduce external DNS traffic.

⑥ **MAC Passthrough** Enable/Disable: The particular MAC address of the computer will bypass the

NAT and operating as Bridge mode and that computer will get the same IP subnet as the WAN IP.

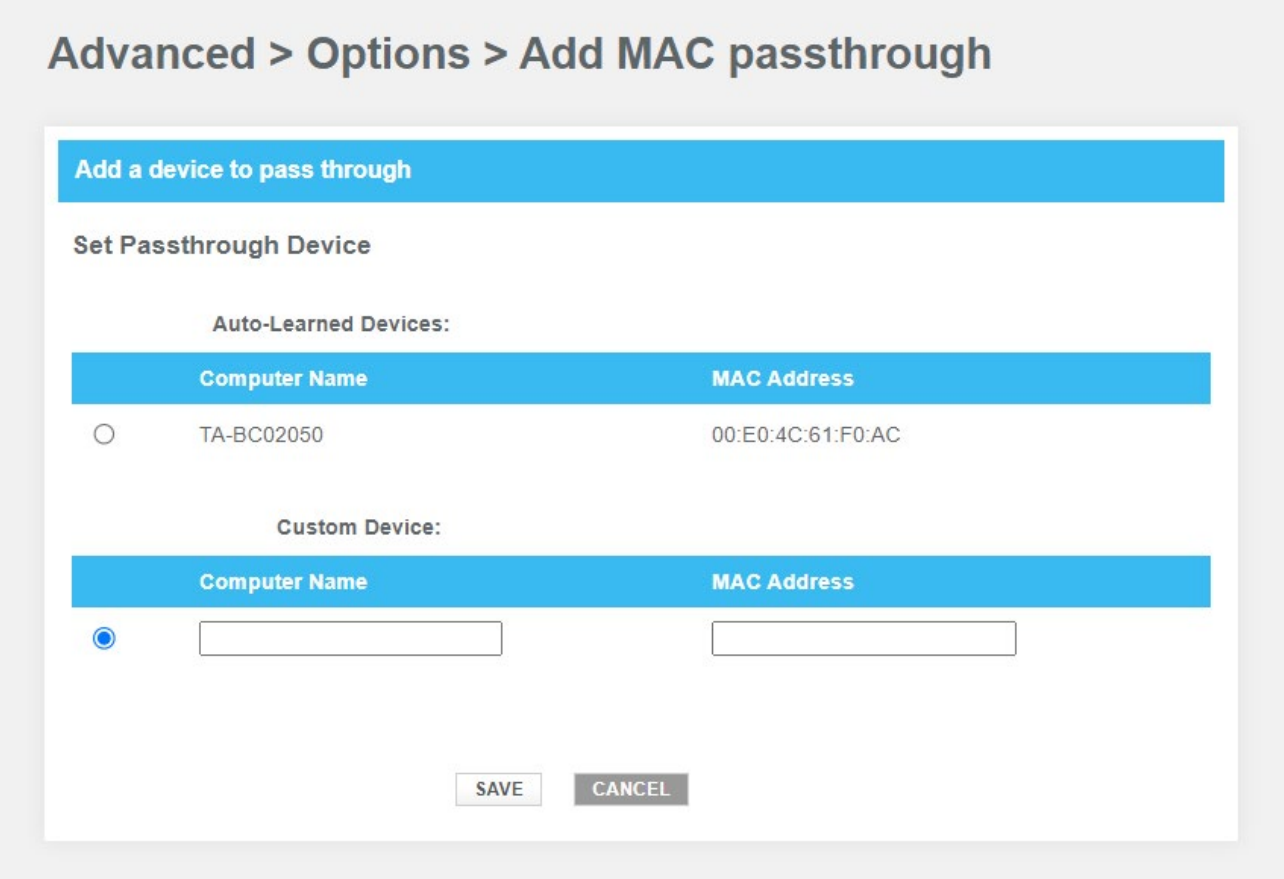
⑦ **RTSP ALG** Enable/Disable: When enabled, it automatically translates RTSP packet IP/port in NAT environments, ensuring smooth RTSP streaming operation.

Click [+ADD MAC PASSTHROUGH]] to add new passthrough rules.

Register the MAC address that will operate as MAC passthrough.

7.5.1. Add Pass Through Devices

Register the MAC address that will operate as MAC passthrough.

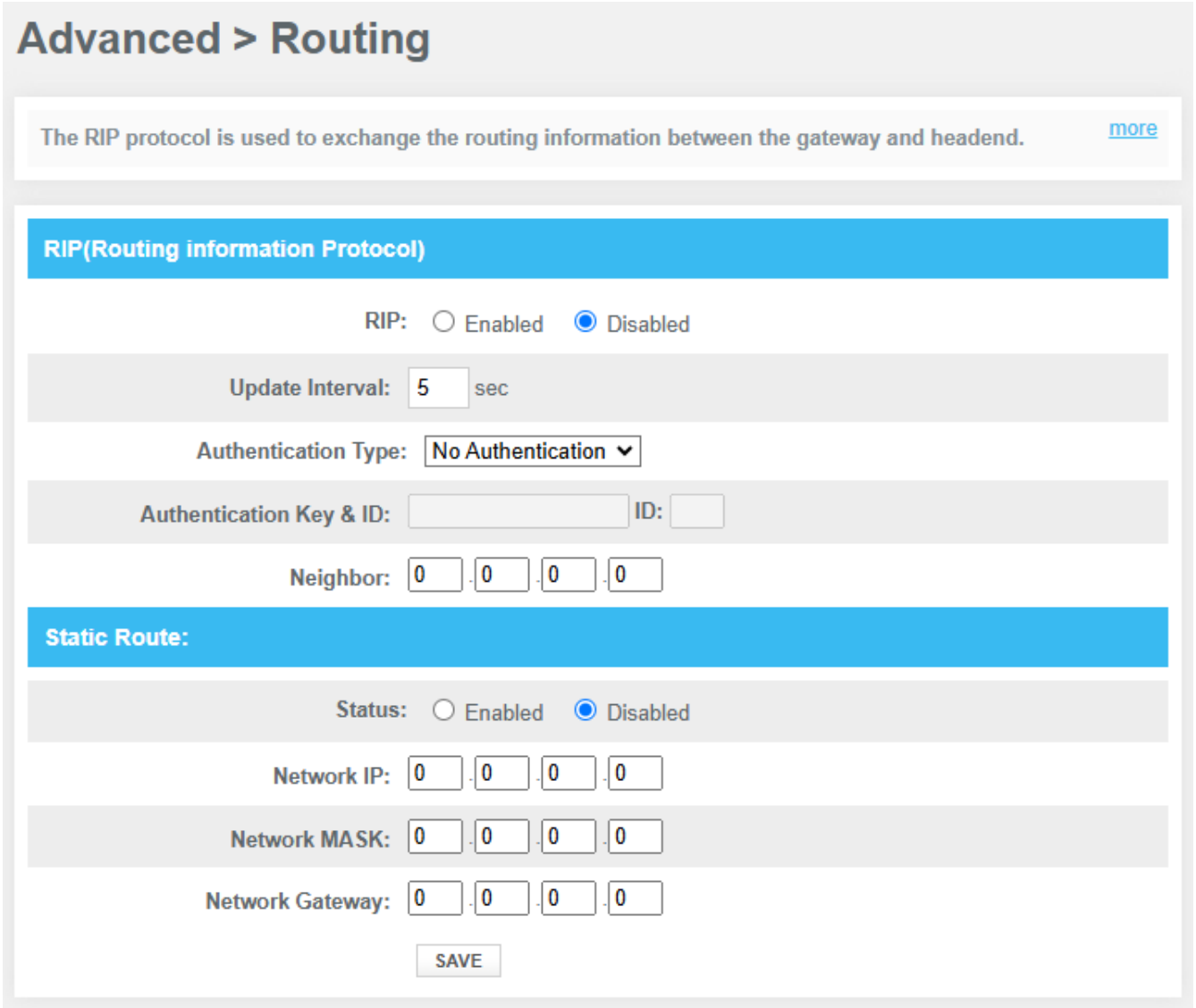


Add Pass Through Devices	
Set Passthrough Device	Set the device you want to block.

Auto-Learned Devices	Select from the list of currently connected devices.
Custom Device	You can directly enter the device name and MAC Address.

- Enter all values and save them by pressing the [SAVE] button.

7.6. Routing



RIP (Routing Information Protocol)

① **RIP** Enable/Disable: Set whether to use RIP.

② **Update Interval**: Set the interval for sending routing updates.

③ **Authentication Type**: Select the RIP authentication type.

④ **Authentication Key & ID**: Enter your Key and ID for authentication.

⑤ **Neighbor**: Enter the IP address of a specific router to which you want to send routing updates directly as unicast.

Static Route

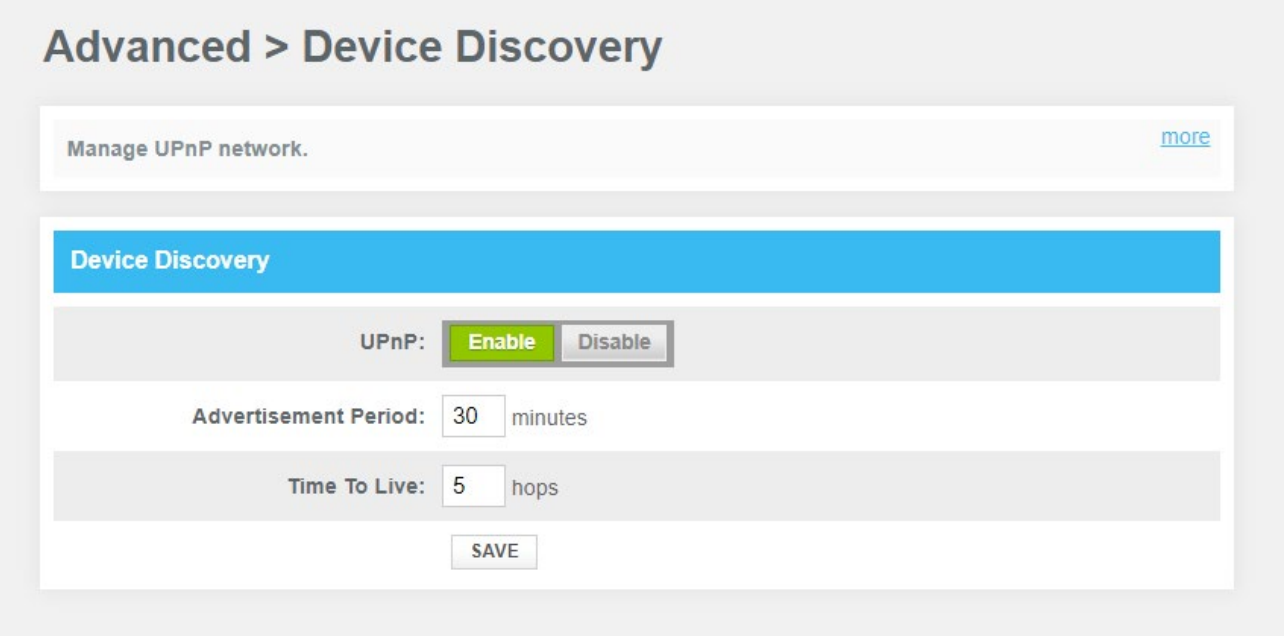
① **Status** Enable/Disable: Set whether to use Static.

② **Network IP**: Set the destination IP address where the packet will arrive.

③ **Network MASK**: Set the subnet mask to use for Static Routing.

④ **Network Gateway**: Set the gateway address to use for Static Routing.

7.7. Device Discovery



Device Discovery

① **UPnP** Enable/Disable: The UPnP enabled device discovers all UPnP enabled client devices, such as network printers and laptops. Using UPnP, the ports are opened automatically for the appropriate

services and applications. The UPnP devices will be auto configured in the network.

② **Advertisement Period**: The Advertisement Period is how often the device will advertise (broadcast) its UPnP information.

③ **Time to Live**: Measured in hops for each UPnP packet sent. A hop is the number of steps an UPnP advertisement is allowed to propagate before disappearing.

- Enter all values and save them by pressing the [SAVE] button.

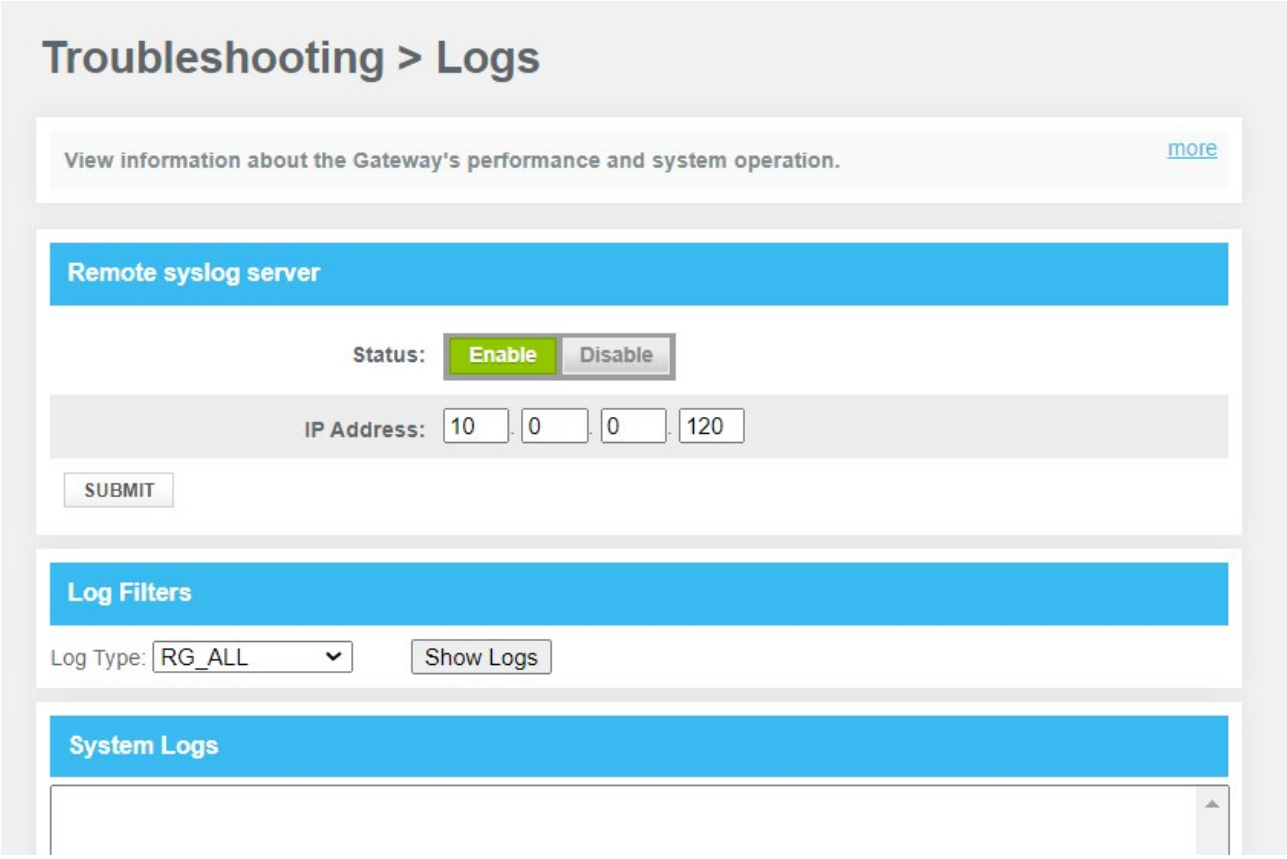
8. Troubleshooting

This category has five menus including Logs, Diagnostic Tools, Wi-Fi Spectrum Analyzer, device Reset/Restore, and Change Password.

8.1. Logs

To check information about the Gateway's performance and system operation, set up a remote syslog server.

Use logs to troubleshoot problems and identify potential security risks.



Remote syslog server

① **Status**: Set whether to use Syslog Server.

② **IP Address**: Enter the server address to forward syslog to.

• Click the [SUBMIT] button to send the Syslog to the entered IP Address.

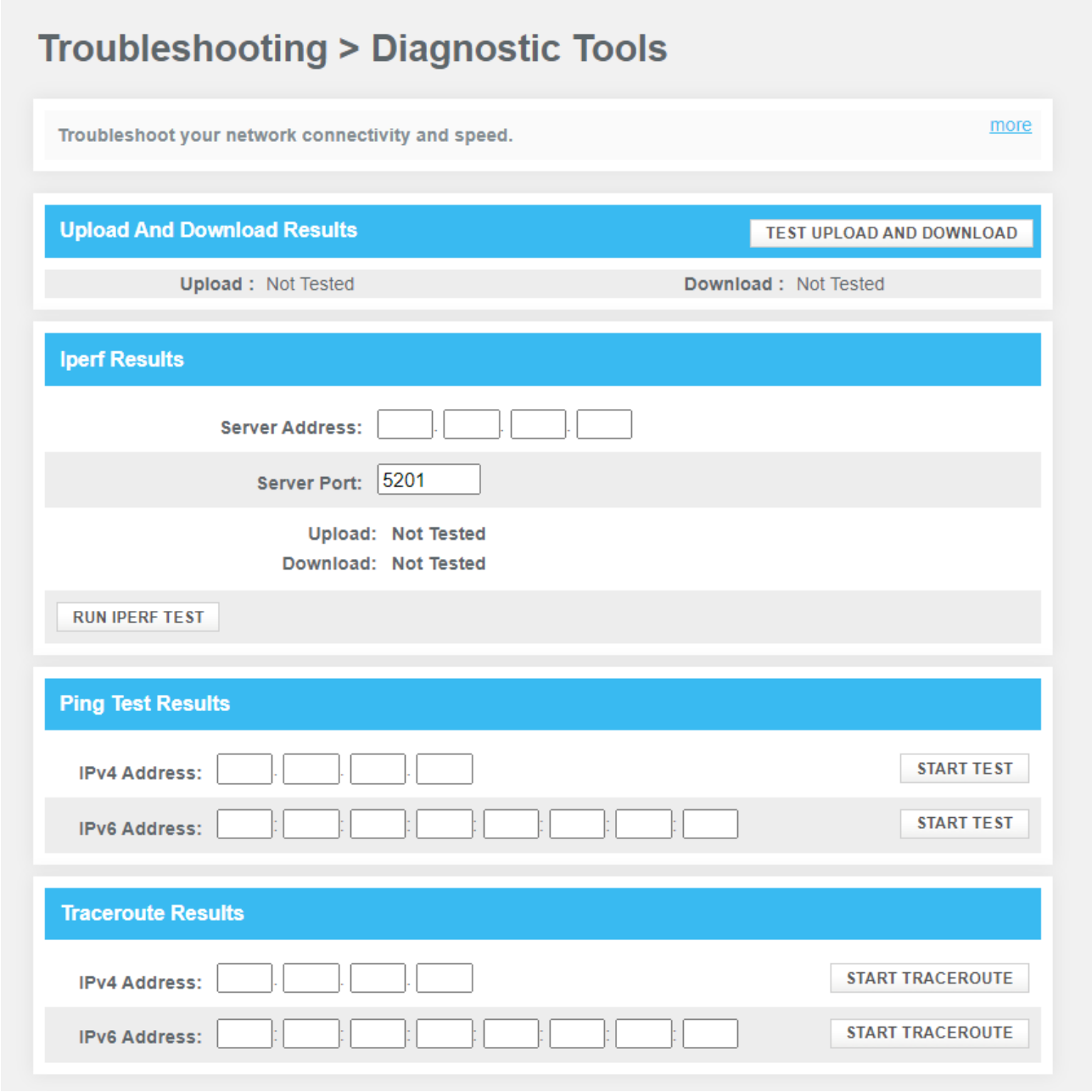
Log Filters

① **Log Type**: Set the type of log data you want to view.

• Click the [Show Logs] button to display the log of the specified type in the System Logs area.

8.2 Diagnostic Tools

Troubleshoot your network connectivity and speed.



Upload And Download Results

Check IPv4 and IPv6 Address Results: Identifies accessibility to specific IP addresses.

;perf Results

① **Server Address**: Enter the address of the server you want to iperf test.

② **Server Port**: Enter port number of the server you want to iperf test.

③ **Upload/Download** : Shows test results.

• Press the [RUN IPERF TEST] button to start testing.

Ping Test Results

① **IPv4 Address**: Enter the IPv4 address for ping test.

② **IPv6 Address**: Enter the IPv6 address for ping test.

• Press the [START TEST] button to start testing.

Traceroute Results

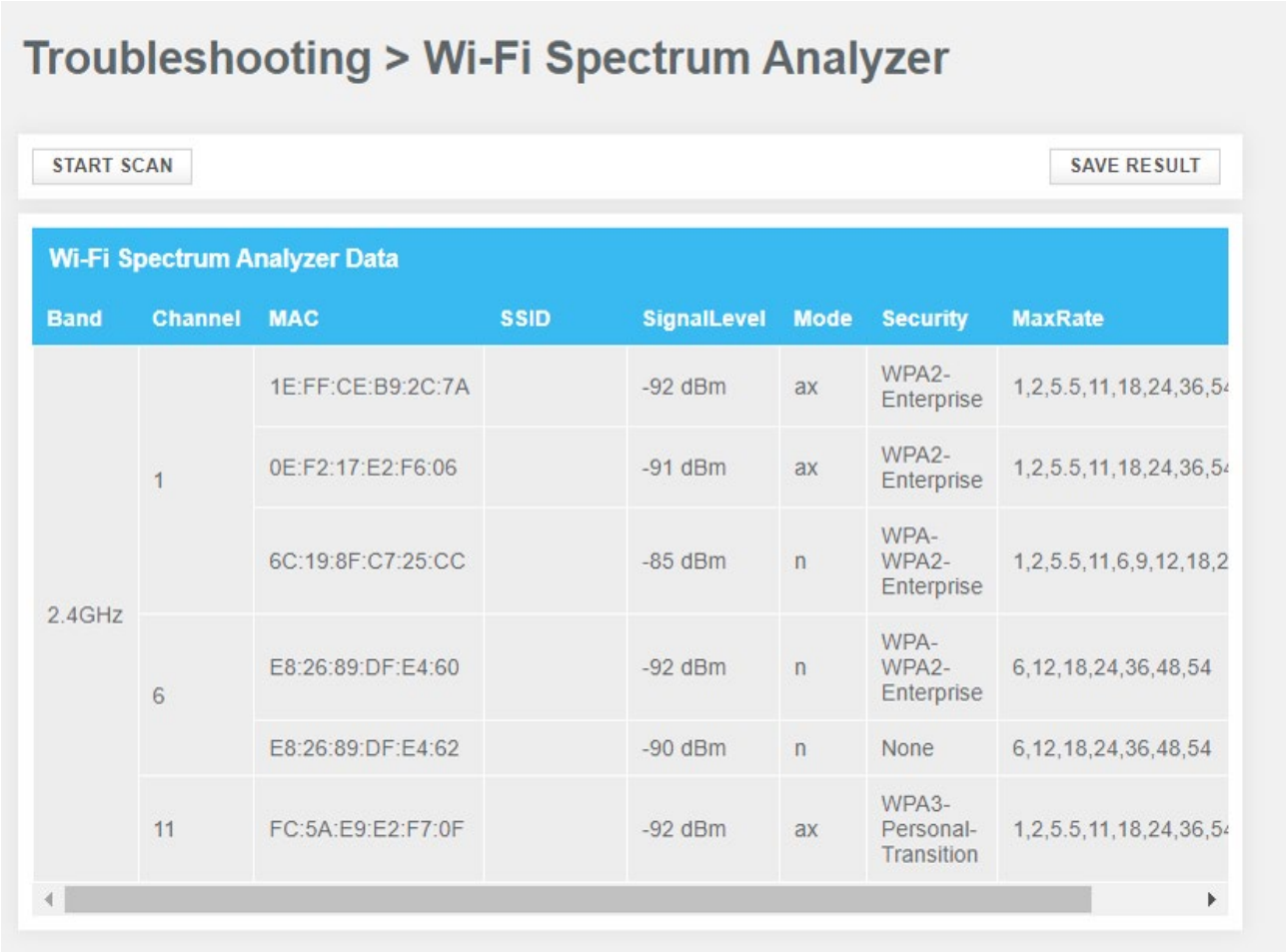
① **IPv4 Address**: Enter the IPv4 address for traceroute test.

② **IPv6 Address**: Enter the IPv6 address for traceroute test.

• Press the [START TRACEROUTE] button to start testing.

8.3 Wi-Fi Spectrum Analyzer

Scans and shows the Wi-Fi spectrum.



- Press the [START SCAN] button to start scanning.

Wi-Fi Spectrum Analyze Data

Shows scan results.

8.4 Reset / Restore Gateway

Reset the device or restore Wi-Fi settings.

If you're having problems with the Gateway, press [RESET] button to restart or [RESTORE to the default factory settings.

① **[RESET]** button: Press the button to restart the device.

② **[RESTORE Wi-Fi SETTINGS]** button: Press the button to reset Wi-Fi setting value.

CAUTION!

All Wi-Fi settings set by the user will be erased. (SSID, Passwords..., etc).

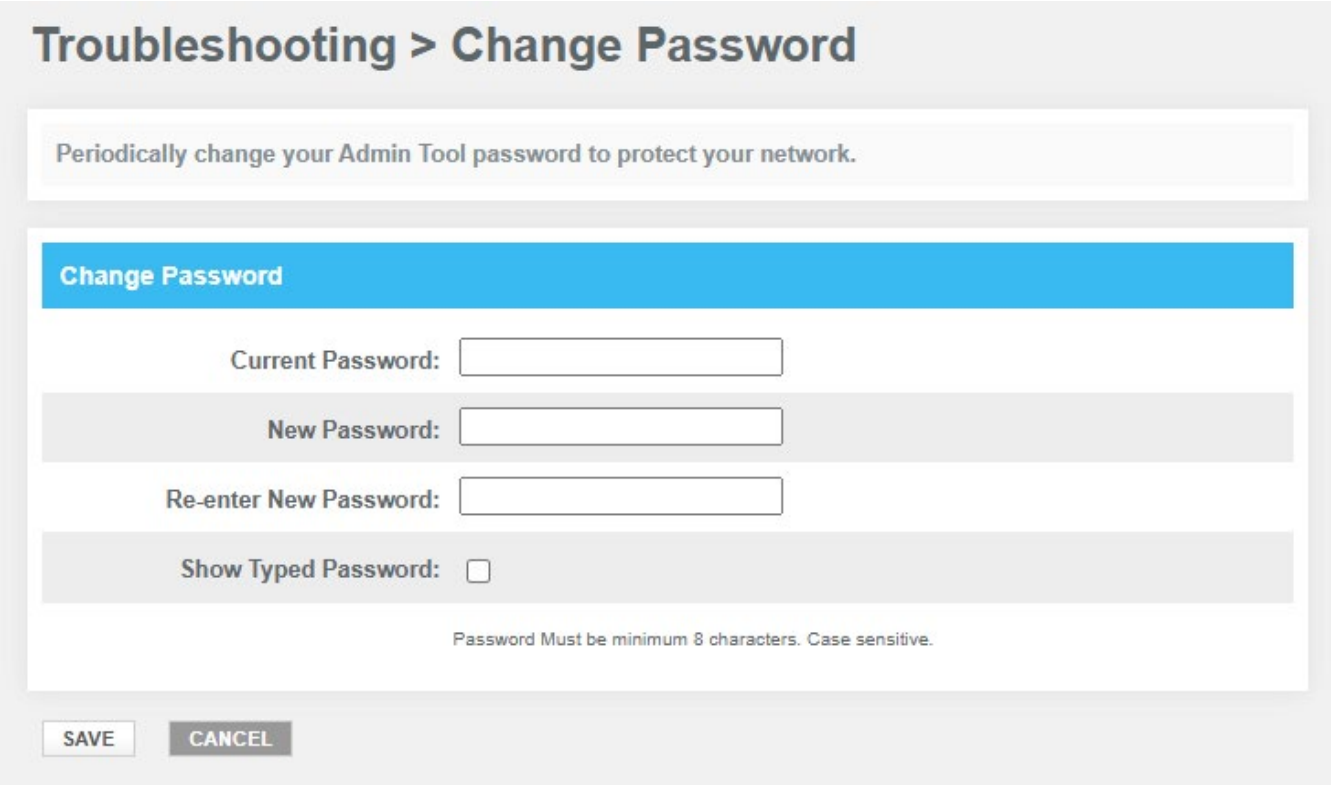
③ **[RESTORE FACTORY SETTINGS]** button: Press the button to reset all setting value.

CAUTION!

RESTORE will erase all your settings (passwords, parental controls, firewall).

8.5 Change Password

Change password on a regular basis to maintain system security.



Change Password	
Current Password	Enter the current password. The initial password is written on the product label.
New Password	Enter the new password you wish to change. Please enter at least 8 characters using a combination of English letters (a~z, A~Z) and numbers. Spaces are not allowed, and it is case sensitive.
Re-enter New Password	Enter the new password again.
Show Typed Password	If checked, the encrypted password will be displayed as the actual entered value.

- Enter all values and save them by pressing the [SAVE] button.

9. Safety Instructions

Please read these instructions carefully before installation/use, and install/use correctly. The precautions given are intended to help you use the product 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.

Usage Caution

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.

RF exposure assessment has been performed to prove that this unit will not generate the harmful EM emission above the reference level as specified in EC Council Recommendation (1999/519/EC)

Energy-Related Products Compliance

Hereby, HUMAX Networks declares that the HGF310/EU devices are in compliance with the essential requirements and other relevant provisions of Directive 2009/125/EC together with Commission Regulation (EC) No 1275/2008 and Commission Regulation (EC) No 801/2013.

The HGF310/EU devices qualify as high network availability (HiNA) equipment. Since the main purpose of HGF310/EU devices is to provide network functionality with HiNA 7 days/24 hours, the modes Off/Standby, Power Management, and Networked Standby are inappropriate.

For information about the type and number of network ports, see “10. Specification”.
For information about power consumption, see “10. Specification”.

Importer: HUMAX Networks GmbH
Alfred-Herrhausen-Allee 3-5 65760 Eschborn Germany

Operation in the 5150 - 5350 MHz band are restricted to indoor usage only.							
AT	EE	IE	NO	CY	CZ	DK	SE
BE	FI	IT	PL	EL	HU	IS	CH
BG	FR	LV	PT	LT	LU	MT	NL
HR	DE	LI	RO	SK	SI	ES	UK(NI)

10. Specification

10 LEDs	
Power, DS, US, Online, LAN, 2.4GHz, 5GHz, WPS, TEL1, TEL2	
2 Buttons	
WPS (Front), Reset (Back panel)	
Interface	
Cable	1 x DOCSIS 3.1 Coaxial Cable US (Switchable): 5~85MHz / 5~204MHz DS (Switchable): 108~1218MHz / 258~1218MHz
LAN Ports	1 x 2.5 Gigabit Ethernet (RJ-45), 3 x 1 Gigabit Ethernet (RJ-45)
TEL	2 x FXS (RJ-11)
USB	1 x USB 2.0 (A-Type)
Power	1 x Power Jack Input: AC100-240V ~ 50/60Hz Output: DC12V, 3.33A (Standby under 8W)
Wireless (2.4GHz)	
Frequency	2412 ~ 2472MHz: 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
MAX Power	19.92dBm

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 (5,470~5,725MHz): 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
MAX Power	29.75dBm
Environmental	
Operating Temperature	0° ~ 40°C
Storage Temperature	-20ºC ~ 60ºC
Operating Humidity	10% ~ 95% (Non-condensing)
Physical Specification	
Dimension	231.2 (H) x 74 (W) x 204 (D) mm (with stand & 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.