Roamii BE Pro Mesh System

User Manual

Table of Contents

COPYRIGHT AND TRADEMARK NOTICE 5

RELEASE VERSION 5

WELCOME TO ROAMII BE PRO MESH SYSTEM 6

1.1 APPEARANCE DESCRIPTION 6
1.2 HOW TO PLACE YOUR ROAMII 7
1.3 SYSTEM REQUIREMENTS 7

2. CREATE YOUR MESH NETWORK 8

2.1 CONNECT YOUR ROAMII 8
2.2 THE INTERNET SETUP WIZARD 9
2.3 CONNECT TO THE WIRELESS NETWORK 11

3. ABOUT THE WEB USER INTERFACE (WEB GUI) 11

3.1 LOGIN WEB GUI 11
3.2 FORGOT PASSWORD? 12
3.3 WEB GUI INTERFACE 13

4. WI-FI SETTINGS 14

4.1 WIRELESS 14
4.1.1 BASIC 14
4.1.2 ADVANCED SETTINGS 16
4.1.3 WPS 18
4.1.4 MAC FILTER 19
4.1.5 FAST ROAMING 20
4.2 GUEST NETWORK 21
4.3 CHILD NETWORK 23
4.4 IOT NETWORK 24

5. ADVANCED 25

5.1 INTERNET 25
5.1.1 INTERNET 25
5.1.2 PORT TRIGGER 26
5.1.3 PORT FORWARDING 27
5.1.4 NAT PASSTHROUGH 29
5.1.5 DMZ 30
5.1.6 DDNS 31
5.2 IPTV&VLAN 32
5.3 FORTISECU 33
5.4 FIREWALL 33
5.4.1 GENERAL 33
5.4.2 ACCESS CONTROL 34
5.4.3 INBOUND FILTER 35
5.4.4 URL FILTER 36
5.4.5 UPNP 37
5.5 QOS 38
5.5.1 TRADITIONAL QOS 38
5.5.2 BANDWIDTH LIMITER 39
5.6 USB 40
5.6.1 FILE SHARING SERVER 40
5.6.2 SAMBA SERVER 41
5.6.3 FTP SERVER 42
5.6.4 BITTORRENT SETTINGS 44
5.6.5 EJECT DEVICE 45
5.7 LOCAL AREA NETWORK (LAN) 46
5.7.1 LAN SETTING 46
5.7.2 DHCP SERVER SETTING 47
5.7.3 ROUTING SETTINGS 49
5.8 IPV6 50
5.9 VPN SERVER 51
5.9.1 OPENVPN 51
5.9.2 PPTP 53
5.9.3 L2TP/IPSEC 55
5.9.4 WIREGUARD 56
5.10 VPN CLIENT 58
5.11 ADMINISTRATION 62
5.11.1 OPERATION MODE 62
5.11.2 SYSTEM MANAGEMENT 63
5.11.3 TIME 64

5.11.4 LOCAL ACCESS CONFIG 65
5.11.5 REMOTE ACCESS CONFIG 66
5.11.6 FIRMWARE UPGRADE 67
5.11.7 RESTORE SETTING 68
5.11.8 SYSTEM LOG 69
5.11.9 PRIVACY 70
5.11.10 FEEDBACK 71
5.11.11 LED DISPLAY 71
5.12 NETWORK TOOLS 72
5.12.1 NETWORK ANALYSIS 72
5.12.2 WIFI ANALYSIS 74

TROUBLESHOOTING 76

Copyright and Trademark Notice

Release Version

Version: v1.0
Date: 2026/06

Welcome to Roamii BE Pro Mesh System

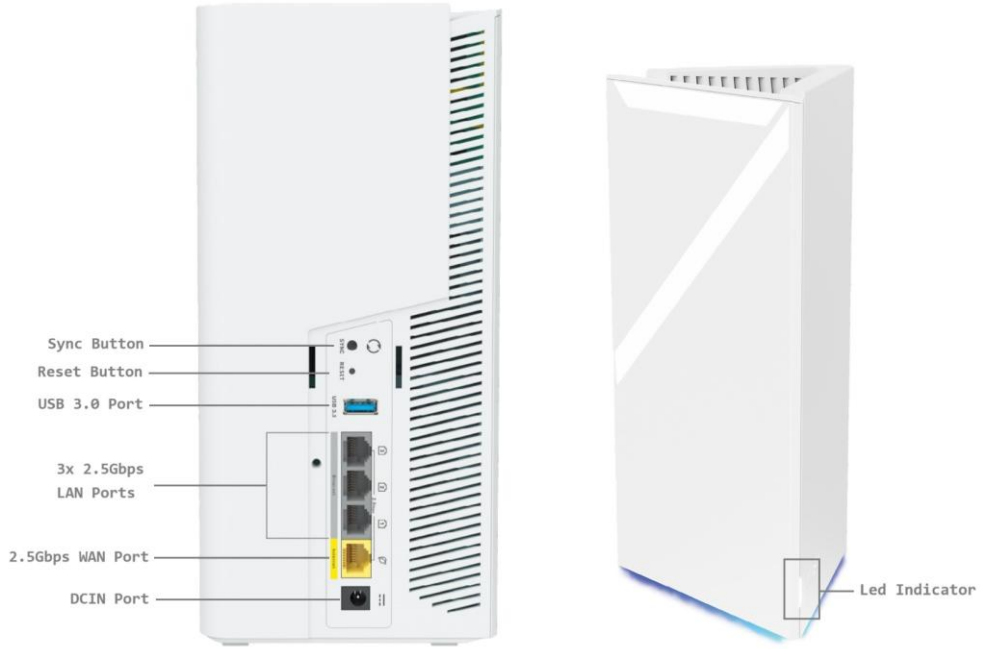
Thank you for choosing the Roamii BE Pro Mesh System Wireless Router.

Roamii BE Pro Mesh System features advanced 802.11be (Wi-Fi 7) technology and a high-power tri-band design. With the addition of satellite units, you can easily expand your Mesh network to provide stable Wi-Fi coverage throughout your home. Whether for high-resolution media streaming, online gaming, remote work, or smart home applications, the Roamii BE Pro Mesh System delivers a high-speed, low-latency, and uninterrupted wireless experience, keeping you connected anytime and anywhere.

1.1 Appearance Description

Roamii routers feature a stylish triangular prism design, which can be placed upright on a deskor mounted on the wall ，

- **Router I/O Interface and Button Description:**
- **Sync Button** (Synchronization Button): Mesh System Expansion Synchronization Pairing, WPS Button
- **Reset Button**: Press and hold for 3 seconds to reset the device
- **USB 3.0 Port**: Connect external storage devices such as external hard drives, USB drives, etc.
- **2.5Gbps LAN Ports** (3 ports) : Connect to wired local devices and are backward compatible with 100 Mbps and 1 Gbps network equipment.
- **2.5Gbps WAN Port**: The primary external connection WAN port, connect to fiber optic modem, ISP network equipment.
- **Power (DCIN) Port**
- **LED Indicator**: Lights indicate the current router status.



- **LED Status:**

LED	Roamii Status
White solid	Roamii is operating normally.
White pulse	The connection between Roamii units is weak.
Blue solid	Roamii is starting up.
Blue pulse	Roamii is ready for setup.
Green solid	Roamii is pairing with mesh network.
Green pulse	Roamii units are connecting.
Orange pulse	Main Roamii: Not connected to the internet. Roamii node: Not connected to the main Roamii.

- **Specifications:**

AC to DC Power Adapter	DC Output: +12V Voltage, Max Current 3A		
Operating Temperature	0~40 °C	Storage Temperature	-30~70 °C
Operating Humidity	10~95 %	Storage Humidity	10~95 %

1.2 How to Place Your Roamii

To ensure optimal wireless signal transmission between the wireless router and connected network devices, please confirm the following points:

- It is recommended to place the router in a central area for optimal wireless signal coverage.
- Do not place the device near metal objects or in direct sunlight.
- Keep away from other 802.11g or 20MHz Wi-Fi devices, 2.4GHz computer wireless routers, bluetooth devices, cordless phones, transmitters, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators, and other industrial equipment to prevent signal interference or degradation.
- Please regularly update the firmware to the latest version. You can update via Web, APP, or visit the MSI official website https://www.msi.com/ to obtain the latest firmware.

1.3 System Requirements

Before setting up your network, you will need one or two computers that meet the following system requirements:

- One RJ-45 (LAN) Ethernet port (10Base-T/100Base-TX/1000BaseTX)

- Support 802.11a/b/g/n/ac/ax/be Wireless Function
- Installed TCP/IP Service
- Web browser, such as Internet Explorer, Firefox, Safari or Google Chrome

Note!

- If your computer does not have built-in wireless network adapter, you can install an IEEE 802.11a/b/g/n/ac/ax/be wireless network adapter to connect to the network.
- Roamii BE Pro Mesh System features tri-band technology, allowing your wireless router to simultaneously support 2.4 GHz, 5 GHz, and 6 GHz wireless signals. This technology enables you to use the 2.4 GHz band for everyday network tasks, such as web browsing or sending and receiving email, while using the 5 GHz and 6 GHz bands for real-time high-definition audio and video streaming.
- Some IEEE 802.11n devices may not support 5GHz bandwidth. Please refer to the device's user manual for specific specifications.
- The RJ-45 Ethernet cable length for connecting network devices cannot exceed 100 meters.

Important!

- Some wireless network adapters may experience connection issues when connecting to 802.11be Wi-Fi access points.
- If you encounter such issues, please ensure your drivers are updated to the latest version. Visit the manufacturer's official website to find software drivers, updates, and other related information.

2. Create Your Mesh Network

2.1 Connect your Roamii

(1) Using an ethernet cable, connect your modem (provided by your ISP or purchased separately) or fiber optic port to any Roamii router's "Internet" Port connection.

※ Ensure both the modem and router are connected to power.

(2) Connection methods can be divided into wireless connection and wired connection:

- Wireless Connection:
  - On your mobile device download the MSI Router 2.0 APP
  - Open the APP and scan the QR Code on the bottom of the device, and follow the instructions to complete the network setup process.
- Wired Connection:
  - Using an ethernet cable, connect your computer directly to any ethernet port on the router (LAN Port)
  - Open a web browser and manually enter https://msirouter.login to enter the Internet Setup Wizard.

2.2 The Internet Setup Wizard

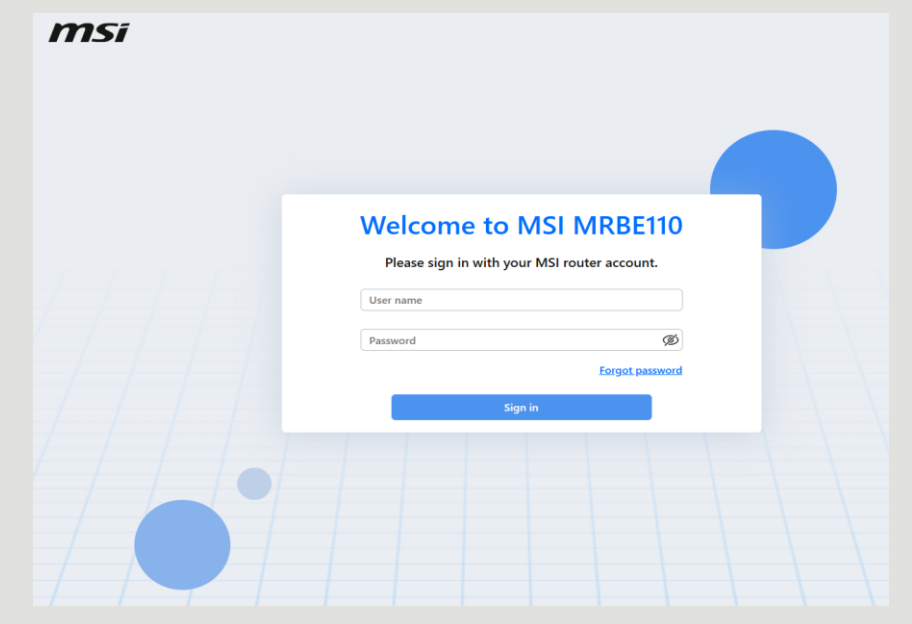
Will guide you through a quick network connection setup.

Note: Press the reset button can restore router to factory settings.

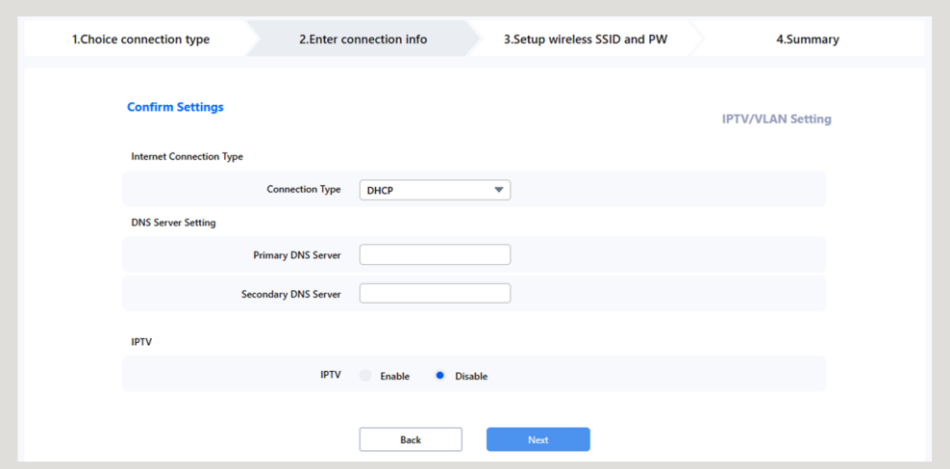
Please follow these steps to set up your network:

(1) Open a web browser and manually enter https://msirouter.login to access the login page.

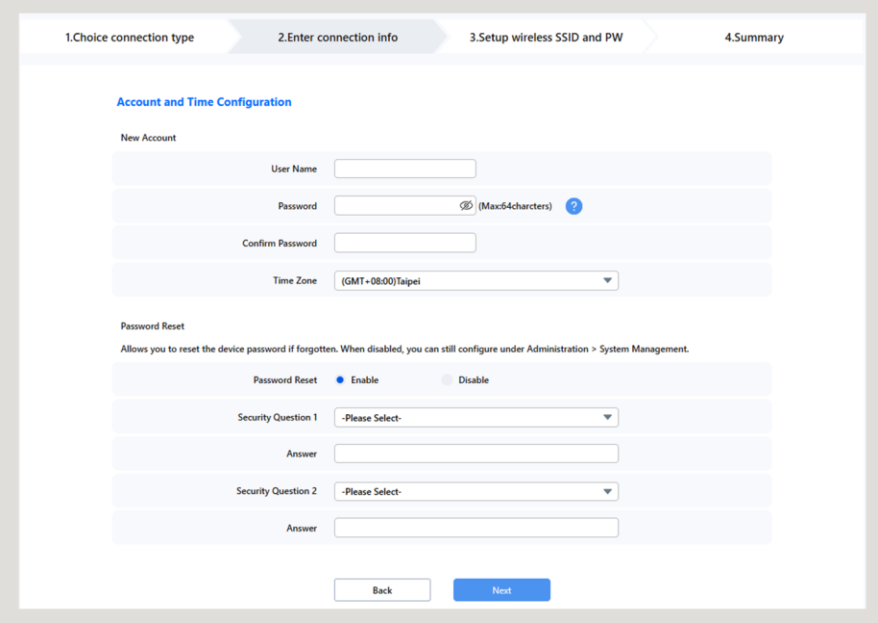
- Default Account: admin / Default Password: As indicated on the sticker on the bottom of the router



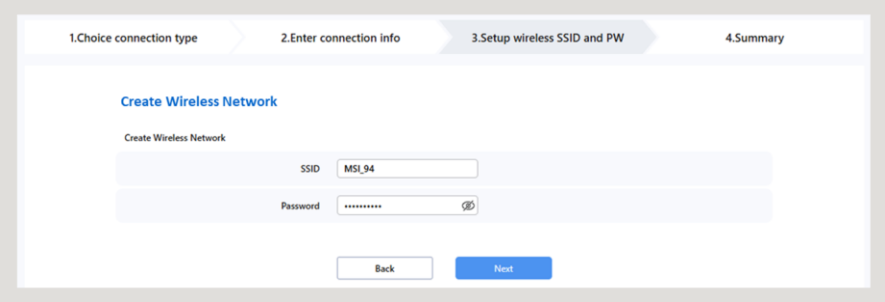
(2) The wireless router can automatically detect your ISP connection type (DHCP, PPPoE), please enter the username and password provided by your ISP (if required). If using Static IP, PPTP or L2TP, please manually enter the required information in the advanced settings. It also supports IPTV/VLAN settings.



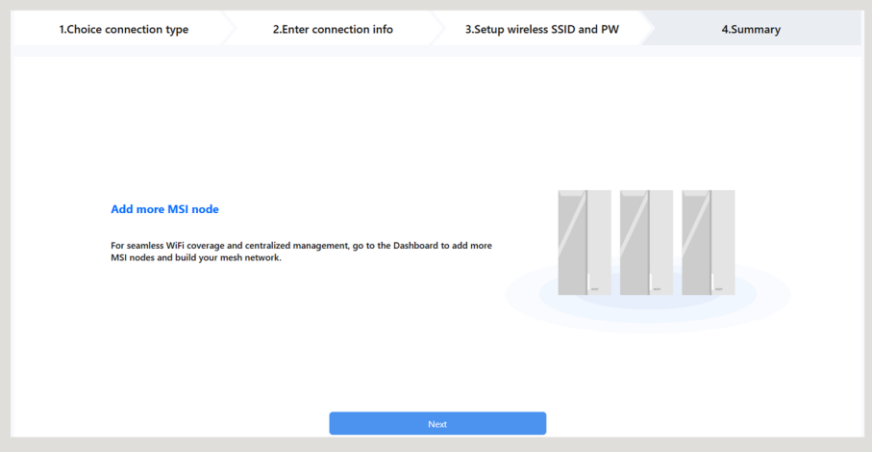
(3) Enter connection information, change the router's login password and set up security questions.



(4) Configure wireless connection, specify the network name (SSID) and security key



(5) Connect the satellite unit to power: The dual-pack combination will automatically pair to establish your home mesh network. If you purchased a satellite unit separately, please use the Sync button to add mesh nodes.



2.3 Connect to the Wireless Network

After completing router setup using the Internet Setup Wizard, your computer or other smart devices can connect to the wireless network.

Follow the steps below to connect to the network:

(1) Click the network icon  in the computer's notification area to display the list of available wireless networks.

(2) Select the wireless network you want to connect to (Default SSID:MSI_XX), then click **Connect**.

(3) If the wireless network is encrypted, enter the network security key, and then click **OK**.

(4) Wait until the computer successfully connects to the wireless network. Once the connection is established, the screen will display the connection status, and the network icon will indicate that the device is connected. 

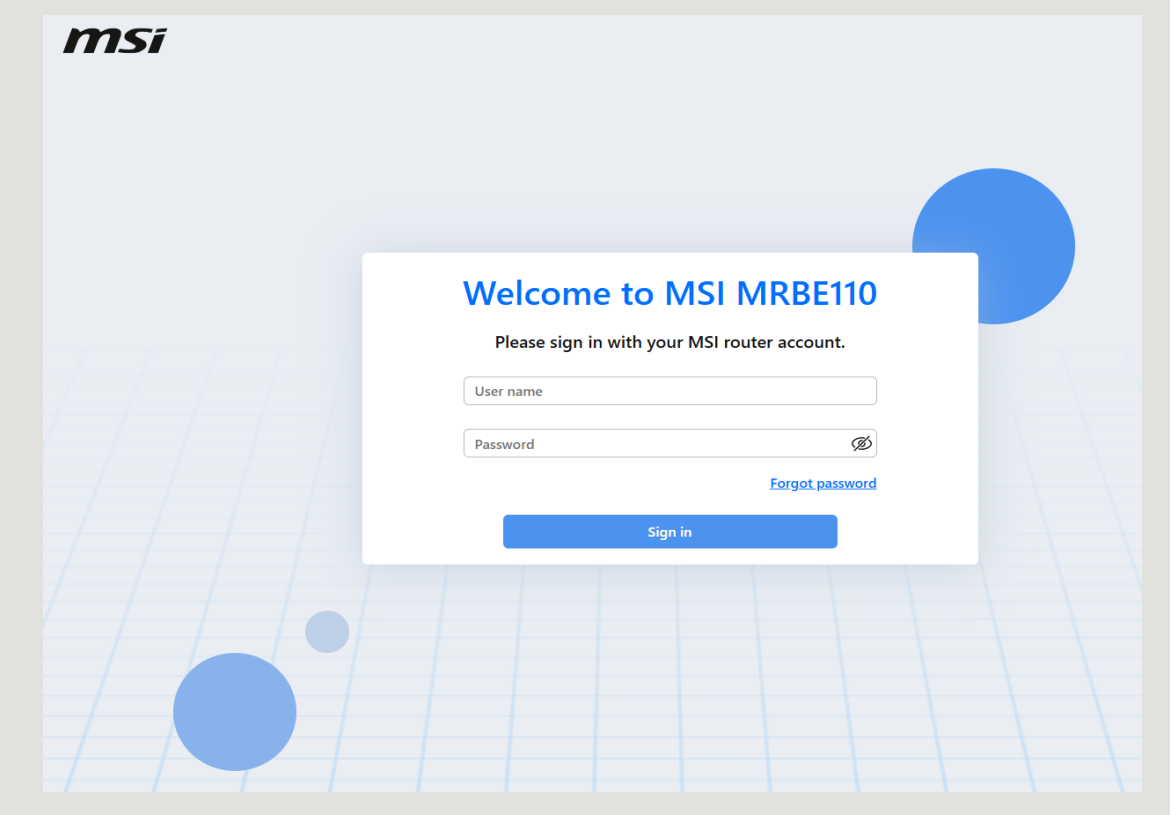
3. About the Web User Interface (Web GUI)

3.1 Login Web GUI

Log in to your wireless router's Web User Interface (Web GUI), allowing you to conveniently configure various router functions through a web browser, such as Internet Explorer, Firefox, Safari or Google Chrome, conveniently configure router functions.

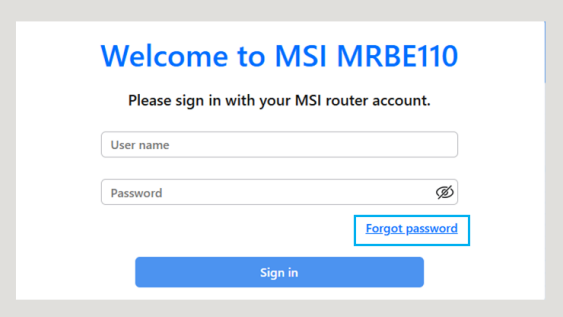
Please follow the steps below to log in to the Web User Interface (Web GUI):

(1) Make sure your device is successfully connected to the router’s network.
(2) Enter https://msirouter.login in the browser address bar.
(3) Enter username and password to log in. (The default login credentials are shown on the label at the bottom of the device, or may be based on the settings configured during the initial installation)
(4) If an incorrect username or password is entered five times, access will be temporarily locked for 5 minutes, and CAPTCHA verification will be enabled.
(5) You can use the Web GUI to configure various settings for the wireless router.



3.2 Forgot Password?

If you have forgotten your administrator login password and have enabled the "Forgot Password" function, you can reset the password by following steps:



(1) On the login page, click "**Forgot Password**"
   - The **Forgot Password** link is located below the input fields on the web login page.

(2) Enter the router's **S/N (serial number)**.
   - You can find the S/N on the label at the bottom of the router.
   - After entering the correct serial number, click "**Next**".

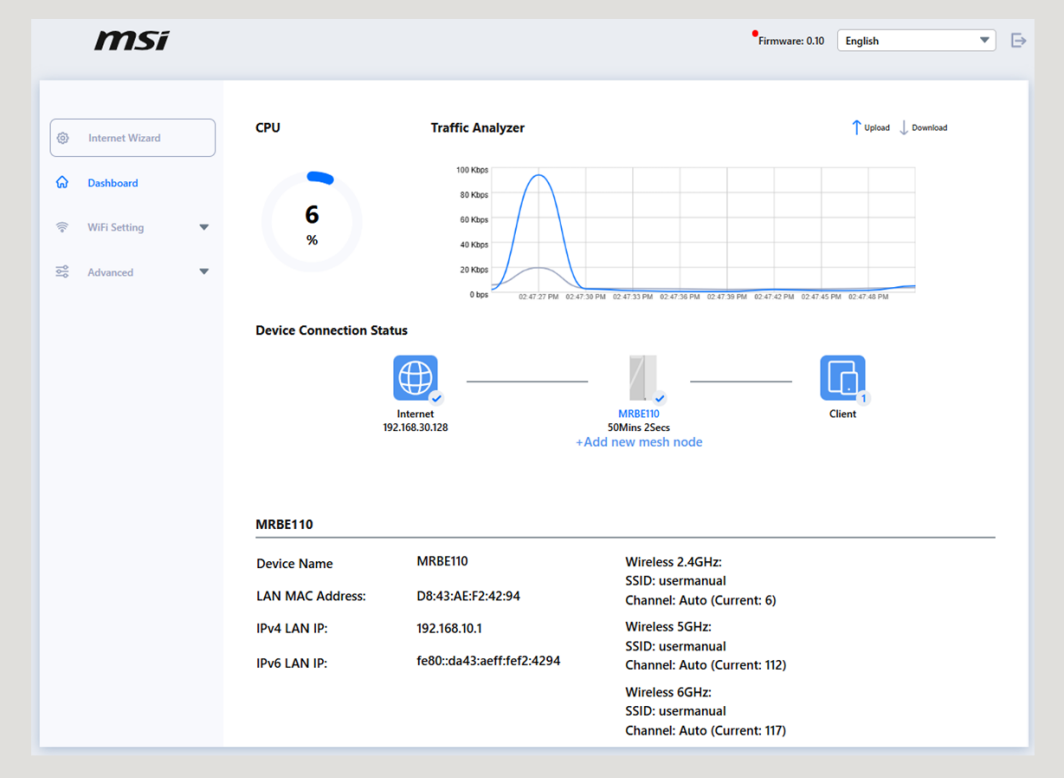
(3) The system will then display the two security questions you configured during the initial setup. Enter the correct answers to the corresponding questions.
   - If the answers are correct, you can proceed to the next step.

(4) Set and confirm your new password.

(5) After the process is complete, you can log in to the login page.

- It is recommended that you keep a secure record of your new password to avoid forgetting it again.
- You can then use the new password to log in through a computer or the app for management and configuration.

3.3 Web GUI Interface



- **Internet Wizard**

  Clicking **Internet Wizard** will enter the router's initial setup process.

Note: If this is your first time logging into the Web GUI, after opening the web browser, you will automatically enter the Internet Wizard.

- **Control Panel (Dashboard)**

  View the router's current operating status and detailed connection information, including:

  (1) **CPU Usage**: Displays the current CPU utilization as a percentage.

  (2) **Real-time traffic analysis**: Shows current upload/download traffic in real time.

  (3) **Connection status**:

  - **Internet**: Provides a direct view of key WAN connection details, including the current WAN connection type and public IP address. You can click **Connect** or **Disconnect** to manually disconnect or reconnect the Internet connection.

    ※ You can switch between IPv4/IPv6 to view connection details.

- **Main router Information**: Displays detailed LAN and wireless information for the main router. You can click **+ Add Mesh Node** to add a satellite device.
- **Node Information:** If satellite devices have been added, they will be displayed in the topology map.
- **Clients**: A list of all client devices currently connected to the router is displayed below. You can edit the device name and IP information as needed.

- **Firmware Version**: Displays the current firmware version. If a newer version is available, a red dot notification will appear.
- **Language List**: Supports multi-language selection, and can also be set to **Auto** (automatically detected based on the browser language).
- **Logout**: Ends the current login session and returns to the login page to ensure account security.
- **Function Settings List**
  - **WiFi Settings**: Configure basic wireless network settings and settings for specific network features.
  - **Advanced**: Configure advanced settings for Internet, IPTV & VLAN, FortiSecu, Firewall, QoS, USB, LAN, IPv6, VPN Server, VPN Client, Administration, Network Tools, and other related functions.

Note: Router features may vary depending on the firmware version.

4. Wi-Fi Settings

4.1 Wireless

To protect your wireless network from unauthorized access, you need to configure wireless network security settings.

4.1.1 Basic

- Enter the **Basic** wireless settings:

  (1) Click **WiFi Setting** > **Wireless** page

  (2) Click the **Basic** tab

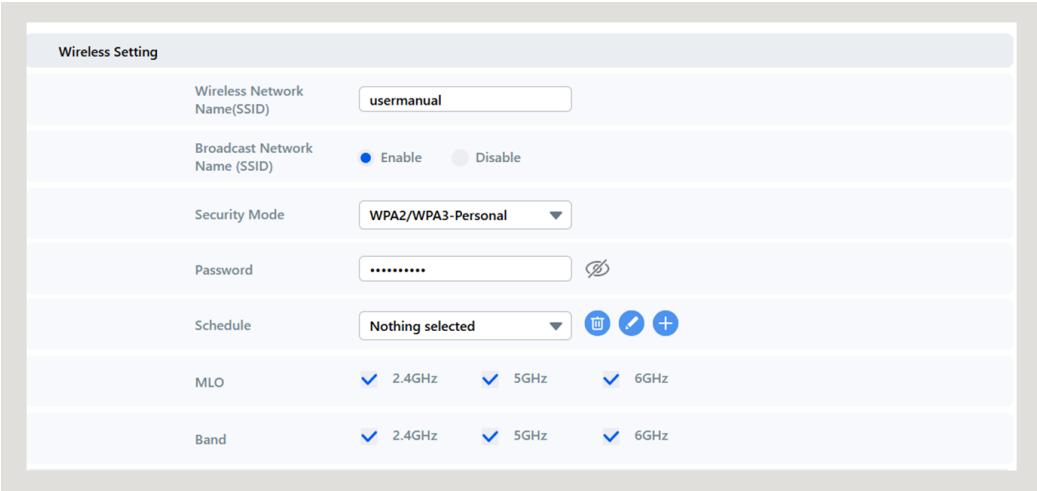
- Settings:

  (1) Wireless Setting
  - **Wireless Network Name (SSID)**: Sets the name of the wireless network for connection. Mesh models do not support separate SSID settings for individual frequency bands.
  - **Broadcast Network Name (SSID)**:

› If this option is disabled, the wireless network name will not be publicly displayed, and users must manually enter the SSID to connect.

- **Security Mode**: Selects the encryption standard. Supported options include Enhanced Open, WPA2/WPA3-Personal, WPA3-Personal, WPA2/WPA3-Enterprise, and WPA3-Enterprise.
- **Password**: Sets the password required to access the Wi-Fi network.
- **Schedule**: Allows you to define the time periods during which the wireless network is available.
- **MLO**: Enables simultaneous multi-band operation to improve transmission efficiency. To use MLO, you must select two or more enabled frequency bands.
  ※ Client devices must also support this feature
- **Band**: Select the desired frequency bands (2.4 GHz /5 GHz /6 GHz) to enable.

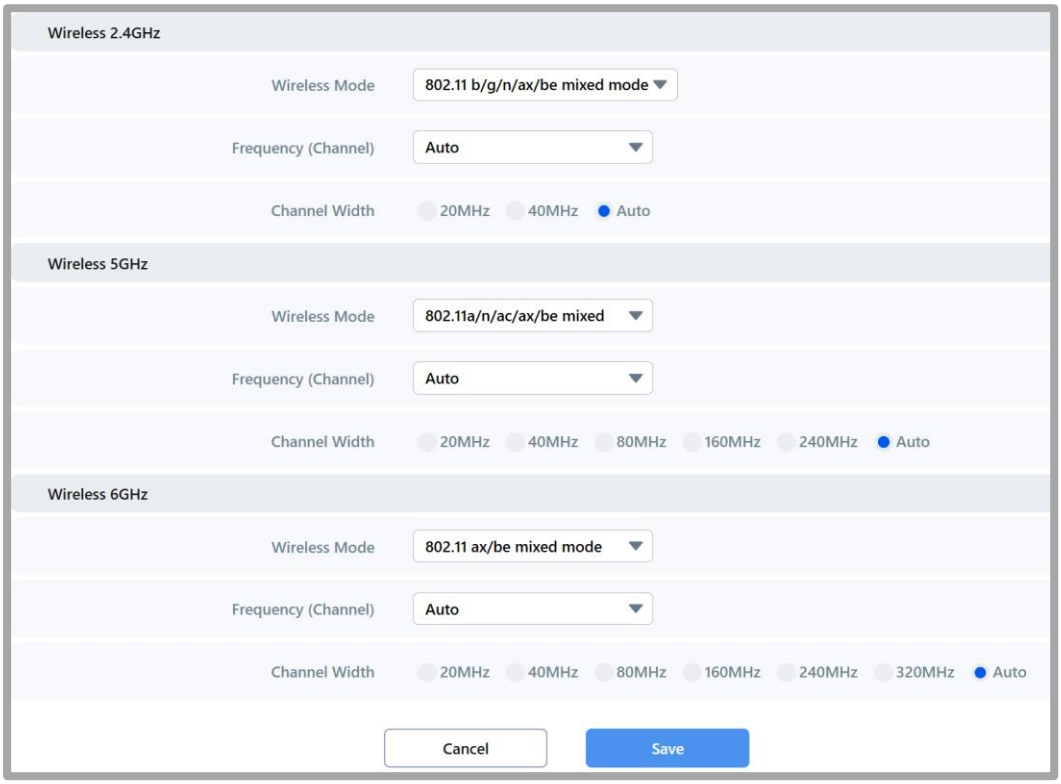
MLO allows Wi-Fi 7 devices to dynamically switch among the 2.4 GHz, 5 GHz, and 6 GHz bands, helping maintain connectivity even when you move out of the range of a higher-frequency band. MLO ensures that your device remains connected at the highest possible speed while maintaining a stable Wi-Fi connection.



(2) 2.4 GHz/5 GHz/6 GHz Band Settings

- **Wireless Mode**: Supports mixed mode operation.
- **Frequency (Channel)**: The default setting is Auto, which automatically avoids interference. You can also manually specify a channel to improve connection stability.
- **Channel Width**: Supports multiple bandwidth options and can adapt automatically based on the network environment.

※ Available channels and channel bandwidth options may vary depending on regional regulatory requirements.



4.1.2 Advanced Settings

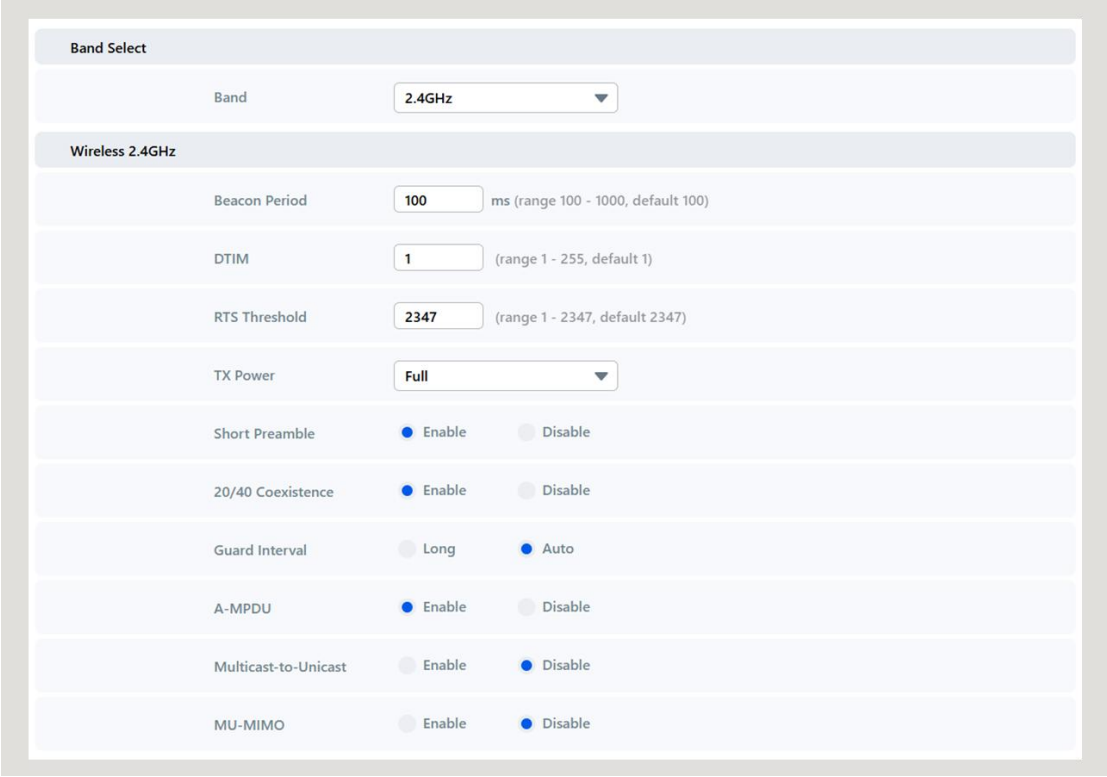
Advanced Wireless Settings allow you to fine-tune low-level wireless protocol parameters. It is recommended to keep the default settings unless you fully understand their functions and potential impact, as improper configuration may cause compatibility issues or reduce wireless performance and stability.

- Enter the wireless **Advanced Settings**:
  (1) Click **WiFi Setting** > **Wireless** page
  (2) Click **Advanced Settings** tab

- Settings:
  (1) **Band** Select: Select the band (2.4 GHz /5 GHz /6 GHz) for which to perform advanced settings.
  (2) Parameter Settings:
    - **Beacon Period**: Specifies how often the wireless access point broadcasts the SSID. A shorter interval allows devices to discover the network more quickly, but it may also increase system overhead.
    - **DTIM**: Specifies the interval for broadcast and multicast delivery notifications. This setting affects how often power-saving devices wake up to receive buffered data.

Lower values cause devices to wake more frequently and are better suited for real-time communication.

- **RTS Threshold**: Specifies the Request to Send (RTS) threshold used for packet collision avoidance. The default setting is the maximum value, which disables RTS.
- **TX Power**: Specifies the wireless transmission power. Reducing the transmission power can limit wireless coverage and help minimize interference.
- **Short Preamble** [Enabled / Disabled]: When enabled, shortens the packet preamble length to improve transmission efficiency.
- **20/40 Coexistence** [Enabled / Disabled]: Automatically detects whether 40 MHz bandwidth can be used in the current environment to help avoid interference.
- **Guard Interval**: Specifies the interval between symbols. Auto mode provides an optimized balance between stability and performance.
- **A-MPDU** [Enabled / Disabled]: Aggregates multiple packets for transmission to improve performance and throughput.
- **Multicast-to-Unicast** [Enable / Disable]: Converts multicast packets into unicast transmissions. Enabling this option can improve reliability and reduce latency in wireless environments.
- **MU-MIMO** [Enable / Disable]: Allows the router to transmit different data streams to multiple devices simultaneously, significantly improving multi-device efficiency in high-density environments.



4.1.3 WPS

WPS allows users to quickly add wireless devices to the router's wireless network without manual input Wi-Fi password.

Note:

- 6 GHz and WPA3 standard does not support WPS mechanism
- WPS function requires SSID broadcast function to be enabled

---

- Enter **WPS** settings:

  (1) Click **WiFi Setting** > **Wireless** page

  (2) Click **WPS** tab

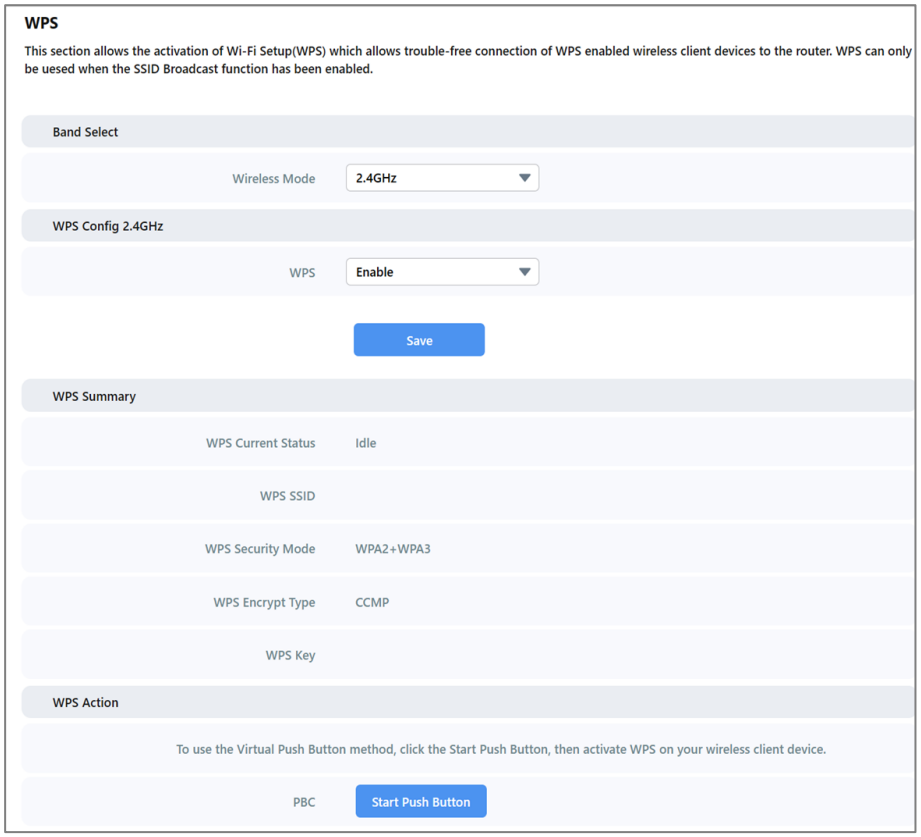
- Settings:

  (1) **Band Select:** Select the band for WPS configuration (2.4 GHz /5 GHz)

  (2) **WPS** [Enable / Disable] :
  - Enabling can activate WPS quick pairing mechanism

  (3) **WPS Summary**:
  - WPS Current Status: Whether the current WPS mode is on standby
  - WPS SSID: Corresponding wireless network name (SSID)
  - WPS Security Mode: Current network encryption mode
  - WPS Encrypt Type: Displays the encryption type used by WPS.
  - WPS key: Built-in security key

  (4) WPS Action:
  - **PBC**: Both devices press the WPS button simultaneously for pairing



4.1.4 MAC Filter

- MAC Filter allows you to control access for specific wireless devices based on their MAC addresses, helping enhance network security and improve traffic control accuracy.

- Enter **MAC Filter** settings:

  (1) Click **WiFi Setting** > **Wireless** page

  (2) Click **MAC Filter** tab

- Settings:

  (1) Basic Settings

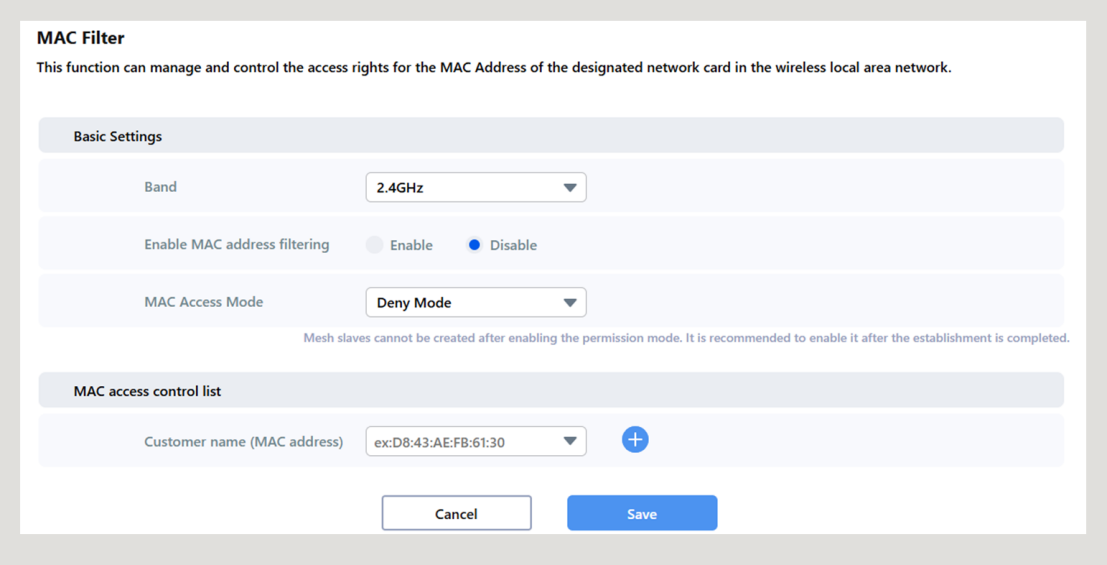
  - **Band** Selection: Select the band for MAC Filter configuration (2.4 GHz /5 GHz/6 GHz)
  - **Enable MAC Address Filtering**: Enable or disable this function.
  - **MAC Access Mode**:
    - **Allow Mode**: Only devices listed in the rule list are allowed to connect; all other devices will be denied. If you are using a Mesh network, it is recommended to enable Allow Mode only after completing the configuration to avoid connection issues.

- **Deny Mode**: Devices listed in the rule list are denied access, while all other devices can connect normally.

(2) MAC Access Control List

- **Device Name (MAC Address)**: Enter or select the MAC address of the device to which access control rules will be applied.
- Click "**+**" to add the device to the rule list

※The list can be modified by adding or deleting entries as needed.



4.1.5 Fast Roaming

Enabling this feature optimizes mobile devices (such as phones and laptops) when switching between different MSI mesh nodes through the 802.11r protocol, the system can significantly reduce the time for device re-authentication, achieving "seamless roaming".

- Enter **Fast Roaming** settings:

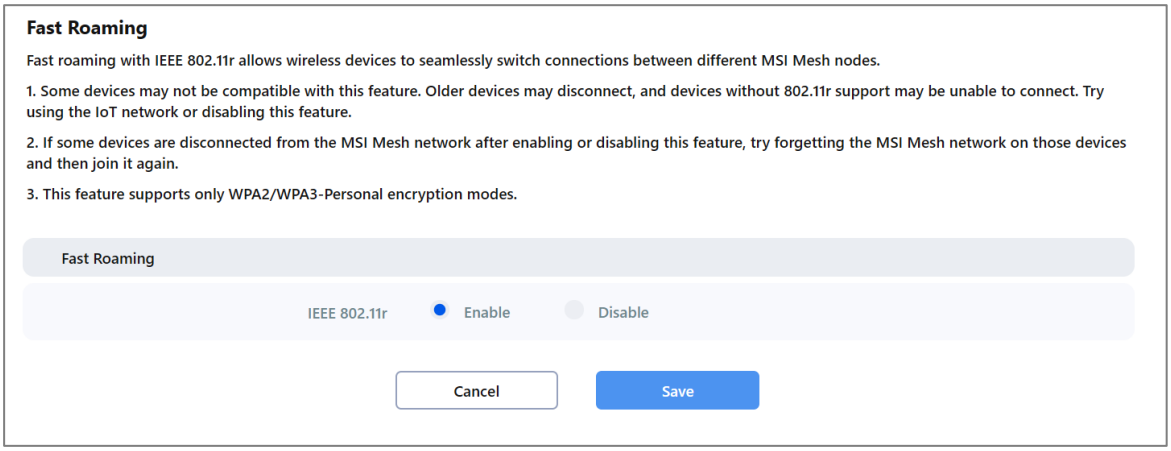
  (1) Click **WiFi Setting** > **Wireless** page

  (2) Click **Fast Roaming** tab

- Settings:

  Fast Roaming [Enable / Disable] the 802.11r protocol

  ※This feature supports only WPA2/WPA3-Personal encryption modes.



4.2 Guest Network

The Guest Network feature provides a separate wireless SSID for guests and short-term users. This network is isolated from your internal primary network to help protect the security and stability of your main network.

- Enter **Guest Network** settings:

  (1) Click **WiFi Setting** > **Guest Network** page

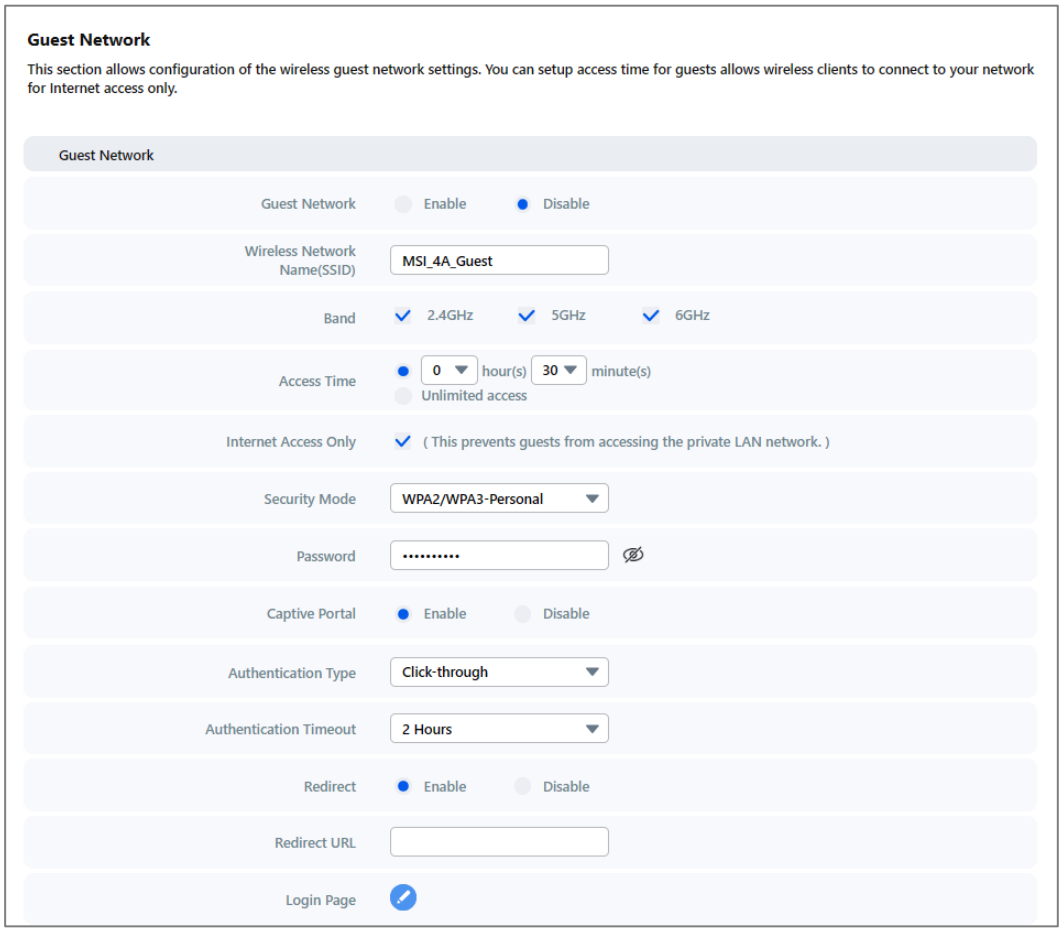
- Settings:

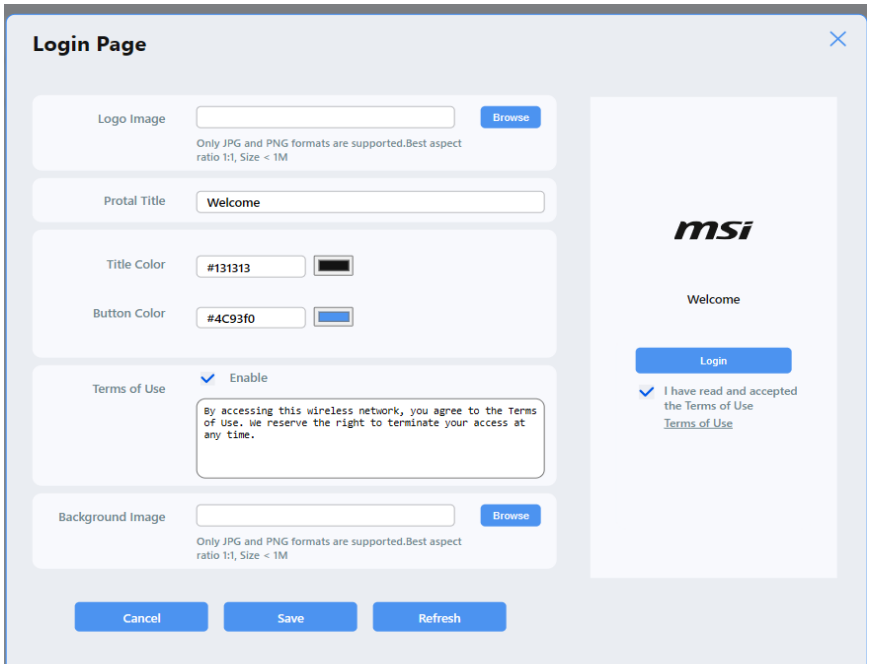
  (1) **Guest Network** [Enable / Disable] :

  - Enabling this feature opens a dedicated SSID for guest connections.

  - **Wireless Network Name (SSID)**: Sets the network name for guest connections.
  - **Band**: Select open band (2.4 GHz /5 GHz/6 GHz)
  - **Access Time**: Set the duration for which guest accounts can connect; the connection will automatically disconnect when the time expires.
  - **Internet Access Only**:
    - When checked, guests are prohibited from connecting to the internal private LAN network and are completely isolated from the main network.
  - **Security Mode**: Set the encryption mode for the guest Wi-Fi (Supports Open, Enhanced Open, WPA2/WPA3-Personal, WPA3-Personal, WPA2/WPA3-Enterprise, WPA3-Enterprise)
  - **Password**: Set the guest network password, which can be different from the main network password to ensure private network security.
  - **Captive Portal**: Requires users to provide additional verification or agree to terms and conditions before accessing the internet after connecting to Wi-Fi.

- When **enabled**, users will be redirected to a login page after connecting to Guest Wi-Fi.
- **Authentication Type**: Two authentication methods are available
  1. **Click-through**: Users simply click “Login” to access the internet; suitable for general home guests
  2. **Simple Password**: Users must enter the portal password to access the internet, providing higher access control.
- **Authentication Timeout**: Set the authentication validity period; after the time expires, users must re-authenticate to continue browsing.
- **Redirect**: When enabled, users will be automatically redirected to a specified webpage after logging in.
- **Redirect URL**: Enter the URL of the webpage you want to redirect to.
- **Login Page**: Click  to customize the appearance of the login page and the terms and conditions.





4.3 Child Network

This feature is designed to manage children's device network usage. Through an independent SSID and scheduling control, it helps parents manage children's internet access times and network security.

- Enter **Child Network** settings:

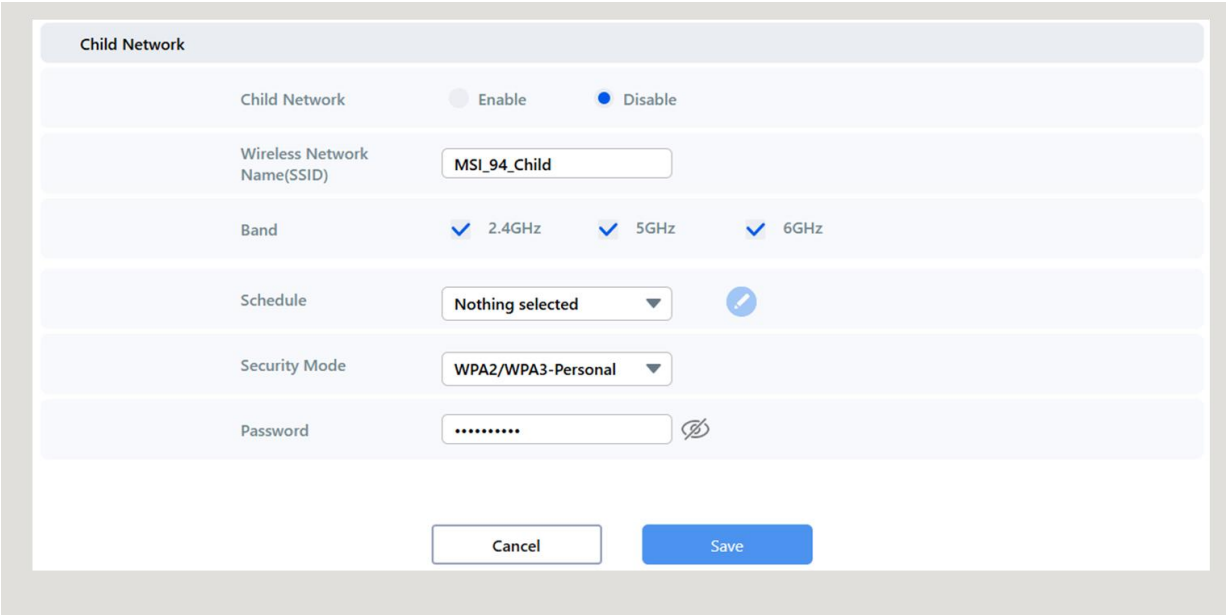
  (1) Click **WiFi Setting** > **Child Network** page

- Settings:

  (1) **Child Network** [Enable / Disable] :

  - After enabling, the Child Network SSID becomes active for children's devices to connect

  - **Wireless Network Name (SSID)**: Set the network name for children's connections
  - **Band**: Select open band (2.4 GHz /5 GHz/6 GHz).
  - **Schedule**: Setting a sleep time allows you to effectively manage your child's internet usage. Once the designated “sleep time” is reached, the internet connection will automatically disconnect.
  - **Security Mode**: Set the encryption mode for the child Wi-Fi (supports Open, Enhanced Open, WPA2/WPA3-Personal, WPA3-Personal, WPA2/WPA3-Enterprise, WPA3-Enterprise).
  - **Password**: Set the child network password, which can be set to a different password than the main network for increased control flexibility.



4.4 IOT Network

IOT Network Provides an independent and isolated dedicated wireless network for smart devices in your home, enhancing overall network security and stability.

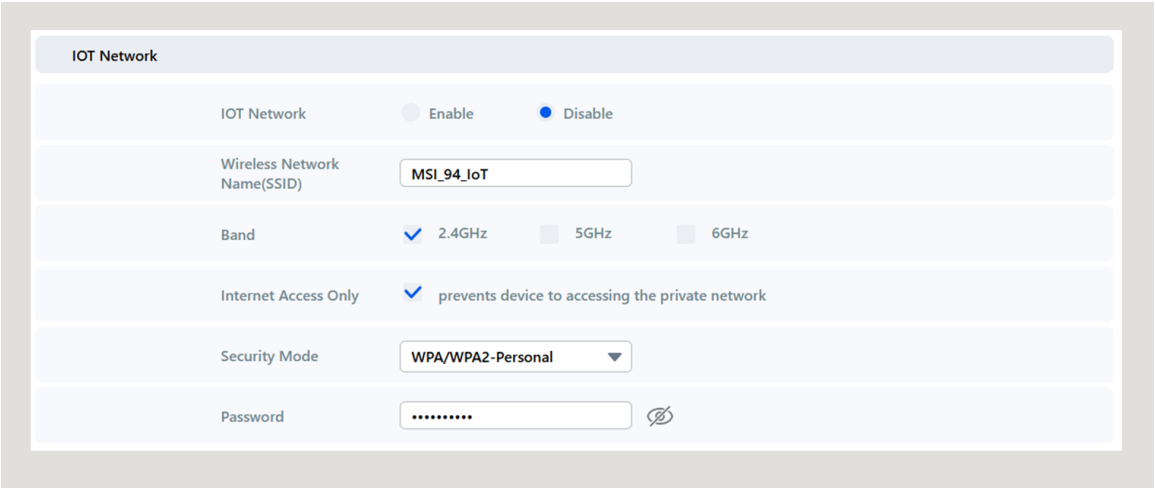
- Enter **IoT Network** settings:

  （1） Click WiFi Setting > **IOT Network** page

- Settings:

  （1） **IoT Network** [Enable / Disable] :

  - After enabling, create an independent IoT dedicated SSID
  - **wireless network name (SSID)**: Customize IoT network name
  - **Band**: Select open band (2.4 GHz /5 GHz/6 GHz), most IoT devices only support 2.4GHz.
  - **Internet Access Only**:
    - Restrict IoT devices to accessing only the external network to prevent them from scanning devices on the internal network after a breach
  - **Security Mode**: Set IoT Wi-Fi encryption mode (Supports on Open, Enhanced Open, WPA/WPA2, WPA2-Personal, WPA2/WPA3-Personal, WPA3-Personal, WPA2/WPA3-Enterprise, WPA3-Enterprise).
  - **Password**: Set a separate password to avoid sharing it with the main network, thereby enhancing the effectiveness of layered security.



5. Advanced

5.1 Internet

5.1.1 Internet

Internet allows you to configure the connection settings between your router and your Internet Service Provider (ISP), including the connection protocol, IP acquisition method, DNS, MTU, and MAC address settings.

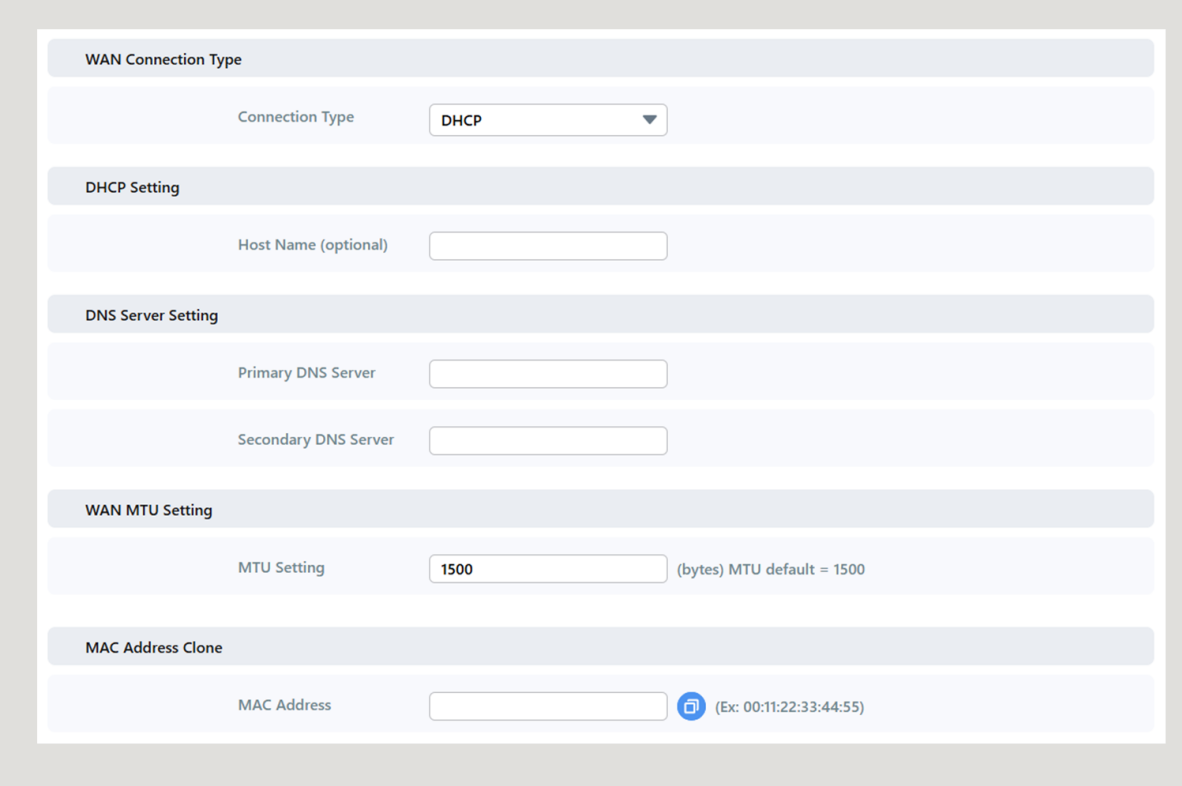
- Enter **Internet** settings:
  (1) Click **Advanced** > **Internet** page
  (2) Click **Internet** tab

- Settings:
  (1) **WAN Connection Type**: Supports DHCP, Static, PPPoE, PPTP, L2TP, etc. Please configure according to the connection protocol provided by your ISP.

  Notes: For most home ISP users, DHCP is used to automatically obtain settings.

  (2) Configure relevant parameters based on the connection type.
  (3) **DNS Server Setting**: Set a third-party DNS to speed up resolution or improve web filtering. ◦
  (4) **WAN MTU Setting**: Set the MTU (Maximum Transmission Unit), which is the maximum amount of data that can be transmitted in a single packet. An appropriate MTU setting helps maintain connection stability and transmission efficiency; if the setting is incorrect, it may prevent certain websites from loading properly, cause packet fragmentation, or affect network performance.

(5) **MAC Address Clone**: Copy the MAC address from your original computer to the router. You can either enter it manually or click “Paste” icon to use the MAC address of the current device's network adapter.



5.1.2 Port Trigger

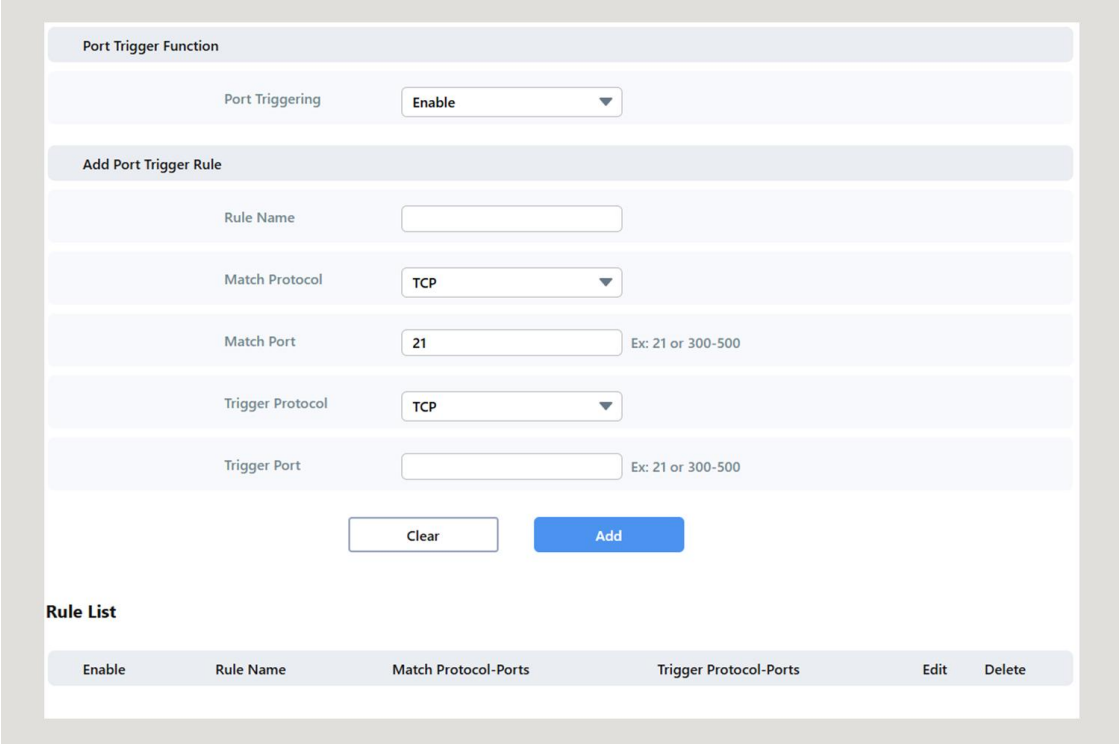
Port Trigger is a dynamic port forwarding mechanism that allows internal devices to automatically open the corresponding external ports for two-way communication when specific applications are launched. This feature is particularly well-suited for applications such as P2P, online gaming, VoIP, and video/audio streaming that require temporary port opening.

- Enter **Port Trigger** settings:
  (1) Click **Advanced** > **Internet** page
  (2) Click **Port Trigger** tab

- Settings:
  (1) **Port Trigger** [Enable / Disable]
    - Enables or disables the Port Trigger function.
  (2) Add Port Trigger Rule
    - **Rule Name:** Specifies the name of the rule.

- **Match Protocol:** Supports TCP, UDP, TCP+UDP, select the protocol type for triggering the connection based on application requirements.
- **Match Port:** Specifies the inbound port number or port range to be opened when the rule is triggered. e.g., 300–500.
- **Trigger Protocol:** The protocol type used by the outbound traffic that activates the rule.
- **Trigger Port:** Specifies the outbound port number or port range that triggers the opening of the corresponding inbound port. e.g., 300–500.

(3) Rule List: Rules can be “enabled,” “edited,” or “deleted” to adjust their content at any time.



5.1.3 Port Forwarding

Connection Port Forwarding allows traffic from the external Internet on a specific port to be forwarded to a designated device within the local network. Commonly used for internal servers providing services to the outside, such as: Web Server, FTP Server, NAS Access, IP monitors, etc.

- Enter **Port Forwarding** setting:

  (1) Click **Advanced** > **Internet** page

  (2) Click **Port Forwarding** tab

- Settings:

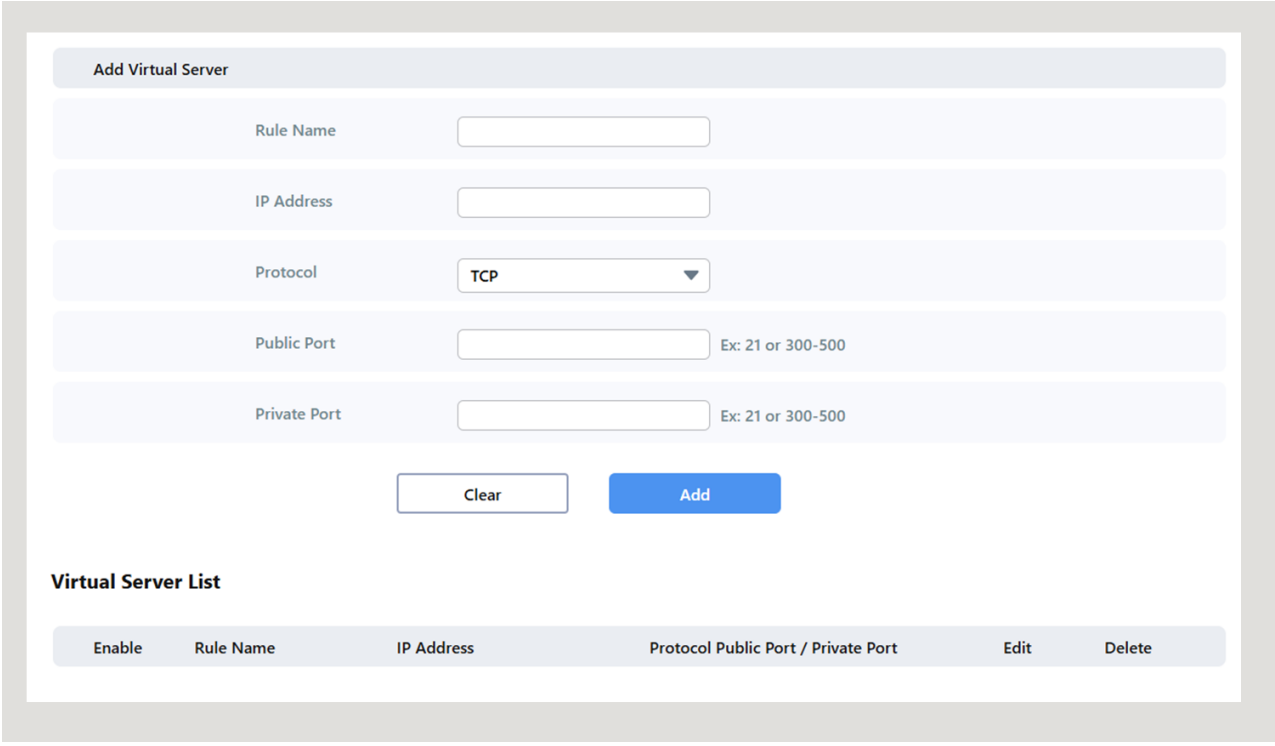
  (1) **Add Virtual Server** Rule:

- **Rule Name:** Specifies the name of the rule.
- **IP Address:** Specify the internal device that will receive the forwarded traffic IP
- **Protocol:** Select traffic protocol
- **Public Port:** The entry port number corresponding to external device connections, Supports single, multiple or continuous range settings, e.g.28, 29 或 100–200(Note: Continuous ranges cannot be mixed with other settings)
- **Private Port**: The actual port number forwarded to the internal device.Only supports single or continuous range settings, e.g.28 or 100-200(If set to a continuous range, Public Port must also correspond to a continuous range.)

(2) **Virtual Server List**: Can be "**enabled**," "**edited**," or "**deleted**" to adjust the content at any time.

Note:

- To ensure port forwarding works properly, please verify that the IP address configured on your internal device is a static address.
- To avoid unnecessarily exposing public ports, we recommend opening only the necessary service ports.
- If UPnP is enabled, some applications may automatically request ports; please be aware of potential conflicts.
- Exposing public ports increases security risks; we recommend using a firewall or VPN to enhance protection.



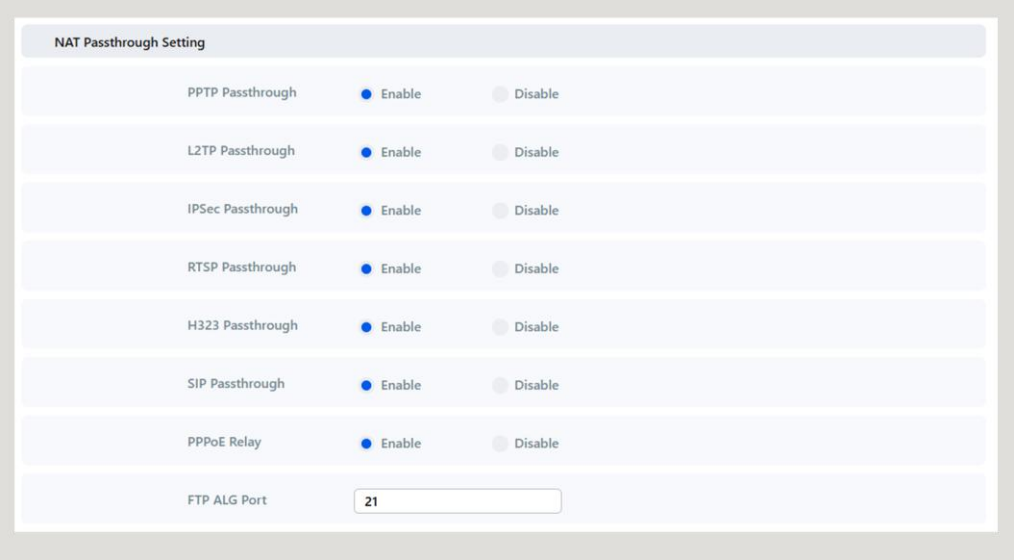
5.1.4 NAT Passthrough

NAT Passthrough allows specific VPN (such as IPsec, PPTP, L2TP) and application protocols to pass through the router's NAT so that client devices on the local network can use these services properly.

- Enter **NAT Passthrough** setting:
  (1) Click **Advanced** > **Internet** page
  (2) Click **NAT Passthrough** tab
- Settings:
  (1) **NAT Passthrough** Settings
    - **PPTP Passthrough** [Enable / Disable]: Point-to-Point Tunneling Protocol VPN traffic to pass through the router.
    - **L2TP Passthrough** [Enable / Disable]: Layer 2 Tunneling Protocol VPN traffic to pass through the router.
    - **IPSec Passthrough** [Enable / Disable]: IPSec VPN traffic to pass through the router.
    - **RTSP Passthrough** [Enable / Disable]: Real Time Streaming Protocol streaming traffic to pass through the router.
    - **H323 Passthrough** [Enable / Disable]: H.323 video conferencing and voice communication traffic to pass through the router.
    - **SIP Passthrough** [Enable / Disable]: Session Initiation Protocol VoIP traffic to pass through the router.
    - **PPPoE Relay** [Enable / Disable] : PPPoE packets to be relayed through the router.
    - **FTP ALG Port** : Specifies the port used by the FTP ALG function. In the current configuration.

Note:

- ALG feature automatically resolves packet reassembly and address translation issues in NAT environments; however, certain applications (such as those in double-NAT environments) may still require additional manual port forwarding.
- If using third-party VPN software encounters connection issues, you can first check whether the NAT Passthrough feature on this page has correctly enabled the corresponding protocol.



5.1.5 DMZ

DMZ (Demilitarized Zone) feature fully exposes specific devices on the internal network to the public internet. All external traffic that does not have explicitly configured port forwarding or firewall exceptions will be forwarded to the designated DMZ device. This feature is suitable for:

- ✓ Applications that require full external access (such as game consoles or test servers)
- ✓ When it is unclear which ports need to be opened for specific applications
- ✓ To temporarily bypass firewall and port forwarding rules and forward external traffic directly to a specified device

- Enter **DMZ** setting:

  (1) Click **Advanced** > **Internet** page

  (2) Click **DMZ** tab

- Settings:

  (1) **DMZ Settings** [Enable / Disable]

  › Effective after enabling DMZ forwarding function

  (2) **DMZ IP Address**: Enter the internal device you wish to use as the DMZ device's IP address (please ensure this device's IP is static).

Note:

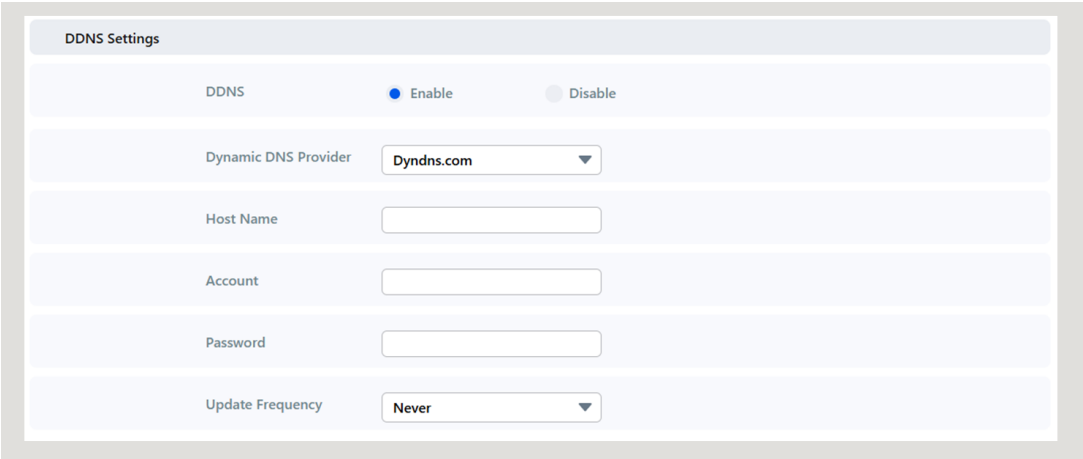
- Enabling DMZ fully exposes the specified device to the public network, which may potentially increase security risks. It is recommended to use this only in necessary scenarios and ensure the device has appropriate security measures.

5.1.6 DDNS

Setting up DDNS (Dynamic DNS) allows you to automatically associate a constantly changing public IP address with a fixed domain name, enabling users to conveniently connect to your home or office router, server, or various network services at any time using a single, consistent domain name.

- Navigate to DDNS settings:
  - (1) Click **Advanced** > **Internet** page
  - (2) Click **DDNS** tab

- Settings:
  - (1) DDNS Settings
    - **DDNS** [Enable / Disable]
      - Synchronize with selected provider after enabling IP
    - **Dynamic DNS Provider**: Supported third-party DDNS service providers
    - **Hostname**: Your registered DDNS domain name
    - **Account**: The account name registered with your DDNS provider
    - **Password**: The password or API key corresponding to the account
    - **Update Frequency**: Set how often the router should perform IP synchronization updates



5.2 IPTV&VLAN

Some ISPs (Internet Service Providers) or IPTV and VoIP services require client routers to support VLAN tagging. This feature allows routers to apply VLAN tags to traffic from different service types, ensuring compatibility and service stability.

- Enter **IPTV & VLAN** settings:

  (1) Click **Advanced** > **IPTV & VLAN** page

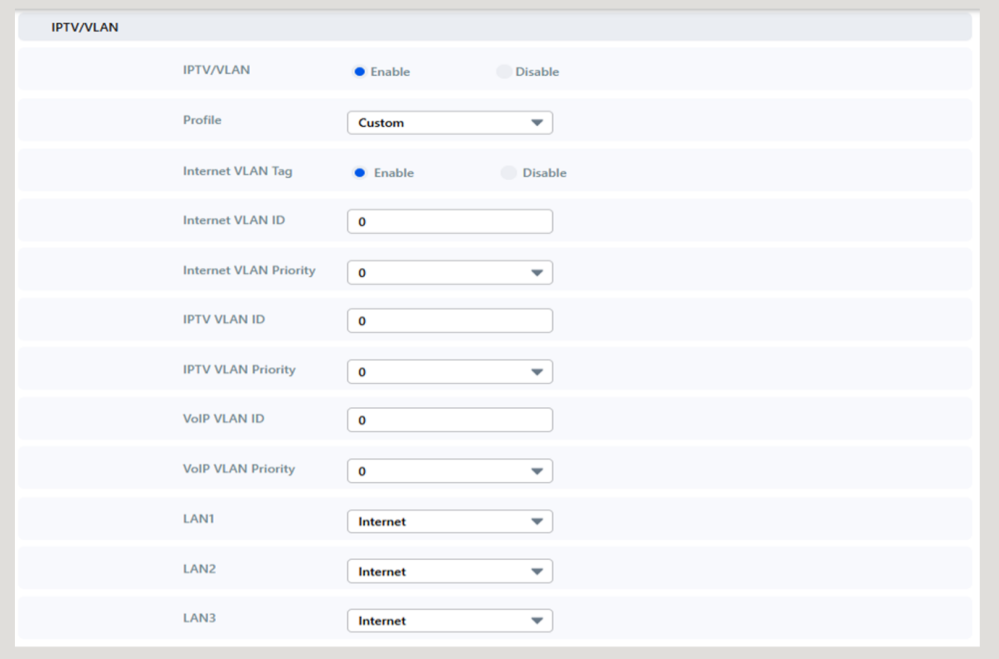
- Settings:

  (1) **IPTV/VLAN** [Enable / Disable]

  - Configuration available after enabling VLAN Setting and Service Routing

  - **Profile:** Select an ISP default profile, or configure with custom settings
  - **Internet VLAN Tag** [Enable / Disable]
    - After enabling Internet Connection Join VLAN Tag
  - **Internet VLAN ID:** Specify internet dedicated VLAN ID
  - **Internet VLAN Priority:** Set the priority for this traffic
  - **IPTV VLAN ID:** Configure IPTV Service VLAN ID
  - **IPTV VLAN Priority:** Configure IPTV Service traffic priority
  - **VoIP VLAN ID:** Configure VoIP Service VLAN ID
  - **VoIP VLAN Priority**: Configure VoIP Service traffic priority
  - **LAN1/LAN2/LAN3:** LAN Port Assignment

Note: When ISP requires a specific VLAN ID to successfully use its IPTV / VoIP services, enter the correct parameters according to its specifications.



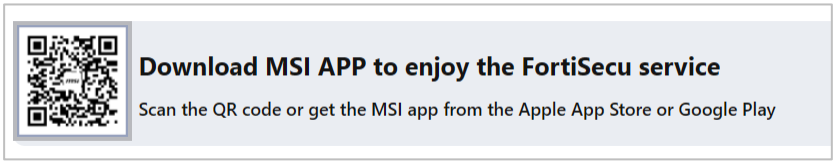
(2) Multicast

- **IGMP Proxy** [Enable / Disable]
  - When enabled, the router can coordinate internal LAN devices to subscribe to IPTV multicast streams.
- **IGMP Snooping** [Enable / Disable]
  - Allows the switch to precisely monitor each device's subscription behavior to multicast groups, effectively reducing network broadcast load.
- **IGMP Version**: Configure according to ISP requirements (V3 is typically used).
- **Wireless Multicast Forwarding** [Enable / Disable]
  - Controls whether multicast traffic is forwarded over the wireless network to connected wireless clients.

5.3 FortiSecu

MSI FortiSecu to shield your smart home and connected devices from security threats.

- Download the MSI Router 2.0 app from the Google Play Store or the App Store to enjoy this service.



5.4 Firewall

5.4.1 General

This feature provides basic network security protection. By enabling SPI firewall and DOS attack protection, it safeguards your router and internal network devices from common network attack threats.

- Enter Firewall「**General**」Settings:

  (1) Click **Advanced** > **Firewall** page

  (2) Click **General** tab

- Settings:

  (1) **SPI Firewall** [Enable / Disable]

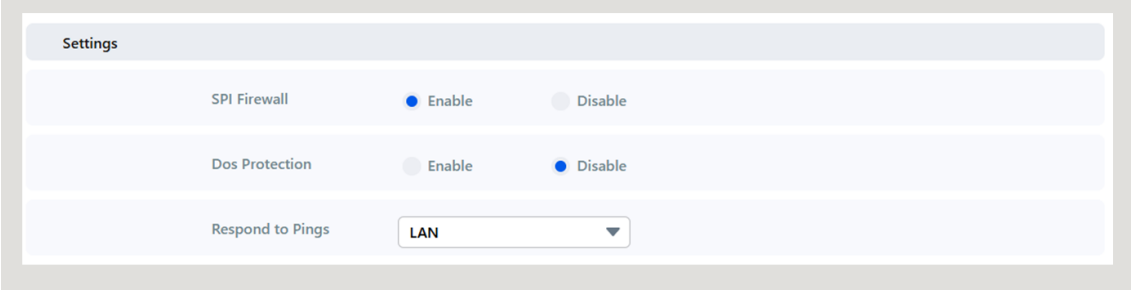
  - Enabled by default, the firewall checks the state and connection association of incoming and outgoing packets, allowing only legitimate session data packets to enter and exit the network.
  - It effectively prevents unauthorized intrusion connections and ensures network security.

  (2) **Dos Protection** [Enable / Disable]

  - When enabled, it effectively defends against common denial-of-service attacks.
  - It prevents hackers from flooding your network with a large number of connection packets and bringing your services to a standstill.

  (3) **Respond to Pings**

  - **WAN/LAN**: Allows Ping requests from both the WAN (external network) and the LAN (internal network).
  - **WAN**: Allows Ping requests from the WAN (external network).
  - **LAN**: Allows Ping requests only from the LAN (internal network).
  - **Disable**: Does not respond to any Ping packets, enhancing stealth and security.



5.4.2 Access Control

The access control feature allows you to set access blocking rules for specific user devices on local area networks (LANs) and wireless networks. It enables precise blocking based on a device's IP address and protocol type, enhancing network security and management flexibility.

- Enter **Access Control** settings:

  (1) Click **Advanced** > **Firewall** page

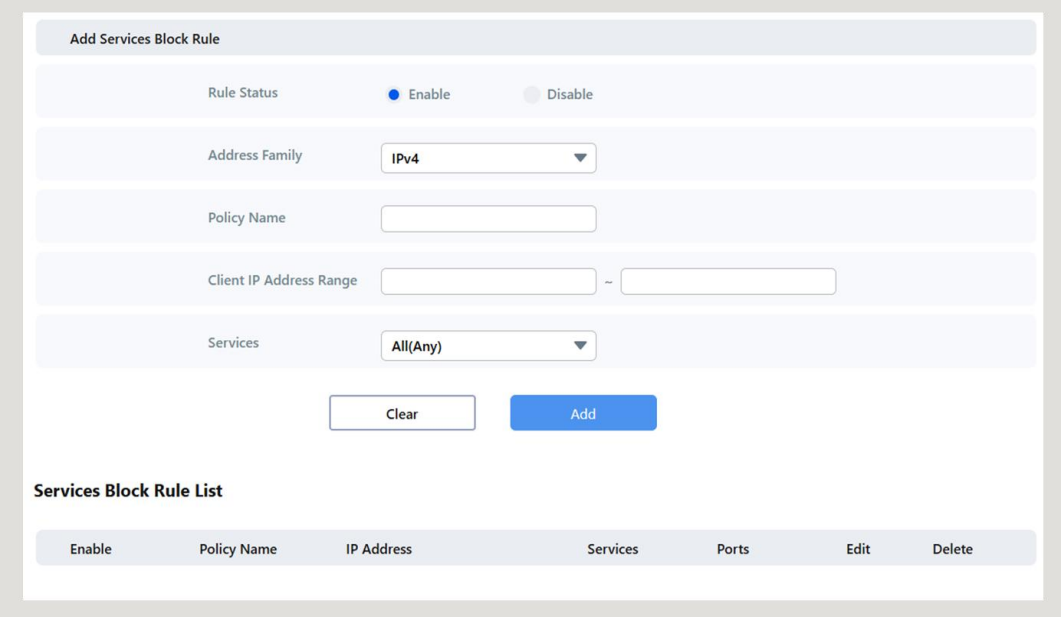
(2) Click **Access Control** tab

- Settings:

(1) Add Services Block Rule

- **Rule Status**: [Enable / Disable]
  - After checking "Enable", the rule takes effect.
- **Address Family**: Select IP protocol type; supports IPv4 and IPv6
- **Policy Name**: Enter a custom name for the rule.
- **Client IP Address Range**: Enter the internal device IP address range to be controlled.
- **Service**: Select the type of application service to block.

(2) Services Block Rule List: Rules can be "Edited" and "Deleted" to adjust content at any time.



5.4.3 Inbound Filter

The Inbound Filter function is used to control connection requests from the external network. It can allow or deny access for specific source IP addresses, thereby limiting external hostsfrom accessing internal services (such as virtual servers or games) and enhancing network security.

- Enter **Inbound Filter** settings:

(1) Click **Advanced** > **Firewall** page

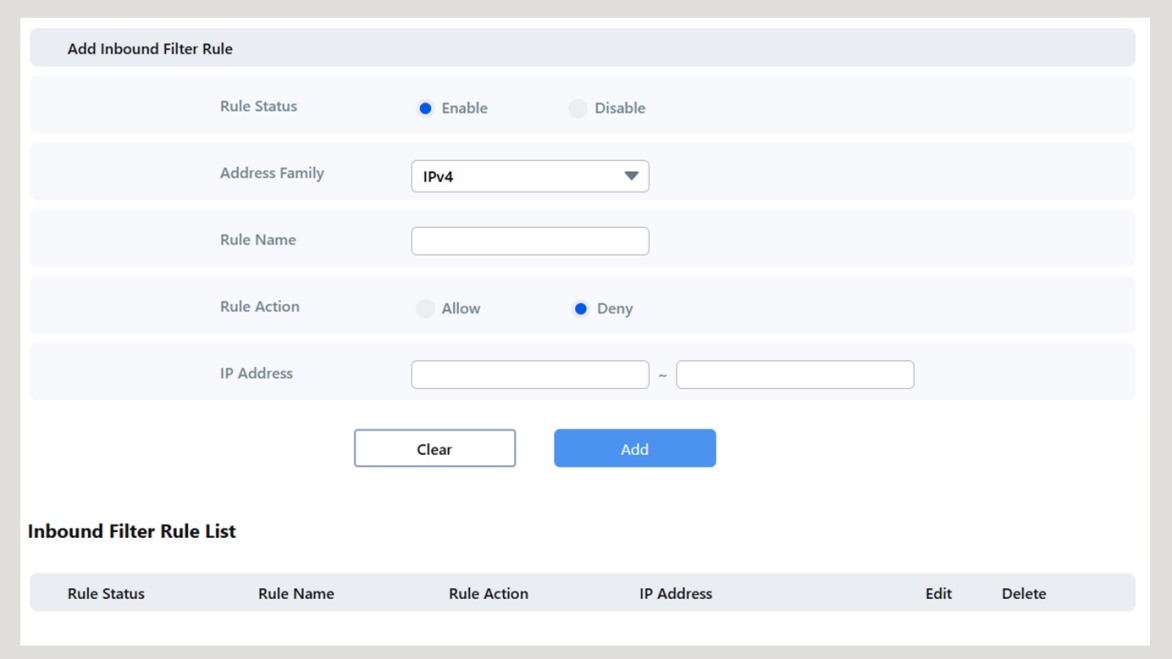
(2) Click **Inbound Filter** tab

- Settings:

(1) Add Inbound Filter Rule

- **Rule Status**: [Enable / Disable]
  - After checking "Enable", the rule takes effect.
- **Address Family**: Select IP protocol type; supports IPv4 and IPv6.
- **Rule Name**: Enter a custom name for the rule.
- **Rule Action**: Select “Allow” or “Deny” access for specific source IP addresses.
- **IP Address**: Enter the internal device IP address range to be controlled.

(2) Inbound Filter Rule List: Rules can be "**Edited**" and "**Deleted**" to adjust content at any time.



5.4.4 URL Filter

Using the “URL Filter,” you can restrict users' access to specific websites, ensuring online safety, improving work focus, or helping parents monitor their children's internet usage.

- Enter **URL Filter** settings:

  (1) Click **Advanced** > **Firewall** page

  (2) Click **URL Filter** tab

- Settings:

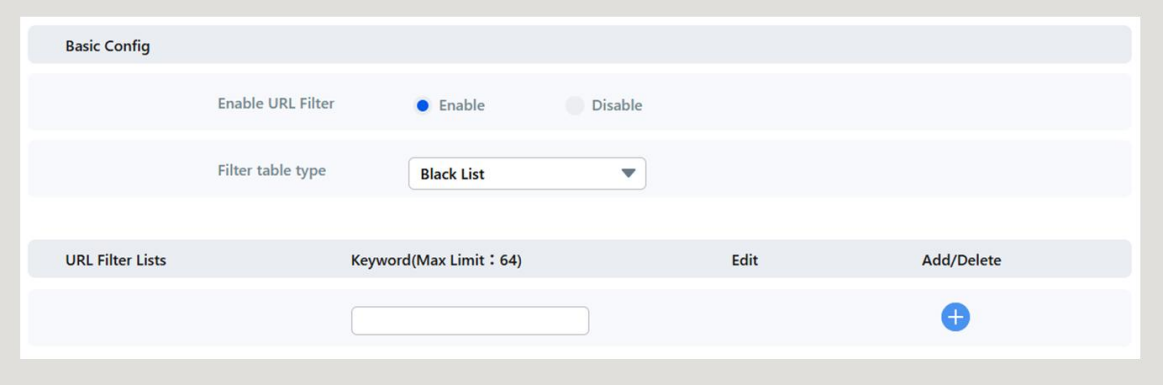
  (1) **Basic Config**

  - **Enable URL Filter** [Enable / Disable]
  - **Filter Table Type:**

- **Blacklist**: Block the URLs listed in the list; all other websites are allowed to pass through normally.
- **Whitelist**: Only allow the URLs listed in the list; all other websites are blocked.

(2) URL Filter List Settings:

- **Keyword**: Enter the keywords for the URLs you want to block or allow.
  - When you enter a keyword such as “youtube.com,” the system will filter and manage all subdomains of that website, such as music.youtube.com and kids.youtube.com
    ※Maximum 64 rules
- Rules can be "**Edited**" and "**Added/Deleted**" to adjust content at any time.



5.4.5 UPnP

UPnP (Universal Plug and Play) allows devices on a local area network to automatically request and open the necessary ports on the router. Since NAT blocks external connections, UPnP eliminates the complexity of manually configuring port forwarding, enabling applications that require external connections to function properly. This feature is suitable for the following scenarios:

- ✓ Multiplayer Online Game
- ✓ Real-time voice calls / Video Conferencing
- ✓ P2P Download Applications
- ✓ Remote Access and Device Control

- Enter **UPnP** settings:

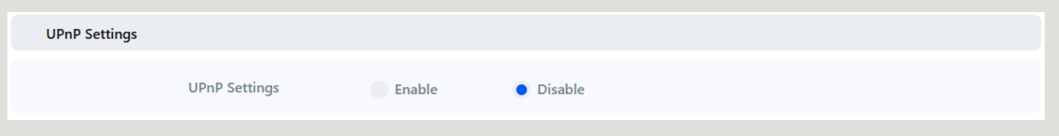
  (1) Click **Advanced** > **Firewall** page

  (2) Click **UPnP** tab

- Settings:

  (1) **UPnP Settings** [Enable / Disable]

- **Enable**: Allows internal devices on the local network to automatically request and open the required corresponding ports on the router, facilitating NAT traversal and real-time communication.
- **Disable**: Completely prohibit automatic port opening, only specific services may be enabled through manually configured port forwarding.



Note:
Enabling UPnP allows internal devices to automatically open ports, which may increase the risk of network exposure. We recommend using this feature only in trusted network environments and ensuring that internal devices have appropriate security measures in place.

5.5 QoS

5.5.1 Traditional QoS

The “Traditional QoS” feature allows you to customize bandwidth allocation and traffic prioritization, ensuring that critical applications or devices receive stable and sufficient bandwidth resources on both wired and wireless networks, thereby enhancing the overall network experience and quality of service.

※ Traditional QoS is statically allocated; users need to set appropriate proportions themselves.

- Enter **Traditional QoS** settings:
  (1) Click **Advanced** > **QoS** page
  (2) Click **Traditional QoS** tab

- Settings:
  (1) Basic Config
    - **Enable Traditional QoS** [Enable / Disable]**:**
      - After enabling, QoS traffic management takes effect.
    - **Upload bandwidth / Download bandwidth:** Enter the network bandwidth values (Mb/s).

      ※ We recommend first checking the data provided by your ISP or visiting https://www.speedtest.net/ to run a speed test and obtain accurate values.

      ※ When entering the total bandwidth value, it is recommended to set it slightly below the actual speed provided by your ISP to allow for packet control buffering.

- **Bandwidth reservation priority settings**: Set the percentage of reserved bandwidth allocated to each priority level (Highest/High/Medium/Low).

※ The values will be automatically calculated and allocated based on the total bandwidth you enter.

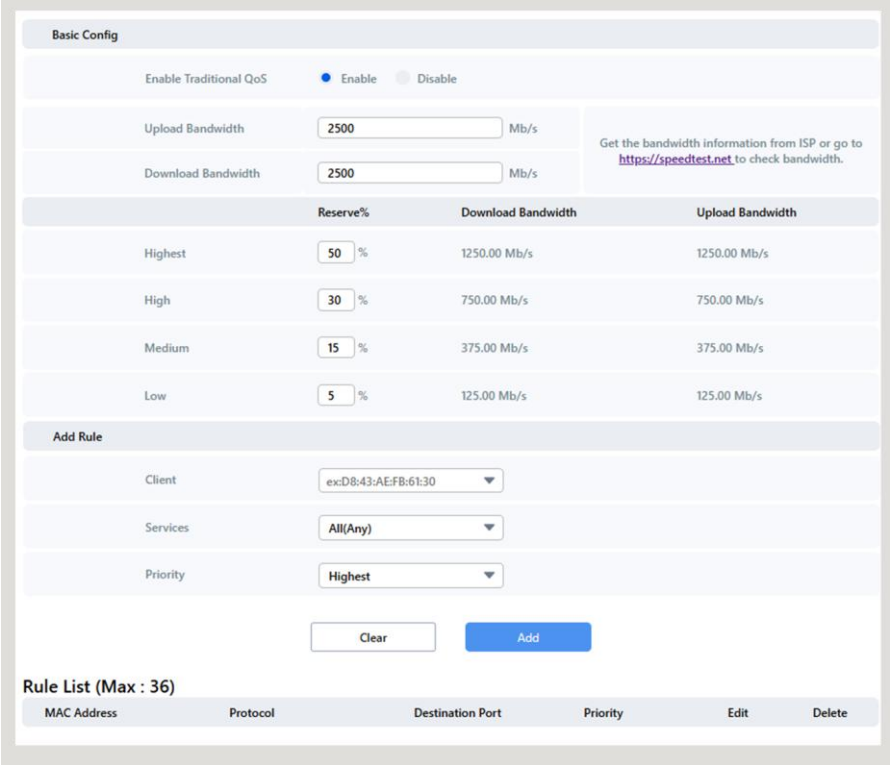
※ The system will prioritize high-priority services during traffic congestion.

(2) Add Rule: Define priority rules for specific devices and services.

- **Client**: Select from currently connected devices (Identification by MAC address)
- **Services**: Select service type
- **Priority**: Highest/High/Medium/Low

(3) Rule List: Supports up to 36 QoS Rules

- For each rule added, the device/service will obtain corresponding bandwidth guarantees based on the set priority when the network is busy.
- Rules can be “edited,” or “deleted” to adjust their content at any time.



5.5.2 Bandwidth Limiter

The “Bandwidth Limiter” feature allows you to set download and upload bandwidth limits for specific devices, preventing individual devices from consuming excessive network resources and ensuring fair usage and stability across the entire network.

- Enter **Bandwidth Limiter** settings:

(1) Click **Advanced** > **QoS** page

(2) Click **Bandwidth Limiter** tab

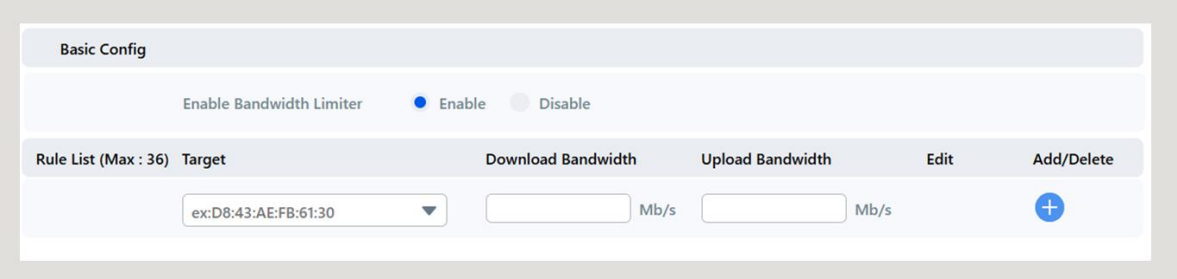
- Settings:

(1) **Enable Bandwidth Limiter** [Enable / Disable]

› After enabling, the bandwidth limit rules for the specified device will take effect.

(2) Rule List: Supports up to 36 Bandwidth Limiter Rules

- **Target**: Select the device to set bandwidth limits for from the current connection list. (By Device MAC Address)
- **Download/Upload Bandwidth**: Limit the maximum download rate (Mb/s) for this device.
- Click "**+**" to add to the rule list.
- Rules can be **Edited** and **Add/Delete** to adjust the limit content at any time.



5.6 USB

5.6.1 File Sharing Server

Through the DLNA protocol, the router can share multimedia files, such as videos, music, and photos, stored on a USB storage device with DLNA-compatible playback devices, such as smart TVs, set-top boxes, and media players, enabling home streaming applications.

- Enter **File Sharing Server** settings:

(1) Click **Advanced** > **USB** page

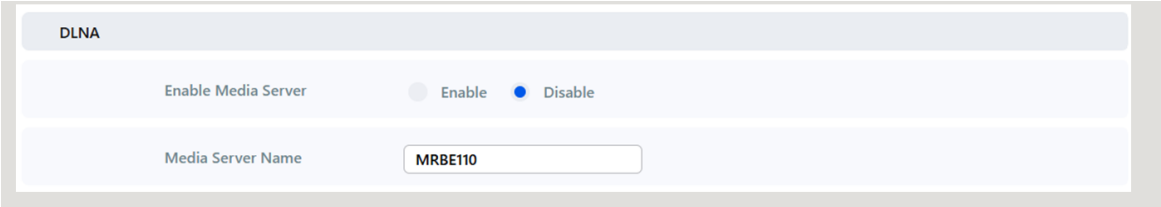
(2) Click **File Sharing Server** tab

- Settings:

(1) **Enable Media Server** [Enable / Disable]

› When enabled, the DLNA media server automatically searches for and shares supported multimedia files on the USB storage device for real-time streaming by other DLNA devices on the LAN.

- **Media Server Name**: Customize the server name displayed on other DLNA playback devices.



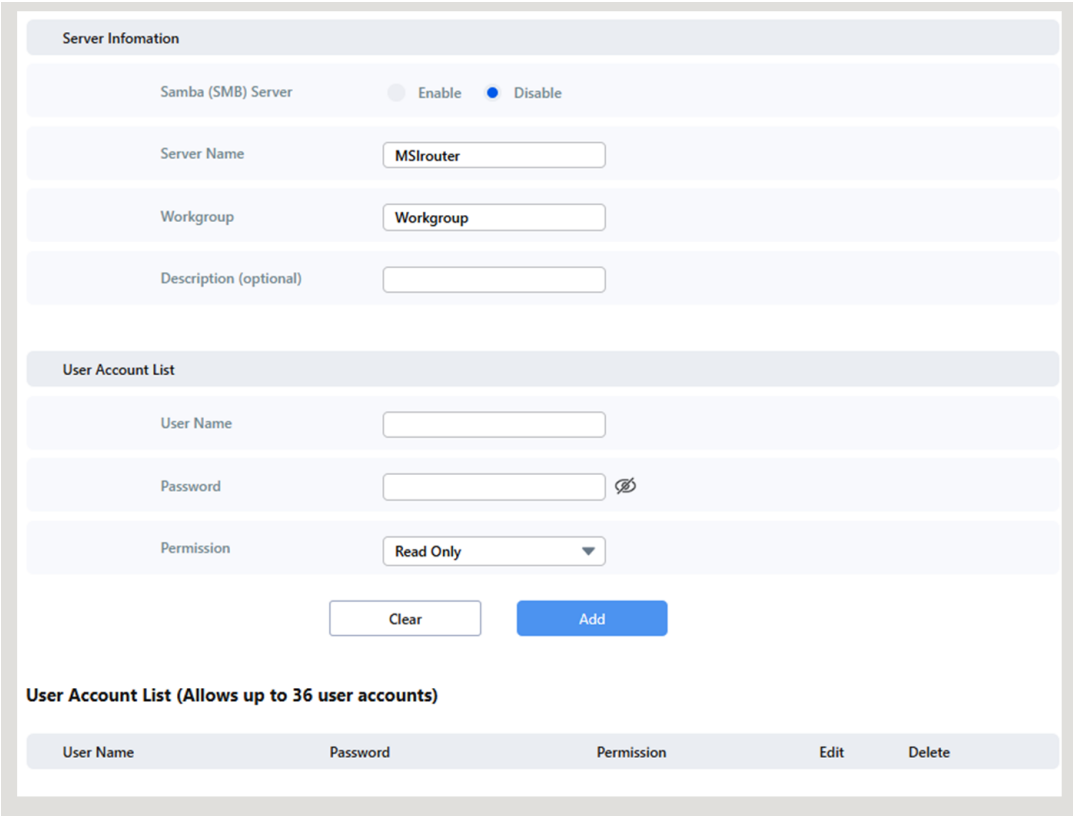
5.6.2 Samba Server

Samba (SMB) is a network protocol that allows shared files to be accessed over a network. You can share the storage device connected to the router USB port with other devices at home or in the office through the LAN.

- Enter **Samba Server** settings:
  (1) Click **Advanced** > **USB** page
  (2) Click the **Samba Server** tab

- Settings:
  (1) **Samba (SMB) Server** [Enable / Disable]
    - When enabled, the Samba server starts and allows internal network devices to access the USB storage device through the SMB protocol.
  - **Server Name**: Customize the server name displayed on the LAN.
  - **Workgroup**: The workgroup name on the LAN.
  - **Description (Optional)** : Enter remarks for easier management.

  (2) User Accounts List (Up to 36 user accounts are supported)
  - **Username**: Customize the account name.
  - **Password**: Password required to log in to the Samba (SMB) server.
  - **Permission**: Sets the access permission for this account (read/write permission).
  - **Edit**: Edit or remove existing accounts at any time.



5.6.3 FTP Server

The router USB port supports external storage devices, such as USB flash drives or hard drives. With the built-in FTP server function, you can:

- ✓ Access files on the USB storage device from the local area network (LAN) or through the Internet (WAN).
- ✓ Upload, download, and share files.
- ✓ Allow family members or remote users to access file resources conveniently.

Note: Enable the remote access option to access FTP from the Internet.

- Enter **FTP Server** Settings:
  - (1) Click **Advanced** > **USB** page
  - (2) Click the **FTP Server** tab

  ※ Make sure a USB flash drive or external hard drive is connected to the router USB port.

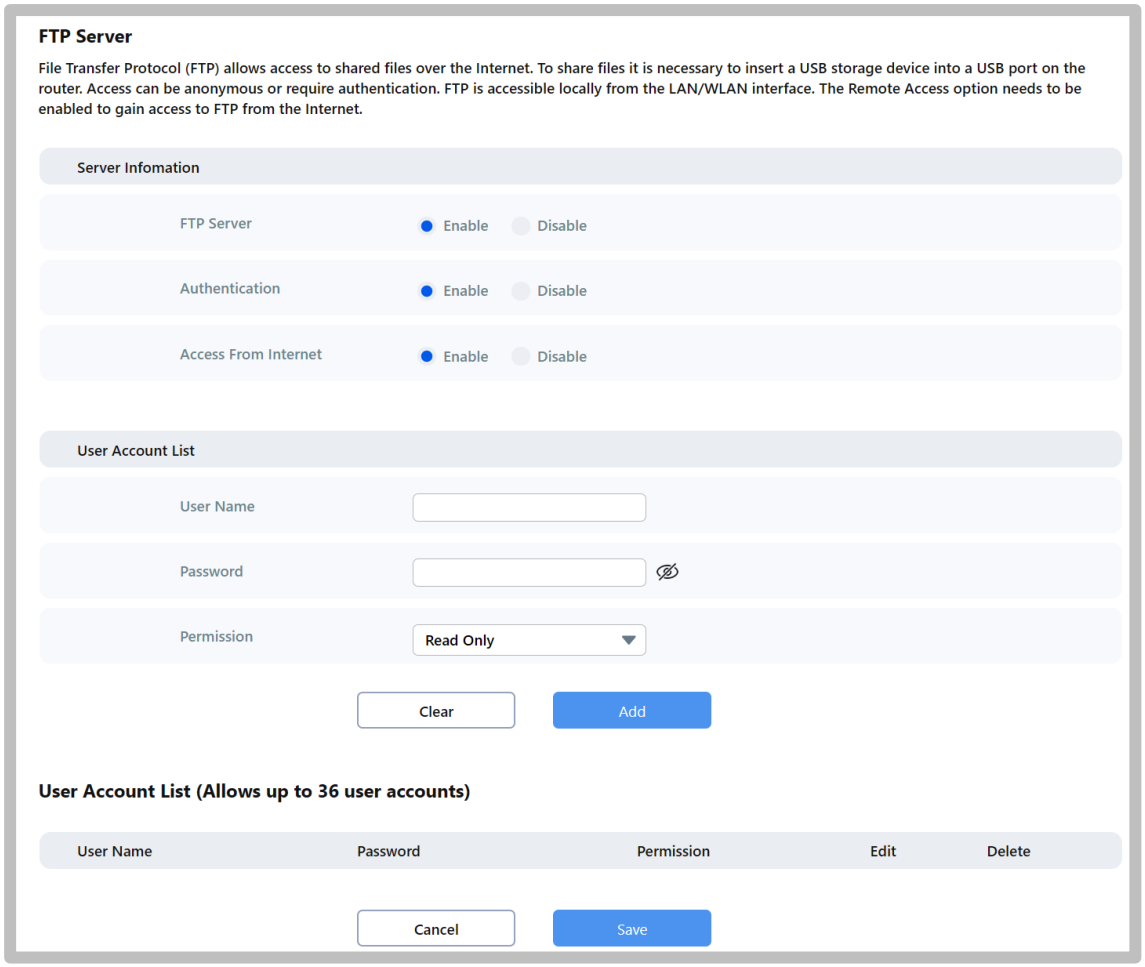
- Settings:
  - (1) **Server Information**
    - **FTP Server** [Enable / Disable]

- When enabled, the router starts the built-in FTP server and allows clients to access the USB storage device through the FTP protocol.

- **Authentication** [Enable / Disable]
  - Enable: Users must provide a username and password for authentication before connecting.
  - Disable: Allows anonymous login (not recommended on public networks).
- **Access from Internet** [Enable / Disable]
  - Enable: Allows access to the FTP server from the Internet through the public IP address or DDNS domain name.
  - Disable: Allows access only from the LAN.

(2) User Accounts (Up to 36 user accounts are supported)

- **Username**: Customize the account name.
- **Password**: Password required to log in to FTP.
- **Permission**: Sets the access permission for this account (read/write permission).
- **Edit**: Edit or remove existing accounts at any time.



5.6.4 BitTorrent Settings

BitTorrent is a peer-to-peer (P2P) file transfer technology that downloads files from multiple nodes, improving download speed and stability. The router built-in BitTorrent download function enables long-term downloads without a computer, saving device resources and reducing power consumption.

- Enter **BitTorrent Settings**:
  (1) Click on **Advanced** > **USB** page
  (2) Click on **BitTorrent Settings** tab

- Settings:
  (1) **BitTorrent Status** [Enable/Disable]
    - Enable: Enables BitTorrent downloads so the router can download torrent tasks directly.
      - Download Manager: Can be opened only after the user account is configured.
    - Disable: Disables BitTorrent and stops all download tasks and seeding.

  (2) **User Account**:
    - Username: Manage login account.
    - Password: Manage login password.

  (3) **Download / Upload** Maximum Speed:
    - Auto: System automatically allocates bandwidth based on network conditions.
    - Manual: User customizes maximum download speed (: Kbit/s)

  : If multiple people share the home network, it is recommended to set an appropriate limit to avoid affecting other devices.

  (4) **Seeding**:
    - NO limited: Continues uploading after download completion without limiting the seeding ratio.
    - Custom Percentage: For example, setting 100% means the upload can stop automatically after the uploaded data reaches the downloaded amount.

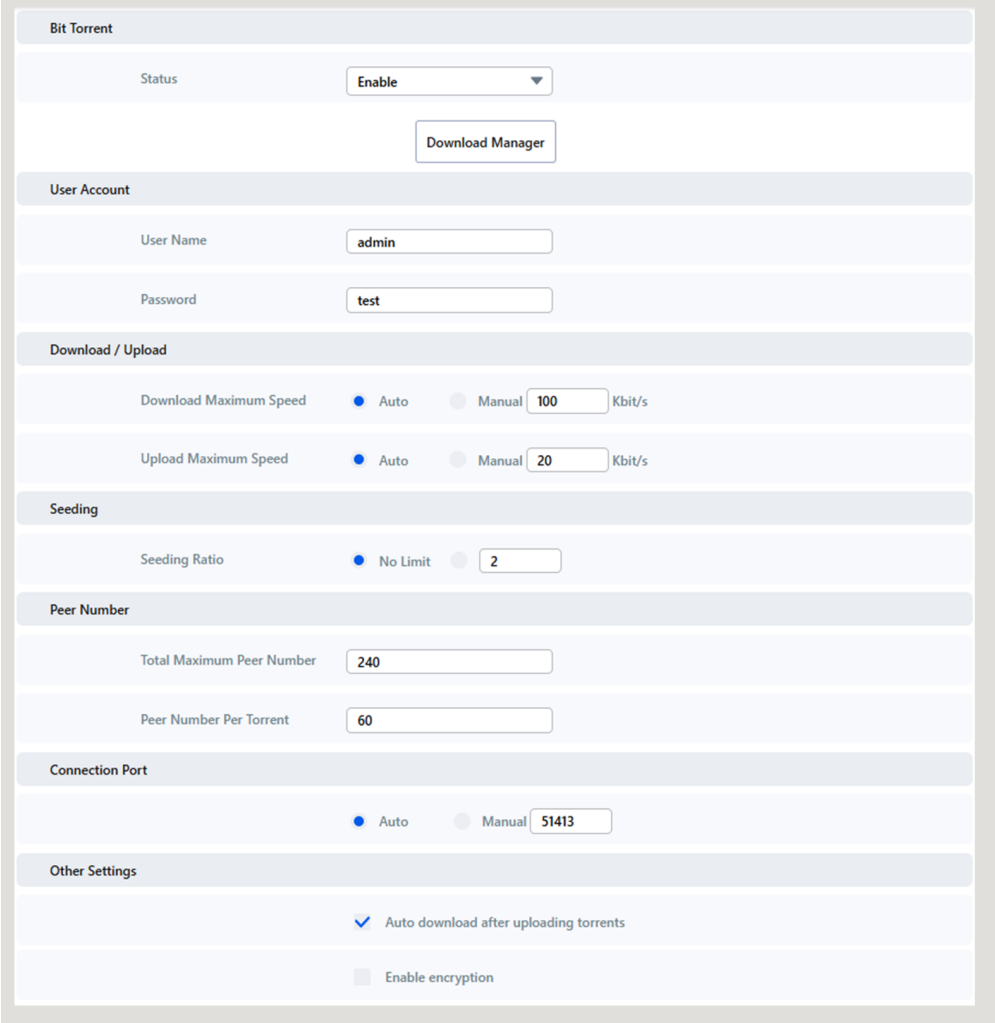
  (5) **Peer Number**:
    - **Total Maximum Number of Peers**:
      - Limits the total number of peers all download tasks can connect to.
      - Default is 240, suitable for most home network environments.
    - **Peer Number Per Torrent:**
      - Limits the number of peers a single task can connect to simultaneously.
      - Default is 60 to balance stable speed and system load.

  (6) **Connection Port**:

- Auto: The system automatically selects the port and performs port forwarding (requires UPnP).
- Manual: User-defined communication port. Make sure the firewall allows external connections through this port.

(7) **Other Settings**:

- **Auto download after uploading torrents**: When selected, uploading a .torrent file automatically starts the download task.
- **Enable Encryption**: When enabled, transmission is encrypted, which may help reduce certain ISP restrictions and improve connection stability.



5.6.5 Eject Device

Before removing a USB storage device, it is strongly recommended to use the Safely Remove function to ensure data integrity and device safety.

- Enter Eject Device Settings:

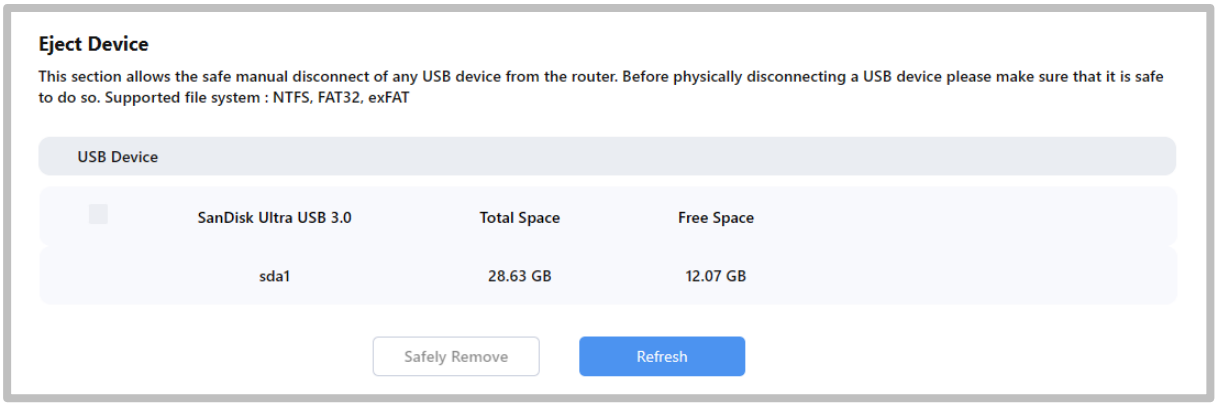
(1) Click **Advanced** > **USB** page

(2) Click **Eject Device** tab

- Settings:

(1) **Safely Remove**: Before physically unplugging the USB device, click this button to notify the system to complete all read/write operations and prevent file corruption or format errors caused by interruption.

(2) **Refresh**: After a new USB device is inserted, manually refresh USB device detection so the system can read the currently connected device again.



5.7 Local Area Network (LAN)

5.7.1 LAN Setting

Local Area Network (LAN) settings mainly manage the internal local network structure of the router, affecting address allocation and communication ranges for home network devices.

LAN settings affect:

- ✓ The DHCP allocation range and default gateway settings for all connected devices.
- ✓ The IP subnet configuration used for communication among internal devices.
- ✓ If large-scale address range adjustments are made, the DHCP server settings must be replanned accordingly.

- Enter Local Area Network (LAN) Settings:

(1) Click **Advanced** > **LAN** page

(2) Click **LAN Settings** tab

- Settings:

(1) LAN Interface Settings

- **IP Address**: Sets the router internal IP address as the LAN gateway (Gateway) usually the core identifier of the entire internal network.
- **Subnet Mask**: Determines the number and range of IP addresses that can be allocated in the internal subnet.
- **MAC Address**: Physical address of the router internal network adapter. It is for identification only and cannot be modified.

5.7.2 DHCP Server Setting

The DHCP Server (Dynamic Host Configuration Protocol Server) allows the router to automatically assign IP addresses to connected devices on the LAN, reducing the need for manual configuration.

- Enter **DHCP Server Setting**:

(1) Click **Advanced** > **LAN** page

(2) Click **DHCP Server Setting** tab

- Settings:

(1) DHCP Server Setting:

- **DHCP Server** [Enable/Disable]:
  - When enabled, the router will automatically assign IP addresses to newly connected devices.
- **DHCP Start IP**: Set the starting address of the DHCP allocation range.
- **DHCP End IP**: Set the ending address of the DHCP allocation range. Plan the IP range appropriately according to the LAN subnet.
- **DHCP Lease Time**: The amount of time each device leases the assigned IP address. (Unit: minutes)

※ A shorter DHCP lease time increases the likelihood of IP release and reassignment.

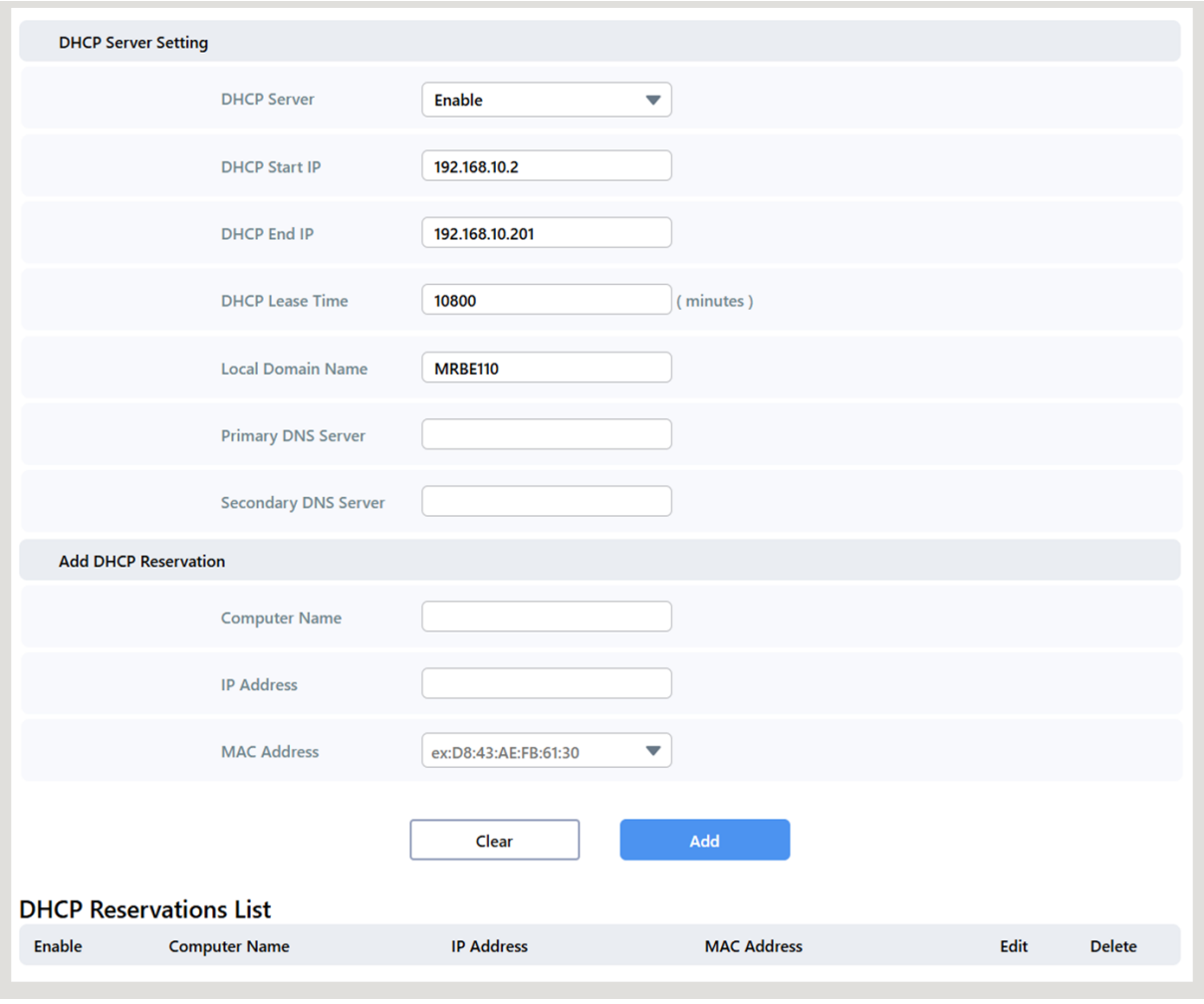
- **Local Domain Name**: Set the internal domain name for the LAN.
- **Primary/ Secondary DNS Server**: If a custom DNS server is used on the internal network, it can be specified manually. If left blank, the router forwards the ISP DNS by default.

(2) Add DHCP Reservation: Allows a fixed IP address to be assigned to a specific device based on its MAC address. The address does not change with lease renewal and is suitable for servers, surveillance devices, and other devices requiring stable addressing.

- **Computer Name**: Enter the corresponding device name (for easier identification and management)
- **IP Address**: Specify the reserved static IP
- **MAC Address**: Hardware address of the corresponding device network adapter.

- After a reservation is configured, the device always obtains the same IP address when connecting, avoiding changes from DHCP allocation.
- It is recommended that the reserved range not overlap with the dynamic DHCP range.

(3) **DHCP Reservations List:** Can be "Edited" and "Deleted" to adjust content at any time.



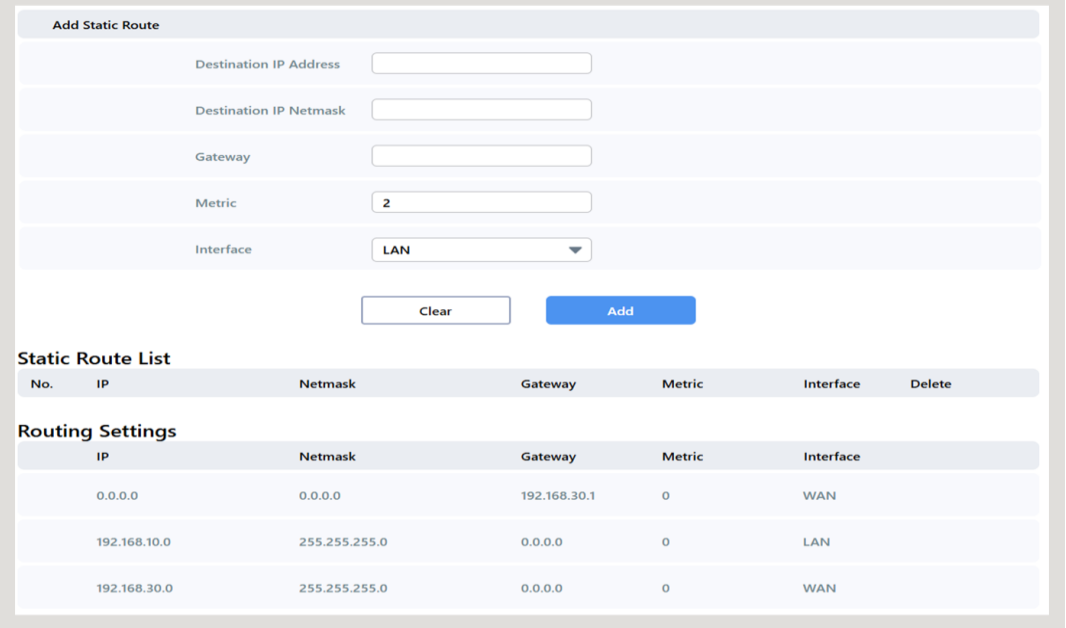
5.7.3 Routing Settings

Routing settings allow administrators to manually configure static routes and control route forwarding among different subnets or networks. This is suitable for environments with multiple subnets, multiple VLANs, or cross-network requirements.

- Enter **Routing** Settings:
  (1) Click **Advanced** > **LAN** page
  (2) Click **Routing** tab

- Settings:
  (1) Add Static Route:
    - **Destination IP Address**: Starting address of the target network segment to route to.
    - **Destination IP Netmask**: Netmask length of the target network segment, which determines the route coverage range.
    - **Gateway**: The next hop for this route traffic (Next Hop) IP Address.
    - **Metric**: Route priority. A smaller value indicates a higher priority (The default value 0 is usually sufficient)
    - **Interface**: Select whether to route through the internal LAN or WAN interface.
  (2) **Static Route List**: The list can be adjusted by deleting entries.

- Static routing is an advanced function and is not required for typical home Internet access.
- The gateway IP must be on an existing reachable network segment to avoid blackhole routing.
- Improper overlapping routes may cause internal communication failures. Make sure the routing plan is correct.



5.8 IPv6

IPv6 settings allow the router to support the next-generation IPv6 protocol, providing full support for future high-speed Internet while offering multiple ISP compatibility modes.

- Enter **IPv6** Settings:
  (1) Click **Advanced** > **IPv6** page

- Settings:
  (1) IPv6 Connection Type:
    - **Static**: Configure a static IPv6 address, prefix length, and DNS according to ISP assignment.
    - **Autoconfiguration (SLAAC / DHCPv6)**: Obtains an IPv6 prefix and DNS through automatic allocation.
    - **Auto Detect**: The system automatically detects the applicable IPv6 mode.
    - **PPPoE**: Used with PPPoE authentication connections required by some service providers.

  (2) WAN IPv6 IP Settings:
    - **WAN IPv6 Address**: External IPv6 IP address assigned by the ISP.
    - **Subnet Prefix Length**: Commonly 64; use the value assigned by the ISP.
    - **Default Gateway**: LAN devices access the external Internet through the default gateway.

  (3) IPv6 DNS Server Settings:
    - **Manually configure DNS**: When enabled, allows you to manually enter the DNS server to use.
    - **Primary DNS Server**: DNS server address primarily used by the system.
    - **Secondary DNS Server**: Automatically switches to the secondary DNS when the primary DNS is unavailable.

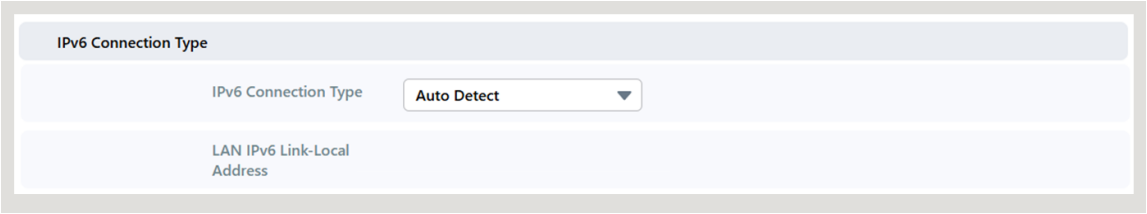
  (4) LAN IPv6 IP Settings:
    - **Enable DHCP-PD**: The ISP assigns a complete IPv6 prefix, and the router further allocates it to the internal LAN.
    - **LAN IPv6 Address**: Internal LAN IPv6 address (Gateway).
    - **LAN Prefix Length**: Size of the LAN IPv6 address space.
    - **LAN IPv6 Link-Local Address**: Generated automatically and does not require manual configuration.
    - **Pass-Through (Bridge)**: When enabled, internal devices can directly obtain IPv6 addresses assigned by the ISP instead of being allocated again by the router.

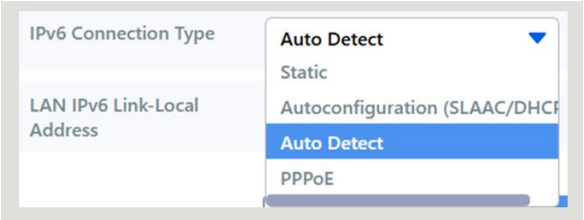
  (5) LAN Address Autoconfiguration Settings:
    - **Enable Autoconfiguration**: Enables SLAAC/DHCPv6 dynamic allocation.

- **Auto Configuration Type**: Supports **Stateless DHCPv6**, **Stateless Auto**, **DHCPv6 (Stateful)**.
- **Router Advertisement Lifetime**: The interval at which IPv6 router broadcasts are sent.

(6) **PPPoE Setting**:

- **PPPoE Session**: Sets whether to share the IPv4 PPPoE session or create an independent IPv6 PPPoE connection.
- **User name/Password/Confirm Password**: Enter according to ISP PPPoE authentication information.
- **Address Mode**:
  - Static: Manually filled in the WAN IPv6 address.
  - Auto: The system automatically obtains all required IPv6 configuration information from the ISP.
- **MTU Setting**: Default 1492 (adjust according to ISP requirements)





5.9 VPN Server

5.9.1 OpenVPN

OpenVPN provides a secure remote access mechanism, allowing users to connect back to the company or home internal network through an encrypted tunnel, ensuring data privacy and security.

- Enter **OpenVPN** Setting:

  (1) Click **Advanced** > **VPN Server** page

  (2) Click **OpenVPN** tab

- Settings:

  (1) OpenVPN Server Information:

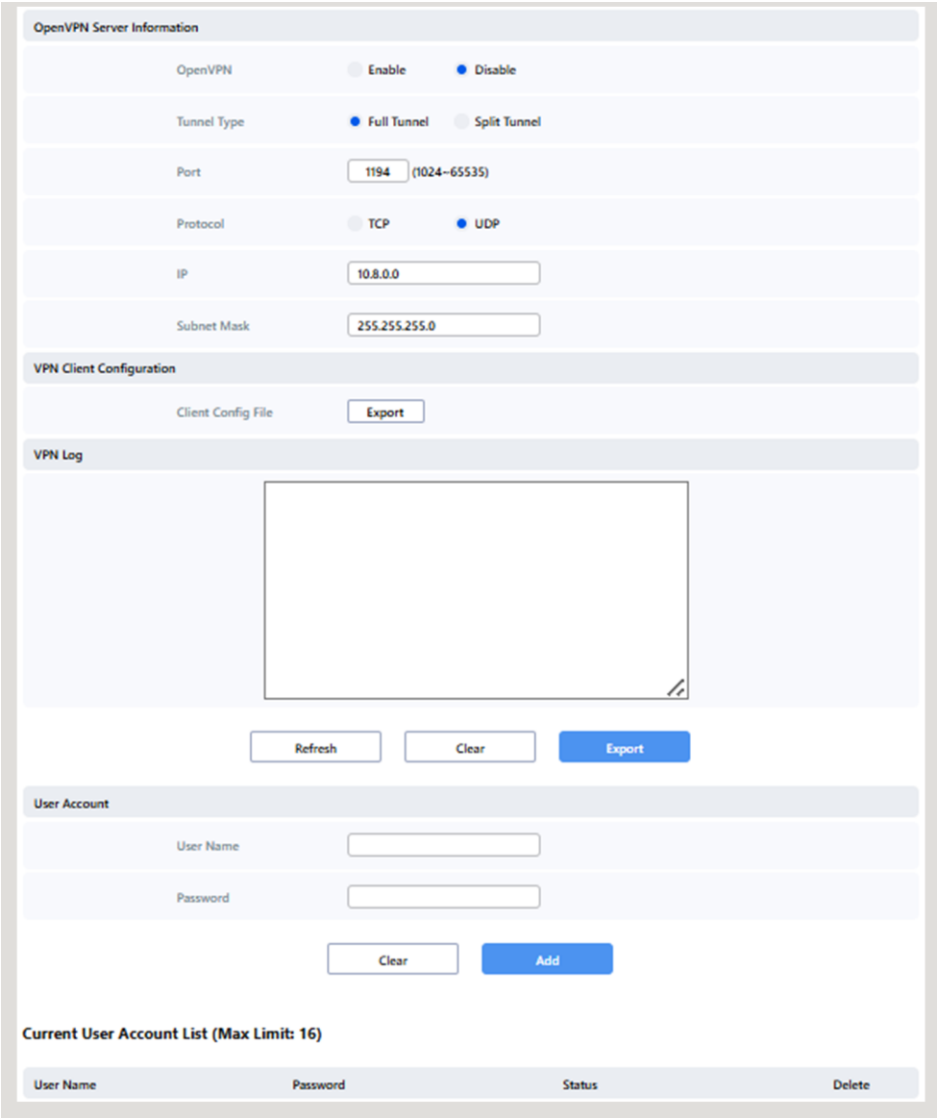
- **OpenVPN** [Enable/Disable]: Enables or disables the VPN server function.
- **Tunnel Type**:
  - **Full Tunnel**: All network traffic is transmitted through the VPN, including general Internet traffic. Suitable for scenarios requiring full traffic management and security.
  - **Split Tunnel:** Only specific network traffic (such as internal resources) is transmitted through the VPN, while other traffic still uses the local network connection. Suitable for balancing performance and general Internet access requirements.
- **Port**: Default is 1194. The communication port can be customized (range 1024-65535).
- **Protocol**: Supports **TCP** and **UDP** transport protocols.
- **IP** : Internal virtual network IP for the VPN, representing the virtual VPN subnet assigned within the OpenVPN server.
- **Subnet Mask**: Corresponding virtual subnet mask.

(2) VPN Client Configuration:
- Client Config File **Export**: Click the button to export a custom OpenVPN client profile for quick import and installation.

(3) VPN Log: Displays current VPN connections and system logs for troubleshooting.

(4) User Accounts: Add or edit user accounts and login passwords for access control.

(5) Current User Account List (Max Limit: 16): Lists all currently created accounts and allows deletion management.



5.9.2 PPTP

PPTP(Point-to-Point Tunneling Protocol) is a VPN (Virtual Private Network)) protocol that allows remote users to securely connect to an internal network over the internet. This settings page provides complete PPTP server configuration options.

- Enter **PPTP** Settings:
  - (1) Click **Advanced** > **VPN Server** page
  - (2) Click **PPTP** tab

- Settings:
  - (1) PPTP Server Information:
    - **PPTP** [Enable/Disable]:

- Enables the PPTP server and allows clients to connect to the router internal network through VPN.

- **Authentication**:
  - Auto: The system automatically selects the authentication mode.
  - MS-CHAPv1: Uses Microsoft CHAP version 1 authentication.
  - MS-CHAPv2: Uses Microsoft CHAP version 2 authentication (more secure).
- **MPPE Encryption**:
  - MPPE-128: Uses 128-bit strong encryption for higher security.
  - MPPE-40: Uses 40-bit weak encryption.
  - No Encryption: No encryption; suitable only for environments that do not require confidentiality protection.
- **Network Place (Samba) Support** [Enable/Disable]:
  - Enable: Allows access to Samba file sharing services on the LAN after VPN connection.
  - Disable: Disables access to Samba.
- **Connect to DNS Server automatically** [Enable/Disable]:
  - Enable: Automatically assigns the DNS server IP.
  - Disable: Clients must specify the DNS server manually.
- **Connect to WINS Server automatically** [Enable/Disable]:
  - Enable: Automatically assigns the WINS server IP(mainly used for legacy Windows network neighborhood name resolution).
  - Disable: Does not assign a WINS server.
- **MRU/MTU**: Maximum Receive Unit(Default 1410)/Maximum Transmission Unit(Default 1410).

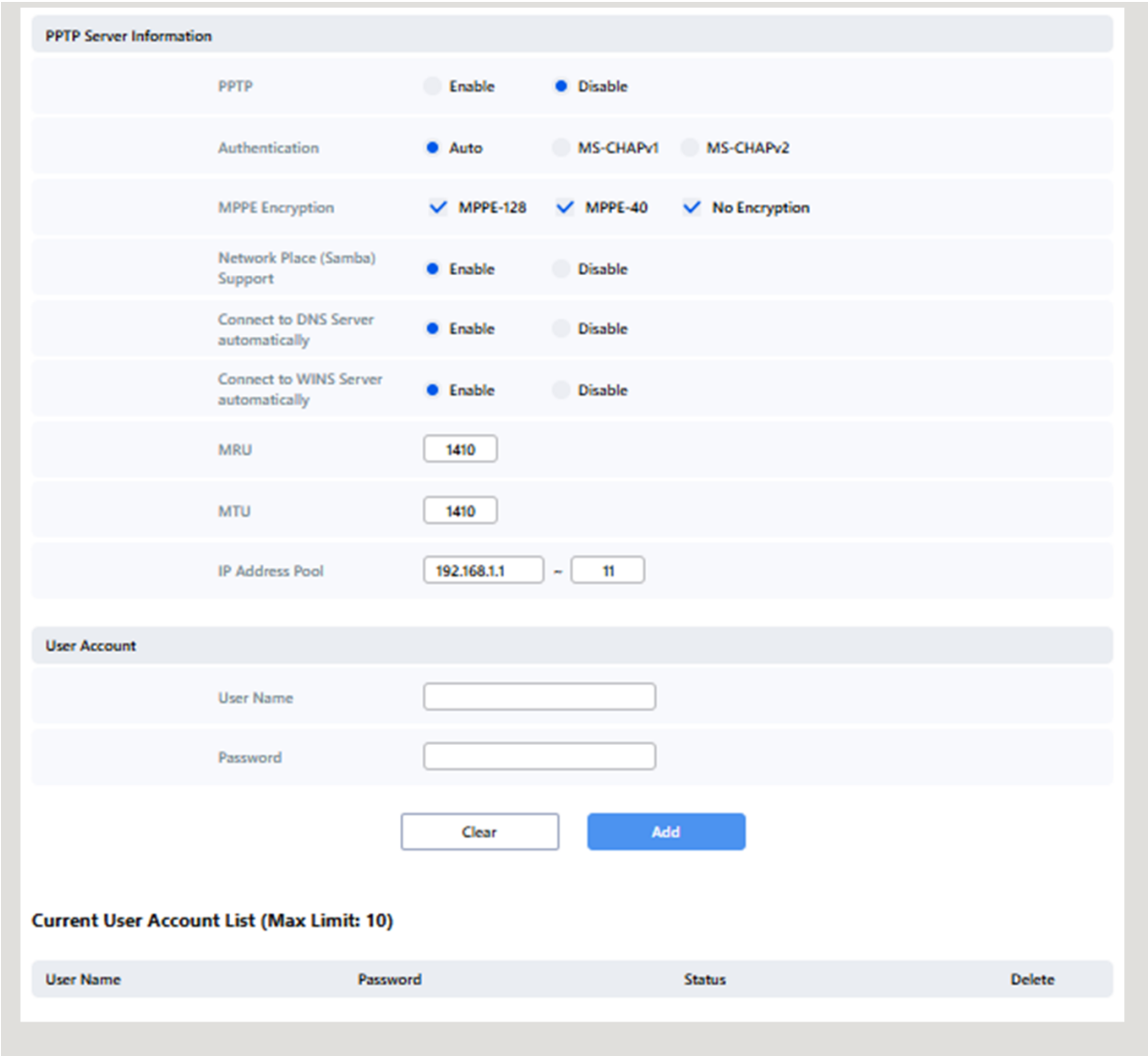
※ Unless there are special requirements, it is recommended to keep the default values to ensure stable connection.

- **IP Address Pool**: Specifies the internal IP address range that can be assigned to VPN clients when connected.

※ Do not overlap with the existing LAN IP range to avoid IP conflicts.

(2) **User Account**: User accounts and passwords can be added.

(3) **Current User Account List (Max Limit: 10)**: Lists all currently created accounts and allows deletion management.



5.9.3 L2TP/IPSec

L2TP/IPSec (Layer 2 Tunneling Protocol with IPSec) is a commonly used secure VPN protocol that combines L2TP tunneling with IPSec encryption, providing a more secure VPN connection than PPTP. This settings page is used to configure the router L2TP/IPSec VPN server function.

- Enter **L2TP/IPSec** Settings:
  (1) Click **Advanced** > **VPN Server** page
  (2) Click **L2TP/IPSec** tab

- Settings:
  (1) L2TP/IPSec Information:
    - **L2TP/IPSec** [Enable/Disable]:

› When enabled, allows remote users to connect to the internal network through L2TP/IPSec.

- **IPSec Encryption**:

› Enables IPSec encryption to provide packet security protection.

- **IPSec Pre-shared Key**: Key used for IPSec authentication.

› Remote clients must enter the same Pre-Shared Key in the VPN settings to connect successfully.

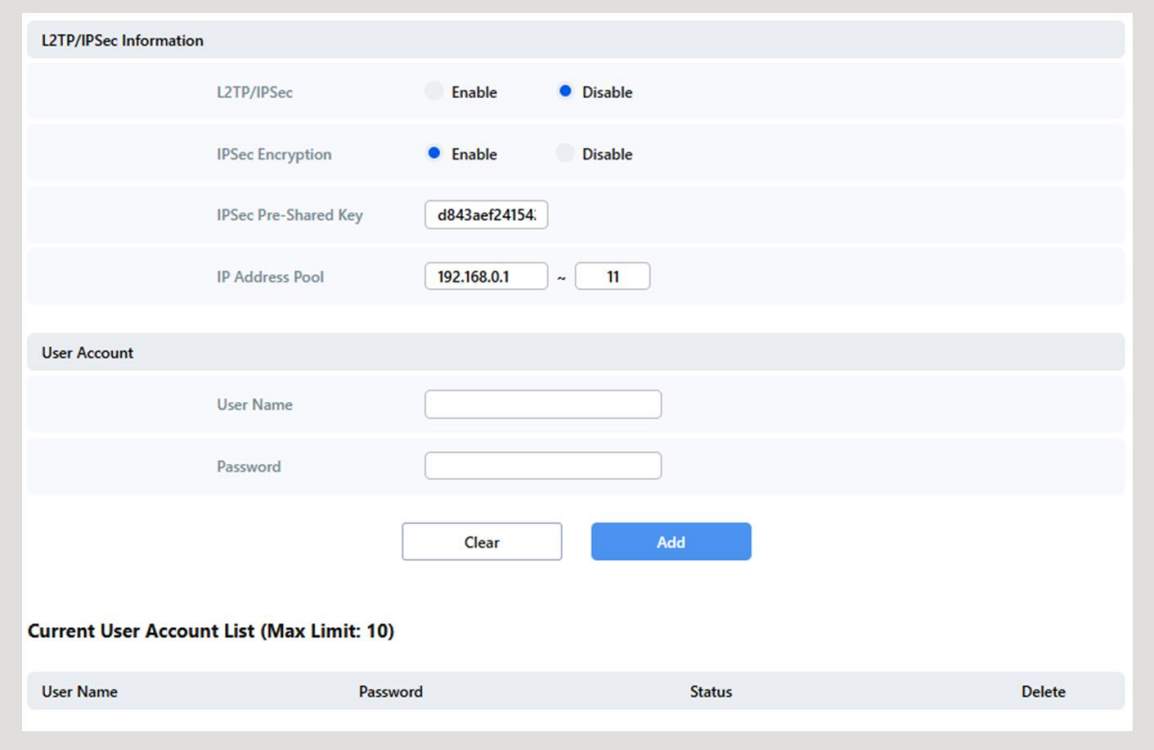
※ Keep this key secure and do not disclose it.

- **IP Address Pool**: Specifies the virtual internal IP address range automatically assigned after remote users connect.

※ Do not conflict with the local area network DHCP range, to avoid IP duplicates.

(2) **User Account**: Allows adding user accounts and passwords.

(3) **Current User Account List (Max Limit: 10)**: Lists all currently created accounts and allows deletion management.



5.9.4 WireGuard

Configure the router built-in WireGuard VPN server to allow remote devices to securely connect to the home/office internal network through the Internet.

- Enter **WireGuard** Settings:

(1) Click **Advanced** > **VPN Server** page

(2) Click **WireGuard** tab

- Settings:

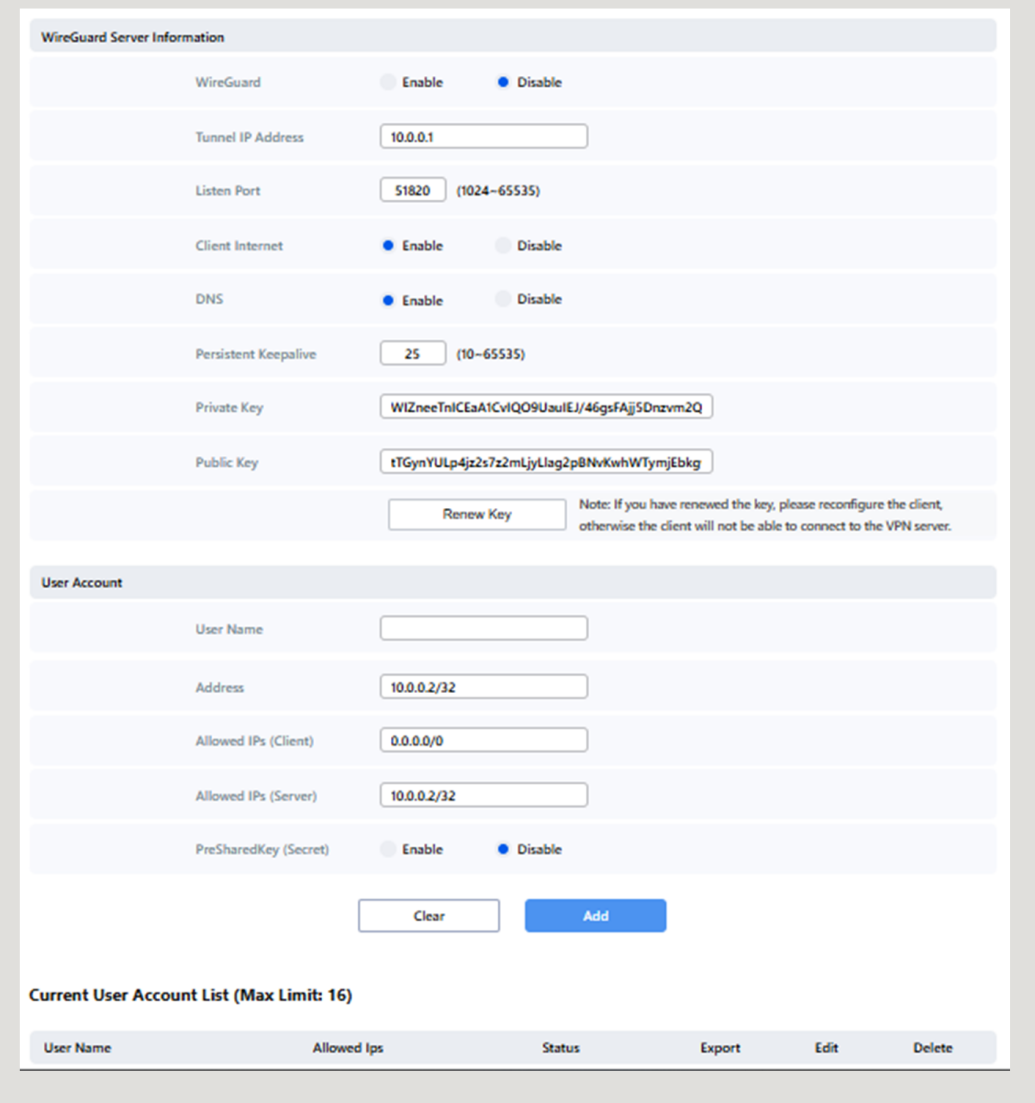
(1) WireGuard Server Information:

- **WireGuard** [Enable/Disable]: Enables or disables the WireGuard server function.
- **Tunnel IP Address**: Specifies the server-side address of the VPN subnet. Clients obtain addresses in the same subnet to access the internal network.
- **Listen Port**: Server listening port (range 1024-65535). Clients must configure the same port to connect.
- **Client Internet** [Enable/Disable]: When enabled, VPN client traffic can access the Internet through the router (suitable for full-tunnel VPN).
- **DNS** [Enable/Disable]: When enabled, VPN clients use the specified DNS.
- **Persistent Keepalive**: Used to keep NAT traversal connections alive (: seconds).
- **Private Key / Public Key**: Server-side private and public keys used for WireGuard encrypted communication.
- **Renew KEY button**: Generates new keys. After regeneration, all clients must be reconfigured to connect.

(2) User Account:

- **User name**: Specifies the name for this user.
- **Address**: Specifies the client IP address in the VPN subnet.
- **Allowed IPs (Client)** : Defines the networks the client is allowed to access.
- **Allowed IPs (Server)** : Specifies the networks the server is allowed to send to this client.
- **Pre-sharedKey (Secret)** [Enable/Disable]: Can enable additional pre-shared key encryption.
- **Clear** button: Clears the input fields.
- **Add** button: Adds the user settings to the list.

(3) Current User Account List (Max Limit: 16): Lists all currently created users and allows **Export/Edit/Delete** management.



5.10 VPN Client

Allows internal devices to establish VPN connections through the router and securely connect to remote VPN servers.

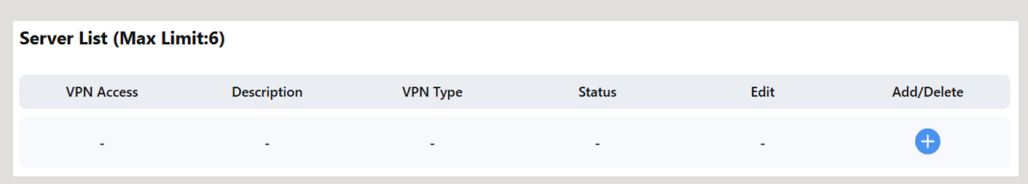
- Enter **VPN Client** settings:

  (1) Click **Advanced** > **VPN Client** page

- Settings:

  (1) **Server List (Max Limit:6)**

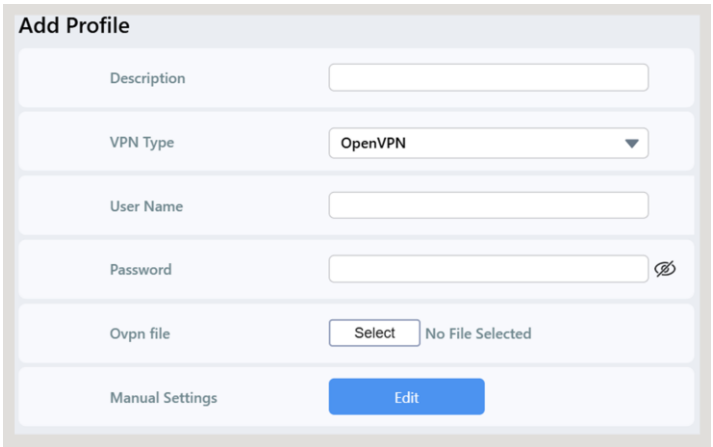
  Up to 6 VPN server profiles can be created, and each profile can be assigned to specified internal clients.



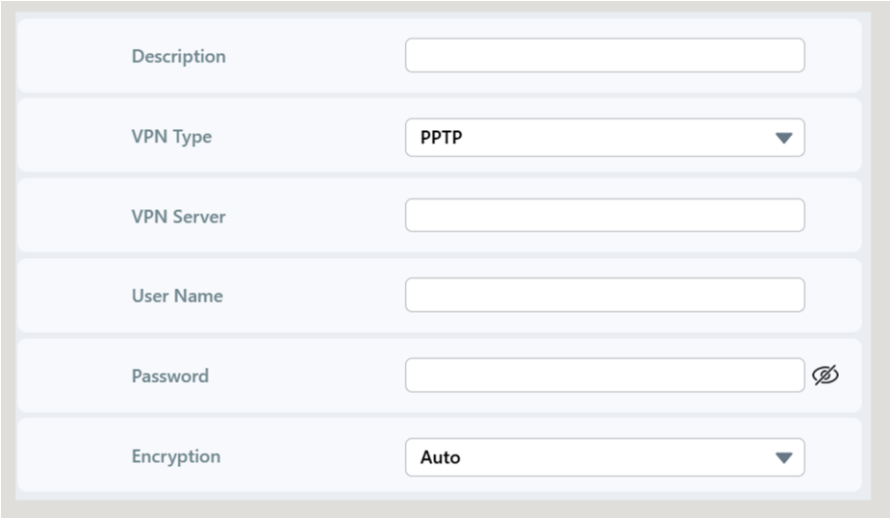
- **VPN Access**: Turn the VPN server on or off.
- **Add/Delete/Edit**: Manage VPN server profiles.
- **Description**: Set a description to identify the purpose or corresponding server of this VPN profile.
- **VPN Type**: Select the VPN protocol to use. (Supports OpenVPN, PPTP, L2TP, WireGuard)
  - **OpenVPN**
    - **User Name/Password**: The account name and corresponding login password for authentication.
    - **Ovpn File**: Upload an OpenVPN configuration file (usually with the **.ovpn** extension). This file is usually provided by the VPN server administrator and contains information such as server address, encryption keys, and connection parameters.
    - **Manual Settings**: If the uploaded **.ovpn** file does not contain complete keys and certificates, or if certificate settings must be adjusted manually, enter them manually.
      - **Certificate Authority**: Enter the Certificate Authority issued by the server (CA) certificate content.
      - **Client Certificate**: Enter the client certificate content used for authentication.
      - **Client Key**: Enter the corresponding client private key.

※ If your VPN service provides a complete ovpn file, the certificates and keys are usually embedded, and manual settings are not required.

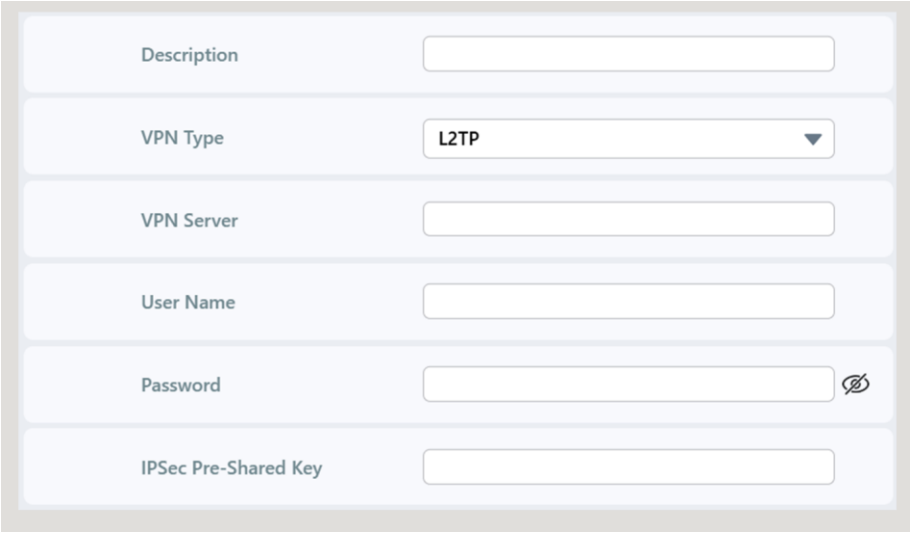
※ If you need to provide certificates and keys yourself, go to **Manual Settings** and paste the content into the corresponding fields.



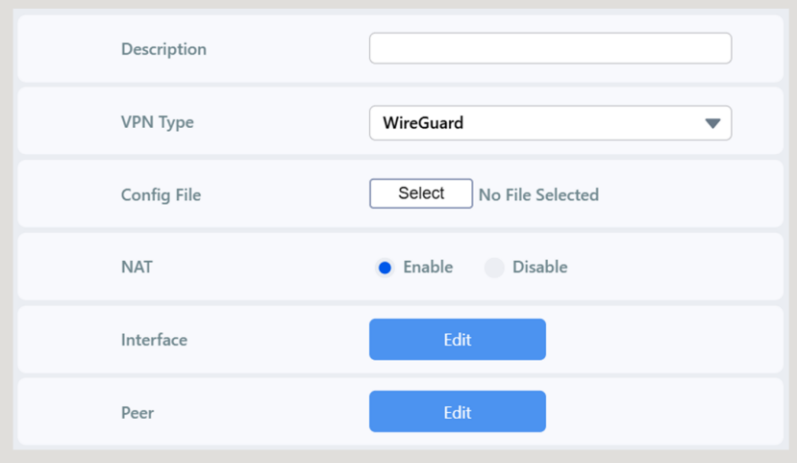
- **PPTP**
  - **VPN Server**: Enter the PPTP VPN server address (IP Address or name).
  - **User Name**: Enter the VPN account used for connection authentication.
  - **Password**: Enter the corresponding VPN password.
  - **Encryption**: Selects the data encryption method (Supports Auto, Max, and None).



- **L2TP**
  - **VPN Server**: Enter the L2TP VPN server address (IP Address or name).
  - **User Name**: Enter the VPN account used for connection authentication.
  - **Password**: Enter the corresponding VPN password.
  - **IPSec Pre-Shared Key**: Pre-Shared key used for IPSec authentication. It must match the VPN server setting to establish a secure connection.

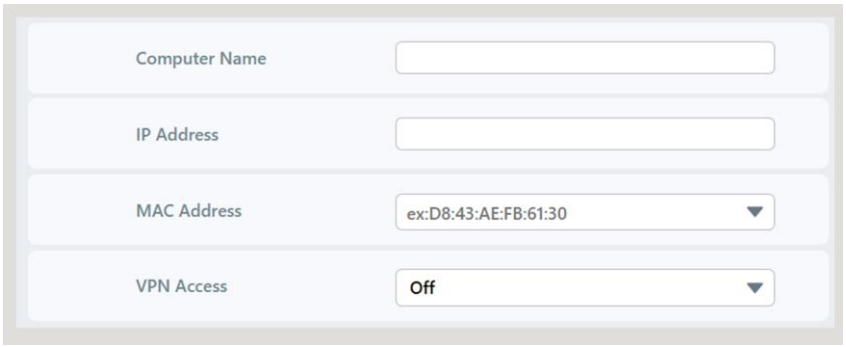


- **WireGuard**
  - **Config File:** Import a WireGuard configuration file that contains the keys and parameters required for connection.
  - **NAT:**
    - **Enable:** Allows internal devices to access external networks through the VPN (commonly used).
    - **Disable:** Only establishes the VPN tunnel without address translation.
  - **Interface:** Sets local WireGuard interface parameters
    - **Private key:** Private key used for local authentication. It must match the peer configuration. Keep it secure and do not disclose it.
    - **Address:** Specifies the IP address of this WireGuard interface (for example 10.0.0.2/24), used for communication within the VPN tunnel.
    - **DNS Server 1 / 2:** Set the DNS server used for VPN connection. If not set, the original network DNS is used.
    - **MTU Size:** Set the maximum packet transmission unit (Default is 1420), can be adjusted according to the network environment to improve transmission performance and stability.
  - **Peer:**
    - **Public Key:** Enter the public key of the peer device, used to establish a secure connection, and authenticate identity.
    - **Pre-Shared Key** (optional): Additional encryption key that can improve connection security and must match the peer setting.
    - **Allowed Ips:** Specifies the IP ranges that can be transmitted through this VPN (for example 0.0.0.0/0).
    - **Endpoint Port:** Enter the IP address or domain name of the peer VPN server.
    - **Endpoint Port:** Specifies the port used by the peer(default is 51820).
    - **Persistent Keepalive:** Sets periodic packet transmission to maintain the connection (: second), suitable for NAT environments (recommended 25 seconds).



(2) Client List:

- **Edit/Add/Delete**: Manage Client Device Settings.
- **Computer Name**: Customize the display name for this internal device
- **IP Address**: The device's IP address on the internal network (Usually auto-filled, can be left blank).
- **MAC Address**: Physical network adapter address of the device. The system automatically lists currently connected devices for selection.
- **VPN Access**: Set whether to enable VPN connections on this device by selecting "Off" (default) or a configured VPN server.



5.11 Administration

5.11.1 Operation Mode

This page provides options for different router operating modes to meet user needs in various network environments.

- Enter **Operation Mode** Settings:

(1) Click **Advanced** > **Administration** page

(2) Click **Operation Mode** tab

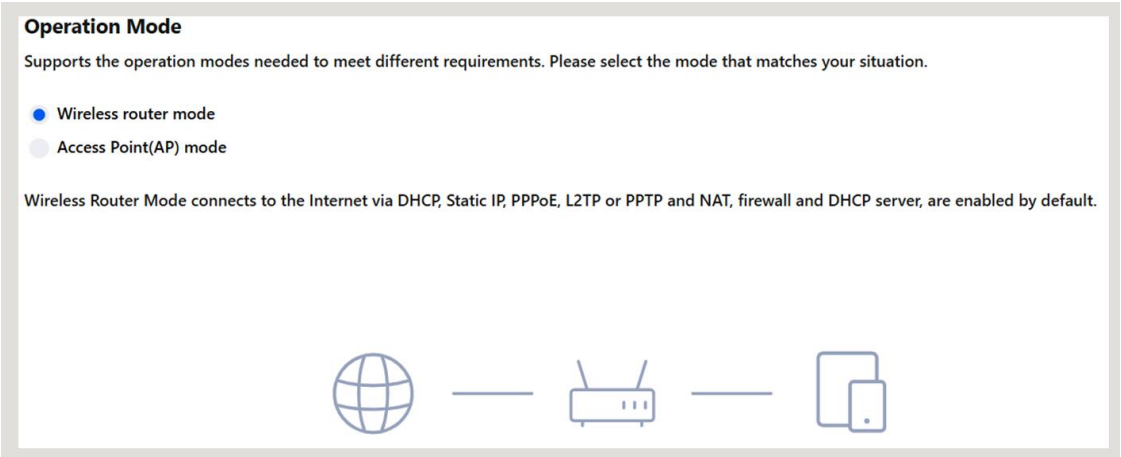
- Settings:

  (1) **Wireless Router Mode** (default Mode):

  - The router connects to the Internet and handles IP allocation, firewall, NAT, VPN, and other functions for all internal network devices.
  - The WAN port connects to the ISP network (for example: fiber modem, cable broadband, ADSL, etc.).

  (2) **Access Point (AP) Mode**:

  - Provides wired network bridging only and extends Wi-Fi coverage. In AP mode, the router connects to the Internet (WAN) through an Ethernet port to extend wireless coverage. In this mode, WAN, Firewall, FortiSecu (parental control and security), QoS, IPv6, and NAT functions are disabled.



5.11.2 System Management

Provides router administrator account security settings, password protection, management authentication, and device naming functions.

- Enter **System Management** Settings:

  (1) Click **Advanced** > **Administration** page

  (2) Click **System Management** tab

- Settings:

  (1) Administrator Settings

  - **Account**: Current router administrator login account (default is admin).
  - **Password**: Set or change the administrator login password.
  - **Confirm Password**: Re-enter the password for confirmation.
  - **Enable Password Reset** [Enable/Disable]:

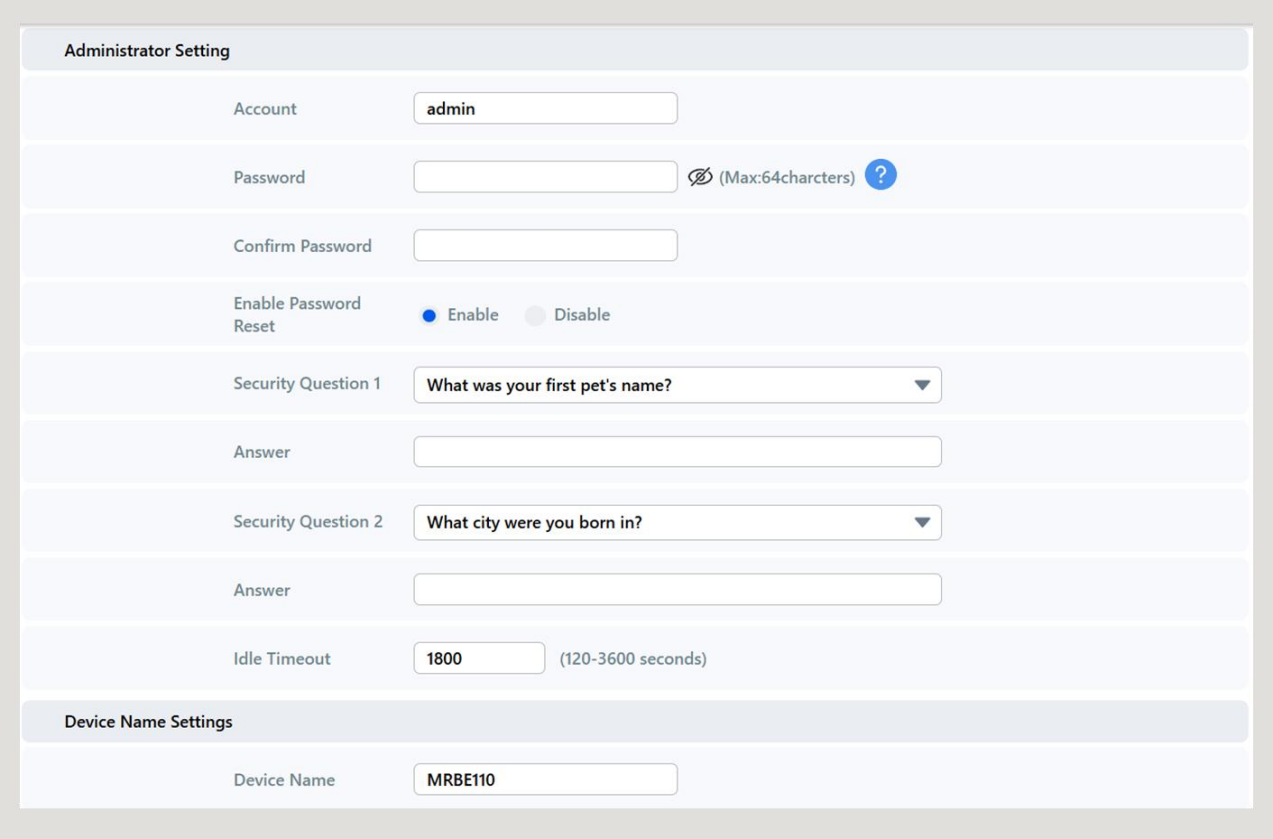
› If enabled, when the password is forgotten, it can be reset through the configured security questions.

- **Security Question and Answer**: Select the question type from the drop-down menu and enter the corresponding answer for future verification.

※ Please Keep the security question answers secure to prevent others from resetting the password.

- **Idle Timeout**: Idle timeout setting (: seconds). After the idle time exceeds the configured time, the system automatically logs out for security.

(2) **Device Name** Settings: Name the router for easier device identification.



5.11.3 Time

The system's time setting affects scheduled functions. It is recommended to configure this section correctly to ensure accurate time synchronization.

- Enter **Time** Settings:

(1) Click **Advanced** > **Administration** page

(2) Click **Time** tab

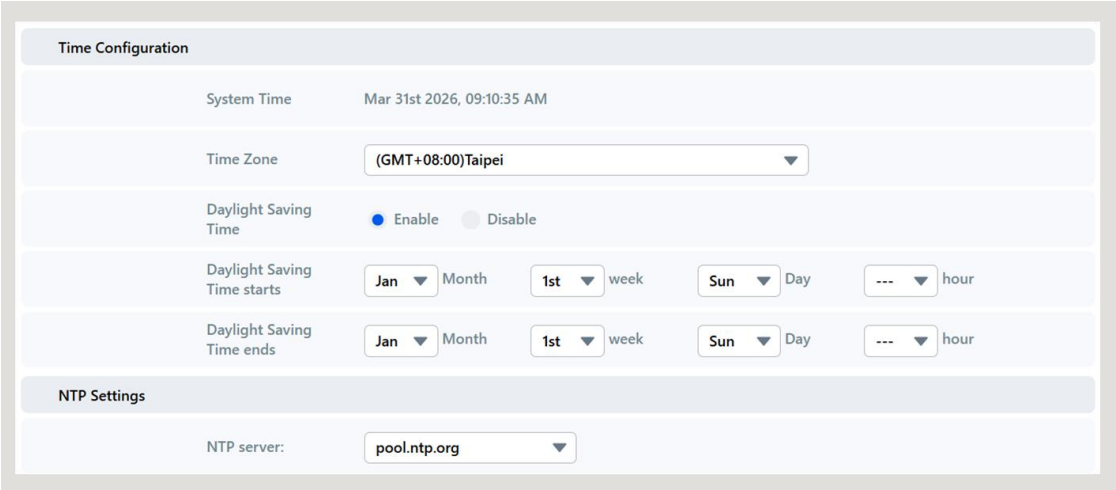
- Settings:

(1) Time Configuration:

- **System Time**: Displays the current router's internal system time.
- **Time Zone**: Select the time zone for your region.
- **Daylight Saving Time** [Enable/Disable]:
  - When enabled, you can configure daylight saving time according to local government regulations.

(2) NTP Settings:

- **NTP Server**: Select the NTP (Network Time Protocol) server address used by the router to automatically synchronize system time.



5.11.4 Local Access Config

This function is used to configure the router management access method on the LAN and related connection parameters.

- Enter **Local Access Config** Settings:

(1) Click **Advanced** > **Administration** page

(2) Click **Local Access Config** tab

- Settings:

(1) Local Access Config:

- **Authorization Method**:
  - BOTH: Allows local LAN management access using both HTTP and HTTPS protocols.
  - HTTPS: Allows access only through the encrypted HTTPS protocol to improve management interface security.

- **HTTPS LAN Port**: Sets the LAN-side port number for the HTTPS management interface. (Default is 443)
- **Download Certificate**: Download the local self-signed certificate (SSL Certificate) of this router to facilitate internal trust management.

5.11.5 Remote Access Config

Configures remote access to the router management interface from the external network (WAN), allowing users to manage the router through the Internet when away from home.

- Enter **Remote Access Config** Settings:
  (1) Click **Advanced** > **Administration** page
  (2) Click **Remote Access Config** tab

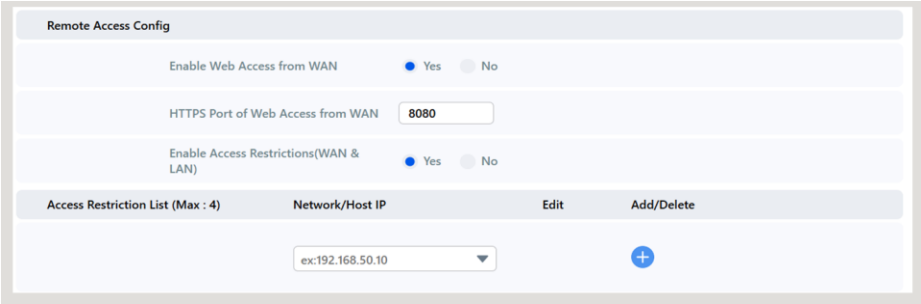
- Settings:
  (1) Remote Access Config:
    - **Enable Web Access from WAN** [Yes/No]:
      - When enabled, the router management interface can be accessed from an external network through the WAN IP address.
      - When disabled, the management interface can be accessed only from the internal LAN.

    ※ Enabling remote management may increase intrusion risk. Enable it only when necessary, and use a strong password and a fixed allow list.
    - **HTTPS Port of Web Access from WAN**:
      - Sets the HTTPS port used for remote management. (Default is 8080)

      ※ Avoid conflict with the local LAN HTTPS port number. (Default is 443)
    - **Enable Access Restrictions (WAN & LAN)** [Yes/No]:
      - When enabled, an access restriction list can be configured. Devices in the list can access the management interface.
      - When disabled, source addresses are not restricted and any IP can attempt to connect to the management interface.

  (2) Access Control List:

- Click + to add allowed IP addresses and manage them by editing or deleting. Up to 4 entries are supported.



5.11.6 Firmware Upgrade

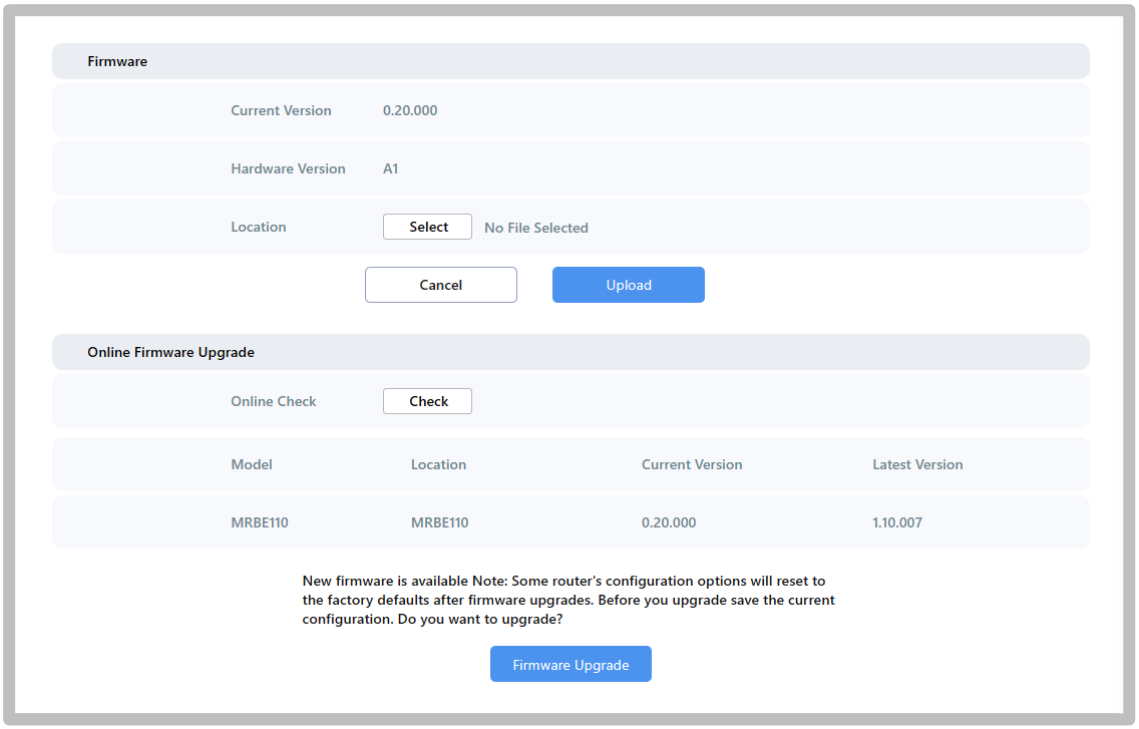
Firmware Upgrade provides router firmware upgrade management to keep the system stable, secure, and up to date. Do not interrupt the update process or turn off the power, as this may damage the router. Wait until the router successfully restarts before continuing.

- Enter **Firmware Upgrade** Settings:
  (1) Click **Advanced** > **Administration** page
  (2) Click **Firmware Upgrade** tab

- Settings:
  (1) Firmware
    - Current Version: Displays the firmware version currently installed on the router.
    - Hardware Version: Displays the hardware version of the router.
    - **Location**: Allows users to manually select a locally downloaded firmware file for upgrade.
      > Click "Select" to browse your local files and choose the firmware upgrade file.
      > After selecting the file, click "Upload" to perform the update.

    ※ Visit the MSI Official Website https://www.msi.com/ to obtain the latest firmware file.

  (2) Online Firmware Upgrade
    - **Online Check**: The system automatically connects to the official server to check if there is a new firmware version available for update.
    - Displays the current connected device model, firmware version, and the latest available version information.
      > If the current version is already the latest, no update is required.
      > If a newer version is available, click the **Firmware Upgrade** button to update.



5.11.7 Restore Setting

Restore Setting provides router backup, restore, reset, and system reboot management for system maintenance, configuration retention, and troubleshooting.

- Enter **Restore Setting** settings:
  (1) Click **Advanced** > **Administration** page
  (2) Click **Restore Setting** tab

- Settings:
  (1) Reset to Factory Defaults:
    - **Load Default**: Restores all router settings to default. All settings will be erased.

  (2) System Reboot:
    - **System Reboot** button: Restarts the router immediately.
    - **Reboot Schedule**: Sets the router to automatically reboot at scheduled times to maintain long-term stability.
    - **Current Time**: Current system time (automatically synchronized according to **Time** settings).
    - **Reboot Time**: Sets the time for automatic reboot.
    - **Repeat**: Select the reboot frequency such as daily, weekly, or monthly.

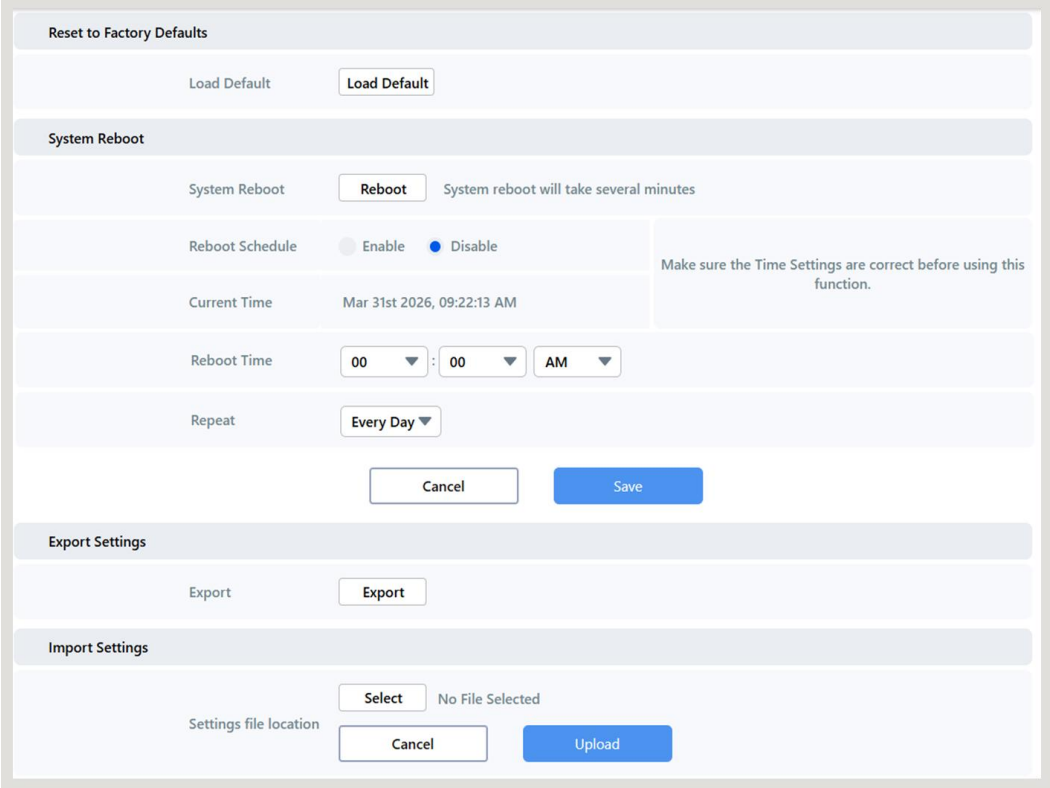
※ For long-term stable operation, scheduled reboots can be arranged to reduce system cache accumulation and improve stability.

(3) Export Settings:

- **Export** button: Backs up all current router settings as a configuration file to the local device.

(4) Import Settings:

- **Select**: Select a previously exported configuration file to quickly restore complete settings.
- **Upload**: Applies the selected configuration file to the router. The router automatically restarts after the settings take effect.



5.11.8 System Log

System Log records internal router operation information, including device login, system exceptions, network connection status, and device behavior, which helps with monitoring, troubleshooting, and technical support.

- Enter **System Log** settings:

(1) Click **Advanced** > **Administration** page

(2) Click **System Log** tab

- Settings:

(1) Save Log:

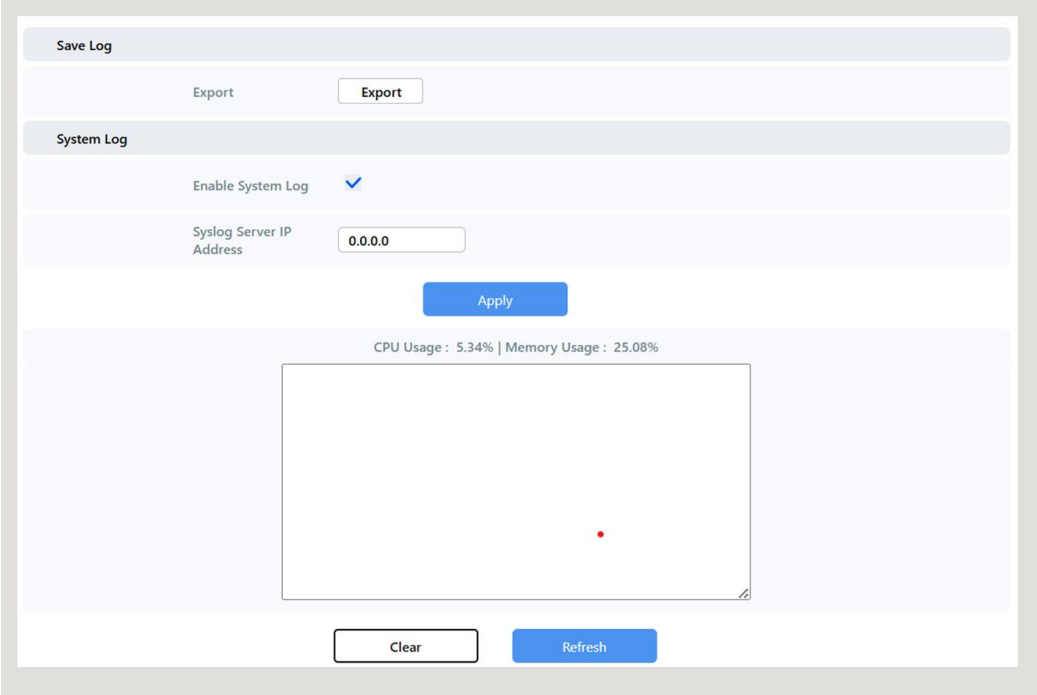
- **Export** button: Downloads the complete current system log for offline analysis or for technical support diagnosis.

(2) System Log:

- **Enable System Log**: When selected, the router continuously collects system logs generated during operation.
- **Syslog Server IP Address**: Sets the IP address of an external Syslog server. The router can forward system logs to that device in real time for centralized management and analysis.

※ When set to 0.0.0.0 , logs will not be forwarded and will only be stored locally.

- **Clear** button: Clears the system log currently stored locally.
- **Refresh** button: Reloads the latest log content, useful for observing real-time system status changes.



5.11.9 Privacy

Allows users to manage authorization related to the FortiSecu service and provides privacy information. You can review the Trend Micro License Agreements and Privacy Notice or withdraw your privacy consent.

- Enter Privacy Settings:

(1) Click **Advanced** > **Administration** page

(2) Click **Privacy** tab

- Settings:

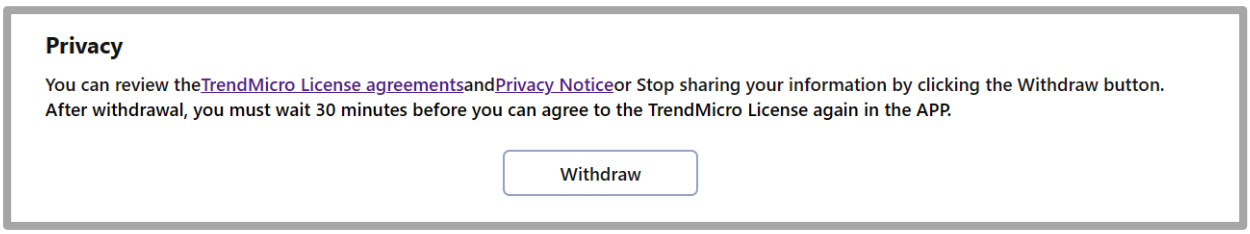
(1) Withdraw

- Click the **Withdraw** button to revoke authorization at any time and stop sharing related protection information with Trend Micro.

※ After withdrawal, related service functions will be suspended until re-authorized.

※ After withdrawal, wait 30 minutes before agreeing again through the MSI Router 2.0 app to enable the Trend Micro License.

※ This tab appears only after FortiSecu is enabled through the app.



5.11.10 Feedback

Click Feedback tab will redirect you to the MSI Member Center official website: https://account.msi.com/en/login

- Enter Feedback Path:

(1) Click **Advanced** > **Administration** page

(2) Click **Feedback** tab

5.11.11 LED Display

Turn the router's LED indicator on or off, or customize a schedule for when it turns off.

- Enter LED Display Settings:

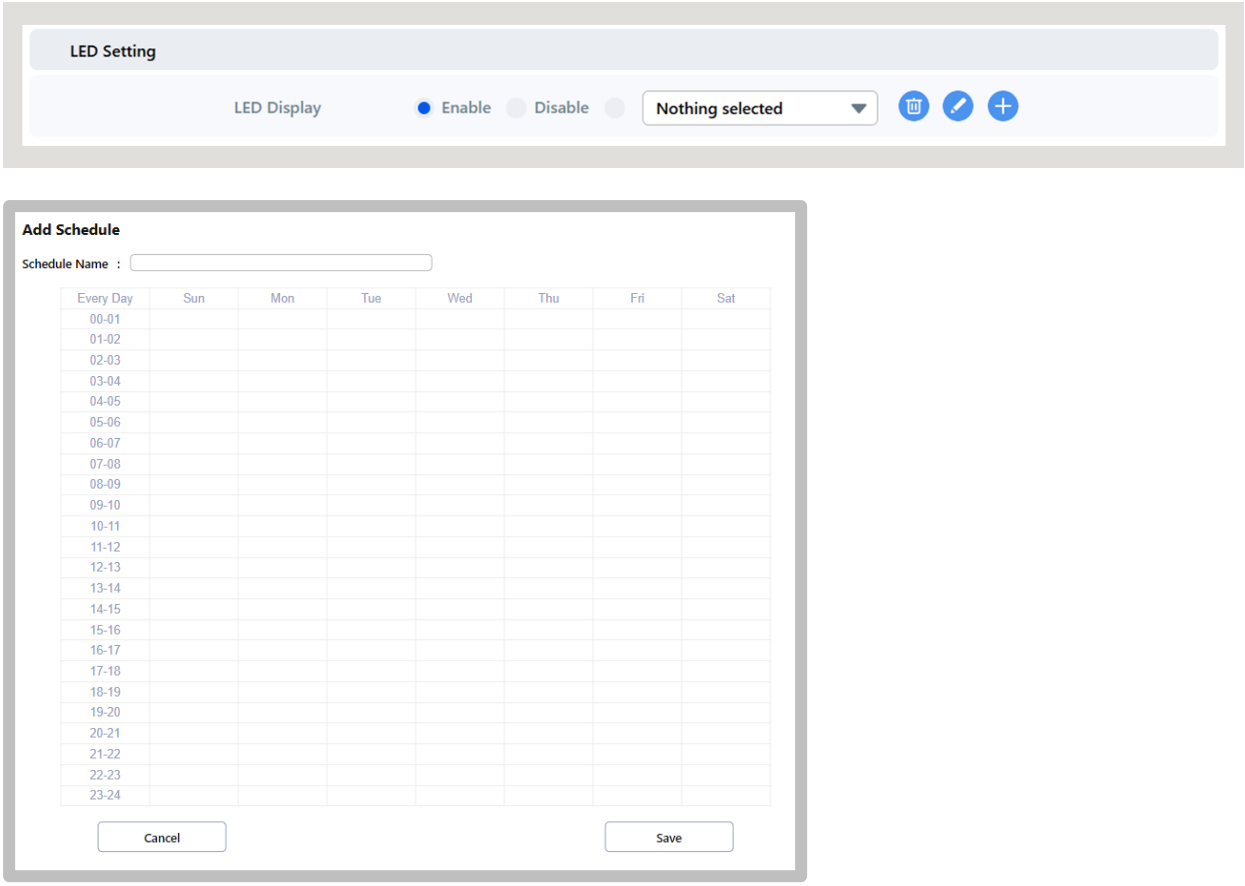
(1) Click **Advanced** > **Administration** page

(2) Click **LED Display** tab

- Settings:

(1) LED Display [Enable/Disable/Custom]

- Custom: Click **+** to add the LED off schedule. Schedule can be edited or deleted.



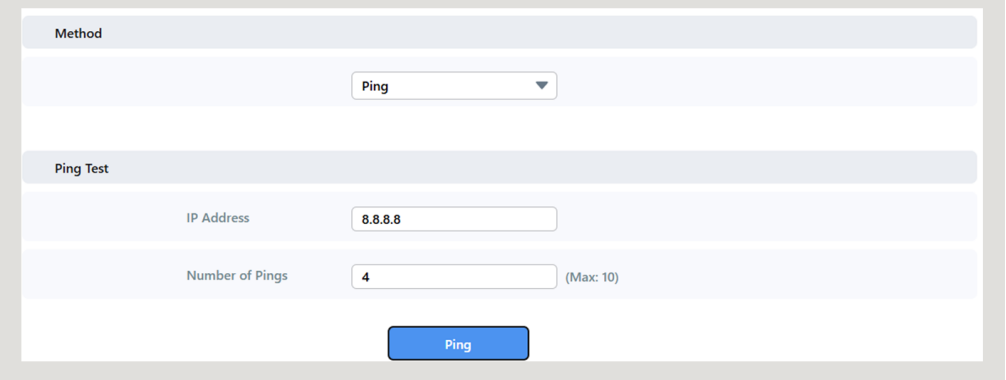
5.12 Network Tools

5.12.1 Network Analysis

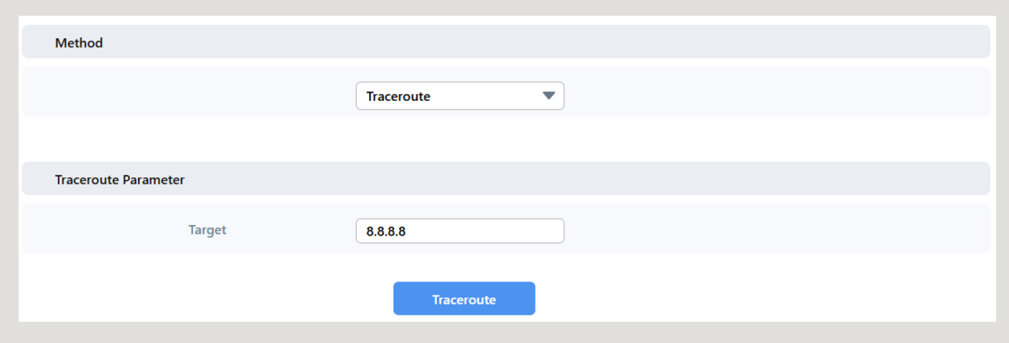
Network Analysis provides multiple built-in network test tools to help users troubleshoot, test connections, and perform diagnostic analysis of network connection status.

- Using **Network Analysis** tool:
  - (1) Click **Advanced** > **Network Tools** page
  - (2) Click **Network Analysis** tab

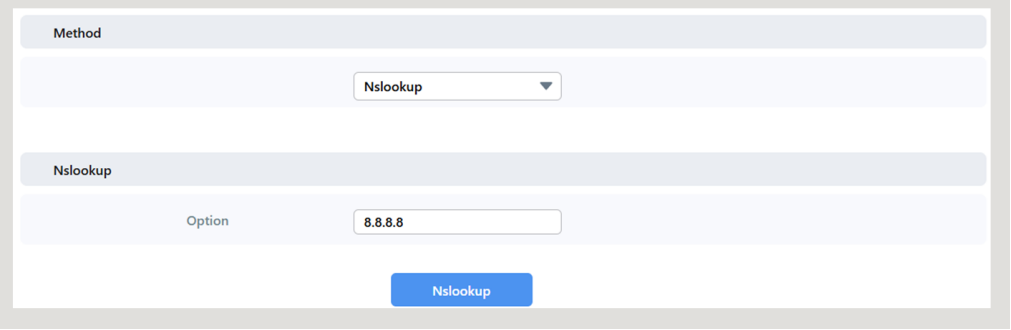
- Settings:
  - (1) Method:
    - **Ping**: Checks basic connection stability and latency with the target IP or host.
      - **IP Address**: Target IP address or domain name for testing.
      - **Number of Pings**: Number of packets to send (maximum 10).



- **Traceroute**: Traces each network node that packets pass through to reach the target host, helping identify bottlenecks or blocking points along the path.
  - **Target**: Enter the domain name or IP address to query.



- **Nslookup**: Queries domain name resolution records to confirm whether DNS services resolve properly.
  - **Options**: Enter the domain name or IP address to query.

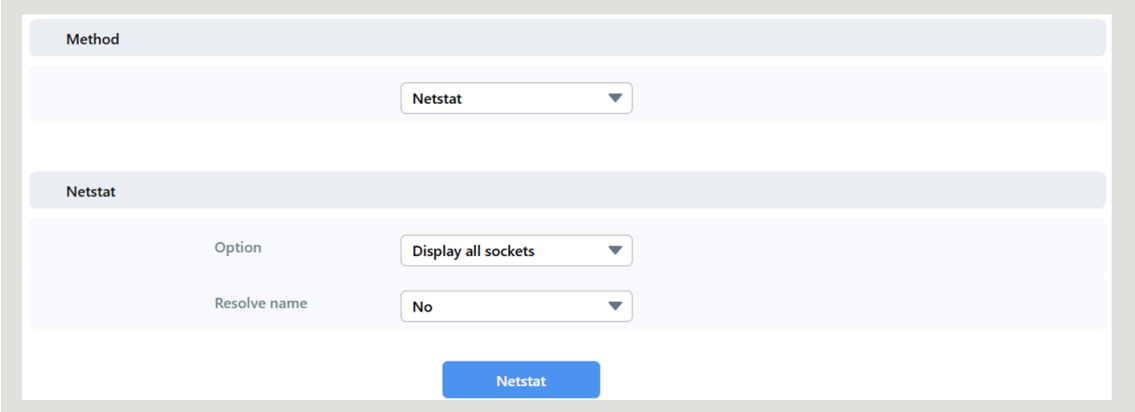


- **Netstat**: View real-time internal network connection status, service listening status, and routing table information of the router.
  - Option:
    - **Display all sockets**: Displays all network sockets in the current system (including established and listening TCP/UDP connections).
    - **TCP sockets**: Displays only current TCP protocol connections.

- **UDP sockets**: Displays only current UDP connection information.
- **RAW sockets**: Displays sockets using raw IP protocol layer packet processing.
- **UNIX sockets**: Displays internal UNIX domain sockets.
- **Display listening server sockets**: Displays only service port information currently listening for connections.
- **Display routing table**: Displays the current router routing table for checking forwarding paths and next-hop settings for each network segment.

› Resolve Name:

- **Yes**: Automatically translates IP addresses into host names for easier source device identification.
- **No**: Displays only IP addresses, suitable for advanced analysis and exact comparison.



5.12.2 WiFi Analysis

The Wi-Fi Analytics tool scans and analyzes Wi-Fi signal distribution and interference on each band in real time, helping users understand on-site wireless network quality and optimize channel configuration appropriately.

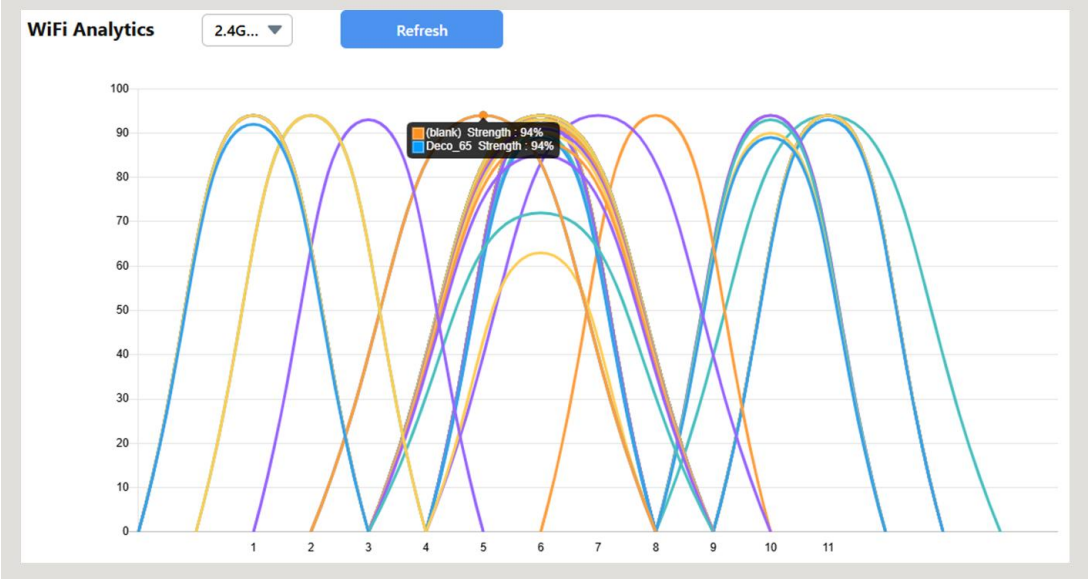
- Using **WiFi Analysis** tool:
  (1) Click **Advanced** > **Network Tools** page
  (2) Click **WiFi Analysis** tab

- Settings:
  (1) **2.4GHz / 5GHz / 6GHz** Band Selection: Users can select the band to analyze from the drop-down menu, and the system displays all detectable wireless signals in that band in the current environment in real time.
  (2) **Chart** Description:
    - **X Axis:** Channel Number / **Y Axis**: Signal Strength (dBm)

- Each colored curve: represents the signal coverage and strength of each Wi-Fi SSID.

※ Move the cursor over a curve to display the SSID name and current signal strength information. (Strength %)

(3) **Refresh**: Runs the scan again and updates the current real-time wireless environment.



Troubleshooting

Q1. What should I do if I forget the login password?

- Answer 1: Use the Forgot Password process on the login page and complete security question verification to reset the password.
- Answer 2: Press and hold the Reset button for 3 seconds to initialize the router, then log in with the default account and password to reset the device.

Q2. How do I add a Roamii node?

- Answer: Roamii devices shipped in the same package are pre-paired. Simply connect the second device to power, and it will automatically establish a Mesh backhaul connection with the main router.
  If the Roamii device to be added comes from a different package, connect it to power first, then press the Sync button on the new device and any existing Roamii device at the same time to pair them.

Q3. Can Roamii replace my modem?

- Answer: Roamii is not a modem and must be used with a separate modem device.

Q4. How many nodes can be added to one Roamii network?

- Answer: It is recommended that each Main Router connect to up to 5 Nodes. If using wireless backhaul (Wireless Backhaul), it is recommended to keep it within 2 layers (2 hops), for a better network experience.

Q5. Can Roamii interoperate with Mesh systems from other brands?

- Answer: Roamii supports pairing only with MSI Roamii devices from the same series to establish a Mesh network and cannot be integrated with Mesh systems from other brands.

Q6. Can multiple users jointly manage the same Roamii network?

- Answer: Anyone with the administrator account and password can log in through the MSI Router 2.0 app or Web GUI to manage the network.