4G LTE Mobile Wi-Fi
Model: WSMRMIFI

User Guide

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, Tenda reserves the right to make changes to the products without obligation to notify any person or organization of such revisions or changes. Tenda does not assume any liability that may occur due to the use or application of the product described herein. Every effort has been made in the preparation of this document to ensure
accuracy of the contents, but all statements, information and recommendations in this document do not constitute the warranty of any kind, express or implied.

INDEX

1. Get to Know Your Device

1.1 Overview

WSMRMIFI are designed as your reliable personal Wi-Fi hotspots.

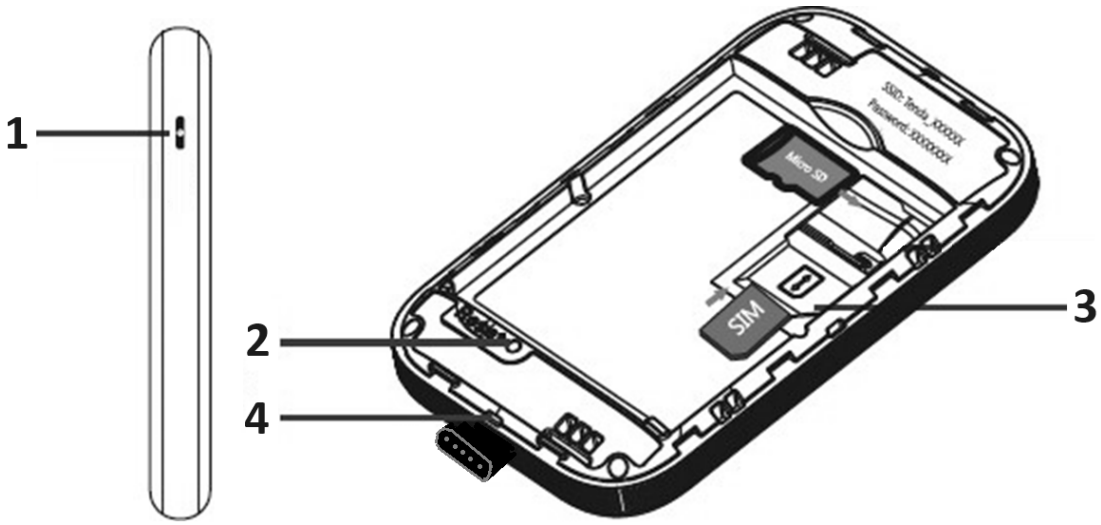
Just inserting a SIM card, you can enjoy fast 4G LTE network with your family and

friends. Please note, the device is set with the SIM PIN active with the unlock code

"1111"

Compact body with a large-capacity battery, the mobile Wi-Fi offers easy networking wherever you go. When the power is low, you can charge the battery with a micro USB cable connected to power supply devices such as a power adapter, laptop or portable charger. Even without a battery, when
the D are connected to such power supply devices with a micro USB cable, they can still be powered on for network connection.

Along with the basic operations achieved through the buttons and port, the devices also allow you to configure more functions on the web UI.



1.2 Buttons, slots and port

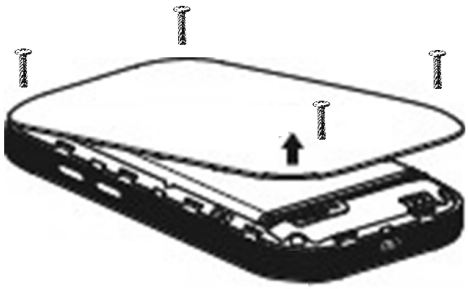
1) Power button.	Hold it for about 5 seconds to turn on/off the Hotspot.
2) Reset	Hold the button using a sharp object for about 6 seconds, and then release it when all LED indicators light up once and then light off. When the LED indicators light again, the Hotspot is restored to factory settings successfully.
3) SIM card slot	Insert your SIM card here.
4) Charging magnetic port	Used to charge the Hotspot,

2. Set up Internet Connection

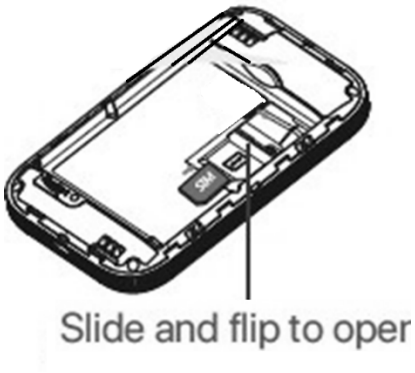
2.1 Connect the hotspot to the internet

To connect the hotspot to the internet, perform the following steps:

Step 1 Open from the lower left corner to remove the back cover.



Step 2 Slide and lift up the slot cover, insert a 3FF SIM card (an LTE, UMTS, or WCDMA SIM card) into the SIM card slot, and slide the cover back to lock.



Step 4 Install the battery.

Step 5 Restore the back cover.

Step 6 Hold the Power button till the LCD screen lights up (WSMRMIFI) to turn on the hotspot.

2.2 Connect clients to the hotspot

You can connect clients to the hotspot in wireless manner so that the clients can access the internet through the hotspot.

Connect a client to the hotspot in a wireless manner

Method One: Using the SSID and Wi-Fi Key

Step 1 Note the default SSID (Wi-Fi name) and Wi-Fi key (Wi-Fi password) on the LCD Screen.

Step 2 Select the Wi-Fi name of the hotspot on your client, and enter the password.

Method Two: Scanning the QR code

The Wi-Fi information QR code is shown on the web UI of the on the LCD screen

You can scan the QR code to connect your own client to the hotspot or take a picture of the QR code to share the hotspot with your family or friends.

Step 1 When the WSMRMIFI LCD screen is on, press the Power button twice to show the QR code.

Step 2 Scan the QR code using the Wi-Fi scan function of your mobile phone to connect to the wireless network of the hotspot.

3. Web Login and Logout

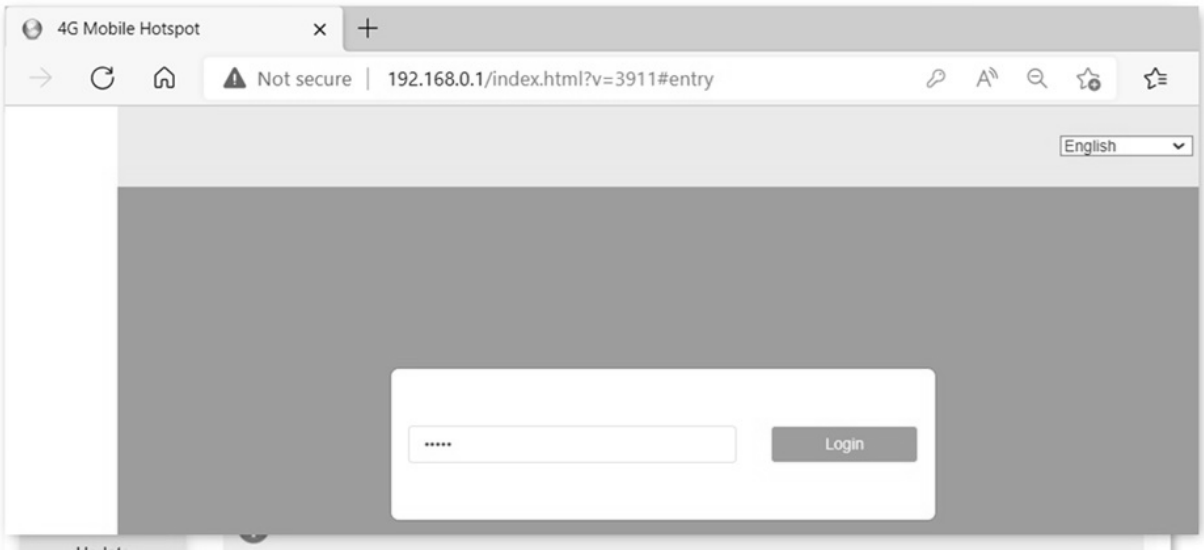
3.1 Log in to the web UI

After a client (such as a smartphone or a computer) is connected to the hotspot, you can start a web browser on the client to log in to the web UI (default IP address: 192.168.0.1) of the hotspot.

Step 1 Connect the client to the hotspot.

Step 2 Start a web browser on the client, and visit **192.168.0.1**.

Step 3 Enter password (**WhisperGig@!** by default) and click **Login**.



3.2 Log out of the web UI

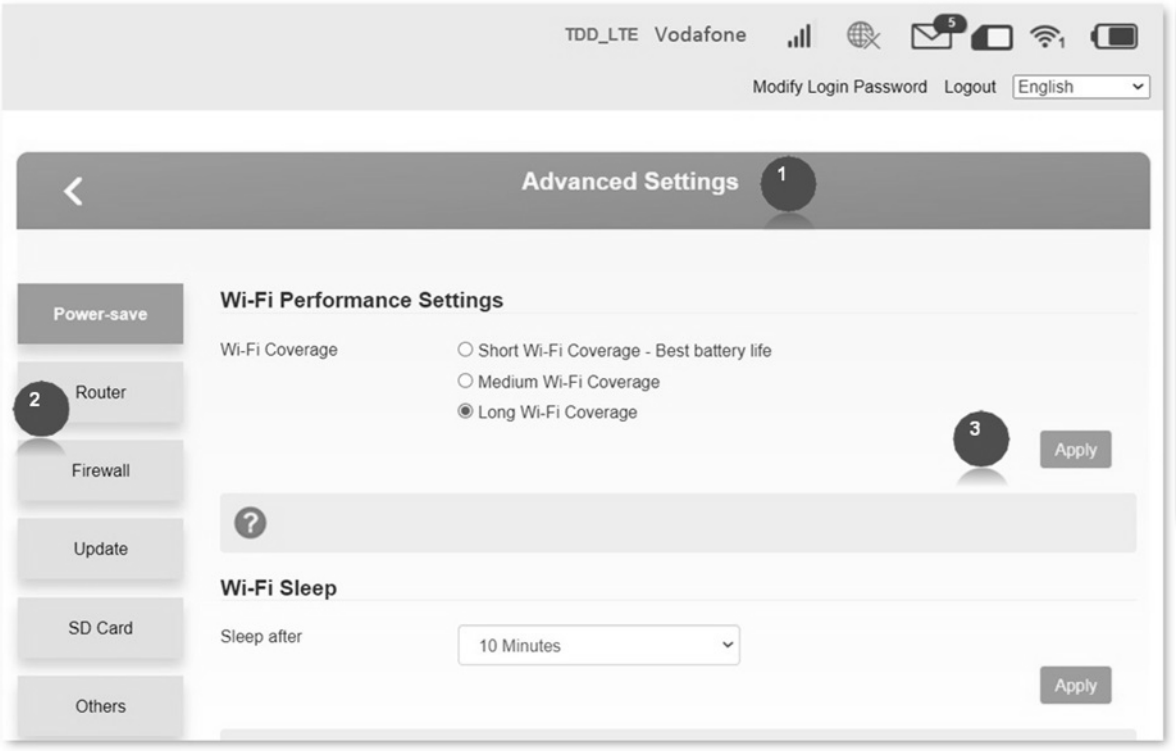
If you perform no operation on the web UI or no wireless client is communicating with the device within the specified **Wi-Fi Sleep** Time (configured at Advanced Settings > Power-save), the system logs you out.

You can log out by clicking **Logout** on the upper right corner of the web UI as well.

When you are logged out, the system does not save the current unsaved configurations. Therefore, it is recommended that you save the current configuration before logging out.

3.3 Web UI layout

The web UI consists of three sections, including the level-1 and level-2 navigation bars, and the configuration area. See the following figure.



No.	Name	Description
1	Level-1 navigation bar	They are used to display the function menu of the device. Users can select functions in the navigation bars and the configuration appears in the configuration area.
2	Level-2 navigation bar	
3	Configuration area	It is used to view or modify your configuration.

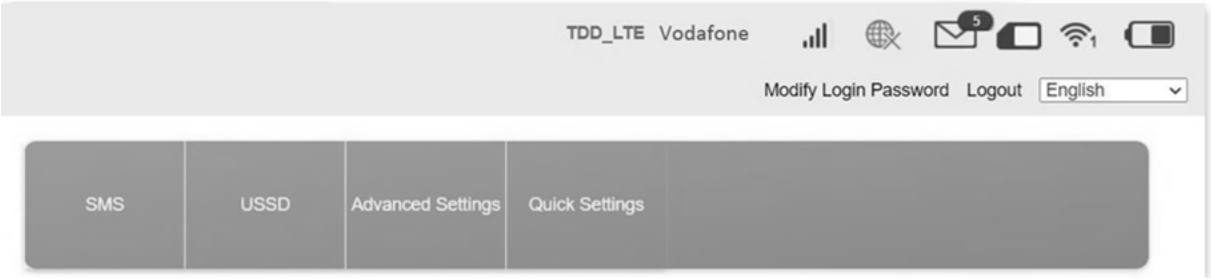
4. Quick Settings

Before moving on to other configurations, you need to configure the internet settings of the hotspot.

To quickly configure the settings, perform the following steps:

Step 1 Start a web browser on the client, and visit **192.168.0.1** to log in to the web UI.

Step 2 Choose **Quick Settings**.

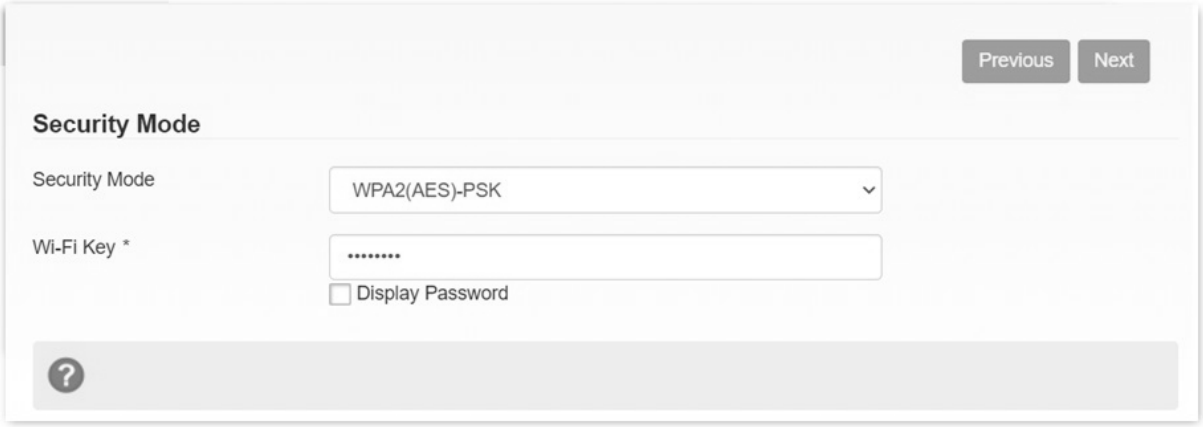


Step 3 Choose to configure APN settings automatically or manually, and click **Next**.

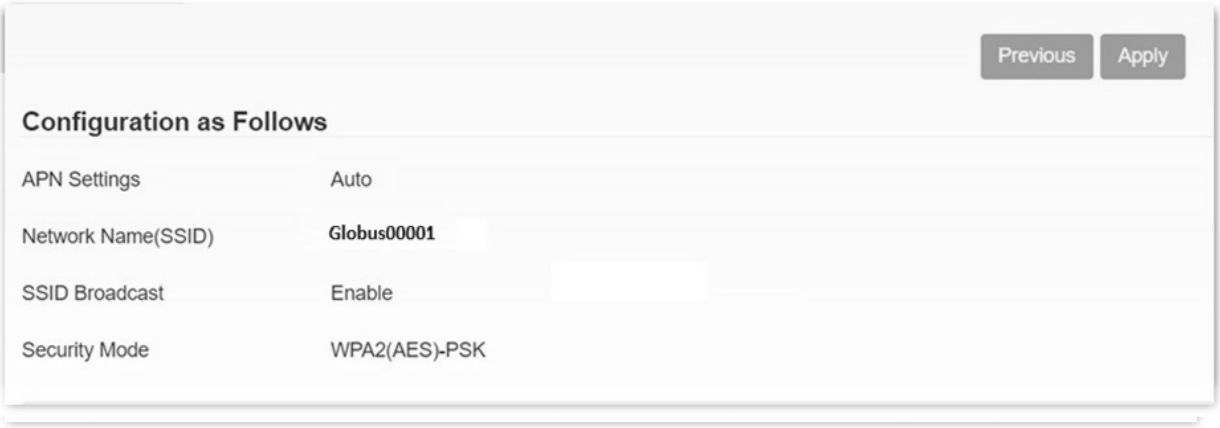
You can manually select an APN only after adding it and setting it as the default APN on the **Network Settings** > **APN** page. In this example, **Auto** is selected.

Step 4 Set **Network Name (SSID)** to a required Wi-Fi name, set **SSID Broadcast** to specify whether to broadcast the Wi-Fi name, and click **Next**.

Step 5 Select a security mode from the **Security Mode** drop-down list box, set **Wi-Fi Key** to the password of the Wi-Fi network, and click **Next**.



Step 6 Verify the settings and click **Apply**.



5. Home Page

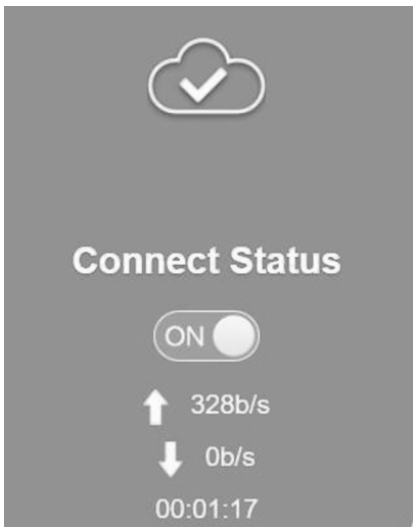
On the home page, you can view or set the following parameters and functions:

- Connect status
- Network settings
- Wi-Fi settings
- Connected devices
- Data management
- Status information

5.1 Connect status

Here, you can click the **ON/OFF** button to connect the hotspot to or disconnect the hotspot from the internet.

When the hotspot is connected to the internet, it displays the upload data, download data and the connection time. See the following figure.



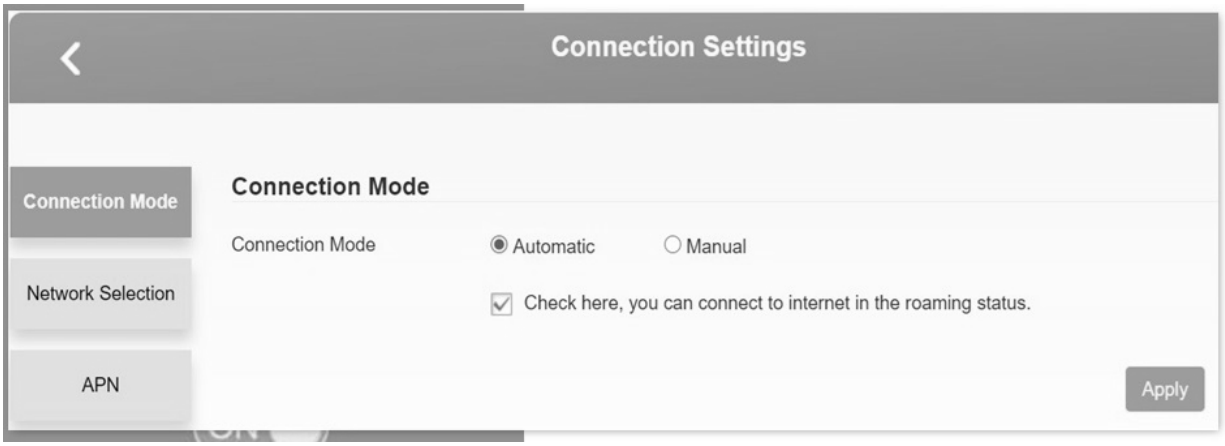
5.2 Network settings

This module enables you to configure the connection mode, select the mobile network to connect, and set APN profiles.

5.2.1 Connection mode

Here, you can specify whether the device connects to the internet automatically after it is powered on.

Navigate to **Network Settings** > **Connection Mode** to enter the page.



- To enable the hotspot to connect to the internet automatically after it is powered on, select **Automatic**, and click **Apply**.

The "**Success**" message appears, and the hotspot is connected to the internet.

.

- To disable the hotspot to connect to the internet automatically after it is powered on, select **Manual**, and click **Apply**.

The "**Success**" message appears, and the hotspot is disconnected from the internet.

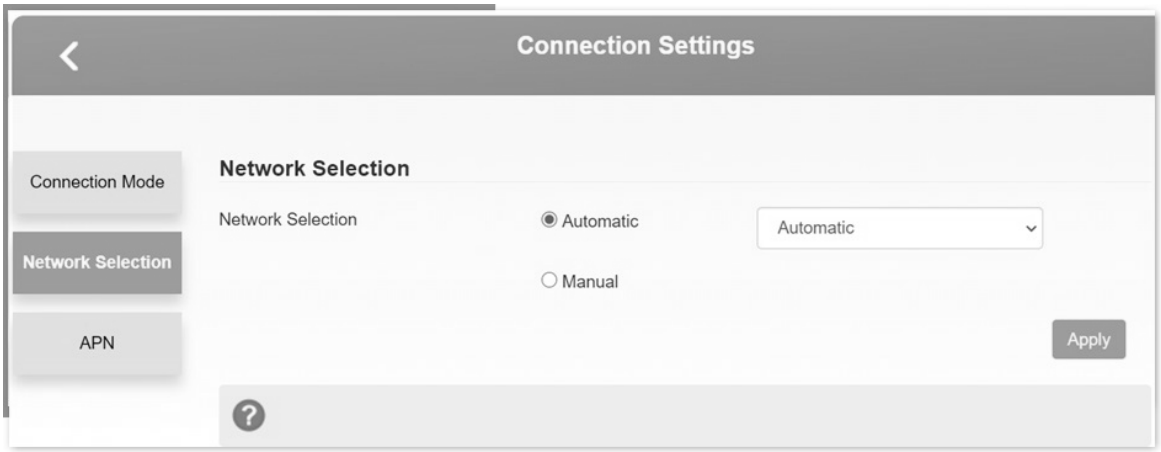
5.2.2 Network selection

This mobile Wi-Fi supports network selection modes of **Automatic**, **4G Only**, **3G Only**, and **Manual**. Navigate to **Network Settings** > **Network Selection** to enter the page.

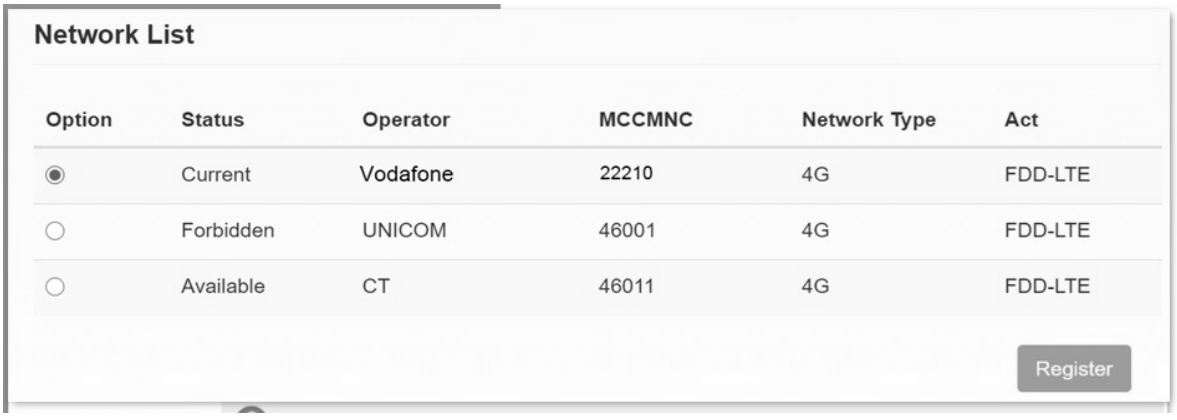
If your SIM card supports WCDMA, you can select **3G Only**.

If your SIM card supports FDD-LTE or TDD-LTE, you can select **4G Only**.

If you are not clear about that, **Automatic** is recommended. The hotspot will automatically establish internet connection when it is started.



If you want to manually select a mobile network, select **Manual**, click **Search**, select an available mobile network from the network list, and click **Register**.



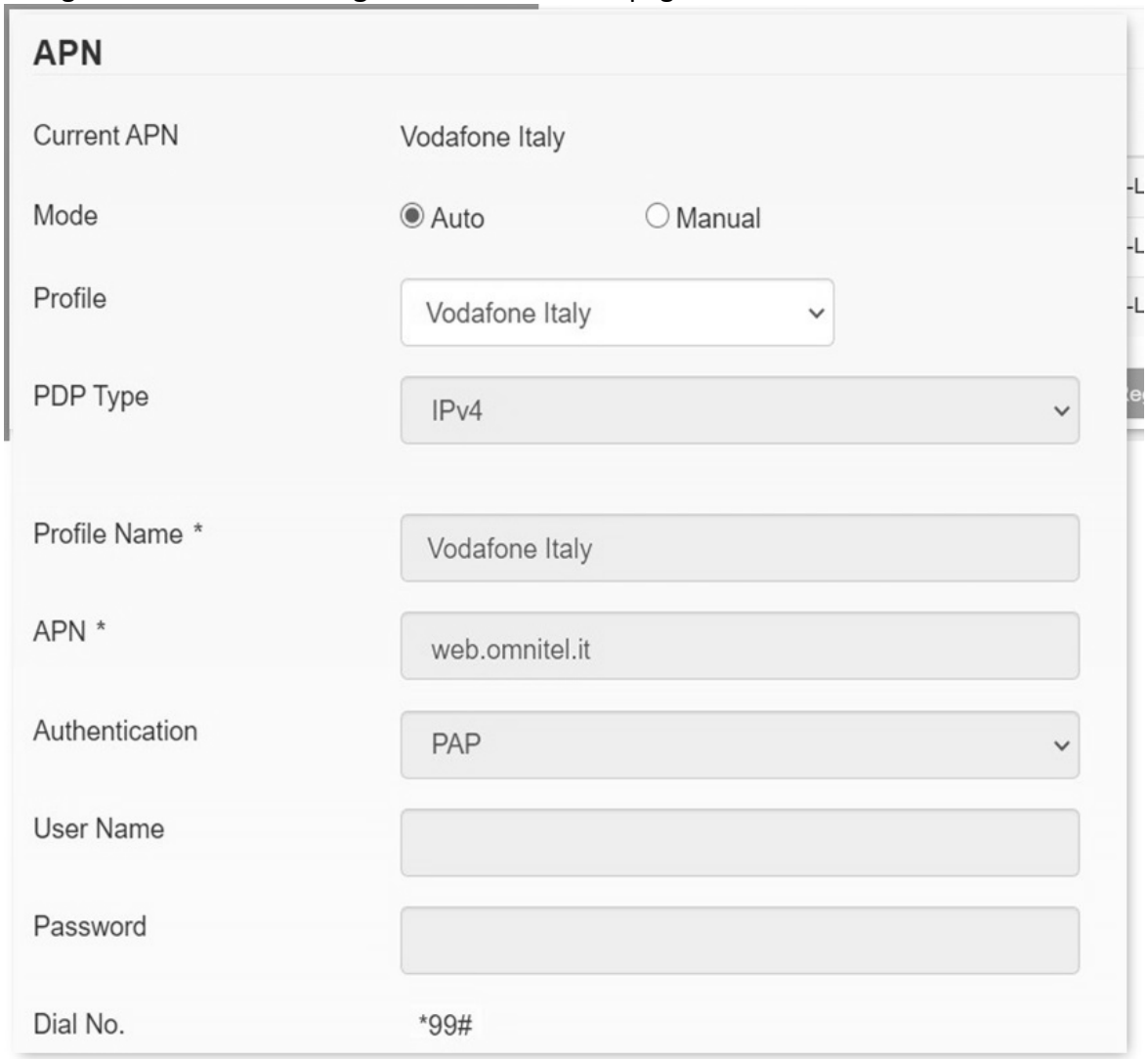
5.2.3 APN

An APN (Access Point Name) is a gateway between a cellular network and the internet. A mobile device making a data connection must be configured with an APN to present to the network

carrier.

When the device already received 4G signal but cannot be connected to the internet properly, in this case, you need to configure the APN dial-up information of the carrier. The APN information can be obtained by consulting the carrier's service personnel.

Navigate to **Network Settings** > **APN** to enter the page.



Parameter	Description
Current APN	It specifies the currently used APN.

Parameter	Description
Mode	It specifies whether to select an APN automatically or manually. If your ISP provides APN settings, select **Manual**; otherwise, select **Auto**.
Profile	It specifies the profile (ISP) of the current APN.
Profile Name	It specifies the name of the profile. You can click **Add New** and add another profile as required.
PDP Type	It specifies the Packet Data Protocol (PDP) type of the APN, including IPv4, IPv6, and IPv4v6.
APN	It specifies the Access Point Name. Only digits, uppercase and lowercase letters, dots (.), and hyphens (-) are allowed in an APN name. An APN name cannot start with or end with a dot or hyphen.
Authentication	It specifies the authentication mode specified by your ISP for the APN. • **PAP**: Password Authentication Protocol (PAP) provides a simple method without encryption for the peer to establish its identity using a 2-way handshake. • **CHAP**: Challenge-Handshake Authentication Protocol (CHAP) is used to periodically verify the identity of the peer using a 3-way handshake.
User Name	It specifies the user name for authentication.
Password	It specifies the password for authentication.
Dial No.	It specifies the dial-up number for mobile networking.

You can select one profile and set the corresponding parameters. If you need to add a new APN profile, perform the following steps:

Step 1 Choose **Network Settings** > **APN**.

Step 2 Select **Manual** and click **Add New**.

Step 3 Set the corresponding parameters based on the APN information provided by your ISP.

Step 4 Click **Apply**.

After adding or selecting an APN profile, click **Set as default** to set the profile as the default one. APN profile is available for manual configuration during quick settings only after being set as a default APN.

5.3 Wi-Fi settings

Before more Wi-Fi settings, you can enable or disable the **Wi-Fi Switch** and **Multi SSID Switch** first.

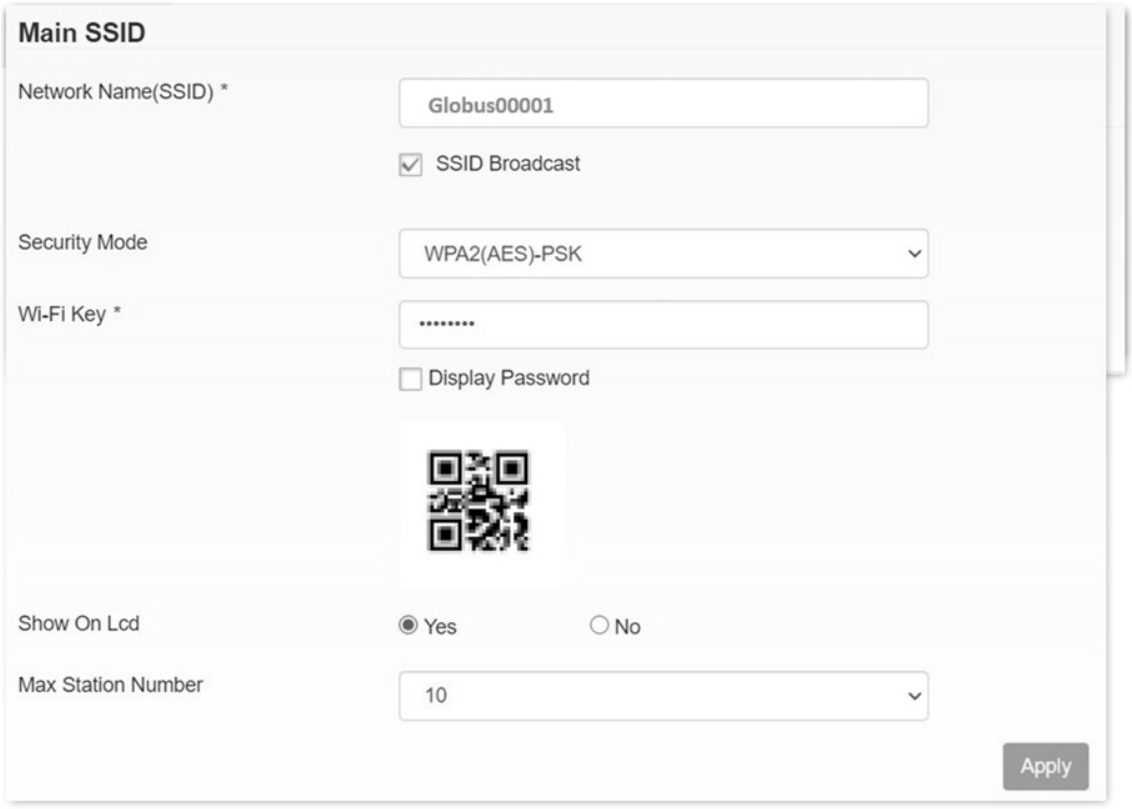
Wi-Fi Switch: It is used to enable or disable the wireless hotspot.

Multi SSID Switch: It is used to enable or disable a guest SSID besides the main SSID.

5.3.1 Main SSID

Here, you can set parameters of the **Main SSID**.

Click **Wi-Fi Settings** > **Main SSID** to enter the page.



Parameter	Description
Network Name (SSID)	It specifies the Wi-Fi name of the device. A maximum of 32 characters are allowed in a Wi-Fi name. Only the following characters are allowed: • Digits • Uppercase and lowercase letters • Space

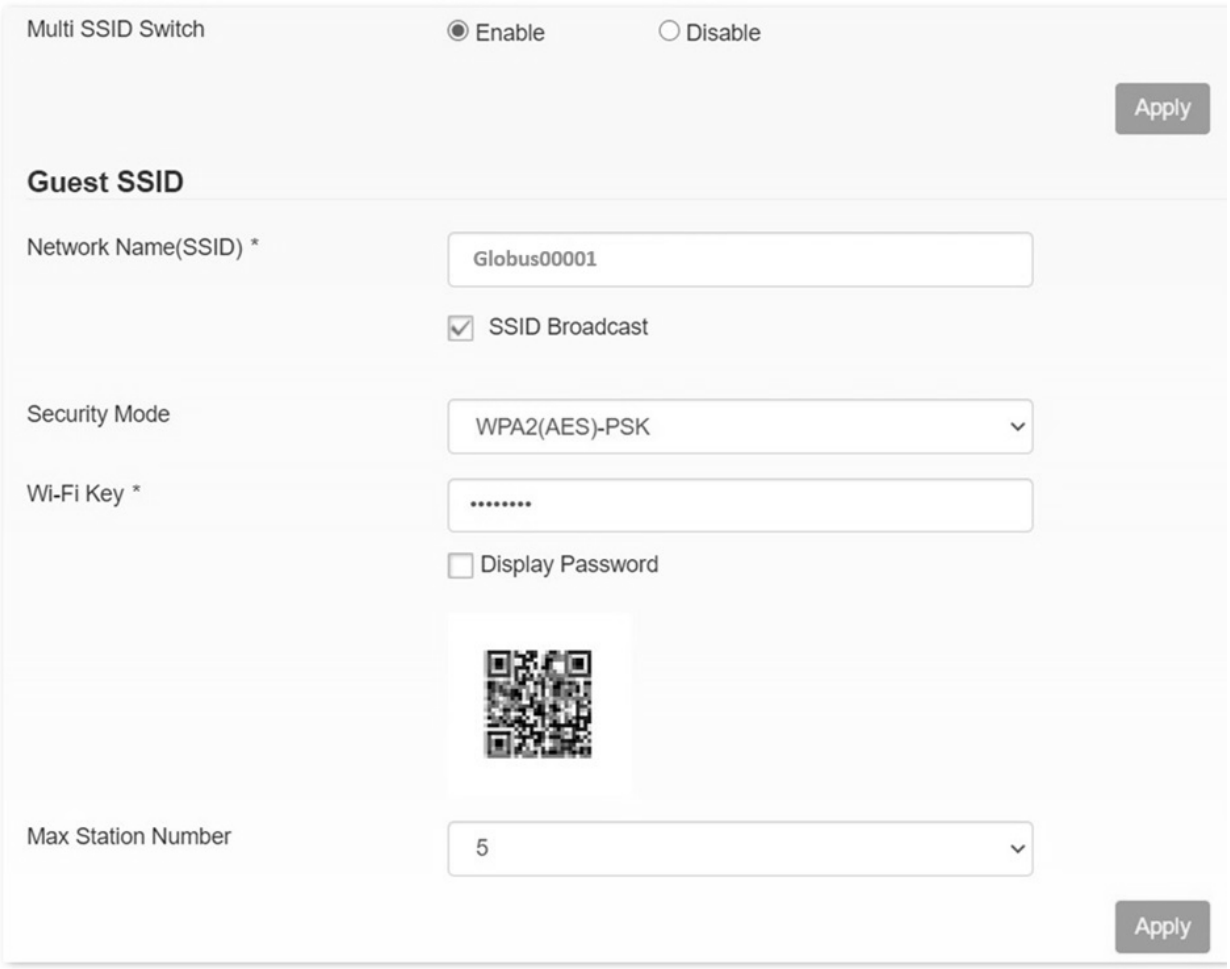
Parameter	Description
	• ! # ( ) + - . / % = ? @ ^ _ { | } ~ A Wi-Fi name cannot start or end with a space.
SSID Broadcast	It specifies whether to broadcast the Wi-Fi name of the device. If the Wi-Fi name is not broadcast, a wireless client cannot detect it. To connect the wireless client to the device, you must manually enter the Wi-Fi name on the client.
Security Mode	It specifies the security mode of the Wi-Fi network. • **OPEN**: No authentication or encryption is performed. In this mode, private information may be intercepted by unauthorized individuals. Therefore, it is not recommended. • **WPA2(AES)-PSK**: WPA2-PSK is used for authentication, which is the more secure version of WPA-PSK based on the 802.11i standard. AES is used for encryption. • **WPA-PSK/WPA2-PSK**: WPA-PSK or WPA2-PSK is used for authentication, where WPA2-PSK is the more secure version of WPA-PSK based on the 802.11i standard.
Wi-Fi Key	It specifies the password corresponding to the selected security mode. Only the following characters are allowed: • Digits • Uppercase and lowercase letters • ! # ( ) + - . / % = ? @ ^ _ { | } ~
Display Password	It specifies whether to display the password in plain text.
QR Code	You can scan the QR code using the Wi-Fi scan function of your mobile phone (as an example) to connect to the Wi-Fi.
Show On Lcd	It specifies whether to display the **SSID** and **Wi-Fi Key** on the LCD screen (only for WSMRMIFI). When you select **Yes**, the **SSID** and **Wi-Fi Key** will show on the LCD screen. When you select **No**, the **SSID** and **Wi-Fi Key** will not show on the LCD screen.
Max Station Number	It specifies the maximum number of wireless clients allowed to connect to the device. By default, it is set to **10**. When **Multi SSID Switch** is enabled, this parameter is changed to **5** automatically.

5.3.2 Guest SSID

When the **Multi SSID Switch** is enabled, you can set parameters of the **Guest SSID**.

In this case, you can press the **Power** button for three times to show the **Guest SSID** and corresponding **Wi-Fi Key**.

Click **Wi-Fi Settings** > **Guest SSID** to enter the page.



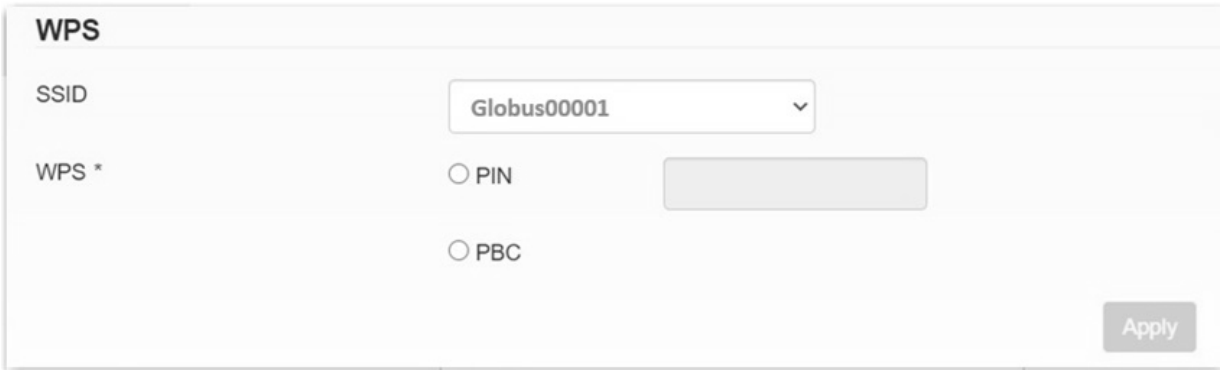
To configure the guest SSID, please refer to the parameter description of the main SSID above.

5.3.3 WPS

WPS (Wi-Fi Protected Setup) is a standard that allows users to set up a wireless network in an easy and secure way without specific configuration, such as: SSID, security mode and password.

If you have a WPS-supported device (such as Android phones or tablets), you can connect your device to the mobile Wi-Fi through two methods: **PIN** and **PBC** (Push Button Configuration).

Click **Wi-Fi Settings** > **WPS** to enter the page.



Through the PIN

This mode requires a PIN code generated by the client.

Step 1 Enable the WPS function of the client.

Step 2 Obtain the PIN code generated by the client.

Step 3 Log in to the web UI of the device.

Step 4 Choose **Wi-Fi Settings** > **WPS**.

Step 5 Select **PIN** for **WPS**, and enter the PIN code in the **PIN** text box.

Step 6 Click **Apply**.

Through the PBC

Step 1 Perform either of the following operations:

- Hold down the **WPS** button for 3 seconds.
- Log in to the web UI of the device, choose **Wi-Fi Settings** > **WPS**, select **PBC** for **WPS**, and click **Apply**.

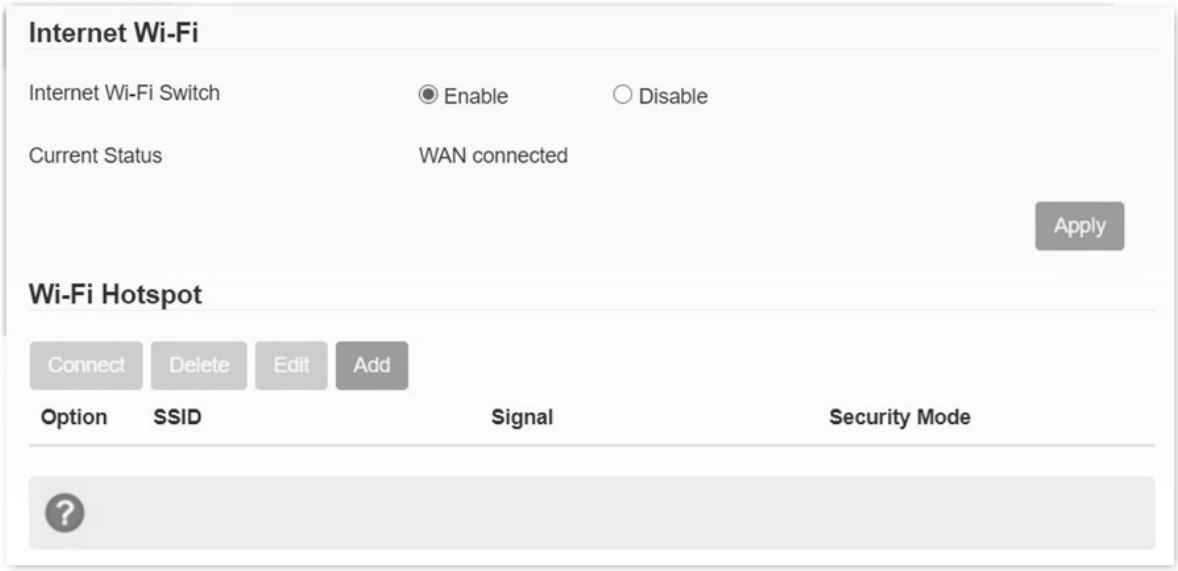
Step 2 Within 2 minutes after the previous step, enable the WPS function of the client.

After the WPS negotiation, your device will be automatically connected to the wireless network of the mobile Wi-Fi.

5.3.4 Internet Wi-Fi

On this page, you can connect the mobile Wi-Fi to an upstream Wi-Fi hotspot available in the network. This function helps you to save the mobile data of your SIM card.

Click **Wi-Fi Settings** > **Internet Wi-Fi** to enter the page.



Connect to a Wi-Fi hotspot

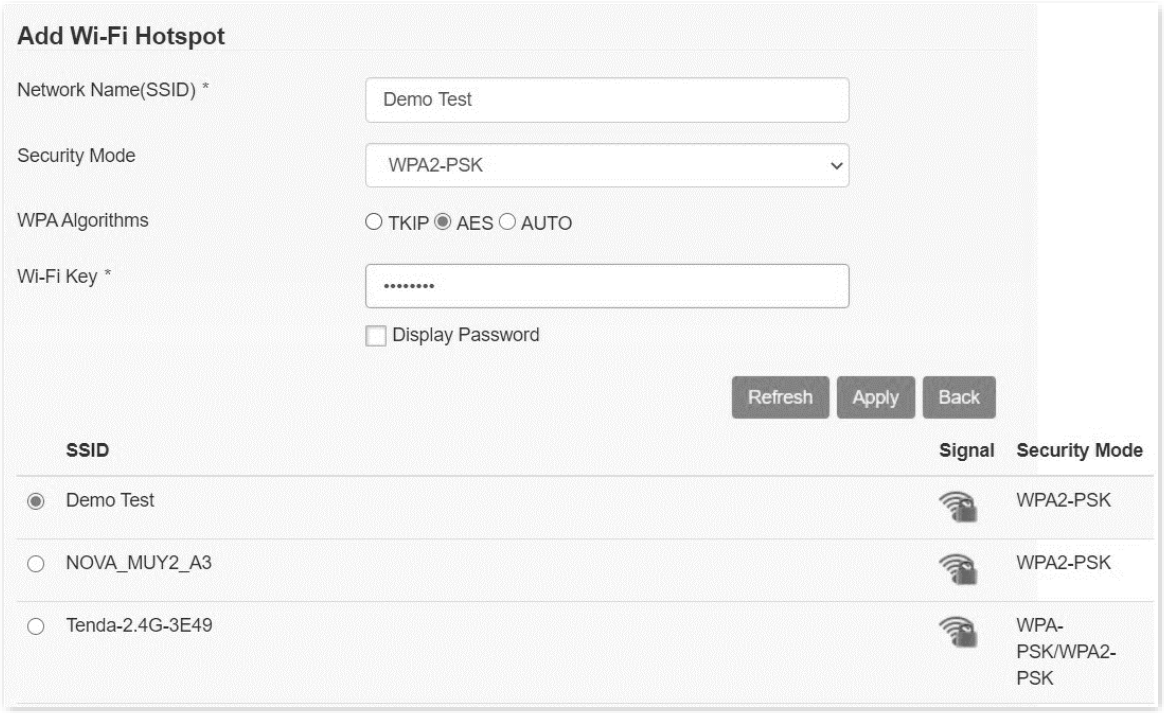
Step 1 Choose **Wi-Fi Settings** > **Internet Wi-Fi** to enter the configuration page.

Step 2 Enable **Internet Wi-Fi Switch**, and click **Apply**. “WAN connected” appears as the current status.

Step 3 Add a Wi-Fi Hotspot.

1. Click **Add** in the Wi-Fi Hotspot module, then the device starts scanning Wi-Fi hotspots.

2. After scanning, select one SSID in the SSID list, which is **Demo Test** in this example.
3. Select a **Security Mode** and **WPA Algorithm**, enter the **Wi-Fi Key**, and click **Apply**.

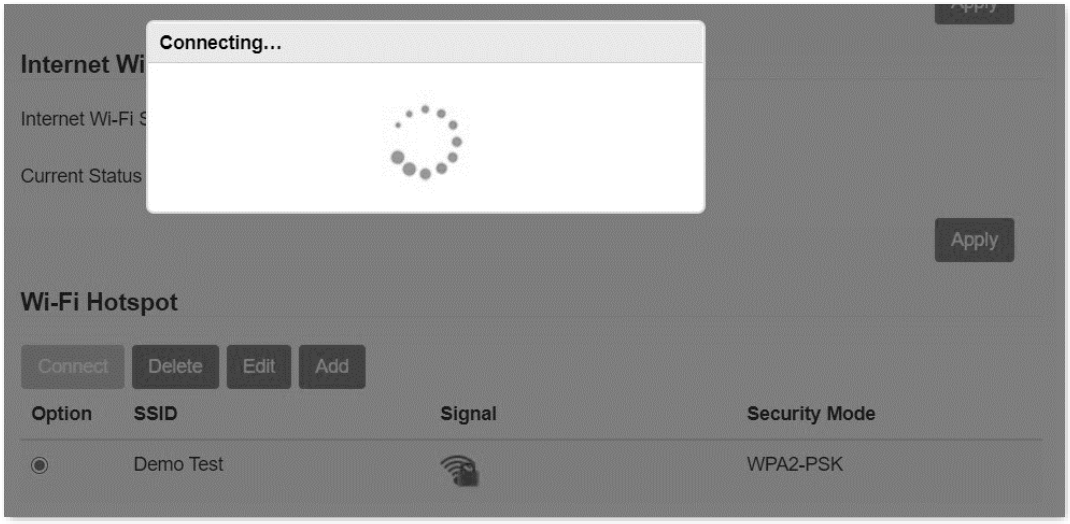


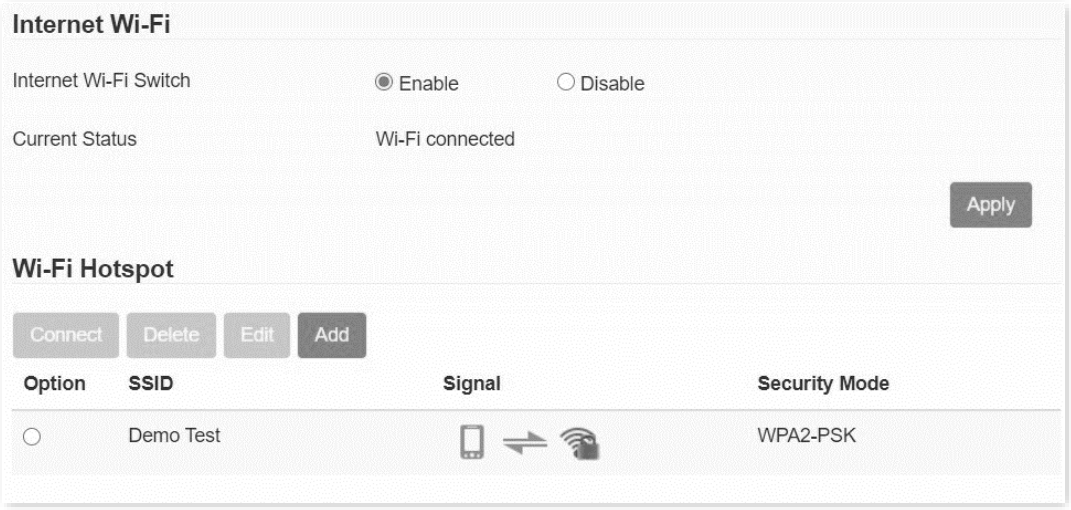
Step 4 Connect to the Wi-Fi hotspot.

(1) Select the SSID you want to connect.

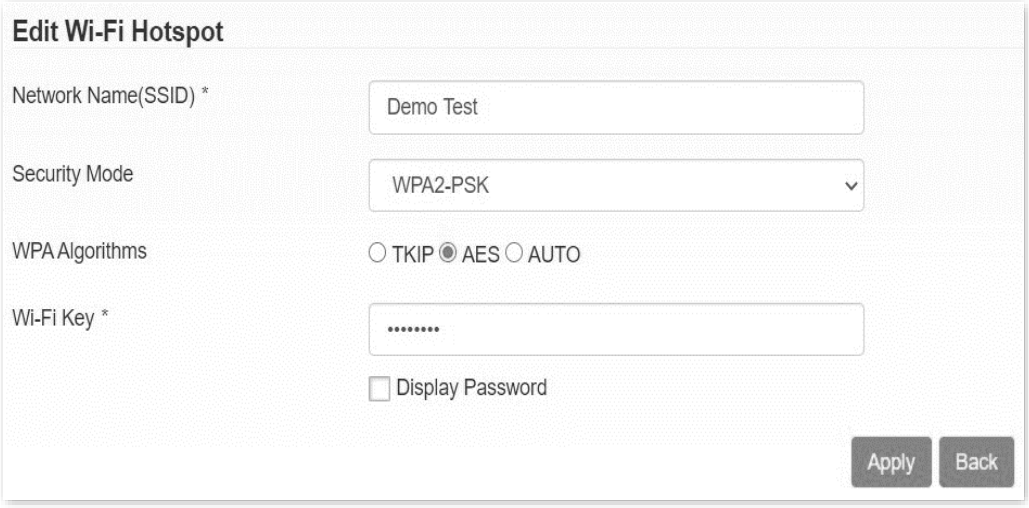
(2) Click **Connect** to connect the mobile Wi-Fi to the Wi-Fi hotspot.

When the **Current Status** becomes **Wi-Fi connected**, the mobile Wi-Fi is connected to the Wi-Fi hotspot.



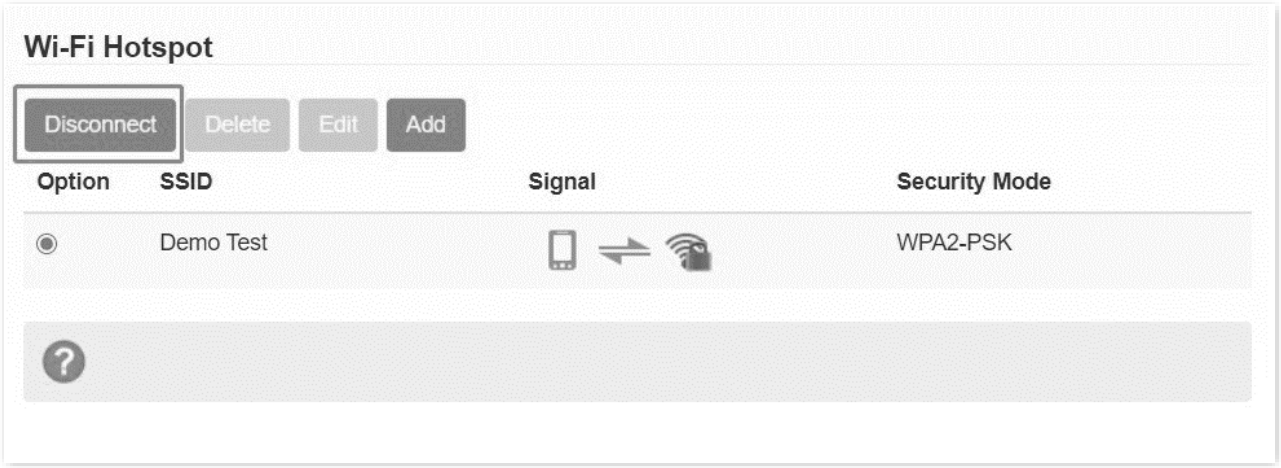


If the **Wi-Fi Key** you entered in Step 3 is incorrect, you can select the SSID and click **Edit** to revise the Wi-Fi Key for connection.

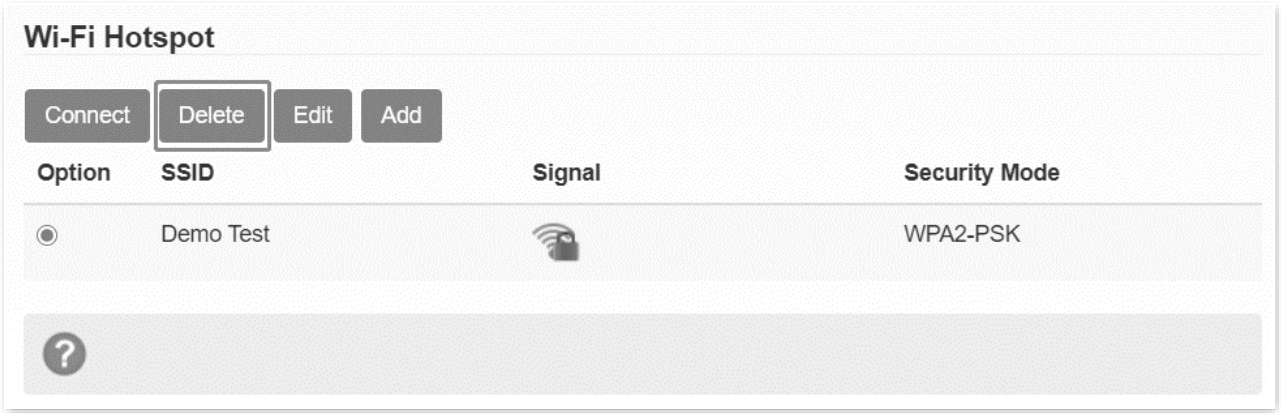


Disconnect from a Wi-Fi hotspot

You can select the connected SSID, and click **Disconnect** to disconnect the mobile Wi-Fi from the Wi-Fi hotspot.

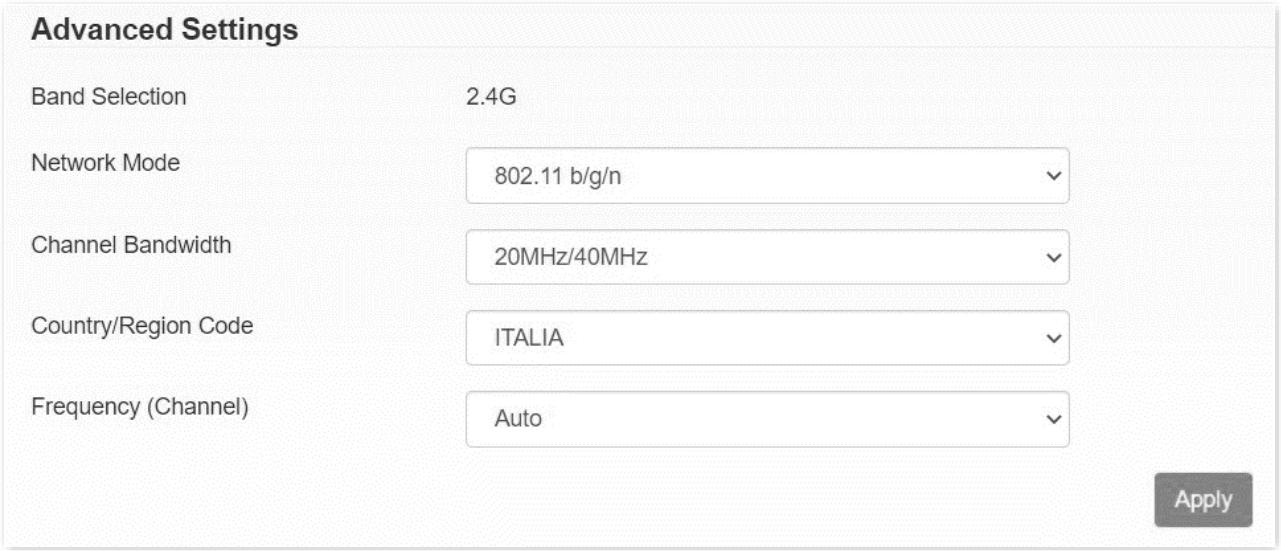


After the SSID is disconnected, you are allowed to delete the SSID from the list.



5.3.5 Advanced settings

On this page, you can configure the advanced Wi-Fi settings of the hotspot. Click **Wi-Fi Settings** > **Advanced Settings** to enter the page.

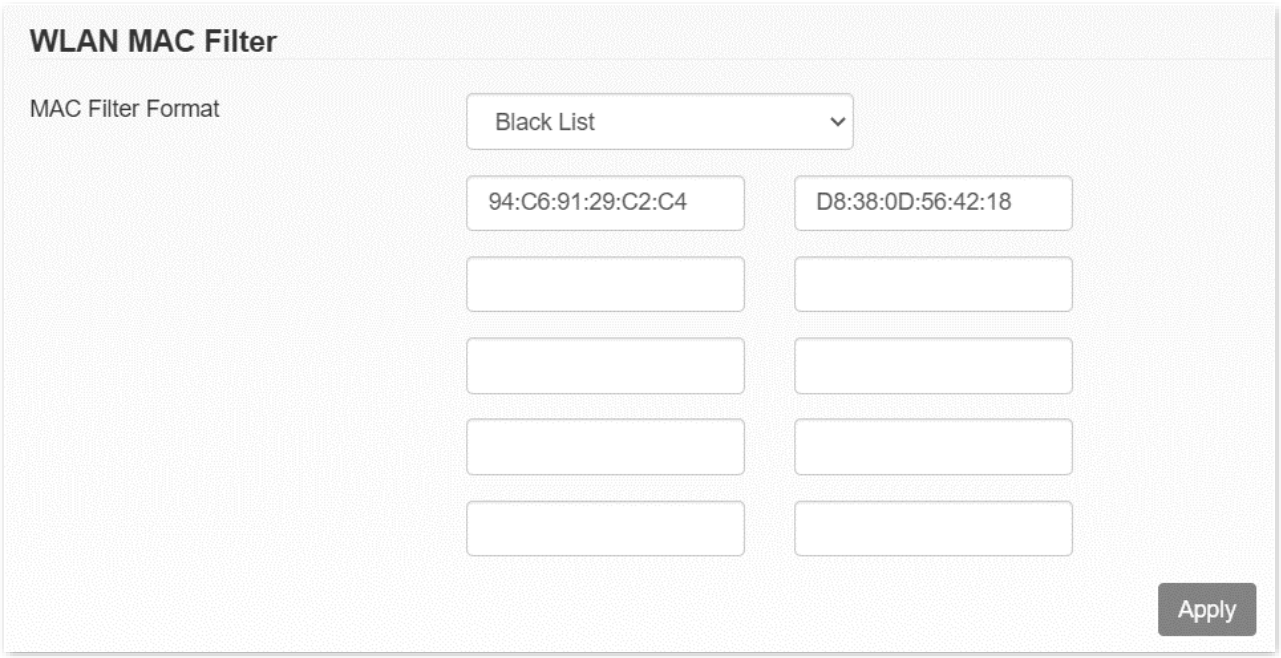


Parameter	Description
Band Selection	It specifies the wireless band of the hotspot's SSID.
Network Mode	It specifies the wireless network standards supported by the hotspot. Only the wireless clients compliant with the selected standards can connect to the hotspot.
Channel Bandwidth	It specifies the bandwidth of the operating channel of the hotspot.
Country/Region Code	It specifies the country or region where the hotspot is used.
Frequency (Channel)	It specifies the operating frequency and channel of the hotspot. The options vary according to the selected country or region. **Auto** is recommended to maximize wireless network transmission and coverage of the hotspot.

After the configuration, click **Apply** for the new settings to take effect. After the settings are applied, wireless clients will be reconnected to the device.

5.3.6 WLAN MAC filter

On this page, you can set a white list or a black list for some MAC addresses. Click **Wi-Fi Settings** > **WLAN MAC Filter** to enter the page.



Parameter	Description
MAC Filter Format	It specifies the MAC filter rules. • **Ruleless**: The WLAN MAC filter is disabled. • **White List**: Only allow clients in the white list to connect to the hotspot using the WLAN. • **Black List**: Only deny clients in the white list to connect to the hotspot using the WLAN.

Example of configuring WLAN MAC Filter

Network requirement

Only procurement personnel are allowed to connect to the Wi-Fi network of the hotspot.

Solution

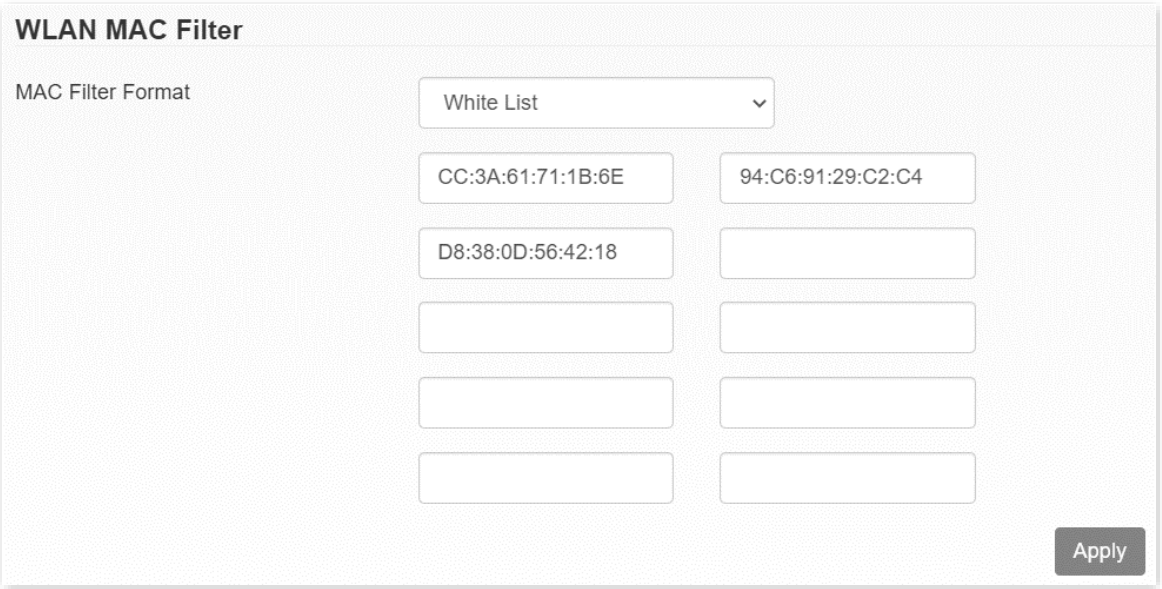
The WLAN MAC Filter function can meet this requirement. Assume that the MAC addresses of computers belonging to procurement personnel are CC:3A:61:71:1B:6E, 94:C6:91:29:C2:C4 and D8:38:0D:56:42:18.

Configuration procedures

Step 1 Click **Wi-Fi Settings** > **WLAN MAC Filter**.

Step 2 Set **MAC Filter Format** to **White List**.

Step 3 Enter the MAC addresses of procurement personnel's computers, which are **CC:3A:61:71:1B:6E**, **94:C6:91:29:C2:C4** and **D8:38:0D:56:42:18** in this example, and click **Apply**.

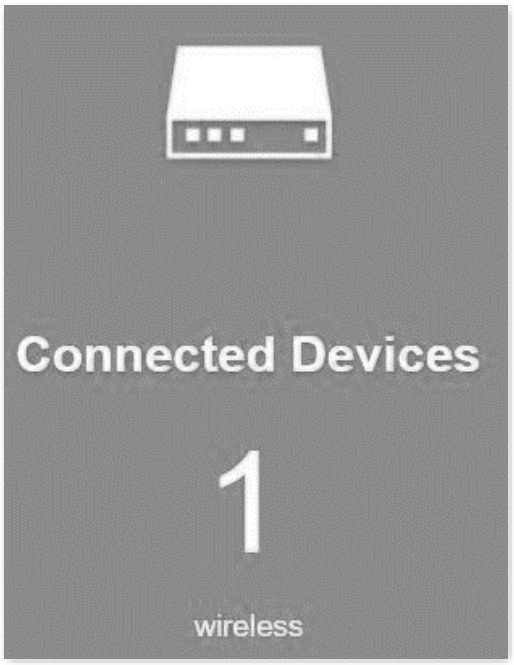


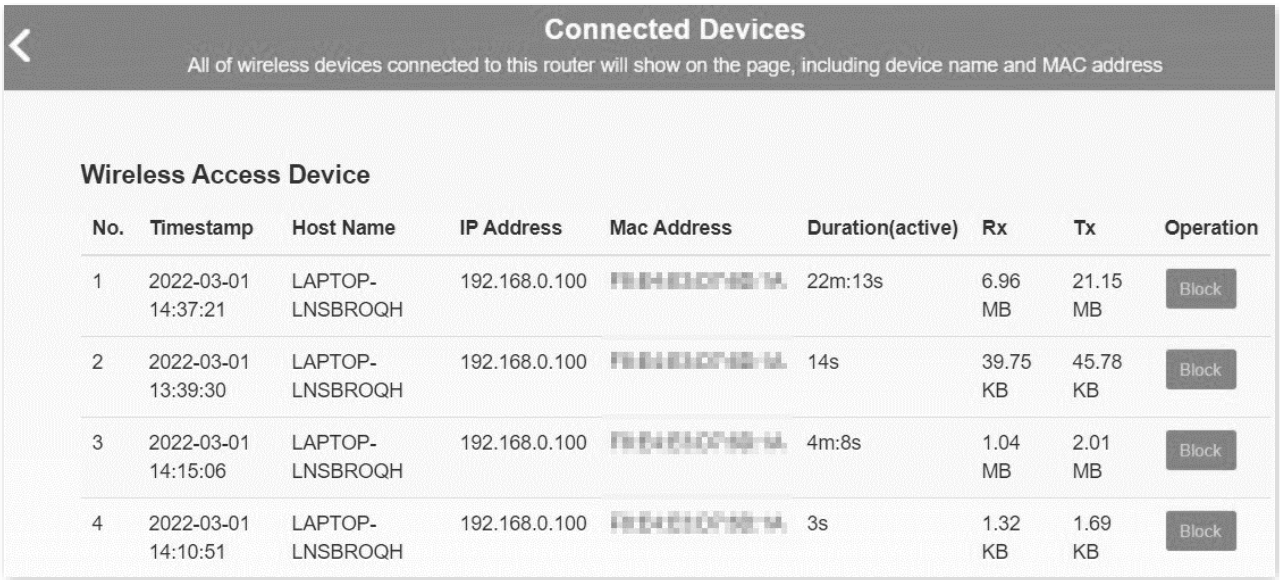
Verification

Only clients with the above-mentioned MAC addresses can connect to the Wi-Fi network of the hotspot while other clients are blocked.

5.4 Connected devices

On this page, you can view the basic information of the connected devices, or block some connected devices.





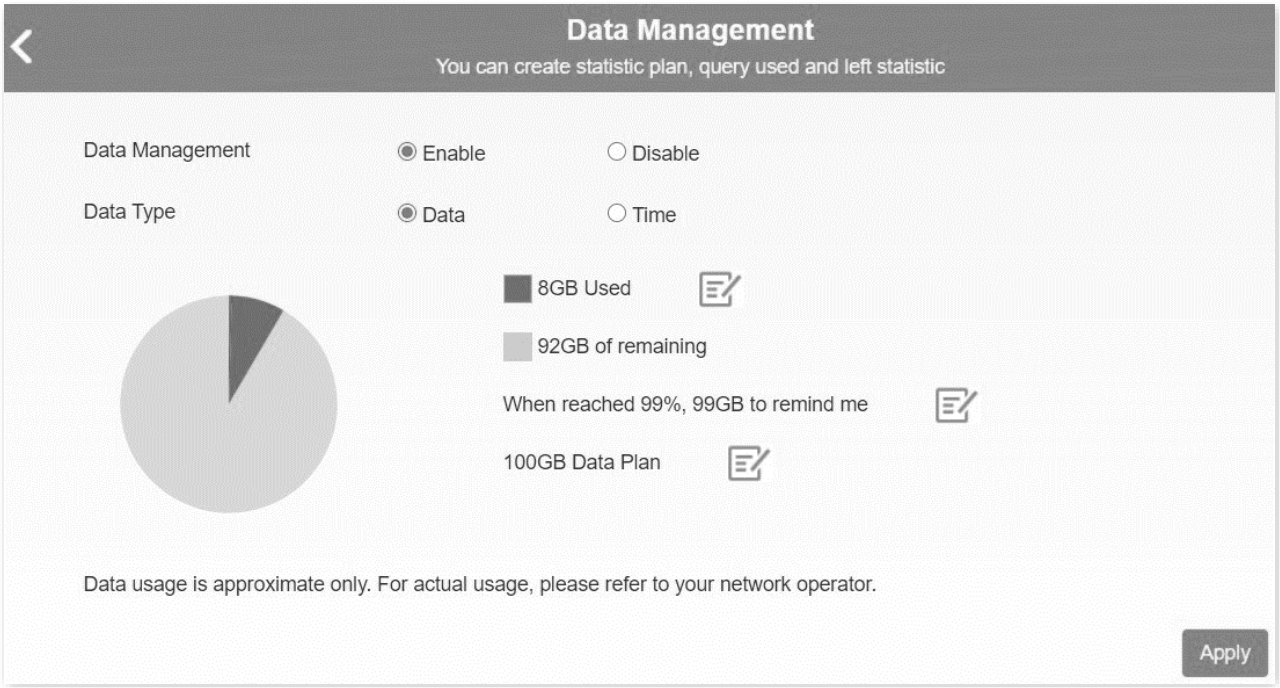
Parameter	Description
Connected Devices (1 wireless)	It specifies the number of currently connected devices and the connection type.

Parameter	Description
Timestamp	It specifies the time when a client device is connected to the hotspot.
Duration	It specifies the connection duration of the client device to the hotspot.
Rx/Tx	It specifies the received/transmitted data between the client device and the hotspot.
Operation	You can click the **Block** button to block certain device from connecting to the hotspot.

5.5 Data management

On this page, you can set data use limits and the reminding condition (by **Data** or **Time**). Click **Statistics** > **Not set, click Settings** to enter the page.

The operation is similar to what you usually do on your mobile phone. The parameters you set will also appear on the LCD screen (WSMRMIFI).



Set data use limit

Step 1 Set **Data Management** to **Enable**, and click **Apply**.

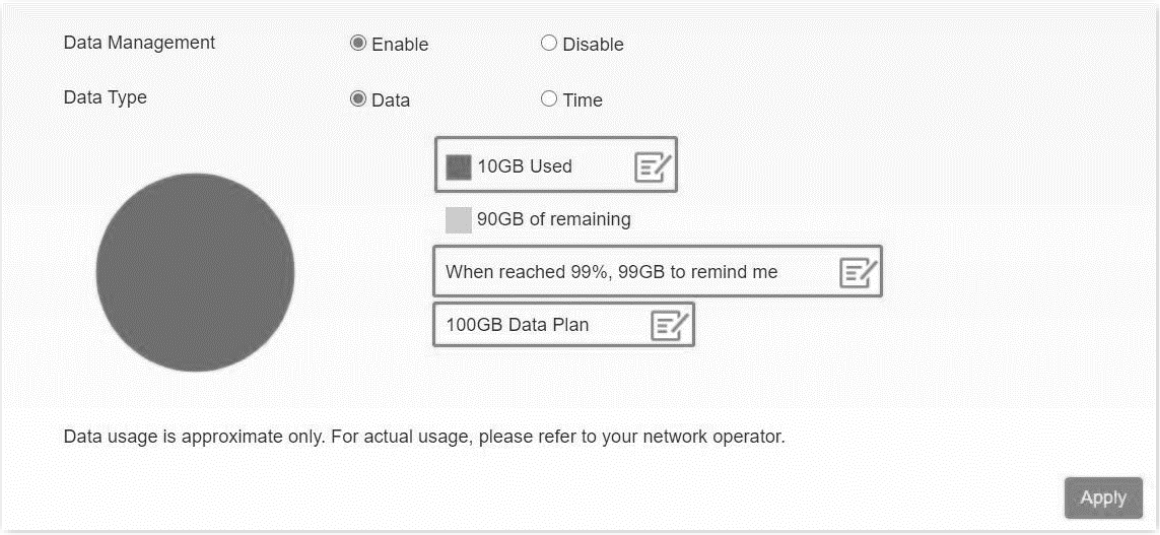
Step 2 Select a **Data Type**, such as **Data**.

Step 3 Click the upper to fill in the used data, such as **10 GB**.

Step 4 Click the lower to set the total data plan, such as **100 GB**.

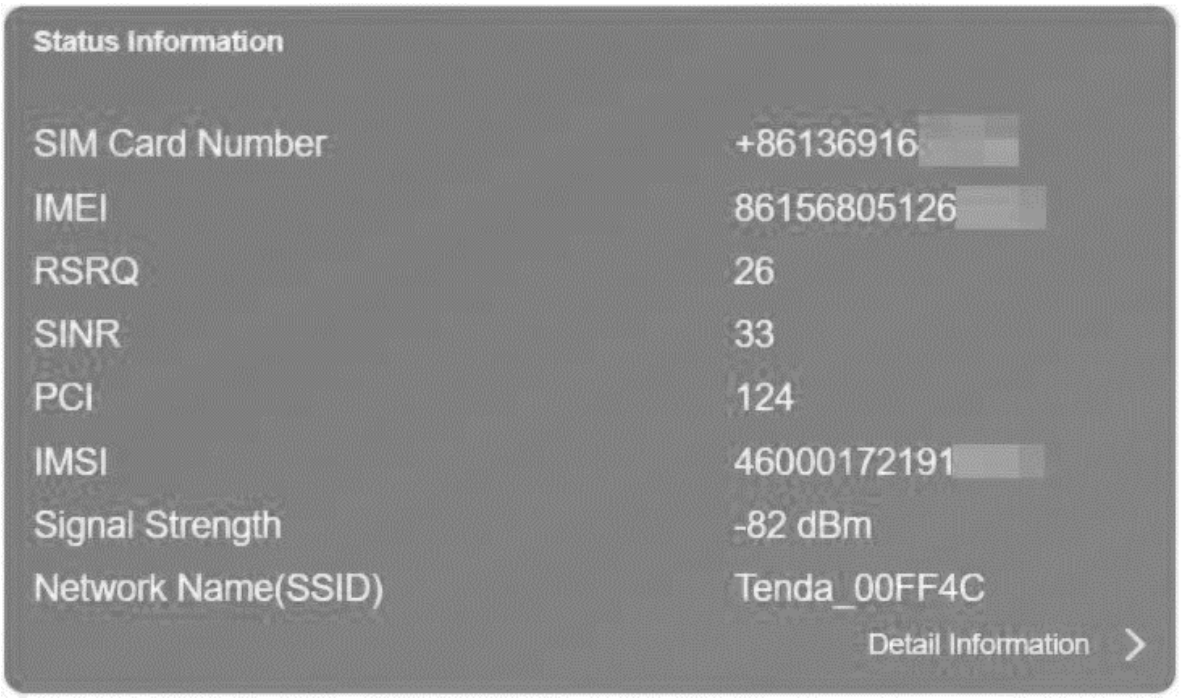
Step 5 Click the middle to set the percent upon which the reminding takes effect, such as **99%**.

Step 6 Click **Apply**.


Data Management
Enable
Disable
Data Type
Data
Time
10GB Used
90GB of remaining
When reached 99%, 99GB to remind me
100GB Data Plan
Data usage is approximate only. For actual usage, please refer to your network operator.
Apply

5.6 Status information

Here, you can view status information of the SIM card and relevant wireless network. You can click **Detail Information** to check more details.



Parameter	Description
SIM Card Number	It specifies the mobile number (Format: *Country code* + *Mobile number*) of the SIM card.
IMEI	It specifies the International Mobile Equipment Identity (IMEI) of the device.
IMSI	It specifies the International Mobile Subscriber Identity (IMSI) of the device.
Signal Strength	It specifies the signal strength of the connected mobile network. Stronger signal strength (-60 dBm is better than -70 dBm) leads to better networking experience.
Network Name (SSID)	It specifies the Wi-Fi name (SSID) of the device. The default Wi-Fi name is Tenda_*XXXXXX*, where *XXXXXX* indicates the last six characters of the MAC address of the device.
Max Access Number	It specifies the maximum number of clients that can be connected to the device.
Wi-Fi Coverage	It specifies the Wi-Fi range setting of the device, including **short Wi-Fi coverage**, **medium Wi-Fi coverage** and **long Wi-Fi coverage**. You can change this parameter on Advanced Settings > Power-save.

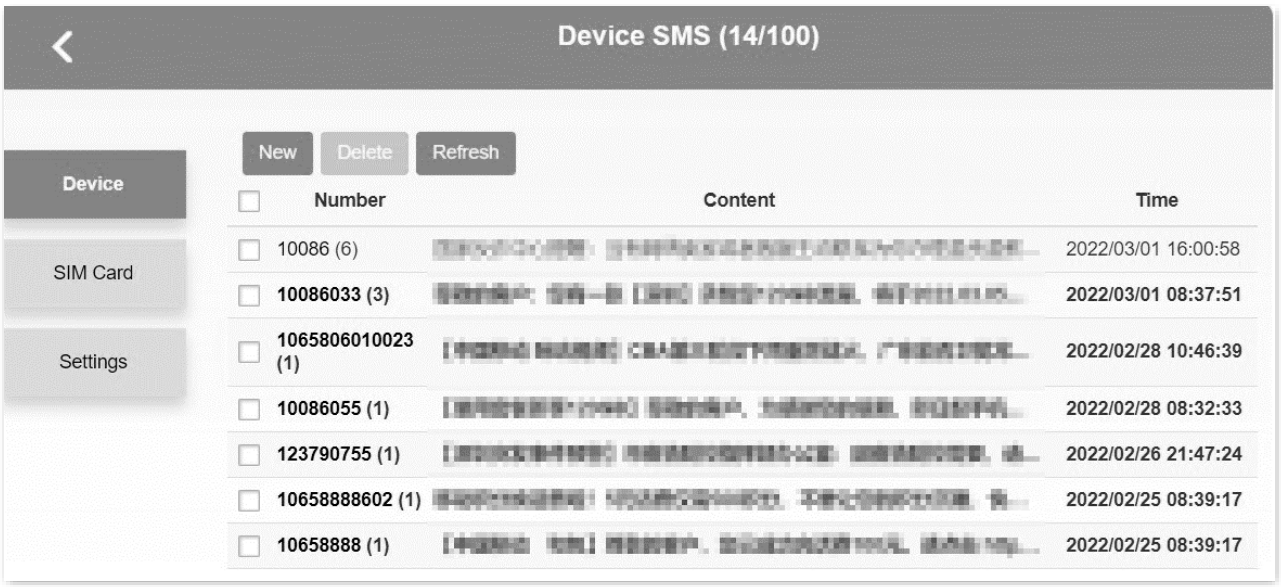
Parameter	Description
LAN Domain	It specifies the LAN domain of the device. The LAN domain maintains a connection between domain names and IP addresses. You can access this web UI by clicking the shortcut corresponding to the LAN domain on the desktop of your computer.
IP Address	It specifies the LAN IP address of the device.
WAN IP Address	It specifies the WAN IP address of the device.
Software Version	It specifies the software version of the device.
Hardware Version	It specifies the hardware version of the device.
RSRP	It specifies the Reference Signal Received Power (RSRP) of the device.
RSRQ	It specifies the Reference Signal Received Quality (RSRQ) of the device.
RSSI	It specifies the Received Signal Strength Indicator (RSSI) of the device. It helps the device to connect to a wireless network with stronger signal.
SINR	It specifies the Signal to Interference plus Noise Ratio of the device. The larger the number, the stronger the signal.
Cell ID	It specifies the Cell ID of the SIM card, which helps locate the device.
PCI	It specifies the Physical Cell ID of the device.
Band	It specifies the operating band upon which the wireless network operates.

6. SMS

This module enables you to manage SMS messages and configure SMS settings.

6.1 Device SMS

On this page, you can view, write, delete and refresh SMS messages received by the mobile Wi-Fi. Click **SMS** > **Device** to enter the page.



Parameter	Description
New	It is used to create a new SMS message.
Delete	It is used to delete SMS messages.
Refresh	It is used to update the SMS message list.

View and reply to messages

Step 1 Click an SMS message to enter a dialog box.

Step 2 You can scroll up and down to see all the history messages between the contact and you.

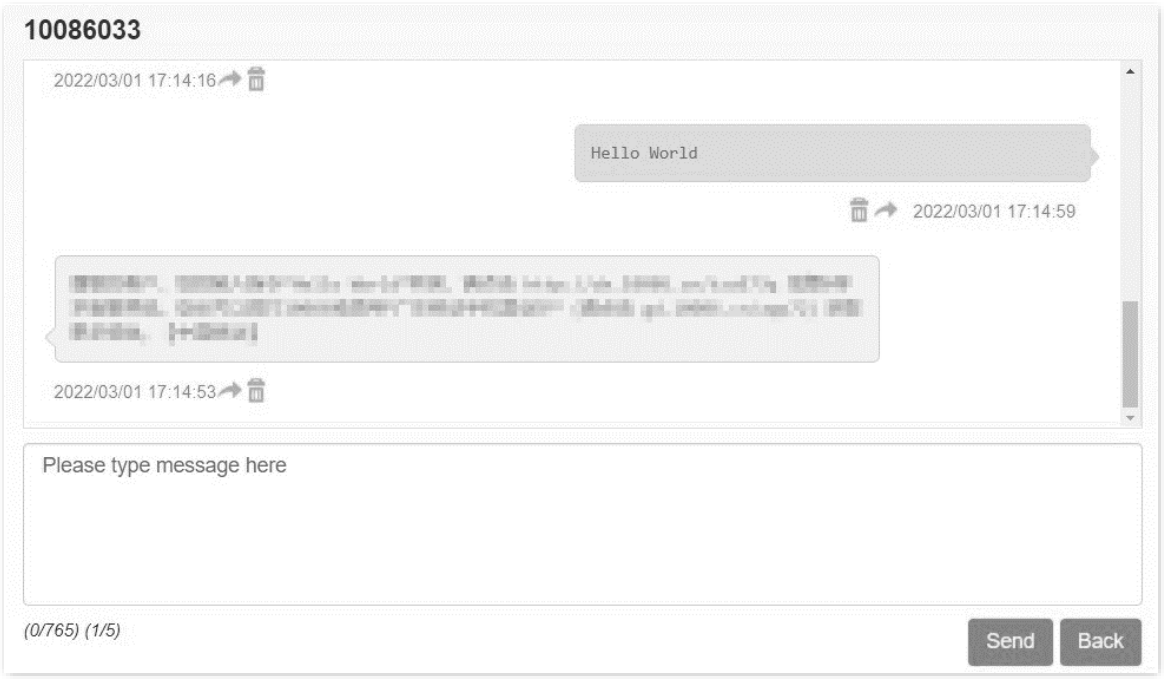
Step 3 To reply, type a message (such as **Hello World**) in the text box, and click **Send**. If you click **Back** instead, the message will be saved as a draft.

Write a new SMS message

Step 1 Click **New** to enter a dialog box.

Step 2 Enter the mobile numbers of the recipients (You can choose 5 contacts at most.).

Step 3 Type a message (such as **Hello World**) in the text box, and click **Send**. If you click **Back** instead, the message will be saved as a draft.

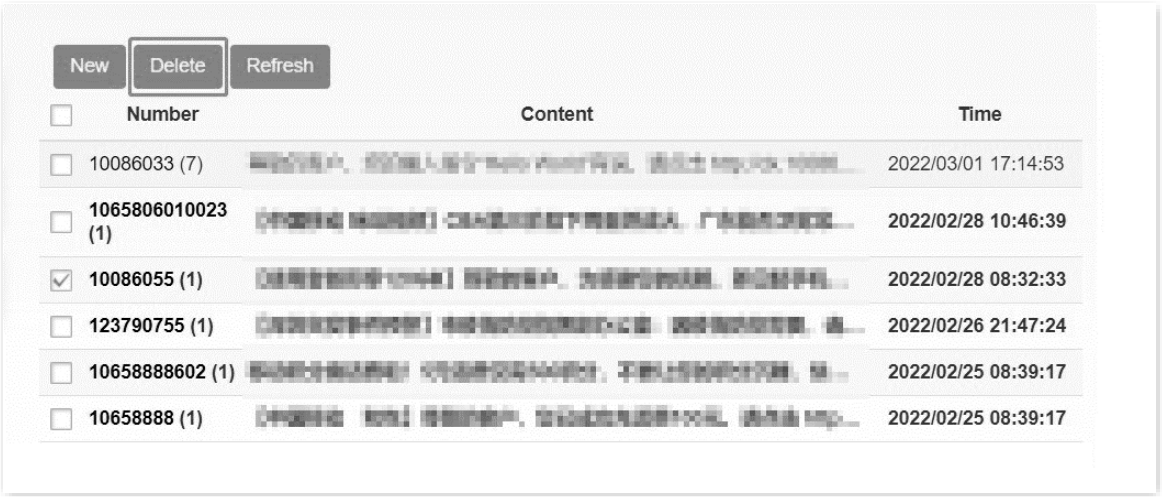


If the delivery report function on the SMS Settings module is enabled, a delivery message appears in the lower-right corner as well.

Delete an SMS message

Step 1 Select the SMS message.

Step 2 Click **Delete**.



Step 3 Click **Yes** in the dialog box that appears.

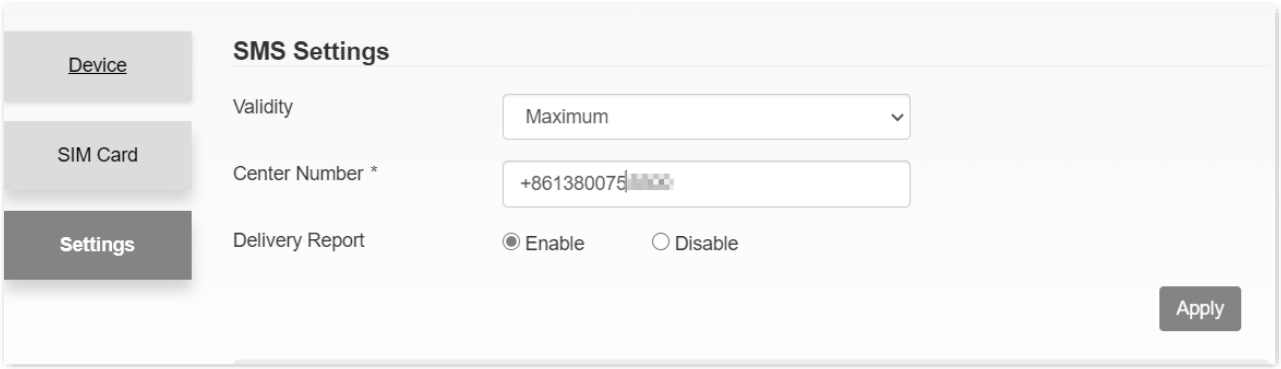
6.2 SIM SMS

On this page, you can view and delete the SMS messages stored in the SIM card. The operations are same as those of the **Device SMS**.

Click **SMS** > **SIM Card** to enter the page.

6.3 SMS settings

On this page, you can configure the SMS settings. Click **SMS** > **Settings** to enter the page.

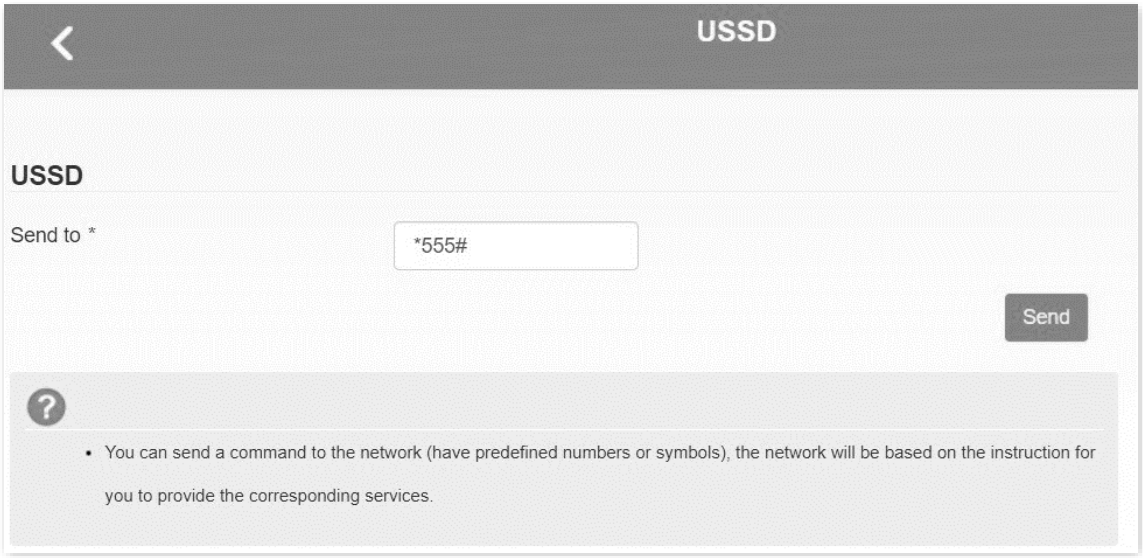


Parameter	Description
Validity	It specifies the validity period of outgoing SMS messages. The options include: • **12 Hours**: It indicates that SMS messages are retained for only 12 hours. • **1 Day**: It indicates that SMS messages are retained for only 1 day. • **1 Week**: It indicates that SMS messages are retained for only 1 week. • **Maximum**: It indicates that SMS messages are retained as long as the memory of the device has available space. Generally, the memory can store a maximum of 500 SMS messages. This number depends on the memory capacity of the device as well as the sizes of SMS messages.
Center Number	It specifies the SMS center number of your SMS service provider.
Delivery Report	It specifies whether to receive or reject a message notifying you that an SMS has been delivered to a recipient.

After changing the settings, click **Apply** to enable the new settings to take effect.

7. USSD

This module enables you to communicate with your ISP using USSD. Click **USSD** to enter the page.

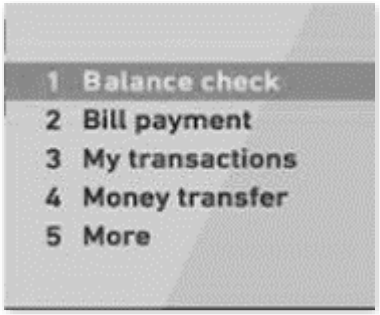


To use the USSD function, perform the following steps:

Step 1 Enter the USSD service number of your mobile carrier, such as ***555#**.

Step 2 Click **Send**.

The response from the mobile carrier appears. See the following figure.



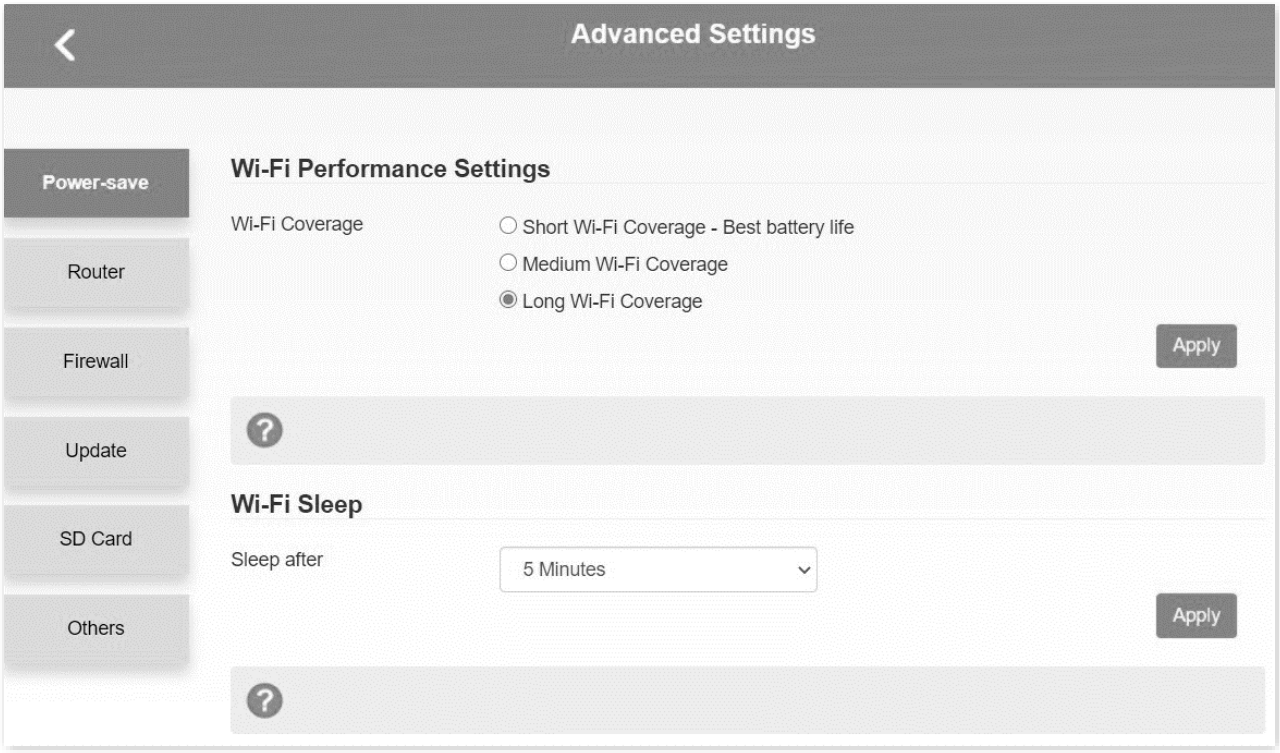
Step 3 Send the number of a menu item to access the menu.

Step 4 Send other commands according to the responses from the carrier.

8. Advanced Settings

8.1 Power-save

Here, you can adjust the Wi-Fi performance and Wi-Fi Sleep time to save battery life. Click **Advanced Settings** > **Power-save** to enter the page.

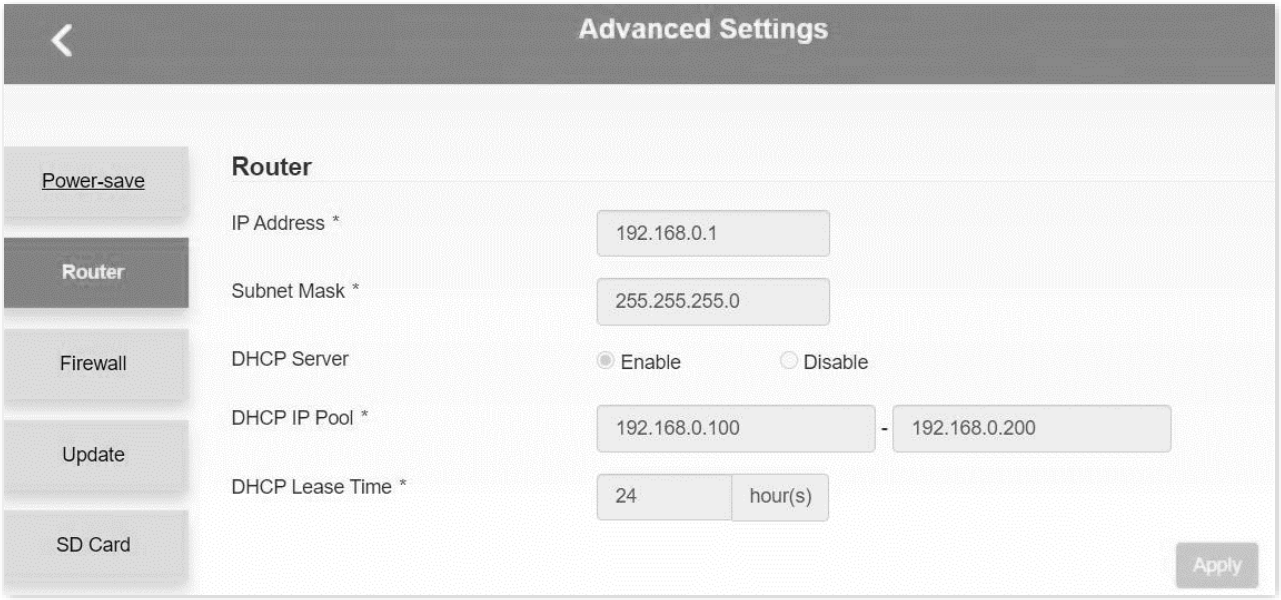


Parameter	Description
Wi-Fi Coverage	It specifies the Wi-Fi coverage settings, including **Short Wi-Fi Coverage**, **Medium Wi-Fi Coverage** and **Long Wi-Fi Coverage**. Shorter Wi-Fi coverage leads to better battery life.

Parameter	Description
Sleep after	• If the device has no wireless connection or USB connection within the specified period, which can be **5 minutes, 10 minutes, 20 minutes, 30 minutes, 1 hour or 2 hours**, the device turns to the sleep mode and the Wi-Fi network becomes unavailable. You can press the **Power** button or connect it to a computer using the USB cable to wake it up. • If the device is set to **Never Sleep**, the Wi-Fi network is always available, but the device will turn to the low power mode after 10 minutes when there is no wireless connection.

8.2 Router

Here, you can configure router settings of the device. Click **Advanced Settings** > **Router** to enter the page.



Parameter	Description
IP Address	It specifies the LAN IP address of the device. You can access the management web UI of the device through this IP address.
Subnet Mask	It specifies the subnet mask of the LAN IP address of the device.
DHCP Server	It specifies whether to enable the DHCP server function of the device. • Enable: The device allocates IP addresses to connected clients. • Disable: The device does not allocate IP addresses to connected clients, and the IP address must be entered manually for each client.
DHCP IP Pool	It specifies the IP address range that can be assigned to clients of the device.
DHCP Lease Time	It specifies the validity period of an IP address assigned to a client of the device. After an IP address expires, the device can assign it to any client.

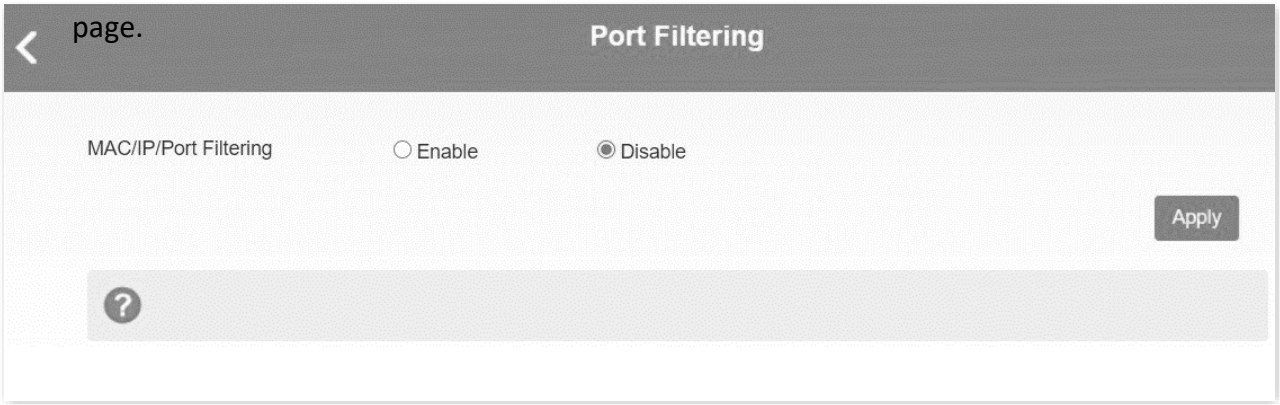
8.3 Firewall

In this module, you can configure the following firewall related functions of the device to protect your network from viruses, worms and malicious activities on the internet.

- Port filtering
- Port mapping
- Port forwarding
- UPnP
- DMZ

8.3.1 Port filtering

Here, you can set port filtering rules to allow or reject certain data packets. Click **Advanced Settings** > **Firewall** > **Port Filtering** to enter the page.



Set a port filter rule

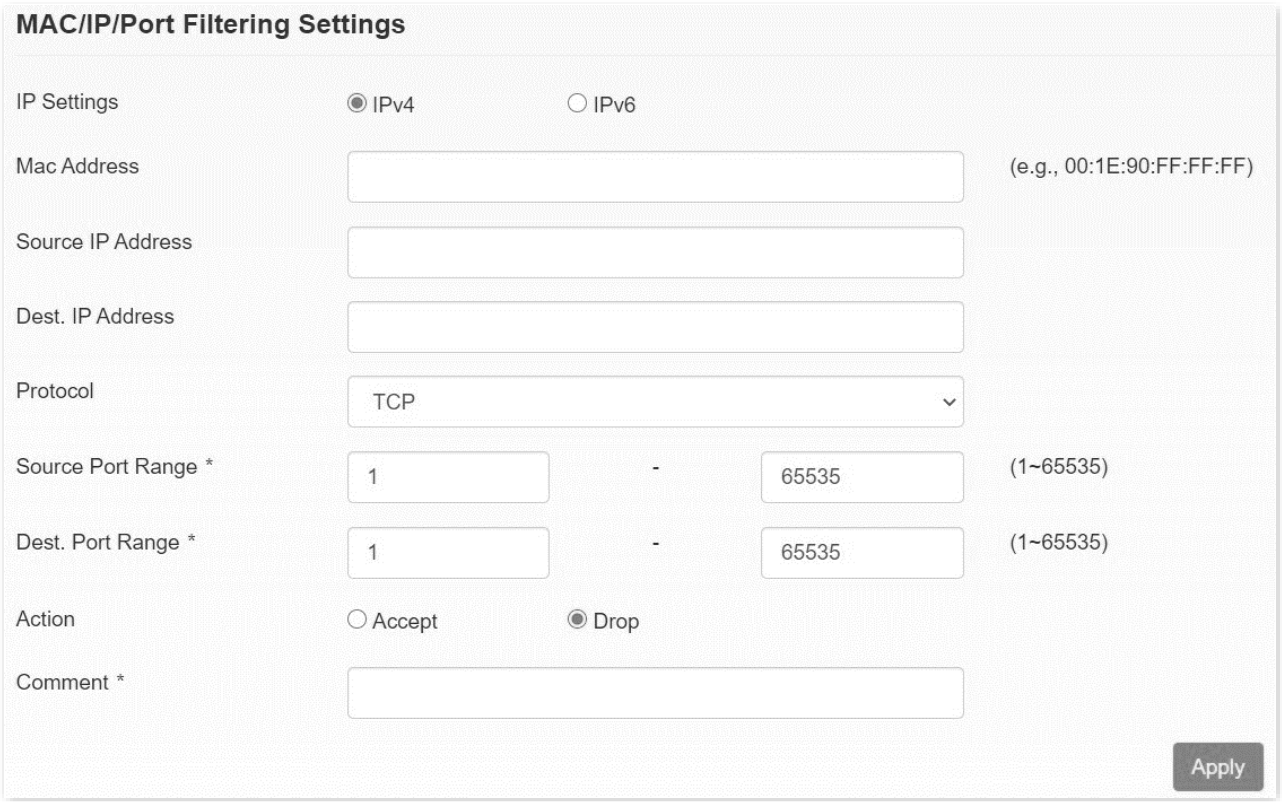
To set a port filtering rule, perform the following steps:

Step 1 Set **MAC/IP/Port Filtering** to **Enable**. **Default Policy** appears.

Step 2 Set **Default Policy** to **Accepted** if you want to allow all the packets not matching the port filtering rule, or to **Dropped** if you want to reject all the packets not matching the port filtering rule.

Step 3 Click **Apply**.

The parameters of port filtering rules appear.



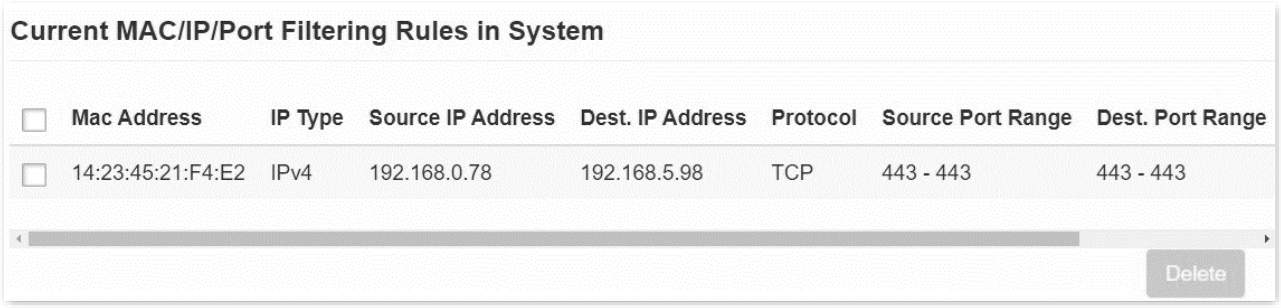
Parameter	Description
IP Settings	It specifies whether the filtering rule is applicable to IPv4 or IPv6.
MAC Address	It specifies the MAC address of the client whose packets are to be filtered.
Source IP Address/Source IPv6 Address	It specifies the source IP address by which packets are filtered.
Dest. IP Address/Dest. IPv6 Address	It specifies the destination IP address by which packets are filtered.
Protocol	It specifies the packet transmission protocol, including **TCP**, **UDP** or **ICMP**.
Source Port Range	It specifies the source port range by which packets are filtered.
Dest. Port Range	It specifies the destination port range by which packets are filtered.
Action	It specifies whether to accept or drop the packets matching the rule.

Parameter	Description
Comment	It specifies the description of the rule. Only the following characters are allowed in the comment: • Digits • Uppercase and lowercase letters • ! # ( ) + - . / % = ? @ ^ _ { | } ~

Step 4 Set the parameters.

Step 5 Click **Apply**.

The rule appears in the **Current MAC/IP/Port Filtering Rules in System** section.



Delete port filtering rules

To delete port filtering rules, perform the following steps:

Step 1 In the **Current MAC/IP/Port Filtering Rules in System** section, select the port filtering rules to be deleted. If you want to delete all rules, select the check box of the entire list.

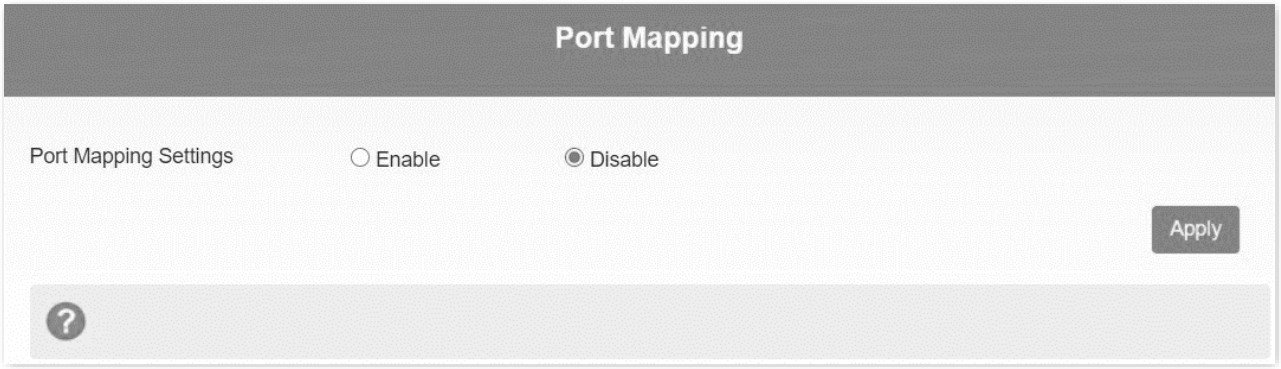
Step 2 Click **Delete**.

Step 3 Click **Yes** in the pop-up dialog box that appears.

8.3.2 Port mapping

Here, you can map an external port to an internal port, so that applications using the internal port (such as a web server) is accessible from the internet.

Click **Advanced Settings** > **Firewall** > **Port Mapping** to enter the page.



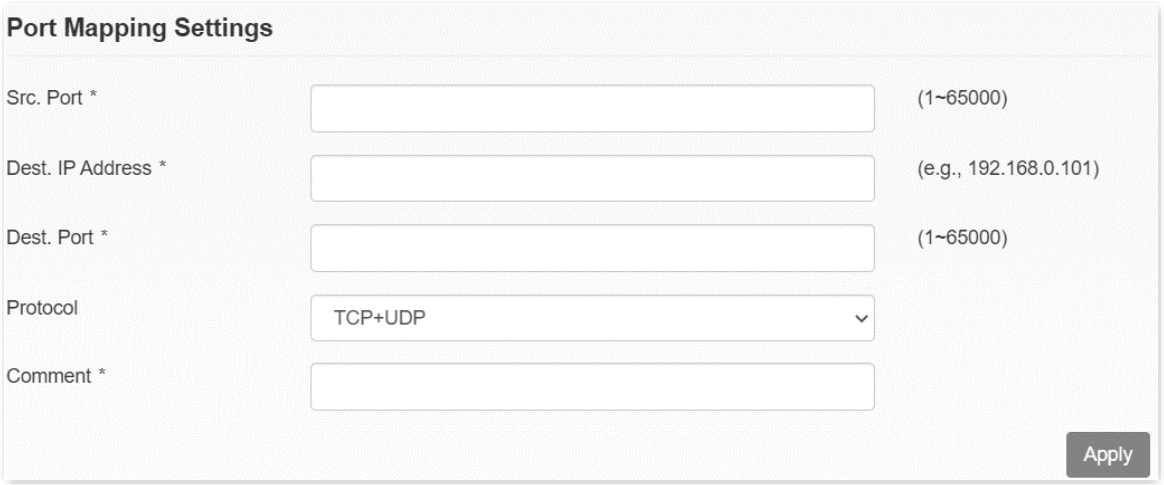
Set a port mapping rule

To set a port mapping rule, perform the following steps:

Step 1 Set **Port Mapping Settings** to **Enable**.

Step 2 Click **Apply**.

The parameters of port mapping rules appear.

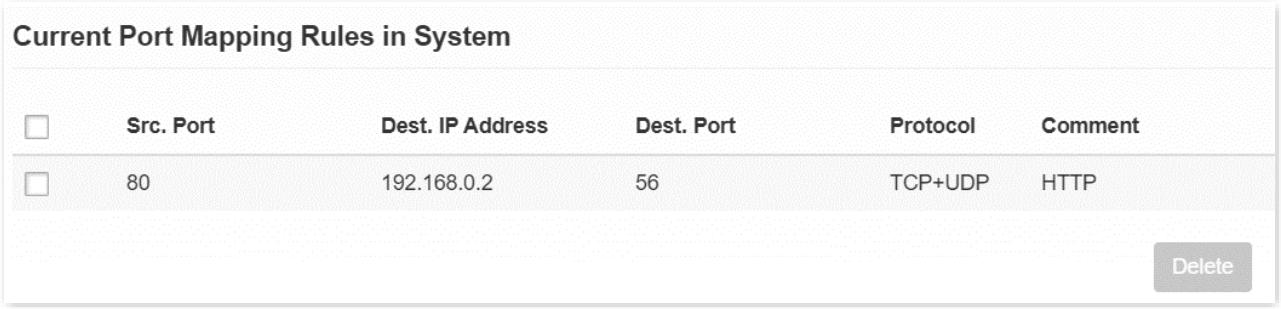


Parameter	Description
Src. Port	It specifies the external port to be mapped onto an internal port.
Dest. IP Address	It specifies the IP address corresponding to the internal port.
Dest. Port	It specifies the internal port.
Protocol	It specifies the packet transmission protocol.
Comment	It specifies the description of the port mapping rule. Only the following characters are allowed in the comment: • Digits • Uppercase and lowercase letters • ! # ( ) + - . / % = ? @ ^ _ { | } ~

Step 3 Set the parameters.

Step 4 Click **Apply**.

The rule appears in the **Current Port Mapping Rules in System** section.



Delete port mapping rules

To delete port mapping rules, perform the following steps:

Step 1 In the **Current Port Mapping Rules in System** section, select the port mapping rules to be deleted. If you want to delete all rules, select the check box of the entire list.

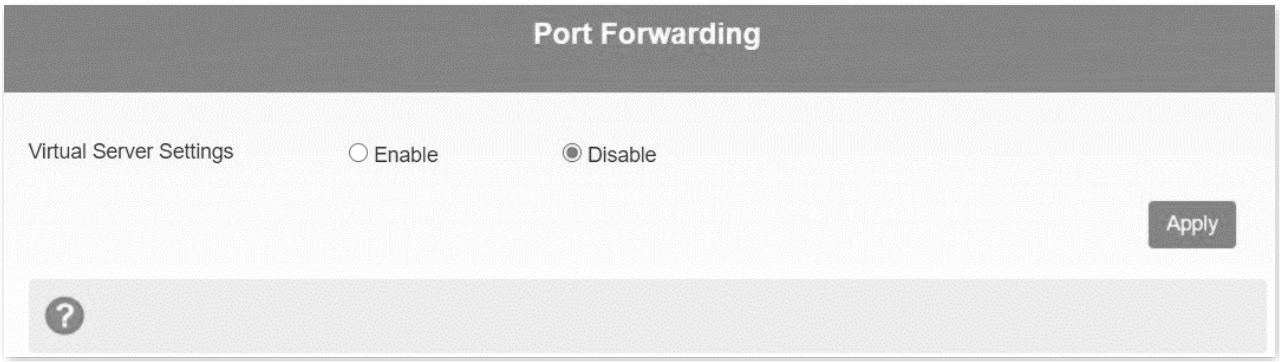
Step 2 Click **Delete**.

Step 3 Click **Yes** in the dialog box that appears.

8.3.3 Port forwarding

Here, you can configure port forwarding to enable external computers to access WWW, FTP or other services provided by LAN.

Click **Advanced Settings** > **Firewall** > **Port Forwarding** to enter the page.



Set a port forwarding rule

To set a port forwarding rule, perform the following steps:

Step 1 Set **Virtual Server Settings** to **Enable**.

Step 2 Click **Apply**.

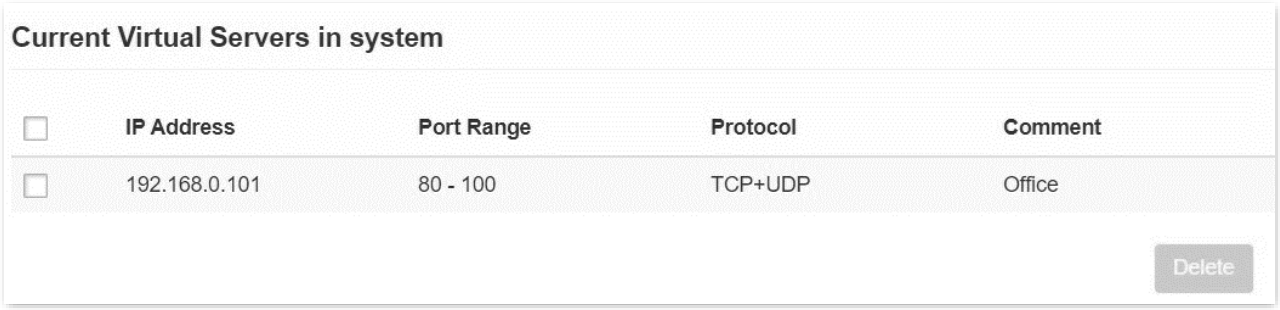
The parameters of port forwarding rules appear.

Parameter	Description
IP Address	It specifies the source IP address to be forwarded.
Port Range	It specifies the range of port numbers to be forwarded.
Protocol	It specifies the packet transmission protocol for forwarding.
Comment	It specifies the description of the port forwarding rule. Only the following characters are allowed in the comment: • Digits • Uppercase and lowercase letters • ! # ( ) + - . / % = ? @ ^ _ { | } ~

Step 3 Set the parameters.

Step 4 Click **Apply**.

The rule appears in the **Current Virtual Servers in System** section.



Delete port forwarding rules

To delete port forwarding rules, perform the following steps:

Step 1 In the **Current Virtual Servers in System** section, select the port forwarding rules to be deleted. If you want to delete all the rules, select the check box of the entire list.

Step 2 Click **Delete**.

Step 3 Click **Yes** in the dialog box that appears.

Example of configuring port forwarding rule

Network requirement

You have set up an FTP server (such as in a computer) within your LAN.

Requirement: Open the FTP server to internet users and enable external computers to access the resources of the FTP server from the internet.

Solution

You can configure a port forwarding rule to meet this requirement.

Assume that the information of the FTP server includes:

- IP address: 192.168.0.136
- Service port: 21
- Protocol: TCP

and the WAN IP address of the hotspot: 183.38.7.216.

Configuration procedures

Step 1 Click **Advanced Settings** > **Firewall** > **Port Forwarding**.

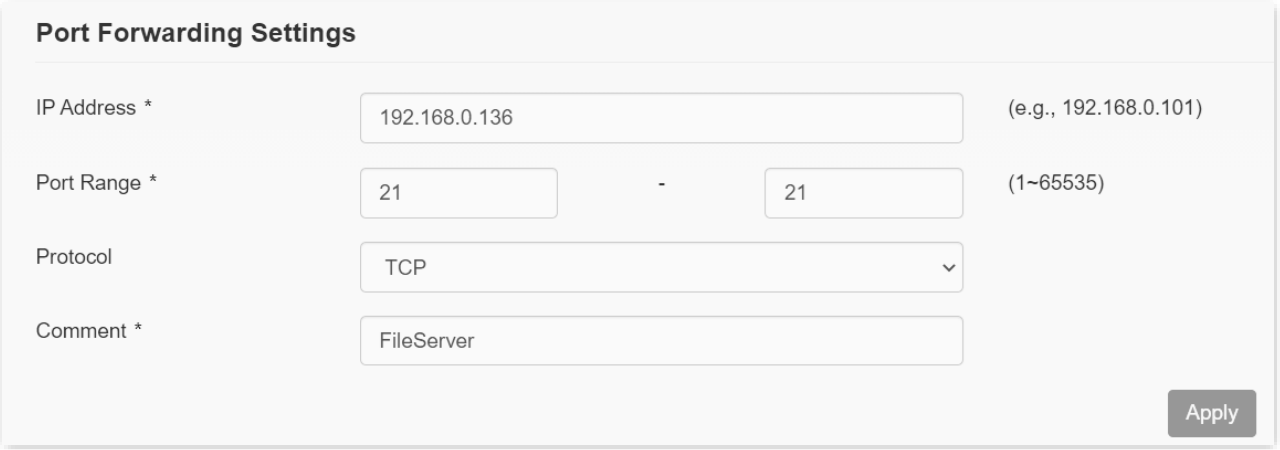
Step 2 Set **Virtual Server Settings** to **Enable**, and click **Apply**.

Step 3 Set **IP Address** to **192.168.0.136**.

Step 4 Set **Port Range** to **21-21**.

Step 5 Select **TCP** as the **Protocol**.

Step 6 Fill in the **Comment**, such as **FileServer**, and click **Apply**.



Verification

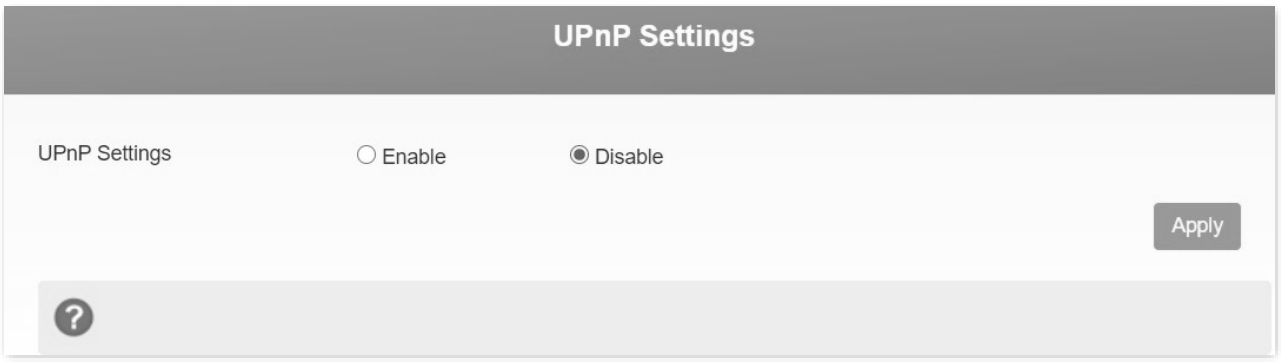
External computers can access the intranet through the IP format **Server Type://Your Hotspot's WAN IP:Port Number**. Here in this example, external computers can access the file in the FTP server within the LAN by entering ftp:// 183.38.7.216:21 in a browser.

8.3.4 UPnP

Universal Plug and Play (UPnP) is a set of networking protocols that allows networked devices, such as PCs, printers, internet gateways, Wi-Fi access points and mobile devices, to seamlessly
discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

Although UPnP facilitates networking among different devices, note that this function may raise the risk of being attacked. Use this function with caution.

Click **Advanced Settings** > **Firewall** > **UPnP** to enter the page.



8.3.5 DMZ

In some cases, you may need to have your device completely exposed to external networks for

bidirectional communication. To do so, set it as a DMZ host.

If a client cannot access the internet properly, you can try this function. If the DMZ function is enabled for a specific client, the client is not protected by the firewall of the device. Therefore, use this function with caution.

Click **Advanced Settings** > **Firewall** > **DMZ** to enter the

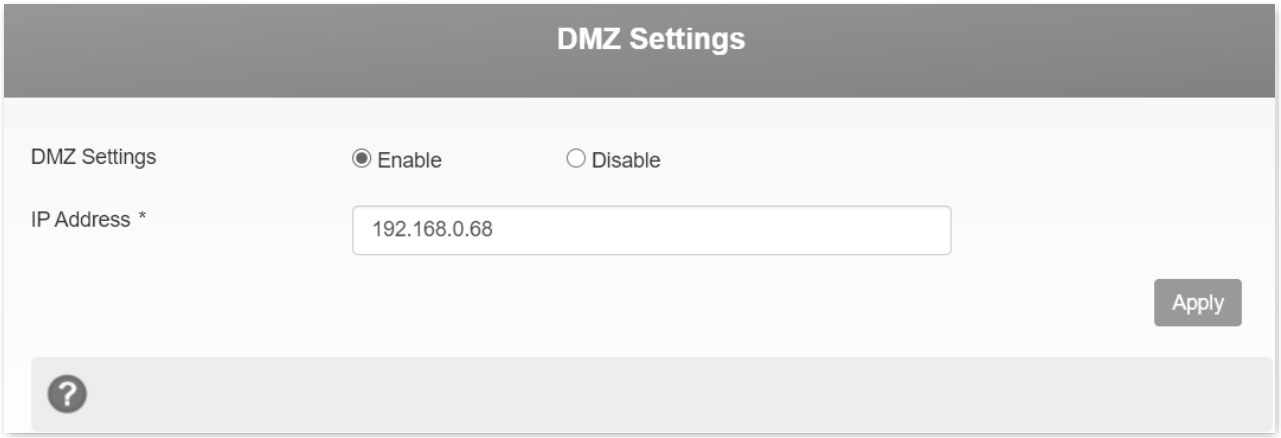
page. To use the DMZ function, perform the following

steps:

Step 1 Set **DMZ Settings** to **Enable**.

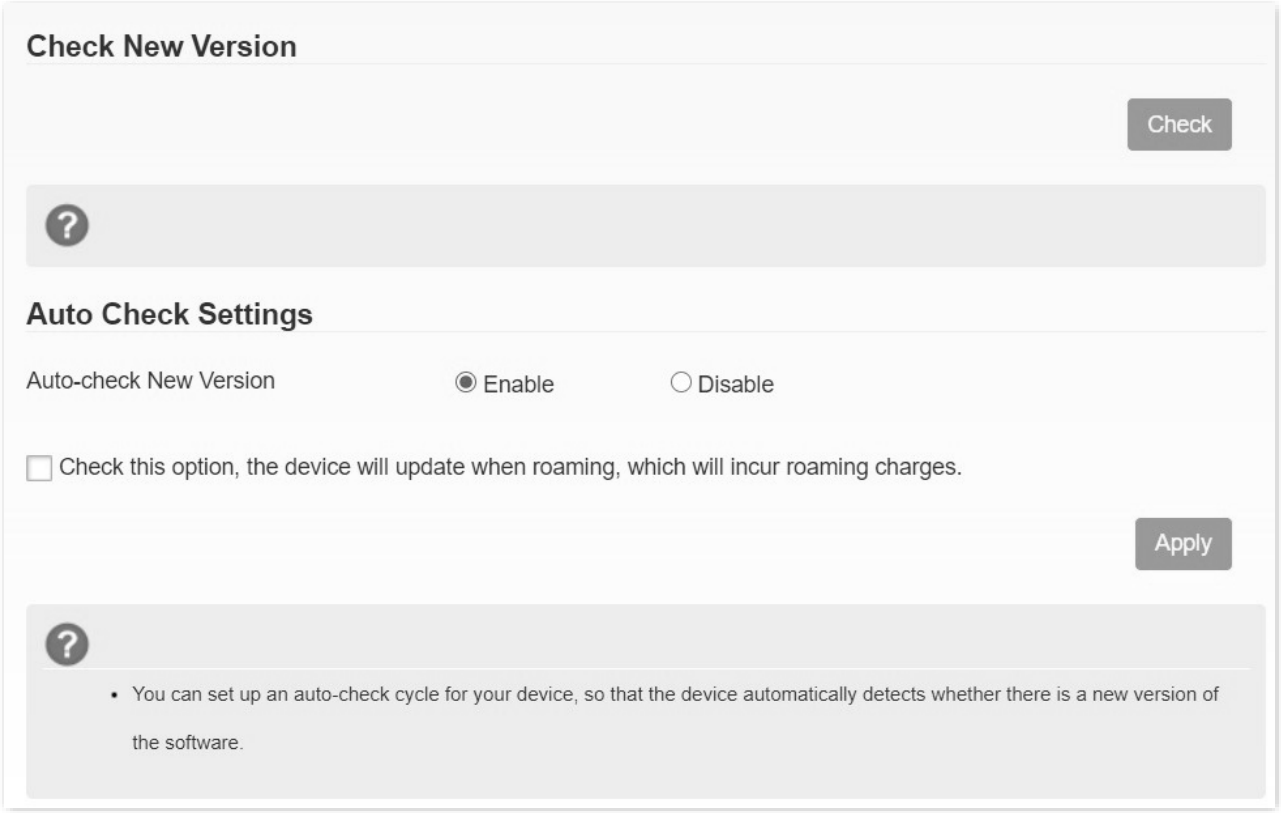
Step 2 Set **IP Address** to the IP address of the client that requires the DMZ function.

Step 3 Click **Apply**.



8.4 Update

Here, you can update the software version of the device manually or automatically. Click **Advanced Settings** > **Update** to enter the page.

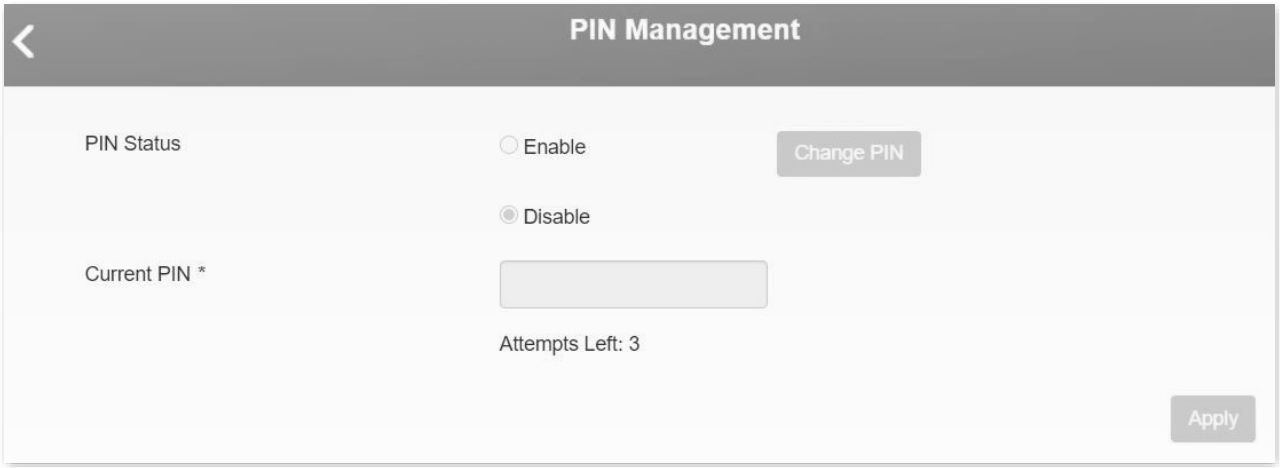


- To update manually, you can click the **Check** button for obtaining a new version immediately.
- To update automatically, you can select **Enable** and click **Apply**. Note that the update during roaming will incur roaming charges.

8.4.1 PIN management

PIN management prevents unauthorized use of the SIM, USIM, or UIM card. If you want to change current settings, please disconnect from network first. Generally, a PIN and a PUK are provided along with a SIM card.

It is recommended to enable the PIN status when you want to increase security.



Change the PIN Status

To change the PIN status, perform the following steps:

Default PIN is active with “1111”

Step 1 Disconnect the device from your mobile network.

Step 2 Set **PIN Status** to **Enable** or **Disable**.

Step 3 Enter the PIN of the SIM card.

Step 4 Click **Apply**.

Step 5 Click **Yes** in the dialog box that appears.

After the **PIN Status** is set to **Enable**, the SIM card is locked each time the device starts (**PIN Lock** will appear on the screen). You need to log in to the web UI of the device, enter the PIN, and click **Next** to unlock the SIM card, so that you can use the SIM card properly. See the following figure.

Change the PIN

To change the PIN, perform the following steps:

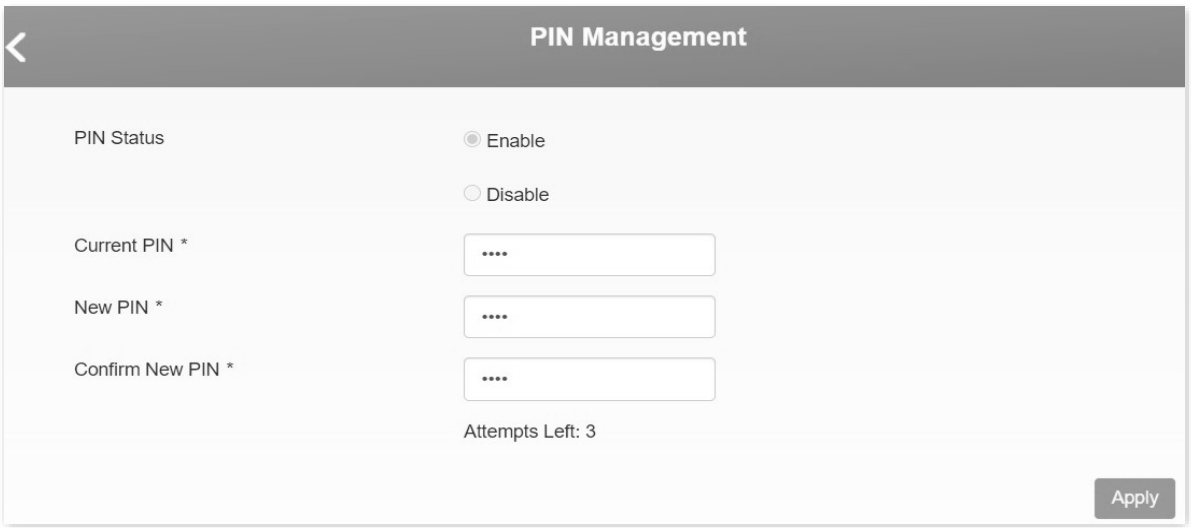
Step 1 Disconnect the device from your mobile network.

Step 2 Set **PIN Status** to **Enable**, enter the **Current PIN**, and click **Apply**.

Step 3 Click **Change PIN**.

Step 4 Set **Current PIN, New PIN** and **Confirm New PIN**.

Step 5 Click **Apply**.



FCC WORRYING

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
-- Reorient or relocate the receiving antenna.
-- Increase the separation between the equipment and receiver.
-- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
-- Consult the dealer or an experienced radio/TV technician for help.
The device has been evaluated to meet general RF exposure requirement. The device can be used in portable exposure condition without restriction
Specific Absorption Rate (SAR) information:
This product meets the government's requirements for exposure to radio waves. The guidelines are based on standards that were developed by independent scientific organizations through periodic and thorough evaluation
of scientific studies. The standards include a substantial safety margin designed to assure the safety of all persons regardless of age or health.
FCC RF Exposure Information and Statement The SAR limit of USA (FCC) is 1.6 W/kg averaged over one gram of tissue. Device types: WSMRMIFI (FCC ID: 2BL4N-WSMRMIFI) has also been tested against this SAR limit. The highest SAR values for body are 0.64W/Kg. This device was tested for typical body-worn operations with the product kept 10cm from the body. To maintain compliance with FCC RF exposure requirements, use accessories that maintain a 10cm separation distance between the user's body and the product. The use of belt clips, holsters and similar accessories should not contain metallic components in its assembly.
The use of accessories that do not satisfy these requirements may not comply with FCC RF exposure requirements, and should be avoided. Body-worn Operation
This device was tested for typical body-worn operations. To comply with RF exposure requirements, a minimum separation distance of 10cm must be maintained between the user' s body and the product, including the antenna. Third-party belt-clips, holsters, and similar accessories used by this device should not contain any metallic components.
Body-worn accessories that do not meet these requirements may not comply with RF exposure requirements and should be avoided. Use only the supplied or an approved antenna.