

MF985U User Manual

ZTE CORPORATION
NO. 55, Hi-tech Road South, ShenZhen, P.R.China
Postcode: 518057

LEGAL INFORMATION

Copyright © 2018 ZTE CORPORATION.

All rights reserved.

No part of this publication may be excerpted, reproduced, translated or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without the prior written permission of ZTE Corporation.

The manual is published by ZTE Corporation. We reserve the right to make modifications on print errors or update specifications without prior notice.

Version No. : 1.0

Edition Time: February 1, 2018



NOTE:

Do not use the device in an enclosed environment or where heat dissipation is poor. Prolonged work in such space may cause excessive heat and raise ambient temperature, which may lead to automatic shutdown of the device for your safety. In the case of such event, cool the device in a well-ventilated place before turning on for normal use.

Contents

Getting Started	2
Introduction	2
Outline and Parts	2
Indicators	3
Installing Your Device	3
Inserting the nano-SIM Card	3
Inserting the battery.....	4
Powering On/Off Your Device	5
Locking/Unlocking the Screen.....	5
Sleep Mode.....	5
Charging Your Device.....	5
About nano-SIM Card	6
Internet Access.....	6
Connection Scenario.....	6
Configuring Your PC	7
Connecting to Your Device	8
Accessing the Internet	10
Disconnecting from the Internet	10
4G Mobile Hotspot Configuration Page.....	11
Accessing the Configuration Page	11
Login	11
Settings	12
Block / unblock devices	12
Network Settings	13
Wi-Fi Settings	16
Data Management Settings.....	21
Status Information	23
File Sharing	23
Advanced Settings	25
Touch Screen.....	33
Data.....	34
Wi-Fi.....	34
Settings	35
Warning and Notice.....	36
To the Owner	36
Using Your Device	36
Using Battery	37
Limited Warranty.....	37
Limitation of Liability.....	38
FCC Regulations:.....	38
FCC RF Exposure Information (SAR).....	39
Troubleshooting	39

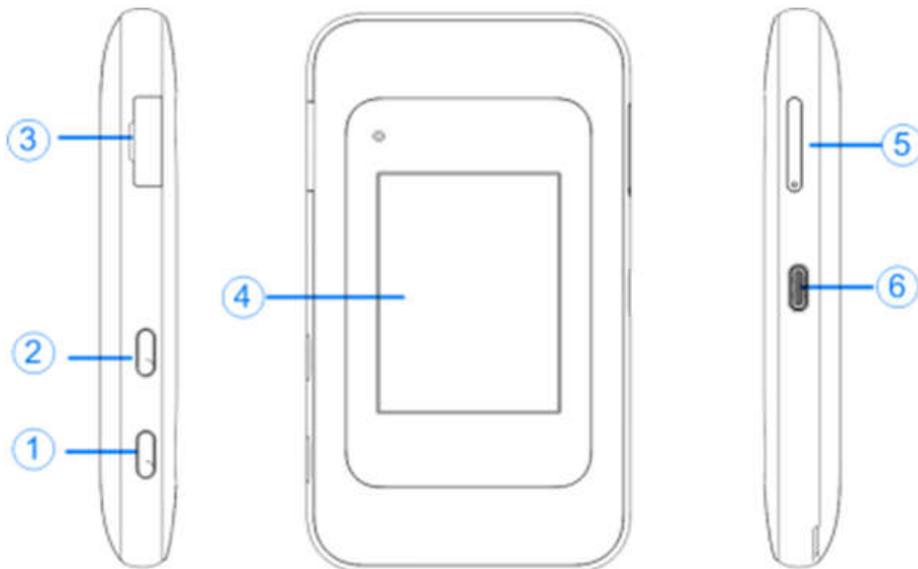
Getting Started

Introduction

MF985U is a 4G mobile hotspot device, working in LTE network. The client devices can connect to it via Wi-Fi. The device supports data services, enabling you to communicate anytime and anywhere.

Outline and Parts

The following figures show the appearance of the device. It is only for your reference. The actual device may be different.



Number	Part	Description
1	Power Key	Turn the device on or off.
2	WPS Key	Enable WPS function.
3	External Antenna Connector	Connect to the external antenna.
4	Touch Screen	Configure basic Wi-Fi and device settings, and view data usage.
5	nano-SIM/ microSDXC Card Tray	Install the nano-SIM card or microSDXC card.

6	Charging/ USB Type-C™ Jack	Connect the USB Type-C™ cable for charging or tethered connections.
---	----------------------------	---

Indicators

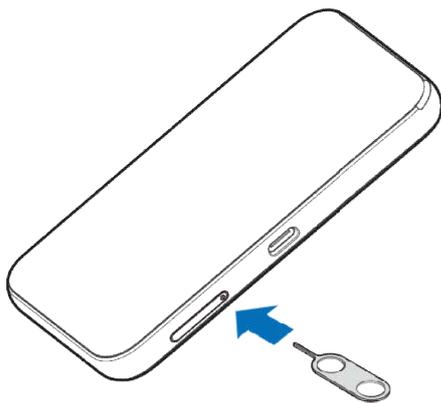
When the device is powered on, the following icons will appear on the LCD screen, with the corresponding indicators listed in the table below:

Icon	Indication	Icon	Indication
	Network signal strength.		Battery is low.
4G LTE	Network type. 4G LTE icons will appear on the LCD screen according to the network being connected.		The device has been connected to the Internet.
	View the number of the connected user.		Battery is full.

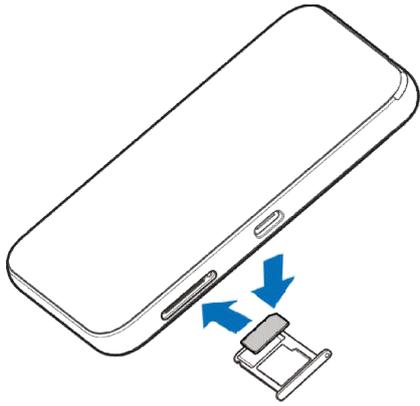
Installing Your Device

Inserting the nano-SIM Card

1. Insert the tip of the tray eject tool into the hole on the nano-SIM card tray on the right side of the device.



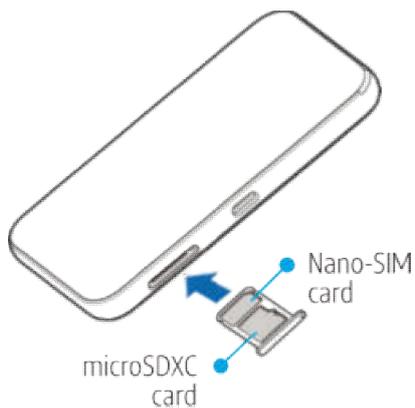
2. Place the nano-SIM card on the tray and then carefully slide the tray back into place.

**⚠ WARNING!**

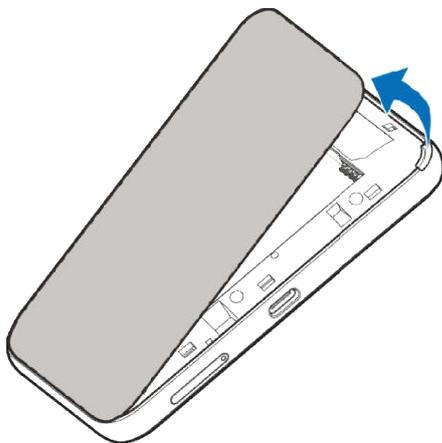
To avoid damage to the device, do not use any other kind of SIM cards, or any non-standard nano-SIM card cut from a SIM card. You can get a standard nano-SIM card from your service provider.

✔ NOTE:

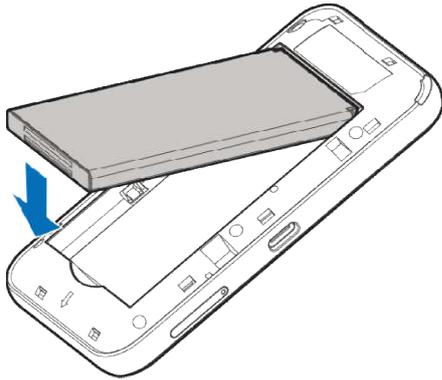
You can also install a microSDXC card(sold separately) on the card tray, as shown.

**Inserting the battery**

1. Remove the battery cover.



2. Insert the battery as shown with the contacts located against the metal springs, and press the battery down into the case.



3. Replace the back cover.

Powering On/Off Your Device

Press and hold the **Power** Key to turn on or off your device.

 **NOTE:**

The device is powered on when the LCD screen lights up.

Locking/Unlocking the Screen

Your device allows you to quickly lock the screen when not in use and to turn the screen back on and unlock it when you need it.

To lock the screen:

To quickly turn the screen off, press the **Power** Key.

To unlock the screen:

1. Press the **Power** Key to turn the screen on.
2. Touch and hold  on the screen.

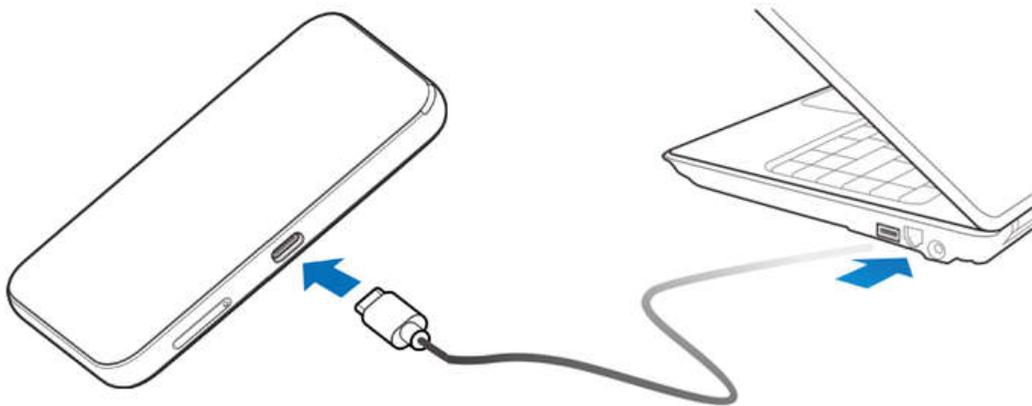
Sleep Mode

When you enable the Wi-Fi function and use the battery to supply power to the device, once no user connects to the device within specified time, the device will go to the sleep mode, and the LCD screen will be turned off. In the sleep mode, the Wi-Fi function will be disabled. Press the **Power Key** to wake up the device and enable the Wi-Fi function, and the LCD screen will be turned on.

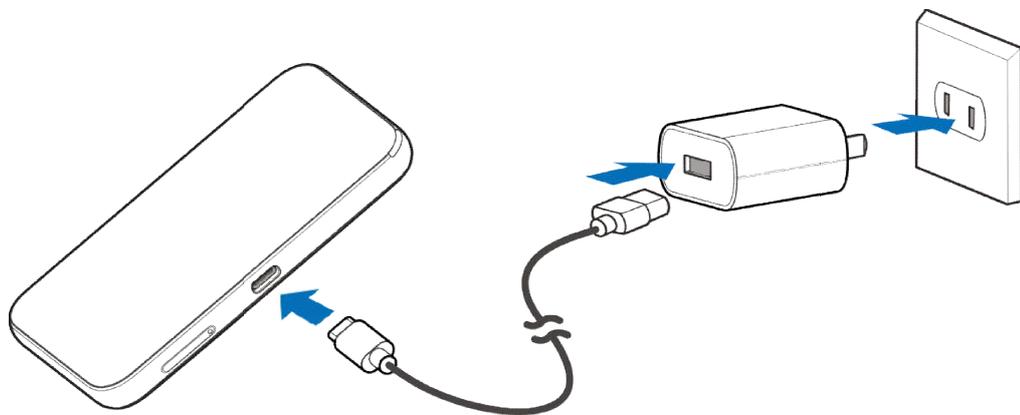
Charging Your Device

You can charge your device by using the USB cable or adapter.

- Use the USB Type-C cable to connect your device and PC directly.



- Use the adapter and USB Type-C cable to connect the wall outlet and your device.



 **NOTE:**

Do not use excessive force to insert the plug.

About nano-SIM Card

Avoid handling the nano-SIM card unnecessarily. Hold the card by the edges to prevent static damage. Keep the nano-SIM card away from electrical and magnetic appliances.

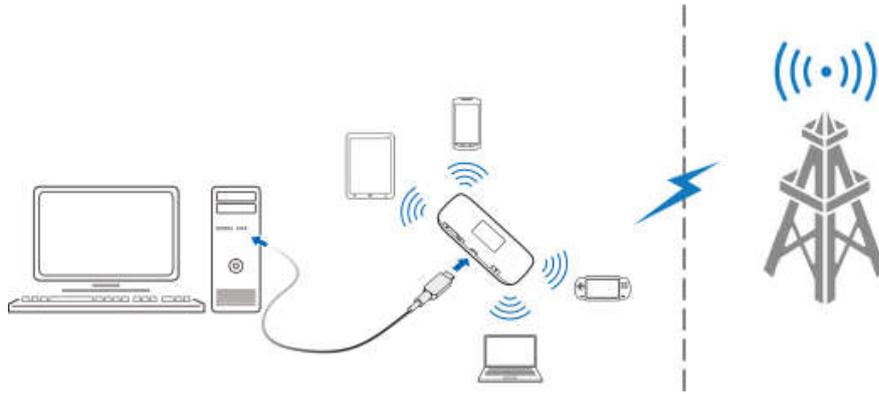
If you cannot get service, make sure that:

- You are in an area which has network coverage.
- You are using the correct nano-SIM card.

Internet Access

Connection Scenario

The following picture is the application example. All of the client devices can surf on the Internet at the same time.

**NOTE:**

You can only use Wi-Fi to connect to this device and make sure the client supports the Wi-Fi function.

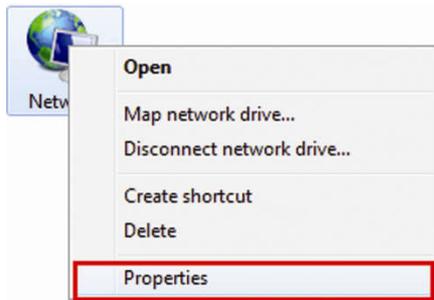
Configuring Your PC

Follow the following steps and figures for Windows 7 to configure the Wireless Internet Protocol for your connection.

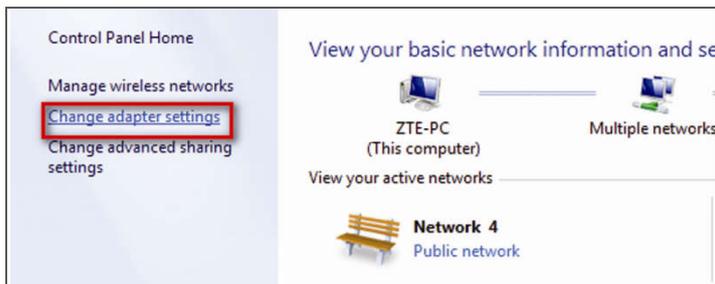
NOTE:

Wireless Network Connection is used for Wi-Fi connection.

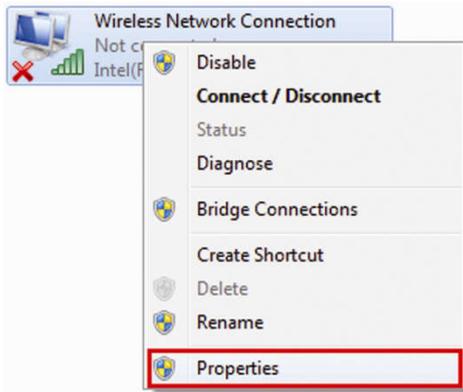
1. Right-click **Network** and select **Properties**.



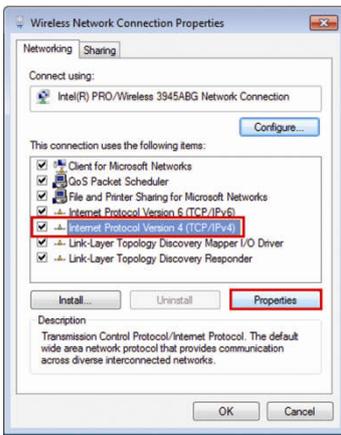
2. Select **Change adapter settings**.



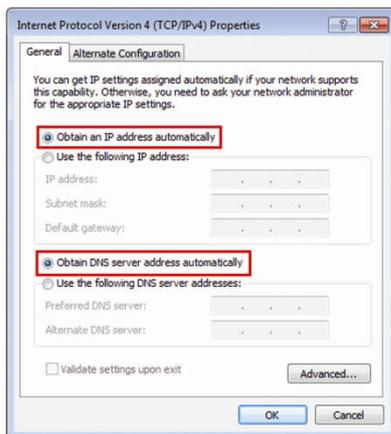
3. Right-click **Wireless Network Connection** and select **Properties**.



4. Select **Internet Protocol Version 4 (TCP/IPv4)**, and click **Properties**.

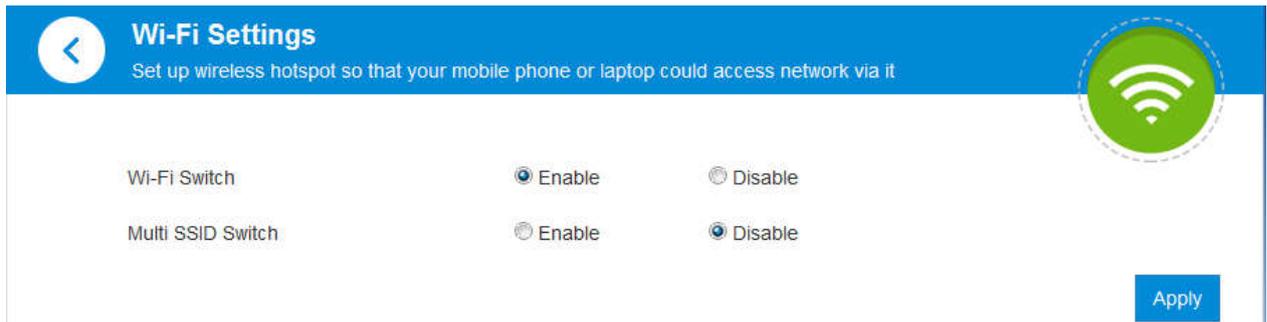


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**, and click **OK**.



Connecting to Your Device

1. Make sure that Wi-Fi is enabled. Please check the Wi-Fi Settings on the 4G Mobile Hotspot configuration page.



2. Use your normal Wi-Fi application on the client to search for available wireless networks.



3. Select the SSID of your device, and then click **Connect**.



 **NOTES:**

- Check the label on your device to get the default SSID and password.
 - Get the default SSID and password on the LCD screen.
4. Input the password, and then click **OK**.



5. Wait a moment, and then the client will connect to your device successfully.

If you want to use WPS function to enable a Wi-Fi connection, please:

1. Power on your device, and enable the Wi-Fi function on your device.
2. Enable the WPS function. Please check the **WPS** Settings on the 4G Mobile Hotspot configuration page.
3. Press and hold the **WPS** Key on your device and touch **Pair with Main Wi-Fi** on the touch screen to start Wi-Fi Protected Setup authentication process.
4. Enable the WPS function on your client to respond to this authentication process.
5. Follow the system prompts on your client to finish the connection.

Accessing the Internet

1. Switch on the device.
2. Connect the client to your device.
3. After the client is connected to your device successfully, you can access the Internet automatically.

Disconnecting from the Internet**On the 4G Mobile Hotspot Configuration Page**

1. Log in the 4G Mobile Hotspot configuration page, and click the (network type) **Settings > Data Settings**.
2. Set **Allow Mobile Data** to **Off**.

On the Touch Screen

1. From the touch screen, touch **Settings > Allow Mobile Data**.
2. Slide the switch next to **Standard Data** to **OFF** position.

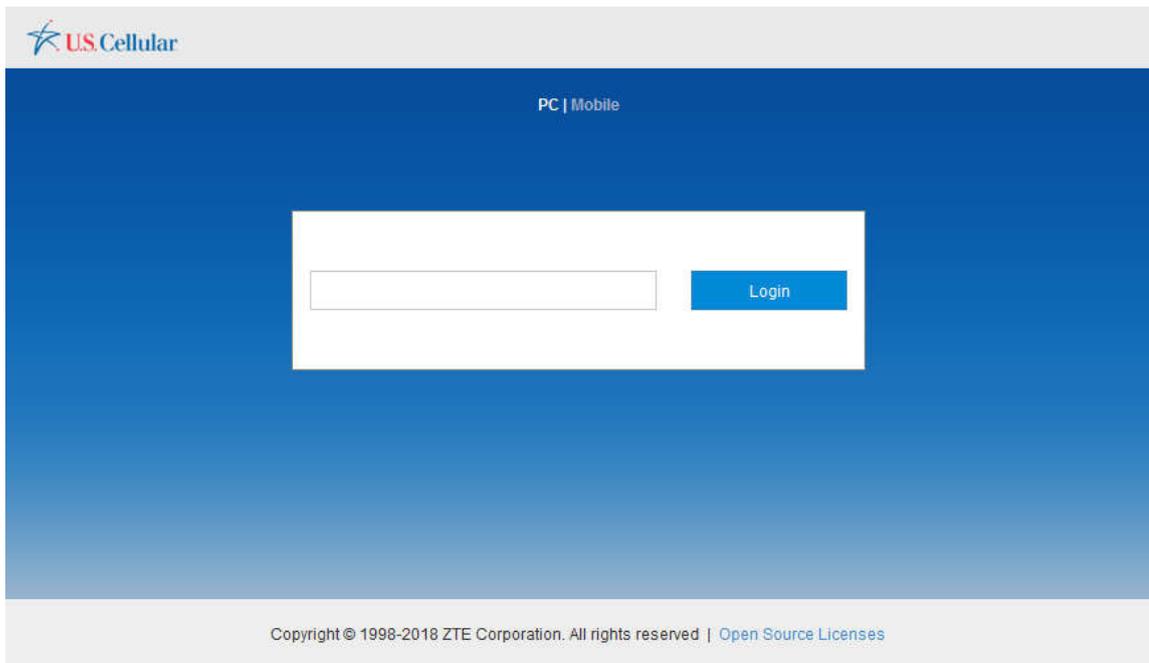
 **NOTE:**

Powering off the device can also terminate the Internet connection.

4G Mobile Hotspot Configuration Page

Accessing the Configuration Page

1. Make sure the connection between your device and the client is correct.
2. Launch the Internet browser and enter <http://192.168.1.1> or <http://uscc.hotspot> in the address bar.
3. The login page appears as follows. The following figure is only for your reference.



Login

1. In the 4G Mobile Hotspot configuration page, input the password.
2. Click **Login** to proceed.

NOTE:

The password is the same as the default Main Wi-Fi password.

The status bar at the top of the 4G Mobile Hotspot configuration page provides device and service status icons on the right side. Below are some of the icons you may see.

Battery indicator	 : Shows the battery level.
Signal strength	 : Shows the network signal intensity.
Internet	 : Connected to the Internet.

status	 : Disconnected from the Internet.
Wi-Fi strength	 : Wi-Fi status and number of the connected users. The maximum number is 15, these connections are shared between the device's Main and Guest Wi-Fi networks.

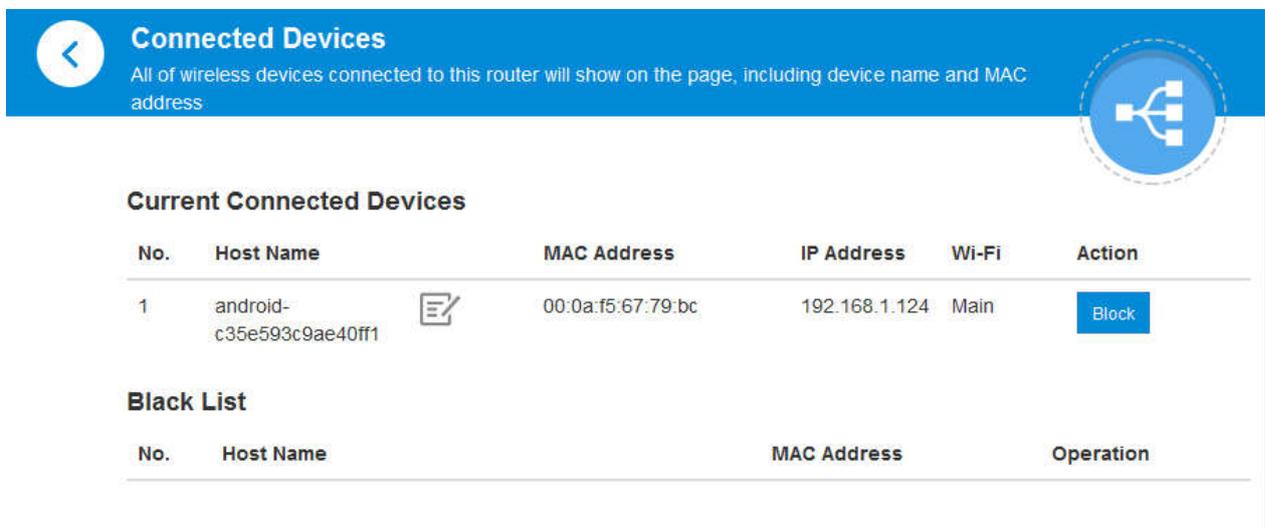
Settings

NOTES:

- Do not modify any settings unless instructed by your service provider.
- Please disconnect the device from the cellular network before making changes to settings.

Block / unblock devices

1. Click **Access device** section, and all of wireless devices connected to your device will show in the following figure.



Connected Devices
All of wireless devices connected to this router will show on the page, including device name and MAC address

Current Connected Devices

No.	Host Name	MAC Address	IP Address	Wi-Fi	Action
1	android-c35e593c9ae40ff1	00:0a:f5:67:79:bc	192.168.1.124	Main	Block

Black List

No.	Host Name	MAC Address	Operation
1	android-c35e593c9ae40ff1	00:0a:f5:67:79:bc	Remove

2. Click **Block** behind the device you want to block and then it will be added to the Black List. Devices on the black list will not be able to use the device to connect to the network.

Black List

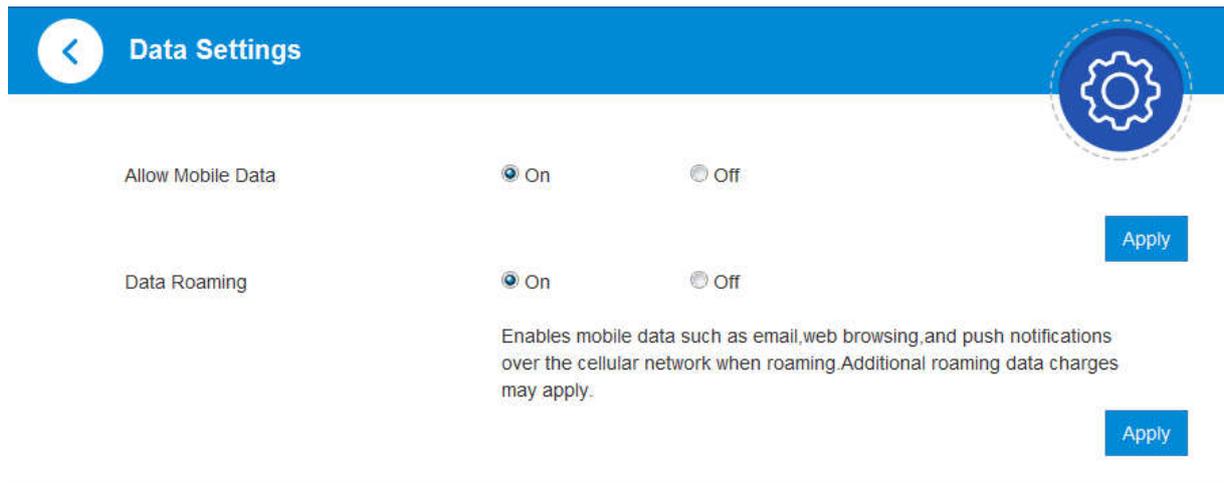
No.	Host Name	MAC Address	Operation
1	android-c35e593c9ae40ff1	00:0a:f5:67:79:bc	Remove

3. Click **Remove** to delete the device from the black list and then the device will be able to access the network again.

Network Settings

Data Settings

Click **Settings > Data Settings**. The data settings are shown in the following figure.



To Enable / Disable Mobile Data

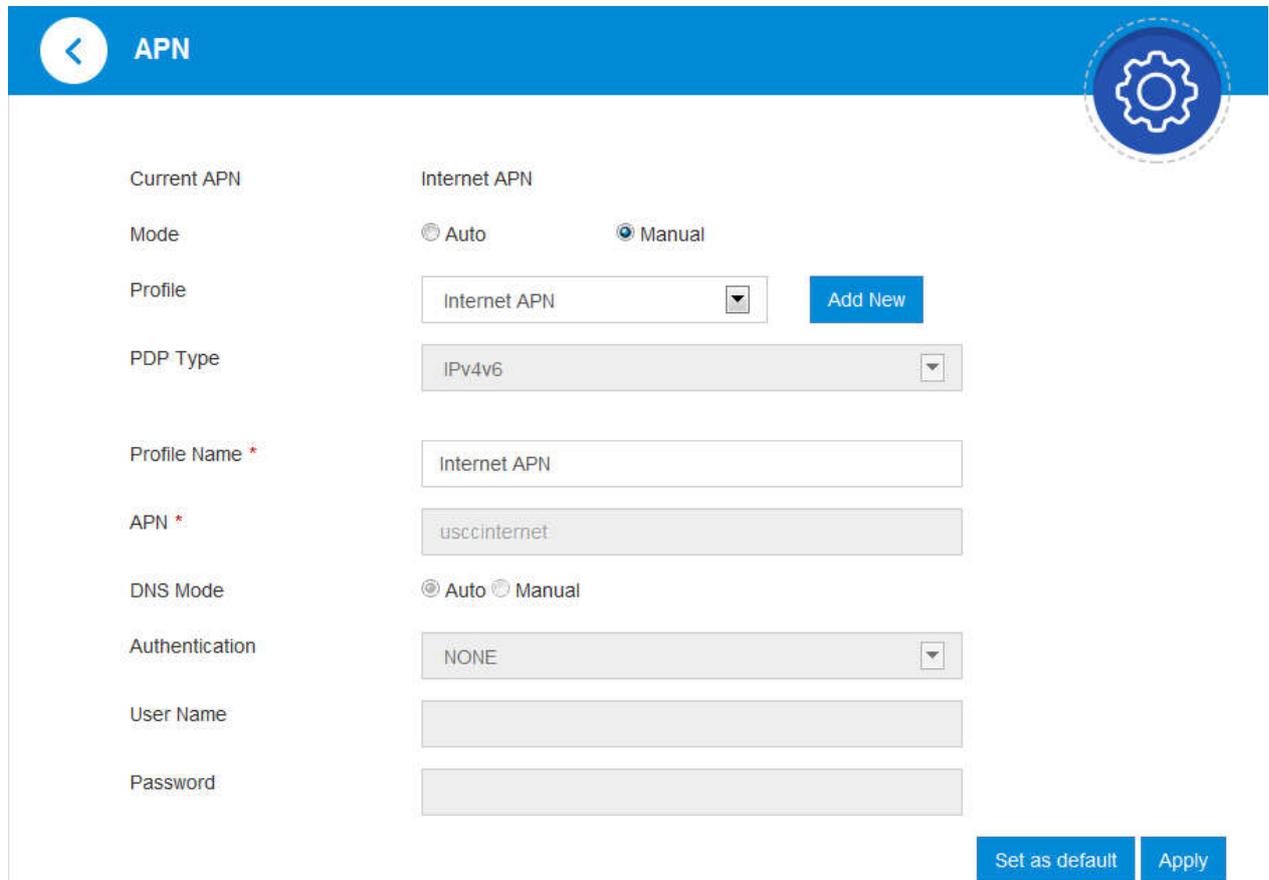
1. Select **On / Off** next to **Allow Mobile Data** in the figure above.
2. Click **Apply**.

To Enable / Disable Data Roaming

1. Ensure that the mobile data is available.
2. Select **On / Off** next to **Data Roaming**.
3. Click **Apply**

APN Setting

Click **Settings > APN**. The APN parameters are shown in the following figure.



The screenshot displays the APN settings interface. At the top, there is a blue header with a back arrow and the text "APN". A gear icon is visible in the top right corner. The settings are organized into two columns:

- Current APN:** Internet APN
- Mode:** Radio buttons for Auto and Manual.
- Profile:** A dropdown menu showing "Internet APN" and an "Add New" button.
- PDP Type:** A dropdown menu showing "IPv4v6".
- Profile Name *:** A text input field containing "Internet APN".
- APN *:** A text input field containing "usccinternet".
- DNS Mode:** Radio buttons for Auto and Manual.
- Authentication:** A dropdown menu showing "NONE".
- User Name:** An empty text input field.
- Password:** An empty text input field.

At the bottom right, there are two buttons: "Set as default" and "Apply".

Set as default: Click to set current profile as the default profile.

To add a new APN profile, follow the steps below:

1. Click **Add New** in the figure above to access the following figure.

← APN

Current APN	usccinternet		
Mode	<input type="radio"/> Auto	<input checked="" type="radio"/> Manual	
Profile	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> usccinternet ▼ </div>	Cancel	
PDP Type	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> IPv4 ▼ </div>		
Profile Name *	<input style="width: 100%;" type="text"/>		
APN *	<input style="width: 100%;" type="text"/>		
DNS Mode	<input checked="" type="radio"/> Auto	<input type="radio"/> Manual	
Authentication	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> NONE ▼ </div>		
User Name	<input style="width: 100%;" type="text"/>		
Password	<input style="width: 100%;" type="text"/>		

Apply

2. Enter the related parameters (please see following table), and then click **Apply** to add a new profile.

Parameter	Function
PDP Type	Choose a PDP type from the drop-down list, IPv4 /IPv6 / IPv4v6.
Profile Name	Type the profile name.
APN	Type the Access Point Name.
DNS Mode	If a fixed IP address is provided by your service provider, select Manual DNS. Otherwise, please select Auto DNS and the device will automatically obtain parameters.
Authentication	Password Authentication Protocol (PAP) provides a simple method without encryption for the peer to establish its identity using a 2-way handshake. Challenge-Handshake Authentication Protocol (CHAP) is used to periodically verify the identity of the peer using a 3-way handshake.
User Name	User name is used to obtain authentication from the ISP when

	the connection is established.
Password	Password is used to obtain authentication from the ISP when the connection is established.

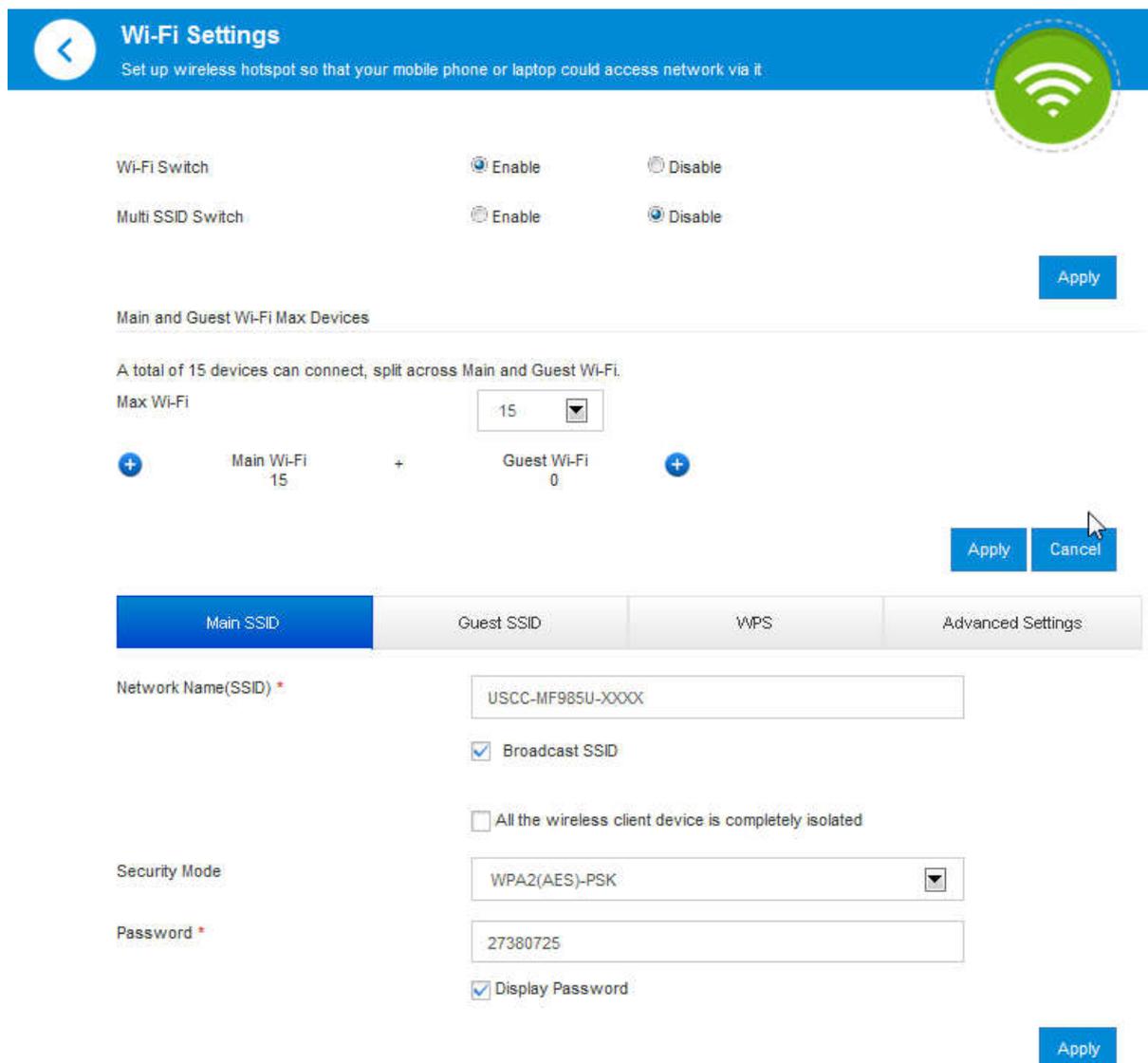
 **NOTES:**

- The **Profile Name** and **APN** are mandatory, others are optional.
- If the Authentication is set to **NONE**, you don't need to set the User Name and Password.

Wi-Fi Settings

Main SSID Settings

1. Select **Settings** below **Wi-Fi** and click **Main SSID**. The main SSID basic parameters are shown in the following figure.



The screenshot displays the 'Wi-Fi Settings' configuration page. At the top, there is a blue header with a back arrow and the title 'Wi-Fi Settings'. Below the header, there are two rows of toggle switches: 'Wi-Fi Switch' (set to 'Enable') and 'Multi SSID Switch' (set to 'Disable'). An 'Apply' button is located to the right of these switches. Below this, the 'Main and Guest Wi-Fi Max Devices' section shows a total of 15 devices can connect. A dropdown menu for 'Max Wi-Fi' is set to '15'. Below this, there are two sliders: 'Main Wi-Fi' (set to 15) and 'Guest Wi-Fi' (set to 0). Another 'Apply' and 'Cancel' button pair is present. At the bottom, there are four tabs: 'Main SSID' (selected), 'Guest SSID', 'WPS', and 'Advanced Settings'. The 'Main SSID' tab contains the following fields: 'Network Name(SSID)' with the value 'USCC-MF985U-XXXX', a checked 'Broadcast SSID' checkbox, an unchecked checkbox for 'All the wireless client device is completely isolated', 'Security Mode' set to 'WPA2(AES)-PSK', 'Password' set to '27380725', and a checked 'Display Password' checkbox. An 'Apply' button is at the bottom right of the form.

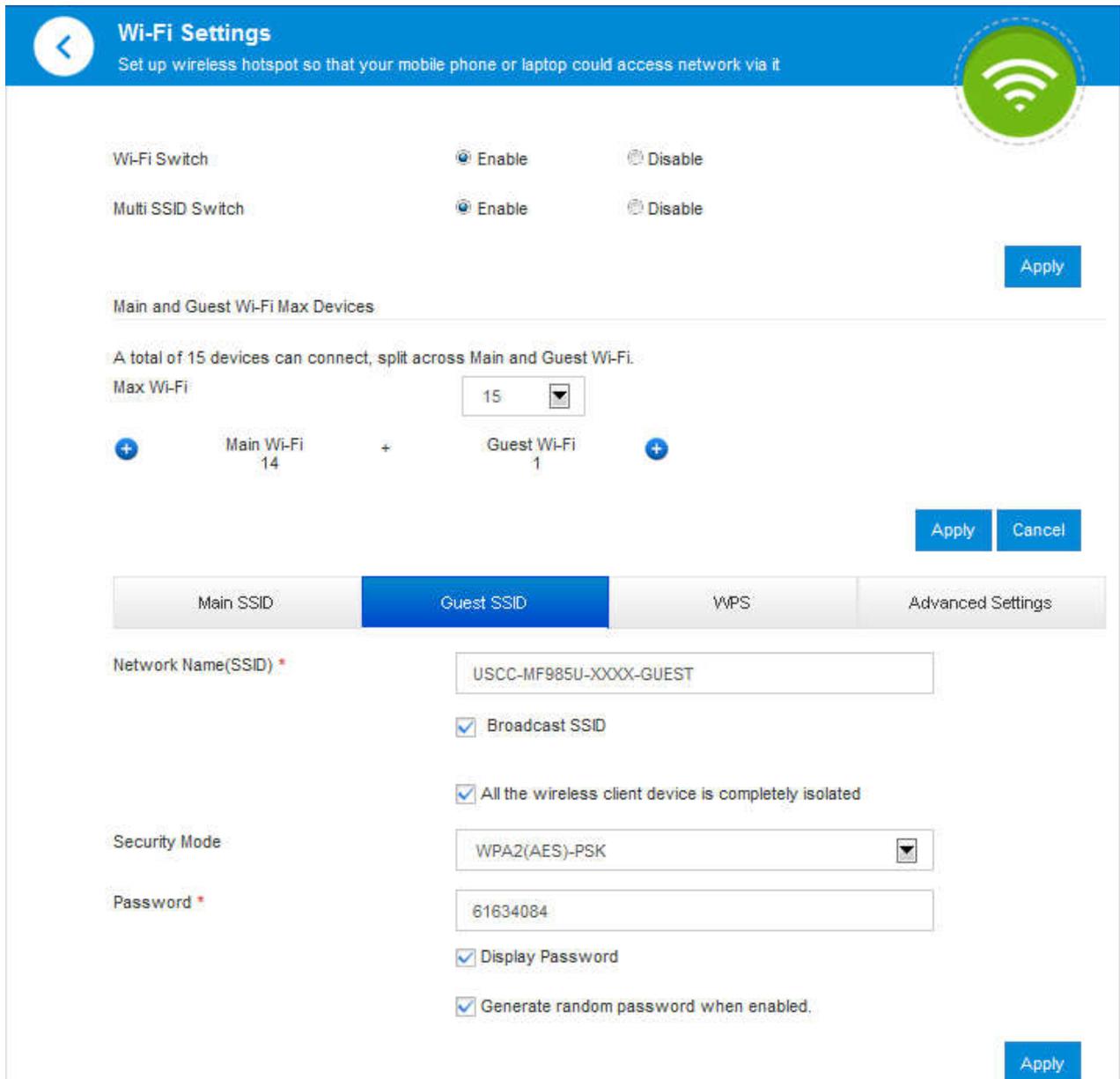
- **Wi-Fi Switch:** Enable or disable Wi-Fi function.
- **Multi SSID Switch:** Enable or disable Multi SSID function. You can use the main SSID and guest SSID at the same time.
- **Main and Guest Wi-Fi Max Devices:** Choose the maximum number of the devices that can connect to the device simultaneously from the drop-down list, these connections are shared between the device's Main and Guest Wi-Fi networks. Click  to adjust the number of connections available for the Main or Guest Wi-Fi networks.
- **Network Name (SSID):** Service Set Identifier (SSID). Enter a string less than 32 characters as the name for your Wi-Fi.
- **Broadcast SSID:** Disable or Enable (Default) this function. When you check the box, the device broadcasts the SSID, and other devices can search and connect to it. When you uncheck the box, other devices cannot search out the SSID. If you want someone to connect, you need to tell them the SSID, and let them setup the connection manually.
- **All the wireless client device is completely isolated:** When you check the box, the devices connected to the Wi-Fi SSID will be unable to communicate with each other.
- **Security Mode:** The security modes are described below:

Mode	Description
OPEN	Authentication and encryption won't be active. There are risks that private information can be intercepted or that the network will be used by unauthorized individuals.
WPA2(AES)-PSK	A more secure version of WPA with implementation of the 802.11i standard.
WPA-PSK/WPA2-PSK	Apply both the WPA-PSK and WPA2-PSK schemes.

- **Password:** Set the password for your wireless local area network.
 - **Display password:** Allow the password to be displayed on the 4G Mobile Hotspot configuration page.
2. Click **Apply** to confirm your configuration.

Guest SSID Settings

1. Select **Settings** below **Wi-Fi** and click **Guest SSID**.
2. Set **Multi SSID Switch** to **Enable**. The Guest SSID basic parameters are shown in the following figure.



- **Network Name (SSID):** Service Set Identifier (SSID). Enter a string less than 32 characters as the name for your Wi-Fi.
- **Broadcast SSID:** Disable or Enable (Default) this function. When you check the box, the device broadcasts the SSID, and other devices can search and connect to it. When you uncheck the box, other devices cannot search out the SSID. If you want someone to connect, you need to tell them the SSID, and let them setup the connection manually.
- **All the wireless client device is completely isolated:** When you check the box, the devices connected to the Wi-Fi SSID will be unable to communicate with each other.
- **Security Mode:** The security modes are described below:

Mode	Description
OPEN	Authentication and encryption won't be active. There are risks that private information can be intercepted or that the network will be used by unauthorized individuals.
WPA2(AES)-PSK	A more secure version of WPA with implementation of the 802.11i standard.
WPA-PSK/WPA2-PSK	Apply both the WPA-PSK and WPA2-PSK schemes.

- **Password:** Set the password for your wireless local area network.
 - **Display password:** Allow the password to be displayed on the 4G Mobile Hotspot configuration page.
 - **Generate random password when enabled:** Allow generate random password for the Guest SSID network.
3. Click **Apply** to confirm your configuration.

<
>

Wi-Fi Settings

Set up wireless hotspot so that your mobile phone or laptop could access network via it.

Wi-Fi Switch Enable Disable

Multi SSID Switch Enable Disable

[Apply](#)

Main and Guest Wi-Fi Max Devices

A total of 15 devices can connect, split across Main and Guest Wi-Fi.

Max Wi-Fi

+
Main Wi-Fi
+
Guest Wi-Fi
+

14
+
1

[Apply](#)
[Cancel](#)

Main SSID	Guest SSID	WPS	Advanced Settings
Wi-Fi Band	<input style="width: 90%;" type="text" value="2.4GHz"/>		
Network Mode	<input style="width: 90%;" type="text" value="802.11 b/g/n"/>		
Channel Bandwidth	<input style="width: 90%;" type="text" value="20MHz/40MHz"/>		
Country/Region Code	<input style="width: 90%;" type="text" value="UNITED STATES"/>		
Frequency (Channel)	<input style="width: 90%;" type="text" value="Auto"/>		

[Apply](#)

- **Wi-Fi Band:** Select the desired frequency for your device.
- **Network Mode:** Select the suitable Wi-Fi network mode.
- **Channel Bandwidth:** Select the bandwidth of the channel.
- **Country/Region Code:** Select the suitable Country/Region Code for your device.
- **Frequency (Channel):** Select appropriate channel to optimize the performance and coverage of your wireless network.

Data Management Settings

1. Click in **Statistics** area, you can create statistic plan, query used and left statistic in the following figure.

2. Set Data Management to Enable.

- **Data Management:** Enable or disable data management function.
 - **Billing date:** Set the usage cycle reset date on the every month.
 - **Used Data:** Check how much data has been used during the time cycle you set. Click  to enter the related parameters.
 - **XX of remaining:** Check how much data remains during the time cycle you set.
 - **Data Alert:** Remind you when used data reaches specified percentage. Click  to adjust the parameters.
 - **Monthly Data Plan:** Set mobile data usage limit. Click  to adjust the parameters.
3. Click **Apply** to confirm your configuration.

Status Information

Click **Detail Information** in **Status Information** area to view the detail status information.

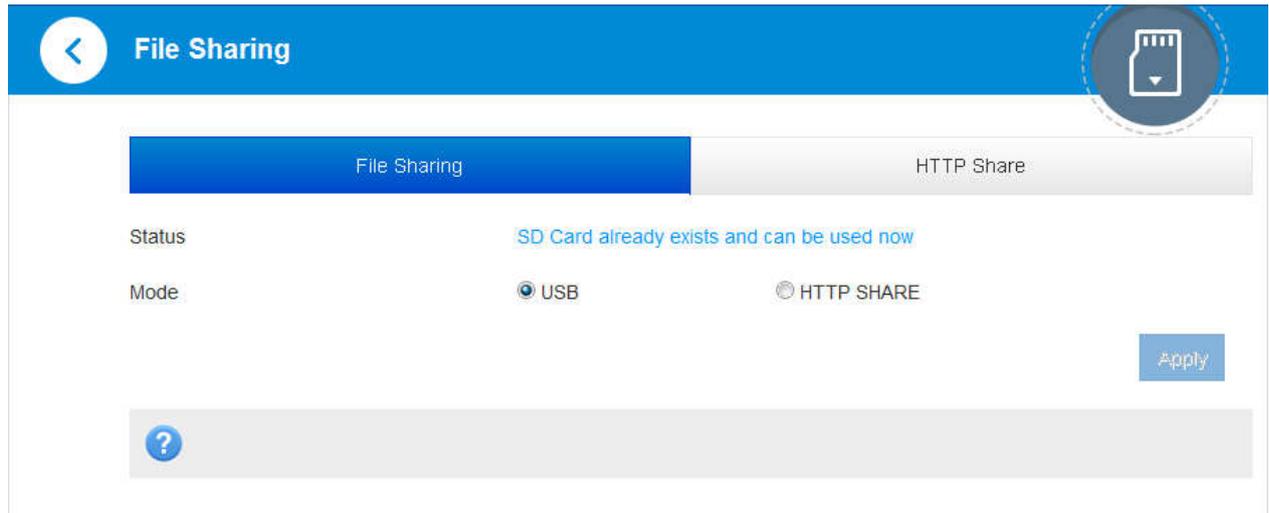
Status Information	
SIM Card Number	— —
MEID(H)/MEI(D)	99000897000025
MEID(D)	256691624700000037
IMSI	460110584812144
Signal Strength	-106 dBm
Network Name(SSID)	USCC-MF985U-XXXX Change
Max Access Number	14
Network Name (Guest SSID)	Disabled Change
Max Access Number (Guest SSID)	Not applicable
Wi-Fi Band	2.4GHz Change
Wi-Fi Coverage	Long
LAN Domain	http://uscc.hotspot
IP Address	192.168.1.1
WAN IP Address	— —
Software Version	USCC_US_MF985UV1.0.0B03
Hardware Version	MF985UHW1.0

File Sharing

File sharing allows you to share the files in a microSDXC card via USB cable or web browser.

Sharing microSDXC Card via USB Cable

1. Log in to the 4G Mobile Hotspot configuration page.
2. Click  to set the sharing mode. The default mode is **USB**.



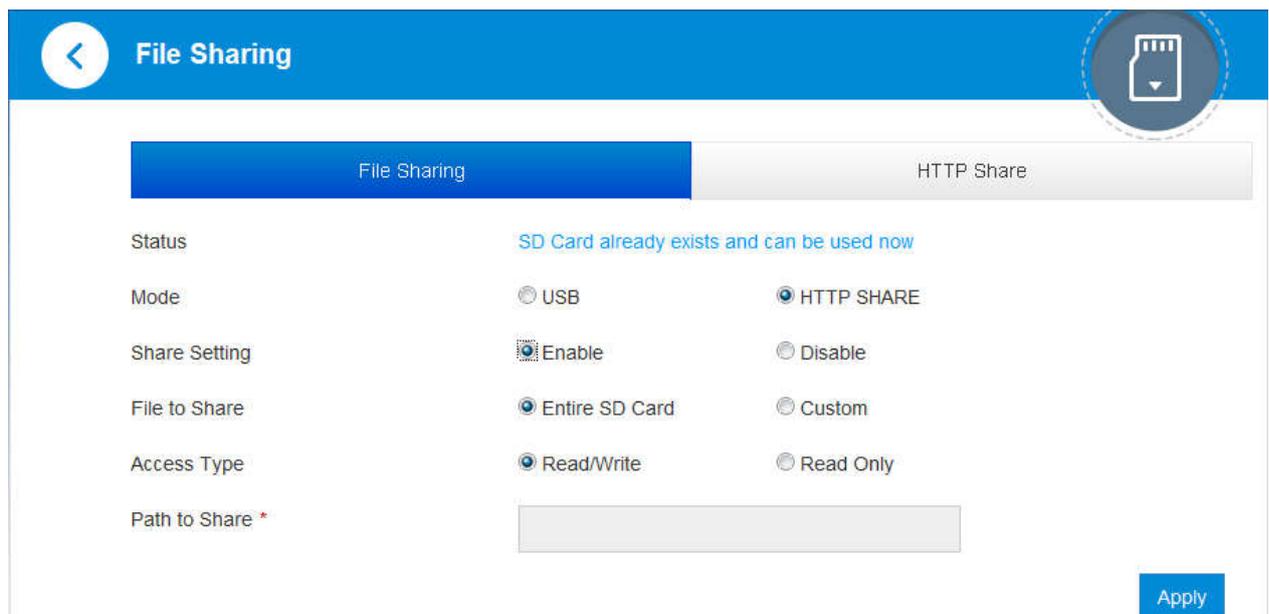
3. Connect the device to PC/Tablet via USB cable.
4. Go to **My Computer** of your PC/Tablet to access all files in microSDXC card.

 **NOTE:**

You can access microSDXC card via USB cable only in USB mode. The web page of sharing microSDXC card will be disabled.

Sharing microSDXC Card via Web Browser

1. Click  on the 4G Mobile Hotspot configuration page.
2. Select **HTTP SHARE** mode.



3. Set **Share Setting** to **Enable**.
4. Set **File to Share**, **Access Type**, and **Path to Share** as you need.

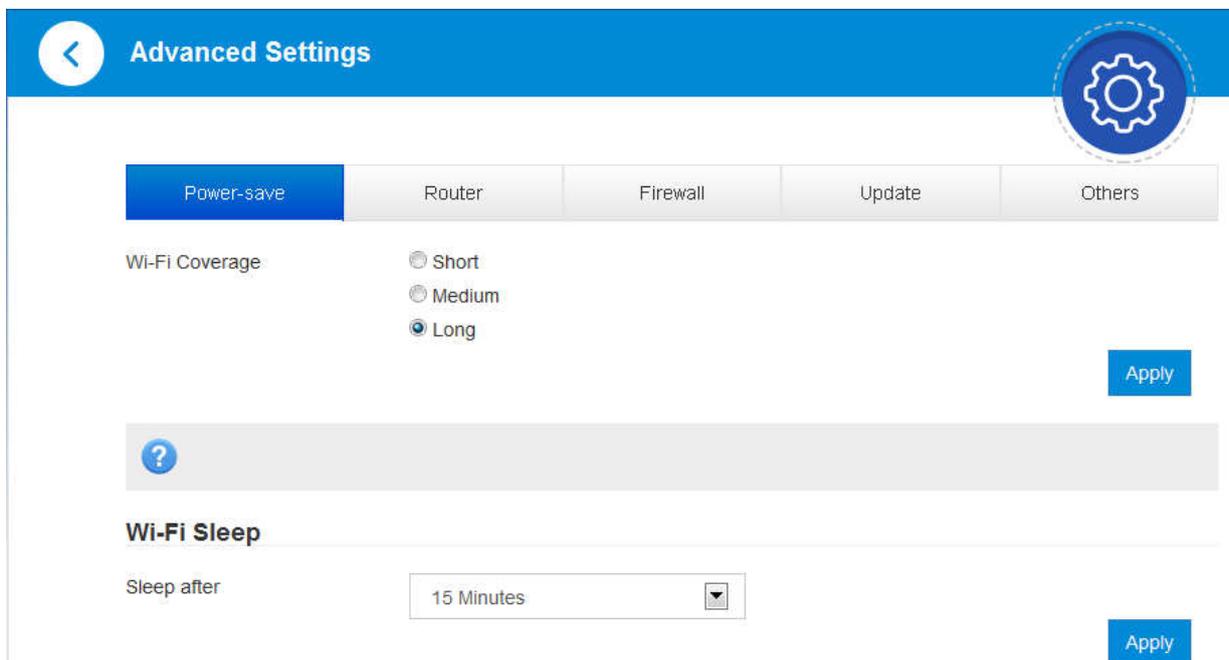
5. Click **Apply** to save the settings.
6. Launch the browser on your PC/Tablet/Smart phone connected to the device via Wi-Fi and enter **http://uscc.hotspot** or **http://192.168.1.1** in the address bar.
7. Click **View SD card** to access the files in microSDXC card.

Advanced Settings

This chapter provides information on how to configure advanced settings for the device such as power-save settings, firewall settings, router settings, etc.

Power-save

Click  > **Power-save** to set the power save settings.



Wi-Fi Coverage

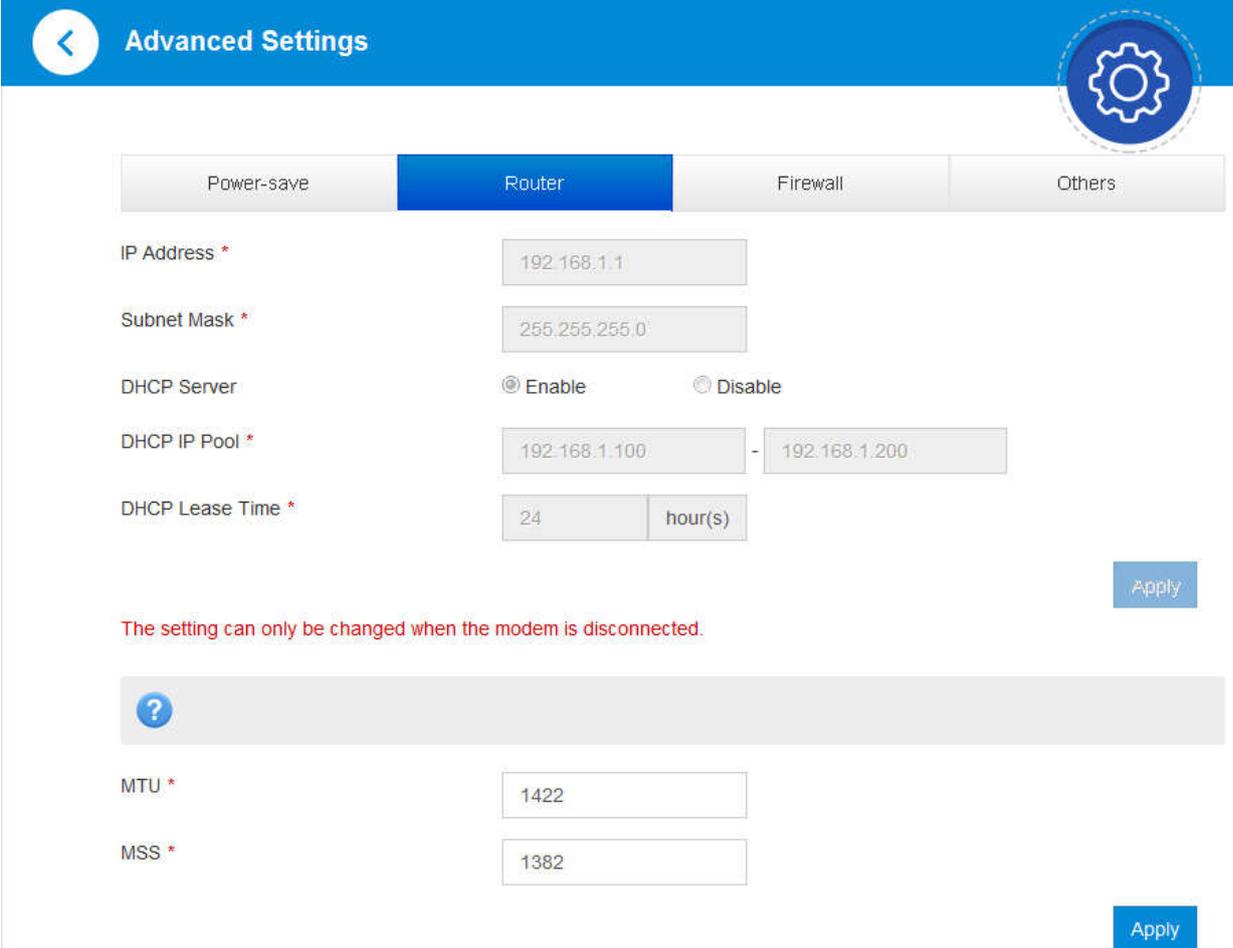
- **Short:** Minimum power consumption and coverage.
- **Medium:** 50% of device power consumption and coverage.
- **Long:** Maximum power consumption and coverage.

Wi-Fi Sleep

Sleep after: Select a time from the drop-down list. When there's no Wi-Fi connection in the specified time, Wi-Fi will be unavailable and the system will turn to sleep mode for power-saving.

Router Settings

1. Click  > **Router**, the router information is shown in the following figure:



The screenshot shows the 'Advanced Settings' interface with the 'Router' tab selected. The settings are as follows:

Setting	Value
IP Address *	192.168.1.1
Subnet Mask *	255.255.255.0
DHCP Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DHCP IP Pool *	192.168.1.100 - 192.168.1.200
DHCP Lease Time *	24 hour(s)
MTU *	1422
MSS *	1382

A warning message is displayed: "The setting can only be changed when the modem is disconnected." There are 'Apply' buttons at the bottom right of the DHCP and MTU/MSS sections.

- **IP Address:** IP address for the LAN interface.
- **Subnet Mask:** Subnet mask for the IP address.
- **DHCP Server:** Enable or disable DHCP Server function.
- **DHCP IP Pool:** Allocate begin and end IP address for IP pool.
- **DHCP Lease Time:** Define how long before the leased IP address will expire. The new IP address will be reallocated after the IP address has expired.

2. Click **Apply** to confirm your configuration.

Firewall

A firewall protects your connected devices against malicious incoming traffic from the

Internet. The firewall cannot be disabled, but the following settings are available.

- **Port Filtering**

1. Click  > **Firewall** > **Port Filtering**, the MAC/IP/Port Filtering section is shown in the following figures.



2. Set **MAC/IP/Port Filtering** to **Enable**, **Default Policy** to **Accepted** or **Dropped** and click **Apply**, the filter settings will appear as shown below:

<
Port Filtering

MAC/IP/Port Filtering Enable Disable

Default Policy Accepted Dropped

Apply

?

MAC/IP/Port Filtering Settings

IP Settings IPv4 IPv6

MAC Address: (e.g., 00:1E:90:FF:FF:FF)

Source IP Address:

Dest. IP Address:

Protocol: ▼

Action Accept Drop

Comment *

Apply

?

Current MAC/IP/Port Filtering Rules in System

<input type="checkbox"/>	MAC Address	IP Type	Source IP Address	Dest. IP Address	Protocol	Source Port Range	Dest. Port Range	/
<							>	

Delete

- **Default Policy:** Set how to handle the packet if none of the rules matches.
 - Accepted:** Internet traffic is allowed by default. Only traffic from the selected applications will be blocked from accessing the Internet. Traffic is identified by port numbers. In particular, you need to know the port numbers and the protocol (TCP, UDP) used by outgoing traffic.
 - Dropped:** Internet traffic is blocked by default. Only traffic from the selected, pre-defined or custom applications is allowed to access the Internet.

- **IP Settings:** Select IPv4 or IPv6.
- **MAC Address:** Set the MAC address that will be filtered.
- **Source IP Address:** Set the source IP address that will be filtered.
- **Dest. IP Address:** Set the destination IP address that will be filtered.
- **Protocol:** Set which protocol will be used for filtering.
- **Action:** Set how to handle the packet if it matches with the rule.
- **Comment:** Type a comment for the filter settings.

**NOTE:**

If rules are in conflict with each other, the first to be triggered will determine how that traffic is handled.

3. Click **Apply** to confirm your configuration.

To add a new rule:

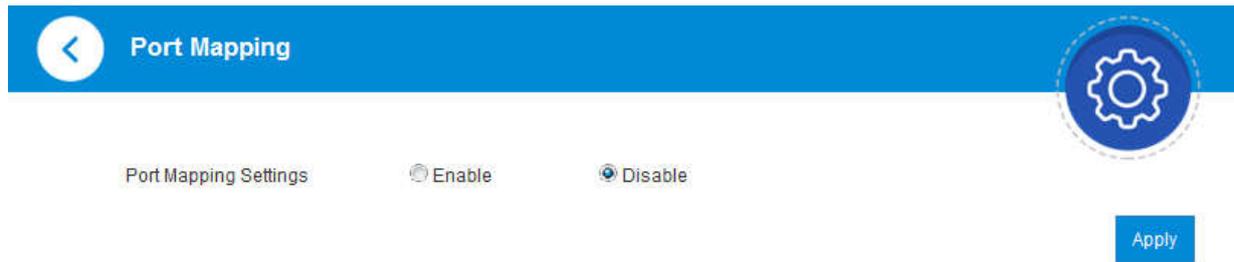
1. Select **Enable**, **Accepted** or **Dropped** in the **Port Filtering** area.
2. Click **Apply**.
3. Input the detailed information in the **MAC/IP/Port Filtering Settings** area.
4. Click **Apply** in the **MAC/IP/Port Filtering Settings** area. The rule will display in the **Current MAC/IP/Port Filtering Rules in System** area.

To delete a rule:

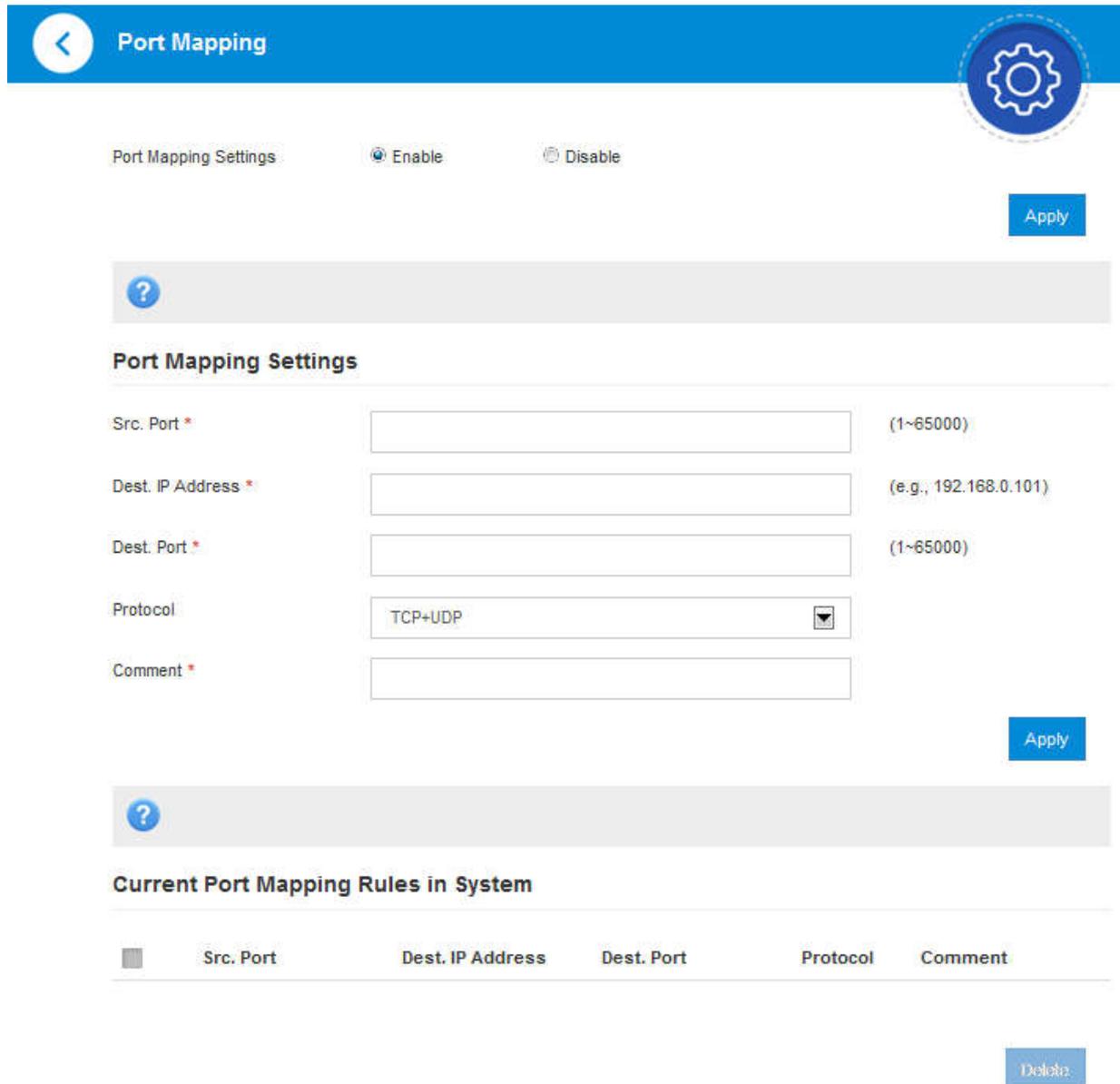
1. Click the rule which you want to delete in **Current MAC/IP/Port Filtering Rules in System** area.
2. Click **Delete** to delete the rule which you selected.

• Port Mapping

1. Click  > **Firewall** > **Port Mapping**, the Port Mapping section is shown in the following figures.



2. If you select **Enable**, and click **Apply**. The following figure will appear:



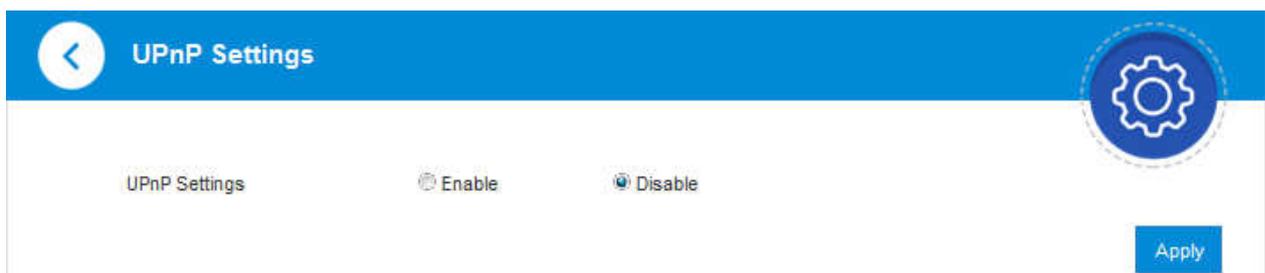
- **Src. Port:** Set the source port that will be filtered.
- **Dest. IP Address:** Set the destination IP address that will be filtered.
- **Dest. Port:** Set the destination Port that will be filtered.
- **Protocol:** Set which protocol will be used for filtering.

- **Comment:** Type a comment for the filter settings.
3. Click **Apply**.
 4. If you want to remove the Port Mapping rule, select the rule and click **Delete**.

- **UPnP**

Universal Plug Play (UPnP) is a set of networking protocols that allows network devices, such as PC, 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.

1. Click  > **Firewall** > **UPnP**. The UPnP settings page is shown in the following figure.

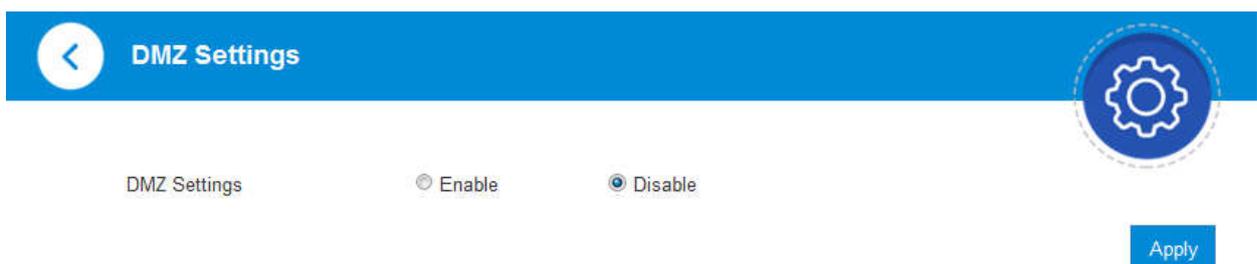


2. Check **Enable** and click **Apply** to enable the function.

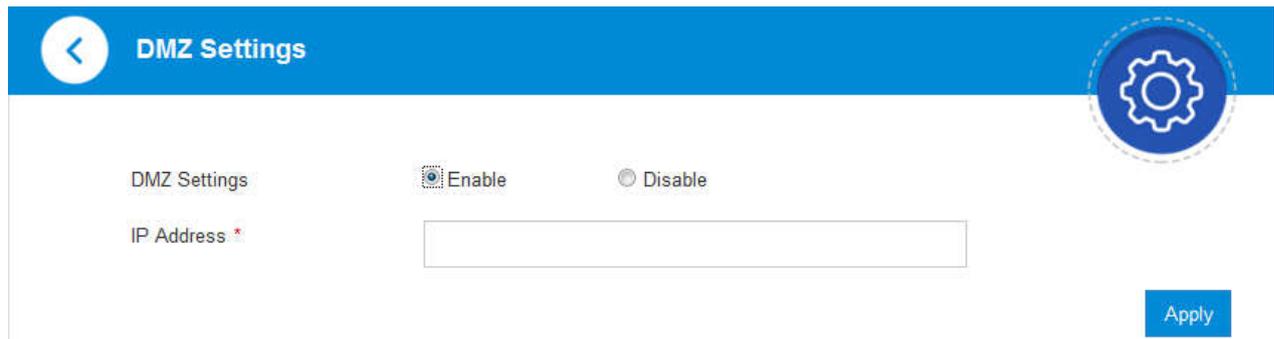
DMZ

The DMZ, or De-Militarized Zone, is a selected internal IP address of a device that allows full access and connectivity from outside traffic, through the firewall, to a specific internal device without being filtered or blocked by your device.

1. Click  > **Firewall** > **DMZ** and the following page will appear:



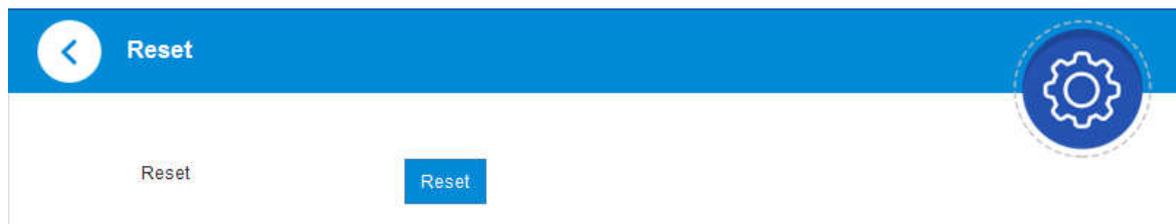
2. If you select **Enable**, the DMZ Settings will appear:



3. Enter the IP address of the device you want to communicate with the Internet unfiltered, and then click **Apply** to save the settings.

Reset

Click  > **Others** > **Reset**. Click **Reset** to set all the settings to their factory default values, and then the device will restart automatically.



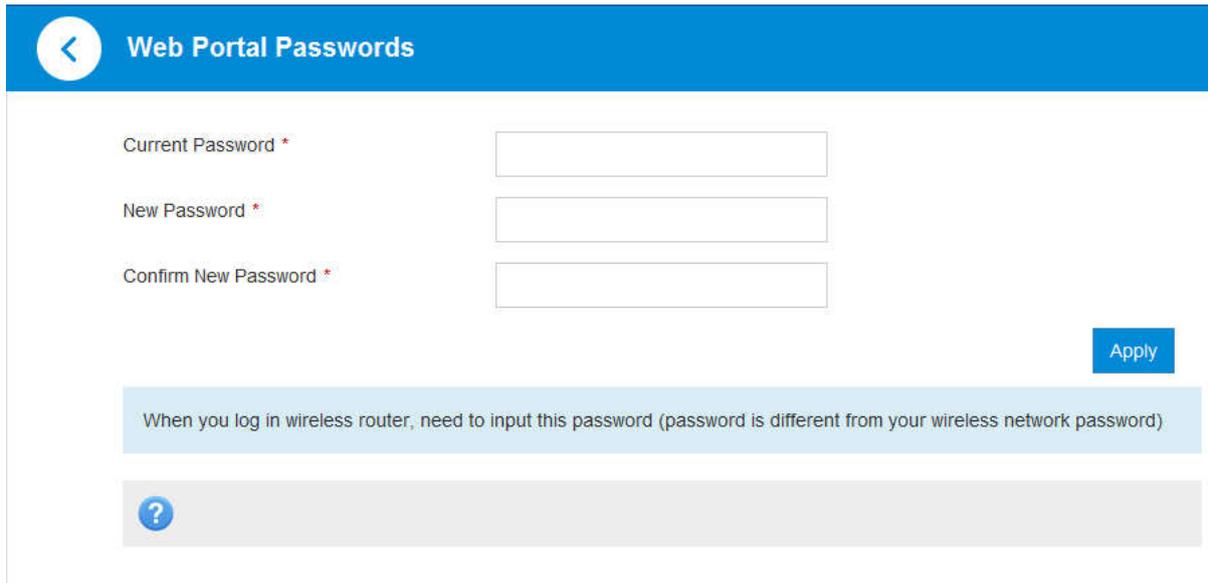
Restart

Click  > **Others** > **Restart**. Click **Restart** to restart your device manually.



Web Portal Passwords

1. Click **Web Portal Passwords** to manage the login password of the 4G Mobile Hotspot configuration page.



Current Password: Enter the current password.

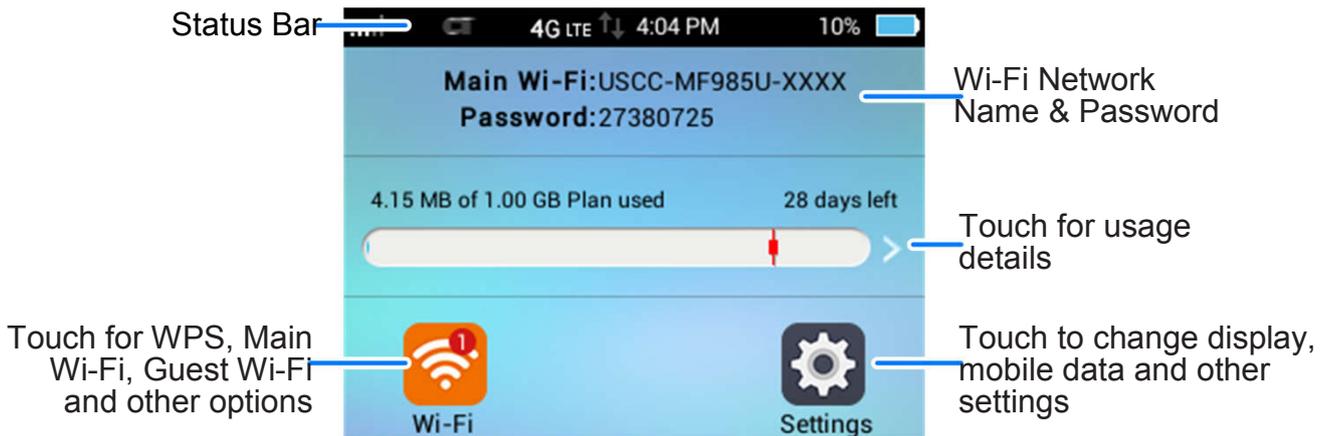
New Password: Enter the new password.

Confirm New Password: Enter the new password again.

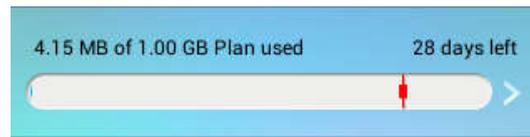
2. Click **Apply** to save your settings.

Touch Screen

You can configure basic Wi-Fi and display settings, view data usage details, customize and configure your device from the touch screen.



Data Usage



You can check how much data has been used on the home page, or touch to set mobile data limit and warning, monthly data plan, and usage cycle rest date.

- **Data Usage Limit:** Turn on or off data usage limit function.
- **Monthly Data Plan:** Set mobile data limit.
- **Used Data:** Check how much data has been used during the time cycle you set. Touch to adjust the parameters.
- **Data Alert:** Remind you when used data reaches specified percentage. Touch to adjust the parameters.
- **Billing date:** Set the usage cycle reset date on the every month.

Wi-Fi

Touch  to configure basic Wi-Fi settings.

- **Wi-Fi:** Turn on or off Wi-Fi.
- **Main Wi-Fi Network:** Touch to view Main Wi-Fi network name and password. You can also touch **WPS > Pair with Main Wi-Fi** to connect other devices to your device without entering your password.
- **Guest Wi-Fi Network:** Touch to turn on or off Guest Wi-Fi network and view network name and password. You can also touch **WPS > Pair with Guest Wi-Fi** to connect other devices to your device without entering your password.
- **WPS:** Touch **Pair with Main Wi-Fi** or **Pair with Guest Wi-Fi** to connect other devices to your device without entering your password.
- **Connected Devices:** View all of wireless devices connected to your device. Touch the device you want to block and touch **Block > OK**, and then it will be added to the Black List. Or touch **Block List**, devices on the black list will not be able to use the

device to connect to the network.

- **Max Wi-Fi Devices:** Touch  /  next to **Max Wi-Fi** to set the maximum number of the devices that can connect to the device simultaneously, these connections are shared between the device's Main and Guest Wi-Fi networks. Touch  to adjust the number of connections available for the Main or Guest Wi-Fi networks.
- **Wi-Fi Band:** Select the desired frequency for your device.
- **Wi-Fi Range:** Select the range for your device.
- **Wi-Fi Sleep Mode:** Select the length of time for your Wi-Fi signal broadcast to remain active if no devices are connected.

Settings

Touch  to configure basic device settings.

- **Allow Mobile Data:** Slide the switch next to **Standard Data** to turn on or off mobile data.
- **Data Roaming:** Slide the switch next to **Data Roaming** to turn on or off data roaming.
- **Data usage:** Check how much data has been used or set mobile usage limit and warning. See [Data Usage](#).
- **Display**
 - ▶ **Screen Brightness:** Set the brightness of the touch screen as you need.
 - ▶ **Display Timeout:** Set the length of time of inactivity before the screen turns off automatically.
 - ▶ **Wi-Fi Info on Home Screen:** Set whether Wi-Fi information should be displayed on the home screen.
- **Lock Screen (PIN):** Disable the screen lock or enable it with PIN.
- **Software Update:** Check, download and install the system updates.
- **Factory Reset:** Touch **Factory Reset > Reset device** to reset the device to its factory

default settings.

- **About Your Device:** Touch to view important device information and legal information.

Warning and Notice

To the Owner

- Some electronic devices are susceptible to electromagnetic interference sent by your device if inadequately shielded, such as the electronic system of vehicles. Please consult the manufacturer of your device before using if necessary.
- Operating your device may interfere with medical devices like hearing aids and pacemakers. Please always keep them more than 20 centimeters away from such medical devices when they are turned on. Turn your device off if necessary. Consult a physician or the manufacturer of the medical device before using your device.
- Be aware of the usage limitation when using your device at places such as oil warehouses or chemical factories, where there are explosive gases or explosive products being processed. Turn off your device if required.
- The use of electronic transmitting devices is forbidden in aircrafts, at petrol stations and in hospitals. Please observe and obey all warning signs and switch off your device in these conditions.
- Do not touch the inner antenna area if not necessary. Otherwise it will affect your device's performance.
- Store your device out of the reach of little children. Your device may cause injury if used as a toy.
- Do not touch the metallic parts of your device so as to avoid a burn, when your device is working.

Using Your Device

- Please use original accessories or accessories that are authorized. Using any unauthorized accessories may affect your device's performance, and violate related national regulations about telecom terminals.
- Avoid using your device near or inside metallic structures or establishments that can emit electromagnetic waves. Otherwise it may influence signal reception.
- Your device is not waterproof. Please keep it dry and store in a shady and cool place.
- Do not use your device immediately after a sudden temperature change. In such case, it will produce dew inside and outside your device, so don't use it until it becomes dry.
- Handle your device carefully. Do not drop, bend or strike it. Otherwise your device will

be damaged.

- No dismantling by non-professionals and only qualified technicians can undertake repair work.
- Operating temperature range of 0°C ~ +35°C and humidity range of 5% ~ 95% are recommended.
- Do not connect the charger while using the device for a long period. Failing to do so will trigger the protection mechanism of the battery, and the battery will not be charged. If you want to charge the battery, please reconnect the charger.
- Do not connect the charger while using the device for a long period or use the device and battery in non-operating temperature. Failing to do so will shorten battery life or cause battery swelling or leakage. If the battery shows signs of swelling or leakage, please stop use immediately.

Using Battery

- Do not short-circuit the battery, as this can cause excessive heat and fire.
- Do not store battery in hot areas or dispose of it in a fire to avoid explosion.
- Do not disassemble or modify the battery.
- When not using the battery for a long period, remove it from your device and store it in a cool dry place.
- Never use any charger or battery damaged or worn out.
- Return the wear-out battery to the provider or put it in the appointed recycle place. Do not put it in familial rubbish.

WARNING!

If the battery is broken, keep away from it. If it taints your skin, wash your skin with abundant fresh water and ask doctor for help if necessary.

Limited Warranty

- This warranty does not apply to defects or errors in the Product caused by:
 - i. Reasonable abrasion.
 - ii. End User's failure to follow ZTE's installation, operation or maintenance instructions or procedures.
 - iii. End User's mishandling, misuse, negligence, or improper installation, disassembly, storage, servicing or operation of the Product.
 - iv. Modifications or repairs not made by ZTE or a ZTE-certified individual.

- v. Power failures, surges, fire, flood, accidents, actions of third parties or other events outside ZTE's reasonable control.
- vi. Usage of third-party products, or usage in conjunction with third-party products provided that such defects are due to the combined usage.
- vii. Any other cause beyond the range of normal usage intended for the Product.

End User shall have no right to reject or return the Product, or receive a refund for the Product from ZTE under the above-mentioned situations.

- This warranty is End User's sole remedy and ZTE's sole liability for defective or nonconforming items, and is in lieu of all other warranties, expressed, implied or statutory, including but not limited to the implied warranties of merchantability and fitness for a particular purpose, unless otherwise required under the mandatory provisions of the law.

Limitation of Liability

ZTE shall not be liable for any loss of profits or indirect, special, incidental or consequential damages resulting from or arising out of or in connection with using of this product, whether or not ZTE had been advised, knew or should have known of the possibility of such damages, including, but not limited to lost profits, interruption of business, cost of capital, cost of substitute facilities or product, or any downtime cost.

FCC Regulations:

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.

This device 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.

CAUTION:

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC RF Exposure Information (SAR)

This device is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission of the United States.

During SAR testing, this device is set to transmit at its highest certified power level in all tested frequency bands, and placed in positions that simulate RF exposure in usage against the head with no separation, and near the body with the separation of 10 mm. Although the SAR is determined at the highest certified power level, the actual SAR level of the device while operating can be well below the maximum value. This is because the device is designed to operate at multiple power levels so as to use only the power required to reach the network. In general, the closer you are to a wireless base station antenna, the lower the power output.

The exposure standard for wireless devices employs a unit of measurement known as the Specific Absorption Rate, or SAR. The SAR limit set by the FCC is 1.6 W/kg.

Tests for SAR are conducted using standard operating positions accepted by the FCC with the device transmitting at its highest certified power level in all tested frequency bands.

The FCC has granted an Equipment Authorization for this model device with all reported SAR levels evaluated as in compliance with the FCC RF exposure guidelines. SAR information on this model device is on file with the FCC and can be found under the Display Grant section of www.fcc.gov/oet/ea/fccid after searching on FCC ID:

SRQ-MF985U.

For this device, the highest reported SAR value for usage near the body is 1.231 W/kg. While there may be differences between the SAR levels of various devices and at various positions, they all meet the government requirement.

SAR compliance for body operation is based on a separation distance of 10 mm between the unit and the human body. Carry this device, at least **10** mm away from your body to ensure RF exposure level compliant or lower to the reported level. To support body operation, choose the belt clips or holsters that do not contain metallic components to maintain a separation of **10** mm between this device and your body.

Troubleshooting

Problem	Suggested Solution
Cannot establish the Wi-Fi connection between your device and client.	<ul style="list-style-type: none"> • Refresh network list and select the correct SSID. • Check the IP address to make sure your client can obtain an IP address automatically in the Internet protocol (TCP/IP) properties. • Type the correct network key (Wi-Fi password) when

	you connect to the device.
The client connected to the device cannot access the Internet.	<ul style="list-style-type: none"> • Make sure your nano-SIM card is available. • Change the location to find a place with good signal. • Contact your service provider.
Cannot visit the 4G Mobile Hotspot configuration page.	<ul style="list-style-type: none"> • Enter the correct address. The default address is http://192.168.1.1 or http://uscc.hotspot. • Only use one network adapter in your PC. • Do not use any proxy server.
About the password	<ul style="list-style-type: none"> • Check the SSID on the LCD screen and Wi-Fi connection password or check the label on the device to get them. • Check the default login password on the LCD screen or check the label on the device to get it. • If you changed the password and forgot the new password, you need to restore the device to the factory default settings.

For more assistance, please:

- Send an E-mail to mobile@zte.com.cn
- Visit www.ztedevice.com