5G Mobile Hotspot

User Manual

Model: JEXtream 5G RedCap Mobile Hotspot

NOTE: All pictures and drawings shown in this document are for illustration purpose only. Actual product may vary due to product variants and enhancement.

Contents

1

Getting Started

Overview

Thank you for choosing your 5G Mobile Hotspots, RG350

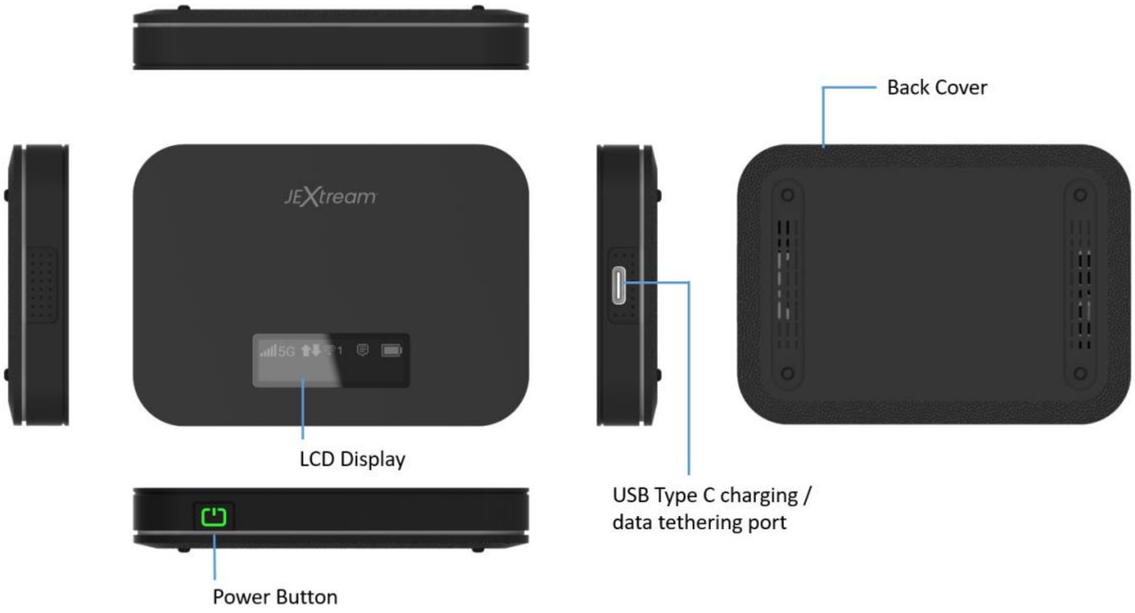
Having the RG350 Mobile Hotspot at your fingertips will allow you to access 5G network for fast uploads and downloads. You can also connect up to 15 Wi-Fi capable devices to the Internet at once - Laptops, Tablets, eReaders, Smartphones and more.

System Requirements

- Compatible with all IEEE802.11 b/g/n/ac Wi-Fi 2.4 & 5GHz enabled devices.
- Works with the latest versions of most browsers*.

** It is recommended to use the latest versions of Internet browsers. Outdated versions may not be compatible with the Mobile Hotspot Web Admin User Interface, http://mobile.hotspot*

Components



Power/Menu Button – Turn on/off your Mobile Hotspot. Navigate device information

Button Operation

	Operations	Actions
⏻	Turn On	Press and hold the button until “Welcome” message appears.
	Turn Off	Press and hold the button until “Goodbye” message appears.
	Display Wake-Up	When the display is off (sleep mode), the first quick press of the button wakes up the display.
	Info Display	When the display is on, press the button quickly to go through the device information.

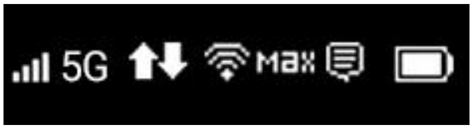
LED Indicator

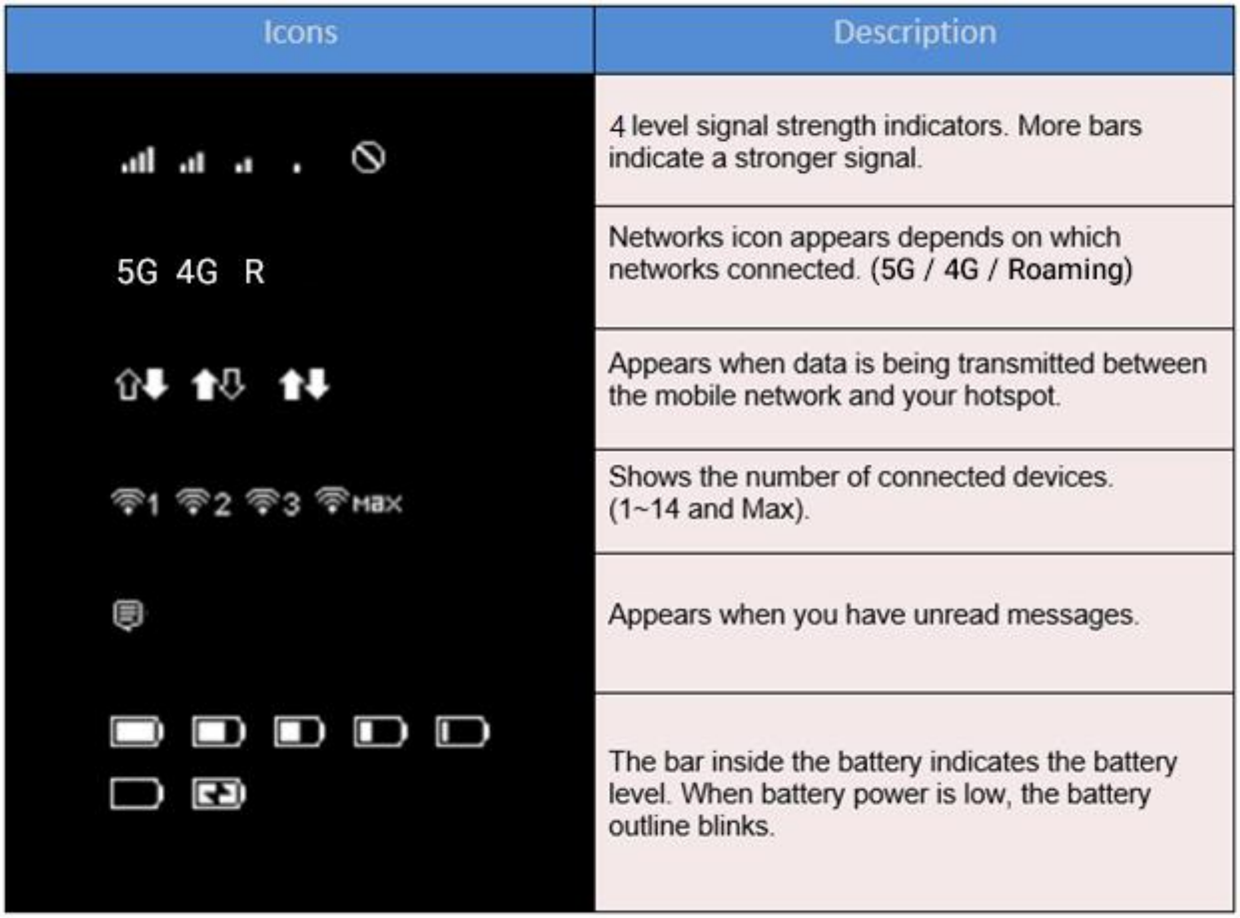
	Colors	Charging Status
⏻	Off	Powered off and not connected to a charger.
⏻	Solid	Connected to a charger and the battery is fully charged.
⏻	Blinking	Powered on and operating normally. Powered off and the battery is being charged.

LCD Display – Provides device status information such as battery, service signal strength, the number of users connected with Wi-Fi etc.

USB Type C Charging / Data Port – The USB charger connects here. The port is also used for USB data tethering to your PC or MAC devices.

Device Display Icons





Icons	Description
.ıll .ıl .ı . ⊘	4 level signal strength indicators. More bars indicate a stronger signal.
5G 4G R	Networks icon appears depends on which networks connected. (5G / 4G / Roaming)
⇧⬇ ⬆⇩ ⬆⬇	Appears when data is being transmitted between the mobile network and your hotspot.
ᯤ1 ᯤ2 ᯤ3 ᯤMax	Shows the number of connected devices. (1~14 and Max).
✉	Appears when you have unread messages.
▭ ▭ ▭ ▭ ▭ ▭ ▭	The bar inside the battery indicates the battery level. When battery power is low, the battery outline blinks.

Battery Management

Your Mobile Hotspot is equipped with a replaceable and rechargeable battery. It works from its charged battery alone or plugged into a power source.

Note: Please do not attempt to open or disassemble your Mobile Hotspot and the battery pack. Doing so may cause damage that voids your warranty.
Charge the battery with the charger provided together with your Mobile Hotspot. While the battery is charging, the battery charging icon 🔋 displays.

IMPORTANT! Please use only an approved charger to charge your Mobile Hotspot battery. Improper handling of the charging port, as well as the use of an incompatible charger, may cause damage to your device and void the warranty.

2

Using Your Mobile Hotspot

Accessing the Network
Using Your Mobile Hotspot for the First Time
Connecting to Your Mobile Hotspot
Using Your Mobile Hotspot After Setup is Complete

Accessing the Network

Your Mobile Hotspot works effectively anywhere with reliable broadband speed that your 5G service provider offers. You can connect to the internet at speeds fast enough to keep up to date on all your email correspondence, download attachments, and access intranet.

Using Your Mobile Hotspot for the First Time

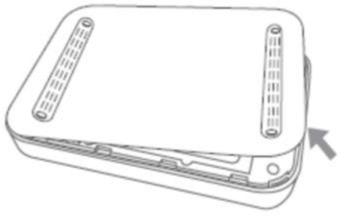
System Requirements

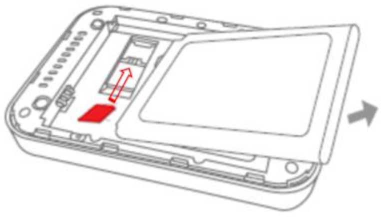
Your computer, tablet, or other wireless devices need Wi-Fi capability and Internet browser only. Your Mobile Hotspot is compatible with most major operating systems and the latest versions of browsers.

Installing the SIM Card

Your SIM (Subscriber Identity Module) card is a small rectangular plastic card that stores important information about your wireless service. The SIM card could be pre-inserted or could be obtained from your wireless service provider upon your subscription. If not already installed, follow the instructions below to install the SIM card.

1. Remove the back cover of your device and take the battery out.
2. Place the SIM card on the SIM slot tray with your Wireless Carrier logo facing up, gently press down and slide it into the SIM card slot.
3. Properly install the battery and put the back cover on.





IMPORTANT! Do not bend or scratch the SIM card. Avoid exposing the SIM card to static electricity, water, or dirt. Whenever you insert or remove the SIM card, ensure your Mobile Hotspot is powered off and is not connected to any power source. Never use tools, knives, keys, or any type of object to force the door open or to remove the SIM card.

Charging the Battery

Before using your Mobile Hotspot, ensure that the battery is fully charged. Be sure to use the charger that came with your device.

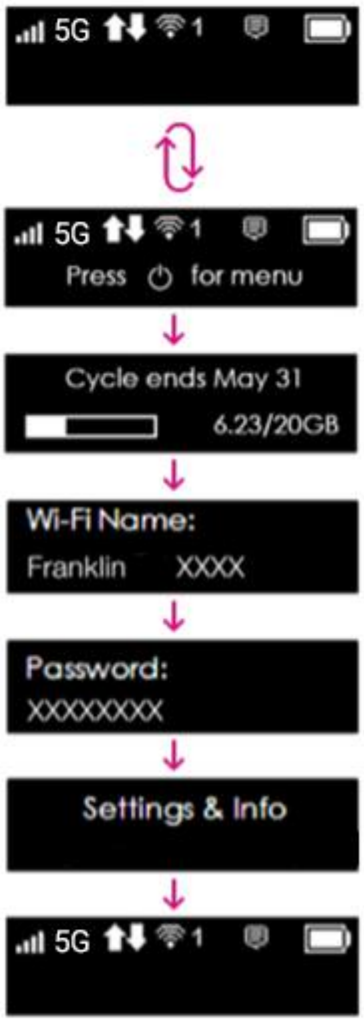
NOTE: Your Mobile Hotspot is equipped with a replaceable rechargeable battery. When handling the battery or SIM card, please make sure the device is not connected to any power sources. Do not use any tools, sharp objects or any utensils when dealing with the battery. Doing so may cause damage that voids your warranty.

- It normally takes 3~5 hours, depending on your power sources and device status to fully charge the battery.
- The battery discharges faster as additional devices connect to your hotspot.
- Battery usage time depends on the network, signal strength, temperature, features, and active connection time.
- When charging, keep your device near room temperature.
- Never leave the Mobile Hotspot in an unattended vehicle due to uncontrolled temperatures that may be outside the desired temperatures for your device.
- It is normal for batteries to gradually wear down and require longer charging time.

Connecting to Your Mobile Hotspot

Wi-Fi Name (SSID) and Password

You can find your Wi-Fi Name and Password any time you need on the device display. Just press the power/menu button (⏻) shortly when the display is on.



Press ⏻ quickly	Home screen, Device menu guide (Switching every 3 seconds)
Press ⏻ quickly	Data usage display
Press ⏻ quickly	Wi-Fi Name display
Press ⏻ quickly	Password display
Press ⏻ quickly	**Web Admin Home** page URL Guide display
Press ⏻ quickly	Back to Home screen

Connecting to the Internet

1. Open the Wi-Fi application or controls on your laptop or Wi-Fi capable device that you want to connect to your Mobile Hotspot. Then find your Mobile Hotspot's Wi-Fi name.
2. Click **Connect** and enter the Password when prompted.

NOTE: The last four characters of your Wi-Fi Name is unique for your Mobile Hotspot. You can change the Wi-Fi Name of your own. See "Settings".

Using Your Mobile Hotspot after Setup is Complete

Mobile Hotspot to share connections

You can use your Mobile Hotspot as a wireless local network gateway to connect maximum 15 Wi-Fi capable devices to the mobile broadband network.

Web Admin Home Page Password Change

The Mobile Hotspot comes from the factory with security turned on. By default, **Web Admin Home** page password is 'admin'. Open a browser and visit your device Web Admin Home page, http://mobile.hotspot. Enter default password 'admin' to sign in. It will automatically guide you to change the **Web Admin Home** password.

After you change your **Web Admin Home** password, you will be required to use the new password to sign into the **Web Admin** home again.

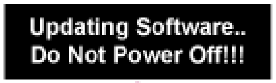
You can change the **Web Admin Home** password any time. To change your **Web Admin Home** password:

1. Connect your Wi-Fi capable device to your Mobile Hotspot.
2. Open a web browser and enter http://mobile.hotspot .
3. From the **Web Admin Home** page, click **Settings > Device > Web Interface**.

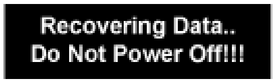
Updating Your Mobile Hotspot software

New software is updated automatically in the following scenarios.

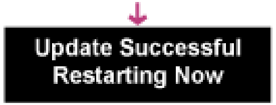
1) Every power up the device will check for a new SW update.
2) If a new update is available, it will be downloaded in the background and wait to be applied on the next power off.
3) The device must have at least 40% battery alone or 20% connected to a charger to apply the update.
4) If the device is continuously powered on, the update will be automatically applied at 2AM next day.
5) If there is traffic or data activity for at 2AM next day, the device will wait until next day 2AM to apply the update.


Updating Software..
Do Not Power Off!!!

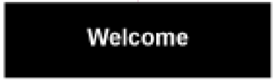
Update starts

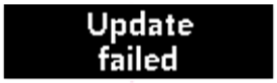

Recovering Data..
Do Not Power Off!!!

Updating


Update Successful
Restarting Now

Update successfully
and Reboot System


Welcome


Update
failed

Update failed

3

Mobile Hotspot Settings

Managing Your Web Admin Home Page
Home
Messages
Settings
About
Support

Managing Your Web Admin Home Page

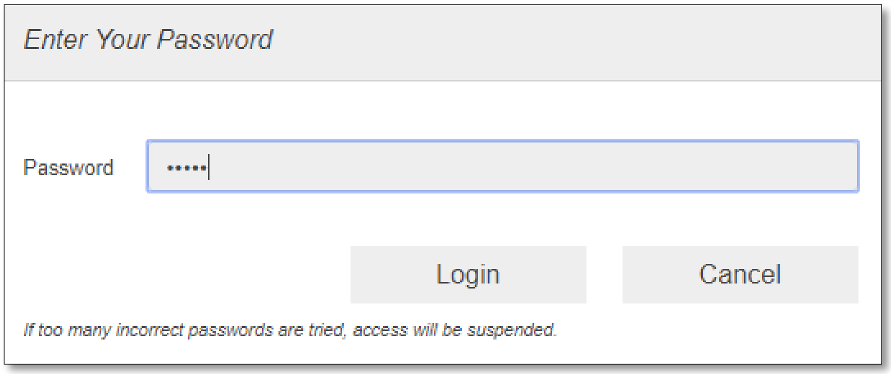
Access the Mobile Hotspot Web Admin Home Page

You can access your Mobile Hotspot Admin Home Page using an internet browser.

Access Mobile Hotspot Web Admin Home Page using a browser

1 Connect your Wi-Fi capable device to the Mobile Hotspot.
2 Open a web browser on your connected device and visit http://mobile.hotspot .
Enter the password and Click **Login.**

NOTE: The default password is 'admin'. On your first login, you will be directed to 'Change password'



Enter Your Password

Password •••••

If too many incorrect passwords are tried, access will be suspended.

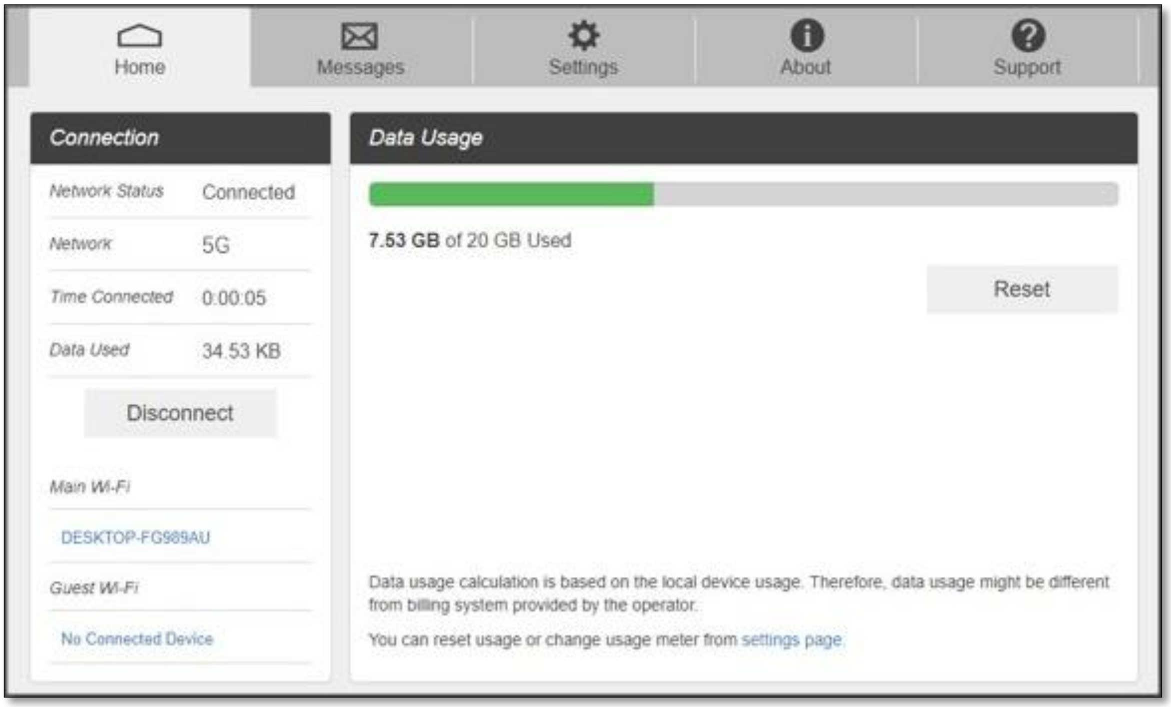
The **Web Admin Home** page allows you to access all menu options for your Mobile Hotspot.

- **Home**
- **Messages**
- **Settings**
- **About**
- **Support**

Home

Check status of network connection and data usage on the Home page.

- Disconnect: Click Disconnect to disconnect the Internet.
- Reset: Reset data usage meter to zero.



Connection

Network Status	Connected
Network	5G
Time Connected	0:00:05
Data Used	34.53 KB

Main Wi-Fi

DESKTOP-FG989AU

Guest Wi-Fi

No Connected Device

Data Usage

7.53 GB of 20 GB Used

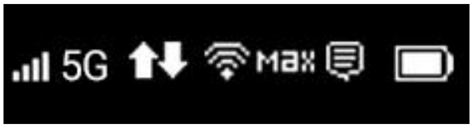
Data usage calculation is based on the local device usage. Therefore, data usage might be different from billing system provided by the operator.

You can reset usage or change usage meter from settings page

Messages

Messages page displays SMS messages your device receives.

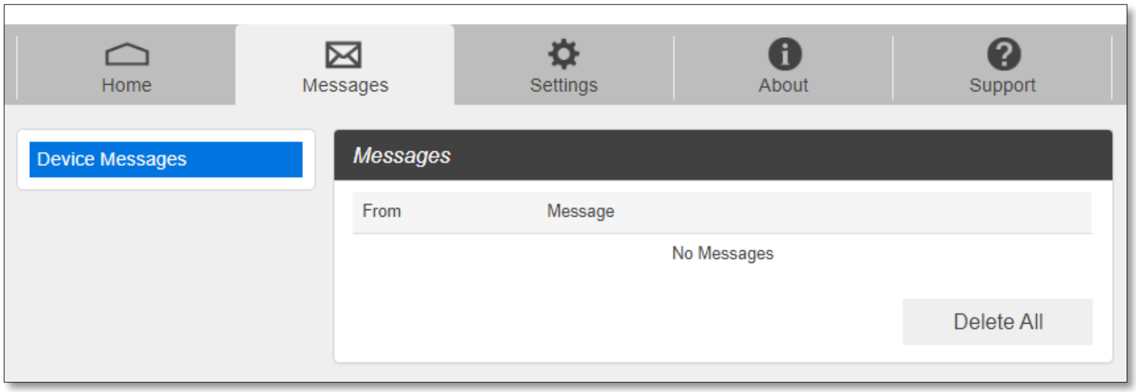
On the Mobile Hotspot device display



When a new message arrives, the message icon appears.

On the Mobile Hotspot Web Admin Home page

You can see the message contents by pressing the **Messages** menu on your **Web Admin** home page. To delete an individual message, click the **Delete** button on the right side of the message. To delete all messages, click **Delete All** Messages button.



No Messages

Settings

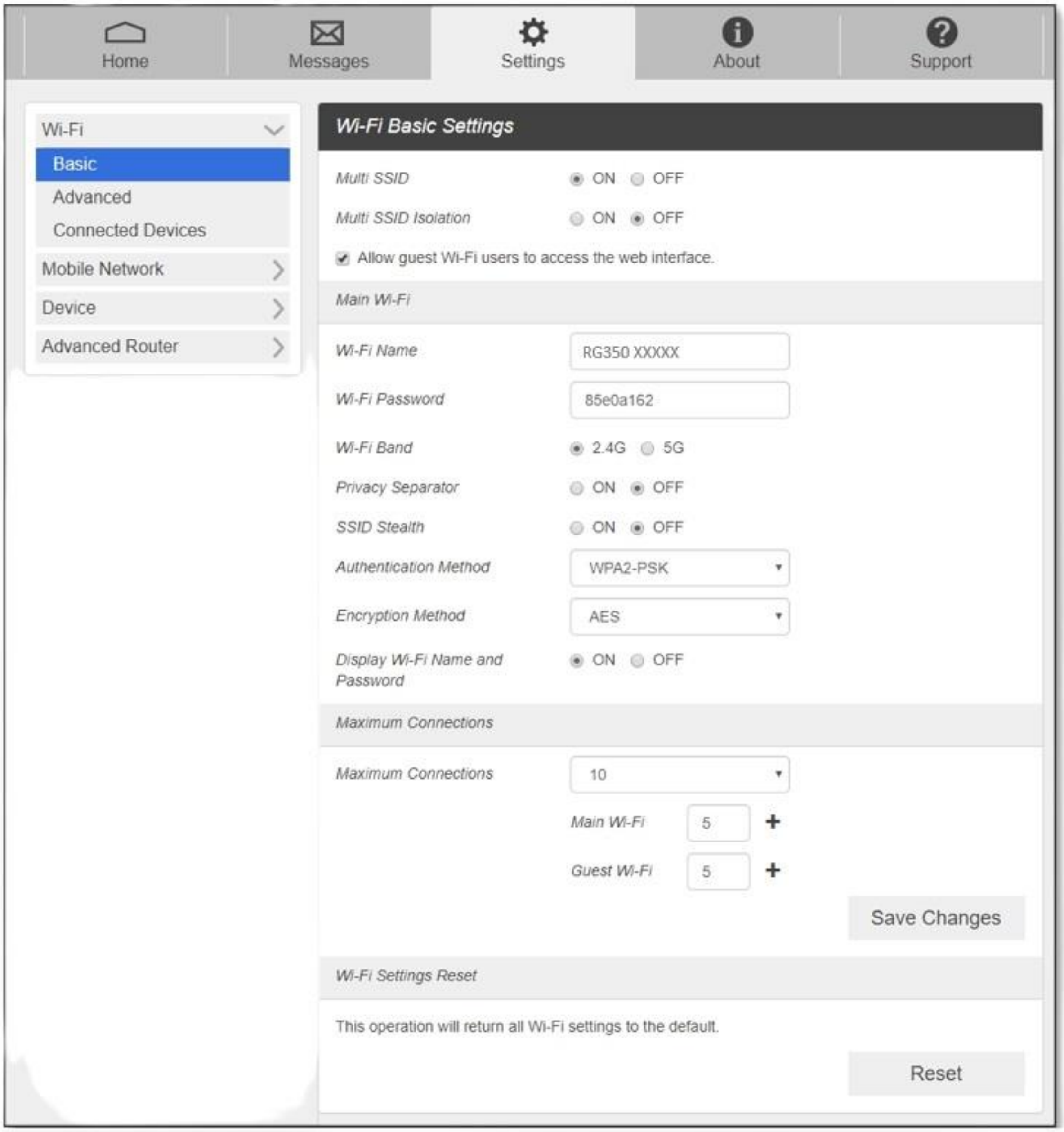
The **Settings** page has the following menu options.

- **Wi-Fi**
- **Mobile Network**
- **Device**
- **Advanced Router**

Wi-Fi

The **Wi-Fi** menu contains the following options:

- **Basic** : the basic Wi-Fi network settings.



Wi-Fi Basic Settings

Multi SSID ● ON ○ OFF

Multi SSID Isolation ○ ON ● OFF

☑ Allow guest Wi-Fi users to access the web interface.

Main Wi-Fi

Wi-Fi Name: RG350 XXXXX

Wi-Fi Password: 85e0a162

Wi-Fi Band ● 2.4G ○ 5G

Privacy Separator ○ ON ● OFF

SSID Stealth ○ ON ● OFF

Authentication Method: WPA2-PSK

Encryption Method: AES

Display Wi-Fi Name and Password ● ON ○ OFF

Maximum Connections

Maximum Connections: 10

Main Wi-Fi: 5 +

Guest Wi-Fi: 5 +

Wi-Fi Settings Reset

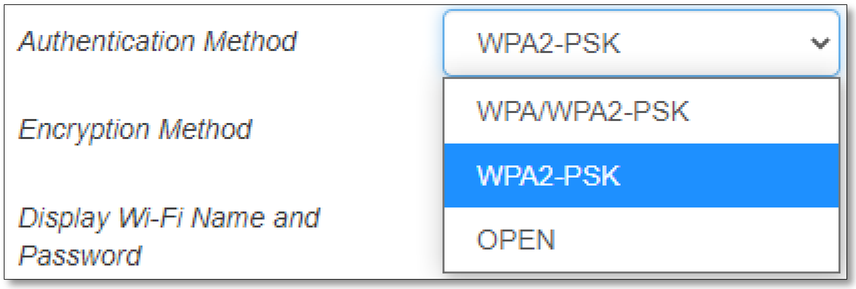
This operation will return all Wi-Fi settings to the default.

- <u>Multi SSID</u>: Select ON if you like to set up a separate guest Wi-Fi network. Your Mobile Hotspot will broadcast two Wi-Fi Names.
- <u>Guest Wi-Fi</u>: If ON is selected for Multi SSID, Guest Wi-Fi menu will appear. You can change Guest Wi-Fi settings.
- <u>Multi SSID Isolation</u>: If On is selected, it prevents your devices from communicating across the Main and Guest Wi-Fi access points.
- <u>Allow Guest Wi-Fi users to access the Web interface</u>: If the box is checked, users on the Guest Wi-Fi also can access the Web User Interface.
- <u>Wi-Fi Name</u>: Service Set Identifier (SSID). To change it, enter a string less than 32 characters as the name for your wireless local area network (WLAN).

- Wi-Fi Password: To change, enter the new Wi-Fi password. The password needs to be at least 8 characters long. I Privacy Separator: If ON is selected, your devices on the same Wi-Fi Name can't make Local Area Network communication.
- Wi-Fi Band: It supports both the 2.4- and 5GHz bands of wi-fi spectrum for top throughput. You can choose Wi-Fi Band depends on your preference.

NOTE: if you connect WLAN printer to your Mobile Hotspot, Privacy Separator should be OFF to send file from your PC to the printer

- SSID Stealth: If ON is selected, the Wi-Fi name won't be found by other devices around it. You need to manually enter the Wi-Fi name and connect.
- Authentication Method: The authentication methods are described below.



Authentication Method WPA2-PSK

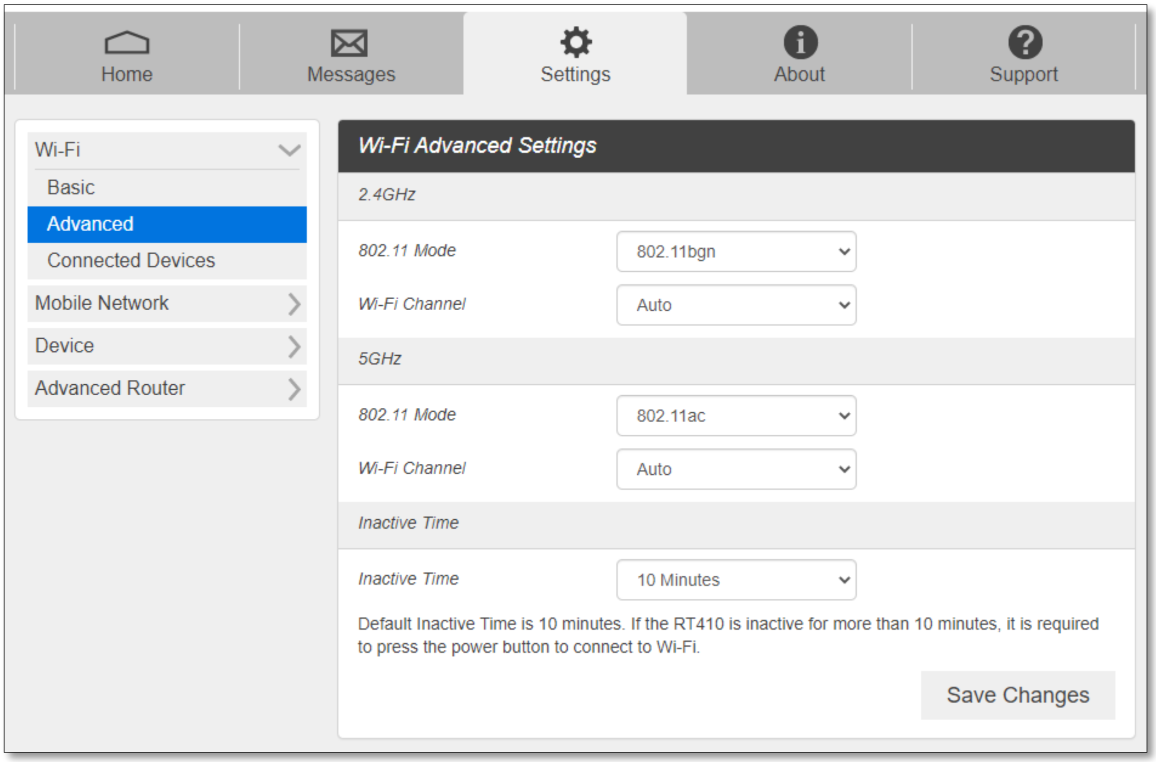
Encryption Method

Display Wi-Fi Name and Password

Mode	Description
WPA-PSK/WPA2-PSK	Apply both the WPA-PSK and WPA2-PSK scheme.
WPA2-PSK	WPA-PSK is the securer version of WPA with implementation of the 802.11i standard.
OPEN	Open authentication

- Encryption Method: Select an encryption method from the drop-down list.
- Display Wi-Fi Name and Password: If ON is selected, the Wi-Fi Name and Password will be displayed on your Mobile Hotspot device display.
- Maximum Connections: Choose the maximum number of the devices which connect to your device simultaneously. You can also click the right or left arrow to distribute the maximum number of the connected devices between the Main Wi-Fi and the Guest Wi-Fi.
- Wi-Fi Settings Reset: Click the Reset button to reset all Wi-Fi settings to the default.

- **Advanced**
  These advanced settings should only be changed for specific circumstances. Changes to the advanced settings could result in loss of Wi-Fi connection with your devices. Consult your devices' manuals for Wi-Fi specifications.



Wi-Fi Advanced Settings

2.4GHz

802.11 Mode	802.11bgn
Wi-Fi Channel	Auto

5GHz

802.11 Mode	802.11ac
Wi-Fi Channel	Auto

Inactive Time

Inactive Time	10 Minutes

Default Inactive Time is 10 minutes. If the RT410 is inactive for more than 10 minutes, it is required to press the power button to connect to Wi-Fi.

- **802.11 Mode**: Select an 802.11 mode from the drop-down list.
- **Wi-Fi Channel**: Select a Wi-Fi channel from the drop-down list.
- **Inactive Time** : Select an Inactive Time from the drop-down list.

NOTE: Default Inactive Time is 10 minutes. Your Mobile Hotspot goes to sleep mode if there's no Wi-Fi connection for the inactive time selected to save the battery power. It is required to press the power button gently once to wake up the device to resume using your device.

- **Connected Devices**

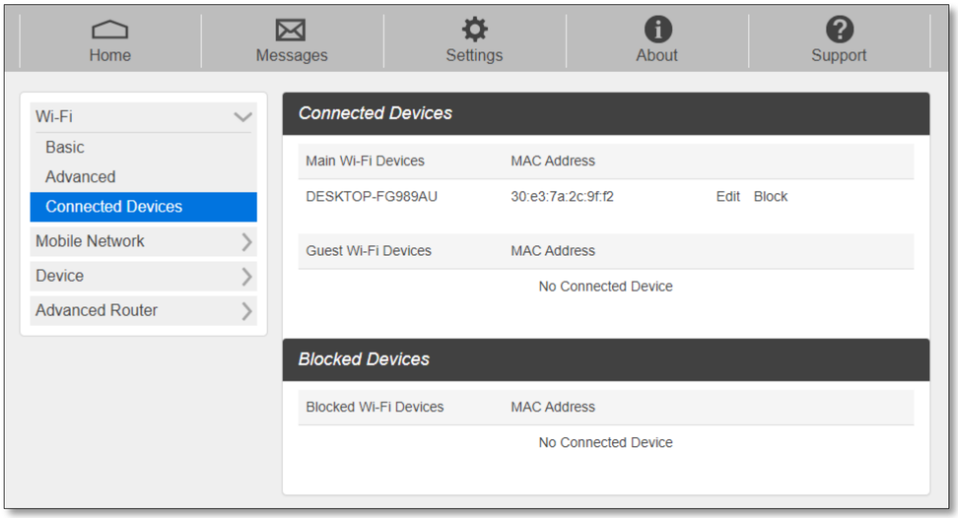
- Connected Devices menu contains the following options:
  - Main Wi-Fi Devices – Normally this is the hostname of the connected device as set on the connected device. You can use the pencil tool to change the name of any connected device.
  - MAC Address – The MAC address is a unique network identifier for this connected device.

To Edit a Connected Device:

1. Click on the **Edit**. A page opens, allowing you to edit the name of the device.
2. Update the name of the device and click **OK**.

- Blocked Devices menu contains the following options:
  - Blocked Wi-Fi Devices – This is a list of devices blocked from Connected Devices menu.

- MAC Address – The MAC address is a unique network identifier for this blocked device.



Connected Devices

Main Wi-Fi Devices	MAC Address	
DESKTOP-FG989AU	30:e3:7a:2c:9f:f2	Edit Block

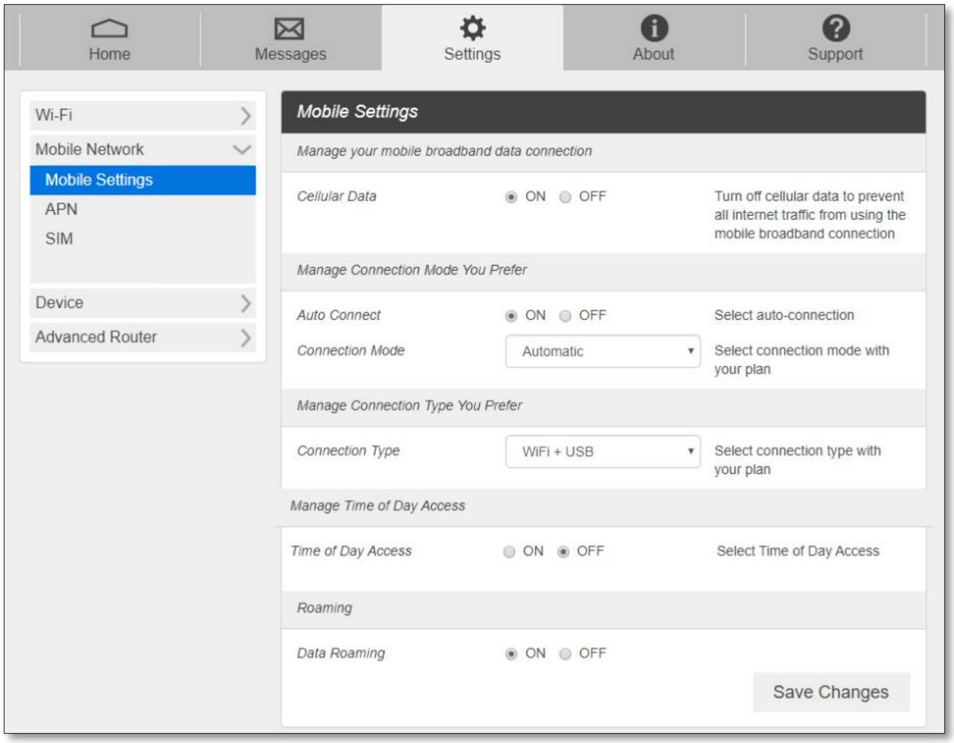
Guest Wi-Fi Devices	MAC Address
	No Connected Device

Blocked Devices

Blocked Wi-Fi Devices	MAC Address
	No Connected Device

Mobile Network

Manage your mobile network settings.



Mobile Settings

Manage your mobile broadband data connection

Cellular Data ● ON ○ OFF — Turn off cellular data to prevent all internet traffic from using the mobile broadband connection

Manage Connection Mode You Prefer

Auto Connect ● ON ○ OFF — Select auto-connection

Connection Mode Automatic ▾ — Select connection mode with your plan

Manage Connection Type You Prefer

Connection Type WiFi + USB ▾ — Select connection type with your plan

Manage Time of Day Access

Time of Day Access ○ ON ● OFF — Select Time of Day Access

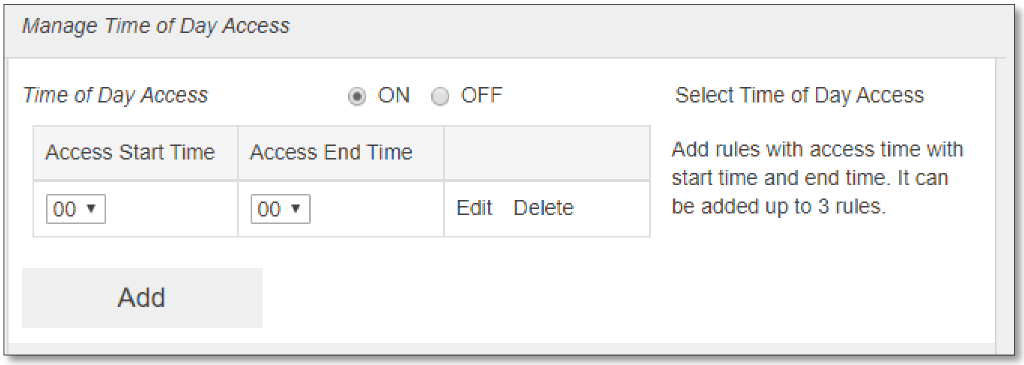
Roaming

Data Roaming ● ON ○ OFF

- **Mobile Settings**
  - Cellular Data: You can turn on/off the data on cellar network.

- Auto Connect: If OFF selected, your Mobile Hotspot won't connect to the network automatically on next powering on. You need to log in the Web Admin Page and connect manually.
- Connection Mode: Automatic / 5G only / 4G only. If Automatic is selected (default), your mobile hotspot will choose the best network available automatically.
- Connection Type: You can select connection between your Mobile Hotspot and other host devices. WiFi + USB Connect / WiFi Only / USB Only

- Time of Day Access: It allows you to select time range a day that allow data connection via your Mobile Hotspot. You can set up to 3 time ranges.



Manage Time of Day Access

Time of Day Access ● ON ○ OFF

Access Start Time	Access End Time	
00 ▾	00 ▾	Edit Delete

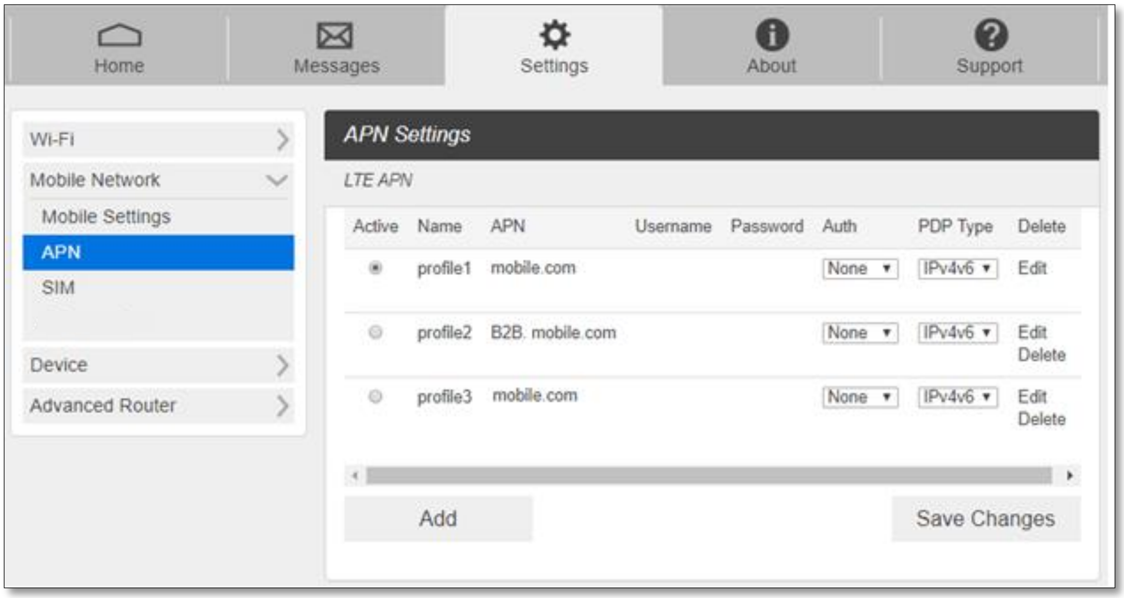
Select Time of Day Access

Add rules with access time with start time and end time. It can be added up to 3 rules.

- Roaming: Turn Data Roaming on or off.
-

CAUTION! Allowing roaming could result in additional service charges. Please contact your service provider for more details.

- **APN**
  It displays the current APN settings.



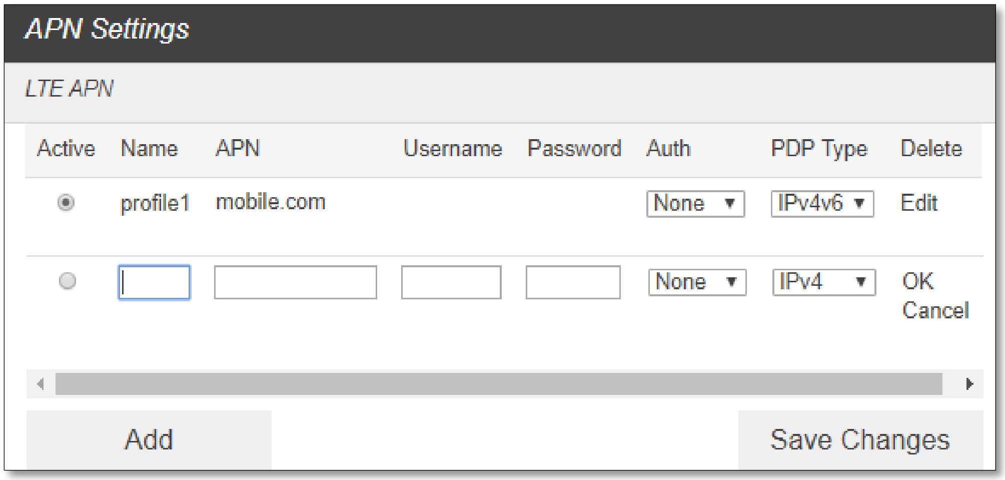
APN Settings

LTE APN

Active	Name	APN	Username	Password	Auth	PDP Type	Delete
●	profile1	mobile.com			None ▾	IPv4v6 ▾	Edit
○	profile2	B2B. mobile.com			None ▾	IPv4v6 ▾	Edit Delete
○	profile3	mobile.com			None ▾	IPv4v6 ▾	Edit Delete

To add a new APN, follow the steps below:

1. Click **Add** to access the following page.



APN Settings

LTE APN

Active	Name	APN	Username	Password	Auth	PDP Type	Delete
●	profile1	mobile.com			None ▼	IPv4v6 ▼	Edit
○					None ▼	IPv4 ▼	OK Cancel

2. Enter the related parameters as described in the following table.

Parameters	**Description**
Name	Type the profile name.
APN	Access Point Name (different per wireless carrier or service)
Username	Username 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.
Auth (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.

3. Click **OK** to add new APN and select Active Profile and **Save Changes** to apply Additional APN Options
   - To activate the new APN, check the circle in front of it and then click **Save Changes**.
   - To edit the new APN, click Edit, change the settings, and then click Save.

   To delete the new APN, click Delete.

CAUTION! Changing APN information could result in connection failure. Please contact your service provider before changing APN only when it's needed.

- **SIM**

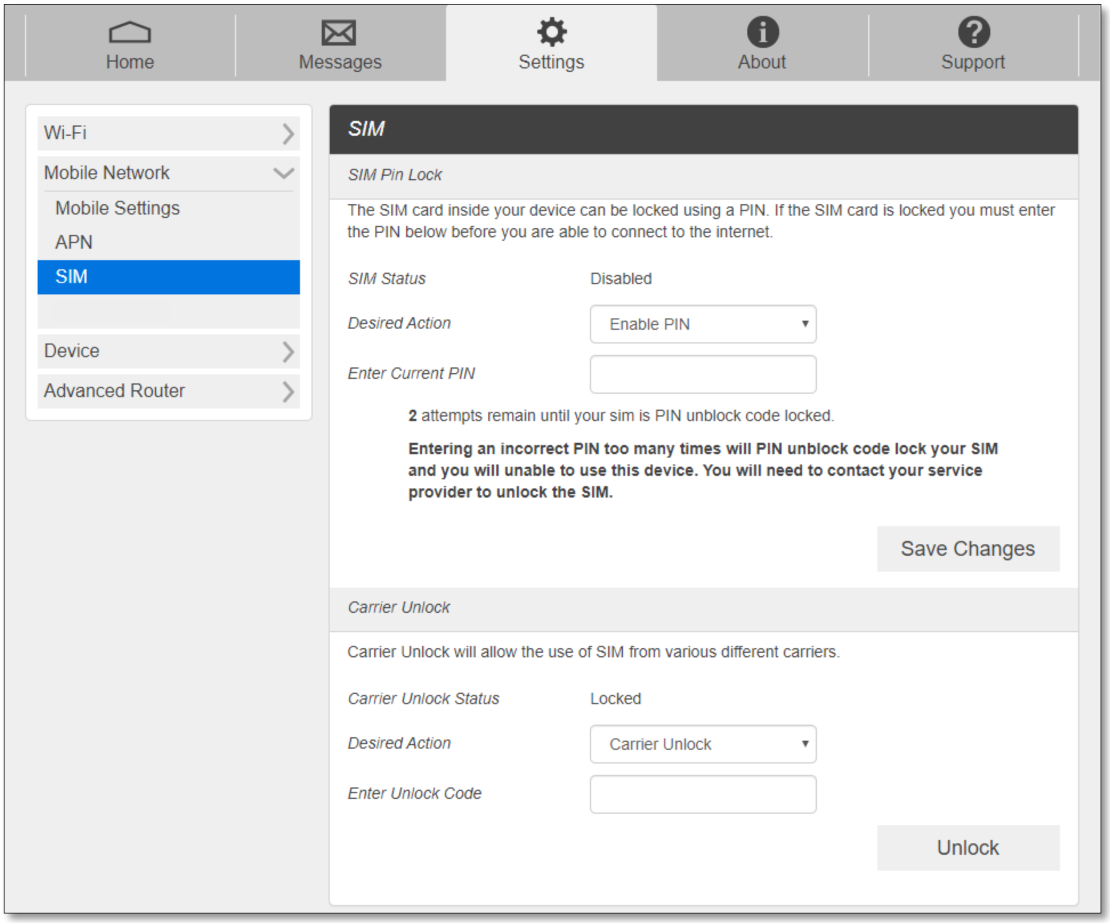
<u>SIM Pin Lock</u>: The **SIM Pin Lock** menu allows you to lock the SIM (Subscriber Identity Module) card in your device. The SIM card inside your device can be locked with a PIN code for additional security. If locked, the PIN code must be entered on the *Web Admin Home* page before the device can connect to the Internet whenever you turn on your device. You can also change the SIM PIN.

To lock your SIM by using a PIN, enter the SIM PIN and press **Save Changes** to save your settings. The SIM Status will be changed to Enabled.

> **NOTE**: If you enter the wrong SIM PIN three times, your SIM will be disabled permanently until you enter the PUK code from your service provider.

<u>Carrier Unlock</u>: Your Mobile Hotspot could be locked to recognize the SIM from your wireless service provider only. To use other SIMs from other wireless service provider, you need to unlock the carrier setting. The unlock code can be provided by your current wireless service provider. Once Carrier Unlock Status is unlocked, you can use the SIM from another wireless service provider

.



SIM

SIM Pin Lock

The SIM card inside your device can be locked using a PIN. If the SIM card is locked you must enter the PIN below before you are able to connect to the internet.

SIM Status Disabled

Desired Action Enable PIN

Enter Current PIN

2 attempts remain until your sim is PIN unblock code locked.

Entering an incorrect PIN too many times will PIN unblock code lock your SIM and you will unable to use this device. You will need to contact your service provider to unlock the SIM.

Carrier Unlock

Carrier Unlock will allow the use of SIM from various different carriers.

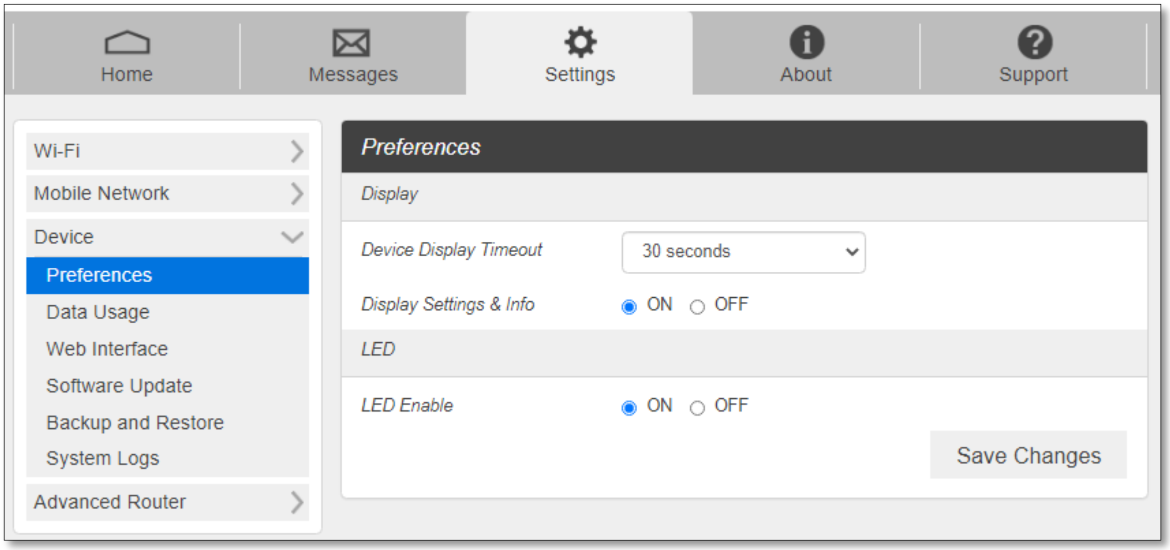
Carrier Unlock Status Locked

Desired Action Carrier Unlock

Enter Unlock Code

Device

- Preferences



Preferences

Display

Device Display Timeout 30 seconds

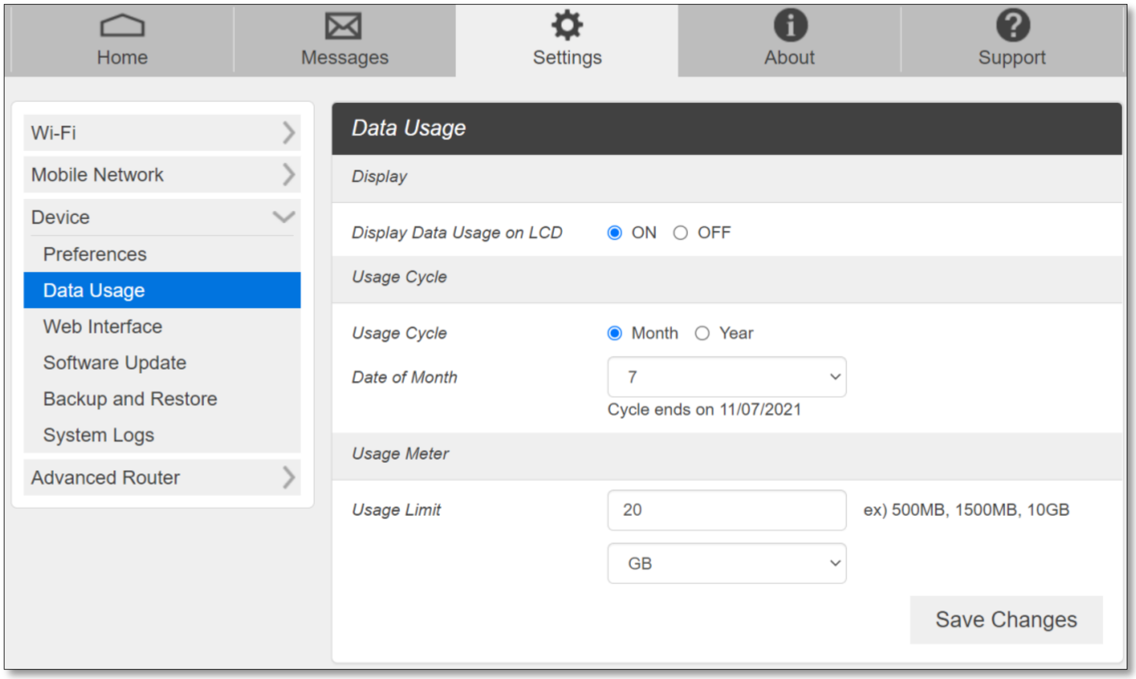
Display Settings & Info ● ON ○ OFF

LED

LED Enable ● ON ○ OFF

Device Display Timeout: Select the time from the drop-down list. Your Mobile Hotspot display goes off after this timeout period if there is no menu button action.
Device Settings & Info: The **Web Admin Home** page information displayed on the device display can be turned On or Off.
LED Enable: If ON is selected, the LED indicator on the power button of your Mobile Hotspot will blink when the device is on. This LED is a power indicator that shows the device is on when the device display is off.

- **Data Usage**



Data Usage

Display

Display Data Usage on LCD ● ON ○ OFF

Usage Cycle

Usage Cycle ● Month ○ Year

Date of Month 7

Cycle ends on 11/07/2021

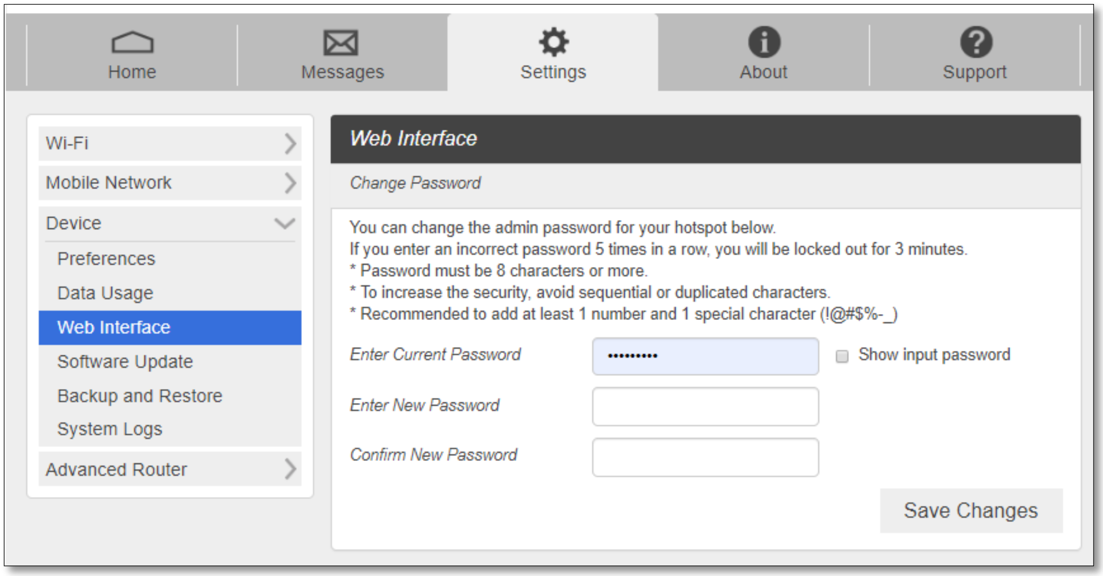
Usage Meter

Usage Limit 20 ex) 500MB, 1500MB, 10GB

GB

Display Data Usage on LCD: Select ON or OFF for the Data Usage Graphic Bar displaying on the device display.
Usage Cycle: User can select Data Usage Cycle either monthly or yearly. For yearly, user must select MM/DD for cycle ending date. On the date set, the data usage information will reset to zero.
Usage Meter: You can select Data Usage Limit and usage information unit (MB or GB).

- **Web Interface**



Web Interface

Change Password

You can change the admin password for your hotspot below.
If you enter an incorrect password 5 times in a row, you will be locked out for 3 minutes.
* Password must be 8 characters or more.
* To increase the security, avoid sequential or duplicated characters.
* Recommended to add at least 1 number and 1 special character (!@#$%-_)

Enter Current Password ••••••••• □ Show input password

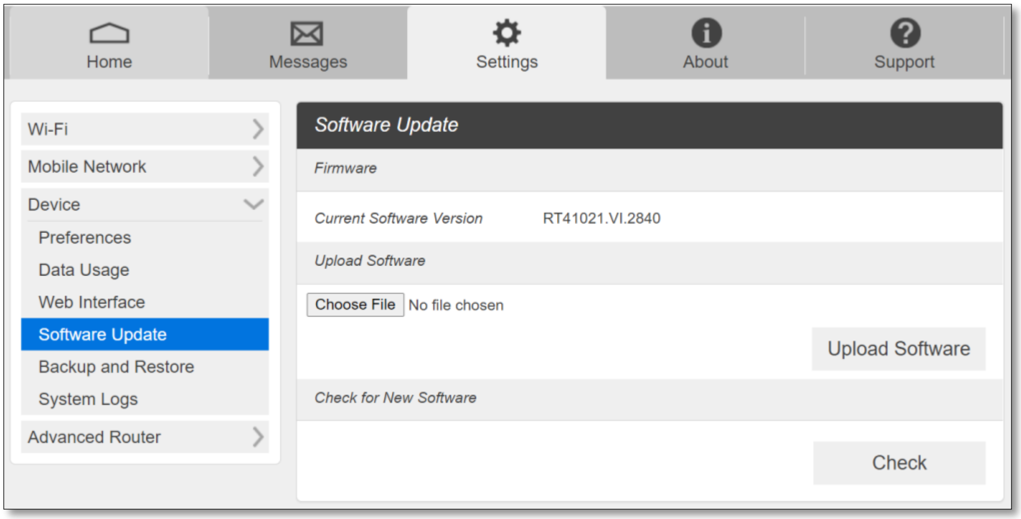
Enter New Password

Confirm New Password

Change Password: You can change Web Admin login password.
- Current Password: Enter the current password.
- New Password: Enter the new password.
- Confirm New Password: Enter the new password again.
- Click **Save Changes** to save your new password.

- **Software Update**

You can check current software version or check if there is a new update is available.



Software Update

Firmware

Current Software Version RT41021.VI.2840

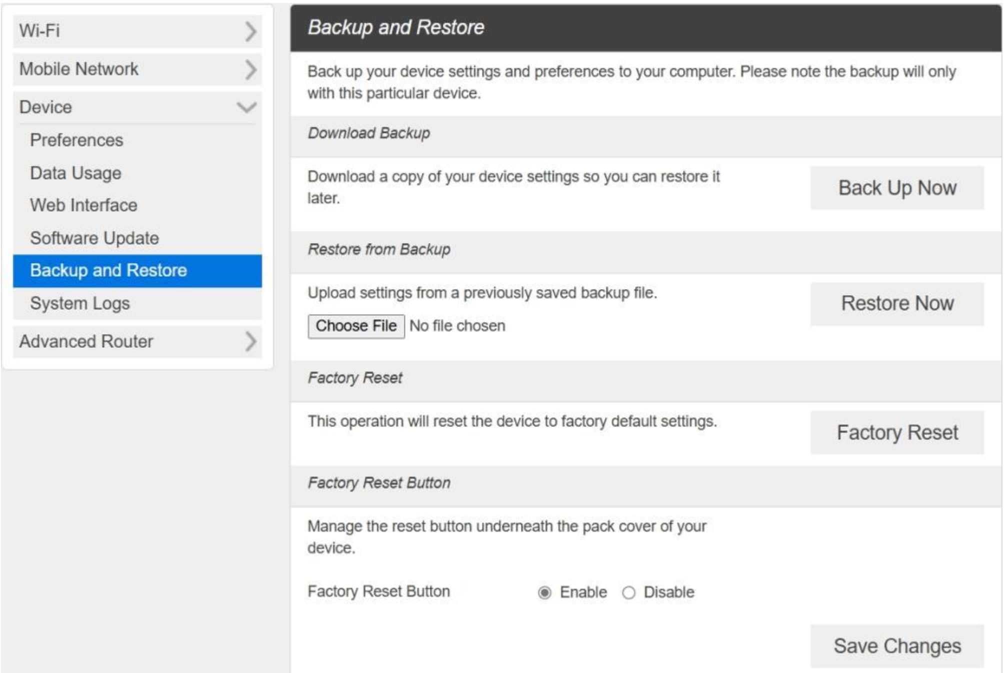
Upload Software

No file chosen

Check for New Software

- Firmware: Current software version
- Upload Software: In case you have a new software file provided by your service provider, select the file, then press **Upload Software** to update your device software.
- Check for New Software: Click **Check** button. Message windows will pop up and guide you through the update process.

- **Backup and Restore**



Backup and Restore

Back up your device settings and preferences to your computer. Please note the backup will only with this particular device.

Download Backup

Download a copy of your device settings so you can restore it later.

Restore from Backup

Upload settings from a previously saved backup file.

No file chosen

Factory Reset

This operation will reset the device to factory default settings.

Factory Reset Button

Manage the reset button underneath the pack cover of your device.

Factory Reset Button ● Enable ○ Disable

To back up your device settings as a file on your computer, follow the steps below:

a. Click **Back Up Now**.
b. Click **Save** on the pop-up window.
c. Choose a location on your computer to save the backup file.
d. Click **Save**.

To restore the device settings from the backup file, follow the steps below:

a. Click **Choose File** to select the backup file in your computer.
b. Click **Restore now**.

To factory reset your device to its factory default settings, follow the steps below:

a. Click **Factory Reset**.
b. Click **OK** to confirm the command.

To manage factory reset button, follow the steps below:

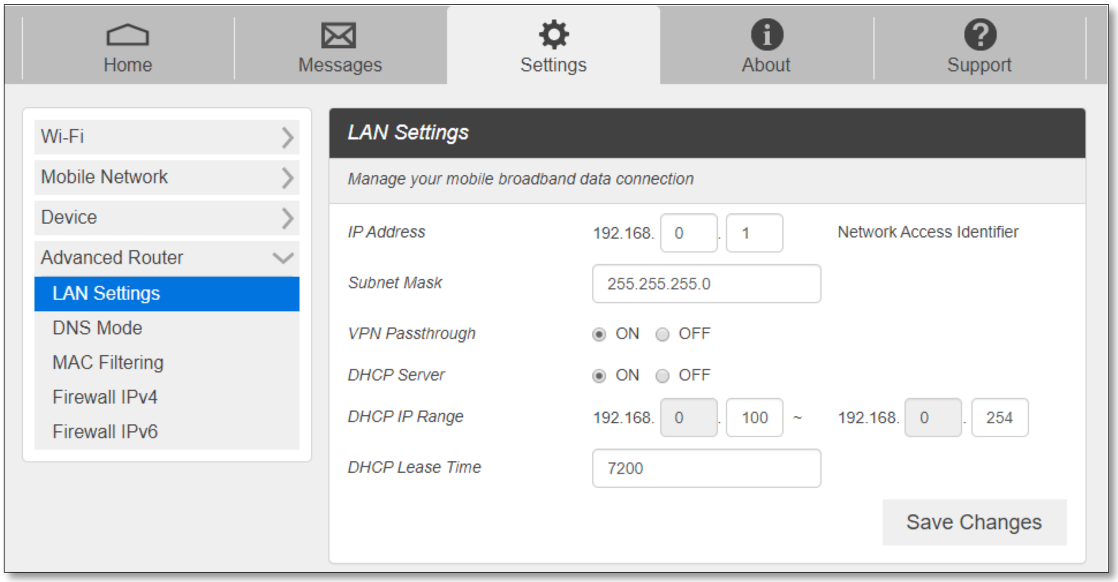
c. Select Enable or Disable, and click **Save Changes**

Advanced Router

Configure LAN, Firewall, and Customization settings.

- **LAN Settings**

From the **Web Admin Home**, click **Settings > Advanced Router > LAN Settings** to display the router information shown in the following figure.



LAN Settings

Manage your mobile broadband data connection

IP Address 192.168. 0 . 1 Network Access Identifier

Subnet Mask 255.255.255.0

VPN Passthrough ● ON ○ OFF

DHCP Server ● ON ○ OFF

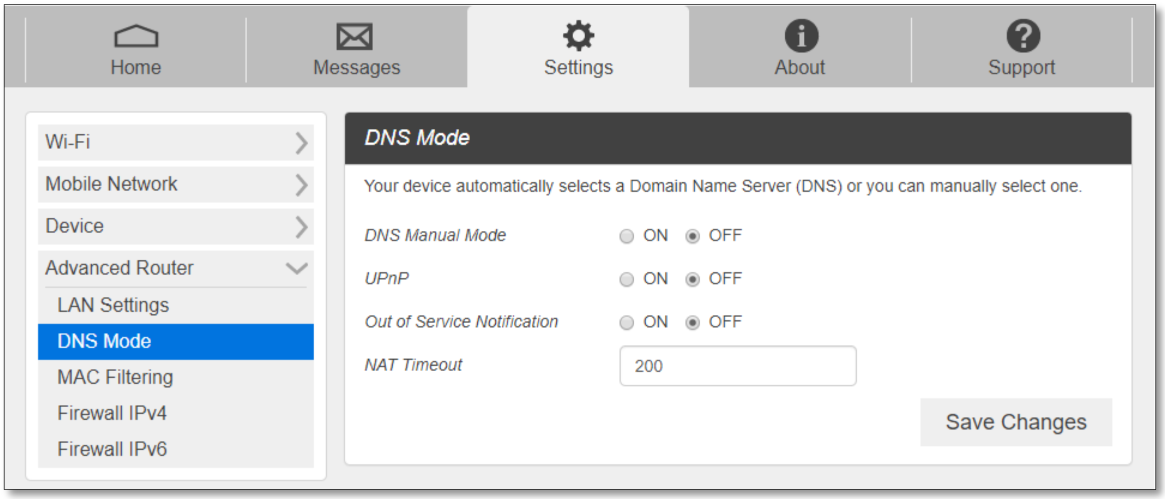
DHCP IP Range 192.168. 0 . 100 ~ 192.168. 0 . 254

DHCP Lease Time 7200

- **IP address** – The IP address of the default gateway and for your device Web Admin
- **Subnet mask** – The Subnet mask network setting for your device. The default value 255.255.255.0 is standard for small (class "C") networks. If you change your LAN IP Address, ensure that you use the correct Subnet mask for the IP address range containing the LAN IP address.
- **VPN Passthrough ON/OFF** – Allowing or preventing connected devices to establish a secure VPN connection. When turned **ON,** this feature allows VPN clients on your connected device to connect through your device to remote VPN servers. The default setting for this feature is **ON.** When turned **OFF**, the VPN clients are not allowed to connect.
- **DHCP (Dynamic Host Configuration Protocol) server** – The **DHCP server** is **ON** by default. When turned **ON**, your device automatically assigns local IPs to your other devices you connect to your device. When turned **OFF**, you will need to set it up manually from the device you want to connect to your device.
- **DHCP IP Range** – Defines the local IP range that DHCP server can assign to connected devices.
- **DHCP Lease Time - DHCP lease time** represents the period between when your connected device obtained its IP address from your device and the time when it expires. When the **DHCP lease time** expires, your connected device automatically releases IP address and asks your device to give it a new one.

- **DNS Mode**

  Your device automatically selects a Domain Name Server (DNS) assigned by your network provider. The **DNS Mode** option allows you to manually set up two DNS IP addresses.



DNS Mode

Your device automatically selects a Domain Name Server (DNS) or you can manually select one.

DNS Manual Mode ○ ON ● OFF

UPnP ○ ON ● OFF

Out of Service Notification ○ ON ● OFF

NAT Timeout 200

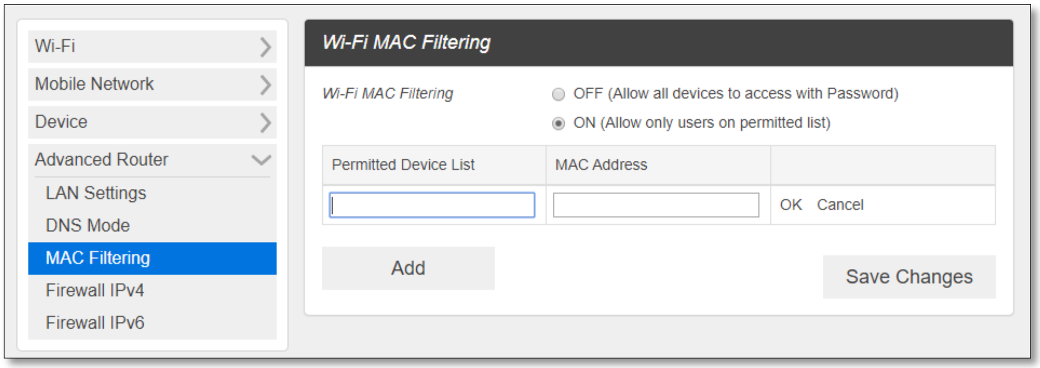
To manually set a Domain Name Server:

1 Click the **ON** button to enable **Manual DNS**.
2 Enter the IP address of the first DNS in the **DNS Address 1** field.
3 Enter the IP address of the second DNS in the **DNS Address 2** field.
4 Click **Save Changes** button

  - UPnP: When it is ON, the devices connected to your Mobile Hotspot seamlessly discover each other's presence on the network and establish functional network services.
  - Out of Service Notification: Enable or disable Out of Service Notification function.
  - NAT Timeout: The device will keep NAT entries in the translation table for this configurable length of time.

- **MAC Filtering**

  The MAC filtering allows only selected devices to access your device Wi-Fi network. By default, MAC filtering is turned **OFF**.



Wi-Fi MAC Filtering

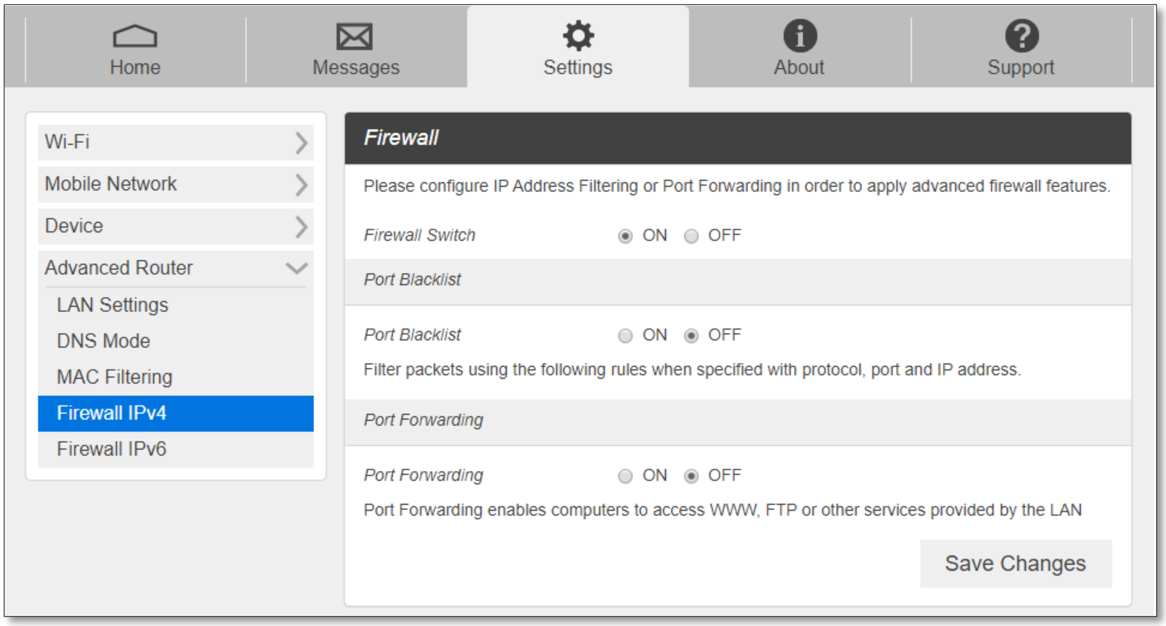
Wi-Fi MAC Filtering ○ OFF (Allow all devices to access with Password)
● ON (Allow only users on permitted list)

Permitted Device List	MAC Address	
		OK Cancel

To enable MAC Filtering,

1. Select **ON**.
2. Press **Add** to add a line to enter permitted device name and MAC address, then click OK. When entering MAC addresses, use ":" as the separators (for example, c2:b5:d7:27:fb:9b).
   To add more, press **Add** to add another line.
3. When completed adding devices, press **Save Changes**.

- **Firewall IPv4**
  You may set up firewall rules to protect your network from virus and malicious activity on the Internet.



Firewall

Please configure IP Address Filtering or Port Forwarding in order to apply advanced firewall features.

Firewall Switch ● ON ○ OFF

Port Blacklist

Port Blacklist ○ ON ● OFF

Filter packets using the following rules when specified with protocol, port and IP address.

Port Forwarding

Port Forwarding ○ ON ● OFF

Port Forwarding enables computers to access WWW, FTP or other services provided by the LAN

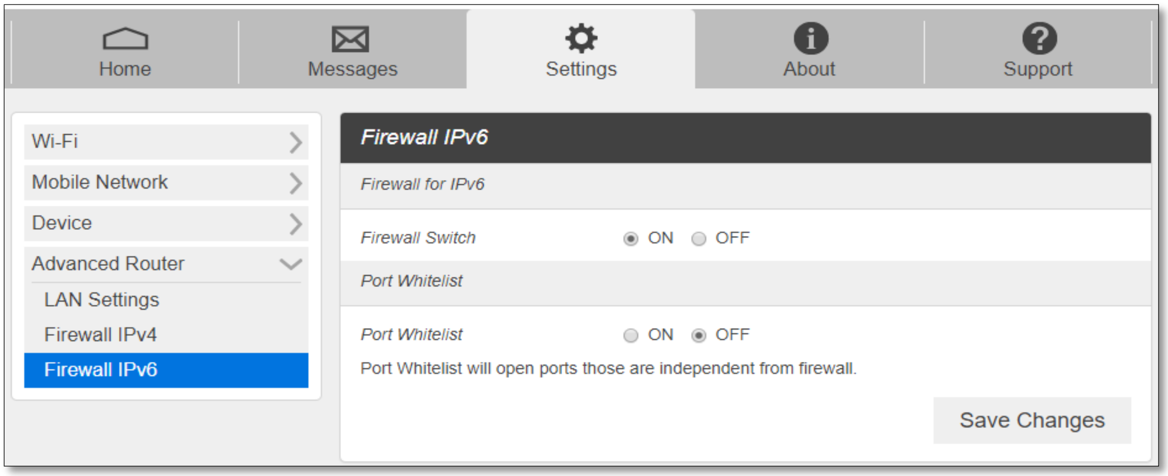
- **Firewall Switch** – To set up Port Blacklist and Port Forwarding, turn Firewall Switch **ON**. If Firewall Switch is **OFF**, both Port Blacklist and Port Forwarding settings are not active.

- **Port Blacklist** – You can block outbound forward packet by setting up a rule in the blacklist. To set up the rule,
  1. Turn **ON** Port Blacklist.
  2. Press **Add** to create a line to setup a rule.
  3. Enter the name of the rule you want to set up.
  4. Enter IP address of the site you want to restrict outbound forward packet.
  5. Enter Port number of the outbound forward packet.
  6. Select Protocol and Status **ON/OFF**: **ON** means the rule is in active. **OFF** means the rule is not active.
  7. Press **OK** to complete set up, then press **Save Changes**.

- **Port Forwarding** – You can allow inbound packet for specific port number by setting up port forwarding rule. To set up Port Forwarding,
  1. Turn **ON** Port Forwarding.

2. Press **Add** to create a line to set up a rule.
3. Enter the name of the rule you want to set up.
4. Enter WAN port number of allowed inbound forward packet.
5. Enter LAN IP address your connected device that is assigned by your device.
6. Enter LAN port number of allowed inbound forward packet.
7. Select Protocol and Status **ON/OFF**: **ON** means the rule is in active. **OFF** means the rule is not active.
8. Press **OK** to complete set up, then press **Save Changes**.

- **Firewall IPv6**



Firewall IPv6

Firewall for IPv6

Firewall Switch ● ON ○ OFF

Port Whitelist

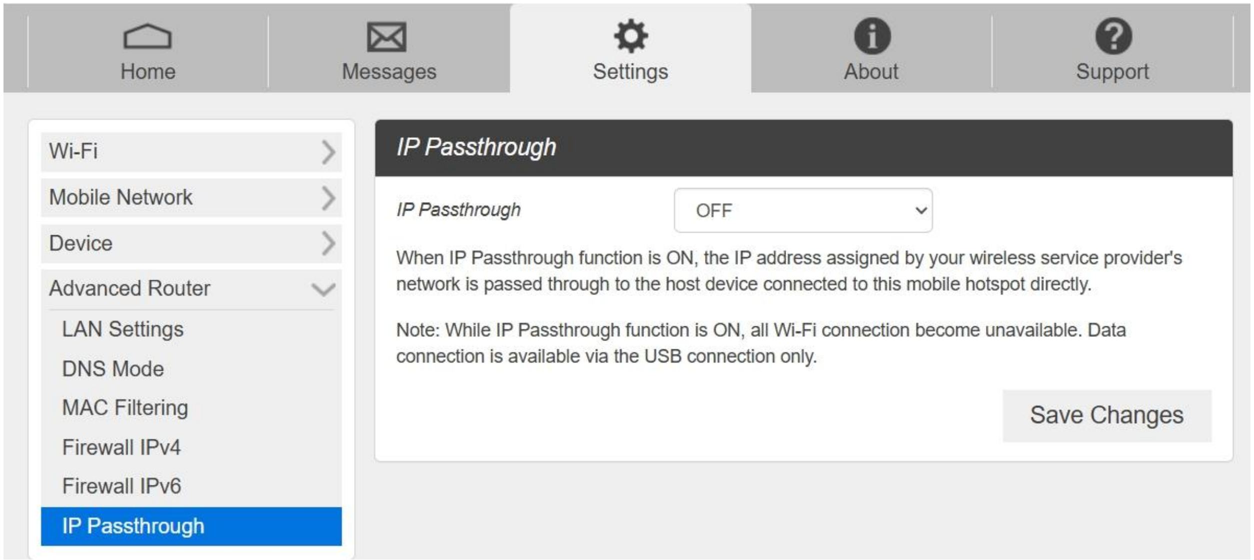
Port Whitelist ○ ON ● OFF

Port Whitelist will open ports those are independent from firewall.

- **Firewall Switch** – To set up Port Whitelist, turn Firewall Switch **ON**. If Firewall Switch is **OFF**, Port Whitelist settings is not active. By default, the Firewall Switch for IPv6 is **ON** to restrict inbound forward packet from outside.
- **Port Whitelist** – You can allow inbound forward packet of specific port number by setting up Port Whitelist. To set up Port Whitelist,
  1. Turn **ON** Port Whitelist.
  2. Press **Add** to create a line to set up a rule.
  3. Enter the name of the rule you want to create.
  4. Enter the port number you want to allow inbound forward packet.
  5. Select Protocol and Status **ON/OFF**: **ON** means the rule is in active. **OFF** means the rule is not active.
  6. Press **OK** to complete set up, then press **Save Changes**.

- **IP Passthrough**

IP Passthrough is a networking feature that enables a designated device on your local network to use the public IP address of RG350. This allows the device to be directly accessible from the internet, making it ideal for use cases such as hosting servers, remote desktop access, or any application that requires unrestricted inbound connectivity.



IP Passthrough

IP Passthrough: OFF

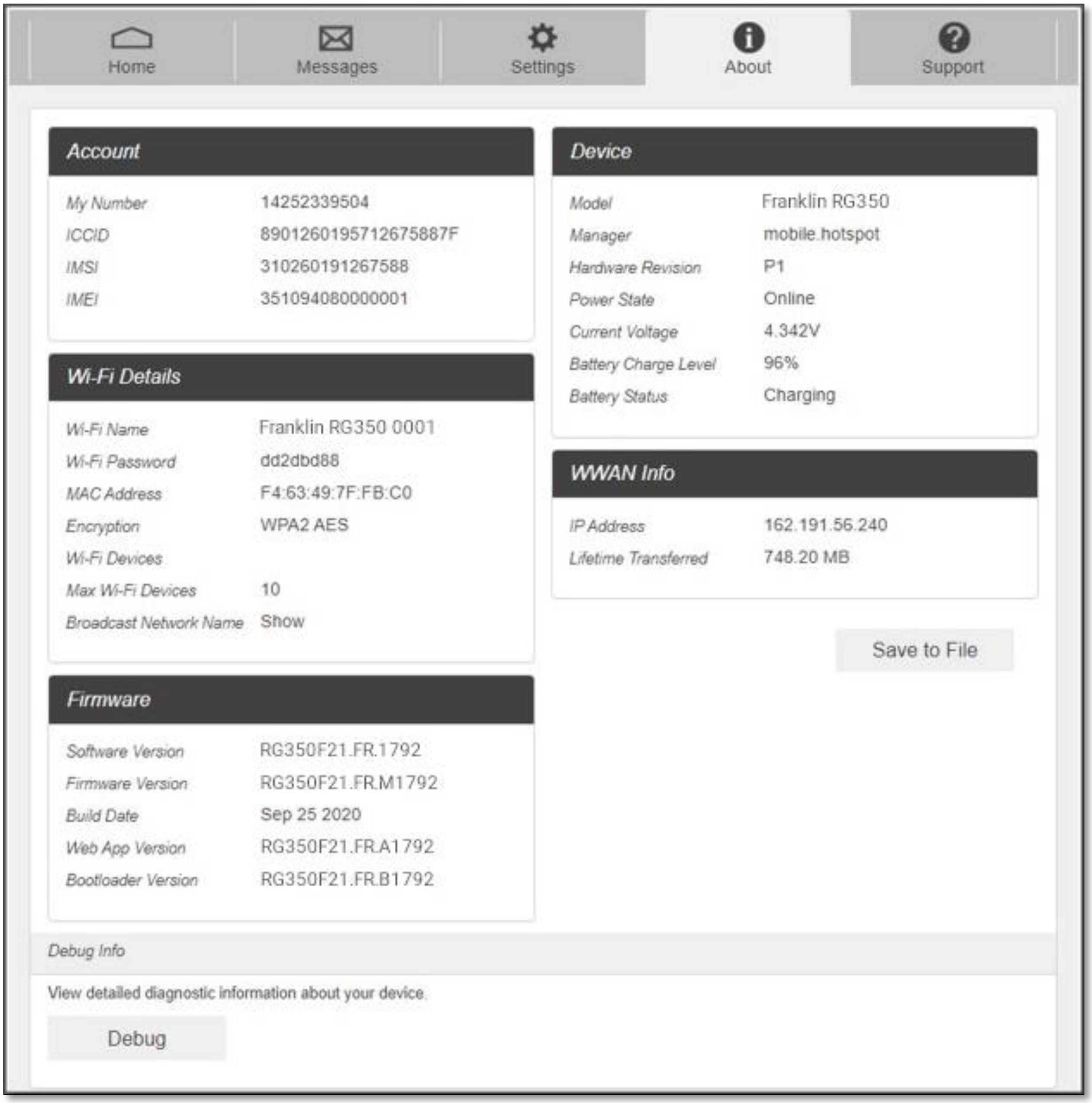
When IP Passthrough function is ON, the IP address assigned by your wireless service provider's network is passed through to the host device connected to this mobile hotspot directly.

Note: While IP Passthrough function is ON, all Wi-Fi connection become unavailable. Data connection is available via the USB connection only.

About

View your device's connection information, firmware information, WWAN information, Wi-Fi details and device information.

From the Web Admin Home main screen, click the **About** tab to view the available information.



Account

My Number	14252339504
ICCID	8901260195712675887F
IMSI	310260191267588
IMEI	351094080000001

Wi-Fi Details

Wi-Fi Name	Franklin RG350 0001
Wi-Fi Password	dd2dbd88
MAC Address	F4:63:49:7F:FB:C0
Encryption	WPA2 AES
Wi-Fi Devices	
Max Wi-Fi Devices	10
Broadcast Network Name	Show

Firmware

Software Version	RG350F21.FR.1792
Firmware Version	RG350F21.FR.M1792
Build Date	Sep 25 2020
Web App Version	RG350F21.FR.A1792
Bootloader Version	RG350F21.FR.B1792

Device

Model	Franklin RG350
Manager	mobile.hotspot
Hardware Revision	P1
Power State	Online
Current Voltage	4.342V
Battery Charge Level	96%
Battery Status	Charging

WWAN Info

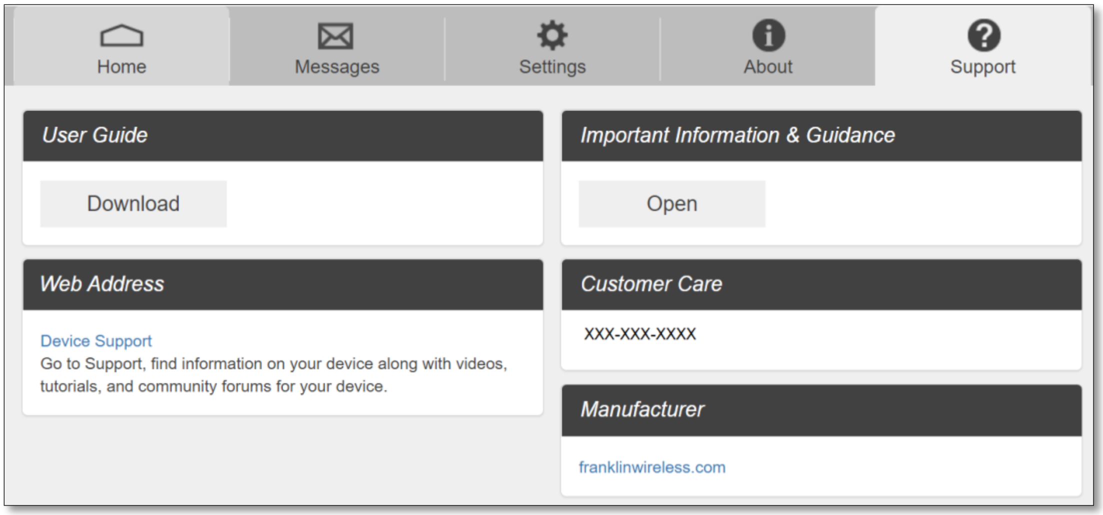
IP Address	162.191.56.240
Lifetime Transferred	748.20 MB

Debug Info

View detailed diagnostic information about your device.

Support

Obtain support information from the Web Admin Home Support Tab.



User Guide

Important Information & Guidance

Web Address

Device Support
Go to Support, find information on your device along with videos, tutorials, and community forums for your device.

Customer Care

XXX-XXX-XXXX

Manufacturer

franklinwireless.com

4

Troubleshooting

Overview
First Steps
Common Problems and Solutions

Overview

The following tips can help solve many common problems encountered while using the Mobile Hotspot.

First Steps

1. Make sure you are using your Mobile Hotspot in the correct geographic region (within coverage).
2. Ensure that your wireless coverage extends to your current location by using the interactive Wireless Carrier's coverage map tool.
3. Ensure that you have an active service plan.
4. Restarting your computer and your Mobile Hotspot can resolve many issues.

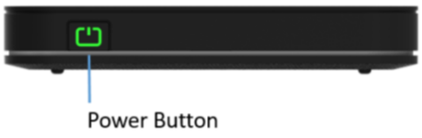
IMPORTANT! Before contacting customer care, be sure to restart both your Mobile Hotspot and any device that is currently connected.

Common Problems and Solutions

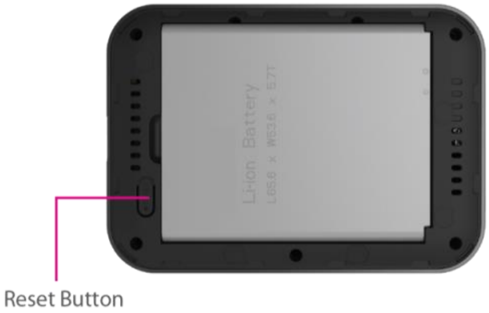
Mobile Hotspot just powered off without pressing the Power/Menu button. Why?
This may occur under Battery depletion.
To restore power, manually press and hold the Power/Menu button to turn on your Mobile Hotspot. If the battery is depleted, charge the battery with the AC charger provided.

IMPORTANT! If the power button will not start your Mobile Hotspot, please try Power Reset (see **How do I perform a Power Reset on Mobile Hotspot?** below).

How do I perform a Power Reset on Mobile Hotspot?
Using the power button: Press and hold the power button for 10 seconds until the Mobile Hotspot restarts.
By replacing the battery: If pressing and holding the power button for 10 seconds does not restart the Mobile Hotspot, open the battery cover, take out the battery and re-install the battery after 5 seconds. Put the battery cover back and turn on the Mobile Hotspot by pressing the power button.



How do I perform a Reset?
Using the reset button: Remove the back cover. Make sure the battery is installed and your Mobile Hotspot is on. Press down the reset button for 3 seconds and release. Then, your Mobile Hotspot will perform the reset and restart automatically.



How do I perform a Factory Reset?
Using **Web Admin Home** : Connect to your Mobile Hotspot and then open **Web Admin Home** page (http://mobile.hotspot). Select **Settings > Mobile Network > Advanced** and Click **Factory Reset**.

I cannot connect to Wi-Fi after changing Wi-Fi password.
Your Wi-Fi devices save the previously used Wi-Fi names associated with the passwords used to access the Wi-Fi name. When you change the Wi-Fi password only for your Mobile Hotspot and keep the same Wi-Fi Name, the devices try to connect to your Mobile Hotspot using the Wi-Fi name and previous Wi-Fi password saved, causing Wi-Fi authentication error.

I cannot log into http://mobile.hotspot **.**
Ensure that you are entering the correct **Web Admin Home** password to sign in. The default **Web Admin Home** login password is “admin” unless you have previously changed. If you have forgotten your password, reset your device by pressing the **Reset button** inside the battery chamber.

5

Regulatory Information

Regulatory Statements
Safety Hazards

Regulatory Statements

FCC Equipment Authorization ID: XHG-RG350

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.

SAR Information
The exposure standard for your device uses a unit of measurement called the Specific Absorption Rate ("SAR").
SAR is the unit of measurement for the amount of RF energy absorbed by the body when using a mobile device. Although the SAR is determined at the highest certified power level, the actual SAR value of the device while in operation can be well below the level reported to the FCC. This is due to a variety of factors including its proximity to a base station, the design of the device and other factors. What is important to remember is that each device meets strict Federal Government guidelines. Variations in SARs do not represent a variation in safety. All devices must meet the federal standard, which incorporates a substantial margin of safety. SAR values at or below the federal standard of 1.6 watts/kg (W/kg) are considered safe for use by the public. This product meets current FCC Radio Frequency Exposure Guidelines. The reported SAR value of the device is 1.58 W/kg.
Additional details at FCC website:
www.fcc.gov/oet/ea

Body-Worn Operation

Please note this important safety information regarding radio frequency (RF) radiation exposure and near-body operation. To ensure compliance with RF exposure guidelines, the device must be used at least 10 mm from your body. Failure to observe this warning could result in RF exposure exceeding the applicable guideline limits.

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.

FCC CAUTION: Any changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

NOTE: The Radio Frequency (RF) emitter installed in your modem must not be located or operated in conjunction with any other antenna or transmitter, unless specifically authorized by Franklin Wireless.

Safety Hazards

Follow Safety Guidelines
Always follow the applicable rules and regulations in the area in which you are using your device. Turn your device off in areas where its use is not allowed or when its use may cause interference or other problems.

Electronic Devices
Most modern electronic equipment is shielded from radio frequency (RF) signals. However, inadequately shielded electronic equipment may be affected by the RF signals generated by your device.

Medical and Life Support Equipment
Do not use your device in healthcare facilities or where medical life support equipment is located as such equipment could be affected by your device's external RF signals.

Pacemakers

- The Health Industry Manufacturers Association recommends that a minimum separation of six inches must be maintained between a device and a pacemaker in order to avoid potential interference with the pacemaker. These recommendations are consistent with the independent research by and recommendations of Wireless Technology Research. Persons with pacemakers should always follow these guidelines:
- Always keep the device at least six inches away from a pacemaker when the device is turned on.
- Place your device on the opposite side of your body where your pacemaker is implanted in order to add extra distance between the pacemaker and your device.
- Avoid placing a device that is on next to a pacemaker (e.g., do not carry your device in a shirt or jacket pocket that is located directly over the pacemaker).
- If you are concerned or suspect for any reason that interference is taking place with your pacemaker, turn your device OFF immediately.

Hearing Devices

When some wireless devices are used with certain hearing devices (including hearing aids and cochlear implants) users may detect a noise which may interfere with the effectiveness of the hearing device.

Use of Your Device while Operating a Vehicle

Please consult the manufacturer of any electronic equipment that has been installed in your vehicle as RF signals may affect electronic systems in motor vehicles.
Please do not operate your device while driving a vehicle. This may cause a severe distraction and in some areas, it is against the law.

Use of Your Device on an Aircraft

Using your device during flight may violate FAA regulations. Because your device may interfere with onboard electronic equipment, always follow the instructions of the airline personnel and turn your device OFF when instructed to do so.

Blasting Areas

In order to avoid interfering with blasting operations, your device should be turned OFF when in a blasting area or in an area with posted signs indicating that people in the area must turn off two-way radios. Please obey all signs and instructions when you are in and around a blasting area.

Proper Battery & Adapter Use and Disposal

- Do not disassemble or open crush, bend or deform, puncture or shred.
- Do not modify or remanufacture, attempt to insert foreign objects into the battery, immerse or expose to water or other liquids, expose to fire, explosion or another hazard.
- Only use the battery for the system for which it is specified.
- Only use the battery with a charging system that has been qualified with the system per CTIA Certification Requirements for Battery System Compliance to IEEE 1725. Use of an unqualified battery or charger may present a risk of fire, explosion, leakage, or another hazard.
- Do not short circuit a battery or allow metallic conductive objects to contact battery terminals.
- Replace the battery only with another battery that has been qualified with the system per this standard, IEEE-Std-1725. Use of an unqualified battery may present a risk of fire, explosion, leakage or other hazard. Only authorized service providers shall replace the battery.
- Promptly dispose of used batteries in accordance with local regulations.
- Battery usage by children should be supervised.
- Avoid dropping the battery. If the battery is dropped, especially on a hard surface, and the user suspects damage, take it to a service center for inspection.
- Improper battery use may result in a fire, explosion or another hazard.
- The host device shall only be connected to CTIA certified adapters, products that bear the USB-IF logo or products that have completed the USB-IF compliance program.

Document Revision History

Revision: Rev.1.2
Date: May 2025

6

Glossary

Glossary

Term	Definition
5G	5th Generation Mobile Network
802.11(b/g/n/ac)	A set of WLAN communication standards in the 2.4GHz frequency band.
Bps	Bits per second
Broadband	High capacity, high-speed transmission channel with a wider bandwidth than conventional modem lines.
DHCP	Dynamic Host Configuration Protocol
DHCP Server	A server or service with a server that assigns IP addresses.
DNS	Domain Name System
Firmware	A computer program embedded in electronic devices. Firmware usually contains operating code for the device.
GB	Gigabyte
Hotspot	A Wi-Fi (802.11b/g/n/ac) access point or the area covered by an access point.
HTTP	Hyper Text Transfer Protocol
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IP Type	The type of service provided over a network.
IP Address	The address of a device attached to an IP network.
ISP	Internet Service Provider
Kbps	Kilobits per second
LAN	Local Area Network
MAC Address	Media Access Control address
Mbps	Megabits per second
MSID	Mobile Station Identifier
Network Operator	The vendor who provides your wireless access.
Port	A virtual data connection used by a program to exchange data.
Port Forwarding	A process that allows remote devices to connect to a specific computer within a private LAN.
Port Number	A 16-bit number used by the TCP and UDP protocols to direct traffic.
PRL	Preferred Roaming List
Protocol	A standard that allows connection, communication, and data transfer between computing endpoints.
Proxy	A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address.
Router	A device that directs traffic from one network to another.
SIM	Subscriber Identification Module
SSID	Service Set Identifier
TCP/IP	Transmission Control Protocol/Internet Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WWAN	Wireless Wide Area Network