4G LTE M2M Box

User Manual

Model: RT410S

Note: All pictures and drawings shown in this document are for illustration purposes only. The actual product may vary due to different variants and enhancements.

Contents

1

Getting Started

Overview
In the Box
Components

Overview

Thank you for choosing the RT410S 4G LTE M2M Box for your M2M applications.
Having the RT410S M2M Box allows you to access the LTE network instantly for your machine-to-machine communication needs. The RT410S provides various connection types to suit your needs, including up to 15 Wi-Fi connections, USB connections, and Ethernet connections.

Ruggedized design The M2M Box RT410S is encased in durable aluminum, making it suitable for installation in harsh environments. It can withstand high temperatures, humidity, and physical impacts, ensuring reliable performance in demanding conditions.

Endless Applications The M2M Box enhances customer interaction in kiosks with reliable internet, ensures connectivity on the go for transport, powers digital signage, secures lottery machines, enables fast payments, and supports remote health monitoring with stable connections.

High Performance Experience high-performance connectivity with the M2M Box. It features Wi-Fi 5 for fast, reliable internet access and dual external antennas for maximum signal strength. Connect up to 15 devices simultaneously and enjoy seamless, uninterrupted performance.

GPS & LTE Diversity Benefit from GPS integration with LTE diversity, offering precise location services and enhanced connectivity.

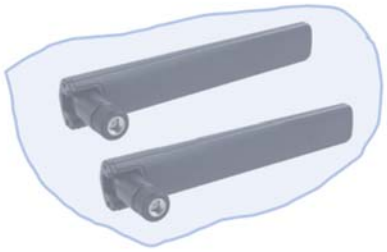
System Requirements

- Compatible with all IEEE802.11 b/g/n/ac Wi-Fi 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 Outdated versions may not be compatible with the Mobile M2M Box Web Admin User Interface, http://mobile.hotspot*

In the Box

1 RT410S M2M Box

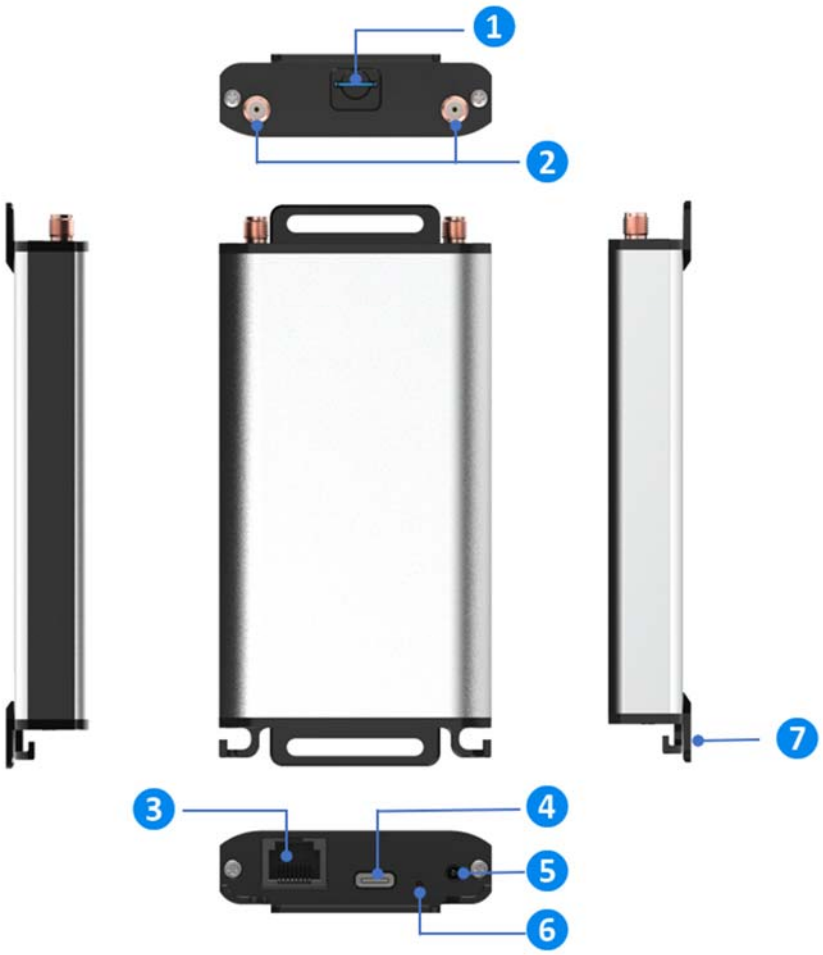


2 2 X Antenna

3 Quick Start Guide

4 Type C USB Cable

Components



1. SIM Card Slot: Insert your service provider's 4FF SIM card here.
2. Antenna Connectors: Connect antennas using SMA-type connectors.
3. Ethernet port: Connect an Ethernet cable here for internet access.
4. Type C USB port: Connect to a USB power source to power on the device. This port can also be used for power supply and data connection via a USB cable.
5. LED Indicator light
   - Blinking Green: Power is applied, but no data connection is available.
   - Solid Green: The device is functioning normally with an active data connection.
6. Factory Rest Button: Use a pin to press and hold the button for 3 seconds, then release to perform a factory reset. This will revert all device settings to their original factory defaults.
7. Mount brackets: Utilize these for various mounting needs.

2

Using Your M2M Box

Accessing the Network

Your M2M Box works effectively anywhere with the reliable broadband speed provided by your LTE service provider. You can stay connected and keep up to date with your application needs.

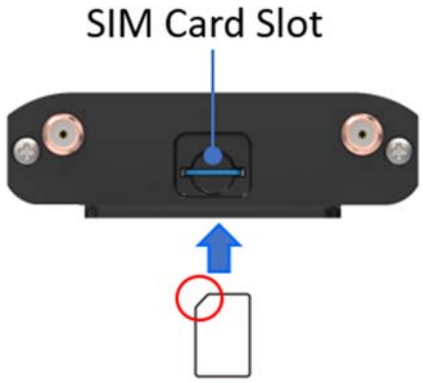
Using Your M2M Box for the First Time

System Requirements

Your computer, tablet, or other wireless devices need Wi-Fi capability and an Internet browser only to configure the RT410S M2M Box. Your M2M Box is compatible with most major operating systems and the latest versions of browsers.

Installing the SIM Card

SIM (Subscriber Identity Module) Card: Your SIM card is a small, rectangular plastic card that stores critical information about your wireless service, such as your phone number, network credentials. It allows your device to connect to your service provider's network. Depending on your service provider, the SIM card may already be pre-inserted in your device, or you may need to obtain it separately upon subscribing to a wireless service. Simply insert the SIM card into the designated slot on your device to activate your service.



Insert your SIM card into the designated SIM Card Slot. Ensure that the card aligns with the slot's orientation. Push the SIM card gently but firmly all the way until it clicks into place, ensuring a secure fit.

To uninstall your SIM card, gently press it once, then it will pop out.

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 M2M Box is powered off and is not connected to any power source.

Power On / Off RT410S M2M Box

There is no power button on the device. Simply connect it to a USB power source using the USB cable provided to power it on.

Connecting to Your M2M Box

Via Wi-Fi

You can find the default Wi-Fi Name (SSID) and Password on the device label located on the back side of the device.

1 Open the Wi-Fi application or controls on your laptop or devices that you want to connect to your M2M Box and find your M2M Box's Wi-Fi name.
2 Click **Connect** and enter the Password when prompted.

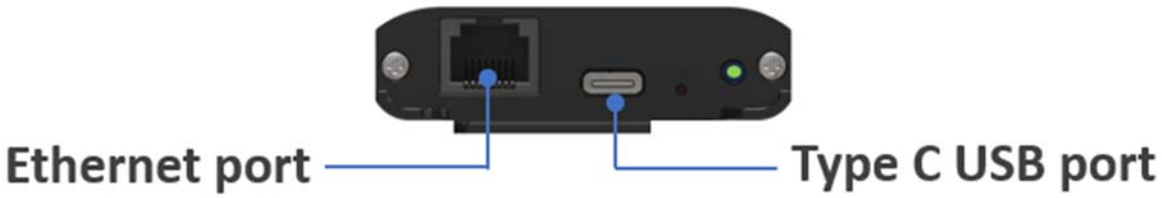
NOTE: The last four characters of your M2M box Wi-Fi network name are unique. You can change the Wi-Fi name to your preference. See the "Settings" section for instructions.

Via USB connection

To enable a data connection via the USB port, simply connect your host device to the M2M Box using the provided USB cable. This will power the M2M Box and simultaneously establish a data connection.

Via Ethernet connection

When your M2M box is on, simply connect your host device to the M2M Box using an Ethernet cable (not included) to establish a data connection through the Ethernet port.



Using Your M2M Box after Setup is Complete

M2M Box to share connections

You can use your M2M Box as a wireless local network gateway to connect a maximum of 15 Wi-Fi capable devices to the mobile broadband network. Data connections through USB port and Ethernet ports are also available for more secure connectivity.

Web Admin Home Page Password Change

The M2M Box 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.

Updating Your M2M Box software

The new software is updated automatically in the following scenarios.

1) The M2M Box will check for a new SW update periodically.
2) If a new update is available, it will be downloaded automatically.
3) If the device is continuously powered on, the update will be automatically applied at 2AM the next day.
4) If there is traffic or data activity at 2AM the next day, the device will wait until the next day 2AM to apply the update.

3

M2M Box Settings

Managing M2M Box via Web Admin Home Page
Home
Messages
Settings
About
Support

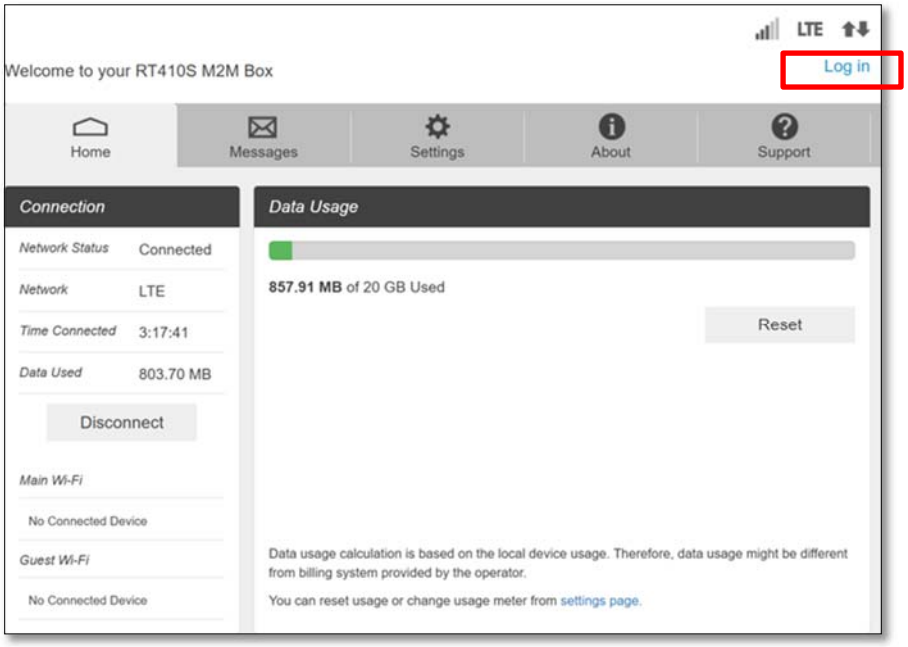
Managing M2M Box via Web Admin Home Page

Access the M2M Box Web Admin Home Page

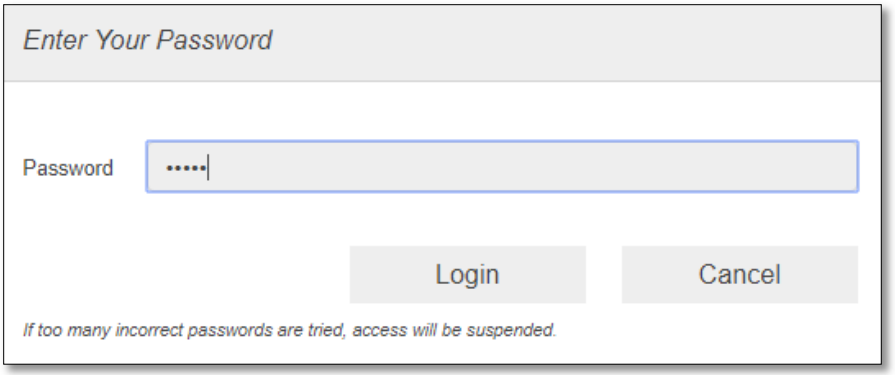
You can access your Mobile M2M Box Admin Home Page using an internet browser.

Access Mobile M2M Box Web Admin Home Page using a browser

1 Connect your Wi-Fi capable device to the Mobile M2M Box.
2 Open a web browser on your connected device and visit http://mobile.hotspot . Enter the password and Click **Log in** located on the upper right corner.



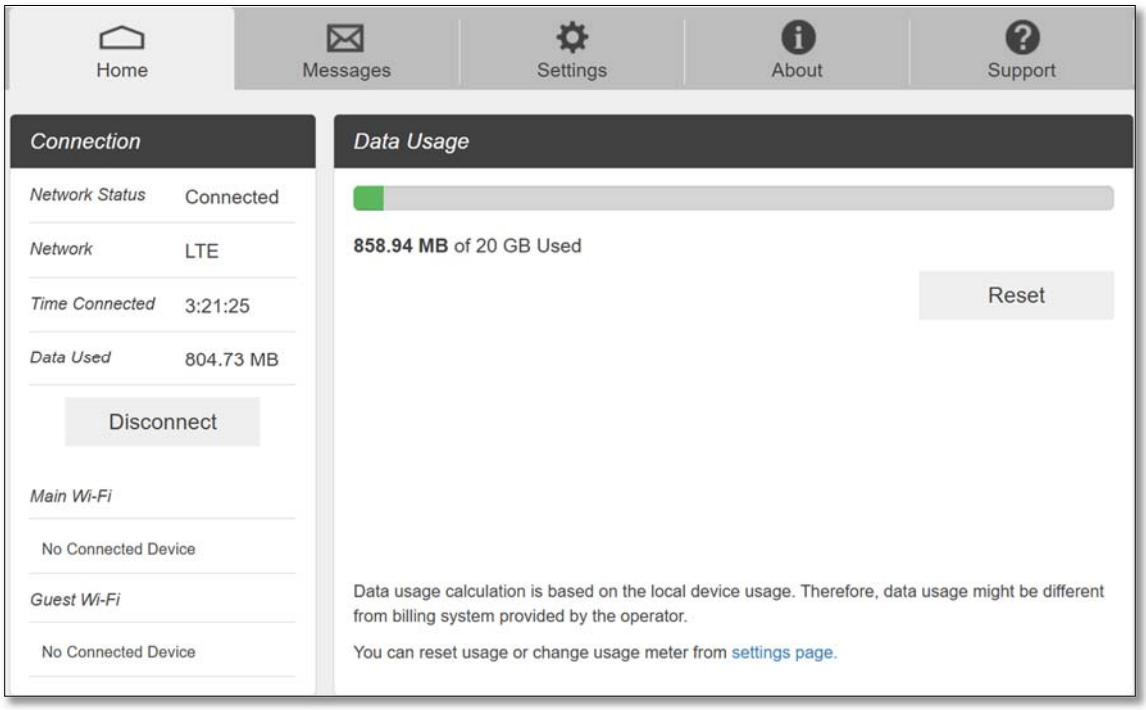
NOTE: The default password is **admin**. On your first login, you will be directed to change the password.



Home

Check status of network connection and data usage

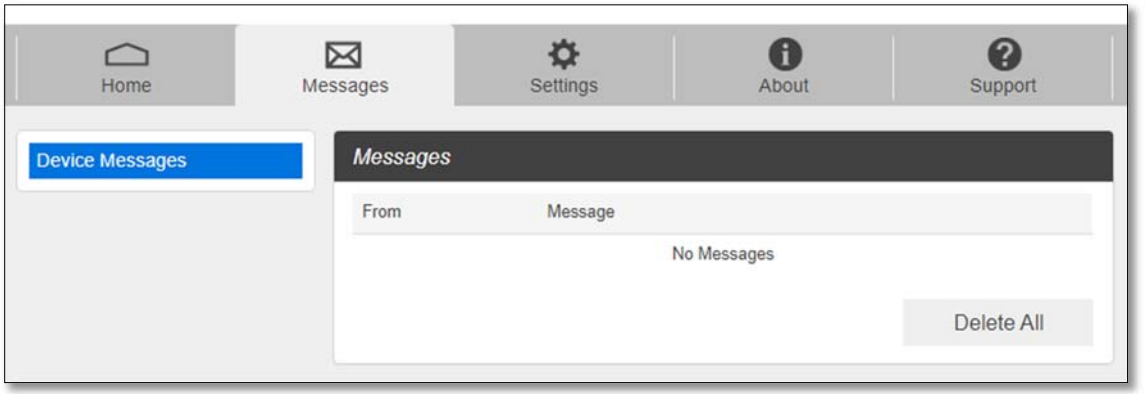
- Disconnect: Click **Disconnect** to disconnect the Internet.
- Reset: Reset data usage meter to zero.



Messages

Messages page displays SMS messages your device receives.

You can see the message received. 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.



Settings

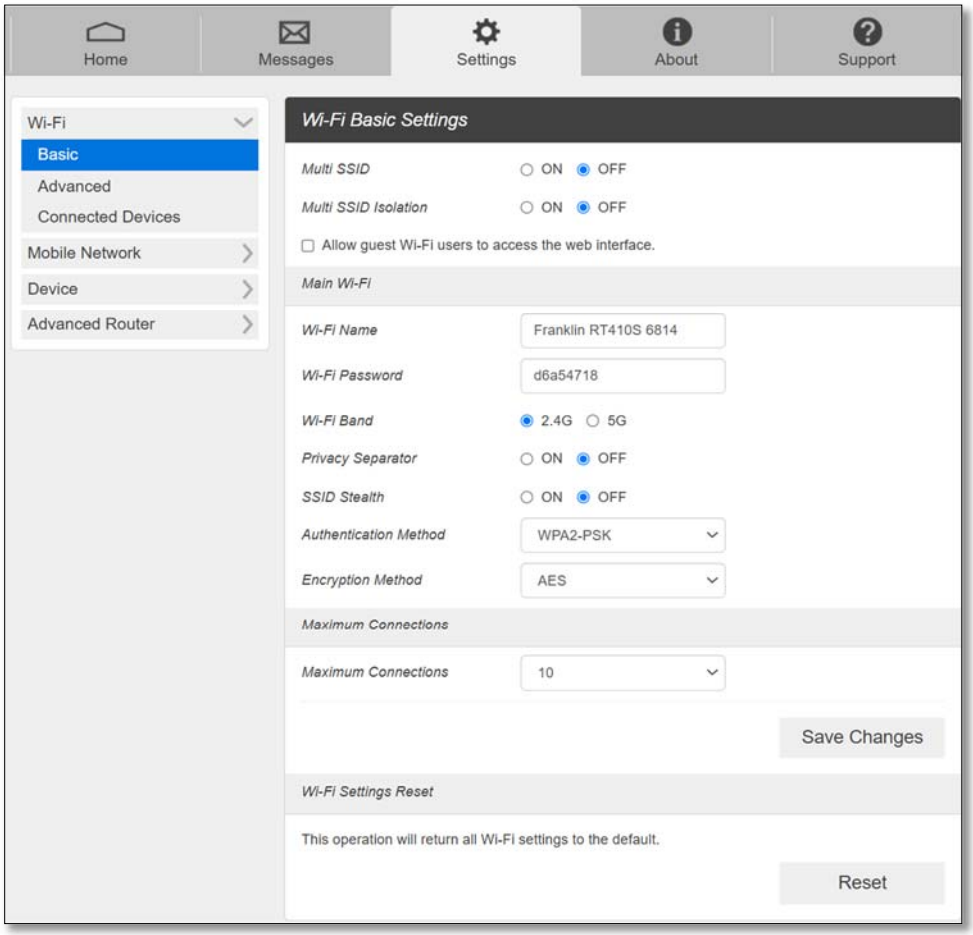
The **Settings** page has the following menu options.

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

Wi-Fi

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

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

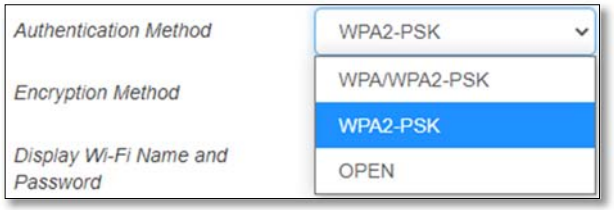


- **Multi SSID**: Select ON if you would like to set up a separate guest Wi-Fi network. Your M2M Box will broadcast two Wi-Fi names.
- **Guest Wi-Fi**: If Multi SSID is set ON, Guest Wi-Fi menu will appear. You can change Guest Wi-Fi settings.
- **Multi SSID Isolation**: If ON is selected, it prevents your devices from communicating across the Main and Guest Wi-Fi access points.
- **Allow Guest Wi-Fi users to access the Web interface**: If the box is checked, users on the Guest Wi-Fi also can access the **Web Admin Page**.

- **Wi-Fi Name**: Wi-Fi Service Set Identifier (SSID). To change it, enter a string of 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.
- **Privacy Separator**: If ON is selected, your devices on the same Wi-Fi Name cannot 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 depending on your preference.

NOTE: if you connect WLAN printer to your M2M Box, Privacy Separator should be OFF to send file from your PC to the printer

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

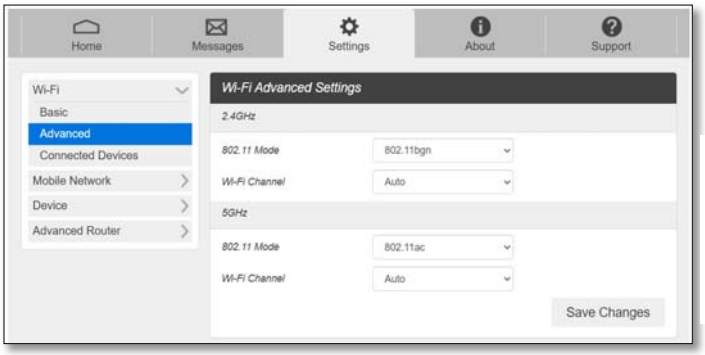


Mode	Description
WPA-PSK/WPA2-PSK	Apply both the WPA-PSK and WPA2-PSK scheme.
WPA2-PSK	WPA-PSK is the securer version of WPA with implementation of the 802.11i standard.
OPEN	Open authentication

- **Encryption Method:** Select an encryption method from the drop-down list.
- **Maximum Connections:** Choose the maximum number of devices that can connect to your M2M Box simultaneously.
- **Wi-Fi Settings Reset:** Click the Reset button to reset all Wi-Fi settings to the default settings.

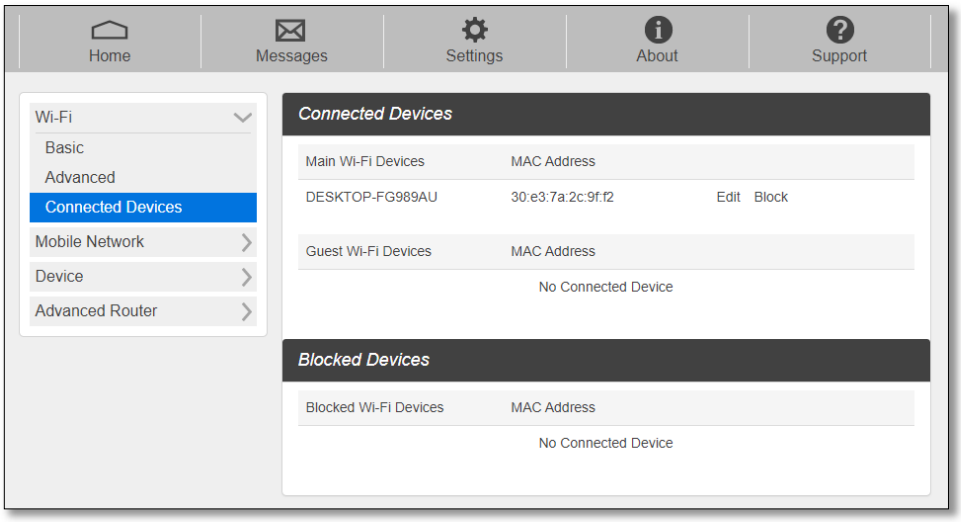
- **Advanced**

Advanced settings allow you to change Wi-Fi mode and channel settings. Be cautious, as changes to these settings could result in the loss of Wi-Fi connections with your devices. Consult your devices' manuals for Wi-Fi specifications before making any changes.



- **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.

- **Connected Devices**



Connected Devices menu has the following information and options:

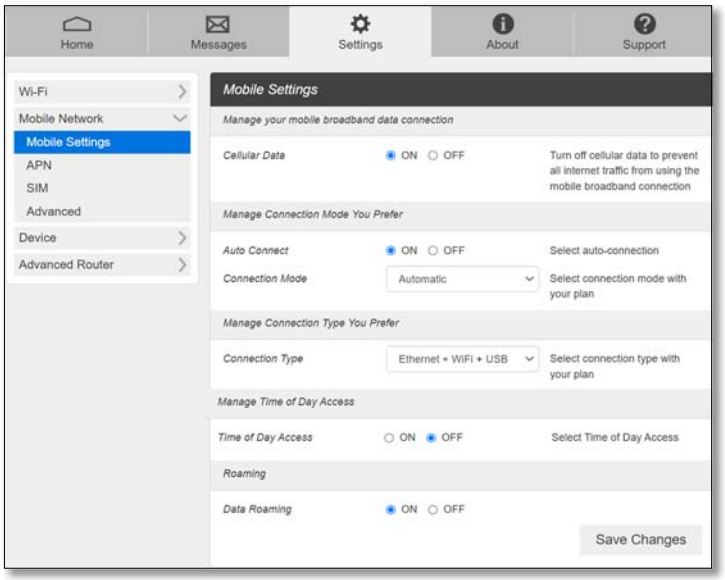
- **Main Wi-Fi Devices**: Normally this is the hostname of the connected device as set on the connected device. You can use the pencil tool to change the name of any connected device.
- **MAC Address**: The MAC address is a unique network identifier for the connected device.

To Edit a Connected Device, click on the **Edit** and update the name of the device and click **OK**.

- **Blocked Devices** menu has the following information and options:
- **Blocked Wi-Fi Devices:** List of devices blocked from Connected Devices menu.
- **MAC Address**: The MAC address is a unique network identifier for this blocked device.

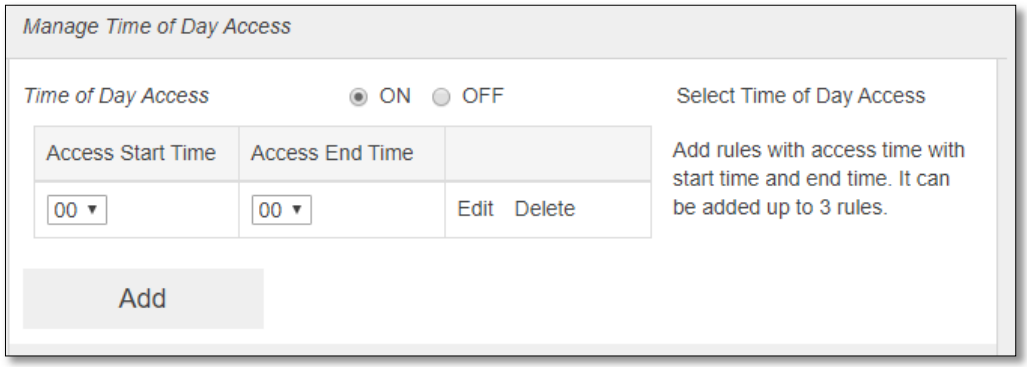
Mobile Network

Manage your mobile network settings.



- **Mobile Settings**
  - **Cellular Data**: You can turn on/off the data connection on cellar network.
  - **Auto Connect**: If OFF is selected, your M2M Box will not connect to the network automatically on next powering on. You need to log in to the Web Admin Page and connect manually.
  - **Connection Mode**: Automatic / 4G only / 3G only. Automatic is selected as a default for your M2M Box to choose the best network available automatically.
  - **Connection Type**: You can select connection between your M2M Box and other host devices. Ethernet + WiFi + USB / Ethernet + WiFi / Ethernet + USB.

  - **Time of Day Access**: This feature allows you to select specific time windows each day during which data connection via your M2M Box is permitted. You can set up three different time ranges.

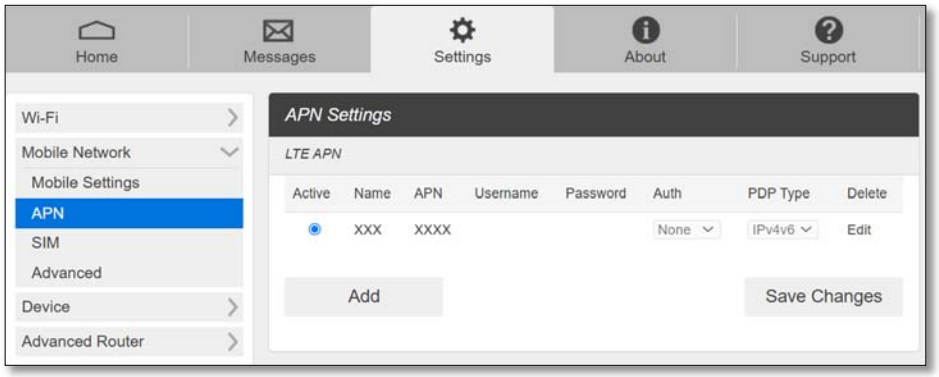


  - **Data Roaming**: Turn Data Roaming on or off.

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

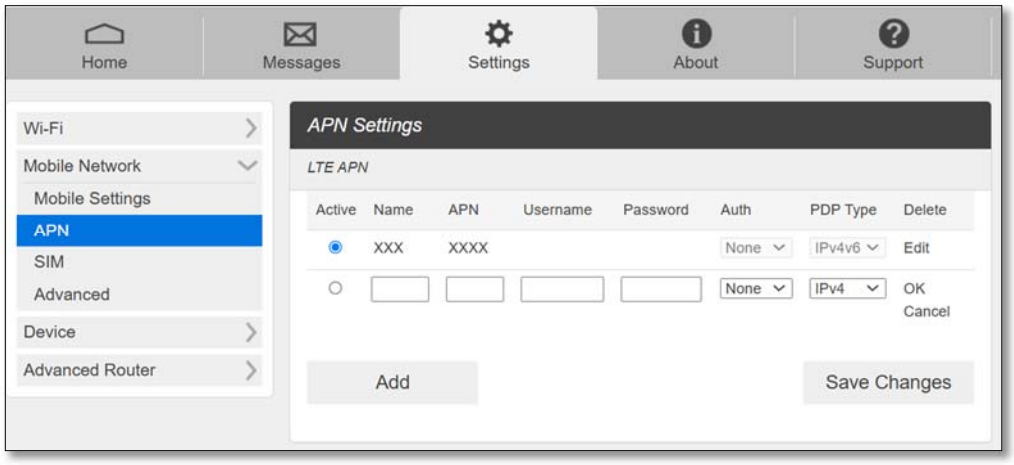
- **APN**

This menu displays the current APN settings.



To add a new APN, follow the steps below:

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



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 press **Save Changes** to apply.

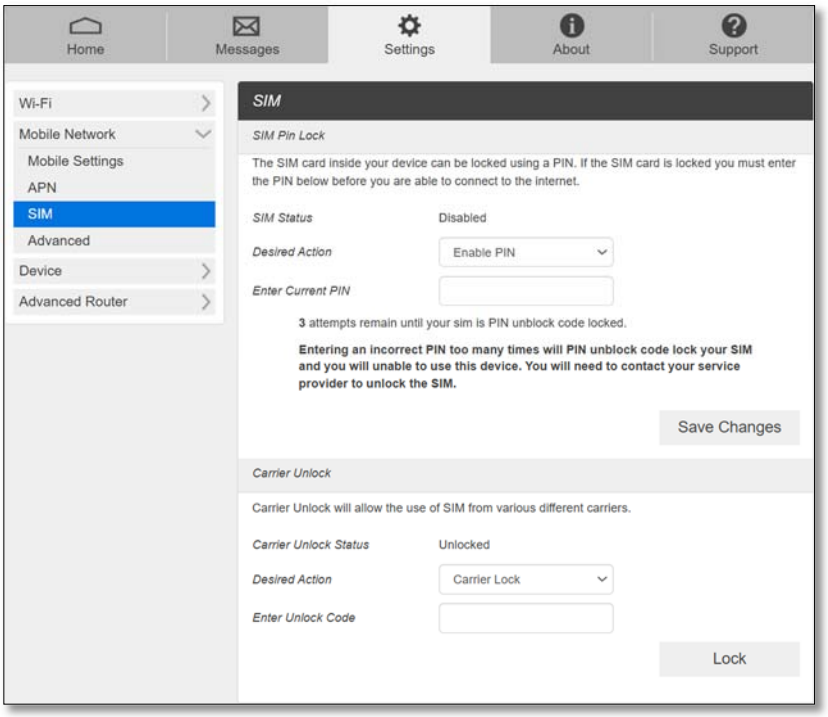
CAUTION! Changing APN information could result in connection failure. Please contact your service provider before changing APN only when it is needed.

- **SIM**
  - **SIM Pin Lock**: 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.

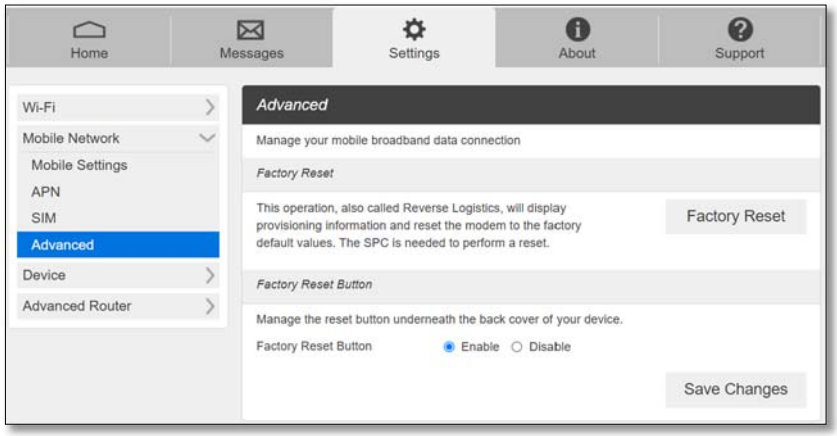
NOTE: If you enter the wrong SIM PIN three times, your SIM will be disabled permanently until you enter the PUK code from your service provider.

- **Carrier Unlock**: Your M2M Box could be locked to recognize the SIM from your wireless service provider only. To use other SIMs from other wireless service providers, you need to unlock the carrier setting. The unlock code can be provided by your current wireless service provider.



.

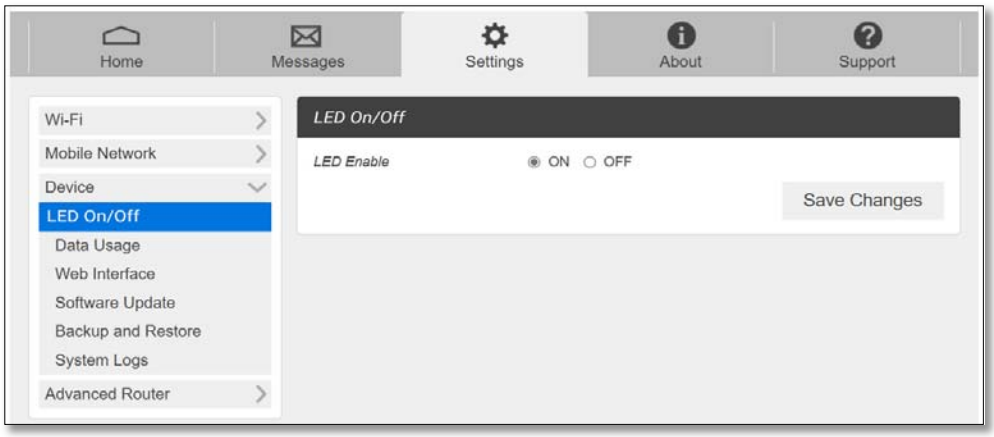
- **Advanced**



- **Factory Reset**: Click Factory Reset to return all device settings to the factory default settings.
- **Factory Reset Button**: You can disable the physical Factory Reset button located on the device front for more security.

Device

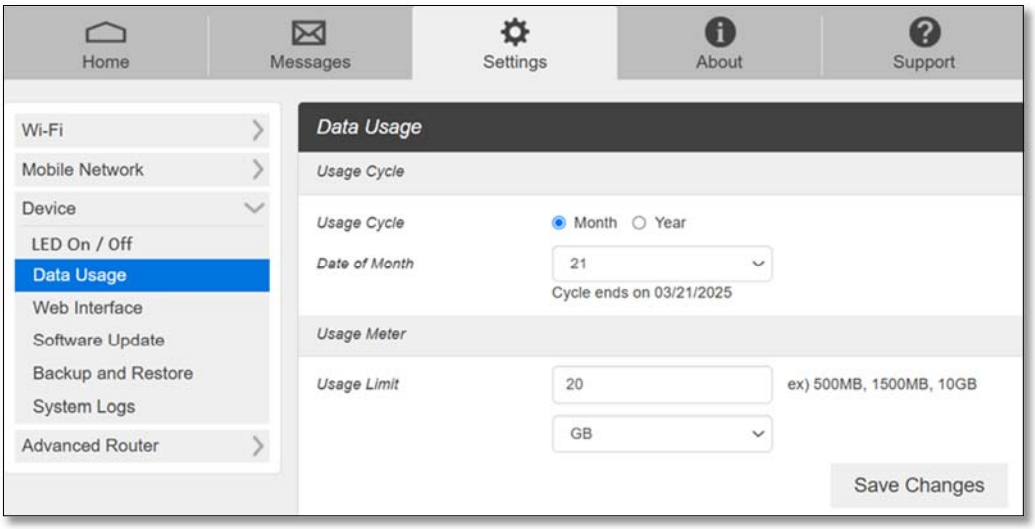
- **LED On/Off**



- **LED Enable**: If ON is selected, the LED indicator on your M2M Box will be on indicating service status.

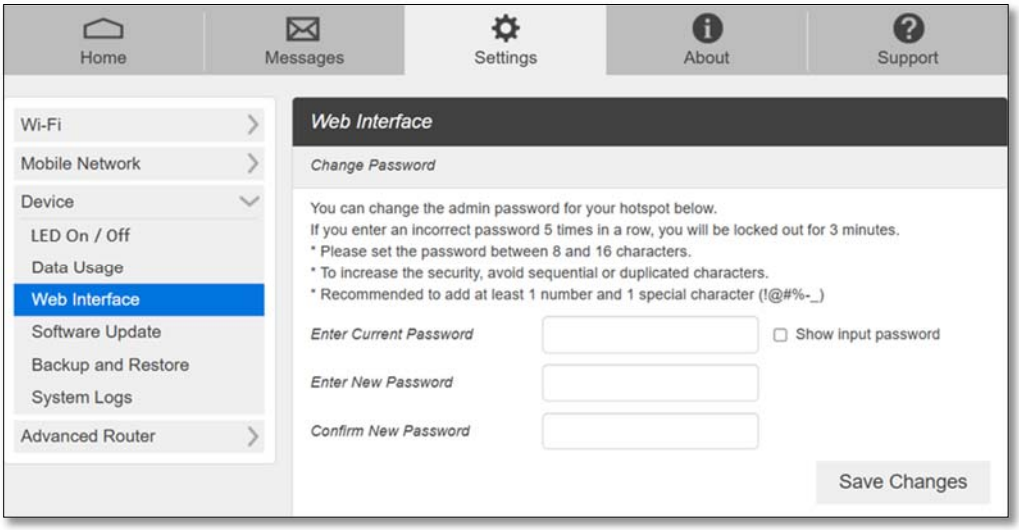
- **Data Usage**

This setting is to display data usage on the Web Admin Home page.



- **Usage Cycle**: Select Data Usage Cycle either monthly or yearly. On the date set, the data usage information will reset to zero.
- **Usage Meter**: You can select Data Usage Limit and usage unit (MB or GB).

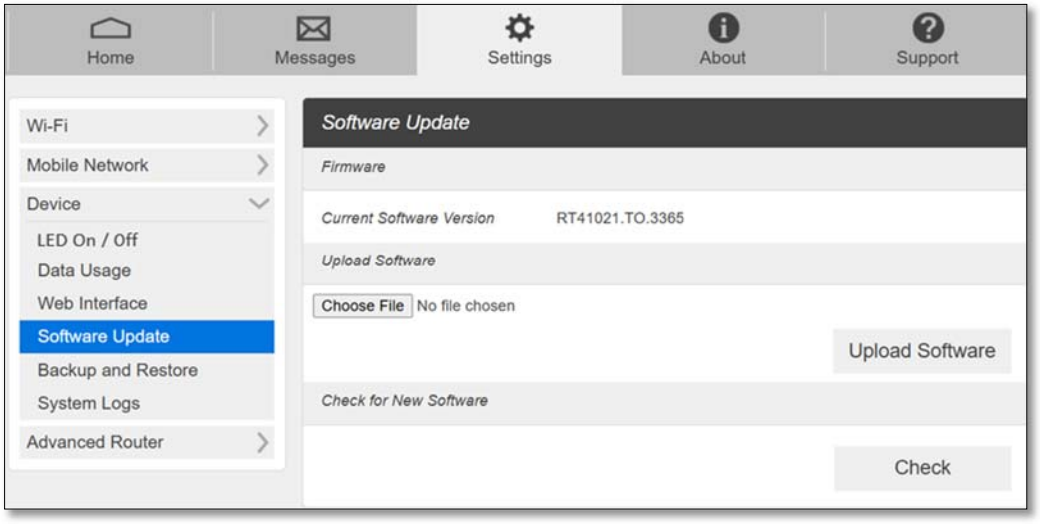
- **Web Interface**



- **<u>Change Password</u>**: You can change Web Admin login password with following steps.
  1. Current Password: Enter the current password.
  2. New Password: Enter the new password.
  3. Confirm New Password: Enter the new password again.
  4. Click **Save Changes** to save your new password.

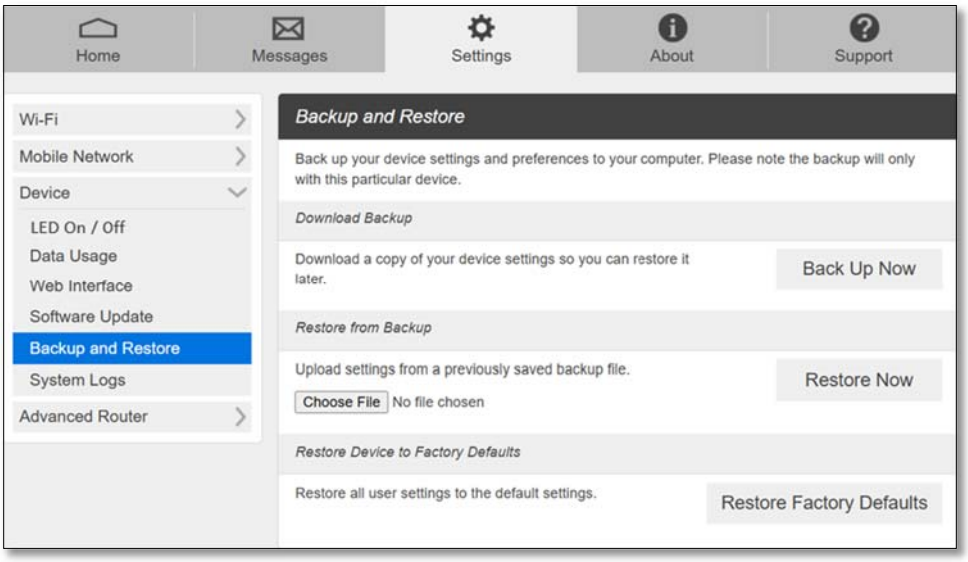
- **Software Update**

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



- **Firmware**: Current software version
- **Upload Software<u>:</u>** 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<u>:</u>** Click **Check** button. Message windows will pop up and guide you through the update process.

- **Backup and Restore**



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

1. Click **Back Up Now**.
2. Click **Save** on the pop-up window.
3. Choose a location on your computer to save the backup file.
4. Click **Save**.

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

1. Click **Choose File** to select the backup file in your computer.
2. Click **Restore now**.

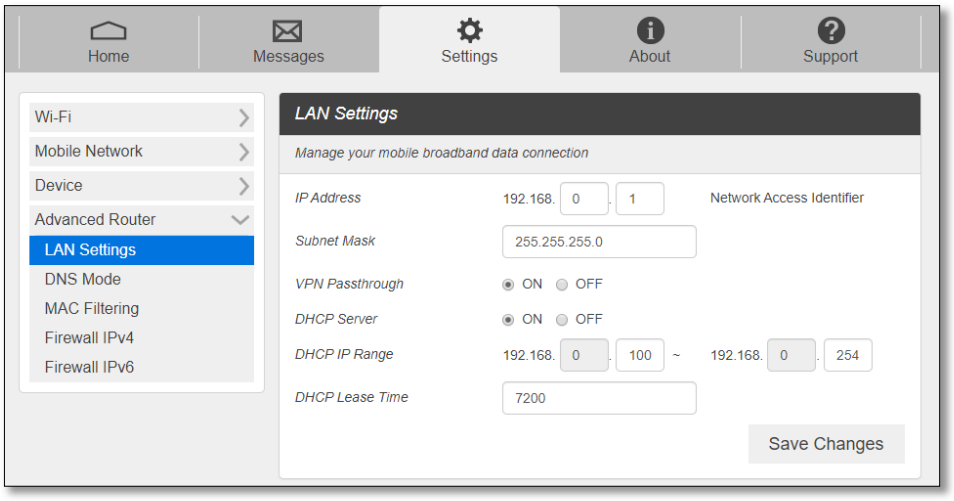
To restore your device to its factory default settings, follow the steps below:

1. Click **Restore Factory Defaults**.
2. Click **OK** to confirm the command.

Advanced Router

Configure LAN, Firewall, and IP Passthrough settings.

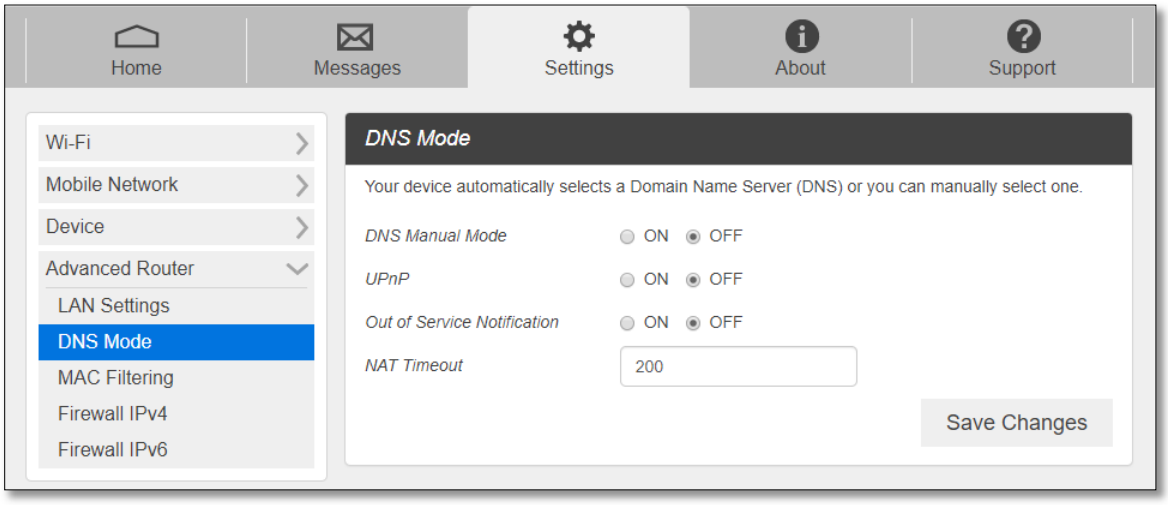
- **LAN Settings**



- **IP address:** The IP address of the default gateway and for your device Web Admin Page.
- **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 it is 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.



  To manually set a Domain Name Server:

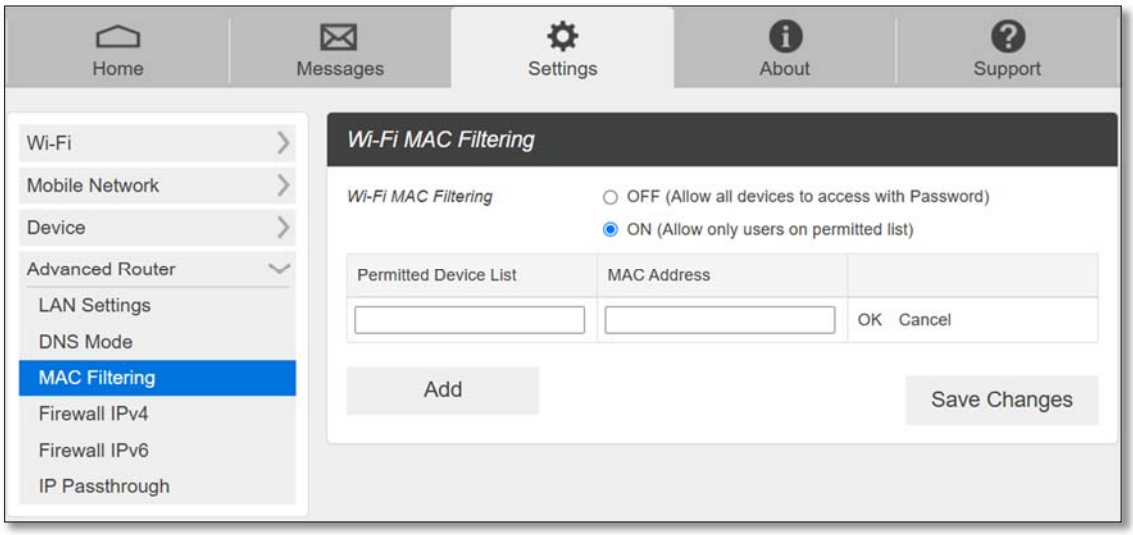
  1 Click the **ON** button to enable **Manual DNS**.
  2 Enter the IP address of the first DNS in the **DNS Address 1** field.

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 M2M Box 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**.

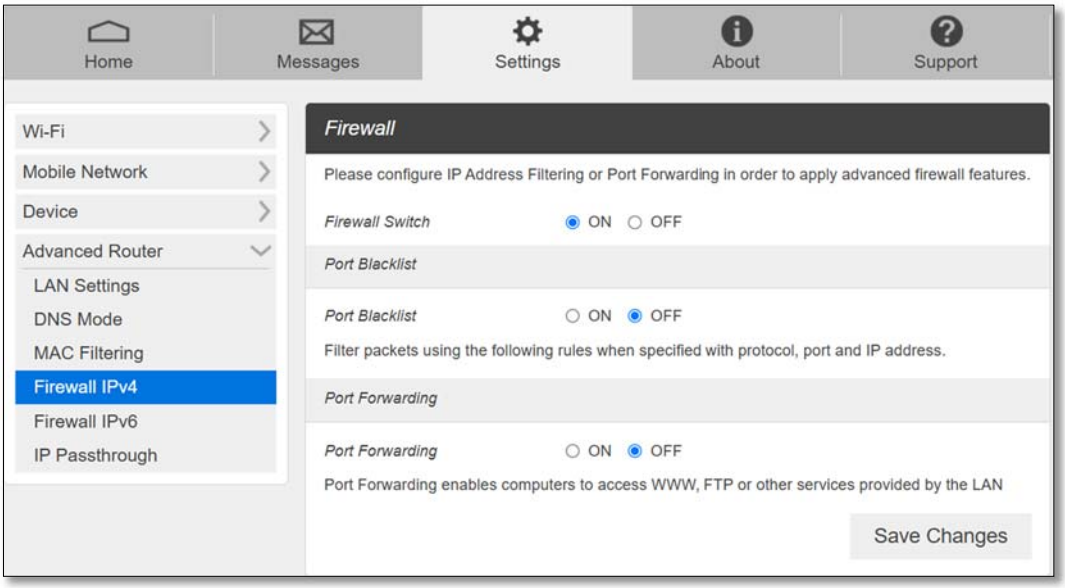


To enable MAC Filtering,

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. Press **Save Changes**.

NOTE: If you enable Wi-Fi MAC filtering, only the devices listed here can connect to your M2M Box Wi-Fi network. MAC filtering works only on Wi-Fi connections. Ethernet or USB connection is not affected by MAC filtering settings.

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

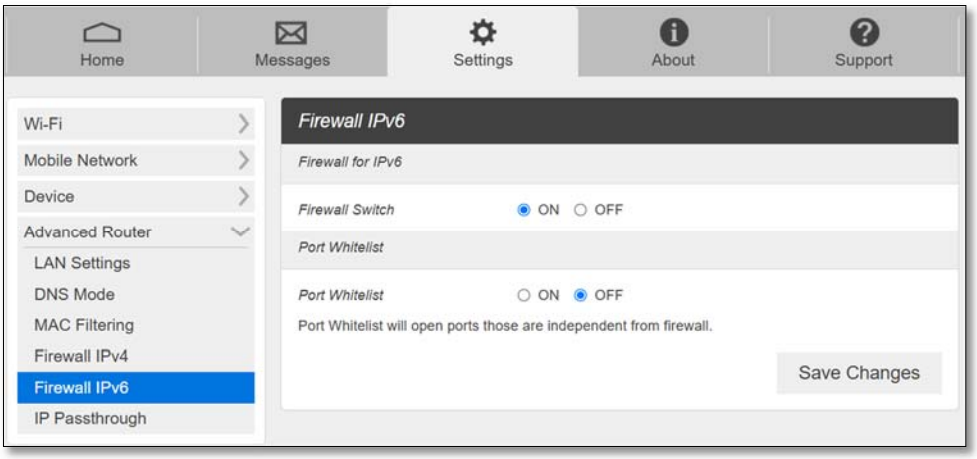


- **Firewall Switch:** To set up Port Blacklist and Port Forwarding, turn Firewall Switch **ON**. If Firewall Switch is **OFF**, both Port Blacklist and Port Forwarding settings are not active.

- **Port Blacklist:** You can block outbound forward packet by setting up a rule in the blacklist. To set up the rules,
  1. Turn **ON** Port Blacklist.
  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 the 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 numbers 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 addresses 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 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**

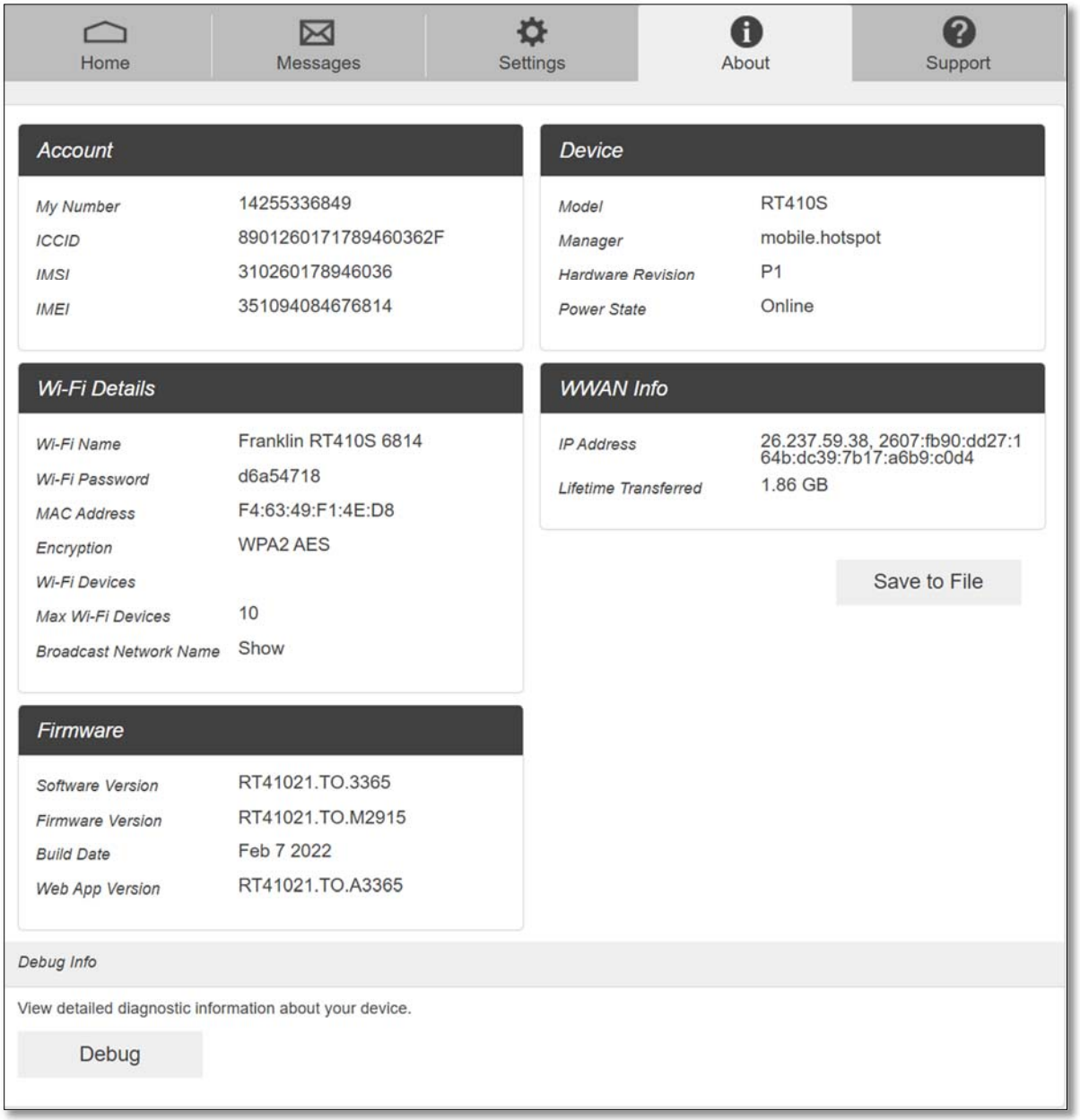
  IP Passthrough is a networking feature that allows a specific device on your local network to be exposed to the internet by assigning the M2M box's public IP address to it. This is particularly useful for hosting servers, remote desktop sessions, or other applications that require direct access from the internet.

To set up IP Passthrough, select USB or Ethernet as needed from the drop menu and press **Save Changes**.

NOTE: If IP passthrough is enabled either on USB or Ethernet, all Wi-Fi function will be disabled, and Wi-Fi connection becomes unavailable. The device connected to your M2M Box USB port or Ethernet will have a direct connection to the Internet with public IP passed through by your M2M box.

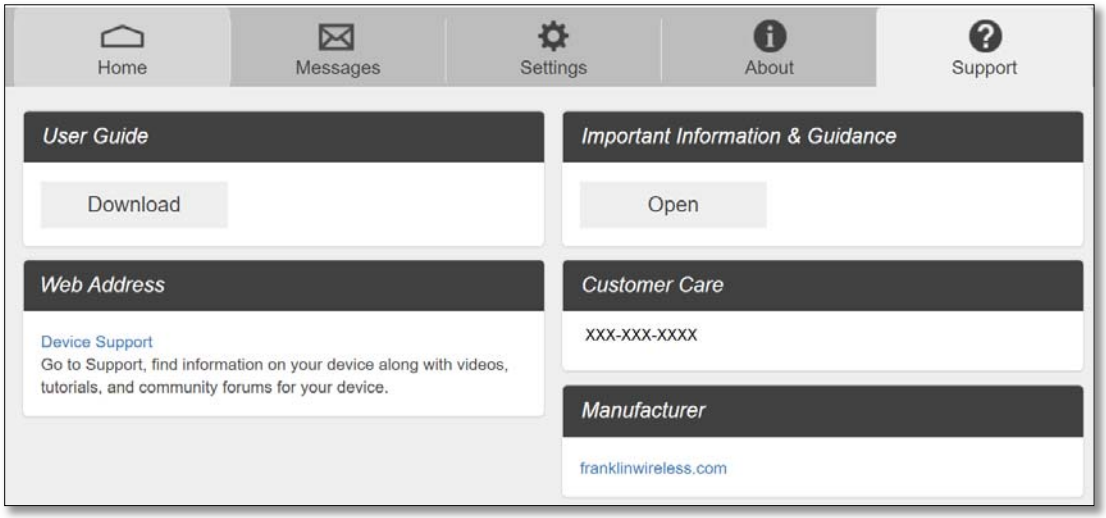
About

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



Support

Obtain additional information from the Web Admin Home Support Tab.



4

Troubleshooting

Overview
First Steps
Common Problems and Solutions

Overview

The following tips can help solve many common problems encountered while using the RT410S M2M Box.

First Steps

1 Make sure you are using your M2M Box 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 M2M Box can resolve many issues.

Common Problems and Solutions

How do I perform Factory Reset?

- **Using the reset button**: Make sure the M2M box is powered on. Press down the reset button with a pin for 3 seconds and release. Your M2M Box will perform the reset and restart automatically.

- **Using Web Admin Home**: Connect to your M2M Box and then open **Web Admin Home** page (http://mobile.hotspot). Select **Settings > Device > Backup and Restore** and press **Restore Factory Defaults.**

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 M2M Box and keep the same Wi-Fi Name, the devices try to connect to your M2M Box using the Wi-Fi name and previous Wi-Fi password saved, causing Wi-Fi authentication errors.

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.**

5

Regulatory Information

Regulatory Statements
Safety Hazards

Regulatory Statements

FCC Equipment Authorization ID: XHG-RT410S

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.
(2) This device must accept any interference received, including interference that may cause undesired operation.

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

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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.2.3
Date: February 25, 2025

6

Glossary

Glossary

Term	Definition
LTE	Long-Term Evolution
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
M2M Box	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