AT&T

AT&T Velocity® 3 User Guide

DOC20210105

Contents

Introduction

The following topics describe the basics of using this guide and your new mobile hotspot.

About the user guide

Thank you for purchasing your new AT&T Velocity® 3 mobile hotspot. The following topics explain how best to use this guide to get the most out of your mobile hotspot.

Before using your mobile hotspot

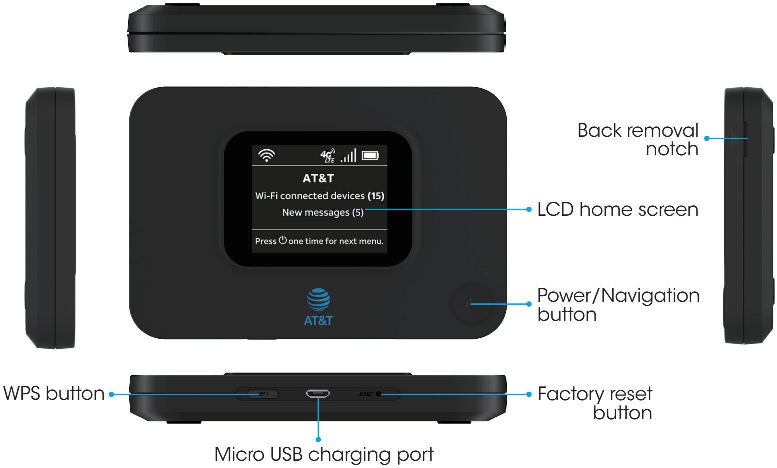
Read the Safety Information Guide that came with your device thoroughly for proper usage. Accessible services may be limited by subscription contract conditions.

Descriptions in the user guide

Note that most descriptions in this guide are based on your mobile hotspot's setup at the time of purchase.

Getting started

Getting to know your mobile hotspot



Note: Your mobile hotspot's screens are subject to change. This user guide uses sample images only.

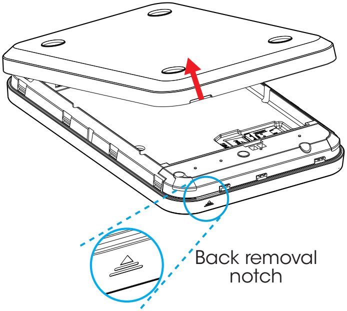
Part	Description
Power/Navigation button	• Press once to turn the screen on. • Press and hold for three (3) seconds to turn your mobile hotspot on or off. • From home screen, press one time to scroll through the main screens. • From main screens, press two times to access the details of each main screen.
LCD home screen	View information and access features of your mobile hotspot.
Micro USB charging port	Connect the included charger for charging. Connect a micro USB cable for tethering (sold separately).
WPS button	Use WPS button to connect without entering the Wi-Fi password.
Factory reset button	Using a narrow object, such as a paperclip or ballpoint pen, press and hold the **Factory reset** button for five (5) seconds to perform a factory reset.
Back removal notch	Use the back removal notch to remove the back cover.

Installation

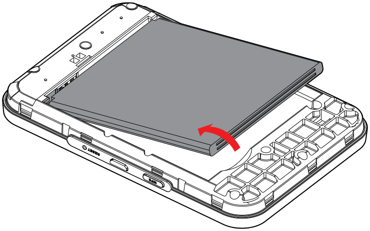
Install the SIM card

A SIM card is pre-inserted. If the SIM card needs to be replaced, follow the below steps:

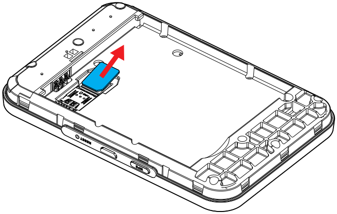
1. Gently remove the back cover via the notch indicated by the arrow.



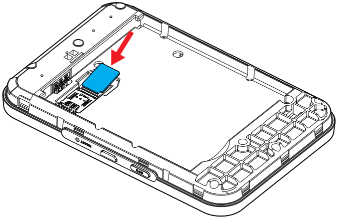
2. Take the battery out.



3. Remove the current SIM by pressing down on the clip and sliding the SIM card out.



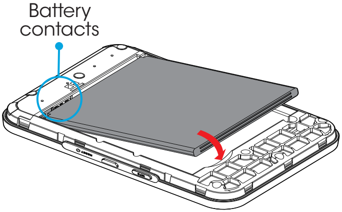
4. Insert a replacement SIM by pressing down on the clip and sliding the SIM card into the SIM slot with the gold contacts facing downward and the cut corner on the bottom left.



Note: A SIM card is pre-inserted and it is recommended that you use the pre-inserted SIM card or one that is provided to you by AT&T.

Install the battery

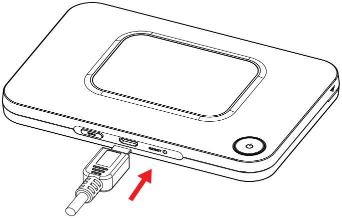
1. Insert the battery by aligning the battery contacts with the terminals in the battery compartment.



2. Reattach the back cover and press firmly around sides and all four corners until it snaps into place.

Charge your mobile hotspot

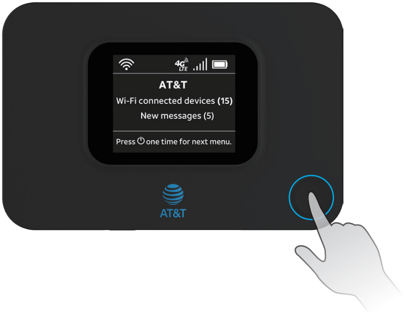
1. Connect the micro USB end of the included charger into the micro USB charging port located at the bottom of your mobile hotspot.



2. Connect the other end of the included charger to an electrical outlet to fully charge your mobile hotspot. It may take approximately 3.5 hours to fully charge.

Turn on your mobile hotspot

Press and hold the **Power/Navigation** button for three (3) seconds to turn on your mobile hotspot.



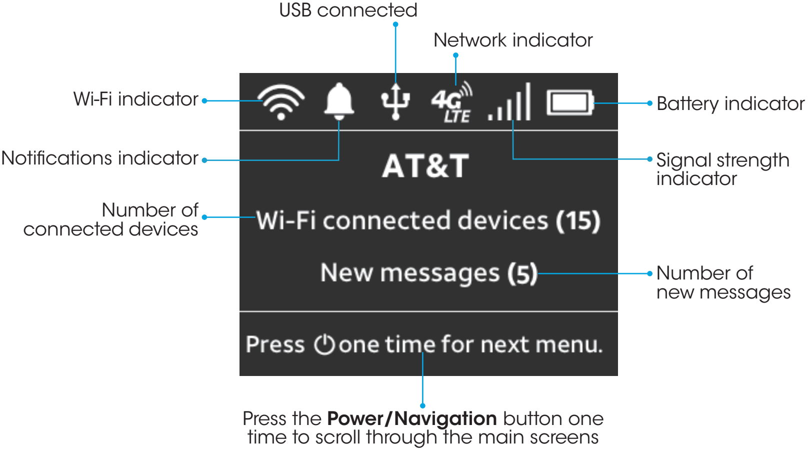
Check the wireless signal

Wait a few seconds for the signal strength icon 📶 to display on the screen, which will confirm that your device is connected to the cellular network.

Confirm signal strength has five (5) bars for optimal performance. Fewer bars indicate a moderate signal, which may be sufficient.

LCD display screen

Home screen



AT&T

Wi-Fi connected devices (15)

New messages (5)

Press ⏻ one time for next menu.

USB connected
Network indicator
Wi-Fi indicator
Battery indicator
Notifications indicator
Signal strength indicator
Number of connected devices
Number of new messages
4G LTE
Press the **Power/Navigation** button one time to scroll through the main screens

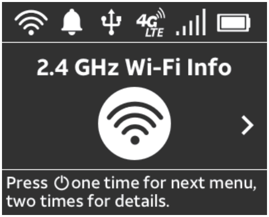
Note: Display screen will timeout after 1 minute of inactivity to save power. Press the **Power/Navigation** button one time to wake the screen. This default setting can be adjusted on the AT&T Wi-Fi Manager, see *"Power saving" on page 46*.

Indicator	Name	Function/Service
🛜	**Wi-Fi indicator**	Wi-Fi on
🔔	**Notifications indicator**	New notifications received
🔌	**USB connected**	USB connected for tethering
4G LTE	**Network indicator**	Network information
📶	**Signal strength indicator**	Indicates the signal strength. More signal bars indicates higher signal strength.
🔋	**Battery indicator**	Show battery status: • White: High • Yellow: Medium • Red: Low or no charge • Charging: Lightning bolt icon
	Wi-Fi connected devices (15)	The number inside the parenthesis indicates the number of Wi-Fi connected devices.
	New messages (5)	The number inside the parenthesis indicates the number of new messages.

Indicator	Name	Function/Service
	Press ⏻ one time for next menu	Press the **Power/Navigation** button one time to scroll through the main screens

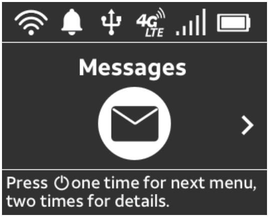
Other main screens

Press the **Power/Navigation** button one time to scroll through the main screens, press it two times to access the details of each main screen.


2.4 GHz Wi-Fi Info

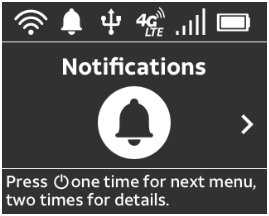
Press ⏻ one time for next menu, two times for details.

Wi-Fi screen


Messages

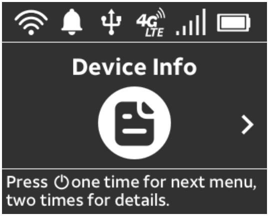
Press ⏻ one time for next menu, two times for details.

Messages screen


Notifications

Press ⏻ one time for next menu, two times for details.

Notifications screen


Device Info

Press ⏻ one time for next menu, two times for details.

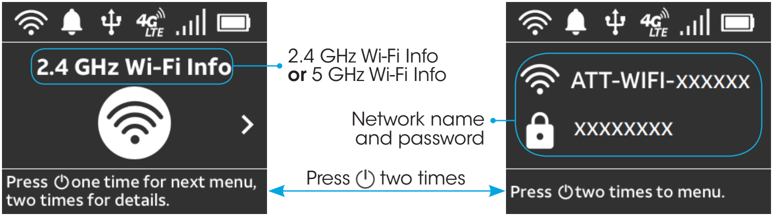
Device info screen

Wi-Fi Info screen

From the Home screen, press the **Power/Navigation** button one time to access the Wi-Fi Info screen.

From the Wi-Fi Info screen, press the **Power/Navigation** button two times to access the Wi-Fi Info details screen to view your Wi-Fi network name and password.

You can change the default Wi-Fi network name and password via the AT&T Wi-Fi Manager, see *"Changing Wi-Fi network name and password" on page 22*.



Press ⏻ one time for next menu, two times for details.

Press ⏻ two times to menu.

2.4 GHz Wi-Fi Info **or** 5 GHz Wi-Fi Info

Network name and password

Press ⏻ two times

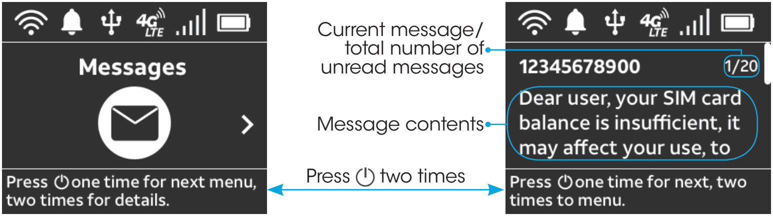
Your mobile hotspot does not simultaneously broadcast 2.4 GHz and 5 GHz Wi-Fi networks. The default Wi-Fi network is 2.4 GHz, but you can go to the AT&T Wi-Fi Manager to switch to the 5 GHz network, see *"Wi-Fi" on page 28*.

Note: The Wi-Fi name and password are visible by default, and you can hide it via the AT&T Wi-Fi Manager, see *"Show network name and password on device" on page 31*

Messages screen

From the Wi-Fi Info screen, press the **Power/Navigation** button one time to access the Messages screen.

From the Messages screen, press the **Power/Navigation** button two times to access the Messages details screen to view the latest unread message.



Press ⏻one time for next menu, two times for details.

12345678900 1/20

Dear user, your SIM card balance is insufficient, it may affect your use, to

Press ⏻one time for next, two times to menu.

If a message is too long to display in one screen, press the **Power/Navigation** button one time to view the next screen of the current message.

From the last screen of the latest message, press the **Power/Navigation** button one time to view the next unread message.

To view or delete the previous read messages, go to the AT&T Wi-Fi Manager, see *"Messages" on page 33*.

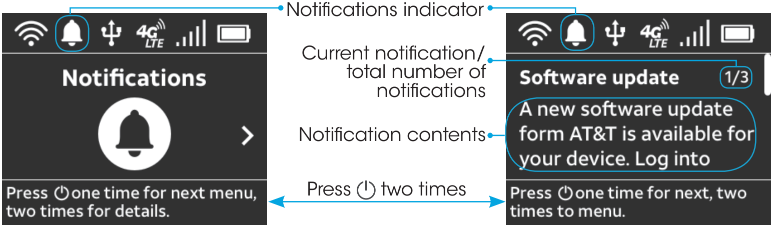
Notifications screen

From the Messages screen, press the **Power/Navigation** button one time to access the Notifications screen.

From the Notifications screen, press the **Power/Navigation** button two times to access the Notifications details screen to view the latest notification.

Notifications screen displays alert and reminder information that requires further action from the user, like a software update available, maximum Wi-Fi connections reached, maximum number of messages reached, etc.

Notifications will disappear automatically when the user has performed the corresponding actions and changed the device status.


Notifications indicator

Notifications

Press ⏻ one time for next menu, two times for details.

Current notification/ total number of notifications

Notification contents

Press ⏻ two times

Software update 1/3

A new software update form AT&T is available for your device. Log into

Press ⏻ one time for next, two times to menu.

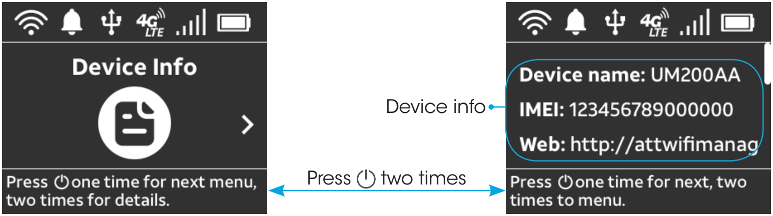
If a notification is too long to display in one screen, press the **Power/ Navigation** button one time to view the next screen of the current notification.

From the last screen of the latest notification, press the **Power/Navigation** button one time to view the next unread notification.

Device Info screen

From the Notifications screen, press the **Power/Navigation** button one time to access the Device Info screen.

From the Device Info screen, press the **Power/Navigation** button two times to access the Device Info details screen to view your hotspot's important information.


Device Info

Press ⏻ one time for next menu, two times for details.

Device info

Press ⏻ two times

Device name: UM200AA

IMEI: 123456789000000

Web: http://attwifimanag

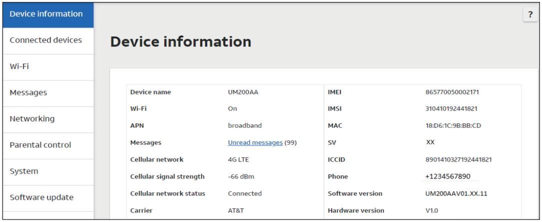
Press ⏻ one time for next, two times to menu.

AT&T Wi-Fi Manager

The AT&T Wi-Fi Manager allows you to easily manage your mobile hotspot.

You can:

- Customize settings
- Change your Wi-Fi network name and password
- Check signal strength and important messages from AT&T
- Get help and information

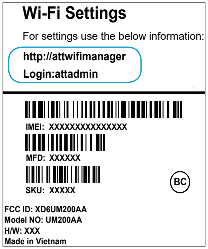


Device information

Device name	UM200AA	IMEI	865770050002171
Wi-Fi	On	IMSI	310410192441821
APN	broadband	MAC	18:D6:1C:9B:BB:CD
Messages	Unread messages (99)	SV	XX
Cellular network	4G LTE	ICCID	8901410327192441821
Cellular signal strength	-66 dBm	Phone	+1234567890
Cellular network status	Connected	Software version	UM200AAV01.XX.11
Carrier	AT&T	Hardware version	V1.0

Access the AT&T Wi-Fi Manager via the Wi-Fi network connection

1. Connect your device to the 2.4 GHz or 5 GHz Wi-Fi networks provided by your mobile hotspot.
2. Enter **http://attwifimanager** or **http://192.168.1.1** into browser address field of your device.
3. Log in using the default AT&T Wi-Fi Manager login password printed on the device label located underneath the battery of your mobile hotspot.



Wi-Fi Settings

For settings use the below information:

http://attwifimanager
Login:attadmin

IMEI: XXXXXXXXXXXXXXX

MFD: XXXXXX

SKU: XXXXX

FCC ID: XD6UM200AA
Model NO: UM200AA
H/W: XXX
Made in Vietnam

Access the AT&T Wi-Fi Manager via a micro USB cable (sold separately)

1. Connect your mobile hotspot and your device using a micro USB cable.
2. Enter **http://attwifimanager** or **http://192.168.1.1** into browser address field of your device.
3. Log in using the default AT&T Wi-Fi Manager login password printed on the

device label.

Note: You can customize the login that is used to access the AT&T Wi-Fi Manager by going to **System** > **Administration**. If you have changed the login and have forgotten the new one, you must restore the device to the factory default settings. Using a narrow object, such as a paperclip or ballpoint pen, press and hold the **Factory reset** button located at the bottom of your mobile hotspot for five (5) seconds. You may then log in using the default login password printed on the device label located underneath the battery of your mobile hotspot.

The AT&T Wi-Fi Manager includes a navigation panel on the left side of the screen, which contains the following sections:

- **Device information** – Display general device information (see *"Device information" on page 26*).
- **Connected devices** – View devices currently connected to your mobile hotspot and block/unblock Wi-Fi devices from connecting (see *"Connected devices" on page 27*).
- **Wi-Fi** – Customize your device's Wi-Fi and security settings (see *"Wi-Fi" on page 28*).
- **Messages** – View messages from AT&T about your service plan (see *"Messages" on page 33*).
- **Networking** – Access a wide range of network and security settings (see *"Networking" on page 34*).
- **Parental control** – Control days and times a device can connect to the Internet and limit the permitted websites (see *"Parental control" on page 42*).
- **System** – Manage system administration functions such as set Date/Time, change Password, Factory reset, Reboot, etc. (see *"System" on page 44*).
- **Software update** – Display the current software version installed and check for updates (see *"Software update" on page 50*).

Status indicators

In addition to the indicators on the LCD display screen of your mobile hotspot, you can find information about your mobile hotspot's current status at the top of the AT&T Wi-Fi Manager screen.

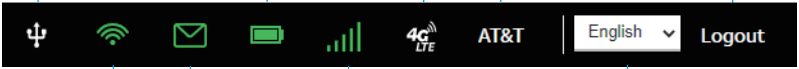
Battery level
Green: High
Yellow: Medium
Red: Low or no charge
Charging: Lightning bolt icon

Network status indicator
Technology Icon: 4G LTE
No Service: No Service
Blank: No SIM

USB connected

Service provider

Logout



Wi-Fi on

Signal strength

Language selector
English or Español

Messages
Green: Unread message(s)
Red: Inbox full
Blank: No unread messages

For more details on the AT&T Wi-Fi Manager, see *"Device settings" on page 25*.

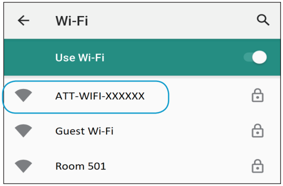
Internet access

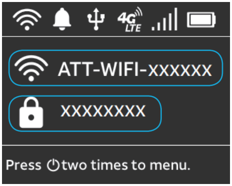
You are required to purchase a Wireless Internet Data plan.

Connect via Wi-Fi

You can simultaneously connect up to fifteen (15) devices, including smartphones, tablets, and laptops, to your mobile hotspot.

1. Open the Wi-Fi network manager on your Wi-Fi enabled device that you would like to connect to your mobile hotspot.
2. Find and select the Wi-Fi network name (SSID) (e.g., **ATT-WIFI-XXXXXX**) shown on your mobile hotspot's Wi-Fi Info details screen.
3. When prompted, enter the Wi-Fi default password shown on your mobile hotspot's Wi-Fi Info details screen.





Press ⏻ two times to menu.

4. Open a web browser and visit your favorite website to confirm your connection.

Changing Wi-Fi network name and password

You can customize your mobile hotspot's Wi-Fi network name (SSID) and password using the AT&T Wi-Fi Manager.

1. On any device that is connected to the mobile hotspot, enter **http://attwifimanager** or **http://192.168.1.1** directly into your browser address field.
2. Enter the login password found on the device label located underneath the battery of your mobile hotspot.
3. Click **LOG IN** button.
4. Go to **Wi-Fi** > **2.4 GHz Wi-Fi** > **EDIT** to change your network name and password.
5. Click **SAVE & APPLY**.

Note: You will need to reconnect any connected Wi-Fi enabled devices to the hotspot after updating any credentials.

Your mobile hotspot does not simultaneously broadcast 2.4 GHz and 5 GHz Wi-Fi networks. The default Wi-Fi network is 2.4 GHz.

To change 5GHz Wi-Fi network name and password, follow the below steps:

1. Go to **Wi-Fi** > **5 GHz Wi-Fi** > **Enable** to enable the 5GHz Wi-Fi network.
2. Click **EDIT** to change your network name and password.
3. Click **SAVE & APPLY**.

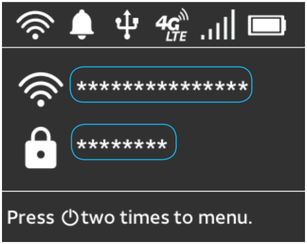
Note: Wi-Fi devices connected to 2.4 GHz Wi-Fi network will be disconnected when you switch from the 2.4 GHz Wi-Fi to the 5 GHz Wi-Fi network.

Hide Wi-Fi network name and password

Your Wi-Fi network and password are set as visible by default on your mobile hotspot's Wi-Fi Info details screen. You can hide them using the AT&T Wi-Fi Manager.

1. Log into the AT&T Wi-Fi Manager.
2. Select **Wi-Fi** > **2.4 GHz Wi-Fi** or **5 GHz Wi-Fi**.
3. Click **EDIT** button.
4. Uncheck the checkbox beside **Show network name and password on device**.
5. Click **SAVE & APPLY**.

Your mobile hotspot's Wi-Fi network and password will then be hidden on the Wi-Fi Info details screen.



****

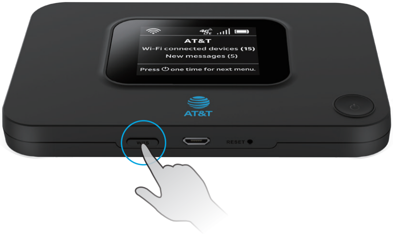
****

Press ⏻two times to menu.

Connect via WPS

Wi-Fi Protected Setup (WPS) allows WPS-enabled devices to be connected to a Wi-Fi network without having to type a Wi-Fi password.

1. With your mobile hotspot powered on, press and hold the **WPS** button for one (1) second.



2. Within two (2) minutes, press the **WPS** button on the wireless device you want to connect with.
3. Your mobile hotspot will display “**WPS success**‟ when the connection has been successfully established.

Connect via USB Tethering

You can also connect your Wi-Fi enabled device to the mobile hotspot using a micro USB cable (sold separately) instead of using the Wi-Fi network.

1. Make sure your mobile hotspot is on and has an active data connection.
2. Connect one end of the micro USB cable to the hotspot and the other end to your device.
3. Your device will detect a network connection via USB automatically.
4. Check your connection by visiting a website.

Device settings

The topics in this section will cover your mobile hotspot settings and options using the AT&T Wi-Fi Manager.

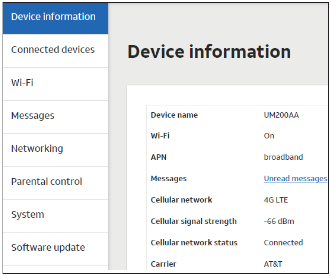
To access the AT&T Wi-Fi Manager, first connect your device to your mobile hotspot and enter **http://attwifimanager** or **http://192.168.1.1** directly into your browser address field. Log in using the default login password printed on the device label located underneath the battery of your mobile hotspot.

Note: You can customize the login that is used to access the AT&T Wi-Fi Manager by going to **System** > **Administration**. See *"Administration" on page 45*.

Navigating the user interface

A navigation panel to the left side of the screen lists out all the main menus on the AT&T Wi-Fi Manager.

Click on the menu items to display related information and settings on the right side of the screen.

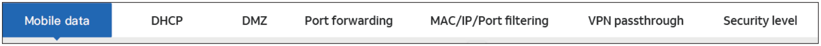


Device information

Device name	UM200AA
Wi-Fi	On
APN	broadband
Messages	Unread messages
Cellular network	4G LTE
Cellular signal strength	-66 dBm
Cellular network status	Connected
Carrier	AT&T

Sub-menu

The Networking and System sections have additional sub-menu displayed horizontally at the top of the screen, for example:

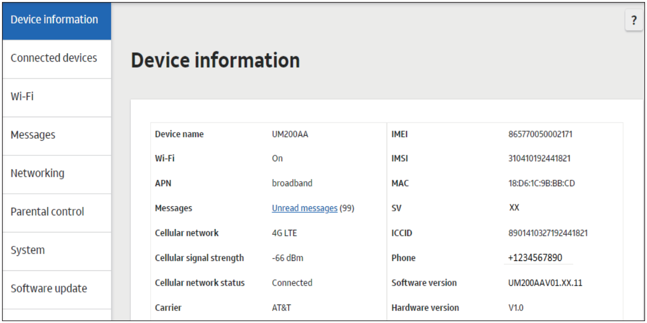


Help

Click the Help icon ? on top of any page to access the information on the settings displayed on that page.

Device information

The Device information page displays an overview of your mobile hotspot's status such as whether there are unread messages, firmware version, network connection status, network type, signal strength, etc.

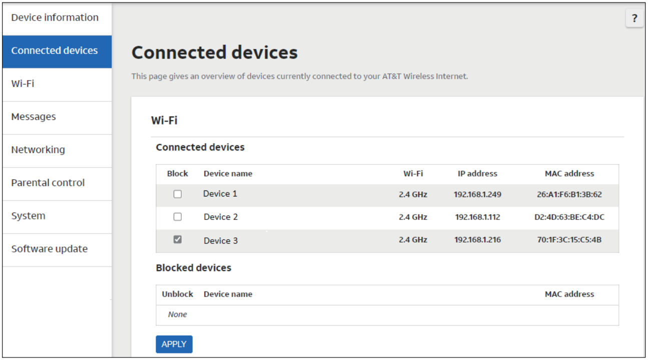


Device information

Device name	UM200AA	IMEI	865770050002171
Wi-Fi	On	IMSI	310410192441821
APN	broadband	MAC	18:D6:1C:9B:BB:CD
Messages	Unread messages (99)	SV	XX
Cellular network	4G LTE	ICCID	8901410327192441821
Cellular signal strength	-66 dBm	Phone	+1234567890
Cellular network status	Connected	Software version	UM200AAV01.XX.11
Carrier	AT&T	Hardware version	V1.0

Connected devices

The Connected devices page displays a list of Wi-Fi devices that are currently connected to your mobile hotspot. You can monitor who has access to your network and block (or unblock) devices as required.



Connected devices

This page gives an overview of devices currently connected to your AT&T Wireless Internet.

Wi-Fi

Connected devices

Block	Device name	Wi-Fi	IP address	MAC address
□	Device 1	2.4 GHz	192.168.1.249	26:A1:F6:B1:3B:62
□	Device 2	2.4 GHz	192.168.1.112	D2:4D:63:BE:C4:DC
☑	Device 3	2.4 GHz	192.168.1.216	70:1F:3C:15:C5:4B

Blocked devices

Unblock	Device name	MAC address
None		

To block a device, follow the below steps:

1. Select a device from your Connected devices list.
2. Click the **APPLY** button.
3. Follow the prompts to complete the process.

To unblock a device, follow the below steps:

1. Select a device from your Blocked devices list.
2. Click the **APPLY** button.
3. Follow the prompts to complete the process.

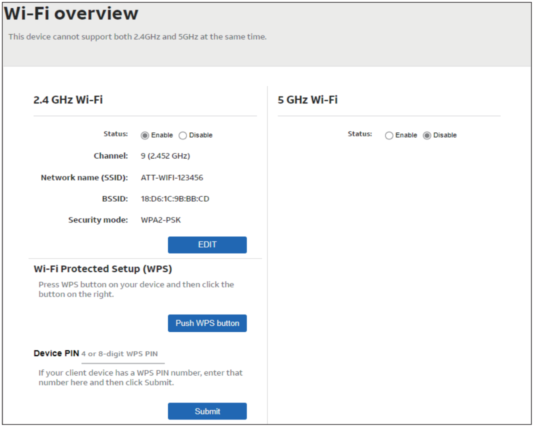
Wi-Fi

Wi-Fi page displays a summary of the current configuration of the 2.4 GHz and 5 GHz Wi-Fi settings of your mobile hotspot.

Your mobile hotspot does not simultaneously broadcast 2.4 GHz and 5 GHz Wi-Fi networks. The default Wi-Fi network is 2.4 GHz. To switch to the 5 GHz Wi-Fi network, select **Enable** at 5 GHz Wi-Fi section. When 5 GHz Wi-Fi network is enabled, 2.4 GHz Wi-Fi network will be disabled automatically. Devices currently connected to 2.4 GHz Wi-Fi network will be disconnected.

Note: If you disabled both 2.4 GHz and 5 GHz Wi-Fi networks and want to enable one of them, you will need to access the AT&T Wi-Fi Manager using a micro USB cable (see *"Access the AT&T Wi-Fi Manager via a micro USB cable (sold separately)" on page 18*) to enable it.

Wi-Fi overview



Wi-Fi overview

This device cannot support both 2.4GHz and 5GHz at the same time.

2.4 GHz Wi-Fi

Status: ● Enable ○ Disable

Channel: 9 (2.452 GHz)

Network name (SSID): ATT-WIFI-123456

BSSID: 18:D6:1C:9B:BB:CD

Security mode: WPA2-PSK

Wi-Fi Protected Setup (WPS)

Press WPS button on your device and then click the button on the right.

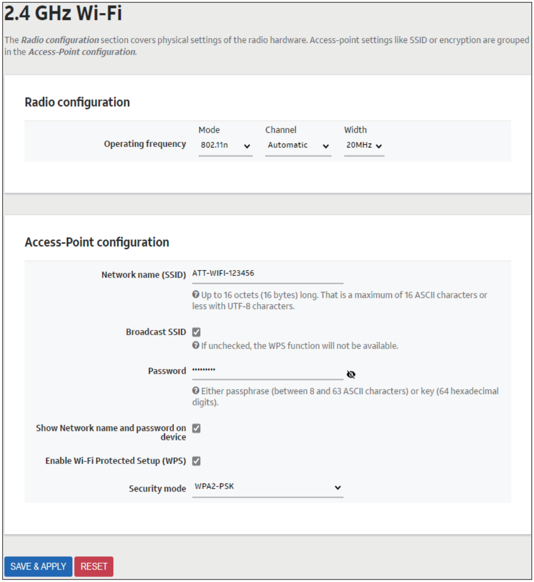
Device PIN 4 or 8-digit WPS PIN

If your client device has a WPS PIN number, enter that number here and then click Submit.

5 GHz Wi-Fi

Status: ○ Enable ● Disable

To make changes to the current configuration, click the **EDIT** button.



2.4 GHz Wi-Fi

The *Radio configuration* section covers physical settings of the radio hardware. Access-point settings like SSID or encryption are grouped in the *Access-Point configuration*.

Radio configuration

	Mode	Channel	Width
Operating frequency	802.11n	Automatic	20MHz

Access-Point configuration

Network name (SSID): ATT-WIFI-123456
Up to 16 octets (16 bytes) long. That is a maximum of 16 ASCII characters or less with UTF-8 characters.

Broadcast SSID: ☑
If unchecked, the WPS function will not be available.

Password: ••••••••
Either passphrase (between 8 and 63 ASCII characters) or key (64 hexadecimal digits).

Show Network name and password on device: ☑

Enable Wi-Fi Protected Setup (WPS): ☑

Security mode: WPA2-PSK

Operating frequency

- **Mode**: Display which mode is active for connecting via Wi-Fi. It allows the device to accept connections from devices supporting 802.11b/g/n (on 2.4 GHz) or 802.11a/n/ac (on 5 GHz).

- **Channel**: Display the wireless channel that the radio is operating on. In most situations, leaving this as Automatic will work best, but you can manually change the channel selection using this option.
- **Width**: When 802.11n is selected in mode, width option is displayed. You can select 20MHz or 40MHz for this option. When 802.11ac is selected in mode, you can select 20MHz, 40MHz, or 80MHz for this option.

Network name (SSID)

The wireless name that is displayed to client devices when they scan for networks to join. You can enter your new network name in this field to change it. When finished, click the **SAVE & APPLY** button.

Broadcast SSID

When selected, your mobile hotspot name will be visible in the list of available Wi-Fi networks when client devices scan for networks to join. If unselected, your mobile hotspot name will be hidden and must be added manually on the client devices to join. This checkbox is marked by default.

Password

The Wi-Fi network password that must be entered on any client devices needing to connect to your mobile hotspot. You can enter your new password in this field to change it. When finished, click the **SAVE & APPLY** button.

Note: If you have changed the login and have forgotten the new one, you must restore the device to the factory default settings. Using a narrow object, such as a paperclip or ballpoint pen, press and hold the **Factory reset** button located at the bottom of your mobile hotspot for five (5) seconds. You may then log in using the default login password shown on your mobile hotspot's Wi-Fi Info details screen.

Show network name and password on device

When selected, the network name and password will be visible on your mobile hotspot’s LCD display screen. To hide the network name and password on your mobile hotspot’s LCD display screen, uncheck this checkbox. This checkbox is marked by default.

Enable Wi-Fi Protected Setup (WPS)

When selected, it allows WPS-enabled devices to be connected to your mobile hotspot without typing a Wi-Fi password. This feature is turned on by default. If unselected, currently connected devices may be disconnected.

Security mode

Select the desired Wi-Fi security option.

- **WPA3-Personal** is the latest and most secure mode.
- **WPA2-PSK/WPA3-Personal** allows client devices that support either WPA2-PSK or WPA3-Personal to connect.
- **WPA2-PSK** can be used for WPA2 devices and is set as the default security mode.
- **WPA-PSK/WPA2-PSK** allows older client devices that do not support WPA2-PSK to connect. This mode also supports WPA2-PSK.
- **Open** allows client devices to connect to your Wi-Fi network without entering a password. For your security, this option should be avoided.

WPS

WPS, or Wi-Fi Protected Setup, is a network security standard that allows for an easy connection to a secure wireless network. This feature is turned on by default. If you change these settings, currently connected devices may be disconnected.

There are two methods to connect a client device using WPS on the Wi-Fi overview page, see below:

- **WPS button**: This will act in the same way as manually pushing the WPS button on the bottom of your mobile hotspot. Click the **PRESS WPS BUTTON**, and within two (2) minutes, you will need to activate WPS on the device you wish to connect to your mobile hotspot via a physical or virtual button to complete the connection process.
- **Device PIN**: If the client device has a 4-digit or 8-digit PIN number, enter the PIN in the PIN field and click the **SUBMIT** button.

Notes:

- Refer to your connecting device's documentation for specific information on how to complete the WPS process on the desired device.
- If the Broadcast Network Name (SSID) option is unselected, the WPS function will not be available.

Maximum number of Wi-Fi devices

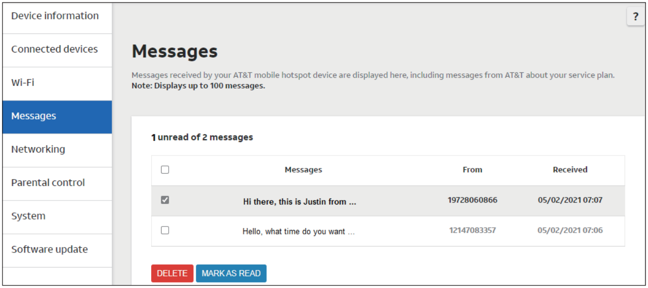
Specify the maximum number of client devices that can simultaneously connect to your mobile hotspot.

The default maximum number of devices is set to 15 devices.

Messages

The Messages page displays text messages received by your mobile hotspot. This may include messages from AT&T about your service plan.

Note: It displays up to 100 messages.



Messages

Messages received by your AT&T mobile hotspot device are displayed here, including messages from AT&T about your service plan.
Note: Displays up to 100 messages.

1 unread of 2 messages

□	Messages	From	Received
☑	**Hi there, this is Justin from ...**	**19728060866**	**05/02/2021 07:07**
□	Hello, what time do you want ...	12147083357	05/02/2021 07:06

When there are more than 100 messages, older messages will be automatically deleted to make room for the new messages.

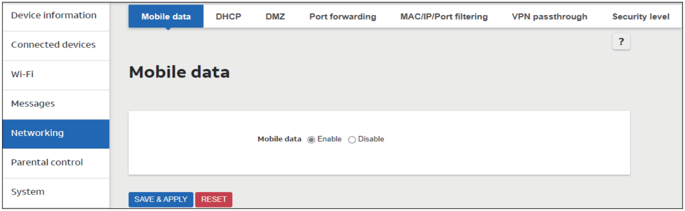
To manually delete messages, follow the below steps:

1. Select the message(s) you wish to delete from the message list.
2. Click the **DELETE** button.

Networking

Mobile data

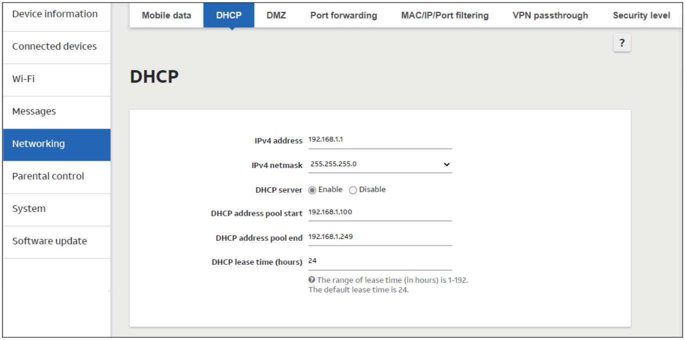
The Mobile data page lets you enable or disable the mobile data.



Mobile data ● Enable ○ Disable

DHCP

These settings affect the Local Area Network connection.



IPv4 address 192.168.1.1

IPv4 netmask 255.255.255.0

DHCP server ● Enable ○ Disable

DHCP address pool start 192.168.1.100

DHCP address pool end 192.168.1.249

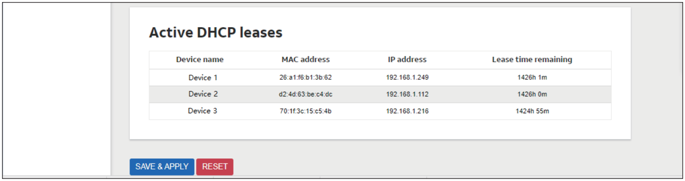
DHCP lease time (hours) 24

The range of lease time (in hours) is 1-192.
The default lease time is 24.

- **IPv4 address**: Display the IPv4 address of your mobile hotspot. By default, this is set to 192.168.1.1.
- **IPv4 netmask**: Display the IPv4 Netmask of your mobile hotspot. By default, this is set to 255.255.255.0.
- **DHCP server**: Select to enable or disable the DHCP server on your mobile hotspot. The DHCP server allows your mobile hotspot to automatically assign a local IP address from the DHCP pool to wireless client devices when they connect.
- **DHCP address pool start**: Display the first address in the DHCP pool which is assigned to client devices.
- **DHCP address pool end**: Display the last address in the DHCP pool which is assigned to client devices.
- **DHCP lease time (hours)**: Display the time length of the DHCP lease. This is the length of time that the IP address is reserved for a particular client device.

Active DHCP leases

Display the active DHCP leases and the length of time remaining.



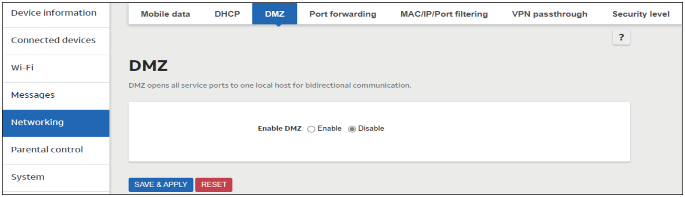
Active DHCP leases

Device name	MAC address	IP address	Lease time remaining
Device 1	26:a1:f6:b1:3b:62	192.168.1.249	1426h 1m
Device 2	d2:4d:63:be:c4:dc	192.168.1.112	1426h 0m
Device 3	70:1f:3c:15:c5:4b	192.168.1.216	1424h 55m

DMZ

The DMZ, or Demilitarized Zone, opens up all ports to a specific local host. This means the specified host will not be protected by the built-in firewall. Therefore, this feature should be used with care.

DMZ is set to **Disable** by default.



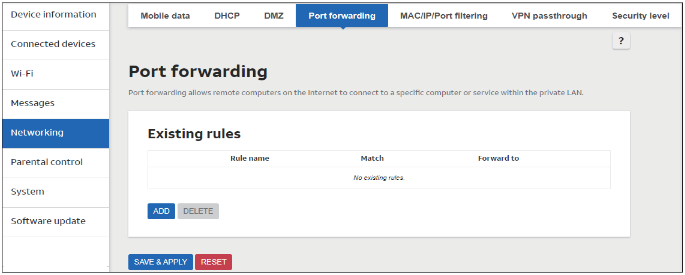
DMZ

DMZ opens all service ports to one local host for bidirectional communication.

Enable DMZ ○ Enable ● Disable

Port forwarding

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN. It operates based on rules specifying a protocol, the external ports, the internal IP address and internal ports.



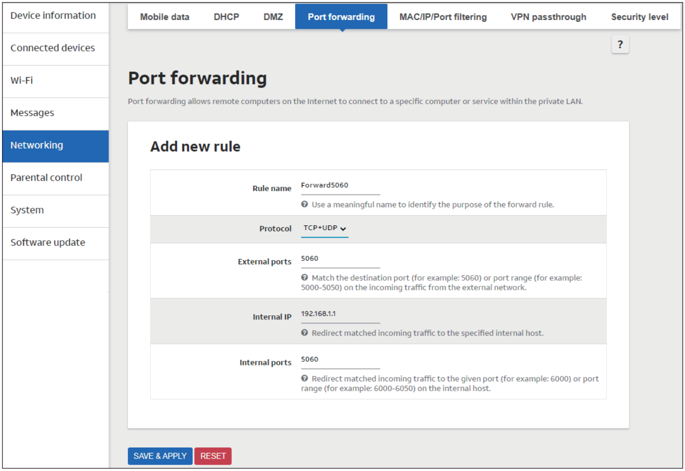
Port forwarding

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Existing rules

Rule name	Match	Forward to
No existing rules.		

To create a new rule, click the **ADD** button.



Port forwarding

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Add new rule

Rule name: Forward5060
Use a meaningful name to identify the purpose of the forward rule.

Protocol: TCP+UDP

External ports: 5060
Match the destination port (for example: 5060) or port range (for example: 5000-5050) on the incoming traffic from the external network.

Internal IP: 192.168.1.1
Redirect matched incoming traffic to the specified internal host.

Internal ports: 5060
Redirect matched incoming traffic to the given port (for example: 6000) or port range (for example: 6000-6050) on the internal host.

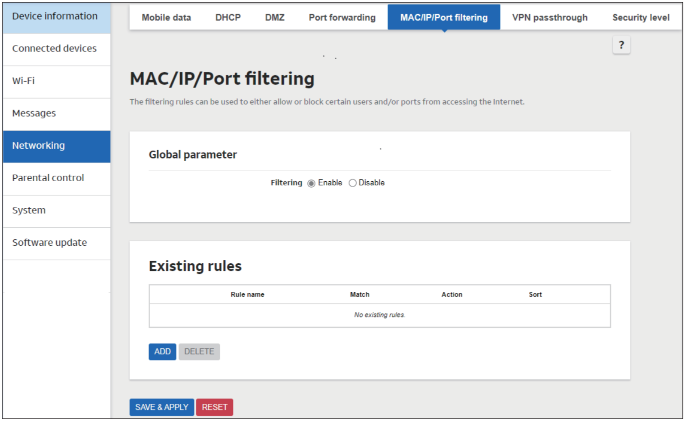
Enter the below required details:

- **Rule name**: Set a name of the new rule to be added.
- **Protocol**: Select TCP+UDP, TCP, or UDP traffic types to be directed.
- **External ports**: Enter the external port number.
- **Internal IP**: Enter the internal IP address that you would like traffic from a specific external port directly to internal port.
- **Internal ports**: Enter the internal port number.

When finished, click the **SAVE & APPLY** button.

MAC/IP/Port filtering

This feature can be used to allow or block certain users and/or ports from accessing the Internet.



MAC/IP/Port filtering

The filtering rules can be used to either allow or block certain users and/or ports from accessing the Internet.

Global parameter

Filtering ● Enable ○ Disable

Existing rules

Rule name	Match	Action	Sort
No existing rules.			

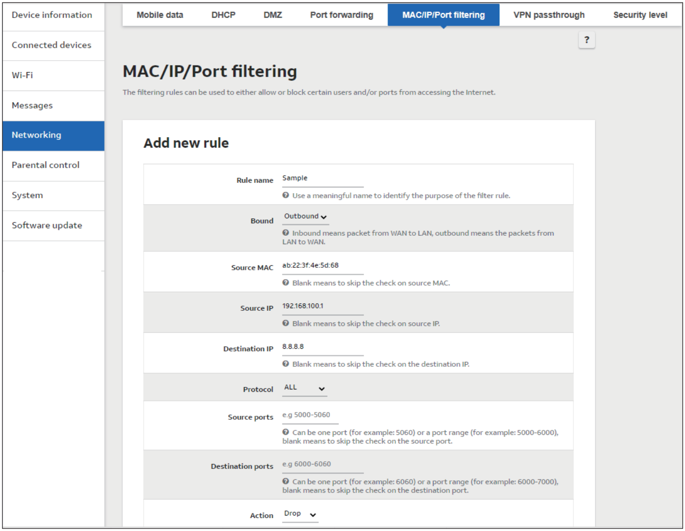
Global parameter

You can quickly turn the filtering on or off for all rules by selecting **Enable** or **Disable** here.

Existing rules

You can view existing rules here.

To add a new rule, click the **ADD** button.



MAC/IP/Port filtering

The filtering rules can be used to either allow or block certain users and/or ports from accessing the Internet.

Add new rule

Rule name	Sample Use a meaningful name to identify the purpose of the filter rule.
Bound	Outbound Inbound means packet from WAN to LAN, outbound means the packets from LAN to WAN.
Source MAC	ab:22:3f:4e:5d:68 Blank means to skip the check on source MAC.
Source IP	192.168.100.1 Blank means to skip the check on source IP.
Destination IP	8.8.8.8 Blank means to skip the check on the destination IP.
Protocol	ALL
Source ports	e.g 5000-5060 Can be one port (for example: 5060) or a port range (for example: 5000-6000), blank means to skip the check on the source port.
Destination ports	e.g 6000-6060 Can be one port (for example: 6060) or a port range (for example: 6000-7000), blank means to skip the check on the destination port.
Action	Drop

Enter the below required details:

- **Rule name**: Set a name of the new rule to be added.
- **Bound**: Select **Outbound** or **Inbound** to set packet from LAN to WAN, or WAN to LAN.
- **Source MAC**: Enter the source MAC address.
- **Source IP**: Enter the IP address that the traffic will be filtered from.
- **Destination IP**: Enter the IP address to which traffic will be filtered.

- **Protocol**: Select **ALL**, **TCP+UDP**, **TCP**, **UDP**, or **ICMP** as the traffic types to be filtered.
- **Source ports**: Enter the ports number that traffic will be filtered from.
- **Destination ports**: Enter the ports number to which traffic will be filtered.
- **Action**: Select **Drop**, **Accept**, or **Reject** to deny or allow the access to the Internet.

When finished, click the **SAVE & APPLY** button.

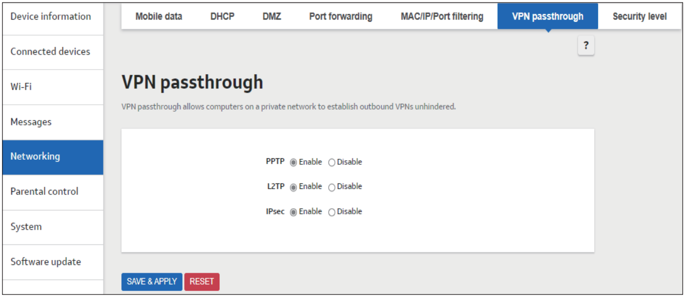
Existing rules can be further edited by clicking the **EDIT** button to the end of each rule entry.

You can also set the priority for the existing rules by clicking **Up** ⌃ and **Down** ⌄ icons.

VPN passthrough

This feature allows VPN client software on connected devices to connect through this device to remote VPN servers. You can specify the VPNs allowed by protocol.

Under normal operation, these should be left as **Enabled**.



VPN passthrough

VPN passthrough allows computers on a private network to establish outbound VPNs unhindered.

PPTP ● Enable ○ Disable

L2TP ● Enable ○ Disable

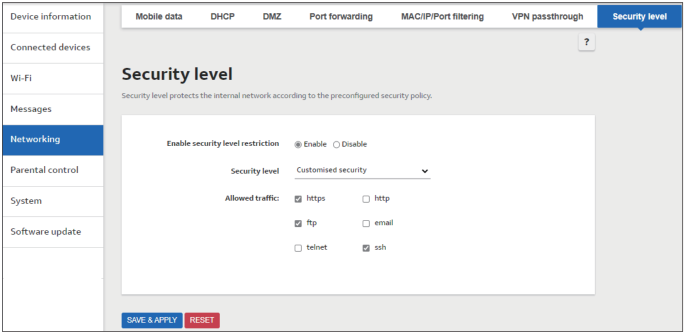
IPsec ● Enable ○ Disable

Security level

This feature protects the internal network according to the preconfigured security policy. The default setting is disabled.

When you select **Enable**, there are **Low**, **Medium** and **High** security levels for your selection.

You can select **Customized security** to set your own options. Mark the checkboxes to allow traffic on the local network via the specified protocols.



Security level

Security level protects the internal network according to the preconfigured security policy.

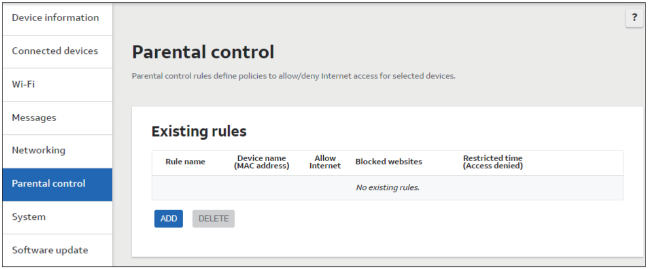
Enable security level restriction ● Enable ○ Disable

Security level: Customised security

Allowed traffic: ☑ https □ http ☑ ftp □ email □ telnet ☑ ssh

Parental control

The Parental control page is used to keep a list of rules to control access to specific websites. Rules can be applied to specific devices on your local area network and at specific times.



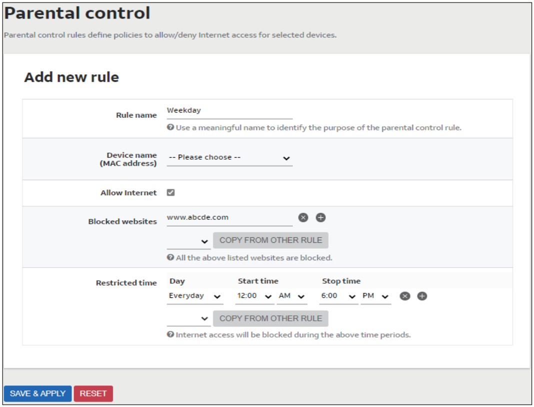
Parental control

Parental control rules define policies to allow/deny Internet access for selected devices.

Existing rules

Rule name	Device name (MAC address)	Allow Internet	Blocked websites	Restricted time (Access denied)
			No existing rules.	

To create a rule, click the **ADD** button.



Parental control

Parental control rules define policies to allow/deny Internet access for selected devices.

Add new rule

Rule name: Weekday

Use a meaningful name to identify the purpose of the parental control rule.

Device name (MAC address): -- Please choose --

Allow Internet: ☑

Blocked websites: www.abcde.com

All the above listed websites are blocked.

Restricted time:

Day	Start time	Stop time
Everyday	12:00 AM	6:00 PM

Internet access will be blocked during the above time periods.

Fill the below required details:

- **Rule name**: Enter a name for this rule so that it is easily identifiable.
- **Device name**: Select the local device on your network to create a rule for.
- **Allow Internet**: Select to allow or deny Internet access to this device.
- **Blocked websites**: Enter the domain name of the site you want to block. You can add as many websites as you want to block by clicking the icon ⊕.
- **Restricted time**: Select a day of the week, then enter a Start time and Stop time.

If there are existing rules available, you can directly copy information on **Blocked website** and **Restricted time** fields by selecting the existing rule name using the droplist icon ∨ and clicking the **COPY FROM OTHER RULE** button.

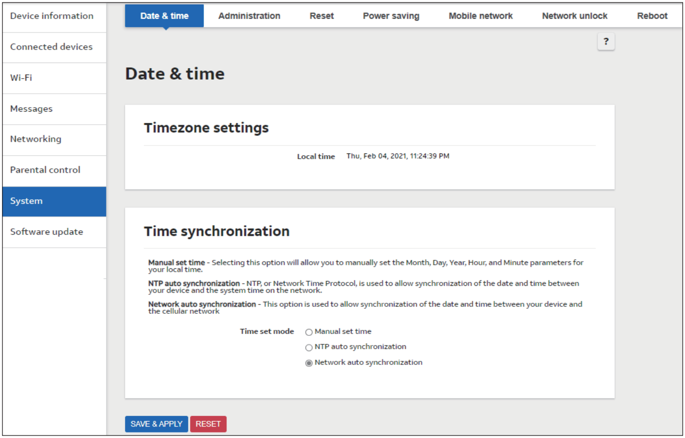
Click the **SAVE & APPLY** button.

Existing rules can be further edited by clicking the **EDIT** button at the end of each rule entry.

System

Date & time

The Date & time page lets you set the time, time zone, and the Network Time Protocol (NTP) server to use for synchronization. The time on your mobile hotspot is important for accurate logging of messages and parental control.



Date & time

Timezone settings

Local time Thu, Feb 04, 2021, 11:24:39 PM

Time synchronization

Manual set time - Selecting this option will allow you to manually set the Month, Day, Year, Hour, and Minute parameters for your local time.

NTP auto synchronization - NTP, or Network Time Protocol, is used to allow synchronization of the date and time between your device and the system time on the network.

Network auto synchronization - This option is used to allow synchronization of the date and time between your device and the cellular network

Time set mode
○ Manual set time
○ NTP auto synchronization
● Network auto synchronization

Manual set time

To manually set the time, select **Manual set time**, then use the drop-down lists to select the date and time, and click the **SAVE & APPLY** button.

NTP auto synchronization

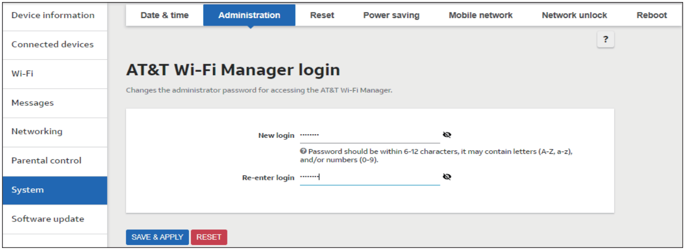
When selected, it enables the synchronization of the date and time between your device and the system time on the network. You will need to select the time zone that the device is located in by using the Timezone drop-down list.

Network auto synchronization

When selected, it enables the synchronization of the date and time between your device and the cellular network. This is the default setting.

Administration

The Administration page is used to configure the administrator password to access the AT&T Wi-Fi Manager.



AT&T Wi-Fi Manager login

Changes the administrator password for accessing the AT&T Wi-Fi Manager.

New login ········

Password should be within 6-12 characters, it may contain letters (A-Z, a-z), and/or numbers (0-9).

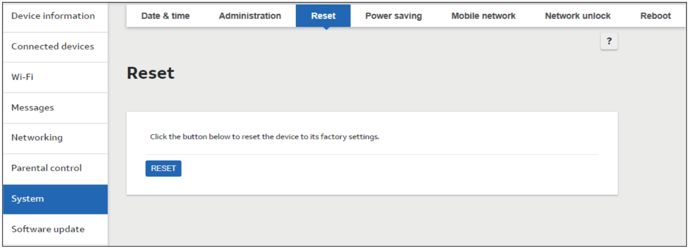
Re-enter login ·······

To change the password, follow the below steps:

1. Enter a new password in the **New login** field
2. Re-enter the new password in the **Re-enter login** field. The passwords entered must be identical, otherwise the password will not be updated.
3. When finished, click the **SAVE & APPLY** button.

Reset

The Reset page is used to reset your mobile hotspot to the factory default settings.

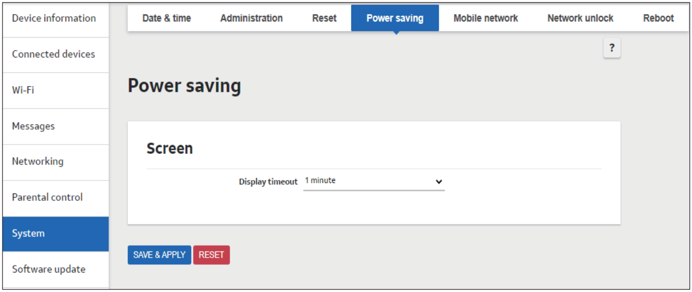


Click the button below to reset the device to its factory settings.

Note: Take care with using this feature as all settings and messages stored on the device will be lost when the device is factory reset.

Power saving

The Power Saving page lets you set the screen timeout.

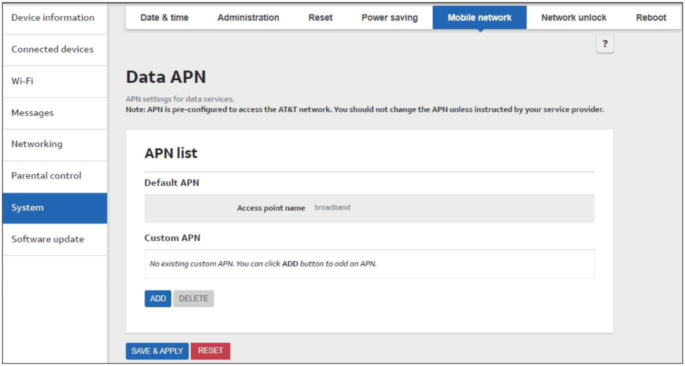


Display timeout 1 minute

Screen: Select the screen timeout. Your screen will be turned off automatically after the set amount of time. The default display timeout set is 1 minute. When finished, click the **SAVE & APPLY** button.

Mobile network

The Mobile network page allows you to set a custom APN for your network connection.



Data APN

APN settings for data services.

Note: APN is pre-configured to access the AT&T network. You should not change the APN unless instructed by your service provider.

APN list

Default APN

Access point name: broadband

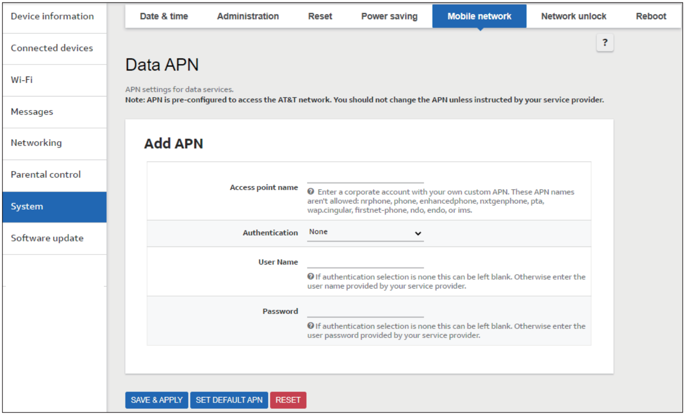
Custom APN

No existing custom APN. You can click ***ADD*** *button to add an APN.*

To use a custom APN, select the **ADD** and fill in the appropriate information before selecting **SAVE & APPLY**.The custom APN can be set to the default APN by selecting **SET DEFAULT APN**.

If you want to change back to the original default APN after a custom APN has been set, you can select it from the drop down box from the Access Point Name in the default APN list and confirm the action by clicking **SAVE & APPLY** button.

Note: Do not change the custom APN settings unless instructed by your service provider.



Data APN

APN settings for data services.

Note: APN is pre-configured to access the AT&T network. You should not change the APN unless instructed by your service provider.

Add APN

Access point name: ❗ Enter a corporate account with your own custom APN. These APN names aren't allowed: nrphone, phone, enhancedphone, nxtgenphone, pta, wap.cingular, firstnet-phone, ndo, endo, or ims.

Authentication: None

User Name: ❗ If authentication selection is none this can be left blank. Otherwise enter the user name provided by your service provider.

Password: ❗ If authentication selection is none this can be left blank. Otherwise enter the user password provided by your service provider.

Access point name

Enter a corporate account with your own custom APN.

Authentication

Select the authentication method specified by your service provider.

User name

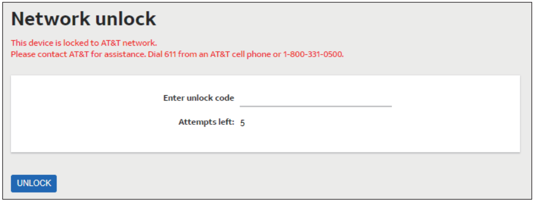
If the authentication selection is none, this can be left blank. Otherwise enter the user name provided by your service provider.

Password

If the authentication selection is none, this can be left blank. Otherwise enter the password provided by your service provider.

Network unlock

The Network unlock page is used to UNLOCK the network.



Network unlock

This device is locked to AT&T network.
Please contact AT&T for assistance. Dial 611 from an AT&T cell phone or 1-800-331-0500.

Enter unlock code

Attempts left: 5

If the device is locked to AT&T network, follow the below steps to unlock:

1. Contact AT&T Customer Care to get an unlock code by the following three ways:
   - Dial 611 from an AT&T cell phone.
   - Dial 1-800-331-0500 from any phone.
   - Submit a request to unlock the device by going to **att.com/deviceunlock**.
2. Enter the unlock code on Network unlock page.
3. Click the **UNLOCK** button.

Reboot

This Reboot page is used to perform a soft reboot of the mobile hotspot.

Click the **PERFORM REBOOT** button to restart and all previous settings and messages will be retained.

Software update

Software updates are delivered automatically over the mobile network. This page allows you to monitor these updates.

Current Software Version

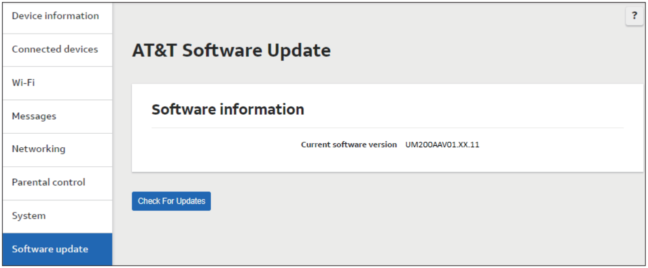
Displays the current software version installed on device.

Check For Updates

Click to check for the latest software update.

Continue Update

Click to resume software update.



Current software version UM200AAV01.XX.11

Troubleshooting

Check below for solutions to common problems you may experience.

Problem	Possible solutions
The device cannot connect to the mobile hotspot	• Restart the mobile hotspot. • Restart the device you want to connect (laptop, smartphone, etc.). • Confirm the Wi-Fi network name (SSID) and password (KEY) and establish a new connection to the mobile hotspot.
The device is connected to the mobile hotspot but cannot access the internet	• Check the signal strength and network indicator on your device's home screen and confirm the hotspot has network coverage in the area. • Make sure your SIM card is active and properly installed. See *"Install the SIM card" on page 8*. • Check to see if Cellular Data is enabled in the AT&T Wi-Fi Manager. See *"Mobile data" on page 34*.
Download and/ or upload speeds are slow	• Check the signal strength on your device's display home screen. A low signal strength can indicate a weak connection to the network in your area. • Please make sure your device is in close range to the mobile hotspot to optimize the Wi-Fi connection.

Problem	Possible solutions
Forgot the password to the Wi-Fi network	The default password to your Wi-Fi network can be easily found on the mobile hotspot's Wi-Fi Info details screen, see *"Wi-Fi Info screen" on page 15*. If you need to change your Wi-Fi password, see *"Changing Wi-Fi network name and password" on page 22*. If you have changed the login and have forgotten the new one, you must restore the device to the factory default settings. Using a narrow object, such as a paperclip or ballpoint pen, press and hold the **Factory reset** button located at the bottom of your mobile hotspot for five (5) seconds. You may then log in using the default login password shown on your mobile hotspot's Wi-Fi Info details screen.

Problem	Possible solutions
Forgot the password to the AT&T Wi-Fi Manager	The default password to the AT&T Wi-Fi Manager can be easily found on the device label located underneath the battery of your mobile hotspot. If you need to change your AT&T Wi-Fi Manager password, see *"Administration" on page 45*. If you have changed the login and have forgotten the new one, you must restore the device to the factory default settings. Using a narrow object, such as a paperclip or ballpoint pen, press and hold the **Factory reset** button located at the bottom of your mobile hotspot for five (5) seconds. You may then log in using the default login password printed on the device label located underneath the battery of your mobile hotspot.

Specifications

The following tables list your mobile hotspot's specifications.

Specification	Description
Weight	Approx. 111g. (3.92 oz.)
Dimensions (L x W x H)	109mm x 73mm x 13.5mm
Display	1.77", 128 x 160
Processor	Single-core, Cortex-A7, 1.3 GHz, Qualcomm MDM9207
Memory	128MB RAM + 256MB ROM
Frequencies	LTE: B2/4/5/12/14/30/66
Battery	Removable Li-ion battery, 2500mAh
Charging time	Approx. 3.5 hours
Charging port	Micro USB
Operation system	Linux 3.18

Licenses

The Wi-Fi Logo is a certification mark of the Wi-Fi Alliance, and any use of such marks by its affiliates is under license.

Safety and use

The topics in this section will introduce how to use your mobile hotspot safely.

Please read before proceeding

THE BATTERY IS NOT FULLY CHARGED WHEN YOU TAKE IT OUT OF THE BOX. DO NOT REMOVE THE BATTERY PACK WHEN THE DEVICE IS CHARGING.

Important health information and safety precautions

When using this product, the safety precautions below must be taken to avoid possible legal liabilities and damages. Retain and follow all product safety and operating instructions. Observe all warnings in the operating instructions on the product.

To reduce the risk of bodily injury, electric shock, fire, and damage to the equipment, observe the following precautions.

Electrical safety

This product is intended for use when supplied with power from the designated battery or power supply unit. Other usages may be dangerous and will invalidate any approval given to this product.

Safety precautions for proper grounding installation

Warning: Connecting to an improperly grounded equipment can result in an electric shock to your device.

When connecting with a USB cable to desktop or notebook computers, be sure your computer is properly grounded (earthed) before connecting this product to the computer. The power supply cord of a desktop or notebook computer has an equipment grounding conductor and a grounding plug. The plug must be plugged into an appropriate outlet that is properly installed and grounded in accordance with all local codes and ordinances.

Safety precautions for power supply unit

Use the correct external power source

A product should be operated only from the type of power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your authorized service provider or local power company. For a product that operates from battery power or other sources, refer to the operating instructions that are included with the product.

This product should be operated only with the following designated power supply unit(s).

Travel charger: Input: 100-240V, 50/60Hz, 0.2A. Output: 5V, 1200mA.

Handle battery packs carefully

This product contains a Lithium-ion battery. There is a risk of fire and burns if the battery pack is handled improperly. Do not attempt to open or service the battery pack. Do not disassemble, crush, puncture, short circuit the external contacts or circuits, dispose of in fire or water, or expose a battery pack to temperatures higher than 113°F (45°C). The operating temperature for the device is 14°F (-10°C) to 113°F (45°C). The charging temperature for the device is 32° F (0°C) to 113°F (45°C).

Warning: Danger of explosion if the battery is incorrectly replaced.

To reduce the risk of fire or burns, do not disassemble, crush, puncture, short circuit the external contacts, expose to temperature above 113°F (45°C), or dispose of in fire or water. Replace only with specified batteries. Recycle or dispose of used batteries according to the local regulations or guide supplied with your product.

Take extra precautions

- Do not disassemble or open, crush, bend or deform, puncture, or shred.
- Do not short circuit a battery or allow metallic conductive objects to contact the battery terminals.
- Only use USB cables that bear the USB-IF logo or have completed the USB-IF compliance program.
- 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 other hazards.
- Battery usage by children should be supervised.
- 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 Requirement for Battery System Compliance to IEEE1725. The use of an unqualified battery or charger may present a risk of fire, explosion, leakage, or other hazards.

- 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 hazards.
- Promptly dispose of used batteries in accordance with local regulations.
- Avoid dropping the device or battery. If the device or 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 other hazards. If the battery leaks:
    - Do not allow the leaking fluid to come into contact with skin or clothing. If already in contact, flush the affected area immediately with clean water and seek medical advice.
    - Do not allow the leaking fluid to come into contact with eyes. If already in contact, DO NOT rub; rinse with clean water immediately and seek medical advice.
    - Take extra precautions to keep a leaking battery away from fire as there is a danger of ignition or explosion.

Safety precautions for direct sunlight

Keep this product away from excessive moisture and extreme temperatures. Do not leave the product or its battery inside a vehicle or in places where the temperature may exceed 113°F (45°C), such as on a car dashboard, window sill, or behind a glass that is exposed to direct sunlight or strong ultraviolet light for extended periods of time. This may damage the product, overheat the battery, or pose a risk to the vehicle.

Safety in aircraft

Due to possible interference caused by this product to an aircraft's navigation system and its communications network, using this device on board an airplane is against the law in most countries. If you want to use this device while on board an aircraft, remember to turn off the device.

Environment restrictions

Do not use this product in gas stations, fuel depots, chemical plants or where blasting operations are in progress, or in potentially explosive atmospheres such as fueling areas, fuel storehouses, below deck on boats, chemical plants, fuel or chemical transfer or storage facilities, and areas where the air contains chemicals or particles, such as grain, dust, or metal powders. Please be aware that sparks in such areas could cause an explosion or fire resulting in bodily injury or even death.

Explosive atmospheres

When in any area with a potentially explosive atmosphere or where flammable materials exist, the product should be turned off and the user should obey all signs and instructions. Sparks in such areas could cause an explosion or fire resulting in bodily injury or even death. Users are advised not to use the equipment at refueling points, such as service or gas stations, and are reminded of the need to observe restrictions on the use of radio equipment in fuel depots, chemical plants, or where blasting operations are in progress. Areas with a potentially explosive atmosphere are often, but not always, clearly marked. These include fueling areas, below deck on boats, fuel or chemical transfer or storage facilities, and areas where the air contains chemicals or particles, such as grain, dust, or metal powders.

Safety precautions for RF exposure

- Avoid using your device near metal structures (for example, the steel frame of a building).
- Avoid using your device near strong electromagnetic sources, such as microwave ovens, sound speakers, TV, and radio.
- Use only original manufacturer-approved accessories or accessories that do not contain any metal.
- Use of non-original manufacturer-approved accessories may violate your local RF exposure guidelines and should be avoided.

Interference with medical equipment functions

This product may cause medical equipment to malfunction. The use of this device is forbidden in most hospitals and medical clinics.

If you use any other personal medical device, consult the manufacturer of your device to determine if they are adequately shielded from external RF energy. Your healthcare provider may be able to assist you in obtaining this information.

Turn your device OFF while inside healthcare facilities when any regulations posted in these areas instruct you to do so. Hospitals or healthcare facilities may be using equipment that could be sensitive to external RF energy.

Non-ionizing radiation

Your device has an internal antenna. This product should be operated in its normal-use position to ensure the radioactive performance and safety of the interference. As with other mobile radio transmitting equipment, users are advised that for satisfactory operation of the equipment and for the safety of personnel, it is recommended that no part of the human body be allowed to come too close to the antenna during operation of the equipment.

Use only the supplied integral antenna. Use of unauthorized or modified antennas may impair call quality and damage the device, causing loss of performance and SAR levels exceeding the recommended limits as well as result in noncompliance with the local regular requirement in your country.

To assure optimal device performance and ensure human exposure to RF energy is within the guidelines set forth in the relevant standards, always use your device only in its normal-use position. Contact with the antenna area may impair call quality and cause your device to operate at a higher power level than needed.

Avoiding contact with the antenna area when the device is IN USE optimizes the antenna performance and the battery life.

Electrical safety

Accessories

- Use only approved accessories.
- Do not connect with incompatible products or accessories.
- Take care not to touch or allow metal objects, such as coins or key rings, to contact or short circuit the battery terminals.

Faulty and damaged products

- Do not attempt to disassemble the device or its accessories.
- Only qualified personnel may service or repair the device or its accessories.

General precautions

You alone are responsible for how you use your device and any consequences of its use. You must always switch off your device wherever the use of a device is prohibited. Use of your device is subject to safety measures designed to protect users and their environment.

Avoid applying excessive pressure to the device

Do not apply excessive pressure on the screen or the device to prevent damage. Cracked display screens due to improper handling are not covered by the warranty.

Device getting warm after prolonged use

When using your device for prolonged periods of time, the device may become warm. In most cases, this condition is normal and therefore should not be interpreted as a problem with the device.

Heed service markings

Except as explained elsewhere in the Operating or Service documentation, do not service any product yourself. Service needed on components inside the device should be done by an authorized service technician or provider.

Protect your device

- Always treat your device and its accessories with care and keep them in a clean and dust-free environment.
- Do not expose your device or its accessories to open flames or lit tobacco products.
- Do not expose your device or its accessories to liquid, moisture, or high humidity.
- Do not drop, throw or try to bend your device, or its accessories.
- Do not use harsh chemicals, cleaning solvents, or aerosols to clean the device or its accessories.
- Do not paint your device or its accessories.
- Do not attempt to disassemble your device or its accessories. Only authorized personnel must do so.
- Do not expose your device or its accessories to extreme temperatures, minimum 14°F (-10°C) and maximum 113°F (45°C).
- Please check local regulations for disposal of electronic products.
- Do not carry your device in your back pocket as it can break when you sit down.

Damage requiring service

Unplug the product from the electrical outlet and refer servicing to an authorized service technician or provide under the following conditions:

- Liquid has been spilled into or an object has fallen onto the product.
- The product has been exposed to rain or water.
- The product has been dropped or damaged.
- There are noticeable signs of overheating.

- The product does not operate normally when you follow the operating instructions.

Avoid hot areas

The product should be placed away from heat sources such as radiators, heat registers, stoves, or any device producing heat.

Avoid wet areas

Never use the product in a wet location.

Avoid using your device after a dramatic change in temperature

When you move your device between environments with very different temperature and/or humidity ranges, condensation may form on or within the device. To avoid damaging the device, allow sufficient time for the moisture to evaporate before using the device.

Notice: When taking the device from low temperature conditions into a warmer environment or from high-temperature conditions into a cooler environment, allow the device to acclimate to room temperature before turning on power.

Avoid pushing objects into the product

Never push objects of any kind into cabinet slots or other openings in the product. Slots and openings are provided for ventilation. These openings must not be blocked or covered.

Airbags

Do not place a device in the area over an airbag or in the airbag deployment area. Store the device safely before driving your vehicle.

Mounting accessories

Do not use the product on an unstable table, cart, stand, tripod, or bracket. Any mounting of the product should follow the manufacturer's instructions and should use a mounting accessory recommended by the manufacturer.

Avoid unstable mounting

Do not place the product with an unstable base.

Use product with approved equipment

This product should be used only with personal computers and options identified as suitable for use with your equipment.

Cleaning

Unplug the product from the wall outlet before cleaning.

Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning, but NEVER use water to clean the LCD screen.

Small children

Do not leave your device and its accessories within the reach of small children or allow them to play with it. They could hurt themselves, or others, or could accidentally damage the device.

Your device contains small parts with sharp edges that may cause an injury, or which could become detached and create a choking hazard.

Operating machinery

Full attention must be given to operating machinery in order to reduce the risk of an accident.

Regulatory agency identifications

FCC Regulations

This mobile hotspot complies with Part 15 of the FCC Rules.

Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

RF Exposure Information (SAR)

This mobile hotspot meets the government's requirements for exposure to radio waves. This device is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission of the U.S. Government. The exposure standard for wireless mobile hotspot employs a unit of measurement known as the Specific Absorption Rate, or SAR. The SAR limit set by the FCC is 1.6 W/kg. Tests for SAR are conducted using standard operating positions accepted by the FCC with the device transmitting at its highest certified power level in all tested frequency bands.

Although the SAR is determined at the highest certified power level, the actual SAR level of the device while operating can be well below the maximum value. This is because the device is designed to operate at multiple power levels so as to use only the power required to reach the network. In general, the closer you are to a wireless base station, the lower the power output.

The highest SAR value for the mobile hotspot as reported to the FCC when worn on the body, is 0.97 W/kg.

While there may be differences between the SAR levels of various devices and at various positions, they all meet the government requirement.

The FCC has granted an Equipment Authorization for this model hotspot with all reported SAR levels evaluated as in compliance with the FCC RF exposure guidelines. SAR information on this mobile hotspot is on file with the FCC and can be found under the Display Grant section of *www.fcc.gov/oet/ea/fccid* after searching on FCC ID: XD6UM200AA.

For body-worn operation, this device has been tested and meets the FCC RF exposure guidelines for use with an accessory that contains no metal and positions the handset a minimum of 1.5 cm from the body. Use of other accessories may not ensure compliance with FCC RF exposure guidelines. If you do not use a body-worn accessory and are not holding the device at the ear, position the handset a minimum of 1.5 cm from your body when the device is switched on.

Warranty

With this manufacturer's warranty (hereinafter: the "Warranty"), Emblem Solutions (hereinafter: the "Manufacturer") guarantees this product against any material, design and manufacturing defects. The duration of this Warranty is specified in article 1 below.

This Warranty does not affect your statutory rights, which cannot be excluded or limited, in particular in relation to the applicable legislation on defective products.

Warranty duration:

The product may consist of several parts, which may have separate warranty periods, to the extent permitted by local laws. The "Warranty Period" (as defined in the table below) takes effect on the date of purchase of the product (as indicated on the proof of purchase).

1. Warranty period (see table below)

Mobile hotspot	24 Months
Accessories (if included in the box)	12 Months

2. Warranty period for repaired or replaced parts:

Subject to special provisions of local laws in force, the repair or replacement of a product does not, under any circumstances whatsoever, extend the original warranty period of the product concerned. However, the repaired or replaced parts are guaranteed in the same manner and for the same defect for a period of ninety days after delivery of the repaired product, even if their initial warranty period has expired. Proof of purchase required.

Implementation of the Warranty

If your product is faulty under normal conditions of use and maintenance, in order to benefit from the present warranty, please contact the Returns Center at **1(800) 801-1101** for assistance. The customer support center will then provide you with instructions on how to return the product for support under warranty. For more information, please visit *att.com/warranty.*

Warranty exclusions

Manufacturer guarantees its products against material, design and manufacturing defects. The Warranty does not apply in the following cases:

1. Normal wear and tear of the product (including on camera lenses, batteries and screens) requiring periodic repair and replacement.
2. Defects and damages due to negligence, to the product being used other than in a normal and customary manner, to the non-compliance with the recommendations of this User Manual, to an accident, regardless of the cause. Instructions for use and maintenance of the product can be found in your product's User Manual.
3. The opening, unauthorized disassembly, modification being carried out or repair of the product by the end user or by persons or by service providers not approved by Manufacturer and/or with spare parts not approved by Manufacturer.
4. Use of the product with accessories, peripherals and other products whose type, condition and/or standards do not meet Manufacturer's standards.
5. Defects associated with the use or connection of the product to equipment or software not approved by Manufacturer. Some defects may be caused by viruses due to unauthorized access by yourself or by a third party service, computer systems, other accounts or networks. This unauthorized access may take place through hacking, misappropriation of passwords or various other means.

6. Defects and damage due to the exposure of the product to humidity, extreme temperatures, corrosion, oxidation, or to any spillage of food or liquids, chemicals and generally any substance likely to alter the product.

7. Any failure of embedded services and applications that have not been developed by Manufacturer and whose functioning is the exclusive responsibility of their designers.

8. Installation and use of the product in a manner that does not comply with the technical or security standards of regulations in force in the country where it's installed or used.

9. Modification, alteration, degradation or illegibility of the IMEI number, serial number or EAN of the product

10. Absence of proof of purchase.

Upon expiration of the warranty period or upon an exclusion of warranty, Manufacturer may, at its discretion, provide a quote for the repair and offer to provide support for the product, at your cost.

The Manufacturer contact and after-sales service details are subject to change. These Warranty terms may vary substantially according to your country of residence.

DOC20210105