

T Mobile®

Hotspot 5G



User Guide

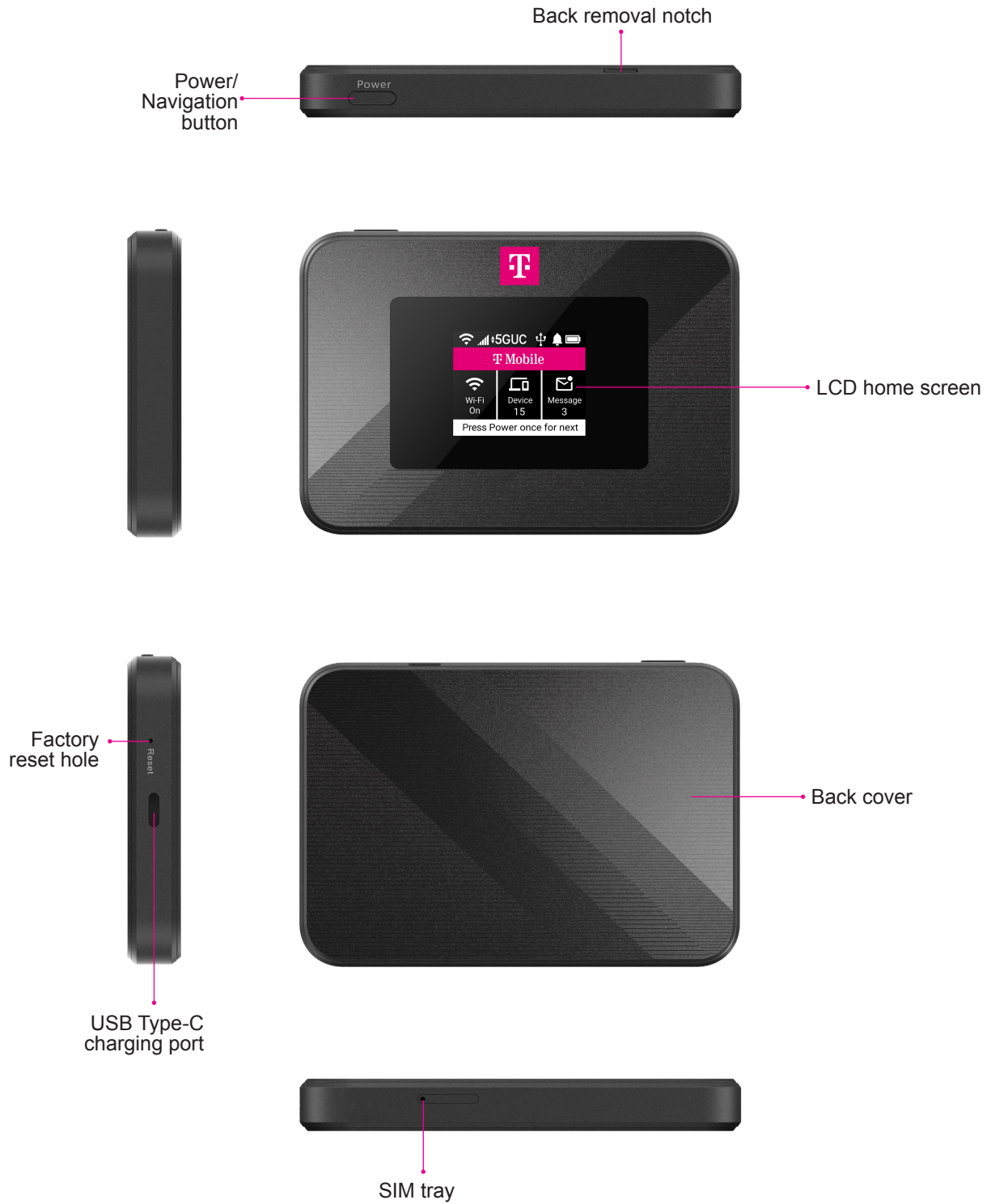
Contents

Getting started	3
Getting to know your device	3
Installation	5
Install the SIM card	5
Charge your hotspot	5
Turn on your hotspot	5
LCD display screen	6
Home screen	6
Wi-Fi Info screen	7
Data usage screen	8
USB Connection Options screen	8
Messages screen	9
Notifications screen	9
Device Info screen	10
Internet access	11
Connect via Wi-Fi	11
Change Wi-Fi network name and password	11
Hide Wi-Fi Network and Password	11
Connect via USB Tethering	11
WebUI	12
Login	12
Device information	13
Data usage	13
Data usage	13
Data statistics	14
Connected devices	14
Wi-Fi	15
Basic	15
Advanced	16
Messages	17
Networking	17
Cellular	17
DNS	18
LAN	18
Firewall	19
Port forwarding	20
MAC/IP/Port filtering	20
VPN	21
System	22
Date & time	22
Administration	22
Device	23
Backup	24
Reset	24
Network unlock	25
SIM	25
Software update	26
Help	26
Troubleshooting	27
Safety and use	28
Important health information and safety precautions	28
FCC Regulations	32
RF Exposure Information (SAR)	32

Getting started

The topics in this section will introduce you to your device, help you get set up with service, provide an overview of the device operations.

Getting to know your device



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

Part	Description
Power/ Navigation key	<ul style="list-style-type: none"> • Press and hold for three (3) seconds to turn your hotspot on or off • Press once to wake display • 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 hotspot
USB Type-C charging port	Connect the included charger for charging or connect to a device for tethering (sold separately)
Factory reset hole	Using the included SIM pin to press and hold the Factory reset hole for five (5) seconds to perform a factory reset
Back removal notch	Use the back removal notch to remove the back cover

CAUTION! Inserting an accessory into the incorrect port may damage the device.

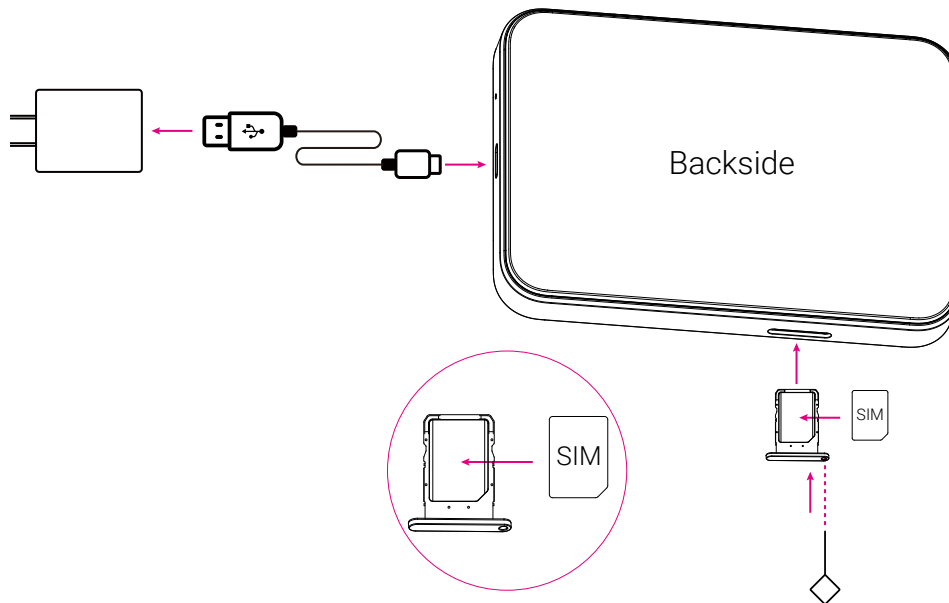
Installation

Install the SIM card

1. From the backside of the device, insert the included SIM pin to eject the SIM tray.
2. Place the Nano SIM card and with the gold contacts facing downward and the cut corner on the bottom right.
3. Gently slide the SIM tray back into the slot.

Charge your hotspot

1. Connect the USB Type-A end to the included charger, then plug the USB Type-C end into your device's charging port located at the side of your hotspot.
2. Connect the other end of the included charger to an electrical outlet to fully charge your hotspot.



Note: Your device only supports Nano SIM cards. It's recommended that you use the SIM card that is provided to you by T-Mobile.

Turn on your hotspot

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

Check the wireless signal

When you turn on your hotspot device (with SIM card inserted), it will automatically connect to the cellular network. You might need to 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



Note: The display will timeout after 30 seconds of inactivity to save power. Press the **Power/Navigation** button one time to wake the screen. This default setting can be adjusted on the WebUI (<http://mifimanager> or <http://192.168.0.1>) under **System > Device > Turn off screen**.

Indicator	Name	Description
	Wi-Fi indicator	Wi-Fi on
	Signal strength indicator	Indicates the signal strength. More signal bars indicates higher signal strength.
	Network indicator	Network information
	USB tethering	USB connected for tethering
	Notifications indicator	New notifications received
	Battery indicator	Show battery status: <ul style="list-style-type: none">• White (> 50%): High• Yellow (20% - 50%): Medium• Red (< 20%): Low or no charge• Charging: Lightning bolt icon

Indicator	Name	Description
	Wi-Fi On/Off status	The On/Off status of the Wi-Fi
	Wi-Fi connected devices	The number inside the parenthesis indicates the number of Wi-Fi connected devices.
	New messages	The number inside the parenthesis indicates the number of new messages.
Press Power once for next		Press the Power/Navigation button one time to scroll through the main screens

Other main screens

From the Home screen, 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.

Wi-Fi Info screen

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

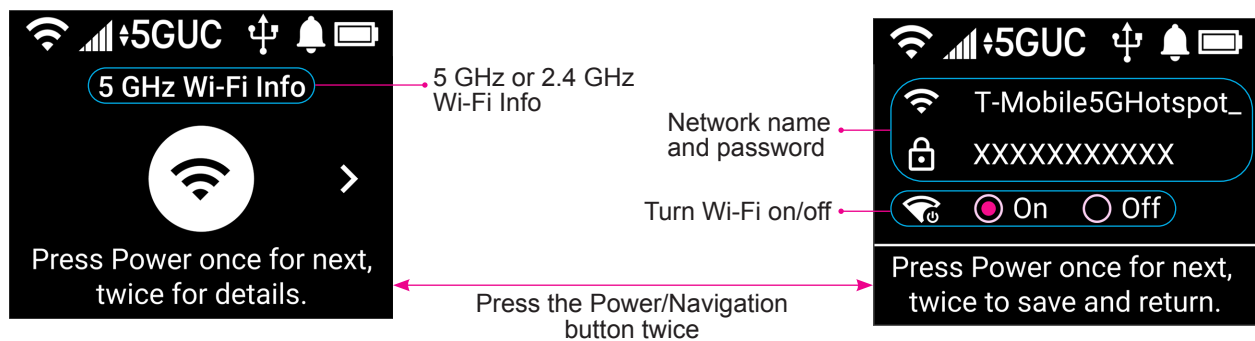
From the Wi-Fi Info screen, press the **Power/Navigation** button two times to access the Wi-Fi Info details screen to view your Wi-Fi network name and password.

You can change the default Wi-Fi network name and password via the WebUI.

Turn Wi-Fi On or Off

You can also enable or disable Wi-Fi on this screen.

1. Press the Power button once to toggle between On and Off.
2. When selected, press the Power button twice to save your choice and return to the main Wi-Fi menu.



Your hotspot does not simultaneously broadcast 5 GHz and 2.4 GHz Wi-Fi networks. The default Wi-Fi network is 5 GHz, but you can go to the WebUI to switch to the 2.4 GHz network.

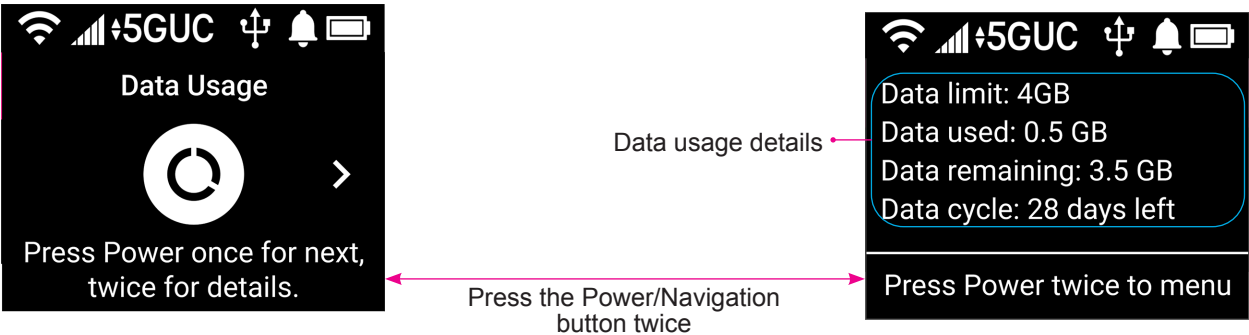
Note: The Wi-Fi name and password are visible by default, and you can hide it via the WebUI.

Data usage screen

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

From the Data Usage screen, press the **Power/Navigation** button two times to access the Data Usage details screen to view the data limit you've set, current data used, etc.

You can change the data limit and data cycle via the WebUI.



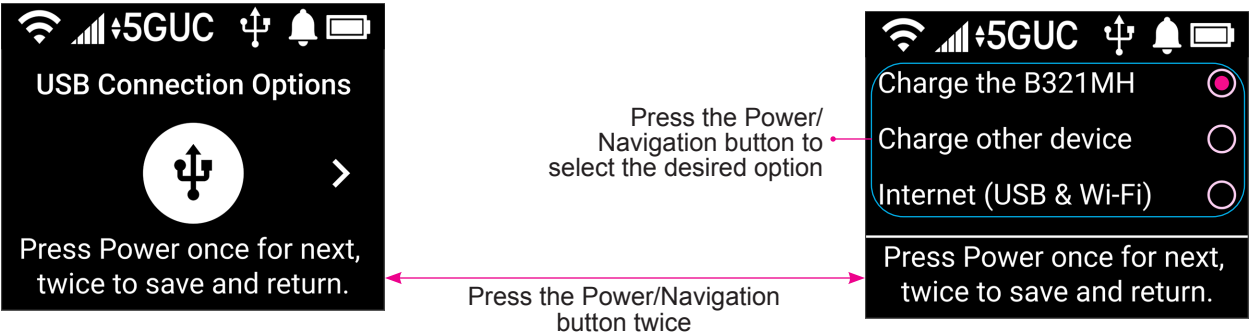
USB Connection Options screen

Note: The USB Connection Options screen will only be displayed when your hotspot is connected to another device.

From the Data Usage screen, press the **Power/Navigation** button one time to access the USB connection options screen.

From the USB connection options screen, press the **Power/Navigation** button two times to access the USB connection options details screen to select the desired option.

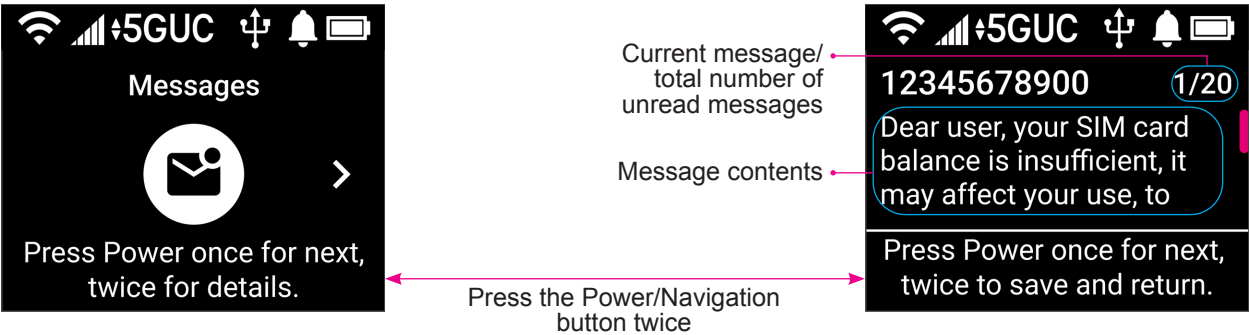
- **Charge the B321MH:** Charge your hotspot.
- **Charge other device:** Use your hotspot to charge other devices, such as a cell phone or tablet. Note: Do not select the Charge other device option if you want to use the battery for a relatively long time.
- **Internet (USB & Wi-Fi):** Access the internet with both USB tethering and Wi-Fi enabled.
- **Internet (USB only):** Access the internet with USB tethering activated.



Messages screen

From the Data Usage or USB Connection Options 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.



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 WebUI.

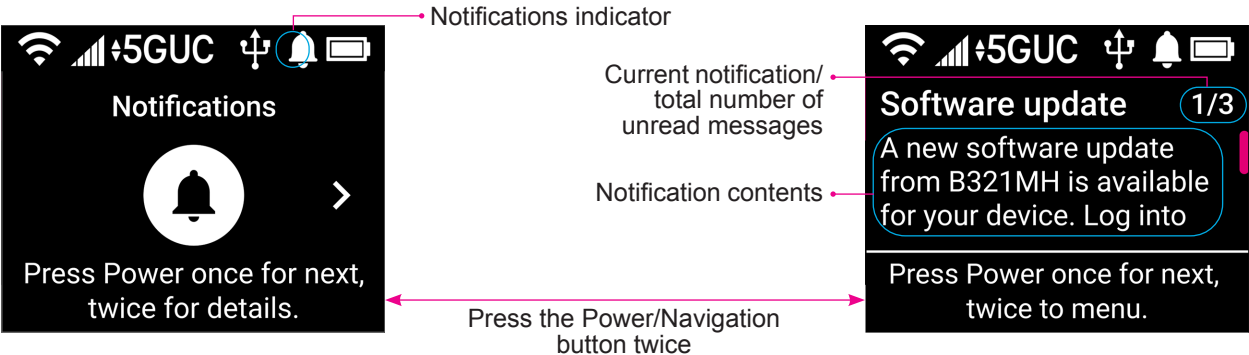
Notifications screen

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.



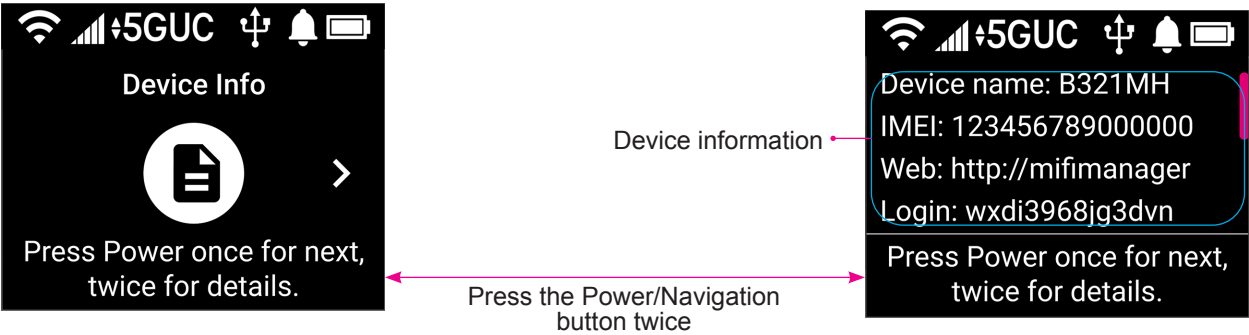
If a notification is too long to display in one screen, press the **Power/Navigation** button one time to view the next screen of the current notification.

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.



Internet access

Connect via Wi-Fi

You can simultaneously connect up to fifteen (15) devices, including smartphones, tablets, and laptops, to your hotspot. Keep your hotspot in range of the device you want to connect with and follow the below steps:

1. Open the Wi-Fi network manager on your Wi-Fi enabled device that you would like to connect to your hotspot.
2. Find and select your hotspot's Wi-Fi network name (**T-Mobile5GHotspot_XXXX**) shown on your hotspot's Wi-Fi Info details screen.
3. Enter the Wi-Fi password shown on your hotspot's Wi-Fi Info details screen.
4. Open a web browser and visit your favorite website to confirm your connection.

Change Wi-Fi network name and password

You can customize your hotspot's Wi-Fi network name and password using the WebUI.

1. On any device that is connected to the hotspot, enter **http://mifimanager** or **http://192.168.0.1** directly into your browser address field.
2. Enter the login password which can be found on the Device Info screen of your device and on the label located under the battery of your hotspot.
3. Click **Log in** button.
4. Go to **Wi-Fi > Advanced**.
5. To rename the Wi-Fi network name, delete the default network name listed in the Network name (SSID) and replace with your custom name.
6. To change the Wi-Fi network password, delete the default network password listed in the Password field and replace.
7. Click **Save**.
8. The hotspot will refresh with the updated Wi-Fi credentials.

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

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

To change 2.4 GHz Wi-Fi network name and password, follow the below steps:

1. Go to **Wi-Fi > Basic > AP Band > 2.4 GHz Band** to enable the 2.4 GHz Wi-Fi network.
2. Click **Advanced** tab to change your network name and password.
3. Click **Save**.

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

Hide Wi-Fi Network and Password

Your Wi-Fi network and password are set as visible by default on your hotspot's Wi-Fi Info details screen. You can hide them using the WebUI.

1. Log in to the WebUI.
2. Select **Wi-Fi > Advanced**.
3. Check the checkbox of **Hide network name on device** and **Hide password on device**.
4. Click **Save**.

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

Connect via USB Tethering

You can also connect your computer to the hotspot using a USB cable to make a connection.

1. Connect one end of the USB cable to your hotspot and the other end to the computer.
2. Select **Internet (USB & Wi-Fi)** or **Internet (USB only)** on the **USB connection options** screen on your device.

Login

You can access the WebUI to manage your hotspot's settings, features, and controls.

- 1.Open a web browser on a computer or Wi-Fi enabled device that is connected to the hotspot's Wi-Fi network.
- 2.Enter **http://mifimanager** or **http://192.168.0.1** in the address bar of the browser.
- 3.Enter the default login password, which can be found on the Device Info screen of your device and on the label located under the battery of your hotspot.
- 4.Click **Log In**.
- 5.You will need to change your password upon your initial login to the WebUI. You can change the password to something easy to remember.

Forgot login password

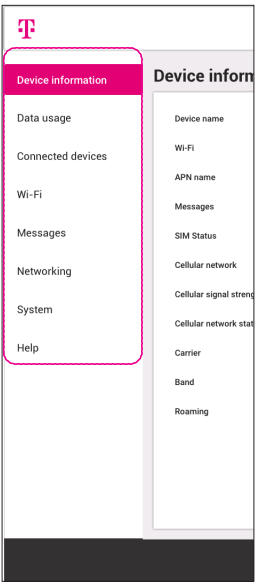
If you have changed the login and have forgotten the new one, you must restore the device to the factory default settings.

Using a narrow object, such as a paperclip or ballpoint pen, press and hold the **Factory reset** hole located at the side of your hotspot for five (5) seconds. You may then log in using the default login password which can be found on the Device Info screen of your device and on the label located under the battery of your hotspot.

Navigating the user interface

A navigation panel to the left side of the screen lists out all the main menus on the WebUI.

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




Sub-menu

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

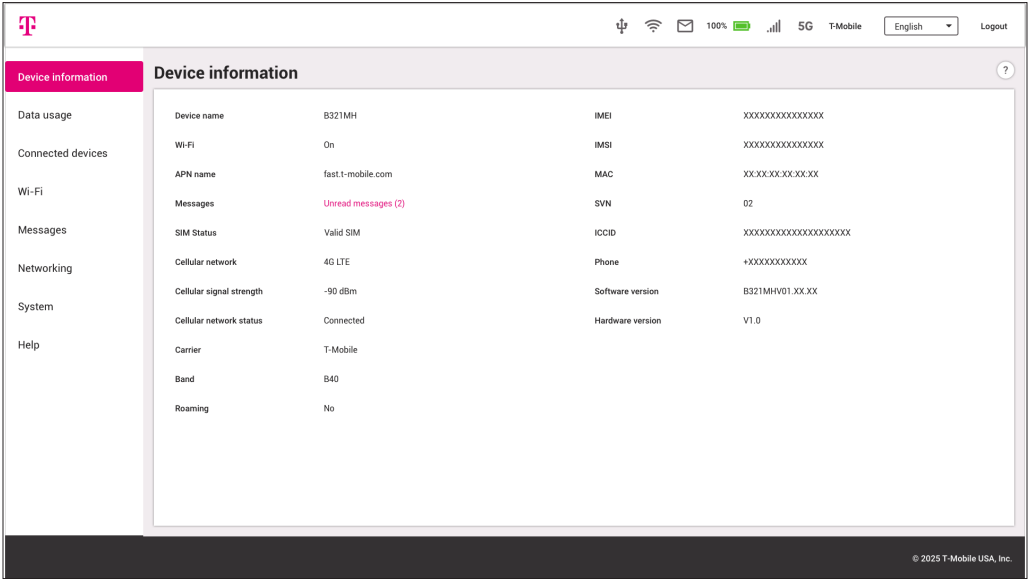


Help

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 hotspot’s status such as whether there are unread messages, firmware version, network connection status, network type, signal strength, etc. You can also view device details such as IMEI, SW version and the phone number associated with the device.

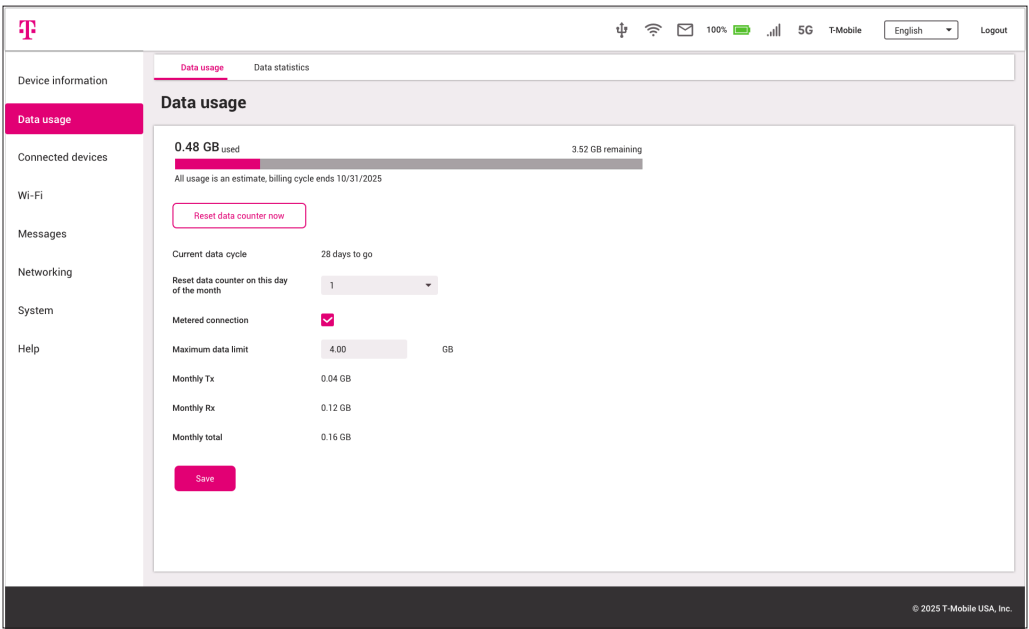


Data usage

This page provides information about your hotspot’s data usage and billing plan. You can control your data consumption by establishing a maximum data limit, resetting the data counter, and more.

Note: The data usage information presented may vary from the official T-Mobile data usage details. For accurate information, always check your T-Mobile account.

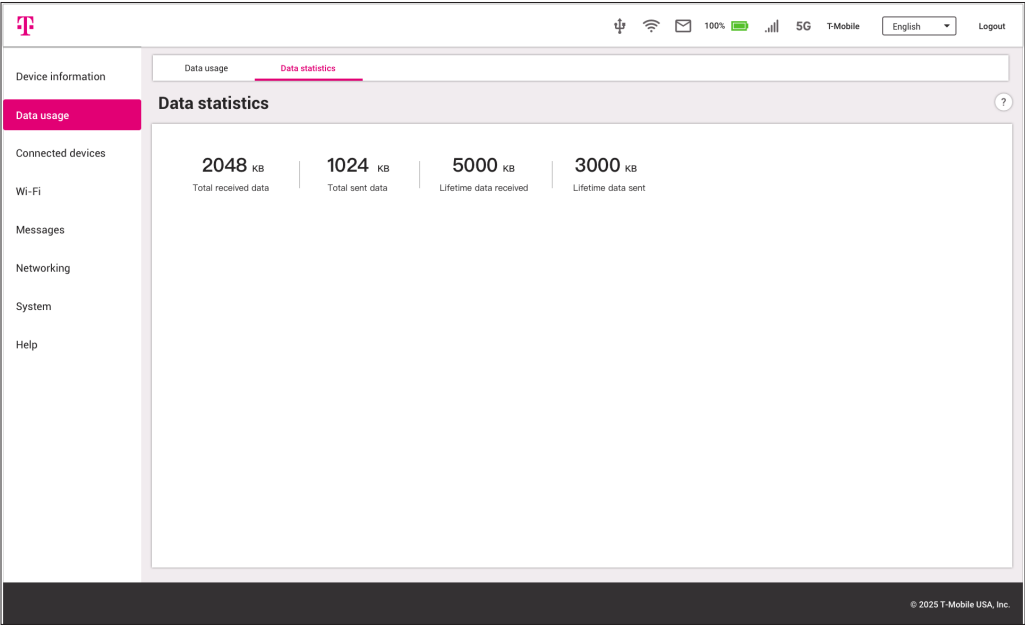
Data usage



- Estimated data usage:** This section shows the estimated data usage for the current billing cycle, up to the specified date.
- Reset data counter now:** Set the Data Counter to zero (0) and update the Reset date counter to today’s date for this month.
- Current data cycle:** This indicates the number of days left in the current cycle.
- Reset date counter on this day of the month:** This is the user-defined start date for data usage.

- Metered connection:** Check this box if you wish to establish a data limit.
- Maximum data limit:** This is the user-defined total data limit used to calculate the remaining and used data within the cycle.
- Monthly Tx (Transmission):** The amount of data sent during the current billing cycle.
- Monthly Rx (Reception):** The amount of data received during the current billing cycle.
- Monthly total:** The total amount of data used during the current billing cycle.

Data statistics



- Click **Data Statistics** tab to view below information:
- Total received data:** The total amount of data received by the hotspot since the last reset.
- Total sent data:** The total amount of data sent by the hotspot since the last reset.
- Lifetime data received:** All data received by the hotspot since its initial activation.
- Lifetime data dent:** All data sent by the hotspot since its initial activation.

Connected devices

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

Block	Device name	Network	IP address	Mac address
<input type="checkbox"/>	Device 1	5 GHz Wi-Fi	XXX.XXX.XXX.XXX	XXXXXXXXXX
<input type="checkbox"/>	Device 2	5 GHz Wi-Fi	XXX.XXX.XXX.XXX	XXXXXXXXXX
<input type="checkbox"/>	Device 3	5 GHz Wi-Fi	XXX.XXX.XXX.XXX	XXXXXXXXXX
<input type="checkbox"/>	Device 4	5 GHz Wi-Fi	XXX.XXX.XXX.XXX	XXXXXXXXXX
<input type="checkbox"/>	Device 5	5 GHz Wi-Fi	XXX.XXX.XXX.XXX	XXXXXXXXXX
<input type="checkbox"/>	Device 6	5 GHz Wi-Fi	XXX.XXX.XXX.XXX	XXXXXXXXXX
<input type="checkbox"/>	Device 7	5 GHz Wi-Fi	XXX.XXX.XXX.XXX	XXXXXXXXXX
<input type="checkbox"/>	Device 8	5 GHz Wi-Fi	XXX.XXX.XXX.XXX	XXXXXXXXXX
<input type="checkbox"/>	Device 9	5 GHz Wi-Fi	XXX.XXX.XXX.XXX	XXXXXXXXXX
<input type="checkbox"/>	Device 10	USB	XXX.XXX.XXX.XXX	XXXXXXXXXX

Unblock	Device name	Mac address
<input type="checkbox"/>	Device 11	XXXXXXXXXX

To block a device, select a device from your Connected devices list and click the **Save** button.

To unblock a device, select a device from your Blocked devices list and click the **Save** button.

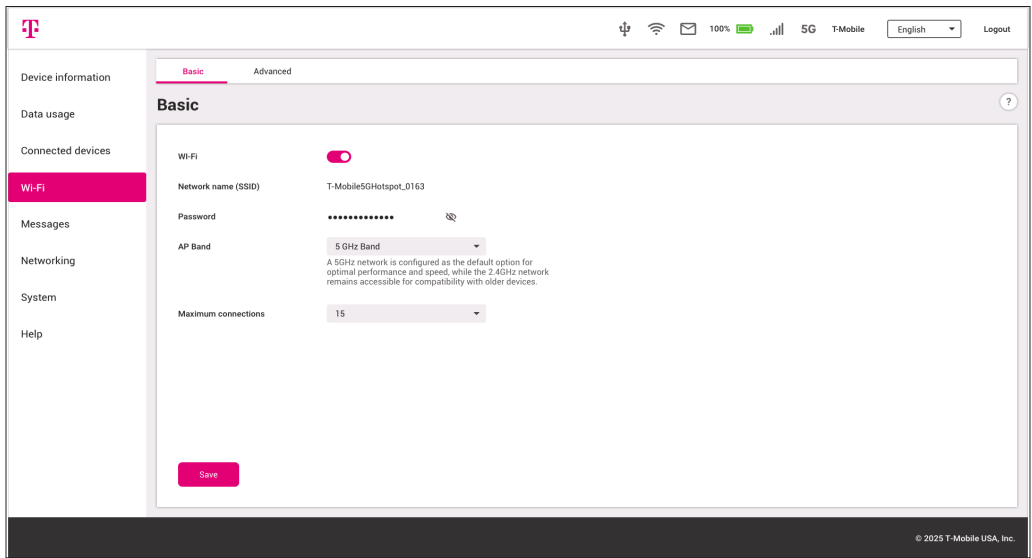
Note: The unblocked device will not be automatically included in the list of connected devices. You will need to connect it manually again.

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 hotspot.

Your hotspot does not simultaneously broadcast 2.4 GHz and 5 GHz Wi-Fi networks.

Basic



Wi-Fi: Turn the Wi-Fi on or off as required. If Wi-Fi is turned off, the hotspot's Wi-Fi network will be unavailable, and the only way to connect to the hotspot will be via a USB cable.

Network Name (SSID): Display the network name that is displayed to client devices when they scan for networks to join. To change your network name, click the **Advanced** tab at the top of the screen, enter your new network name, and then click the **Save** button to apply the changes..

Password: Display the Wi-Fi password that must be entered on any client devices needing to connect to your hotspot.

To change your Wi-Fi password, click the **Advanced** tab at the top of the screen, enter your new password, and then click the **Save** button to apply the changes.

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** hole located at the side of your hotspot for five (5) seconds. You may then log in using the default login password shown on your hotspot's Wi-Fi Info details screen.

AP Band: Select the Wi-Fi network band, 2.4 GHz or 5 GHz. The system automatically detects and displays the current band.

Maximum connections: Set the maximum number of devices that can connect simultaneously to the hotspot's Wi-Fi network. The default maximum number of devices is set to 15 devices.

The screenshot displays the 'Advanced' configuration page for a T-Mobile hotspot. The left sidebar contains navigation links: Device information, Data usage, Connected devices, Wi-Fi (selected), Messages, Networking, System, and Help. The main content area is titled 'Advanced' and is divided into two sections: 'Access-Point configuration' and 'Radio configuration'. In the 'Access-Point configuration' section, the AP Band is set to 5 GHz. The Network name (SSID) is 'T-Mobile5GHotspot_XXXX' with a note about character limits. The BSSID is 'XX:XX:XX:XX:XX:XX'. The Password is 'XXXXXXXXXX'. The Security mode is 'WPA2-PSK'. There are checkboxes for 'Hidden network', 'Hide network name on device', and 'Hide password on device'. The 'Radio configuration' section shows '802.11 Mode' as '802.11ac', 'Channel' as '149 (5745 MHz)', and 'Bandwidth' as '80MHz'. 'Save' and 'Reset' buttons are at the bottom. The footer shows '© 2025 T-Mobile USA, Inc.'.

Access-Point configuration

AP Band: Current Wi-Fi network band.

Network Name (SSID): Set the network name or SSID for the Wi-Fi network

BSSID: BSSID is a unique identifier for a specific access point (AP) within a Wi-Fi network. This field is not editable.

Password: Enter the Wi-Fi Password in this field.

Security mode: Choose your preferred option for Wi-Fi security.

- **WPA2-PSK** can be used for WPA2 devices and is set as the default security mode.
- **WPA2-PSK/WPA3-Personal** allows client devices that support either WPA2-PSK or WPA3-Personal to connect.
- **WPA3-Personal** is the latest and most secure mode.
- **Open** allows client devices to connect to your Wi-Fi network without entering a password. For your security, this option should be avoided.

Hidden network: Hide your hotspot from being visible in the list of available Wi-Fi networks.

Hide network name on device: Check this box to hide the Wi-Fi network name on the hotspot's screen. If not checked, the Wi-Fi network name will be visible on hotspot's Wi-Fi menu.

Hide password on device: Check this box to hide the Wi-Fi password on the hotspot's screen. If not checked, the Wi-Fi password will be visible on hotspot's Wi-Fi menu.

Radio configuration

802.11 mode: Displays the hotspot's Wi-Fi connecting mode. 802.11ac operates in the 5 GHz band with higher throughput.

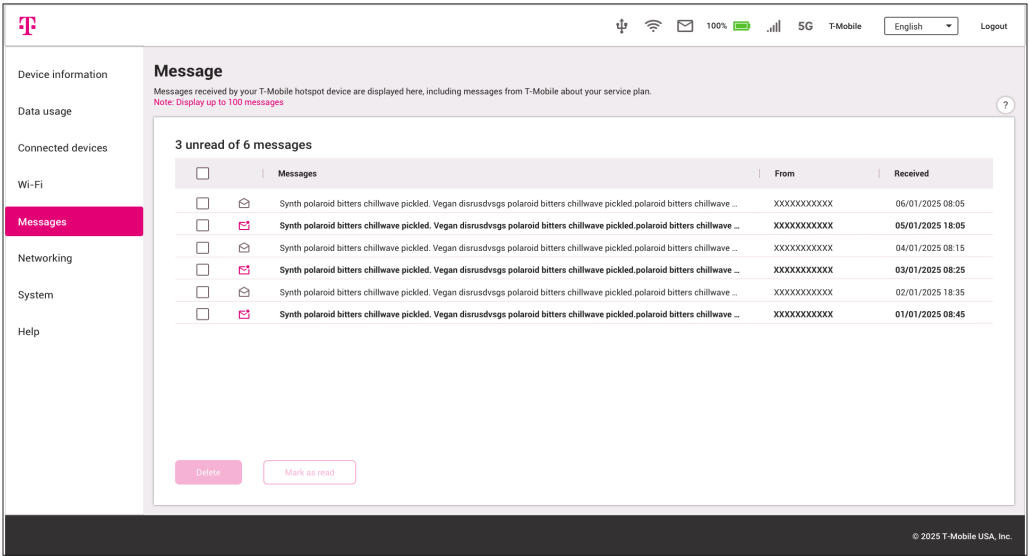
Channel: Shows the wireless channel that the radio is operating on. In most situations, leaving this as Automatic will work best, but you can manually change the channel selection using this option.

Bandwidth: Shows the bandwidth of the frequency range used by a channel, which affects the amount of data that can be transmitted simultaneously. In most situations, leaving this as Automatic will work best, but you can manually change the channel selection using this option.

Messages

The Messages page displays text messages received by your hotspot. This may include messages from T-Mobile about your service plan.

Note: It displays up to 100 messages.



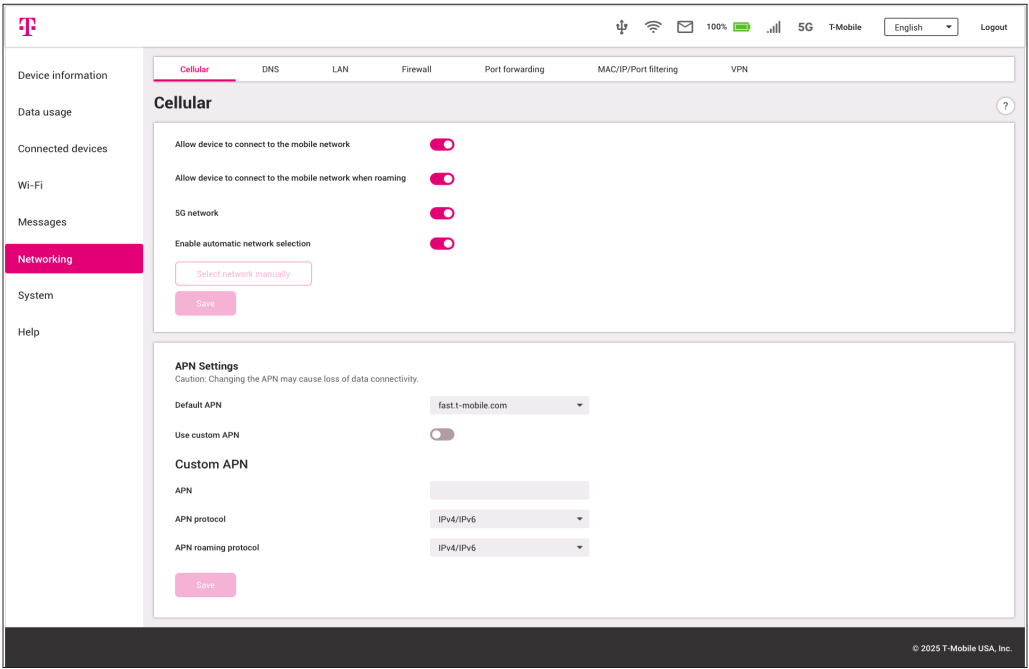
When there are more than 100 messages, older messages will be automatically deleted to make room for the new messages.

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

Cellular



Allow device to connect to the mobile network: Enable or disable cellular data when necessary, preventing access to the mobile network. This will stop connected devices from using your hotspot’s mobile data plan. By default, this setting should be enabled.

Allow device to connect to the mobile network while roaming: Enable or disable international and domestic roaming as needed. Additional data charges may apply when roaming.

5G network: Enable or disable 5G network.

Enable automatic network selection: Enable or disable automatic network selection. When enabled, your hotspot will automatically select the best available network, and the Select Network Manually option will be disabled.

Select Network Manually: Click the button to scan for available networks and then select your preferred network. This option is only accessible if Enable Automatic Network Selection is turned OFF.

APN Settings

Default APN: Select a pre-configured VPN service that comes built-in with your hotspot or is provided by your network carrier.

Use Custom APN: Set a custom VPN manually. You can configure settings such as APN protocol and APN roaming protocol.

Custom APN

You can manually configure a custom VPN. First, enable the **Use custom APN** option, then enter the **APN name**, select the **APN protocol** and **APN roaming protocol**. When finished, click **Save** to apply the settings.

DNS

The screenshot shows the 'DNS' configuration page within a T-Mobile hotspot management interface. The top navigation bar includes 'Cellular', 'DNS' (selected), 'LAN', 'Firewall', 'Port forwarding', 'MAC/IP/Port filtering', and 'VPN'. A left sidebar lists 'Device information', 'Data usage', 'Connected devices', 'Wi-Fi', 'Messages', 'Networking' (highlighted), 'System', and 'Help'. The main content area is titled 'DNS' with a subtitle: 'Your hotspot automatically selects a Domain Name Server (DNS) or you can manually set one.' Below this, there is a 'Manual DNS' section with a toggle switch currently turned off. Two input fields are present: 'DNS 1 IP address' with a placeholder 'Required (IPv4 address)' and 'DNS 2 IP address' with a placeholder 'Optional (IPv4 address)'. A 'Save' button is at the bottom left of the form area. The footer shows '© 2025 T-Mobile USA, Inc.'

Normally, the DNS (Domain Name System) server address is assigned automatically. This page allows you to manually specify a DNS address if necessary.

- Manual DNS:** Enable or disable the Manual DNS feature.
- DNS 1 IP address:** Enter the IP address of the primary DNS you wish to use. This address is required for the Manual DNS feature to function.
- DNS 2 IP address:** Enter the IP address of the secondary (backup) DNS. This address is optional and can be left blank if not needed

LAN

The screenshot shows the 'LAN' configuration page within a T-Mobile hotspot management interface. The top navigation bar includes 'Cellular', 'DNS', 'LAN' (selected), 'Firewall', 'Port forwarding', 'MAC/IP/Port filtering', and 'VPN'. A left sidebar lists 'Device information', 'Data usage', 'Connected devices', 'Wi-Fi', 'Messages', 'Networking' (highlighted), 'System', and 'Help'. The main content area is titled 'LAN'. It contains several input fields: 'IP address' (192.168.1.1), 'Subnet mask' (255.255.255.0), 'MAC address' (18:27:86:84:c8:02), 'DHCP lease time' (1440 min), 'Start DHCP address range at' (192.168.1.2), and 'End DHCP address range at' (192.168.1.102). There is a 'Reserved IP addresses' button. A 'Save' button is at the bottom left of the form area. The footer shows '© 2025 T-Mobile USA, Inc.'

IP address: The default internet IP address assigned to your hotspot.

Subnet mask: The subnet mask network setting for the device. The default value of 255.255.255.0 is standard for small (Class “C”) networks. This field is read-only and can’t be modified.

MAC address: The MAC address is a unique identifier assigned to each network device during manufacturing. This field is read-only and displays the MAC Address for the interfaces on this hotspot.

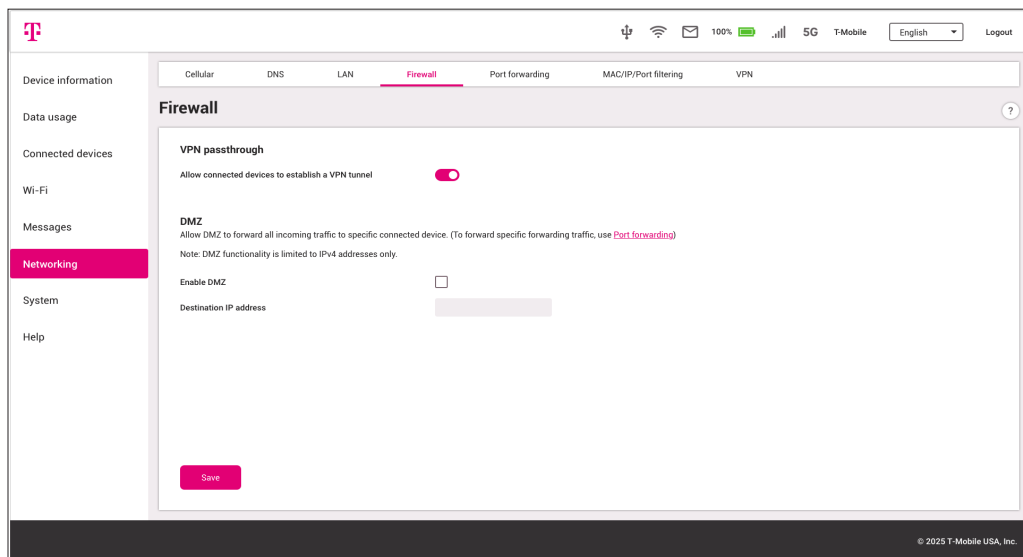
DHCP lease time: DHCP (Dynamic Host Configuration Protocol) Lease Time refers to the duration for which a DHCP server assigns an IP address to a device on a network. During this lease period, the hotspot is allowed to use the assigned IP address. You can leave this at the default value, but it can be adjusted if you have specific requirements.

Start DHCP address range at: The start of the IP address range used by the DHCP server. This setting should only be modified by advanced users.

End DHCP address range at: The end of the IP address range used by the DHCP server. This setting should only be modified by advanced users.

Reserved IP Addresses: Reserved IP Addresses are fixed addresses assigned to specific devices, ensuring consistent connectivity and simplifying network management while preventing address conflicts. Click this button to add or edit the reserved IP addresses. Each reserved IP address must be within the range of IP addresses used by DHCP.

Firewall



VPN Passthrough

Allow connected devices to establish a VPN tunnel: This feature allows VPN client software on connected devices to connect through this hotspot to remote VPN servers. This option should be left on by default.

DMZ

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

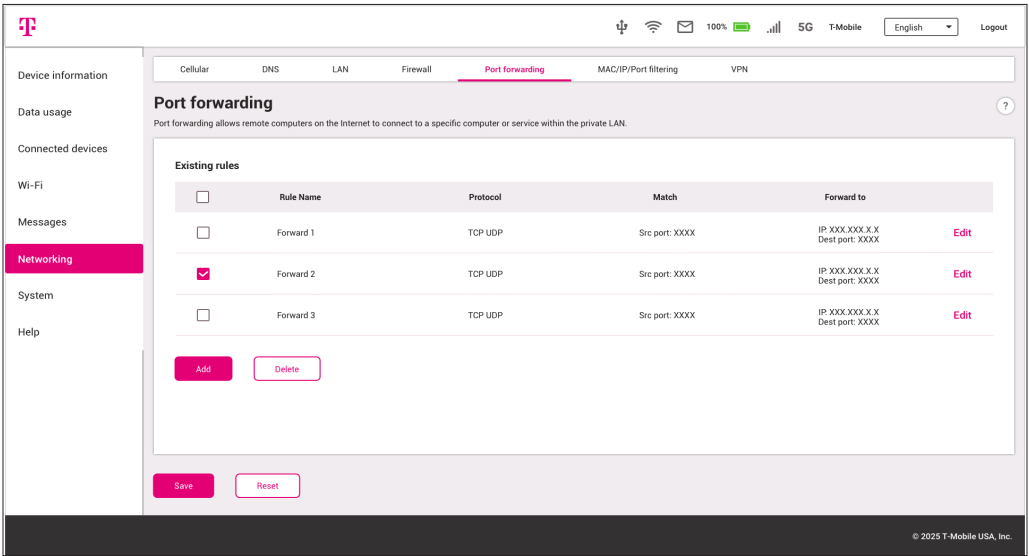
Enable DMZ: Enable or disable DMZ. If enabled, the connected device designated as the DMZ IP address (DMZ destination) will receive all traffic that would typically be blocked by the firewall.

Note: This may help certain problematic network applications function properly, but the DMZ device should have its own firewall to protect against malicious traffic. Normally, DMZ should be disabled unless really necessary.

Destination IP address: Enter the IP address of the connected device you want to designate as the DMZ device (DMZ destination) in this field. You can find the IP address of each connected device on the connected devices screen.

Port forwarding

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN. You can add a new rule, edit or delete the existing rules.



To create a new rule, click the **Add** button and enter the below required details:

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

Protocol: Select the protocol used by the port from the dropdown list (TCP, UDP, or TCP+UDP).

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

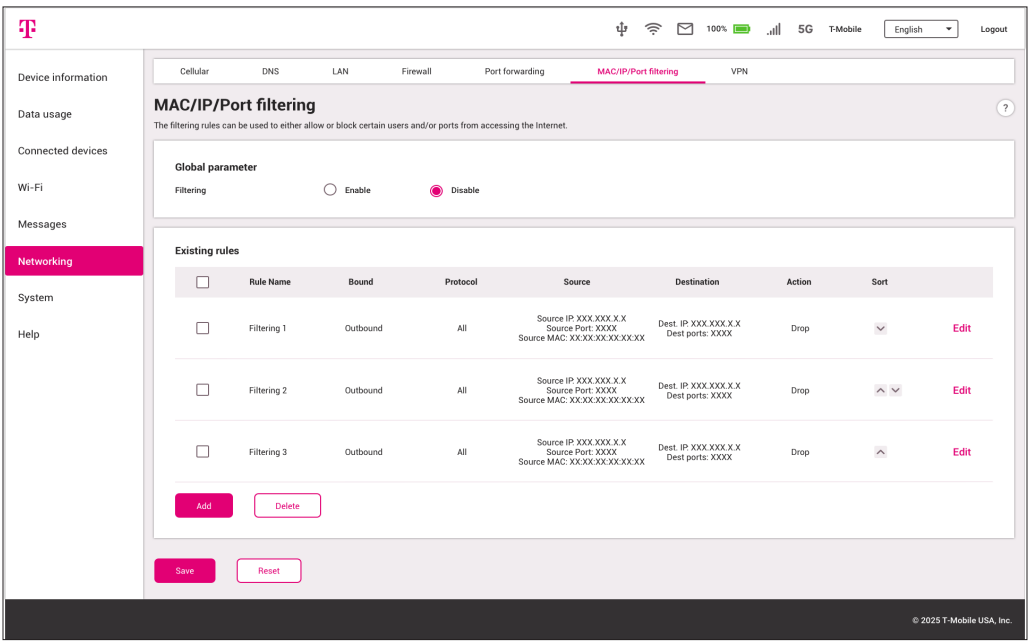
Internal IP: Redirect matched incoming traffic to the specified internal host

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

When finished, click the **Save** button.

MAC/IP/Port filtering

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



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 and enter the below required details:

Rule name: Assign a meaningful name to identify the purpose of the filter rule.

Bound: Select bound type. Inbound refers to packets coming from the WAN (Wide Area Network) to the LAN (Local Area Network). Outbound refers to packets moving from the LAN to the WAN.

Source MAC: Specify a source MAC address to allow or block its access to the Internet.

Source IP: Specify a source IP address to allow or block its access to the Internet.

Destination IP: Specify a destination IP address to allow or block access.

Protocol: Select the protocol used by the port (TCP, UDP, or TCP+UDP)).

Source ports: Enter the ports number that traffic will be filtered from. This can be a single port (e.g., 5060) or a range of ports (e.g., 5000-6000). Leaving this blank means the source port check will be skipped.

Destination ports: Enter the ports number to which traffic will be filtered. This can be a single port (e.g., 6060) or a range (e.g., 6000-7000). Leaving this blank means the destination port check will be skipped.

Action: Select Drop, Accept, or Reject to deny or allow the access to the Internet

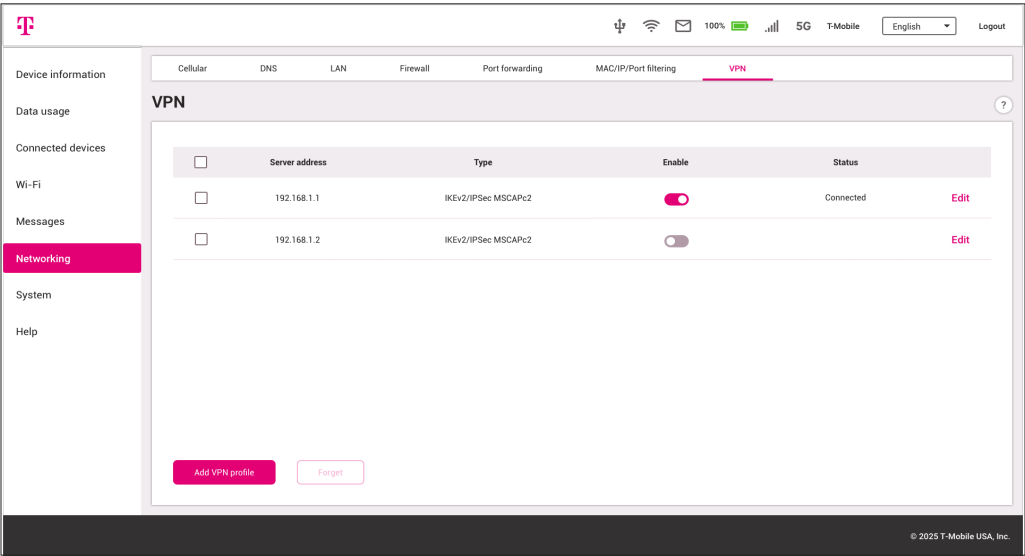
When finished, click the **Save** button.

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

Use this page to establish a tunnel connection to an Open VPN server and route all traffic on connected devices through the tunnel.



This section show user configured Open VPN list.

To add a new rule, click the **Add VPN profile** button and enter the below required details:

Type: Select VPN protocol type (IKEv2/IPSec MSCAPV2 or IKEv2/IPSec PSK).

Server address: Specifies where to connect for the VPN service, crucial for establishing the connection.

IPSec identifier: A unique identifier used in the IPSec protocol to specify the security association for a VPN connection.

Username: Enter your VPN connection username.

Password: Enter your VPN connection password.

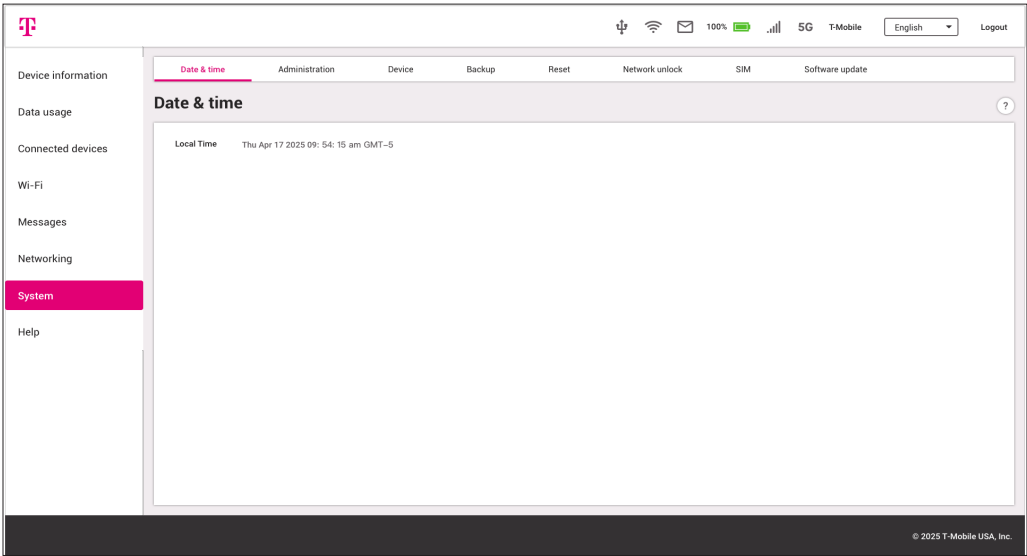
Enable: Check this box to keep this function active at all times

When finished, click the **Save** button.

System

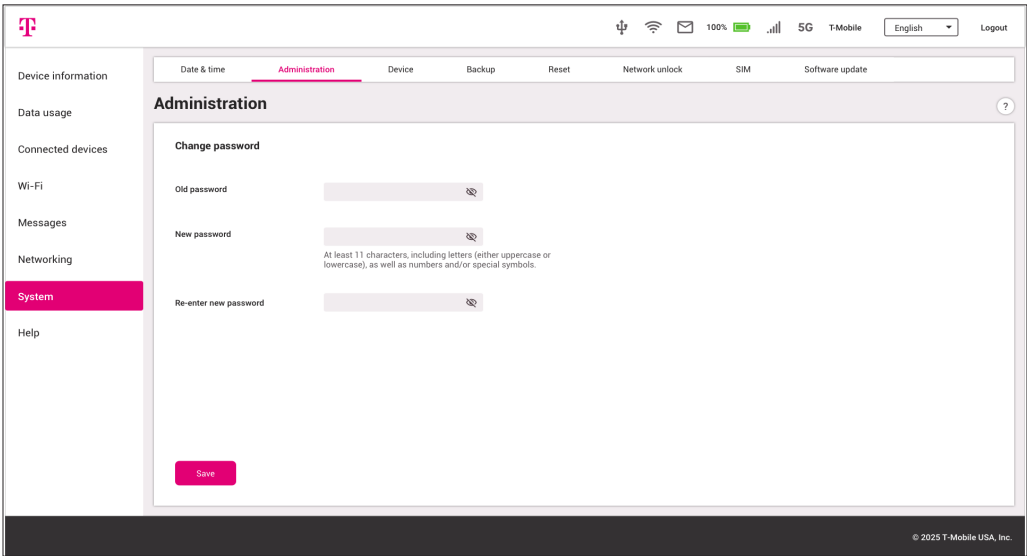
Date & time

View the date and time



Administration

Change the admin password for accessing your hotspot's WebUI.



To change the password, follow the below steps:

1. Enter the current password in the **Old password** field.
2. Enter a new password in the **New password** field
3. Re-enter the new password in the **Re-enter new password** field. The passwords entered must be identical, otherwise the password will not be updated.
4. When finished, click the **Save** button.

Device

You can customize the device's behavior to better suit your preferences.

The screenshot shows the T-Mobile Device settings page. The top navigation bar includes icons for USB, Wi-Fi, Signal, 100% battery, 5G, T-Mobile, Language (English), and Logout. The left sidebar lists settings categories: Device information, Data usage, Connected devices, Wi-Fi, Messages, Networking, System (highlighted in red), and Help. The main content area is titled 'Device' and contains several settings: 'USB mode when connected to a computer' (set to 'Charge the B321MH'), 'Turn off screen' (set to 'After 30 seconds'), 'Sleep' (set to 'After 10 minutes'), 'Shutdown' (set to 'After 2 hours'), 'Turn on battery preservation mode' (toggle is on, with a note: 'After about 16 hours of charging, the battery stays between 70% and 80%, preventing overcharging and preserving its integrity.'), 'Device language' (set to 'English'), 'Charge Other Device' section with 'Current status' (set to 'Available') and 'Stop charging other devices when battery reaches' (set to '25%'), and 'Hide WebUI URL & password on device' (checkbox is unchecked). A red 'Save' button is at the bottom.

USB mode when connected to a computer: Select the connection option when your device is connected to a computer via the USB cable.

Turn off screen: Set the duration of inactivity after which the device's screen will turn off.

Sleep: Choose the desired time interval for entering sleep mode. The hotspot will enter sleep mode after a specified period of inactivity

Shutdown: Set the time period of inactivity that will trigger the device to shut down.

Turn on battery preservation mode: Battery Preservation Mode helps extend your battery life by maintaining the charge level between 70% and 80%. It is recommended that you enable this mode if you often charge your device for extended periods of time. When enabled, Battery Preservation Mode will activate after an extended period of continuous charging.

Device language: Set the language for your device's screen display.

Charge other device

Use your hotspot's battery to charge devices like your phone or Bluetooth headset. Just connect your device's USB cable to the hotspot's charging port.

Current status:

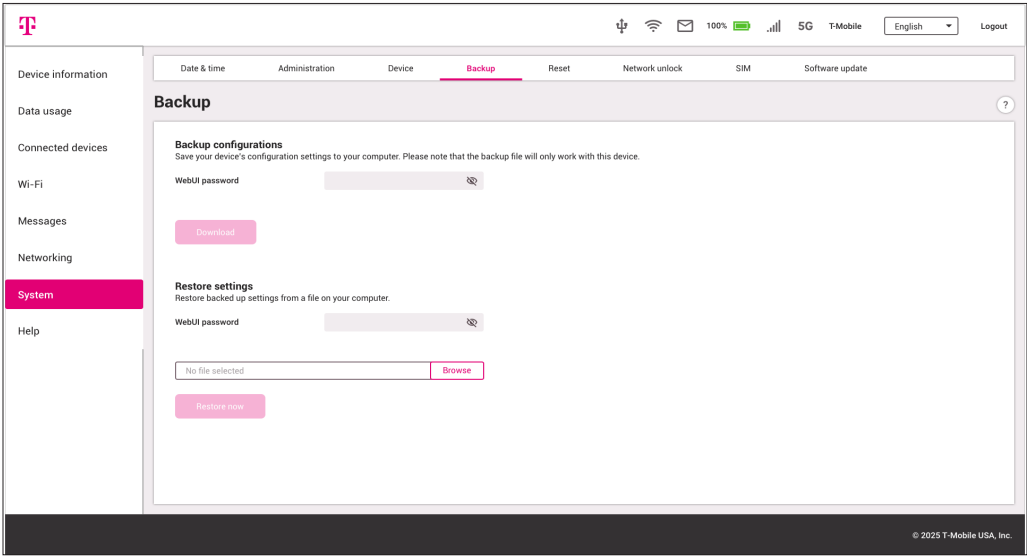
- **Charging:** An external device is currently being charged from the hotspot's battery.
- **Available:** Charging other devices function is available, you can connect your device's USB cable to the hotspot's charging port to start charging.
- **Not available (Low battery):** Charging other devices function is not available due to the hotspot's low battery level.

Stop charging other devices when battery reaches: Select a battery percentage at which you want to stop charging other devices in order to reserve hotspot's battery power. Avoid using the Charge Other Devices function if you need the battery to last for a full day.

Hide WebUI URL & password on device: If this setting is enabled, the WebUI URL and default login password will not be displayed on the device. If disabled, the WebUI URL and default login password will be visible on the device information screen on the device.

Backup

You can back up (download) a copy of the device's configuration settings to a file on your computer or restore (upload) a previously saved configuration file. This configuration file contains all settings related to the device, router and system functions, but it does not include any settings or data for the 4G/5G modem. Please note that you can only restore a file to the original device from which it was created.



Backup configurations

WebUI password: Enter the current login password for the hotspot's WebUI.

Download: Click the **Download** button to download a copy of the current configuration file to your computer. If prompted to save the file, you may rename it if desired.

Note: The backup file cannot be edited or viewed on any devices. This file can only be restored to this hotspot, and settings can only be viewed or modified through the WebUI.

Restore settings

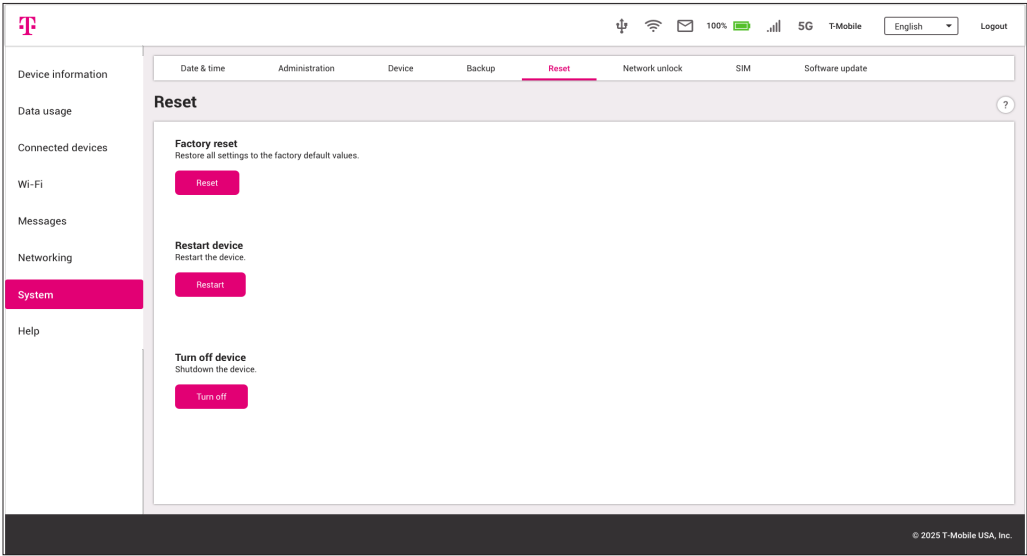
WebUI password: Enter the current login password for the hotspot's WebUI.

Browse: Click the **Browse** button to select the configuration file you previously downloaded from this hotspot to your computer.

Restore now: After selecting a configuration file, click the Restore now button to upload the file. After uploading, the configuration file will be applied immediately, and the hotspot will restart.

Note: Uploading a configuration file will change ALL existing settings. All current connections to this hotspot will be disconnected, including your web browser session.

Reset



Factory reset: Click the **Reset** button to restore all settings to their factory default values. This action will restart the device, disconnecting all current connections to this hotspot, including your web browser session.

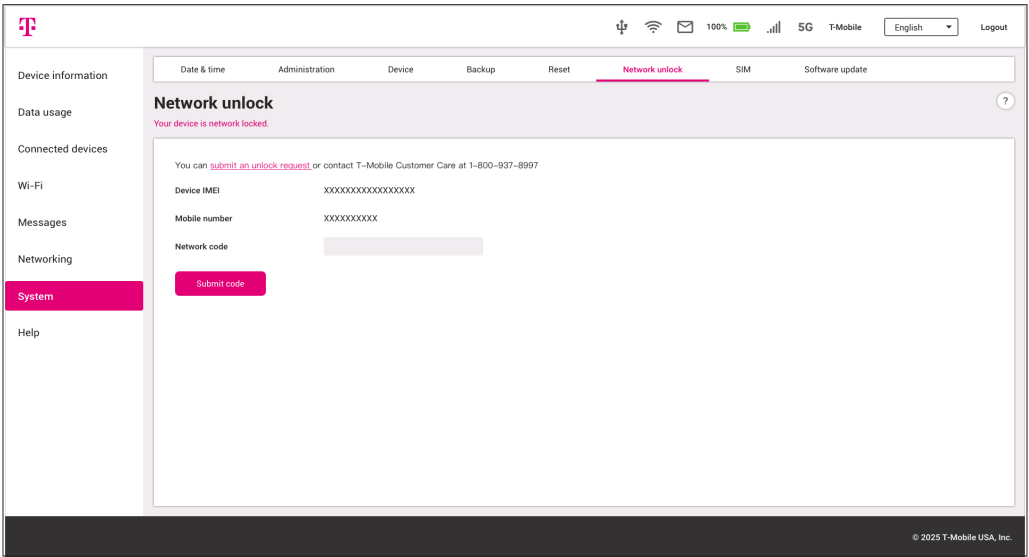
Note: Take care with using this feature as all settings and messages stored on the device will be lost when the device is factory reset.

Reboot device: Click the **Restart** button to restart your hotspot.

Turn off device: Click the **Turn off** button to turn off your hotspot.

Network unlock

The Network unlock page is used to UNLOCK the network.

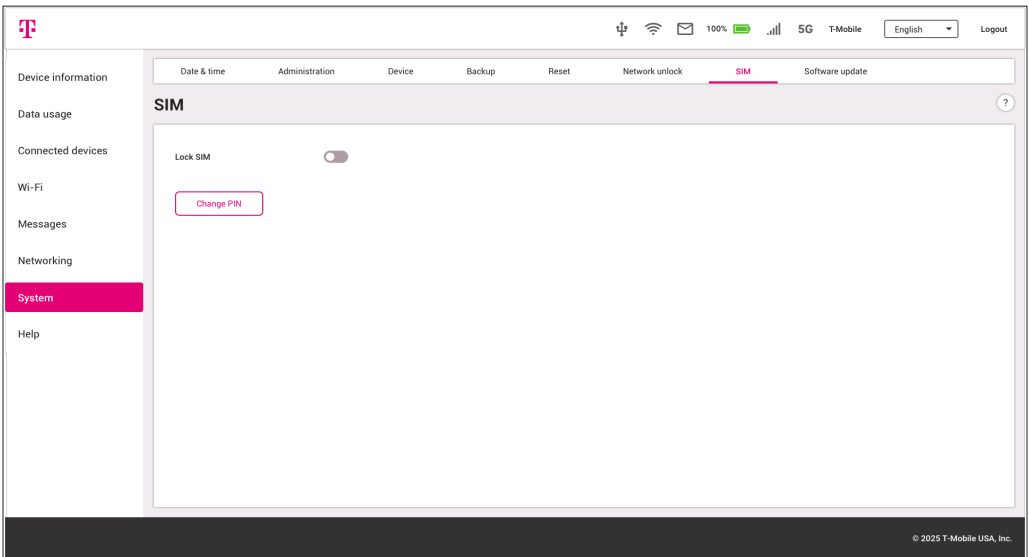


If the hotspot is locked to T-Mobile network, follow the below steps to unlock:

- 1.Contact T-Mobile Customer Care to get a network unlock code.
- 2.Enter the network unlock code on **Network code** field
- 3.Click the **Submit code** button.

SIM

SIM PIN lock is a security feature that requires a Personal Identification Number (PIN) to access the SIM card in your device. When the SIM PIN lock is enabled, the user must enter the correct PIN each time the hotspot is powered on or the SIM card is inserted into a new device.



If the wrong PIN is entered three times, the SIM card will become locked, requiring a PUK (Personal Unblocking Key) code to unlock it.

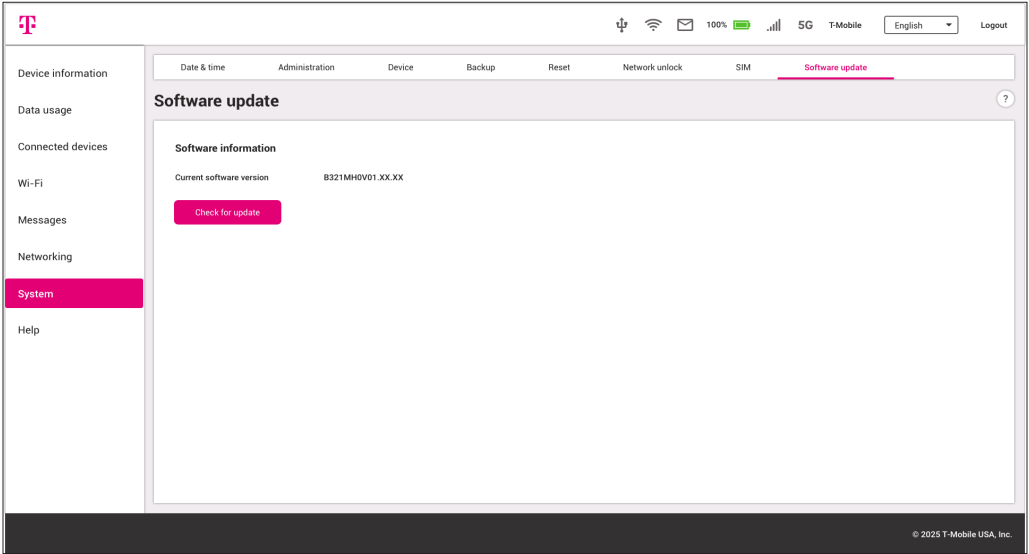
Entering the wrong PUK code 10 times will permanently lock the SIM card, making it unusable.
If you require assistance, please reach out to your service provider.

Lock SIM: Enable or disable SIM PIN lock.

Change PIN: Change your SIM PIN code

Software update

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



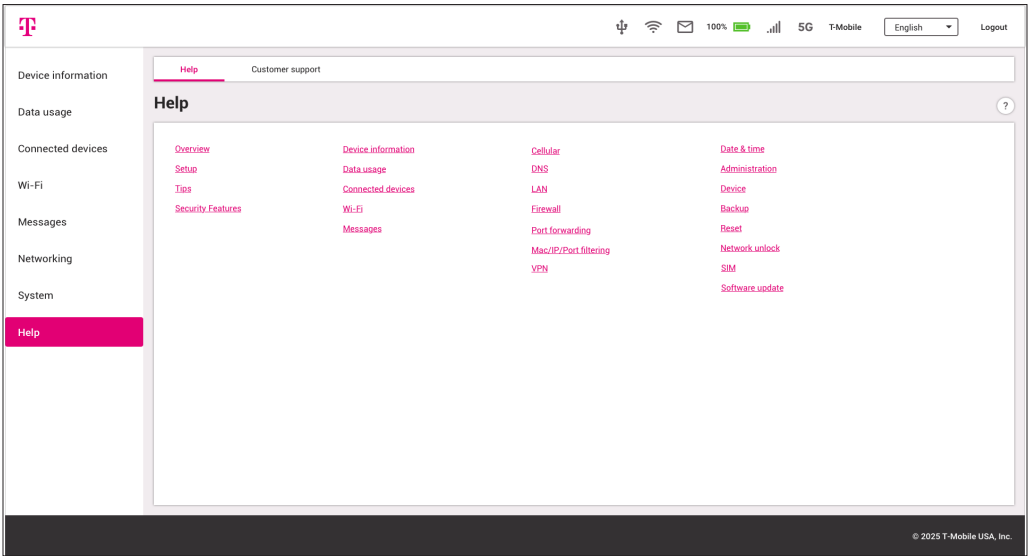
Current software version: The current software version installed on hotspot.

Check for update: Click the Check for update button to check for the latest software update.

Continue update: This button will appear when you have incomplete update available. Click the Continue update button to resume software update.

Help

This page provides links to help topics for every page of the WebUI and general topics useful for getting started with your hotspot. Use the Customer support tab for useful links and support information.



Troubleshooting

Check below for solutions to common problems you may experience.

Problem	Possible solutions
The device cannot connect to the hotspot	<ul style="list-style-type: none">• Restart the hotspot.• Restart the device you want to connect (laptop, smartphone, etc.).• Confirm the Wi-Fi network name (SSID) and password and establish a new connection to the hotspot.
The device is connected to the hotspot but cannot access the internet	<ul style="list-style-type: none">• 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 5.• Check to see if Cellular is enabled in the WebUI. See "Cellular" on page 17.
Download and/or upload speeds are slow	<ul style="list-style-type: none">• 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 hotspot to optimize the Wi-Fi connection.
Forgot the password to the Wi-Fi network	<p>The password to your Wi-Fi network can be easily found on the hotspot's Wi-Fi Info details screen, see "Wi-Fi Info screen" on page 7.</p> <p>If you need to change your Wi-Fi password, see "Change Wi-Fi network name and password" on page 11.</p>
Forgot the password to the WebUI	<p>The default login information of the WebUI can be found on the Device Info screen of your device and on the label located under the battery of your hotspot.</p> <p>If you need to change your WebUI password, see "Administration" on page 22.</p> <p>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 hole located at the side of your hotspot for five (5) seconds. You may then log in using the default login password which can be found on the Device Info screen of your device and on the label located under the battery of your hotspot.</p> <p>.</p>
Can't access the WebUI	<ul style="list-style-type: none">• Confirm that you are trying to access the WebUI from a device that is currently connected to your hotspot via either a Wi-Fi or USB connection.• Confirm that you have entered the correct URL (http://mifimanager or http://192.168.0.1) directly into the browser address field on your connected device.• Confirm that you have entered the correct login credentials. The default login password can be found on the Device Info screen of your device and on the label located under the battery of your hotspot.

Safety and use

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

This product is equipped with a USB cable for connecting with 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, 0.35A.

Output: 5V, 2000mA.

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 45°C (113°F). The operating temperature for the device is 14°F (-10°C) to 131°F (55°C). The charging temperature for the device is 32°F (0°C) to 122°F (50°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 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.
- Only use the battery for the system for which it is specified.
- Only use the USB cable provided with the device or that bear the USB-IF logo or have completed the USB-IF compliance program.
- 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. Use of an unqualified battery or charger may present a risk of fire, explosion, leakage, or other hazards.
- 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 hazards. Only authorized service providers shall replace battery. (If the battery is non-user replaceable).
- Promptly dispose of used batteries in accordance with local regulations.
- Battery usage by children should be supervised.
- 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.
- Do not replace an embedded battery pack. Improper replacement may present a risk of fire, explosion, leakage, or other hazards. Contact the manufacturer for replacement instructions.
- The device identifies the battery by the NTC Pin.
- 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.

Plastics content

The percentage of post-consumer recycled and biobased plastics content in your device is 0%.

FCC Regulations

This 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 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 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 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 hotspot as reported to the FCC when worn on the body, is 1.19 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 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: XD6B321MH.

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 0.5 cm from the body. Use of other accessories may not ensure compliance with FCC RF exposure guidelines.