



M100

User Manual

Contents

Safety information	3
Getting started	4
Getting to know your device	4
Installation	5
Install the SIM card	5
Charge your mobile hotspot	6
Turn on your mobile hotspot	6
Check the wireless signal	6
LCD display screen	7
Home screen	7
Wi-Fi screen	8
Data usage screen	8
Devices screen	9
Messages screen	9
Notifications screen	10
Device info screen	10
Admin website screen	11
Software update screen	11
Internet access	12
Connect via Wi-Fi	12
Connect via USB Tethering	13
Admin website	14
Login	14
Homepage	14
Device information	15
Data usage	15
Connected devices	16
Wi-Fi	16
Messages	18
Networking	18
System	24
Software update	28
Help	28
Troubleshooting	29
Regulatory Information	30
FCC regulations	30
RF Exposure Information (SAR)	30
Safety precautions for power supply unit	31

Safety information

Please carefully read the items bellow:

Use Safely

Do not use the device in situations where it might cause danger.

Transportation Safety

Please observe all transportation laws and regulations. Please drive with both hands on the wheel.

Hospitals

Please follow limitations.

Please turn off your device when near medical instruments.

Airports

Remember to follow all airport and flight safety regulations. Please do not use your device during flight.

Toxic Chemicals

Do not use your device around fuels or chemicals.

Hazard

Do not use in hazardous areas where explosions may occur.

Accessories and Batteries

Use only BLU authorized batteries and accessories.

Backup

Remember to keep a written record of all important information.

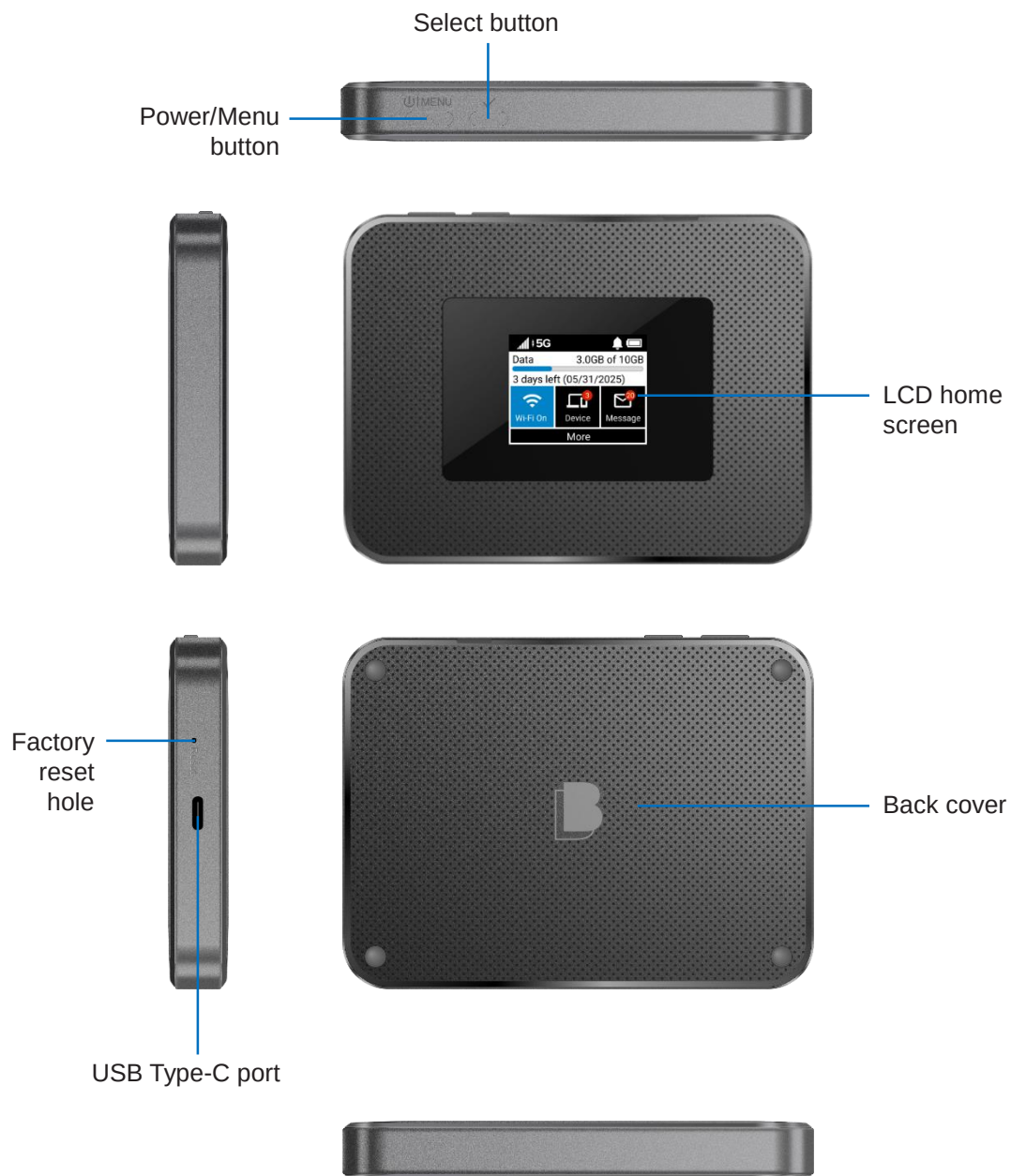
Water

Your device has an IP52 water resistance rating.

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

Part	Description
Power/Menu button	- Press and hold the Power/Menu button for three (3) seconds to turn your mobile hotspot on or off. - Short press the Power/Menu button to scroll through the options. - When the screen is on, quickly press the Power/Menu button twice to turn the screen off. - When the screen is off, press the Power/Menu button once to turn the screen on.
Select button	- Press the Select button to confirm your choice. - From any screens except Home screen and pop-ups, press and hold the Select button for three (3) seconds to return to the previous screen.
LCD home screen	View information and access features of your mobile hotspot
Factory reset hole	Using a narrow object, such as a paperclip or ballpoint pen, press and hold the Factory reset hole for five (5) seconds to perform a factory reset
USB Type-C charging port	Connect the included charger for charging or connect to a device for tethering.

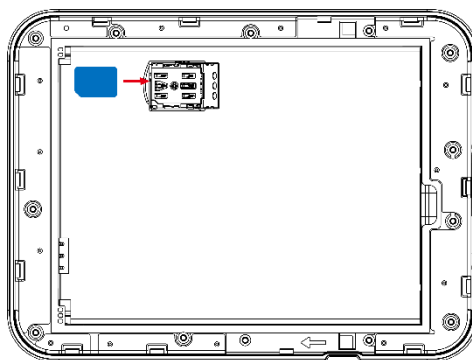
CAUTION! Inserting an accessory into the incorrect port may damage the device.

Installation

Install the SIM card

Please contact your service provider directly to obtain your SIM card if your card is not preinstalled.

1. Remove the back cover and battery.
2. Slide the clip to the right to open it, place the new SIM card into the SIM slot with gold contacts facing downward, and slide the clip to the left to lock it.
3. Insert the battery and reattach the back cover.

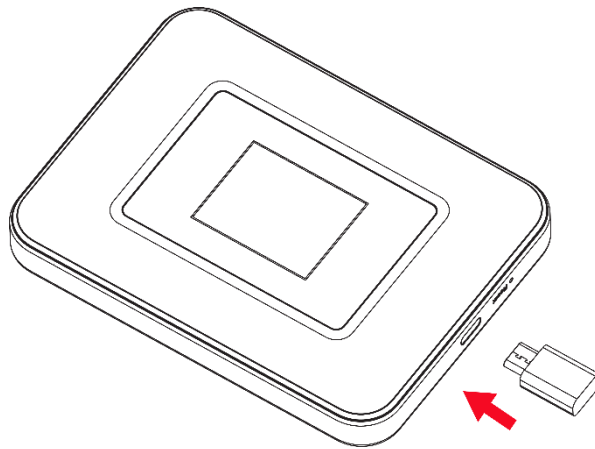


Warning: Please keep the SIM card out of the reach of children. The SIM card and its contact are easily damaged due to scratching or bending.

Please use caution when carrying, installing, or taking out the SIM card.

Charge your mobile hotspot

1. Connect one end of the data cable to the USB port located on the side of your mobile hotspot.
2. Connect the other end to the power adapter.
3. Connect the power adapter to an electrical outlet to fully charge your mobile hotspot.



Turn on your mobile hotspot

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

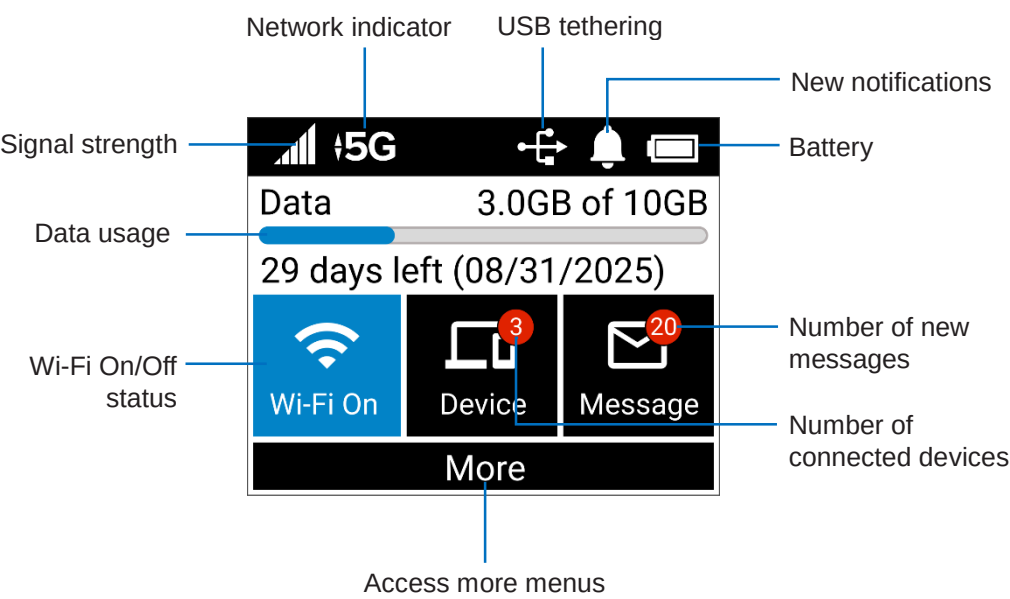
Check the wireless signal

When you turn on your mobile hotspot (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



Name	Description
Network indicator	Network information
USB tethering	USB connected for tethering
New notifications	New notifications received.
Signal strength	Indicates the signal strength. More signal bars indicates higher signal strength.
Battery	Show battery status.
Data usage	View data usage information.
Wi-Fi On/Off status	Show On/Off status of the Wi-Fi.
Wi-Fi connected devices	The number on top right indicates the number of Wi-Fi connected devices.
New messages	The number on top right indicates the number of new messages.
More	Access Notifications, Device info, Admin website, and Software update screens.

Wi-Fi screen

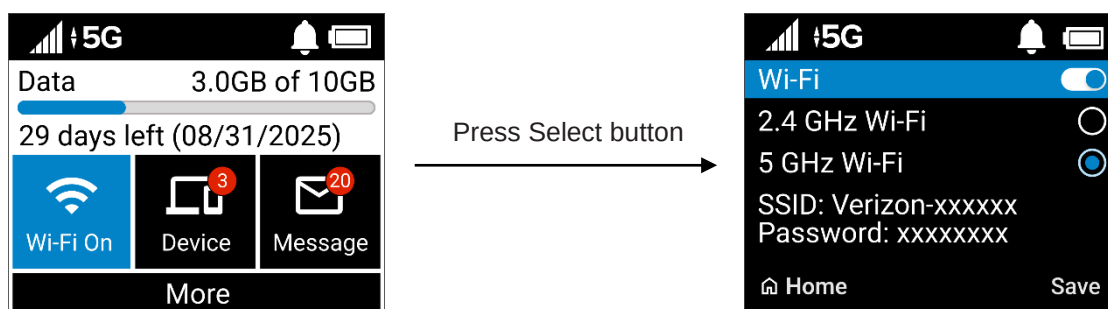
From the Home screen, use the **Power/Menu** button to highlight the **Wi-Fi** section, then press **Select** button to access the Wi-Fi details screen to view your Wi-Fi SSID and password.

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

Turn Wi-Fi On or Off

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

1. Use the **Power/Menu** button to highlight the Wi-Fi toggle, then press **Select** button to switch between On and Off.
2. When selected, use the **Power/Menu** button to highlight the **Save** button, then press the **Select** button to save your choice.



Your mobile hotspot does not simultaneously broadcast 5 GHz and 2.4 GHz Wi-Fi networks. The default Wi-Fi network is 5 GHz. You can switch to the 2.4 GHz Wi-Fi network by selecting **2.4 GHz Wi-Fi** on Wi-Fi screen and selecting the **Save** button to apply the change.

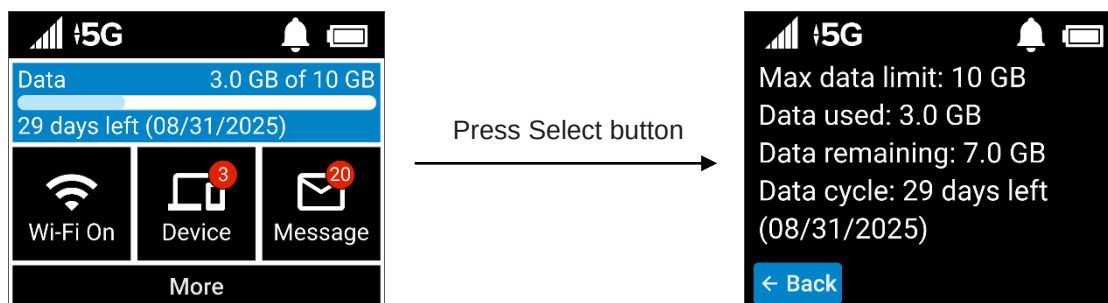
Note: The Wi-Fi name and password are visible by default, and you can hide it via the Admin website.

Data usage screen

From the Home screen, use the **Power/Menu** button to highlight the **Data usage** section, then press **Select** button to access the data usage details screen.

Data usage screen provides information about the data limit you've set, current data used, data cycle, etc.

You can change the data limit and data cycle via the Admin website.

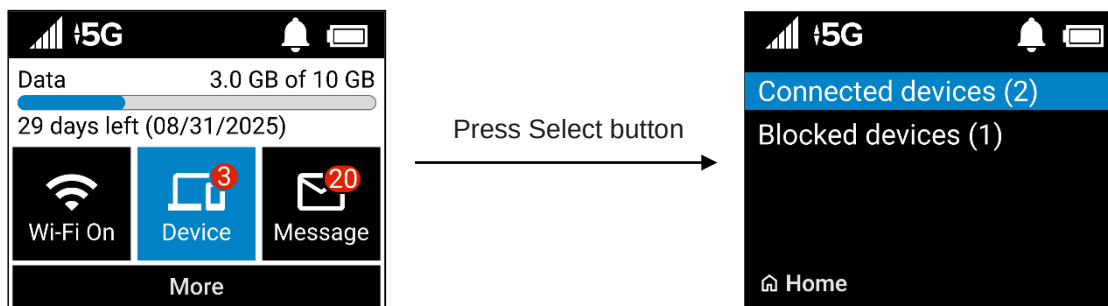


Note: The data usage information presented may vary from the official Carrier's data usage details. For accurate information, always check your Carrier account.

Devices screen

From the Home screen, use the **Power/Menu** button to highlight the **Device** section, then press **Select** button to access the connected or blocked device list.

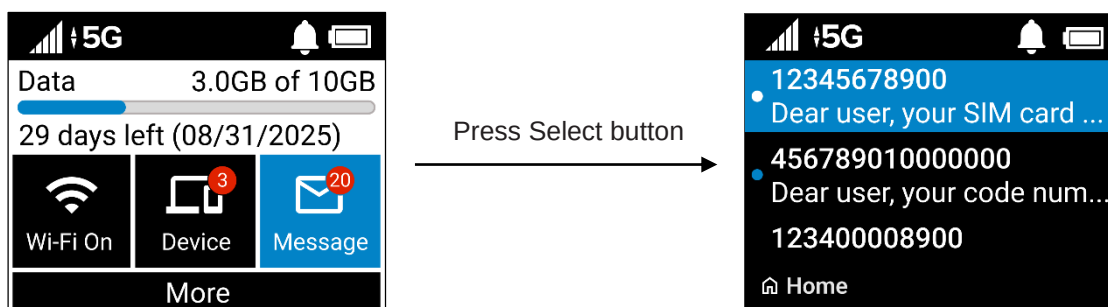
1. Select **Connected devices** to view currently connected devices. Select a device to view detailed information. You can block the device by selecting the **Block** button.
2. Select **Blocked devices** to view currently blocked devices. Select a device and select the **Unblock** button to unblock it.



Messages screen

From the Home screen, use the **Power/Menu** button to highlight the **Message** section, then press **Select** button to access the message list.

From the messages list screen, use the **Power/Menu** button to highlight the message you want to view, then press the **Select** button to access the messages details.



If a message is too long to display in one screen, press the **Power/Menu** button to scroll down to view the rest screens of the current message.

From the message details screen, you can select **Delete** button to delete the message.

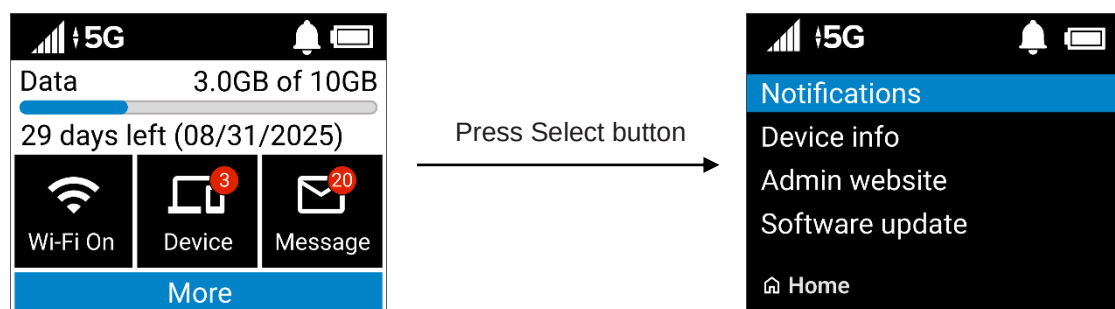
Notifications screen

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.

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

To access the **Notifications** screen, follow the below steps:

1. From the Home screen, use the **Power/Menu** button to highlight the **More** section.
2. Press **Select** button to access more menus.
3. Select **Notifications** to access the notifications screen.
4. If a message is too long to display in one screen, press the **Power/Menu** button to scroll down to view the rest screens of the current notification.
5. You can select **Next** button to view the next unread notification.

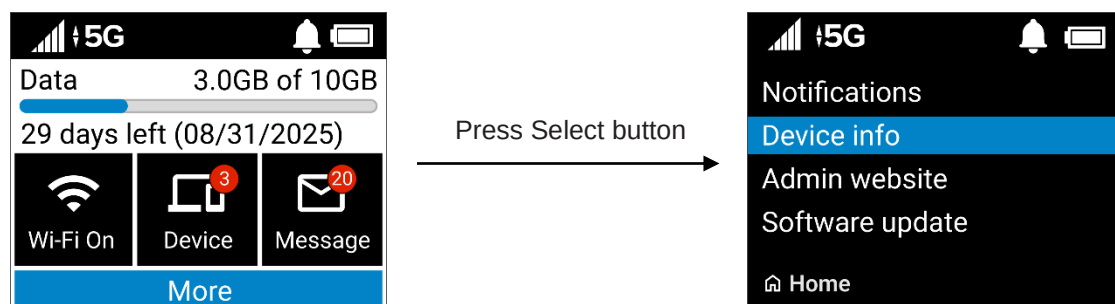


Device info screen

Device info screen displays your mobile hotspot's important information, such as device name, mobile number, connection status, IMEI, IP address, and more.

To access the **Device Info** screen, follow the below steps:

1. From the Home screen, use the **Power/Menu** button to highlight the **More** section.
2. Press **Select** button to access more menus.
3. Select **Device info** to access the device detailed information screen.
4. You can use the **Power/Menu** button to scroll down to view the rest screens.

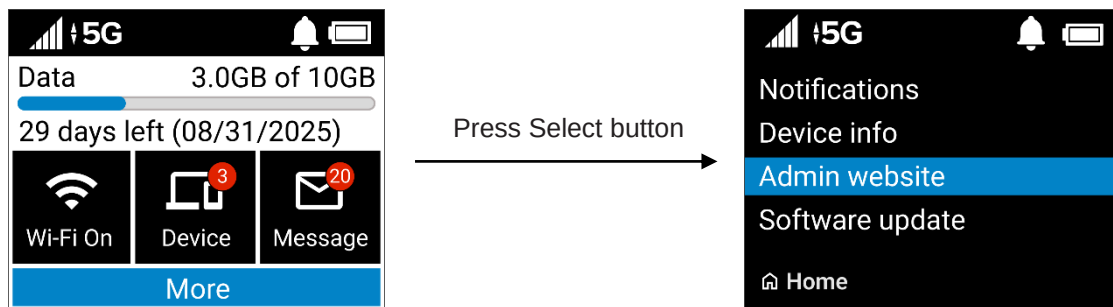


Admin website screen

Admin website screen shows the URL and login password of your mobile hotspot's Admin website where you can manage various settings of your mobile hotspot, including changing Wi-Fi network name or password, configuring your LAN and VPN control, Port forwarding, and more.

To access the **Admin website** screen, follow the below steps:

1. From the Home screen, use the **Power/Menu** button to highlight the **More** section.
2. Press **Select** button to access more menus.
3. Select **Admin website** to view URL and password of the admin website.

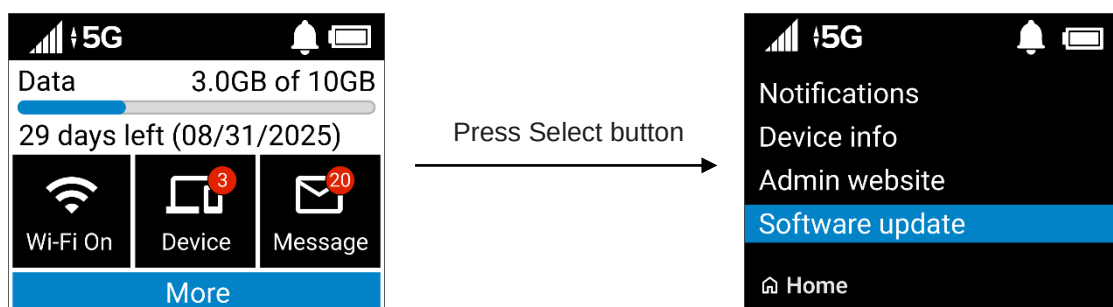


Software update screen

Software update screen allows you to check for the software update and always keep your mobile hotspot in the latest software version.

To access the **Software update** screen, follow the below steps:

1. From the Home screen, use the **Power/Menu** button to highlight the **More** section.
2. Press **Select** button to access more menus.
3. Select **Software update** to view the current software version. You can select **Check for update** button to check if the latest software version is available.



Internet access

Connect via Wi-Fi

You can simultaneously connect up to 16 devices, including smartphones, tablets, and laptops, to your mobile hotspot. Keep your mobile 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 computer, smartphone, tablet, or any Wi-Fi enabled device that you want to connect to your mobile hotspot.
2. Locate and select your mobile hotspot's Wi-Fi network name, which can be found on the Wi-Fi screen of your mobile hotspot.
3. Enter the Wi-Fi password shown on your mobile 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 mobile hotspot's Wi-Fi network name and password using the Admin website.

1. Open a web browser on a computer that is connected to your mobile hotspot via Wi-Fi or USB tethering.
2. Enter **https://my.mobilehotspot** or **https://192.168.1.1** in the address bar of the browser.
3. Enter your login password displayed on your mobile hotspot's Admin website screen (**Home screen > More > Admin website**).
4. Click **Log in** button.
5. Go to **Wi-Fi** page.
6. Enter your new network name or password.
7. Click **Save**.
8. The mobile hotspot will refresh with the updated Wi-Fi credentials.

Note: You will need to reconnect any connected Wi-Fi enabled devices to the mobile 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 5 GHz. To switch to the 2.4 GHz Wi-Fi network, go to your mobile hotspot's Wi-Fi screen (**Home screen > Wi-Fi > 2.4 GHz Band**).

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 mobile hotspot's Wi-Fi screen. You can hide them using the Admin website.

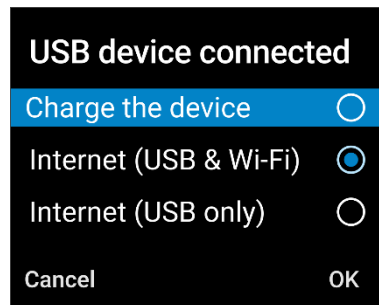
1. Log in to the Admin website.
2. Select **Wi-Fi** page.
3. Check the checkbox of **Hide network name on device** and **Hide password on device**.
4. Click **Save**.

Your mobile hotspot's Wi-Fi network and password will then be hidden on your mobile hotspot's Wi-Fi info screen.

Connect via USB Tethering

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

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



3. Select **OK** button to save. You now share your Mobile hotspot's network connection to your computer.

Admin website

Login

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

1. Open a web browser on a computer or Wi-Fi enabled device that is connected to the mobile hotspot's Wi-Fi network.
2. Enter **https://my.mobilehotspot** or **https://192.168.1.1** in the address bar of the browser..
3. Enter your login password displayed on your mobile hotspot's Admin website screen (**Home screen > More > Admin website**).
4. Click **Log In**.
5. You will need to change your password upon your initial login to the Admin website. You can change the password to something easy to remember.

Forgot login password

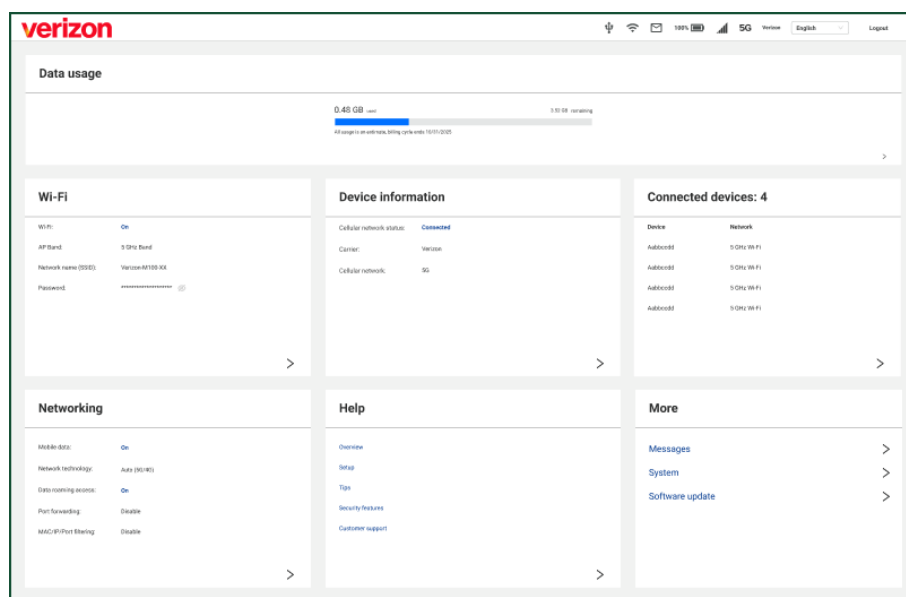
If you have changed the login and have forgotten the new one, you must restore the device to the factory default settings.

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

Homepage

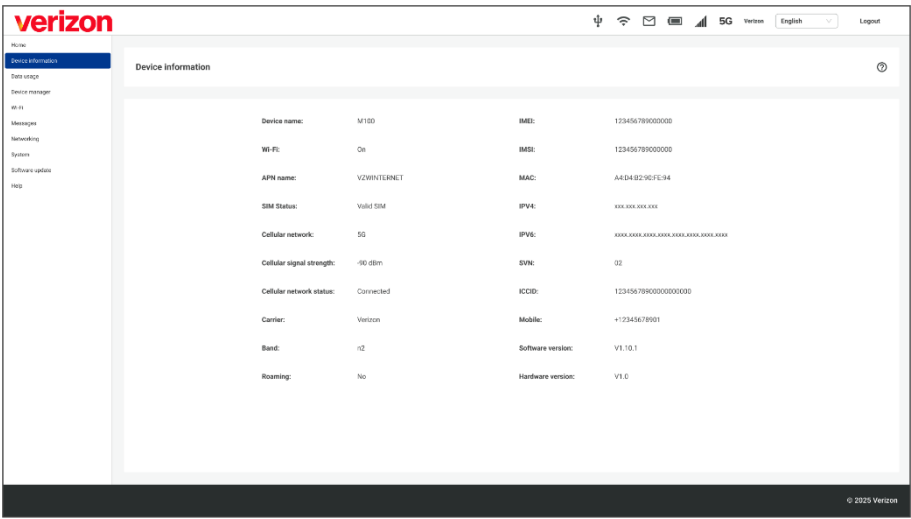
The home page serves as the central hub for you to access essential features and information related to the mobile hotspot. From this page, users can view data usage, Wi-Fi info, connected devices, networking options, and more.

You can click ➤ at the bottom right corner of each section to go to the corresponding page.



Device information

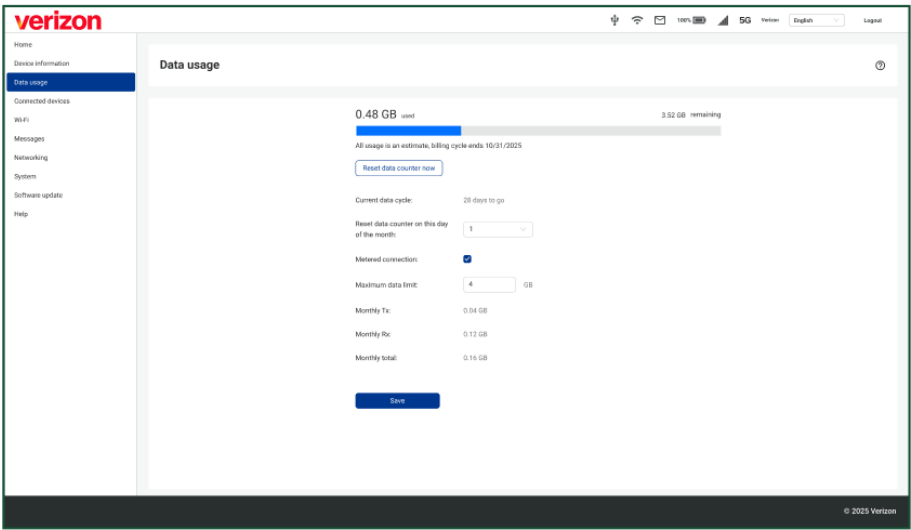
The Device information page displays an overview of your mobile hotspot's status such as network connection status, network type, signal strength, etc. You can also view device details such as IMEI, software version and the mobile number associated with your mobile hotspot.



Data usage

The Data usage page provides information about your mobile 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 carrier's data usage details. For accurate information, always check your carrier account.



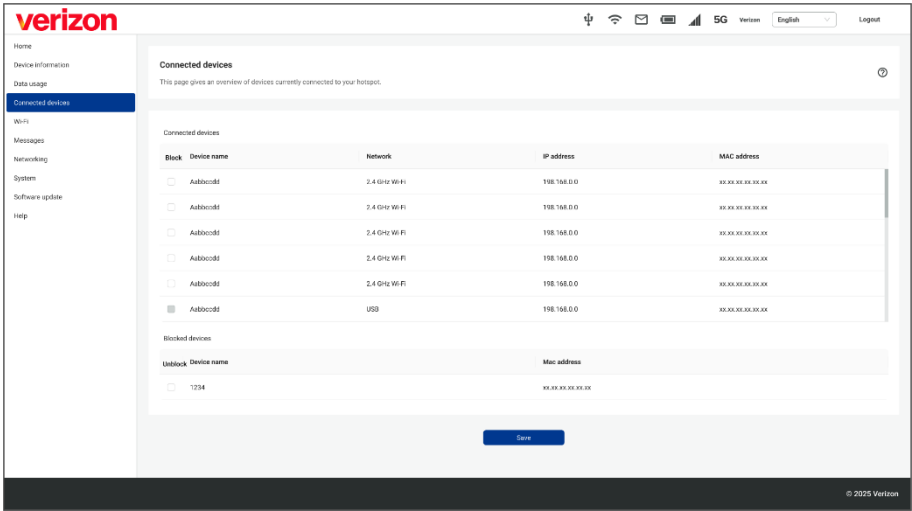
- Reset data counter now:** Set the data counter to 0 and update the reset date counter to today's date for this month.
- Current data cycle:** Display the number of days left in the current cycle.
- Reset date counter on this day of the month:** Set the start date for data usage.
- Metered connection:** Check this box if you wish to establish a data limit.
- Maximum data limit:** Set 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.

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.



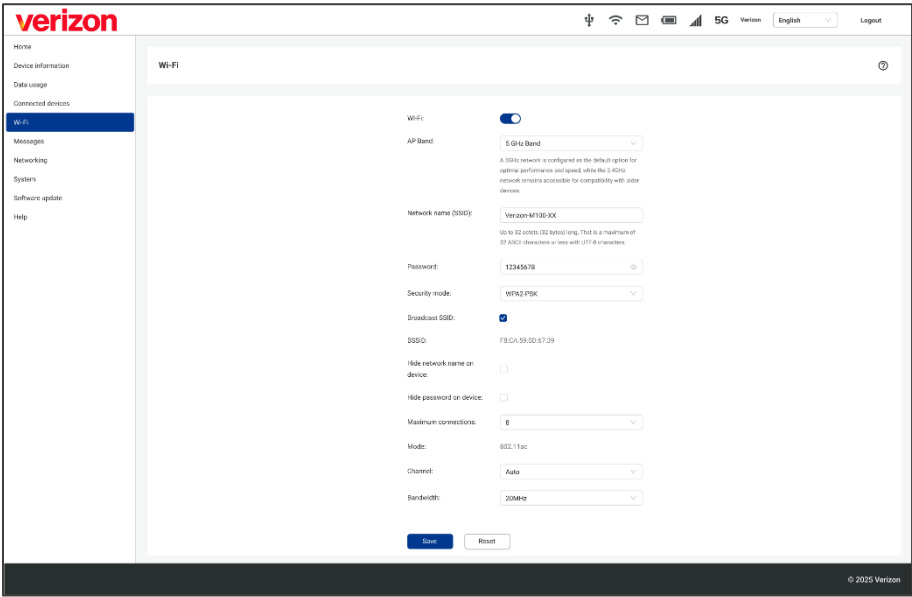
To block a device, select a device from your Connected devices list and click the **Save** button.

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



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

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

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, 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 mobile hotspot. To change your Wi-Fi password, 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 mobile hotspot for five (5) seconds. You may then log in using the default login password shown on your mobile hotspot's Wi-Fi details screen.

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.

Broadcast SSID: Check or uncheck the box to show or hide your mobile hotspot from being visible in the list of available Wi-Fi networks.

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

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

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

Maximum connections: Set the maximum number of devices that can connect simultaneously to the mobile hotspot's Wi-Fi network. The default maximum number of devices is set to 16 devices.

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

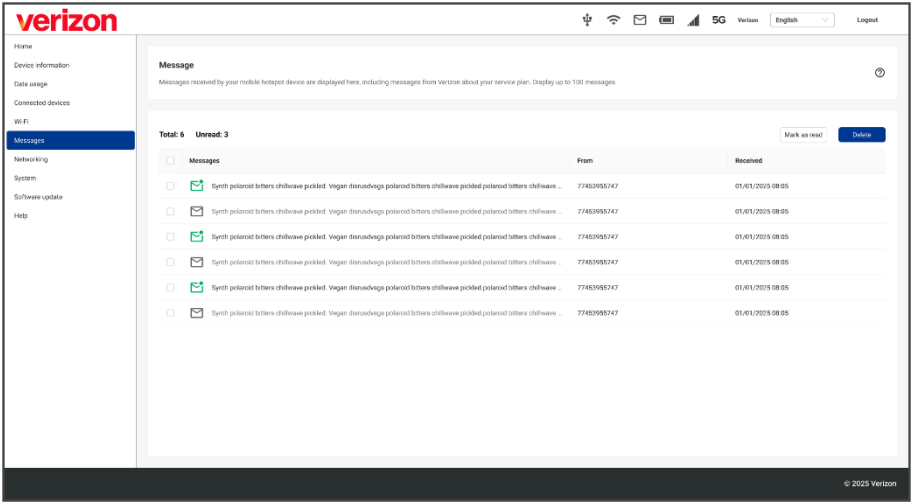
Channel: Shows the wireless channel that the radio is operating on. In most situations, leaving this as Automatic will work best, but you can manually change the channel selection using this option.

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 mobile hotspot. This may include messages from your carrier 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.

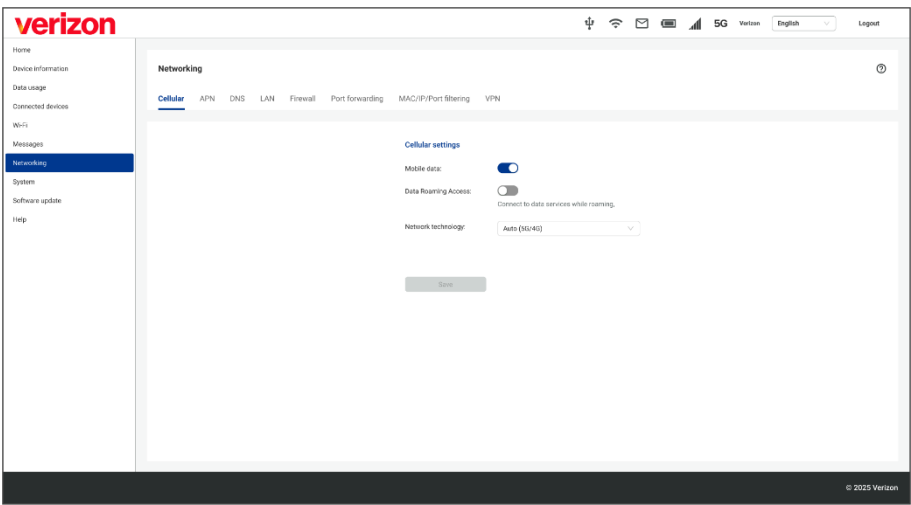


To manually delete messages, follow the below steps:

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

Networking

Cellular

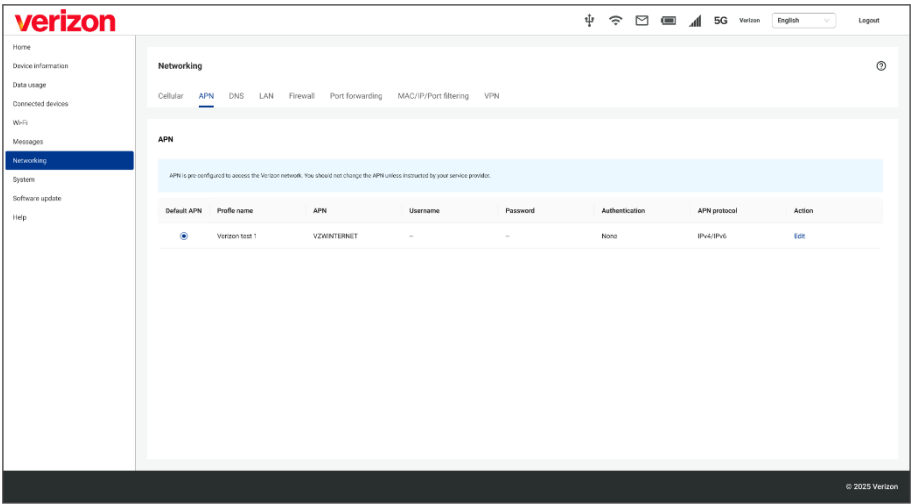


Mobile data: Enable or disable mobile data when necessary, preventing access to the mobile network. This will stop connected devices from using your mobile hotspot’s mobile data plan. By default, this setting should be enabled.

International roaming: Enable or disable international and domestic roaming as needed. Additional data charges may apply when roaming.

Network technology: Select the type of cellular data connection.

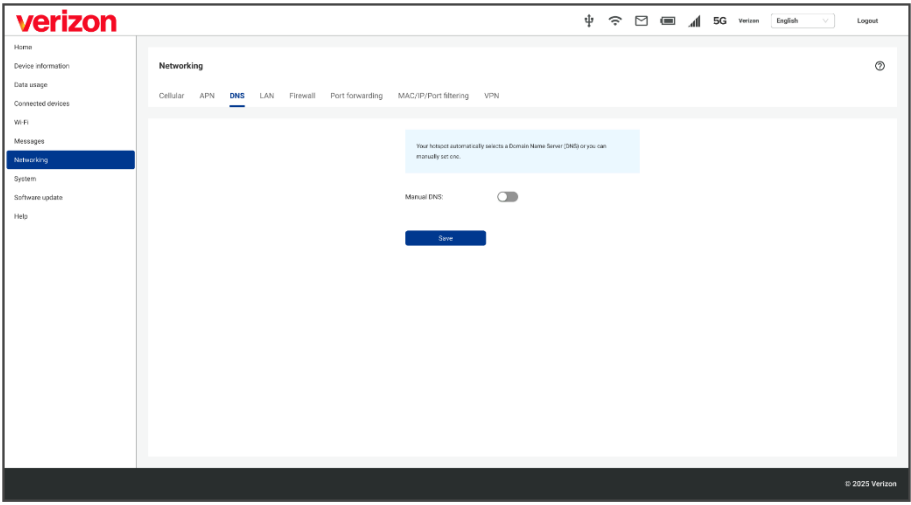
APN



APN is pre-configured to access the carrier network. You should not change the APN unless instructed by your service provider.

To edit the APN, click **Edit**.

DNS



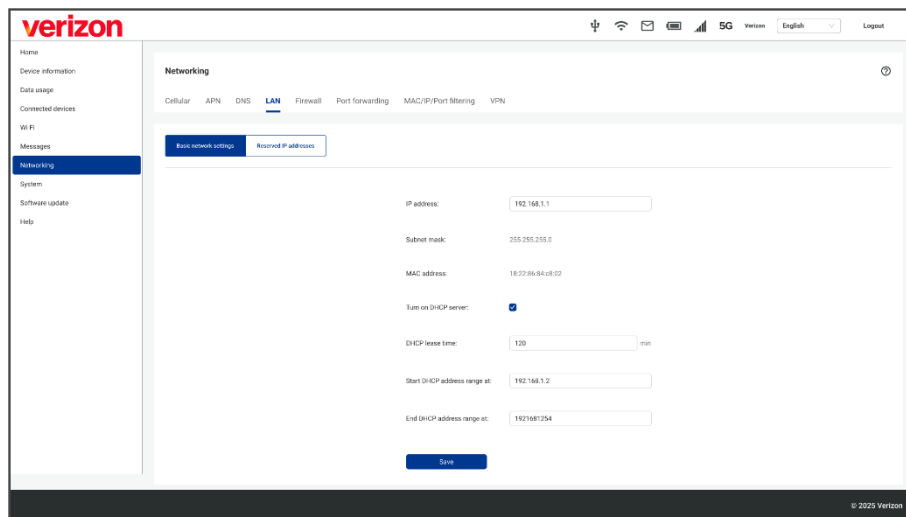
Normally, the DNS (Domain Name System) server address is assigned automatically. This page allows you to manually specify a DNS address if necessary.

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



Basic network settings

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

Turn on DHCP server: Enable the DHCP server to automatically assign IP addresses and network configurations to devices on your network. When it is disabled, all connected devices need to have a fixed IP address assigned on each device. Meanwhile, Reserved IP addresses tab will be greyed out.

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 mobile 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.

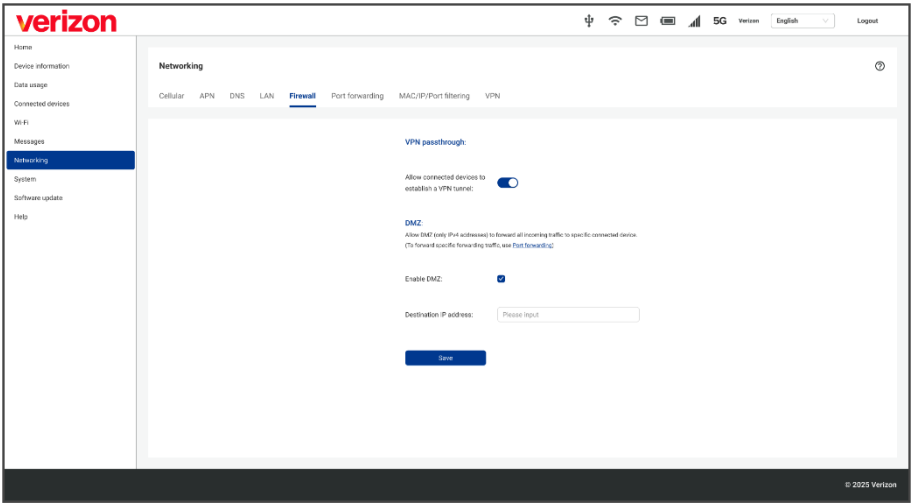
Reserved IP Addresses

Reserved IP Addresses are fixed addresses assigned to specific devices, ensuring consistent connectivity and simplifying network management while preventing address conflicts.

Click **Add** button to add a new reserved IP address.

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 mobile 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 built-in firewall. Therefore, this feature should be used with care.

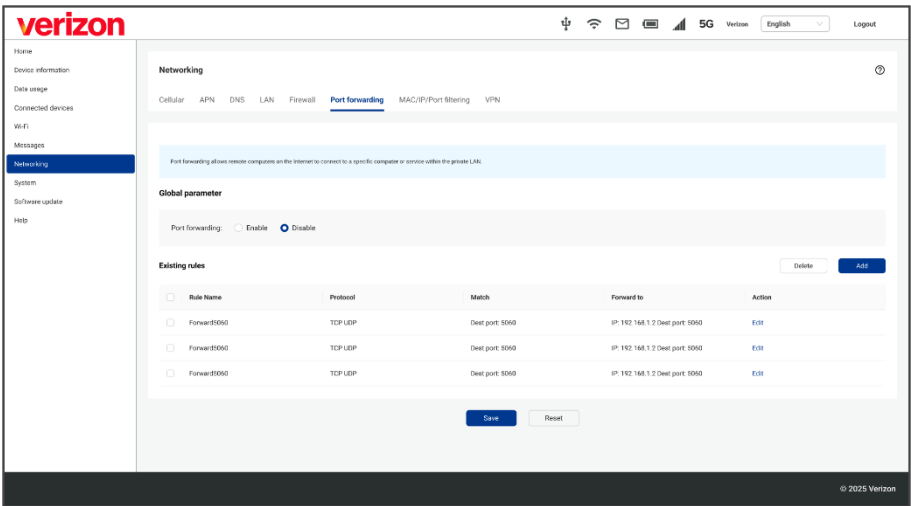
Enable DMZ: Enable or disable DMZ. If enabled, the connected device designated as the DMZ IP address (DMZ destination) will receive all traffic that would typically be blocked by the firewall.

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.



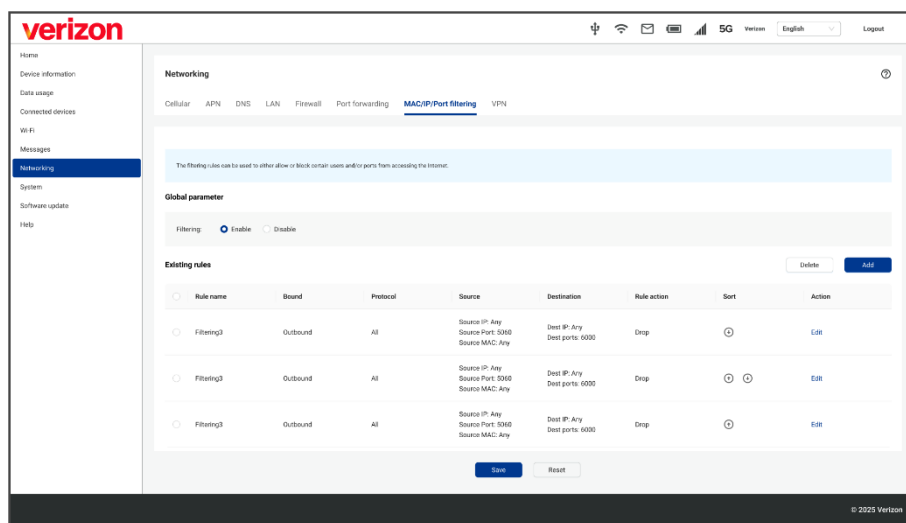
To create a new rule, click the **Add** button and enter the below required details:

- **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 or port range 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 or port range 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 or a range of ports. 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 or a range. Leaving this blank means the destination port check will be skipped.
- **Rule action:** Select **Drop**, **Accept**, or **Reject** to deny or allow the access to the Internet

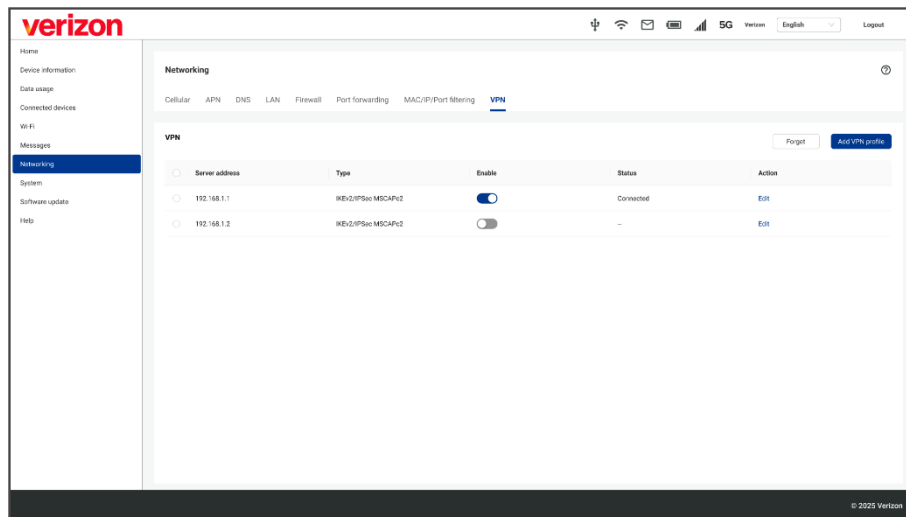
When finished, click the **Save** button.

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.



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

- **Type:** Show 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.
- **IPsec pre-shared key:** A unique secret key shared between devices in the IPsec protocol, used to authenticate and establish a secure connection for a VPN.
- **Enable:** Check this box to keep this function active at all times

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

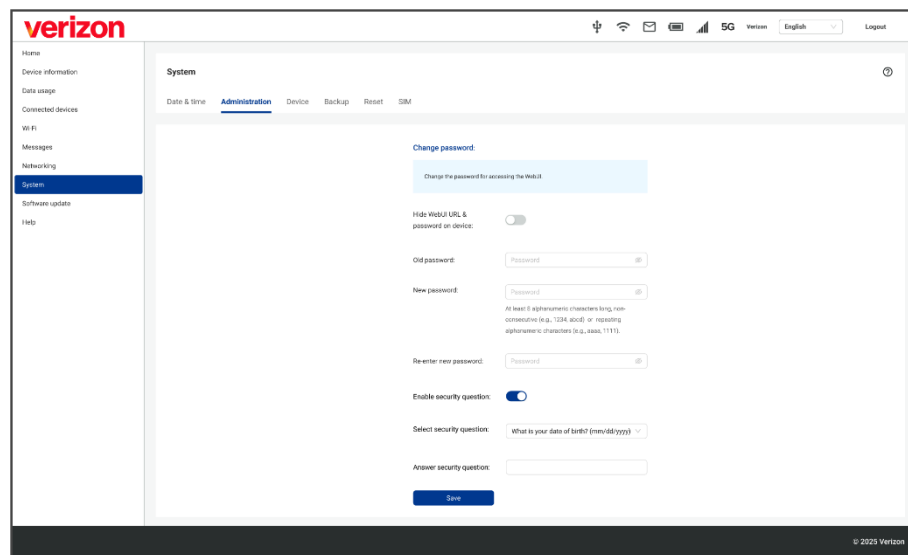
System

Date & time

View the date and time

Administration

Change the admin password for accessing your mobile hotspot's Admin website.



The screenshot shows the Verizon mobile hotspot administration interface. The top bar includes the Verizon logo, status icons (signal, Wi-Fi, battery, 5G), language (English), and a Logout button. A left sidebar lists navigation options: Home, Device information, Data usage, Connected devices, Wi-Fi, Messages, Networking, System (highlighted), Software update, and Help. The main content area is titled 'System' and has tabs for Date & time, Administration (selected), Device, Backup, Reset, and SIM. The 'Change password' section is active, displaying a blue header 'Change password:' and a sub-header 'Change the password for accessing the WebUI.' Below this is a toggle for 'Hide WebUI URL & password on device:' which is currently disabled. The form includes three password input fields: 'Old password:', 'New password:', and 'Re-enter new password:'. A note specifies password requirements: 'At least 8 alphanumeric characters long, non-consecutive (e.g., 1234abcd) or repeating alphanumeric characters (e.g., aaaa1111)'. There is also an 'Enable security question:' toggle (checked), a 'Select security question:' dropdown menu (showing 'What is your date of birth? (mm/dd/yyyy)'), and an 'Answer security question:' text input field. A blue 'Save' button is at the bottom. The footer shows '© 2023 Verizon'.

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

Old password: Enter the current password.

New password: Enter the new password.

Re-enter new password: Enter the new password again. The passwords entered must be identical, otherwise the password will not be updated.

Enable security question: Enable or disable security question. A security question adds an extra layer of protection for your account. It helps verify your identity if you forget your password or need to recover your account. Enabling this feature ensures you can securely regain access.

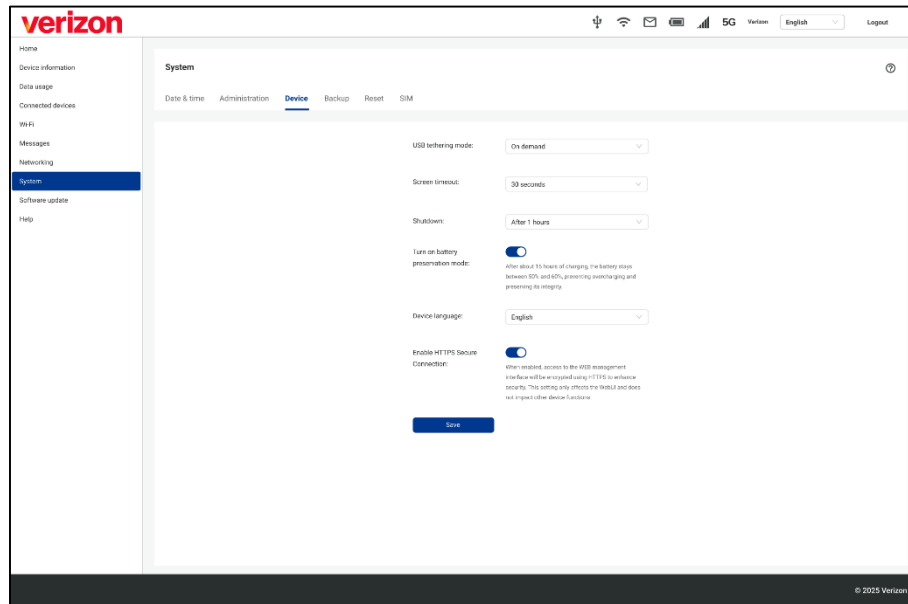
Select security question: Choose a question that will help verify your identity.

Answer security question: Provide a secure answer to the selected question.

To change the Admin website password, enter your current password, then your new password, and re-enter the new password for confirmation. If the security question is enabled, select the security question from the dropdown list and provide the answer. When done, click the **Save** button to apply the changes.

Device

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



USB tethering mode:

- **On-demand** is the default state. With this option selected, when your mobile hotspot is connected to a computer via the USB-C port, you will see the USB device connected popup window on your device screen for you to choose your desired connection mode, charge the device, Internet (USB & Wi-Fi), or Internet (USB only).
- **Always on** will enable USB tethering automatically when connected.
- **Disabled** will disable USB tethering when connected.

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

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

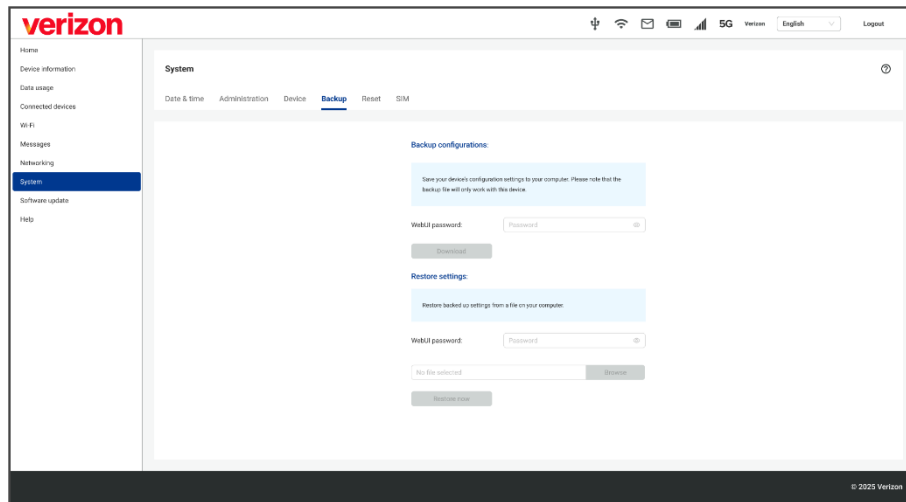
Turn on battery preservation mode: Battery Preservation Mode helps extend your battery life by maintaining the charge level between 50% and 60%. It is recommended that you enable this mode if you often charge your device for extended periods of time. When enabled, Battery Preservation Mode will activate after an extended period of continuous charging.

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

Enable HTTPS Secure Connection: When enabled, access to the WEB management interface will be encrypted using HTTPS to enhance security.

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

Admin password: Enter the current login password for the mobile hotspot's Admin website.

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 mobile hotspot, and settings can only be viewed or modified through the Admin website.

Restore settings

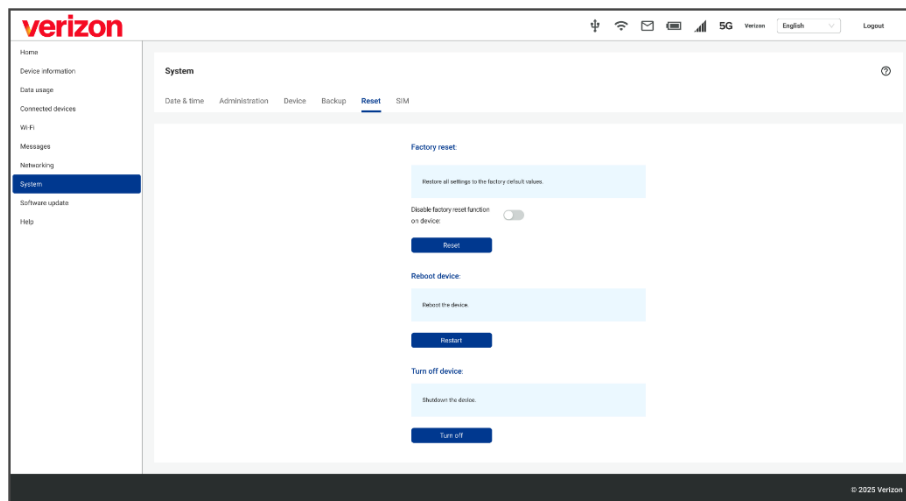
Admin password: Enter the current login password for the mobile hotspot's Admin website.

Browse: Click the **Browse** button to select the configuration file you previously downloaded from this mobile 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 mobile hotspot will restart.

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

Reset



Disable factory reset function on device: Prevents the device from being restored to its original factory settings via the factory reset hole located on the side of the device.

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 mobile hotspot, including your web browser session.

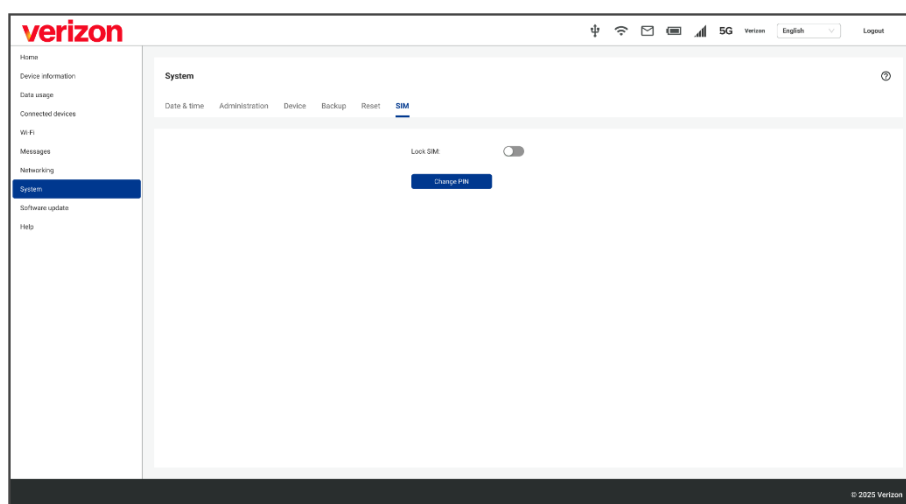
Note: Take care with using this feature as all settings and messages stored on the device will be lost when the device is factory reset.

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

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

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 mobile hotspot is powered on or the SIM card is inserted into a new device.



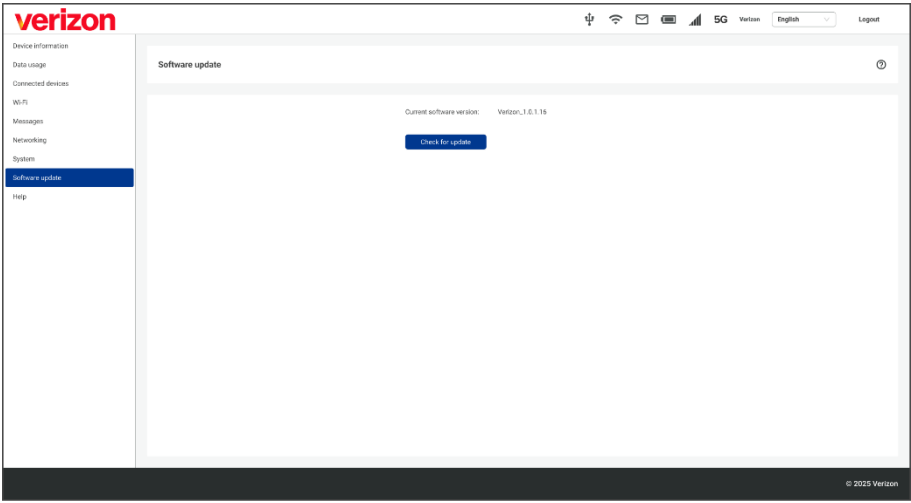
If the wrong PIN is entered three times, the SIM card will become locked, requiring a PUK (Personal Unblocking Key) code to unlock it. Entering the wrong PUK code 10 times will permanently lock the SIM card, making it unusable. If you require assistance, please reach out to your service provider.

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 mobile hotspot.

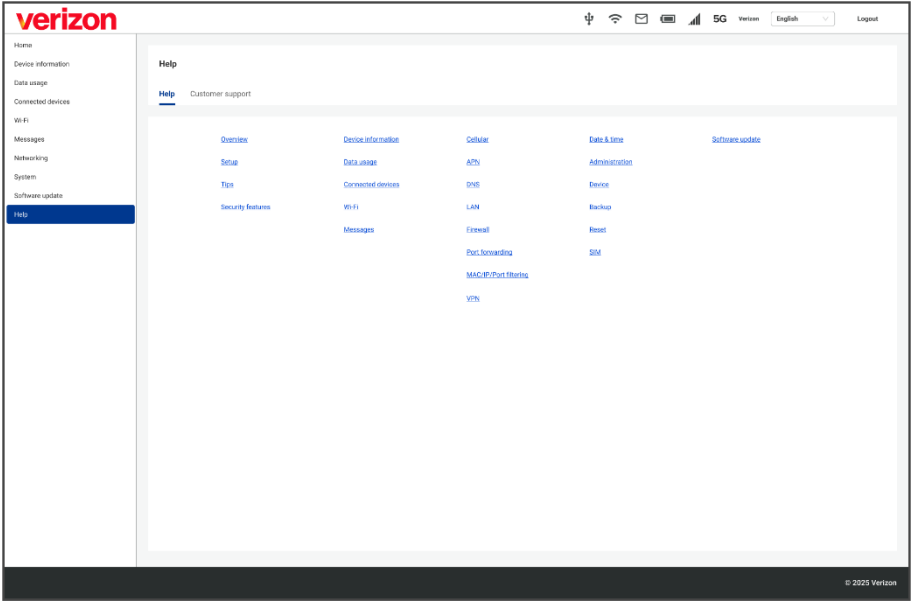
Check for update: Click the **Check for update** button to check for the latest software update.

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 Admin website and general topics useful for getting started with your mobile hotspot.

Use the **Customer support** tab for useful links and support information.



Troubleshooting

Below is a list of common problems that may occur when using your device. Try these easy troubleshooting steps to resolve any type of issues you may encounter.

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 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 mobile hotspot has network coverage in the area. - Make sure your SIM card is active and properly installed. - Check to see if Mobile data is enabled in the Admin website.
Download and/or upload speeds are slow	- Check the signal strength on your mobile hotspot's 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.
Forgot the password to the Wi-Fi network	The password to your Wi-Fi network can be easily found on the mobile hotspot's Wi-Fi screen.
Forgot the password to the Admin website	The default login information of the Admin website can be found on the Admin website screen of your device (Home screen > More > Admin website). 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 mobile hotspot for five (5) seconds. You may then log in using the default login password which can be found on your mobile hotspot's Admin website screen (Home screen > More > Admin website).
Can't access the Admin website	- Confirm that you are trying to access the Admin website from a device that is currently connected to your mobile hotspot via either a Wi-Fi or USB connection. - Confirm that you have entered the correct URL (https://my.mobilehotspot or https://192.168.1.1) 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 your mobile hotspot's Admin website screen (Home screen > More > Admin website).

Regulatory Information

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.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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 antenna, the lower the power output.

The highest SAR value for the mobile hotspot as reported to the FCC when worn on the body, is 1.26 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 mobile 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: YHLBLUM100.

For body worn operation, this mobile hotspot has been tested and meets the FCC RF exposure guidelines for use with an accessory that contains no metal and the positions the handset with a minimum of 10mm from the body. Use of other accessories may not ensure compliance with FCC RF exposure guidelines.

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 140°F (60°C). The operating temperature for the mobile hotspot is 14°F (-10°C) to 113°F (45°C).

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

To reduce 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.
- Only use the CTIA Certification certified adapters, products that bear the USB-IF logo or products that 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.
- 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.
- 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.
- 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 Battery NTC Pin.

If the battery leaks:

- Do not allow the leaking fluid to come in 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 in 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.

The information provided in this user manual is subject to change without notice and BLU Products reserves the right to modify the manual at any given time.

BLU Products has made every effort to ensure that this user manual is accurate and disclaims responsibility and liability for any inaccuracies or omissions. BLU Products makes no commitment to keep current the user manuals, however, does reserve the right to make improvements to the user manual at any given time without notice.