verizon

User Guide

jetpack®

4G LTE
Mobile Hotspot - MHS291L

5U000748C0A REV.00

BC

jetpack®

4G LTE
Mobile Hotspot - MHS291L

verizon

Guía del Usuario

PANTECH

User Manual

Thank you for purchasing the Verizon Jetpack® 4G LTE Mobile Hotspot MHS291L. The MHS291L is a Global Ready™ wireless device that provides high-speed wireless communication and easily connects at high speeds to the internet, your corporate Intranet, and your email while you're away from the office or out of the country.

The MHS291L is simple to use.

Table of Contents

HARDWARE

SOFTWARE

Getting Started

System Requirements

- Wi-Fi: Compatible with all major operating systems
- USB tethering: Compatible with Windows 8 (32-bit/64-bit), Windows 7 (32-bit/64-bit), Windows Vista SP2 (32-bit/64-bit), Windows XP SP3 32-bit
- Works with the latest versions of browsers, including Android™, Chrome™, Firefox®, Internet Explorer®, Safari™, Mobile Safari™, and Konqueror.

To use Wi-Fi mode, your computer or connected device needs Wi-Fi capability.

Note

- When multiple users are connected to the MHS291L, all of their data usage will be combined and applied to the data plan associated with this jetpack.
- USB 3.0 is not supported.

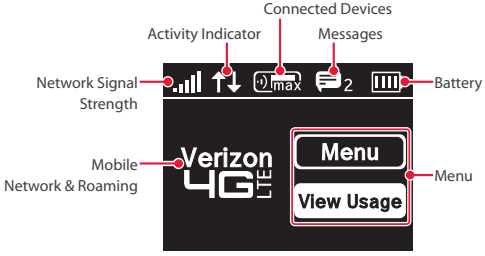
Components

Number	Description
1	**Red Lighting Effect** - Illuminates when the display is on.
2	**Home Screen** - Provides connection and battery status, network signal strength, roaming status, and the number of users connected with Wi-Fi.
3	**Scroll Up/Down**(▲/▼) - Scrolls up or down through the available menu options.
4	**OK Button**(OK) - Press to select a menu option.

Number	Description
5	**Power Button**( ) - Press and hold to turn the Jetpack on and off.
6	**External Antenna Adapter Port**( ) - Connects to an external antenna (sold separately) for improved signal reception under certain conditions.
7	**Micro USB Port** - Connects to the included USB cable for charging or tethering.

Display Icons

The icons on the LCD screen indicate the status of the Jetpack.



Display Icon	Description
	Network signal strength indicator.
	Indicates data is being transferred between the Verizon Wireless network and the Jetpack.
	Indicates the number of connected devices. When available connections are filled, MAX is displayed.
	Indicates the number of unread SMS messages. If no unread messages, this icon does not appear.
	Battery charge indicator.
	Indicates the current network connection and roaming status.
	Access to Jetpack settings and Data Usage.

Using Your Jetpack

About Broadband Networks

4G LTE

With Verizon 4G LTE, you can get the broadband-like speed you require to work efficiently outside the home or office. You can connect to the Internet, access your corporate intranet, check your email and download attachments at speeds that are up to 10 times faster than 3G*.

4G LTE Mobile Broadband*

- Download: typical download speeds of 5-12 Mbps.
- Upload: typical upload speeds of 2-5 Mbps.

3G Mobile Broadband with EVDO Rev. A**

- Download: typical download speeds of 600 kbps–1.4 Mbps with bursts up to 3.1 Mbps.
- Upload: typical upload speeds of 500-800 kbps with bursts up to 1.8 Mbps.

Wi-Fi 802.11 a/b/g/n

- 802.11a uses the 5 GHz frequency with Wi-Fi speeds of up to 54 Mbps.
- 802.11b uses the 2.4 GHz frequency with Wi-Fi speeds of up to 11 Mbps.
- 802.11g uses the 2.4 GHz frequency with Wi-Fi speeds of up to 54 Mbps.
- 802.11n uses the 2.4 GHz frequency with Wi-Fi speeds of up to 72 Mbps.
- 802.11n uses the 5 GHz frequency with Wi-Fi speeds of up to 150 Mbps.

* Speeds shown are those published by Verizon Wireless, Inc. and are theoretical in nature. Actual throughput speed and coverage may vary. Speed claims not applicable when roaming.

** Mobile Broadband Rev.A speed claim based on Verizon Wireless network tests with 5 MB FTP data files without compression.
Your Mobile Broadband Rev. A-enabled Jetpack will indicate coverage when you are in a Mobile Broadband Rev. A service area.
When outside the Rev. A service area, your wireless Jetpack will revert to Mobile Broadband Rev. 0 (typical download speeds will be 400–700 Kbps and upload speeds will be 60–80 Kbps).

Removing/Attaching the Back Cover

To remove the back cover on your Jetpack:

1. Rotate it to view the bottom side.
2. Place your fingernail in the cutout on the side of the Jetpack and pop the cover off.

To attach the back cover:

1. Replace the cover so the arrows on the Jetpack and inside of the cover face in the same direction.
2. Press down around the edges of the cover until it clicks into place and is flat across the entire bottom surface.

Installing/Removing the 4G LTE SIM Card

Your SIM (Subscriber Identity Module) Card is a small rectangular plastic card that stores your phone number and important information about your wireless service.
You can move the SIM Card from one device to another and your wireless service will work seamlessly as long as you have a compatible device and service plan. To see which devices are compatible with the Verizon Wireless SIM Card, visit verizonwireless.com/certifieddevice.

1. Remove the back cover and battery.
2. Position the SIM card ("SIM" is inscribed near the slot opening) with the Verizon logo facing up and the notched edge facing towards the center of the battery compartment. Slide the SIM card into the slot, insert the battery and attach the back cover. Then, close the back cover.

3. To remove the SIM card, turn off your Jetpack and remove the back cover. Remove the battery and gently slide the SIM card out. Gently pull the SIM card out to remove it.

Note

- Contact Verizon support if your SIM is lost or damaged.
- To insert/remove the SIM card, you should remove the battery.

Installing/Removing the Battery

1. Insert your fingernail into the slot at the left of the Jetpack and gently lift the back cover to remove.
2. Slide the battery into the slot by aligning the gold-colored contacts and press down until it clicks into place.

3. Replace the cover so the arrows on the Jetpack and cover face in the same direction.

4. Press down around the edges of the cover until it clicks into place and is flat across the entire bottom surface.
5. To remove the battery, turn off your Jetpack and remove the back cover.
6. Insert your fingernail into the slot and lift the battery from the compartment.

Charging the Battery

The Jetpack uses a Lithium Ion (Li-Ion) battery. Make sure to use the authorized battery and charger only.

1. Connect the USB cable with the Wall/USB Charger Adapter.

Note

Make sure to align the connector as indicated in the image. Otherwise, the charging connector may become damaged and the battery will not be charged.

2. Insert the micro USB end of the charging cable into the charging port.

3. Plug the other end of the wall charger into the appropriate electrical outlet. The battery starts charging.

4. Disconnect the charger when the battery is fully charged.

Battery Tips

Warning

Always use only approved batteries and chargers with your MHS291L. The warranty does not cover damage caused by non-approved batteries and/or chargers.

- It normally takes at least three hours to fully charge the battery with the wall charger.
- Do not use sharp objects to access the battery well, this may damage the Jetpack and the battery.
- Do not use excessive force to remove the battery or to access the battery well.
- The battery discharges more rapidly as additional devices connect to your Jetpack.
- Battery life depends on the network, signal strength, temperature, features, and accessories you use.
- New batteries or batteries stored for a long time may take more time to charge.
- When charging your battery, keep it near room temperature.

- When storing your battery, keep it uncharged in a cool, dark, dry place.
- Never expose batteries to temperatures below -22°F (-30°C) or above 140°F (60°C).
- Never leave the Jetpack in an unattended vehicle due to uncontrollable temperatures that may be outside the desired temperature for this Jetpack.
- Some batteries perform best after several full charge/discharge cycles.
- It is normal for batteries to gradually wear down and require longer charging time. If you notice a change in your battery life, it is probably time to purchase a new battery.

Important

Whenever you remove or insert either the battery or the SIM card, ensure your Jetpack is not connected to any device or power source.

Powering Your Jetpack On/Off

Power On

- Press and hold the Power Button until the display lights up.

Power Off

- Press and hold the Power Button until the display shows **Powering Off**. The Jetpack will continue its shutdown procedures for several seconds and then automatically turn off the display.

Power Management

Your Jetpack can operate with either its battery or external power source.

- **Battery Charge Indicator** - Charge the battery by plugging in the wall charger. While the battery is charging the battery icon bars blink with a lightning bolt. Four battery bars indicate that the battery is fully charged.
- **USB wall charger** - You can use the Jetpack when the charger is plugged into a wall socket.
  Please ensure the wall socket is located near the equipment and is easily accessible. The battery charges while it is plugged into the charger.

Before using the Jetpack, read the battery safety information. (See ***Battery Tips*** on page 15.)

Activating Your Jetpack

If the device has not been activated yet, follow the instructions below.

- Depending on your account status or how and where you purchased your device, it may be ready to use or may need to be activated on your Verizon Wireless account.
- If you purchased your device at a Verizon Wireless Store, it is likely activated and ready to use.
- If you received your device in the mail, you can activate it by clicking **My Jetpack Home** > **My Verizon Wireless** after connecting to Verizon Wireless Web Based User Interface. See ***Start the Verizon Wireless Web based User Interface*** on page 30

Connecting to Your Jetpack

To connect with your Jetpack using Wi-Fi, your computer, tablet, or other Wi-Fi enabled devices need Wi-Fi capability. Your default Wi-Fi Name (SSID) and Wi-Fi Password can be found on the display upon initial power up and within your Jetpacks **Menu** > **Wi-Fi Name/ Password** option at anytime.

1. Turn on your computer and Jetpack.
2. On your computer, use the Wi-Fi manager (Windows OS) or AirPort menu bar icon (Max OS) to connect to the wireless network named Verizon-291LVW-XXXX.

Tip!

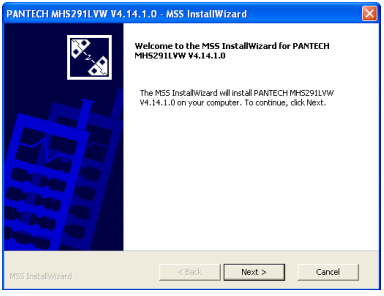
The steps to connect to a Wi-Fi network vary depending on your operating system and whether you use the native application or third-party software. Generally, you click an icon in the Windows notification area where you can select **View Available Wireless Networks**, or click the Airport icon in the menu bar on a Mac. If you are unfamiliar with wireless networking on your computer, consult your computer's or network administrator help system.

3. Connect to network name shown on Jetpack display under **Menu** > **Wi-Fi Name/Password**. The network name or SSID is in the format Verizon-291LVW-XXXX, where XXXX are four digits unique to your device.
4. Enter the 8-digit Wi-Fi password.
5. You can change device settings by connecting to http://my.jetpack and Signing In with the default **Wi-Fi/Admin password**. (See ***Jetpack Settings*** on page 34)

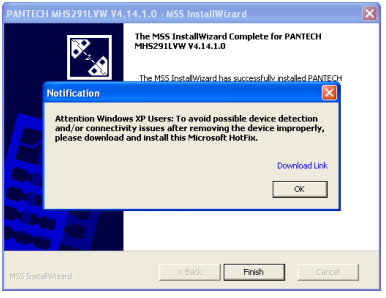
Installing USB Driver for USB Tethering

You can connect the Jetpack to your computer via USB tethering and connect to the internet. It recommended using USB 2.0 ports but if your computer only has USB 3.0 ports, try to update the USB 3.0 host controller driver. If your computer has a mix of USB 2.0 and USB 3.0 ports, you can identify USB 3.0 ports by color. On many newer systems, a USB 3.0 port may be identified by having blue plastic components.

1. Turn on your computer.
2. Plug the USB cable into the Jetpack's micro USB port. Then insert the USB cable into your computer's USB port.
3. The install wizard screen will appear automatically. If your computer won't recognize the Jetpack, select **My Computer** > **Verizon Mobile** > **Windows**, and then double-click the driver file.
4. To continue with installation, click **Next** > **Install**. Setup may take a few minutes.



5. If prompted during the installation to install the Windows XP Hotfix, you can choose whether or not to install this fix. It is recommended that you should install the Windows Hotfix.
6. When the prompt appears, leave the installation manager open, use the Wi-Fi manager(Windows OS) to connect to the wireless network.
7. Connect to network name shown on Jetpack display under **Menu** > **Wi-Fi Name/Password**. The network name or SSID is in the format Verizon-291LVW-XXXX, where XXXX are four digits unique to your device.
8. Enter the 8-digit Wi-Fi password.
9. Return to the installation manager. Now click **Download Link** in the prompt and install the Windows Hotfix.



10. Follow the onscreen instructions. When complete, click **OK** on the prompt. Then click **Finish** to complete the installation.

HARDWARE

Settings

Settings

You can configure the settings on your Jetpack using the scroll up/down and OK button. Select the desired menu by pressing (WPS) or (▼) and press (OK). When you have finished settings, select **Close** and press (OK). And, you can go to the Home screen directly by pressing and holding (OK).

Wi-Fi Name/Password

1. From the Home screen, select **Menu** > **Wi-Fi Name/Password** and press (OK).
2. You can see the current Wi-Fi information about the Jetpack.
3. If you select **Setting** at bottom of screen, you can change Wi-Fi band. See ***Wi-Fi Band Select*** on page 25.

Connected Devices

1. From the Home screen, select **Menu** > **Connected Devices** and press (OK).
2. Select device name and press (OK).
3. You can disconnect the device by selecting **Disconnect** and pressing (OK).

Messages

1. From the Home screen, select **Menu** > **Messages** and press (OK).
2. Select a message and press (OK).
3. You can delete a message by selecting **Delete** and pressing (OK).

Network Settings

1. From the Home screen, select **Menu** > **Network Settings** and press (OK).
2. You can change the network type by selecting **Global Mode**, **LTE/CDMA Mode** or **GSM/UMTS Mode** and pressing (OK).

Wi-Fi Settings

Start WPS

WPS (Wi-Fi Protected Setup) provides an easy procedure to make wireless connections between the Jetpack and a wireless device with the encryption of either WPA or WPA2.

1. From the Home screen, select **Menu** and press (OK).
2. Select **Wi-Fi Settings** > **Start WPS** and press (OK). You can also start the WPS mode by pressing and holding (WPS).
3. Press the WPS button on your Wi-Fi device within 2 minutes to set up a connection.

Wi-Fi Band Select

Wi-Fi uses unlicensed wireless spectrum that can be subject to interference and degraded performance as the 2.4 GHz band becomes saturated with Wi-Fi networks, Bluetooth, cordless phones, microwaves and other wireless devices use those frequencies. If your Wi-Fi client device(s) can take advantage of 5 GHz Wi-Fi networks, you may want to consider configuring the Jetpack device to broadcast Wi-Fi on 5 GHz instead of at 2.4 GHz.

1. From the Home screen, select **Menu** and press (OK).
2. Select **Wi-Fi Settings** > **Wi-Fi Band Select** and press (OK).
3. You can change Wi-Fi band by selecting **2.4GHz** or **5.0GHz** and pressing (OK).

Note

You can use only one Wi-Fi band at a time on the MHS291L.

Wi-Fi Network Mode

Some older Wi-Fi devices may experience connectivity issues with Wi-Fi networks that broadcast multiple modes. If your Wi-Fi devices are unable to connect to the Jetpack device's Wi-Fi network, you may want to change the Wi-Fi network technology used by your Jetpack device to one that is supported by your Wi-Fi client device.

1. From the Home screen, select **Menu** and press (OK).
2. Select **Wi-Fi Settings** > **Wi-Fi Network Mode** and press (OK).
3. You can change Wi-Fi network mode by selecting **802.11b+802.11g+802.11n**, **802.11b+802.11g**, **802.11b only**, or **802.11g only**, and pressing (OK).

Broadcast SSID

If you want networking devices to be able to detect your Jetpack Wi-Fi network performing a site scan, turn on Broadcast SSID.

1. From the Home screen, select **Menu** and press (OK).
2. Select **Wi-Fi Settings** > **Broadcast SSID** and press (OK).
3. You can set Broadcast SSID by selecting **On** or **Off** and pressing (OK).

AP Isolation

AP (Access Point) isolation is a technique for preventing mobile devices connected to an AP from communicating directly with each other. If the access point will be used in a public place where you do not want wireless clients to be able to share files, turn on AP Isolation.

1. From the Home screen, select **Menu** and press (OK).
2. Select **Wi-Fi Settings** > **AP Isolation** and press (OK).
3. You can set AP Isolation by selecting **On** or **Off** and pressing (OK).

Wi-Fi On/Off

You can turn Wi-Fi on or off.

1. From the Home screen, select **Menu** and press (OK).
2. Select **Wi-Fi Settings** > **Wi-Fi On/Off** and press (OK).
3. You can turn Wi-Fi on or off by selecting **On** or **Off** and pressing (OK).

Max Connections

1. From the Home screen, select **Menu** and press (OK).
2. Select **Wi-Fi Settings** > **Max Connections** and press (OK).
3. You can set maximum number of devices (up to 10) that can be connected.

Note
When you are using 3G networks, up to 5 devices can be connected.

Software Update

Software Check

The Check for Update menu allows you to update software.

1. From the Home screen, select **Menu** and press (OK).
2. Select **Software Update** > **Software Check** and press (OK).
3. Select **Check Now** and press (OK).
4. Follow the steps to update.

Factory Reset

1. From the Home screen, select **Menu** and press (OK).
2. Select **Software Update** > **Factory reset** and press (OK).
3. Select **Yes** and press (OK).
4. The Jetpack will restart automatically.

Note
You can disable the Factory reset by using Jetpack settings. See ***Backup and Restore*** on page 37.

About Jetpack

Jetpack Info

1. From the Home screen, select **Menu** and press (OK).
2. Select **About Jetpack** > **Jetpack Info** and press (OK).
3. You can see detailed information about the Jetpack.

Note
You can change the admin password. See ***Jetpack Admin Password*** on page 34.

Data Usage

1. From the Home screen, select **View Usage** and pres (OK). You can also select **Menu** > **About Jetpack** > **Data Usage** and press (OK).
2. You can see the usage history details. When you select the **Refresh**, the usage history will be updated accordingly.

SOFTWARE

Start the Verizon Wireless Web based User Interface

Jetpack Settings

Messages

About Jetpack

Start the Verizon Wireless Web based User Interface

You can configure the Wi-Fi settings by visiting http://my.jetpack from your browser.

1. Turn on your computer/tablet and turn on the Jetpack.
2. On your computer, use the Wi-Fi manager (Windows) or the AirPort menu bar icon (Mac) to connect wirelessly to the Jetpack wireless network.

   Note

   The steps to connect to a Wi-Fi network vary depending on your operating system and whether you use the native application or third-party software. Generally, you click an icon in the Windows notification area where you can select **View Available Wireless Networks**, or click the Airport icon in the menu bar on a Mac. If you are unfamiliar with wireless networking on your computer, consult the computer help system.
3. Connect to network name shown on Jetpack display under **Menu** > **Wi-Fi Name/Password**. From your device the network name or SSID is in the format Verizon-291LVW-XXXX, where XXXX are four digits unique to your device.
4. Enter the 8-digit Wi-Fi password. The password appears under **Menu** > **Wi-Fi Name/Password**.
5. Open the web browser on your computer. To start the Verizon Wireless Web based User Interface, enter http://my.jetpack in the browser's address line then press **Enter** key.

6. Type your Wi-Fi/Admin password in the Sign In field in the upper right corner of the window and click **Sign In**.

My Jetpack Home

My Jetpack Home is your gateway to configuring and managing your Jetpack.

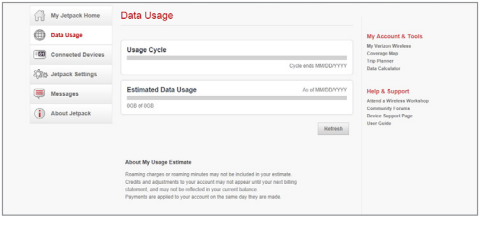
1. Click **My Jetpack Home**.

2. You can see the current status information.

Data Usage

The Data Usage page allows you to obtain data usage and billing cycle information for your mobile broadband plan. Click Data Usage on the Menu panel to display the Data Usage page and access information specific to your particular plan. You can also access and manage your account by clicking on My Verizon.

1. Click **Data Usage**.

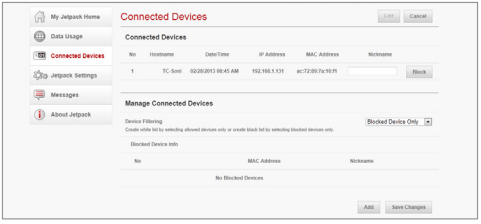


2. You can review your usage history.

Connected Devices

You can view, edit, or block Wi-Fi devices currently connected to your Jetpack, as well as any currently blocked devices.

1. Click **Connected Devices**.



2. Click **Edit** and adjust settings for connected devices.
   - Enter the nickname of a device in the **Nickname** field.
   - To add a device to **Blocked Device Info**, select **Blocked Device Only** from **Device Filtering** drop-down list, Then click **Block** next to **Nickname** field. You can also block a device by click **Add** and enter the MAC Address.
   - To delete a device from **Blocked Device Info**, select **Blocked Device Only** from **Device Filtering** drop-down list. Then click **Allow** next to nickname.
   - To add a device to **Allowed Device Info**, select **Allowed Device Only** from **Device Filtering** drop-down list. Then click **Allow** next to **Nickname** field. You can also allow a device by click **Add** and enter the MAC Address.
   - To delete a device from **Allowed Device Info**, select **Allowed Device Only** from **Device Filtering** drop-down list. Then click **Delete** next to nickname.
3. Click **Save Changes**.

Jetpack Settings

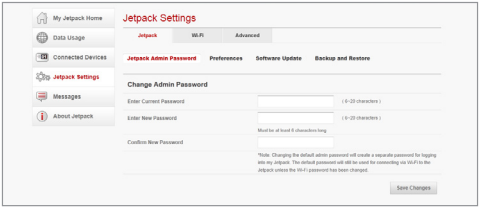
The Jetpack settings page allows you to make Jetpack changes, select mobile network options, update software, and backup and restore files to your Jetpack.

Jetpack

Jetpack Admin Password

The Jetpack Admin Password page allows you to display, hide and/or change the Admin Password.

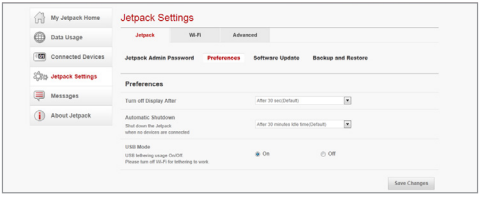
1. Click **Jetpack Settings** > **Jetpack** > **Jetpack Admin Password**.



2. Enter your password in the **Enter Current Password** field.
3. Enter the new password in the **Enter New Password** field. Then enter the new password again in the **Confirm New Password** field.
4. Click **Save Changes**.

Preferences

1. Click **Jetpack Settings** > **Jetpack** > **Preferences**.



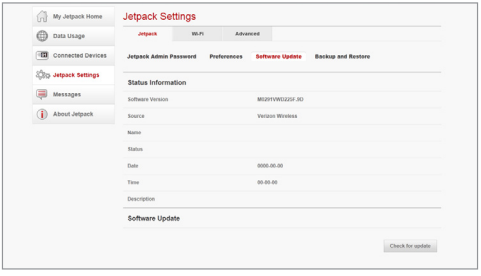
2. Adjust settings.
   - **Turn off Display After**: Select the amount of time that expires before the display turns off.
   - **Automatic Shutdown**: Select the amount of time that expires before the device automatically shuts down.
   - **USB Mode**: Turns the USB tethered mode on or off.
3. Click **Save Changes**.

Note

If you using the USB mode, you should turn off Wi-Fi in your computer.

Software Update

1. Click **Jetpack Settings** > **Jetpack** > **Software Updates**.

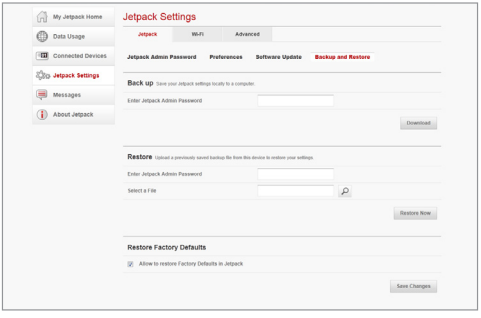


2. Click **Check for update** to check for new software updates and follow the instructions.

Backup and Restore

The backup and restore feature allows you to make a copy of the configuration settings from Jetpack to a file on your computer, and restore (upload) a previously-saved configuration file.

1. Click **Jetpack Settings** > **Jetpack** > **Backup and Restore**.

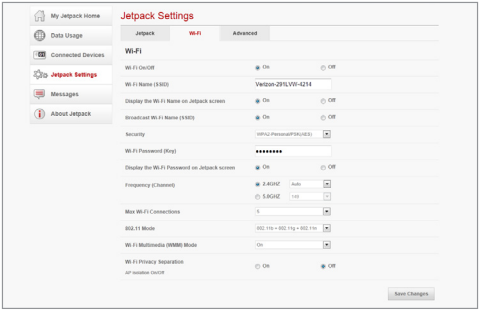


2. To download(backup) the settings file to your computer, enter your administration password in the **Enter Jetpack Admin Password** field in the **Back up** section and click **Download**. Then click **Save** in the File Download pop-up screen to save the settings file to a specified location on your computer.
3. To restore a setting file from your PC, enter your administration password in the **Enter Jetpack Admin Password** field in the **Restore** section and click and select the file you want to restore. Then click **Restore Now**.
4. If you want to enables the factory reset feature, click the checkbox next to **Allow to restore Factory Defaults in Jetpack**.
5. Click **Save Changes**.

Wi-Fi

The Wi-Fi menu allows you to customize the Wi-Fi profiles and view details about the devices connected to your Jetpack.

1. Click **Jetpack Settings** > **Wi-Fi**.



2. Adjust settings for Wi-Fi.
   - **Wi-Fi On/Off**: Turn Wi-Fi on or off.
   - **Wi-Fi Name (SSID)**: Enter the network name of the Jetpack.
   - **Display the Wi-Fi Name on Jetpack screen**: Displays the current Wi-Fi name.
   - **Broadcast Network Name (SSID)**: Broadcasts Network Name (SSID).
   - **Security**: Select the security type used to encrypt the wireless network.
   - **Wi-Fi Password (Key)**: Enter the new password of the Wi-Fi connection.

- **Display the Wi-Fi Password on Jetpack screen**: Displays the current Wi-Fi password.
- **Frequency (Channel)**: Select the frequency and channel. If channel setting is available, select **Auto**. If **Auto** is not available, you can experiment to see which channel provides the best results, or use the default settings.
- **Max Wi-Fi Connections**: Select the maximum number of devices that can be connected.
- **802.11 Mode**: Select the wireless network technology used. **802.11b** + **802.11g** + **802.11n** is most compatible, allowing 802.11b, 802.11g, and 802.11n devices to connect to the wireless network.
- **Wi-Fi Multimedia (WMM) Mode**: Wi-Fi Multimedia (WMM) is a Quality of Service (QoS) feature that prioritizes wireless data packets. If this is **On**, the Jetpack optimizes the way shared network resources are allocated among different applications.
- **Wi-Fi Privacy Separation**: Turn the privacy separation on or off.

3. Click **Save Changes**.

Advanced

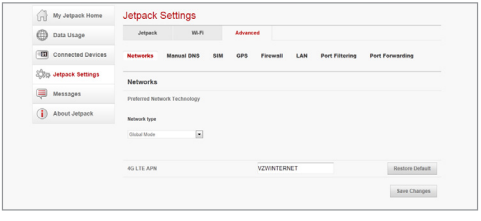
The Advanced page allows you to change advanced settings. The Advanced page provides network, manual DNS, SIM, firewall and LAN settings; and options for configuring port filtering applications.

Important

Changing advanced settings can adversely affect stability, performance and security.

Networks

1. Click **Jetpack Settings** > **Advanced** > **Networks**.



2. Adjust settings.
   - **Network Type**: Select the preferred network type to change the type of technology you want to use to connect to the internet.
   - **4G LTE APN**: Enter a new APN (Access Point Name). If you want to reset back to default APN, click **Restore Default**.
3. Click **Save Changes**.

Network Selection

Automatic Selection

1. Click **Jetpack Settings** > **Advanced** > **Networks**.
2. Select **GSM/UMTS Mode** from **Network Type** drop-down list.
3. Select the network subtype from **Sub type** drop-down list. You can select **GSM/UMTS Dual**, **GSM only**, or **UMTS only**.
4. Select **Automatic** from **Network Selection** drop-down list.
5. Click **Save Changes**.

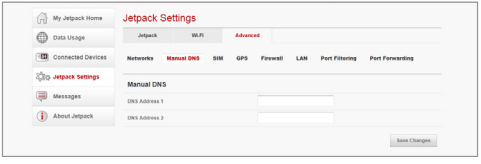
Manual Selection

1. Click **Jetpack Settings** > **Advanced** > **Networks**.
2. Select **GSM/UMTS Mode** from **Network Type** drop-down list.
3. Select the network subtype from **Sub type** drop-down list. You can select **GSM/UMTS Dual**, **GSM only**, or **UMTS only**.
4. Select **Manual** from **Network Selection** drop-down list.
5. Click **Save Changes**.
6. Click **select** next to a desired network.

Manual DNS

The Jetpack automatically selects a Domain Name Server (DNS). The Manual DNS menu allows you to manually select up to two DNS IP addresses.

1. Click **Jetpack Settings** > **Advanced** > **Manual DNS**.

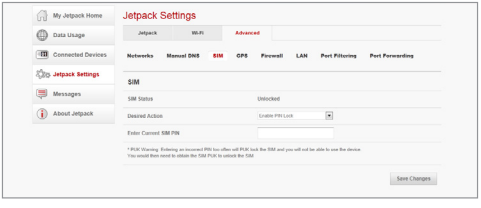


2. Enter the DNS address.
3. Click **Save Changes**.

SIM

The SIM menu gives you settings and information about the SIM card. The SIM card can be locked with a PIN code for additional security. If locked, the PIN code must be entered before the Jetpack can connect to the Internet. The SIM menu takes you to the SIM page.

1. Click **Jetpack Settings** > **Advanced** > **SIM**.



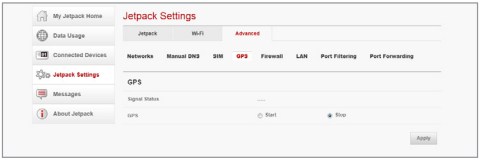
2. To lock the SIM card, select **Turn on PIN Lock** from **Desired Action** drop-down list. Enter the PIN code in the **Enter Current SIM PIN** field.
3. Click **Save Changes**.

Important

- Entering an incorrect PIN will lock the SIM.
- If you enter the wrong PUK (PIN Unlock Key) code 10 times in a row, your SIM card will be locked and will display an error message. If you see this error, please contact your wireless service provider to obtain another SIM card.

GPS

1. Click **Jetpack Settings** > **Advanced** > **GPS**.

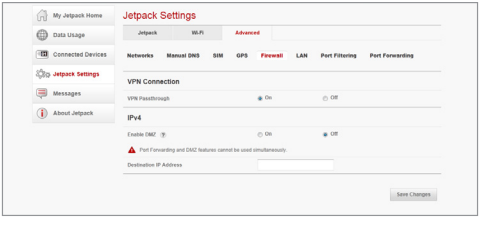


2. To enable the GPS, click **Start** > **Apply**.
3. Click **Yes** to accept the notification.

Firewall

The Jetpack firewall determines which Internet traffic is allowed.

1. Click **Jetpack Settings** > **Advanced** > **Firewall**.



2. Adjust settings.
   - **VPN Passthrough**: If this is **On**, this feature allows VPN clients to connect through the Jetpack to remote VPN servers. If this is **Off**, VPN clients will not be allowed to connect.

- **Enable DMZ**: Turns the DMZ feature on or off. If this is **On**, DMZ feature allows all unknown traffic to be sent to a designated IP address.
- **Destination IP Address**: Enter the IP address for the DMZ feature.

3. Click **Save Changes**.

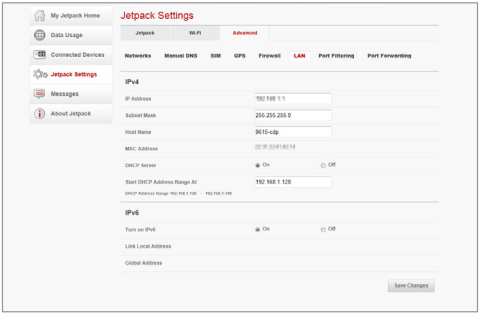
Note

The **Port Forwarding** and DMZ features cannot be used simultaneously.

LAN

The LAN page gives you settings and information about the Jetpack's network.

1. Click **Jetpack Settings** > **Advanced** > **LAN**.

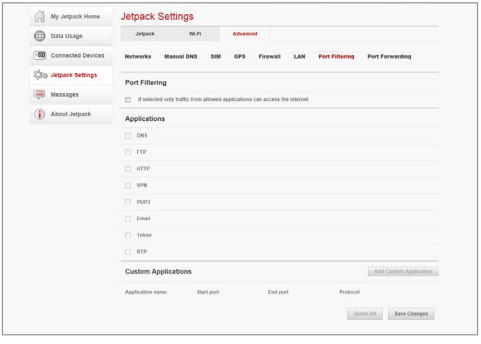


2. Adjust settings.
   - **IP Address**: Enter the IP address for the Jetpack.
   - **Subnet Mask**: Enter the subnet mask address for the Jetpack. The default value 255.255.255.0 is standard for small networks. If you change the **IP Address**, ensure you use the current subnet mask for IP address range.
   - **Host Name**: Enter the network name for connected device.
   - **MAC Address**: Displays the MAC(Media Access Controller) or physical IP address for the Jetpack.
   - **DHCP Server**: Turns the DHCP server on or off.
   - **Start DHCP Address Range At**: Enter the start range of IP address reserved for use by DHCP server table of the Jetpack.
   - **DHCP Address Range**: Displays the current range of IP address reserved for use by DHCP server table of the Jetpack.
   - **Turn on IPv6**: Turns the IPv6 on or off.
   - **Link Local Address**: Displays the local address when IPv6 is enabled.
   - **Global Address**: Displays the global address when IPv6 is enabled.
3. Click **Save Changes**.

Port Filtering

Port Filtering allows you to block outgoing Internet connections and permit only allowed applications to access the Internet. You can also customize a list of allowed applications which permits only certain programs to connect to the Internet.

1. Click **Jetpack Settings** > **Advanced** > **Port Filtering**.

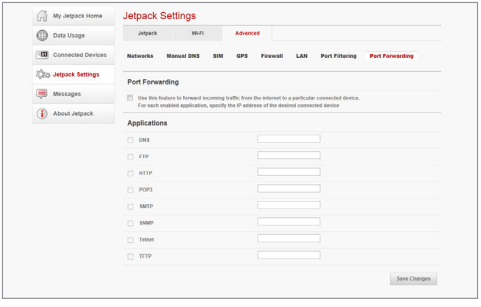


2. The **Port Filtering** allows you to block outgoing internet connections. When the **Port Filtering** is enabled, you must select a port filtering application in the **Applications** to allow that application to connect to the internet.
3. Enable each port filtering application that are needed to access the internet.
4. Click **Add Custom Application** to define and enable custom port filtering application. You need to know details of the traffic used by the applications you wish to add.
5. Enter the **Application name, Start port** and **End port**. Then select the protocol used by port range.
6. Click **Save Changes**.

Port Forwarding

Port Forwarding allows remote devices to connect to a specific computer within a private LAN.

1. Click **Jetpack Settings** > **Advanced** > **Port Forwarding**.



2. The **Port Forwarding** allows you to forward incoming traffics from the Internet to a particular connected computer or device that are connected to the wireless network of the Jetpack.
3. Click **Save Changes**.

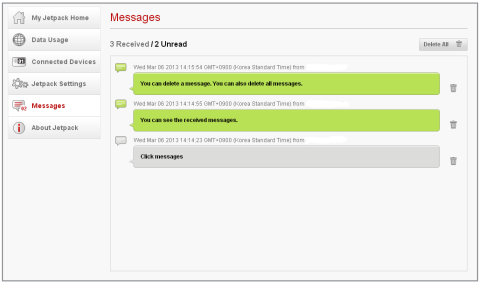
Note

The **Port Forwarding** and DMZ features cannot be used simultaneously.

Messages

Messages display SMS messages sent to you and includes counters for the total number of messages and new messages.

1. Click **Messages**.



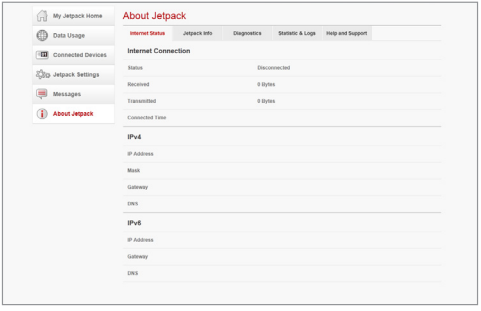
2. You can see the received messages.
3. Click to delete a message. You can also click **Delete All** to delete all messages.

About Jetpack

About Jetpack allows you to view detailed device specific information about your MHS291L.

Internet Status

1. Click **About Jetpack** > **Internet Status**.



2. You can see the detailed information about current internet status.

Jetpack Info

The Jetpack Info page contains detailed information about the MHS291L.

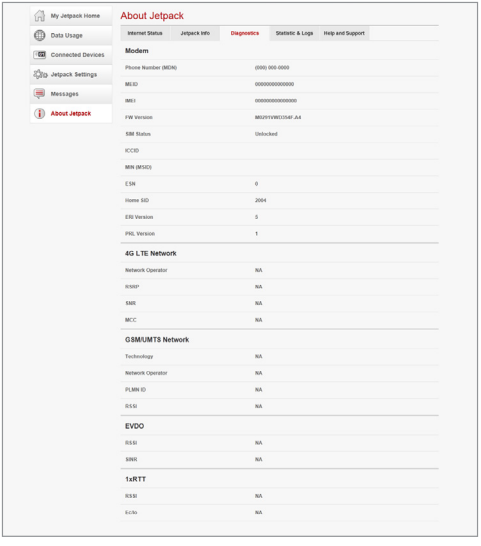
1. Click **About Jetpack** > **Jetpack Info**.

2. You can see the detailed information about the Jetpack.

Diagnostics

The Diagnostics page shows information about the MHS291L information.

1. Click **About Jetpack** > **Diagnostics**.

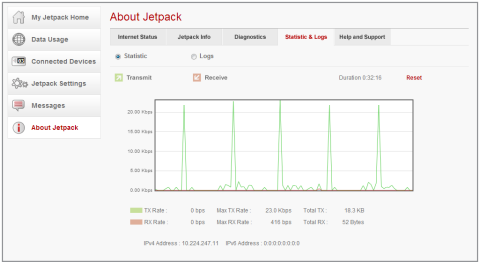


2. You can see the information about the Jetpack firmware and other system-level information. This screen is used mostly for troubleshooting and is not required for normal operation.

Statistic & Logs

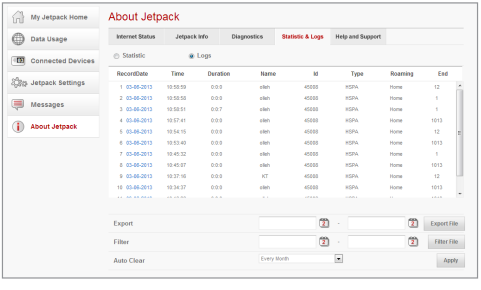
The Logs page allows you to enable or disable logs and to delete system logs.

1. Click **About Jetpack** > **Statistic & Logs** > **Statistic**.



2. You can see the data usage statistics. Click **Reset** to reset the statistics.

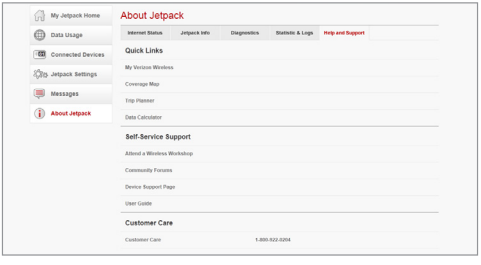
3. Click **About Jetpack** > **Statistic & Logs** > **Logs**.



4. You can see detailed usage logs.
   - **Export**: To export a log file, click and select start date and end date. Then click **Export File**.
   - **Filter**: To review the log for specified time period, click and select start date and end date. Then click **Filter File**.
   - **Auto Clear**: To change the period of time that system log is deleted, select a option from **Auto Clear** drop-down list and then click **Apply**.

Help and Support

1. Click **About Jetpack** > **Help and Support**.



2. It provides you contact information and useful links to use the Jetpack.

Troubleshooting

Windows XP(SP3)

Symptom 1

The RNDIS device no longer works correctly. For example, the data application on the computer may report an error that the data transmission has failed. To resolve this problem, you have to restart the computer.

Resolution

Consider the following scenario:

- A Remote Network Driver Interface Specification (RNDIS) device is installed on a Windows XP-based computer, such as a USB radio device.
- You perform a surprise removal of the RNDIS device from the computer.
- You attach the RNDIS device to the computer again.

Please proceed by installing the Microsoft Hotfix located at the following Web site:
http://support.microsoft.com/kb/959765

Windows Vista(SP2)

Symptom 1

A bus driver that manages a Network Driver Interface Specification (NDIS) miniport is not loaded as expected. Therefore, a yellow exclamation mark (!) appears in Device Manager next to the device that is driven by the miniport. The driver also displays error code 38 (CM_PROB_DRIVER_FAILED_PRIOR_UNLOAD).
For example, this problem may occur on a bus driver that manages a USB composite device that includes a network adapter.

Resolution

Consider the following scenario:

- You are running a Windows Vista-based computer.
- You resume the computer from standby.

Please proceed by installing the Microsoft Hotfix located at the following Web site:
http://support.microsoft.com/kb/948278

Windows 7 / Vista(SP2)

Symptom 1

The communication between the modem and the computer stops. Additionally, a yellow exclamation mark (!) appears next to the device name in Device Manager.

Resolution

Consider the following scenario:

- You have a computer that is running Windows 7, Windows Server 2008 R2, Windows Vista or Windows Server 2008.
- You attach a USB Remote Network Driver Interface Specification (RNDIS) device to the computer through an external USB hub.
- You remove the modem from the USB hub and then reattach.

Please proceed by installing the Microsoft Hotfix located at the following Web site:
http://support.microsoft.com/kb/2477042

Symptom 2

The NDIS device is not completely removed from the fault-tolerant system. The fault-tolerant system cannot fail over to another NDIS device. Therefore, the system is in a non-redundant state.

Resolution

Consider the following scenario:

- You use a fault-tolerant system that is running Windows Server 2008 R2 or Windows 7.
- You suddenly remove a Network Driver Interface Specification (NDIS) device from the system.

Please proceed by installing the Microsoft Hotfix located at the following Web site:
http://support.microsoft.com/kb/2471472

Windows 7

Symptom 1

Windows does not load the WWAN adapter driver. Additionally, you receive an error message that resembles the following:
Windows cannot load the device driver for this hardware because a previous instance of the device driver is still in memory.

Resolution

Consider the following scenario:

- You have a Windows 7-based or Windows Server 2008 R2-based computer that uses a third-party Wireless Wide Area Network (WWAN) adapter.
- You plug a SIM card into the WWAN adapter and then connect to the network by using the adapter.
- You put the computer into sleep mode.
- You remove the SIM card from the WWAN adapter, and then you plug the SIM card back into the adapter.
- You resume the computer from sleep mode.

Please proceed by installing the Microsoft Hotfix located at the following Web site:
http://support.microsoft.com/kb/2688892

Glossary

- **1X** — Internet at 1/10 the speed of EV-DO.
- **3G** — Third Generation. 3G refers to the third generation of mobile telephony technology.
- **4G LTE** — Fourth Generation. 4G LTE refers to the fourth generation of mobile telephony technology.
- **802.11 (a, b, g, n)** — A set of WLAN communication standards in the 2.4, 3.6 and 5 GHz frequency bands.
- **bps** — Bits per second. The rate of data flow.
- **Broadband** — High-capacity high-speed transmission channel with a wider bandwidth than conventional modem lines.
- **CDMA** — Code Division Multiple Access. It is the underlying channel access method used by some mobile phone standards.
- **DHCP** — Dynamic Host Configuration Protocol. Software found in servers and routers that automatically assigns temporary IP addresses to clients logging into an IP network.
- **DHCP Server** — A server or service with a server that assigns IP addresses.
- **DNS** — Domain Name System. A system for converting host names and domain names into IP addresses on the Internet or on local networks that use the TCP/IP protocol.
- **EDGE** — Enhances Data rates for GSM Evolution. A digital mobile phone technology that allows improved data transmission rates as a backward-compatible extension of GSM.

- **GSM** — A computer program embedded in an electronic device. Firmware usually contains operating code for the device.
- **Hotspot** — A Wi-Fi (802.11) access point or the area covered by an access point. Used for connecting to the Internet.
- **HTTP** — Hypertext Transfer Protocol. An application-level protocol for accessing the World Wide Web over the Internet.
- **IP** — Internet Protocol. The mechanism by which packets are routed between computers on a network.
- **IP Type** — The type of service provided over a network.
- **IP address** — Internet Protocol address. The address of a device attached to an IP network (TCP/IP network).
- **Kbps** — Kilobits per second. The rate of data flow.
- **LAN** — Local Area Network. A type of network that lets a group of computers, all in close proximity (such as inside an office building), communicate with one another. It does not use common carrier circuits though it can have gateways or bridges to other public or private networks.
- **MAC Address** — Media Access Control. A number that uniquely identifies each network hardware device. MAC addresses are 12-digit hexadecimal numbers. This is also known as the physical or hardware address.
- **Mbps** — Megabits per second.
- **Network Technology** — The technology on which a particular network provider's system is built; such as CDMA or EVDO.
- **Port** — A virtual data connection used by programs to exchange data. It is the endpoint in a logical connection. The port is specified by the port number.

- **Port Forwarding** — A process that allows remote devices to connect to a specific computer within a private LAN.
- **Port Number** — A 16-bit number used by the TCP and UDP protocols to direct traffic on a TCP/IP host. Certain port numbers are standard for common applications.
- **Protocol** — A standard that enables connection, communication, and data transfer between computing endpoints.
- **Proxy** — A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it.
- **Router** — A device that directs traffic from one network to another.
- **SIM** — Subscriber Identification Module. Found in LTE and GSM network technology, the SIM is a card containing identification information for the subscriber and their account. The SIM card can be moved to different devices.
- **SSID** — Service Set IDentifier. The name assigned to a Wi-Fi network.
- **TCP/IP** — Transmission Control Protocol/Internet Protocol. The set of communications protocols used for the Internet and other similar networks.
- **USB** — Universal Serial Bus. A connection type for computing device peripherals such as a printer, mobile modem, etc. USB connectors may be used for data transfer or charging.

- **USB Port Types** — The USB ports on computers and hubs have a rectangular Type A socket, and peripheral devices have a cable with a Type A plug. Peripherals that do not have an attached cable have a square Type B socket on the device and a separate cable with a Type A and Type B plug. Ports and connectors are available in different sizes (for example, standard, mini, and micro).
- **VPN** — Virtual Private Network. A secure private network that runs over the public Internet. Commonly used to connect to an office network from elsewhere.
- **WCDMA** — Wideband Code Division Multiple Access. An air interface standard found in 3G mobile telecommunications networks. The most-commonly used member of the UMTS family.
- **WWAN** — Wireless Wide Area Network. A public network that extends beyond architectural, geographical, or political boundaries (unlike a LAN, which is usually a private network located within a room, building, or other limited area).
- **WEP** — Wired Equivalent Privacy. An IEEE standard security protocol for 802.11 networks. Superseded by WPA and WPA2.
- **WPA/WPA2** — Wi-Fi Protected Access. A security protocol for wireless 802.11 networks from the Wi-Fi Alliance.

Safety and Warranty

Regulatory Notices

MHS291L complies with Parts 15, 22, 24, and 27 of the FCC rules. This mobile hotspot must not be co-located or operated in conjunction with any other antenna or transmitter. If you use this mobile hotspot in any other configuration, the FCC RF Exposure compliance limit can be exceeded.

Warnings and Cautions

- Modifying or changing this mobile hotspot without express authorization can nullify compliance with RF exposure guidelines.
- This mobile hotspot has been tested and found to comply with the limits pursuant to Part 15, 22, 24, and 27 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when appropriately installed. This mobile hotspot generates, uses, and can radiate radio frequency and, if not installed and used according to the instructions provided, it may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in any particular installation.
- If this mobile hotspot does cause harmful interference with radio or television signals (determine this by turning the mobile hotspot off and on), attempt to correct the interference by trying one or more of the following:

- Increase the separation between the mobile hotspot and receiver.
- Connect the mobile hotspot into a different outlet than the receiver.
- Consult the dealer or an experienced radio/TV technician for help.

- This mobile hotspot does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference causing equipment standard entitled "Digital Apparatus", ICES-003 of the Department of Communications.
- If you have purchased this product under a United States Government contract, it shall be subject to restrictions as set forth in subparagraph (C)(1)(ii) of Defense Federal Acquisitions Regulations (DFARs) Section 252.227-7013 for Department of Defense contracts, and as set forth in Federal Acquisitions Regulations (FARs) Section 52.227-19 for civilian agency contracts or any successor regulations. If further government regulations apply, it is your responsibility to ensure compliance with such regulations.
- Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instruction.
- The failure to use approved batteries and chargers may increase the risk of your Jetpack to overheat, catch fire, or explode, resulting in serious bodily injury, death, or property damage. To avoid risk of explosion, never dispose the batteries in a fire.

Warning

- This product contains a chemical known to the State of California to cause cancer.
- This product contains a chemical known to the State of California to cause birth defects or other reproductive harm.

Product Handling

- Keep the mobile hotspot in a dry and clean place. Keep your device away from liquids, dust and excessive heat.
- Storage temperature: -22˚F to 140˚F (-30˚C to 60˚C)
- Operating temperature: -22˚F to 140˚F (-30˚C to 60˚C)
- This device may cause harmful interference, and must accept any interference received, including interference that may cause undesirable operations.

Caring for Your Device

Like any electronic device, the mobile hotspot must be handled with care to ensure reliable operation.

The following guidelines are recommended:

- Protect the mobile hotspot from liquids, dust, and excessive temperatures.
- Do not apply adhesive labels to the Jetpack; they might cause the Jetpack to potentially overheat and they might alter the performance of the antenna.
- Store the mobile hotspot in a safe place when not in use.

Safety Information for Mobile Hotspot

READ THIS INFORMATION BEFORE USING YOUR MOBILE HOTSPOT

Exposure to radio frequency signals

Your mobile hotspot is a low power radio transmitter and receiver. When it is ON, it receives and also sends out radio frequency (RF) signals. In August 1996, the Federal Communications Commissions (FCC) adopted RF exposure guidelines with safety levels for mobile hotspot. Those guidelines are consistent with the safety standards previously set by both U.S. and international standards bodies:

* ANSI C95.1 (1992)

** NCRP Report 86 (1986)

*** ICNIRP (1996)

Those standards were based on comprehensive and periodic evaluations of the relevant scientific literature. For example, over 120 scientists, engineers, and physicians from universities, government health agencies, and industry reviewed the available body of research to develop the ANSI Standard (C951).

The design of your device complies with the FCC guidelines (and those standards).

* American National Standards Institute.

** National Council on Radiation Protection and Measurements.

*** International Commission on Nonionizing Radiation Protection.

Antenna safety

Use only the approved replacement antenna. Unauthorized antennas, modifications, or attachments could result in violation of FCC regulations. Please contact your local dealer for replacement antenna.
Do not use the mobile hotspot with a damaged antenna. If a damaged antenna comes into contact with the skin, a minor burn may result. Please contact your local dealer for replacement antenna.

Electronic devices

Your mobile hotspot is a low power radio transmitter and receiver. When it is ON, it receives and also sends out radio frequency (RF) signals. Most modern electronic equipment is shielded from RF energy. However, certain electronic equipment may not be shielded against the RF signals from your mobile hotspot. Therefore, use of your device must be restricted in certain situations.

Pacemakers

The Health Industry Manufacturers Association recommends that a minimum of six inches (6") separation must be maintained between a mobile hotspot and a pacemaker to avoid potential interference with the pacemaker. These recommendations are consistent with the independent research by and recommendations of Wireless Technology Research. Persons with pacemakers:

- ALWAYS keep the mobile hotspot more than six inches from your pacemaker when the mobile hotspot is turned on.

- If you have any reason to suspect that interference is taking place, turn your mobile hotspot OFF immediately.

Other medical devices

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 physician may be able to assist you in obtaining this information. Turn your mobile hotspot OFF in 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.

Vehicles

RF signals may affect improperly installed or inadequately shielded electronic systems in motor vehicles. Check with the manufacturer or its representative regarding your vehicle. You should also consult the manufacturer of any equipment that has been added to your vehicle.

Posted facilities

Turn your device OFF where posted notices require so.

Other safety guidelines

Aircraft

FCC regulations prohibit using your device while in the air. Turn your device OFF before boarding an aircraft. Always request and obtain prior consent and approval of an authorized airline representative before using your device aboard an aircraft. Always follow the instructions of the airline representative whenever using your device aboard an aircraft to prevent any possible interference with airborne electronic equipment.

Blasting areas

To avoid interfering with blasting operations, turn your device OFF when in a "blasting area" or in areas posted: "Turn off two-way radio." Obey all signs and instructions.

Potentially explosive atmospheres

Turn your device OFF when in any area with a potentially explosive atmosphere and obey all signs and instructions. Sparks in such areas could cause an explosion or fire resulting in bodily injury or even death.

Areas with a potentially explosive atmosphere are often, but not always, clearly marked. They include fueling areas such as gas stations; below deck on boats; fuel or chemical transfer or storage facilities; vehicles using liquefied petroleum gas (such as propane or butane); areas where the air contains chemicals or particles, such as grain, dust, or metal powders; and any other area where you would normally be advised to turn off your vehicle's engine.

Precautions

Your mobile hotspot is a high quality piece of equipment. Before operating, read all instructions and cautionary markings in the User Guide.

- DO NOT use this equipment in an extreme environment where high temperature or high humidity exists.
- DO NOT abuse the equipment. Avoid striking, shaking or shocking. When not using, lay down the unit to avoid possible damage due to instability.
- DO NOT expose this equipment to rain or spilled beverages.
- DO NOT use unauthorized accessories.
- DO NOT disassemble the device. If service or repair is required, return unit to an authorized service center. If unit is disassembled, the risk of electric shock or fire may result.
- Data transmission and reception cannot be guaranteed because of the nature of wireless communications. Data can be delayed, corrupted or lost during transmission. Even though it is quite rare that significant data delay or loss occurs if the USB device is used in a normal manner, this USB device should not be used in cases that data transmission or reception failure could result in damage of any kind to the user or another party, including but not limited to personal injury, death or loss of personal property. Personal Communications Devices, LLC., bears no responsibility for damages or losses of any kind resulting from delays or errors in data transmission using the mobile hotspot, or for failure of the mobile hotspot to transmit or receive such data.

Safety Information for FCC RF Exposure

WARNING! READ THIS INFORMATION BEFORE USING

CAUTIONS

In August 1996 the Federal Communications Commission (FCC) of the United States with its action in Report and Order FCC 96-326 adopted an updated safety standard for human exposure to radio frequency electromagnetic energy emitted by FCC regulated transmitters. Those guidelines are consistent with the safety standard previously set by both U.S. and international standards bodies. The design of this mobile hotspot complies with the FCC guidelines and these international standards.

Body-worn operation

This device was tested in multiple computer configurations with USB port configurations for typical near-body operations with the back of the mobile hotspot kept 10 mm from body. To maintain compliance with FCC RF exposure requirements it can be used in computers with substantially similar physical dimensions, construction, and electrical and RF characteristics, and that maintain a minimum 10 mm separation distance between the user's body and the back of the mobile hotspot, including the antenna. The antenna(s) used for this device must not be co-located or must not operate in conjunction with any other antenna or transmitter within a host device.

* CE: The Body SAR tests has been performed at 15 mm.

Note

For more information about RF exposure please visit the FCC website at www.fcc.gov.

SAR Information

THIS MODEL MEETS THE GOVERNMENT'S REQUIREMENTS AND EUROPEAN UNION (EU) STANDARDS FOR EXPOSURE TO RADIO WAVES.

Your mobile hotspot is a radio transmitter and receiver. It 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. These limits are part of comprehensive guidelines and establish permitted levels of RF energy for the general population. The guidelines are based on standards that were developed by independent scientific organizations through periodic and thorough evaluation of scientific studies. The standards include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

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* and EU standards is 2.0 W/ kg. Tests for SAR are conducted 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.

Before a device model is available for sale to the public, it must be tested and certified to the FCC that it does not exceed the limit established by the government adopted requirement for safe exposure. The tests are performed in positions and locations (e.g.,

at the ear and worn on the body) as required by the FCC for each model. The highest SAR value for this model device when tested for use when worn on the body, as described in this user guide, and for simultaneous transmission, uses the conditions of both 1.52 W/kg, and 1.54 W/kg respectively. (Body-worn measurements differ among device models, depending upon available accessories and FCC requirements). While there may be differences between the SAR levels of various devices and at various positions, they all meet the government requirement for safe exposure. The FCC has granted an Equipment Authorization for this model device with all reported SAR levels evaluated as in compliance with the FCC RF exposure guidelines. SAR information on this model is on file with the FCC and can be found under the Display Grant section of http://www.fcc.gov/oet/fccid after searching on FCC ID: **JYCORBIT**.

Additional information on Specific Absorption Rates (SAR) can be found on the Cellular Telecommunications Industry Association (CTIA) web-site at http://www.ctia.org.

* In the United States and Canada, the SAR limit for mobile phones used by the public is 1.6 watts/kg (W/kg) averaged over one gram of tissue. The standard incorporates a substantial margin of safety to give additional protection for the public and to account for any variations in measurements.
* CE Max SAR : 0.898 W/Kg.

The Declaration of Conformity at the back of this guide demonstrates your device's compliance with the European Radio & Terminal Telecommunications Equipment (R&TTE) directive.

FCC Compliance Information

This device complies with Part 15 of 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.

Information to the user

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the mobile hotspot into a different outlet than the receiver.
- Consult the dealer or an experienced radio/TV technician for assistance.

CAUTION

Changes or modifications that are not expressly approved by the responsible party of Compliance could void the user's authority to operate the equipment.

12-Month Limited Warranty

Personal Communications Devices, LLC. (the "Company") warrants to the original retail purchaser of this mobile hotspot, that should this product or any part thereof during normal consumer usage and conditions, be proven defective in material or workmanship that results in product failure within the first twelve (12) month period from the date of purchase, such defect(s) will be repaired or replaced (with new or rebuilt parts) at the Company's option, without charge for parts or labor directly related to the defect(s).

The antenna, keypad, display, rechargeable battery and battery charger, if included, are similarly warranted for twelve (12) months from date of purchase.

This Warranty extends only to consumers who purchase the product in the United States or Canada and it is not transferable or assignable.

This Warranty does not apply to:

(a) Product subjected to abnormal use or conditions, accident, mishandling, neglect, unauthorized alteration, misuse, improper installation or repair or improper storage;

(b) Product whose mechanical serial number or electronic serial number has been removed, altered or defaced.

(c) Damage from exposure to moisture, humidity, excessive temperatures or extreme environmental conditions;

(d) Damage resulting from connection to any accessory or other product that are not approved by the Company;
(e) Defects in appearance, cosmetic, decorative or structural items such as framing and nonoperative parts;
(f) Product damaged from external causes such as fire, flooding, dirt, sand, weather conditions, battery leakage, blown fuse, theft or improper usage of any electrical source.

The Company disclaims liability for removal or reinstallation of the product, for geographic coverage, for inadequate signal reception by the antenna or for communications range or operation of the cellular system as a whole.

When sending your wireless device to Personal Communications Devices for repair or service, please note that any personal data or software stored on the device may be inadvertently erased or altered. Therefore, we strongly recommend you make a back up copy of all data and software contained on your device before submitting it for repair or service. This includes all contact lists, downloads (i.e. third-party software applications, ringtones, games and graphics) and any other data added to your device. In addition, if your wireless device utilizes a SIM or Multimedia card, please remove the card before submitting the device and store for later use when your device is returned, Personal Communications Devices is not responsible for and does not guarantee restoration of any third-party software, personal information or memory data contained in, stored on, or integrated with any wireless device, whether under warranty or not, returned to Personal Communications Devices for repair or service.

To obtain repairs or replacement within the terms of this Warranty, the product should be delivered with proof of Warranty coverage

(e.g. dated bill of sale), the consumer's return address, daytime phone number and/or fax number and complete description of the problem, transportation prepaid, to the Company at the address shown below or to the place of purchase for repair or replacement processing. In addition, for reference to an authorized Warranty station in your area, you may telephone in the United States (800) 229- 1235, and in Canada (800) 465-9672 (in Ontario call 416-695-3060).

THE EXTENT OF THE COMPANY'S LIABILITY UNDER THIS WARRANTY IS LIMITED TO THE REPAIR OR REPLACEMENT PROVIDED ABOVE AND, IN NO EVENT, SHALL THE COMPANY'S LAIBILITY EXCEED THE PURCHASE PRICE PAID BY PURCHASER FOR THE PRODUCT.

ANY IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, SHALL BE LIMITED TO THE DURATION OF THIS WRITTEN WARRANTY. ANY ACTION FOR BREACH OF ANY WARRANTY MUST BE BROUGHT WITHIN A PERIOD OF 18 MONTHS FROM DATE OF ORIGINAL PURCHASE. IN NO CASE SHALL THE COMPANY BE LIABLE FOR AN SPECIAL CONSEQUENTIAL OR INCIDENTAL DAMAGES FOR BREACH OF THIS OR ANY OTHER WARRANTY, EXPRESS OR IMPLIED, WHATSOEVER. THE COMPANY SHALL NOT BE LIABLE FOR THE DELAY IN RENDERING SERVICE.

UNDER THIS WARRANTY OR LOSS OF USE DURING THE TIME THE PRODUCT IS BEING REPAIRED OR REPLACED.

No person or representative is authorized to assume for the Company any liability other than expressed herein in connection with the sale of this product.

Some states or provinces do not allow limitations on how long an implied warranty lasts or the exclusion or limitation of incidental or consequential damage so the above limitation or exclusions may not apply to you. This Warranty gives you specific legal rights, and you may also have other rights, which vary from state to state or province to province.

IN USA:
Personal Communications Devices
1516 Motor Parkway
Hauppauge, New York 11749
www.pcdphones.com

IN CANADA:
Personal Communications Devices, LLC
5535 Eglinton Avenue West, Suite 210
Toronto, Ontario
M9C 5K5
www.pcdphones.com